Cisco Wireless LAN Controller Configuration Guide, Release 7.0 alah CISCO Chapter 4 - Configuring Controller Settings Cisco Wireless LAN Controller Configuration Guide, Release 7.0 Downloads: This chapter T (PDF - 3.23MB) The complete book (PDF - 34.93MB) | I Feedback sou mireas cart Council e onfiguration Calk, Release 7.0 Preface Chapter 1 - Overview Chapter 2 - Using the Web-Browser and CLI Interfaces Chapter 3 - Configuring Ports and Interfaces Chapter 4 - Configuring Video Streams Chapter 6 - Configuring Security Solutions Chapter 7 - Configuring WLANs Chapter 7 - Controlling Lightweight Access Points Chapter 9 - Controlling Lightweight Access Points Table of Contents Configuring Controller Settings Installing and Configuring Licenses Obtaining an Upgrade or Capacity Adder License Installing a License Installing a License Using the GUI to Install a License Using the CLI to Install a License Viewing Licenses Using the GUI to View Licenses Using the CLI to View Licenses Mewing Lichises
Using the CUI to View Licenses
Using the CUI to View Licenses
Using the CUI to View Licenses
Using the CUI to Activate and Extenses
Choosing the License feature. Set
Using the CUI to Activate an AP-Court Evaluation Licenses
Using the CUI to Activate an AP-Court Evaluation Licenses
Using the CUI to Activate an AP-Court Evaluation Licenses
Using the CUI to Activate an AP-Court Evaluation Licenses
Using the CUI to Activate an AP-Court Evaluation Licenses
Using the CUI to Activate an AP-Court Evaluation Licenses
Using the CUI to Rehost a License
Using the CUI to Activate an AP-Court Evaluation Licenses
Using the CUI to Activate an AP-Court Evaluation Licenses
Using the CUI to Configure the License Activate and AP-Court Evaluation Licenses
Using the CUI to Configure the License Activate and AP-Court Evaluation Licenses
Using the CUI to Configure the License Activate and AP-Court Evaluation Licenses
Using the CUI to Configure the License Activate and AP-Court Evaluation Licenses
Using the CUI to Configure Application
Using the CUI to Configure A Access Points Chapter 9 - Controlling Mesh Access Points Chapter 9 - Controlling Mesh Access Points Chapter 10 - Managing Controller Software and Configurations Chapter 11 - Managing User Accounts Chapter 12 - Configuring Radio Resource Management Chapter 13 - Configuring Clisco CleanAir Chapter 14 - Configuring Mohility Chapter 14 - Configuring Mobility Groups Chapter 15 - Configuring Hybrid RFAP REAP Appendix A - Safety Considerations and Translated Safety Warnings Appendix B - Declarations of Conformity and Regulatory Information Appendix C - End User License and Warnanty Appendix D - Troubleshooting Appendix D - Troubleshooting Appendix E - Logical Connectivity Diagrams Index Configurio SNMP Control the GUI to Chano the SNMP Community Strings Using the GUI to Chano the SNMP Community String Default Values Using the GUI to Chano the SNMP Community String Default Values Changing the Default Values for SNMP v3 User Default Values Using the GUI to Chano the SNMP v3 User Default Values Configuring Agrometic the SNMP v3 User Default Values Client Association Limits for Autonomous IOS Access Points Client Association Limits for Autonomous IOS Access Points Using the GUI to Configure Agrometicave Load Balancia Literrit Association Limits for Autonomous IOS A Using the GUI to Configure Aggressive Load Balancing Using the CLI to Configure Aggressive Load Balancing nliguring Band Selection Lining the CLI to Configure Aggressive Load Balancing Confloring Band Selection Guidelinas for Using the Band Selection Using the GLU to Configure Band Selection Using the GLU to Configure Band Selection Configure Fast SSID Changing Using the GLU to Configure B02.3 Bridging Using the GLU to Fashle Multicast Mode Using the GLU to Verw Multicast Hode Using the GLU to Fashle Multicast Mode Co Configuing Client Rearing Inter-Schröder Rearing Inter-Schröder Rearing Inter-Schröder Rearing Volke-over P-Telephone Rearing Coll Legich Rearing Using the CLI to Configure CCX Client Rearing Parameters Using the CLI to Configure CCX Client Rearing Parameters Using the CLI to Configure CCX Client Rearing Information Using the CLI to Configure CCX Client Rearing Information Using the CLI to Configure CCX Client Rearing Information Using the CLI to Configure CCX Client Rearing Information Configuring Quality of Service Configuring Quality of Service Configuring Cuality of Service Cail Admission Control Bandwidth-Based CAC Lace-Based CAC Lace-Service Cuality Configure Configure Configure Tarille Stream Metrics Using the CLI to Configure Noise Parameters Taffle Stream Metrics Using the GUI to Configure Voice Parameters Using the GUI to Configure Video Parameters Using the GUI to Configure Video Settings Using the GUI to Configure Media Parameters Using the GUI to Configure Media Parameters Using the CLI to Configure Video Parameters Using the GUI to Configure Deco Parameters Using the GUI to Configure EDCA Parameters Using the CLI to Configure EDCA Parameters onfiguring Clisco Discovery Protocol Using the GUI to Configure EDce Discovery Protocol Using the GUI to View Clisco Discovery Protocol Informati Using the CLI to Ordigure the Clisco Discovery Protocol Using the CLI to Ordigure the Clisco Discovery Protocol Using the CLI to View Clisco Discovery Protocol Informatic Optimizing EPC Tage Tageting Using the CL to View Cisco Discovery Protocol Infor onfiguring RFD Tag Tracking Using the CL to Configure RFD Tag Tracking Using the CL to View RFD Tag Tracking Information Using the CL to Debug RFID Tag Tracking Issues onfiguring and Mewing Location Settings Installing the Location Appliance Certificate Synchronizing the Controller and Location Appliance Configuring Location Settings Viewing Location Settings Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues Instantial Table Residence Constrained Instrument Automatic Residence Networks IMSE Settings Destinguing IMSE Settings Using ImSE CLI to Reset the Controller to Default Settings Using ImSE CLI to Reset the Controller to Default Settings Using ImSE CLI to Reset the Controller to Default Settings Using ImSE CLI to Reset the Controller to Default Settings

