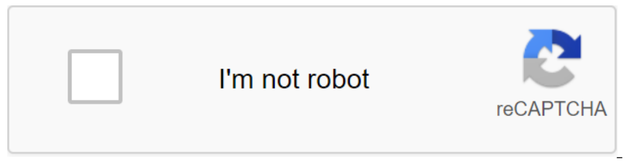
Cisco macsec configuration guide



Continue

Suppllicants are unauthorized devices that try to access the network. Authenticators are devices that control physical access to the network based on the applicant's authentication status. As shown in the following diagram, the devices are connected directly. The router acts as an EAP Supplicant and Authenticator in the port. The image below shows two EAP call streams (with a separate EAP-Session ID) on the router. The red thread portrays router 1 as a supplicant and router 2 as an authentic, and the blue stream is the opposite. When the interface is configured for 802.1x as both, the router authentication manager creates a two-session EAP session (blue and red with a separate EAP session ID) threads with the applicant, as well as the role of the authenticator, and both trigger mutual EAP-TLS authentication with a remote authentic server (AAA server/ISE/RADIUS). After the MSK flow was mutually authenticated, the router with the higher MAC address and the role of the authenticator was selected to receive the CAK. In the chart above, if the Router 1 MAC address is smaller than router 2, then the Master Session Key (MSK) derived from the EAP session (blue stream) is used as EAP-MSK for MKA (Router 1 acts as an authentic and router 2 as a supplicant). This ensures that router 1 acts as a key MKA server and router 2 is a keyless server. If the Router 2 MAC address is smaller than router 1, the MSK derived from the EAP session (red stream) is used (both routers) as EAP-MSK for MKA to obtain CAK. Do you have an account? Personalized content your products and support log in forgot your user ID and/or password? MaCsec account management is an IEEE 802.1AE standard based on Layer 2 hop-by-hop encryption that ensures the privacy and integrity of data for independent media access protocols. MACsec provides MAC-level encryption through wired networks, using out-of-range methods to encrypt keys. The MACsec Key Agreement Protocol (MKA) provides the necessary session keys and controls the necessary encryption keys. MaCsec can only provide host links (links between network access devices and endpoint devices such as pCs or IP phones). Encryption 802.1AE with a key MACsec agreement (MKA) is supported at downlink ports for encryption between routers or switches and placement devices. MACsec encrypts all data except source and Destination MAC of the Ethernet package. To provide MACsec wan or Metro Ethernet services, service providers offer transparent Level 2 services such as E-Line or E-LAN using different protocols layers such as Ethernet over Multiprotocol Label Switching (EoMPLS) and L2TPv3. The package organ in the EAP-over-LAN (EAPOL) (PDU) data block is called the MACsec PDU (MKPDU) key agreement. When MKPDU is not received from participants after 3 hearbeats (each (each 2 seconds), peers are removed from the peer list in real time For example, if the customer shuts down, the switch member continues to work MKA until 3 heartbeats have passed after receiving the last MKPDU from the customer. The MKA support provides information about tunnelings such as the VLAN tag (tag 802.1) in clear information, so that the service provider can provide multiplexing services so that multiple points to point or multi-point services can coexist on a single physical interface and are differentiated based on the now visible VLAN ID. In addition to multiplexing services, the VLAN's Clear tag also allows service providers to provide quality service (zoS) in an encrypted Ethernet package across the SP network based on the 802.1P (CoS) field, which is now visible as part of the 802.1 tag. MACsec is an IEEE 802.1AE standard based on Layer 2 hop-by-hop encryption that ensures the privacy and integrity of data for independent media access protocols. MACsec provides MAC-level encryption through wired networks, using out-of-range methods to encrypt keys. The MACsec Key Agreement Protocol (MKA) provides the necessary session keys and controls the necessary encryption keys. Encryption 802.1AE with MKA is supported on all types of links, i.e. on host links (links between network access devices and endpoint devices such as pCs or IP phones), or links connected to other switches or routers. MACsec encrypts all data except source and Destination MAC of the Ethernet package. The user also has the option to skip encryption up to 50 bytes after the MAC source and destination address. To provide MACsec wan or Metro Ethernet services, service providers offer transparent Level 2 services such as E-Line or E-LAN, using various transport layer protocols such as Ethernet over Multiprotocol Label Switching (EoMPLS) and L2TPv3. When MKPDU is not received from participants after 3 hearbeats (each hearbeat is 2 seconds), peers are removed from the peer list in real time. For example, if a customer shuts down, the switch member continues to work mKA until 3 heartbeats have passed after receiving the last MKPDU from the customer. APIC will be responsible for distributing the MACsec keychain to all nodes in the pod or in certain ports on the site. Below are the supported key MACsec chains and MACsec policy distribution supported by APIC. One user provided a key fob and policy in Pod User provided a key fob and the user provided a policy in the fabric interface Auto generated and the user provided the policy in the Pod A node can have several policies deployed for more than one tissue link. When this happens, the interface keychain on the fabric and policy are preferred Interface. The automatic trinket and associated MACsec policy is then given the least preference. APIC MACsec supports two security modes. MACsec should only provide encrypted traffic on the link while must provide allows both clean and encrypted traffic on the link. Before deploying MACsec in the necessary safe mode, the keychain should be deployed on the affected links or the links will go down. For example, a port might turn on MACsec in the required safe mode before its colleague receives a keychain, causing the link to shut down. To solve this problem it is recommended to deploy MACsec in safe mode and once all links are up then change the security mode to be provided. Please note that any change in the MACsec interface configuration will result in packages falling. The MACsec policy definition consists of a configuration specific to the key fob and configuration associated with the function function. Identify the keychain and determine the functionality of functions are placed in separate policies. Incorporating MACsec on or on the pod interface involves the deployment of a combination of key fob policy and MACsec functionality policy. Note The use of internal generated key fobs does not require the user to specify the keychain. MACsec is used to provide connections between the L3out Leaf Switch interfaces and external devices. APIC provides GUI and CLI to allow users to program MACsec keys and MacSec configurations for L3Out fabric-based L3Out interfaces based on the physical/pc/vpc interface. The user has a responsibility to ensure that external peers are programmed with the correct MacSec information. Page 2 Group Endpoint (EPG) is the most important object in the policy model. The following image shows where EPG applications are located in the Management Information Tree (MIT) and their attitude to other sites in the tenant. Figure 1. The endpoint of the EPG group is a controlled object, which is a named logical person that contains a set of endpoints. Endpoints are devices that are connected to the network directly or indirectly. They have an address (identity), location, attributes (such as a version or patch level), and can be physical or virtual. Knowing the endpoint address also allows you to access all of its other identification data. EPG is completely separated from physical and logical topology. Examples of endpoints include servers, virtual machines, connected to a store network or customers on the Internet. Membership at the END point of EPG can be dynamic or static. ACI fabric may contain the following types of EPG: App EndPoint Group (fvAEPg) Layer 2 external external network copy of the end group Layer 3 external external network copy of the end group (l3extInstP) Managing the end point of the group for out-of-range (mgmtOoB) or in the access (mgmtInB) range. EPGs contain endpoints that have common political requirements, such as security, security, Mobility Machine (VMM), zos, or layer 4 to level 7 services. Instead of setting up and managing endpoints individually, they are placed in EPG and managed as a group. Policies apply to EPG, not to individual endpoints. EPG can be statically configured by an administrator in APIC or dynamically configured by an automated system such as vCenter or OpenStack. Note When EPG uses a static binding path, the VLAN encapsulation associated with this EPG should be part of the VLAN static pool. For double-stack iPv4/IPv6 configurations, the IP address property is contained in the children's property fvStIp fvStCEp MO. Several fvStIp objects that support IPv4 and IPv6 addresses can be added under a single fvStCEp object. When ACI is updated from IPv4-only firmware to firmware versions that support IPv6, the existing IP property is copied to fvStIp MO. No matter how EPG is configured, EPG policies apply to the end point they contain. Connecting the WAN router to the fabric is an example of a configuration that uses a static EPG. To set up the WAN router connection to the fabric, the administrator sets up EPG l3extInstP, which includes any endpoints in the associated WAN subnet. The fabric learns about EPG endpoints through the detection process as endpoints of progress through their life cycle connections. Upon learning of the endpoint, the fabric applies the L3extInstP EPG policy accordingly. For example, when a customer connected to WAN initiates a TCP session with an in-app server (fvAEPg) EPG, l3extInstP EPG applies its policy to the client's endpoint before starting a connection to the EPG fvAEPg web server. When the client server TCP session ends and the communication between the client and the server stops, this endpoint no longer exists in the fabric. Note If the sheet switch is configured for static binding (leaf switches) under EPG, the following limitations apply: static binding cannot be redefined by static path. The interfaces in this switch cannot be used for route configurations of the external network (L3out). Interfaces in this switch can't be assigned IP addresses. The virtual connection to VMware vCenter is an example of a configuration that uses a dynamic EPG. Once you've set up the virtual machine control domain in vCenter fabric, it launches a dynamic EPG configuration that allows the machine's virtual endpoints to run, move on and off as needed. While tenant network policies are set apart from tissue access policies, tenant policies are not activated unless their basic access policies are available. Fabric access interfaces to external devices such as virtual machine controllers and hypervisors, hosts, routers, or Fabric Extenders (FEXs). Access policies Administrator set up port channels and virtual virtual channels, protocols such as LLDP, CDP or LACP, as well as functions such as monitoring or diagnostics. Figure 2. Association of end groups with policy access policies in the policy model, EPGs are closely related to VLANs. For traffic flow, EPG must be deployed on a sheet port with VLAN in the physical domain VMM, L2out, L3out or Fibre Channel. For more information, see the EPG-related domain profile in the policy model. The domain profile contains both the VLAN instance profile (VLAN pool) and the attached access profile (AEP), which are directly related to the application's EPG. AEP deploys EPG-related applications to all the ports to which it is attached and automates the task of assigning VLaNs. While a large data center can easily have thousands of active virtual machines on hundreds of VLANs, ACI fabric can automatically assign VLAN IDs from VLAN pools. This saves a huge amount of time compared to the trunk down VLANs in a traditional data center. Use the following guidelines to customize VLANs where epG traffic will flow. Multiple domains can share a VLAN pool, but one domain can only use one VLAN pool. To deploy multiple EPGs with the same VLAN encapsulation on one switch sheet, see the ACI versions prior to the v1.1 release, given the VLAN encapsulation card with only one EPG on the switch sheet. If there is a second EPG that has the same VLAN encapsulation on the same switch sheet, ACI picks up the bug. Starting with the release of v1.1, you can deploy multiple EPGs with the same VLAN encapsulation on this leaf switch (or FEX) in a Per Port VLAN configuration similar to the following chart: to deploy multiple EPGs using the same encapsulation number, use the following recommendations on the same switch sheet: EPG must be associated with different bridge domains. EPG should be deployed at various ports. Both the port and the EPG must be associated with the same domain that is associated with the VLAN pool, which contains the VLAN number. Ports must be configured with the portLocal VLAN area. For example, with Per Port VLAN for EPG deployed in ports 3 and 9 on the chart above, both using VLAN-5, port 3 and EPG1 are related to Dom1 (pool 1) and Port 9 and EPG2 are associated with Dom2 (Pool 2). Traffic coming from Port 3 is associated with EPG1, and traffic coming from Port 9 is associated with EPG2. This does not apply to ports configured to externally connect layer 3. If EPG has more than one physical domain with overlapping VLAN pools, avoid adding more than one domain to AEP, which is used to deploy EPG in ports. This avoids the risk of traffic distillation problems. When EPG has only one physical domain with an overlapping VLAN pool, you can link a few with one AEP. Only ports that have a vlanScope set for portlocal allow the distribution of individual (Port, VLAN) translation records in both directions of entry and exit. For this vlanScope port installed for portGlobal (by default), each VLAN used by EPG must be unique on this leaf switch. The Per Port VLAN note is not supported on multi-spanning tree (MST) interfaces, which requires VLAN IDs to be unique on a single switch sheet, and the VLAN area to be global. If you've previously configured VLANs for EPG that are deployed in the leaf switch port, and you want to reuse the same VLAN numbers for different EPGs at different ports on one switch sheet, use a process such as the following example to set them up without crashing: In this example, EPGs were previously deployed to a port associated with a domain, including a VLAN pool with a range of 9-100. You want to set up EPG with VLAN encapsulations from 9-20. Set up a new VLAN pool in another port (with a range of, for example, 9-20). Set up a new physical domain that includes leaf ports that are connected to firewalls. Link a physical domain to a VLAN pool set up in step 1. Set up the VLAN area as portLocal for the port sheet. Link the new EPG (used by the firewall in this example) to a physical domain created in step 2. Deploy EPG on port sheets. Figure 3. VLANs for two feet vPC When EPG is deployed on vPC, it