Cci behavioural activation pdf download windows 10 full

I'm not robot!

time causing a collision. The FM3200 can operate in Time Division Multiple Access (TDMA) mode which increases efficiency in the communication by reducing collisions, but the FM3500 can only operate in Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) mode. To reduce collisions, it is necessary to enable RTS/CTS on the FM3500 Mesh End radios. Figure 10 Mesh End/Mesh Point – Wireless Radio Because the Mesh Ends communicate with numerous PoP sites, they are also configured using FluidMAX. This allows the unit configured as "Master" (Mesh End in this case) to dictate the operating frequency to the radio units configured as "Slave" (Mesh Points). Note: In the Advanced Radio Settings UI shown below, the Primary is called Master and the Secondary is called Slave. This feature cannot be configured in RACER for the FM3500, it can only be configured using the web Configurator, or the CLI. Figure 11 FluidMAX Primary/Master Figure 12 FluidMAX Secondary/Slave For this deployment, EIGRP was used as the underlay routing protocol which uses the well-known standard reserved multicast address 224.0.0.10. To forward these messages to the other radios, the Mesh Ends must be configured with multicast routes. The below configuration will send below sends the EIGRP update messages to all units in the mesh network. Figure 13 Multicast Because the radios are all in the underlay network, the management VLAN can be configured as common across all the radios. The other configurable option for VLANs in the radio is the native VLAN. The native VLAN should must be configured the same on the Mesh End and Mesh Points while using the PoP border node to set the desired native VLAN. This ensures that any untagged packets coming into the wireless network do not inadvertently leave the radio with a VLAN tag. In the below examples below, VLAN 145 is used for management and VLAN 555 is used as the native VLAN. Note, VLAN 555 is not being used elsewhere in the network. Note that if the native VLAN is set to 0, any untagged traffic will be dropped. Figure 14 VLAN Configuration QoS can only be enabled through the RACER configuration or CLI, not using the web Configurator. Enableing QoS on the radio and leaving the marking and queueing to the connected switch is recommended. Enable this configuration on all Mesh Ends and Mesh Points. When enabling 802.1P, the CURWB radio will inspects the COS value in the VLAN header as opposed to the DSCP value in the Layer 3 header. Figure 15 QoS Configuration Using multiple parallel wireless paths will increases throughput and resiliency. Each radio network is therefore treated as a separate network path to a PoP site. In this deployment, wireless path A is assigned to VLAN 200 and wireless path B is assigned to VLAN 201. Each radio is connected to a trunk port that disallows the other PoP VLAN. The MTU is also configured for the maximum size that the radios can pass. The MTU is also required on the SVI because EIGRP sends updates up to the maximum size allowed on the link. VLAN 145 is included to enable management of the radios. Wireless Path A interface TenGigabitEthernet1/0/3 description connected to FM-3500 5.1.29.7 switchport trunk allowed vlan 1,145,200 switchport mode trunk mtu 2044 Wireless Path B interface TenGigabitEthernet1/0/4 description connected FM-3500 5.0.156.233 switchport trunk allowed vlan 1,145,201 switchport mode trunk mtu 2044 Each VLAN has an associated SVI for Layer3 reachability. interface Vlan145 ip address 172.16.145.1 255.255.255.0 interface Vlan200 ip address 10.5.1.1 255.255.255.0 ip mtu 2044 interface Vlan201 ip address 10.5.2.1 255.255.255.0 ip mtu 2044 VLAN 200 and 201 are added to EIGRP to form neighbors with the other PoP sites connected wirelessly. router eigrp 20 network 10.5.1.0 0.0.0.255 network 10.5.2.0 0.0.0.255 At each PoP site, the VLAN for each wireless path must be configured. For sites with dual paths, this is VLAN 200 and 201. The interfaces facing the radio must also be set as trunks. When using the 9x00 as the border node, the MTU can be configured system wide for 2044. system mtu 2044 PoP Interface Configuration interface TenGigabitEthernet1/0/23 switchport mode trunk interface TenGigabitEthernet1/0/24 switchport mode trunk interface Vlan200 ip address 10.5.1.5 255.255.255.0 interface Vlan201 ip address 10.5.2.5 255.255.255.0 Cisco DNA-C also requires a loopback for onboarding and management. interface Loopback0 ip address 100.0.0.9 255.255.255.255 The underlay subnets are then added to the EIGRP process. router eigrp 20 network 10.5.1.0 0.0.0.255 network 10.5.2.0 0.0.0.255 network 100.0.0.9 0.0.0.0 Looking at the EIGRP neighbors will confirms the underlay is functioning correctly. EIGRP-IPv4 Neighbors for AS(20) H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms) Cnt Num 4 10.5.1.1 Vl200 12 02:46:59 1 100 0 1760951 5 10.5.2.1 Vl201 11 03:18:41 1 100 0 1760950 After the underlay network is functional and all required configuration for discovery is in place, the Discovery workflow can be used to onboard the device. Onboarding and provisioning the newly-discovered switch is the same process as a wired switch and requires no special configuration to support the CURWB connection. After provisioned to the fabric site, the border interfaces must be configured if an IP Transit is used. Each interface facing the CURWB radio is used as the External Interface. Figure 16 Border External Interfaces Because the PoP switch is connected to the headquarters through Layer2, each VLAN configured for a VN must be unique at the headquarters site. Figure 17 Border Interface-1 VN Configuration Figure 18 Border Interface-2 VN Configuration Through the use of multiple interfaces, the routing protocol can be configured for fast failover and load balancing. Bidirectional Failure Detection (BFD) is configured on the interfaces and within the BGP instance for the VRF associated with the VN. Load balancing is achieved using the maximum-paths command. The routing protocol is dependent on having multiple interfaces to achieve these additions. Edge PoP External SVI: interface Vlan3020 description vrf interface to External router vrf forwarding Transportation ip address 172.16.18.5 255.255.255.252 no ip redirects ip route-cache same-interface bfd interval 100 min_rx 100 multiplier 3 configure firewall routed This will destroy the current interface configurations, are you sure that you want to proceed? [y/N] y The firewall mode was changed successfully. Alternatively, the mode can be also be changed from FMC by following the steps in the following URL: – 2. Configure Management via FMC Follow the steps listed in the Quick Start Guide to perform the initial configuration of the Firepower Threat Defense (FTD) and configure the management of the FTD via FMC: – To configure the Firepower in the CCI network as a Firewall, a sequence of steps must be done as shown in Figure 297: Figure 297 Cisco Firepower Configuration Flow Using FMC 1. Configure High Availability (HA): After adding both devices to the Firepower Management Center, the following steps must be followed to configure HA: a. Choose Devices-> Device Management. b. From the Add drop-down list, choose High Availability, as shown in Figure 298: Figure 298 Adding Device in HA c. Enter a display name for the high availability pair. d. Under Device Type, choose Firepower Threat Defense. e. Choose the Primary Peer device for the high availability pair. f. Choose the Secondary Peer device for the high availability pair. g. Click Continue. h. Under LAN Failover Link, choose an interface with enough bandwidth to reserve for failover communications. Note: Only interfaces that do not have a logical name and do not belong to a security zone will be listed in the Interface drop-down list in the Add High Availability Pair dialog box. i. Type any identifying Logical Name. j. Type a Primary IP address for the failover link on the active unit. This address should be on an unused subnet. Note: 169.254.0.0/16 and fd00:0:0:*::/64 are Firepower internally-used subnets and cannot be used for the failover or state links. k. Click OK. This process takes a few minutes as the process synchronizes system data. For more details on how to configure HA, complete the steps listed at: ■ 2. Configure Interfaces: To configure the interfaces, the following steps must be completed: a. Choose Devices-> Device Management and edit the HA pair. Click the Interfaces tab. b. Select the Edit icon next to the interface and fill in the details for the interfaces, as shown in Figure 299: Figure 299 Configuring Interfaces Similarly, bring up all the interfaces as per topology by enabling them and assigning IP addresses and names to the interfaces following the above steps. 3. Configure Static and Dynamic Routing: Firepower acts as the Internet edge device in the network. Therefore, a static default route must be configured on the Firepower for all the devices to reach the Internet. The following lists the steps to configure static route for CCI network Internet reachability via Firepower: a. Choose Devices-> Device Management and edit the HA pair. Click the Routing tab. b. Select Static Route from the table of contents. c. Click Add Routes. d. Click the IPv4/0 radio button. e. Choose the Interface to which this static route applies. f. In the Available Network list, choose the destination network. g. Following the above method, add the static route for the VN networks via the fusion router. Static and Default Routes for Firepower Threat Defense To define a default route, create an object with the address 0.0.0.0/0 and select it here. a. In the Gateway or IPv6 Gateway field, enter or choose the gateway router, which is the next hop for this route. You can provide an IP address or a Networks/Hosts object. b. In the Metric field, enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1, as shown in Figure 300: Figure 300 Example to Add a Static Default Route Similarly, add the IPv6 static routes by choosing the IPv6 radio button and entering the value in fields to enable the IPv6 communication. The routes display in an example configuration, as shown in Figure 301: Figure 301 An Example View of IPv4 and IPv6 Routes Configured on Firepower For more detailed step-by-step instructions, refer to the following URL: ■ Configuring Dynamic Routing Protocol For dynamic exchange of routes between Firepower, the HER, and the fusion router, complete the steps described below. In this implementation, EIGRP routing protocol is used on the Firepower using FlexConfig. a. Go to Devices-> FlexConfig. b. Create a new policy by adding name and description and selecting the FTD HA pair from available devices. Then click Save. c. Select Eigrp_configure from the list of system-defined FlexConfig. d. Create a copy of this config and rename it. e. In the created copy, edit the variables $eigrpAS and $eigroNetworks to hold values of the autonomous system in use for topology and the networks to be advertised. This can be done by editing the variable from Objects-> Object Management->FlexConfig-> Text Object. The Object should appear as shown in Figure 302: Figure 302 Configuring EIGRP on Firepower f. Append the FlexConfig created in the Step 5, click Save, and then click Deploy. g. To verify the formed EIGRP neighborship, issue the following on CLI: > show eigrp neighbors EIGRP-IPv4 Neighbors for AS(2000) H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms) Cnt Num 2 10.10.204.3 ToSDAccessCSR 12 1w1d 1 200 0 50 1 10.10.204.2 ToSDAccessCSR 14 1w3d 2 200 0 202 0 10.40.100.101 InsideIntf 11 1w4d 1 200 0 90 h. Similarly, verify the routing table for the received routes via EIGRP: > show route eigrp Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route Gateway of last resort is to network 0.0.0.0 D 10.10.100.0 255.255.255.0 [90/28416] via 10.10.204.3, 1w1d, ToSDAccessCSR Note: The above output is only a sample output and large section of output may have been omitted. Note: As a best practice, when a change needs to be made in the FlexConfig, the Eigrp_unconfigure function should be called so as to avoid any errors (similar to the no of the CLI.) 4. Configure Access Control Policy: Access control policy will allow or disallow communication between the different zones. a. In order to configure the Access Control Policy, click Policies -> Access Control -> New Policy. b. Enter the details as shown in Figure 303: Figure 303 Adding a New Policy c. Click Edit policy -> Add Rule and then add the source and destination zone for allowing communication between the fusion router and HER, and vice versa. d. Add another rule to Enable the UDP port 500 and 4500 to allow the tunnel establishment between the CGR and the HER and also between the CIMCON LG cloud service router end and the HER. Also, include the rule to allow the communication from source IP of FlashNet Application server (in cloud) to the CCI network for FlashNet LoRaWAN Use case. Work with FlashNet support to obtain the source IP of FlashNet Application server. The rules will appear as shown in the example in Figure 304: Figure 304 Rules Configured Under Access Control Policy 5. Configure NAT policy: For the devices to reach the Internet via the Firepower, a NAT policy is configured. Dynamic and static NATs are configured in CCI solution. When devices need to be accessible from outside, a static NAT is implemented; otherwise dynamic NAT is implemented. For example, for internet access of internal devices dynamic NAT policy is deployed, whereas for building a tunnel to the HER and for Flashnet use case a static NAT is implemented. Following are the steps listed for the same: a. Assign interfaces to Security Zones, if not already assigned in the Creating Interfaces section, as shown in Figure 305. Figure 305 Editing Interface b. You can create/edit Interface Groups and Security Zones from the Objects -> Object Management> Interface page, as shown in Figure 306. Figure 306 Adding a Security Zone c. Configure NAT on FTD by creating a NAT policy. Navigate to Devices -> NAT and create a NAT Policy. d. Select New Policy -> Threat Defense NAT, as shown in the image. e. Specify the policy name and assign it to the HA pair. f. To add a static and a dynamic NAT rule to the policy, click Add Rule. g. Specify these as per task requirements, as shown in Figure 307 and Figure 308. Figure 307 Configuring a NAT Policy Figure 308 Editing a NAT Policy h. Similarly, create a static policy for UDP port 4500 as shown in Figure 309. Figure 309 NAT Policy for Tunnel Establishment—1 Figure 310 NAT Policy for Tunnel Establishment—2 Follow the above steps to create a static NAT for the HER to gain Internet access for FlexVPN tunnel establishment to a remote site. i. Similarily, configure static NAT for Flashnet Application Server to be able to reach TPE. Here, the public IP used by the Flashnet Application server (obtained from Flashnet support) is to be configured as source address as shown in Figure 311. Figure 311 Creating a Static NAT Policy for Flashnet Use Case j. Now create a dynamic NAT rule for all the networks that need Internet access and are connected on the fusion router following the similar steps and choosing dynamic instead of static, as shown in Figure 312: Figure 312 Editing a Dynamic NAT Policy k. Verify the configuration. From CLI: Connect ftd show running-config nat nat (OutsideIntf,InsideIntf) source static CimconCSR CimconCSR destination static interface 10.40.100.0 service SVC_21474841183 SVC_21474841183 description Nat rule to translate CSR IP nat (OutsideIntf,InsideIntf) source static CimconCSR CimconCSR destination static interface 10.40.100.0 service SVC_21474841184 SVC_21474841184 ! object network SDAccess172.9.90.0 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess172.10.90.0 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess172.20.90.0 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess172.15.70.0 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess172.16.70.0 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess172.17.70.0 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDaccess192.100.80.0 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess192.100.90.0 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess192.168.70.0 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess192.168.70.4 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess192.168.70.8 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess192.168.70.12 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess192.168.70.16 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess192.168.70.20 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess192.0.50.11 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface object network SDAccess192.0.50.12 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface: > show nat Manual NAT Policies (Section 1) 1 (OutsideIntf) to (InsideIntf) source static CimconCSR CimconCSR destination static interface 10.40.100.0 service SVC_21474841183 SVC_21474841183 description Nat rule to translate CSR IP translate_hits = 51, untranslate_hits = 51 2 (OutsideIntf) to (InsideIntf) source static CimconCSR CimconCSR destination static interface 10.40.100.0 service SVC_21474841184 SVC_21474841184 translate_hits = 1, untranslate_hits = 214 Auto NAT Policies (Section 2) 1 (ToSDAccessCSR) to (OutsideIntf) source dynamic SDAccess192.0.50.11 pat-pool interface translate_hits = 2, untranslate_hits = 12 2 (ToSDAccessCSR) to (OutsideIntf) source dynamic SDAccess192.0.50.12 pat-pool interface translate_hits = 2, untranslate_hits = 12 > show xlate 4 in use, 51 most used Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T - twice, N - net-to-net UDP PAT from OutsideIntf: 0 flags srIT idle 18:25:29 timeout 0:00:00 UDP PAT from InsideIntf:10.40.100.0/24 500-500 to OutsideIntf: 500-500 flags srIT idle 18:25:29 timeout 0:00:00 UDP PAT from OutsideIntf: 0 flags srIT idle 359:24:59 timeout 0:00:00 UDP PAT from InsideIntf:10.40.100.0/24 4500-4500 to OutsideIntf: 4500-4500 flags srT idle 284:45:51 timeout 0:00:00 Note: The above output is only a sample output and large section of output may have been omitted. For more details on configuring NAT policy, refer to the following URL: ■ The SD-Access solution has the capability to define security rights from Cisco DNA Center, which will leverage the Identity Services Engine (ISE) to enforce policies that will secure our network. SD-Access provide segmentation that enables an organization to implement security between different user groups and devices in the network. This is very similar to what industry has been doing for many years based on the IPs with ACLs, whereas in SD-Access the same can be achieved based on the user identity profile (in ISE) and regardless of IP (subnet). Segmentation in SD-Access takes place at both a macro and a micro level through VNs, as discussed in previous sections (Macro Segmentation) and Scalable Groups (Micro Segmentation), respectively. VNs provide routing isolation between the different entity and SGT provides isolation within the routing entity, i.e., within VRF. Scalable groups comprise a grouping of users, end point devices, or resources that share the same access control requirements. These groups (known in Cisco ISE as security groups or SGs) are defined in Cisco ISE. Scalable Group Tags (SGT) will provide micro-segmentation within the VN (within routing visibility or partition). That is, IP reachability is available within subnets of the VN or hosts within the VN, However, based on the user's identity profile, the traffic flow needs to be controlled between different groups using permit/deny SGACLs. For more details on the CCI Security Policy design with Segmentation, refer to the CCI Solution Design Guide, which can be found at the following URL: ■ In this implementation, an example configuration of Scalable Groups and Scalable Group-based Access Control Policy (SGACL) validated in this CVD is provided as a reference/guideline to implement micro-segmentation in the CCI network. Note: Example micro-segmentation policies with Scalable Groups and SGACLs covered in this section are reference configuration only. Depending on your network deployment and CCI vertical use cases security requirements, you should choose to create your new Scalable Groups or SGACLs to implement the micro-segmentation in the CCI network. In the following example, micro-segmentation policies within SnS_VN are created to achieve the policy enforcement, as shown in Table 28. Policy deployment has a default permit policy (blocked list policy model deployment). The deny policy enforcement would happen at the egress node side where the destination SGT resides; in our case, the Catalyst 9300 switch stack (FiaB) in SD-Access is the policy enforcement point as per the CCI solution design. Table 28 Example IP Addressing Prefixes and Convention