- Configuring Controller Settings
- This chapter describes how to configure settings on the controller. It contains these sections
 - Installing and Configuring Licenses
 - Configuring 802.11 Bands
 - Configuring 802.11n Parameters Configuring 802.11h Parameters

- Configuring DHCP Prox Configuring Administrator Usernames and Passwords Configuring SNMP . Changing the Default Values of SNMP Community Strings Changing the Default Values for SNMP v3 Users Configuring Aggressive Load Balancing Configuring Band Selection Configuring Fast SSID Changing Enabling 802.3X Flow Control Configuring 802.3 Bridging Configuring Multicast Mode Configuring Client Roaming Configuring IP-MAC Address Binding Configuring Quality of Service Configuring Voice and Video Parameters Configuring EDCA Parameters Configuring Cisco Discovery Protoco Configuring RFID Tag Tracking Configuring and Viewing Location Settings Configuring the Supervisor 720 to Support the WiSM Using the Wireless LAN Controller Network Module Resetting the Controller to Default Settings Installing and Configuring Licenses You can order Cisco 5500 Series Controllers with support for 12, 25, 50, 100, 250 or 500 access points as the controller's base capacity. You can add additional access point capacity through capacity adder licenses available at 25, 50, 100 and 250 access point capacities. You can add additional access points. The base and adder licenses are supported through both rehosting and RMAs 0 Note These controller platforms do not require licenses: Cisco 2100 and Cisco 4400 Series Controllers, Cisco WiSMs, Controller Network Modules, and Catalyst 3750G Integrated Wireless LAN Controller Switches. The base license supports the standard base software set and, for releases 6.0196.0 and later, the premium software set is included as part of the base feature set, which includes this functionality · Datagram Transport Layer Security (DTLS) data encryption for added security across remote WAN and LAN links 0 Note See the "Configuring Data Encryption" section for more information on data encryption. Support for OfficeExtend access points, which are used for secure mobile teleworking 0 Note See the "OfficeExtend Access Points" section for more information on OfficeExtend access points. Support for the 1130AG and 1240AG series indoor mesh access points, which dynamically establish wireless connections in locations where it might be difficult to connect to the wired network 0 Note See "Controlling Mesh Access Points." for more information on mesh access points. All features included in a Wireless LAN Controller WPLUS license are now included in the base license: this chance is introduced in release 6.0.196.0. These WPlus license features are included in the base license OfficeExtend Al Enterprise Mesh CAPWAP Data Encryption The licensing change can affect features on your wireless LAN when you upgrade or downgrade software releases, so you should be aware of these guidelines • If you have a WPlus license and you upgrade from 6.0.xx to 7.0.98.0, your license file contains both Basic and WPlus license features. You won't see any disruption in feature availability and operation • If you have a WPlus license and you downgrade from 7.0.98.0 to 6.0.196.0 or 6.0.188 or 6.0.182, your license file contains only base license, and you will lose all WPLUS features If you have a base license and you downgrade from 6.0.196.0 to 6.0.188 or 6.0.182, when you downgrade, you lose all WPIus features. To view the controller trap log, choose Monitor and click View All under "Most Recent Traps" on the controller GUI (see Figure 4-1). 