must be associated with the same domain (with the same VLAN pool) that is assigned to the port of the leaf switch on two vPC legs. In this chart, EPG A is deployed on vPC, which is deployed in ports on the Leaf 1 and Leaf switch 2. The two sheet switch ports and EPG are connected to the same domain containing the same VLAN pool. Page 3 This example sets up 1/44/1, 1/44/2, 1/44/3, 1/44/4 on Switch 1017, for example, in the example below, we set up the interface 1/44/3. It also creates an infraSubPortBlk facility instead of an infraPortBlk object. infraAccPortP: attributes: dn:uni/infra/accportprof-brkout44, name:brkouttest1, rn:accportprof-brkout44, status:created, changed, children: infraHPortS: attributes: dn:uni/infra/accportprof-brkout44/hports-sel1-typ-range, name sel1, rn:hports-sel1-typ-range, status: created, changed, children: infraSubPortBlk: attributes: dn:uni/infra/accportprof-brkout44/hports-sel1-typ-range/subportblk-block2, fromPort:44, toPort:44, fromSubPort:3, toSubPort:3, name:block2, rn:subportblk-block2, status:created children: infraRsAccBaseGrp: attributes: tDn:uni/infra/funcprof/accportgrp-p1, status:created, changed , children: Management Protocol (LACP) based on vPC. This restriction is specific to LACP-based port channels. In the usual topology of the host-in-VPC, the vFC interface facing the host is tied to the vPC, and the vPC must be logically up before the vFC interface can come up. In this topology, the host will not be able to download from SAN when LACP is set up for vPC, because LACP on the host is usually sold in the host driver rather than in the adapter firmware. To download SAN, vFC interfaces facing the host are tied to members of the port channel, not the port channel itself. This binding ensures that the vFC host side comes while downloading SAN, as soon as the link to the CNA/Host Bus Adapter (HBA) comes without relying on the PORT's LACP channel to form in the first place. Figure 2. SAN Boot Topology with vPC Starting with Cisco APIC Release 4.0 (2), SAN download is supported through the host interface FEX (HIF) vPC port, as shown in the next digit. Figure 3. SAN Boot Topology with FEX Host (HIF) port vPC Multi-member port channels are not supported. If vFC is tied to a member port, the port channel may not have more than 1 member. If vFC is tied to a port channel, the port channel can only have one member port. This example suggests that the following elements have been configured: the VLAN domain tenant, the application profile, and the PORT template OF EPG A Switch101-102-1-ports-49_PolGrp In this example, the VSAN 200 is tied to the Ethernet 1/49 physical interface on Page 101 and VSAN 300 is associated with the Ethernet 1/49 physical interface on the 10222 sheet. These two interfaces are members of the virtual port channel Switch101-102-1-ports-49_PolGrp. apic1(config-leaf)# show running-config # Command: show running-config leaf 101 # Time: Sat Sep 1 12:51:23 2018 leaf 101 interface ethernet 1/49 # channel-group Switch101-102_1-ports-49_PolGrp vpc switchport trunk native vlan 5 tenant newtenant application AP1 epg epgNative port-direction downlink exit # Port-Channel inherits configuration from template port-channel Switch101-102_1-ports-49_PolGrp interface port-channel Switch101-102_1-ports-49_PolGrp exit interface vfc 1/49 # Interface inherits configuration from channel-group Switch101-102_1-ports-49_PolGrp applied to interface ethernet 1/49 switchport vsan 200 tenant newtenant application AP1 epg epg200 exit apic1(config-leaf)# show running-config # Command: show running-config leaf 102 # Time: Sat Sep 1 13:28:02 2018 leaf 102 interface ethernet 1/49 # channel-group Switch101-102_1-ports-49_PolGrp vpc switchport trunk native vlan 1 tenant newtenant application AP1 epg epgNative port-direction downlink exit # Port-Channel inherits configuration from template port-channel Switch101-102_1-ports-49_PolGrp interface port-channel Switch101-102_1-ports-49_PolGrp exit interface vfc 1/49 # Interface inherits configuration from channel-group Applied to the Interface Ethernet 1/49 switchport vsan 300 tenant newtenant application AP1 epg epg300 Page 5 Port feeds are logical interfaces in NX-OS used to aggregate bandwidth for multiple physical ports, as well as to ensure redundancy in the event of a link failure. In NX-OS, port channel interfaces are identified by user-specified numbers ranging from 1 to 4,096 unique nodes. The port channel interfaces are either explicitly configured (using the interface port channel command) or are created implicitly (using a team of channel groups). The port channel interface configuration applies to all port-member ports in the port channel. There are certain compatibility parameters (speed, for example) that cannot be configured on member ports. In the ACI model, port channels are configured as logical entities identified by name to represent a set of policies that can be assigned to set ports in one or more pieces of the sheet. This assignment creates one port channel interface in each of the sheet nodes, identified by an automatically generated number ranging from 1 to 4096 in a sheet node that may be the same or different among the nodes for the same port channel name. Membership in these port channels may also be the same or different. When creating a port channel in FEX ports, the same port channel name can be used to create the same port channel interface in each of the FEX devices attached to the sheet node. In this way, you can create up to 1 unique port channel interfaces (identified by automatically generated port channel numbers) for each node of the sheet attached to the N FEX modules. This is evidenced by the examples below. Port channels in FEX ports are identified by fex-id along with the name of the port channel (port channel interface foo fex 101, for example). If each sheet is connected to N FEX nodes, N-1s can be added on the port-channel foo sheet. Leaf ports and FEX ports cannot be part of the same port channel. Each FEX node can only have one copy of the foo port channel. Set up a port channel (global configuration). A logical foo of an entity is created, which is a set of policies with two configurations: speed and channel mode. Additional properties can be configured as needed. Note that the channel mode command is equivalent to the mode option in the NX-OS channel team. At ACI, however, this is supported for the port channel (not on the member port). apic1 (configuration) template port-channel foo apic1 (config-po-ch-if) , Switch access vlan 4 tenant ExampleCorp application Web epg webEpg apic1 (config-po-ch-if) speed 10G apic1 (config-po-ch-if) In this example the port channel is assigned to Ethernet 1/1-2 ports in FEX 101, attached to the 102 sheet node to create a port foo instance. The node of the sheet automatically generates a number, a number, 1002 to identify the port channel in the switch. This port channel number will be unique to the 102 sheet no matter how many instances of the port channel foo are created. Please note that the configuration for the FEX module to attach to the sheet node must be completed before the port channels are created using FEX ports. apic1 (config) sheet 102 apic1 (config list) interface Ethernet 101/1/1-2 apic1 (config list-if) channel-group foo In sheet 102, this port channel interface can be called the interface of the port channel foo FEX 101. apic1 (config) sheet 102 apic1 (list configuration) the interface of the port channel foo fex 101 apic1 (list configuration) closed The Configure ports for the port channel in several nodes of the sheet. In this example, the port channel foo is assigned to Ethernet 1/1-2 