CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-1.htm

I. Architecture

1. Explain the different design principles used in an enterprise network

1.1. Enterprise network design such as Tier 2, Tier 3, and Fabric Capacity planning.

Spine-leaf: With the increased focus on massive data transfers and instantaneous data travel in the network, the aging three-tier design within a data center is being replaced with what is being called the Leaf-Spine design. It is also referred to as leaf and spine topology, in this design there are switches found at the top of each rack that connect to the servers in the rack,with a server connecting into each switch for redundancy. People refer to this as a top-of-rack (ToR) design because the switches physically reside at the top of the rack.

The Leaf layer consists of access switches that connect to devices like servers, firewalls, load balancers, and edge routers. The Spine layer (made up of switches that perform routing) is the backbone of the network, where every Leaf switch is interconnected with each and every Spine switch.

SOHO: Means small office,home office, and is a small network connecting a user or small handful of users to the internet and office resources such as servers and printers. Usually just one router and a switch, or two, plus a firewall.

3-tier architecture: In this cisco defines 3 layers of hierarchy, the core,distribution, and access each with specific function and it's referred to as a 3-tier network architecture.

2-Tier Architecture: It's also known as collapsed core design because it's only 2 layers. In this the distribution layer is merged with the core layer.

A core is called collapsed when you move the role of the core switches to the distribution switches, merging the core- and distribution layer. We do this by directly connecting the distribution switches to each other, instead of through a core switch.

Common features of most NGFWs:

1. Standard firewall features: These include the traditional (first-generation) firewall functionalities such as stateful port/protocol inspection, Network Address Translation (NAT), and Virtual Private Network (VPN).

2. Application identification and filtering: This is the chief characteristic of NGFWs. This feature identifies and filters traffic based upon the specific applications, rather than just opening ports for all kinds of traffic. This prevents malicious applications and activity from using non-standard ports to avoid the firewall.

3. SSL and SSH inspection: NGFWs can even inspect SSL and SSH encrypted traffic. This feature decrypts traffic, makes sure the applications are allowed, checks other policies, and then re-encrypts the traffic. This provides additional protection from malicious applications and activity that tries to hide itself by using encryption to avoid the firewall.

4. Intrusion prevention: These are more intelligent capabilities and provide deeper traffic inspection to perform intrusion detection and prevention. Some of the NGFWs have built-in IPS functionality so that a stand-alone IPS might not be needed.

5. Directory integration: Most NGFWs include directory support (such as, Active Directory). For instance, they manage authorized applications based upon users and user groups.

6. Malware filtering: NGFWs can also provide reputation-based filtering to block applications that have a bad reputation. This functionality can check for phishing, viruses, and other malware sites and applications

A traditional firewall provides stateful inspection of network traffic. It allows or blocks traffic based on state, port, and protocol, and filters traffic based on administrator-defined rules.

A next-generation firewall (NGFW) does this, and so much more. In addition to access control, NGFWs can block modern threats such as advanced malware and application-layer attacks. According to Gartner's definition, a next-generation firewall must include:

1. Standard firewall capabilities like stateful inspection
2. Integrated intrusion prevention
3. Application awareness and control to see and block risky apps
4. Threat intelligence sources
5. Upgrade paths to include future information feeds
6. Techniques to address evolving security threats

In summary, a next-generation firewall includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

1.2. High availability techniques such as redundancy, FHRP, and SSO

First-hop router (FHR): A router that is directly attached to the source, also known as a root router. It is responsible for sending register messages to the RP. A Rendezvous Point (RP) is a router in a multicast network domain that acts as a shared root for a multicast shared tree.

Multicast Routing Information Base (MRIB): A topology table that is also known as the multicast route table (mroute), which derives from the unicast routing table and PIM. MRIB contains the source S,group G, incoming interfaces (IIF), outgoing interfaces (OIFs), and RPF neighbor information for each multicast route as well as other multicast-related information.

Multicast Forwarding Information Base (MFIB): A forwarding table that uses the MRIB to program multicast forwarding information in hardware for faster forwarding.

Last-hop router (LHR): A router that is directly attached to the receivers, also known as a leaf router. It is responsible for sending PIM joins upstream toward the RP or to the source.

Outgoing interface (OIF): Any interface that is used to forward multicast traffic down the tree, also known as the downstream interface.

Previous Contents Next

CCNP ENCOR Cram Notes Contents

Cisco CCNP
ENCOR
Practice Tests
www.simulationexams.com

CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-2.htm

I. Architecture

2. Analyze design principles of a WLAN deployment

2.1 Wireless deployment models (centralized, distributed, controller-less, controller based, cloud, remote branch)

Note that the connectivity was slow or intermittent. If there were any mode/SSID mismatch, there wouldn't be any communication at all. It is also likely that the wireless phones, filing cabinets, and antenna mismatch errors are adding to the problem.

A trunk link can be negotiated between two switches only if both switches belong to the same VLAN Trunking Protocol (VTP) management domain or, if one or both switches have not defined their VTP domain (that is, the NULL domain). If the two switches are in different VTP domains and trunking is desired between them, you must set the trunk links to ON mode or no-negotiate mode. This setting forces the trunk to be established.

A hacker begins a DDoS attack by exploiting a vulnerability in one computer system and making it the DDoS "master", also called as "zombie". It is from the zombie that the intruder identifies and communicates with other systems that can be compromised. The intruder loads hacking tools on the compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. This causes Distributed Denial of Service (DDoS) attack on the target computer.

The SSID needs to be consistent for a wireless client to roam between LWAPs that are managed by the same WLC. However, if the LAPs are managed by different WLCs, then the Mobility group must be same on the WLCs. A Mobility Group is a group of Wireless LAN Controllers (WLCs) in a network with the same Mobility Group name. These WLCs can dynamically share context and state of client devices, WLC loading information, and can also forward data traffic among them, which enables inter-controller wireless LAN roaming and controller redundancy. Note that the WLCs may be in the same or different IP subnet or VLAN. WLCs use what is known as Ether-IPtunnel to transfer User traffic from one WLC to another.

Assuming that a User (or Client) originally joined the WLAN on WLC1, WLC1 will always refer to itself as the User's anchor point. Any controller that is serving the User from a different subnet is known as a foreign agent. As the client continues to roam, the anchor

WLC will follow its movement by shifting the Ether-IP tunnel to connect with the User's foreign WLC.

In order for a wireless client to seamlessly roam between mobility group members (WLCs), WLAN's SSID and security configuration must be configured identically across all WLCs comprising the mobility group.

Intruder Prevention System (IPS): IPS analyses network traffic, can report and take corrective action on traffic that it deems malicious or harmful. This can be implemented as an appliance, as a blade, or as a module in an ASA or IOS router. The primary method for identifying problem traffic is through signature matching.

Cisco Security Manager (CSM): This is an enterprise-level configuration tool that you can use to manage most security devices.

Cisco Security Intelligence Operations (SIO) Service: The SIO researches and analyses threats and provides real-time updates on these threats. There is also an application for smart phones.

2.2 Differentiate between on-premises and cloud infrastructure deployments

Different cloud models are explained below:

Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

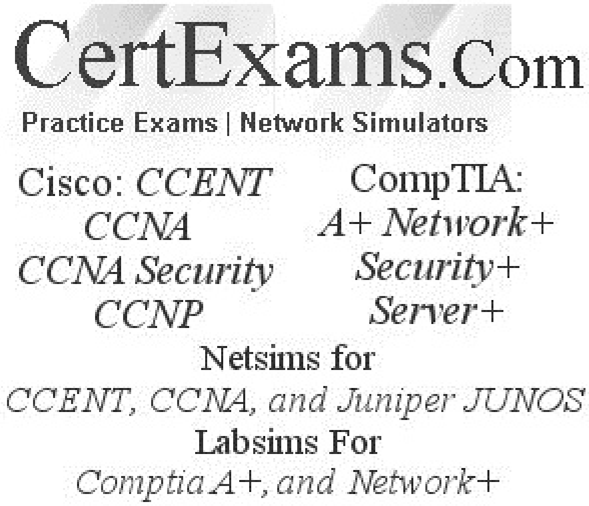
Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but that are bound together by standardized or proprietary technology enabling data and application portability.

Previous Contents Next

CCNP ENCOR Cram Notes Contents

Ad



CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-3.htm

I. Architecture

3. Explain the working principles of the Cisco SD-WAN solution

3.1 SD-WAN control and data planes elements

vManage Network Management System (NMS): The vManage NMS provides unified access via network management system (NMS) GUI. NMS GUI is used to configure and manage the full SD-WAN solution. It enables centralized provisioning and simplifies network changes.

The Cisco SD-WAN solution has four main components and an optional analytics service:

vManage Network Management System (NMS): This is a single pane of glass (GUI) for managing the SD-WAN solution. vSmart controller: This is the brains of the solution.

SD-WAN routers: SD-WAN involves both vEdge and cEdge routers.

vBond orchestrator: This authenticates and orchestrates connectivity between SD-WAN routers and vSmart controllers.

vAnalytics: This is an optional analytics and assurance service.

3.2 Traditional WAN and SD-WAN solutions

1. Traditional WAN : Traditional network is based on completely hardware network devices which mostly rely on Multi Protocol Label Switching (MPLS) for resilient and efficient network traffic flow. Number of hardware devices are installed along with proprietary circuits to route IP services to their intended clients. IT teams gives a lot great effort to manage the network as it involves layers of underlying hardware installed.

Scaling of traditional network is difficult as it needs a proper advanced planning along with required network infrastructure to set up and run. A Traditional connects many Local Area Networks (LANs) and Virtual Private Networks (VPNs) and it is limited to enterprise, branch, and data center. It allows to prioritize your data, voice, and video traffic on network. Security issues and management difficulties are the major problems in traditional WAN now a days.

2. Software Defined Wide Area Network (SD WAN) : SD WAN stands for Software Defined Wide Area Network which is a software defined approach to manage Wide Area Network. In SD WAN software controls everything starting from connectivity to management and providing service. It is a virtual network approach which combines traditional WAN technologies, such as MPLS, LTE and broadband connections.

SD WAN is good for global enterprises as it provides a better and secure application performance as well as optimized cloud connectivity and simplified management. Means in the cloud centric world SD WAN are more preferable than traditional WAN. Software Defined Network (SDN) is utilized which helps in determining the optimal way of routing.

4. Explain the working principles of the Cisco SD-Access solution

4.1 SD-Access control and data planes elements

The Cisco SD-Access fabric is one of the main components of the Cisco Digital Network Architecture (Cisco DNA). Cisco DNA is the solution for the future of intent-based networking in Cisco enterprise networks. SD-Access provides policy-based network segmentation, host mobility for wired and wireless hosts, and enhanced security as well as other benefits in a fully automated fashion. Cisco SD-Access was designed for enterprise campus and branch network environments and not for other types of network environments, such as data center, service provider, and WAN environments.

There are three basic planes of operation in the SD-Access fabric:

Control plane, based on Locator/ID Separation Protocol (LISP)

Data plane, based on Virtual Extensible LAN (VXLAN)

Policy plane, based on Cisco TrustSec

Cisco Digital Network Architecture (Cisco DNA), a software-driven platform that helps to create an intuitive and automated network. This allows network administrators to use software to execute policy and configuration changes they want to be made throughout the network. Many other operational tasks are streamlined through drag-and-drop provisioning, proactive troubleshooting, immediate remediation guidance and fast network segmentation.

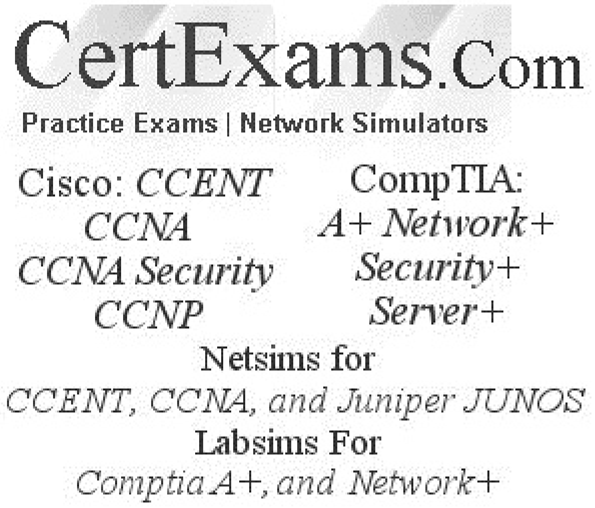
The architecture uses Cisco's Software-Defined Access (SD-Access) feature, which provides policy-based automation from the edge to the cloud through a virtual overlay network. Automating day-to-day tasks such as configuration, provisioning and troubleshooting, SD-Access is done using SD Access.

With SDA, the underlay exists to provide connectivity between the nodes in the SDA environment for the purpose of supporting VXLAN tunnels in the overlay network. VXLAN, short for Virtual Extensible LAN is a flexible encapsulation protocol used for creating tunnels (overlays)

Cisco DNA Center includes northbound REST API along with a series of southbound APIs. For most of network engineers, the northbound API matters most, because as the user of SDA networks, you interact with SDA using Cisco DNA Center's northbound REST API or the GUI interface.

Previous Contents Next

CCNP ENCOR Cram Notes Contents



CCNP ENCOR 350-401 Exam Cram Notes

I. Architecture

3. Explain the working principles of the Cisco SD-WAN solution

3.1 SD-WAN control and data planes elements

vManage Network Management System (NMS): The vManage NMS provides unified access via network management system (NMS) GUI. NMS GUI is used to configure and manage the full SD-WAN solution. It enables centralized provisioning and simplifies network changes.

The Cisco SD-WAN solution has four main components and an optional analytics service:

vManage Network Management System (NMS): This is a single pane of glass (GUI) for managing the SD-WAN solution. vSmart controller: This is the brains of the solution.

SD-WAN routers: SD-WAN involves both vEdge and cEdge routers.

vBond orchestrator: This authenticates and orchestrates connectivity between SD-WAN routers and vSmart controllers.

vAnalytics: This is an optional analytics and assurance service.

3.2 Traditional WAN and SD-WAN solutions

1. Traditional WAN : Traditional network is based on completely hardware network devices which mostly rely on Multi Protocol Label Switching (MPLS) for resilient and efficient network traffic flow. Number of hardware devices are installed along with proprietary circuits to route IP services to their intended clients. IT teams gives a lot great effort to manage the network as it involves layers of underlying hardware installed.

Scaling of traditional network is difficult as it needs a proper advanced planning along with required network infrastructure to set up and run. A Traditional connects many Local Area Networks (LANs) and Virtual Private Networks (VPNs) and it is limited to enterprise, branch, and data center. It allows to prioritize your data, voice, and video traffic on network. Security issues and management difficulties are the major problems in traditional WAN now a days.

2. Software Defined Wide Area Network (SD WAN) : SD WAN stands for Software Defined Wide Area Network which is a software defined approach to manage Wide Area Network. In SD WAN software controls everything starting from connectivity to management and providing service. It is a virtual network approach which combines traditional WAN technologies, such as MPLS, LTE and broadband connections.

SD WAN is good for global enterprises as it provides a better and secure application performance as well as optimized cloud connectivity and simplified management. Means in the cloud centric world SD WAN are more preferable than traditional WAN. Software Defined Network (SDN) is utilized which helps in determining the optimal way of routing.

4. Explain the working principles of the Cisco SD-Access solution

4.1 SD-Access control and data planes elements

The Cisco SD-Access fabric is one of the main components of the Cisco Digital Network Architecture (Cisco DNA). Cisco DNA is the solution for the future of intent-based networking in Cisco enterprise networks. SD-Access provides policy-based network segmentation, host mobility for wired and wireless hosts, and enhanced security as well as other benefits in a fully automated fashion. Cisco SD-Access was designed for enterprise campus and branch network environments and not for other types of network environments, such as data center, service provider, and WAN environments.

There are three basic planes of operation in the SD-Access fabric:

Control plane, based on Locator/ID Separation Protocol (LISP)

Data plane, based on Virtual Extensible LAN (VXLAN)

Policy plane, based on Cisco TrustSec

Cisco Digital Network Architecture (Cisco DNA), a software-driven platform that helps to create an intuitive and automated network. This allows network administrators to use software to execute policy and configuration changes they want to be made throughout the network. Many other operational tasks are streamlined through drag-and-drop provisioning, proactive troubleshooting, immediate remediation guidance and fast network segmentation.

