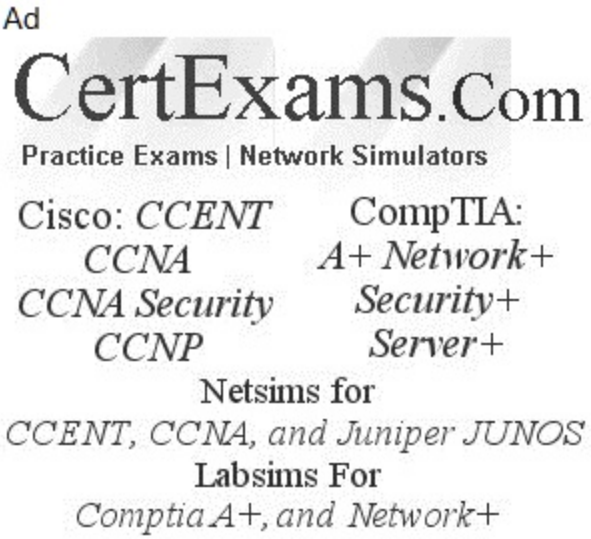
Juniper® JNCIA Exam Cram Notes : Collision Domains And Broadcast Domains

examguides.com/Juniper-JNCIA/juniper-jncia-1.htm

Ad



1. Networking Fundamentals

1.1 Collision domains and broadcast domains

A **collision domain** is, as the name implies, a part of a network where packet collisions can occur. A collision occurs when two devices send a packet at the same time on the shared network segment. The packets collide and both devices must send the packets again, which reduces network efficiency. Collisions are often in a hub environment, because each port on a hub is in the same collision domain. By contrast, each port on a bridge, a switch or a router is in a separate collision domain. Each port of the switch belongs to a single collision domain. In case of switch, the collision domain is limited to each device and in a hub, the collision domain includes all devices connected to the hub.

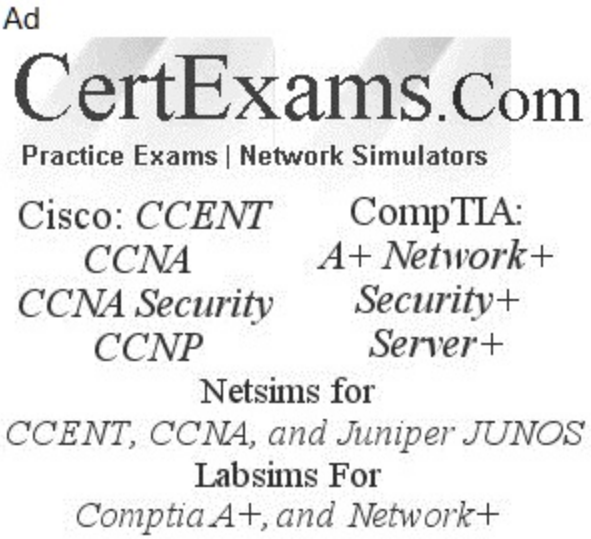
A **broadcast domain** is a domain in which a broadcast is forwarded. A broadcast domain contains all devices that can reach each other at the data link layer (OSI layer 2) by using broadcast. All ports on a hub or a switch are by default in the same broadcast domain. All ports on a router are in the different broadcast domains and routers don't forward broadcasts from one broadcast domain to another.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Function Of Routers And Switches

examguides.com/Juniper-JNCIA/juniper-jncia-2.htm

Ad



1. Networking Fundamentals

1.2 Function of routers and switches

Router is a layer 3 device which works on network layer of OSI model which connects two different networks and it identifies network devices based on their IP addresses.

The Routers are the devices used for connecting local network to the other local network/s. They are generally located at the gateway where two or more than two networks connect.

Switch is a layer 2 device which works on data link layer of OSI model, it communicates by using frames and it identifies network devices on the basis of MAC addresses or physical addresses.

System Switching Board (SSB) and Forwarding Engine Board (FEB) are the two different router models used for the control board functionality.

An **aggregate route** is the second form of a locally configured route within the JUNOS software.

System Switching Board (SSB) and Forwarding Engine Board (FEB) are the two different router models used for the control board functionality.

An aggregate route is the second form of a locally configured route within the JUNOS software.

Each router model uses a different name for the control board functionality. The possible names include:

Forwarding Engine Board (FEB): The Forwarding Engine Board is found in both the M5 and M10 platforms and integrates the circuit board with the FPC. Each router contains no more than one FEB, which is specific to either the M5 or the M10 chassis.

System Switching Board (SSB):The System Switching Board is found in the M20 platform. Each platform is configured to hold dual SSBs, but only one board is operational at any one time.

System Control Board (SCB): The System Control Board is found in the M40 platform. Each chassis contains no more than one SCB.

Switching and Forwarding Module (SFM): The Switching and Forwarding Module is found in the M40e and M160 platforms. Each M40e router can contain 2 SFMs, with only one operational at a time. The M160 router contains four SFMs working in parallel.

Memory Mezzanine Board (MMB): The Memory Mezzanine Board is found in the T320 and T640 platforms and is located on the FPC itself.

Each Routing and Control Board (RCB) consists of the following internal components:

CPU-Runs Junos OS to maintain the routing tables and routing protocols and handles these exception packets and performs the appropriate action.

EEPROM- Stores the serial number of the Routing Engine.

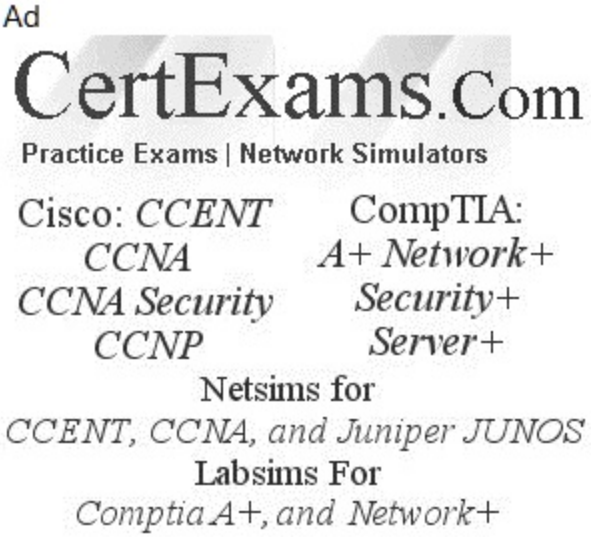
DRAM-Provides storage for the routing and forwarding tables and for other Routing Engine processes.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Optical Network Fundamentals - Sonet/sdh, Otn

examguides.com/Juniper-JNCIA/juniper-jncia-3.htm

Ad



1. Networking Fundamentals

1.3 Optical network fundamentals - SONET/SDH, OTN

Synchronous Digital Hierarchy (SDH) is a CCITT standard for a hierarchy of optical transmission rates. Synchronous Optical Network (SONET) is a USA standard that is largely equivalent to SDH. Both are widely used methods for very high speed transmission of voice and data signals across the numerous world-wide fiber-optic networks.

SDH and SONET use light-emitting diodes or lasers to transmit a binary stream of light-on and light-off sequences at a constant rate. At the far end optical sensors convert the pulses of light back to electrical representations of the binary information.

The basic building block of the SONET/SDH hierarchy in the optical domain is an OC1; in the electrical domain, it is an STS-1. An OC1 operates at 51.840 Mbps. OC3 operates at 155.520 Mbps.

Optical Transport Network (OTN) technology represents both a technical leap forward in optical networking over SONET/SDH and a business opportunity for carriers and service providers alike.

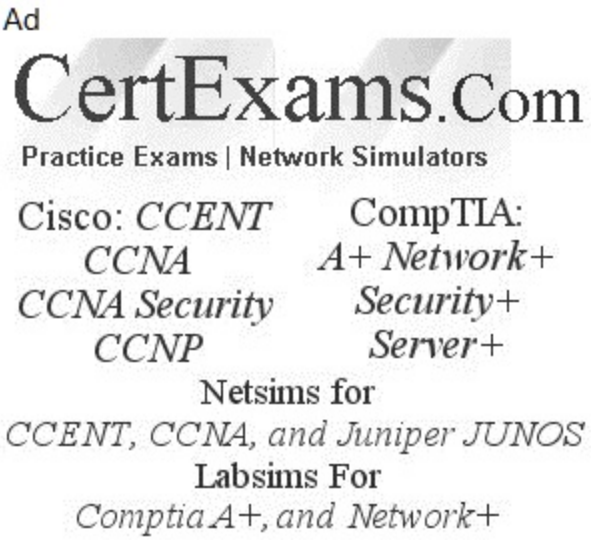
OTN	SONET/SDH

Asynchronous mapping of payloads	Synchronous mapping of payloads
Timing distribution not required	Requires right timing distribution across networks
Designed to operate on multiple wavelengths	Designed to operate on multiple wavelengths
Scales to 100Gb/s (and beyond)	Scales to a maximum of 40 Gb/s
Performs single-stage multiplexing	Performs multi-stage multiplexing
Uses a fixed frame size and increases frame rate to match client rates	Uses a fixed frame rate for a given line rate and increases frame size as client size increases
FEC sized for error correction to correct 16 blocks per frame	Not applicable (no standardized FEC)

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Ethernet Networks

examguides.com/Juniper-JNCIA/juniper-jncia-4.htm

Ad


1. Networking Fundamentals

1.4 Ethernet Networks

Ethernet is a Layer 2 technology that operates in a shared bus topology. Ethernet supports broadcast transmission, uses best-effort delivery, and has distributed access control. Ethernet is a point-to-multi point technology.

In a shared bus topology, all devices connect to a single, shared physical link through which all data transmissions are sent. All traffic is broadcast so that all devices within the topology receive every transmission. The devices within a single Ethernet topology make up a broadcast domain.

Ethernet uses best-effort delivery to broadcast traffic. The physical hardware provides no information to the sender about whether the traffic was received. If the receiving host is offline, traffic to the host is lost. Although the Ethernet data link protocol does not inform the sender about lost packets, higher layer protocols such as TCP/IP might provide this type of notification.

Ethernet Access Control and Transmission: Ethernet's access control is distributed because Ethernet has no central mechanism that grants access to the physical medium within the network. Instead, Ethernet uses carrier-sense multiple access with collision detection (CSMA/CD). Because multiple devices on an Ethernet network can access the physical medium, or wire, simultaneously, each device must determine whether the physical medium is in use. Each host listens on the wire to determine if a message is being transmitted. If it

detects no transmission, the host begins transmitting its own data.The length of each transmission is determined by fixed Ethernet packet sizes. By fixing the length of each transmission and enforcing a minimum idle time between transmissions, Ethernet ensures that no pair of communicating devices on the network can monopolize the wire and block others from sending and receiving traffic.

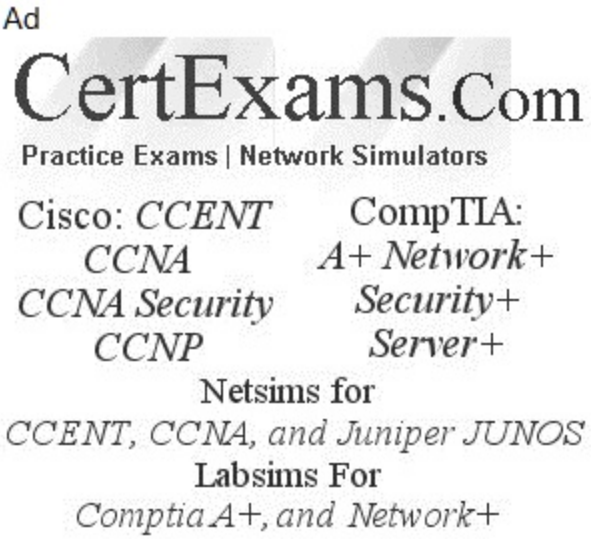
Collisions and Detection

When a device on an Ethernet network begins transmitting data, the data takes a finite amount of time to reach all hosts on the network. Because of this delay, or latency, in transmitting traffic, a device might detect an idle state on the wire just as another device initially begins its transmission. As a result, two devices might send traffic across a single wire at the same time. When the two electrical signals collide, they become scrambled so that both transmissions are effectively lost.

To handle collisions, Ethernet devices monitor the link while they are transmitting data. The monitoring process is known as collision detection. If a device detects a foreign signal while it is transmitting, it terminates the transmission and attempts to transmit again only after detecting an idle state on the wire. Collisions continue to occur if two colliding devices both wait the same amount of time before re transmitting. To avoid this condition, Ethernet devices use a binary exponential backoff algorithm.

Juniper® JNCIA Exam Cram Notes : Layer2 Addressing And Address Resolution

examguides.com/Juniper-JNCIA/juniper-jncia-5.htm



1. Networking Fundamentals

1.5 Layer2 addressing and address resolution

The Internet is a global, public network with IP subnets connected by routers and exchanging packets. Both Ethernet and IP use globally unique network addresses that can be used as the basis for a truly global network. Ethernet MAC addresses come from the IEEE and IP subnet addresses come from various Internet authorities. (IP also employs a naming convention absent in Ethernet, but we'll ignore that in this discussion.) The key differences in how these addresses are assigned make all the difference when it comes to the basic functions of a bridge as opposed to a router.

All devices on LANs that are attached to the Internet have both MAC layer and IP addresses. Frames and packets contain both source and destination addresses in their headers.

In general:

- MAC addresses are 48 bits long. The first 24 bits are assigned by the IEEE and form the organizationally unique identifier (OUI) of the manufacturer or vendor requesting the address. The last 24 bits form the serial number of the LAN interface cards and their uniqueness must be enforced by the company (some companies reuse numbers of bad or returned cards while others do not).

- IPv4 addresses are 32 bits long. A variable number of the beginning bits are assigned by an Internet authority and represent a subnet located somewhere in the world. The remaining bits are assigned locally and, when joined to the network portion of the address, uniquely identify some host on a particular network.
- IPv6 addresses are 128 bits long.

Virtual Local Area Network (VLAN) creates a separate broadcast domain in layer 2 network. VLANs can also help create multiple layer 3 networks on a single physical infrastructure.

Address Resolution: ARP is the Address Resolution Protocol, which maintains a table named as ARP table. Sending IP packets on a multi access network requires mapping from an IP address to a media access control (MAC) address (the physical or hardware address).

In an Ethernet environment, ARP is used to map a MAC address to an IP address. ARP dynamically binds the IP address (the logical address) to the correct MAC address. Before IP unicast packets can be sent, ARP discovers the MAC address used by the Ethernet interface where the IP address is configured.

Hosts that use ARP maintain a cache of discovered Internet-to-Ethernet address mappings to minimize the number of ARP broadcast messages. To keep the cache from growing too large, an entry is removed if it is not used within a certain period of time. Before sending a packet, the host searches its cache for Internet-to-Ethernet address mapping. If the mapping is not found, the host sends an ARP request.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Ipv4 And Ipv6 Fundamentals

examguides.com/Juniper-JNCIA/juniper-jncia-6.htm

1. Networking Fundamentals

1.6 IPv4 and IPv6 Fundamentals

IP addresses are assigned by a central numbering authority called the Internet Assigned Numbers Authority (IANA). IANA ensures that addresses are globally unique where needed and has a large address space reserved for use by devices not visible outside their own networks.

IPv4 addressing: IPv4 addresses are 32-bit numbers that are typically displayed in dotted decimal notation. A 32-bit address contains two primary parts: the network prefix and the host number.

All hosts within a single network share the same network address. Each host also has an address that uniquely identifies it. Depending on the scope of the network and the type of device, the address is either globally or locally unique. Devices that are visible to users outside the network (webservers, for example) must have a globally unique IP address. Devices that are visible only within the network must have locally unique IP addresses.

IPv4 classful addressing: To provide flexibility in the number of addresses distributed to networks of different sizes, 4-octet (32-bit) IP addresses were originally divided into three different categories or classes: class A, class B, and class C. Each address class specifies a different number of bits for its network prefix and host number:

- Class A addresses use only the first byte (octet) to specify the network prefix, leaving 3 bytes to define individual host numbers.
- Class B addresses use the first 2 bytes to specify the network prefix, leaving 2 bytes to define host addresses.
- Class C addresses use the first 3 bytes to specify the network prefix, leaving only the last byte to identify hosts.

In binary format, with an x representing each bit in the host number, the three address classes can be represented as follows:

00000000 xxxxxxxx xxxxxxxx xxxxxxxx (Class A)
00000000 00000000 xxxxxxxx xxxxxxxx (Class B)
00000000 00000000 00000000 xxxxxxxx (Class C)

Subnetting: Subnetting an IP Network is done primarily for better utilization of available IP address space, and routing purpose. Other reasons include better organization, use of different physical media (such as Ethernet, WAN, etc.), and securing network resources.

A subnet mask enables you to identify the network and node parts of the address. The network bits are represented by the 1s in the mask, and the node bits are represented by the 0s. A logical AND operation between the IP address and the subnet mask provides the Network Address.

