Cisco® CCNP Route Exam Notes : Identifying Cisco Express Forwarding Concepts

examguides.com/CCNP-Route/ccnp-routing-1.htm

1. Network Principles

1.1 Identify Cisco Express Forwarding concepts

Cisco Express Forwarding (CEF) is a Cisco proprietary Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet. It is most suitable on networks characterized by intensive Web-based applications, or real-time inter-active use such as video conferencing sessions.

CEF offers the following benefits

Improved performance: By design, CEF is less CPU-intensive than fast switching route caching. By using CEF, more CPU processing power can be utilized to Layer 3 services such as quality of service (QoS) and encryption.

Scalability: CEF offers full switching capacity at each line card when dCEF mode is active, thus ensuring scalability of operation.

Resilience: CEF aims at providing better switching consistency and stability in large dynamic networks. In dynamic networks, fast-switched cache entries are frequently invalidated due to routing changes. These changes can cause traffic to be process switched using the routing table, rather than fast switched using the route cache. Because the

Forwarding Information Base (FIB) lookup table contains all known routes that exist in the routing table, it eliminates frequent route cache maintenance, thereby enabling CEF to switch traffic more efficiently than typical demand caching schemes.

CEF Components: The two main components of CEF are

FIB (Forwarding Information Base): CEF uses an FIB to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next hop address information based on the information in the IP routing table. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths such as fast switching and optimum switching.

Adjacency Tables: Nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. In addition to the FIB, CEF uses adjacency tables to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Ipv4 And Ipv6 Fragmentation

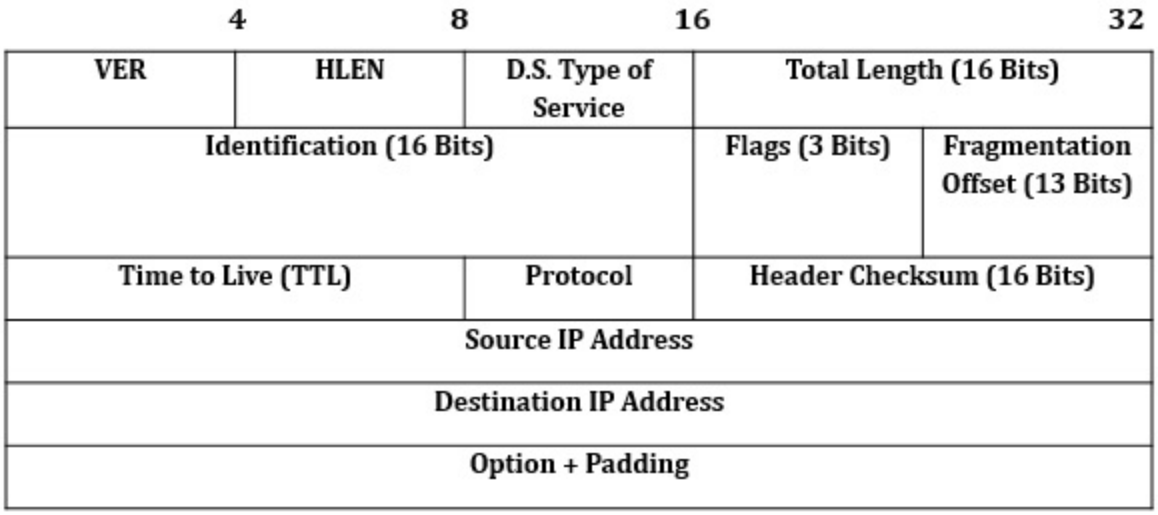
examguides.com/CCNP-Route/ccnp-routing-2.htm

1. Network Principles

1.2 IPv4 and IPv6 fragmentation

IP Fragmentation: is an Internet Protocol (IP) process that breaks packets into smaller pieces (fragments), so that the resulting pieces can pass through a link with a smaller maximum transmission unit (MTU) than the original packet size. The fragments are reassembled by the receiving host.

IPv4 Fragmentation: An IP v4 header format is given below:



The following list describes the function of each header field.

- **Version:** This Field defines the version of IP. It is Static 4 bit value.
- **Header Length:** This Field defines the length of the datagram . It is 4 bit value.
- **Type of Service:** It is 8 bit value. It is used tell the network how to treat the IP packet. These bits are generally used to indicate the Quality of Service (QoS) for the IP Packet.
- **Packet Length:** 16 bit value indicating the size of the IP Packet in terms of bytes. This gives a maximum packet size of 65536 bytes.
- **Identification:** 16 bit field used for reassembling the packet at the destination.

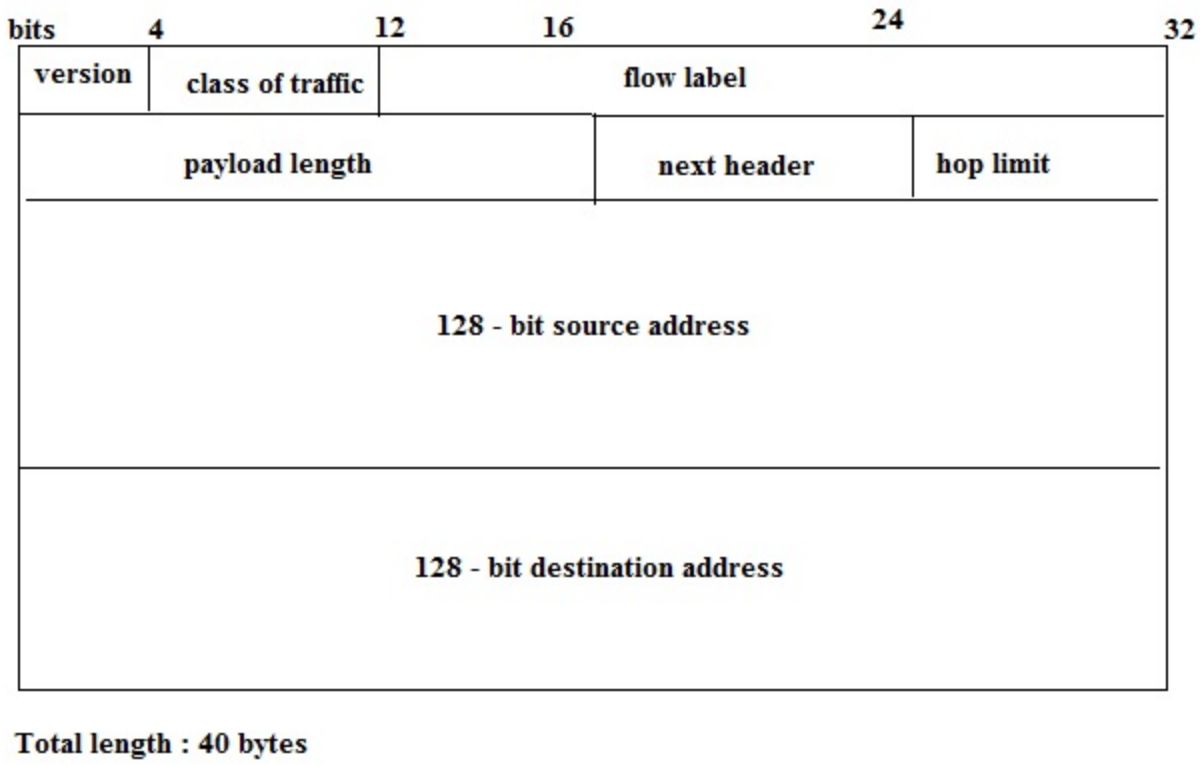
- **Flags:** It is 3 bits value. It indicates if the IP packet can be further fragmented or not and if the packet is the last fragment or not of a larger transfer.
- **Fragment offset:** 13 bit value used in the reassembly process at the destination.
- **Time to Live:** 8 bit value telling the network how long an IP packet can exist in a network before it is destroyed.
- **Protocol:** 8 bit value used to indicate the type of protocol being used (TCP, UDP etc.).
- **Header checksum:** It is 16 bit value. It is used to indicate errors in the header only. Every node in the network has to check and re-insert a new checksum as the header changes at every node.
- **Source address:** 32 bit value representing the IP address of the sender of the IP packet.
- **Destination address:** 32 bit value representing the IP address of the packets final destination.
- **Options:** Options are not required for every datagram. They are used for network testing and debugging.
- **Padding:** Variable size bit field. These bits are used to ensure a 32 bit boundary for the header is achieved.

IPv6 Fragmentation: IPv6 packet is 320 bits or 40 octets long. It will have basic packet header, and optional extension header. The next header field within an extension header points to the next header in the chain. The following figure shows the fields that appear in the IPv6 header and the order in which the fields appear.

Note that there is no fragment information in Ipv6 header. In order to send a packet larger than the PMTU, an IPv6 node may fragment a packet at the source and have it reassembled at the destination.

Note that in IPv6, only hosts can fragment whereas in IPv4, both hosts and routers can fragment.

IPv6 Fragmentation has always been discouraged as the reassembly is computationally expensive and inefficient. Additionally, there are some security concerns with fragmentation.



The following list describes the function of each header field.

- **Version** - 4-bit version number of Internet Protocol = 6.
- **Traffic class** - 8-bit traffic class field.
- **Flow label** - 20-bit field. Flow label is a new field in the IPv6 header. A 6-to-4 tunnel works similarly to a manual tunnel, except that the tunnel is set up automatically. 6-to-4 tunnels use IPv6 addresses that concatenate 2002::/16 with the 32-bit IPv4 address of the edge router, creating a 48-bit prefix.
- **Payload length** - 16-bit unsigned integer, which is the rest of the packet that follows the IPv6 header, in octets.
- **Next header** - 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. Uses the same values as the IPv4 protocol field.
- **Hop limit** - 8-bit unsigned integer. Decremented by one by each node that forwards the packet. The packet is discarded if the hop limit is decremented to zero.
- **Source address** - 128 bits. The address of the initial sender of the packet.
- **Destination address** - 128 bits. The address of the intended recipient of the packet. The intended recipient is not necessarily the recipient if an optional routing header is present.

The extension header may include the following:

- Hop-by-Hop options

- Destination options
- Routing (specifies intermediate routers that the route must include forcing an administratively defined path)
- Fragment (Used to divide packets that are too large for the maximum unit (MTU))
- Authentication and Encapsulating Security Payload (ESP)

Previous Contents Next

Cisco® CCNP Route Exam Notes : Migrating Parts Of The Network To Ipv6

examguides.com/CCNP-Route/ccnp-routing-3.htm

1. Network Principles

1.3 Migrate parts of the network to IPv6

IP Fragmentation: is an Internet Protocol (IP) process that breaks packets into smaller pieces (fragments), so that the resulting pieces can pass through a link with a smaller maximum transmission unit (MTU) than the original packet size. The fragments are reassembled by the receiving host.

The main methods for ipv4 to ipv6 transition are Manual, Teredo, 6 to 4, ISATAP Tunnelling, and NAT-PT. GRE is another tunnelling technology that is similar to the other tunnelling technologies, and used for IPv4 to IPv6 tunnelling and vice versa.

GRE (Generic Routing Encapsulation): IPv6 traffic can be carried over IPv4 GRE tunnels using the standard GRE tunneling technique. The tunnels are not tied to a specific passenger or transport protocol, but in this case, carry IPv6 as the passenger protocol with the GRE as the carrier protocol and IPv4 or IPv6 as the transport protocol. The primary use of GRE tunnels is for stable connections that require regular secure communication between two edge routers or between an edge router and an end system. The edge routers and the end systems must be dual-stack implementations.

NAT-PT: The term NAT-PT stands for Network Address Translation and Protocol Translation. NAT refers to translation of an IPv4 address into an IPv6 address and vice-versa and PT stands for the translation of the IPv4 packet into a semantically equivalent IPv6 packet and vice-versa. NAT-PT allows native IPv6 hosts and applications to communicate with native IPv4 hosts and applications, and vice-versa. A NAT-PT device resides at the boundary between an IPv6 and IPv4 network. Using a protocol translator between IPv6 and IPv4 allows direct communication between hosts speaking a different network protocol. One of the benefits of NAT-PT is that no changes are required to existing hosts, because all the NAT-PT configurations are performed at the NAT-PT router. Customers with existing stable IPv4 networks can introduce an IPv6 network and use NAT-PT to allow communication without disrupting the existing network. NAT-PT is not recommended for a scenario in which an IPv6-only network is trying to communicate to another IPv6-only network via an IPv4 backbone or vice versa .

6 to 4: 6to4 enables dual-stack devices to transmit IPv6 traffic across an IPv4 backbone via 6to4 relay servers without the need to manually configure tunnels. Similar to ISATAP, the tunneled IPv6 traffic is encapsulated in IPv4 protocol packets on the IPv4 network. 6to4 may be used by an individual host, or by a local IPv6 network.

ISATAP: ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an IPv6 transition mechanism meant to transmit IPv6 packets between IPv6 and IPv4 hosts. ISATAP works by mapping an IPv4 address into the IPv6 address and requires an ISATAP gateway on the IPv6 Internet and the IPv4 Intranet. Its addresses are formatted in a very unique way. Here is an example of an ISATAP address: 2002:9D36:1:2:0:5EFE:192.168.12.9

If you look closely, you will notice that the first portion of the address, 2002:9D36:1:2:0:5EFE: is formatted like a typical IPv6 address. The subsequent portion of the address looks like an IPv4 address - 192.168.12.9. The format of this address provides some key information:

1) It is a valid IPv6 address that can be used for IPv6 communication

2) The presence of the IPv4 address indicates the IPv4 information that will be used to shuttle the IPv6 traffic over the IPv4 network.

Teredo: is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts which are on the IPv4 Internet but which have no direct native connection to an IPv6 network. Compared to other similar protocols its distinguishing feature is that it is able to perform its function even from behind network address translation (NAT) devices such as home routers.

Following are true when an ipv6 enabled router running 6 to 4 tunnel must transmit a packet to a remote IPv6 destination

- Tunneling is used when two hosts using IPv6 want to communicate through a region of IPv4.
- When a packet enters and passes through the IPv4 region, IPv6 packet is encapsulated in IPv4 packet.
- The IPv6 packet leaves the capsule when it exits the region of IPv4.
- The source and destination fields are set to IPv4 addresses of tunnel endpoints.
- The IPv4 Protocol field within the IPv4 header is set to 41 to indicate an encapsulated IPv6 packet.
- When using the tunnel, firewalls and/or routers using packet filtering must be configured to allow IPv4 Protocol 41 packets to be received and forwarded.

Unicast 6to4 addresses (2002::/16) - IPv6 uses 6to4 addresses 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. Therefore, the IPv4 address 159.60.91.119 translates into a 6to4 address prefix of 2002:9F3C:5B77 ::/48.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Describing UDP Operations

examguides.com/CCNP-Route/ccnp-routing-4.htm

1. Network Principles

1.4 Describe UDP Operations

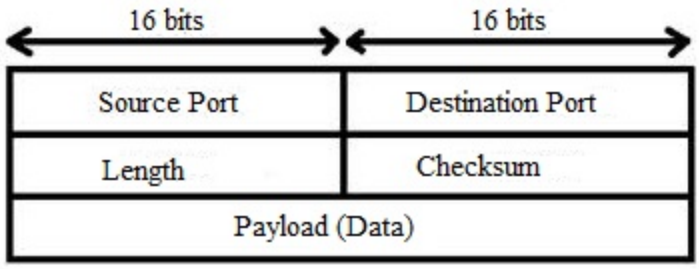
UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.