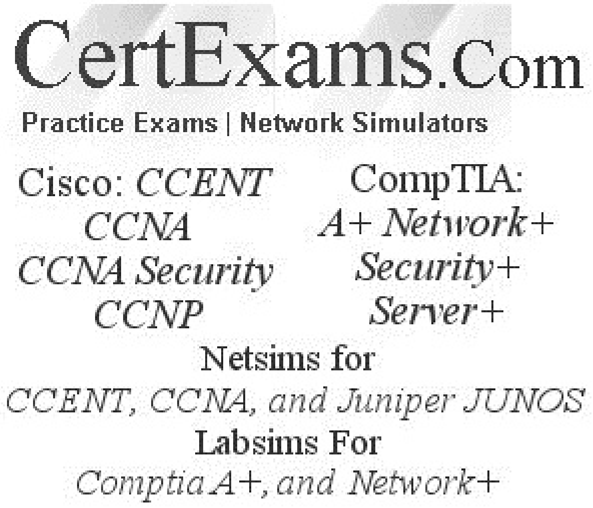
The architecture uses Cisco's Software-Defined Access (SD-Access) feature, which provides policy-based automation from the edge to the cloud through a virtual overlay network. Automating day-to-day tasks such as configuration, provisioning and troubleshooting, SD-Access is done using SD Access.

With SDA, the underlay exists to provide connectivity between the nodes in the SDA environment for the purpose of supporting VXLAN tunnels in the overlay network. VXLAN, short for Virtual Extensible LAN is a flexible encapsulation protocol used for creating tunnels (overlays)

Cisco DNA Center includes northbound REST API along with a series of southbound APIs. For most of network engineers, the northbound API matters most, because as the user of SDA networks, you interact with SDA using Cisco DNA Center's northbound REST API or the GUI interface.

Previous Contents Next

CCNP ENCOR Cram Notes Contents



CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-4.htm

I. Architecture

5.Describe concepts of wired and wireless QoS

5.1 QoS components and Policy

A switch interface can have only one policy applied at a given time in each direction. You can apply the same policy for both inbound and outbound traffic or you can apply different QoS policy for both inbound and outbound traffic on a given interface.

QoS can be quantified by the following methods:

CoS: Class of Service. CoS is applied at Layer 2 or at frames level. A 3-bit value (known as priority bits) in the range of 0 to 7 is carried along the frames in a VLAN trunk. 0 represents the lowest priority, and 7 represents the highest priority.

CoS: Class of Service. CoS is applied at Layer 2 or at frames level. A 3-bit value (known as priority bits) in the range of 0 to 7 is carried along the frames in a VLAN trunk. 0 represents the lowest priority, and 7 represents the highest priority.

IP Precedence: IP Precedence is a 3-bit value represented in the ToS (Type of Service) byte of Layer 3 IP packets. Here also, value 0 represents the lowest priority and 7 represent the highest priority.

DSCP: DSCP stands for Differentiated Service Code Point. DSCP consists of a 3-bit Selector, and a 3-bit Drop Precedence value. DSCP is backward compatible with IP Precedence, and works at layer 3.

QoS policy is applied to an interface. You can apply one for inbound traffic, and another for outbound traffic on the same interface.

DSCP	Codepoint Name	DSCP Bits
	Binary	Decimal
Default	000 000	0
AF11	001 010	10

AF12	001 100	12
AF13	001 110	14
AF21	010 010	18
AF22	010 100	20
AF23	010 110	22
AF31	011 010	26
AF32	011 100	28
AF41	100 010	34
AF42	100 100	36
AF43	100 110	38
EF	101 110	46

CAC: CAC mechanisms extend the capabilities of the QoS tool suite to protect voice traffic from being negatively affected by other traffic, and to keep excess voice traffic off the network. For example, if a WAN access link between the two PBXs has the bandwidth to carry only two VoIP calls, admitting a third call will impair the voice quality of all three calls. After the call is rejected, the originating gateway must find another means of handling the call.

Policing: Monitor the bit rate of the interface and discard the packet immidiately if it reaches the configured bandwidth.

Shaping: Allows excess traffic to be queued in memory buffers.

Normally Service Provider prefers Policing cause it discard the packet once reaches specific threshold, besides its not CPU intensive.

Additional notes: Call Admission Control (CAC) is a concept that applies to voice traffic only - not data traffic. CAC is a deterministic and informed decision that is made before a voice call is established and is based on whether the required network resources are available to provide suitable QoS for the new call. Though some other options such as QoS appears to be relevant answer, CAC is the best answer within the given context.

DSCP (Differentiated Services Code Point): It is associated with IPv4 and IPv6 headers.

CoS (Class of Service): It is associated with 802.1Q and used over VLAN trunk.

TID (Traffic ID): It is associated with 802.11 and used over Wi-Fi network.

EXP (EXPerimental): It is associated with MPLS label and used over MPLS WAN.

IPP (IP Precedence): It is associated with IPv4 and IPv6 headers.

Based on past experience, the following values are recommended by Cisco for interactive voice:

- Delay (one way) - 150ms or less
- Jitter - 30 ms or less
- Loss - 1% or less
- Bandwidth: 30 kbps to 320 kbps

Note that jitter is invariably smaller than the delay by a magnitude.

When migrating from internally hosted services to cloud, the following may need to be taken care of:

1. Security: The cloud services reside outside the organization, and it is possible that man-in-the-middle and other attacks might happen, particularly if you are using public Internet to connect to the Cloud. You might consider a private WAN connection for this reason.

2. Quality of Service: Usually, ISP do not provide quality of service agreement to the end users. If you organization is using time sensitive applications, connectivity via public Internet may not be desirable. In such cases, it is recommended to have a private WAN connectivity between your organization and the cloud resources.

3. SLA (Service Level Agreement): You may demand SLA from WAN providers, whereas it is difficult to negotiate the same with ISP Internet providers.

4. The cost of accessing the cloud resources via Internet is always the most cost effective solution, however, it comes with limited security and QoS. The needs of the organization are to be analyzed before making a choice.

Usually, network availability and cost are not a problem for Internet connectivity.

1.Best Effort Delivery: The best effort delivery method does not distinguish between a priority traffic and a non-priority traffic. The packets are forwarded in the order that they arrive. However, the routers or switches put their best effort to forward the packets that are received.

2.Integrated Services (IntServ) Model: The protocol that does scheduling and reserving adequate path bandwidth (end-to-end bandwidth) for application is know as Resource Reservation Protocol (RSVP). The source application requests QoS parameters through RSVP from the network devices along the route to destination. The minimum set of commonly agreed parameters is arrived at, and the source is informed of the same. RSVP enables traffic prioritization according to a pre-determined set of rules.

3.Differentiated Services Model (DiffServ): In the DiffServ model, the resources are dynamically arranged. The advantage over IntServ model is that the bandwidth utilization is more efficient in DiffServ. With IntServ, QoS is applied on a per-flow basis, whereas it is applied on a per-hop basis on DiffServ.

There are 3 basic types of QoS:

1.Best Effort Delivery: The best effort delivery method does not distinguish between a priority traffic and a non-priority traffic. The packets are forwarded in the order that they arrive. However, the routers or switches put their best effort to forward the packets that are received.

2.Integrated Services (IntServ) Model: The protocol that does scheduling and reserving adequate path bandwidth (end-to-end bandwidth) for application is know as Resource Reservation Protocol (RSVP). The source application requests QoS parameters through RSVP from the network devices along the route to destination. The minimum set of commonly agreed parameters is arrived at, and the source is informed of the same. RSVP enables traffic prioritization according to a pre-determined set of rules.

3.Differentiated Services Model (DiffServ): In the DiffServ model, the resources are dynamically arranged. The advantage over IntServ model is that the bandwidth utilization is more efficient in DiffServ. With IntServ, QoS is applied on a per-flow basis, whereas it is applied on a per-hop basis on DiffServ.

The terms are explained below:

Bandwidth - The rate at which traffic is carried by the network.

Latency - The delay in data transmission from source to destination.

Jitter - The variation in latency.

Reliability - The percentage of packets discarded by a router.

1.policy-map <policy-name>: Defines a policy map.

2.class <class-name>: Classify with a class map.

3.set ip dscp <dscp-value>: Mark the DSCP value

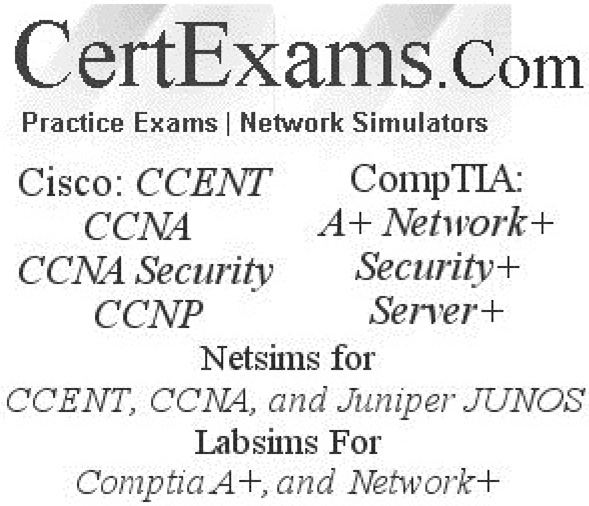
4.set ip ip precedence <ip-precedence-value>: Mark the ip precedence value.

5.trust {cos|dscp|ip-precedence}: Trust the inbound QoS information

6.service-policy [input|output] <policy-name>: Apply the policy map to an interface.

Previous Contents Next

CCNP ENCOR Cram Notes Contents



CCNP ENCOR 350-401 Exam Cram Notes

I. Architecture

6. Differentiate hardware and software switching mechanisms

6.1 Process and CEF

The command: **Switch# show ip cef** displays the entire FIB contents of a switch running CEF (Cisco Express Forwarding).

When CEF (Cisco Express Forwarding) is enabled on a switch, an FIB (Forwarding Information Base) is build that enables forwarding of arriving packets at wire speed. However, there are packets that may still need intervention by Layer 3 Engine. If an arriving packet is required to be forwarded to Layer 3 Engine, then the packet is marked as "CEF punt" and sent to Layer 3 engine for further processing.

The following are the occasions when the packet is marked as CEP punt and forwarded to Layer 3 engine:

1. An entry can not be found in the FIB

2. The FIB is full

3. The IP TTL has expired

4. The MTU is exceeded, and the packet needs to be fragmented.

5. The encapsulation type is not supported

6. Compression or encryption operation is needed etc.

A switch configured for CEF, uses adjacency tables to prepend Layer 2 addressing information. Nodes in the network are said to be adjacent if they are within a single hop from each other. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries. The adjacency table information is build from the ARP table.

When CEF (Cisco Express Forwarding) is enabled on a switch, an FIB (Forwarding Information Base) is build that enables forwarding of arriving packets at wire speed. However, there are packets that may still need intervention by Layer 3 Engine. If an arriving packet is required to be forwarded to Layer 3 Engine, then the packet is marked as "CEF punt" and sent to Layer 3 engine for further processing.

The following are the occasions when the packet is marked as CEP punt and forwarded to Layer 3 engine:

1. An entry can not be found in the FIB

2. The FIB is full

3. The IP TTL has expired

4. The MTU is exceeded, and the packet needs to be fragmented.

5. The encapsulation type is not supported

6. Compression or encryption operation is needed etc.

The first 24 bits of a multicast MAC address always start with 01:00:5E. The Ethernet MAC Address Range used for IPv4 multicast traffic is from 01:00:5e:00:00:00 to 01:00:5e:7f:ff:ff. The low-order bit of the first byte is the individual/group bit (I/G) bit, also known as the unicast/multicast bit, and when it is set to 1, it indicates that the frame is a multicast frame, and the 25th bit is always 0. The lower 23 bits of the multicast MAC address are copied from the lower 23 bits of the multicast group IP address.

Administratively scoped block (239.0.0.0/8): These addresses are limited to a local group or organization. These addresses are similar to the reserved IP unicast ranges (such as 10.0.0.0/8) and will not be assigned by the IANA to any other group or protocol. In other words, network administrators are free to use multicast addresses in this range inside of their domain without worrying about conflicting with others elsewhere on the Internet.

6.2 MAC address table and TCAM

In the multicast address space, multiple blocks of addressing are reserved for specific purposes, as shown in Table below.

Designation	Multicast Address Range
Local network control block	224.0.0.0 to 224.0.0.255
Internetwork control block	224.0.1.0 to 224.0.1.255
Ad hoc block I	224.0.2.0 to 224.0.255.255
Reserved	224.1.0.0 to 224.1.255.255

SDP/SAP block 224.2.0.0 to	224.2.0.0 to 224.2.255.255
Ad hoc block II	224.3.0.0 to 224.4.255.255
Reserved	224.5.0.0 to 224.255.255.255
Reserved	225.0.0.0 to 231.255.255.255
Source Specific Multicast (SSM) block	232.0.0.0 to 232.255.255.255
GLOP block	233.0.0.0 to 233.251.255.255
Ad hoc block III	233.252.0.0 to 233.255.255.255
Reserved	234.0.0.0 to 238.255.255.255
Administratively scoped block	239.0.0.0 to 239.255.255.255

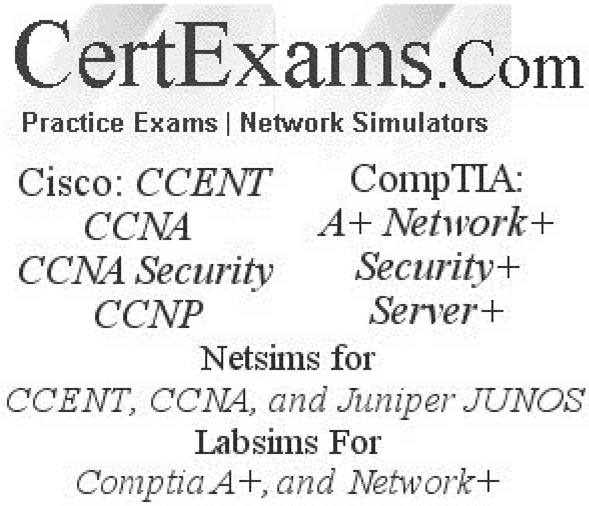
6.3 FIB vs. RIB

Routing Information Base (RIB): The Routing Information Base RIB is where all IP Routing information is stored. It is not specific to any routing protocol, rather a repository where all the routing protocols place all of their routes. Routes are inserted into the RIB whenever a routing protocol running on the router learns a new route. When a destination becomes unreachable, the route is first marked unusable and later removed from the RIB as per the specifications of the routing protocol they were learned from. The RIB lives in the control plane. The RIB table does not directly guide the forwarding, but guides the generation of the FIB table. The FIB table provides guidance for forwarding, which is irrelevant to route generation.

Forwarding Information Base (FIB): Forwarding Information Base (FIB) is used to make IP destination prefix-based switching decisions. FIB contains the interface identifier and next hop information for each reachable destination network prefix. The FIB is conceptually similar to a routing table. It maintains a mirror image of the forwarding information contained in the IP routing table. The FIB lives in the data plane. FIB entries are used to guide the actual forwarding of packets on the device. The FIB entries specify the actual interface to which packets are forwarded and the interface on which packets are transmitted.

Previous Contents Next

CCNP ENCOR Cram Notes Contents



CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-6.htm

II. Virtualization

1. Describe device virtualization technologies

1.1. Hypervisor type 1 and 2

A hypervisor is a software process that abstracts the hardware layer from the operating systems allowing multiple virtual machines to run simultaneously.

A Hypervisor also known as Virtual Machine Monitor (VMM) can be a piece of software, firmware or hardware that gives an impression to the guest machines(virtual machines) as if they were operating on a physical hardware. It allows multiple operating system to share a single host and its hardware. The hypervisor manages requests by virtual machines to access to the hardware resources (RAM, CPU, NIC etc) acting as an independent machine.

Hypervisor is mainly divided into two types namely

Type 1/Native/Bare Metal Hypervisor

Type 2/Hosted Hypervisor

Type 1 Hypervisor : This is also known as Bare Metal or Embedded or Native Hypervisor. It works directly on the hardware of the host and can monitor operating systems that run above the hypervisor. It is completely independent from the Operating System.

The hypervisor is small as its main task is sharing and managing hardware resources between different operating systems.A major advantage is that any problems in one virtual machine or guest operating system do not affect the other guest operating systems running on the hypervisor.

Type 2 Hypervisor: This is also known as Hosted Hypervisor.

In this case, the hypervisor is installed on an operating system and then supports other operating systems above it. It is completely dependent on host Operating System for its operations While having a base operating system allows better specification of policies, any problems in the base operating system a ffects the entire system as well even if the hypervisor running above the base OS is secure.

1.2 Virtual machine

A virtual machine, commonly shortened to just VM, is no different than any other physical computer like a laptop, smart phone or server. It has a CPU, memory, disks to store your files and can connect to the internet if needed. While the parts that make up your computer (called hardware) are physical and tangible, VMs are often thought of as virtual computers or software-defined computers within physical servers, existing only as code.

