# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-1.htm



## 1.0 Layer 3 technologies

### 1.1 Troubleshoot administrative distance (all routing protocols)

**The default administrative distances are as below:**

Directly connected : 0

Directly connected : 0

Enhanced Interior Gateway Routing Protocol (EIGRP) summary route : 5

EIGRP (internal) : 90

OSPF : 110

RIP : 120

External BGP : 20

Internal BGP : 200

Unreachable : 255

The default metric for a redistributed route should be set to a value larger than the largest metric within the AS.

The proper command to set a different administrative distance is distance <admin-distance> {ip-address {wildcard-mask}}

example: distance 150 10.1.1.0 0.0.0.255

The command "distance 99 0.0.0.0 255.255.255.255 11" is used to assign an administrative distance of 99 for all routes matching access list 11 from any router.

The router will assign an administrative distance as specified in the command instead of the default AD to routes learned through this ip address. The ip-address and wildcard-mask refers to the IP address of the router from which the routes are being learned. This command is very useful when you want to assign different AD for redistributed routes into RIP from other protocols. In the example, a AD of 150 is assigned to the routes specified. This distance command should not be confused with route metrics that are used by the various routing protocols - RIP, EIGRP, OSPF, ISIS, etc.

**Static Routing:** It may be implemented in either one of two ways by using ip route command:

**1. By using the next-hop address :** Ex: Router(config)#ip route 192.204.1.64 255.255.255.240 192.204.1.2

192.204.1.64 = destination network
255.255.255.240 = subnet mask
192.204.1.2 = next-hop address

Remember this by reading as: To get to the destination network of 192.204.1.64, with a subnet mask of 255.255.255.240, send all packets to 192.204.1.2

**2. By using the exit interface :** Router(config)#ip route 192.204.1.64 255.255.255.240 s0/0

192.204.1.64 = destination network
255.255.255.240 = subnet mask
s0/0 = exit interface

Remember this by reading as: To get to the destination network of 192.204.1.64, with a subnet mask of 255.255.255.240, send all packets out interface Serial 0/0

Remember this by reading as: To get to the destination network of 192.204.1.64, with a subnet mask of 255.255.255.240, send all packets out interface Serial 0/0

Router(config)# ip route A.B.C.D (destination network/host) A.B.C.D (subnet mask) A.B.C.D (next hop)

You can also use the port identifier such as e0, s1 etc. to define the next hop address.

Optionally, the "administrative distance " can be added at the end of the command to change the default weight.

The correct syntax for setting default route is

**Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1**

You can also set default route by specifying the interface as below:

**Router(config)#ip route 0.0.0.0 0.0.0.0 s0**

**Distance Vector routing protocols** use frequent broadcasts (255.255.255.255 or FF:FF:FF:FF) of their entire routing table every 30 sec. on all their interfaces in order to communicate with their neighbors. The bigger the routing tables, the more broadcasts. This methodology limits significantly the size of network on which Distance Vector can be used. Routing Information Protocol (RIPv1 and RIPv2) and Interior Gateway Routing Protocol (IGRP and EIGRP) are two popular Distance Vector routing protocols.

**Link state routing protocols** maintain complete road map of the network in each router running a link state routing protocol. Each router running a link state routing protocol originates information about the router, its directly connected links, and the state of those links. This information is sent to all the routers in the network as multicast messages. Link-state routing always try to maintain full networks topology by updating itself incrementally whenever a change happen in network. Examples of Link State protocol is OSPF (Open Shortest Path First) and IS-IS. Link State Routing Protocols converge more quickly and they are less prone to Routing Loops than Distance Vector Routing Protocols. On the other hand, Link State Routing Protocols require more CPU power and memory than Distance Vector Routing Protocol algorithms.

**A Floating static route** is a route that has a higher administrative distance than the current route in a routing table. The routes that have a lower administrative distance number will be the ones installed into the routing table whereas higher AD numbers will not. Static floating route is static route like any other but with added administrative distance in the configuration The Administrative Distance of a static route can be changed to form a floating static route, which will only be used if there are no other routes with a lesser AD in the routing table. A floating static route is often used as a backup route to a dynamic routing protocol.

To create a floating static route, we need to use the distance option at the end of the ip route command. We really just need to set an AD for the static route.

**There are three ways a router learns how to forward a packet:**

**1. Static Routes** - Configured by the administrator manually. The administrator must also update the table manually every time a change to the network takes place. Static routes are commonly used when routing from a network to a stub (a network with a single route) network.  The command is

ip route network mask address/interface [distance]

ex: ip route 165.44.34.0 255.255.255.0 165.44.56.5

Here, 165.44.34.0 is the destination network or subnet

255.255.255.0 is the subnet mask

165.44.56.5 is the default gateway.

**2. Default Routes** - The default route (gateway of last resort) is used when a route is not known or is infeasible. The command is

ip route 0.0.0.0 0.0.0.0 165.44.56.5

The default gateway is set to 165.44.56.5

**3. Dynamic Routes** - As soon as dynamic routing is enabled, the routing tables are automatically updated. Dynamic routing uses broadcasts and multicasts to communicate with other routers. Each route entry includes a subnet number, the interface out to that subnet, and the IP address of the next router that should receive the packet. The commands to enable rip are:

router rip
network <major network number>.

## 1.2 Troubleshoot route map for any routing protocol (attributes, tagging, filtering)

When configuring route map, the match and set route map configuration commands are used to define the condition portion of a route map. The match command specifies a criteria that must be matched, and the set command specifies an action that is to be performed if the routing update meets the condition defined by the match command. Here the sequence number of 10 is used. Route map starts with the lowest sequence number and go on with increasing sequence numbers (if exists) till a match is occurred. Once a match occurs, it stops there and performs the match/set statements on the route. If no match occurs, there is an implicit deny at the end and the route is not redistributed or controlled.

Packets originated by the router are not policy routed. There is a feature for policy routing of locally generated traffic through local PBR. Local PBR policies are applied to the router with the global configuration command

**ip local policy** *route-map-name*

The command ip policy route-map route-map-name used to apply the route map to the inbound interface. Configure the route map by using the command route-map route-map-name [permit | deny] [sequence-number]

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-2.htm



## 1.0 Layer 3 technologies

### 1.3 Troubleshoot loop prevention mechanisms (filtering, tagging, split horizon, route poisoning)

**All the following are possible solutions for preventing routing loops.**

**1. Split Horizon** - Based on the principle that it is not useful to send the information about a route back in the direction from which the information originally came.

**2. Poison Reverse** - A router that discovers an inaccessible route sets a table entry in a consistent state (infinite metric) while the network converges.

**3. Hold-down Timers** - Holddown timers prevent regular update messages from reinstating a route that has gone bad. Here, if a route fails, the router waits a certain amount of time before accepting any other routing information about that route.

**4. Triggered Updates** - Normally, new routing tables are sent to neigbhoring routers at regular intervals (IP RIP every 30 sec / and IPX RIP every 60 sec). A triggered update is an update sent immediately in response to some change in the routing table. Triggered updates along with Hold-down timers can be used effectively to counter routing loops.

**Route summarization is calculated as below:**

Step 1:

1. Take the first IP: 172.24.54.0/24 : 172.24. 0 0 1 1 0 1 1 0.0

2. Take the second IP: 172.24.53.0/24 : 172.24. 0 0 1 1 0 1 0 1.0

Note that we are not really concerned about the octets that have equal decimal values. This is because they don't come into play while calculating summarization route, in this case.

Step 2:

Count the number of bits in the third octet that are aligned (or lined up) with same values. In this case 6 bits are lined up in the third octet. The summarization route is calculated by adding this number (6) to the octets preceding the third (first and second octets).

Therefore, the number of bits in the summarized route is 8+8+6 = 22

Step 3:

Calculate the decimal equivalent for third octet with 6 bits as given in the matching binary. That is 0 0 1 1 0 1 x x. Note x is because it corresponds to non matching binary number. It is equal to 128*0 + 64*0 + 32*1 + 16*1 + 8*0 + 4*1 or 32+16+4 or 52.

Therefore, the summarized route is: 172.24.52.0/22

**Poison Reverse** -When a router advertises a poisoned route to its neighbors, its neighbors break the rule of split horizon and send back to the originator the same poisoned route, with an infinite metric.

**Split Horizon -** If a neighboring router sends a route to a router, the receiving router will not propagate this route back to the advertising router on the same interface.

**Hold-down Timers -** The purpose is to provide the routers enough time to propagate the routes and to ensure that no routing loops occur while propagation occurs

**LSA's** - The packets flooded when a topology change occurs, causing network routers to update their topological databases and recalculate routes.

**IP helper addresses** forward a client broadcast address (such as a DHCP or BOOTP requests) to a unicast or directed broadcast address. Helper-address is required due to the fact that routers do not forward broadcasts. By defining a helper-address, a router will be able to forward a broadcast from a client to the desired server or network. There can be more than one helper-address on a network. The helper-address must be defined on the interface that receives the original client broadcast.

Note that "ip unnumbered" command is used to enable IP processing on a serial interface without assigning a specific IP address to the interface.

The command clear ip route * will clear all dynamically created routes from a routers routing table.

**Hold-down timer:** Helps preventing routing loops during periods when the topology is converging.

**Split Horizon:** Blocks the information about routes from being advertised by any router to the interface from which the information originated.

**Defining a maximum count:** Used for preventing Updates from looping the network indefinitely.

**Route Poisoning:** Advertises an infinite metric for a failed route to all its neighbors.

**Triggered update:** Allows a RIP router to announce route changes almost immediately rather than waiting for the next periodic announcement.

Split horizon is a method of preventing a routing loop in a network. The basic principle is simple: Information about the routing for a particular packet is never sent back in the direction from which it was received.

Normally, routers that are connected to broadcast-type IP networks and that use distance-vector routing protocols employ the split horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. If an interface is configured with secondary IP addresses and split horizon is enabled, updates might not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

To enable or disable split horizon, use the following commands in interface configuration mode, as needed:

**Router(config-if)#ip split-horizon - Enables split horizon.**
**Router(config-if)#no ip split-horizon - Disables split horizon.**

An example of such a situation is when an interface connects to the Internet. You do not want your routing updates to go out to the Internet. In such situations, you can use the passive-interface interface command in the routing configuration mode to stop RIP from sending updates out that interface. This command stop RIP from sending updates but it will continue to receive updates on that interface.

The (config-router)#passive-interface <interface> command stops updates from being sent out an interface, but route updates are still received.

## 1.4 Troubleshoot redistribution between any routing protocols or routing sources

Only classless routing protocols like, RIPv2, EIGRP, and OSPF can support routev summarization. Route summarization is a technique where a router can take a group of subnetworks and summarize them as one network for external advertisement. Route summarization is also known as route aggregation.

The appropriate commands for redistributing OSPF routes in to EIGRP are given below:

**router eigrp** 1
**redistribute ospf 1 metric** *10000 100 255 1 15000*
**passive-interface Ethernet1**
**network** *169.10.0.0*

The metric could be set to default, or specified as required.

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-3.htm



## 1.0 Layer 3 technologies

### 1.5 Troubleshoot manual and auto-summarization with any routing protocol

IP route summarization is used to make networks more flexible and efficient. Although some routing protocols such as RIPv1 and IGRP summarize only at the boundaries of major network numbers, others support route summarization (aggregation) at any bit boundary. Variable-length subnet masks enable routing protocols to summarize on bit boundaries. The following are the advantages to summarizing addresses into a hierarchy:

1. Reduces the amount of information stored in routing tables - Without summarization, a router needs to process every single route in the network. With summarization, routers can condense network addresses down to a single link advertisement, resulting in a reduction in both the resource load on the router and the overall network complexity. Route summarization is most effective in large networks.

2. Allocates an existing pool of addresses more economically - The available IP addresses are limited. Route summarization ensures that IP addresses are utilized efficiently.

3. Makes the routing process more efficient - With less overhead, routers are faster and more efficient.

4. Lowers the network convergence time - The network convergence time would reduce with route summarization.

5. Isolates topology changes - If any individual route changes, the change would be localized. The summary address may remain the same, thus saving unnecessary updates over the network.

6. Facilitates monitoring, reporting, and troubleshooting - A hierarchical address space is relatively easy to monitor and troubleshoot.

The reduction in route propagation and routing information overhead can be significant. Take a sample network of 172.16.1.0 /24. Without summarization, each router in a large enterprise network of 250 subnets (28 = 256 subnets with 28 - 2 = 254 hosts each) would need to know about 250 routes. With route summarization, you can quickly reduce the size of the routing tables by almost 75%. If the 172.16.0.0 Class B network used 7 bits of subnet address space (/23) instead of 8 bits (/24), the original 250 subnets could be broken up into two major subnetworks of about 125 each. Each router would still need to know all the routes for each subnet in its network number. However, that number would be reduced to 125 routes plus one additional route for the other major network. This process of collapsing many subnet routes into a single network route is a fundamental goal of route summarization.