TCP uses sequence numbers for tracking the receipt of the packets at the destination. UDP is more like a telegram, and any packets that does not arrive at the destination can not be determined. This function has to be done by the application layer (or higher level protocols). Hence, it (UDP) is also known as connectionless protocol.

Udp is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from a large numbers of clients.UDP Header size is 8 bytes.

UDP does error checking but simply discards erroneous packets. Error recovery is not attempted. No Acknowledgment, No handshake (connectionless protocol)

The frame for UDP is as given below:



UDP frame fields: Total 8 bytes long.

1. Length

2. Source port

3. Destination port

4. Check Sum

Cisco® CCNP Route Exam Notes : Configure And Verify PPP

examguides.com/CCNP-Route/ccnp-routing-5.htm

2. Layer2 Technologies

2.1 Configure and verify PPP

Point-to-Point Protocol (PPP) is a Layer 2 protocol (Data-link layer) used on serial links in a Wide Area Network (WAN). PPP features two methods of authentication PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) . A connection is established between two peers only after authentication succeeds. PAP sends the password in clear text where as CHAP encrypts the password while sending over the network for authentication. PPP encapsulation is possible only over a serial link.

Config-if# encapsulation ppp

This command enables PPP encapsulation and functionality on a serial interface.

2.1.a Authentication (PAP, CHAP)

Password authentication protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) are both used to authenticate PPP sessions and can be used with many VPNs. The remote system authenticates itself by using a static user name and password combination. The password can be encrypted for additional security, but PAP is subject to numerous attacks. In particular, since the information is static, it is subject to password guessing as well as snooping.

Config-if# ppp authentication chap pap

The ppp authentication command is used to configure the PPP PAP or CHAP authentication protocols on an interface. The interface must be using ppp encapsulation to access these protocols. Enables both CHAP and PAP, and performs CHAP authentication before PAP.

2.1.b PPPoE (client side only):

PPPoE stands for Point-to-Point Protocol over Ethernet, a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. PPPoE is a networking protocol that also offers essential networking features, like authentication, encryption and compression. Because of that, PPPoE is one of the most preferred means of delivering Internet access. It is used mainly with DSL services where individual users connect to a DSL modem over Ethernet.

PPPoE uses one extra eight bytes long header which eats into the payload.

Given below are some of the important commands that you need to configure while enabling PPPoE on an Ethernet interface at the client side.

1. **encapsulation** *ppp* : Sets the datalink protocol to PPP

2. **dialer pool 1** : Used to reference a dialer pool

3. **pppoe-client dial-pool-number** *1* : Adds the interface to a pool available to dialer interfaces

4. **pppoe enable** : Enables PPPoE feature on the interface

Important show commands that are used for troubleshooting PPPoE connectivity are given below:

1. **show interfaces tunnel** <*number*> - Displays the status of a tunnel interface.

2. **show interfaces dialer** <*number*> - Displays the status of a dialer interface.

3. **show interfaces virtual-access** <*number*> - Displays the status of a virtual-access interface.

4. **show interfaces virtual-access** <*number*> configuration - Displays the configuration that IOS builds for the given virtual-access interface.

5. **show pppoe session** - Displays status out on each of the PPPoE sessions.

The following are the steps in brief for configuring a router for PPPoE operation:

Basic Layer 1 commands:

1. Configure dialer interface using the interface **dialer** <*number*> command

ex. Interface dialer

2. Configure the physical interface using the **pppoe-client dial-poo-number** <*number*> command.

ex: pppoe-client dial-pool-number 1

Basic layer 2 commands:

1. Configure ppp using encapsulation ppp command

ex. **encapsulation** *ppp*

2. Configure PPPoE on the Ethernet interface using pppoe enable command.

ex. **pppoe enable**

Basic layer 3 commands:

1. Configure IP on the dialer interface using ip address negotiated command.

ex. **ip address negotiated**

2. Disable IP on the Ethernet interface using no ip address command. Ex. no ip address

Previous Contents Next

Cisco® CCNP Route Exam Notes : Operations,Frame Relay Devices

examguides.com/CCNP-Route/ccnp-routing-6.htm

2. Layer2 Technologies

2.2 Explain Frame Relay

2.2.a Operations

Frame Relay is a WAN protocol that operates at the physical and data link layers of the OSI reference model. Frame relay is a type of WAN connection used to connect one site to many remote sites through a single physical circuit.

Frame Relay Devices: Devices attached to a Frame Relay WAN fall into the following two general categories: Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE)

DTEs are considered to be terminating equipment for a specific network and typically are located on the premises of a customer. They may be owned by the customer. DTE devices are terminals, personal computers, routers, and bridges.

DCEs are carrier-owned internetworking devices. The purpose of DCE equipment is to provide clocking and switching services in a network, which are the devices that actually transmit data through the WAN. In most cases, these are packet switches located on ISPs.

The following are true about Frame Relay

1. Frame Relay is primarily, a Layer 2 standard.

2. Frame Relay DLCIs have local significance.

3. Cisco supports three types of LMIs (Link Management Interface): cisco, ansi, and q933a

4. Cisco supports two types of Frame Relay encapsulation: cisco, and ietf. When you are connecting a Cisco router with a non-Cisco router, use ietf as the encapsulation method.

Given below are salient features of Frame Relay DLCIs:

1. DLCIs (Data Link Connection Identifier) have only local significance, It means, the end devices over FR network can have different DLCI numbers.

2. DLCI number is provided by the FR service provider. DLCI number is mapped to Layer

3 protocol address using "frame-relay map" statement.

4. DLCI numbers must be unique on a router.

Frame Relay supports two types of virtual circuits (VCs):

1. Permanent Virtual Circuits (PVCs) - These are permanently established connection that are used for frequent and consistent data transfers between DTEs across a Frame Relay cloud.

2. Switched Virtual Circuits (SVCs) - These are temporary connections used in situations requiring only occassional data transfers between DTEs across Frame Relay cloud.

The terms "Call Setup", "Data Transfer", "Idle", and "Call Termination" are associated with SVCs. Frame Relay SVCs are not widely supported by manufacturers.

When the sub-interfaces on a serial interface are to be configured for Frame Relay, each sub interface needs to be assigned individual DLCI. The following command assigns a dlci of 100 to any sub-interface is:

R(config-if)# frame-relay interface-dlci *100*

Note that prior to issuing the above command; issue the following command to get into proper sub interface configuration mode:

R(config)# interface serial0.1 point-to-point

The command "**show frame-relay lmi**" displays the LMI status,

The following is the sample output of "**show frame-rely lmi**"

```
Router# show frame-relay lmi

LMI Statistics for interface Serial3 (Frame Relay NNI) LMI TYPE = ansi
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Rcvd 11               Num Status msgs Sent 11
  Num Update Status Rcvd 0              Num St Enq. Timeouts 0
  Num Status Enq. Sent 10               Num Status msgs Rcvd 10
  Num Update Status Sent 0              Num Status Timeouts 0
```

where as the command "**show frame-relay pvc**" displays the frame-relay pvc status.

Frame Relay Generic Configuration Example

The following sample output shows a generic Frame Relay configuration on DLCI 100:

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial4/0/1:0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE (EEK UP), INTERFACE = Serial4/0/1:0.1