Virtualisation is the process of creating a software-based or "virtual" version of a computer, with dedicated amounts of CPU, memory and storage that are "borrowed" from a physical host computer - such as your personal computer and/or a remote server such as a server in a cloud provider's datacentre. A virtual machine is a computer file, typically called an image, which behaves like an actual computer. It can run in a window as a separate computing environment, often to run a different operating system or even to function as the user's entire computer experience - as is common on many people's work computers. The virtual machine is partitioned from the rest of the system, meaning that the software inside a VM cannot interfere with the host computer's primary operating system.

Here are a few ways virtual machines are used:

1. Building and deploying apps to the cloud.

2. Trying out a new operating system (OS), including beta releases.

3. Spinning up a new environment to make it simpler and quicker for developers to run dev-test scenarios.

4. Backing up your existing OS.

5. Accessing virus-infected data or running an old application by installing an older OS.

6. Running software or apps on operating systems that they were not originally intended for.

1.3. Virtual switching

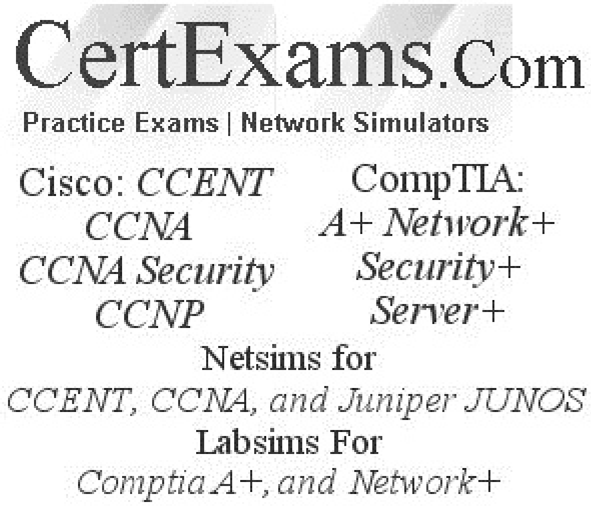
vSwitches are created under a virtualized server and enable VMs to communicate with each other and with external networks. Distributed virtual switching reduces administrative overhead by providing configuration consistency across all the hosts that are part of the distributed switch.

Virtual Network Function (VNF): VNF focus primarily on optimization of the network services, contrary to software-defined networking (SDN), which separates the control and forwarding plane for a centralized view of the network. VNF basically provides a virtual networking device that a customer can access and configure according to his security/access requirements. It is also possible that a group of virtual devices form a virtual network function, and is offered to the customer. Network Functions Virtualization (NFV) is different from VNF in the sense that the former is used by the service providers for virtualizing the SPs' networking functions.

Note: In Cisco's official version VNF represents a single virtual device. Some others use VNF and NFV interchangeably

Previous Contents Next

CCNP ENCOR Cram Notes Contents



CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-7.htm

II. Virtualization

2. Configure and verify data path virtualization technologies

2.1. VRF

Virtual routing and forwarding (VRF): VRF is an IP-based computer network technology that enables the simultaneous co-existence of multiple virtual routers (VRs) as instances or virtual router instances (VRIs) within the same router. One or multiple physical or logical interfaces may have a VRF but none of the VRFs share routes. Packets are forwarded only between interfaces on the same VRF.

VRFs work on Layer 3 of the OSI model. The independent routing instances allow users to deploy IP internet protocol addresses that overlap or are the same without conflict. Because users may segment network paths without multiple routers, network functionality improves —one of the key benefits of virtual routing and forwarding.

Advantages of Virtual Routing and Forwarding

1. Enables the virtual creation of multiple routes instate on one physical device

2. Allows users to simultaneously manage multiple routing tables

3. Can be used for MP BGP and MPLS deployments

4. Multiple VPNs for customers can use overlapping IP addresses without conflict

5. Users may segment network paths without multiple routers, improving network functionality

2.2. GRE and IPsec tunneling

IPSec uses authentication Header (AH), and Encapsulating Security Payload (ESP) protocols for transporting packets securely over the Internet. Note that PPTP and L2TP are tunneling protocols, where as IPSec provides strong encryption.

The two primary security services that are provided by IPSec are:

Authentication Header (AH), and Encapsulating Security Payload

AH provides the authentication of the sender, and ESP provides encryption of the payload

Given below are the important protocols or suite of protocols used frequently with IPSec:

ESP(Encapsulating Security Payload): ESP provides confidentiality, in addition to authentication, integrity, and anti-replay. ESP can be used alone, or in combination with AH. ESP uses HMAC-MD5 and HMAC-SHA algorithms to provide authentication functions. VPN uses Data Encryption Standard (DES), triple-DES (3DES), RC5, RC4, or Advanced Encryption Standard (AES) for encryption

Authentication Header (AH): AH provides authentication, integrity, and anti-replay for the entire packet (both the IP header and the data payload carried in the packet). It does not provide confidentiality, which means it does not encrypt the data. The data is readable, but protected from modification. AH uses the HMAC algorithms. HMAC Authentication

Hash-based message authentication code (HMAC): HMAC is a mechanism for calculating a message authentication code involving a hash function in combination with a secret key. This can be used to verify the integrity and authenticity of a message.

Other hash based algorithms include DES, triple DES, and AES.

Diffie-Hellman (DH) can be used to dynamically generate symmetrical keys to be used by symmetrical algorithms.

The following are true about IPS (Intruder Prevention System):

1. It adds some amount of delay to the network traffic, as it scans each packet for any malicious content.

2. Because the IPS is inline, it can normalize (manipulate or modify) traffic inline based on a current set of rules.

3. Unlike IDS (Intruder Detection System), an IPS works inline. So, every packet goes through IPS before being forwarded.

When a router encapsulates a packet for a GRE tunnel, it adds new header information (known as encapsulation) to the packet, which contains the remote endpoint IP address as the destination. The new IP header information allows the packet to be routed between the two tunnel endpoints without inspection of the packet's payload. After the packet reaches the remote endpoint, the GRE headers are removed (known as deencapsulation), and the original packet is forwarded out the remote router. The tunnel source interface or source IP address should not be advertised into a GRE tunnel because it would cause recursive routing issues.

The steps for configuring GRE tunnels are as follows:

Step 1:Create the tunnel interface by using the global configuration command interface tunnel tunnelnumber.

Step 2:Identify the local source of the tunnel by using the interface parameter command tunnel source {ipaddress | interface-id}. The tunnel source interface indicates the interface that will be used for encapsulation and de-encapsulation of the GRE tunnel. The tunnel source can be a physical interface or a loopback interface. A loopback interface can provide reachability if one of the transport interfaces fails.

Step 3:Identify the remote destination IP address by using the interface parameter command tunnel destination ip-address The tunnel destination is the remote router's underlay IP address toward which the local router sends GRE packets.

Step 4:Allocate an IP address to the tunnel interface to the interface by using the command ip address ipaddress subnet-mask.

GRE is a tunneling protocol that provides connectivity to a wide variety of network-layer protocols by encapsulating and forwarding packets over an IP-based network. GRE was originally created to provide transport for non-routable legacy protocols such as Internetwork Packet Exchange (IPX) across an IP network and is now more commonly used as an overlay for IPv4 and IPv6. GRE tunnels have many uses. For example,they can be used to tunnel traffic through a firewall or an ACL or to connect discontiguous networks, and they can even be used as networking duct tape for bad routing designs. Their most important application is that they can be used to create VPNs.

3 Describe network virtualization concepts

3.1 LISP

Proxy ETR (PETR): PETRs act just like ETRs(Egress Tunnel Router) but for EIDs(Endpoint Identifier) that send traffic to destinations at non-LISP sites.

Proxy ITR (PITR): An ITR but for a non-LISP site that sends traffic to EID destinations at LISP sites.

Map resolver (MR): This is a network device (typically a router) that receives LISP-encapsulated map requests from an ITR and finds the appropriate ETR to answer those requests by consulting the map server.

Map server/Map resolver (MS/MR): When MS and the MR functions are implemented on the same device, the device is referred to as an MS/MR.

LISP site: This is the name of a site where LISP routers and EIDs (Endpoint Identifiers) reside.

Ingress Tunnel Router (ITR): ITRs are LISP routers that LISP encapsulate IP packets coming from EIDs that are destined outside the LISP site.

Egress Tunnel Router (ETR): ETRs are LISP routers that deencapsulate LISP-encapsulated IP packets coming from sites outside the LISP site and destined to EIDs within the LISP site.

Tunnel router (xTR): xTR refers to routers that perform ITR and ETR functions (which is most routers).

Cisco Locator ID Separation Protocol (LISP) is a mapping and encapsulation protocol, originally developed to address the routing scalability issues on the Internet. LISP separates these two functions of an IP address into two separate functions:

Endpoint Identifier (EID): Assigned to hosts like computers, laptops, printers, etc.

Routing Locators (RLOC): Assigned to routers. We use the RLOC address to reach EIDs.

3.2 VXLAN

VXLAN allows the SD-Access fabric to support Layer 2 and Layer 3 virtual topologies (overlays) and the ability to operate over any IPbased network with built-in network segmentation (VRF instance/VN) and built-in group-based policy. The original VXLAN specification was enhanced for SD-Access to support Cisco TrustSec Scalable Group Tags (SGTs). This was accomplished by adding new fields to the first 4 bytes of the VXLAN header in order to transport up to 64,000 SGT tags.

The new fields in the VXLAN-GPO packet format include the following:

Group Policy ID: 16-bit identifier that is used to carry the SGT tag.

Group Based Policy Extension Bit (G Bit): 1-bit field that, when set to 1, indicates an SGT tag is being carried within the Group Policy ID field and set to 0 when it is not.

Don't Learn Bit (D Bit): 1-bit field that when set to 1 indicates that the egress virtual tunnel endpoint (VTEP) must not learn the source address of the encapsulated frame.

Policy Applied Bit (A Bit): 1-bit field that is only defined as the A bit when the G bit field is set to 1. When the A bit is set to 1, it indicates that the group policy has already been applied to this packet, and further policies must not be applied by network devices. When it is set to 0, group policies must be applied by network devices, and they must set the A bit to 1 after the policy has been applied.

VXLAN(Virtual Extensible LAN): VXLAN is an extension to the Layer 2 VLAN. It was designed to provide the same VLAN functionality with greater extensibility and flexibility. VXLAN offers the following benefits:

VLAN flexibility in multitenant segments: It provides a solution to extend Layer 2 segments over the underlying network infrastructure so that tenant workload can be placed across physical pods in the data center.

Higher scalability:VXLAN uses a 24-bit segment ID known as the VXLAN network identifier (VNID), which enables up to 16 million VXLAN segments to coexist in the same administrative domain.

Improved network utilization:VXLAN solved Layer 2 STP limitations. VXLAN packets are transferred through the underlying network based on its Layer 3 header and can take complete advantage of Layer 3 routing, equal-cost multipath (ECMP) routing, and link aggregation protocols to use all available paths.

A **VTEP** is virtual or physical device that maps end devices to VXLAN segments. Devices that terminate VXLAN tunnels are known as VTEPs.

VXLAN: VXLAN is an overlay data plane encapsulation scheme that was developed to address the various issues seen in traditional Layer 2 networks. It extends Layer 2 and Layer 3 overlay networks over a Layer 3 underlay network, using MAC-in-IP/UDP tunneling. Each overlay is termed a VXLAN segment

Location/ID Separation Protocol (LISP):LISP is a routing architecture and a data and control plane protocol that was created to address routing scalability problems on the Internet:

Cisco TrustSec: TrustSec is a next-generation access control enforcement solution developed by Cisco to address the growing operational challenges related to maintaining firewall rules and ACLs by using Security Group Tag (SGT) tags.

Intermediate System-to-Intermediate System (IS-IS): It is the common dynamic routing protocols found on most routing platforms today

Previous   Contents   Next

CCNP ENCOR Cram Notes Contents

CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-7.htm

II. Virtualization

2. Configure and verify data path virtualization technologies

2.1. VRF

Virtual routing and forwarding (VRF): VRF is an IP-based computer network technology that enables the simultaneous co-existence of multiple virtual routers (VRs) as instances or virtual router instances (VRIs) within the same router. One or multiple physical or logical interfaces may have a VRF but none of the VRFs share routes. Packets are forwarded only between interfaces on the same VRF.

VRFs work on Layer 3 of the OSI model. The independent routing instances allow users to deploy IP internet protocol addresses that overlap or are the same without conflict. Because users may segment network paths without multiple routers, network functionality improves—one of the key benefits of virtual routing and forwarding.

Advantages of Virtual Routing and Forwarding

1. Enables the virtual creation of multiple routes instate on one physical device

2. Allows users to simultaneously manage multiple routing tables

3. Can be used for MP BGP and MPLS deployments

4. Multiple VPNs for customers can use overlapping IP addresses without conflict

5. Users may segment network paths without multiple routers, improving network functionality

2.2. GRE and IPsec tunneling

IPSec uses authentication Header (AH), and Encapsulating Security Payload (ESP) protocols for transporting packets securely over the Internet. Note that PPTP and L2TP are tunneling protocols, where as IPSec provides strong encryption.

The two primary security services that are provided by IPSec are:

Authentication Header (AH), and Encapsulating Security Payload

AH provides the authentication of the sender, and ESP provides encryption of the payload

Given below are the important protocols or suite of protocols used frequently with IPSec:

ESP(Encapsulating Security Payload): ESP provides confidentiality, in addition to authentication, integrity, and anti-replay. ESP can be used alone, or in combination with AH. ESP uses HMAC-MD5 and HMAC-SHA algorithms to provide authentication functions. VPN uses Data Encryption Standard (DES), triple-DES (3DES), RC5, RC4, or Advanced Encryption Standard (AES) for encryption

Authentication Header (AH): AH provides authentication, integrity, and anti-replay for the entire packet (both the IP header and the data payload carried in the packet). It does not provide confidentiality, which means it does not encrypt the data. The data is readable, but protected from modification. AH uses the HMAC algorithms. HMAC Authentication

Hash-based message authentication code (HMAC): HMAC is a mechanism for calculating a message authentication code involving a hash function in combination with a secret key. This can be used to verify the integrity and authenticity of a message.

Other hash based algorithms include DES, triple DES, and AES.

Diffie-Hellman (DH) can be used to dynamically generate symmetrical keys to be used by symmetrical algorithms.

The following are true about IPS (Intruder Prevention System):

1. It adds some amount of delay to the network traffic, as it scans each packet for any malicious content.

2. Because the IPS is inline, it can normalize (manipulate or modify) traffic inline based on a current set of rules.

3. Unlike IDS (Intruder Detection System), an IPS works inline. So, every packet goes through IPS before being forwarded.

When a router encapsulates a packet for a GRE tunnel, it adds new header information (known as encapsulation) to the packet, which contains the remote endpoint IP address as the destination. The new IP header information allows the packet to be routed between the two tunnel endpoints without inspection of the packet's payload. After the packet reaches the remote endpoint, the GRE headers are removed (known as deencapsulation), and the original packet is forwarded out the remote router. The tunnel source interface or source IP address should not be advertised into a GRE tunnel because it would cause recursive routing issues.

The steps for configuring GRE tunnels are as follows:

Step 1:Create the tunnel interface by using the global configuration command interface tunnel tunnelnumber.

Step 2:Identify the local source of the tunnel by using the interface parameter command tunnel source {ipaddress | interface-id}. The tunnel source interface indicates the interface that will be used for encapsulation and de-encapsulation of the GRE tunnel. The tunnel source can be a physical interface or a loopback interface. A loopback interface can provide reachability if one of the transport interfaces fails.

Step 3:Identify the remote destination IP address by using the interface parameter command tunnel destination ip-address The tunnel destination is the remote router's underlay IP address toward which the local router sends GRE packets.

Step 4:Allocate an IP address to the tunnel interface to the interface by using the command ip address ipaddress subnet-mask.

GRE is a tunneling protocol that provides connectivity to a wide variety of network-layer protocols by encapsulating and forwarding packets over an IP-based network. GRE was originally created to provide transport for non-routable legacy protocols such as Internetwork Packet Exchange (IPX) across an IP network and is now more commonly used as an overlay for IPv4 and IPv6. GRE tunnels have many uses. For example,they can be used to tunnel traffic through a firewall or an ACL or to connect discontiguous networks, and they can even be used as networking duct tape for bad routing designs. Their most important application is that they can be used to create VPNs.