For example, using our test IP address and the default Class C subnet mask, we get:

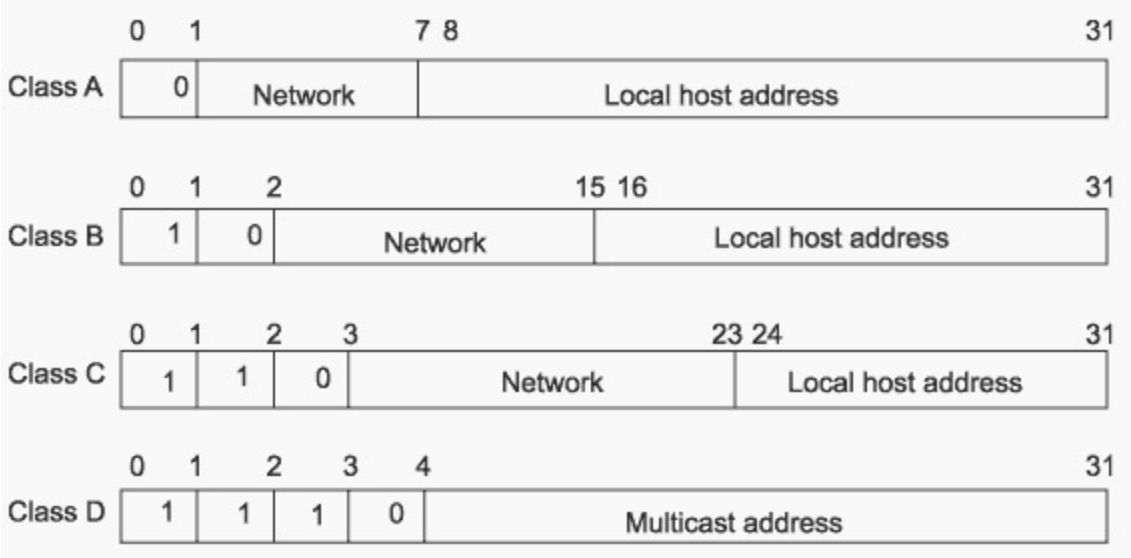
192.189.210.078: 1100 0000.1011 1101.1101 0010.0100 1110 Class C IP Address

255.255.255.000: 1111 1111.1111 1111.1111 1111.0000 0000 Default Class C subnet mask

192.189.210.0 1100 0000 1011 1101 1101 0010 0000 0000

As can be seen above, by using and AND operator, we can compute the network portion of an IP address. The network portion for the IP address given in the above example is 192.189.210.0, and the host portion of the IP address is 078.

Below fig. Shows the format of IP address classes



- Class A -The leading bit is set to 0, a 7-bit number, and a 24-bit local host address. Up to 125 class A networks can be defined, with up to 16,777,214 hosts per network.
- Class B - The two highest-order bits are set to 1 and 0, a 14-bit network number, and a 16-bit local host address. Up to 16,382 class B networks can be defined, with up to 65,534 hosts per network.

- Class C - The three leading bits are set to 1, 1, and 0, a 21-bit network number, and an 8-bit local host address. Up to 2,097,152 class C networks can be defined, with up to 254 hosts per network.
- Class D -The four highest-order bits are set to 1, 1, 1, and 0. Class D is used as a multicast address.

Subnetwork Mask Format: IPv4 subnetwork masks specified in one of the two ways: dotted decimal or prefix length notation.

Dotted decimal notation expresses IP addresses and masks in dotted quads - four octets separated by dots (A.B.C.D). In this format, each octet in the address or mask is represented as a decimal number and the dots are used as octet separators.

For example, an IP address and subnetwork mask in dotted decimal notation would appear as 192.168.100.1 255.255.255.0

Prefix length notation (often called network prefix format) allows for more efficient allocation of IP addresses than the old Class A, B, and C address scheme. The prefix length is the number of leftmost contiguous bits equal to 1 in the subnetwork mask. This format appears immediately following the dotted decimal IP address using a /N format.

For example, the same IP address and subnetwork mask mentioned above would appear as follows using /N format: 192.168.100.1/24

A network mask is used to separate the network information from the host information about an IP address. Figure below shows the network mask 255.0.0.0 applied to network 10.0.0.0. The mask in binary notation is a series of 1s followed by a series of contiguous 0s. The 1s represent the network number; the 0s represent the host number. The sample address splits the IP address 10.0.0.1 into a network portion of 10 and a host portion of 0.0.1.

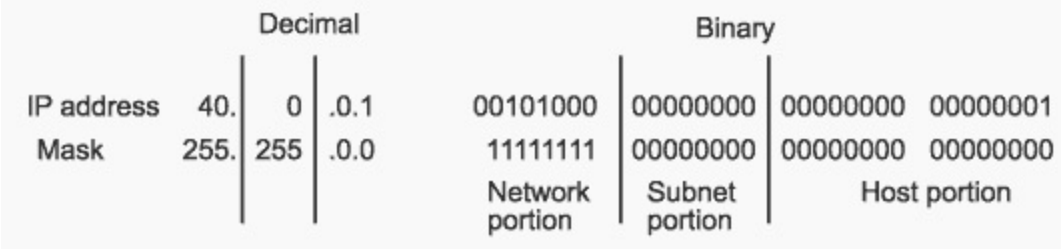
	Decimal		Binary			
IP address	40.	0.0.1	00101000	00000000	00000000	00000001
Mask	255.	0.0.0	11111111	00000000	00000000	00000000
			Network portion	Host portion		

Classes A, B, and C have the following natural masks, which define the network and host portions of each class:

Class A natural mask 255.0.0.
Class B natural mask 255.255.0.0
Class C natural mask 255.255.255.0

The use of masks can divide networks into subnetworks by extending the network portion of the address into the host portion. Subnetting increases the number of subnetworks and reduces the number of hosts.

For example, a network of the form 10.0.0.0 accommodates one physical segment with about 16 million hosts on it. Below figure shows how the mask 255.255.0.0. is applied to network 10.0.0.0. The mask divides the IP address 10.0.0.1 into a network portion of 10, a subnet portion of 0, and a host portion of 0.1. The mask has borrowed a portion of the host space and has applied it to the network space. The network space of the class 10 has increased from a single network 10.0.0.0 to 256 subnetworks, ranging from 10.0.0.0 to 10.255.0.0. This process decreases the number of hosts per subnet from 16,777,216 to 65,536.



Classless Addressing with CIDR

CIDR is a system of addressing that improves the scaling factor of routing in the Internet. CIDR does not use an implicit mask based on the class of network. In CIDR, an IP network is represented by a prefix, which is an IP address and an indication of the leftmost contiguous significant bits within this address.

For example, without CIDR, the class C network address 192.56.0.0 would be an illegal address. With CIDR, the address becomes valid with the notation: 192.56.0.0/16. The /16 indicates that 16 bits of mask are being used (counting from the far left). This would be similar to an address 198.32.0.0. with a mask of 255.255.0.0.

A network is called a supernet when the prefix boundary contains fewer bits than the network's natural mask. For example, a class C network 192.56.10.0 has a natural mask of 255.255.255.0. The representation 192.56.0.0/16 has a shorter mask than the natural mask (16 is less than 24), so it is a supernet. Network Mask is a 32bit value that identifies the network to which an IP address belongs.

The CIDR Value table is as shown below:

Subnet Mask	CIDR value
255.255.0.0	/16
255.255.128.0	/17

255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23

Important points to note:

1. A subnet mask is used to determine the break between network and host subsections of an IP addressing

2. VLSM allows for conservation of address space by allowing the subnet mask to allocate bits across the entire range of the IP address

3. An address where all the host bits are set to 1 is the broadcast

4. An address where all the host bits are set to 0 is the network

5. There are 2^n-2 addresses in a CIDR block, where n is the number of host bits

IPv6 addressing: IP version 6 (IPv6) increases the size of the IP address from the 32 bits found in IPv4 to 128 bits. This increased size provides for a broader range of addressing hierarchies and a much larger number of addressable nodes.

IPv6 addresses consist of eight hexadecimal groups. Each hexadecimal group, separated by a colon (:), consists of a 16-bit hexadecimal value.

The following is an example of the IPv6 format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

A group of xxxx represents the 16-bit hexadecimal value. Each individual x represents a 4-bit hexadecimal value.

The following is an example of a possible IPv6 address:
4FDE:0000:0000:0002:0022:F376:FF3B:AB3F

Comparison between IPv4 and IPv6 addressing

IPv4	IPv6

32-bit (4 byte) address supporting 4,294,967,296 address (although many were lost to special purposes, like 10.0.0.0 and 127.0.0.0)	128-bit (16 byte) address supporting 228 (about 3.4 x 1038) addresses
NAT can be used to extend address limitations	No NAT support (by design)
IP addresses assigned to hosts by DHCP or static configuration	IP addresses self-assigned to hosts with stateless address auto-configuration or DHCPv6

IPv4 and IPv6 addressing concepts:

IPv4	IPv6
Mulitcast address space at 224.0.0.0/4	Multicast address space at FF00::/8
Has broadcast addresses for all devices	No such concept in IPv6 (uses multicast groups)
Uses 0.0.0.0 as unspecified address	Uses :: as unspecified address
Uses 127.0.0.1 as loopback address	Uses ::1 as loopback address
Supports globally unique "public" addresses	Supports globally unique unicast addresses
Uses 10.0.0.0/8, 172.16.0.0/16, and 192.168.0.0/16 as "private" addresses	Uses FD00::/8 as unique local addresses

Figure below compare the header of a IPv4 packet and an IPv6 packet

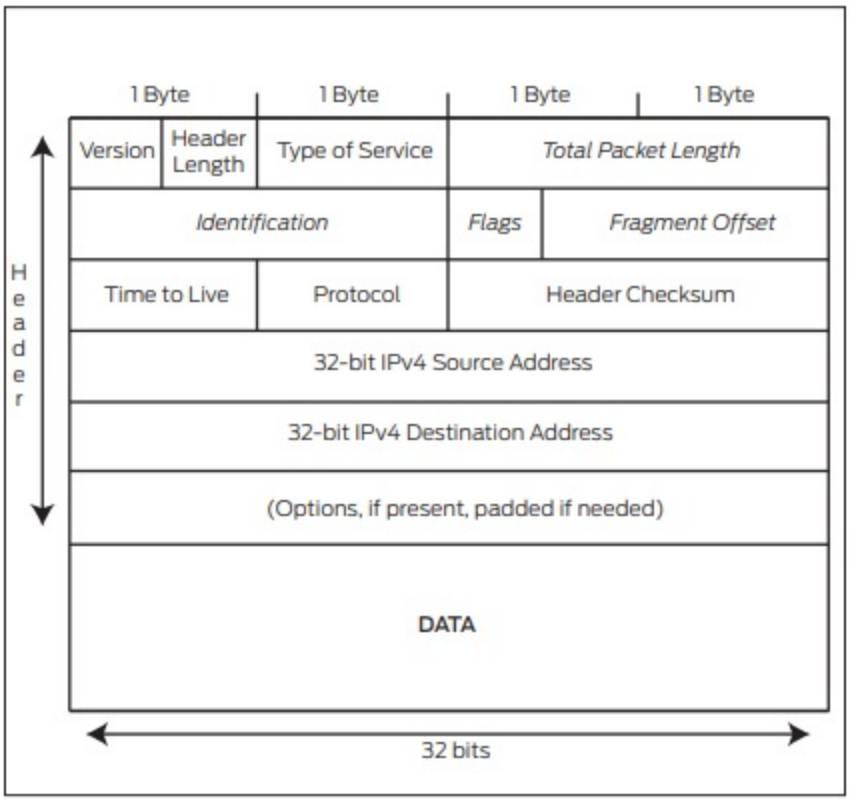


Fig: IPv4 Header

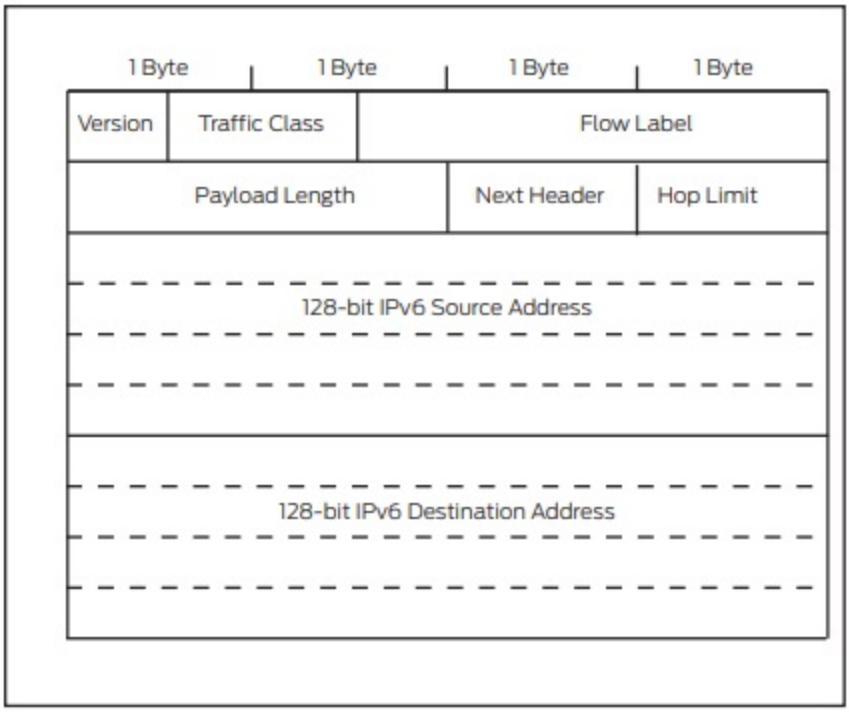


Fig: IPv6 header

IPv6 packets have their own frame Ethertype value, 0x86dd, making it easy for receivers that must handle both IPv4 and IPv6 to distinguish the frame content on the same interface. The IPv6 header is comprised of the following fields:

- Version: A four-bit field for the IP version number (0x06).
- Traffic Class: An 8-bit field that identifies the major class of the packet content (for example, voice or video packets). The default value is 0, meaning it is ordinary bulk data (such as FTP) and requires no special handling.
- Flow Label: A 20-bit field used to label packets belonging to the same flow (those with the same values in several TCP/IP header parameters). The flow label is normally 0 (flows are detected in other ways).
- Payload Length: A 16-bit field giving the length of the packet in bytes, excluding the IPv6 header.
- Next Header: An 8-bit field giving the type of header immediately following the IPv6 header (this serves the same function as the Protocol field in IPv4).
- Hop Limit: An 8-bit field set by the source host and decremented by 1 at each router. Packets are discarded if Hop Limit is decremented to zero (this replaces the IPv4 Time To Live field). Generally, implementers choose the default to use, but values such as 64 or 128 are common.

IPv6 Host Addressing: IPv4 hosts are fairly easy to configure: usually, the network interface has one IPv4 address. When coupled with the default router - if there is a way off the subnet- the host has everything it needs to decide where things go. But IPv6 does much more. In contrast to IPv4 hosts, IPv6 hosts (end devices) normally have multiple addresses on each interface. But these multiple addresses greatly simplify the operation of the IPv6 network layer (finding network neighbors, routers, and so on).

Unicast addresses

- Link-local address on each interface (Unique Local Addresses, ULA, beginning with FE00::/7 can use www.sixxs.net/tools/grh/ula/ to generate and register site local prefixes based on RFC 4193)
- Additional unicast addresses for each interface, which can be multiple global addresses or unique local addresses
- Loopback address (::1)

Multicast addresses

- FF01::1 - The interface-local scope all-nodes multicast address
- FF02::1 - The link-local scope all-nodes multicast address
- The solicited-node address for each assigned unicast address
- The multicast addresses of any groups the host has joined

All IPv6 router interfaces also listen for traffic on the following multicast addresses:

- FF01::1 - The interface-local scope all-nodes multicast address
- FF01::2 - The interface-local scope all-routers multicast address
- FF02::1 - The link-local scope all-nodes multicast address
- FF02::2 - The link-local scope all-routers multicast address
- FF05::2 - The site-local scope all-routers multicast address
- The solicited-node address for each assigned unicast address
- The multicast addresses of any groups the router has joined

What is Reverse Path Forwarding and why it is required: To protect against IP spoofing, and some types of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, Unicast Reverse-path Forwarding (RPF) verifies that packets are arriving from a legitimate path. It does this by checking the source address of each packet that arrives on an untrusted ingress interface and, comparing it to the forwarding-table entry for its source address.

Unicast RPF is supported for the IPv4 and IPv6 protocol families. There are two modes of unicast RPF, strict mode, and loose mode.

The default is strict mode, which means the switch forwards a packet only if the receiving interface is the best return path to the packet's unicast source address. Strict mode is useful in identifying untrusted interfaces and sending packets via the best route.

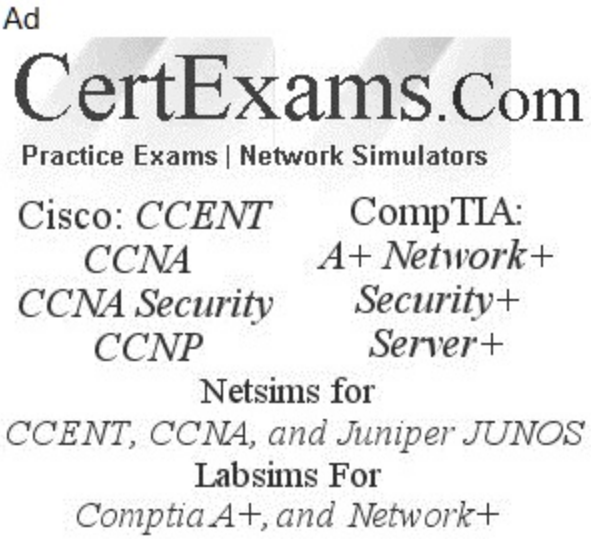
The other mode is loose mode, which means the system checks to see if the packet has a source address with a corresponding prefix in the routing table, but it does not check whether the receiving interface is the best return path to the packet's unicast source address.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Binary Numbers To Decimal Number Conversion And Vice Versa

examguides.com/Juniper-JNCIA/juniper-jncia-7.htm

Ad



1. Networking Fundamentals

1.7 Binary Numbers to Decimal Number Conversion and Vice Versa

Decimal is a Base 10 system with 10 possible values (0 to 9) and Binary is a Base 2 system with only two numbers 0 or 1.

i. Converting binary to decimal - The weightage of binary digits from right most bit position to the left most bit position is given below.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Example: Convert 10011101 into a decimal value.