0 Note You can also view traps by using SNMP-based management tools. Figure 4-1 Trap Logs Page cisco Tun 4p - 57 Of 15:59 2009 Control path to mobility member 17:17:17:13 18 is down Monitos 10 Dense Not Available for feature. Tr F Access Points 20 ▶ Statistics San Spr 27 pr 11:056 3000 APS Interface (5:15:12) Operation State Up: Base Radio MAC(00118174:05:65:80 Cause+Admin Configured San Ger 27 pr 11:050 7000 APS Interface (5:05:51:10) Operation State Down: Base Radio MAC 00:18:74:15:05:00 Cause+Admin Configured F CDP The An 2017 Bin An 2017 Bin Res 2009 MPS Interface (JRS2 2120 Operation State Own: Teste Red(J RAC 0018 Heiselie State Operation Configu-Bin An 2017 Bin An 2017 Bin Res Interface (JR22 Bin Annument Configured Content of Configured Content of Configured Content Bin Annument Configured Content (JR22 Bin Annument Content of Content of Content of Content of Content of Content Bin Annument Content of Content 45 F Reques Clients Multicast 30 AP's Interface 1(11511a) Operation State Down, Dase Radio MAC 00-10-74-55-05-08 Cause-Admin Contiguied Sun Ken 20 Sun Ken 20 State Values Radio MAC:00110174/165165100 Cause+Acmin Configured Sun An 31 614 45 AP's Interface (2017, 11b) Constitute State Up: Pass Radio MAC(00)10: No.60(60:00, Constan Action Continues) The ap-count licenses and their corresponding image-based licenses are installed together. The controller keeps track of the licensed access point count and does not allow more than the number of access points to associate to it. The Cisco 5500 Series Controller is shipped with both permanent and evaluation base and base-ap-count licenses. If desired, you can activate the evaluation licenses, which are designed for temporary use and set to expire after 60 days. 1 Note See the "Choosing the Licensed Feature Set" section for instructions on activating an image-based evaluation license and the "Activating an AP-Count Evaluation License" section for instructions on activating an ap-count evaluation license. No licensing steps are required after you receive your Cisco 5500 Series Controller because the licenses you ordered are installed at the factory. In addition, licenses and product authorization keys (PAKs) are preregistered to serial numbers. However, as your wireless network evolves, you might want to add support for additional access points or upgrade from the standard software set to the base software set. To do so, you need to obtain and install an upgrade license. Obtaining an Upgrade or Capacity Adder License A certificate with a product authorization key (PAK) is required before you can obtain an upgrade license You can use the capacity adder licenses to increase the number of access points supported by the controller up to a maximum of 500 access points. The capacity adder licenses are available in access point capacities of 10, 25, 50, 100 and 250 access points. You can add these licenses to any of the base capacity licenses of 12, 25, 50, 100 and 250 access points. For example, if your controller was initially ordered with support for 100 access points (base license AIR-CT5508-100-K9), you could increase the capacity to 500 access points by purchasing a 250 access point, 100 access point, and a 50 access point additive capacity license (LC-CT5508-250A, LC-CT5508-100A, and LIC-CT5508-50A). You can find more information on ordering capacity adder licenses at this URL: http://www.cisco.com/en/US/products/ps10315/products/ps103 0 Note If you skip any tiers when upgrading (for example, if you do not install the -25U and -50U licenses along with the -100U), the license registration for the upgraded capacity fails. For a single controller, you can order different upgrade licenses in one transaction (for example, -25U, -50U, -100U, and -250U), for which you receive one PAK with one license. Then you have only one license (instead of four) to install on your If you have multiple controllers and want to upgrade all of them, you can order multiple quantities of each upgrade license in one transaction (for example, you can order 10 each of the -25U, -50U, -100U, and -250 upgrade licenses), for which you receive one PAK with one license. You can continue to register the PAK for multiple controllers until it is exhausted. Base license SKUs for the Cisco 5500 Series Controllers are as follows: AIR-CT5508-12-K9 AIR-CT5508-25-K9 • AIR-CT5508-50-K9 AIR-CT5508-100-K9 AIR-CT5508-250-K9
 - The capacity adder SKUs are as follows: LIC-CT5508-25A
 - LIC-CT5508-50A
 - LIC-CT5508-100A
 - LIC-CT5508-250A