Route Summarization: Route summarization means summarizing a group of routes into a single route advertisement. The net result of route summarization, and its most obvious benefit, is a reduction in the size of routing tables on the network. This in turn reduces the latency associated with each router hop since the average speed for routing table lookup will be increased due to the reduced number of entries. The routing protocol overhead can also be significantly reduced since fewer routing entries are being advertised. This can become critical as the overall network (and hence the number of subnets) grows.

IP Packets are transported from source network to the destination network by what is known as routing. Hop-by-hop routing model is used by the Internet for delivery of packets. At each hop, the destination IP address is examined, the best next hop is determined by the routing protocol (such as RIP, OSPF or BGP) and the packet is forwarded by one more hop through this route. The same process takes place at the next hop. During this process, the logical addresses remain same. In an IP network, the logical addresses are IP addresses. The hardware interface addresses, such as MAC address change with each hop.

# CCNP ENARSI 300-410 Exam Cram Notes



## 1.0 Layer 3 technologies

### 1.8 Describe Bidirectional Forwarding Detection

BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable.

BFD (Bidirectional Forwarding Detection) is basically another Hello protocol based on UDP that detects link failures on forwarding plane. BFD runs on top of Layer 2 protocols that is in use between two adjacent systems.

BFD mechanism is independent from media, routing protocols and data protocols. By being independant from media, routing protocols and data protocols, BFD mechanism can be used with all routing protocols and data protocols. BFD mechanism is over these protocols.

Routing protocols has an hello mechanism by default to detect the link failures. But this mechanism is differenciate from router to router. With BFD mechanims, a common link failure detection mechanism created. And this BFD mechanism can be used with all routing protocols. Using BFD mechanism provides a very fast convergence after a link failure if you compare with routing protocol hello mechanism.

### 1.9 Troubleshoot EIGRP (classic and named mode)

With EIGRP running on a network, the passive-interface command stops both outgoing and incoming routing updates, since the effect of the command causes the router to stop sending and receiving hello packets over that interface.

To prevent routing updates through a specified interface, use the passive-interface type number command in router configuration mode.

Passive interface command is used in all routing protocols to disable sending updates out from a specific interface. However the command behavior varies from one protocol to another.

EIGRP takes metric values if redistribution is taking place from another EIGRP process. In all other cases, metric needs to be set. Otherwise, redistribution will not take place.

In EIGRPv6 , hello packets and updates are sent using multicast transmission and it uses FF02::A for the purpose.

Unlike RIPng and OSPFv3, EIGRPv6 is configured from both global configuration mode and interface configuration mode and also "no shutdown" command is to be issued to enable the command.

The command "ipv6 eigrp <as-number>" enables EIGRP for IPv6 on a specified interface. And the command "ipv6 router eigrp <as-number>" enters router configuration mode and creates an EIGRP IPv6 routing process. The command eigrp router-id <ip-address> enables the use of a fixed router ID. Use this command only if an IPv4 address is not defined on the router eligible for router ID.

**EIGRPv6 involves the following configuration steps:**

Enable IPv6 routing using "ipv6 unicast-routing" command.

Create an EIGRPv6 process using "ipv6 router eigrp <asn>" command.

Assign an EIGRPv6 router ID using the "eigrp router-id <router-id>" command in router configuration mode.

Enable EIGRPv6 on interfaces using the "ipv6 eigrp <asn>" command in interface configuration mode.

EIGRP (as well as IGRP) uses Bandwidth and Delay as default criteria to determine the best path. The description of the terms is given below:

Bandwidth: This is the smallest bandwidth between the source and destination.

Delay: This is the cumulative interface delay along the path.

Reliability: This is the worst case reliability between source and destination based on keepalives.

Loading: This is the worst case load on a link between source and destination based on bps.

MTU: Smallest MTU in path.

**The following are the key points that you may need to remember with respect to forming neighbor relationship in EIGRP-IPV6:**

The interfaces must be in up-up state. (true for both ipv6 and ipv4)

Ipv6 addresses need not be in the same subnet for forming neighbor relationship. Note that in EIGRP ipv4, the neighbor interfaces should be on the same subnet.

Both devices should use the same Autonomous System Number (ASN).

ACLs should not be filtering routing messages. This is true for ipv4 also.

Must be able to pass routing protocol authentication, if configured. This is true for ipv4 also. K values must match (true for ipv4 also)

Hello and Hold timers need NOT match (for both ipv4 and ipv6)

**The following command starts EIGRP routing process:**

Router(config)# router eigrp <Autonomous System Number>

The Autonomous System Number should be same the on all routers.

EIGRP uses multicasts to send queries to neighbor routers. EIGRP Hello packets are multicast to 224.0.0.10.

Typical show ip eigrp topology output is given below:

**R1#show ip eigrp topology**

IP-EIGRP Topology Table for process 77

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status

P 192.168.10.0 255.255.255.0, 1 successors, FD is 0 via 172.24.1.2 (46277376/46251776), Serial0

DUAL (Diffusing Update Algorithm) used by EIGRP tracks all the routes advertised by neighbors and selects routes based on feasible successors. It inserts lowest cost paths into the routing table (these routes are known as primary routes or successor routes).

EIGRP has certain features that belong to link-state algorithms (like OSPF) than distance-vector algorithms. Ex: EIGRP sends a partial routing table update, which includes just routes that have been changed, not the full routing table like distance-vector algorithms.

The feasible successor route will become the primary route when its advertised distance is higher than the feasible distance of the successor route. The feasible successor is kept in the topology table as a backup route and can be used in the event that the successor route goes down.

**The features of EIGRP are:**

Support VLSM, route summarization, and routing update authentication.

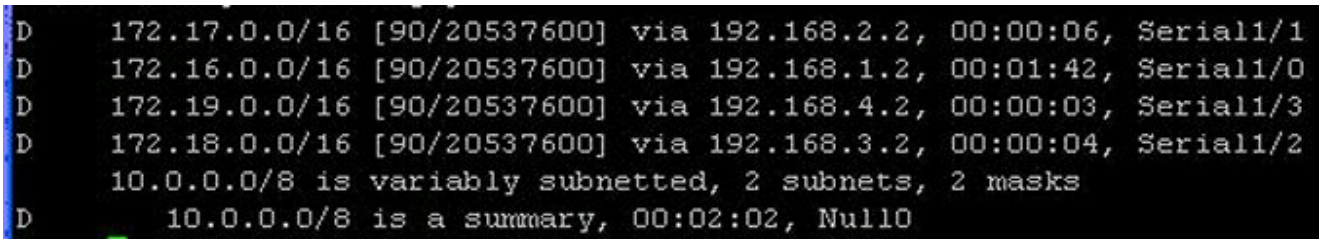
EIGRP uses a distributed algorithm called DUAL when a route fails and has no feasible successor to discover a replacement for a failed route. When a new route is found, DUAL adds it to the routing table.

**To turn off automatic summarization, use the command,**

**router(config-router)#no auto-summary**

Please note that EIGRP automatically summarizes routes at classful boundary (I.e. the network boundary), unless otherwise specified.

EIGRP uses auto summarization of routes at major network boundaries. The exhibit shows the output of the command: show IP route EIGRP.




**The following are main features of route summarization in EIGRP:**

1. By default, EIGRP summarizes routes at the major network boundaries (classful boundaries).

2. To enable summarization at any level other than major network boundary, you need to disable auto summarization using the command: "No auto-summary"

3. The following command enables summarization at an arbitrary network boundary: "Ip summary-address <as-number> <address-mask>"

Note that you need to specify the IP address and routing mask of the summary route. No need to specify the metrics.

4. Successor: A route (or routes) selected as the primary route(s) used to transport packets to reach destination. Note that successor entries are kept in the routing table of the router.

5. Feasible successor: A route (or routes) selected as backup route(s) used to transport packets to reach destination. Note that feasible successor entries are kept in the topology table of a router. There can be up to 6 (six) feasible successors for IOS version 11.0 or later. The default is 4 feasible successors.

6. DUAL (Diffusing Update Algorithm): Enhanced IGRP uses DUAL algorithm to calculate the best route to a destination.

7. Unlike RIP and IGRP, EIGRP updates are not periodic. EIGRP updates are sent only when there is a topological change in the network.

8. In EIGRP, the router doing the summarization will build a route to null0 for the summarized address. This ensures that the packets that are not destined for any network are routed to null and thus dropped.

9. EIGRP provides the option of disabling route summarization. The command no auto-summary can be used for this purpose. This option is not available in RIP and IGRP.You can summarize routes in EIGRP at any arbitrary bit boundary

**Neighbor relationship and authentication**

The EIGRP neighbor table includes the following key elements:

1.Neighbor Address: IP address of neighbor router interfaces

2.H (Handle): Here you will find the order when the neighbor adjacency was established. Your first neighbor will have a value of 0, the second neighbor a value of 1 and so on.

3.Hold Uptime (sec): This is the holddown timer per EIGRP neighbor. Once this timer expires we will drop the neighbor adjacency. The default holddown timer is 15 seconds. On older IOS versions only a hello packet would reset the holddown timer but on newer IOS versions any EIGRP packet after the first hello will reset the holddown timer.

4.SRTT (Smooth round-trip time): The number of milliseconds it takes to send an EIGRP packet to your neighbor and receive an acknowledgment packet back.

5.RTO (Retransmission timeout): The amount of time in milliseconds that EIGRP will wait before retransmitting a packet from the retransmission queue to this neighbor

6.Q Cnt (Q count): The number of EIGRP packets (Update, Query or Reply) in the queue that are awaiting transmission. Ideally you want this number to be 0 otherwise it might be an indication of congestion on the network.

7.Seq Num (Sequence number): This will show you the sequence number of the last update,query or reply packet that you received from your EIGRP neighbor.

**Neighbor table:** The neighbor table stores information about neighboring EIGRP routers:

1. Network address (IP)

2. Connected interface

3. Holdtime - how long the router will wait to receive another HELLO before dropping the neighbor; default = 3 * hello timer

4.Uptime - how long the neighborship has been established

5. Sequence numbers

6.Retransmission Timeout (RTO) - how long the router will wait for an ack before retransmitting the packet; calculated by SRTT

7.Smooth Round Trip Time (SRTT) - time it takes for an ack to be received once a packet has been transmitted

8.Queue count - number of packets waiting in queue; a high count indicates line congestion

**EIGRP will use six different packet types when communicating with its neighboring EIGRP routers**

**Hello Packets:** EIGRP sends Hello packets once it has been enabled on a router for a particular network. These messages are used to identify neighbors and once identified, serve or function as a keepalive mechanism between neighbors. EIGRP Hello packets are sent to the link local Multicast group address 224.0.0.10. Hello packets sent by EIGRP do not require an Acknowledgment to be sent confirming that they were received. Because they require no explicit acknowledgment, Hello packets are classified as unreliable EIGRP packets. EIGRP Hello packets have an OPCode of 5.

Acknowledgment Packets:An EIGRP Acknowledgment (ACK) packet is simply an EIGRP Hello packet that contains no data. Acknowledgment packets are used by EIGRP to confirm reliable delivery of EIGRP packets. ACKs are always sent to a Unicast address, which is the source address of the sender of the reliable packet, and not to the EIGRP Multicast group address. In addition, Acknowledgment packets will always contain a non-zero acknowledgment number. The ACK uses the same OPCode as the Hello Packet because it is essentially just a Hello that contains no information. The OPCode is 5.

**Update Packets:** EIGRP Update packets are used to convey reachability of destinations. Update packets contain EIGRP routing updates. When a new neighbor is discovered, Update packets are sent via Unicast to the neighbor which can build up its EIGRP Topology Table. It is important to know that Update packets are always transmitted reliably and always require explicit acknowledgment. Update packets are assigned an OPCode of 1.

**Query Packets:** EIGRP Query packets are Multicast and are used to reliably request routing information. EIGRP Query packets are sent to neighbors when a route is not available and the router needs to ask about the status of the route for fast convergence. If the router that sends out a Query does not receive a response from any of its neighbors, it resends the Query

as a Unicast packet to the non-responsive neighbor(s). If no response is received in 16 attempts, the EIGRP neighbor relationship is reset. EIGRP Query packets are assigned an OPCode of 3

**Reply Packets:**EIGRP Reply packets are sent in response to Query packets. The Reply packets are used to reliably respond to a Query packet. Reply packets are Unicast to the originator of the Query. The EIGRP Reply packets are assigned an OPCode of 4.

**Request Packets:**Request packets are used to get specific information from one or more neighbors and are used in route server applications. These packet types can be sent either via Multicast or Unicast, but are always transmitted unreliably.

**Topology table:** Topology Table confusingly named, this table does not store an overview of the complete network topology; rather, it effectively contains only the aggregation of the routing tables gathered from all directly connected neighbors. This table contains a list of destination networks in the EIGRP-routed network together with their respective metrics. Also for every destination, a successor and a feasible successor are identified and stored in the table if they exist. Every destination in the topology table can be marked either as "Passive", which is the state when the routing has stabilized and the router knows the route to the destination, or "Active" when the topology has changed and the router is in the process of (actively) updating its route to that destination.

**Routing table:** Stores the actual routes to all destinations; the routing table is populated from the topology table with every destination network that has its successor and optionally feasible successor identified (if unequal-cost load-balancing is enabled using the variance command). The successors and feasible successors serve as the next hop routers for these destinations.