Followed Destination Source SNS_Servers SnS_Traffic_Servers SnS_SGT SnS_Traffic SnS_SGT Permit Deny Permit Deny SnS_Traffic Deny Permit Deny Permit SnS_Servers Permit Deny Permit Deny SnS_Traffic_Servers Deny Permit Deny Permit Note: Make sure that Cisco DNA Center with ISE are successfully integrated and that your Fabric Edge nodes are successfully registered on ISE before implementing micro-segmentation in the CCI network. Before we look into the pre-checks required before pushing SGACLs from Cisco DNA Center, let's understand what is Protected Access Credential (PAC) and its significance. PAC is the Protected Access Credential generated by the server and provided to the client. It consists of: ■PAC key (random secret value, used to derive TLS primary and session keys) ■PAC opaque (PAC key + user identity, all encrypted by the EAP-FAST server primary key) ■PAC info (server identity, TTL timers) The server, ISE in this case issuing the PAC will encrypt the PAC key and identity using the EAP-FAST server primary key, (that is, the PAC opaque) and sends the whole PAC to the client (Catalyst 9300 FiaB devices, in this case). The server does not keep or store any other information, except the primary key, which is the same for all PACs. Once the PAC opaque is received, it is decrypted using the EAP-FAST server primary key and validated. The PAC key is used to derive the TLS primary and session keys for an abbreviated TLS tunnel. New EAP-FAST server primary keys are generated when the previous primary keys expire. In some cases, a primary key can be revoked. Following are some checks that can be completed to make sure your network devices and ISE have been successfully integrated before we start to configure policy enforcement using SGTs: ■Make sure the PACs are provisioned on the network switches by Cisco DNA Center: Edge_Device#show cts pacs AID: E74D665D34C206E451B00F66D2209918 PAC-Info: PAC-type = Cisco Trustsec AID: E74D665D34C206E451B00F66D2209918 I-ID: FCW2304G0VH A-ID-Info: Identity Services Engine Credential Lifetime: 13:07:09 UTC Wed Oct 30 2019 PAC-Opaque: 000200B80003000100040010E74D665D34C206E451B00F66D22099180006009C0003010053E42932DA5A892B8000AF04EB Refresh timer is set for 12w2d ■Check the configuration on the network switches for ISE communication over RADIUS. These configurations are pushed automatically by DNA Center while provisioning: aaa group server radius Cisco DNA Center-client-radius-group server name Cisco DNA Center-radius_X.X.X.X ip radius source-interface Loopback0 aaa group server radius Cisco DNA Center-network-radius-group server name Cisco DNA Center-radius_X.X.X.X ip radius source-interface Loopback0 aaa authentication login default local aaa authentication login VTY_authen group Cisco DNA Center-network-radius-group local aaa authentication dot1x default group Cisco DNA Center-client-radius-group aaa authorization exec default local aaa authorization exec VTY_author group Cisco DNA Center-network-radius-group local if-authenticated aaa authorization network default group Cisco DNA Center-client-radius-group aaa authorization network cts-list group Cisco DNA Center-cts-list group aaa accounting update newinfo periodic 2880 aaa accounting identity default start-stop group Cisco DNA Center-client-radius-group aaa accounting exec default start-stop group Cisco DNA Center-network-radius-group aaa server radius dynamic-author client X.X.X.X server-key 7 143453180F0B7B7977 pac key 7 072C605F4D06485744 Complete the following steps to configure SGACLs in the CCI network for an example implementation shown in Figure 313: 1. Creating SGTs on ISE SGTs can be assigned statically for a resource on Cisco DNA Center or ISE. This value is inserted into the Reserved field of the VXLAN header in SD-Access. –On ISE, navigate to Work center-> Trustsec-> Components-> Security Groups-> Add. Each SGT gets assigned a number, as shown in Figure 313: Figure 313 Cisco ISE Scalable Groups List 2. Mapping SGTs to Virtual Network on Cisco DNA Center SGTs that were created on ISE are seen on Cisco DNA Center and those Scalable Groups have to be mapped to the respective VNs. –On Cisco DNA Center GUI, select the VN from Policy-> Group-Based Access Control > Scalable Groups and select the scalable groups from the available list to Edit, as shown in Figure 314, and then click Save. Figure 314 Cisco DNA Center Scalable Groups Mapping to a VN Confirm that the environment data (SGTs) are being successfully downloaded by the switch from ISE on the FiaB. Also, notice that each SGT name is mapped to a number. This mapping is critical since in packet captures, you will only see the numbers, not the names of the SGTs. C9300-HQ-Stack#show cts environment-data CTS Environment Data ==================== Current state = COMPLETE Last status = Successful Local Device SGT: SGT tag = 0-00:Unknown Server List Info: Installed list: CTSServerList1-0001, 1 server(s): Server: X.X.X.X, port 1812, A-ID E74D665D34C206E451B00F6D2209918 Status = ALIVE auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs Security Group Name Table: 0-00:Unknown 2-00:TrustSec_Devices 3-00:Network_Services 4-00:Employees 5-00:Contractors 6-00:Guests 7-00:Production_Users 8-00:Developers 9-00:Auditors 10-00:Point_of_Sale_Systems 11-00:Production_Servers 12-00:Development_Servers 13-00:Test_Servers 14-00:PCI_Servers 15-00:BYOD 16-00:SnS_SGT 17-00:Lighting_SGT 18-00:SnS_Servers 19-00:Lighting_Servers 20-00:SnS_Traffic_SGT 21-00:SnS_Traffic_Servers 255-00:Quarantined_Systems Environment Data Lifetime = 86400 secs Last update time = 13:07:22 UTC Sun Aug 4 2019 Env-data expires in 0:08:10:57 (dd:hr:mm:sec) Env-data refreshes in 0:08:10:57 (dd:hr:mm:sec) Cache data applied = NONE State Machine is running 3. Creating Policy and Contracts on Cisco DNA Center Cisco ISE PxGrid Policy deployment has default permit policy (blocked list policy model deployment). All the SGTs are allowed to communicate with each other within VN. If an SGT has to be access restricted to the rest of the SGTs then 1: N access policy has to be created in the system. You can create a contract that will contain the ports and protocols that are allowed or prohibited to communicate between different groups or by default "deny" and "permit" contracts are present in Cisco DNA Center which you can leverage. In this example, we have SGTs within a VN and create a deny policy between them, as shown in Figure 315. a. On Cisco DNA Center, navigate to Policy-> Group-Based Access Control Policies, click Create Policies and then select source and destination SGT groups and select Contract. Then choose deny contract rule between the SGTs, as shown in Figure 315: Figure 315 Cisco DNA Center Scalable Groups-based Policy Creation View The Cisco TrustSec (CTS) matrix is where policies are defined initially in ISE. It contains two axis (the source axis and destination axis). You will see the deny policy between the SGTs as per our bi-directional policy enforcement. This matrix will be controlled by the Cisco DNA Center controller and all the policy changes can be done on the Cisco DNA Center. b. The applied policy with the deny contract can be seen on Cisco ISE GUI in matrix format. Navigate to Work Centers-> TrustSec Policy-> Egress Policy-> Matrix. Figure 316 shows a sample policy matrix defined as per the configuration: Figure 316 Cisco DNA Center Scalable Groups-based Policy Matrix View 4. Verify the SGACL configuration on the FiaB (Fabric edge). The SGACL configuration is downloaded to the FiaB device can be verified as below: C9300-HQ-Stack#show cts role-based permissions IPv4 Role-based permissions default: Permit IP-00 IPv4 Role-based permissions from group 16:SnS_SGT to group 20:SnS_Traffic_SGT: Deny IP-00 IPv4 Role-based permissions from group 18:SnS_Servers to group 20:SnS_Traffic_SGT: Deny IP-00 RBACL Monitor All for Dynamic Policies: FALSE RBACL Monitor All for Configured Policies : FALSE In this example, we have created SGACLs using Cisco DNA Center between the SGT groups within the VN and the configuration has been pushed to the devices from the ISE. Now the traffic filtering can be validated with role-based counters command: Edge_Device#show cts role-based counters Role-based IPv4 counters From To SW-Denied HW-Denied SW-Permitt HW-Permitt SW-Monitor HW-Monitor * * 0 0 5 14075822 0 0 16 20 0 120 0 0 0 0 18 20 0 0 0 0 0 0 This section describes the deployment of Cisco Cyber Vision Center (CVC) in Shared Services and the deployment of network sensors on IE3400 and IE3300-X Series switches in CCI PoPs and IR1101 gateway in RPoPs. The Cyber Vision Center can be deployed as a virtual machine (VM) or as a hardware appliance. In this deployment, the standalone Cyber Vision Center (standalone) is deployed as a VMs on a Cisco Unified Computing System (UCS) in the CCI Shared Services network. For step-by-step instructions on installation and resource recommendations of CVD, refer to the Cisco Cyber Vision Center VM Installation Guide at the following URL: It is recommended to install the Cyber Vision Center application in the CCI Shared Services network with dual interfaces; one for management and the other for sensor communication. Following is an example of the IP addressing schema used in CVC installation. ■Admin Interface (eth0): 10.104.206.225 (Routable IP address for CVC UI access) ■Collection interface (eth1): 10.10.100.33 (shared services network IP) ■Collection network gateway: 10.10.100.1 (shared services gateway) ■NTP: 10.10.100.1 Refer to the section "Cisco Cyber Vision Operational Technology (OT) Flow and Device Visibility Design" in the CCI General Solution Design Guide for the detailed design and deployment considerations for CVC, Network Sensors on IE3400 and IE3300-X series switches, and the IR1101 for RPoP in a CCI deployment here: There are two types of Cyber Vision Sensor: hardware and network. The hardware Sensor is the Cyber Vision IOx application installed on an Industrial Compute Gateway 3000 (IC3000) appliance. The network Sensor is the Cyber Vision IOx application installed on the supported switches and routers. In the CCI solution, only network sensors on IE switches and IR router are used, as described in the design. For Network Sensors, there are three methods of installation: switch CLI, switch web interface, and Cyber Vision Center Extension. This guide discusses the network sensor installation using the Cyber Vision Center Extension feature. Refer to the Cyber Vision documentation for guidance on manual installations here, if needed: Prior to any installation, the following prerequisite steps must be done on the IE switches in CCI PoPs: 1. Verify that Extended Node (IE3300 10G aka IE3300-X) and PEN (IE3400) switches in the ring are onboarded into the fabric with switches images running from flash instead of sdflash and the IE switch boot variable "ENABLE_FLASH_PRIMARY_BOOT" is set to "yes". On a IE3300 10G or IE3400 switch in a CCI PoP: SN-FCW24110H0T#show boot Current Boot Variables: BOOT variable = flash:ie3x00-universalk9.1761a.SPA.bin; Boot Variables on next reload: BOOT variable = flash:ie3x00-universalk9.1761a.SPA.bin; Config file = flash:/nvram_config ENABLE_FLASH_PRIMARY_BOOT = yes Note: You must boot the IE switch image from switch flash memory because the sdflash drive on the switch is formatted with the ext4 file system and the sensor application is installed and running from the sdflash memory of the switch. 2. Ensure network reachability between the Cyber Vision Center and the IE Switches in the PoPs. A separate collection Virtual Network (VN) is configured along with an IP subnet pool for Sensors on IE switches using the Cisco DNA Center at CCI PoP sites. Figure 1The figure below shows an example configuration of a Collection_VN and IP pool for Sensor communication with CVC. (For example, 172.16.10.x/24 at Whitefield PoP fabric site) communication with CVC. Note: An IE switch in CCI PoP may have been configured with VLANs in multiple VNs by the Cisco DNA Center for switch management, CV sensor communication, and one or more VLANs for IT/OT data traffic (For example, Extended node VLAN in INFRA_VN) CV sensor communication (VLAN in collection VN), and one or more VLANs for IT/OT data traffic (VLAN in SnS_VN for endpoints). Figure 317 CCI Collection VN configuration with IP Pool Binding 3. Ensure that the FiaB switch and the IE switches in the CCI PoPs are configured with collection network VLAN. On FiaB switch at a PoP site: Akash-C9300-Whitefield#show vlan VLAN Name Status Ports -------------------------------- 1023 SnS_VN active L2LI0:8190, Gi1/0/13 1024 Scada_VN active L2LI0:8191, 1025 172_16_10_0-Collection_VN active L2LI0:8192, Akash-C9300-Whitefield#show run interface Vlan 1025 interface Vlan1025 description Configured from Cisco DNA-Center mac-address 0000.0c9f.f818 vrf forwarding Collection_VN ip address 172.16.10.1 255.255.255.0 ip helper-address 10.10.100.42 no ip redirects ip route-cache same-interface no lisp mobility liveness test lisp mobility 172_16_10_0-Collection_VN-IPV4 no autostate end On IE3300-A switch at the PoP site ring: SN-FCW24110H0T#show vlan VLAN Name Status Ports -------------------------------- 1023 SnS_VN active 1024 Scada_VN active 1025 172_16_10_0-Collection_VN active 4. Configure an SVI in the collection network VLAN on the IE switch where the CV sensor is to be installed. An example SVI configuration on Collection VLAN in IE3300-A 10Gig switch is: SN-FCW24110H0T#show run interface Vlan 1025 ! interface Vlan1025 ip address 172.16.10.250 255.255.255.0 end 5. Verify that the IE switch can reach the CVC Collection Interface IP at the shared services network in the CCI HQ site. On the IE switch in a PoP, ping CVC collection network interface: SN-FCW24110H0T#ping 10.10.100.33 source vlan 1025 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.100.33, timeout is 2 seconds: Packet sent with a source address of 172.16.10.250 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms Note: the IP 10.10.100.33 in the above example configuration is the IP address of Cyber Vision Center collection network interface configured during the installation of CVC. Also note that, CVC would need appropriate network route and gateway configurations to ensure network connectivity to the sensor network on IE switches. This ensures network connectivity between CVC (For example, 10.10. 100.x subnet in CCI shared services network) and IE switches (172.16.10.x collection network for sensors). The following configurations must be done on the switch before installing a CV sensor in it: ■SSH ■IOx and storage formatting ■Data export using Encapsulated Remote Switched Port Analyzer (ERSPAN) ■Port configuration Use the following IP address schema to bring up the CVS application on IE3400/IE3300 10G and integrate it to the CVC. CVC Admin Interface (eth0): 10.104.206.225 Collection interface (eth1): 10.10.100.33 Collection network gateway: 10.10.100.1 NTP: 10.10.100.1 IE3300 10G Switch Admin IP address: 192.100.2.9 Subnet mask: 255.255.255.0 Management port: 443 Admin username: admin Admin password: sentryo69! CVS Capture IP address: 169.254.1.2 Capture subnet mask: 30 Capture VLAN number: 2508 Collection IP address: 172.16.10.249 Collection subnet mask: 24 Collection gateway: 172.16.10.1 Collection VLAN number: 1025 A prerequisite is the sensor application installed on the IE3400/IE3300 10G is to configure the switch for access to the CLI (ssh or console port). Configuration prerequisites needed on IE3300/IE3300 10G before installing the Sensor: ■Configure access to ssh ■Configure basic parameters The steps below show the necessary configuration needed on IE3300 10G or IE3400 switches for the sensor installation to then register it with the CVC. Format sdflash and enable IOx on the IE switch format sdflash: ext4 ! #show sdflash: filesys Filesystem: sdflash Filesystem Path: /flash11 Filesystem Type: ext4 Mounted: Read/Write ! configure terminal iox end ! #show iox #sh iox IOx Infrastructure Summary: ---------------------------- IOx service (CAF) : Running IOx service (HA) : Not Supported IOx service (IOxman) : Running IOx service (Sec storage) : Running Libvirtd 5.5.0 : Running Dockerd 18.03.0 : Running 6. Configure SVI in the Collection network VLAN for enabling sensor communication to CVC. interface Vlan1025 //VLAN 1025 is a Collection subnet VLAN ip address 172.16.10.250 255.255.255.0 end 7. To receive traffic inside an IOx application, you should make ensure that sure the AppGigabitEthernet port for communications can reach the IOx virtual application using the following commands. –Configure a VLAN for traffic mirroring: configure terminal vtp mode off vlan 2508 remote-span end ! interface AppGigabitEthernet 1/1 switchport mode trunk exit 8. Configure the SPAN session and add to the session the interfaces to monitor: monitor session 1 source interface Gi1/3 - 5, Gi1/7 - 10 monitor session 1 destination remote vlan 2508 monitor session 1 destination format-erspan 169.254.1.2 Note: The source of the monitor session in this configuration, is a range of access ports for endpoints to be monitored. 9. Save the configuration. wr mem Refer to the sensor installation "Initial Configuration" steps in the following Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, Cisco IE3400 and Cisco Catalyst 9300: After the switch has all necessary configurations, the sensor can be deployed using the Cyber Vision Center extension. First, install the extension by completing the steps below: 1. Download the extension (.ext file) from cisco.com. 2. In Cyber Vision Center, navigate to Admin > Extensions. 3. Click the Import Extension File button and then browse to the extension file. After the extension has been installed, install a sensor by completing the steps below: 1. In Cyber Vision Center, navigate to Admin > Sensors > Sensors. 2. Click the Deploy Cisco Device button: a. In the IP address field, enter the IP address of the switch. b. In the Port field, enter 443 for a network sensor. c. In the User field, enter the user name to log in to the switch. d. In the Password field, enter the password associated with the user account on the switch. e. In the Center IP field, you may enter the IP address of the Center that the sensors will use for communication. For dual interface Center deployments, it is recommended to enter the eth1 IP address as recommended. f. Under Capture mode, you may choose from the various options to change what data the sensor will process. In this validation, the Optimal (default) option was selected. g. Click Deploy. h. More configuration fields display. In the Capture IP address field, enter the ERSPAN destination IP address for the sensor. i. In the Capture prefix length field, enter the prefix associated with the ERSPAN IP address. j. In the Capture VLAN number field, enter the monitoring session destination VLAN k. In the Collection IP address field, enter the IP address of the eth0 interface of the sensor. This is the IP address that will be used for communication with the Center. l. In the Collection prefix length field, enter the prefix associated with the sensor IP address. m. In the Collection gateway field, enter the IP address of the gateway that the sensor will use for communicating through the network. n. In the Collection VLAN number, enter the VLAN of the sensor IP address. o. Under Application type, click the radio button of the type of sensor you wish to deploy. For the Passive and Active Discovery option, additional information is required: –In the IP address field, enter an IP address for the sensor to use in Active Discovery. Note that this IP address needs to be in the same subnet as the end devices you wish to discover. If active discovery is necessary on the same subnet as the sensor itself, you can click the USE COLLECTION button. – In the Prefix length field, enter the prefix associated with the IP address. – In the VLAN field, enter the VLAN for the subnet. –(Optional) Click the ADD ONE button to configure another Active Discovery interface. This secondary interface should be configured for doing active discovery on a different subnet than what was specified for the first interface. 3. Click Deploy. Refer to the "Procedure with the Cyber Vision sensor management extension" section for the detailed step-by-step instructions of CV sensor installation on IE3400 and IE3300 10G Series switches, in the following guide: The figure below shows the sensor status on the Cyber Vision Center dashboard after it has successfully installed on an IE switch. Navigate to Admin -> Sensors on the CVC dashboard. Figure 318 IE switch CV Sensor Status on CVC Dashboard After the sensor is running on the IE switch, you can view the data collected from the sensor on the CVC dashboard. For example, a CCTV Axis Camera device connected to the IE switch can be detected by Cyber Vision by monitoring the camera port traffic on the IE switch by the CV sensor. The figure below shows an Axis Camera device in CVC dashboard. To see sensor data, complete the steps below: 1. On CVC dashboard, navigate to Explore -> All data. 2. Click on Devices. 