  input pkts 4360          output pkts 4361         in bytes 146364
  out bytes 130252         dropped pkts 3735        in pkts dropped 0
  out pkts dropped 3735             out bytes dropped 1919790
  late-dropped out pkts 3735        late-dropped out bytes 1919790
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 337       out bcast bytes 102084
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 05:34:06, last time pvc status changed 05:33:38
```

Frame Relay offers **NBMA (Non Broadcast Multi Access)** connectivity to various destinations. There might be several PVCs residing on one serial interface. A result of this would be, no broadcasts are forwarded among these PVCs due to implementation of split horizon rule Split horizon rule prevents a route from being advertised onto the same interface (through which the router was learned).

One way to allow broadcasts to propagate among these PVCs is to disable split horizon. But, this may again result in routing loops. The recommended solution to this problem is sub-interfaces. A sub-interfaces are logical subdivisions of a physical interface. Routing updates received on one sub interface can be sent to another sub interface. This enables the FR network administrator to implement the split horizon, and at the same time use multiple PVCs on one physical interface.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Frame Relay Connection Types

examguides.com/CCNP-Route/ccnp-routing-7.htm

2. Layer2 Technologies

2.2 Explain Frame Relay

2.2.b Frame Relay connection Types

Frame-Relay support point-point and multipoint connection types.

In **point-to-point connection** type, a single sub interface establishes a PVC connection to another physical interface or sub-interface.

In **multipoint connection** type, a single sub-interface is used to establish multiple PVC connections to several physical interfaces or sub-interfaces. In multipoint Frame-Relay network, split horizon rule is applicable to broadcast traffic.

Another important thing to note when configuring Frame-Relay using sub-interfaces: The physical interface on which sub-interfaces are configured would not be assigned any IP address. Even if one is assigned, it should be removed prior to configuring Frame-Relay. Note that if an IP address is assigned to a physical interface, the sub-interfaces defined within the physical interface will not receive any frames.

The correct command syntax is:

Router1(config-if)# frame-relay map <*protocol*> <*protocol-address*> <*dlci*> **[broadcast][ietf | cisco]**

Here, the protocol-address specifies the destination network protocol address.

Example: **Router1(config-if)# frame-relay map ip** 192.168.36.9 200

The following are true about Multipoint, and point-to-point Frame-Relay configuration at sub-interfaces:

1. In multipoint, all interfaces use same subnet, whereas, in point-to-point each pair requires its own subnet.

2. No IP address is defined at the physical interface, if sub-interfaces are used for frame-relay configuration.

3. Point-to-point sub-interfaces act as point-to-point leased lines.

1. You must specify either multipoint or point-to-point when configuring the frame-relay interface. There is no default configuration assumed.

2. Point-to-point configuration is good for star and partial mesh topologies, where as multipoint is suitable for full mesh topologies.

Characteristics of Frame-Relay point-to-point subinterface:

Only one DLCI can be configured per point-to-point subinterface.

The command **"frame-relay interface-dlci"** associates the selected point-to point subinterface with only one DLCI.

Sub-interfaces were originally created to take care of split-horizon issues from distance vector routing protocols over non-broadcast multiple access networks, because split horizon prevents routing updates received on one interface from retransmitting out onto the same interface. This is true even if the routing update is received on one frame relay PVC destined out to another frame relay PVC. By partitioning the frame relay network into numerous point-to point networks using subinterfaces; each new point-to-point subnetwork gets their own network number assigned. Therefore, the routed protocol views each subnetwork as if it was located on a separate interface.

- Since only one DLCI is assigned per subnet in a logical point to point interface, there is no need for Inverse ARP, since both the DLCI and IP addresses are already known.
- The IP subnet is mapped across a single virtual circuit, so only one DLCI is mapped per subinterface.

- Frame-relay map command is needed when multiple virtual circuits are being configured on one physical interface. When logical subinterfaces are used, the "frame-relay interface-dlci" command is used, not this command. In short, "Frame-relay interface-dlci" is used for point-to-point subinterfaces and "frame-relay map" is used for multipoint subinterfaces.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Address Types (unicast, Broadcast, Multicast, And Vlsm)

examguides.com/CCNP-Route/ccnp-routing-8.htm

3. Layer3 Technologies

3.1 Identify IPv4 addressing and subnetting

3.1.a Address types (Unicast, broadcast, multicast, and VLSM)

Unicast addresses are assigned to a single interface on a device. They are used for one-to-one communication.

Broadcast addresses are assigned to all interfaces in a subnet. Broadcast packets are sent from one host to everyone.

Multicast addresses are assigned to a group of devices on various subnets. These are used for one-to-many communications. The multicast address range specified by RFC 1112 is 224.0.0.0 through 239.255.255.255.

VLSM (Variable Length Subnet Mask): VLSM (Variable Length Subnet Masking) allows efficient use of IP addresses. Networks implemented with VLSM can be summarized more efficiently due to manual control. With a distance vector protocol such as RIP , only one subnet mask value can be used on a network, as subnet mask values are not sent in routing updates.

EIGRP supports aggregation and variable length subnet masks (VLSM). Unlike Open Shortest Path First (OSPF), EIGRP allows summarization and aggregation at any point in the network. EIGRP supports aggregation to any bit. This allows properly designed EIGRP networks to scale exceptionally well without the use of areas. EIGRP also supports automatic summarization of network addresses at major network borders.

EIGRP is an advanced routing protocol that combines many of the features of both link-state and distance-vector routing protocols, EIGRP's DUAL algorithm contains many features which make it more of a distance vector routing protocol than a link-state routing protocol.

Given below are some important features of classful and classless routing protocols:

Classfull routing protocols: RIPv1, IGRP are examples of classful routing protocols. It is important to know that classful routing protocols do not exchange subnet information during routing information exchanges. The summarization is always done automatically at major network boundaries.

Classless routing protocols: RIPv2, EIGRP, OSPF, BGPv4, and IS-IS are examples of classless routing protocols. In classless routing protocols, subnet information is exchanged during routing updates. This results in more efficient utilization of IP addresses. The summarization in classless networks is manually controlled.

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 reouter 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.

Cisco® CCNP Route Exam Notes : ARP(address Resolution Protocol)

examguides.com/CCNP-Route/ccnp-routing-9.htm

3. Layer3 Technologies

3.1 Identify IPv4 addressing and subnetting

3.1.b ARP

The ARP stands for the address resolution protocol is the telecommunication protocol. This ARP is mostly used to convert the IP address to the physical address like Ethernet address. When a packet is sent to another device within the same network out an interface, ARP is used if the layer 2 address of the destination is not known. The transmitting device will send an ARP request in order to figure out the address mapping. The ARP request contains the destination IP address and a destination MAC of FF:FF:FF:FF:FF. The destination MAC is flooded out all switchports (if connected to a switch). Normally ARP takes place within the same device when the traffic is within the same subnet. If traffic is destined to a different subnet, the ARP request will be sent by the router instead.

3.1.c DHCP relay and server

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal

forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface.

IOS contains a method for handing out IPv4 addresses while simultaneously maintaining a database which has a record for all the addresses that have been handed out. Automatic DHCP address allocation is typically based on an IP address, whether it be the gateway address or the incoming interface IP address. In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using option 82, the Cisco IOS relay agent has long been able to include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. The Cisco IOS DHCP server can also use option 82 as a means to provide additional information to properly allocate IP addresses to DHCP clients.

DHCP configuration commands

DHCP configuration commands

ip dhcp pool <*poolname*>

Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode

network *192.168.2.0 255.255.255.0*

Provides the IP address range for allocation to the dhcp client computers.

domain-name *xyz.com*

Assigns the domain name for the dhcp client. The domain name is used as a suffix for any domain requests sent out.

Dns-server *192.168.2.2*

Specifies the IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line

Default-router *192.168.2.1*

Specifies the IP address of a router. One IP address is required, although you can specify up to eight addresses in one command line.

Lease *2*

To configure the duration of the lease for an IP address that is assigned from a Cisco IOS DHCP Server to a DHCP client, use the lease DHCP pool configuration command. To restore the default value, use the no form of this command. The default lease period is 1 day.

IP helper addresses forward a client broadcast address (such as a DHCP or DNS request) 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. The command ip helper-address 172.25.9.3, defined on interface e 0 of routerA will route the broadcasts originating at that interface to network resource at 172.25.9.3.

ip helper-address command enable to route broadcasts from client computers. However, you may not want all that broadcast be routed through the network. To prevent certain broadcasts from being carried onto the network, use the command "no ip forward-protocol "

When you enable the IP Helper address, all traffic for the UDP ports are automatically forwarded to the address specified. To restrict the forwarded traffic, you can specify the restrictions by adding any of the no commands to your configuration at the Global Configuration mode.

UDP port 69 is used for TFTP (Trival File Transfer Protocol).

Ex: **no ip forward-protocol udp** *69*

3.1.d DHCP protocol operations

A DHCP device which joins a LAN goes through a couple different steps before it can communicate with other devices on the network:

- The device sends out DHCPDISCOVER frames to broadcast address 255.255.255.255
- The DHCP server responds with a DHCPOFFER. The pool the server chooses depends on the GADDR which is received in original broadcast
- The client then responds with a DHCPREQUEST broadcast letting the broadcast segment know what address it is being assigned
- The DHCP server finally responds with a DHCPACK unicast packet, and the process is completed.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Identify Ipv6 Addressing And Subnetting

examguides.com/CCNP-Route/ccnp-routing-10.htm

3. Layer3 Technologies

3.2 Identify IPv6 addressing and subnetting

IPv6 packet is 128 bits long. It will have basic packet header, and optional extension header.

IPv6 hosts should support the following addresses:

- Assigned global unicast and anycast addresses (2000::/3)
- Loopback address (::1/128)
- Link-local address (FE80::/10), autoconfigured
- All-nodes multicast addresses (FF01::1 and FF02::1)

1. Unicast site-local addresses - IPv6 unicast site-local addresses are similar to IPv4 private addresses. The scope of a site-local address is the internetwork of an organization's site. (You can use both global addresses and site-local addresses in your network.) The prefix for site-local addresses is FEC0::/48.

2. Unicast unspecified address - The IPv6 unicast unspecified address is equivalent to the IPv4 unspecified address of 0.0.0.0. The IPv6 unspecified address is 0:0:0:0:0:0:0:0:, or a double colon (::).

3. Unicast loopback address - The IPv6 unicast loopback address is equivalent to the IPv4 loopback address, 127.0.0.1. The IPv6 loopback address is 0:0:0:0:0:0:0:1, or ::1

In an IPv6 network, a host can autoconfigure its IP address without the help of a DHCP server.

1. Automatic 6to4 is a point-to-multipoint tunneling method, where the tunnel destination is determined from the border router IPv4 address facing the IPv4 network.

2. The border routers that delimit the 6to4 tunnel must support IPv4 and IPv6 and are not configured in pair.

3. Automatic 6to4 can be used to connect two IPv6 networks as well an IPv6 host to an IPv6 network.

4. IPv6 network is treated as NBMA link.

5. The IPv4 embedded in IPv6 is used to find the other end of the tunnel.

6. Border routers create a tunnel on a per packet basis to other IPv6 Border router.

The following are true about IPv6 address format

1. The total length of IPv6 address is 128 bits

2. The first 48 bits of the IPv6 global unicast address are used for global routing at the Internet Service Provider (ISP) level.

3. 16 bits (after the first 48-bit global unicast address) are used for subnetting, allowing organizations to subdivide their network

4. Multicast addresses are in the range FF00::/8.

5. In an IPv6 network, a host can auto configure its IP address without the help of a DHCP server.

Basic rules:

1. ":" in every 2 bytes.

2. heading 0s in each block can be omitted

3. "0: all zeros in between :0" can be written as "::"

How to map IP Multicast address to MAC address:

The high order 9 bits (out of total of 32 bits) of the IP address are not used for mapping into the MAC address. The lower 23 bits are mapped to lower 23 bits of MAC address.

For example, take a Multicast address: 224.252.6.24. Convert to binary equivalent:224.252.6.24 = 1110.0000.1111.1100.0000.0110.0001.1000

Take only the last 23 bits = 111.1100.0000.0110.0001.1000 = 7C-09-24

Append the Ethernet Multicast address: 01-00-5E. Note that 01-00-5E always precedes a Multicast MAC address. The bit following this is always a zero.

Therefore, Multicast MAC address for IP address 224.252.6.24 is:01-00-5E-7C-09-24.

Note that 01-00-5E-FC-09-18 is NOT correct, since 9th bit needs to be replaced by 0, as explained above.

The EUI-64 format interface ID is derived from the 48-bit MAC address by inserting the hex FFFE between the organizationally unique identifier (OUI) field (the upper three bytes) and the vendor code (the lower three bytes) of the MAC address. The seventh bit in the first byte of the resulting interface ID, corresponding to the Universal/Local (U/L) bit, is set to binary 1.

IPv4 and IPv6 networks can exist simultaneously. It is possible to tunnel IPv6 packets through IPv4 networks. IPv6 is downwards compatible with IPv4.

IPv6 hosts should support the following addresses:

- Assigned global unicast and anycast addresses (2000::/3)
- Loopback address (::1/128)
- Link-local address (FE80::/10), autoconfigured
- All-nodes multicast addresses (FF01::1 and FF02::1)
- Solicited-nodes multicast addresses (FF02::1:FF00:/104 and appending the last 24 bits of the corresponding unicast or anycast address of the device)
- Any other assigned multicast addresses (in the range FF00::/8)

Routers should additionally support at least the following:

- Subnet-router anycast address
- All-routers multicast addresses (FF01::2, FF02::2, and FF05::2)
- The minimum MTU supported in IPv6 is 1280 octets. The recommended MTU value for IPv6 links is 1500 octets.

IPv6 Multicast Addresses used by different routing protocols:

RIPv6 : FF02::9
OSPF speaker: FF02::5
OSPF DR and BDR: FF02::6
Multicast Address Node Local::
FF01:0:0:0:0:0:0:1 or FF01::1 All Nodes Address
FF01:0:0:0:0:0:0:2 or FF01::2 All Routers Address
Link Local:
FF02:0:0:0:0:0:0:1 or FF02::1 All Nodes Address
FF02:0:0:0:0:0:0:2 or FF02::2 All Routers Address
FF02:0:0:0:0:0:0:D or FF02::D All PIM Routers

Previous Contents Next

Cisco® CCNP Route Exam Notes : Configure And Verify Static Routing

examguides.com/CCNP-Route/ccnp-routing-11.htm

3. Layer3 Technologies

3.3 Configure and verify static routing

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.

Correct command syntax for creating static route in cisco router is

ip route <*destinaiton_network_address*> <*subnet_mask*> < *default_gateway*>"

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.

3.4. Configure and verify default routing

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

Default routes are used to direct packets addressed to networks not explicitly listed in the routing table. Default routes are widely used where learning specific networks is not feasible or desirable, as in case of stub networks, or limitations due to hardware and software resources.

There are three types of default routes:

1. ip default-gateway - It should only be used when ip routing is disabled on the Cisco router.

2. ip default-network - Unlike the ip default-gateway command, you can use ip default-network when ip routing is enabled on the Cisco router. The device considers the default network as the route to any ip address that is not on any attached/connected interfaces, or in its routing table. Default gateway need to configure on every router to get path for unknown destination packets.By using Default network command you need to configure only on one router in the network, so other routers can learn the exit gate by using routing protocol which distribute this information to others.

3. ip route 0.0.0.0 0.0.0.0 - The ip route command is used with static routing, whereas the ip default-network command is used mostly with routing protocols. Both are achieving the same goals but can be used in different scenarios. If you have a routing protocol for a domain, and you would like to advertise to the rest of the routers that a default route, you would implement the ip default-network command. This would cause the routing protocol to carry the candidate for default network in its routing updates to all routers in the domain.