**Successor:** A successor for a particular destination is a next hop router that satisfies these two conditions: The successor route provides the least distance to that destination, and guaranteed not to be a part of some routing loop The successor route is installed in the Routing table.

**Feasible successor:** The feasible successor effectively provides a backup route in the case that existing successors die. Also, when performing unequal-cost load-balancing (balancing the network traffic in inverse proportion to the cost of the routes), the feasible successors are used as next hops in the routing table for the load-balanced destination.

By default, the total count of successors and feasible successors for a destination stored in the routing table is limited to four. This limit can be changed in the range from 1 to 6. In more recent versions of Cisco IOS (e.g. 12.4), this range is between 1 and 16.

**Metrics: IGRP (as well as EIGRP) use the following components as metrics:**

**1. Delay:** Calculated by adding up the delay along the path to the next router.

**2. Reliability:** This is representative of how many errors are occurring on the interface. The best reliability value is 255. A value of 128 represents only 50% reliability.

**3. Load:** Load metric also has a range from 1 to 255. If a serial link is being operated at 50% capacity, the load value is 255X0.5 or 12.5. Lower load value is better.

**4. MTU:** Stands for Maximum Transmit Unit size, in bytes. Ethernet and serial interface has a default MTU of 1500. Larger MTU size means that the link is more efficient.

**5. Bandwidth:** The bandwidth is specified in Kbps. Larger the bandwidth, better the link.

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes



## 1.0 Layer 3 technologies

### 1.10 Troubleshoot OSPF (v2/v3)

**Neighbor relationship and authentication**

The Hello and Dead timers must match for forming neighbour relationship.

The routers should be in the same Area to form neighbour relationship.

**OSPF determines the router ID using the following criteria:**

1. Use the address configured by the ospf router-id command

2. Use the highest numbered IP address of a loopback interface

3. Use the highest IP address of any physical interface

4. If no interface exists, set the router-ID to 0.0.0.0

If no OSPF router ID is explicitly configured, OSPF computes the router-ID based on the items 2, 3, and 4 and restarts OSPF (if the process is enabled and router-ID has changed).

A router with highest priority becomes the designated router and a router with priority 0 can never become designated router. If the priorities are the same, then the router with the highest router ID becomes the DR.

There is a mismatch in Hello, and Dead timers. It is important to configure the Hello and Dead timers to same value in neighboring routers. Otherwise, adjacencies will not take place. By default Dead timer is configured as 4 times the Hello timer.

**The major advantages of hierarchical nature of OSPF are:**

1.Reduced frequency of SPF calculations: This is because the packets are flooded only within an area, and not to the other areas.

2.Smaller routing tables.

3.Reduced LSU overhead.

1. A stub AS is a single-homed network with only one entry and exit point. This type of AS can be connected to the external world through the use of a statically configured route.

2. Transit AS: Data from one AS need to reach a remote AS, then it has to travel through intermediate AS. The AS or Autonomous Systems which carry the data from one AS to another AS is (are) called Transit AS (es).

3. eBGP: External BGP is used between two or more Autonomous Systems.

4. iBGP: Internal BGP is used within an AS.

**Network types, area types, and router types**

**In an OSPF network, when a packet need to traverse from one area to another area to reach its destination, it is routed as below:**

Source Area -> Source ABR -> Backbone Area -> Destination ABR -> Destination Area Routers

**The sequence of steps followed in OSPF operation are as below:**

1. Establish router adjacencies

2. Elect DR and BDR

3. Discover Routes

4. Choose appropriate routes for use

5. Maintain routing information.

The path cost in OSPF network is calculated using bandwidth. The formula used is [10^8 / Bandwidth]. For example, the cost of a 56kbps serial link is 1785. The default cost of a 10mbps Ethernet is 10. Higher the bandwidth, lower will be the path cost.

OSPF is a link state technology that uses Dijkstra algorithm to compute routing information. It has the following advantages over Distance Vector protocols such as RIP:

1. Faster convergence: OSPF network converges faster because routing changes are flooded immediately and computer in parallel.

2. Support for VLSM: OSPF supports VLSM. However, please note that RIP version2 also supports VLSM.

3. Network Reachability: RIP networks are limited to 15 hops. Therefore, networks with more than 15 hops can not be reached by RIP by normal means. On the other hand, OSPF has practically no reachability limitation.

4. Metric: RIP uses only hop count for making routing decisions. This may lead to severe problems in some cases, for example, that a route is nearer but is very slow compared to another route with plenty of bandwidth available. OSPF uses "cost" metric to choose best path. Cisco uses "bandwidth" as metric to choose best route.

5. Efficiency: RIP uses routing updates every 30 seconds. OSPF multicasts link-state updates and sends the updates only when there is a change in the network.

In an OSPF network, Type 2 LSAs are generated by a Designated Router (DR). Type 2 LSAs describe the set of routers attached to a particular network and are flooded within the area that contain the network only.

An OSPF area is a collection of networks and routers that has the same area identification.

OSPF process identifier is locally significant. Two neighboring router interfaces can have same or different process ids. It is required to identify a unique instance of OSPF database.

OSPF keeps up to six equal-cost route entries in the routing table for load balancing.

Further, OSPF uses Dijkstra algorithm to calculate lowest cost route. The algorithm adds up the total costs between the local router and each destination network. The lowest cost route is always preferred when there are multiple paths to a given destination.

The Hello packet contains the router ID and the hello and dead intervals and is sent to the multicast address 224.0.0.5.

**Important features of stub area are:**

1. A stub area reduces the size of the link-state database to be maintained in an area, which in turn result in less overhead in terms of memory capacity, computational power, and convergence time.

2. The routing in Stub and totally Stubby areas is based on default gateway. A default route (0.0.0.0) need to be configured to route traffic outside the area.

3. The stub areas suited for Hub-Spoke topology.

4. Area 0 is not configured as Stubby or totally Stubby. This is because stub areas are configured mainly to avoid carrying external routes, whereas Area 0 carries external routes.

OSPF uses a reference bandwidth of 100 Mbps for cost calculation. The formula to calculate the cost is reference bandwidth divided by interface bandwidth. For example, in the case of Ethernet, it is 100 Mbps / 10 Mbps = 10.

Note: If ip ospf cost is used on the interface, it overrides this formulated cost.

LSA Type 1: Router link entry, generated by all routers for each area to which it belongs. These are flooded within a particular area.

LSA Type 2: Network link entry, generated by designated router (DRs). Type 2 LSAs are advertised only to routers that are in the area containing the specific network.

LSA Type 3 and Type 4: Summary link entry, these LSAs are generated by area border routers (ABRs). These are sent to all routers within an area. These entries describe the links between the ABR and the internal routers of an area. These entries are flooded throughout the backbone area and to the other ABRs.

LSA Type 5: Autonomous System External Link Entry, These are originated by ASBR. These entries describe routes to destinations external to the autonomous system. These LSAs are flooded throughout the OSPF autonomous system except for stubby and totally stubby areas.

Area backbone LSAs: The LSAs generated by Area Backbone Routers are LSA1, LSA2, LSA3, LSA4, and LSA5. Note that LSA6 is not supported by Cisco, and LSA7 is generated by NSSA router.

Stub area LSAs: The Stub area router generates LSA types 1, 2, and 3. i.e. Router LSA, Network LSA, and Summary LSA.

Totally Stubby LSAs:The Totally Stubby area routers generate LSA types 1 and 2

NSSA LSAs: A NSSA (Not So Stubby Area) router generates LSA types 1, 2, and 7. LSA 7 is translated into LSA 5 as it leaves the NSSA

**Different LSA types are described below:**

a. LSA 1 (Router LSA): Generated by all routers in an area to describe their directly attached links (Intra-area routes). These do not leave the area.

b. LSA 2 (Network LSA): Generated by the DR of a broadcast or Nonbroadcast segment to describe the neighbors connected to the segment. These do not leave the area.

c.LSA 3 (Summary LSA): Generated by the ABR to describe a route to neighbors outside the area. (Inter-area routes)

d. LSA 4 (Summary LSA): Generated by the ABR to describe a route to an ASBR to neighbors outside the area.

e. LSA 5 (External LSA): Generated by ASBR to describe routes redistributed into the area. These routes appear as E1 or E2 in the routing table. E2 (default) uses a static cost throughout the OSPF domain as it only takes the cost into account that is reported at redistribution. E1 uses a cumulative cost of the cost reported into the OSPF domain at redistribution plus the local cost to the ASBR.

f. LSA 6 (Multicast LSA): Not supported on Cisco routers.

g. LSA 7 (NSSA External LSA): Generated by an ASBR inside a NSSA to describe routes redistributed into the NSSA. LSA 7 is translated into LSA 5 as it leaves the NSSA. These routes appear as N1 or N2 in the ip routing table inside the NSSA. Much like LSA 5, N2 is a static cost while N1 is a cumulative cost that includes the cost upto the ASBR.

**The cost of external route depends on the configuration of ASBR. There are two external packet types possible.**

1. Type 1 (E1) - Here the metric is calculated by adding the external cost to the internal cost of each link that the packet crosses.

Type 2 (E2) - This type of packet will only have the external cost assigned, irrespective of where in the area it crosses. Type 2 packets are preferred over Type 1 packets unless there are two same cost routes existing to the destination.

Cost is a number from 1 to 65535 that indicates the metric assigned to the interface.

The cost of external route depends on the configuration of ASBR. There are two external packet types possible.

1.Type 1 (E1) - Here the metric is calculated by adding the external cost to the internal cost of each link that the packet crosses.

2.Type 2 (E2): E2 is the default route type for routes learned via redistribution.

The command, **RouterD(config-router)#default-information originate**

is used to instruct all the other OSPF routers to learn the default route.

OSPF process identifier is locally significant. Two neighboring router interfaces can have same or different process ids. It is required to identify a unique instance of OSPF database

When an area is configured as stub or totally stubby, a default route (0.0.0.0) is injected into the area.

**"show ip ospf interface"** can be used to check whether the interfaces have been configured properly. The command also gives the timer intervals, including hello intervals as well as neighbor adjacencies.