ports in each of the 101-103 sheet nodes. Leaf nodes automatically generate a number unique in each node (which may be the same or different among the nodes) to represent the interfaces of the port channel. apic1 (config) sheet 101-103 apic1 (config list) interface Ethernet 1/1-2 apic1 (config list-if) channel-group foo Add members of port channels. This example will add two eth1/3-4 members to the port channel in each sheet node, so that the foo port in each site will have members eth 1/1-4. apic1 (config) sheet 101-103 apic1 (config list) interface Ethernet 1/3-4 apic1 (config-list-if) channel-group foo Remove members from the port channels. This example would remove two members of eth1/2, eth1/4 from the foo port in each node sheet, so that the port foo channel in each node would have members eth 1/1, eth1/3. apic1 (configuration) sheet 101-103 apic1 (list configuration) interface eth 1/2.1/4 apic1 (configuration-list-if) no channel-group Foo Configure port channel with different members in several nodes of the sheet. This example shows how to use the same port channel foo policies to create a port channel interface in multiple sheet nodes with different member ports in each sheet. Port channel numbers in leaf nodes may be the same or different for the same port channel foo. In CLI, however, the configuration will be called the foo port interface. If the port channel is configured for FEX ports, it will be called the foo fex'lt.' foo-channel interface. apic1 (config) sheet 101 apic1 (config list) interface ethernet 1/1-2 apic1 (config-list-if) channel-group foo apic1 (config-leaf-if) exit apic1 (config list) output apic1 (config) sheet 102 apic1 (config list) Ethernet interface 1/3-4 apic1 (conf if you're a channel-group foo apic1 (config-list-if) release apic1 (config list) exit apic1 (config) sheet 103 apic1 (config-ethernet interface 1/5-8 apic1 (config-list-if), channel-group foo apic1 (configuration-list-if) , output apic1 (configuration-list) interface 101/1/1-2 apic1 (A-list configuration-if) Foo Configure Channel Group for Port Properties for LACP. This example shows how to set up port-member ports for each port's properties for LACP. </fex-id> </fex-id> In the ACI model, these commands are only allowed after the ports are members of the port channel. If the port is removed from the port channel, the configuration of these properties in the port will also be removed. apic1 (configuration) sheet 101 apic1 (list configuration) interface ethernet 1/1-2 apic1 (config-list-if) channel-group foo apic1 (config list-if) lacp port-priority 1000 apic1 (config-list-if) lacp speed to quickly adjust the administrator of the state for port channels. In this example, each of the 101-103 sheet nodes is configured to foo the port channel using the channel group command. The port channel administrator's status can be configured in each sheet using the port channel interface. In the ACI model, the status of the port channel administrator cannot be configured on a global scale. create a foo port channel in each sheet apic1 (configuration) sheet 101-103 apic1 (list configuration) Ethernet interface 1/3-4 apic1 (configuration-list-if) channel-group foo // admin status in a particular sheet apic1 (config) sheet 101 apic1 (config-list) the interface port-channel foo apic1 (config-list-if) closed Override config is very useful to assign a specific vlan domain, for example, to the port channel interfaces in each sheet when other properties are shared. customize the port-channel global configuration apic1 (configuration) interface port-channel foo apic1 (configuration-if) speed 1G apic1 (configuration-if) channel-mode active / create a port-channel foo in each sheet apic1 (config) sheet 101-103 apic1 (config list) interface ethernet 1/1-2 apic1 (config-list-if) channel-group foo // override port-channel foo in sheet 102 apic1 (config) sheet 102 apic1 (config-list) interface port-channel foo apic1 (config-list-if) speed q10G apic1 (config-list-if) channel-mode on apic1 (config-list-if) vlan-domain home-foo This example shows how to change the purpose of the port channel for ports with the help of a group of channel commands. There is no need to delete membership in the port channel before being assigned to another port channel. apic1 (config) sheet 101-103 apic1 (config list) interface Ethernet 1/3-4 apic1 (config-list-if) channel-group foo apic1 (config-list-if) channel-group bar Page 6 ACI provides the tenant's default gateway functionality that routes between ACI fabric VXlan networks. For each tenant, the fabric provides a virtual default gateway that covers all the leaf switches assigned to the tenant. It does this by entering the interface of the first sheet switch connected to the end point. Each entry interface supports the default gateway interface. All input interfaces have the same router IP address and MAC address for the tenant's subnet. ACI fabric disconnects the address of the tenant's endpoint, its ID, from the location point defined by its locator or the endpoint of the VXLAN tunnel (VTEP). Rewind inside the fabric is between VTEPs. The next figure shows the disconnected identity and location in ACI. Figure 4. Aci Aci Identity and Location VXLAN use VTEP devices to map tenants' end devices in VXLAN segments and to encapsulate and de-oxapsulate VXLAN. Each VTEP feature has two interfaces: the switch interface in the local LAN segment to support local endpoint communication by overcoming the IP interface with the IP transport network IP interface has a unique IP address that identifies the VTEP device in the transport IP network known as the VLAN infrastructure. The VTEP uses this IP address to encapsulate Ethernet footage and encapsulate packages to the transportation network via IP interface. The VTEP device also detects remote VTEPs for its VXLAN segments and learns how to remotely display MAC Address-to-VTEP through its IP interface. VTEP in ACI displays the tenant's internal MAC address or IP address to the location using a distributed map database. Once VTEP completes the review, VTEP sends the original data package encapsulated to VXLAN with the VTEP destination address on the destination sheet switch. The destination sheet switch de-encapsulates the package and sends it to the host. With this model, ACI uses a full grid, one jump, no topology cycle without the need to use a spanning-tree protocol to prevent loops. VXLAN segments are independent of the topology of the main network; on the contrary, the basic IP network between VTEPs does not depend on VXLAN overlay. It is shoeed encapsulated packages based on the external IP address header, which has the initiating VTEP as the ip address of the source and the termination of VTEP as an IP destination address. The next figure shows how routing within the tenant is done. Figure 5. Layer 3 VNIDs Transport ACI Intersubed Tenant Traffic for each VRF tenant in fabric, ACI assigns one L3 VNID. ACI transported traffic through the fabric according to the L3 VNID. When the aggression sheet is switched, ACI will send a package from L3 VNID to the VNID subnet. Traffic arriving at the input of the fabric, which is sent to the ACI fabric gateway by default, is directed to layer 3 of the VNID. This provides a very efficient rewind in the fabric for the traffic that is routed inside the tenant. For example, with this model, traffic between 2 VM belonging to the same tenant on the same physical host, but on different subnets, should only go to the input switch interface before being routed (using the minimum cost of the path) to the desired destination. ACI multiprotocol (MP-BGP) is used to distribute external