There are eight bits in the binary number. The decimal value for each bit position is given below:

128	64	32	16	8	4	2	1	« Decimal equivalent of the binary position
1	0	0	1	1	1	0	1	« Given binary number

To convert, you simply take a value from the top row wherever there is a 1 below, and then add the values together. For instance, in our example we would have

$1*2^7 + 0*2^6 + 0*2^5 + 1*2^4 + 1*2^3 + 1*2^2 + 0*2^1 + 1*2^0$
= 128 + 0 + 0 + 16 + 8 + 4 + 0+ 1
= 157 (decimal value)

ii. Converting decimal to binary

To convert decimal to binary is also very simple, you simply divide the decimal value by 2 and then write down the remainder, repeat this process until you cannot divide by 2 anymore.

For example, take the decimal value 157:

157 ÷ 2 = 78 with a remainder of 1
78 ÷ 2 = 39 with a remainder of 0
39 ÷ 2 = 19 with a remainder of 1
19 ÷ 2 = 9 with a remainder of 1
9 ÷ 2 = 4 with a remainder of 1
4 ÷ 2 = 2 with a remainder of 0
2 ÷ 2 = 1 with a remainder of 0
1 ÷ 2 = 0 with a remainder of 1 <--- to convert, write this remainder first

Next write down the value of the remainders from bottom to top (in other words write down the bottom remainder first and work your way up the list) which gives: 10011101 = 157

Example: What is the possible decimal equivalent of 10101010?

Position of Bit	7^{th}	6^{th}	5^{th}	4^{th}	3^{rd}	2^{nd}	1^{st}	0^{th}
Decimal Value	128	64	32	16	8	4	2	1

Calculate the decimal equivalent based on the above predefined values.

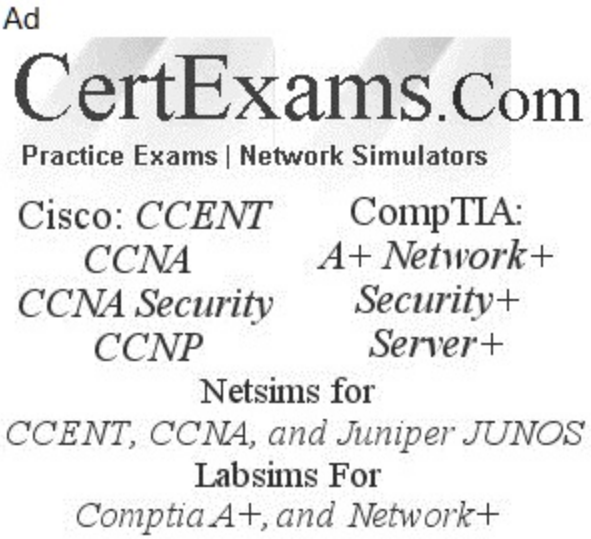
Given Binary Number is: 10101010, it's decimal equivalent is:

1*(2^7) + 0*(2^6) + 1*(2^5) + 0*(2^4) + 1*(2^3) + 0*(2^2) + 1*(2^1) + 0*(2^0)=170 in decimal format.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes :Longest Match Routing

examguides.com/Juniper-JNCIA/juniper-jncia-8.htm

Ad


1. Networking Fundamentals

1.8 Longest match routing

Specify the static route on the device to resolve and determine the packet's next-hop interface using the Longest Match Routing Rule (most specific entry), sometimes referred to as the longest prefix match or maximum prefix length match. The Longest Match Routing Rule is an algorithm used by IP routers to select an entry from a routing table. The router uses the longest (prefix) match to determine the egress (outbound) interface and the address of the next device to which to send a packet. Typically, the static route prefers the directly connected subnet route for resolving the next hop rather than performing a longest prefix match with any other available routes.

The router implements the Longest Match Routing Rule as follows:

- The router receives a packet.
- While processing the header, the router compares the destination IP address, bit-by-bit, with the entries in the routing table.
- The entry that has the longest number of network bits that match the IP destination address is always the best match (or best path) as shown in the below example.

Longest Match Example:

The router receives a packet with a destination IP address of 192.168.1.33.

The routing table contains the following possible matches:

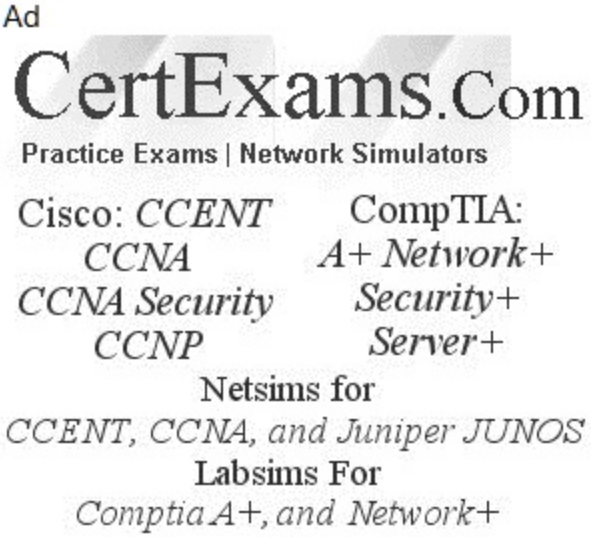
192.168.1.32/28 ,192.168.1.0/24,192.168.0.0/16

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Connection Oriented And Connectionless Protocols

examguides.com/Juniper-JNCIA/juniper-jncia-9.htm

Ad



1. Networking Fundamentals

1.9 Connection Oriented and Connectionless protocols

Connection oriented Protocols:

1. It guarantees transmitted data will reach its destination

2. It sequences the packets such that the packets are received in a sequenced manner at the destination.

3. TCP/IP is an example of connection oriented protocol.

Connectionless protocols:

1. Connectionless protocols do not guarantee packet delivery.

2. The advantage is less over-head.

3. UDP/IP is an example of connectionless protocol.

TCP/IP is a suite of data communications protocols. Two of the more important protocols in the suite are the TCP and the IP. The full form of TCP/IP is Transmission Control Protocol/Internet Protocol. A suite of protocols for communication between computers and specifying standards for transmitting data over networks.

IP provides the basic packet delivery service for all TCP/IP networks. IP is a connectionless protocol, which means that it does not exchange control information to establish an end-to-end connection before transmitting data. A connection-oriented protocol exchanges control information with the remote computer to verify that it is ready to receive data before sending it.

IP relies on protocols in other layers to establish the connection if connection-oriented services are required and to provide error detection and error recovery. IP is sometimes called an unreliable protocol, because it contains no error detection or recovery code.

TCP is a connection oriented protocol whereas UDP is connectionless protocol. 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. A detailed comparison of both TCP and UDP protocols is given below.

Two types of Internet Protocol (IP) are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is connection oriented and data can be sent bidirectional after establishment of a connection. UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.

Suitability	TCP is suited for applications that require high reliability, and not very critical of transmission delays.	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.
Use by protocols	HTTP, HTTPs, FTP, SMTP, Telnet	DNS, DHCP, TFTP, SNMP, RIP, VOIP.
Ordering of data packets	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed and reliability	The speed for TCP is slower than UDP. When using TCP, any missing packets are retransmitted. TCP guarantees packet delivery and hence more reliable.	UDP is faster because error recovery is not attempted. It is a "best effort" protocol. There is no guarantee that a packet is received at the destination and hence less reliable than TCP.
Header Size	TCP header size is 20 bytes	UDP Header size is 8 bytes.

Common Header Fields	Source port, Destination port, Check Sum	Source port, Destination port, Check Sum
Streaming of data	Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.	Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent.
Connection Setup	TCP requires three packets to set up a socket connection, before any user data can be sent.	UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.
Data Flow Control	TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP does not have an option for flow control
Error Checking	TCP does error checking and error recovery. Erroneous packets are retransmitted from the source to the destination.	UDP does error checking but simply discards erroneous packets. Error recovery is not attempted.
Fields	1. Sequence Number, 2. AcK number, 3. Data offset, 4. Reserved, 5. Control bit, 6. Window, 7. Urgent Pointer 8. Options, 9. Padding, 10. Check Sum, 11. Source port, 12. Destination port	1. Length, 2. Source port, 3. Destination port, 4. Check Sum
Acknowledgement	Acknowledgement segments	No Acknowledgment
Handshake	SYN, SYN-ACK, ACK	No handshake (connectionless protocol)

UDP is sometimes referred to as "send and pray" because there is no reliable delivery mechanism inherent in UDP. TCP is known as a reliable protocol.

IP Packets: A packet is a block of data that carries with it the information necessary to deliver it to a destination address. A packet-switching network uses the addressing information in the packets to switch packets from one physical network to another, moving

them toward their final destination. Each packet travels the network independently of any other packet. The datagram is the packet format defined by IP.

IP Functions: Some of the functions IP performs include:

- Moving Data Between the Network Access Layer and the Host-to-Host Transport Layer
- Routing Datagrams to Remote Hosts
- Fragmenting and Reassembling Datagrams

Moving Data Between the Network Access Layer and the Host-to-Host Transport Layer : When IP receives a datagram that is addressed to the local host, it must pass the data portion of the datagram to the correct host-to-host transport layer protocol. IP uses the protocol number in the datagram header to select the transport layer protocol. Each host-to-host transport layer protocol has a unique protocol number that identifies it to IP.

Routing Datagrams to Remote Hosts: Internet gateways are commonly referred to as IP routers because they use IP to route packets between networks. In traditional TCP/IP terms, there are only two types of network devices: gateways and hosts. Gateways forward packets between networks, and hosts do not. However, if a host is connected to more than one network (called a multi-homed host), it can forward packets between the networks. When a multi-homed host forwards packets, it acts like any other gateway and is considered to be a gateway.

Fragmenting and Reassembling Datagrams: As a datagram is routed through different networks, it may be necessary for the IP module in a gateway to divide the datagram into smaller pieces. A datagram received from one network may be too large to be transmitted in a single packet on a different network. This condition occurs only when a gateway interconnects dissimilar physical networks.

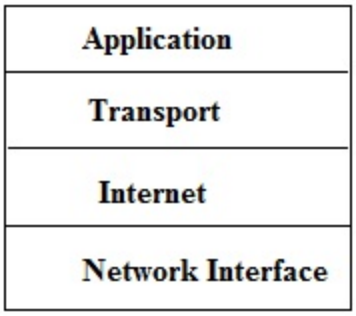
Each type of network has a maximum transmission unit (MTU) that determines the largest packet it can transfer. If the datagram received from one network is longer than the other network's MTU, it is necessary to divide the datagram into smaller fragments for transmission in a process called fragmentation.

IP Layering: TCP/IP is organized into four conceptual layers (as shown in Figure 1). Below fig shows TCP/IP Conceptual Layers

TCP/IP Conceptual Layers

Network Interface Layer: The network interface layer is the lowest level of the TCP/IP protocol stack. It is responsible for transmitting datagrams over the physical medium to their final destinations.

Internet Layer: The Internet layer is the second level of the TCP/IP protocol stack. It provides host-to-host communication. In this layer, packets are encapsulated into datagrams, routing algorithms are run, and the datagram is passed to the network interface layer for transmission on the attached network.



Transport Layer: The transport layer is the third level of the TCP/IP protocol stack. It is responsible for providing communication between applications residing in different hosts. By placing identifying information in the datagram (such as socket information), the transport layer enables process-to-process communication. The transport layer provides either a reliable transport service (TCP) or an unreliable service (User Data Protocol). In a reliable delivery service, the destination station acknowledges the receipt of a datagram.

Application Layer: The application layer is the fourth and highest level of the TCP/IP protocol stack. Some applications that run in this layer are: Telnet,FTP,SMTP,Simple Network Management Protocol (SNMP),Domain Name System (DNS)

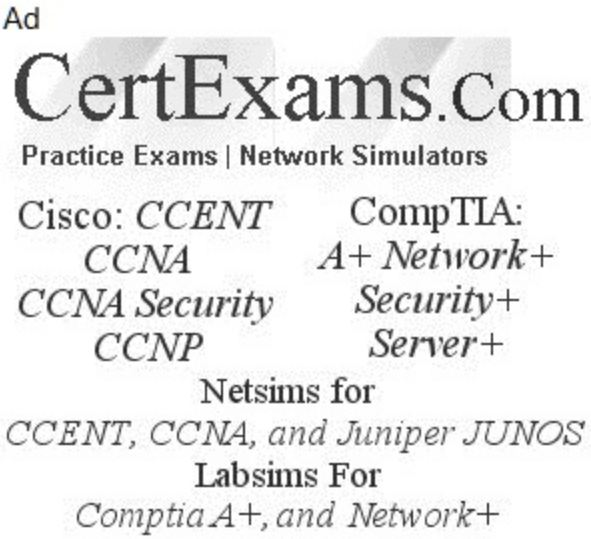
Transmission Control Protocol(TCP) and User Datagram Protocol (UDP) operate at the Transport Layer. IP operates at Network Layer whereas FTP operates at the Application Layer

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Junos Device Portfolio

examguides.com/Juniper-JNCIA/juniper-jncia-10.htm

Ad



2. Junos OS Fundamentals

2.1 Junos Device portfolio

The operating system software that powers the Juniper routers is called JUNOS. The software is modular and standards based. Another important feature of JUNOS is that the software is platform independent (within Juniper hardware systems, not to be confused with other vendor hardware), thus delivering the same scalability and security across several hardware platforms.

JTAC refers to Juniper Networks Technical Assistance Center. JTAC is the recommendation body of Juniper Networks that provides suitable guidelines for Juniper devices.

Main products offered by Juniper include T-Series, M-Series, E-Series, MX-Series, J-Series routers, EX-Series Ethernet switches and SRX-Series Security products. JUNOS is the operating system that runs on most of the juniper's networking equipment.

M-Series: M7i, M10i, M40e, M120, M320

J-Series: J2320, J2350, J4350, J6350

T-Series: T320, T640, T1600, TX Matrix, TX Matrix Plus

E-Series: E120, E320, ERX310, ERX705, ERX710, ERX1410, ERX1440

MX-Series: MX80, MX240, MX480, MX960

Differences between different series of juniper routers are

1. Juniper J-Series routers are a series of enterprise routers called as modular routers for enterprises running desktops, servers, VoIP etc applications and these kind of routers are typically deployed at remote offices or branch locations.

2. Juniper M-Series routers are called Multiservice Edge routers designed for enterprise and service provider networks.

3. Juniper T-Series routers are a series of core routers designed for high-end and core networks with throughput from 320 Gbit/s to 25.6 Tbit/s with a max forwarding rate of 30.7 billion pps.

4. Juniper E-Series routers are a series of broadband services routers or edge routers which provides multiple services including broadband remote access server, broadband video services, security services, NAT etc on a single platform.

5. Juniper MX-Series routers are a family of high-performance Ethernet Services routers with powerful switching features and are designed for high-performance service providers and enterprises.

Juniper switches are available in two series

a. EX Series Ethernet Switches : Deliver high performance, carrier-class solutions built to meet the needs of today's converged branch office, campus, and data center networks.

b. QFX Series : High-performance devices deliver Juniper's unique QFabric architecture, supporting thousands of ports within a single-tier data center or cloud network with ultra-low latency, high resiliency, and the simplicity of a single switch.

Control and Forwarding plane: On juniper router, there is a separation of control and forwarding planes. Control plane is where the OS of the device resides. Control plane also maintains the routing table and the best route to reach a particular destination. Control plane then forwards the best path to the forwarding plane. Then, the forwarding plane forwards the data to the destination. Forwarding Plane enhances the performance using ASICs whereas the intelligence of the router operates in Forwarding Plane. The forwarding plane of the router is divided into multiple segments thus controlled by application specific integrated circuits (ASICs). When the interactions between these ASICs take place, the forwarding path is achieved in Juniper routers.

On Juniper Networks routers, the PFE is designed to perform Layer 2 and Layer 3 switching, route lookups, and rapid forwarding of packets. Using ASICs, the PFE itself is split into several major components:

- Midplane
- PICs
- FPCs (Flexible PIC Concentrator)
- Control board (switching/forwarding)

The midplane, sometimes referred to as the backplane, is really the back of the cage that holds the line cards. The line cards connect into the midplane when inserted into the chassis from the front. The routing engine plugs into the rear of the midplane from the rear of the chassis. The purpose of the midplane is to carry the electrical signals and power to each line card and to the routing engine.

The PICs are the actual components that contain the interface ports. Each PIC is plugged into a FPC, Each individual PIC contains an ASIC that handles media-specific functions, such as framing or encapsulation, and has its own LED status indicator on the front. PICs are available for SDH/SONET, ATM, Gigabit Ethernet, Fast Ethernet, and DS3/E3.

The physical media in your network connects to the Physical Interface Card (PIC) in your router. The number of PICs supported by an FPC depends on the device model. A media-specific ASIC is located on each PIC.