The following output provides a sample output of the command:

```
Router1# show ip ospf interface
Ethernet0 is up, line protocol is up
  Internet Address 10.10.10.1/24, Area 0
  Process ID 1, Router ID 192.168.45.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.10.1, Interface address 10.10.10.2
  Backup Designated router (ID) 192.168.45.1, Interface address 10.10.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.10.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

*<Output omitted for brevity>*

**Each field in the output is explained below**

Interface State: The first line of the output shows the Layer 1 and Layer 2 states of the interface. In this example, the interface Ethernet0 senses the carrier on line and shows Layer 1 as up. Line protocol on the Ethernet0 interface confirms that Layer 2 is up. For proper functioning, the interfaces should be in an up/up state.

IP Address and Area: The second line shows the IP address configured on this interface and the area in which this interface is placed. In the above example, the Ethernet0 has an IP address of 10.10.10.1/24 and is in OSPF area 0.

Process ID: The process ID is the ID of the OSPF process to which the interface belongs. The process ID is local to the router, and two OSPF neighboring routers can have different OSPF process IDs. (This is not true of Enhanced Interior Gateway Routing Protocol [EIGRP], in which the routers need to be in the same autonomous system). In this example, the process ID is 1.

Router ID: The OSPF router ID is a 32-bit IP address selected at the start of the OSPF process. The highest IP address configured on the router is the router ID. If a loopback address is configured, it is the router ID. In the case of multiple loopback addresses, the highest loopback address is the router ID. Once the router ID is elected, it does not change unless OSPF restarts or is manually changed with the router-id 32-bit-ip-address command under router ospf process-id . In this example, 192.168.45.1 is the OSPF router ID.

Network Type: In the example, the OSPF network type is BROADCAST, which uses OSPF multicasting capabilities. Under this network type, a designated router (DR) and backup designated router (BDR) are elected. For routers on an interface to become neighbors, the

network type for all should match.

**The possible OSPF network types are:**

POINT-TO-POINT (for example, the interfaces of two routers connected through E1 or T1 links) ,NON-BROADCAST (such as X.25 and Frame Relay) ,POINT-TO-MULTIPOINT (such as Frame Relay)

Cost: This is an OSPF metric. Cost is calculated with this formula: 108 / bandwidth (in bits per second [bps])

In the formula, bandwidth refers to the bandwidth of the interface in bps, and 108 is the reference bandwidth. In the example, the bandwidth of Ethernet0 is 10 Mbps, which is equal to 107. The formula yields 108 /107, equaling a cost of 10.

Transmit Delay: The transmit delay is the amount of time OSPF waits before flooding a link-state advertisement (LSA) over the link. Before transmitting an LSA, the link-state age is incremented by this number. In this example, the transmit delay is 1 second, which is the default value.

State: This field defines the state of the link and can be any of these:

DR:The router is the DR on the network to which this interface is connected, and it establishes OSPF adjacencies with all other routers on this broadcast network. In this example, this router is the BDR on the Ethernet segment to which the Ethernet0 interface is connected.

BDR:The router is the BDR on the network to which this interface is connected, and it establishes adjacencies with all other routers on the broadcast network.

DROTHER:The router is neither the DR nor the BDR on the network to which this interface is connected, and it establishes adjacencies only with the DR and the BDR.

Waiting:The interface is waiting to declare the state of the link as DR. The amount of time the interface waits is determined by the wait timer. This state is normal in a nonbroadcast multiaccess (NBMA) environment.

Point-to-Point:This interface is point-to-point for OSPF. In this state, the interface is fully functional and starts exchanging hello packets with all of its neighbors.

Point-to-Multipoint:This interface is point-to-multipoint for OSPF.

Priority: This is the OSPF priority that helps determine the DR and BDR on the network to which this interface is connected. Priority is an 8-bit field based on which DRs and BDRs are elected. The router with the highest priority becomes the DR. If the priorities are the same,

the router with the highest router ID becomes the DR. By default, priorities are set to 1.

Designated Router: This is the router ID of the DR for this broadcast network. In the example, it is 172.16.10.1.

Interface Address: This is the IP address of the DR interface on this broadcast network. In the example, the address is 10.10.10.2, which is Router 2.

Backup Designated Router: This is the router ID of the BDR for this broadcast network. In the example, it is 192.168.45.1.

Interface Address: This is the IP address of the BDR interface on this broadcast network. In the example, it is Router 1.

Timer Intervals: These are the values of the OSPF timers:

Hello-Interval: time in seconds that a router sends an OSPF hello packet. On broadcast and point-to-point links, the default is 10 seconds. On NBMA, the default is 30 seconds.

Dead:Time in seconds to wait before declaring a neighbor dead. By default, the dead timer interval is four times the hello timer interval.

Wait:Timer interval that causes the interface to exit out of the wait period and select a DR on the network. This timer is always equal to the dead timer interval.

Retransmit:Time to wait before retransmitting a database description (DBD) packet when it has not been acknowledged.

Hello Due In: An OSPF hello packet is sent on this interface after this time. In this example, a hello is sent three seconds from the time the show ip ospf interface is issued.

Neighbor Count: This is the number of OSPF neighbors discovered on this interface. In this example, this router has one neighbor on its Ethernet0 interface.

Adjacent Neighbor Count: This is the number of routers running OSPF that are fully adjacent with this router. Adjacent means that their databases are fully synchronized. In this example, this router has formed an OSPF adjacency with one neighbor on its Ethernet0 interface.

Suppress Hello: When IP OSPF demand circuits are created over ISDN links, the OSPF hello packets are suppressed to keep the link from continually staying up. In the above example, the output is shown for an Ethernet interface; therefore, hello packets are not suppressed for any neighbors.

Index: This is the index of the interface flood lists (area/autonomous system) used. In the example, the value is 1/1.

Flood Queue Length: This is the number of LSAs waiting to be flooded over an interface. From the example, the number of LSAs waiting to be flooded over the Ethernet interface is 0.

Next: This is the pointer to the next LSAs (index) to flood. It refers to the flood lists.

Last Flood Scan Length/Maximum: This is the size of the last list of LSAs flooded and the maximum size of the list. When using pacing, one LSA is transmitted at a time.

Last Flood Scan Time/Maximum: This is the time spent in the last flooding and the maximum time spent flooding.

The command that is used for configuring OSPF in NBMA mode is: "ip ospf network non-broadcast". However, note that NBMA mode is used by default.

**OSPF determines the router ID using the following criteria:**

1. Use the address configured by the ospf router-id command

2. Use the highest numbered IP address of a loopback interface

3. Use the highest IP address of any physical interface

4. If no interface exists, set the router-ID to 0.0.0.0

If no OSPF router ID is explicitly configured, OSPF computes the router-ID based on the items 2, 3, and 4 and restarts OSPF (if the process is enabled and router-ID has changed).

To modify router priority in an OSPF ip network, issue the command: "ip ospf priority <number>" where <number> is any number between 0 and 255. The default is 1.

A default route can be advertised into OSPF domain by an ASBR router in one of two ways:

"default-information originate" command: This command can be used when there is a default route (0.0.0.0/0) already existing. This command will advertise a default route into the OSPF domain.

"default-information originate always" command: This command can be used when there is a default route (0.0.0.0/0) is present or not. This command is particularly useful when the default route is not consistent. An inconsistent default route may result in flipping of the route advertised into the OSPF domain, resulting in instability of the OSPF domain routing information. Therefore, it is recommended to use "always" keyword.

In general, the path cost in OSPF network is calculated using bandwidth only. The formula used is [10^8 divided by Bandwidth]. For example, the cost of a 56kbps serial link is 1785. The default cost of a 10mbps Ethernet is 10.

The statements identify that the process-id of the OSPF is 100, and the statement "area 1 stub no-summary" signifies totally stubby area. The router is connecting two area, and hence not a backbone router.

The command that is used for configuring OSPF in NBMA mode is: "ip ospf network non-broadcast". However, note that NBMA mode is used by default.

### Virtual link

The command "show ip ospf virtual-links" will show up the status of virtual links of a router.

Use the "area virtual-link" command to configure an OSPF virtual link between two routers

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#area 10 virtual-link 10.54.0.1
Router(config-router)#exit
Router(config)#end
Router#
```

This feature is commonly used when an area has become fragmented and two routers need to tunnel their OSPF neighbor relationship across multiple links. This is usually not a problem if the two routers and the intervening networks are all in the same area. However, it can be a serious problem in particular if you have an ABR(Area Border Router) that is buried inside a non-backbone area without a direct connection to area 0.

You can see the status of a virtual link with the "show ip ospf virtual-links" command: The following output provides a sample output of the command:

```
Router#show ip ospf virtual-links
Virtual Link OSPF_VL1 to router 10.54.0.1 is up
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 10, via interface serial0/0, Cost of using 74
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:00
Router#
```

### Path preference

Path cost is the total of the costs assigned to all interfaces that forward traffic along the path to the destination. External and summary routes are not injected into a totally stubby area in an OSPF network. The advantages of totally stubby areas are reduced routing tables, faster

convergence, and stability.

The path cost in OSPF network is calculated using bandwidth only. The formula used is [10 ^8 divided by Bandwidth]. For example, the cost of a 56kbps serial link is 1785. The default cost of a 10mbps Ethernet is 10.

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-6.htm



## 1.0 Layer 3 technologies

### 1.11 Troubleshoot BGP (Internal and External)

**Neighbor relationship and authentication (next-hop, mulithop, 4-byte AS, private AS, route refresh, synchronization, operation, peer group, states and timers)**

Below is the list of BGP states in order, from startup to peering:

**1. Idle:** the initial state of a BGP connection. In this state, the BGP speaker is waiting for a BGP start event, generally either the establishment of a TCP connection or the re-establishment of a previous connection. Once the connection is established, BGP moves to the next state.

**2. Connect:** In this state, BGP is waiting for the TCP connection to be formed. If the TCP connection completes, BGP will move to the OpenSent stage; if the connection can not complete, BGP goes to Active

**3. Active:** In the Active state, the BGP speaker is attempting to initiate a TCP session with the BGP speaker it wants to peer with. If this can be done, the BGP state goes to OpenSent state.

**4. OpenSent:** the BGP speaker is waiting to receive an OPEN message from the remote BGP speaker

**5. OpenConfirm:** Once the BGP speaker receives the OPEN message and no error is detected, the BGP speaker sends a KEEPALIVE message to the remote BGP speaker

**6. Established:** All of the neighbor negotiations are complete. You will see a number (2 in this case), which tells us the number of prefixes the router has received from a neighbor or peer group.

BGP can load balance up to six links. You can have up to six links to ISPs and use those links for Internet traffic. This arrangement provides redundancy as well as load balancing.

When route map is configured in BGP, there is an implicit "deny any" at the end of a route map. When a route map is configured in BGP, after checking all the route map statements, there is an automatic denial of route if no match is found. This is same as in ACLs.

The sequence numbers of 5, 10,15,20 etc. are assigned automatically when no sequence numbers are used while configuring prefix lists. As can be seen, the first number assigned is 5 and the increment value is also 5.

**Show ip bgp neighbor:** The show ip bgp neighbors command is used to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance. This command displays information only about IPv4 address-family sessions unless the all keyword is entered.

Routers running BGP in an AS use network Policy to choose the best path. Metrics are not used in BGP. Remember that Internet is made of autonomous systems (AS) that are connected together based on Policies specific to each AS. Also, AS numbers (ASN) are assigned by AINA and are unique over the Internet. In an internet (not big I) the ASNs can be assigned by the corporation itself that is implementing internet.

Routers running BGP in an AS use network Policy to choose the best path. Metrics are not used in BGP. Remember that Internet is made of autonomous systems (AS) that are connected together based on Policies specific to each AS. Also, AS numbers (ASN) are assigned by AINA and are unique over the Internet. In an internet (not big I) the ASNs can be assigned by the corporation itself that is implementing internet.

The command : **clear ip bgp** *

clears all the entries from the BGP routing table and reset BGP sessions. This command is used after every configuration change to ensure that the change is activated and that peer routers are informed.

Another command, **clear ip bgp** <*address*>

ex: clear ip bgp 172.31.0.0 removes the specified network from the BGP table.

iBGP routers don't have to be directly connected, as long as there is some IGP running that allows the two neighbors to reach one another. If two routers belong to the same AS, then they run iBGP, whereas, if they belong to different ASs, they need to run eBGP.

**While selecting best route in BGP, the order of preferences are as below:**

1. Weight - If multiple routes exist, the route with the highest weight is preferred.

2. Local preference - If multiple routes have the same weight, the route with the highest local preference is preferred.

3. Local router - If multiple routes have same local preference, prefer the route originated by the local router.

4. AS path - If multiple routes have the same local preference, prefer the route with shortest AS path.

The syntax for establishing neighbor relationship is:

**router bgp 100**

**neighbor 175.23.1.2 remote-as 200**

Also, it is important to know that the eBGP peers are directly connected while the iBGP peers are not.

iBGP routers don't have to be directly connected, as long as there is some IGP running that allows the two neighbors to reach one another. If two routers belong to the same AS, then they run iBGP, whereas, if they belong to different ASs, they need to run eBGP.

**Path preference (attributes and best-path)**

Route maps are used with BGP to control and modify routing information and to define the conditions by which routes are redistributed between Autonomous Systems. The format of a route map is as follows:

**route-map** *map-name [permit | deny] | [sequence-number]*

The map-name is a name that identifies the route map, and the sequence number indicates the position that an instance of the route map is to have in relation to other instances of the same route map.

Communities are basically labels that are attached to BGP routes. A few of these labels have pre-defined meanings. The well-known communities are:

Communities are basically labels that are attached to BGP routes. A few of these labels have pre-defined meanings. The well-known communities are:

NO_EXPORT: The NO_EXPORT community tells a router it should only propagate any prefixes this community is attached to over iBGP, and not propagate it over eBGP to external autonomous systems.

NO_ADVERTISE: NO_ADVERTISE Tells the router to not advertise the prefix over BGP at all. Most, if not all, routers automatically honor these communities when they're present. So if you want to overrule this behavior, you need to filter them out.

NO_EXPORT_SUBCONFED: NO_EXPORT_SUBCONFED does something similar to NO_EXPORT in networks using confederations to limit the number of iBGP sessions.

NOPEER: NOPEER was defined later and indicates that a prefix "need not" be advertised over peering relationships.

Many routers don't automatically propagate communities. On a Cisco router, you'll have to enable this explicitly for a BGP neighbor with the "send-community" keyword:

Any two routers that have formed a TCP connection in order to exchange BGP routing information are called peers, or neighbors. BGP peers initially exchange their full BGP routing tables. After this exchange, incremental updates are sent as the routing table changes. BGP keeps a version number of the BGP table, which should be the same for all of its BGP peers.

The version number changes whenever BGP updates the table due to routing information changes. Keepalive packets are sent to ensure that the connection is alive between the BGP peers and notification packets are sent in response to errors or special conditions.

The following are a few examples of how a prefix list can be used (while configuring BGP policies to filter route updates):

**To deny the default route 0.0.0.0/0:** ip prefix-list mylist1 deny 0.0.0.0/0

**To permit the prefix 20.0.0.0/8:** ip prefix-list mylist1 permit 20.0.0.0/8

**The following examples show how to specify a group of prefixes.**

**To accept a mask length of up to 24 bits in routes with the prefix 192/8:** ip prefix-list mylist1 permit 192.0.0.0/8 le 24

**To deny mask lengths greater than 25 bits in routes with a prefix of 192/8:** ip prefix-list mylist1 deny 192.0.0.0/8 ge 25

Well-Known mandatory attributes must appear in all BGP update messages. The well-known mandatory messages are:

**1. AS_PATH :** BGP messages carry the sequence of AS numbers indicating the complete path a message has traversed.

**2. NEXT_HOP :** This attribute indicates the IP address of the next-hop destination router.

**3. ORIGIN :** This attribute tells the receiving BGP router, the BGP type of the original source of the NLRI information.

Given are :

AS number : 100
Peer group name : mygroup
The basic commands required are :
!
router bgp 100
neighbor mygroup peer-group
!