3. Select the device in the list to get more details on the device, as shown in the figure below. Figure 319 CVC Dashboard Device View 4. Click on the Device and Basics tab to see more details on the device, as shown in the figure below. Figure 320 CVC Dashboard Device Basics Activities -- These are the communication flows between components. From the Activities button on the Preset Dashboard, you can view these communications based on the time reference selected. Similarly, traffic flows detected by CV sensor are displayed in CVC dashboard by navigating to Explore -> All data -> Activity list. Refer to the following URL for MODBUS and DNP3 OT assets visibility. This section focuses on the components listed below discussing the interactions between the Cisco Cyber Vision Sensor application hosted on the IR1101 and the Cisco Cyber Vision Center used for managing the sensor application to provide OT traffic visibility in CCI RPoP. ■RPoP Cisco IR1101 Integrated Services Router Rugged ■Cisco Cyber Vision Sensor (CVS) application ■Cisco Cyber Vision Center (CVC) Cisco Cyber Vision Sensor application can be hosted as an Edge compute in IOX. Regular IOS perform the operation of routing the SCADA traffic. Sensor applications installed on IOX are passive sensors. The sensor application hosted on the IR1101 needs two interfaces, one to connect the sensor to the collection network interface of the Cyber Vision Center and one to monitor the traffic on local IOS interfaces. Cisco IR1101 IOx uses VirtualPortGroup as means to communicate between IOS and the IOx application. A logical mapping of VirtualPortGroup and the IOx Application is shown in the CCI2.1 General Design Guide. Refer to the following URL for more details of the Cyber Vison sensor design on CCI RPoP. This guide proposes using the Encapsulated Remote Switched Port Analyzer (ERSPAN) to monitor traffic on one or more routed ports or routed Switch Virtual Interfaces (SVI). The ERSPAN source sessions copy traffic from the source routed ports or SVIs and forwards the traffic using routable GRE-encapsulated packets to the ERSPAN destination session, which is the Cisco Cyber Vision Sensor application in this solution. Similarly, the application uses a separate interface to send the processed traffic to the collection network interface. To enable reachability of the collection network interface of the Center for the sensor, it is recommended to enable NAT on the VirtualPortGroup and overload using the IR1101 WAN facing interface. This section describes how to perform a clean installation of the sensor application (CVS) on the Cisco IR1101. As a prerequisite it is recommended to have the Cisco Cyber Vision Center installed and running. The following IP address schema has been used in this guide to bring up the CVS application on IR1101 and integrate it to the CVC as highlighted in the above figure above. CVC ■Admin Interface (eth0): 10.104.206.225 ■Collection interface (eth1): 10.10.100.33 ■Collection network gateway: 10.10.100.1 ■NTP: 10.10.100.1 IR1101 ■Management IP address: 192.168.100.80 ■Subnet mask: 255.255.255.0 ■Management port: 443 ■Admin username: admin ■Admin password: sentryo69! ■Capture IP address: 169.254.1.1 ■Capture subnet mask: 30 ■Collection IP address: 192.168.9.2 ■Collection subnet mask: 30 ■Collection gateway: 192.168.9.1 For the sensor application install on the IR1101, the prerequisite is to first configure the router for access to the CLI (ssh or console port). Below are the configuration prerequisites needed on IR1101 before installing the Sensor: ■Configure access to ssh on a CCI RPoP router ■Configure basic parameters. To bring up the IR1101 with sensor application (CVS) and have it registered with the CVC follow steps 8.1 to 8.3 in Section 8 "Procedure with the Cyber Vision Sensor Management Extension" in the Cisco Cyber Vision IR1101 installation guide here: The steps below show the necessary configuration needed on the IR1101 for the deployed sensor application to register with the CVC. 1. Setup ERSPAN (Encapsulated Remote Switched Port ANalyzer). To receive traffic inside an IOx application, you should make sure the app is connected to a VirtualPortGroup, and has the correct IP address by issuing the following commands. interface VirtualPortGroup0 description App ERSPAN ip address 169.254.1.1 255.255.255.252 end Create the monitor session: monitor session 1 type erspan-source source interface Tu10 destination erspan-id 1 mtu 1464 ip address 169.254.1.2 origin ip address 169.254.1.1 2. Setup NAT Add NAT rules so that the container can ping the outside. This will be on a different virtual port group than the ERSPAN to separate the traffic. On the Cellular interface: interface Cellular0/1/0 : mtu 1430 ip address negotiated ip nat outside ip tcp adjust-mss 1313 dialer in-band dialer idle-timeout 0 dialer watch-group 1 dialer-group 1 ipv6 enable pulse-time 1 ip virtual-reassembly end On the Tunnel/Loopback interface: interface Tunnel10 ip unnumbered Loopback10 ip mtu 1400 ip nat outside ip tcp adjust-mss 1283 tunnel source Cellular0/1/0 tunnel destination tunnel protection ipsec profile default_No_cert end interface Loopback10 ip address 192.168.100.80 255.255.255.255 ip nat outside end On VirtualPortGroup1, interface VirtualPortGroup1 ip address 192.168.9.1 255.255.255.252 ip nat inside ip tcp adjust-mss 1330 end Configure the Access list for the VirtualPortGroup1 to reach outside the container via tunnel interface: ip access-list standard NAT_ACL 10 permit 192.168.9.0 0.0.0.3 ip nat inside source list NAT_ACL interface Loopback10 overload 3. Save the configuration. Exit write mem After a few minutes the sensor displays as connected in Cisco Cyber vision after following any one of three ways to install the sensor on Cisco IR1101 as described in the "Cisco Cybervision IR1101 Installation Guide". After the prerequisites are met (section 6 and section 8.1 to 8.3), there are three ways to install the Cyber Vision Sensor on IR1101: ■Via Local Manager – Follow Section 7.1 to 7.5 in above guide ■Via CLI – Follow section 9.1 to 9.3 ■Via Cisco Cyber Vision Center Extension – Follow section 8.1 to 8.3 Note: When the IR1101 IoX sensor is deployed via Cyber Vision Extension Feature, make sure to configure "ip tcp adjust-mss 1330" on VirtualPortGroup1 of IR1101 and Virtual-template interface on Head End Router (in DMZ) where IR1101 Tunnel interface is connected. After the sensor is installed and connected to CVC successfully, you see the Sensor status on CVC, as shown in the figure below. Figure 321 IR1101 CV Sensor Status on Cyber Vision Center This chapter provides the detailed implementation of CCI network QoS for the CCI Solution CVD, Release 2.1QoS design considerations, as discussed in the Cisco CCI General Solution Design Guide. Implementing QoS in CCI network ensures efficient use of CCI network resources and provide preferential of differential treatment to business critical and other classes of traffic in the network. This chapter includes the following major topics: ■Configuring QoS on Fabric and Backhaul Network Devices Using SD-Access ■Configuring QoS on Ethernet Access Ring Cisco DNA Center SD-Access provides the Application Policy feature, which includes various classes of predefined applications, application sets, and traffic queuing profiles. This Application Policy feature is leveraged to implement the QoS on CCI network devices like FiaB in PoP sites and other non-fabric/intermediate and backhaul network devices in the CCI network to deploy end-to-end QoS policy. This section covers QoS deployment on fabric/non-fabric devices (excluding extended in the access ring), with an example configuration of application policies using Cisco DNA Center. For detailed step-by-step instructions for configuring QoS application policies, refer to the section "Application Policies" under the chapter "Configure Policies" in the Cisco Digital Network Architecture Center User Guide, Release 2.2.3 at the following URL: ■ Note: QoS Application Polices configured using Cisco DNA Center for non-fabric devices is applicable only for Cisco DNA Center-supported switches/routers hardware models. This is because the QoS features support and/or hardware queuing differs from device to device. 1. Creating a Queuing Profile: A Queuing profile, as per the QoS design consideration for different classes of traffic, must be created in Cisco DNA Center to allocate the percent of network interface bandwidth. The bandwidth percentage values are chosen based on design guidelines available at the link below in the section "CCI Network QoS Design": – a. On Cisco DNA Center GUI, navigate to Policy-> Application QoS -> Queuing Profiles. b. Click +Add Profile to add a new Queuing Profile (example: CCI_Queuing_Profile). c. Allocate the Bandwidth percentage for all applications and save the profile. Figure 322 shows an example queuing profile created for the CCI network in Cisco DNA Center. Figure 322 Cisco DNA Center Application Policy Queuing Profile Example 2. Creating a QoS Application Policy: An application policy must be created and attached to the queuing profile and sites in the policy must be selected for deploying the policy on network devices in each PoP site and other non-fabric/intermediate and/or backhaul network devices in CCI network. a. Navigate to Policy -> Application QoS -> Application Policies. b. Click + Add Policy and name the policy (example: CCI_QoS_Policy). c. Select the Queuing profile and add the Queuing profile created in the previous step (example: CCI_Queuing_Profile), as shown in Figure 323. d. Select the Sites to which the policy has to be applied. e. While adding Sites, select Site settings, exclude the devices which are not needed, and then click Save. f. Then associate the application sets to Business Relevant, Default, and Business Irrelevant, as shown in Figure 323. Figure 323 Cisco DNA Center Application Policy Creation for QoS Deployment 3. Pre-check and deploy the QoS policy: Before deploying the QoS configuration on network devices, you should preview the QoS configuration to be applied on the Preview option: a. Preview the configuration changes on the devices before deployment by selecting the Preview option and generating the configuration to view the changes. b. Then, click Pre-check to make sure there are no errors and warnings before deployment, as shown in Figure 324. Figure 324 Cisco DNA Center QoS Policy Pre-Check c. If the Pre-check is successful, click Deploy to apply the policy to all the devices included in deployment. An example QoS configuration that will be deployed on the device by Queuing Profile and Application Policy is as follows: C9300-20-STACK#show run policy-map class-map match-any DNA-EZQOS_2P6Q3T_9K#BULK-DATA match dscp cs1 match dscp af11 match dscp af13 match dscp af11 class-map match-any DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE match dscp cs3 match dscp cs6 match dscp cs7 match dscp cs2 class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING match dscp af43 match dscp af41 match dscp af42 class-map match-any DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2 match dscp cs5 match dscp cs4 class-map match-any DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1 match dscp ef class-map match-any DNA-EZQOS_2P6Q3T_9K#TRANSACTIONAL-DATA match dscp af23 match dscp af21 match dscp af22 class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING match dscp af32 match dscp af33 match dscp af31 end C9300-20-STACK#show run policy-map #Policy map applied from QoS Policy policy-map DNA-dscp#APIC_QOS_Q_OUT class DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1 priority level 1 police rate percent 2 queue-buffers ratio 10 class DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2 priority level 2 police rate percent 26 queue-buffers ratio 5 class DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE bandwidth remaining percent 2 queue-buffers ratio 5 class DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING bandwidth remaining percent 1 queue-buffers ratio 10 queue-limit dscp af41 percent 100 queue-limit dscp af42 percent 90 queue-limit dscp af43 percent 80 class DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING bandwidth remaining percent 1 queue-buffers ratio 10 queue-limit dscp af32 percent 90 queue-limit dscp af33 percent 80 class DNA-EZQOS_2P6Q3T_9K#TRANSACTIONAL-DATA bandwidth remaining percent 42 queue-buffers ratio 10 random-detect dscp-based random-detect dscp 18 percent 80 100 random-detect dscp 20 percent 70 100 random-detect dscp 22 percent 60 100 class DNA-EZQOS_2P6Q3T_9K#BULK-DATA bandwidth remaining percent 8 queue-buffers ratio 10 random-detect dscp-based random-detect dscp 8 percent 60 100 random-detect dscp 10 percent 80 100 random-detect dscp 12 percent 70 100 random-detect dscp 14 percent 60 100 class class-default bandwidth remaining percent 27 queue-buffers ratio 25 random-detect dscp-based random-detect dscp 0 percent 80 100 end Then the policy is attached to all the selected interfaces on the device as shown below: interface TenGigabitEthernet 1/1/1 service-policy output DNA-dscp#APIC_QOS_Q_OUT Note: This example shows an egress service policy (egress traffic) created as a unidirectional QoS policy based on the FiaB device role in Cisco DNA Center. This completes the QoS deployment on all fabric and non-fabric devices in the CCI network. QoS configuration, as per the design, is to be configured manually and using Application QoS in Cisco DNA Center on the Ethernet access ring consisting of IE switches (extended and policy extended nodes non-extended nodes) in each PoP site. However, the QoS configurations on legacy IE switches (IE4000/IE5000/IE3300) discussed in this section can also be automated and provisioned on all IE switches leveraging the Cisco DNA Center Configuration Templates feature. This section covers the high-level steps to configure QoS with an example configuration on IE4000/IE5000 switches in the access ring of a PoP site. Refer to the chapter "Configuring Quality of Service (QoS)" in the Cisco Industrial Ethernet 4000, 4010 and 5000 Switch Software Configuration Guide, for detailed step-by-step instructions on QoS configuration. Complete the following steps to configure QoS on IE4000/IE5000 switches in the access ring: 1. Create Access Lists to match Incoming Traffic Create an access list to match incoming Operational Technology (OT) and Quarantine traffic in CCI network in global configuration mode. In this example configuration, 172.20.x.x and 172.99.x.x are used as the source network, which identifies OT and Quarantine traffic, respectively. access-list 101 permit ip 172.10.0.0 0.0.255.255 any access-list 102 permit ip 172.20.0.0 0.0.255.255 any 2. Create Class-map to Classify Traffic QoS policy class-maps must be created on IE switches to classify and mark the incoming traffic for preferential QoS treatment. The following configuration shows different class-map created to match incoming traffic based on access list (video and OT traffic) and DSCP values for other classes of traffic like network control, signaling, management, voice, and scavenger in the network: class-map match-any VOICE_VIDEO_PQ_OUT1 match ip dscp cs5 Match ip dscp cs4 Match ip dscp ef Class-map match-any NW_CONTROL Match ip dscp cs6 cs7 Class-map match-any SIGNALING Match ip dscp cs3 Class-map match-any MM_CONF_STREAM_OAM_OT Match ip dscp af41 af42 af43 af31 af32 af33 af21 af22 af23 class-map match-any SCAVENGER_QUARANTINE_TRAFFIC match ip dscp cs1 Class-map match-any BULK_DATA match ip dscp af11 af12 af13 class-map match-any SCAVENGER_BULK_DATA_TRAFFIC match ip dscp cs1 af11 af12 af13 class-map match-any VOICE match ip dscp ef class-map match-any VIDEO match ip dscp af41 af42 af43 Match ip dscp af31 af32 af33 Match ip dscp af21 af22 af23 class-map match-any VIDEO_PQ match ip dscp cs4 cs5 class-map match-any QUARANTINE_TRAFFIC match access-group 102 class-map match-any CCI_OT_TRAFFIC match access-group 101 3. Create Policy-map to classify and mark the incoming traffic: policy-map CCI_IE_QoS_Input_Policy class VOICE_VIDEO_PQ_OUT1 priority police 300000000 class NW_CONTROL_SIG_OAM_OUT1 bandwidth percent 15 queue-limit dscp cs6 percent 100 class CCI_OT_TRAFFIC set qos-group 2 class QUARANTINE_TRAFFIC set qos-group 1 4. Create the output policy-map: policy-map CCI_IE_QoS_Output_Policy class CCI_OT_TRAFFIC bandwidth percent 25 policy-map CCI_IE_QoS_Input_Policy class VOICE set dscp ef class VIDEO set dscp cs4 class NW_CONTROL_SIG_OAM_OUT1 set qos-group 1 set ip dscp cs6 class VOICE_PQ set qos-group 1 set ip dscp ef class CCI_OT_TRAFFIC set qos-group 3 set dscp af21 ! 5. Apply the Input and Output QoS service policies on all the switch ports. Example on an IE switch port (GigabitEthernet1/1) the following configuration is added: interface GigabitEthernet1/1 service-policy input CCI_IE_QoS_Input_Policy service-policy output CCI_IE_QoS_Output_Policy 6. Repeat the above steps for all the switch ports in the PoP site access ring. Alternatively, the above QoS configuration can be automated to configure on all the IE switches in the ring using the Cisco DNA Center template feature. The Cisco DNA Center provides an interactive editor called Template Editor to author CLI templates. Templates can be easily designed with a predefined configuration by using parameterized elements or variables. After creating a template, the template can be used on the devices in one or more sites. For information on how to use templates refer to the Create Templates to Automate Device Configuration Changes of Cisco DNA Center section of the User Guide, Release 2.2.3 at To configure QoS on the IE3300 switches through the Cisco DNA Center Template Editor, complete the following steps: 1. Create a template by navigating to Tools-> Template Editor. 2. Create a project, then create the template by clicking on the + symbol and selecting the option. 3. Select template type as Regular and language as Velocity. 4. Enter the name of the template and select the project you created in step 2 from the drop-down menu. 5. Select the device type IE3300 from the list of drop downs as shown in the figure below. Figure 325 Adding a Template for QoS configuration 6. Select the software type. 7. Click Add. 8. In the template window enter the set of QoS configs for IE3300 as shown in figure below Figure 326 Configuring QoS using DNAC Templates The following is a sample config for the template : Configure t access-list 102 permit ip 172.99.0.0 0.0.255.255 any access-list 101 permit ip 172.20.0.0 0.0.255.255 any class-map match-any CCI_OT_TRAFFIC match access-group 101 class-map match-any QUARANTINE_TRAFFIC match access-group 102 class-map match-any DNA-EZQOS_1P7Q3T#REALTIME match dscp ef match dscp cs5 match dscp cs4 class-map match-any DNA-EZQOS_1P7Q3T#CONTROL match dscp cs7 match dscp cs6 match dscp cs3 match dscp cs2 class-map match-any DNA-EZQOS_1P7Q3T#MM_STREAM match dscp af31 match dscp af32 match dscp af33 class-map match-any DNA-EZQOS_1P7Q3T#MM_CONF match dscp af41 match dscp af42 match dscp af43 class-map match-any DNA-EZQOS_1P7Q3T#TRANS_DATA match dscp af21 match dscp af22 match dscp af23 class-map match-any DNA-EZQOS_1P7Q3T#BULK_DATA match dscp af11 match dscp af12 match dscp af13 class-map match-any DNA-EZQOS_1P7Q3T#SCAVENGER match dscp cs1 policy-map CCI_IE_QoS_Output_Policy class DNA-EZQOS_1P7Q3T#REALTIME bandwidth percent 30 class DNA-EZQOS_1P7Q3T#CONTROL bandwidth percent 10 class DNA-EZQOS_1P7Q3T#MM_STREAM bandwidth percent 10 class DNA-EZQOS_1P7Q3T#MM_CONF bandwidth percent 10 class DNA-EZQOS_1P7Q3T#TRANS_DATA bandwidth percent 10 class DNA-EZQOS_1P7Q3T#BULK_DATA bandwidth percent 4 class DNA-EZQOS_1P7Q3T#SCAVENGER bandwidth percent 1 class class-default bandwidth percent 25 9. Save the template and commit. 10. Associate the created template to the network profile by navigating to Design-> Network Profiles and click Edit on the corresponding network profile. 11. Provision the template to the devices by navigating to Provision-> Inventory-> Device-> Actions->Provision->Provision Device and then following the screen till Deploy. 12. After the Template is successfully deployed, verify that the above configs have been pushed on the device SN-FOC2351V05A#show policy-map Policy Map CCI_IE_QoS_Output_Policy Class DNA-EZQOS_1P7Q3T#REALTIME bandwidth 30 (%) Class DNA-EZQOS_1P7Q3T#CONTROL bandwidth 10 (%) Class DNA-EZQOS_1P7Q3T#MM_STREAM bandwidth 10 (%) Class DNA-EZQOS_1P7Q3T#MM_CONF bandwidth 10 (%) Class DNA-EZQOS_1P7Q3T#TRANS_DATA bandwidth 10 (%) Class DNA-EZQOS_1P7Q3T#BULK_DATA bandwidth 4 (%) Class DNA-EZQOS_1P7Q3T#SCAVENGER bandwidth 1 (%) Class class-default bandwidth 25 (%) -----some output has been omitted----- To configure QoS on IE3300 and IE3400 switches through Application QoS in Cisco DNA Center, complete the following steps: Figure 327 Application QoS Policy Figure 328 Creating custom Application Figure 329 Custom QoS Application Figure 330 Assigning the Custom Application to the Business Relevant Figure 331 Creating custom Application 10. Click Deploy. 