The ip route 0.0.0.0 0.0.0.0 is a command that is statically assigned. This is called a default network because the all-zeros syntax means to catch all routes. The ip route command is not automatically carried in routing updates like the ip default-network command is in some routing protocols. You must redistribute the static command into a routing protocol for it to be carried.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Evaluate Routing Protocol Types

examguides.com/CCNP-Route/ccnp-routing-12.htm

3. Layer3 Technologies

3.5 Evaluate routing protocol types

The Internet is based on the AS concept, therefore, two types of routing protocols are required:

Interior Gateway Protocol (IGP) : A routing protocol that was designed and intended for use inside a single autonomous system (AS) Known Interior Gateway Protocols (IGP) are Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS)

Exterior Gateway Protocol (EGP): A routing protocol that was designed and intended for use between different autonomous systems Exterior Gateway Protocol (EGP) is commonly used in the Internet to exchange routing table information. There is only one Exterior Gateway Protocol (EGP) exists and it is Border Gateway Protocol (BGP).

3.5.a Distance vector:

In distance vector routing: a router need not know the entire path to every network segment, it only requires to know the direction or vector in which to send the packet. The technique determines the direction (vector) and distance (hop count) to any network in the internetwork. Distance vector routing algorithms periodically send all or parts of their

routing table to their adjacent neighbors. The routers running a distance vector routing protocol will automatically send periodic updates even if there are no changes in the network. It uses Bellman Ford algorithm for calculating the shortest cost path.

RIP and EIGRP is a commonly used distance vector protocol that uses hop counts or its routing metrics.

3.5.b Link state:

In link-state routing: each router attempt to construct its own internal map of the network topology. At the initial stage of start-up, when a router becomes active, it sends the messages into the network and collects the information from the routers to which it is directly connected. It also provides the information about whether the link to reach the router is active or not. This information is used by other routers to build a map of network topology. Then the router uses the map to choose the best path. . It uses dijkstras algorithm for calculating the shortest path.OSPF, BGP and EGP are the examples for link state.

3.5.c Path Vector:

A path vector protocol is a network routing protocol which maintains the path information that gets updated dynamically. Each entry in the routing table contains the destination network, the next router and the path to reach the destination. Border Gateway Protocol (BGP) is an example of a path vector protocol. A path vector protocol does not rely on the cost of reaching a given destination to determine whether each path available is loop free or not. Instead, path vector protocols rely on analysis of the path to reach the destination to learn if it is loop free or not.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Describing Administrative Distance

examguides.com/CCNP-Route/ccnp-routing-13.htm

3. Layer3 Technologies

3.6 Describe administrative distance

Administrative distance is the suitable feature that the routers will use to select the perfect path when there are 2 or more different routes to a same destination from the 2 different routing protocol

An administrative distance of 0 represents highest trustworthiness of the route.

An administrative distance of 255 represents the lowest trustworthiness of the route.

The below table describes default administrative distances.

Route Source	Default Distance values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

Previous Contents Next

Cisco® CCNP Route Exam Notes : Route Maps

examguides.com/CCNP-Route/ccnp-routing-14.htm

3. Layer3 Technologies

3.7 Explain Route Maps

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.

The command mode used to configure filtering of routing update traffic from an interface is

Router(config-router)#

To configure filtering on outgoing update traffic, use the distribute-list command :
distribute-list <*access-list number*> **out** <*interface-name*>

The route map command syntax is:

route-map <*route-map-name*> **[permit/deny] [sequence_number_1-65535]**

Here, the route_map_name is also called as the map tag. It is the text-based route map name. In that the name is logically grouped and unique as well as defined all the route map policies. It is the name which is used to call a route map during the process and redistribution. The deny and permit keywords are always optional and a default keyword is permit.

If a route map is called from the redistribution process, then the keywords are set to permit and a match criteria are met for a route map, a route is redistributed. If a keyword is set to deny, in same criteria, then a route might be denied.

Suppose a route map is called from the policy routing statement, then match criteria is met for route map as well as a keywords are set to permit, then the packets might be policy routed. If a deny keyword is used, hen the packets are forwarded based on the normal route processes.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Route Redistribution

examguides.com/CCNP-Route/ccnp-routing-15.htm

3. Layer3 Technologies

3.8 Explain Route Redistribution

To perform redistribution, one or more routers run both routing protocols, with each routing protocol placing routes into that router's routing table. Then, each routing protocol can take all or some of the other routing protocol's routes from the routing table and advertise those routes

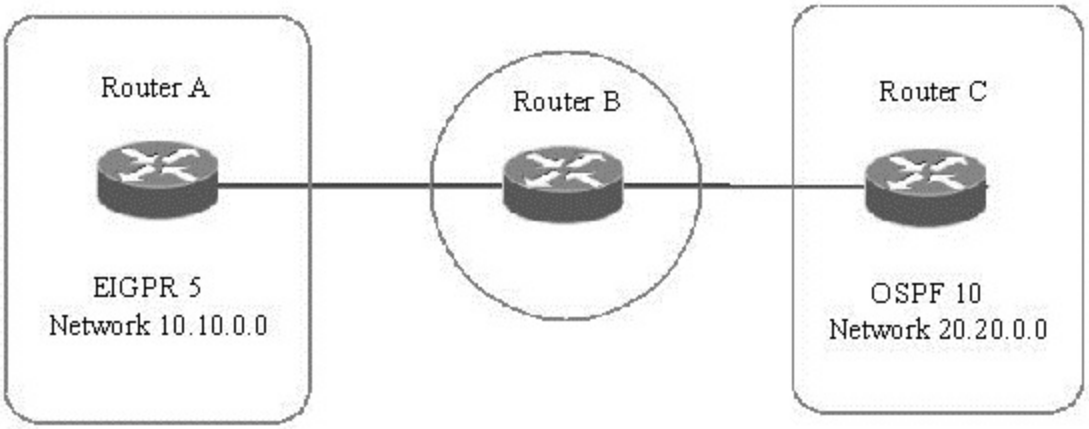
The default metric for a redistributed route should be set to a value larger than the largest metric within the AS.

Redistribution is configured in two steps:

Step 1: In the routing protocol configuration that is to receive the redistributed routes, use the redistribute command to specify the source of the routes.

Step 2: Specify the metric to be assigned to the redistributed routes. The metric should be appropriate for the host protocol, for example, if you are importing routes into RIP, the metric should reflect the hop count. The metric needs to be configured such that it will not lead to routing loops.

Example1: Considere redistribution of two networks, each running EIGRP and OSPF as shown in the figure. The default metric values to be assigned are also given in the figure. What is the basic sequence of commands need to be given for redistribution of EIGRP into OSPF? Assume proper router configuration mode.



EIGRP metrics tobe assigned for redistribution 64,100,255,1,1500
OSPF metric to be assigned for redistribution: 128

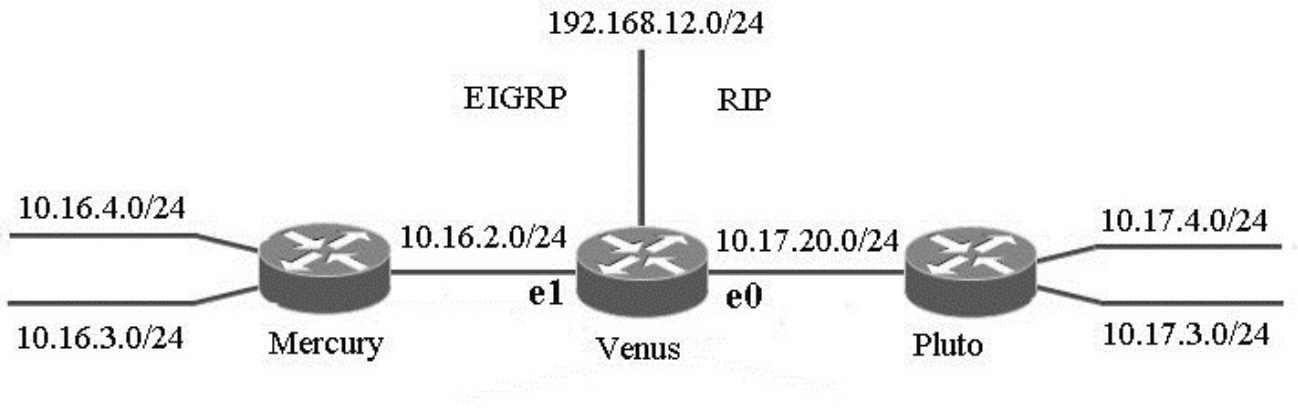
Here, it is required to redistribute EIGRP into OSPF. The command sequence for this is:

!RouterB
router ospf *10*
redistribute eigrp *5*
default-metric *128*

The command "**redistribute eigrp 5**" signifies that OSPF is being redistributed into EIGRP.

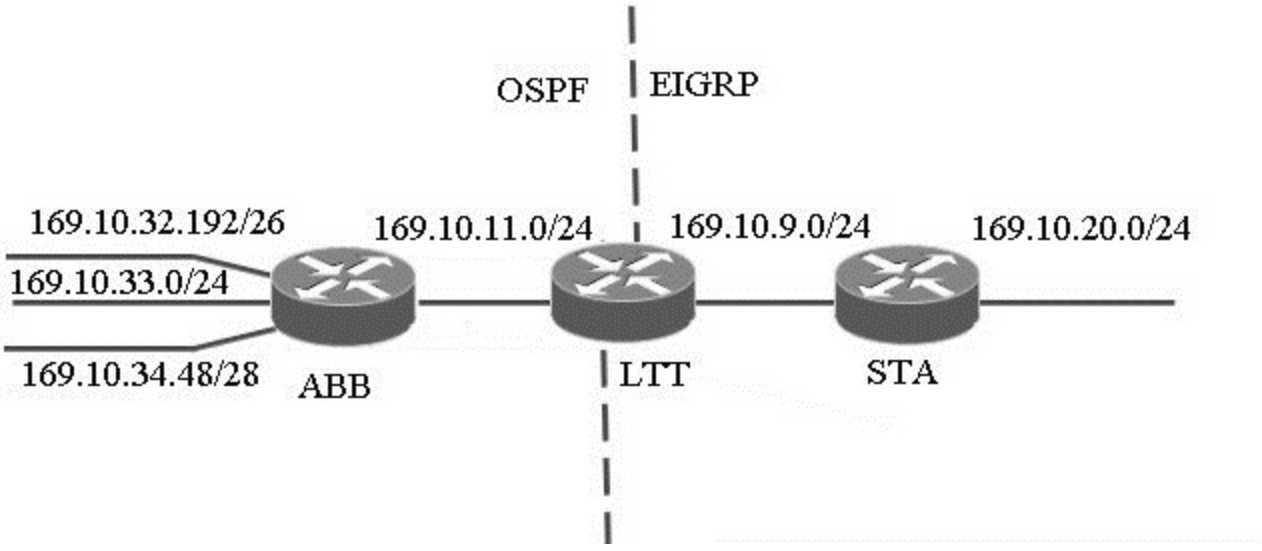
Also, default-metric 128 signifies the default metrics to be assigned to routes being redistributed.

Example2: You want the stub network 192.168.10.0 to be propagated into the EIGRP domain, and at the same time do not want to create unnecessary EIGRP broadcasts. Which command is most appropriate? Please refer the figure below



Notice that Venus is also connected to a stub network (192.168.12.0/24). In this case, the stub network should be advertised into the EIGRP domain, but not into the RIP domain. One way to accomplish this configuration is to simply add the appropriate network statement under EIGRP. However, doing so will create unnecessary EIGRP broadcasts on the stub network. Another way to achieve the desired configuration is to redistribute the stub network into the EIGRP domain.

Example3: See the figure enclosed. You want to redistribute OSPF routes into EIGRP. What command sequence is most appropriate?



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*

Policy-based routing is applied to incoming packets. All packets received on an interface with policy-based routing enabled are considered for policy-based routing. The router passes the packets through enhanced packet filters called route maps. Based on the criteria defined in the route maps, packets are forwarded/routed to the appropriate next hop.

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

Previous Contents Next

Cisco® CCNP Route Exam Notes : RIPv1 And RIIPv2

examguides.com/CCNP-Route/ccnp-routing-16.htm

3. Layer3 Technologies

3.9 RIPv1 and RIPv2

Routing Information Protocol Version 1 (RIPv1): This is a simple distance vector protocol. It has been enhanced with various techniques, including Split Horizon and Poison Reverse in order to enable it to perform better in somewhat complicated networks.

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*>

RIP sends its complete routing table out to all active interfaces at regular intervals (every 30 seconds by default) and when the network topology changes. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform neighbors of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. In RIP, update packets are sent to the immediate neighbors.

"Show IP route" this command will show the routing table and it keeps a list of the best paths to destinations in a routing table. There is a separate routing table for each routed protocol.

- RIPv1 is a Distance-Vector Routing protocol.
- RIPv1 is a Classful routing protocol. Classful routing protocols support only the networks which are not subnetted. Classful routing protocols do not send subnet mask information with their routing updates. In other words, if you have a subnetted network in your RIPv1 routing domain, RIPv1 will announce that network to other as unsubnetted network.
- RIPv1 does not support VLSM (Variable Length Subnet Masking).
- RIPv1 support maximum metric (hop count) value of 15. Any router farther than 15 hops away is considered as unreachable.
- RIPv1 send routing updates periodically every 30 seconds as broadcasts using destination IP address as limited broadcast IP adddress 255.255.255.255. Since the updates are sent using the destination IP address of limited broadcast IP adddress 255.255.255.255, every router need to process the routing update messages (whether they are running RIPv1 or not).
- RIPv1 does not support authentication of update messages (plain-text or MD5).

Routing Information Protocol Version 2 (RIPv2)

RIPv2 is a Hybrid Routing Protocol. A Hybrid Routing Protocol is basically a Distance-Vector protocol which some characteristics of Link State routing protocols.

RIPv2 is classless routing, which allows us to use subnetted networks also. RIPv2 has the option for sending network mask in the update to allow classless routing.

Features of RIPv2 :

- RIPv2 support VLSM (Variable Length Subnet Masking).
- RIPv2 support maximum metric (hop count) value of 15. Any router farther than 15 hops away is considered as unreachable.
- RIPv2 supports triggered updates.
- RIPv2 routing updates are sent as Multicast traffic at destination multicast address of 224.0.0.9. Multicast updates reduce the network traffic. The Multicast routing updates also helps in reducing routing update message processing overhead in routers which are not running RIPv2. Only the routers running RIPv2 join to the multicast group 224.0.0.9. Other routers which are not running RIPv2 can simply filter the routing update packet at Layer 2.
- RIPv2 support authentication of RIPv2 update messages (plain-text or MD5). Authentication helps in confirming that the updates are coming from authorized sources

The router rip command selects RIP as the routing protocol. The network command assigns a major network number that the router is directly connected to. The RIP routing process associates interface addresses with the advertised network number and begins RIP packet processing on the specified interfaces.

Configuration of Routing Information Protocol version 1 (RIPv1)

The necessary configuration steps for doing the same are as given below:

Step1 : Enter into Global Configuration Mode

R1>enable
R1#configure terminal

Step2 : Enable RIP routing on the router

R1(config)#router rip

Step3: Associate network 1.0.0.0 in the RIP routing process

R1(config-router)#network *1.0.0.0*

The command "**no router rip**" is used for removing all rip entries from the router. Once this is cleared, you must reconfigure RIP again using the "**router rip**" command.

Example: **hostname(config)#router rip**

This starts the RIP routing process and places you in router configuration mode

hostname(config)#no router rip

The above command removes the entire RIP configuration you have enabled on the router.

Configuration of Routing Information Protocol version 2 (RIPv2)

The command syntax for configuring RIPv2 on a router is:

router rip
version 2
network <*network number*>

Example:

router rip
version 2

network *156.14.0.0*
network *196.12.12.0*

As soon as RIP is enabled, it will start sending and receiving updates on interfaces. Many situations require you to stop RIP from sending updates out an interface. 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.

Various timers in RIP are given below:

Update-30 sec, Interval between route update advertisements

Hold-Down-90 sec, Period a route is withdrawn from the table to prevent a routing loop.

Timeout-180 sec, Interval a route should stay 'live' in the routing table. This counter is reset every time the router hears an update for this route.

Flush-120 sec, How long to wait to delete a route after it has timed out.

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

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

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.

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.

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

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.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Describing Ripng

examguides.com/CCNP-Route/ccnp-routing-17.htm

3. Layer3 Technologies

3.10 Describe RIPng

RIPng is an extension of RIP for support of IPv6.

The configuration of RIPng is requires at least two steps:

1. Enable RIPng using the global configuration command ipv6 router rip tag. The tag is used to differentiate between multiple RIP processes. It does not have to be the same on all routers.

2. Enable the routing protocol on the interface using the ipv6 rip tag enable. The tag has to match the one used in the ipv6 router rip tag command

The following lists the characteristics of the RIPng protocol:

1. Runs over User Datagram Protocol (UDP).

2. Uses the standard port number 521. Routers that use RIPng listen on the multicast address FF02::9 and send their update messages to this address.

3.11 EIGRP for IPv4

Some of the important terms used in Enhanced IGRP are

1. 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.

2. 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.

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

Please note that EIGRP does not summarize received routes. That is, if a network was not summarized at the major network boundary (this may happen, if you use "no auto-summary" command), then all the subnet routes will be carried into the routing tables of subsequent routers in the rest of the world.

Giving 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.

Feature of EIGRP:

1. EIGRP has certain features that belong to link-state algorithms (like OSPF) than distance-vector algorithms.

2. 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.

3. 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.

4. Support VLSM, route summarization, and routing update authentication". Therefore B is correct.

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

6. 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.

7. 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.

8. You can summarize routes in EIGRP at any arbitrary bit boundary.

9. 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.

IGRP (as well as EIGRP) uses the following routing 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. This is represents the maximum throughput of a link.

6. MTU (Maximum Transmission Unit): This is the maximum message length that is acceptable to all links on the path. The larger MTU means faster transmission of packets.

7. Reliability: This is a measurement of reliability of a network link. It is assigned by the administrator or can be calculated by using protocol statistics.

8. Delay: This is affected by the band width and queuing delay.

9. Load: Load is based among many things, CPU usage, packets processed per sec.

The following are some of the important characteristics of an autonomous system:

1. An autonomous system consist of routers, that present a consistent view of the routing to the external world.

2. Exterior routing protocols are used for communication between autonomous systems

3. Interior routing protocols are used within a single autonomous system

4. An autonomous system can run both interior and exterior protocol simultaneously. However, Interior protocols such as RIP, IGRP are used for communication within the autonomous system, and exterior routing protocols such as BGP are used for communication between autonomous systems.

EIGRP uses multicasts to send queries to neighbor routers.

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*>

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

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.

The command : "**ipx router eigrp** *10*" specifies that eigrp is used for routing protocol, and 10 is the autonomous system number.

The command : "**network** *20*" assigns EIGRP for IPX updates to network 20.

EIGRP maintains a number of timers and variables containing time intervals. These include an update timer, an invalid timer, a hold-time period, and a flush timer. The update timer specifies how frequently routing update messages should be sent. The EIGRP default for this variable is 90 seconds. The invalid timer specifies how long a router should wait in the absence of routing-update messages about a specific route before declaring that route invalid. The EIGRP default for this variable is three times the update period. The hold-time variable specifies the holddown period. The EIGRP default for this variable is three times the update timer period plus 10 seconds. Finally, the flush timer indicates how much time should pass before a route should be flushed from the routing table. The EIGRP default is seven times the routing update period.

The correct command to disable auto-summary in EIGRP environment Is : **no auto-summary**

The above command will turn off route summarization in EIGRP network.

show ip eigrp topology: To display entries in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the show ip eigrp topology command in EXEC mode.

The following is the sample output of "**show ip eigrp topology**" command