1. A BGP peer group is useful to decrease the overhead of configuring policies on all individual BGP neighbors in an AS. When a peer group is created, policies are assigned to the peer group name and not to the individual neighbors.

2. Update policies are normally set by route maps, distribution lists, and filter lists.

3. Members of the peer group can be configured to override the configuration options for incoming updates, but not to the outgoing updates.

The "hello" packets are sent periodically out of each interface using IP multicast addresses. The hello interval specifies the frequency in seconds that a router sends hello's. This is 10 seconds on multi access networks.

When a route reflector in a BGP AS  receives an update, it takes the following actions, depending on the type of peer that sent the update:

1. If the update is from a non-client peer : It sends the update to all clients in the cluster.

2. If the update is from a client peer: It sends the update to all nonclient peers and to all client peers.

3. If the update is from eBGP peer: It sends the update to all nonclient peers and to all client peers.

External BGP (eBGP): eBGP is used to establish session and exchange route information between two or more autonomous systems. Internal BGP (iBGP) is used by routers that belong to the same Autonomous System (AS).

Show ip bgp: Displays entries in the BGP routing table for one network prefix or the entire BGP routing table.

Syntax: **show ip bgp** *[prefix-length]*

prefix-length: Display BGP information for a single network prefix.

Description: Use the show ip bgp command to display entries in the BGP routing table. It will also displays the Metric, LocPrf, Weight, and Path attribute values for each route.

Use the prefix-length keyword to display information for a single network prefix.

Show ip bgp summary: The show ip bgp summary command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route. A path is a route to a given destination. By default, BGP will install only a single path for each destination. If multipath routes are configured, BGP will install a path entry for each multipath route, and only one multipath route will be marked as the bestpath.

**Show ip route bgp:** Typical output of this command is given below:

**R1# show ip route bgp**
128.13.0.0/24 is subnetted, 1 subnets
B 128.13.16.0 [20/0] via 10.10.10.2, 00:09:32
B 130.130.0.0/16 [20/0] via 10.10.10.2, 02:48:46

The administrative distance (20) is shown in the command output along with the route information and the up-time.

**Few recommended scenarios, where you use BGP are:**

1. Connect two or more ISPs

2. The traffic flow out of your network need to be managed to suit the requirements of your organization.

3.The traffic need to be sent through one AS to get to another AS.

**Given below is the list of BGP attributes and their significance:**

1. AS path - An ordered list of all the autonomous systems through which this update has passed. Well-known, mandatory.

2. Origin - How BGP learned of this network. i = by network command, e = from EGP, ? = redistributed from other source. Well-known, mandatory.

3. Local Preference - A value telling IBGP peers which path to select for traffic leaving the AS. Default value is 100. Well-known, discretionary.

4. Multi-Exit Discriminator (MED) - Suggests to a neighboring autonomous system which of multiple paths to select for traffic bound into your autonomous system. Lowest MED is preferred. Optional, non-transitive.

5. Weight - Cisco proprietary, to tell a router which of multiple local paths to select for traffic leaving the AS. Highest weight is preferred. Only has local significance.

**Prefix lists (filtering)  are available only in Cisco IOS versions 12.0 and later. The following are important characteristics of Prefix lists:**

1. These are used for filtering BGP routing updates, so that certain path policy is applied.

2. Prefix lists doesn't put as much load on the processor as that of Access lists.

3. Prefix lists are easier to configure and implement.

4. These are read one line at a time as that of Access lists.

There is an implicit deny all at the bottom of the Prefix list. One exception is that, if the prefix list is empty, there will be an implicit permit any!

The statement with smallest sequence numbers are read first.

MED (Multi_EXIT_DESCRIMINATOR) attribute is an optional non-transitive attribute that is used by BGP to inform the neighboring AS which link to use to receive traffic.

**The output is that of "show ip bgp summary". It contains the following among other details:**

1. BGP router identifier: Router identifier specified by the bgp router-id command, loop back address, or lowest IP address.

2. BGP table version: Internal version number of BGP database.

3. Main routing table version: Last version of BGP database that was injected into main routing table.

4. Neighbor: IP address of a neighbor.

5. V: BGP version number spoken to that neighbor.

6. AS: Autonomous system.

To specify the networks to be advertised by the Border Gateway Protocol (BGP) use the network command -"network network-number [mask network-mask]"

To remove an entry, use the no form of this command -"**no network** *network-number [mask network-mask]*"

1. Prefer the path with the highest WEIGHT. Note that WEIGHT is a Cisco-specific parameter. It is local to the router on which it is configured.

2. Prefer the path with the highest LOCAL_PREF. Note that a path without LOCAL_PREF is considered to have had the value set with the bgp default value of 100.

3. Prefer the path that was locally originated via a network or aggregate BGP subcommand or through redistribution from an IGP.

4. Local paths that are sourced by the network or redistribute commands are preferred over local aggregates that are sourced by the aggregate-address command.

5. Prefer the path with the shortest AS_PATH.

6. Prefer the path with the lowest origin type. Among the paths, note that,  IGP is lower than Exterior Gateway Protocol (EGP), and EGP is lower than INCOMPLETE.

7. Prefer the path with the lowest Multi Exit Discriminator (MED).

Prefer eBGP over iBGP paths.

IBGP works a little different from EBGP. There are a set of rules that apply to IBGP implementation which make IBGP different from EBGP.

1.Routes learnt from One IBGP Peer cannot be advertised to another IBGP Peer.

2 Rule of Synchronization: For A Route to be learnt from an IBGP neighbor, it must first be known via an IGP. Any route learnt from IBGP is entered into the routing table only if that route is first learnt by an IGP. In iBGP, the routes learnt from one iBGP neighbor are not advertised to another iBGP neighbor due to the BGP Split Horizon Rule. To overcome the issues generated by this rule, one option is to have a full mesh of iBGP routers, where each iBGP router is peering directly with all other iBGP routers in the AS. The solution is feasible if you have a small number of iBGP routers, but it will not scale if you need a large number of iBGP speaking routers in the AS.

The number of iBGP Sessions needed in an AS for Full mesh IBGP are calculated with the formula N(N-1)/2.

So assuming you have 10 iBGP routers then the number of iBGP peering sessions would be

10(10-1)/2 = 45 iBGP Sessions to manage within the AS. Thats a lot of configuration and a lot of room for errors and may become difficult to troubleshoot.

Route Reflectors and Confiderations are used as alternative mechanisms to address this problem:

1. Route Reflectors

2. Confederations

To configure a fixed router ID for a BGP-speaking router, use the bgp router-id router configuration command.

**bgp** *router-id {ip-address}*

By default, The router ID is set to the IP address of a loop back interface if one is configured. If no virtual interfaces are configured, the highest IP address is configured for a physical interface on that router. Note that peering sessions will be reset if the router ID is changed

It is true that, if Prefix lists are applied for filtering BGP updates, a route is advertised when prefix is permitted. A route is not advertised when the prefix is not permitted.

To distribute Border Gateway Protocol (BGP) neighbor information as specified in an access list, use the neighbor distribute-list command in address family or router configuration mode.

**Various debug commands useful in troubleshooting bgp are:**

1. Debug ip bgp events: Displays all bgp events as they occur.

2. Debug ip bgp dampening: Displays bgp dampening events as they occur.

3. Debug ip bgp keepalives: Displays all events related to bgp keepalive packets.

4. Debug ip bgp updates: Displays information on all bgp update packets.

Well-known mandatory attributes: These attributes must be included in all UPDATE messages of BGP.

Well-known discretionary: These attributes may be included in a route description, but not mandatory.

Optional transitive: AGGREGATOR and COMMUNITIES are the optional transitive attributes.

Optional non-transitive: These attributes are used in many private BGP enabled networks.

You can increase the AS-PATH length by adding dummy AS numbers.

The route map configuration command: **set as-path prepend** *100*

causes a router to prepend 100 once to the value of the AS_path attribute before it sends updates to the specified neighbor.

If you want to prepend 100 twice, use the command : set as-path prepend 100 100

Effectively, this will increase the AS-PATH length in the updates being sent to the neighbor and therefore the path selection.

You can delete a prefix list that was configured earlier on a BGP speaking router by using the command "no ip prefix-list" followed by the list name.

To disable automatic summarization of subnet routes into network level routes use the command : no auto-summary

To enable automatic summarization of subnet routes into network level routes use the command : auto-summary

Note that by default, auto-summary is enabled.

**1. Distribute lists:** To restrict the routing information that the router learns or advertises, you can filter based on routing updates to or from a particular neighbor. The filter consists of an access list that is applied to updates to or from a neighbor.

2. AS_Path filtering: Here, you specify an access list on both incoming and outgoing updates based on the value of the AS_path attribute.

**3. Route Map Filtering:** Here, the "neighbor route-map" router configuration command is used to apply a route map to incoming and outgoing routes.

**4. Community Filtering:** You can filter by setting the community attribute on router updates.

iBGP runs between routers of the same AS, where as eBGP runs between the routers belonging to distinct ASs.

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes



## 2.0 VPN Technologies

### 2.1 Describe MPLS operations (LSR, LDP, label switching, LSP)

LDP is a protocol that automatically generates and exchanges labels between routers. Each router will locally generate labels for its prefixes and will then advertise the label values to its neighbors. LDP uses the Transmission Control Protocol (TCP) to transmit Session, Advertisement, and Notification messages to ensure reliable message transmission. LDP uses the User Datagram Protocol (UDP) only for transmitting Discovery messages.

Cisco Express Forwarding is an advanced layer 3 switching technology used mainly in large core networks or internet to enhance the overall network performance is mainly used to increase packet switching speed by reducing the overhead and delays introduced by other routing techniques. CEF consists of two key components: The Forwarding Information Base (FIB) and adjacency.

LDP(Label Distribution Protocol):A protocol used between MPLS-enabled routers to generate and exchange labels that will be used to forward packets in the MPLS domain.

LSP(Label Switched Path):The cumulative labeled path (sequence of routers) that a labeled packet takes through the MPLS domain.

LFIB(Label Forwarding Information Base):A data plane table that is used to forward labeled packets.

LIB(Label Information Base): A control plane table that stores label information.

LSR(Label Switching Router):A router in an MPLS domain that forwards packets using label information.

1. MPLS PEs form a backbone area

2. Each PE-CE link can be any area.

3. MPLS uses MPBGP to redistribute routes

4. The Area 0 may exist in both customer premise as well as the Service providers (SP) network.

**CE(Customer Edge):**CE A CE router ( Customer Edge router ) is a router located on the customer premises that provides an Ethernet interface between the customer's LAN and the provider's core network. Customer Edge normally unaware of mpls labeling. Connects customer network to MPLS network

**PE(Provider Edge):** Provider edge is the egress and ingress for the mpls domain , it remove labels before sending them to CE and add labels to traffic received from CE

**P(Provider):** Provider , MPLS devices in the core of the MPLS domain , forward traffic based on labels

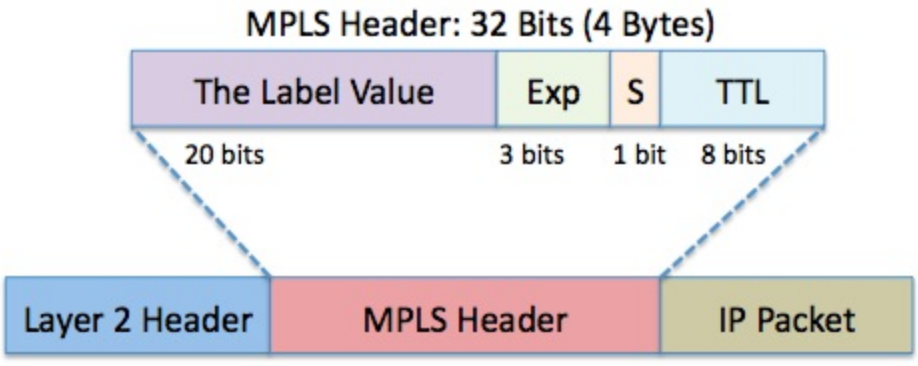
**LSP (Label Switch path():** LSP is a predefined path that the packet takes during the transmission

**LSR( Label Switch Router) :** MPLS network contains Label Switch Routers(LSR). These routers are capable of understanding MPLS labels and of receiving and transmitting the labeled packet.

**ingress LSR**:A router at the edge of the MPLS domain that adds labels to packets that are entering the MPLS domain.

**egress LSR:** A router at the edge of the MPLS domain that removes labels from packets that are leaving the MPLS domain.

The MPLS header is of 32 bits. It contains the following information:-




**1. Label:** The label field is of 20 bits.

**2. Experimental(Exp):**The three bits are reserved as experimental bits. They are used for Quality of Service(QoS).

**3. Bottom of Stack(BoS):** A network packet can have more than one MPLS labels which are stacked one over another. To ensure which MPLS label is at the bottom of stack we have a BoS field which is of 1 bit.

**4. Time to Live(TTL):** The last 8 bits are used for Time to Live(TTL).

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-8.htm



## 2.0 VPN Technologies

### 2.2 Describe MPLS Layer 3 VPN

For the MPLS domain to forward traffic, a label stack is required. Specifically, two labels are required for traffic to be successfully forwarded through the MPLS domain. The first label that is attached to the packet is a VPN label, and the second label that is attached is the LDP label.