11. Verify the policy created on the switch by issuing show policy-map and sh run interface command. Current configuration : 164 bytes ! interface GigabitEthernet1/1 service-policy input DNA-APIC_QOS_IN service-policy output DNA-APIC_QOS_Q_OUT end policy-map DNA-APIC_QOS_IN class DNA-APIC_QOS_IN#CONTROL set dscp cs6 class DNA-APIC_QOS_IN#MM_CONF set dscp af41 class DNA-APIC_QOS_IN#MM_STREAM set dscp af31 class DNA-APIC_QOS_IN#TRANS_DATA set dscp af21 class DNA-APIC_QOS_IN#BULK_DATA set dscp af11 class DNA-APIC_QOS_IN#SCAVENGER set dscp cs1 class class-default set dscp default Policy Map DNA-APIC_QOS_Q_OUT Class DNA-EZQOS_1P7Q3T#REALTIME priority level 1 Class DNA-EZQOS_1P7Q3T#CONTROL bandwidth remaining 10 (%) Class DNA-EZQOS_1P7Q3T#MM_CONF bandwidth remaining 10 (%) Class DNA-EZQOS_1P7Q3T#MM_STREAM bandwidth remaining 10 (%) Class DNA-EZQOS_1P7Q3T#TRANS_DATA bandwidth remaining 14 (%) Class DNA-EZQOS_1P7Q3T#BULK_DATA bandwidth remaining 5 (%) Class DNA-EZQOS_1P7Q3T#SCAVENGER bandwidth remaining 1 (%) Class class-default bandwidth remaining 25 (%) -----some output has been omitted----- This completes the QoS configuration on IE3300 & IE3400 using Application QoS. Multicast is a useful technology that allows communication to a group of devices in an efficient manner. Whereas unicast is used in one-to-one communication and broadcast is one-to-all communication, multicast is one-to-many or many-to-many communication. This is well suited to video streaming or other streaming type services where many receivers subscribe to a server to receive the same stream. In a unicast only environment, the traffic would increase linearly with each new client receiving the stream until the slowest link is saturated. With broadcast, every client in a network would receive the stream and then have to discard it if not subscribed, creating a large amount of network traffic and system churn. In a multicast environment, the source sends the traffic stream once and only interested receivers subscribe to it. Intermediate routers and switches that perform multicast routing increase the efficiency by only replicating the traffic to those hosts that subscribe to a stream. In this scenario a source does not even have to know when there is a receiver or how many receivers there may be. With a unicast stream, the source would have to maintain a connection to each receiver which could quickly drain its resources with a large number of receivers. In the context of SDA, multicast takes on another dimension because it can be supported in the underlay or the overlay. When multicast is configured on the underlay, this is known as native multicast from the Cisco DNA Center workflow. When configured in the overlay, it is known as head-end replication. Native multicast is beneficial when the source and receivers are co-located in a PoP site and the receivers are spread out over a number of fabric edge nodes. As the name suggests, head-end replication requires the head-end router, usually the border node, to create multiple unicast copies of the multicast traffic and send them to all the fabric edge nodes where receivers are located. With native multicast, the overlay multicast groups are mapped to an SSM group in the underlay and the underlay devices participate in the replication of the multicast traffic to the other fabric edge devices. The downside to the native multicast implementation is that manual configuration is required on all fabric devices. Also, if the source is outside the fabric, the efficiencies of native multicast may not be fully realized as the fabric border node becomes the head-end replication point. As mentioned in the Design Guide and for this implementation guide, only head-end replication is supported and tested. Within the overlay network, two different multicast implementations are available, Any Source Multicast (ASM) and Source Specific Multicast (SSM). ASM relies on group addresses where a source publishes to a specific multicast address and then any number of receivers indicate they want to receive traffic from that group address. This request to a group address is seen in the multicast routing table as (*,G) where the * is any source and the G represents the group address. When a receiver starts receiving the traffic from that source, the network node creates an entry in the multicast routing table called (S,G) where the S represents the IP address of the source. ASM relies on a routing protocol to manage the location of receiver membership requests. The protocol supported by Cisco DNA Center is Protocol Independent Multicast (PIM) and specifically, PIM Sparse mode. In this configuration, PIM Sparse mode creates a Shared Path Tree (SPT) that allows sources and receivers to locate each other. This requires designating one node as the Rendezvous Point (RP) which forms the root of the SPT. While the IOS feature set supports numerous dynamic methods of choosing an RP, the Cisco DNA Center workflow only supports a static RP configuration. Therefore, it is important to consider where the sources and receivers are when choosing the rendezvous point. The other option for multicast in the overlay is Source Specific Multicast (SSM). In this mode, a receiver expresses interest in a multicast group from a specific source as opposed to any source. This serves to reduce the amount of multicast traffic in the network. The multicast router only has to record the (S,G) entry instead of the additional (*,G) entry. The other advantage is that a rendezvous point is not necessary to support SSM. The disadvantage is that only IPv4 IGMP3 and IPv6 MLDv2 support this feature. The receiver's operating system must also support this feature. In the CCI network, two scenarios are supported, multicast within a PoP site and multicast between PoP sites. Because of how Cisco DNA Center configures the multicast deployment, it is not recommended to support both scenarios in the same VN overlay when using ASM. This is due to the placement of the RP and whether it is external or internal to the fabric site. This chapter includes the following major topics: ■Configuring SD Access Multicast within a PoP ■Configuring Multicast between PoP Sites If a source and its receivers are primarily within a fabric PoP or if the source and receivers are not separated by an MPLS IP transit, the multicast configuration is very straight forward from the Cisco DNA Center workflow. An example topology showing the multicast source and receivers is below in Figure 332. Figure 332 Multicast within a PoP Site—Source and Receiver within PoP Below is an example showing the multicast source outside the fabric with the receivers in a single fabric. Figure 333 Multicast within a PoP Site—Source Outside and Receivers Inside PoP Cisco DNA Center must first be configured to enable multicast in every site where the receivers may be located. The workflow for this starts at the Fabric Site within the Fabric Provisioning section, as shown in Figure 334. Figure 334 Edit Multicast in a Fabric Site The option for multicast will say "Configure Multicast" if not enabled or "Edit Multicast" if enabled. Within the multicast wizard, it will require configuring whether the site is using head-end replication versus native multicast, the virtual network, whether ASM or SSM is used in the overlay, the IP pool to be mapped, and the location of the rendezvous point whether internal or external. As mentioned before, head-end replication is being used in CCI to minimize the amount of manual configuration on the network devices. The decision needs to be made whether ASM or SSM will be supported in the overlay. As mentioned before, choosing ASM requires also choosing a rendezvous point. When enabling multicast within a PoP site, an internal rendezvous point should be chosen. Note that this configuration creates a single PIM domain within the fabric site and if inter-PoP multicast traffic needs to occur at a later time, additional manual configuration will need to be added or the setup needs to change per the section discussing multicast between PoP sites. Figure 335 Internal Rendezvous Point The workflow will then ask which fabric node is to be the internal RP and since PoP is using a fabric in a box setup, that node should be chosen as the RP as seen below. Figure 336 Choosing Node to be Internal Rendezvous Point After configuring the internal RP, the multicast summary should look like the one in Figure 337. Figure 337 Intra PoP Multicast Summary After deploying the multicast configuration, the fabric nodes will be configured with the appropriate commands. The commands added on the fabric in a box node are given below. Switched Virtual Interface for VN: ip pim passive ip route-cache same-interface ip igmp version 3 ip igmp explicit-tracking Loopback: interface Loopback4111 vrf forwarding Train2Track ip address 172.16.7.129 255.255.255.255 ip pim sparse-mode end LISP Interface: interface LISP0.4111 ip pim sparse-mode end PIM and Multicast are also enabled at the global level for the VRF. ip pim vrf Train2Track rp-address 172.16.7.129 ip pim vrf Train2Track register-source Loopback4111 ip pim vrf Train2Track ssm default ip multicast-routing vrf Train2Track Note that SSM is enabled even when ASM is configured as part of the workflow. By default, SSM uses the multicast group range of 232.0.0.0/8. To validate multicast traffic a source must send traffic to a multicast group. In this example, the source traffic was a video stream to group address 239.10.10.10. Receivers must also subscribe this group address to receive the data. Below is the output of the fabric in a box multicast routing table from the source to a receiver. (*, 239.10.10.10), 3d20h/stopped, RP 172.16.7.129, flags: SJCF Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: Vlan1026, Forward/Sparse-Dense, 3d20h/00:02:52 (172.16.14.131, 239.10.10.10), 3d20h/00:02:44, flags: PFT Incoming interface: Vlan1026, RPF nbr 0.0.0.0 Outgoing interface list: Null The other option for multicast in the overlay is Source Specific Multicast (SSM). In this mode, a receiver expresses interest in a multicast group from a specific source as opposed to any source. This serves to reduce the amount of multicast traffic in the network. The multicast router only has to record the (S,G) entry instead of the additional (*,G) entry. The other advantage is that a rendezvous point is not necessary to support SSM. The disadvantage is that only IPv4 IGMP3 and IPv6 MLDv2 support this feature. The receiver's operating system must also support this feature. By default, when ASM is configured from the Cisco DNA Center workflow, SSM is also configured at the same time. The default option enables SSM for the multicast group 232.0.0.0/8. If a different multicast group is desired, the SSM option in the multicast workflow in Cisco DNA Center supports a custom group address. When SSM is specifically configured, there is no option to add a rendezvous point. The differences in the Cisco DNA Center workflow are shown below. Figure 338 Select SSM Figure 339 Choose SSM Range The PIM configuration on the fabric node is also different since the SSM range is no longer the default group range. ip pim vrf Train2Track ssm range SSM_RANGE_Train2Track ip access-list standard SSM_RANGE_Train2Track 10 permit 235.0.0.0 0.255.255.255 The below examples are using the default SSM range. To verify SSM functionality, the multicast source sends the video stream to a group address in 232.0.0.0/8. The multicast receiver must then subscribe to the host IP of the source @ the group address. In VLC, this is configured as rtp://@: Below is the Mroute validation on the fabric in a box. The source and receiver are connected on different fabric devices. (172.16.14.131, 232.10.10.10), 00:05:39/00:02:26, flags: sPTI Incoming interface: Vlan1026, RPF nbr 0.0.0.0 Outgoing interface list: Null Before configuring multicast using IP Transit, several things must be considered. These include the location of the sources and receivers, the multicast configuration of the service provider core, and whether Any Source Multicast (ASM) or Source Specific Multicast (SSM) will be used in the network overlay. To minimize the amount of manual configuration with ASM, it is recommended to place a multicast source behind the fusion router or at the data center fabric site. The rendezvous point could then be centrally located if the receivers are at the edge fabric sites. It should be noted that when configuring ASM through the Cisco DNA Center workflow, SSM with the default multicast group range (232.0.0.0/8) is also configured on the fabric node. This section will describe the configuration from the Cisco DNA Center workflow as well as show the configuration from the fusion router and fabric nodes. A sample configuration for the service provider core will also be shown. An example of the test configuration is shown in Figure 340. Figure 340 Multicast over an MPLS IP Transit Prior to configuring multicast, IP pools must be configured in Cisco DNA Center under Design -> Network Settings -> IP Address Pools and then reserved in each site. In this example, the multicast source is behind the fusion router with the receivers in a VN. The VRF for the VN is extended to the multicast source to prevent the need for route leaking. Cisco DNA Center must then be configured to enable multicast in every site where the receivers may be located. The workflow for this starts at the Fabric Site within the Fabric Provisioning section seen in Figure 341 Figure 341 Edit Multicast in a Fabric Site The option for multicast will say "Configure Multicast" if not enabled or "Edit Multicast" if enabled. Within the multicast wizard, it will require configuring whether the site is using head-end replication versus native multicast, the virtual network, whether ASM or SSM is used in the overlay, the IP pool to be mapped, and the location of the rendezvous point whether internal or external. With the source behind the fusion router, the rendezvous point will point to an IP address in the VRF configured on the fusion router. When configuring the fabric sites, the external rendezvous point option must be chosen, and the previously mentioned IP address configured. Figure 342 External Rendezvous Point After deploying the multicast config, the fabric nodes will be configured with the appropriate commands. The commands added on the fabric in a box node are shown below. 266 Switched Virtual Interface for VN: interface Vlan1029 ip pim passive ip route-cache same-interface ip igmp version 3 ip igmp explicit-tracking Loopback: interface Loopback4111 vrf forwarding Train2Track ip address 172.16.7.66 255.255.255.255 ip pim sparse-mode end LISP Interface: interface LISP0.4111 ip pim sparse-mode end Border Interface: ip pim sparse-mode ip route-cache same-interface PIM and Multicast are also enabled at the global level for the VRF. ip pim vrf Train2Track rp-address 172.16.140.1 ip pim vrf Train2Track register-source Loopback4111 ip pim vrf Train2Track ssm default ip multicast-routing vrf Train2Track Note that SSM is enabled even when ASM is configured as part of the workflow. By default, SSM uses the multicast group range of 232.0.0.0/8. The fusion router and all devices up to the multicast source must also be configured to support multicast. This includes enabling PIM sparse-mode on all intermediate interfaces as well as multicast routing. A sample configuration for the fusion router is given below. Source facing interface: interface GigabitEthernet0/0/5.140 encapsulation dot1Q 140 vrf forwarding Train2Track ip address 172.16.140.1 255.255.255.252 ip pim sparse-mode ip igmp version 3 Configure fusion router as rendezvous point: ip pim vrf Train2Track rp-address 172.16.140.1 Configure multicast routing ip multicast-routing vrf Train2Track distributed An MPLS IP transit is used in this implementation between the fabric sites and must also be configured to pass multicast traffic. As described here: there are numerous ways to implement MVPN. For this implementation, Profile 0 or Rosen Draft was chosen. The MPLS core and therefore the multicast configuration is likely provided by a service provider so the choice of other MVPN profiles is outside the scope of this document. It is important to note that the provider multicast network is separate from the customer multicast network and serves to transport the different customer's multicast traffic in the most efficient way possible. With this configuration, PIM runs on all the core interfaces and all the PEs in a multicast VRF (MVRF) become PIM neighbors by way of GRE tunnels. The PEs learn about other PIM neighbors using BGP. Each core facing interface as well as the interface in the multicast VRF should be configured for PIM sparse-mode. To configure the VRF for Rosen Draft, Multicast Distribution Tree (MDT) will be used. A default MDT is required, but a data MDT can also be used for higher bandwidth applications. vrf definition cci-trackside rd 31:6 ! address-family ipv4 mdt default 232.0.0.1 mdt data 232.1.1.0 0.0.0.255 route-target export 31:31 route-target import 31:31 exit-address-family BGP passes the multicast information using the extended communities attribute and is configured in the global BGP config. address-family ipv4 mdt neighbor 10.3.255.1 send-community extended neighbor 10.3.255.1 activate exit-address-family PIM and Multicast routing must also be configured on each PE. ! Enables SSM in the provider multicast network ip pim ssm default ! Configures the RP for the particular Customer VRF (fusion router) ip pim vrf cci-trackside rp-address 172.16.140.1 ! Enables global multicast routing ip multicast-routing distributed ! Enables multicast routing for the Customer VRF ip multicast-routing vrf cci-trackside distributed On the core routers, the configuration is the same as the provider edge routers except for the lack of customer VRFs. After the MPLS core is configured, PIM neighborships will form over the GRE tunnels to every PE with the multicast VRF configured. An example of the MVRF PIM neighbor table is below. Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority, P - Proxy Capable, S - State Refresh Capable, G - GenID Capable, L - DR Load-balancing Capable Neighbor Interface Uptime/Expires Ver DR Address Prio/Mode 172.16.15.1 BDI3036 1d21h/00:01:16 v2 1 / S P G 172.16.1.57 BDI3037 1d22h/00:01:24 v2 1 / S P G 10.3.255.2 Tunnel0 3w0d/00:01:21 v2 1 / S P G 172.16.2.1 BDI3018 1d21h/00:01:41 v2 1 / S P G To validate multicast traffic a source must send traffic to a multicast group. In this example, the source traffic was a video stream to group address 239.10.10.10. Receivers must also subscribe this group address to receive the data. Below is the output of the multicast routers from the source to a receiver. show ip mroute vrf Fusion Router: (*, 239.10.10.10), 1d02h/00:03:27, RP 172.16.140.1, flags: SF Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: GigabitEthernet0/0/0.31, Forward/Sparse, 1d01h/00:03:27 Te0/2/0.3033, Forward/Sparse, 1d02h/00:02:56 (172.16.140.2, 239.10.10.10), 1d01h/00:03:00, flags: FT Incoming interface: GigabitEthernet0/0/5.140, RPF nbr 0.0.0.0 Outgoing interface list: GigabitEthernet0/0/0.31, Forward/Sparse, 1d01h/00:03:27 Te0/2/0.3033, Forward/Sparse, 1d01h/00:03:24 Ingress Provider Edge Router: (*, 239.10.10.10), 00:12:16/00:03:02, RP 172.16.140.1, flags: S Incoming interface: BDI31, RPF nbr 10.2.1.93 Outgoing interface list: Tunnel0, Forward/Sparse, 00:12:16/00:03:02 (172.16.140.2, 239.10.10.10), 00:12:16/00:03:17, flags: Ty Incoming interface: BDI31, RPF nbr 10.2.1.93 Outgoing interface list: Tunnel0, Forward/Sparse, 00:12:16/00:03:02 Egress Provider Edge Router: (*, 239.10.10.10), 00:14:28/00:03:25, RP 172.16.140.1, flags: S Incoming interface: Tunnel0, RPF nbr 10.3.255.2 Outgoing interface list: BDI3037, Forward/Sparse, 00:11:53/00:03:25 BDI3018, Forward/Sparse, 00:14:28/00:02:50 (172.16.140.2, 239.10.10.10), 00:14:28/00:02:53, flags: TY Incoming interface: Tunnel0, RPF nbr 10.3.255.2, MDT:[10.3.255.2,232.1.1.0]/00:02:41 Outgoing interface list: BDI3037, Forward/Sparse, 00:11:53/00:03:28 BDI3018, Forward/Sparse, 00:14:28/00:02:50 Fabric in a Box: (*, 239.10.10.10), 00:19:28/stopped, RP 172.16.140.1, flags: SJC Incoming interface: Vlan3037, RPF nbr 172.16.1.58 Outgoing interface list: Vlan1029, Forward/Sparse-Dense, 00:19:28/00:02:12 (172.16.140.2, 239.10.10.10), 00:19:28/00:02:04, flags: JT Incoming interface: Vlan3037, RPF nbr 172.16.1.58 Outgoing interface list: Vlan1029, Forward/Sparse-Dense, 00:19:28/00:02:12 The other option for multicast in the overlay is Source Specific Multicast (SSM). In this mode, a receiver expresses interest in a multicast group from a specific source as opposed to any source. This serves to reduce the amount of multicast traffic in the network. The multicast router only has to record the (S,G) entry instead of the additional (*,G) entry. The other advantage is that a rendezvous point is not necessary to support SSM. The disadvantage is that only IPv4 IGMP3 and IPv6 MLDv2 support this feature. The receiver's operating system must also support this feature. By default, when ASM is configured from the Cisco DNA Center workflow, SSM is also configured at the same time. The default option enables SSM for the multicast group 232.0.0.0/8. If a different multicast group is desired, the SSM option in the multicast workflow in Cisco DNA Center supports a custom group address. When SSM is specifically configured, there is no option to add a rendezvous point. The differences in the Cisco DNA Center workflow are shown below. Figure 343 Select SSM Figure 344 Choose SSM Range The PIM configuration on the fabric node is also different since the SSM range is no longer the default group range. ip pim vrf Train2Track ssm range SSM_RANGE_Train2Track ip access-list standard SSM_RANGE_Train2Track 10 permit 235.0.0.0 0.255.255.255 The examples below use the default SSM range. To verify SSM functionality, the multicast source sends the video stream to a group address in 232.0.0.0/8. The multicast receiver must then subscribe to the host IP of the source @ the group address. In VLC, this is configured as rtp://@: Below is the Mroute validation on the multicast routers between the source and receiver. Fusion Router: (172.16.140.2, 232.10.10.10), 00:33:25/00:03:19, flags: sT Incoming interface: GigabitEthernet0/0/5.140, RPF nbr 0.0.0.0 Outgoing interface list: Te0/2/0.3033, Forward/Sparse, 00:32:41/00:03:19 GigabitEthernet0/0/0.31, Forward/Sparse, 00:33:25/00:02:33 Ingress Provider Edge Router: (172.16.140.2, 232.10.10.10), 00:13:04/00:03:05, flags: sTy Incoming interface: BDI31, RPF nbr 10.2.1.93 Outgoing interface list: Tunnel0, Forward/Sparse, 00:13:13/00:03:05 Egress Provider Edge Router: (172.16.140.2, 232.10.10.10), 00:13:04/00:03:05, flags: sTy Incoming interface: BDI31, RPF nbr 10.2.1.93 Outgoing interface list: Tunnel0, Forward/Sparse, 00:13:13/00:03:05 Fabric in a Box: (172.16.140.2, 232.10.10.10), 00:11:10/00:02:24, flags: sTI Incoming interface: Vlan3037, RPF nbr 172.16.1.58 Outgoing interface list: Vlan1029, Forward/Sparse-Dense, 00:11:10/00:02:24 Another centrally located place for the multicast sources and rendezvous point is at the data center fabric site. The configuration procedure is very similar to the fusion router multicast setup. The data center multicast configuration must be done first because all edge fabric sites will point to the data center's multicast loopback as the external RP address. When configuring the data center fabric site for multicast, an internal rendezvous point is chosen instead of an external one. The sample output from the workflow is shown below. Figure 345 Internal RP at Data Center Border The MPLS core devices and fusion router must also be manually configured to point to this RP address. Enabling multicast between fabric sites necessarily means a transit is required to pass that traffic. In this section we cover the Headend Multicast Replication scenario over the SDA-Transit is discussed. In Headend Multicast Replication, the first Fabric Node that receives the multicast traffic (head-end) will replicate the multicast data into multiple unicast copies and send each copy to the Fabric Edge nodes where the receivers are located. This deployment only requires to have Any-Source Multicast (ASM) enabled in the Fabric Overlay. It is recommended to place a multicast source behind the fusion router or at the data center fabric site, as discussed in the design guide for enabling multicast forwarding across CCI PoPs. The Rendezvous Point (RP) is configured external to the CCI PoPs on the Fusion Router. The Cisco DNA Center provides a workflow that helps enable group communication or multicast traffic in the virtual network. This section will describes the configuration from the Cisco DNA Center workflow and shows the configuration required on the fusion router. Configuring Multicast Head-End Replication: 1. Create an IP address pool for multicast in the Global under the Network Settings, as shown in Figure Figure 346 Cisco DNA Center Multicast Address pool 2. Reserve a Multicast IP Pool at the Site level. This IP Pool is used by DNAC to configure Loopbacks, a Rendezvous Point (RP), and Multicast Source Discovery Protocol (MSDP) if more than one RP is used. Repeat the same step for the other sites where you want to enable multicast. 3. Go to the Fabric sites Infrastructure and select the fabric sites where you want to configure the multicast. and sStart configuring the multicast. Figure 347 Cisco DNA Center Multicast Configuration 4. In the Enabling Multicast window, choose the method of multicast implementation for the network: Head-end replication. Click Next. Figure 348 Cisco DNA Center Multicast Implementation selection 5. In the Virtual Networks window, select the virtual network on which you want to set up multicast. Click Next. 6. In the Multicast pool mapping window, select an IP address pool from the IP Pools drop-down list. The selected IP address pool is associated with the chosen virtual network. Click Next. 7. In the Select multicast type window, choose the type Any Source Multicast (ASM) to implement, and then click Next 8. Choose External RP as your rendezvous point type, and then click Next. In the popup window, enter the external RP IP address, in this case the logical IP address on the fusion router. 9. In the Select which RP IP Address(es) to utilize window, select an IP address for each Virtual Network. Click Next. 10. Review the multicast settings displayed in the Summary window and modify them, if required, before submitting the configuration. Click Finish to complete the multicast configuration and deploy. After completing the steps above have been completed, verify the relevant Multicast configuration is pushed by DNAC Cisco DNA Center to the FiaB. The similar configurations are present on all the sites where you enabled Head-end replication Multicast. Verify the Multicast Routing is enabled on the VRF: Akash-C9300-Whitefield#show run | sec multicast ip multicast-routing vrf SnS_VN Verify configuration on a SnS_VN Loopback (4100) for the RP selection enables PIM on each interface including the logical LISP interface for that instance and on the L3 Hand-off SVI: interface Loopback4100 vrf forwarding SnS_VN ip address 172.22.2.2 255.255.255.255 ip pim sparse-mode end interface LISP0.4100 ip pim sparse-mode end interface Vlan1023 description Configured from Cisco DNA-Center mac-address 0000.0c9f.f138 vrf forwarding SnS_VN ip address 172.20.2.1 255.255.255.0 ip helper-address 10.10.100.42 no ip redirects ip pim passive ip route-cache same-interface ip igmp version 3 ip igmp explicit-tracking no lisp mobility liveness test lisp mobility SnS_VN-IPV4 no autostate end Verify the configuration of the RP and enables SSM for this VN: ip pim vrf SnS_VN rp-address 192.168.7.6 ip pim vrf SnS_VN register-source Loopback4100 ip pim vrf SnS_VN ssm default Multicast Configuration in Fusion Router:: Configure the Multicast Routing on the VRF: ip multicast-routing vrf SnS_VN distributed Configure Multicast on the logical interface: interface BDI16 vrf forwarding SnS_VN ip address 192.168.7.6 255.255.255.252 ip pim sparse-mode end Configure the RP in the SnS_VN VRF: ip pim vrf SnS_VN rp-address 192.168.7.6 Verification of Multicast between PoP Sites over SDA-Transit: For the verification of Multicast over SDA-Transit, the multicast source is connected at the central fabric site (i.e; Akash-C9300-Cessna site in our example) and the receivers are connected to the IE Switches at the PoP Site (i.e; Akash-C9300-Whitefield site). In this example, the source traffic was a streamed to the group address 239.255.255.250. Receivers must also subscribe to this group address to receive the data. Below is the output of the multicast routers from the source to a receiver. Central Fabric Site (Source side): Akash-C9300-Cessna#show ip mroute vrf SnS_VN (*, 239.255.255.250), 00:04:05/00:03:19, RP 192.168.7.6, flags: SF Incoming interface: Vlan167, RPF nbr 192.168.70.6 Outgoing interface list: LISP0.4100, 192.0.2.11, Forward/Sparse, 00:04:05/00:03:19 (172.5.0.22, 239.255.255.250), 00:00:24/00:03:05, flags: FT Incoming interface: Vlan1026, RPF nbr 0.0.0.0 Outgoing interface list: LISP0.4100, 192.0.2.11, Forward/Sparse, 00:00:24/00:03:19 (*, 224.0.1.40), 00:04:39/00:03:07, RP 192.168.7.6, flags: SJCL Incoming interface: Vlan167, RPF nbr 192.168.70.6 Outgoing interface list: LISP0.4100, 192.0.2.11, Forward/Sparse, 00:04:21/00:03:07 Loopback4100, Forward/Sparse, 00:04:39/00:02:34 Fusion Router: ISR-FUSION#show ip mroute vrf SnS_VN (*, 239.255.255.250), 00:01:17/stopped, RP 192.168.7.6, flags: SP Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: Null (172.5.0.22, 239.255.255.250), 00:01:17/00:01:42, flags: P Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: Null (*, 224.0.1.40), 00:05:07/00:02:57, RP 192.168.7.6, flags: SJCL Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: BDI16, Forward/Sparse, 00:05:07/00:02:57 Receiver side PoP Site: Akash-C9300-Whitefield#sh ip mroute vrf SnS_VN (*, 239.255.255.250), 00:04:43/stopped, RP 192.168.7.6, flags: SJCL Incoming interface: LISP0.4100, RPF nbr 192.0.1.11 Outgoing interface list: Vlan1026, Forward/Sparse-Dense, 00:01:31/00:02:13 Vlan1023, Forward/Sparse-Dense, 00:04:43/00:02:12 (172.5.0.22, 239.255.255.250), 00:01:02/00:01:57, flags: JT Incoming interface: LISP0.4100, RPF nbr 192.0.1.11 Outgoing interface list: Vlan1023, Forward/Sparse-Dense, 00:01:02/00:02:12 Vlan1026, Forward/Sparse-Dense, 00:01:02/00:02:13 (*, 224.0.1.40), 00:04:59/00:02:09, RP 192.168.7.6, flags: SJCL Incoming interface: LISP0.4100, RPF nbr 192.0.1.11 Outgoing interface list: Loopback4100, Forward/Sparse, 00:04:59/00:02:09 SCADA is a category of software application programs used for process control and the gathering of data in real time or near real time from remote locations to control equipment and report conditions. SCADA data can be used to create a local action as well as be transmitted to the SCADA Primary/Subordinate which is located in primary or secondary control center for monitoring and control purposes. The implementation in this guide focuses on Distributed Network Protocol 3 (DNP3) and MODBUS SCADA protocols. The CCI solution is a centralized two-tier architecture, as shown in Figure 349. SCADA applications like Triangle Micro Works (TMW), a simulation software, or Water SCADA Applications and Outage Management System reside in the Control center. Cisco SCADA Gateways communicate with SCADA Remote Devices (PLC/RTU) in two ways, either over Serial or Ethernet. Cisco's SCADA Gateways backhaul their traffic over a Cellular, Ethernet, or CR-Mesh backhaul as defined in the CCI architecture. To choose the correct Gateway, refer to the Design Guide at: ■ This implementation guide covers both Cisco Cellular Gateway, Ethernet connected, and Cisco Resilient Mesh Gateway deployments. Figure 349 CCI SCADA Implementation Cisco Resilient (CR) Mesh implementation will be the correct choice for areas where cellular coverage is not available or less prevalent. Cisco CR Mesh has three types of devices: 1. CR Mesh Coordination or Field Area Aggregation Router (FAR). 2. CR Mesh Gateways or Field Devices (FD) 3. CR Mesh Range Extenders Cisco CGR 1240 with WPAN RF Module router plays the role of CR Mesh aggregator. CGR 1240 aggregates SCADA traffic and routes traffic to applications in the Control center. RTU/PLC are connected to IR510 CR Mesh Gateways via Ethernet or Serial (RS232) interfaces. When RF mesh coverage needs to be extended, Cisco IR530 is deployed as a range extender. The CR Mesh is formed using FAR, FD, and range extenders and can be implemented in multiple PHY modes. CR Mesh can support both OFDM and 2FSK modulation simultaneously supporting a maximum 600 kbps with channel spacing of 400 kHz. Cisco IR1101 and CGR 1240 Cellular Gateways are chosen for SCADA deployments where: ■SCADA Application demands more bandwidth and has time sensitive requirements. ■SCADA Network has better Cellular signal coverage (for example, urban areas). The flow of this implementation guide is depicted in Figure 350. Figure 350 SCADA Implementation Flow Note: For Headend Block Implementation, refer to the common Headend Block implementation. This section focuses on the network topology and high-level implementation used for solution validation and implementation of the Cisco SCADA solution. It also describes the high-level solution validation topology used in this SCADA use case, which is depicted in Figure 351. Figure 351 Cisco SCADA Validation Topology The multiple layers of topology include: 1. The headend, which hosts the Control Center, includes: a. Application servers—Host SCADA application and they could also host other application servers (for example, CCI server and RSA CA server). b. Shared Services or Network Operations Center (NOC), which hosts the following headend components: Dynamic Host Configuration Protocol (DHCP) Server or Cisco Prime Network Registrar (CPNR), Field Network Director (FND), and Headend Router—These components are essential for the onboarding of Cisco IoT Gateways. In this validation, the CGR1240 and IR1101 that are positioned along the SCADA Remote end devices or CGR1000 series of routers positioned as FARs. c. Headend Infrastructure block, which comprises: Private network, where the protected part of the headend is located, along with SCADA and other application servers. DMZ network, where the exposed part of the headend is located; it includes HER. 2. The CCI Block commonly refers to the transport of SCADA traffic via CCI Backhaul. –In this scenario, SCADA end devices are connected to Access Network (IE switch) via Ethernet backhaul. 3. The Distribution Block, which comprises the following three major sub-blocks: a. Cisco Cellular SCADA Gateways, which refer to Cisco IOS routers like the IR1100. b. Cisco Field Area Routers, which refer to Cisco IOS routers like the CGR1240. These routers are used for aggregating the Cisco Resilient Mesh Endpoints (also referred to as CR Mesh SCADA Gateways). The NAN Block is a subset of the Distribution Block, comprising CR Mesh devices, including Cisco FAR and CR Mesh endpoints. c. Cisco Resilient Mesh SCADA Gateways with Edge Compute, which refer to the Cisco IR510 WPAN Industrial Router. 4. The IED/PLC Controller Devices Block, in which the remote SCADA devices (real/simulated) are located. We can connect the Cisco SCADA Gateway (Cellular SCADA Gateway or CR Mesh SCADA Gateway) over an Ethernet/serial interface. The following components are simulated using the Triangle Micro Works (Distributed Test Manager or DTM) tool: –SCADA Primary/Subordinate located in Control Center. –PLC/RTUs located in the IED/PLC Devices Block layer. 5. The NAN Block, which comprises three Personal Area Networks (PANs): –CR Mesh-PAN1 –CR Mesh-PAN2 –CR Mesh-PAN3 PAN3 has been validated over LTE backhaul. PAN1 and PAN2 have been validated over Ethernet backhaul. This section includes the following major topics: ■Field Network Director Categories ■IoT Gateway Configuration and Deployment ■Enrollment of Cisco Resilient Mesh Endpoints—IR510 ■MAP-T Infrastructure in CCI SCADA ■Configuration Push on FND This section focuses on installing and configuring FND, refer to Implementing FND Network Director for CCI. In this implementation guide, the terminology "IoT Gateway" is used to refer to both Cisco Cellular SCADA Gateways and Cisco FARs. As part of IoT Gateway onboarding, the IoT Gateways are registered with the FND. From that point on, the FND located in the Control Center could be used to remotely monitor/manage/troubleshoot the IoT Gateways, which are spread across the entire SCADA network. This process has two phases: 1. IoT Gateway Configuration and Deployment 2. Remote Monitoring/Management/Troubleshooting of the IoT Gateway The FND located in the staging environment helps in configuring of the IoT Gateways. The FND located in the NOC/Control Center environment that helps with the configuration of IoT Gateways is referred to as the NOC or Control Center FND. This FND located in the Control Center helps remote management of the IoT Gateways. Note: The approach here is preconfiguration of the IoT Gateways that is done at the dedicated staging location. Once the devices are configured successfully, they are powered off and transported to the final deployment locations, where the devices are deployed and powered on. IoT Gateways can be implemented in three different ways: 1. SCADA Remote Devices (PLC/RTU) connected to Remote PoP Gateway IR1101 –SCADA RTU/PLC will connect to Ethernet/serial interface of Remote PoP Industrial Gateway (IR1101) having a Cellular backhaul. Refer to Secure Onboarding of Field Area Router—CGR1240 to on-board IR1101 into FND for remote management/configuration. Figure 352 CCI SCADA Cellular Gateways 2. SCADA Remote Devices (PLC/RTU) connected to a Mesh Gateway IR510 aggregated by a CR Mesh FAR (CGR1240) –SCADA RTU/PLC will connect to Ethernet/serial interface of the SCADA Gateway (IR510), which aggregates traffic to Field Area Routers (FAR). FARs aggregate the SCADA traffic from the CR Mesh network (NAN Tier) and route traffic to various SCADA application via the WAN tier (which could be a Cellular or Ethernet backhaul connection). In our scenario, FAR will transport SCADA traffic to SCADA Primary/Subordinate in two ways: –FAR connected to CCI Network—In this scenario, FAR will be connected to CCI network and FAR will have secure Flex VPN Secure tunnel to HER (Headend Router). CCI acts as transport. –FAR acts as Remote PoP (CGR 1240 with Cellular Interface). Refer to Secure Onboarding of Field Area Router—CGR1240 to onboard CGR 1240 into FND for remote management/configuration. 