The FPC can contain from one to four PICs in a mix-and-match style. In other words, you could have four different kinds of PICs on a single FPC. This reflects a great deal of flexibility that is welcome in most networks. Installed from the front of the chassis, the FPC carries the signals from the PICs to the midplane. Each FPC has its own input-output (I/O) ASIC and buffer memory. The Flexible PIC Concentrator(FPC) connects to both the switching control board and the router's interfaces within the Packet Forwarding Engine. The FPC is a component of the Packet Forwarding Engine. FPCs house the various PICs used in the router.

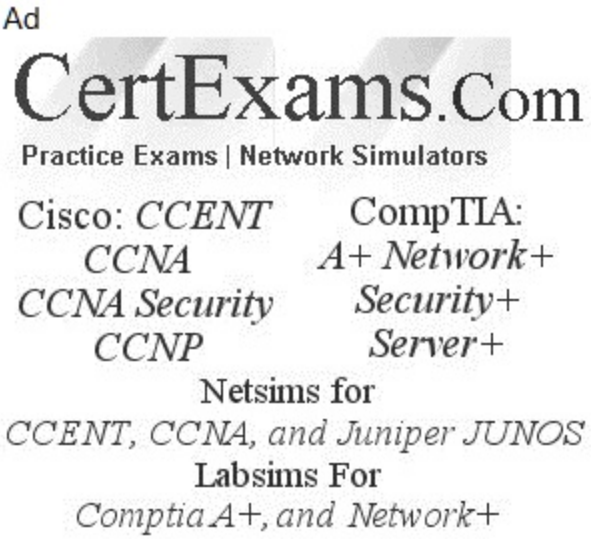
As the organizations increasingly move towards cloud based services, vSRX and vMX Virtual devices provide scalable, secure protection across private, public, and hybrid clouds.

For example, the vSRX offers the same features as physical SRX Series firewalls but in a virtualized form factor for delivering security services that scale to match network demand.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : junos Software Architecture

examguides.com/Juniper-JNCIA/juniper-jncia-11.htm

Ad


2. Junos OS Fundamentals

2.2 Software Architecture

The jdocs package contains the complete JUNOS software documentation set. Jbundle is a single file which contains all the packages.

The removable media is the first boot location examined. Solid-State Drive is the second boot examined after removable media.

It takes about 5 minutes to completely boot the junos device. Enough time must be given to boot the Juniper devices in compared to other devices.

The solid-state flash drive is the primary boot media used to boot the juniper devices. Besides this, the secondary boot media is the Hard Drive.

Junos software updates are contained in four packages. Among the above, jroute and jdocs are two update packages. Along with this, the other two are jpfe and jkernel.

We can actually backup a software and configuration to rotating disk on junos devices. This backup functionality is best used when system is stable and before any major upgrade to ensure system recovery when necessary.

We use 'request system snapshot' command in our operational mode to backup a system software and configuration so that it might come handy during the time of recovery.

In case, if we want two juniper devices working as a single stack with primary and backup routing engine then the software version of both juniper devices must be same. Otherwise our redundancy process may not work properly.

In JUNOS software, every interface requires at least one logical interface. That logical interface is known as unit. This is where all addressing and protocol information is configured

Action modifiers are log, count and sample. Along with this there is also another action modifier and it is syslog. We can include any combination of action modifiers in a single filter term.

In the default syslog configuration on the Junos router, logs are saved to a file called messages, which resides in the default log file directory. On M-, MX-, and T-series routers, the default log file directory is /var/log/. On J-series routers, it is /cf/var/log/. To view the log messages, give the command show log messages.

If you want to get a live monitoring while looking at your console, you can use the monitor start command. As soon as a message is written to your monitored file, it will additionally be redirected to the console and shown live.

Package is referred to each section of the software. The jbase, jbundle and jroute are the packages found in each copy of the Junos Software.

Package and Type are the JUNOS software naming conventions. Package represents the specific portion of the JUNOS software contained in the file. There are five junos software naming convention. All packages may include the signed notation. This means that the package file is protected using the MD5 algorithm.

The JUNOS software is actually made up of multiple pieces working together to control the router's functions. Each section of the software is referred to as a package and contains files specific to its particular function. The current packages found in each copy of the JUNOS software are:

jkernel The jkernel package contains the basic components of the JUNOS software operating system.

jbase The jbase package contains additions to the JUNOS software since the last revision of the jkernel package.

jroute The jroute package contains the software that operates on the Routing Engine. This controls the Unicast routing protocols, the multicast routing protocols, and the Multiprotocol Label Switching (MPLS) signaling protocols. The package also contains the software for some daemons, such as mgd.

Jpfe: The jpfe package contains the Embedded OS software that controls the components of the Packet Forwarding Engine.

Jdocs: The jdocs package contains the complete JUNOS software documentation set.

Jcrypto: The jcrypto package contains software that controls various security functions, such as IP Security (IPSec) and Secure Shell (SSH). This package is available only in U.S. and Canadian versions of the software.

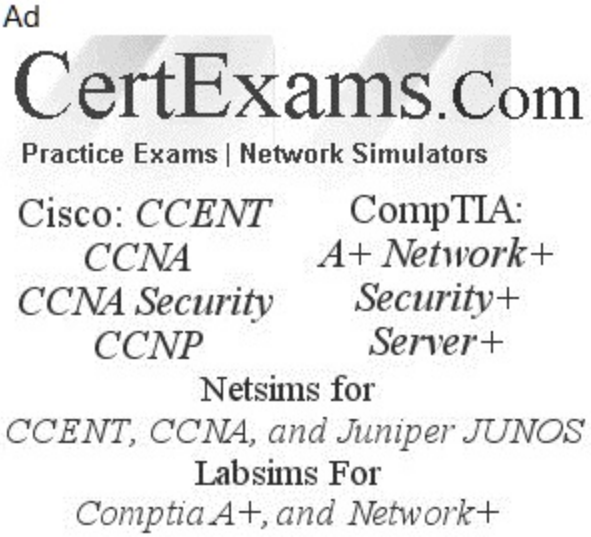
Jbundle: The jbundle package is a single file that contains all of the other packages we discussed previously.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Routing Engine And Packet Forwarding Engine

examguides.com/Juniper-JNCIA/juniper-jncia-12.htm

Ad



2. Junos OS Fundamentals

2.3 Routing Engine and Packet Forwarding Engine

The Routing Engine is the central location for control of the system in a juniper networks router and it consists of an Intel-based PCI platform running JUNOS software. The Routing Engine constructs and maintains one or more routing tables. From the routing tables, the Routing Engine derives a table of active routes, called the forwarding table, which is then copied into the Packet Forwarding Engine.

Functions of the routing engine include the following

- Handling of routing protocol packets
- Management Interface
- Configuration Management
- Accounting and alarms
- Modular Software
- Scalability

The Packet Forwarding Engine is the central location for data packet forwarding through the router.

- Switching control board.

- Flexible PIC Concentrator, and
- Physical Interface Card

The packet forwarding engine uses four ASICs:

- The Internet Processor ASIC
- The I/O Manager ASIC
- The PIC I/O Manager ASIC
- The Distributed Buffer Manager ASICs.

The software upgrades and the maintenance are performed on the Routing Engine. Routing Engine is the central location that controls the system. It is often referred as the intelligence of the router.

Routing Engine is the place where the entire JUNOS software resides. It is the logical location where software is stored. Routing Protocols and routing tables are also stored in this engine.

Routing Engine 2 is found in the M-Series routers of Juniper Networks. It contains the 333MHz processor and 768MB of Random Access Memory(RAM). M-Series is the first series of router introduced by the Juniper Networks.

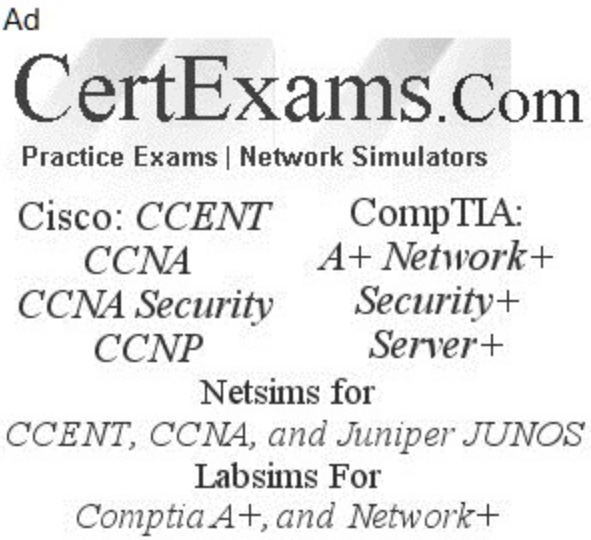
The main components of the Packet Forwarding Engine in the juniper devices are the Physical Interface card(PIC), the Flexible PIC Concentrator(FPC) and a switching control board. All these components consist of the ASICs designed by Juniper Networks.

The Routing Engine in a Juniper Networks router is the central location for control of the system. This is where the intelligence of the router operates. You can perform software upgrades and maintenance on the Routing Engine. In addition, you can interface with the Routing Engine for monitoring and configuring the router. Each Routing Engine is based on an Intel PCI motherboard. The actual components of each Routing Engine depend on the model you are using and include the following:

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Protocol Daemons

examguides.com/Juniper-JNCIA/juniper-jncia-13.htm

Ad


2. Junos OS Fundamentals

2.4 Protocol daemons

The actual functions of the router are controlled by the daemon. Each daemon operates in its own protected memory space, which is also controlled by the kernel.

The Management Daemon process controls all user access to the router. For example, the user's CLI is a client of mgd. The Chassis Daemon process controls the properties of the router itself, including the interaction of the passive midplane, the FPCs, and the control boards.

The Management Daemon process controls all user access to the router.

For example, the user's CLI is a client of mgd.

The router's interfaces are configured and maintained by the Device Control Daemon.

Exception Traffic: Packets addressed to the router, such as ICMP pings, Telnet, and SSH traffic are the exceptional packet.

By default, the firmware file will be copied to the /var/sw/pkg/ directory on internal storage upon software installation. With the no-copy option, the firmware file will not be copied to internal storage.

best-effort-load: Activate a partial load and treat parsing errors as warnings instead of errors.

no-copy: Install the software package but does not saves the copies of package files.

no-validate: Do not check the compatibility with current configuration before installation starts.

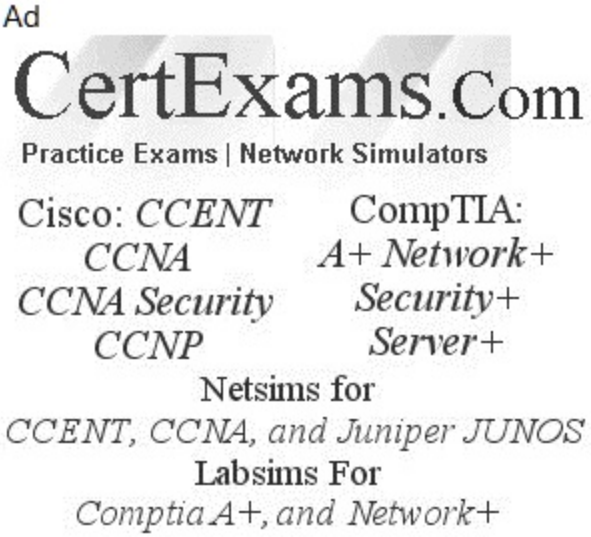
unlink: Remove the software package after successful installation.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Concepts, Operation And Functionality Of The Junos User Interfaces

examguides.com/Juniper-JNCIA/juniper-jncia-14.htm

Ad



3. User Interfaces

3.1 Concepts, operation and functionality of the Junos user interfaces

CLI Functionality: JUNOS CLI is a simple to use, text-based command interface. We give various commands on CLI for configuring, troubleshooting and monitoring the software.

JUNOS primarily supports two types of command modes.

a) Operational Mode: When we log in to the router and the CLI starts, we are at the top level of the CLI operational mode. In this mode, we enter the commands for

1. Controlling the CLI environment, and

2. Monitor and troubleshoot network connectivity, and

3. Initiating the Configuration Mode.

Frequently used commands in this mode include ping, show, traceroute, configure, etc.

Operational mode is indicated by the > prompt-for

example, **user@switch>**

b) Configuration Mode: We use the Configuration mode for configuring the JUNOS software by creating a hierarchy of configuration statements. We enter the configuration mo9+de by using the command "configure" as shown below:

user@host>configure
Entering configuration mode
[edit]
user@host#

Issuing the commands one at a time using CLI can configure a JUNOS™ router or alternately, we can configure by creating a text (ASCII) file that contains the statement hierarchy. Remember to activate the configuration by using the command "commit" on the router.

As shown in the above example, the generic configuration prompt is user@host#. Ofcourse, we can change the prompt by using appropriate command.

Statement Hierarchy: We use the above configuration mode commands to create a statement hierarchy, and then configure the JUNOS software. The term "statement hierarchy" is used to define the sequence of commands used for configuring a particular feature (or features) of the router. An example statement hierarchy is given below:

user@host>configure

----Top level
user@host#edit protocols ospf
[edit protocols ospf] ----protocols ospf hierarchy level
user@host#

"set" commands are used to configure specific leaf statements.

Ex: **user@host#**set hello-interval 14

The command 'set system services web-management' allows us to access our juniper device based on Graphical User Interface (GUI). We can either enable http based and https based web-management on Juniper devices.

CLI Help: The CLI includes several ways to get help about commands. Some examples of how to get help are as below

1. Type ? to show the top-level commands available in operational mode.

root@> ?

Possible completions:

clear - Clear information in the system
configure - Manipulate software configuration information
diagnose - Invoke diagnose script
file - Perform file operations
help - Provide help information monitor
Show - real-time debugging information
mtrace - Trace multicast path from source to receiver
ping - Ping remote target
quit - Exit the management session
request - Make system-level requests
restart - Restart software process
set - Set CLI properties, date/time, craft interface message
show - Show system information
ssh - Start secure shell on another host
start - Start shell
telnet - Telnet to another host
test - Perform diagnostic debugging
traceroute - Trace route to remote host

2. Type file ? to show all possible completions for the file command.

root@> file ?

Possible completions:

<[Enter]> Execute this command

archive - Archives files from the system
checksum - Calculate file checksum
compare - Compare files
copy - Copy files (local or remote)
delete - Delete files from the system
list - List file information
rename - Rename files
show - Show file contents source-address Local address to use in originating the connection
| - Pipe through a command

3. Type file archive ? to show all possible completions for the file archive command.

root@> file archive ?

Possible completions:

compress - Compresses the archived file using GNU gzip (.tgz)
destination - Name of created archive (URL, local, remote, or floppy)
source - Path of directory to archive

We use 'exit' command to move down into the operational mode hierarchy once we are in configuration mode hierarchy. In other vendor devices, it may be quit, undo, etc. command used to get out of a particular hierarchy.

Configure or edit command takes us from operational mode to the configuration mode hierarchy. Edit command is the hidden command which doesn't show in our operational mode hierarchy when we enter '?' symbol.

Filtering Output: The Junos OS enables you to filter command output by adding the pipe (|) symbol when you enter a command. For example

user@host>show rip neighbor ?

Possible completions:

<[Enter]> Execute this command
<name> Name of RIP neighbor
instance Name of RIP instance
logical-system Name of logical system, or 'all'
| Pipe through a command

The following example lists the filters that can be used with the pipe symbol (|):

user@host>show interfaces | ?

For the show configuration command only, an additional compare filter is available:

user@host> show configuration | ?

You can enter any of the pipe filters in conjunction. For example:

user@host>command | match regular-expression | save filename

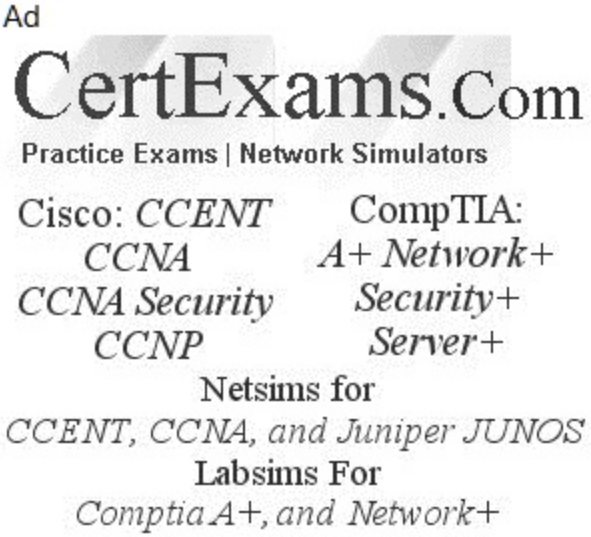
'Match' option prompts the router to display only lines in the output containing the text string we provide when used with pipe key. There are also other options used with pipe key. They are save, resolve, no-more, repeat, etc.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Active Vs. Candidate Configuration

examguides.com/Juniper-JNCIA/juniper-jncia-15.htm

Ad



3. User Interfaces

3.2 Active vs. candidate configuration

Active Configuration: In junos OS, the new configuration changes that we actually made can be compared with an active configuration that is currently running on our junos devices. In order to compare the candidate configuration with an active configuration, 'show | compare' command is used in the configuration mode on juniper device. After entering this command, The plus sign represents variables in the candidate configuration that are not present in the active configuration; we've added them to the file. Whereas, the minus sign shows that we've deleted variables from the file.

Candidate Configuration: We can view the candidate configuration that is present on our juniper device from configuration mode hierarchy. Candidate configuration allows us to make configuration changes without causing operational changes to the current operating configuration. In order to write the current candidate configuration to the permanent storage, we enter a save command along with the path to locate the candidate configuration. We use commit command on configuration mode hierarchy in order to activate candidate configuration. After we enter the commit command, candidate configuration becomes the active configuration.