```
Router_B#show ip eigrp topology
IP-EIGRP Topology Table for AS 10

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

P 20.0.0.0/8, 1 successors, FD is 2169856
        via Connected, Serial0/0
P 10.0.0.0/8, 1 successors, FD is 2172416
        via 20.0.0.1 (2172416/28160), Serial0/0
Router_B#
```

P: Passive: means the router is not looking for the route actively, thus it means it is in good situation. The status of "Active" means some instability in network.

FD: Feasible Distance: metric to a destination

2172416 / 28160: In the output 2172416 is the feasible distance and 28160 is the advertised distance.

Advertised distance is the distance from your neighbor to destination.

show ip eigrp neighbors: To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP), use the show ip eigrp neighbors command in EXEC mode. It shows when neighbors become active and inactive. The neighbor parameters displayed include Address, Interface, Holdtime, Uptime, Q, Seq Num, SRTT, and RTO.

The following is sample output of the "show ip eigrp neighbors" command

```
R1#show ip eigrp neighbors

Address            Interface   Holdtime  Uptime     Q      Seq   SRTT   RTO
                               (secs)    (h:m:s)    count  Num   (ms)   (ms)
192.168.1.2        Ethernet0   12        01:58:22   0      1     40     1000
192.168.100.2      Serial0     12        01:58:22   0      1     40     1000
```

The fields in the neighbor table are as under

- H: Handle: Order in which neighbor adjacency is formed. The first router will have '0' the following one will have '1' and so on.
- Address: IP address of the neighbor
- Interface: Interface of the neighbor connected
- Hold Time: Timer how long to hold a neighbor if a hello is not received. By default it is 15 seconds.
- Uptime: Since when the neighbor is up

- SRTT: Smooth Round Trip Time: Time taken for a packet to reach the neighbor and get an acknowledgment back. This time is in milliseconds.
- RTO(Retransmission Timeout): Time taken to wait before router retransmits a packet to the neighbor
- Q Cnt: Queue Count: Number of packets that are waiting to be transmitted (Update, Reply, Query). Any number greater than 0, signifies some congestion in the network.
- Seq Number: Sequence Number: It is the sequence number of the last packet received from neighbor.

show ip route eigrp: Displays the EIGRP routes installed in the route table. Displays the current EIGRP entries in the routing table.

By giving the command "show ip route eigrp", we can see the routes found by eigrp. A route discovered by EIGRP is denoted by letter "D" before start of the entry. Cisco chose letter D for EIGRP, because letter E was already taken by Exterior Gateway Protocol (EGP)

A typical output from a show ip route command is as shown below:

R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 5 subnets
C 10.1.3.0 is directly connected, Loopback3
D 10.1.2.0 [90/156160] via 10.1.100.2, 00:14:46, FastEthernet0/0
D 10.1.1.0 [90/156160] via 10.1.100.1, 00:14:55, FastEthernet0/0
C 10.1.100.0 is directly connected, FastEthernet0/0
D 10.1.200.0 [90/2172416] via 10.1.100.2, 00:14:46, FastEthernet0/0
[90/2172416] via 10.1.100.1, 00:14:46, FastEthernet0/0
192.168.100.0/30 is subnetted, 2 subnets
C 192.168.100.4 is directly connected, Loopback15
C 192.168.100.0 is directly connected, Loopback11

Show ip eigrp interface: Use the "show ip eigrp interfaces" command to determine on which interfaces EIGRP is active, and to find out information about EIGRP relating to those interfaces. The details shown include interfaces on which EIGRP is configured, number of directly connected EIGRP neighbors on each interface, Mean SRTT, etc.

The following is sample output of the "show ip eigrp interfaces" command

```
R1#show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(100)
                        Xmit Queue   PeerQ        Mean   Pacing Time   Multicast    Pending
Interface         Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se3/0               1        0/0        0/0          20       10/390        458          0
Se3/1               1        0/0        0/0          24         0/0         104          0
Lo11                0        0/0        0/0           0         0/0           0          0
R1#
```

The significant field are described below

- Peers : Number of EIGRP neighbors connected on this interface.
- Xmit Queue Un/Reliable : Number of packets remaining in the Unreliable and Reliable transmit queues.
- Mean SRTT : Mean smooth round-trip time interval, in milliseconds.
- Pacing Time Un/Reliable : Pacing time used to determine when reliable and unreliable EIGRP packets should be sent out of the interface.
- Multicast Flow Timer : Maximum number of seconds the router sends multicast EIGRP packets.
- Pending Routes : Number of routes in the packets in the transmit queue waiting to be sent.

show ip eigrp traffic: This command can be used to learn the number of EIGRP packets sent and received.

The following is sample output of the "show ip eigrp traffic" command