The control plane functions include the system configuration,management, and exchange of routing table information. These are performed relatively infrequently. The route controller exchanges the topology information with other routers and constructs a routing table based on a routing protocol, for example,

RIP (Routing Information Protocol), OSPF (Open Shortest Path Forwarding), or BGP (Border Gateway Protocol). It can also create a forwarding table for the forwarding engine. Since the control functions are not performed on each arriving individual packet, they do not have a strict speed constraint and are implemented in software in general. The Control plane feeds the forwarding/data plane with what it needs to create its forwarding tables and updates topology changes as they occur. A list of functions performed in traditional routing engines/route processors are the following:

1. Allocates resources to the forwarding engine/plane.

2. Routing state

3. ARP handling is always processed by general purpose processor located in the routing engine.

4. Security functions to secure the control plane access. Telnet, SSH, AAA etc.

5. Establishes and maintains management sessions, such as Telnet connections

6. Routing state to neighboring network elements.

7. Vendor and platform specific stacking, clustering, pairing etc.

1. A CE router forms a neighbor relationship with the PE router on the other end of the access link.

2. A CE router cannot form a neighbor relationship with other CE routers.

3. The MPLS network advertises the customer's routes between the various PE routers.

4. The MPLS network uses route redistribution to advertise CE routes among other CE routers.

5. It is possible that the PE routers use different layer-3 protocols to connect to the MPLS network.

**Multiprotocol Label Switching (MPLS)** is a protocol for speeding up and shaping network traffic flows. MPLS allows most packets to be forwarded at Layer 2 (the switching level) rather than having to be passed up to Layer 3 (the routing level). Each packet gets labeled on entry into the service provider's network by the ingress router. All the subsequent routing switches perform packet forwarding based only on those labels - they never look as far as the IP header. Finally, the egress router removes the label(s) and forwards the original IP packet toward its final destination.

MPLS is an IETF initiative that integrates Layer 2 information about network links (e.g. bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system, or ISP, in order to simplify and improve IP packet exchange. MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks.

MPLS Layer 3 VPNs provide peer-to-peer connectivity between private customer sites across a shared network. Customer isolation is achieved on the PE (Provider Edge) router by the use of virtual routing tables or instances, also called virtual routing and forwarding tables/instances (VRFs). VRF is a technology for creating separate virtual routers on a single physical router.

A Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each site, there are one or more customer edge (CE) devices, which attach to one or more provider edge (PE) devices. PEs use the Multiprotocol-Border Gateway Protocol (MP-BGP) to dynamically communicate with each other.

**Advantages of using MPLS:**

1. The label-switching technology offers QoS capabilities.

2. MPLS VPNs are available in Layer-2 as well as Layer-3 designs. Layer-2 typically uses Metro Ethernet, where as Layer-3 connectivity may use a variety of L3 technologies such as EIGRP, OSPF, RIPv2, etc., depending on what the SP could provide.

3. By keeping your traffic on a single vendor using MPLS VPNs gives the vendor the ability to offer your company service-level agreements (SLAs) for network performance.

4. MPLS supports many types of access links such as Metro Ethernet, Serial (TDM), ATM, and Frame Relay.

Some of the disadvantages are given below:

1. Your routing protocol choice might be limited.

## 2.3 Configure and verify DMVPN (single hub)

The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IPSec VPNs by combining generic routing encapsulation (GRE) tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP) to provide users with easy configuration through crypto profiles, which override the requirement for defining static crypto maps, and dynamic discovery of tunnel endpoints.

IPSec Virtual Tunnel Interfaces (VTI) provide a routable interface type for terminating IPSec tunnels an easy way to define protection between sites to form an overlay network. IPSec virtual tunnel interfaces simplify configuration of IPSec for protection of remote links, supports multicast, and simplifies network management and load balancing.

Next Hop Resolution Protocol (NHRP) is a resolution protocol that allows a Next Hop Client (NHC) to dynamically register with Next Hop Servers (NHSs). With the Dynamic Multipoint Virtual Private Network (DMVPN) design the NHC is the spoke router and the NHS is the hub router.

ip nhrp holdtime (seconds) - changes the number of seconds that NHRP dynamic entries expire. The default is 7,200 seconds (two hours). The NHRP cache can contain static and dynamic entries.

Dynamic Multipoint Virtual Private Network (DMVPN) is a Cisco feature that dynamically creates a mesh VPN network. This helps to avoid having to statically create VPN tunnels for a mesh network as the network grows in size.

DMVPN has 3 phases:

1. Phase 1 – Hub & Spoke Only

2. Phase 2 – Spoke-to-Spoke Capability (dynamic tunnels)

3. Phase 3 – Allows spokes to respond to NHRP requests

DMVPN Phase 2 does not work well with summarized spoke addresses because of the lack of next-hop preservation.

DMVPN (Dynamic Multipoint VPN) is a routing technique that can be used to build a VPN network with multiple sites without having to statically configure all devices. It's a "hub and spoke" network where the spokes will be able to communicate with each other directly without having to go through the hub. Encryption is supported through IPsec which makes DMVPN a popular choice for connecting different sites using regular Internet connections. DMVPN is combination of the following technologies:

1 Multipoint GRE (mGRE)

2 Next-Hop Resolution Protocol (NHRP)

3 Dynamic Routing Protocol (EIGRP, RIP, OSPF, BGP)

4.Dynamic IPsec encryption

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-9.htm



## 3.0 Infrastructure Security

### 3.1 Troubleshoot device security using IOS AAA (TACACS+, RADIUS, local database)

The syntax for a method list is as follows:

aaa type { default | list-name} method-1 [ method-2 method-3 method-4]

Given the AAA command:

aaa authentication login default group radius local

In the above command:

1. AAA type is authentication login
2. The named list is the default one (default).
3. There are two authentication methods (group radius and local).

All users are authenticated using the Radius server (the first method). If the Radius server doesn't respond, then the router's local database is used (the second method). For local authentication, define the username and password: username xxx password yyy

Because we are using the list default in the aaa authentication login command, login authentication is automatically applied for all login connections (such as tty, vty, console and aux)

The command : **aaa authentication login CONSOLE line**

In the above command:

i) The named list is CONSOLE.
ii) There is only one authentication method (line).

Once a named list (in this example, CONSOLE) is created, it must be applied to a line or interface for it to come into effect. This is done using the login authentication list name command:

line con 0
exec-timeout 0 0
password cisco
login authentication CONSOLE

You need to enter the password "cisco" (configured on line con 0) to get console access. The default list, if specified, is used on tty, vty and aux.

You need to use the login local command to authenticate with the local database or the login authentication {default | list_name} command to authenticate with an AAA server

**The following are the important features of RADIUS server:**

1. Open standard, and widely supported. Note that TACACS+ is a Cisco proprietary standard, but well supported too.

2. Uses UDP port

3. Provides extensive accounting capability when compared with TACACS+ server

4. Only the password is encrypted in packets transiting between the RADIUS server and the client (any device acting as client, such as a router or a switch or a host computer). On the other hand, TACACS+ provides complete encryption for communication between the TACACS+ server and the client.

5. There is a new upgrade expected, named Diameter.

6. Creating the method list.

**R1(config)# aaa authentication login AUTHLIST local**

Applying the method list to the VTY lines 0-4

**R1(config)# line vty 0 4**
**R1(config-line)# login authentication AUTHLIST**
**R1(config-line)# exit**

With respect to the given command "test aaa group tacacs+ admin Frisco123 legacy ", the following are true:

a. It enables you to verify that the ACS to router authentication component is working

b. Frisco123 is the shared secret that has been configured on the ACS server

c. It tests the reachability of ACS server

d. tacacs+ is the group name

**The sequence of steps in creating and applying a method list on a router are:**

a. Enable AAA

b. Create method lists for authentication. You may create more than one method. The second method (local) is used only when the first method fails.

c. Apply the method lists per line/per interface

Typical configuration commands for enabling AAA, and creating a list method AUTHLIST, and applying the same on vty lines is given below:

**Frisco(config)# aaa new-model**
**Frisco(config)# aaa authentication login AUTHLIST local**
**Frisco(config)# line vty 0 4**
**Frisco(config-line)# login authentication AUTHLIST**

i. Granular control : TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. TACACS+ is very commonly used for device administration.

ii. TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.

iii. TACACS+ is a Cisco proprietary protocol (later became an Open standard), and very widely supported by various vendors offering AAA servers. Note that RADIUS is an Open Standard and widely supported too.

iv. TACACS+ uses TCP port (port #49) to communicate between the server and the client.

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-10.htm



## 3.0 Infrastructure Security

### 3.2 Troubleshoot router security features

**IPv4 access control lists (standard, extended, time-based)**

The mask address 0.0.0.255 specifies that the first three octets should match the given IP address (in this case 192.168.1) to permit the ip traffic. 255 in the last octet indicates that the router can ignore the last octet of the IP address being filtered.

If you add an access list to an interface and you do not have at least one permit statement, then you will effectively shut down the interface because of the implicit deny any at the end of every list.

The following statements permits access to VTYs (Router command prompt) from the 192.168.1.0/24 netblock while denying access from everywhere else:

RTA(config)#access-list 1 permit 192.168.1.0 0.0.0.255
RTA(config)#line vty 0 4
RTA(config-line)#access-class 1 in

Standard ACLs: Standard ACLs control traffic by the comparison of the source address of the IP packets to the addresses configured in the ACL.

This is the command syntax format of a standard ACL.

access-list access-list-number {permit|deny}
{host|source source-wildcard|any}

In all software releases, the access-list-number can be anything from 1 to 99. In Cisco IOS Software Release 12.0.1, standard ACLs begin to use additional numbers (1300 to 1999). These additional numbers are referred to as expanded IP ACLs. After the ACL is defined, it must be applied to the interface (inbound or outbound).

Extended ACLs: Extended ACLs control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL. In all software releases, the access-list-number can be 100 to 199. In Cisco IOS Software Release 12.0.1, extended ACLs begin to use additional numbers (2000 to 2699). These additional numbers are referred to as expanded IP ACLs.

An example configuration for extended ACL is given below. Note that www is a TCP protocol.:

access-list 100 deny tcp host 10.0.0.2 host 10.0.1.2 eq www
access-list 100 permit ip any any
interface fastEthernet 0/0
ip access-group 100 in

Observe that the command "ip access-group 100 in" applies the access list to the interface fe 0/0.

IP Named ACLs: The standard and extended ACLs to be given names instead of numbers

This is the command syntax format for IP named ACLs.

**ip access-list {extended|standard} name**

**IPv6 traffic filter**

Here we see that the IPv6 access list called "acltest" is being applied to incoming VTY connections to the router. IPv6 access list has just one entry, which allows only the single IPv6 IP address of 2001:DB8:0:4::32 to connect using SSH only.

Wild card masking: Wild card masking is used to permit or deny a group of addresses. For example, if we have a source address 185.54.13.2 and want all the hosts on the last octet to be considered, we use a wild card mask, 185.54.13.255.

Special cases : Host 185.54.13.2 is same as 185.54.13.2 with a wild card mask of 0.0.0.0, considers only specified IP.

Any is equivalent to saying 0.0.0.0 with a wild card mask of 255.255.255.255. This means none of the bits really matter. All IP addresses need to be considered for meeting the criteria.

The syntax for configuring ipv6 ACL is as given below:

deny | permit <protocol>
{ source-ipv6-prefix / prefix-length | any | host source-ipv6-address } [ operator [ port-number ]] {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address } [ operator [ port-number ]] [ dscp value ] [ fragments ] [ log ] [ log-input ] [ sequence value ] [ time-range name ]

The command "permit tcp any host 2001:DB8:10:10::100 eq 25" command permits traffic from any host to an SMTP server on network 2001:DB8:10:10::/64

Some of the widely used port numbers are given below:

| Port Number | Description |
|---|---|
| 21 | FTP |
| 22 | SSH |
| 23 | Telnet |
| 25 | Simple mail Transfer Protocol |

**The following are the key similarities and differences between ipv4 and ipv6 ACLs:**

1. Ipv4 uses both numbered and named access lists whereas Ipv6 uses named access lists only.

2. IPv4 ACLs are typically written as a sequence of permit statements that include an implicit deny clause as their last line. Although this implicit deny is also present on IOS IPv6 ACLs, there are a couple of things to be aware of:

There are other implicit permit statements designed to allow two of the main Neighbor Discovery (ND) messages: permit icmp any any nd-na (which handles Neighbor Advertisement messages) and permit icmp any any nd-ns (which takes cares of Neighbor Solicitation messages).

If your environment requires Router Advertisement (RA) and Router Solicitation (RS) messages to be allowed, these lines will need to be configured explicitily (in the same way as the regular permits).

In the event you add an explicit deny as the last line of the ipv6 ACL, this statement will take precedence over the implicit permits earlier described (for nd-na and nd-ns).

Both ipv4 and ipv6 ACLs can match on specific values unique to ipv4 and ipv6 header respectively. Note that Ipv4 can not match values on Ipv6 header and vice versa.