routes inside the fabric. The fabric administrator provides the Autonomous System Number (AS) and identifies the spine switches that become route reflectors. Page 7 Figure 1. ACI 802.1 Tunnels with Cisco ACI and Cisco APIC release 2.2 (1x) and above, you can 802.1 tunnels on the edge of (tunnel) ports to point to many ethernet tunneling points in fabrics, with quality-of-service priorities (AIA) settings. The Dot1q tunnel is transported without tags, 802.1 is tagged, and 802.1ad double-tagged frames like-it-all throughout the fabric. Each tunnel carries traffic from one customer and is connected to one domain bridge. The ACI front ports can be part of the Dot1q tunnel. Layer 2 switches are based on the MAC (DMAC) destination, and regular MAC training is done in the tunnel. Edge-port Dot1q tunnels are supported on the second-generation Cisco Nexus 9000 switches with the EX at the end of the Switch model name. With Cisco ACI and Cisco APIC Release 2.3(x) and above, you can also customize multiple tunnels 802.1 on the same core port to transport double-tagged traffic from multiple customers, each different to the encapsulation of access configured for each tunnel 802.1. You can also disable the MAC Learning Address at 802.1 Tunnels. Both edge ports and core ports can belong to the 802.1 tunnel with access encapsulation and disconnected MAC Address Learning. Both the edges of the ports and the main ports in the Dot1q tunnels are supported by the third generation Cisco Nexus 9000 series switches with FX and FX2 at the end of the Switch model name. The terms used in this document may differ in the Cisco Nexus 9000 series documents. Table 1. 802.1 Туннель Терминология ACI Документы Cisco Nexus 9000 Серия Документы Edge Port Port Port Core Port Trunk Port Порт Следующие руководящие принципы и ограничения применяются: Слой 2 туннелирования VTP, CDP, LACP, LLDP, и STP протоколы поддерживается со следующими ограничениями: Ссылка Агрегации Протокол контроля (LACP) туннелирование функций, как ожидается, только с точки точки точки туннели. It is not supported on port channels (PCs) or virtual port channels (VPCs). Tunneling CDP and LLDP with PC or VPC is not a determinant; It depends on the link it chooses as the traffic destination. To use VTP to tunnel the Layer 2 protocol, CDP must be included in the tunnel. STP is not supported in the 802.1 tunnel domain when Layer 2 protocol tunneling is enabled and the bridge domain is deployed at the main ports of the Dot1q Tunnel. ACI sheet switches respond to STP TCN packages by flushing the endpoints in the tunnel bridge domain and flooding them into the bridge domain. CDP and LLDP tunneling with more than two interfaces flood packages on all interfaces. With Cisco APIC Release 2.3 (x) or above, the address of the MAC destination of the Layer 2 protocol packages, tunneled from edge to main ports, rewritten as 01-00-0c-cd-cd-d0, and the address of the MAC destination of the Layer 2 protocol packages, tunneled from core to edge of ports, rewritten with the default MAC address for the protocol. If the PC or VPC is the only interface in the Dot1q tunnel and it is removed and reconfigured, remove the PC/VPC association with the Dot1q tunnel and reconfigure With Cisco APIC APIC Ethertypes for two tagged frames must be 0x9100 followed by 0x8100. However, with Cisco APIC release 2.3 (x) and above, this restriction no longer applies to edge ports, the third generation Cisco Nexus switches from FX at the end of the Switch model name. For the main Ethertypes ports, the two frames tagged must be 0x8100 followed by 0x8100. You can include multiple edge ports and main ports (even through sheet switches) in the Dot1q tunnel. The edge port may only be part of one tunnel, but the main port may belong to several Dot1q tunnels. With Cisco APIC Release 2.3 (x) and above, regular EPGs can be deployed at major ports that are used in 802.1 tunnels. L3Outs are not supported on the interfaces included for the Dot1q tunnels. FEX interfaces are not supported as members of the Dot1q tunnel. Interfaces configured as breakout ports do not support 802.1 euro tunnels. Interface level statistics are supported for interfaces in Dot1q tunnels, but statistics at the tunnel level are not supported. Page 8Configure storm traffic management levels in accordance with the following guidelines and limitations: Typically, a fabric administrator adjusts storm control in fabric access policies on the following interfaces: a normal trunk interface. A direct port channel on one switch sheet. Virtual port channel (port channel on two sheet switches). Starting with APIC Release 4.2 (1), support is now available to run Cisco ACI's SNMP traps when storm control thresholds are met, with the following limitations: There are two actions related to storm management: drop and turn. With the action shutdown, the interface traps will be raised, but storm control traps to indicate that the storm is active or clear is not determined by the shutdown action. Therefore, you should ignore the storm control traps with the policy shutdown. If the ports flap with storm management policies, clear and active traps are visible together when the stats are collected. Clear and active traps are usually not seen together, but this is expected behavior in this case. For port channels and virtual port channels, storm control values (packages per second or percentage) apply to all individual members of the port channel. Don't adjust storm management on interfaces that are members of the port channel. Note On the hardware switch, starting with APIC 1.3 (x) and Switch 11.3 (x) release, for port channel configurations, traffic suppression on the aggregated port can be up to two times the customized value. The new hardware ports are internally divided into these two groups: Slice-0 and Slice-1. To check the slicing of the map, use the vsh_lc the command platform of the internal hal l2 port gpd and look for slice 0 or slice 1 under the Sl column. port channels fall by both slice-0 and Slice-1, the permitted storm control traffic can be twice as high as the formula is calculated on the basis of each slice. When you adjust for a percentage of available bandwidth, 100 means no storm traffic control and 0.01 suppresses all traffic. Because of the hardware limitations and the method by which packages of different sizes are counted, the level percentage is an approximation. Depending on the size of the frames that make up the incoming traffic, the actual coercive level may differ from the set level by several percentage points. Packages per second (PPS) are converted into a percentage based on 256 bytes. Maximum splash is the maximum accumulation of speed, which is allowed when traffic does not pass. When you start traffic, all traffic to the accumulated speed is allowed in the first interval. In subsequent intervals, traffic is only allowed to the tuned speed. Maximum support is 65535 KB. If the set rate exceeds this value, it is limited in this value for both PPS and percentage. The maximum splash that can be accumulated is 512MB. On the E.P. light switch in the optimized multi-caucasian flooding mode (OMF), storm traffic control will not be applied. On the egress sheet switch in non-OMF mode, the motion storm control will be applied. On the FEX switch sheet, traffic storm management is not available on the host interfaces. Storm traffic control unicast / multicast differentiation is not supported by Cisco Nexus C93128TX, C9396PX, C9396TX, C93120TX, C9332P, C9372PX, C9372TX, C9372PX-E, or C9372TX-E switches. SNMP storm control traps are not supported by Cisco Nexus