```
Router# show ip eigrp traffic
EIGRP-IPv4 Traffic Statistics for AS(60)
Hellos sent/received: 21429/2809
Updates sent/received: 22/17
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 16/13
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
Hello Process ID: 204
PDM Process ID: 203
Socket Queue: 0/2000/2/0 (current/max/highest/drops)
Input Queue: 0/2000/2/0 (current/max/highest/drops)
```

The significant fields in the above display are described as below

- Hellos sent/received : Number of hello packets sent and received.

- Updates sent/received : Number of update packets sent and received.
- Queries sent/received : Number of query packets sent and received.
- Replies sent/received : Number of reply packets sent and received.
- Acks sent/received : Number of acknowledgement packets sent and received.
- SIA-Queries sent/received : Number of stuck in active query packets sent and received.
- SIA-Replies sent/received : Number of stuck in active reply packets sent and received.
- Hello Process ID : Hello process identifier.
- PDM Process ID : Protocol-dependent module IOS process identifier.
- Socket Queue : The IP to EIGRP Hello Process socket queue counters.
- Input queue : The EIGRP Hello Process to EIGRP PDM socket queue counters.

The neighbor table in EIGRP include the following key elements:

1. Neighbor address: This is the network layer address of the neighbor router.

2. Queue: This represents the number of packets waiting in queue to be sent.

3. Smooth Round Trip Time (SRTT): This represents the average time it takes to send and receive packets from a neighbor. This timer is used to determine the retransmit interval (RTO).

4. Hold Time: This is the period of time that a router will wait for a response from a neighbor before considering the link unavailable.

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

- Network address (IP)
- Connected interface
- Holdtime - how long the router will wait to receive another HELLO before dropping the neighbor; default = 3 * hello timer
- Uptime - how long the neighborship has been established
- Sequence numbers
- Retransmission Timeout (RTO) - how long the router will wait for an ack before retransmitting the packet; calculated by SRTT
- Smooth Round Trip Time (SRTT) - time it takes for an ack to be received once a packet has been transmitted
- Queue count - number of packets waiting in queue; a high count indicates line congestion

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

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.

Acknowledgement Packets - An EIGRP Acknowledgment (ACK) packet is simply an EIGRP Hello packet that contains no data. Acknowledgement 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, Acknowledgement 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 acknowledgement. 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

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.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Configure And Verify Eigrp For Ipv6

examguides.com/CCNP-Route/ccnp-routing-18.htm

3. Layer3 Technologies

3.12 Configure and Verify EIGRP for IPv6

EIGRPv6 involves the following configuration steps

1. To enable EIGRPv6 on a router interface, use the command **"ipv6 eigrp"** as on individual interfaces that will be part of the EIGRPv6 process.

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

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

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

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

6. 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.

7. The command **eigrp router-id** <*ip-addressv* 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. The "AS" stands for Autonomous System number. This number should be the same on all routers.

Example:

1. **Router>enable**

2. **Router#configure terminal**

3. **Router(config)#ipv6 unicast-routing configures the router to route IPv6 packets**

4. **Router(config)#interface type** <*number*>

Specifies the interface on which EIGRPv6 is to be configured.

Router(config-if)#ipv6 enable

Enables IPv6 processing on the specified interface.

6. **Router(config-if)#ipv6 eigrp** *as-number* - Enables the EIGRP for IPv6 process on the specified interface.

7. **Router(config-if)#no shutdown** - Starts the EIGRP for IPv6 protocol (process) without changing any per-interface configuration.

8. **Router(config-if)#ipv6 router eigrp** <*as-number*> - Puts the router into router configuration mode and creates an EIGRP for IPv6 routing process.

9. **Router(config-router)#router-id** *{ip-address | ipv6-address}* - Enables the router to use a fixed router ID. (Remember each router Id must be unique)

10. **Router(config-router)#no shutdown** - Put the EIGRPv6 routing process in "no shutdown" mode in order to start the EIGRPv6 process.

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

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

2. 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.

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

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

5. Must be able to pass routing protocol authentication, if configured. This is true for Ipv4 also.

6. K values must match (true for ipv4 also)

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

8. EIGRP-IPV6 denotes EIGRP route with the letter "D", and not "E" as in the case of EIGRP ipv4.

EIGRPv6 show commands:

show ipv6 eigrp traffic: Displays the number of EIGRP IPv6 packets sent and received, to used in user EXEC or privileged EXEC mode.

show ipv6 eigrp neighbors: The show ipv6 eigrp neighbors command lists each neighbor using link-local IPv6 address along with local interface.

show ipv6 eigrp interfaces command shows three interfaces that have EIGRPv6 enabled Note that the command does not show eigrp interfaces that had been configured as passive interface.

show ipv6 eigrp topology: This command displays entries in the EIGRP IPv6 topology table The "show ipv6 eigrp topology" command can be used without any keywords or arguments. If this command is used without any keywords or arguments, then only routes that are feasible successors are displayed.

Previous Contents Next

Cisco® CCNP Route Exam Notes : OSPF For Ipv4

examguides.com/CCNP-Route/ccnp-routing-19.htm

3. Layer3 Technologies

3.13 OSPF for IPv4

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.

Note: By default, OSPF keeps 4 routes in routing table if there are 4 or more equal cost routes exist for the same subnet. However, OSPF can include up to 16 equal cost routes in the routing table and perform load balancing amongst them. In order to configure this feature, you need to use the OSPF sub command **maximum-paths**, i.e. maximum-paths 16.

To configure an area as totally stubby, use the command "**area** <*area-id*> **no-summary**"

The cost of the default route that is injected into the stub area is equal to 1 by default. To change this value, use the command "**area** <*area-id*> **default-cost** <*cost*>" command. For example, if you want to set a value of 5 for the default route, use the command "**area** *2* **default-cost** *5*".

A default route can be advertised into OSPF domain by an ASBR router in one of two ways: By using "**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.

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

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 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.

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.

- 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 hellos. This is 10 seconds on multi access networks.
- Open Shortest Path First (OSPF) uses "Cost" as the value of metric and 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 10 Mbps Ethernet , OSPF Metric Cost value is 100 Mbps / 10 Mbps = 10.
- The default Reference Bandwidth of OSPF is 100 Mbps and the default OSPF cost formula doesn't differentiate between interfaces with bandwidth faster than 100 Mbps. These days, 1 Gbps and 10 Gbps links are also common.
- According to the default OSPF metric Cost value calculation, the default OSPF Cost for Fast Ethernet interface (100 Mbps) and a Gigabit Ethernet interface (1 Gbps) are same.
- If you want to change the default behavior, the cost formula can be adjusted using the "auto-cost" command under the OSPF routing process. If you are changing the default OSPF Reference Bandwidth, make sure that you have changed the OSPF Reference Bandwidth in all your OSPF Routers.

Default cost of essential interfaces.

Interface Type bandwidth Metric Calculation Cost

Ethernet Link 10Mbps 100Mbps/10Mbps 10

FastEthernet Link 100Mbps 100Mbps/100Mbps 1

Serial Link 1544Kbps(default) 100Mbps/1.544Mbps= 64.76 64

OSPF uses SPT tree to calculate the best route for routing table. A SPT tree cannot grow beyond the area. So if a router has interfaces in multiple areas, it needs to build separate tree for each area. SPF algorithm calculates all possible routes from source router to destination network.

- Cumulative cost is the sum of the all costs of the outgoing OSPF interfaces in the path.
- While calculating cumulative cost, OSPF consider only outgoing interfaces in path. It does not add the cost of incoming interfaces in cumulative cost.
- If multiple routes exist, SPF compares the cumulative costs. Route which has the lowest cumulative cost will be chosen for routing table.
- When a serial line is configured on a Cisco router, the default bandwidth is 1.544Mbps. If the line is slower speed, "bandwidth" command can be used to specify the real link speed. The cost of the link will then automatically correspond to the changed value.

In short:**Cumulative cost = *Sum of all outgoing interfaces cost in route***

Best route for routing table = *Route which has the lowest cumulative cost*

1. LSA (Link State Advertisement): LSAs are included in the database description packets (DDPs or DBDs). LSA entries include link-state type, the address of the advertising router, the cost of the link, and the sequence number.

2. LSR (Link State Request): When a slave router receives an DDP (Database Description Packet), it sends and LSAck packet. Then it compares the received information with the information it has. If the DDP has more recent information, the slave router sends a link-state request (LSR) to the master router.

3. LSU (Link State Update): LSU packet is sent in response to LSR (Link-State Request) packet sent from a slave router to a master router. LSU contains complete information about the requested entry.

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: Routes can be summarized when being advertised out side an area, thus reducing the routing table entries.

3. Reduced LSU overhead: Fewer number of LSUs can be sent with a single or fewer summarized routes between areas to reduce the overhead associated with link-state updates when they are crossing areas.

Important features of stub area are:

- 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.
- 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.
- The stub areas suited for Hub-Spoke topology.
- 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.
- When an area is configured as stub or totally stubby, a default route (0.0.0.0) is injected into the area

Virtual-link in OSPF: Theoretically, all areas in an OSPF autonomous system must be physically connected to the backbone area (area 0). In some cases where this physical connection is not possible, you can use a virtual link to connect to the backbone through a

non-backbone area. You can also use virtual links to connect two parts of a partitioned backbone through a non-backbone area. The area through which you configure the virtual link is known as a transit area.

Use the "area area-id virtual-link router-id" command in order to configure a virtual link, where the area-id is the area ID assigned to the transit area (this can be either a valid IP address or a decimal value), and where router-id is the router ID associated with the virtual link neighbor.

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

Sometimes when you issue a "show ip ospf virtual-link" the output shows that the Virtual-Link is UP, but you see no communication going on, neither a OSPF Relationship established. To make sure that the Virtual-Link is "really" working, issue a show ip ospf virtual-link command and see if the adcency state id FULL, and communication is there as given in the example below (typical output):

R(config-router)#do sh ip ospf virtual-link

Virtual Link OSPF_VL0 to router 3.3.3.3 is up
Run as demand circuit
DoNotAge LSA allowed.
Transit area 1, via interface Serial1/0, Cost of using 64
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Adjacency State FULL (Hello suppressed)
Index 2/3, retransmission queue length 1, number of retransmission 1
First 0x65593B80(11)/0x0(0) Next 0x65593B80(11)/0x0(0)
Last retransmission scan length is 1, maximum is 1
Last retransmission scan time is 0 msec, maximum is 0 msec
Link State retransmission due in 2986 msec

Yes, 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.

224.0.0.5 and 224.0.0.6 are the multicast addresses used by OSPFv2.

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.

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 following is true about OSPF area

- An OSPF area is a collection of networks and routers that has the same area identification.
- The command "show ip ospf database" displays the contents of the topological database maintained by the router. This command also displays router id and the ospf process id.
- "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.
- 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 the each destination network. The lowest cost route is always preferred when there are multiple paths to a given destination.

The following are the types of OSPF routers:

1. Internal router: An internal router has all the interfaces in the same area. All internal routers have same link state databases.

2. Backbone router: Backbone routers sit on the perimeter of Area 0, with at least one interface connected to backbone (Area 0).

3. Area Border Router (ABR): ABRs are routers that have interfaces attached to multiple areas. It may be noted that these routers maintain separate link-state databases for each area that they are connected. They are capable of routing traffic destined for or arriving from other areas.

4. Autonomous System Boundary Router (ASBR): These are the routers that have at least one interface to the external network (another autonomous system). This autonomous network can be non-OSPF. ASBRs are capable of route redistribution, a term used to imply that the concerned router can import routing information from non-OSPF networks and distribute the same in OSPF network for which it is responsible and visa versa.

OSPF LSA Types

- 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. Type 2 LSAs describe the set of routers attached to a particular network and are flooded within the area that contain the network only.
- 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.

Note: In OSPF, lower the metric value higher the priority

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.

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) - 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.

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

By using **"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.

By using **"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.

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.

In an OSPF environment

1. A DDP (Data Description Packet) is used during the exchange protocol and includes summary information about link-state entries.

2. A hello packet is used during the hello process and includes information that enables routers to establish neighbor relationship.

3. An internal router is a router that resides within an area.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Configure And Verify Ospf For Ipv6

examguides.com/CCNP-Route/ccnp-routing-20.htm

3. Layer3 Technologies

3.14 Configure and verify OSPF for IPv6

1. Multiple OSPF processes are supported as in OSPFv2

2. OSPFv3 supports IPv6 whereas OSPFv2 doesn't.

3. Uses multicast addresses FF02::5 and FF02::6

4. Type 3 and type 9 LSAs carry IPv6 prefix information, whereas IPv4 prefix information is carried in type 1 and type 2 LSAs

OSPF for IPv6 requires the use of IPsec to enable authentication. The IPv6 AH (Authentication Hearder) and ESP extension headers are used to provide authentication and confidentiality to OSPF for IPv6.

1. ipv6 ospf authentication - This command enables the IPsec AH

2. The ipv6 ospf encryption - This command initiates the IPsec ES

3. The ESP header may be applied alone or in combination with the AH, and when ESP is used, both encryption and authentication are provided.

4. OSPFv3 uses the IPv6 multicast addresses FF02::5 (for all OSPF routers) and FF02::6.

5. OSPFv3 IPv6 routers can support many addresses per interface, including the linklocal address, global unicast addresses, and multicast addresses.

Typical steps involved to enable OSPFv3 are

Router>enable
Router#configure terminal
Router(config)#ipv6 router ospf 1

Note that you need to enable ipv6 routing on the interface prior to configuring OSPFv3.

Steps required for enabling ospf in area 0 are (assuming that the interface Ethernet 0/0 is being configured):

Router>enable
Router#configure terminal
Router(config)#interface ethernet 0/0
Router(config-if)#ipv6 ospf 1 area 0

OSPFv3 uses the IPv6 multicast addresses FF02::5 (for all OSPF routers) and FF02::6

Internet's Multicast backbone (known as MBONE) uses DVMRP (Distance Vector Multicast Routing protocol) for Multicasting.

PIM is a Multicast routing protocol (just as DVMRP and MOSPF) supported by Cisco routers, and used between routers. Cisco routers does not support DVMRP and MOSPF. However, Cisco routers support PIM to DVMRP interaction, so that DVMRP packets are read, and necessary action is taken.

CGMP is a protocol used between Cisco routers and Cisco Catalyst switches.

Cisco routers do not support MOSPF.

Previous Contents Next

Cisco® CCNP Route Exam Notes : BGP (border Gateway Protocol)

examguides.com/CCNP-Route/ccnp-routing-21.htm

3. Layer3 Technologies

3.15 BGP

The border gateway protocol is the standardized exterior gateway protocol proposed to exchange routing and the reachability information between the autonomous systems on the internet. The BGP neighbors are called as peers. This peer is established by the manual configuration between the routers to create the TCP session on the port.

There are three ways to advertise networks into BGP:

1.Using network command

2.Redistributing static routes to null 0 into BGP

3.Redistributing dynamic IGP routes into BGP

However, redistributing dynamic IGP routes into BGP may result in instability, and therefore not recommended.

BGP version 4 supports CIDR (Classless InterDomain Routing). Important features are:

1. BGP update messages include both the prefix and prefix length.

2. Addresses can be aggregated when advertised by a BGP Router.

3. The AS path attributes can include a combined list of all AS numbers that all of the aggregated routes have passed through and should be considered to ensure that the route is loop free.

To distribute Border Gateway Protocol (BGP) neighbor information use the neighbor distribute-list command in address family or router configuration mode

When the aggregate-address command is used within BGP routing, the aggregated address is advertised, along with the more specific routes. The "summary-only" keyword suppresses the more specific routes and announces only the summarized route.

External BGP (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).

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.

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.

The following are the four possible message types in a BGP header:

- Type 1: OPEN message - This is the first message sent after TCP session is established.
- Type 2: UPDATE message - An UPDATE message contains a new route or a route to be withdrawn or both. Note that only one new route can be advertised with one UPDATE message.
- Type 3: NOTIFICATION message - this message is sent if an error occurs during a BGP session. This message can be used to troubleshoot the problem.
- Type 4: KEEPALIVE message - KEEPALIVE message is used to confirm that the connection between the neighboring routers is still active.

BGP Configuration command Example:

RouterA(config)#router bgp *1340*

The above command sets the RouterA to autonomous system number 1340. where 1340 is the AS number which can have a value between 1 and 65535 in an internetwork.

The command: **clear ip bgp** *

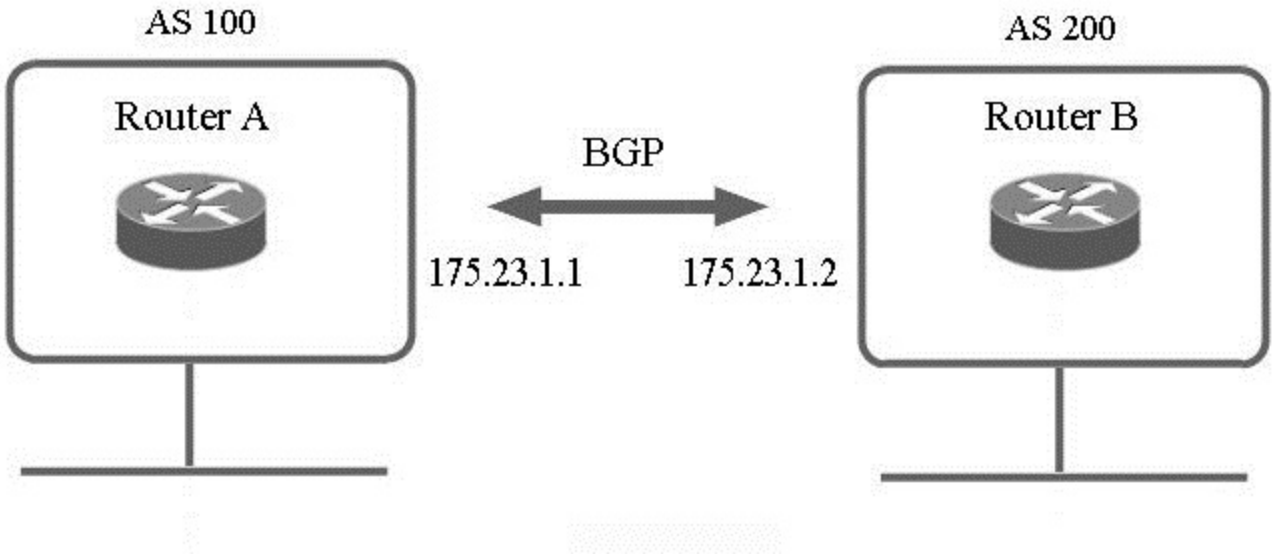
clears all the entries from the BGP routing table and reset BGP sessions. This command is used after every configuration change to ensure that the change is activated and that peer routers are informed.

Another command,

clear ip bgp <*address*>

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

Example: Consider the example, RouterA and RouterB are running eBGP as shown in the fig.



RouterA to establish neighbor relationship with RouterB command syntax 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.

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

The following router configuration mode example sets the weight of all routes learned via 165.22.10.1 to 50:

router bgp *110*
neighbor *165.22.10.1* **weight** *50*

To assign a weight to a neighbor connection, use the neighbor weight command.

neighbor *{ip-address | peer-group-name}* **weight** <*weight*>

To remove a weight assignment, use the no form of this command:

no neighbor *{ip-address | peer-group-name}* **weight** <*weight*>

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]**

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

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

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*

Do not apply both a neighbor distribute-list and a neighbor prefix-list command to a neighbor in any given direction (inbound or outbound) on a BGP router. Please note that these two commands are mutually exclusive, and only one command (neighbor prefix-list or neighbor distribute-list) can be applied to each inbound or outbound direction.

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.

- 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.
- Update policies are normally set by route maps, distribution lists, and filter lists.
- Members of the peer group can be configured to override the configuration options for incoming updates, but not to the outgoing updates.

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:

- If the update is from a non-client peer : It sends the update to all clients in the cluster.
- If the update is from a client peer: It sends the update to all nonclient peers and to all client peers.
- If the update is from eBGP peer: It sends the update to all nonclient peers and to all client peers.

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:

The following are well known communities in BGP:

- Internet: All routers belong to this community by default. Advertises the route to internet community.
- No-export: This indicates not to advertise a route to eBGP
- No-advertise: This indicates not to advertise a router to peers.

The community attribute in BGP can contain a value in the range 0 to 4294967200.

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).

8. Prefer eBGP over iBGP paths.

The correct syntax to configure a router as a BGP route reflector is:

RouterA(config-router)#neighbor <*ip-address*> **route-reflector-client**

Here, it is:

RouterA(config-router)#neighbor *144.44.44.1* **route-reflector-client**

The above command will configure RouterA as a route reflector with the specified neighbor 144.44.44.1 as the route reflector's client.

Router(config-router)#neighbor *10.10.10.1* **weight** *55*

The above command assigns a weight of 55 to a BGP neighbor connection at 10.10.10.1,that is routes received from neighbor router with ip address 10.10.10.1 will be assigned a weight of 55.

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

- Routes learnt from One IBGP Peer cannot be advertised to another IBGP Peer.
- 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 and Confiderations are used as alternative mechanisms to address this problem: Route Reflectors and Confederations

The assignable BGP autonomous system numbers are from 1 to 65,535 (I.e. 65,535 in total). Autonomous system numbers are of 16 bit length. This 2 ^ 16 = 65536 -1 possible ASNs, since ASN of all 0s is not assigned. Out of this,

The Internet Assigned Numbers Authority (IANA) has reserved the following block of AS numbers for private use (not to be advertised on the global Internet) :

64512 through 65535

Before any route information is exchanged between any two routers running BGP, a TCP connection need to be established. Route information is exchanged between the BGP routers only after the TCP connection is established.

Port number 179 is used to establish a session between two routers running BGP.

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

- AS_PATH : BGP messages carry the sequence of AS numbers indicating the complete path a message has traversed.
- NEXT_HOP : This attribute indicates the IP address of the next-hop destination router.
- ORIGIN : This attribute tells the receiving BGP router, the BGP type of the original source of the NLRI information.

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. Keep alive 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.

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.

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) - 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. 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.

Various debug commands useful in troubleshooting bgp are:

- Debug ip bgp events: Displays all bgp events as they occur.
- Debug ip bgp dampening: Displays bgp dampening events as they occur.
- Debug ip bgp keepalives: Displays all events related to bgp keepalive packets.
- Debug ip bgp updates: Displays information on all bgp update packets.

Methods available for filtering BGP updates

- 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.
- AS_Path filtering: Here, you specify an access list on both incoming and outgoing updates based on the value of the AS_path attribute.
- Route Map Filtering: Here, the "neighbor route-map" router configuration command is used to apply a route map to incoming and outgoing routes.
- Community Filtering: You can filter by setting the community attribute on router updates.
- Distribute lists: are standard or extended access lists applied to a BGP router's session that permit or deny advertised routes on the network based on the applicable criteria.

In a router running BGP, when you are configuring prefix lists, the sequence numbers automatically assigned are :5, 10,15,20 etc.

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.

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

- These are used for filtering BGP routing updates, so that certain path policy is applied.
- Prefix lists doesn't put as much load on the processor as that of Access lists.
- Prefix lists are easier to configure and implement.
- 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.

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*

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 incoming advertisements to neighbor 192.10.0.0:

router bgp *100*
network *120.101.0.0*
neighbor *192.10.0.0* **prefix-list** *mylist1* **in**

To enable the synchronization between Border Gateway Protocol(BGP) and Interior Gateway Protocol (IGP) system, we use the synchronization command. To enable the Cisco IOS software to advertise a network route without waiting for the IGP, use the no synchronization command. By default, synchronization is enabled.

The following router configuration mode is an example that enables a router to advertise a network route without waiting for the IGP:

router bgp *160*
no synchronization

Given are :

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

In BGP, when a route reflector is configured in a cluster, clients belonging to that cluster should not establish peer relationship with iBGP speakers outside of their cluster.

Below is a review of various terms associated with route reflectors:

Some of the terms used commonly with route reflectors are:

- Route reflector: It is a router that is configured to advertise the routes learned from iBGP neighbors.
- Client: A router that will share information with the router configured as route reflector.
- Cluster: The set of all routers configured as route reflectors and clients.
- Cluster ID: There can be more than one route reflector in a cluster. Then, cluster ID is used to identify the route reflectors uniquely in the specified cluster.

Range of numbers that can be assigned to BGP distribution list:

Note that distribute lists are created using IP standard access lists and IP extended access lists. The range of numbers for standard access list is 1 to 99 and extended access list is 100 to 199. Therefore, the allowed range of numbers is 1 to 199.

The BGP split horizon rule says that routes learned via an IBGP are never propagated to other IBGP peers. However, in the case of BGP route reflectors, there is an exception. A route reflector propagates the routes learned by IBGP to other IBGP peers.

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.

Few recommended scenarios, where you use BGP are:

- Connect two or more ISPs
- The traffic flow out of your network need to be managed to suit the requirements of your organization.
- The traffic need to be sent through one AS to get to another AS.

TCP is the protocol used to establish session, when two BGP routers are exchanging route information.

BGP Show commmands:

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.

The following is the sample output of "**show ip BGP**" command-line

```
R1#show ip bgp

BGP table version is 5, local router ID is 20.20.20.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric  LocPrf      Weight  Path
10.10.10.0       10.10.10.2        0       100         0       100
10.10.10.0       10.10.10.2        0       100         0       100
20.20.20.0       20.20.20.2        0       100         0       200
20.20.20.0       20.20.20.2        0       100         0       200
R1#
```

Show ip bgp summary: To display the status of all Border Gateway Protocol (BGP) connections use the command show ip bgp summary. It displays 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.

```
R1#show ip bgp summary

Neighbor          V  AS      MsgRcvd  MsgSent  Up/Down  State/PfxRcd
10.10.10.2        4  100     -        -        never    estab
10.10.10.2        4  100     -        -        never    estab
20.20.20.2        4  200     -        -        never    estab
20.20.20.2        4  200     -        -        never    estab
R1#
```

"State/PfxRcd" column, which shows the BGP states. Below is the list of BGP states in order, from startup to peering:

- 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.

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

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

The command "show ip bgp routes" shows the BGP routes.

Your enterprise need to use BGP to connect to an ISP if it has different policy requirements than the ISP.

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.

```
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

Cisco® CCNP Route Exam Notes : Configure And Verifying GRE

examguides.com/CCNP-Route/ccnp-routing-22.htm

4. VPN Technologies

4.1 Configure and verify GRE

Tunneling provides a mechanism to transport packets of one protocol within another protocol. The protocol that is carried is called as the passenger protocol, and the protocol that is used for carrying the passenger protocol is called as the transport protocol. Generic Routing Encapsulation (GRE) is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint. IPv6 traffic can be carried over IPv4 GRE tunnels using the standard GRE tunneling technique. The tunnels are not tied to a specific passenger or transport protocol, but in this case, carry IPv6 as the passenger protocol with the GRE as the carrier protocol and IPv4 or IPv6 as the transport protocol. The primary use of GRE tunnels is for stable connections that require regular secure communication between two edge routers or between an edge router and an end system. The edge routers and the end systems must be dual-stack implementations.