3 Describe network virtualization concepts

3.1 LISP

Proxy ETR (PETR): PETRs act just like ETRs(Egress Tunnel Router) but for EIDs(Endpoint Identifier) that send traffic to destinations at non-LISP sites.

Proxy ITR (PITR): An ITR but for a non-LISP site that sends traffic to EID destinations at LISP sites.

Map resolver (MR): This is a network device (typically a router) that receives LISP-encapsulated map requests from an ITR and finds the appropriate ETR to answer those requests by consulting the map server.

Map server/Map resolver (MS/MR): When MS and the MR functions are implemented on the same device, the device is referred to as an MS/MR.

LISP site: This is the name of a site where LISP routers and EIDs (Endpoint Identifiers) reside.

Ingress Tunnel Router (ITR): ITRs are LISP routers that LISP encapsulate IP packets coming from EIDs that are destined outside the LISP site.

Egress Tunnel Router (ETR): ETRs are LISP routers that deencapsulate LISP-encapsulated IP packets coming from sites outside the LISP site and destined to EIDs within the LISP site.

Tunnel router (xTR): xTR refers to routers that perform ITR and ETR functions (which is most routers).

Cisco Locator ID Separation Protocol (LISP) is a mapping and encapsulation protocol, originally developed to address the routing scalability issues on the Internet. LISP separates these two functions of an IP address into two separate functions:

Endpoint Identifier (EID): Assigned to hosts like computers, laptops, printers, etc.

Routing Locators (RLOC): Assigned to routers. We use the RLOC address to reach EIDs.

3.2 VXLAN

VXLAN allows the SD-Access fabric to support Layer 2 and Layer 3 virtual topologies (overlays) and the ability to operate over any IPbased network with built-in network segmentation (VRF instance/VN) and built-in group-based policy. The original VXLAN specification was enhanced for SD-Access to support Cisco TrustSec Scalable Group Tags (SGTs). This was accomplished by adding new fields to the first 4 bytes of the VXLAN header in order to transport up to 64,000 SGT tags.

The new fields in the VXLAN-GPO packet format include the following:

Group Policy ID: 16-bit identifier that is used to carry the SGT tag.

Group Based Policy Extension Bit (G Bit): 1-bit field that, when set to 1, indicates an SGT tag is being carried within the Group Policy ID field and set to 0 when it is not.

Don't Learn Bit (D Bit): 1-bit field that when set to 1 indicates that the egress virtual tunnel endpoint (VTEP) must not learn the source address of the encapsulated frame.

Policy Applied Bit (A Bit): 1-bit field that is only defined as the A bit when the G bit field is set to 1. When the A bit is set to 1, it indicates that the group policy has already been applied to this packet, and further policies must not be applied by network devices. When it is set to 0, group policies must be applied by network devices, and they must set the A bit to 1 after the policy has been applied.

VXLAN(Virtual Extensible LAN): VXLAN is an extension to the Layer 2 VLAN. It was designed to provide the same VLAN functionality with greater extensibility and flexibility. VXLAN offers the following benefits:

VLAN flexibility in multitenant segments: It provides a solution to extend Layer 2 segments over the underlying network infrastructure so that tenant workload can be placed across physical pods in the data center.

Higher scalability:VXLAN uses a 24-bit segment ID known as the VXLAN network identifier (VNID), which enables up to 16 million VXLAN segments to coexist in the same administrative domain.

Improved network utilization:VXLAN solved Layer 2 STP limitations. VXLAN packets are transferred through the underlying network based on its Layer 3 header and can take complete advantage of Layer 3 routing, equal-cost multipath (ECMP) routing, and link aggregation protocols to use all available paths.

A **VTEP** is virtual or physical device that maps end devices to VXLAN segments. Devices that terminate VXLAN tunnels are known as VTEPs.

VXLAN: VXLAN is an overlay data plane encapsulation scheme that was developed to address the various issues seen in traditional Layer 2 networks. It extends Layer 2 and Layer 3 overlay networks over a Layer 3 underlay network, using MAC-in-IP/UDP tunneling. Each overlay is termed a VXLAN segment

Location/ID Separation Protocol (LISP):LISP is a routing architecture and a data and control plane protocol that was created to address routing scalability problems on the Internet:

Cisco TrustSec: TrustSec is a next-generation access control enforcement solution developed by Cisco to address the growing operational challenges related to maintaining firewall rules and ACLs by using Security Group Tag (SGT) tags.

Intermediate System-to-Intermediate System (IS-IS): It is the common dynamic routing protocols found on most routing platforms today

Previous Contents Next

CCNP ENCOR Cram Notes Contents

CCNP ENCOR 350-401 Exam Cram Notes

III. Infrastructure

1. Describe network virtualization concepts

1.1 Layer 2

Troubleshoot static and dynamic 802.1q trunking protocols

In order to troubleshoot trunking Protocols. The first step is to understand the use case for trunking and the difference between static and dynamic trunking protocols.

Trunking is a feature that enables multiple vlans to be forwarded between two or more switches. There is an industry-standard trunking protocol call IEEE 802.1q. The prime purpose of this protocol is to enable all vendors to apply the same standards to multiple vlans when forwarding vlans to a directly-connected network device. This could be a switch, router, firewall, load balancer, server etc.

We will try to better understand this concept using 2 switches directly connected labelled switch 1 and switch 2.

Cisco also has its own proprietary trunking protocol call ISL (inter-switch Link) which means it only works with Cisco network devices.

Cisco uses a protocol called DTP (Dynamic Trunking Protocol). This protocol is installed as default on some of the Cisco Catalyst switches. This protocol enables trunk links to form automatically or with minimal configuration. The downside to this is that it is a very chatty protocol and causes increased traffic on the network. For security reasons and better network efficiency, it is a good idea to disable any unwanted chatter on the network.

By having a trunked interface This will mean that a broadcast on one switch will be extending across the trunk link to another switch creating a larger broadcast domain.

This all happens at layer 2 of the OSI model.

All vlans that traverse the link need to be tagged with the correct vlan. Once the adjoining switch takes receipt of the vlan. It will untag the vlan and forward it to the required switch port interface.

when configuring trunk interfaces. you need to ensure that you have a good understanding of the difference between the vlan you configure and the default native vlan. The native vlan carries untagged traffic and can be changed from the default to another vlan number for security and network efficiency.

To summarise.

There are two trunking standards ISL & 802.1q. They can both form links using the dynamically dynamic trunking protocol DTP.

The first key point to recognise is that for the purpose of our study, we always want our switches to trunk with the industry-standard protocol 802.1q.

DTP manages trunk negotiation only if the port on the neighbour switch is configured in a trunk mode that supports DTP.

A VLAN trunk is a point-to-point link between two network devices that carry more than a single VLAN. This allows the movement of traffic to various sections of a network that have been configured as a VLAN. By using a VLAN trunk, you can extend your VLAN across your whole network.

IEEE 802.1Q is the most common VLAN trunking protocol and is an open standard. It works by marking an Ethernet frame as it passes through a switch, tagging it as belonging to a particular VLAN.

With the VLAN Trunking Protocol (VTP), your switches can exchange VLAN configuration data. A Cisco-proprietary protocol, VTP broadcasts information about every VLAN based on its VLAN ID and name.

You can configure a switch port as a trunk link by using the switchport mode trunk command. This will set the port's interface into trunking mode. It will also negotiate the conversion between neighboring switches or links into trunk links.

A trunk can be configured on a single interface or on a group of interfaces.

The following switch port mode settings exist:

Access: Puts the Ethernet port into permanent non trunking mode and negotiates to convert the link into a nontrunk link. The Ethernet port becomes a nontrunk port even if the neighboring port does not agree to the change.

Trunk: Puts the Ethernet port into permanent trunking mode and negotiates to convert the link into a trunk link. The port becomes a trunk port even if the neighbouring port does not agree to the change.

Dynamic Auto: Makes the Ethernet port willing to convert the link to a trunk link. The port becomes a trunk port if the neighbouring port is set to trunk or dynamic desirable mode. This is the default mode for some switch ports. Dynamic Desirable - Makes the port actively attempt to convert the link to a trunk link. The port becomes a trunk port if the neighbouring Ethernet port is set to trunk, dynamic desirable or dynamic auto mode.

No–negotiate - Disables DTP. The port will not send out DTP frames or be affected by any incoming DTP frames. If you want to set a trunk between two switches when DTP is disabled, you must manually configure trunking using the (switchport mode trunk)

Troubleshoot static and dynamic EtherChannels

The following are available PAgP modes and the corresponding action:

1. ON mode does not send or receive PAgP packets. Therefore, both ends should be set to ON mode to form an EtherChannel.

2. Desirable mode tries to ask the other end in order to bring up the EtherChannel.

3. Auto mode participates in the EtherChannel only if the far end asks for participation. Two switches in auto mode will not form an EtherChannel.

The following are true about bundling ports using EtherChannel:

1. The bundled ports must have identical Spanning Tree settings

2. The bundled ports must have the same speed, duplex, and Ethernet media.

3. The bundled ports must belong to the same VLAN if not used as VLAN trunk

4. If the bundled ports represent a VLAN trunk, they must have same native VLAN, and each port should have same set of VLANs in the trunk.

The command: Switch(config)#port-channel load-balance src-ip will configure load balancing on EtherChannel switch links using source IP address.

Note that the load balancing can be done based on source IP, destination IP, both source and destination IP (XOR), source and destination MAC addresses or TCP/UDP port numbers.

The command "**switch#show etherchannel port**" can be used for verifying the channel negotiation mode of an EtherChannel.

Configure and verify common Spanning Tree Protocols (RSTP and MST)

The following are true about Rapid Spanning Tree Protocol:

1. RSTP uses 802.1D BDPU format to provide backward compatibility. However, the BDPU version is set to 2 to distinguish RSTP BDPU from 802.1D BDPUs.

2. A switch running RSTP can detect a neighbor failure in three Hello intervals or 6 seconds. This is much shorter than the normal 20 seconds max age used for 802.1D.

- RSTP uses "Root Bridge" in the same manner as that of 802.1D STP.
- 2. If a switch running RSTP receives and 802.1D BDPU, the switch begins to use 802.1D rules on that port.

1. 802.1D: This is a Spanning Tree Protocol (STP) that provides loop free switched or bridged network. Topology changes are made dynamically.

2. 802.1Q: The IEEE 802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information.

3. 802.1w: This standard is developed subsequent to 802.1D and offers faster convergence. 802.1w is known as Rapid Spanning Tree Protocol (RSTP).

4. 802.1s: IEEE 802.1s standard represents Multiple Spanning Tree protocol.

Rapid Spanning Tree Protocol (RSTP): is based on the IEEE standard 802.1w. The standard has evolved from its predecessor 802.1D. 802.1w has the advantage of faster convergence over 802.1D.

The command "**show spanning-tree**" includes information about the following:

1. VALN number

2. Root bridge priority, MAC address

3. Bridge timers (Max Age, Hello Time, Forward Delay)

Three parameters are required for defining an MST region. These are:

a. The region name

b. Configuration revision number

c. Instance to VLAN mappings

To configure Rapid Spanning Tree Protocol (RSTP) on an edge port, use the command: **Switch(config-if)# spanning-tree portfast**

To enable Multiple Spanning Tree (MST) on a switch, use the command : **Switch(config)# spanning-tree mode mst**

To enter MST configuration mode on a switch, use the command: **Switch(config)# spanning-tree mst configuration**

1. The instance 0 of MST corresponds to Internal Spanning Tree (IST).

2. By default all VLANs within an MST region belong to IST

3. MST and PVST+ are interoperable.

4. IST of MST corresponds to CST of 802.1Q

The advantages of Common Spanning Tree (CST) approach to VLAN implementation are fewer BPDUs and less processing overhead. Remember that in PVST, each VLAN has a separate instance of STP running.

The disadvantages of CST implementation are sub-optimal root bridge (since there will be only one root bridge for all VLANs, which may not be place optimally for some VLANs), and possibly, longer convergence times.

PVST+ implementation of Spanning-Tree interoperates with 802.1Q compliant switches, that are using Common Spanning Tree (CST) protocol.

If you have enabled RSTP protection features, the following command lists the ports that have been labeled as having inconsistent state:

show spanning-tree inconsistentports

The following command enables you to look at reasons for inconsistencies: **show spanning-tree interface <type> <mod>/<num> [detail]**

To configure Rapid Spanning Tree Protocol (RSTP) on an edge port, use the command **Switch(config-if)#spanning-tree portfast.**

To enable Multiple Spanning Tree (MST) on a switch, use the command **Switch(config)#spanning-tree mode mst**

To enter MST configuration mode on a switch, use the command **Switch(config)#spanning-tree mst configuration**

RSTP defines port states according to what the port does with the incoming frames. The allowed port states are as given below:

a. Discarding: The incoming frames are discarded. No MAC addresses are learned.

b. Learning: The incoming frames are dropped, but MAC addresses are learned.

c. Forwarding: The incoming frames are forwarded according to the learned MAC addresses.

Given below are some of the important characteristics of SPAN/RSPAN:

1. You can configure SPAN sessions on disabled ports

2. The switch does not support a combination of local SPAN and RSPAN in a single session.

3. You can run both a local SPAN and an RSPAN source session in the same switch stack.

4. Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.

5. The monitored port cannot be a destination port. In other words, a destination port cannot be monitored.

6. You can monitor multiple source ports in a single session.

7. Source port can be an access port, trunk port, or voice VLAN port.

8. If a destination port belongs to a source VLAN, it is excluded from the source list and is not monitored.

9. You can monitor only Ethernet VLANs.

10. The destination port does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).

11. The destination port can participate in only one SPAN session at a time (a destination port in one SPAN session cannot be a destination port for a second SPAN session).

1.2 Layer 3

Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. linked state, load balancing, path selection, path operations, metrics)

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

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

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

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

Configure and verify simple OSPF environments, including multiple normal areas, summarization, and filtering (neighbor adjacency, point-to-point and broadcast network types, and passive interface)

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

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

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

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

The router is an ABR (Area Border Router) since it connects two OSPF areas. Area 2 is configured as stubby and not totally stubby. To configure an area as totally stubby, use the command "area no-summary"

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

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

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

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

Configure and verify eBGP between directly connected neighbors (best path selection algorithm and neighbor relationships)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. In the example, RouterA and RouterB are running eBGP. The correct syntax for establishing neighbor relationship is:

router bgp 100
neighbor 175.23.1.2 remote-as 200

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

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

Previous Contents Next

CCNP ENCOR Cram Notes Contents

CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-9.htm

III. Infrastructure

1. Describe network virtualization concepts

1.3 Wireless

Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference noise,band and channels, and wireless client devices capabilities

SNR (Signal-to-Noise Ratio) is a ratio based value that evaluates your signal based on the noise being seen.SNR is comprised of 2 values and is measured as a positive value between 0db and 120db and the closer it is to 120db the better: signal value and noise value typically these are expressed in decibels (db).

RSSI (Received signal strength indication) will look at the Signal (Also known as RSSI) first this value is measured in decibels from 0 (zero) to -120 (minus 120) now when looking at this value the closer to 0 (zero) the stronger the signal is which means it's better, typically voice networks require a -65db or better signal level while a data network needs -80db or better.

Normal range in a network would be -45db to -87db depending on power levels and design; since the signal is affected by the APs transmit power & antenna as well as the clients antenna.

Signal strength (RSSI, “signal strength”, Signal/Noise Ratio.) It’s generally best to focus on RSSI

EIRP (Effective Isotropic Radiated Power) is the actual amount of signal leaving the antenna and is a value measured in db that is based on 3 things: Transmit Power (db), Cable Loss (db), & Antenna Gain (dbi). To determine EIRP follow this equation: Transmit Power - Cable Loss + Antenna Gain = EIRP.

EXAMPLE: We have a AP 124 access points running at full power with a 6dbi antenna on the 802.11a radio and a 2.5dbi antenna on the 802.11bg radio.

802.11a EIRP = 17db (40mw) - 0db + 6dbi = 23db = 200mw of actual output power

802.11bg EIRP = 20db (100mw) - 0db + 2.5dbi = 22.5db = 150mw (approx.) of actual output power, based on the example above in theory if you were to measure it right at the antenna you could get an RSSI of -23 or -22.5 respectively.

Free Space Path Loss is a measure of how much signal power you lose over a given distance typically you lose about 0.020 db per foot in an outdoor or wide open office; doors, walls, glass, and etc. affect this. This is why as you walk away from an AP your signal gets weaker.

Describe AP modes and antenna types

Cisco dCloud content include support for wireless clients and devices. Wireless connectivity is provided by Cisco Access Points (APs). Client connectivity to the AP is determined by how the AP is configured.

Access Point Mode of Operation: A Cisco Access Point (AP) is configured to operate in either lightweight mode or autonomous mode.