"Configure private" allows us to enter into the private configuration mode where every user have their own private candidate configuration. Also, when a user commits, only the users own changes are commited.

Commit synchronize command is used when we have two routing engine and we need to apply the candidate configuration to both routing engine. This option is helpful in the event of a Routing Engine failure; the backup Routing Engine now has the latest operational parameters in the network.

Example:

The plus sign represents variables in the candidate configuration that are not present in the active configuration; we've added them to the file. Whereas, the minus sign shows that we've deleted variables from the file.

```
[edit]
user@router# show | compare
[edit system]
-   host-name router;
+   host-name Shiraz;
```

Commit Check: To verify that the syntax of a Junos configuration is correct, use the configuration mode commit check command:

Ex:

[edit]
user@host#commit check
configuration check succeeds
[edit]
user@host#

If the commit check command finds an error, a message indicates the location of the error.

Commit: To save Junos OS configuration changes to the configuration database and to activate the configuration on the device, use the commit configuration mode command. You can issue the commit command from any hierarchy level.

Ex:
[edit]
user@host#commit
commit complete
[edit]
user@host#

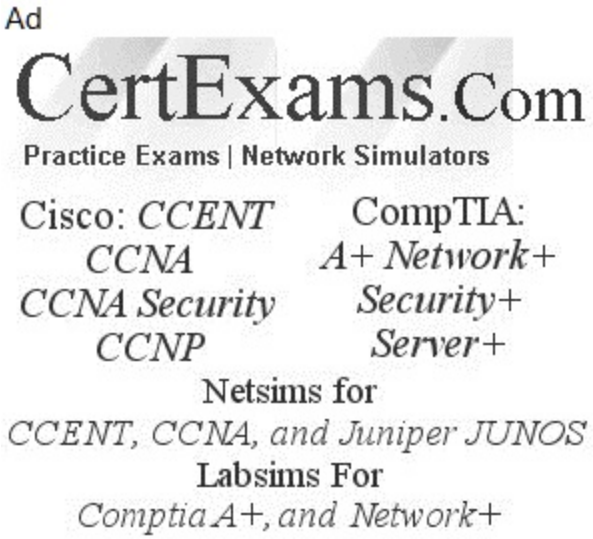
When you enter the commit command, the configuration is first checked for syntax errors (commit check). Then, if the syntax is correct, the configuration is activated and becomes the current, operational device configuration. The commit complete message tells us that the

process was successful.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : How to Go Back to a Previous Junos Configuration

examguides.com/Juniper-JNCIA/juniper-jncia-16.htm



3. User Interfaces

3.3 Reverting to Previous configurations

We can place the previously configured file in the candidate configuration with the rollback command. To return to a configuration prior to the most recently committed one, include the configuration number, 0 through 49, in the rollback command. The most recently saved configuration is number 0 (which is the default configuration to which the system returns), and the oldest saved configuration is number 49.

Example:

[edit]
user@host# rollback number
load complete

The 'show | compare rollback' command allows us to compare our current configuration with the rollback configuration that we want. This command is used in configuration mode hierarchy.

We use 'rollback 1' command on our configuration mode hierarchy in order to load the previous configuration on our juniper device. This is a kind of life savior command which enables us to get back to our previous configuration.

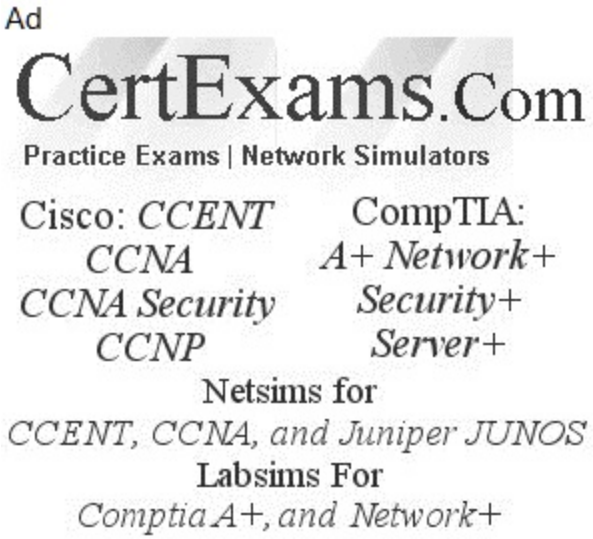
Command "show | compare" is used in junos device to compare the candidate configuration with the active configuration. Differences between the two files are displayed with either a plus (+) or a minus (-) sign.

The plus sign represents variables in the candidate configuration that are not present in the active configuration; that you've added them to the file.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Modifying, Managing, And Saving Configuration Files

examguides.com/Juniper-JNCIA/juniper-jncia-17.htm



3. User Interfaces

3.4 Modifying, managing, and saving configuration files

In order to write the current candidate configuration to the permanent storage, we enter a save command along with the path to locate the candidate configuration.

Ex:

[edit]
user@host#save filename
[edit]
user@host#

The contents of the current level of the statement hierarchy (and below) are saved, along with the statement hierarchy containing it. This allows a section of the configuration to be saved, while fully specifying the statement hierarchy. By default, the configuration is saved to a file in your home directory, which is on the flash drive. The load command helps us to restore files to the candidate configuration.

/var/home directory is located on the router's hard drive. It contains a subdirectory for each configured user on the router. These individual user directories are the default file location for many JUNOS software commands.

Viewing, comparing, and loading configuration files: You can create a file containing configuration data for a device running Junos OS, copy the file to the local router, and then load the file into the CLI. After you have loaded the file, you can commit it to activate the configuration on the router, or you can edit the configuration interactively using the CLI and commit it at a later time.

You can also create a configuration while typing at the terminal and then load it. Loading a configuration from the terminal is generally useful when you are cutting existing portions of the configuration and pasting them elsewhere in the configuration.

Ex:

[edit]
user@host# load (factory-default | merge | override | patch | replace | set | update) filename *<relative> <json>*

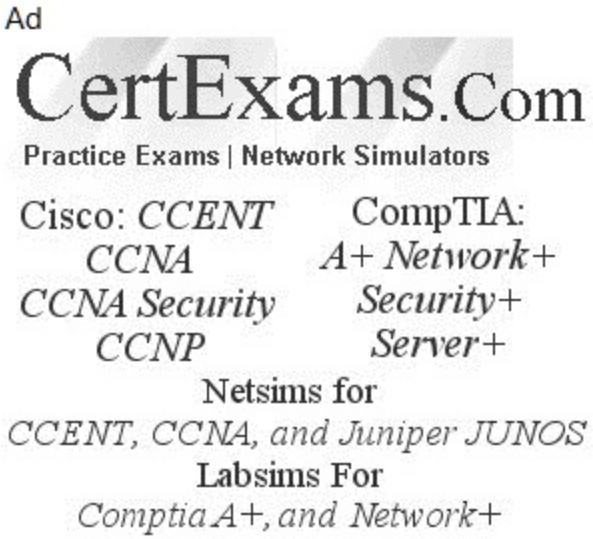
config directory is located on the router's internal flash drive.

/var/log directory is located on the router's hard drive.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : J-web - Core/common Functionality overview

examguides.com/Juniper-JNCIA/juniper-jncia-18.htm



3. User Interfaces

3.5 J-Web - core/common functionality

J-Web is a GUI used to configure the junos devices. The J-Web interface allows you to monitor, configure, troubleshoot, and manage the routing platform by means of a Web browser enabled with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS). J-Web provides access to all the configuration statements supported by the routing platform, so you can fully configure it without using the Junos OS CLI.

You can perform the following tasks with the J-Web interface:

Monitoring - Display the current configuration and information about the system, interfaces, chassis, routing protocols, routing tables, routing policy filters, and other features.

Configuring - The J-Web interface provides the following different configuration methods:

- Configure the routing platform quickly and easily without configuring each statement individually.
- Edit a graphical version of the Junos OS CLI configuration statements and hierarchy.
- Edit the configuration in a text file.

- Upload a configuration file.
- The J-Web interface also allows you to manage configuration history and set a rescue configuration.

Maintaining - Manage log, temporary, and core (crash) files and schedule reboots on the routing platforms.

Configuring and monitoring events - Filter and view system log messages that record events occurring on the router. You can configure files to log system log messages and also assign attributes, such as severity levels, to messages.

The JUNOS software stores multitudes of information in files on the router. The configuration and rollback files are stored using save command, and new versions of the JUNOS software itself. The router stores these files in various directories, including:

/config: This directory is located on the router's internal flash drive. It contains the active configuration (juniper.conf) and rollback files 1, 2, and 3.

/var/db/config: This directory is located on the router's hard drive and contains rollback files 4 through 9.

/var/tmp: This directory is located on the router's hard drive. It holds core files from the various daemons on the Routing Engines. Core files are generated when a particular daemon crashes and are used by Juniper Networks engineers to diagnose the reason for failure.

/var/log: This directory is located on the router's hard drive. It contains files generated by both the router's logging function as well as the traceoptions command.

/var/home: This directory is located on the router's hard drive. It contains a subdirectory for each configured user on the router. These individual user directories are the default file location for many JUNOS software commands.

/altroot: This directory is located on the router's hard drive and contains a copy of the root file structure from the internal flash drive. This directory is used in certain disaster-recovery modes where the internal flash drive is not operational.

/altconfig: This directory is located on the router's hard drive and contains a copy of the /config file structure from the internal flash drive. This directory is also used in certain disaster recovery modes where the internal flash drive is not operational.

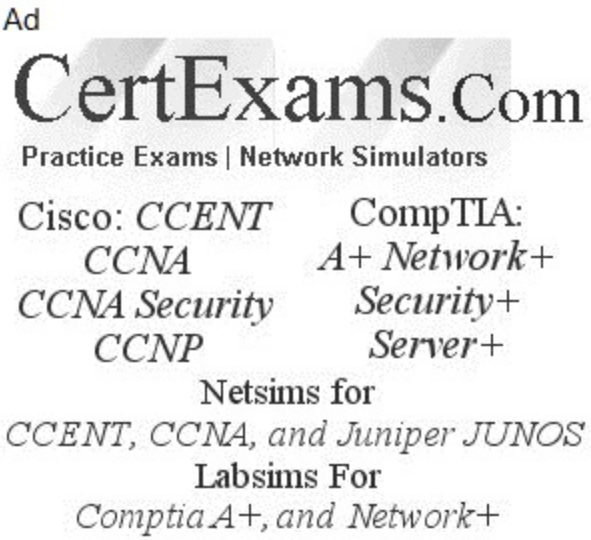
You can view the router's directory structure as well as individual files by issuing the file command in operational mode:

user@router> file ?

Juniper® JNCIA Exam Cram Notes : Factory Default State

examguides.com/Juniper-JNCIA/juniper-jncia-19.htm

Ad



4. Junos Configuration Basics

4.1 Factory Default state

In juniper devices, there is an option to load our configuration back to the factory default state. The use of 'load factory-default' command in configuration mode hierarchy reverts our device to the factory default state. You can also use the load factory-default command to revert to the factory-default configuration file that contains all default settings except the root password setting, which is retained.

The load factory-default command in Config mode will erase only the existing configuration and load the factory-default configuration. However, the root-authentication password must be set before committing the configuration.

If a configuration fails or denies management access to the services gateway, you can use the RESET CONFIG button to restore the services gateway to the factory default configuration or a rescue configuration. For example, if someone inadvertently commits a configuration that denies management access to a services gateway, you can delete the invalid configuration and replace it with a rescue configuration by pressing the RESET CONFIG button. The button is recessed to prevent it from being pressed accidentally.

The rescue configuration is a previously committed, valid configuration. You must have previously set the rescue configuration through the J-Web interface or the CLI.

Juniper® JNCIA Exam Cram Notes : User Authentication Methods

examguides.com/Juniper-JNCIA/juniper-jncia-20.htm

4. Junos Configuration Basics

4.2 User authentication methods

The two authentication methods supported by the JUNOS software are MD5 and simple authentication. Simple authentication uses a plain-text password that is included in the transmitted packet whereas, MD5 does hashing while transmitting the packets.

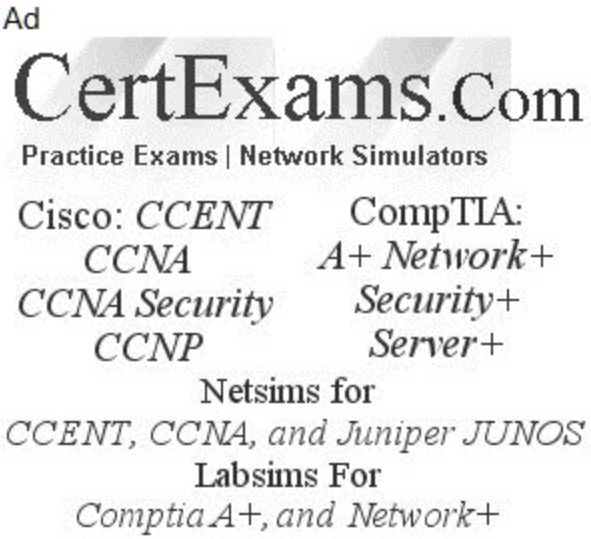
```
[edit protocols]
user@Cabernet# show
rip {
    authentication-type md5;
    authentication-key " $9$09-4OhrW87Vs4xN"; # SECRET-DATA
    group neighbor-routers {
        export [connected-routes transit-rip-routes];
        neighbor fe-0/0/0.0;
        neighbor fe-0/0/1.0;
    }
}
```

Referring to the above output, md5 authentication method is used. The receiving router uses its authentication key (password) and the same algorithm to calculate its one-way hash value and compares it with the one in the packet.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Initial Configuration Basics

examguides.com/Juniper-JNCIA/juniper-jncia-21.htm



4. Junos Configuration Basics

4.3 Initial Configuration

1. Connect a terminal or laptop computer to the router through the console port -a serial port on the front of the router. Only console access to the router is enabled by default.

2. Power on the router and wait for it to boot.

The Junos OS boots automatically. The boot process is complete when you see the login: prompt on the console.

3. Log in as the user root.

Initially, the root user account requires no password. You can see that you are the root user, because the prompt on the router shows the username root@#.

4. Start the Junos OS command-line interface (CLI):

root@#cli
root@>

5. Enter Junos OS configuration mode:

cli>configure
[edit]
root@#

6. When we use 'run' command, the router allows us to access the operational mode command by sitting on configuration mode hierarchy. This is one of the powerful junos commands that exist in configuration mode.

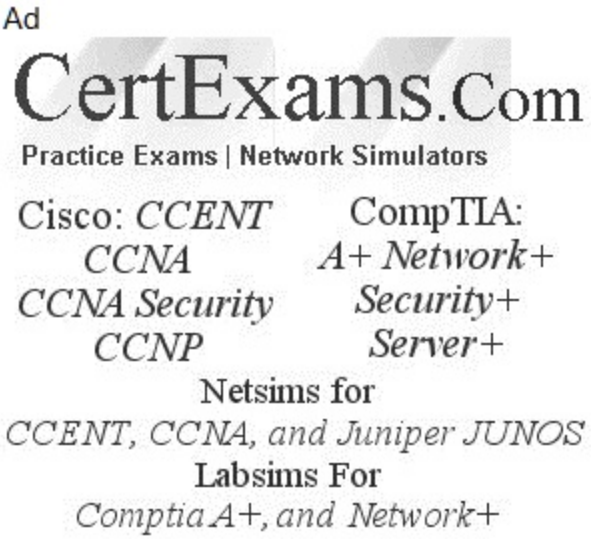
7. The 'up' command allows us to move one hierarchy upper from the existing hierarchy. The 'top' command allows us to move towards the top of the hierarchy. There is no command called middle and upper when it comes to move one hierarchy up from the existing hierarchy.

'Ctrl + L' keystroke redraws the current command line. Whereas 'Ctrl + F' moves the cursor forward one character and 'Ctrl + X' deletes the entire current command line.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Interface Types And Properties

examguides.com/Juniper-JNCIA/juniper-jncia-22.htm

Ad


4. Junos Configuration Basics

4.4 Interface Types and Properties

Juniper Networks platform has primarily two types of interface. These are:

1. Permanent Interfaces: These are always present in the router and Transient interfaces, these can be inserted or removed from the router by user.

Each router has two permanent interfaces. These are:

- **Management Ethernet interface:** This interface enables us to access the router using ssh, and telnet. The interface uses out-of-band connectivity, and does not provide packet forwarding capabilities for the transit data packets.
- **Internal Ethernet interface:** Connects the Routing Engine (running the JUNOS Internet software) to the Packet Forwarding Engine. The router uses this interface as the main communications link between the JUNOS software and the components of the Packet Forwarding Engine. The Internal Ethernet interface is configured automatically when the JUNOS software boots.

2. Transient Interfaces: Transient Interfaces are the interfaces that receive user's data packets from the network and transmit the packets to the network. These interfaces are physically located on a Physical Interface Card. They can be inserted and removed at any

time.

These interface need to be configured before using it. We can also configure the interfaces that are not in the chassis. When the JUNOS software activates the router's configuration it finds out the interfaces that are present and activates only those interfaces.

The maximum transmission unit (MTU) of the physical interface can be changed. Each interface has a different default value. In juniper, the possible MTU range is 256 to 9192 bytes.

In addition, each router has two serial ports, labeled console and auxiliary. Console port can be used to connect tty-type terminals to the router. The auxiliary port can connect to a modem.