C93128TX, C9396PX, C9396TX, C93120TX, C9332P, C9372PX, C9372TX, C9372TX, C9372PX-E, C9372TX-E. Motion storm control traps are not supported by Cisco Nexus C93128TX, C9396PX, C9396TX, C93120TX, C9332P, C9372PX, C9372TX, C9372PX-E or C9372TX-E. Storm management is only supported on Ethernet's physical interfaces and port channel interfaces. Since the release of 4.1(1), the Storm Control Option is supported. When the shutdown is selected for the default Soak Instance interface, packages exceeding the threshold swing for 3 seconds and the shutdown port on the 3rd second. Drop's default action. When choosing a Shutdown action, the user has the ability to specify the soaking interval. The default soaking interval is 3 seconds. The customized range is 3 to 10 seconds. Since the release of 4.1(1), the storm-turning option is supported for ports that are disconnected due to storm shutdown. Cisco ACI's 9 Proxy ARP page allows endpoints on the network or subnet to communicate with others points without knowing the real address of MAC endpoints. The ARP proxy is aware of the location of the traffic destination and offers its own MAC address as its final destination. To include ARP Proxies, inside EPG EPG insulation should be included on the EPG to see the next figure for the details. For more information on insulation within EPG and Cisco ACI, see the Cisco ACI virtualization guide. Figure 1. ARP and Cisco APIC Proxy ARP proxies in Cisco ACI fabrics are different from the traditional ARP proxy. As an example of a communication process, when an ARP proxy is enabled on EPG, if endpoint A sends an ARP request to end point B, and if the endpoint B is studied in the fabric, the end point A will receive an ARP proxy response from the bridge domain (BD) MAC. If the endpoint A sends an ARP request to end point B, and if the endpoint B is not yet studied in the ACI fabric, the fabric will send the ARP proxy request to BD. Endpoint B will respond to this ARP proxy request back into the fabric. At the moment, the fabric does not send an ARP proxy response to the end point A, but the end point B is learned in the fabric. If the endpoint A sends another ARP request to the end point B, the fabric will send an ARP proxy response from BD MAC. The following example describes the steps of ARP proxy permission to communicate between VM1 and VM2 customers: you need a VM1 message to VM2. Figure 2. VM1 for VM2 Communications is desirable. Table 1. ARP Table State of the VM1 IP Device - MAC - ACI Fabric IP - MAC - VM2 IP - MAC - VM1 sends an ARP request with a MAC transmission address to VM2. Figure 3. VM1 sends an ARP request with a MAC transmission address to the VM2 2 table. State of the state device ARP Table VM1 IP and VM2 IP; MAK YI? ACI IP and VM1 IP fabric; MAC - VM1 MAC VM2 IP - MAC - ACI fabric floods the ARP proxy query in the Bridge Domain (BD). Figure 4. ACI Fabric floods the ARP proxy request in the BD 3 table. State of the state device ARP Table VM1 IP and VM2 IP; MAK YI? ACI IP and VM1 IP fabric; MAC and VM1 MAC VM2 IP VM1; MAC and BD MAC VM2 sends ARP response to ACI fabric. Figure 5. VM2 sends an ARP response to the ACI Fabric Table 4. State of the state device ARP Table VM1 IP and VM2 IP; MAK YI? ACI IP and VM1 IP fabric; MAC and VM1 MAC VM2 IP VM1; Mac and BD MAC VM2 studied. Figure 6. VM2 is a learned table 5. State of the state device ARP Table VM1 IP and VM2 IP; MAK YI? ACI IP and VM1 IP fabric; MAC AND VM1 MAC IP - VM2 IP; MAC and VM2 MAC VM2 IP VM1; MAC and BD MAC VM1 sends an ARP request with a MAC broadcast address on VM2. Figure 7. VM1 sends an ARP request with a MAC address to table 6 VM2. ARP Table State of the VM1 IP Device - VM2 IP MAC ? ACI IP and VM1 IP fabric; MAC AND VM1 MAC IP - VM2 IP; MAC and VM2 MAC VM2 IP VM1; MAC and BD MAC ACI Fabric sends ARP proxy response to VM1. Figure 8. ACI Fabric sends an ARP proxy response to the VM1 7 table. State of the state device ARP Table VM1 IP and VM2 IP; MAC - BD MAC ACI IP fabric and VM1 IP; MAC AND VM1 MAC IP - VM2 IP; MAC and VM2 MAC VM2 IP VM1; Mac and BD MAC Page 10 Have an account? Personalized Your products and support log in to forget your user ID and/or password? Page 11 ACI account management uses the bridge domain as a layer 2 broadcast boundary, and each bridge domain can include multiple endpoint groups (EPGs). You can link the VLAN encapsulation with the desired EPG to transport user traffic. In some design scenarios, flooding can cross different custom VLANs (EPGs) when EPGs are in the same bridge domain. Using multiple VLANs in tunnel mode can introduce several problems. In a typical deployment using Cisco Application Centric Infrastructure (ACI) with one tunnel, as shown in the next digit, there are several EPGs under one bridge. In this case, certain traffic is flooded in the bridge domain (and therefore in all EPG), with the risk of MAC address learning ambiguities that can lead to distillation errors. Figure 4. Calling ACI with VLAN tunnel mode In this topology, the fabric has a single network tunnel identified that uses one uplink to connect with the ACI sheet node. Two VLANs users, VLAN 10 and VLAN 11, are transferred to this link. The bridge domain is set up in flood mode because the server gateways are outside the ACI cloud. ARP negotiations take place in the following process: the server sends one request for ARP broadcast on the VLAN 10 network. The ARP package is moved through a network of tunnels to an external server that records the original MAC address extracted from its downlink. The server then sends the package to the ACI sheet switch. The ACI fabric sees the ARP broadcast package coming into the VLAN 10 access port and displays it on EPG1. Because the bridge domain is configured to flood ARP packages, the package is flooded in the bridge domain and thus to the ports under both EPGs because they are in the same bridge domain. The same ARP broadcast package is returned via the same link. The external server sees the original mac address from that link. Result: The external device has the same MAC address extracted from both the downlink port and the uplink port in a single MAC forward table, resulting in traffic disruptions. The Flood in Encapsulation option is used to limit flood flow within the bridge domain by one encapsulation. When two EPGs have the same bridge domain and flooding in the encapsulation is included, the EPG flood stream does not reach another EPG. Starting with Cisco Application Policy Infrastructure Controller (APIC) 3.1(1), Cisco Nexus 9000 Switches (with names ending EX and FX and beyond), all protocols are flooded into encapsulation. In addition, while providing a deluge in encapsulation for any inter-VLAN traffic, Proxy ARP ensures that the MAC flap issue does not occur and it limits all flooding (ARP, GARP, and BUM) to encapsulation. This applies to all EPGs under the bridge area where it is included. Before the release of Cisco APIC 3.1 (1), these not supported (ARP proxies and all protocols included in flooding within encapsulation). In the previous release of Cisco APIC or the switches of an earlier generation (without EX or FX in their names), if you encapsulate Flood, it does not function, no information malfunction is generated, but Cisco APIC reduces the health score by 1. The recommended solution is to support multiple EPGs under one domain bridge by adding an external switch. This design with multiple EPGs under one domain bridge with an external switch is illustrated on the next digit. Figure 5. Designed with multiple EPGs under the same domain bridge with an external switch in the same bridge domain, some EPGs may be service hubs and other EPGs may have flooding in encapsulation