LAP (Lightweight AP Protocol [LWAPP]): A Cisco LAP is part of the Cisco Unified Wireless Network architecture. An LAP is an AP designed to be connected to a wireless LAN controller (WLC). The WLC manages the AP configurations and firmware; therefore, the LAP cannot act independently of a WLC. This mode is sometimes called controller-based. Enterprise Networking and Security content require lightweight mode.

Autonomous AP: A Cisco IOS Software-based AP that functions independently of a WLC. This mode is sometimes called standalone. Collaboration and Customer Collaboration content require autonomous mode.

Access Point Connectivity: A Cisco AP can be included in most Cisco dCloud sessions. Cisco dCloud supports three (3) types of AP connectivity:

Embedded: The AP is integrated into the router chassis. The 819W is a common example of this type of connection.

AP behind an endpoint router: The AP is a separate physical unit connected to an Ethernet port on a Cisco dCloud configured router.

AP only: The AP is a separate physical unit connected to the network through some other means.

Note: When you are deploying the AP on your network, you must decide what mode you want to run. If you are dealing with a single location, a small office or home network, autonomous mode is recommended. If you are setting up a wireless network for a larger office space that requires more than 3 access points locally or remotely across multiple geographic locations, deploying in Lightweight mode is recommended.

On a lightweight AP, the MAC function is divided between the AP hardware and the wireless LAN controller (WLC). Therefore, the architecture is known as split-MAC.

Split-MAC Architecture: The LAP-WLC division of labor is known as a split-MAC architecture, where the normal MAC operations are pulled apart into two distinct locations. This occurs for every LAP in the network; each one must boot and bind itself to a WLC to support wireless clients. The WLC becomes the central hub that supports a number of LAPs scattered about in the network. The two devices must use a tunneling protocol between them, to carry 802.11-related messages and also client data. Remember that the AP and WLC can be located on the same VLAN or IP subnet, but they do not have to be. Instead, they can be located on two entirely different IP subnets in two different locations.

By default, a controller has a limited initial configuration, so no WLANs are defined. Before you create a new WLAN, the following parameters it will need to have:

- SSID string
- Controller interface and VLAN number
- Type of wireless security needed

Describe access point discovery and join process (discovery algorithms, WLC selection process)

The switch interfaces feeding a WLC should be configured as trunk links. Some WLCs need a single interface, others have several interfaces that should be bundled into a single EtherChannel. The WLC shown in Figure has a four-interface Gigabit EtherChannel. Note that we need to use the command "channel-group 1 mode on" because the WLC cannot negotiate an EtherChannel. Therefore, we cannot use other options like "desirable".

The EtherChannel also provides link redundancy. If one of the bundled links fail, the traffic through the failed link is distributed to other working links in the channel. The failover is transparent to the end user. Similarly traffic again flows through the restored link, as and when a link is restored.

Because the network is built with a WLC and LAPs, CAPWAP tunnels are required. One CAPWAP tunnel connects each LAP to the WLC, for a total of 32 tunnels. CAPWAP encapsulates wireless traffic inside an additional IP header, so the tunnel packets are routable across a Layer 3 network. That means the LAPs and WLC can reside on any IP subnet as long as the subnets are reachable. There is no restrictions for the LAPs and WLC to lie on the same Layer 2 VLAN or Layer 3 IP subnet.

An LAP builds a CAPWAP (Control and Provisioning of Wireless Access Points protocol) tunnel with a WLC. The CAPWAP tunneling allows the AP and WLC to be separated geographically and logically. CAPWAP communications between the controller and lightweight access points are conducted at Layer 3. Layer 2 mode does not support CAPWAP.

CAPWAP (Control and Provisioning of Wireless Access Points): CAPWAP encapsulates the data between LAP and WLC within new IP packets. The tunneled data is then switched or routed over a campus network.

CAPWAP control messages: They are used to configure the AP and manage its operation. The control messages are authenticated and encrypted so the AP is securely controlled by only the appropriate WLC,then transported over the control tunnel. Only the CAPWAP(Control and Provisioning of Wireless Access Points) control tunnel is secured by default. Client data passes over the CAPWAP data tunnel, but is optionally encrypted. DHCP requests are client data and are not encrypted by default. Finally, 802.11 beacons are sent over the air from an LAP, so they are not encrypted or transported by CAPWAP.

In a converged design, an access layer switch also functions as a WLC so that all user access (wired and wireless) converges in a single layer. Catalyst 3650, 3850, and 4500 offer converged wireless capability.

Wireless Controller ports are physical connections to the switched network infrastructure. Controller Ports are the physical ports of the device. The following are the most important Controller physical ports.

Service Port (SP): Used for initial boot function, system recovery and out of band management. If you want to configure the controller with GUI you need to connect your computer with service port.

Redundancy Port (RP): This port is used to connect another controller for redundant operations.

Distribution Ports: These ports are used for all Access Points and management traffic. A Distribution Port connects to a switch port in trunk mode. 4400 series controllers have four distribution ports and 5500 series controllers have eight distribution ports.

Console port: Used for out-of-band management, system recovery and initial boot functions.

Describe the main principles and use cases for Layer 2 and Layer 3 roaming

Mobility, or roaming, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible.

Layer2 Roaming: Layer 2 roaming, which occurs when the wireless LAN interfaces of the controllers are on the same IP subnet. When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains transparent to the user.

Layer3 Roaming: Layer 3 roaming, which occurs when the wireless LAN interfaces of the controllers are on different IP subnets. Layer 3 roaming is similar to Layer 2 roaming in that the controllers exchange mobility messages on the client roam. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains transparent to the wireless client, and the client maintains its original IP address.

Guidelines and Restrictions

If the management VLAN of one controller is present as a dynamic VLAN on another controller, the mobility feature is not supported.

If a client roams in web authentication state, the client is considered as a new client on another controller instead of considering it as a mobile client.

When the primary and secondary controller fail to ping each other’s IPv6 addresses, and they are in the same VLAN, you need to disable snooping to get the controller to ping each other successfully.

Cisco Wireless Controllers (that are mobility peers) must use the same DHCP server to have an updated client mobility move count on intra-VLAN.

Troubleshoot WLAN configuration and wireless client connectivity issues

Management interface: Used for normal management traffic, such as RADIUS user authentication, WLC-to-WLC communication, web-based and SSH sessions, SNMP, Network Time Protocol (NTP), syslog, and so on. The management interface is also used to terminate CAPWAP tunnels between the controller and its Aps.

Virtual interface: IP address facing wireless clients when the controller is relaying client DHCP requests, performing client web authentication, and supporting client mobility.

Service port interface: Bound to the service port and used for out-of-band management.

Dynamic interface: Used to connect a VLAN to a WLAN.

1.4 IP Services

Describe Network Time Protocol (NTP)

This is an example of output from the "show ntp status" command:

```
SW01#show ntp status
Clock is synchronized, stratum 2, reference is 10.4.2.254
nominal freq is 250.0000 Hz, actual freq is 250.5320 Hz, precision is 2**18
reference time is D36968F7.7E3019A9 (02:12:07.492 UTC Fri Mar 05 2020)
<output omitted>
```

From the above output, we know that the IP address of the reference is 10.4.2.254 and that the Switch SW01 has synchronized with the reference.

Configure and verify NAT/PAT

Note that the packets leaving port S0 on the NAT router should have global IP addresses. The source IP address should be within the pool allocated. In this case, only one IP address is allocated with "overload" command. Hence, the public IP 200.200.1.1 will be used as the source IP address for a packet leaving the NAT router.

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

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

where < access-list-number > is the standard access list number, and < pool-name > is the pool name.

Note that the option 'overload' specifies many to one relationship.This configuration is typically used when many hosts with private IP addresses need to access Internet through a specified globally unique IP address.

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

Static NAT: It is a one-to-one mapping between an unregistered IP address and a registered IP address. Static NAT maps an unregistered IP address to registered IP (globally unique) addresses on one-to-one basis.

The command used for this purpose is: **ip nat inside source static < local-ip > < global-ip >**

where, < local-ip > is the local IP address assigned to a host on the inside network.
< global-ip > is the globally unique IP address of an inside host as it appears to the outside world.

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

Overloading: A variation of Dynamic NAT, also known as Network Address Port Translation (NAPT) maps multiple unregistered IP addresses to a single registered IP address by multiplexing streams differentiated by the TCP/UDP port number. A special case of dynamic NAT that maps multiple unregistered IP addresses to a single registered (globally unique) IP address by using different port numbers. Dynamic NAT with overloading is also known also as PAT (Port Address Translation).

Overlapping - This occurs when your internal IP addresses belong to global IP address range that belong to another network. In such case, the internal IP addresses need to be hidden from the outside network to prevent duplication. NAT overlapping allows the use of internal global addresses by mapping them to globally unique IP addresses using static or dynamic NAT. When Overlapping is employed, the IP addresses used on the internal network are registered IP addresses utilized on another network. To avoid conflict, a NAT Table is built to translate these redundant internal addresses to a unique IP address. Vice versa, when sending packets into the private network, the registered addresses must be translated to an address unique in the network.

Enable dynamic NAT on an interface include the following:

1. Defining a standard IP access-list using the command: **access-list < access-list-number > {permit | deny} < local-ip-address >**

2. Defining an IP NAT pool for the inside network using the command: **ip nat pool < pool-name > < start-ip > < end-ip > {netmask < net-mask > | prefix-length < prefix-length >} [type-rotary]**

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

3. Mapping the access-list to the IP NAT pool by using the command: **ip nat inside source list < access-list-number > pool < pool-name >**

4. Enabling NAT on at least one inside and one outside interface using the command: **ip nat {inside | outside}**

Configure first hop redundancy protocols, such as HSRP and VRRP

The command: **standby < group-number > preempt** is used to force an interface to resume Active router state. Note that the priority of the router should be higher than the current Active router.

The correct command syntax for configuring a router as a member of an HSRP standby group is: **R(config-if)#standby < group-number > ip < virtual-ip-address >**

For group number 45 and virtual IP address of 192.32.16.5, the command is: **R(config-if)#standby 45 ip 192.32.16.5**

All routers in an HSRP standby group can send and/or receive HSRP message. Also, HSRP protocol packets are addressed to all-router address (224.0.0.2) with a TTL of 1. Note that the HSRP messages are encapsulated in the data portion of UDP packets.

An HSRP router status can be displayed by using the command: **RouterA# show standby**

The above command displays the router priority, state (active/standby), group number among other things.

Also, to enable HSRP debugging, use the command: **RouterA# debug standby**

To disable debugging, use the command: **no debug standby**

1. HSRP: Hot Standby Router Protocol (HSRP): HSRP is a Cisco proprietary protocol that offers router redundancy. Here one router is elected as active router, and another router is elected as standby router. All other routers are put in listen HSRP state. HSRP messages are exchanges using multicast destination address 244.0.0.2 to keep a router aware of all others in the group.

2. Virtual Router Redundancy Protocol (VRRP): VRRP is very similar to HSRP. VRRP is a standards based protocol and defined in RFC 2338. VRRP sends advertisements to multicast destination address 244.0.0.18 using IP protocol.

3. Gateway Load Balancing Protocol (GLBP): GLBP overcomes some of the limitations of HSRP/VRRP. Here, instead of just one active router, all routers in the group can participate and offer load balancing.

4. Server Load Balancing (SLB): SLB provides a virtual server IP address to which client machines can connect. The virtual server, in turn, is a group of real physical servers arranged in a server farm.

HSRP authentication is carried out in clear text.

Given below are the important characteristics of Virtual Router Redundancy Protocol (VRRP):

a. VRRP advertisements are sent at 1-second intervals.
b. VRRP has no mechanism for tracking interfaces to allow more capable routers to take over the master role.

c. Router priorities range from 1 to 254.
d. The default VRRP router priority is 100
e. The Virtual Router Redundancy Protocol (VRRP) is a standards-based protocol
f. The router with highest priority is called Master router

The multicast address 224.0.0.18 is used by VRRP to send advertisements. It uses IP protocol 112.

Contrast this with HSRP that uses multicast address 224.0.0.3 UDP port 1985 for sending its hello messages.

The default HSRP standby priority is 100. If the standby priorities of routers participating in HSRP are same, the router with the highest IP address becomes the Active router.

Within the standby group of routers, the router with the highest standby priority in the group becomes the active router. For example, a router with a priority of 100 will become active router over a router with a priority of 50. The active router forwards packets sent to the virtual router. It maintains its active state by using Hello messages.

Each router in a standby group can be assigned a priority value. The range of priority values is between 0 and 255 (including 0 and 255). The default priority assigned to a router in a standby group is 100. The router with numerically higher priority value will become Active router in the HSRP standby group.

The command used to set the router's priority in standby group is: **R(config-if)# standby <group-number > priority <priority-value >.**

HSRP, or Hot Standby Routing Protocol, is a Cisco proprietary protocol that allows two or more routers to work together to represent a single virtual IP address to the end-user. Among the HSRP configured routers, one will work as Active and the others (one or more) work as Standby routers. The Active and Standby routers are determined by a set of rules. Only the virtual IP address that was created within the HSRP configuration along with a virtual MAC address is known to other hosts on the network. Hosts will use the virtual IP address as their default gateway. The active router will respond to ARP requests for the virtual IP with the virtual MAC address.

When an Active router fails in HSRP environment, Standby router assumes the Active router role. This new Active router will remain as Active router even if the failed Active router comeback to service, irrespective of the priority levels.

To enable the previous Active router to resume its activity as Active router by taking over the role from a lower priority Active router, use the command: **Rtr(config-if)# standby < group-number > preempt**

Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP), which were introduced before Gateway Load Balancing Protocol (GLBP), balance the packet load per subnet.

Gateway Load Balancing Protocol (GLBP) is a Cisco proprietary solution for redundancy and load balancing in an IP network. GLBP allow automatic selection and simultaneous recovery from first hop router failures. GLBP provides load balancing over multiple (router) gateways using a single virtual IP address and multiple virtual MAC addresses. Each host is configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets.

HSRP stands for Hot Standby Routing Protocol. The following are members of HSRP group:

1. Virtual router: virtual router is what is seen by the end user device. The virtual router has its own IP and MAC addresses.

2. Active router: Forwards packets sent to the virtual router. An active router assumes the IP and MAC addresses of the virtual router.

3. Standby router: Standby router monitors the state of HSRP by using Hello massages. It assumes the role of Active router, should the current Active router fail.

Image router does not exist and is not a part of HSRP group.

The following are true about Virtual Router Redundancy protocol (VRRP):

1. VRRP will have one master router, and all other routers are in the backup state.

2. VRRP router priorities range from 1 to 254. By default, the priority is set to 100. 254 is the highest priority.

3. The MAC address of the virtual router is of the form 0000.5e00.01xx, where xx is the VRRP group number in the range 0 to 255 or 0 to ff hex.

4. The interval for VRRP advertisements is 1 second by default.

5. All VRRP routers are configured to preempt the current master router by default. The router priority should be highest for the preemption to occur.

Describe multicast protocols, such as PIM and IGMP v2/v3

There are currently five PIM operating modes:

PIM Dense Mode (PIM-DM)
PIM Sparse Mode (PIM-SM)
PIM Sparse Dense Mode
PIM Source Specific Multicast (PIM-SSM)
PIM Bidirectional Mode (Bidir-PIM)

PIM routers can be configured for PIM Dense Mode (PIM-DM) when it is safe to assume that the receivers of a multicast group are located on every subnet within the network -in other words, when the multicast group is densely populated across the network.

PIM is a multicast routing protocol that routes multicast traffic between network segments. PIM can use any of the unicast routing protocols to identify the path between the source and receivers.

PIM Distribution Trees: Multicast routers create distribution trees that define the path that IP multicast traffic follows through the network to reach the receivers. The two basic types of multicast distribution trees are source trees, also known as shortest path trees (SPTs),and shared trees.

There are 3 versions of IGMP, IGMPv1 is old and rarely used. IGMPv2 is common in most multicast networks, and IGMPv3 used by SSM.

In IGMPv2, when a receiver sends a membership report to join a multicast group, it does not specify which source it would like to receive multicast traffic from. IGMPv3 is an extension of IGMPv2 that adds support for multicast source filtering, which gives the receivers the capability to pick the source they wish to accept multicast traffic from. IGMPv3 is designed to coexist with IGMPv1 and IGMPv2.

IGMPv3 supports all IGMPv2's IGMP message types and is backward compatible with IGMPv2. The differences between the two are that IGMPv3 added new fields to the IGMP membership query and introduced a new IGMP message type called Version 3 membership report to support source filtering.