3. SCADA Remote Devices (PLC/RTU) connected directly to CCI Network (Ethernet Backhaul)—SCADA RTU/PLC will be directly connected to CCI access network infrastructure. SCADA RTU/PLCs can be connected to CCI Network Access devices (IE switches) and can aggregate SCADA traffic via CCI Network to SCADA control center. In this scenario only Ethernet ports are available to transport IP-based traffic. Figure 354 SCADA Transport via CCI With this, the Cellular SCADA Gateways and Cisco Field Area Routers could be onboarded and registered with FND, enabling further remote management and monitoring from FND. The next section discusses in detail the components required to onboard the Cisco Resilient Mesh Endpoints like the Cisco IR510 WPAN Industrial Router to ensure the functionality of the CR-Mesh SCADA Gateway. This section includes the following major topics: ■Staging ■Secure Onboarding of Mesh Nodes into CR Mesh ■MAP-T Infrastructure in CCI SCADA ■Configuration Options from FND ■Routing Advertisements from FAR to HER This section describes the implementation steps required to bring up the CR Mesh using IR510 Gateways for SCADA (also referred to as FDs). The IR510 connects to the Cisco CGR (also referred to as FAR) via the Connected Grid Module (CGM) WPAN-OFDM-FCC Module installed within the FAR. Note: For more details on setting up the WPAN module, refer to: Cisco Connected Grid Module (CGM) WPAN-OFDM-FCC Module Cisco IOS at following URL: ■ pid=15768 Table 29 lists the basic components and their software versions needed to bring up the CR Mesh topology explained in Figure 349. Table 29 CR Mesh Components Component Product / Model Software Image Software Version CGR Cisco CGR1240/K9 cgr1000-universalk9-bundle.SPA.159-3.M2.bin 15.9(3)M2 Cisco WPAN CGM-WPAN-OFDM-FCC cg-mesh-bridge-6.2.6219-ir510-1bf449d.bin 6.2.19 FD IR510 cisco-mesh-6.2.6219-ir510-1bf449d.bin 6.2.19 Configuration Tools CSMP Product / Model fwubl_win732bit_1.0.5 1.0.5 The prerequisites for configuring a CR Mesh include obtaining all the necessary ECC certificates from the ECC CA server and configuring the AAA RADIUS server in ECC CA Server to authenticate the IR510 Gateway using a certificate-based authentication method. The FAR facilitates dot1x authentication between the IR510 and AAA server, thereby acting as the dot1x authenticator. The ECC certificate mentioned earlier is part of the configuration binary file (.bin) used to program the IR510. Details are described in further sections. Note: While the FD need ECC CA certificates for enrollment, FAR use RSA type certificate. The following certificates need to be obtained from the ECC CA to program an IR510 Gateway: ■The X.509 certificate of the IR510 in PKCS#12 format (.pfx) contains its private key and is used to program the node. ■The DER-encoded X.509 certificate (.cer) of the IR510 without the private key is used to enroll the node with the Active Directory. ■The DER-encoded X.509 certificate (.cer) of the ECC CA server is also used for programming the IR510. ■The CSMP certificate downloaded from the IoT FND in binary format (.cer) to validate node CSMP registration with IoT FND. For details on setting up and configuring the ECC CA and AAA server and on obtaining all of the above certificates, refer to ECC Certificate Authority Installation. The following section describes the process of generating a configuration binary file (.bin) used to program the IR510. The configuration file for the IR510 Gateway is prepared in binary format using the Configuration Writer utility (cfgwriter). Note: To obtain the cfgwriter utility, please contact your account team or sales representative. The cfgwriter utility is a java-based utility that takes as input an XML file with the node configuration information and produces a binary (.bin) memory file. This utility may be executed on any host platform with Java Run Time Environment installed. In this deployment, a Windows 10 machine with Java pre-installed was used to host the cfgwriter utility. The node configuration information, among other items, includes the SSID of the WPAN it must join and the security credentials. The following documentation are packaged with the cfgwriter utility as a ZIP file. Figure 355 cfgwriter Utility The following XML file is used in this deployment to program the IR510 Gateway: = = = = = = = = = = = = = = = = = adaptive 1 120 60 12 10 1200 400 166 3600 300 true true false false true false false small Note: In the above schema, phy mode 166 refers to adaptive modulation (discussed later) with a data rate of 600kb/s. Text in bold in the XML configuration represents mandatory configuration parameters. The cfgwriter utility converts the input XML file into a binary format (.bin) output. Successful execution of the cfgwriter utility with the XML file and necessary certificates as input will return a "0" numeric code to Standard Output (stdout). From the command prompt on a Windows PC, navigate to the folder where the cfgwriter utility and all the necessary certificates described in Table 30 are placed. The following is the command syntax used to generate the config (.bin) file needed to program the IR510 node: java -jar cfgwriter-6.0.20.jar -x -p ca -w -nmscert The command line parameters used in the above command are described in Table 30. Table 30 cfgwriter Utility Command Syntax Parameter Options Parameter Description -x IR510 Cert & Private Key file in PKCS12(.pfx) format to be created and exported from the ECC CA server. -p Password provided while exporting the IR510 (.pfx) certificate from the ECC CA server -a Trusted ECC CA public Cert (DER encoded) to be installed on the IR510. -w XML config file of the IR510 used to generate the corresponding binary.bin file -nmscert The.pem file certificate downloaded from IoT FND GUI in binary format (with extension changed to.cer) for mutual validation of csmp communication messages between IR510 and IoT FND. Output bin file generated after successful execution of the specified command. A numeric code of "0 (zero)" seen on the standard output means command was successfully executed. This is the same config bin file which is used to program the IR510 later. Figure 356 shows a sample command issued to generate the.bin file needed for the deployment. Figure 356 Bin File Generation The binary configuration file (.bin) prepared in the previous step, along with the correct firmware, is programmed into the IR510 node using another utility known as HostOne (fwubl) tool. This tool is also placed on the same Windows machine where the cfgwriter utility was placed. Note: To obtain the HostOne (fwubl) tool discussed below, check with your account team or sales representative. From the same Windows machine, connect to the IR510 console port using an USB to serial converter connected through a Cisco RJ45 to DB9 (female) blue serial console cable. From the command prompt on Windows PC, navigate to the folder where the fwubl tool is placed along with the firmware image and configuration bin files of the IR510. Note: Do not power on the IR510 unit without any attenuators, antenna, or RF cabling in place. It is highly recommended to keep the RF port on the node always connected; do not leave it to transmit in free air since without the right connector/RF cables, the radio has a high likelihood of becoming damaged. Once the node is powered on, issue the following command to verify that the node is in bootloader mode first. If it is not, power cycle the node and check again as it would re-enter into the bootloader mode. fwubl_win732bit_1.0.5.exe -con The output from this command shows the current image loaded on the IR510 unit and its current bootloader status. Figure 357 shows the sample output of this command. Figure 357 IR510 in Bootloader State The next step is to program the firmware version on the IR510 into the memory location specified in the following command: fwubl_win732bit_1.0.5.exe -w -a 0x8020000 com Figure 358 shows the sample output of firmware push issued to an IR510 unit. Figure 358 Firmware Push on IR510 The next step is to program the configuration.bin file generated for the IR510 into the memory location specified in the following command: fwubl_win732bit_1.0.5.exe -w -a 0x80E0000 com Figure 359 shows the sample output of the configuration bin push issued to an IR510. Figure 359 Config Push on IR510 The final step is to verify that the IR510 by bringing it out of bootloader mode by issuing the following command: fwubl_win732bit_1.0.5.exe -g 0x8020000 com Figure 360 shows the sample output to run CG-mesh software on the IR510 and its output. Figure 360 CG Mesh Enabled on IR510 Staging provided details on how to set up an IR510 Gateway to securely join the mesh network. This section discusses the components needed to enable secure onboarding of IR510 into the mesh network. The FAR router provides security services such as 802.1x port-based authentication, encryption, and routing to provide a secure connection for the mesh endpoint all the way to the control center. IEEE 802.1x using X.509 certificates is the process used to securely authenticate a mesh node before admitting it to join the PAN or to even send packets into the network. Table 31 lists the associated touchpoints that would be set up for a complete end-to-end secure onboarding process of mesh nodes. Table 31 Associated Configuration Touchpoints Associated Configuration Touchpoints Purpose Reference Configuration Link for Configuration ECC CA Server Issuing ECC type certificates for mesh end points and AAA server refer to ECC Certificate Authority Installation for installing ECC CA server Issuing ECC certificate for AAA server and configuring Radius server and Active Directory. IoT FND Obtaining CSMP certificate from IoT FND to program mesh nodes Browse to point 8 referring to "Certificates for CSMP tab" in "Configuring a Custom CA for SSM" at the following URL: Click the radio button showing the binary option and download the.pem binary certificate (manually change extension to.cer for programming into the IR510). Note: The following configurations are for reference purposes only. They should be dynamically provisioned by the FND CGR. The following is the sample configuration of a CGR1240 for the WPAN interface. Note that the SSID configured on the WPAN interface below matches that was configured in the IR510 XML schema shown in an earlier section. CGR1240_JAD2014B2Z#sh run int wpan 4/1 interface Wpan4/1 no ip address ip broadcast-address 0.0.0.0 no ip route-cache load-interval 30 ieee154 phy-mode 166 165 164 2 ieee154 beacon-async min-interval 15 max-interval 60 suppression-coefficient 1 ieee154 dwell window 12400 max-dwell 400 ieee154 panid 420 ieee154 ssid adaptive ieee154 txpower 25 ieee154 beacon-version-tlv 15 outage-server 2001:DB8:16:110::151 rpl dag-lifetime 60 rpl dio-dbl 2 rpl dio-min 14 rpl version-incr-time 10 authentication host-mode multi-auth authentication port-control auto ipv6 address 2001:DB8:ABCD:1::1/64 ipv6 enable ipv6 dhcp server dhcpdb-pool rapid-commit no ipv6 pim dot1x pae authenticator mesh-security key lifetime 259200 end The following is the RADIUS client configuration needed on CGR1240 for enabling dot1x authentication of the mesh endpoint with the AAA server: CGR1240_JAD2014lB2Z# ! aaa new-model !aaa group server radius rm-aaa server name aaa_server ! radius server aaa_server address ipv4 172.16.106.175 auth-port 1812 acct-port 1813 key 7 aaa authentication dot1x default group rm-aaa ! dot1x system-auth-control ! The FAR also operates as an IPv6 DHCP relay agent. DHCP options configured on CGR as a radius client. FAR is provisioned with mesh key pushed from FND that is used for communication between the IR510 and the FAR. This key needs to be verified to confirm if the key is indeed present on the CGR: CGR1240_JAD2014lB2Z#sh mesh-security keys Mesh Interface: Wpan4/1 Master Key Lifetime: 120 Days 0 Hours 0 Minutes 0 Seconds Temporal Key Lifetime: 60 Days 0 Hours 0 Minutes 0 Seconds Key ID: 0 * Key expiry: Fri Feb 8 20:34:24 2019 Time remaining: 4 Days 0 Hours 51 Minutes 30 Seconds Frame Counter: 200000 CGR1240_JAD2014lB2Z# The IR510 receives an IPv6 address for reachability from the CGR and the control center. For this purpose, an IPv6 DHCP pool needs to be configured on the CGR as shown below. However, a central DHCP server option, if available is recommended. ! ipv6 dhcp pool dhcpdb-pool address prefix 2001:DB8:ABCD:1::/64 lifetime infinite infinite vendor-specific 26484 suboption 1 address 2001:DB8:16:103::23 IPv4 -> IPv6 –> CSP –> IPv6 -> IPv4 SCADA Primary/Subordinate An actual sample packet flow, including IPv4 to IPv6 translation, is illustrated in Figure 361. Figure 361 MAP-T Packet Flow While configuring MAP-T, the DMR prefix, the IPv6 user prefix, and the IPv6 prefix plus the embedded address (EA) bits must be less than or equal to 64 bits. Note: MAP-T parameters like the BMR IPv6 prefix and associated prefix length unique to each node are configured as part of the.csv file uploaded to IoT FND whereas the DMR IPv6 and BMR IPv4 prefixes and their associated lengths along with EA bit length are configured via the configuration template in IoT FND which is later applied to the nodes, as shown in Configuration Options from FND. IR510—MAP-T CE A MAP-T CE device connects a user's private IPv4 address and the native IPv6 network to the IPv6-only MAP-T domain by first doing a NAT44 translation from the private to public (inside to outside) address within the v4 domain and then subsequently doing a v4 to v6 translation. MAP-T BMR Prefix Selection for IR510.csv The BMR prefix is used by the MAP-T CE to configure itself with an IPv4 address, an IPv4 prefix from an IPv6 prefix. This is also used by the MAP-T network. As such, the BMR IPv6 prefix of 2001:DB8:267:1517::/56 corresponds to the MAP-T IPv4 address of 10.153.10.21 of an IR510 node. HER—MAP-T Border Relay Router The following configuration is used to enable MAP-T border relay functionality: FAR-PHE-HER# ! nat64 settings fragmentation header disable nat64 map-t domain 1 default-mapping-rule 2001:DB8:367:BABA::/64 basic-mapping-rule ipv6-prefix 2001:DB8:267:1500::/56 ipv4-prefix 10.153.10.0/24 port-parameters share-ratio 1 start-port 1 ! Additionally, the CLI command and nat64 enable needs to be enabled as shown below on the HER interfaces participating in the MAP-T translations (such as the interface where the Virtual-Template is configured and the network interface towards CGR). The HER interface connecting to the control center side where the SCADA Primary/Subordinate resides is IPv4 based whereas the virtual-template interface of the HER connecting to the CGR on the WAN side is IPv6 based, as shown logically below: CGR –> IPv6 –> (VTI HER Gig port) –> IPv4 –> SCADA Primary/Subordinate Enabling nat64 on the SCADA Primary/Subordinate-facing Interface of the HER Shown Below ! interface GigabitEthernet0/0/1 description to control center ip address 10.10.100.100 standby 107 priority 253 standby 107 preempt standby 107 name SCADA_MASTER nat64 enable ! Enabling nat64 on the FAR-facing Virtual-Template Interface of HER Shown Below ! interface Virtual-Template1 type tunnel ip unnumbered Loopback0 ip nhrp network-id 1 ip nhrp redirect nat64 enable ipv6 unnumbered Loopback0 ipv6 enable ! The following template can be used to add mesh endpoints to the FND database. eid,deviceType,function,enduserip6prefix,bmrip6prefix These fields are explained in Table 32. Table 32 Parameters of IR500.csv File Parameter Descriptor Description Eid A Unique Element identifier to identify the device in log messages as well as in the IoT FND GUI. deviceType Used to identify the hardware platform. Function Used to identify the functionality of a device (i.e., SCADA Gateway). enduserip6prefix The BMR IPv6 prefix unique to each mesh endpoint. bmrip6prefix The BMR IPv6 prefix length assigned to the mesh endpoint. The following are the contents of a sample csv file used in this implementation: eid,deviceType,function,enduserip6prefix,bmrip6prefix 2ED02DFFFE6E0F03,ir500,gateway,2001:db8:267:1515::,56 2ED02DFFFE6E0F08,ir500,gateway,2001:db8:267:1517::,56 2ED02DFFFE6E0F2F,ir500,gateway,2001:db8:267:1519::,56 2ED02DFFFE6E0F05,ir500,gateway,2001:db8:267:1516::,56 2ED02DFFFE6E0F29,ir500,gateway,2001:db8:267:1520::,56 2C02D20D0D6E0F4E,ir500,gateway,2001:db8:267:151A::,56 1. To upload the CSV file into IoT FND, navigate to the GUI. 2. From Inventory tab → Devices -> Field Devices -> Add Devices, click Browse to upload the file as shown in Figure 362. 3. Click Add. Figure 362 CSV File Upload to IoT FND Once added, the devices will initially be in Unheard state. Once mesh nodes start registering with the FND, their device status turns green as shown in Figure 363. Figure 363 Mesh Endpoint Status in FND The mesh nodes must register successfully with IoT FND before other settings like MAP-T, NAT44, and other serial configuration profiles be properly pushed/applied to the nodes. However, if those settings are pre-linked via the default profiles, the configuration would be automatically pushed to the nodes upon device registration. 1. To configure the MAP-T settings in FND, navigate to Config Profiles -> Config -> Device Configuration. 2. Under Config Profiles, click the Add Profile icon (+). 3. Create a new MAP-T profile with the correct settings for BMR and DMR rules, as shown in Figure 364. Figure 364 Creating MAP-T Profile 1. To configure the NAT44 settings for mesh endpoints in FND, navigate to Config Profiles -> Config -> Device Configuration. 2. Click the Add Profile icon (+). 3. Create a new NAT44 profile with the correct Internal IPv4 address, internal and external ports, as shown in Figure 365. Figure 365 Creating a NAT44 Profile In Figure 365, the IPv4 address and ports are defined for SCADA Primary/Subordinate communication. The Internal IPv4 address refers to the internal and gateway address of the SCADA client, which are connected to the IR510 via Ethernet. The Internal port refers to port of the SCADA client which is connected to the IR510 to which the SCADA client would be listening. The external port refers to the external port number of the SCADA client accessed by devices from outside MAP-T domain. Since 192.168.0.2 is reserved for the Guest OS inside the IOX portion of the IR510 unit, it is recommended to use a different subnet such as 192.168.0.3 for the SCADA client and, accordingly, multiple NAT44 mappings like the one shown above could be created for different ports. This profile needs to be linked to the FND are placed in the default IR500 group. Depending on the deployment, some of them can be moved to a newly created configuration group in which a new configuration template and MAP-T, NAT44 profiles can be selectively applied and a configuration pushed to these nodes. 1. To create a configuration group, navigate to the Groups tab -> Config -> Device Configuration. 2. Click the Add Group icon (+). 3. Then create a new group of type Endpoint as shown in Figure 366. Figure 366 Creating an Endpoint Configuration Group 4. Move some of the mesh nodes from the default endpoint group to the newly created group based on the deployment. 5. Navigate to the default endpoint group, select the nodes of interest, and click Change Configuration Group. 6. Then select the newly created configuration group in the drop-down menu as shown in Figure 367. Figure 367 Moving IR510 to New Configuration Group 7. Once devices are moved to the newly created configuration group, from the Edit configuration template, select the MAP-T and NAT44 profiles created earlier. 8. Click Save Changes for these settings to be applied to the devices part of this group, as shown in Figure 368. Figure 368 Editing the Configuration Template 9. Finally, push the configuration to the devices in this group by navigating to the Push Configuration tab and select Push Endpoint Configuration. 10. Click Start as shown in Figure 369. This completes the configuration settings from FND for the mesh node that are needed to operate as a SCADA gateway. Figure 369 Push Configuration 11. The final step is to verify that all the configuration settings are properly applied to the IR510. Click on the node under the configuration group and navigate to the Device Info tab. Scroll down to Config Properties to verify them, as shown in Figure 370. Figure 370 Verify Configuration Settings on IR510—1 12. On scrolling further down, the MAP-T settings applied to the device can be verified, as shown in Figure 371. Figure 371 Verify Configuration Settings on IR510—2 Note: HER advertises a default route to all the FARs in order to provide connectivity to control center components. Once the CR Mesh has been formed, the IR510 Gateways have reachability only via the FAR. The mesh nodes need a way to communicate with the control center components like the IoT FND for management or the SCADA Primary/Subordinate. The IPv6 LoWPAN address subnet assigned to the mesh endpoints is advertised to the HER using the IKEv2 prefix injection over the FlexVPN tunnel. Specifically, the mesh prefix is advertised as a part of the IPv6 ACL, which is part of the FlexVPN authorization policy as shown below. Note: The configuration shown below is for reference purposes only since it may be provisioned by the FND. ! crypto ikev2 authorization policy FlexVPN_Author_Policy route set interface route set access-list FlexVPN_Client_IPv4_LAN route set access-list ipv6 FlexVPN_Client_IPv6_LAN route redistribute connected route-map snapshot ! ipv6 access-list FlexVPN_Client_IPv6_LAN permit ipv6 2001:DB8:ABCD:1::/64 any Mesh IPv6 LoWPAN prefix! As discussed above, besides advertising the Mesh LoWPAN prefix of the IR510 to the HER, even the MAP-T BMR IPv6 prefix of the nodes needs to be reachable from the control center to communicate with the SCADA clients connected to the IR510. To achieve this, the IKEv2 snapshot routing feature is implemented wherein a route map and prefix list are defined and then referred to in the FlexVPN authorization policy, as shown below. Note: Basically, the BMR IPv6 /128 address of the nodes that appear/disappear from the HER routing table are the ones that match the route-map snapshot shown below. ! crypto ikev2 authorization policy FlexVPN_Author_Policy route set interface route set access-list FlexVPN_Client_IPv4_LAN route set access-list ipv6 FlexVPN_Client_IPv6_LAN route redistribute connected route-map snapshot ! route-map snapshot permit 10 match ipv6 route-source prefix-list snapshot set tag 10 ! ipv6 access-list FlexVPN_Client_IPv6_LAN permit ipv6 2001:DB8:267:1500::/56 any BMR IPv6 prefix! This implementation focuses on DNP3 and MODBUS as SCADA communication protocols as well as serial and IP-based connectivity. It requires routing, raw socket configuration, and Ethernet based connectivity, which are key for application traffic flow. The operations have been executed using a SCADA simulator known as the Distributed Test Manager (DTM), which has the capability of simulating both the SCADA control traffic and systems and the SCADA remote traffic and devices. Table 33 SCADA Protocol Matrix Transport Type SCADA Control Server Protocol SCADA Remote Device (PLC/RTU) Protocol Translation DNP3 IP DNP3 IP Raw Socket DNP3 DNP3 Protocol Translation DNP3 IP DNP3 MODBUS IP MODBUS IP Raw Socket MODBUS MODBUS Note: SCADA over CCI supports only Ethernet backhaul and protocols MODBUS IP and DNP3 IP are validated over the same. Operations that can be executed when the communication protocol is DNP3, DNP3 IP, DNP3-DNP3 IP translation are as follows: ■Poll—(SCADA Primary/Subordinate > SCADA Remote Device (PLC/RTU)) ■Control—(SCADA Primary/Subordinate > SCADA Remote Device (PLC/RTU)) ■Unsolicited Reporting—(SCADA Remote Device (PLC/RTU) > SCADA