Ipv4 ACLs can match only on Ipv4 packets, and Ipv6 ACLs can match only on Ipv6 packets.

**Ipv6 configuration looks like this**

interface FastEthernet0/1
ipv6 traffic-filter Deny_Subnet_A_IPv6 out
ipv6 access-list Deny_Subnet_A_IPv6
deny ipv6 2001:DB8:0:100::/64 any
permit ipv6 any any

Unicast 6to4 addresses (2002::/16) are used to communicate between two IPv6/IPv4 nodes over the IPv4 Internet. A 6to4 address combines the prefix 2002::/16 with the 32 bits of the public IPv4 address of the node to create a 48-bit prefix - 2002:WWXX:YYZZ::/48, where WWXX:YYZZ is the colon-hexadecimal representation of w.x.y.z, a public IPv4 address.

**The syntax for configuring ipv6 ACL is as given below:**

deny | permit <protocol>
{ source-ipv6-prefix / prefix-length | any | host source-ipv6-address } [ operator [ port-number ]] {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address } [ operator [ port-number ]] [ dscp value ] [ fragments ] [ log ] [ log-input ] [ sequence value ] [ time-range name ]

The command "deny tcp any any eq telnet" command restricts any host telnetting to any destination host

IP access lists are a sequential list of permit and deny conditions that apply to IP addresses or upper-layer protocols. Access Control Lists are used in routers to identify and control traffic.

There are two types of IP access lists:

1. Standard IP Access Lists: These have the format,

access-list [number] [permit or deny] [source_address]

Keep in mind that:

- Place standard access lists as near the destination as possible and extended access lists as close to the source as possible.

- Access lists have an implicit deny at the end of them automatically. Because of this, an access list should have at least one permit statement in it; otherwise the access list will block all remaining traffic.
- Access lists applied to interfaces default to outbound if no direction is specified.

2. Extended IP Access Lists: IP Extended Access lists have the format,

access-list {number} {permit or deny} {protocol} {source} {destination} {port}

**With extended IP access lists, we can act on any of the following:**

- Source address

- Destination address

- IP protocol (TCP, ICMP, UDP, etc.)

- Port information (WWW, DNS, FTP, etc.)

**The permitted numbers for some important access-lists are:**

1-99 : IP standard access list

100-199 : IP extended access list

800-899 : IPX standard access list

900-999 : IPX extended access list

1000-1099 : IPX SAP access list

1100-1199 : Extended 48-bit MAC address access list

**Unicast reverse path forwarding (uRPF)**

uRPF(Unicast Reverse Path Forwarding): uRPF is used to prevent common spoofing attacks. The router will actually rely on the CEF table to perform lookups. uRPF works in 2 modes strict mode and loose mode.

Strict Mode: In this mode the router verifies the source of the IP packet arrives on the same interface the router would use to reach that source address. Beware of asymmetric routing.

Loose Mode: In this mode the router simply verifies the source IP can be reached via the CEF table using any interface.

ip verify unicast source reachable-via rx configures URF in strict mode

ip verify unicast source reachable-via any configures URF in loose mode

The allow-default option may be used with either the rx or any option to include IP addresses not specifically contained in the routing table. The allow-self-ping option should not be used because it could create a denial of service condition. An access list such as the one that follows may also be configured to specifically permit or deny a list of addresses through Unicast RPF

Ex: interface FastEthernet 0/0

ip verify unicast source reachable-via {rx | any} [allow-default]

[allow-self-ping] [list]

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes



## 3.0 Infrastructure Security

### 3.3 Troubleshoot control plane policing (CoPP) (Telnet, SSH, HTTP(S), SNMP, EIGRP, OSPF, BGP)

This protocol can collects and manipulate valuable network information from switches, routers, servers, printers, and other network-attached devices.

**An SNMP-managed network consists of two components:**

**Network management station (NMS):** the software which runs on the administrative computer. This software gathers SNMP data by requiring the devices on the network to disclose certain information. Devices can also inform the NMS about problems they are experiencing by sending an SNMP alert (called a trap).

**Agent:** the software which runs on managed devices and reports information via SNMP to the NMS.

SNMP agents use a UDP port 161, while the manager uses a UDP port 162. The current SNMP version is SNMPv3. The prior versions, SNMPv1 and SNMPv2 are considered obsolete.

**The following security levels and encryption are available in SNMPv3:**

**NoAuthNoPriv -** Uses only User Name for authentication and no encryption or privacy.

**AuthNoPriv -** Provides authentication based on the Hashed Message Authentication Code (HMAC)- MD5 or HMAC-SHA algorithms

**AuthPriv -** Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. In addition to authentication, provides DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES (DES-56) standard.

Note that there is no such "AuthEncr" level.

**IGMP:** The Internet Group Management Protocol is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast.

**ICMP:** The Internet Control Message Protocol is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.

To measure end-to-end response time we have to use ICMP echo to continuously ping to a remote device. The difference between ICMP path echo and ICMP echo is the former can measure hop-by-hop response time on its whole path while the latter can only measure to a specific destination.

A BGP speaking router will have two tables: one for IP routing information, and the other for BGP information. It is possible to share the information between the two tables.

The traceroute command allows you to determine the path a packet takes in order to get to a destination from a given source by returning the sequence of hops (with IP addresses) the packet has traversed. This utility comes with your host operating system (for example, Linux or Microsoft (MS) Windows), as well as with Cisco IOS® Software. The traceroute command is a privileged EXEC command in Cisco IOS.

**SNMPv3 Agent supports the following set of security levels as defined in the USM MIB (RFC 2574) :**

**noAuthnoPriv -** Communication without authentication and privacy.

**authNoPriv -** Communication with authentication and without privacy. The protocols used for Authentication are MD5 and SHA (Secure Hash Algorithm).

**authPriv -** Communication with authentication and privacy. The protocols used for Authentication are MD5 and SHA ; and for Privacy, DES (Data Encryption Standard) may be used.

You can configure MD5 authentication between two BGP peers, and the password must be same on both BGP peers; otherwise, the connection between them will not succeed. There are two cases with setting up of MD5 authentication:

a. If a router has a password configured for a peer, but the other peer does not, a message "No MD5 digest from" will appear on the console while the routers attempt to establish a session between them. Therefore A is correct because Router NY (with an ip address of 10.0.0.1) is not configured with a password.

b. If the two routers have different passwords configured, a message "Invalid MD5 digest from" will show up in the debug output.

To distribute Border Gateway Protocol (BGP) neighbor information as specified in an access list, use the neighbor distribute-list command in address family or router configuration mode.

To distribute Border Gateway Protocol (BGP) neighbor information as specified in a prefix list, use the neighbor prefix-list command in address family or router configuration mode.

The following router configuration mode example applies the prefix list named mylist1 to outgoing advertisements from the neighbor 192.10.0.0:

router bgp 100
network 120.101.0.0
neighbor 192.10.0.0 prefix-list mylist1 out

The following are a few examples of how a prefix list can be used (while configuring BGP policies to filter route updates):

To deny the default route 0.0.0.0/0:
ip prefix-list mylist1 deny 0.0.0.0/0

To permit the prefix 20.0.0.0/8:
ip prefix-list mylist1 permit 20.0.0.0/8

**The following examples show how to specify a group of prefixes.**

To accept a mask length of up to 24 bits in routes with the prefix 192/8:

**ip prefix-list mylist1 permit** *192.0.0.0/8 le 24*

To deny mask lengths greater than 25 bits in routes with a prefix of 192/8:

**ip prefix-list mylist1 deny** *192.0.0.0/8 ge 25*

The command "**show ip bgp neighbors**" is most useful in troubleshooting BGP connections. When the connection is established, the peer/neighbor router exchanges BGP information. If a TCP connection (BGP session) is not established, a BGP router can not exchange any BGP routing information with the adjacent router with which it is trying to establish neighbor relationship.

```
RouterA#sh ip bgp neighbors
BGP neighbor is 10.10.1.1, remote AS 100, external link
  -----Omitted-----
BGP version 4, remote router ID 170.215.1.1
BGP state = Established, table version =5, up for 00:52:12
Last read 00:01:40, hold time is 180, keepalive interval is 60 seconds
Minimum time between advertisement runs is 30 seconds
Received 18 messages, 0 notifications, 0 in queue
Sent 17 messages, 0 notifications, 0 in queue
Prefix advertised 1, suppressed 0, withdrawn 0
Connection established 1, dropped 0
Last reset 00:20:33, due to peer closed the session
----omitted---
```

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-12.htm



## 3.0 Infrastructure Security

### 3.4 Describe IPv6 First Hop security features (RA guard, DHCP guard, binding table, ND inspection/snooping, source guard)

**IPv6 First-Hop Security Features**

**1. Router Advertisement (RA) Guard:** is a feature that analyzes RAs and can filter out unwanted RAs from unauthorized devices.

**2. DHCP guard:** The DHCPv6 Guard feature blocks reply and advertisement messages that come from unauthorized DHCP servers and relay agents

**3. Binding Table:** The binding table is a database that lists IPv6 neighbors that are connected to a device.

4**. IPv6 neighbor discovery inspection/snooping:** It is a feature that learns and populates the binding table for stateless auto-configuration addresses.

**5. Source guard:**IPv6 Source Guard is a Layer 2 snooping interface feature for validating the source of IPv6 traffic. If the traffic arriving on an interface is from an unknown source, IPv6 Source Guard can block it.

6. It is likely that the DHCP information available with the client workstation had become obsolete. Issuing "ipconfig" command with /release and /renew commands will enable the client workstation to obtain latest changes to the DHCP server.

1. **Router#show ip dhcp conflict:** This command shows information about IP conflicts that are detected during the DHCP negotiation. IP conflicts occur when hosts have statically assigned IP addresses that are within the DHCP configured range, but are not excluded.

2. **Router>show ip dhcp binding [IP-address]** The following examples show the DHCP binding address parameters, including an IP address, an associated MAC address, a lease expiration date, and the type of address assignment that have occurred.

Example:**Router>show ip dhcp binding 172.16.1.11**

IP address Hardware address Lease expiration Type 172.16.2.22 00a0.9802.32fc Feb 21 2016 12:00 AM Automatic

3. To display Cisco IOS DHCP Server database agent information, use the show ip dhcp database privileged EXEC command.

**show ip dhcp database [url]**

Related command: **ip dhcp database**: Configures a Cisco IOS DHCP Server to save automatic bindings on a remote host called a database agent.

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-13.htm



## 4.0 Infrastructure Services

### 4.1 Troubleshoot device management

**Console and VTY**

Because the "service password-encryption" is not set on RouterA, so the password to access privileged mode (via the command "enable password cisco") is unencrypted. Also, the password for VTY is unencrypted (notice that the password "cis@clr!" is unencrypted).

The banner is not appropriate and provides information on the router, which can be considered as a security threat. The banner login, is supposed to be a permanent "do not enter if you dont belong message".

In the line vty 0 4? configuration, the password is not encrypted.

a. We can telnet from line 0 to line 4 (line vty 0 4).

b. We can use both telnet and SSH to connect to this router.

c. By default, the timeout is set to 10 minutes on both the console and the vty ports.

d. NAT Console password is not encrypted.

a. Privilege mode on RouterA is protected with unencrypted password (via "enable password" command)

b. It is the default exec time-out.

c. The password of VTY lines is configured in plain text. It is a good practice to encrypt passwords.

d. The config command username cisuser privilege 15 password 0 Cisco enables one to enter highest privileged mode. This may be a security risk. It is recommended to configure multiple levels of privileges.

Each Telnet port is known as a virtual terminal. There are a maximum of five virtual terminal (VTY) ports, allowing five concurrent Telnet sessions. Please note that the communication server provides more VTY ports. The virtual terminal ports are numbered from 0 through 4.

The console and auxiliary ports on Cisco IOS routers and switches are asynchronous serial ports and use asynchronous protocols such as PPP, SLIP, and ARA.

**The Cisco router can be configured from many locations.**

**1. Console port:** During the initial installation, you configure the router from a console terminal connected to the "Console port" of the router.

**2. Virtual Terminals (vty):** A virtual terminal (vty) is typically accessed through Telnet. A router can be accessed through vty after the initial installation in the network. There are five virtual terminals, namely, vty0,vty1,vty2,vty3,vty4.

**3. Auxiliary Port:** you can configure a router through auxiliary port. Typically, a modem is used to configure the modem through aux port.

**4. TFTP Server:** Configuration information can be downloaded from a TFTP server over the network.

**5. NMS (Network Management Station):** You can also manage router configuration through NMS such as CiscoWorks or HP OpenView.

The auxiliary password is used to set the password for the auxiliary port.

Assuming that you are at # prompt, the sequence of commands are:

RouterA#config t
RouterA(config)#line aux 0
RouterA(config-line)#login
RouterA(config-line)#password <password>

Now you are set with a password <password>. Type "<ctrl>Z " to take you to the # prompt or "exit" to go back to global configuration "RouterA(config)#" prompt.