IGMPv3 is enabled by using the following command: Device(config-if)# ip igmp version 3

Enables IGMPv3 on this interface. The default version of IGMP is IGMP version 2. Version 3 is required by SSM.

Note: IGMPv3 is used to provide source filtering for Source Specific Multicast (SSM).

Internet Group Management Protocol (IGMP): IGMP snooping constrains the flooding of IPv4 multicast traffic on VLANs on a device. With IGMP snooping enabled, the device monitors IGMP traffic on the network and uses what it learns to forward multicast traffic to only the downstream interfaces that are connected to interested receivers. The device conserves bandwidth by sending multicast traffic only to interfaces connected to devices that want to receive the traffic, instead of flooding the traffic to all the downstream interfaces in a VLAN

Benefits of IGMP Snooping

Optimized bandwidth utilization:IGMP snooping's main benefit is to reduce flooding of packets. The device selectively forwards IPv4 multicast data to a list of ports that want to receive the data instead of flooding it to all ports in a VLAN.

Multicast communication is a technology that optimizes network bandwidth utilization and conserves system resources. It relies on Internet Group Management Protocol (IGMP) for its operation in Layer 2 networks and Protocol Independent Multicast (PIM) for its operation in Layer 3 networks.

Internet Group Management Protocol (IGMP):Used by a host to notify the local router that it wishes to receive (or stop receiving) multicast traffic for a given destination address or "group". 2. RFC 2236 specifies version 2 of IGMP and RFC 3376 specifies version 3 of IGMP

Protocol Independent Multicast(PIM) Used by a router to notify an upstream router that it wishes to receive (or stop receiving) multicast traffic for a given group (G).

Open Shortest Path First(OSPF):Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 .

Auto-RP is a Cisco proprietary mechanism that automates the distribution of group-to-RP mappings in a PIM network.

BSR (Bootstrap) is similar to Cisco's AutoRP, it's a protocol that automatically find the RP (Rendezvous Point) in multicast network. BSR however, is a standard and included in PIMv2, unlike AutoRP which is a Cisco proprietary protocol.

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

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

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

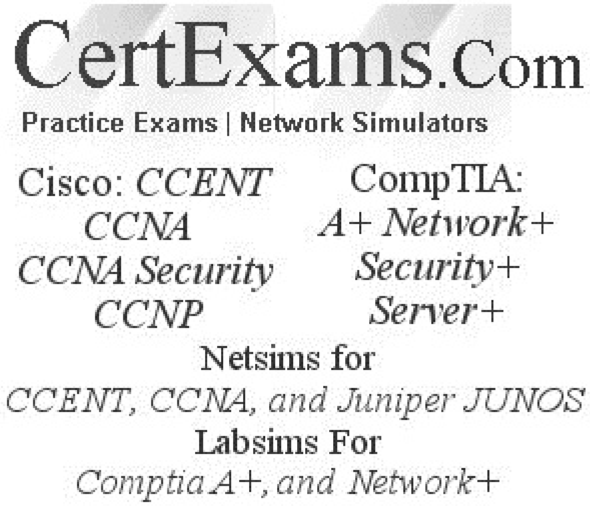
The cost of external route depends on the configuration of ASBR. There are two external packet types possible.

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

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

Previous Contents Next

CCNP ENCOR Cram Notes Contents



CCNP ENCOR 350-401 Exam Cram Notes

IV. Network Assurance

1.Diagnose network problems using tools such as debugs, conditional debugs, trace route,ping, SNMP, and syslog.

This is a syslog config command, where you want to collect the logs related to the trap level you configured via this command.

Trap level is nothing but the severity level, and lower the trap level/number higher the severity.

Trap Level	Severity
1	Alert
2	Critical
3	Error
4	Warning
5	Notificational
6	Informational
7	Debugging

Now if you configure this command: "# **logging trap 3**" then it means that logging is enabled for level 3 and lower (i.e. 3, 2, 1 & 0), in other words severity from "**Error**" (trap level-3) to "**Emergency**" (trap level-0) is logged.

Note that by default logging is enabled.

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

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

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

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

Cisco routers log messages can handle in five different ways:

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

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

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

```
CertExamsR1#terminal monitor
```

Buffered logging: This type of logging uses router's RAM for storing log messages. buffer has a fixed size to ensure that the log will not deplete valuable system memory. The router accomplishes this by deleting old messages from the buffer as new messages are added. Use the following commands to store the Syslog messages in Cisco Router's / Switch's memory. "4048" is the size of memory allocated to store Syslog messages and "0" is the severity level.

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

Syslog Server logging : The router can use syslog to forward log messages to external syslog servers for storage. This is considered to be the best best practice as there is no loss of data (huge storage capacities) and there is no overload on the router or switch as in the case of buffered logging. A syslog server also provides for centralized logging for all network devices. Use the following commands to send Syslog messages to a Syslog server, configured at 192.168.1.100.

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

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

Security Model	Security Level	Authentication	Encryption Type
SNMPv1	noAuthNoPriv	Community string	None

SNMPv2c	noAuthNoPriv	Community string	None
SNMPv3	noAuthNoPriv	User name	None
	AuthNoPriv	MD5 or SHA	None
	authPriv	MD5 or SHA	CBC-DES (DES-56)

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

There are seven SNMP protocol data units (PDU):

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

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

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

4. GetBulkRequest - enhanced version of GetNextRequest.

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

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

7. InformRequest - simultaneous messages between managers.

There are three versions of SNMP:

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

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

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

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

The advantages are given below, in brief:

1. Authentication

2. Privacy

3. Authorization and Access Control

4. Remote configuration and administration capabilities

2. Configure and verify NetFlow and Flexible NetFlow

NetFlow has two components that must be configured: NetFlow Data Capture and NetFlow Data Export. NetFlow Data Capture captures the traffic statistics. NetFlow Data Export exports the statistical data to a NetFlow collector, such as Cisco DNA Center or Cisco Prime Infrastructure.

Flexible NetFlow was created to aid in more complex traffic analysis configuration than is possible with traditional NetFlow.

Flexible NetFlow Components

1. Flow Records: Combination of key and non-key fields. There are predefined and user-defined records.

2. Flow Monitors: Applied to the interface to perform network traffic monitoring.

3. Flow Exporters: Exports NetFlow Version 9 data from the Flow Monitor cache to a remote host or NetFlow collector.

4. Flow Samplers: Samples partial NetFlow data rather than analyzing all NetFlow data.

show ip flow interface: shows the interfaces that are configured for NetFlow.

show ip flow export: command, which shows the destination for the NetFlow data to be exported to as well as statistics on the export, including any errors that may arise.

show ip cache flow: command shows the traffic flows that NetFlow is capturing.

show ip interface brief: command provides a quick status of the interfaces on the router, including their IP address, Layer 2 status, and Layer 3 status.

3.Configure and verify SPAN/RSPAN/ERSPAN

The following methods are used for implementing Spanning-Tree in a VLAN environment:

1. PVST (Per VLAN Spanning Tree): This is a Cisco proprietary method. Requires Cisco ISL encapsulation. Separate instances of Spanning-Tree are for every VLAN.

2. CST (Common Spanning Tree): This is supported by IEEE802.1Q. Here, A single instance of Spanning Tree runs for all VLANs. BPDU information is exchanged on VLAN1

3. PVST+ (Per VLAN Spanning Tree Plus): This is also a Cisco proprietary method for implementing STP in VLAN environment.

4.Configure and verify IPSLA

Given below are the basic steps involved in configuring ICMP echo-based IP SLA, assuming that you are already in appropriate configuration mode:

1. Begins configuration for an IP SLAs operation and enters IP SLA configuration mode Switch(config)# ip sla 10

2. Defines an ICMP Echo operation and enters IP SLA ICMP Echo configuration mode Switch(config-ip-sla)# icmp-echo 172.18.135.123

3. Sets the rate at which a specified IP SLAs operation repeats Switch(config-ip-sla-echo)# frequency 300

4. Exits to privileged EXEC mode - Exits to privileged EXEC mode

There are three different types of Switch Port Analyzers:

1. Local SPAN: Mirrors traffic from one or more interface on the switch to one or more interfaces on the same switch

2. Remote SPAN (or RSPAN): RSPAN allows you to monitor traffic from source ports distributed over multiple switches, which means that you can centralize your network capture devices. RSPAN works by mirroring the traffic from the source ports of an RSPAN session onto a VLAN that is dedicated for the RSPAN session. This VLAN is then trunked to other switches, allowing the RSPAN session traffic to be transported across multiple switches. The destination session collects all RSPAN VLAN traffic and sends it out the RSPAN destination port.

3. Encapsulated remote SPAN (ERSPAN): Encapsulated Remote SPAN (ERSPAN), as the name says, brings generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains. ERSPAN is a Cisco proprietary feature

The primary advantage of MST over RSTP (or Cisco's PVSTP+) is that it requires less number of Spanning Tree instances running on a switch network. Several VLANs can be grouped and assigned to an MST instance. Cisco supports a maximum of 16 MSTIs in each region. IST always exists as MSTI number 0, leaving MSTI 1 through 15 available for use. MST must be manually configured on the all switches using CLI or SNMP.

All switches in the same MST regison must have the same VLAN-to-instance mapping to exchange VLAN information.

You need to configure region name, revision number, and VLAN-to-instance mapping on each switch running MST. On enabling MST, all VLANs are mapped to instance 0 by default, MST (802.1s) uses a modified version of RSTP (802.1w). This modified version is incorporated inside of MST and provides a fast convergence time in case of a failure in the network. Note that RSTP that gets enabled with MST is different from Cisco's PVSTP+. The UplinkFast, BackboneFast, and cross-stack UplinkFast features are not supported with the RSTP and MSTP.

Three parameters are required for defining an MST region. These are:

a. The region name

b. Configuration revision number

c. Instance to VLAN mappings

5.Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management

Cisco Digital Network Architecture (DNA) offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center GUI provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience. Cisco DNA Center allows you to:

Move faster: Provision thousands of devices across your enterprise network. Act fast with centralized management and automate device deployment.

Lower costs: Reduce errors with automation. Policy-driven deployment and onboarding deliver better uptime and improved security.

Reduce risk: Predict problems early. Use actionable insights for optimal performance of your network, devices, and applications

DNA center stores network snapshot for 1 week

The code preview feature can generate a simple code snippet for several programming language so you can quickly add it into your script

Overall Health Summary dashlet contains the following:

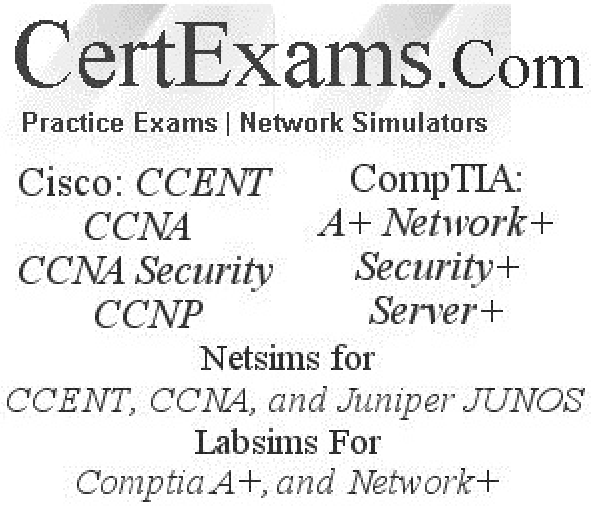
1. Network Devices area, which provides the following information:

- Network Score - Percentage of healthy (good) devices (routers, switches, wireless controllers, and access points) in your overall enterprise.
- Device Category Health Score - Provides score distribution between device categories: Router, Core, Access , Distribution, Controller and Access Point. The device category score is the percentage of healthy (good) devices in a particular device category.

2. Wired Clients and Wireless Clients area that provides score distribution between wired and wireless clients. The Wired Client score or the Wireless Client score is the percentage of healthy (good) wired or wireless client devices in your overall enterprise.

Previous Contents Next

CCNP ENCOR Cram Notes Contents



CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-11.htm

V. Security

1. Configure and verify device access control

1.1 Lines and password protection

To change the enable password, you use "**enable password password**".

To change the enable secret, you use "**enable secret password**".

Enable / Disable - Enables or Disables privileged exec mode.

There are five different types of passwords:

1. Enable Password - A global command that restricts access to privileged exec mode. This is a non-encrypted password.

2. Enable Secret - Assigns a one-way encryptographic secret password, available in versions 10.3 and up. This secret password is used instead of the enable password when it exists.

3. Virtual Terminal Password (vty password): The virtual terminal password is used for Telnet sessions into the router. The password can be changed at any time. It can be set up when you configure the router from the console. There can be five distinct passwords corresponding to each vty (vty0 to vty4) or there can be a single password for all vtys.

4. Auxiliary Password: Auxiliary password is used to set password to the auxiliary port. This port is used to access a router through a modem.

5. Console Password: Console password is used to set the console port password.

All passwords configured on an IOS device, with the exception of the passwords configured with enable secret password, are stored in clear-text in the device configuration file. This means that all that attacker needs to do to find out the passwords is to run the show running-config command.

By using "service password encryption" command in global configuration mode, the console and VTY passwords are displayed in encrypted format, making it difficult for a hacker to steal the passwords.

The following are the options considered as a security issues with current configuration of Switch A

The wording in the banner is not appropriate. It should typically read something like "do not enter if you dont belong message".

Virtual terminal lines are protected only by a password requirement.

telnet connections can be used to remotely manage the switch. (see, line vty 5 15 , and login)

The option privilege mode is protected with an unencrypted password - is not relevant as no password is configured for privilege mode.

The option Cisco user will be granted privilege level 15 by default is not correct - as the user will only be granted privilege level 15 if configured.

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

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

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

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

Similar procedure is applicable for setting vty and console passwords as well.

By default, an IOS device will disconnect a console or VTY user after 10 minutes of inactivity. You can specify a different inactivity timer using the exec-timeout MINUTES SECONDS line mode command. For example, to disconnect a console user after 90 seconds of inactivity, Use the following command:

```
R1(config)#line console 0
R1(config-line)# exec-timeout 1 30
```

After 90 seconds of inactivity, the session will be disconnected and the user will need to supply the console password to log back in:

The encryption algorithm used by service password-encryption is a weak one, it is reversed easily. The hashing algorithm used by enable secret (md5) is not so easily broken.

1.2 Authentication and authorization using AAA

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

On the client side:

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

2. Specify AAA server to be accessed by the client

t**acacs-server host 192.168.1.2 key cisco@123**

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

aaa authentication login MYAUTHLIST group tacacs+ local

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

aaa authorization exec MYAUTHORIZATIONLIST group tacacs+ local

5. Apply the method lists to a device interface

a. line vty 0 4

b. login authentication MYAUTHLIST

c. authorization exec MYUAUTHORIZATIONLIST

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

a. Enable AAA

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

c. Apply the method lists per line/per interface

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

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

The given command is: aaa authentication login CONSOLE line

In the above command:

i) The named list is CONSOLE.

ii) There is only one authentication method (line).

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

```
line con 0
exec-timeout 0 0
password cisco
```

```
login authentication CONSOLE
```

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

Creating the method list.

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

Applying the method list to the VTY lines 0-4

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

The syntax for a method list is as follows:

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

Given the AAA command: aaa authentication login default group radius local

In the above command:

1. AAA type is authentication login

2. The named list is the default one (default).

3. There are two authentication methods (group radius and local).

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

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

For recording any switch events, you need to configure and enable Accounting module of the AAA.

WLC provides a failover system between radius servers. So if the first server does not reply, it tries the second. If the username does not show up in the first radius server, that radius server will most probably send back a radius reject which means the WLC should not authenticate the user. The 2nd radius server will not be checked. Some radius servers would allow customization and would then simply to answer if the user is not found, but even then. This means that if one user is not found on the first radius server, the WLC will mark that server dead and won't try it until the 2nd WLC fails.

TACACS+ uses TCP and provides separate authentication, authorization and accounting services. Port used by TACACS+ is TCP 49. The RADIUS or TACACS+ protocol can provide a central authentication protocol to authenticate users, routers, switches or servers

WLC provides a failover system between radius servers. So if the first server does not' reply, it tries the second. If the username does not show up in the first radius server, that radius server will most probably send back a radius reject which means the WLC should not authenticate the user. The 2nd radius server will not be checked. Some radius servers would allow customization and would then simply to answer if the user is not found, but even then. This means that if one user is not found on the first radius server, the WLC will mark that server dead and won't try it until the 2nd WLC fails.