The state of the interface are Down, BDR and DR. There are also other states of the interface other than this. BDR and DR are the election carried out in OSPF network.

fxp interfaces are used for managing our juniper devices. The fxp interfaces are the only current interface types that do not follow the two-letter designator format. These interfaces are special in their function.

Each Juniper Networks router contains the fxp0 and fxp1 permanent interfaces. The fxp0 interface performs the management functionality. This provides the out-of-band method used while connecting the router. The operation of a Juniper Networks platform itself relies on the fxp1.The fpc slot locates the interface which begin at 0 on Juniper Networks router.

The fxp1 interface connects the Routing Engine to the Packet Forwarding Engine. This communications link is how routing protocol packets reach the Routing Engine to update

The media type 'lo' indicate the loopback interface. These are the virtual interface that we can create on our juniper routers. These interfaces are mostly created for testing purposes.

Deactivate is the command used to deactivate the interface on junos devices. This command disables the interface from both receiving and transmitting the data.

Each interface has two types of properties assigned to it: physical properties and logical properties. Physical properties are tied to the entire physical port, whereas logical properties affect only that logical portion of the interface represented by unit numbers or channel numbers.

A physical property should always be configured before any logical identifier, such as a unit number.

All router interfaces that will send and receive transit traffic require a logical unit to be configured. This logical unit creates a division of the physical interface into multiple parts. For instance, an Ethernet interface can be subdivided into multiple virtual LANs (VLANs), each requiring its own logical unit.

Link-mode is used to specify full duplex, half duplex, or autonegotiation.

Syntax

link-mode mode (automatic | full-duplex | half-duplex);

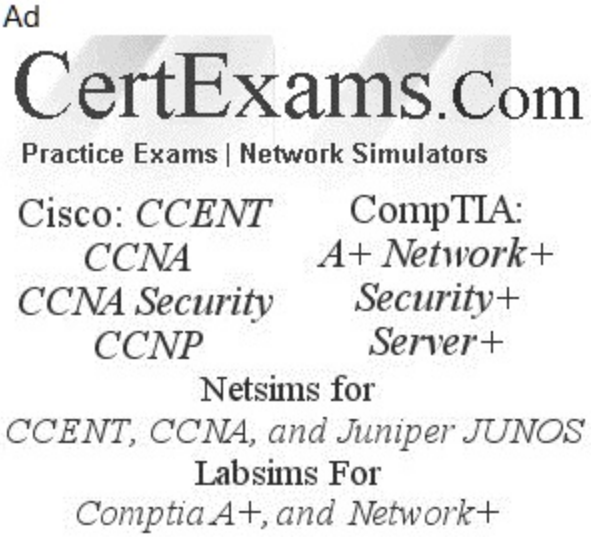
Note that protocol family and lo0 are configured at logical interface.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Describe How To Configure Basic Components Of A Junos Device

examguides.com/Juniper-JNCIA/juniper-jncia-23.htm

Ad



4. Junos Configuration Basics

4.5 Describe how to configure basic components of a Junos device

1. Configuring Hostname of the device: The hostname of a device is its identification. A router or switch must have its identity established to be accessible on the network to other devices. That is perhaps the most important reason to have a hostname, but a hostname has other purposes: Junos OS uses the configured hostname as part of the command prompt, to prepend log files and other accounting information, as well as in other places where knowing the device identity is useful. We recommend that the hostname be descriptive and memorable. We can configure the hostname at the [edit system] hierarchy level.

The following example configures hostname of router R1 as "juniper1"

step1 : Enter into configuration mode

user@R1>configure
[edit]

step 2 : Enter into system hierarchy mode

user@R1#edit system
[edit system]

step 3 : set the hostname as "juniper1"

user@R1#set host-name *juniper1*
[edit system]

In Junos devices, 'set' command is used whenever we need to enter new information into the configuration.

2. Configure name-server on our juniper device: The command 'set system name-server' configures DNS servers to resolve hostnames, we use the set system name-server command.

Ex:

step1 : Enter into configuration mode

user@R2>configure
[edit]

step 2 : Enter into System hierarchy mode

user@R2#edit system
[edit system]

step 3 : set the name server address as 192.168.201.1

user@R2#set name-server *192.168.201.1*
[edit system]

3. Configuring Hold-down Timer: Hold-time value is used to damp interface transitions. When an interface goes from up to down, it is not advertised to the rest of the system as being down until it has remained down for the hold-time period. Similarly, an interface is not advertised as being up until it has remained up for the hold-time period.

step1 : Enter into configuration mode

user@R1>configure
[edit]

step 2 : Move to so-0/0/0 interface hierarchy mode

user@R1#edit interfaces so-0/0/0
[edit interfaces so-0/0/0]

step 3 : Set the holdtime value of 200 milliseconds to use when an interface transitions from down to up and holdtime value of 200 milliseconds to use when an interface transitions from up to down .

user@R1#set hold-time up *200* **down** *200*
[edit interfaces so-0/0/0]

4. We use 'delete' command to delete the configuration from our juniper devices. This command is used in configuration mode either to delete a particular configuration statement or completely delete the entire configuration. We use delete command to remove the variables from the configuration.

For example : **root@root # delete system radius-server** *172.30.10.1*

The delete and deactivate are two different command that performs separate tasks. 'Delete' command deletes each and every configuration present on our junos devices. 'Deactivate' command doesn't delete the configuration but keeps the configuration into an inactive state.

Example: To delete the static route destined for address 192.168.1.0/24 with a next-hop address 192.168.1.1. The command is

delete routing-options static route *192.168.1.0/24* **next-hop** *192.168.1.1*

5. The command "load override common", compares the results of the load override command with the common file that we saved earlier.

6. To configure encrypt password on router: Configuring the root password on your Junos OS-enabled router helps prevent unauthorized users from making changes to your network. The root user (also referred to as superuser) has unrestricted access and full permissions within the system, so it is crucial to protect these functions by setting a strong password when setting up a new router. After a new router is initially powered on, you log in as the user root with no password. Junos OS requires configuration of the root password before it accepts a commit operation. On a new device, the root password must always be a part of the configuration submitted with your initial commit.

step1 : Enter into configuration mode

user@R1>configure
[edit]

step 2 : Move to the root-authentication hierarchy

user@R1#edit system root-authentication
[edit system root-authentication]

step 3 : Set the encrypted password as 24adr3e

user@R1#set encrypted-password *24adr3e*
[edit system root-authentication]

7. Configure the device interface to shutdown state: By default, an interface will be in upstate. We need to issue disable command to bring-down the interface. We can disable a physical interface, marking it as being down, without removing the interface configuration statements from the configuration. To do this, include the disable statement at the [edit interfaces interface-name] hierarchy level

step1 : Enter into configuration mode

user@R1>configure
[edit]

step 2 : Move to so-0/0/0 interface hierarchy mode

user@R1#edit interfaces *so-0/0/0*
[edit interfaces so-0/0/0]

step 3 : Bring the so-0/0/0 to no shutdown state(disable)

user@R1#set disable
[edit interfaces so-0/0/0]

8. To configure ppp enacapsulation: When we configure a point-to-point encapsulation (such as PPP or Cisco HDLC) on a physical interface, the physical interface can have only one logical interface (that is, only one unit statement) associated with it. When you configure a multipoint encapsulation (such as Frame Relay), the physical interface can have multiple logical units, and the units can be either point-to-point or multipoint.

step1 : Enter into configuration mode

user@R1>configure
[edit]

step 2 : Move to so-0/0/0 interface hierarchy mode

user@R1#edit interfaces *so-0/0/0*
[edit interfaces so-0/0/0]

step 3 : set the encapsulation as ppp

user@R1#set encapsulation ppp
[edit interfaces so-0/0/0]

9. The juniper devices are powered off using **"request system power-off"** command. We must write this command staying on operational mode hierarchy

10. The command used to copy the JUNOS software into the hardware is **'request system snapshot'**. To successfully boot the router from the hard drive, you first need to copy the JUNOS software and other critical files to it with the request system snapshot command.

The command used in juniper devices to commit our configuration for 30 minutes is 'commit confirmed 30'. This command makes our configuration active for 30 minutes.

11 The command used to set the generated route is: The 'set routing-options generate route' command on the configuration mode hierarchy helps us in configuring the generated routes on our junos device. Unlike static route, it doesn't have the next hop option

12 To configure the description of the interface

The description to an interface is set by using set description command

Step 1 : 1. Enter into configuration mode of R3

user@R1>configure
[edit]

step 2 : Enter into so-0/0/0 interface configuration mode

user@R1#edit interfaces *so-0/0/0*
[edit interfaces so-0/0/0]

step 3 : Set the description of interface so-0/0/0 as "interface-so-0/0/0"

user@R1#set description "interface-so-0/0/0"
[edit interfaces so-0/0/0]

13. Command syntax to configure IP address of a particular interface's: The 'set interfaces <interface-name> unit 0 family inet address <address>' command configures IPv4 address to a particular interface. This command is executed in configuration mode of Junos CLI.

Example: **set interfaces ge-0/0/0 unit 0 family inet address** *192.168.1.1/24* configures the ge-0/0/0 interface with ip address as 192.168.1.1/24

14. To configure Keepalive intervals

Syntax: **keepalives** *<interval seconds> <down-count number> <up-count number>*

Sending of keepalives is enabled by default. The default keepalive interval is 10 seconds for PPP, Frame Relay, or Cisco HDLC. The default down-count is 3 and the default up-count is 1 for PPP or Cisco HDLC.

Example:

step1 : Enter into configuration mode

user@R1>configure
[edit]

step 2 : Move to so-0/0/0 interface hierarchy mode

user@R1#edit interfaces so-0/0/0
[edit interfaces so-0/0/0]

step 3: Set keepalive interval as 40 ,down count as 30 and up count as 20 of interface so-0/0/0

user@R1#set keepalives 40 30 20
[edit interfaces so-0/0/0]

Additional Initial Configuration elements:

NTP: The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source. We enable NTP client or server within the [edit system ntp] hierarchy.

By default, network time synchronization is unauthenticated. The system will synchronize to whatever system appears to have the most accurate time. To authenticate other time servers, include the trusted-key statement at the [edit system ntp] hierarchy level. Only time servers transmitting network time packets that contain one of the specified key numbers and whose key matches the value configured for that key number are eligible to be synchronized to. Other options are not appropriate.

SNMP: By default, SNMP is disabled on devices running Junos OS. We must enable SNMP on our device by including configuration statements at the [edit snmp] hierarchy level. SNMP is Simple Network Management Protocol. By default, SNMP is disabled in juniper devices. We must enable it and configure it in '[edit snmp]' hierarchy in operational mode

Syslog: Syslog is a standard for computer message logging. It permits separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. In juniper we configure it in [edit system syslog] hierarchy. Syslog messages on juniper devices can be seen using 'show log messages' command in operational mode hierarchy.

Juniper Configuration Hierarchy:

```
[edit]
root@show
system {
        host-name hostname;
        domain-name domain.name;
        backup-router address;
        root-authentication {
                (encrypted-password "password" | public-key);
                ssh-dsa "public-key";
                ssh-ecdsa "public-key";
                ssh-rsa "public-key";
        }
        name-server {
                address;
        }
        interfaces {
                fxp0 {
                        unit 0 {
                                family inet {
                                        address address;
                                }
                        }
                }
        }
}
```

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Show Commands

examguides.com/Juniper-JNCIA/juniper-jncia-24.htm

5. Operational Monitoring and Maintenance

5.1 Show commands

Show version brief: We use "show version brief" command to view the currently running version on our Junos devices. When upgrading our device, we first check the current OS version that is running on our device. The sample output of "show version brief" command is as shown below.

```
Hostname: Merlot
Model: m5
JUNOS Base OS boot [5.2R2.3]
JUNOS Base OS Software Suite [5.2R2.3]
JUNOS Kernel Software Suite [5.2R2.3]
JUNOS Packet Forwarding Engine Support [5.2R2.3]
JUNOS Routing Software Suite [5.2R2.3]
JUNOS Online Documentation [5.2R2.3]
JUNOS Crypto Software Suite [5.2R2.3]
```

show route protocol rip: The 'show route protocol rip' - shows all the RIP routes learned by a router from its neighbor routers. The sample output of "show route protocol rip" command is as shown below.

```
inet.0: 27 destinations, 27 routes (27 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.2.0/24      *[RIP/100] 00:08:25, metric 6
                    > to 172.16.1.2 via fe-0/0/0.0
192.168.8.1/32     *[RIP/100] 00:08:25, metric 6
                    > to 172.16.1.2 via fe-0/0/0.0
192.168.24.1/32    *[RIP/100] 00:01:02, metric 7
                    > to 172.16.1.2 via fe-0/0/0.0
```

show interface terse: 'show interface terse' command shows the interfaces that are currently installed on a router. Interfaces are always displayed in numerical order, from the lowest to the highest FPC slot number. The command 'show interface terse | match inet' displays the interfaces that are provided with an IPv4 addresses. This command displays only the lines on our router with the inet string. The sample output is as shown below

```
fe-0/0/1.0      up    up   inet  10.0.31.1/24
so-0/3/0.0      up    up   inet  10.0.24.2          --> 0/0
fxp0.0          up    up   inet  172.64.0.24/16
lo0.0           up    up   inet  192.168.24.1       --> 0/0
```

show interface's filters: The 'show interface's filters' command displays all firewall filters configured on all interfaces on the router. We can only specify a particular interface filters by using 'show interface filters ' command. The command output is as shown below

Interface	Admin	link	Proto	Input Filter	Output Filter
fe-0/0/0	up	up			
fe-0/0/0.0	up	up	inet	filter-1	filter-2
fe-0/0/1	up	up			
fe-0/0/1.0	up	up	inet	filter-3	filter-4
fe -0/0/2	up	down			
fe-0/0/3	up	down			

The 'show interfaces filters' command displays all firewall filters configured on all interfaces on the router. We can only display the filters of particular interface using 'show interfaces filters <filter-name>' command.

```
Interface       Admin Link Proto Input Filter  Output Filter
fe-0/0/0        up    up
fe-0/0/0.0      up    up   inet  filter-1
   filter-2
fe-0/0/1        up    up
fe-0/0/1.0      up    up   inet  filter-3
   filter-4
fe-0/0/2        up    down
fe-0/0/3        up    down
```

show ospf statistics: The 'show ospf statistics' command displays the counter based on the OSPF packet type. Both the total number of packets and the number in the last 5 seconds is shown with this command.

show chassis hardware: We issue 'show chassis hardware' command on our juniper devices to verify our hardware contents. Each Juniper Networks M-series and T-series router contains an Internet Processor ASIC. We verify its existence by using the show chassis hardware command.

```
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                   50375            M5
Midplane         REV 03   710-002650   HF1437
Power Supply A   Rev 04   740-002497   LK22981           AC
Display          REV 04   710-001995   HF1278
Host                                   8a00000749a99a01  teknor
FEB              REV 08   710-002503   AL0781            Internet Processor II
FPC 0
  PIC 0          REV 04   750-002992   HC5418            4x F/E, 100 BASE-TX
  PIC 1          REV 03   750-002971   HE5256            4x OC-3 SONET, MM
```

We can view the route information on our device by using a simple **'show route'** command. This command shows all the routes that is known to our router. To view only the BGP-learned routes, we use 'show route protocol bgp' command. The sample output of **"show route protocol bgp"** is as shown below.

```
inet.0: 26 destinations, 27 routes (26 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.1.0/24       *[BGP/170] 00:23:21, MED 0, localpref 100
                      AS path: 10 I
                    > to 172.16.1.1 via so-0/0/1.0
10.10.2.0/24       *[BGP/170] 00:23:21, MED 0, localpref 100
                      AS path: 10 I
                    > to 172.16.1.1 via so-0/0/1.0
10.10.3.0/24       *[BGP/170] 00:23:21, MED 0, localpref 100
                      AS path: 10 I
                    > to 172.16.1.1 via so-0/0/1.0
10.10.4.0/24       *[BGP/170] 00:23:21, MED 0, localpref 100
                      AS path: 10 I
                    > to 172.16.1.1 via so-0/0/1.0
10.20.1.0/24       *[BGP/170] 02:37:11, MED 0, localpref 100, from 192.168.6.6
                      AS path: I
                    > to 192.168.100.2 via ge-0/2/0.0
```

The **'show firewall log'** command displays entries in the memory-resident buffer or kernel cache. The router stores information in this buffer when the log filter action is used.

show ospf neighbor: The 'show ospf neighbor' command on the operational mode hierarchy shows the status of our ospf neighbor router. We should check the status of the neighbor's adjacency by using the 'show ospf neighbor' command.

Address	Interface	State	ID	Pri	Dead
10.0.1.46	at-0/1/0.100	Full	10.0.1.103	128	36
10.0.1.34	so-0/0/1.0	Full	10.0.1.102	128	35
10.0.1.9	so-0/0/0.0	Full	10.0.1.21	128	38
10.0.1.5	so-0/0/2.0	Full	10.0.1.22	128	32
10.0.1.1	so-0/0/3.0	Full	10.0.1.23	128	39

show interfaces extensive: The "show interfaces extensive" command displays all possible information about every interface currently installed in the router. We have the option of specifying a particular interface

By default, every IPv6 unicast information are placed in the inet6.0 routing table. We can verify this table using 'show route table inet6.0' command. This command is written in operational mode hierarchy.

RIP protocol is configured on our router from configuration mode hierarchy. Once this configuration has been committed, then only we can view the operational status of RIP by using the 'show rip neighbor' command.