**Telnet, HTTP, HTTPS, SSH, SCP,TFTP**

**Telnet** is a terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

**FTP** is the abbreviation of File Transfer Protocol, the protocol used on the Internet for sending files.

**SSH (Secure SHell)** is a protocol for remotely logging into a machine via a shell. It is very similar in functionality to telnet, however unlike telnet, all data between the client and server is encrypted.

**SCP** is Secure CoPy, a protocol to allow you to transmit files from one machine to another with the encryption benefits of SSH. Most SSH clients include SCP capability. In the future, we will be disabling FTP due to the same security problems as telnet, and at that time SCP will be one way for you to transfer files between machines. When we get closer to disabling FTP, more information on this will be made available.

**TFTP** can be used to download configuration files. However, note that TFTP (Trivial File Transfer Protocol) is known as unreliable protocol since it does not incorporate any error correction and packet sequencing. TFTP does not use passwords and hence considered insecure.

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-14.htm



## 4.0 Infrastructure Services

### 4.2 Troubleshoot SNMP (v2c, v3)

Internet Protocol (IP) networks use managing devices such as Simple Network Management Protocol (SNMP) to monitor network attached devices. In a computer network, a group of devices are attached, and they are managed and monitored by a manager. An agent, which is a software module in a managed device, reports information through the SNMP to the manager which has a Network Management System (NMS) that executes the applications that monitor and control managed devices.

**There are seven SNMP protocol data units (PDU):**

1. GetRequest - request to retrieve the value of a variable from the manager to the agent.

2. SetRequest - request to change the value of a variable from the manager to the agent.

3. GetNextRequest - request to find variables from the manager to the agent.

4. GetBulkRequest - enhanced version of GetNextRequest.

5. Response - reply from the agent to the manager through the return of variables.

6. Trap - simultaneous message from the agent to the manager.

7. InformRequest - simultaneous messages between managers.

**There are three versions of SNMP:**

1. SNMPv1, which is the network management protocol being used by the Internet.

2. SNMPv2, which is a revised version of the SNMPv1. It contains improvements in performance, confidentiality, security, and communications between managers. Its party-based security system is very complex, though, and has to be revised in order to be able to use it with the SNMPv1.

3. SNMPv3, which has added cryptographic security and new concepts, terminology, remote configuration enhancements, and textual conventions.

The main difference between SNMP v3 and v2 (or v1) is that the v3 version addresses the security and privacy issues. For example, in SNMP v2, passwords are transmitted in plain text, whereas v3 uses encryption.

**The advantages are given below, in brief:**

1. Authentication

2. Privacy

3. Authorization and Access Control

4. Remote configuration and administration capabilities

| Security Model | Security Level | Authentication | Encryption Type |
|---|---|---|---|
| SNMPv1 | noAuthNoPriv | Community string | None |
| SNMPv2c | noAuthNoPriv | Community string | None |
| SNMPv3 | noAuthNoPriv | User name | None |
| | AuthNoPriv | MD5 or SHA | None |
| | authPriv | MD5 or SHA | CBC-DES (DES-56) |

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-15.htm



## 4.0 Infrastructure Services

### 4.3 Troubleshoot network problems using logging (local, syslog, debugs, conditional debugs, timestamps)

In the command sequence given below:

CertExamsR1#configure terminal
CertExamsR1(config)#logging buffered 4048 0
CertExamsR1(config)#exit
CertExamsR1#

the statement "logging buffered 4048 0" enables the syslog messages to be sent to the router/switch memory, and allocates 4048 bytes of router or switch memory (RAM). Once the buffer is full, the router deletes old messages from the buffer as new messages are added (First in first out).

"0" represents the severity level of the syslog message that needs to be sent to the memory. As can be seen from the table below, severity level "0" represents emergency messages. Severity level may have values ranging from 0 to 7 as given in the table below:

0 - Emergency (System is unusable)

1 - Alert (Action must be taken immediately)

2 - Critical (Critical conditions)

3 - Error (Error conditions)

4 - Warning (Warning conditions)

5 - Notice (Normal but significant condition)

6 - Informational (Informational messages)

7 - Debug (Debug-level messages)

The default level for console, monitor, and syslog is debugging. By default, the router logs anything at the level of debugging and greater. That means that logging occurs from level 7 (debugging) up to level 0. The logging on command is the default. To disable all logging, use the no logging on command.

**Cisco routers log messages can handle in five different ways:**

**Console logging:**By default, the router sends all log messages to its console port. Hence only the users that are physically connected to the router console port can view these messages.

**Terminal logging:**It is similar to console logging, but it displays log messages to the router's VTY lines instead. This is not enabled by default.

Use the following commands to collect the Syslog messages when you are connected to an SSH terminal.

CertExamsR1#terminal monitor

**Buffered logging:**This type of logging uses router's RAM for storing log messages. buffer has a fixed size to ensure that the log will not deplete valuable system memory. The router accomplishes this by deleting old messages from the buffer as new messages are added.

Use the following commands to store the Syslog messages in Cisco Router's / Switch's memory. "4048" is the size of memory allocated to store Syslog messages and "0" is the severity level.

```
CertExamsR1#configure terminal
CertExamsR1(config)#logging buffered 4048 0
CertExamsR1(config)#exit
CertExamsR1#
```

**Syslog Server logging:**The router can use syslog to forward log messages to external syslog servers for storage. This is considered to be the best practice as there is no loss of data (huge storage capacities) and there is no overload on the router or switch as in the case of buffered logging. A syslog server also provides for centralized logging for all network devices.

Use the following commands to send Syslog messages to a Syslog server, configured at 192.168.1.100.

```
CertExamsR1#configure terminal
CertExamsR1(config)#logging 192.168.1.100
CertExamsR1(config)#exit
CertExamsR1#
```

**SNMP trap logging:**The router can send syslog message to an external SNMP server. This is accomplished using SNMP trap.

From the show logging command output, we can interpret that the router has the following logging configuration:

1. Syslog logging and is sending it to host 10.2.2.2,

2. In addition, console logging is at the debugging level, and

3. The setting for local buffered logging is 1048576 bytes.

By default, the timestamps are in hr:min:sec. If you want to enable greater resolution, you can enable millisecond level resolution by using the command "service timestamps log datetime msec"

**The syntax is as given below:**

Router(Config)#service timestamps log {uptime |datetime [msec |localtime |show-timezone]} The options are self explanatory.

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-16.htm



## 4.0 Infrastructure Services

### 4.4 Troubleshoot IPv4 and IPv6 DHCP (DHCP client, IOS DHCP server, DHCP relay, DHCP options)

**The DHCP Discover message is sent as a broadcast on the network.DHCP messages are as below:**

DHCP DISCOVER: broadcast the client computer sends out a broadcast on the LAN because it does not know where the DHCP server is.

DHCP OFFER: unicast. The broadcast is received by the DHCP server and it responds with a DHCP offer which contains an IP address, Subnet Mask and Default Gateway and any other optional information (configured on the DHCP server).

DHCP REQUEST:broadcast. The client computer gets the IP info, with the corresponding Subnetmask and Default Gateway, from the DHCP server. When the client computer decides it is going to use the IP address, it lets the DHCP server know that it will accept the IP address that was send by the DHCP server. So it send out a request, asking the DHCP server if it can use the information/IP provided by the DHCP server. The Client does this by the means of unicast. The client computer now knows what IP address the DCHP server uses and send this message as a unicast.

DHCP ACK: broadcast or unicast.The DHCP Request comes in at the DHCP server and the DHCP server will then send a DHCP ACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested.

**clear ip dhcp conflict * - Clears all ip address conflicts.**

clear ip dhcp server statistics - DHCP server counters will be initialized, or set to zero, with the clear ip dhcp server statistics command.

clear ip dhcp binding * Clears all automatic bindings.

clear ip dhcp binding a.b.c.d - deletes the specified address binding from DHCP server database

## 4.5 Troubleshoot network performance issues using IP SLA (jitter, tracking objects, delay, connectivity)

Cisco IP SLA can be done between two Cisco devices or between a Cisco device and another vendor's device. There are different network components that have different roles in the network. These are:

**IP SLA Source:** is a Cisco device that generates the simulated traffic to a Cisco device IP SLA Responder or to any ip device.

**IP SLA Responder:** is a component in remote Cisco device that receives and sends the traffic with the help of IP SLA Control Protocol. Only Cisco devices can be an IPSLA Responder.

**IP SLA Control Protocol** is the protocol used by IPSLA Responder to determine which port to listen and to respond.

Any IP Device is the device if you use IP SLA between Cisco device and it.

**Performance Management Application** is the program that the performance analyze is done.

Cisco IP SLA can be done between two Cisco devices or between a Cisco device and another vendor's device. There are different network components that have different roles in the network. These are:

**IP SLA Source:** is a Cisco device that generates the simulated traffic to a Cisco device IP SLA Responder or to any ip device.

**IP SLA Responder:** is a component in remote Cisco device that receives and sends the traffic with the help of IP SLA Control Protocol. Only Cisco devices can be an IPSLA Responder.

IP SLA Control Protocol is the protocol used by IPSLA Responder to determine which port to listen and to respond.

Any IP Device is the device if you use IP SLA between Cisco device and it.

Performance Management Application is the program that the performance analyze is done.

**ip sla operation-number :** Defines an IP SLA object and enter IP SLA configuration mode. The operation-number is the identification number of the IP SLAs operation you want to configure SLAs operation you want to configure. Once entered, the router prompt changes to IP SLA configuration mode.

**UDP Jitter:** Measures round-trip delay, one-way delay,one-way jitter, one-way packet loss, and connectivity testing of networks that carry UDP traffic, such as voice. Note that one-way delay requires time synchronization between source and target routers.

**ICMP Path Jitter:** Measures hop-by-hop jitter, packet loss, and delay measurement statistics in an IP network.

**UDP Echo:** Measures round-trip delay of UDP traffic.

**ICMP Echo:** Measures round-trip delay for the full path.

**show ip sla configuration:** Displays configuration values including all defaults for all Cisco IOS IP SLAs operations, or for a specified operation.

**show ip sla statistics:** Displays the current operational status and statistics of all Cisco IOS IP SLAs operations, or of a specified operation.

To verify the operation of the IP SLA responder, use the command show ip sla responder

Previous Contents Next

# CCNP ENARSI 300-410 Exam Cram Notes

examguides.com/CCNP-ENARSI/ccnp-enarsi-cramnotes-17.htm



## 4.0 Infrastructure Services

### 4.6 Troubleshoot NetFlow (v5, v9, flexible NetFlow)

**show ip cache flow:** Displays a summary of the NetFlow switching statistics.

**show ip flow interface:** Displays NetFlow switching configuration for interfaces.

**show ip flow export:** Displays the current NetFlow configuration

**show flow timeout:** Displays information about NetFlow timeouts

NetFlow collection is enabled on an interface-by -interface basis, and it is unidirectional. This means you can enable it to capture traffic inbound on an interface with the ip flow ingress command or outbound on an interface with the ip flow egress command.

Flexible NetFlow is basically an extension of NetFlow v9. Flexible NetFlow provides enhanced optimization, reduces costs and improves capacity planning and security detection beyond traditional flow technologies. Flexible NetFlow, similar to traditional Netflow, requires CEF to be enabled for IPv4 and IPv6. So, if you are using NetFlow for IPv4, the command ip cef is required, and if you are using NetFlow for IPv6, the command ipv6 cef is required. Use the commands show ip cef and show ipv6 cef to verify whether NetFlow for IPv4 and IPv6 are running.

You can verify the version of NetFlow that is being used for export by using the "show ip flow export" command. To display the status and the statistics, including the main cache and all other enabled caches, use the "show ip flow export" command in user EXEC or privileged EXEC mode.

## 4.7 Troubleshoot network problems using Cisco DNA Center assurance (connectivity, monitoring, device health, network health)

Cisco DNA Assurance delivers comprehensive network visibility. With it, you can easily manage all your connected devices and services, prioritize and resolve network issues with the help of machine learning, and ensure a better user experience across the network.

**Categories in All Issues of Cisco DNA Center Assurance is as follows**

1. Onboarding - Displays the wireless and wired client onboarding issues.

2. Connectivity- Displays network connectivity issues, such as OSPF, BGP tunnels, and so on.

3. Connected- Displays issues related to clients.

4. Device - Displays device-related issues, such as CPU, memory, fan, and so on.

5. Availability- Displays device availability issues for APs, wireless controllers, and so on.

6. Utilization- Displays utilization issues of APs, wireless controllers, radios,and so on.

7. Application - Displays Application Experience issues.

8. Sensor Test- Displays sensor global issues.

A troubleshooting feature in DNA Center Assurance ,with Path Trace, you can graphically see the path that applications and services running on a client will take through all the devices on the network to reach the destination.

**Device 360 and client 360:** An Assurance feature allowing viewing and troubleshooting devices or clients from any angle or context. These features display information about the topology, throughput, and latency from various times and applications so you can get a detailed view on the performance of the specific device or client over a specified period.

**Network Time Travel:** Allows the operator to see device or client performance in a timeline view to understand the network state when an issue occurred. Allows an operator to go back in time up to 14 days and see the cause of a network issue, instead of trying to re-create the issue in a lab.