tuned. The load balancer is on another EPG. The load balancer receives packages from EPG and sends them to other EPGs (no ARP proxy and flooding within the encapsulation does not occur). If you want to add flood to encapsulation only for individual EPGs using the NX-OS CLI style, enter flood-by-encapsulation allow commands under EPGs. If you want to add flooding to encapsulation for all EPG, you can use the multipurpose incap-flood CLI team under the Domain Bridge. Using CLI, flooding in encapsulation configured for EPG takes precedence over flooding in encapsulation configured for the bridge domain. When you set up bridge domains and EPG, the behavior is described as follows: Table 1. Behavior When both Domain Bridge and EPGs are configured flooding configuration behavior in encapsulation on EPG and flooding in encapsulation on the Flood Domain Bridge in encapsulation occurs for traffic on all VLANs within the Domain Bridge. No flooding in the encapsulation on EPG and flooding in encapsulation on the Flood Domain Bridge in encapsulation occurs for traffic at all VLANs within the bridge area. Flooding in encapsulation on EPG and no flooding in encapsulation on the bridge domain Flood in encapsulation takes place for traffic on that VLAN in bridge domain EPG. No flooding in encapsulation on EPG and no flooding in encapsulation on the Bridge Domain Flooding occurs within the entire bridge domain. Segmentation of broadcasting at the EPG/bridge domain level is supported for the following network management protocols: OSPF EIGRP CDP LACP LACP ISDP IS-IS BGP IG PIM PIM-BPDU (flooded EPG) ARP/GARP (controlled by ARP Proxy) ND Here are the restrictions for the use of floods in the encapsulation for all protocols: Flooding in the encapsulation mode does not work. The Neighborly Request (NS/ND) is not supported for this release. You should include in the CoPP port with flooding in the encapsulation. Flooding in encapsulation is supported only in the bridge domain in flood mode and ARP in flood mode. Bridge proxy mode is not IPv4 L3 L3 not supported. IPv6 is not supported. VM migration to another VLAN has immediate problems (60 seconds). The load balancer acting as a gateway is supported, for example, in connection between VMs and load balancer in a non-trusted mode. There is no communication with layer 3. Traffic between VMs and load balancer is on layer 2. However, if the intra-EPG connection passes through the load balancer, the load balancer changes the SIP and SMAC; Otherwise it could cause a MAC flap. Thus, the Source Dynamic Routing Mode (DSR) is not supported in the load balancer. Setting up a link between VMs through firwall, like a gateway, is not recommended because if the VM IP address changes to a gateway IP address instead of an IP firewall address, then the firewall can be bypassed. Previous releases are not supported (even compatibility between previous and current releases). Prior to the release of 3.2 (5) ARP proxies and the flow of encapsulation functions are not supported for VXLAN encapsulation. The topology of the mixed mode with the application sheet engine (ALE) and the engine of the spine application (ASE) is not recommended and is not supported by flooding in encapsulation. Putting them together can prevent AIA priorities from being met. Flooding is not supported by Remote Leaf and Cisco ACI Multi-Site switches. Flooding at encapsulation is not supported for the

general pervasive gateway (CPGW). Page 12 This chapter contains the following sections: The Tissue Administrator creates domain policies that set up ports, protocols, VLAN pools, and encapsulation. These policies can only be used by a single tenant or shared. Once a tissue administrator sets up domains in the ACI structure, tenant administrators can link tenant endpoint groups (EPGs) with domains. The following domain network profiles can be configured to integrate the virtual machine hypervisor: VMM Domain Profiles (vmmDomP). Physical domain profiles (physDomP) are commonly used to attach and access a bare metal server. External Network Domain (l2extDomP) profiles are typically used to connect the bridge's external network switch to the leaf switch in the ACI fabric. Route external network domain profiles (l3extDomP) are used to connect the router to the leaf switch in the ACI fabric. Fibre Channel (fcDomP) domain profiles are used to connect VLANs and VSANs Fibre Channel. The domain is configured to communicate with the VLAN pool. EPG are customized to use VLANs associated with the domain. The configurations of the EPG and VLAN port must be consistent with the domain infrastructure configurations with which epG is associated. If not, APIC will make a mistake. If you're in a malfunction, make sure your domain infrastructure configuration is consistent with the configurations of the EPG and VLAN port. For more information about Layer 3 See The Cisco APIC Layer 3 network configuration guide. For information about setting up VMM domains, see domain bridge domain bridge (BD) is a layer 2 of the rewinding of the structure into the fabric. One or more endpoint groups (EPGs) may be associated with a single bridge domain or subnet. The bridge domain may have one or more subnets that are associated with it. One or more bridge domains together form a network of tenants. When you insert a service function between two EPGs, these EPGs should be in a separate BD. To use the service function between the two EPG, these EPGs must be isolated; this follows the insertion of an outdated service based on Level 2 and Layer 3. VMM Domains ACI (VMM) virtual machine manager domains (VMM) domains allow the administrator to set up connectivity policies for virtual machine controllers. The main components of the ACI VMM domain policy include: a virtual machine manager domain profile, a group of VM controllers with similar network policy requirements. For example, VM controllers can share VLAN pools and application endpoint groups (EPGs). APIC communicates with the controller to publish network configurations, such as port groups, which are then applied to virtual workloads. The VMM domain profile includes the following important components: Credential-Associates is a valid custom VM controller with APIC VMM domain. Controller -Specifes how to connect to the VM controller, which is part of the policy enforcement area. For example, the controller identifies a connection to VMware vCenter, which is part of the VMM domain. Please note that a single VMM domain may contain multiple instances of VM controllers, but it must be from the same vendor (e.g. from VMware or Microsoft. THE EPGs of the VMM domain behave as follows: APIC pushes these EPGs as a group of ports in the VM controller. EPG can cover multiple VMM domains, and the VMM domain may contain multiple EPGs. The Association of Attached Ities Profiles links the VMM domain to the physical network infrastructure. The Edged Essence Profile (AEP) is a network interface template that allows you to deploy VM controller policies in a large set of leaves switch ports. AEP determines which switches and ports are available and how they are configured. VLAN Pool Association - The VLAN pool identifies VLAN ID-shaped data or the ranges used to encapsulate the VLAN consumed by domain VMM. The APIC VMM domain profile is the policy of defining the VMM domain. The VMM domain policy is created in APIC and pushed into leaf switches. VMM domains provide the following: a common layer in ACI fabric that allows scalable fault-resistant multiple platforms of the VM controller. Vmm Vmm for several tenants within the ACI fabric. VMM domains contain VM controllers such as