When running GRE tunnel over IPSec, a packet is first encapsulated in a GRE packet and then GRE is encrypted by IPSec

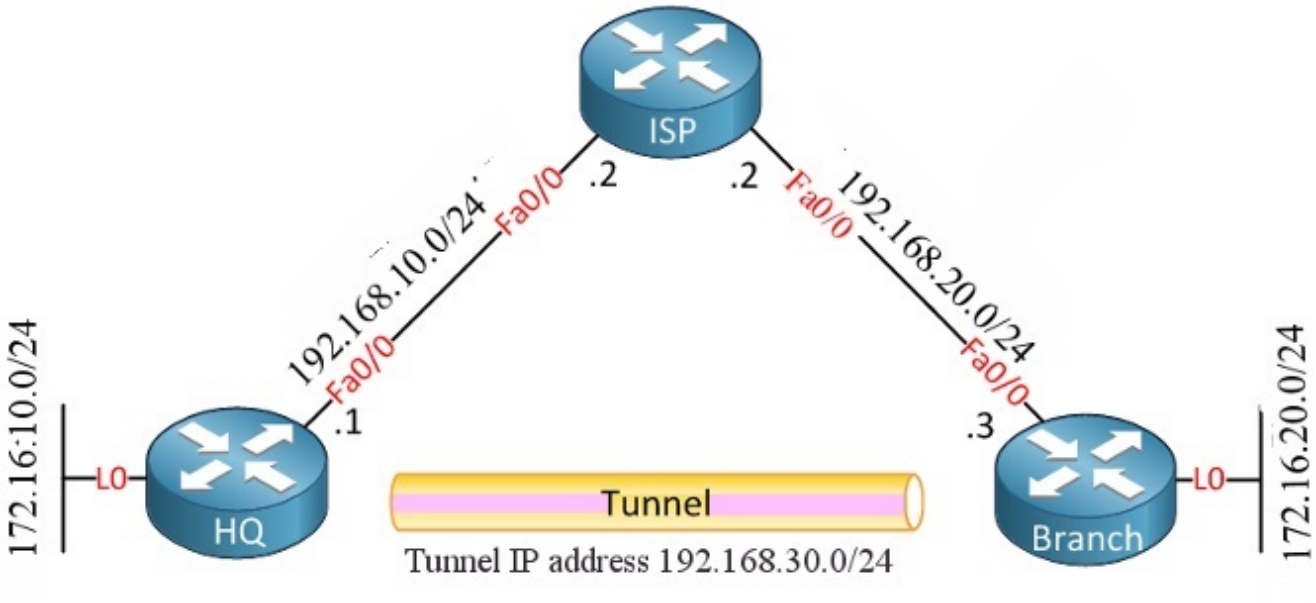
A drawback of IPSec is it does not support multicast traffic. But most popular routing protocols nowadays rely on multicast (like OSPF, EIGRP, RIP except BGP) to send their routing updates. A popular solution to this is using GRE tunnels. GRE tunnels do support transporting IP multicast and broadcast packets to the other end of the GRE tunnel. Non-IP traffic (such as IPX, AppleTalk) can be wrapped inside GRE encapsulation and then this packet is subjected to IPSec encapsulation so all traffic can be routed

Advantages of GRE tunnels include the following:

- GRE tunnels encase multiple protocols over a single-protocol backbone.
- GRE tunnels provide workarounds for networks with limited hops.
- GRE tunnels connect discontinuous sub-networks.
- GRE tunnels allow VPNs across wide area networks (WANs).

While GRE provides a stateless, private connection, it is not considered a secure protocol because it does not use encryption like the IP Security (IPSec) Encapsulating Security Payload (ESP), defined by RFC 2406

Configuring GRE Tunnel: Configuring a GRE tunnel involves creating a tunnel interface, which is a logical interface. Then you must configure the tunnel endpoints for the tunnel interface. Refer below fig



As seen, the GRE tunnel configuration at the minimum involves configuring the IP addresses at the Branch, HQ, and the ISP. Then, configuring the tunnel interfaces at the HQ and the Branch.

Configuration on HQ router:

HQ(config)#interface fastEthernet *0/0*
HQ(config-if)#ip address *192.168.10.1 255.255.255.0*
HQ(config-if)#exit
HQ(config)#interface loopback0
HQ(config-if)#ip address *172.16.10.1 255.255.255.0*
HQ(config-if)#exit
HQ(config)#ip route *192.168.20.3 255.255.255.255 192.168.10.2*
HQ(config)#interface tunnel *9*
HQ(config-if)#tunnel source *fastEthernet 0/0*
HQ(config-if)#tunnel destination *192.168.20.3*
HQ(config-if)#ip address *192.168.30.1 255.255.255.0*

Configuration on Branch office router:

Branch(config)#interface *fastEthernet 0/0*
Branch(config-if)#ip address *192.168.20.3 255.255.255.0*
Branch(config-if)#exit
Branch(config)#interface loopback *0*
Branch(config-if)#ip address *172.16.20.3 255.255.255.0*
Branch(config-if)#exit
Branch(config)#ip route *192.168.10.1 255.255.255.255 192.168.20.2*
Branch(config)#interface tunnel *9*
Branch(config-if)#tunnel source *fastEthernet 0/0*
Branch(config-if)#tunnel destination *192.168.10.1*
Branch(config-if)#ip address *192.168.30.3 255.255.255.0*

Configuration on ISP router:

ISP(config)#interface *fastEthernet 0/0*
ISP(config-if)#ip address *192.168.10.2 255.255.255.0*
ISP(config-if)#exit
ISP(config)#interface *fastEthernet 1/0*
ISP(config-if)#ip address *192.168.20.2 255.255.255.0*

Four steps to configure GRE tunnel over IPsec are:

1. Create a physical or loopback interface to use as the tunnel endpoint. Using a loopback rather than a physical interface adds stability to the configuration.

2. Create the GRE tunnel interfaces.

3. Add the tunnel subnet to the routing process so that it exchanges routing updates across that interface.

4. Add GRE traffic to the crypto access list, so that IPsec encrypts the GRE tunnel traffic.

An example of configuring GRE Tunnel is shown below:

interface Tunnel0

ip address *192.168.16.2 255.255.255.0*

tunnel source *FastEthernet1/0*

tunnel destination *14.38.88.10*

tunnel mode gre ip

Note: The last command is enabled by default so we can ignore it in the configuration)

Cisco® CCNP Route Exam Notes : Describing DMVPN(single Hub)

examguides.com/CCNP-Route/ccnp-routing-23.htm

4. VPN Technologies

4.2 Describe 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.

Some of the popular DMPVPN models are:

- Hub-and-spoke -This basic DMVPN model facilitates Spoke-to-spoke traffic through a single hub.
- Spoke-to-spoke - This model enables spoke-to-spoke tunnels that are dynamic in nature.

Some of the benefits of DMVPN are:

- Hubs can be configured with static NAT and spokes with dynamic NAT
- Supports dynamic addressing of spoke routers
- Additional, new spoke routers don't require any configuration
- Supports IPSec, NHRP, and GRE tunnels

- Simple hub and spoke deployment can provide full-mesh connectivity
- Supports Unicast, Multicast, and dynamic routing protocols
- Deployments can be with or without IPsec encryption
- Supports partial- or full-mesh VPNs

4.3 Describe Easy Virtual Networking (EVN)

EVN is an IP-based virtualization technology that provides end-to-end virtualization over Layer-3 networks. Network virtualization can be used to secure a network and to reduce network expenses by utilizing the same network infrastructure for multiple virtual networks. It provides a pure IP alternative to MPLS in enterprise networks for up to 32 VNs.

The following are the advantages of EVNs(Easy Virtual Networks):

- It uses existing physical IP infrastructure in providing virtual networks, simplifying Layer 3 network virtualization
- It provides shared services and support for organization, reducing the overall cost. Providing an alternative to MPLS.
- It provides enhanced management, troubleshooting, and usability.

The following are the important features of Easy Virtual Networks (EVN):

1. It is an IP-based virtualization technology that provides end-to-end virtualization of two or more Layer-3 networks.

2. It provides separate virtual networks whose traffic paths remain isolated from each other.

3. EVN supports IPv4, static routes, Open Shortest Path First version 2 (OSPFv2), and Enhanced Interior Gateway Routing Protocol (EIGRP) for unicast routing, and Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) for IPv4 Multicast routing.

4. EVN also supports Cisco Express Forwarding (CEF) and Simple Network Management Protocol (SNMP).

5. You must have a functioning campus design in place before adding virtualization to a network.

6. EVN uses virtual routing and forwarding (VRF) instances to maintain traffic separation across the network.

7. Each EVN runs a separate instance of a routing protocol

8. Routing Protocols Supported by EVN(Easy Virtual Network): Each EVN runs a separate instance of a routing protocol. Different virtual networks may run different routing protocols concurrently.

9. EVN supports static routes, OSPFv2, and EIGRP for unicast routing, and PIM, MSDP, and IGMP for multicast routing.

Previous Contents Next

Cisco® CCNP Route Exam Notes : AAA(Authentication, Authorization and Accounting) Concepts

examguides.com/CCNP-Route/ccnp-routing-24.htm

5. Infrastructure Security

5.1 AAA

AAA stands for Authentication, Authorization, and Accounting.

Authentication: Authentication provides the method of identifying users, primarily using login and password. The communication is usually encrypted. Authentication is the way a user is identified prior to being allowed access to the network and network services.

Authorization: Authorization provides authorization for access to network resources. Remote security servers, such as RADIUS and TACACS+, authorize users for accessing specific resources by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.

Accounting: Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

Given below are the steps in brief that one needs to go through for configuring AAA.

On the client side:

1. Configure AAA : **aaa new model**

2. Specify AAA server to be accessed by the client:

acacs-server host *192.168.1.2 key cisco@123*

3. Create a name method list. MYAUTHLIST is used for example only. You can use whichever name you want.

aaa authentication login *MYAUTHLIST* **group tacacs+ local**

4. Create authorization method list to apply on users that have been authenticated.

aaa authorization exec *MYAUTHORIZATIONLIST* **group tacacs+ local**

5. Apply the method lists to a device interface

line vty *0 4*
login authentication *MYAUTHLIST*
authorization exec *MYUAUTHORIZATIONLIST*

Example:The given command is:

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.

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 name 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)

! 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

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*

Previous Contents Next

Cisco® CCNP Route Exam Notes : Radius Server and TACACS+ Server

examguides.com/CCNP-Route/ccnp-routing-25.htm

5. Infrastructure Security

5.2 RADIUS Server

an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. RADIUS implements a client/server architecture, where typical client is a router, switch, or AP and the typical server is a Windows or Unix device that is running RADIUS software.

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).

5. On the other hand , TACACS+ provides complete encryption for communication between the TACACS+ server and the client.

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

5.3 TACACS+ Server

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. We must have access to and must configure a TACACS+ server before the configured TACACS+ features on a network access server are available. It provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service authentication, authorization, and accounting independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon. The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service. The Cisco family of access servers and routers and the Cisco IOS user interface (for both routers and access servers) can be network access servers.

Syntax : **Router(config)#tacacs-server host** <*ip-address*> **key** <*keyname*>

Ex: **Router(config)#tacacs-server host** *192.168.10.1* **key** *cisco123*

Features of TACACS+ Server

a. 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.

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

c. 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.

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

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

Previous Contents Next

Cisco® CCNP Route Exam Notes : Configure And Verify Device Access Control

examguides.com/CCNP-Route/ccnp-routing-26.htm

5. Infrastructure Security

5.4 Configure and verify device access control

an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. RADIUS implements a client/server architecture, where typical client is a router, switch, or AP and the typical server is a Windows or Unix device that is running RADIUS software.

5.4.a Lines (VTY, AUX, console):

There are three types of lines on Cisco routers:

VTY - Virtual lines that allow SSH or Telnet access to the device

AUX - Provides CLI access via an aux cable.

CON - Provides CLI access via a console cable.

The range of privilege levels that can be set are from 0 to 15, that is sixteen in total. Level 1 is the default user EXEC privilege. Level 15 is the highest level and allows the user to have full access to the device commands. The command used to set additional privilege levels is:

privilege <*mode*> **level** <*level*>

For example, to assign a privilege level of 4 in exec mode, use the command:

privilege exec level 4 trace

Note that all commands that were assigned to the previous privilege levels are inherited along with the new command(s) defined in the privilege statement.

This type of granular control is very useful in large networks where there are many network administrators with different set of access rights.

The traceroute privileged EXEC command can be used to find the routes that a packet travels when passing from a router to its destination address.

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.

The following are the features of the ip unnumbered interface:

1. Any packet generated by an unnumbered interface will have the IP address of the interface that was defined in the creation of the unnumbered interface.

2. Certain protocols such as X.25, and SMDS do not support ip unnumbered interface.

3. Ping EXEC command is not supported by the unnumbered interface.

4. If the interface from which an unnumbered interface got the ip address is down, then the unnumbered interface also will be down. Therefore, it is advisable to use loop back interface while defining an unnumbered interface.

5.4.b Management plane protection

Management plane protection refers to allowing certain protocols on the management interface. When configuring protocols for security, you should use encrypted protocols wherever possible. For example, use SSH instead of telnet or https instead of http.

To create the Public/Private key pair used by SSH, the following command sequence is used.

Hostname other than the default "router" needs to be configured first before issuing the

command crypto key generate rsa. You also need to configure the domain name before issuing the crypto key generate command.

The correct sequence of commands would be:

hostname *Frisco*
ip domain-name *cisco.com*
crypto key generate *rsa*

The following are the important features of CCP (Cisco Configuration Professional):

1. Cisco Configuration Professional supports secure protocols such as Secure Shell (SSH) Protocol and Secure HTTP (HTTPS) to communicate with the devices.

2. Cisco Configuration Professional manages only Cisco devices

3. Currently there is no limitation on the number of communities that can be created.

4. When you move away a router from one community to another, you need to rediscover the routers in the new community.

5. Cisco Configuration Professional is a GUI device-management tool for Cisco IOS Software-based access routers, the Cisco Integrated Services Routers

6. A community is a group of devices that are managed together.

The following precautions may be taken to harden network infrastructure:

a. Use physical barriers such as room lock so that un-authorized persons do not have access to the network devices.

b. Use firewall so that outsiders cannot access network devices from outside the network

c. Enable SSH so that passwords are transmitted in encrypted form

5.4.c Password encryption

Password protection enables that unauthorized users do not log into the network. However, once an authorized user logs into the network and leaves the device unattended, the session will remain open. An unauthorized person may misuse the login session initiated by an authorized user earlier.

To prevent such misuse, session timeout need to be configured on Cisco devices. The command for configuring session timeout on a router interface is:

Router(config-line)#exec-timeout <*minutes*> <*seconds*>

The command "**ip unnumbered**" is used for enabling an interface for IP processing without assigning any explicit IP address. The interface configured with unnumbered command uses the IP address of the interface specified in the command. The correct syntax for this command is : ip unnumbered <type number>

Ex: **ip unnumbered** *Etherneto*

The above command enables the unnumbered interface to use the IP address of Etherneto. Note that the interface specified by the must have explicit IP address, and not another unnumbered interface.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Configure And Verify Router Security Features

examguides.com/CCNP-Route/ccnp-routing-27.htm

5. Infrastructure Security

5.5 Configure and verify router security features

The access control list features enable to filter traffic depends on the information in an IP packet header. You can use the access control list on IPv4 as well as IPv6. You can configure the access list on the layer 3 switch or router to offer the basic security for the network. Suppose you did not configure the ACL, all the packets which flowing via the switch can be allowed in all parts of a network.