2. Configure and verify infrastructure security features

2.1 ACLs

The syntax for extended access list is given below:

access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard
destination destination-wildcard [precedence precedence]
[tos tos] [log | log-input] [time-range time-range-name]

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

We can use the statement

access-list <access-list #> [permit/deny] [protocol] host <source-ip-address> <destination-ip-address> <destination-wildcard-mask>

To permit or deny a specific host from accessing a network. Note that if we use "host" command, source wild card mask is not required.

The syntax for extended access list is given below:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard
destination destination-wildcard [precedence precedence]
[tos tos] [log | log-input] [time-range time-range-name]
```

Standard IP 1- 99 and 1300 - 1999
Extended IP 100 - 199 and 2000 - 2699

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

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

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

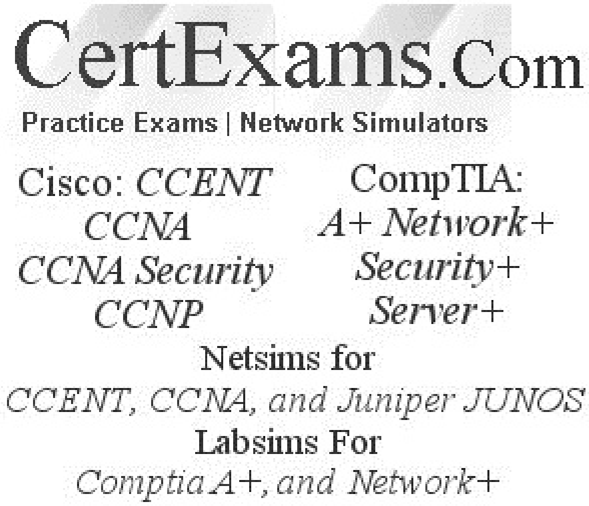
2.2. CoPP

A control plane policing (CoPP): A policy applied to the control plane of a router to protect the CPU from high rates of traffic that could impact router stability. It was created with the sole purpose of protecting the CPU or control plane of a router.

The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Previous Contents Next

CCNP ENCOR Cram Notes Contents



CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-12.htm

V. Security

3. Configure and verify wireless security features

3.1 EAP

Extensible Authentication Protocol (EAP): A standardized authentication framework defined by RFC 4187 that provides encapsulated transport for authentication parameters. EAP authentication types provide a potentially better means of securing the WLAN connection. Some of the most commonly deployed EAP authentication types include EAP-MD-5, EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-Fast, and Cisco LEAP. EAP-TTLS and PEAP requires server-side certificate where as EAP-TLS requires both client and server side certificates.

Extensible Authentication Protocol (EAP): A standardized authentication framework defined by RFC 4187 that provides encapsulated transport for authentication parameters. There are many different EAP authentication methods available, most of them based on Transport Layer Security (TLS).

Following is a description of each of the EAP authentication methods:

EAP-MD5: Uses the MD5 message-digest algorithm to hide the credentials in a hash. The hash is sent to the authentication server,where it is compared to a local hash to validate the accuracy of the credentials. EAP-MD5 does not have a mechanism for mutual authentication; in other words, the authentication server validates the supplicant, but the supplicant does not validate the authentication server to see if it is trustworthy. This lack of mutual authentication makes it a poor choice as an authentication method.

EAP-TLS: Uses the TLS Public Key Infrastructure (PKI) certificate authentication mechanism to provide mutual authentication of supplicant to authentication server and authentication server to supplicant. With EAP-TLS, both the supplicant and the authentication server must be assigned a digital certificate signed by a certificate authority (CA) that they both trust. Because the supplicant also requires a certificate, this is the most secure authentication method; however, it is also the most difficult to deploy due to the administrative burden of having to install a certificate on the supplicant side.

PEAP(Protected Extensible Authentication Protocol): In PEAP, only the authentication server requires a certificate, which reduces the administrative burden of implementing EAP. PEAP forms an encrypted TLS tunnel between the supplicant and the authentication server.

EAP-TLS: This is the most secure EAP authentication since it is essentially a TLS tunnel within another TLS tunnel. It is rarely used due to its deployment complexity because it requires certificates to be installed on the supplicants.

EAP-FAST: EAP-FAST, which is similar to PEAP, was developed by Cisco Systems as an alternative to PEAP to allow for faster re-authentications and support for faster wireless roaming. Just like PEAP, EAP-FAST forms a TLS outer tunnel and then transmits the client authentication credentials within that outer TLS tunnel. EAP-FAST includes the option of EAP chaining, which supports machine and user authentication inside a single outer TLS tunnel.

EAP-TTLS: EAP-TTLS is similar in functionality to PEAP but is not as widely supported as PEAP. One major difference between them is that PEAP only supports EAP inner authentication methods, while EAP-TTLS can support additional inner methods such as legacy Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally on the controller. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, so it removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users. Local EAP supports LEAP, EAP-FAST, EAP-TLS, PEAP authentication between the controller and wireless clients. Local EAP can use an LDAP server as its backend database to retrieve user credentials.

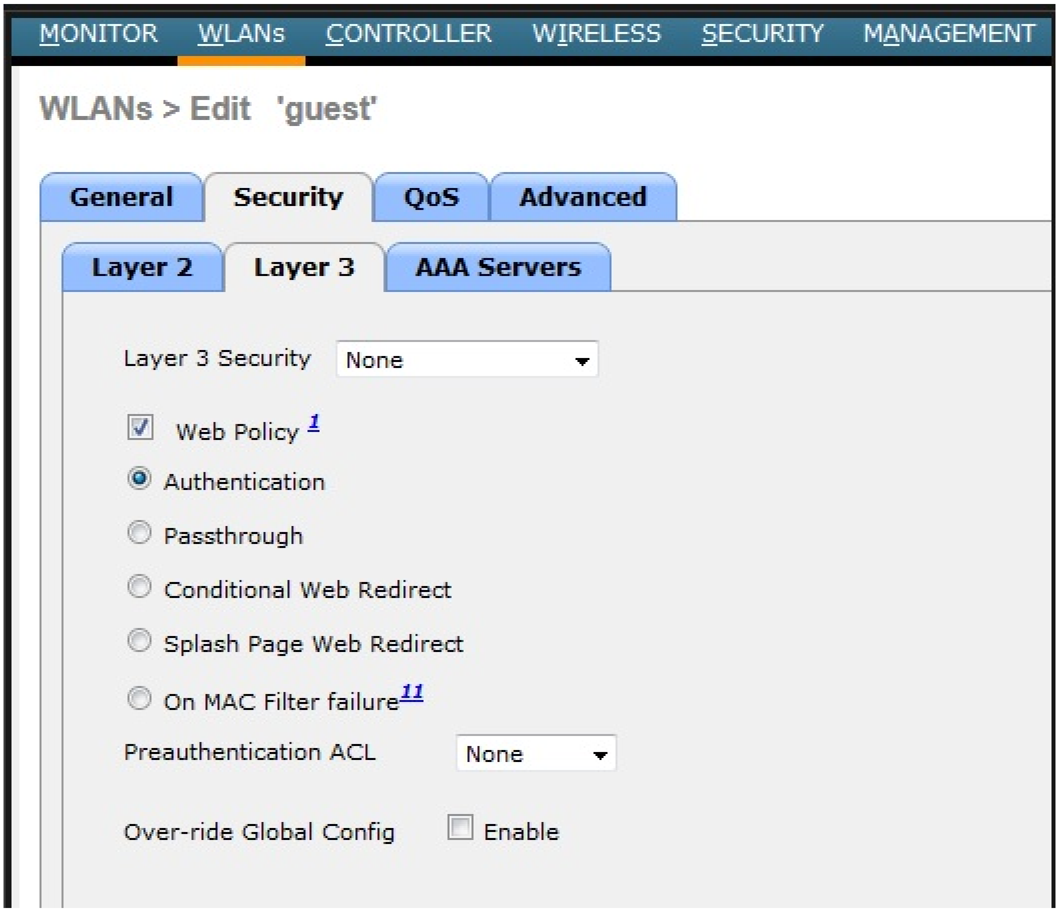
3.2.WebAuth

Web Authentication or Web Auth is a layer 3 security method that allow client to pass DHCP & DNS traffic only untill they have passed some form of authentication. This is greatly used in wireless guest access service where no client side configuration required.

WLC has four authentication policies.

1. Authentication
2. Passthrough
3. Conditional Web Redirect
4. Splash Page Web Redirect

Below shows the authentication policies on layer 3 security tab for a given WLAN of WLC with 7.0.116.0 code.



WLANs > Edit 'guest'

Layer 3 Security: None

☑ Web Policy [1]

● Authentication

○ Passthrough

○ Conditional Web Redirect

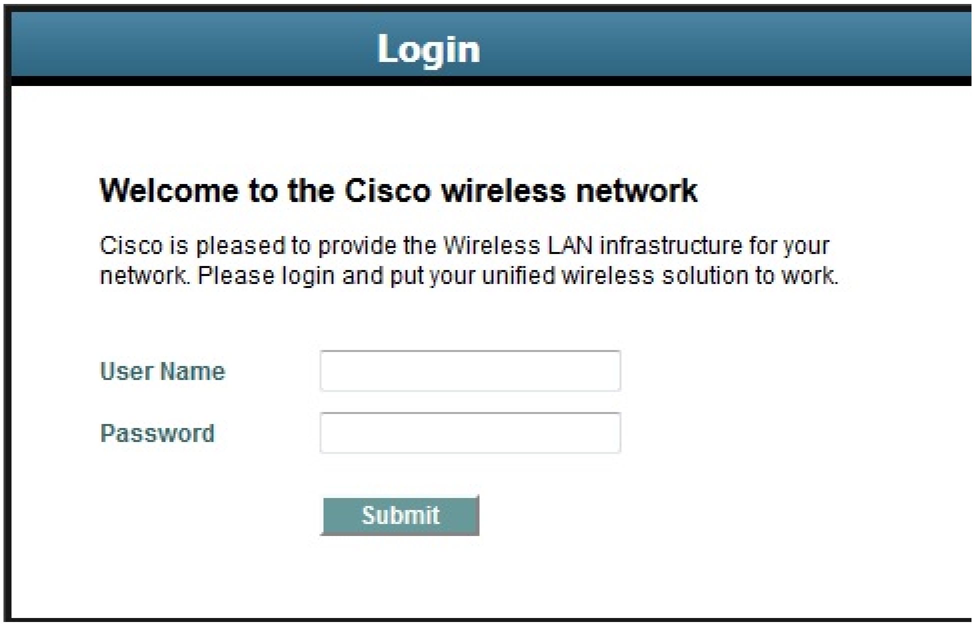
○ Splash Page Web Redirect

○ On MAC Filter failure[11]

Preauthentication ACL: None

Over-ride Global Config: □ Enable

When you enable Authentication option (as shown in the above screen capture), a guest client has to enter a username & password to gain access to the guest network. Once user get an IP & try to access an URL it authentication screen appear like this.



Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name

Password

3.3 PSK

Phase-shift keying (PSK) is a digital modulation process which conveys data by changing (modulating) the phase of a constant frequency reference signal (the carrier wave). A symmetric algorithm is one which uses the same key for encryption and decryption. Examples of symmetric algorithm are DES, 3DES, AES, and IDEA. An asymmetric algorithm is one which uses different keys for encryption and decryption. Examples of asymmetric algorithm are RSA, and Diffie-Hellman.

According to Cisco, security solutions for an organization may be broadly divided into three categories. These are:

A. Physical security: The following form physical security

a. Security cameras, and other monitoring devices
b. Security personnel
c. Climatic controls for proper temperature, humidity, etc.
d. Physical barriers

B. Administrative security: the following form administrative security

a. Maintaining log books
b. Screening employees, and security personnel
c. Maintaining security policies
d. Security awareness programs, etc.

C. Logical security

a. Authentication systems
b. Firewalls
c. Encryption schemes, etc.

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The elements of the triad are considered the three most crucial components of security. Confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

To secure wireless connections on a WLAN, you can use one of the Wi-Fi Protected Access (WPA) versions -WPA (also known as WPA1), WPA2, or WPA3. All three WPA versions support two client authentication modes, Pre-Shared Key (PSK) or 802.1x, depending on the scale of the deployment. These are also known as personal mode and enterprise mode, respectively. With personal mode, a key string must be shared or configured on every client and AP before the clients can connect to the wireless network. The pre-shared key is normally kept confidential so that unauthorized users have no knowledge of it. The key string is never sent over the air. Instead, clients and APs work through a four-way handshake procedure that uses the pre-shared key string to construct and exchange encryption key material that can be openly exchanged.

Extensible Authentication Protocol (EAP):EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication. It can integrate with the IEEE 802.1x port-based access control standard. When 802.1x is enabled, it limits access to a network medium until a client authenticates. This means that a wireless client might be able to associate with an AP but will not be able to pass data to any other part of the network until it successfully authenticates.

Open authentication: It is one of the two authentication methods from the first 802.11 standard. As the name implies, open authentication offers open authentication to a wireless network. The wireless client sends an authentication request to the AP, which the AP accepts without question. You dont need a pre-shared key or credentials. After authentication, the wireless client associates with the AP.

Wired Equivalent Privacy (WEP): WEP is a security algorithm and the second authentication option that the first 802.11 standard supports. The idea behind WEP is to make a wireless network as secure as a wired link. WEP has become obsolete and rarely used.

WPA: WPA stands for Wi-Fi Protected Access. There are two versions of WPA: WPA and WPA2. WPA is a standards-based security solution from the Wi-Fi Alliance that addresses the vulnerabilities in native WLANs and provides enhanced protection from targeted attacks.

4.Describe the components of network security design

4.1 Endpoint security

Endpoint security is an approach to secure computer networks and all client devices remotely bridged to the network. Endpoints are devices such as laptops, desktops, mobile phones, etc., that are connected across networks. These devices serve as entry points for cybercriminals looking to gain unauthorized access to sensitive assets and information.

An endpoint is a spot where two devices interact in a network. It includes a wide array of devices that employ remote connectivity. Some examples of endpoints that require security are:

- Desktops
- Laptops
- Smartphones

- IoT devices
- Workstations
- Servers
- Tablets

Endpoint security helps you protect your assets from hackers in the following ways:

1. It monitors an application's activity for any threats. It’s connected to the cloud, where its directories update dynamically to save your assets from multivector threats and zero-day attacks.

2. It secures sensitive data exchanged between partners and vendors while maintaining confidentiality.

3. It prevents third-party applications from establishing a connection with your devices and includes various security procedures to ensure comprehensive security.

4. It ensures network security by monitoring and alerting whenever the endpoint security tool spots an anomaly.

5. It protects individual devices and enterprise networks from threats and allows better flexibility and functionality in the company.

4.2 Next-generation firewall

NGFW: A next-generation firewall (NGFW) is a security appliance that processes network traffic and applies rules to block potentially dangerous traffic. NGFWs evolve and expand upon the capabilities of traditional firewalls. They do all that firewalls do, but more powerfully and with additional features.

Benefits of Next Generation Firewall

The differentiating features of next generation firewalls create unique benefits for the companies using them. NGFWs are able to block malware from entering a network, something that traditional firewalls would never be able to achieve. They are better equipped to address Advanced Persistent Threats (APTs). NGFWs can be a low-cost option for companies looking to improve their basic security because they can incorporate the work of antiviruses, firewalls, and other security applications into one solution. The features of this include application awareness, inspection services, as well as a protection system and awareness tool that benefit

4.3 TrustSec, MACsec

TrustSec is a next-generation access control enforcement solution developed by Cisco, to address the growing operational challenges related to maintaining firewall rules and ACLs by using Security Group Tag (SGT) tags. TrustSec uses SGT tags to perform ingress tagging and egress filtering to enforce access control policy.

TrustSec configuration occurs in three phases:

- Ingress classification : Ingress classification is the process of assigning SGT tags to users, endpoints, or other resources as they ingress the TrustSec network, and it can happen in one of two ways: Dynamic assignment and Static assignment.
- Propagation : Propagation is the process of communicating the mappings to the TrustSec network devices that will enforce policy based on SGT tags.
- Egress enforcement : After the SGT tags have been assigned (classification) and are being transmitted across the network (propagation), policies can be enforced at the egress point of the TrustSec network.

4.4 Network access control with 802.1X, MAB, and WebAuth

The syntax for configuring a switch port to use 802.1x is:

Switch(config-if)# dot1x port-control [force-authorized | force-un-autorized | auto]

Ports can be in one of three authorization modes. The first mode, force-authorized, and default mode. In first mode, a port is always authorized. Force-authorized mode is used when you do not want to run 802.1X on a particular port. This is typically the case when connecting to another switch, or a client PC that do not support 802.1X. The next mode, auto, is the normal 802.1X mode. A port in auto mode will not become authorized unless it receives a positive response from the authentication server. The final mode, force-unauthorized, prevents a port from becoming authorized even if the user has the appropriate credentials. This mode essentially disables the port from use by any user or device.

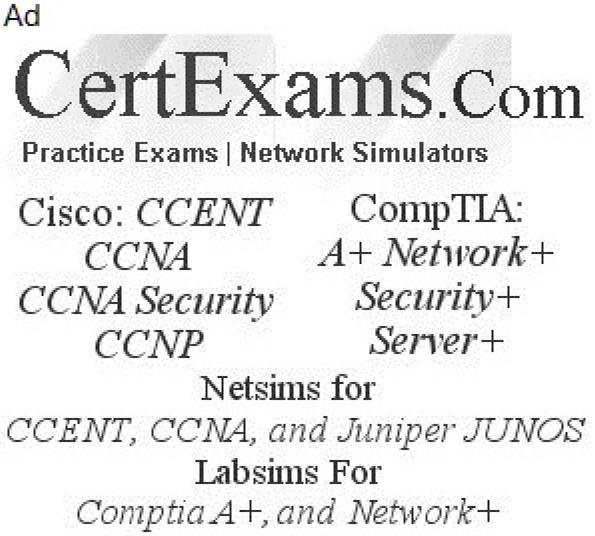
Web authentication (WebAuth) is Layer 3 security. It allows for user-friendly security that works on any station that runs a browser. It can also be combined with any pre-shared key (PSK) security (Layer 2 security policy). Web Authentication (WebAuth) presents the end user with content to read and interact with before granting access to the network. For example, it can present an Acceptable Use Policy (AUP) that the user must accept before accessing the network. It can also prompt for user credentials, display information about the enterprise, and so on. Naturally, the user must open a web browser to see the WebAuth content. WebAuth can be used as an additional layer in concert with Open Authentication, PSK-based authentication, and EAP based authentication. Web Authentication can be handled locally on the WLC for smaller environments through Local Web Authentication

(LWA). You can configure LWA in the following modes:

- LWA with an internal database on the WLC
- LWA with an external database on a RADIUS or LDAP server
- LWA with an external redirect after authentication
- LWA with an external splash page redirect, using an internal database on the WLC
- LWA with pass through, requiring user acknowledgment

Previous Contents Next

CCNP ENCOR Cram Notes Contents



CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-13.htm

VI Automation

1. Interpret basic Python components and scripts

Python has become one of the most common programming languages in terms of network programmability. It is one of the easier languages to get started with and interpret.

Ex: Set the Environment Information Needed to Access Your Lab!

The provided sample code in this repository will reference this file to get the information needed to connect to your lab backend. You provide this info here once and the scripts in this repository will access it as needed by the lab

In the above example python script starts with three quotation marks. These three quotation marks begin and end a multiple line string. A string is simply one or more alphanumeric characters. A string can comprise many numbers or letters, depending on the Python version in use.

2.Construct valid JSON encoded file.

JSON stores all its information in key/value pairs. JSON uses objects for its format. Each JSON object starts with a { and ends with a }. (These are commonly referred to as curly braces.)

For Ex:

```
        {
"student": "john",
"Section": "D",
"friend": "Lee",
“School:"VBV"
}
```

JSON: JSON short for JavaScript Object Notation, is an open-standard file format or data interchange format that uses human-readable text to transmit data objects consisting of attribute - value pairs and array data types.

Syntax for JSON objects and arrays is given briefly as below;

{ } - Object: A series of key;value pairs enclosed in a matched pair of curly brackets, with an opening left curly bracket and its matching right curly bracket.

[ ] - Array: A series of values (not key:value pairs) enclosed in a matched pair of square brackets, with an opening left square bracket and its matching right square bracket .

Key:value pairs inside objects: All key:value pairs inside an object conform to the earlier rules for key:value pairs.

Values inside arrays; All values conform to the earlier rules for formatting values (for example, double quotes around text, no quotes around numbers.

3.Describe the high-level principles and benefits of a data modeling language, such as YANG

Yet Another Next Generation (YANG): YANG (Yet Another Next Generation) is different from YAML, XML, and JSON. YANG is a data modeling language used to define data. YANG models data using a hierarchical, tree-based structure with nodes. YANG defines four nodes types. Each node has a name, and depending on the node type, the node might either define a value or contain a set of child nodes. The nodes types are:

1. leaf node - Contains a single value of a specific type

2. leaf-list node - Contains a sequence of leaf nodes

3. container node- Contains a grouping of related nodes containing only child nodes, which can be any of the four node types

4. list node - Contains a sequence of list entries, each of which is uniquely identified by one or more key leafs

YANG is a significantly refined data modeling language. It allows definition of constraints and separation of configuration and state elements. Unlike SNMP, NETCONF supports atomic transactions for configuration change. YANG Data models are very powerful in that they create a uniform way to describe data, which can be beneficial across vendors platforms. Data models allow network operators to configure, monitor, and interact with network devices holistically across the entire enterprise environment. YANG models make a clear distinction between configuration data and state information.

YANG (Yet Another Next Generation): YANG is a data modeling language used to model configuration data, state data, Remote Procedure Calls, and notifications for network management protocols

NETCONF: NETCONF is an IETF standard protocol that uses the YANG data models to communicate with the various devices on the network.

RESTCONF: An IETF draft that describes how to map a YANG specification to a RESTful interface.

4.Describe APIs for Cisco DNA Center and vManage

The DNA center provides Path trace feature that allows the operator to visualize the path of an application or service from the client through all devices and to the server. A common, and critical, troubleshooting task that normally requires 6 to 10 minutes is displayed instantly upon clicking on a client or application. Troubleshoots issues along the network path. Using this feature, you can Run a path trace from source to destination to quickly get key performance statistics for each device along the network path Identify access control lists (ACLs) that may be blocking or affecting the traffic flow.

5.Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF

The REST API (or RESTful API) is one of the Northbound APIs supported by NSO, and the client can operate NSO using HTTP(S). The REST API itself is used not only in NSO but also in other products, and because it is easy to call from Javascript, it is often used in web portals and so on. The token is used to authenticate the restful API service. Restful API does not support authorization.

RESTCONF uses HTTP methods to identify the CRUD operations defined in NETCONF for accessing the YANG-defined data.

Following are the RESTCONF operations methods

GET: The GET method is used to obtain device configuration and state data.

HEAD: The HEAD method is used to query whether device configurations and status data exist.

POST: The POST method is used by the client to create configuration or invoke a remote procedure call (RPC) operation.

PATCH: The PATCH method is used to modify configuration.

DELETE: The DELETE method is used to delete the target data and returns the specific state.

HTTP functions are similar to the functions that most applications or databases use to store or alter data - whether the data is stored in a database or within the application. These functions are called "CRUD" functions. CRUD is an acronym that stands for CREATE, READ, UPDATE, and DELETE. For example, in a SQL database, the CRUD functions are used to interact with or manipulate the data stored in the database.

CRUD Function	Action	Use Case
CREATE	Inserts data in a database or application	Updating a customer's home address in a database
READ	Retrieves data from a database or application	Pulling up a customer's home address from a database
UPDATE	Modifies or replaces data in a database or application	Changing a street address stored in a database
DELETE	Removes data from a database or application	Removing a customer from a database

Following table lists most common HTTP status codes as well as the reasons users may receive each one

HTTP Status Code	Result	Common Reason for Response
200	OK	Using GET or POST to exchange data with an API
201	Created	Creating resources by using a REST API call
400	Bad Request	Request failed due to client-side issue
401	Unauthorized	Client not authenticated to access site or API call
403	Forbidden	Access not granted based on supplied credentials
404	Not Found	Page at HTTP URL location does not exist or is hidden

6.Construct EEM applet to automate configuration, troubleshooting, or data collection

The EEM(Embedded Event manager is a software component of cisco IOS, XR, and NX-OS makes life easier for administrators by tracking and classifying events that take place on a router and providing notification options for those events. EEM allows you to automate tasks, perform minor enhancements and create workarounds.

EEM consists of three components:

Policies: Policies, or scripts, are either applets or Tcl scripts configured by the administrator.

EEM server: The EEM server is the director of EEM. When a configured event occurs, the associated action is implemented.

Event detectors: An event detector is used as a trigger, based on certain conditions. Some of these conditions include monitoring for syslog events, online insertion and removal (IOR), CLI input, and timers.

There are two independent pieces: **Applets** and **Scripting**

1. Applets are a collection of CLI commands

2. Scripts are actions coded up in TCL(interpreter language)

EEM uses event detectors and actions to provide notifications of those events:

EEM detectors can be:

1) SNMP:-Monitoring SNMP objects.

2) Syslog:-Responds to various syslog messages, allowing for matching on regular expressions.

3) Counter: Monitoring and responding to interface counter when cross threshold settings.

4) CLI events: Screening CLI input for a regular expression match.

5) None: This event detector is use to test EEM script/applet using "event manager run" command.

6) Timers :(Countdown, watchdog and CRON)

7) IP SLA and Netflows events.

Common regular expressions:

^ = Start of string

$ = End of string

. = Any single character

* = Zero or more instances

+ = One or more instance

? = Zero or one instance

EEM Actions can be:

1)Sending a email messages

2)Executing a cisco command.

3)Generating SNMP traps

4)Reloading the router

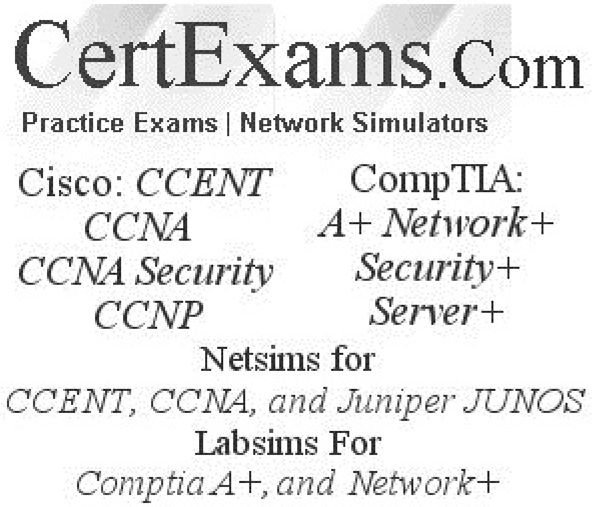
5)Generating priotized syslog messages

6)Switching to a secondary processor in a redundant platform

7)requesting system information when an event occurs(like sh tech,sh process cpu history).

Previous Contents Next

CCNP ENCOR Cram Notes Contents



CCNP ENCOR 350-401 Exam Cram Notes

examguides.com/CCNP-ENCOR/ccnp-encor-cramnotes-14.htm

VI Automation

7. Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack

Puppet and chef requires to install agent on nodes before configuration server manage it
Comparing Ansible,Puppet and chef

Action	Ansible	Puppet	Chef
Term for that lists actions	Playbook	Manifest	Recipe,Runlist
Protocol to network device	SSH,NetConf	HTTP(Rest)	HTTP(Rest)
Uses agent or agentless model	Agentless	Agent	Agent

Configuration management is the process of tracking and controlling the changes in a software with respect to its requirement, design, function, and development of a product. There are two types of configuration management approaches.

Pull Model: The nodes are dynamically updated with the configurations that are present in the server.

Push Model: Centralized server pushes the configurations on the nodes.

Puppet, Chef, and Ansible are three different tools that represent different paths to achieve a common goal of managing a large-scale server infrastructure efficiently with minimal input from the developers and system administrators. All three configuration management tools are designed to reduce the complexity of configuring distributed-infrastructure resources, enabling speed, and ensuring reliability and compliance.

Puppet: Puppet is a software configuration management tool that is mainly used by system administrators and cloud administrators. It helps an administrator to declare the system configuration and apply it across one or many systems at a time. Puppet is an open-source configuration management solution, which is built with Ruby and offers custom Domain Specific Language (DSL) and Embedded Ruby (ERB) templates to create custom Puppet language files, offering a declarative-paradigm programming approach. Puppet server can run on any Ruby-installed platform, such as Microsoft Windows Server, CentOS, Linux, or Oracle Enterprise.

Puppet Components:

Puppet Master: Puppet Master is a mechanism that handles all configuration-related activities and helps in configuring nodes using a Puppet Agent. Puppet Agents: Working machines that are managed by the Puppet Master are known as Puppet Agents.

Configuration Repository: This repository saves and pulls all nodes and server-related configurations, when required.

Facts: Facts are the details related to the node or the master machine that are used for analysing the status of any node. Changes are done on any target machine based on the facts. Puppet has pre-defined and custom facts.

Catalog: All manifest files or configurations, which are written in Puppet, are first converted into a compiled format called catalog. Later, these catalogs are applied on the target machine.

Chef: Chef is a configuration management technology, developed on the basis of Ruby DSL language and is used to automate the infrastructure provisioning. It is a flexible cloud infrastructure automation framework that allows the users to install the apps to bare metal VMs and cloud containers. A user can manage the infrastructure through the code rather than using a manual process. Chef supports multiple platforms, like AIX, RHEL/CentOS, Solaris, Ubuntu, and all Linux flavours.

Chef Components:

Nodes: A node is any machine (physical, virtual, cloud, network device, etc.) that is under management by Chef.

Workstations: A workstation is a computer where Chef Development Kit (Chef DK) is run to author cookbooks, and also to interact with the Chef server and nodes.

Knife: Knife is a Chef command-line tool that provides an interface between a local Chef repository and the Chef server.

Repository: The repository structure in which cookbooks are authored, tested, and maintained is called Chef repository (or Chef repo).

Cookbooks:A cookbook is the fundamental unit of configuration and policy distribution that defines and supports a scenario. Chef cookbooks contains recipes, attributes, custom resources, libraries, files, templates, tests, and metadata.

Ansible: Ansible is a simple open-source IT engine which automates application deployment, intra-service orchestration, cloud provisioning, and many other attributes. It is relatively easy to deploy an Ansible since it does not use any agents or custom security infrastructure. Compared with Puppet and Chef, Ansible was developed to simplify complex orchestration and configuration management tasks. Ansible platform is written in Python and it allows the users to script commands in YAML.

Ansible Components:

Control Node: Any machine with an installed Ansible can act as a control node and can run the commands invoking usr/bin/ansible or /usr/bin/ansible-playbook. Managed Nodes: Ansible can enable the management of the network devices or servers. Managed nodes sometimes called "hosts".

Inventory: An inventory is a file which contains a list of managed nodes; it is also known as a "host-file" Inventory file can contain the information like IP address of the managed nodes.

Modules: The units of code that are executed by Ansible are known as Modules. We can invoke a single module with a task or invoke several different modules in a playbook.

Tasks: The unit of action in Ansible is called a Task. It can be execute once with an ad-hoc command.

Playbooks: It is a list of tasks that runs repeatedly in an order. Playbooks can contain variables and tasks that are written in YAML (Ain't Markup Language).

SaltStack: It is an open-source platform based on Python, and it is used for managing and configuring cloud infrastructure developed to create a better tool for collecting and executing data at high speeds

Ansible: is a python-based configuration management tool that uses YAML play books to push configuration to nodes. It's an agentless solution offering wide support for network devices because it uses SSH to reach nodes. Because there is no nodes. Ansible can only push configuration to nodes.

Puppet: is a Ruby based configuration management tool that uses custom manifest files to configure devices.It requires agent to be installed on the node, so it has less network support. Puppet also doesn't support pushing configuration to nodes.Instead configuration is applied when the agent checks in. Puppet does not suport Cisco network devices that can install the puppet agent.

Chef: It is a Ruby based configuration tool that uses cook books to apply configuration.

A cookbook is the fundamental unit of configuration and policy distribution. A cookbook defines a scenario and contains everything that is required to support that scenario:

- Recipes that specify the resources to use and the order in which they are to be applied
- Attribute values
- File distributions
- Templates
- Extensions to Chef, such as custom resources and libraries

Chef Infra Client uses Ruby as its reference language for creating cookbooks and defining recipes, with an extended DSL for specific resources. Chef Infra Client provides a reasonable set of resources, enough to support many of the most common infrastructure automation scenarios; however, this DSL can also be extended when additional resources and capabilities are required. Chef is a cloud infrastructure framework. It is a tool that allows us to manage configurations, similar to Puppet and a few other tools, but Chef is is written in Ruby. Chef can help you manage your infrastructure dependencies, create folder structure (with 'knife') and bootstrap our entire system or update configurations with just a few commands.

Puppet is specially designed to manage the configuration of Linux and Windows systems. It is written in Ruby and uses its unique Domain Specific Language (DSL) to describe system configuration.

Previous Contents

CCNP ENCOR Cram Notes Contents