VMware vCenter or Microsoft SCVMM Manager, as well as credentials needed to interact with the VM controller. The VMM domain provides VM mobility in the domain, but not in different domains. A single VMM domain may contain multiple instances of VM controllers, but they must be of the same kind. For example, a VMM domain may contain many VMware vCenters that control multiple controllers, each of which works with multiple VMs, but it also cannot contain SCVMM Managers. Elements of the VMM domain inventory controller (such as pNICs, vNICs, VM names, and so on) both pushes policies into the controller (s), creating port groups and other necessary items. The ACI VMM domain listens to controller events, such as VM mobility, and responds accordingly. Physical domain settings Control the area where this VLAN name space is used. The VLAN domain name space for non-virtualized servers, although it can also be used for static mapping of port groups from virtualized servers. You can set up a physical domain for physical types of devices. Step 1 On the bar menu, click Fabric. Step 2 On the spoof bar, click Foreign Access Policy. Step 3 In the navigation glass, expand physical and external domains and click Physical Domains. Step 4 From the list of fall out actions, select Create a physical domain. Create Physical Domain dialogue window appears. Step 5 Will get the following fields: Name the domain's physical profile. Associated profiles of attached entities select attached entity profiles that will be associated with that domain. VLAN Pool VLAN Pool, used physical area. The VLAN pool identifies the range or pool for VLANs allocated by APIC for service graph templates that use that physical domain. Click Dynamic or Static Distribution. Step 6 (optional) Add AAA security domain and click on Check-box Select. Step 7 Click Send. The physical domain acts as a link between the VLAN pool and the Access Entity (AEP) profile. The domain also links the fabric configuration to the tenant's configuration, as the tenant administrator is the one who connects the domains to THE EPG, while the domains are created under the fabric tab. When you set up this order, only the profile name and the VLAN pool are configured. Set up a physical domain by sending a message to XML, zlt;physDomP dn'uni/phys-bsprint-PHY lcown'local modts'2015-02-23T16:13:21.906-08:00 monpoldn/uni/fabric/monfab-default-name'bsprint-PHY ownerkey' ownertag's status q uid'8131'gt; zlt;infraRsVlanNs childAction forceResolve'no lcOwn'local modTs'2015-02-23T16:13:22.065-08:00 monPolDn'uni/fabric/monfab-default rType childaction= forceresolve=no lcown=local modts=2015-02-23T16:13:22.065-08:00 monpoldn=uni/fabric/monfab-default rtype=mo rn=rsvlanNs state=formed statequal=none></infraRsVlanNs childAction= forceResolve=no lcOwn=local modTs=2015-02-23T16:13:22.065-08:00 monPolDn=uni/fabric/monfab-default rType=mo rn=rsvlanNs state=formed stateQual=none > </physDomP> например, следующий пример: пример: tCl'fvnsVlanInstP tDn'uni/infra/vlanns-'bsprint-vlan-pool-static tTypemo uid8131/zgt; page q lt;infraRsVlanNsDef forceresolve'no lcown'local modts' 2015-02-23T16:13:13:13:13:22.065-08:00 rtype'mo rn'rsvlanNsDef state'formed statequal'none status q tcl'fvnsAInstP tdn'uni/infra/vlanns-'bsprint-vlan-pool'-static ttype'mo'gt;'lt;infraRsVlanNsdef'gt; 2015-02-23T16:13:52.945-08:00 rn'rtdomP --uni/infra/attentp-bsprint-AEP) status tcl'infraAttEntityP tdn/uni/infra/attentp-bsprint-aEP/lt;/infraRtDomDom'gt; 13 This foreword includes the following sections: This guide is designed primarily for data center administrators with responsibilities and experience in one or more of the following: Virtual Machine Installation and Server Administration Switch And Network Management Administration Cloud Command Descriptions use the following conventions: Convention Description bold bold text indicates commands and keywords that you enter literally As shown. Italian Italian text points to arguments for which the user delivers values. Square brackets attach an additional element (key word or argument). (x) Square brackets that attach keywords or arguments separated by a vertical bar indicate an optional choice. (x) Braces that attach keywords or arguments separated by a vertical bar indicate the choice you need. The nested set of brackets or brackets indicates an optional or necessary choice within the additional or required elements. Braces and vertical brackets indicate the necessary choice within the additional element. the variable indicates the variable for which you are supplying the values, in a context where it cannot be used. line unquote set of characters. Don't use quotes around a string or a line will include quotes. Examples of use of the following conventions: Conference description of the screen terminal sessions and the information switch displayed in the font of the screen. Boldface screen font information that you have to enter in bold screen font. Italic font screen arguments for which you deliver values in a multi-nal screen font. Unprintable symbols, such as passwords, are in corner brackets. The default responses to system queries are in brackets. !, an exclamation point (!) or a pound sign (l) at the beginning of the code line points to the comment line. This document uses the following conventions: Note means that the reader takes note. Notes contain useful suggestions or links to content not covered in the manual. Caution means that the reader be careful. In this situation, you can do something that could damage equipment or lose data. IMPORTANT SAFETY INSTRUCTIONS This warning symbol means danger. You are in a situation that can lead to bodily injury. Before you work on any equipment, be aware of the dangers associated with the electrical circuit and be with the standard practice of preventing accidents. Use the application number provided at the end of each alert to find its translation in the translated security alerts that accompanied the device. SAVE THESE INSTRUCTIONS Documentation Cisco Cloud APIC available at the following URL: The following companion guides provide documentation for Cisco APIC: Cisco APIC Start Guide Cisco APIC Basic Configuration Guide Cisco ACI Basics Cisco APIC Layer 2 Network Configuration Guide Cisco APIC Layer 3 Network Configuration Guide Cisco APIC NX-OS Style Cisco APIC REST API Configuration Guide Cisco APIC Layer 4 to Layer 7 Services Deployment Guide Cisco ACI Virtualization Guide Cisco Application Oriented Infrastructure Best Practices Guide All these documents are available at the following URL: More extensive Cisco ACI documentation is available at the following URL: . Cisco ACI Simulator documentation is available . The Cisco Nexus 9000 Series Switches documentation is available on . Cisco Application Virtual Switch (AVS) documentation is available on . Cisco Application Virtual Edge documentation is available by . Cisco Application Virtual Pod (vPod) is available . Cisco ACI integration with OpenStack documentation is available on . To get technical feedback on this document or to report an error or omission, please send your comments apic-docfeedback@cisco.com. We appreciate your feedback. For information about obtaining documentation using the error-finding tool (BST), sending a service request and For more information, see what's new in Cisco's product documentation: Sign up for a new cisco documentation in which all new and revised Cisco technical documents are listed as an RSS feed and the contents are delivered directly to your desktop using the reading app. RSS feeds are a free service. Service. cisco 3850 macsec configuration guide. cisco nexus 9000 macsec configuration guide