Neighbor	State	Source Address	Destination Address	Send Mode	Receive Mode	In Met
fe-0/0/0.0	Up	172.16.1.2	224.0.0.9	mcast	both	1
fe-0/0/1.0	Up	172.16.2.1	224.0.0.9	mcast	both	1

The **'show ospf route'** command is used to verify the OSPF routes in Juniper devices. This command also displays the state of the OSPF network learned from other router in its OSPF network.

The **'show interfaces'** command on the operational mode hierarchy and 'run show interfaces' command on configuration mode hierarchy shows the information of all the interfaces on our juniper devices.

Show arp: The 'show arp' command displays the entries in the Address Resolution Protocol (ARP) table. This command shows only entries for hosts that the router has attempted to send traffic to.

MAC Address	Address	Name	Interface
00:a0:a5:28:15:f5	172.16.0.1	172.16.0.1	fxp0.0
00:a0:a5:12:29:bd	172.16.5.1	172.16.5.1	fxp0.0
00:a0:a5:12:2a:4b	172.16.8.1	172.16.8.1	fxp0.0

Total entries: 3

show route protocol aggregate: The command 'show route protocol aggregate' displays the route learned from other routers configured with aggregate route. By default, the aggregate route will appear in the inet.0 routing table when at least one contributing route is in the routing table.

```
inet.0: 11 destinations, 16 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/17     *[Aggregate/130] 00:01:52
                      Reject
```

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Monitor Commands

examguides.com/Juniper-JNCIA/juniper-jncia-25.htm

5. Operational Monitoring and Maintenance

5.2 Monitor commands

The **'monitor interface interface-name'** command displays per-second real-time statistics for a physical interface. We can also view common interface failures, such as alarms, errors, or loopback settings. The below fig shows the output of the monitor command

```
Cabernet            Seconds: 11            Time: 12:41:55
                                           Delay: 2/0/2
Interface: so-2/0/0, Enabled, Link is Up
Encapsulation: PPP, Keepalives, Speed: OC3
Traffic statistics:                                    Current delta
  Input bytes:              1103360 (40 bps)          [36]
  Output bytes:             1190328 (48 bps)          [26]
  Input packets:              13839 (0 pps)           [3]
  Output packets:             15246 (0 pps)           [2]
Encapsulation statistics:
  Input keepalives:             410                   [1]
  Output keepalives:            407                   [1]
  LCP state: Opened
Error statistics:
  Input errors:                   0                   [0]
  Input drops:                    0                   [0]
  Input framing errors:           0                   [0]
  Input runts:                    0                   [0]
  Input giants:                   0                   [0]
  Policed discards:             235                   [0]
  L3 incompletes:                 0                   [0]
  L2 channel errors:              0                   [0]
```

show route table inet.0 : We use 'show route table inet.0' command in the operational mode hierarchy to view the IPv4 unicast routes whereas, 'show route table inet.1' command displays the IPv4 multicast routes.

We use 'show route table inet.1' command to view the routing table that stores IPv4 multicast routes. In the below output, the multicast group 224.2.2.2/32 is being advertised by a source located at 10.10.200.200/32.

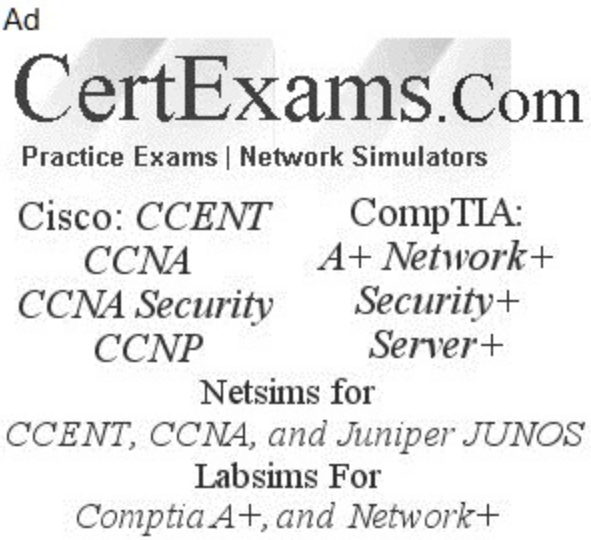
```
inet.1: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

224.2.2.2,10.10.200.200/32*[PIM/105] 00:01:58
                    Multicast
```

The monitor traffic command prints packet headers to your terminal screen for information sent or received by the Routing Engine. It is very similar in operation to the Unix tcpdumputility.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Network Tools

examguides.com/Juniper-JNCIA/juniper-jncia-26.htm

Ad


5. Operational Monitoring and Maintenance

5.3 Network tools

We can use a number network tools to help with troubleshooting and end-to-end connectivity. The ping, traceroute, ssh and telnet commands we use mostly. We would use ping to check end-to-end connectivity testing and we would use traceroute to check the path that we are using to get from one device to another, whether that is on our internal LAN or across the internet. With Junos if we are using a DNS name (i.e. google.co.uk), it will by default use IPv6 AAAA record to try and get find the host in question. If you don't have IPv6 configured on your network this is no help at all!

The ping destination command is a common troubleshooting tool used to check host reachability and network connectivity. It sends ICMP ECHO_REQUEST messages to elicit ICMP ECHO_ RESPONSE messages from the specified host.

We use 'set system services ping' command on our juniper devices to allow ping service. This command is written in configuration mode hierarchy.

Ping and traceroute are the network troubleshooting tools. We often use traceroute when the result of the ping command shows that end-to-end network connectivity is not established.

The 'deactivate system services telnet' command only deactivates the telnet service from our device. In order to remove the telnet service from our device, we use 'delete system services telnet'.

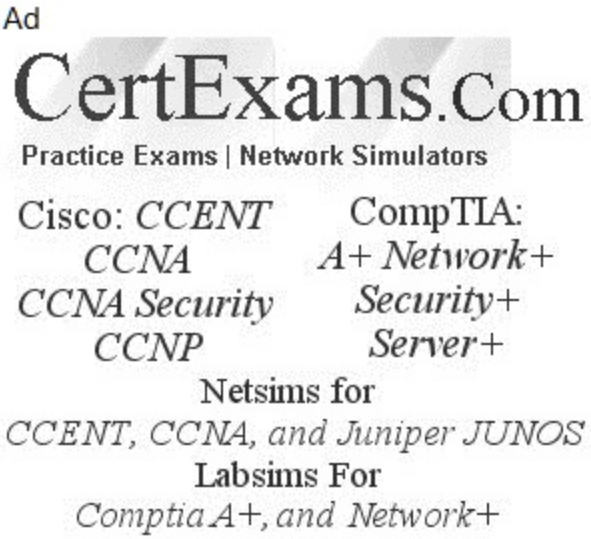
Traceroute command output is as shown below

```
traceroute to 192.168.5.1 (192.168.5.1), 30 hops max, 40 byte packets
 1  10.0.2.2 (10.0.2.2)  0.432 ms  0.347 ms  0.320 ms
 2  192.168.5.1 (192.168.5.1)  1.210 ms  1.005 ms  0.919 ms
```

After executing 'traceroute 192.168.5.1' command, the given output is obtained. We can determine the actual network path taken by the IP packets and also know where the problem might exist. The traceroute command lists all the routers that it passes through until the destination is reached, or fails to and is discarded.

Juniper® JNCIA Exam Cram Notes : Root Password Recovery

examguides.com/Juniper-JNCIA/juniper-jncia-27.htm

Ad


5. Operational Monitoring and Maintenance

5.4 Root password recovery

To recover the root password, perform the following steps:

1. Power off your switch by unplugging the power cord or turning off the power at the wall switch.

2. Insert one end of the Ethernet cable into the serial port on the management device and connect the other end to the console port at the back of the switch.

3. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).

4. Configure port settings as follows:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

5. Power on your switch by plugging in the power cord or turning on the power at the wall switch.

6. When the following prompt appears, press the Spacebar to access the switch's bootstrap loader command prompt:

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel] in 1 second...

7. At the following prompt, type boot -s to start up the system in single-user mode:

loader> boot -s

8. At the following prompt, type recovery to start the root password recovery procedure:

Enter the full pathname of the shell or recovery for root password recovery or RETURN for /bin/sh: recovery.

A series of messages describe consistency checks, mounting of filesystems, and initialization and checkout of management services. Then the Command Line Interface (CLI) prompt appears.

9. Enter configuration mode in the CLI:

user@switch> configure

10. Set the root password, for example:

user@switch# set system root-authentication *plain-text-password*

11. At the following prompt, enter the new root password, for example:

New password: juniper1

Re-type the new password:

12. At the second prompt, re-enter the new root password.

13. If you have finished configuring the network, commit the configuration.

root@switch# commit
commit complete

14. Exit configuration mode in the CLI.

root@switch# exit

15. Exit operational mode in the CLI.

root@switch> exit

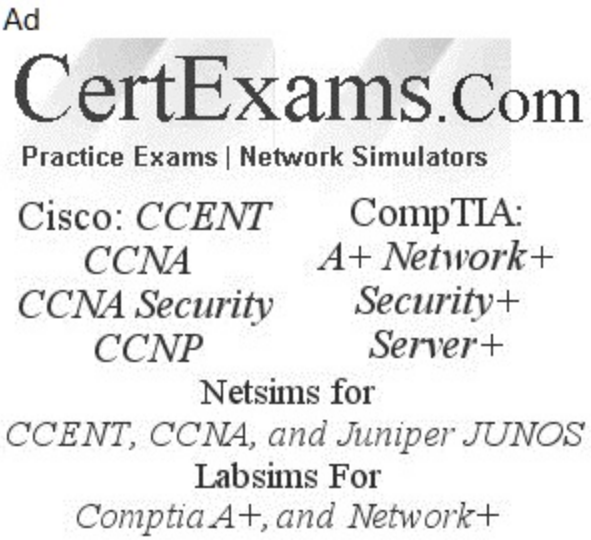
16. At the prompt, enter y to reboot the switch.

Reboot the system? [y/n] y

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Routing Table

examguides.com/Juniper-JNCIA/juniper-jncia-28.htm

Ad


6. Routing Fundamentals

6.1 Routing Table

Junos OS automatically creates and maintains several routing tables. Each routing table is used for a specific purpose. In addition to these automatically created routing tables, you can create your own routing tables.

Each routing table populates a portion of the forwarding table. Thus, the forwarding table is partitioned based on routing tables. This allows for specific forwarding behavior for each routing table. For example, for VPNs, each VPN-based routing table has its own VPN-specific partition in the forwarding table. It is common for the routing software to maintain unicast routes and multicast routes in different routing tables. The policy considerations that would lead to create separate routing tables to manage the propagation of routing information.

Creating routing tables is optional. If you do not create any, Junos OS uses its default routing tables, which are as follows:

inet.0 and inet.2 are the default routing table used in the Junos devices.

The inet.0 routing table is the table used to store IPv4 unicast routes. The router interfaces and all routing protocols place information into this table by default.

Inet.2 table stores unicast routes that are used for multicast reverse-path-forwarding (RPF) lookup.

The default next-hop entry that is placed into a forwarding table for each valid route is 1.

The mpls.0 table is not actually a routing table but is instead a switching table. MPLS label values are stored in this table. We can view the mpls table using 'show route table mpls.0' command.

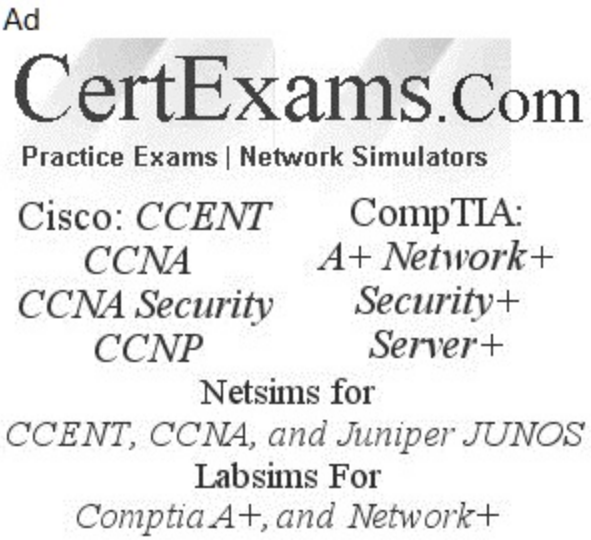
There are nine JUNOS software routing table. The JUNOS software provides multiple routing tables that are used to store routes for our network. Each table is represented within the output of the 'show route' command.

Preference value defines the believability of the individual protocol. All the routing protocols has its individual preference value. The lesser the preference value, the more it is believed in the routing table.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Static Routing

examguides.com/Juniper-JNCIA/juniper-jncia-29.htm

Ad


6. Routing Fundamentals

6.2 Static Routing

Static and Generated routes are the two locally configured routes in the Junos Software. To create both static and generated route in the routing table, we must, at minimum, define the route as static and associate a next-hop address with it. There are six different options for a static route next hop. They are reject, Remote IP address, directly connected IP address, qualified next hop, Label Switched path and discard.

The two options available within the junos software for next-hop values are reject and discard

Both 'reject' and 'discard' is configured null value. Route lookups that match an aggregate route with a reject next hop are dropped.

The value reject is a configured null value. Route lookups that match an aggregate route with a reject next hop are dropped and an ICMP "Destination Host Unreachable" message is returned to the source of the packet.

In case of generated route, the ip address of the primary contributing routes is taken as the default next hop.

While configuring the static route, we must provide the valid next-hop address on our routing table. Possible values include an IP address, a configured null value and a qualified next hop address.

Static routes are useful in situations where ultimate routing control is required. By manually configuring the next-hop to the destination you are certain where the traffic will go. Especially in edge situations static routes are very useful and often used.

The basic syntax for configuring static route is

set routing-options static route <*ipadd*> **next-hop** <*next-hop-ipadd*>

step1 : Enter into configuration mode

user@R1>configure
[edit]

step 2 : Move to routing-options hierarchy mode

user@R1#edit routing-options
[edit routing-options]

step 3 : Configure a static route to a destination sub-network (172.16.1.0) with 24-bit subnet mask

user@R1#edit static route *172.16.1.0/24*
[edit routing-options static route 172.16.1.0/24]

step 4 : Set the next-hop ip address as 172.16.2.1

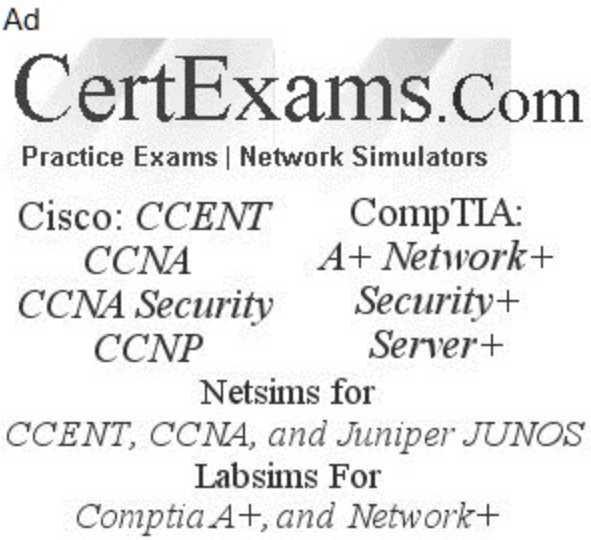
user@R1#set next-hop *172.16.2.1*
[edit routing-options static route 172.16.1.0/24]

We can set the static route by configuring it either on 'edit' hierarchy or 'edit routing-options' hierarchy. Both these commands perform the same function. These commands add the static route destined for 192.168.1.0/24 network with a next-hop address of 2.2.2.2

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Routing Protocols

examguides.com/Juniper-JNCIA/juniper-jncia-30.htm

Ad


6. Routing Fundamentals

6.3 Routing Protocols

There are three locally configured routes. They are static route, aggregated route and generated route. These routes are not learned through a dynamic routing protocol but are manually entered by you, the administrator.

The Junos OS routing protocol process assigns a default preference value (also known as an administrative distance) to each route that the routing table receives. The default value depends on the source of the route. The preference value is a value from 0 through 4,294,967,295 (232 -1), with a lower value indicating a more preferred route.

Given below are the route preference values (administrative distances for various protocols):

Directly Connected:0
Static route: 5
OSPF internal: 10
IS-IS level 1 internal:15
IS-IS level 2 internal:18
RIP, RIPng:100
OSPF AS external:150

IS-IS external level 1:160
IS-IS external level 2:165
BGP:170

RIP: RIP refers to Routing Information Protocol, which is one of the dynamic routing. It receives the response message to trigger an update response sent by a neighbor. Response messages are also received in response to a request message generated by the router and for an unsolicited response message sent by the neighbor.