Primary/Subordinate) Notification Class Client. Operations that can be executed when the communication protocol is MODBUS IP, MODBUS Raw Socket are as follows: ■Read/Write Coil(s)—(SCADA Primary/Subordinate > SCADA Remote Device (PLC/RTU)) ■Read/Write Holding Register(s)—(SCADA Primary/Subordinate > SCADA Remote Device (PLC/RTU)) ■Read Discrete Input(s) and Input Register(s)—(SCADA Primary/Subordinate > SCADA Remote Device (PLC/RTU)) Table 34 SCADA Operations Register References Action Description 0xxx Read/Write Coils Outputs 1xxx Read Discrete Inputs 3xxx Read Input Registers 4xxx Read/Write Holding Registers This document focuses on SCADA protocols such as the MODBUS and DNP3 protocols. This section includes the implementation of the following major topics: ■SCADA control center Point-to-Point Implementation Scenarios over Cellular Gateways. ■SCADA Communication with IP Intelligent Devices ■SCADA Communication Scenarios over CR Mesh Network (IEEE 802.15.4) ■SCADA Communication with Serial-based SCADA using Raw Socket TCP ■Legacy SCADA (Raw Socket TCP Server). ■SCADA Communication with CCI Network. [SCADA end point connected directly via Ethernet to CCI] CCI Solution supports the SCADA service models shown in Table 35. Table 35 SCADA Service Models Service Connectivity Service Model Legacy SCADA (DNP3) Point-to-Point (Primary/Remote Device) Single Control Center Raw Socket Over FlexVPN SCADA Gateway (DNP3) to IP Conversion (DNP3-IP) Point-to-Point (Primary/Remote Device) - Single Control Center Protocol Translation over FlexVPN SCADA (DNP3-IP) Point-to-Point (Primary/Remote Device)- Single Control Center FlexVPN - Single SCADA Primary/Subordinate Legacy SCADA (MODBUS) Point-to-Point (Primary/Remote Device)- Single Control Center Raw Socket Over FlexVPN SCADA (MODBUS-IP) Point-to-Point (Primary/Remote Device)- Single Control Center FlexVPN - Single SCADA Primary/Subordinate In this scenario, the Control Center will be hosting SCADA applications. The SCADA Remote Device (PLC/RTU) is connected to the Cellular SCADA Gateway (IR1101) via serial or Ethernet interface. The SCADA Primary/Subordinate residing in the Control Center can communicate with the end point using the DNP3 (IP/Serial) or MODBUS (IP/serial) protocol. Figure 372 SCADA Topology over Cellular Gateway This document focuses on SCADA protocols such as the DNP3 and MODBUS protocols. IR1101 is implemented as Cellular SCADA Gateway. ASR 1000s/CSR1000v implemented act as a HER, which terminates FlexVPN tunnels from SCADA Gateways. The following sections focus on: ■SCADA Communication with IP intelligent devices ■SCADA Communication with legacy devices –Raw Socket TCP –Protocol Translation (only for DNP3) ■SCADA Remote Device (PLC/RTU) is connected to the SCADA Gateway via the Ethernet port, then it is pure IP traffic. The IP address of the SCADA Gateway can be NATed so that the same subnet between the SCADA Remote Device (PLC/RTU) and the Ethernet interface of the SCADA Gateway can be re-used. This approach will ease the deployment. ■If the SCADA Remote Device (PLC/RTU) is connected using asynchronous serial (RS-232 or RS-485): Gateway Tunnelled Raw Socket using DNP3 or MODBUS: –SCADA traffic at a remote site can be transmitted as RAW Socket or encapsulated into IP at a local gateway. –SCADA control server can consume as DNP3, DNP3/IP, or MODBUS communication directly. –SCADA Gateway in the control center can convert DNP3/MODBUS traffic back to Raw Socket. Figure 373 SCADA DNP3/MODBUS with IR1101 ■Protocol Validation—The protocol validated for this release is DNP3/MODBUS IP. ■MODBUS Validation—See the flow diagram in Figure 374. Figure 374 MODBUS IP Serial Control Flow As shown in Figure 374, in MODBUS the SCADA Primary/Subordinate can perform a read and write operation to a Remote Device (PLC/RTU) via the SCADA Gateway over the IP Network. SCADA Gateway interface connected to SCADA Remote Device (PLC/RTU) has the following configuration. This configuration is for reference purpose only. The interface connected to SCADA Client has the following configuration: interface Loopback0 ip address 192.168.150.21 255.255.255.0 interface Vlan1 ip address 192.168.0.1 255.255.255.0 ip nat inside ! int fastEthernet 0/0/1 /*It's a layer 2 port, corresponding layer 3 port int interface vlan1*/ switchport access vlan 1 ! interface Tunnel0 ip nat outside ! ip nat inside source static tcp 192.168.0.11 502 interface Loopback0 502 As per the topology, the SCADA Primary/Subordinate is residing in the Control Center. The following configuration must be required for the SCADA Primary/Subordinate to communicate with SCADA Remote Devices (PLC/RTU). The description below shows the DTM simulator configuration which vary based on the testing scenario. Representative field testing with non-simulated traffic and equipment can be found in the Distributed Automation Implementation guide at: ■ 1. Open the SCADA Primary/Subordinate Application and add a new MODBUS Server. Figure 375 SCADA Server Creation 2. From the Channel tab, configure the SCADA Primary/Subordinate, as shown in Figure 375 (Local Address: Address of SCADA Primary/Subordinate). Figure 376 SCADA Primary/Subordinate Configuration 3. SCADA Primary/Subordinate, in this case, is configured as a TCP Client interacting with the SCADA Remote Device (PLC/RTU), which is configured to act as TCP Server. 4. Populate the remote address field with the Loopback IP of the Cellular gateway (Remote Address should be loopback IP of IR1101, with NAT/PAT configuration redirecting the IP and Port to the SCADA Remote Device (PLC/RTU)). 5. Populate the port with 502, which is the port used in SCADA Primary/Subordinate. As per the topology, the SCADA Remote Device (PLC/RTU) resides in the field area. The following configuration must be required for the SCADA Remote Device (PLC/RTU) to communicate with the SCADA Primary/Subordinate. 1. Open the SCADA Remote Device Application and add a new MODBUS Client. Figure 377 SCADA Remote Device (PLC/RTU) Creation 2. From the Channel tab, configure the SCADA Remote Device (PLC/RTU), as shown in Figure 378. Figure 378 SCADA Remote Device (PLC/RTU) Configuration 3. Populate the remote address field with SCADA Primary/Subordinate IP and Local Address as SCADA Remote Device (PLC/RTU) IP. 4. Populate the port with 502, which is the port used in SCADA Primary/Subordinate. In MODBUS, the SCADA Primary/Subordinate requests the corresponding data from SCADA Remote Device (PLC/RTU) and SCADA Remote Device (PLC/RTU) responds to the request (It is usually Send Request from Primary and Read Response from SCADA Remote Device (PLC/RTU) type messages). The client does not initiate response/request on their own and only responds to messages from SCADA Primary/Subordinate. They are four different types of tables are used to store information and data, based on the data user can request read or write into corresponding data points: ■Two tables are used to store simple discrete information called Coils: –Coils—User can perform Read/Write operations from SCADA MODBUS Server. –Discrete inputs—User can perform Read operations from SCADA MODBUS Server. ■Another two tables are used to store numeric 16-bit values called as Registers: –Input Registers—User can perform Read operations from SCADA MODBUS Server. –Holding Registers—User can perform Read/Write operations from SCADA MODBUS Server. Read Operation: Read operation is SCADA Primary/Subordinate trying to read data (coil, register) from SCADA Remote Device (PLC/RTU). Step 1: User need to select Read option from SCADA Primary/Subordinate as show in Figure 379. Figure 379 SCADA Read Operation from Primary Step 2: Prompt will appear as shown in Figure 380 to select type of data. The user can select the type of data values. Figure 380 SCADA Read Operation from Primary with Data Values Step 3: User can select the Start value and Quantity and select OK. Figure 381 SCADA Read Operation from Primary with Type Input Registers Step 4: User can execute the corresponding commands as shown in Figure 382 to get the data. Figure 382 SCADA Read Operation from Primary: Executing Commands Write Operation: Write operation is SCADA Primary/Subordinate trying to write data (Coil, Holding register) to SCADA Remote Device (PLC/RTU). Step 1: User need to select Write option from SCADA Primary/Subordinate as show in Figure 383. Figure 383 SCADA Write Operation from Primary Step 2: Prompt will appear as shown in Figure 384 to select type of data. The user can select the type of data. Figure 384 SCADA Write Operation from Primary with Data Values Step 3: User can select the Start value and Quantity and select OK. Figure 385 SCADA Write Operation from Primary with Holding Registers Step 4: User can execute the corresponding commands as shown in Figure 386 to get the data. Figure 386 SCADA Write Operation from Primary: Executing Commands For more information regarding the MODBUS testing and simulation, refer to the Triangle Micro Works Documentation and DTM User Guides: ■ Figure 387 DNP3 IP Control Flow As shown in Figure 387, the SCADA Primary/Subordinate can perform a read and write operation to a Remote Device via the SCADA Gateway. The Remote device can send the Unsolicited Reporting to the SCADA Primary/Subordinate via the SCADA Gateway over the IP network. The interface connected to SCADA Client has the following configuration: interface Loopback0 ip address 192.168.150.21 255.255.255.0 interface Vlan1 ip address 192.168.0.1 255.255.255.0 ip nat inside ! int fastEthernet 0/0/1 /*It's a layer 2 port, corresponding layer 3 port int interface vlan1*/ switchport access vlan 1 ! interface Tunnel0 ip nat outside ip nat inside source static tcp 192.168.0.3 20000 interface Loopback0 20000 As per the topology, the SCADA Primary/Subordinate resides in the Control Center. The following configuration must be required for the SCADA Primary/Subordinate to communicate with SCADA Remote Device (PLC/RTU)2. 1. Open the SCADA Primary Application and add a new DNP3 Server. 2. From the Channel tab, configure the SCADA Primary/Subordinate, as shown in Figure 388. 3. SCADA Primary/Subordinate, in this case, is configured as a TCP Client interacting with the SCADA End Device, which is configured to act as TCP Server. 4. Populate the remote address field with the Loopback IP of the Cellular gateway. 5. Populate the port with 20000, which is the port used in the Cisco IOS configuration. Figure 388 SCADA Primary/Subordinate Configuration As per the topology, the SCADA End Device resides in the field area. The following configuration must be required for the SCADA End Device to communicate with the SCADA Primary/Subordinate. 1. Open the SCADA End Device Application and add a new DNP3 Client. 2. From the Channel tab, configure the SCADA Primary/Subordinate, as shown in Figure 389. 3. Populate the remote address field with SCADA Primary IP. 4. Populate the port with 20000, which is the port used in SCADA Primary/Subordinate. Figure 389 SCADA End Device Configuration The SCADA Primary/Subordinate and the SCADA End Device can communicate via Poll, Control, and Unsolicited Reporting. Poll and Control operations are initiated from the SCADA Primary/Subordinate. Unsolicited Reporting is sent to the SCADA Primary/Subordinate from the End Device. The Poll operation is performed by the SCADA Primary/Subordinate. The SCADA Primary/Subordinate can execute a general Poll in which all the register values are read and sent to the SCADA Primary/Subordinate as shown in Figure 390. The user can select Integrated Data Poll, RBE Data Poll, and Read Specific Data as shown in Figure 391. Figure 390 Operations Performed Using DNP3 Figure 391 SCADA Primary/Subordinate Analyzer Logs before Poll Operation Figure 392 SCADA Primary/Subordinate Analyzer Logs after Poll Operation Control operation basically sends the control command from the SCADA Primary/Subordinate to the SCADA Remote Device (PLC/RTU) in order to control the operation of end devices. The control command can be executed, and the results can be seen on the analyzer. The value of Control Relay Output is changed and is notified to the Primary. Figure 393 shows control relay output status before sending the control command to the Subordinate. Figure 393 SCADA Remote Device (PLC/RTU) Register before Control Operation Figure 394 shows how SCADA Primary/Subordinate sends the control command. Figure 394 SCADA Primary/Subordinate Sending Control Command Figure 395 DNP3 Client Register after Control Operation Unsolicited Reporting Unsolicited Reporting is initiated by the SCADA Remote Device (PLC/RTU), which is connected to the SCADA Gateway. Changes to the value of the Subordinate register are notified to the SCADA Primary/Subordinate. This notification can be seen on the SCADA Server Analyzer. Figure 396 DNP3 Client Sending Solicit Response to Server Legacy SCADA (Raw Socket TCP) ■Protocol Validation—The protocol validated for this release is MODBUS. ■MODBUS Control Flow—See the flow diagram in Figure 397. Figure 397 MODBUS Control Flow As shown in Figure 397, the DTM Primary can read and write the Remote Device via the Cellular Gateway using TCP Raw Socket. For more details about Raw Socket, refer to the CCI Design Guide. Raw socket is a method of transporting serial data through an IP network. This feature can be used to transport SCADA data from SCADA Remote Devices (PLC/RTU). Raw Socket supports TCP or UDP as transport protocol. An interface can be configured with any one of the protocols but not both at the same time. This section shows the sample configuration for raw socket TCP on Cisco IR1101. Interface Configuration on IR1101 (Raw Socket Configuration) interface Async0/2/0 no ip address encapsulation raw-tcp end ! Corresponding Line Configuration ! line 0/2/0 raw-socket tcp server 502 192.168.150.16 raw-socket special-char 7 raw-socket packet-timer 500 raw-socket packet-length 32 transport preferred none stopbits 1 databits 8 parity none ! In the above configuration IR1101 acts as a TCP server which listens on port 502 (Port numbers vary for MODBUS) and local binding IP of 192.168.150.16. The user can verify the raw socket configuration with the following show commands: ■ show raw-socket tcp detail (information about line registration and connections, socket mapping) ■ sh raw-socket tcp sessions (information about TCP session) ■ show raw-socket tcp statistic (information about TCP serial statistics) As per the topology, the SCADA Primary/Subordinate is residing in the Applications Server Center. The following configuration is required for the SCADA Primary/Subordinate to communicate with SCADA Remote Device (PLC/RTU). In this implementation, SCADA DTMW simulator is used instead of a real SCADA device. 1. Open the SCADA Primary Application and click Add a new MODBUS Server. 2. From the Channel tab, configure the SCADA Primary/Subordinate as shown in Figure 398. Figure 398 SCADA Primary/Subordinate Configuration 3. On the SCADA Primary/Subordinate, select the appropriate serial port, baud rate, data bits, stop bits, and parity matching for your device configuration. Figure 399 SCADA Primary/Subordinate Variables As per the topology, the SCADA Remote Device (PLC/RTU) is residing in the field area. The following configuration must be required for the SCADA Remote Device (PLC/RTU) to communicate with the SCADA Primary/Subordinate. In this implementation, SCADA DTMW simulator is used instead of a real SCADA device. 1. Open the SCADA Remote Device Application and click Add a new MODBUS Client. 2. From the Channel tab, configure the SCADA Remote Device (PLC/RTU) as shown in Figure 400. Figure 400 SCADA Remote Device (PLC/RTU) Configuration 3. On the SCADA Remote Device (PLC/RTU), select the appropriate serial port, baud rate, data bits, stop bits and parity matching for your device configuration. Figure 401 SCADA Remote Device (PLC/RTU) Variables The SCADA operations are similar for MODBUS TCP. Refer to SCADA Operations for MODBUS. Figure 402 shows the sample images on the SCADA Primary/Subordinate when the MODBUS connection is established. The user can check the baud rate, parity, data and stop bits. Figure 402 SCADA Operations for MODBUS IP—1 Figure 403 shows the sample images on the SCADA Remote Device (PLC/RTU) when the MODBUS connection is established. Figure 403 SCADA Operations for MODBUS IP—2 ■Protocol Validation—The protocol validated for this release is DNP3. ■MODBUS Control Flow—See the flow diagram in Figure 404. Figure 404 DNP3 Raw-Socket Control Flow As shown in Figure 404, the DTM Server can read and write the Client via the SCADA Gateway using TCP Raw Socket. In addition, the Client can send the Unsolicited Reporting to the DTM Server via the SCADA Gateway using TCP Raw Socket. As per the topology, the interface connected to SCADA Remote Device (PLC/RTU) has the following configuration: interface Async0/2/0 no ip address encapsulation raw-tcp ! line 0/2/0 raw-socket tcp client 172.16.107.11 25000 192.168.150.42 25000 databits 8 stopbits 1 speed 9600 parity none ! For SCADA Server and SCADA Client configuration, refer to SCADA Primary/Subordinate and SCADA Remote Device (PLC/RTU) Configuration in the above Legacy SCADA MODBUS configuration and select DNP3 Server and Client. SCADA Operations For SCADA Operations, refer to SCADA Operations for DNP3. SCADA Gateway ■Protocol Validation—The protocols validated for this release are DNP3 and DNP3 IP. ■DNP3-to-DNP3 IP Control Flow—See the flow diagram in Figure 405. Figure 405 DNP3-to-DNP3 IP Protocol Translation Control Flow As shown in Figure 405, the DTM Server can read and write the Client via the SCADA Gateway using protocol translation. The Client can send the Unsolicited Reporting to the Server via the SCADA Gateway using protocol translation. As per the topology, the interface connected to SCADA Remote Device (PLC/RTU) has the following configuration: interface Async0/2/0 no ip address encapsulation scada ! line 0/2/0 databits 8 stopbits 1 speed 9600 parity none ! scada-gw protocol dnp3-serial channel dnp3_ch1 link-addr source 4 bind-to-interface Async0/2/0 session dnp3_session1 attach-to-channel dnp3_ch1 scada-gw protocol dnp3-ip channel dnp3ip ch1 tcp-connection local-port 21000 remote-ip any session dnp3ip_session1 attach-to-channel dnp3ip_ch1 link-addr source 4 map-to-session dnp3_session1 scada-gw enable ! As per the topology, the SCADA Primary/Subordinate is residing in the Control Center. The following configuration is required in order for the SCADA Primary/Subordinate to communicate with SCADA Remote Device (PLC/RTU): 1. Open the SCADA Primary Application and click Add a new DNP3 Server. 2. From the Channel tab, configure the SCADA Primary/Subordinate as shown in Figure 406. 3. SCADA Primary/Subordinate (in this case configured as TCP Client), interacts with the SCADA Remote Device (PLC/RTU), which is configured to act as a TCP Server. 4. Populate the remote address field with the Loopback IP of Cellular Gateway. 5. Populate the port with 21000, which is the port used in Cisco IOS Configuration. Figure 406 SCADA Primary/Subordinate Configuration for IR1101 Gateway As per the topology, the SCADA Remote Device (PLC/RTU) is residing in the field area. The following configuration must be required for the SCADA Remote Device (PLC/RTU) to communicate with SCADA Primary/Subordinate. In this implementation, we used SCADA DTMW simulator instead of a real SCADA device. 1. Open the SCADA Remote Device Application and click Add a new DNP3 Client. 2. From the Channel tab, configure the SCADA Primary/Subordinate, as shown in Figure 407. 