5.5.a IPv4 access control lists (standard, extended, time-based)

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 three types of IP access lists:

1. Standard IP Access Lists:

This is the command syntax format of a standard ACL.

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

Keep in mind that:

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

2. 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.

3. Access lists applied to interfaces default to outbound if no direction is specified.

2. Extended IP Access Lists: 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. IP Named ACLsIP 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.)

As seen from the syntax, the source ip address precedes the destination. Extended access lists are applied close to source where as standard access lists are applied close to destination.

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

Using a named access list just replaces the number used when applying the list to the router's interface

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

We can use the statement **access-list** *<access-list #> [permit/deny] [protocol] host <source-ip-address> <destination-ip-address> <destination-wildcard-mask>*

To permit or deny a specific host from accessing a network.

Note: if we use "host" command, source wild card mask is not required.

Access lists are primarily used for two purposes:

1. Controlling traffic through a router, and

2. Controlling VTY access to a router's VTY ports

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 fastethernet 0/0

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

Numbered Access List have a major disadvantage, which is the ability to edit specific lines in the access-list. Unfortunately the only way to do that is to edit the lines in a text editor and completely remove and re-add the ACL. Named ACL's also have a big advantage of being descriptive in the name such as an ACL named "Deny_Telnet" its quite obvious that that ACL would be for denying telnet access.

This is the command syntax format for IP named ACLs

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

The following commands can be used to view access lists:

sh ip access-list

Given below are the sequence of commands that are used for configuring named access lists:

1. enable

2. configure terminal

3. ip access-list extended <*name*>

4. deny protocol [source source-wildcard] {any | host {address | name} {destination [destination-wildcard] {any | host {address | name} [log]

5. permit protocol [source source-wildcard] {any | host {address | name} {destination [destination-wildcard] {any | host {address | name} | object-group object-group-name} [log]

The necessary configuration steps for doing the same are as given below:

R1>enable
R1#configure terminal
Enter into global configuration mode
R1(config)#ip access-list extended *DenyPing*
R1(config-ext-acl)#deny icmp host *192.168.100.18 192.168.100.1 0.0.0.0*
R1(config-ext-acl)#permit ip any any

Notice that we have to explicit allow other traffic (access-list 101 permit ip any any) as there is an "deny all" command at the end of each ACL.

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, note the following:

- 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.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Ipv6 Traffic Filter

examguides.com/CCNP-Route/ccnp-routing-28.htm

5. Infrastructure Security

5.5 Configure and verify router security features

5.5.b IPv6 traffic filter

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]

Example 1: The command "**deny tcp any any eq telnet**" command restricts any host telnetting to any destination host

ipv6 access-list <*access-list-name*>

the command defines IPv6 access list name, and enter IPv6 access-list configuration mode.

Example 2: deny ipv6 host *2001:db8:100::18 2001:db8:100::1/64*

The statement **deny ipv6 host** *2001:db8:100::18 2001:db8:100::1/64* denies any ipv6 traffic with a source IP Address of - 2001:db8:100::18 that is destined for 2001:db8:100::1/64, That is the IP Address must match exactly

Example3:

Step 1 : Create an IPv6 ACL, and enter IPv6 access list configuration mode.

Switch#configure terminal
Switch(config)#ipv6 access-list <*list-name*>

Ex:

Switch(config)#ipv6 access-list *myipv6list*
myipv6list is the list name.
Switch(config-ipv6-acl)#

Step 2 : Configure the IPv6 ACL to block (deny) or pass (permit) traffic, use the command:

Switch(config-ipv6-acl)#deny | permit protocol

Ex.: **Switch(config-ipv6-acl)#permit icmp any any**

Step 3 : Apply the IPv6 ACL to an interface. For router ACLs, you must also configure an IPv6 address on the Layer 3 interface to which the ACL is applied.

Step: 3.1
Switch# configure terminal
Switch(config)# interface *interface-id*

Ex: **Switch(config)# interface** *gigabitethernet1/0/2*

Switch(config-if)#no switchport ; this command enables switch interface for layer-3 operation.

Step 3.2 : **ipv6 address** <*ipv6-address*>

Ex: **Switch(config-if)# ipv6 address** *2001::/64 eui-64*

Here you assigned an ipv6 address to the interface.

Step 3.3 : **ipv6 traffic-filter** <*access-list-name*> *{ in | out }*

Switch(config-if)# ipv6 traffic-filter *myipv6list out*

here you applied the access-list to an out going interface.

IPV6 uses traffic-filter command to filter traffic that is forwarded, not originated by router.

To filter incoming or outgoing IPv6 traffic on an interface, use ipv6 traffic filter command in interface configuration mode.

Syntax: **R1 (config-if)#ipv6 traffic-filter** *<access-list-name> { in | out }*

The commands are typically given while configuring router connectivity with an ISP.

IPv6 ACLs cannot be numbered they can only be configured as named access list

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 command "**show ipv6 access-lists**" is given in the privileged EXEC mode. Given below is an example of the output and it shows IPv6 access lists configured on the switch.

Switch#show ipv6 access-list

IPv6 access list inbound
permit tcp any any eq eigrp (12 matches) sequence 10
permit tcp any any eq telnet (5 matches) sequence 20
permit udp any any sequence 30
IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20

Previous Contents Next

Cisco® CCNP Route Exam Notes : SNMPv2 and SNMPv3

examguides.com/CCNP-Route/ccnp-routing-29.htm

6. Infrastructure Services

6.1 SNMPv2 and SNMPv3

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

noAuthNoPriv - Security level that does not provide authentication or encryption.

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.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed.

The main difference between SNMPv3 and v2 (or v1) is that the v3 version addresses the security and privacy issues. For example, in SNMPv2, 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

The following are the snmp security model and their encryption types

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

Cisco® CCNP Route Exam Notes : Configure And Verify Logging

examguides.com/CCNP-Route/ccnp-routing-30.htm

6. Infrastructure Services

6.2 Configure and verify logging

Cisco routers log messages can handle in five different ways:

1. 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.

2. 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

3. 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#

4. 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 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#

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

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]}*

Previous Contents Next

Cisco® CCNP Route Exam Notes : Configure And Verify Network Time Protocol (NTP)

examguides.com/CCNP-Route/ccnp-routing-31.htm

6. Infrastructure Services

6.3 Configure and verify Network Time Protocol (NTP)

Network Time Protocol (NTP) is a networking protocol designed to time-synchronize device with in a network. NTP time server works within the TCP/IP suite and uses User Datagram Protocol (UDP) port 123 as its transport protocol. An NTP network usually receives its time from an authoritative time resource, such as an atomic clock or a radio clock attached to a time server and distributes this time across the network.

NTP servers are normally dedicated NTP devices that use a single time reference to which they can synchronize a network. This time reference is a Coordinated Universal Time (UTC) source, a global time scale distributed by atomic clocks over the internet. The dedicated NTP servers are required for Security, Accuracy, Protection, Legality, and Control.

Unlike PCs or servers, Cisco network devices specifically need to run NTP to synchronize the time and date. That's because most Cisco devices don't have an internal clock. An NTP client synchronizes the time and date with an NTP server. The NTP server should be a reliable source.

To configure NTP on your IOS router, follow the steps given below:

1. Choose the NTP server your Cisco router/switches will use.

2. Find out the IP address for this server. It could be an external source such as NIST or internal.

3. Enter the following commands on the IOS device:

Router# configure terminal
Router(config)# ntp server <*IP address of NTP Server*>

4. Verify the association with the server using the show ntp status and show ntp associations commands.

The NTP service can be activated by entering any ntp command. When you use the ntp broadcast client command, the NTP service is activated (if it has not already been activated) and the device is configured to receive NTP broadcast packets on the specified interface simultaneously.

The command "**ntp broadcast client**" Allows the system to receive NTP broadcast packets on the specified interface.

Following is the sample output from "**show ntp association**"

```
Router> show ntp associations

  address         ref clock       st  when  poll  reach  delay  offset  disp
~192.168.7.1      192.168.7.1      9    50    64    377    0.0    0.00   0.0
 ~192.31.32.2     192.31.32.1      5    29  1024    377    4.2   -8.59   1.6
+~192.168.13.33   192.168.1.111    3    69   128    377    4.1    3.48   2.3
*~10.50.36.42     86.79.127.250    4   188   256    377    0.7   -0.17   0.3
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

The device with ip address 192.168.7.1 is NTP master. The first entry shows 192.168.7.1. This indicates that the local machine has synced with itself. Generally, only an NTP master syncs with itself.

The third column shows how many hops that the master clock is away from the local machine. It is called stratum in NTP terminology. 192.168.13.33 is 3 hops away as seen in the output.

Previous Contents Next

Cisco® CCNP Route Exam Notes : Configure And Verify Ipv4 Network Address Translation (NAT)

examguides.com/CCNP-Route/ccnp-routing-32.htm

6. Infrastructure Services

6.4 Configure and verify IPv4 Network Address Translation (NAT)

Given below are the four important forms of NAT (Network Address Translation):

Static NAT: It is a one-to-one mapping between an unregistered IP address and a registered IP address.

Dynamic NAT:

Usually, Dynamic NAT is implemented, where a pool of public IP addresses is shared by an entire private IP subnet. When a private host initiates a connection, a public IP address is selected. The mapping of the computer's non-routable IP address matched to the selected IP address is stored in the NAT Table. As long as the outgoing connection is maintained, the private host can be reached by incoming packets sent to the specified public address. When the binding expires, the address is returned to the pool for reuse.

Overloading: A variation of Dynamic NAT, also known as Network Address Port Translation (NAPT) maps multiple unregistered IP addresses to a single registered IP address by multiplexing streams differentiated by the TCP/UDP port number.

Overlapping: When Overlapping is employed, the IP addresses used on the internal network are registered IP addresses utilized on another network. To avoid conflict, a NAT Table is built to translate these redundant internal addresses to a unique IP address. Vice versa, when sending packets into the private network, the registered addresses must be translated to an address unique in the network.

When you are configuring NAT, NAT should be enabled on at least one inside and one outside interface. Typically "ip nat inside" is configured on the interfaces in local environment which cannot be routed to the internet(typically private range of IP Addresses) and "ip nat outside" is configured on the interface which is connected to the internet

The following command configures a static NAT translation by mapping inside local address to the inside global address.

ip nat inside source static *192.168.0.100 88.248.153.137*

Here, 192.168.0.100 is the inside local address, and 88.248.153.137 is the inside global address. A packet's source address 192.168.0.100 is changed to 88.248.153.137 by the NAT device.

The correct syntax for enabling dynamic NAT to translate many inside hosts to an inside global IP address is:

ip nat inside source list <*access-list-number*> **pool** <*pool-name*> **overload**

where <access-list-number> is the standard access list number, and <pool-name> is the pool name. Note that the option "overload" specifies many to one relationship. This configuration is typically used when many hosts with private IP addresses need to access Internet through a specified globally unique IP address.

The following two statements are true about dynamic NAT translations:

1. The inside IP addresses eligible for address translation are defined in a standard IP access-list.

2. Only packets moving between inside and outside networks will get translated. This is true even for static NAT. If a packet is destined for another host, but does not require to cross the NAT boundary, the packet source /destination addresses are not translated. This is understandable, since the packet is not crossing the inside network boundary.

Enable dynamic NAT on an interface include the following:

1. Defining a standard IP access-list using the command

access-list <*access-list-number*> *{permit | deny}* <*local-ip-address*>

2. Defining an IP NAT pool for the inside network using the command

ip nat pool *<pool-name> <start-ip> <end-ip> {netmask <net-mask> | prefix-length <prefix-length>} [type-rotary]*

Note that type-rotary is optional command. It indicates that the IP address range in the address pool identifies hosts among which TCP load is distributed.

3. Mapping the access-list to the IP NAT pool by using the command

ip nat inside source list *<access-list-number> pool <pool-name>*

4. Enabling NAT on at least one inside and one outside interface using the command:

ip nat *{inside | outside}*

Defining "type-rotary" to identify real inside hosts is not an essential command.

The following are statements true about NAT

1. NAT allows several hosts be connected to Internet by using fewer globally unique IP addresses. This in turn results in conserving the scarce public IP addresses. The terms public / global is used in the sense that the IP addresses are globally unique and officially registered.

2. NAT supports load sharing on inside machines. The inside machines are accessed in a round robin fashion, thus sharing load.

3. NAT offers some degree of security since IP addresses are not easily traceable. This is because, the actual host IP that is accessing the Internet is translated into outside IP address and vice versa. Thus, NAT offers protection against hacking.

4. One disadvantage of NAT is that it increases delay. This is obvious since address translation is involved.

5. Another disadvantage of NAT is that, when an application uses physical IP address, it may not function properly. This is because the physical IP address is changed by NAT.

The following is sample output of the Show ip nat translations command

```
router# show ip nat translations
Pro Inside global         Inside local       Outside local      Outside global
udp 172.56.211.205:1120   192.168.1.15:1120      ----               ----
tcp 172.56.211.205:10014  192.168.1.19:10014     ----               ----
tcp 172.56.211.205:1056   192.168.1.15:1056      ----               ----
```

The output shows Dynamic NAT translation with Overloading. This is evident from the fact that different inside local addresses have translated to the same inside global IP address, with different port mappings.

Cisco® CCNP Route Exam Notes : Describe Ipv6 NAT

examguides.com/CCNP-Route/ccnp-routing-33.htm

6. Infrastructure Services

6.5 Describe IPv6 NAT

IPv6 NAT helps to translate IPv4 addresses to IPv6 addresses of network devices. IPv6 NAT also helps to translate the address between IPv6 hosts. IPv6 NAT supports source NAT, destination NAT, and static NAT. NAT-PT was the original translation scheme for communication between IPv4 and IPv6, but has since been deprecated and replaced by NAT64. NAT64 allows one or multiple public IPv4 addresses are shared by many IPv6-only devices using overloading. NAT64 performs both address and header translation.

NAT64 is a mechanism to allow IPv6 hosts to communicate with IPv4 servers or hosts. The NAT64 server is the endpoint for at least one IPv4 address and an IPv6 network segment of 32-bits The IPv6 client embeds the IPv4 address it wishes to communicate, and sends its packets to the resulting address. The NAT64 server then creates a NAT-mapping between the IPv6 and the IPv4 address, allowing them to communicate.

Network Prefix Translation (NPTv6): is a one-to-one stateless translation. One IPv6 address in an inside network is translated to one IPv6 address in an outside network. The reason for using NPTv6 and the overriding idea behind it is that internal networks can be independent of an ISPs address space which makes changing ISP a simpler process. It translates the prefix portion of an IPv6 address but not the host portion or the application port numbers. The host portion is simply copied, and therefore remains the same on either side of the firewall. The host portion also remains visible within the packet header.