Important points on RIP and RIPv2:

- RIP(Routing Information Protocol) uses Bellman-Ford algorithm.
- Diffusing Update Algorithm is used by EIGRP.
- Classless Inter Domain Routing(CIDR) is not supported in RIPV1. For example, if I have a network 10.0.0.0 using /24 subnet mask then, RIPV1 changes /24 subnet mask into /8 mask i.e. it doesn't support CIDR. But CIDR is supported in RIP version 2.
- The hop count in case of RIP is limited. It doesn't support Classless routing. The convergence time is slow and the security is weak.
- RIPV2 supports Variable Length Subnet Mask(VLSM) also with the support of authentication. Unlike RIPV1, RIPV2 support classless routing.
- RIP version1 is less preferred over RIP version2. However the hop count value is same on both versions of RIP
- It supports simple authentication and md5 authentication. A simple authentication uses a plain-text password that is included in the transmitted packet. MD5 authentication uses the hash algorithm in the transmitted packet.
- The largest usable metric that is available in case of RIP is 15. Any destination with 16 hop-count is considered unreachable
- Request and Response are the two packet types used in the RIP network.
- Request packet is sent to a neighbor to request neighbor's routing table.
- Response packet is sent as a reply to a neighbor's request packet.
- Split Horizon, Triggered update, and Hold-down timers avoid routing loops in RIP.
- The maximum size of an IP RIP packet is limited to 512 bytes. This means that an individual Request or Response message can contain no more than 25 entries.
- Authentication between RIP neighbors is disabled in JUNOS software. We can configure the authentication if we wish to provide authentication on our network environment.
- A minimum RIP configuration must include at least the rip, group, and neighbor statements. All other RIP configuration statements are optional. We include one neighbor statement for each logical interface on which you want to receive routes.
- The receive-options values in RIP are version-1, none and both. The 'none' receive-options value do not receive RIP packets, the version-1 value only accepts RIPv1 packets and 'both' receive-options accept RIPv1 and v2 packets.

- Broadcast and Multicast are the two send-options values in RIP. Along with this there are also other two send-options values. They are version-1 and none.
- Broadcast send-options value broadcast the RIPv2 packets and multicast send-options value multicast RIPv2 packets.
- The maximum number of route entries that can be advertised in a single message of RIP is 255. We can also change this default value by using 'message size' command.
- In RIP network, 15 is the largest usable metric allowed. We cannot use RIP network if the hop count in our network is more than 15. A metric of 16 is considered unreachable.
- The entire routing table of RIP is advertised to its neighbor on a regular interval. This regular update is controlled by the update timer which runs every 30 seconds.
- Route tagging is only supported in RIPv2. There are various features in RIP network supported in RIPv2 but not in RIPv1. These features include authentication, VLSM, etc.
- RIP routers use UDP (User Datagram Protocol) port 520 to send messages to their neighbors. In addition, the RIP specification does not provide its own mechanism for reliable delivery.
- The default operation of RIP within the JUNOS software is to receive routes but not to advertise routes. After configuring a routing policy, we can advertise the routes on our RIP network.
- 20-byte trailer is added to the length of the RIP message with the use of MD5 authentication. Also, an additional route entry is used by the algorithm.

RIP configuration hierarchy as shown below

```
rip {
        group group-name {
        export [ policy-names ];
        neighbor neighbor-name {
        import [ policy-names ];
        }
      }
    }
```

The preference value of the aggregated route is 130. RIP has the preference of 100 and Border Gateway Protocol (BGP) has the preference value of 170.

OSPF: Open Shortest Path First (OSPF) is an Open-Standard Interior Gateway Protocol (IGP) routing protocol. Unlike other Routing Protocols such as Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) or Border Gateway Protocol (BGP), OSPF uses the Link State Algorithm in conjunction with Edsger W. Dijkstra Shortest Path First (SPF) algorithm to send out OSPF advertisements, known as Link-State

Advertisements (LSAs), to share its Local Link-State Database (LSDB) with OSPF enabled devices to create an overall topology of every router, link state and link metric within a network. OSPF is defined in RFC2328:

OSPF is a link-state routing protocol. It is designed to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a shortest-path tree.

OSPF recalculates routes quickly in the face of topological changes, utilizing a minimum of routing protocol traffic. OSPF provides support for equal-cost multipath. An area routing capability is provided, enabling an additional level of routing protection and a reduction in routing protocol traffic. In addition, all OSPF routing protocol exchanges are authenticated.

OSPF advertises and receives LSAs to/from neighbouring routers; these LSAs are stored with the router's local LSDB. Whenever there is a change in the network new LSA's will be flooded across the routing domain and all the routers will have to update their LSDB. This is due to the nature of the Link State and SPF Algorithms; essentially all OSPF routers have to same synchronized identical copy of the Link State Database to have a complete loop-free map of the network topology.

Down is the first starting state for all OSPF routers. After this state Init state is seen. Also, 2-way is one of the state for all OSPF routers. It indicates that the local router has received hello packets with its own router ID in the neighbor field. OSPF uses Dijkstra Algorithm. hello packets and link-state update packets are the two packets of OSPF. Along with this, there are other OSPF packets like Database Descriptor packets, link-state request packets and link-state acknowledge packets. In an OSPF network, DR and BDR election takes place. DR is known as the Designated Router and BDR is known as Backup Designated Router.

Backbone router is a router that has at least one interface in area 0.

Internal Router maintains all operational interfaces.

Area border router connects one or more OSPF areas to the backbone.

We use "show ospf route" command to verify the route of OSPF network. It displays the result of the SPF algorithm.

The two criteria used to elect a designated router are the router priority and the router ID. Designated Router (DR) is responsible for sending the routing updates to the other routers on our network.

There are six different LSA type which are router, network, network summary, ASBR summary, AS external, and NSSA external LSAs.

By default, internal OSPF routes have a preference value of 10, and external OSPF routes have a preference value of 150

Multi-area OSPF is supported in Juniper devices. It means that we can create two different OSPF areas on the same Autonomous System (AS). But all OSPF network must be a member of Area 0.

The inet protocol supports an IPv4 packet. The Intermediate System to Intermediate System (IS-IS) routing protocol uses a data link encapsulation defined by the International Standards Organization (ISO).

DD packets are exchanged by the local router and the neighbor router, that describe their local database. If the OSPF state is stuck at exchange state, OSPF neighborship is not established. It is because of OSPF MTU mismatch.

An internal router, a backbone router and an area border router are the types of OSPF router. Other than this, there is still one other type of OSPF router and that is an Autonomous System Border Router.

To establish and maintain a neighbor relationship, an OSPF-speaking router determines whether any directly connected routers also speak OSPF. The OSPF router sends hello packets out all configured interfaces.

The full-form of DR in OSPF network is Designated Router. Designated Router is responsible for sending out updates to all other routers in OSPF network. Backup Designated Router (BDR) is the backup router in OSPF network. If DR fails, BDR becomes DR.

OSPF has five different packet types they are:

1. hello
2. link-state acknowledgement
3. link-state request packet
4. database description
5. link-state updates

OSPF Configuration Hierarchy

```
ospf {
      area area-id {
         interface interface-name {
            disable;
            hello-interval seconds;
            dead-interval seconds;
            neighbor neighbor_address;
         }
         stub <(no-summaries | summaries)>;
         virtual-link neighbor-id router-id transit-area area-id {
         }
      }
      export [ policy-names ];
}
```

BGP: The Border Gateway Protocol (BGP) is the routing protocol that is extensively used in the Internet to connect ISP networks. BGP is a path vector routing protocol. BGP uses route mechanism that is comparable to OSPF or IS-IS. The two of the BGP states used when establishing relationships are Idle and Active. Idle is the initial neighbor state, in which it rejects all incoming session requests. In the Active state, the local router is trying to initiate a TCP session with its peer.

In BGP networks, 4 message types are exchanged between two peers. Those 4 message types are Open, Update, Notification, and keepalive.

Routing information is sent and withdrawn in BGP using the Update message. If needed, each message contains information previously advertised by the local router that is no longer valid.

A BGP peer sends a Notification message to the remote router when a BGP peer detects an error. This is the error that is detected within the session and immediately both BGP and TCP sessions are closed.

A BGP Keepalive message contains only the 19-octet message header and no other data. These messages are exchanged at one-third the negotiated hold-time value for the session, if necessary.

The full-form of RIB is Routing Information Base. Each BGP router establishes memory locations in which to store routing knowledge. These are collectively known as Routing Information Base (RIB).

BGP Configuration hierarchy:

```
     bgp {
        group <group_name> {
                type <type-name>
                peer-as <asnum of the peer>
                neighbor <neg_ipaddress>
                neighbor <neg_ipaddress> {
                        peer-as <asnum of the peer>
                }
                hold-time <seconds>
        }
}
```

Local loopback and the Remote loopback are configured as a physical interface property and affect the operations of PIC and ports.

BGP is not the junos protocol family.

The inet is the protocol family that supports IPv4 packtets.

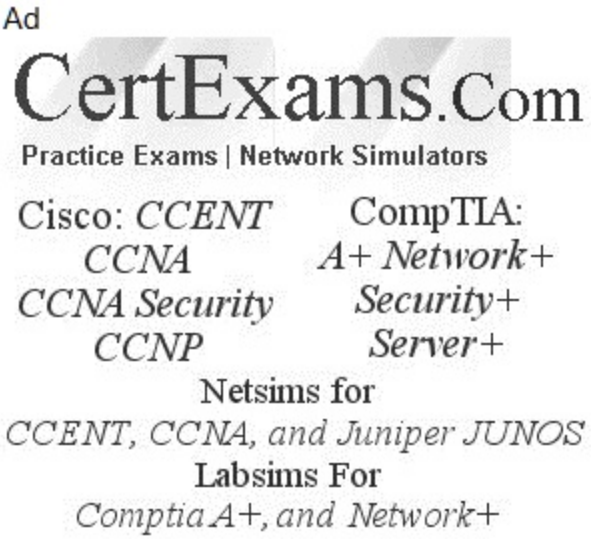
The mpls protocol family provides support for MPLS packets.

The iso protocol family allows the processing of the IS-IS protocol.

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Default Routing Policies

examguides.com/Juniper-JNCIA/juniper-jncia-31.htm



7. Routing Policy and Firewall Filters

7.1 Default Routing Policies

Routing policy Allows you to control the routing information between the routing protocols and the routing tables and between the routing tables and the forwarding table. All routing protocols use the Junos OS routing tables to store the routes that they learn and to determine which routes they should advertise in their protocol packets. Routing policy allows you to control which routes the routing protocols store in and retrieve from the routing table.

In Junos device, the policy is written first then only a policy is applied. We can define security zones on our junos devices. Considering those security zones, policy is written and applied. Policing uses two different types of values to rate-limit user traffic. The first is the bandwidth - limit value, which is the average number of bits per second permitted in the range of 32Kbps to 32Gbps. The second is burst-size-limit, which is the amount of data allowed to exceed the given bandwidth constraints.

Reasons to Create a Routing Policy

The following are typical circumstances under which you might want to preempt the default routing policies in the routing policy framework by creating your own routing policies:

- You do not want a protocol to import all routes into the routing table. If the routing table does not learn about certain routes, they can never be used to forward packets and they can never be redistributed into other routing protocols.
- You do not want a routing protocol to export all the active routes it learns.
- You want a routing protocol to announce active routes learned from another routing protocol, which is sometimes called route redistribution.
- You want to manipulate route characteristics, such as the preference value, AS path, or community. You can manipulate the route characteristics to control which route is selected as the active route to reach a destination. In general, the active route is also advertised to a router's neighbors.
- You want to change the default BGP route flap-damping parameters.
- You want to perform per-packet load balancing.
- You want to enable class of service (CoS).

Policy Components

All policies are composed of the following components that you configure:

- Match conditions - Criteria against which a route or packets are compared. You can configure one or more criteria. If all criteria match, one or more actions are applied.
- Actions - What happens if all criteria match. You can configure one or more actions.
- Terms - Named structures in which match conditions and actions are defined. You can define one or more terms.

The policy framework software evaluates each incoming and outgoing route or packet against the match conditions in a term. If the criteria in the match conditions are met, the defined action is taken.

In general, the policy framework software compares the route or packet against the match conditions in the first term in the policy, then goes on to the next term, and so on. Therefore, the order in which you arrange terms in a policy is relevant.

The order of match conditions within a term is not relevant because a route or packet must match all match conditions in a term for an action to be taken.

Import and export policies: Import and export policies controls the view of the local router and the neighbor router. We configure an import and an export policy under [edit protocols] hierarchy. There is no default import policy for OSPF. But the default export policy for OSPF is to reject all routes.

There are three such possible results that each policy contains. Both accept and reject are considered terminating actions and they have a special meaning-they stop the policy evaluation. The next policy clarifies that the route should be evaluated by the next position in

the policy chain.

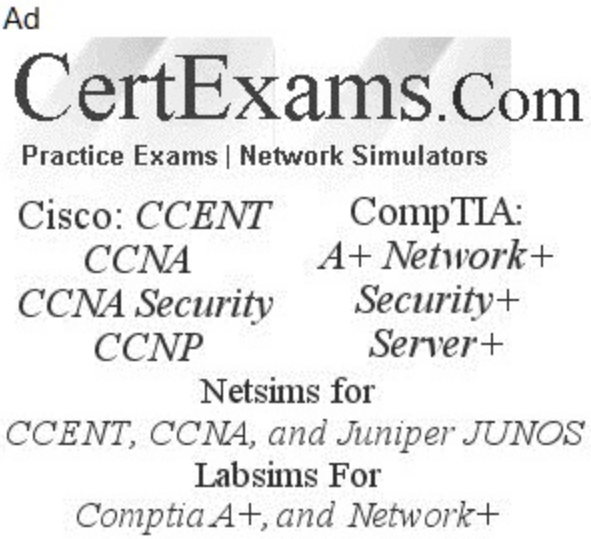
Policy-Options Hierarchy

```
policy-options {
 policy-statement policy-name {
 term term-name {
        from {
             match-conditions;
           }
       to {
          match-conditions;
          }
     then actions;
     }
   }
}
```

Previous Contents Next

Juniper® JNCIA Exam Cram Notes : Firewall Filter Concepts

examguides.com/Juniper-JNCIA/juniper-jncia-32.htm

Ad


7. Routing Policy and Firewall Filters

7.2 Firewall Filter Concepts

Firewall filter policy: Allows you to control packets transiting the router to a network destination and packets destined for and sent by the router.

In junos devices, a firewall filter in router is implemented using Internet Processor ASIC. The Internet Processor builds on the fundamental performance and reliability by adding enhanced security functions, increased visibility into network operations. Each firewall filter in the JUNOS software contains a hidden term that causes a single final action for all filters. This final action is to discard all packets.

Firewall filters enables to control packets transiting the device to a network destination as well as packets destined for and sent by the device. You can configure a firewall filter to perform specified actions on packets of a particular protocol family, including fragmented packets, that match specified conditions based on Layer3 or Layer4 packet header fields.

Stateless and Stateful Firewall Filters

A **stateless firewall filter**, also known as an access control list (ACL), does not statefully inspect traffic. Instead, it evaluates packet contents statically and does not keep track of the state of network connections. Stateless firewalls watch network traffic, and restrict or block

packets based on source and destination addresses or other static values. They are not 'aware' of traffic patterns or data flows.

In contrast, a **stateful firewall filter** uses connection state information derived from other applications and past communications in the data flow to make dynamic control decisions. tateful firewalls can watch traffic streams from end to end. They are are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption. In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, synchronization acknowledge or established), it can tell if the MTU has changed, whether packets have fragmented etc.

Stateless firewalls are typically faster and perform better under heavier traffic

Stateful firewalls are better at identifying unauthorized and forged communications.

Firewall Filter Components

In a firewall filter, you first define the family address type (ethernet-switching, inet (for IPv4), inet6 (for IPv6), circuit cross-connect (CCC), or MPLS), and then define one or more terms that specify the filtering criteria and the action to take if a match occurs.

Each term consists of the following components:

- Match conditions - Specify values that a packet must contain to be considered a match. You can specify values for most fields in the IP, TCP, UDP, or ICMP headers. You can also match on interface names.
- Action- Specifies what to do if a packet matches the match conditions. A filter can accept, discard, or reject a matching packet and then perform additional actions, such as counting, classifying, and policing. If no action is specified for a term, the default is to accept the matching packet.

Firewall Filter Processing: If there are multiple terms in a filter, the order of the terms is important. If a packet matches the first term, the switch executes the action defined by that term, and no other terms are evaluated. If the switch does not find a match between the packet and the first term, it compares the packet to the next term. If no match occurs between the packet and the second term, the system continues to compare the packet to each successive term in the filter until a match is found. If the packet does not match any terms in the filter, the switch discards the packet by default.

The command to configure a firewall filter is made at the [edit firewall family inet] hierarchy level

```
filter filter-name {
  term term-name {
    from {
      match-conditions;
    }
    then {
      action;
    }
  }
}
```

where filter-name is the name of the filter, term-name is the name of the filter term, match-conditions is the condition that the incoming packets must match for the action to be applied, and action is the steps to take for packets that match the filter condition.

The **'show firewall'** command displays counter and policer statistics for all firewall filters. We can also specify the name of specific filter using **'show firewall filter <*filter-name*>'** command.

Count, log and sample are the action modifiers used in firewall filters. This modifiers help us in gathering additional information about the contents of packets.

You use the clear firewall counter-name command to reset the counters associated with your firewall filters. You can clear an individual counter, an individual filter, or all filters on the router.

Example: To clear the counter and policier statistics of MY-FILTER firewall filter, we use 'clear firewall filter MY-FILTER' command. Whereas the 'clear firewall filter' command clears all the counter and policier statistics of all the firewall filters applied on our device.

'icmp-code number',**'dscp number'** and **'destination-port number'** are the numeric range firewall filter match condition. Destination-port number denotes the TCP or UDP destination port field.

The JUNOS software uses firewalls filters not only to drop or accept data packets but also to rate - limit those packets. Rate policing enables you to limit the amount of traffic that passes into or out of a particular interface.

We use **'show'** command to display our configuration that we have configured. In order to modify our configuration we use rename and insert commands. Rename command renames the filter configuration with other configuration.

Previous Contents