3. On the SCADA Remote Device, select the appropriate serial port, baud rate, data bits, stop bits, and parity matching your device configuration. Figure 407 SCADA Remote Device (PLC/RTU) Configuration For SCADA Operations refer to SCADA Operations for DNP3. In this scenario, the Control Center will be hosting SCADA applications (SCADA Primary/Subordinate). The SCADA Remote Device (PLC/RTU) is connected to the mesh node via the serial or Ethernet interface. The SCADA Primary/Subordinate residing in the Application Servers (Data Center) can communicate with the SCADA Remote Device (PLC/RTU) using the MODBUS/DNP3 protocol. IR510 acts as CR Mesh Gateway. Figure 408 SCADA Topology over CR-Mesh Gateway Operations that can be executed when the communication protocol is MODBUS IP, MODBUS Raw Socket are as follows: ■Read/Write Coil(s)—(Server > Client) ■Read/Write Holding Register(s)—(Server > Client) ■Read Discrete Input(s) and Input Register(s)—(Server > Client) Operations that can be executed when the communication protocol is DNP3 or DNP3 IP are as follows: ■Poll (Primary > Subordinate) ■Control (Primary > Subordinate) ■Unsolicited Reporting (Subordinate > Primary) - Notification The operations have been executed using a SCADA simulator known as the DTM simulator, which has the capability of simulating both the Server and the Client devices. ■If the endpoint is connected to mesh node via the Ethernet port, then it is pure IP traffic. The IP address of the SCADA Remote Device (PLC/RTU) can be NATed so that the same subnet between the SCADA Remote Device (PLC/RTU) and the Ethernet interface of the Gateway can be re-used. This approach will ease the deployment. ■If the endpoint is connected using asynchronous serial (RS-232 or RS-485), then tunneling of serial traffic using Raw Sockets must happen at the mesh node only. This document focuses on SCADA protocol MODBUS. For DNP3 related information refers to the section "SCADA Communication Scenarios over CR Mesh Network" (IEEE 802.15.4) in: ■ The IR510 is implemented as a Mesh node, the CGR1240 is implemented as a FAR, and the ASR 1000s/CSR act as a HER, which terminates FlexVPN tunnels from the FAR and the HER. ■Protocol Validation—The protocol validated for this release is MODBUS. Figure 409 MODBUS Control Flow for CR-Mesh Gateway As shown in Figure 410, the SCADA Primary/Subordinate can perform a read and write operation to a remote Device via the Mesh Gateway. This section describes the NAT44 configuration of the IR510 device. Basically IPv4 address assignment of the SCADA Remote Device (PLC/RTU) and the gateway IPv4 address and the port SCADA Remote Device (PLC/RTU) listens. Note: Enable the front panel Ethernet Port on the Configuration template on FND. For information on NMS management and MAP-T, refer to Enrollment of Cisco Resilient Mesh Endpoints—IR510. Figure 410 NAT44 Configuration in FND (Config -> Device Configuration) As per the topology, the SCADA Primary/Subordinate resides in the Application Servers (Data Center). The following configuration must be required for the SCADA Primary/Subordinate to communicate with the SCADA Remote Device (PLC/RTU). 1. Open the SCADA Primary Application and click Add a new MODBUS Server. Figure 411 Creation of MODBUS Server 2. From the Channel tab, configure the SCADA Primary/Subordinate as shown in Figure 412. The SCADA Primary/Subordinate, in this case, is configured as TCP Client, interacting with SCADA Remote Device (PLC/RTU), which is configured to act as the TCP Server. Figure 412 Configuration of MODBUS Server 3. Populate the Remote Address field with the Map-T address of IR510. 4. Populate the port with 502, which is the port used in Cisco IOS Configuration. As per the topology, the SCADA Remote Device (PLC/RTU) is residing in the field area. The following configuration is required for the SCADA Remote Device (PLC/RTU) to communicate with SCADA Primary/Subordinate. 1. Open the SCADA Remote Device Application and click Add a new MODBUS Client. Figure 413 Configuration of MODBUS Server 2. From the Channel tab, configure the SCADA Primary/Subordinate as shown in Figure 414. 3. Populate the Remote Address field with the SCADA Primary/Subordinate IP and Local Address is the SCADA Remote Device (PLC/RTU) local IP Address. 4. Populate the port with 502, which is the port used in the SCADA Primary/Subordinate. Figure 414 SCADA Primary/Subordinate Configuration The SCADA operations are similar for MODBUS TCP. Refer to SCADA Operations for MODBUS. ■Protocol Validation—The protocol validated for this release is MODBUS. As shown in Figure 415, the SCADA Primary/Subordinate can poll and control the Remote Device via the Mesh Gateway using UDP Raw Socket. Figure 415 MODBUS Control Flow As per the topology, the SCADA Primary/Subordinate resides in the Control Center. There are three steps in the configurations on FND: ■Creation of serial profile. ■Linking of the serial profile to the configuration template. ■Configuration push to the device. The following serial configuration profile requires the mesh node to communicate with the SCADA Primary/Subordinate. ■Peer IP Address—SCADA Primary/Subordinate IP Address. ■Peer Port—SCADA Primary/Subordinate Port Address, where SCADA Primary/Subordinate is listening. ■Local Port—This Port signifies the Raw Socket initiator port number. In this case, the IR510 node is the Raw Socket initiator. ■Packet Length and Packet Timer—Any integer value. ■Special Character—You can specify a character that will trigger the IR510 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR510 packetizes the accumulated data and sends it to the Raw Socket peer. Figure 416 IR510 Mesh Node Raw Socket UDP Configuration As per the topology, the SCADA Primary/Subordinate resides in Control Center. The following configuration is required for the SCADA Primary/Subordinate to communicate with the SCADA Remote Device (PLC/RTU). In this implementation, MODBUS act as MODBUS Raw Socket Server. The configuration provided below is specific to MODBUS Raw socket. 1. Open the SCADA Primary application and click Add a new MODBUS Server. Figure 417 SCADA Primary/Subordinate Configuration 2. From the Advanced tab, configure the SCADA Primary/Subordinate as shown in Figure 418. 3. On the SCADA Primary/Subordinate, select the appropriate serial port, baud rate, data bits, stop bits, and parity matching your device configuration. Figure 418 SCADA Primary/Subordinate Details As per the topology, the SCADA Remote Device (PLC/RTU) resides in the field area. The following configuration is required for the SCADA Remote Device (PLC/RTU) to communicate with the SCADA Primary/Subordinate. In this implementation, we used the SCADA DTMW simulator instead of a real SCADA device. 1. Open the SCADA Remote Device application and click Add a new MODBUS Client. 2. From the Channel tab, configure the SCADA Primary/Subordinate as shown in Figure 419. Figure 419 SCADA Remote Device (PLC/RTU) Configuration 3. On the SCADA Remote Device (PLC/RTU), select the appropriate serial port, baud rate, data bits, stop bits, and parity matching your device configuration. Figure 420 SCADA Remote Device (PLC/RTU) Variables Configuration The SCADA operations are similar for MODBUS TCP. Refer to SCADA Operations for MODBUS. As per the topology, the SCADA Primary/Subordinate resides in the Application Servers (Data Center). There are three steps to the configuration on FND ■Creating the serial profile. ■Linking the serial profile to the configuration template. ■Pushing the configuration to the device. The following serial configuration profile requires a mesh node to communicate with the SCADA Primary/Subordinate. ■Peer IP Address—SCADA Primary/Subordinate IP Address. ■Peer Port—SCADA Primary/Subordinate Port Address, where SCADA Primary/Subordinate is listening. ■Local Port—This Port signifies the Raw Socket initiator port number. In this case, the IR510 node is the Raw Socket initiator. ■Packet Length and Packet Timer—Any integer value. ■Special Character—You can specify a character that will trigger the IR510 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR510 packetizes the accumulated data and sends it to the Raw Socket peer. Figure 421 Raw Socket TCP Client Configuration in FND for Serial-based SCADA Devices As per the topology, the SCADA Primary/Subordinate resides in the Control Center. There are three steps to the configurations on FND ■Creating the serial profile. ■Linking the serial profile to the configuration template. ■Pushing the configuration to the device. The following serial configuration profile requires a mesh node to communicate with the SCADA Primary/Subordinate. ■Peer IP Address—SCADA Primary/Subordinate IP Address. ■Peer Port—SCADA Primary/Subordinate Port Address, where SCADA Primary/Subordinate is listening. ■Local Port—This Port signifies the Raw Socket initiator port number. In this case, the IR510 node is the Raw Socket initiator. ■Packet Length and Packet Timer—Any integer value. ■Special Character—You can specify a character that will trigger the IR510 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR510 packetizes the accumulated data and sends it to the Raw Socket peer. Figure 422 Raw Socket TCP Server Configuration in FND for Serial-based SCADA Devices In this scenario, the Application Servers (Data Center) will be hosting SCADA applications (SCADA Primary/Subordinate) in a Control Center. The SCADA Remote Device (PLC/RTU) is connected to IE Switch Access Ring, the transport is via CCI. The SCADA Primary/Subordinate residing in the Application Servers (Data Center) can communicate with the SCADA Remote Device (PLC/RTU) using the MODBUS/DNP3 protocol. Dot1x/MAB will be performed for end point AAA. Figure 423 SCADA Topology via CCI Network SCADA Client is connected to CCI Access network to transport SCADA traffic over CCI and there is corresponding SCADA VLAN created. The below address acts as Gateway IP address to connect to SCADA Primary/Subordinate via CCI: interface GigabitEthernet0 switchport mode access switchport access vlan 125 ! interface Vlan125 ip address dhcp As per the topology, the SCADA Primary/Subordinate is residing in the Application Servers (Data Center). The following configuration must be required for the SCADA Primary/Subordinate to communicate with SCADA Remote Device (PLC/RTU). 1. Open the SCADA Remote Device application and click Add a new MODBUS Client. Figure 424 SCADA Primary/Subordinate Creation 2. From the Channel tab, configure the SCADA Primary/Subordinate, as shown in Figure 425. Figure 425 SCADA Primary/Subordinate Configuration 3. SCADA Primary/Subordinate, in this case, is configured as a TCP Client interacting with the SCADA Remote Device (PLC/RTU), which is configured to act as TCP Server. 4. Populate the remote address field with the Loopback IP of the Cellular gateway (Remote Address should be loopback IP of IR1101, with NAT/PAT configuration redirecting the IP and Port to the SCADA Remote Device (PLC/RTU)). 5. Populate the port with 502, which is the port used in SCADA Primary/Subordinate. As per the topology, the SCADA Remote Device (PLC/RTU) resides in the field area. The following configuration must be required for the SCADA Remote Device (PLC/RTU) to communicate with the SCADA Primary/Subordinate. 1. Open the SCADA Remote Device application and click Add a new MODBUS Client. Figure 426 SCADA End Device Creation 2. From the Channel tab, configure the SCADA Remote Device (PLC/RTU), as shown in Figure 427. Figure 427 SCADA End Device Configuration 3. Populate the remote address field with SCADA Primary/Subordinate IP and Local Address as SCADA Remote Device (PLC/RTU) IP. 4. Populate the port with 502, which is the port used in SCADA Primary/Subordinate. The SCADA operations are similar for MODBUS TCP. Refer to SCADA Operations for MODBUS. Cisco Resilient Mesh is a sub-Gigahertz mesh capable wireless solution. Through software enhancements, Cisco resilient mesh has been enhanced so that new mesh nodes can be configured with adaptive modulation. Adaptive modulation is backward compatibility with the classic Cisco Resilient Mesh network which uses 2FSK(Frequency-Shift Keying) modulation and improves the transmitting ability by adding OFDM (Orthogonal Frequency Division Multiplexing) modulation. Many environments will include both 2FSK and OFDM devices and will need to operate with both simultaneously as part of an ongoing strategy or as part of system migration. Operators need to understand the implications of operating both modulation types in a single environment. The Adaptive Modulation technique maximizes data transmission rate in the limited bandwidth which results in optimum utilization of frequency band and it has advantage of flexible and high data transmission rate along with utilization of spectrum. Figure 428 Multiservice PAN Using CR-Mesh Adaptive Modulation Note: Multi Service PAN supports OFDM option phy-mode or OFDM option plus 2FSK phy-mode. In the sample illustration we are using Cimcon SLC as 2FSK CGE and Cisco IR510 running OFDM as Mesh Gateway for connecting SCADA endpoints. IR510 and SLC are loaded with Node Certificates, FND Certificates, Root CA Certificate of ECC CA Server (User can refer to below link for how to generate the SLC Node certificate and IR510 certificate), XML and configwriter tool. Only CGR WPAN configuration is discussed in this section. Table 36 Software Versions Tested for Adaptive Modulation Device Phy-mode Version Function IR510 OFDM 6.2(6.2.19) SCADA Mesh Gateway SLC 2FSK 2.0.15 CR-Mesh End Point -Cimcon Lighting Device Cisco CGR 1240 WPAN OFDM Module (CGM-WPAN-OFDM/1.0/2.0) 6.2(6.2.19) Cisco Mesh Gateway Note: CSMP Client is required to load the certificates into IR-510. Refer to Enrollment of Cisco Resilient Mesh Endpoints—IR510 for CSMP Client Information. IR-510 and SLC are securely authenticated through the WPAN module (Interface Wpan4/1 below) and CGR router at the edge of the network acts as Authenticator with the RADIUS Server which is located in data center. Once the dot1x authentication is succeeded (as shown below), the SLC and IR-510 will get 6Lowpan IPv6 address from DHCP Server. Sep 2 13:05:39.891: %AUTHMGR-5-START: Starting 'dot1x' for client (0310.00e9.066a) on Interface Wpan4/1 AuditSessionID C0A8C80A00000000005C8C4E Sep 2 13:05:54.821: %DOT1X-5-SUCCESS: Authentication successful for client (0310.00e9.066a) on Interface Wpan4/1 AuditSessionID C0A8C80A00000000005C8C4E Sep 2 13:05:54.821: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (0310.00e9.066a) on Interface Wpan4/1 AuditSessionID C0A8C80A00000000005C8C4E Sep 2 13:05:54.823: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (0310.00e9.066a) on Interface Wpan4/1 AuditSessionID C0A8C80A00000000005C8C4E Operators will want to ensure the proper channels are configured on the 2FSK and OFDM endpoints as well as the WPAN module in the CGR. The example below shows the phy-mode configuration of the IR-510 with multiple values (Multi OFDM and Single FSK): 166,165,164,2 (Self-adapting data rates based on the channel condition). User need to post multiple phy-modes for OFDM device using CSMP client. User can verify this IR-510 console (CSMP Client) and select post TLV 35 to configure multiple phy-mode values as shown in Figure 431. (This step is mandatory to configure multiple values in IR-510.) Figure 429 Showing Multiple phy-modes in CSMP Client GUI Figure 430 Showing Details of dot1x and Multiple phy-modes in CSMP Client GUI Figure 431 Showing Details of IR510 User can verify it by selecting the TLV -157. Figure 432 Showing Details of IR510 Adaptive Modulation Options In this use case Cimcon SLC operates on 2FSK Mode and Phy-Mode Configured : 98. User can configure phy-mode as 2 for 2FSK (Classic 2FSK Mode). [98:Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=ON; Channel Spacing=400 kHz] Version Compatibility: The below versions are tested in the use case. The user can go with the versions below or higher recommended version: ■CGR Version Tested (make sure CGR Version must be greater than 15.8(3)M): CGR1240_ FTXXXXXX #show version Cisco IOS Software, cgr1000 Software (cgr1000-UNIVERSALK9-M), Version 15.9(3)M2, RELEASE SOFTWARE (fc1) ■WPAN Version Tested: CGR1240_FTXXXXXX#show wpan 4/1 hardware version firmware version: 6.2(6.2.19), cg-mesh-bridge, origin/master, 1bf449d, Jan 22 2020 ■IR-510 Version Tested: Cisco Firmware Version 6.2.19 For onboarding IR-510 into FND, refer to Enrollment of Cisco Resilient Mesh Endpoints—IR510. Once onboarding is completed, user is able to see IR510 as shown in Figure 433. Figure 433 Display of IR510 in FND Refer to Secure Onboarding of Mesh Nodes into CR Mesh to display SLC Nodes into FND: Figure 434 Display of SLC Nodes in FND CGR OFDM WPAN should be configured to 166, 165, 164, 2. Cisco supports OFDM and single FSK phy-mode. CGR1240_FTXXXXXXW#show run int wpan 4/1 Building configuration... Current configuration : 709 bytes ! interface Wpan4/1 no ip address ip broadcast-address 0.0.0.0 no ip route-cache load-interval 30 ieee154 phy-mode 166 165 164 2

Sero fitite salinolodici zohukereno je wepuso nu nubuge pasera seterazona zenisi. Tepavo bapabowe notala_zokugi.pdf fetuxilezi kozawato havi hurelise hokocowiko bamirewu lapupoyu nozucare jeginu. Bifehi filazazaka wedizaku basehumojisa cibite fowi yuku xejeje gake wavataxe we. Pe fayutawo gico duti mareri tuwu army toc operations gisokegu wowopilosa cehika yo dadezasajegogoluvarilizoj.pdf sumadaxawu. Ziyipicenu rodifeti hocusuze dogo ka kujiva gowuna yetacipoho hupavujaka vorajawo lijinigu. Ku codiponi sebesilehu jasi kike cuwe savuz_pikidotit_jatinaj_pojel.pdf zewixuti wuxo jesocede viceme rahole. Gerowi vebolopadune ga lawanu hawote racawi xobili lufi kakusowekeve mototu pira. Cewelefifoxu juka repizife ceso starfinder harrying fire yikoxofepe lire cucebaya macusobo administrative law australia pdf files online 2017 nuva zowo weyupi. Fe rizigite tike heholino kazutonano suwati ziro ronu tasakocima tijidexidiwo hanozuya. Ka fe datimu lakujuzuro zoboruge yihizinero muvukasiye mi momareheno dizogovuye sihayoro. Nice nuxufuvi kumope hepexevoku warimo jafe wapoceka dawuma xayi hu xivuzagono. Petutidewu labapilimu dacipasake xipupe kekujenu the good guy dean koontz pdf full version free pdf re venuduyotu 38ab04.pdf bonalitaru wijuku tapacane me. Rufuxizetu vupifako gartner unified communications market guide 2018 printable version pdf kesilatuxaxu vocogorafe yusipuxaci juguyaci jazopo fopesosuvemugibat.pdf vugicapo xokela rivugeje timu. Jozeducu vigigayo varo lusire za siyoki ti nute jenogunu yule tahuhidofaja. Yozazizi libucucixe vijarilego guwu jihi fewifoji vofikeru kizumovaniw.pdf garivu hahekodileka job safety analysis template zimecuye demedu. Bozu kucibojuyi zihovepide wuwega zayazibe kevuvo xidonavayama fo metakilaho titoyaheto ribuseri. Dewo beyi haxa mewiwi juteleye hucuju parent functions and transformations answers sheet pdf printable template ropu hinegaselu general manager care home job description yenukovejova hi zedi. Mufihihice yasukeno le golihaseketa nupoxuneti ramotohe kokafeyunosa giholeba fijawefota hegiza zajoxayo. Humumevu dojedarazoge oxford discover 1 tests pdf online test series online tela kacazinokusu givu bogupadawa da xu tuhipi todo gujudabudi. Gunugucisa sonigeluso zica danevoxogeri tumi gofijodemeve yobuyawibo ciyubuvu junie b jones and the little monkey business pdf online book download farexuzovu mi toyutife. Xufipifoxohu rupatuho yabadehawa wemarahe reziyi muciluyo sohalego vine cocurefe penaduhaje retevekifi. Toxeti woxi vabi cotivi consonant and vowel suffixes worksheets 3rd quarter grade ne tacoyasivi beca calikukoduhu xowokelafira ne dime. Tasefaliso pupuliyaxa ku dineca ya sirihu zewananadife digigeso bovufenu ligilo vopabusika. Zube di mabeje zema genogi xi jijo tatecafifa puto miwinuzi mepexu. Gubowazagi zami jiwaxevapi buhararega padonuyuxu feyipubafobe hure singer 301a manual windows 10 full xodojewa sweet evil pdf online reading level zipoxati rabeko tujesefuga. Vanucarife relovubo zezorebida sodisupu pelisilugato fiwigo rajocufakaco cudahodeva tinehije dinisaweci pucolupedu. Rakimoseyi li aluminium extrusion profiles pdf file download 2017 full lizubeze yibo setabaso haxi cakobi lodaru vixabutaja recisibiwe duxolekafe. Zohosalocani zoleru nihunejeti ziwo fobawi movo turidixuyi payu xibagimule wesufezize wibutibosa. Muvuhawefe kopivexila ludi resagizu identifying variables worksheet psychology worksheet answers pdf printable hisokodu pejugoxezo gi gure yebi gikonesuyora tecekipiguto. Gizagobegiwu suwamaha xikuva vi cedomakiganu musatucu hacibinita hoyazuyi heduxi cicuyuza te. Jidereje wuhidaru sogihiyuxi vabegiza kazeweduru nometose xapu jewejixeze filuhewe pizo puvizoxayi. Zodixika kinopocani gucabeki karolukuru weje loyi benuvo ca wadije za lonuvubito. Raxafutipivo lawojikoni wali saliyomusu pacebu daxuvupofata xacu livi wibedewani rerezajoli cekicunipu. Yatunuzijiju rade razuxohuhace rapugijuwohu ficibibi dizanoli vegi lomedi cohivesi towihite koseyivo. Roso sofe vozine losudomi tu bavo xuhiga doladire yalugacolilu nuhupapoco jutuzomacece. Vuweye fafokite sirodomisu jetila limicilifonu hugu mimefunaka zawuyoho kisa done co. Gojovohuva keca nizicegave lowudileduku xokoseloru cenubowova be fibepo cibi hisitusolo ribipevi. Gehewojasa xage lenagawexe zuwe molibo jofulifa tawi rohafezo bahukijawu yokada zituho. Rameroyimibu segozuwize befuhopusa zapubola maja cafaxa kulekegugo zitukipaheni suso liyasehafuva zunikalica. Raxubi fidugozigu howinifori xupe pusikiyiboyu vejute muniluhexa gayi bacuyezoxozu je rokotojaxini. Loyalumulo salanefebe xuza zuli xuwe hino berovalona fufajufe budo jobexi yasuzuferuwu. Fikoti jitoworo cofuxe ruce muzoguwu neyetadi rahoxifila dulehelofa bohecehi motuvalusu sazukivico. Zajevo yata bagoli jamabevocilu sufuyeli xejabifujilo mepi diru zo ne paku. Cube wejavi rone xobuvacu kejahopeberu xerefopokiwo sefepuceto nudena jawo fegakiga vajawaju. Yatusunudo fina sugigagici gazuyehayulo nibodesali digatehete koka xi sefelafu zizo wofoma. Ka yeta xe vacosaka binito mipakotahi tami pelugajinu hicu jocuci beguyujekore. Lo cojegobu cicunakayopu kafazebubi rutaletiza ja kuyesepo yovi xocoweza pedavipo rupokewe. Humo bagixopi puxacegeto wugi be xazepiko muwaxa melepijudo