• AIR-CT5508-500-K9

To obtain and register a PAK certificate, follow these steps

Step 1 Order the PAK certificate for an upgrade license through your Cisco channel partner or your Cisco sales representative, or order it online at this URL:

http://www.cisco.com/go/ordering

Step 2 If you are ordering online, begin by choosing the primary upgrade SKU L-LIC-CT5508-UPG or LIC CT5508-UPG . Then, choose any number of the following options to upgrade one or more controllers under one PAK. Table 4-1 lists the capacity adder licenses available through email or on paper.

Table 4-1 Available Capacity Adder Licenses

Туре	Part Number	Description
email	L-LIC-CT5508-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many controllers under one product authorization key
	L-LIC-CT5508-25A	25 AP Adder License for the 5508 Controller (eDelivery)
	L-LIC-CT5508-50A	50 AP Adder License for the 5508 Controller (eDelivery)
	L-LIC-CT5508-100A	100 AP Adder License for the 5508 Controller (eDelivery)
	L-LIC-CT5508-250A	250 AP Adder License for the 5508 Controller (eDelivery)
paper	LIC-CT5508-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU, to upgrade one or many controllers under one product authorization key
	LIC-CT5508-25A	25 AP Adder License for the 5508 Controller
	LIC-CT5508-50A	50 AP Adder License for the 5508 Controller
	LIC-CT5508-100A	100 AP Adder License for the 5508 Controller
	LIC-CT5508-250A	250 AP Adder License for the 5508 Controller
	•	

Note If you require a paper certificate for Customs, order it without the "L-" in the SKU (for example, LIC-CT5508-250A) and choose to ship it using U.S. mail.

Step 3 After you receive the certificate, use one of two methods to register the PAK:

Cisco License Manager (CLM) —This method automates the process of obtaining licenses and deploying them on Cisco devices. For deployments with more than five controllers, we recommend using CLM to register PAKs and install licenses. You can also use CLM to rehost or RMA a license.

0

Note 'Voic cannot use CLM to change the licensed feature set or activate an ap-count evaluation license. To perform these operations, you must follow the instructions in the "<u>Choosing the Licensed Feature Set" section</u> and the '<u>Activating</u> an <u>AP-Count Evaluation License</u>' section, Because you can use CLM to perform all other license operations, you can disregard the remaining licensing information in this chapter except these two sections and the '<u>Conflouring the</u> <u>License Aperts</u> section' you wan your controller to use HTTP to communicate with CLM.

9

Note You can download the CLM software and access user documentation at this URL:

http://www.cisco.com/

• Licensing portal —This alternative method enables you to manually obtain and install licenses on your controller. If you want to use the licensing portal to register the PAK, follow the instructions in Use the licensing portal to register the PAK.

Step 4 Use the licensing portal to register the PAK as follows

- a. Go to http://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet
- b. On the main Product License Registration page, enter the PAK mailed with the certificate in the Product Authorization Key (PAK) text box and click Submit
- c. On the Validate Features page, enter the number of licenses that you want to register in the Qty text box and click Update
- d. To determine the controller's product ID and serial number, choose Controller > Inventory on the controller GUI or enter the show license udi command on the controller CLI.

Information similar to the following appears on the controller CLI:

Device# PID SN UDI

- 0 AIR-CT5508-K9 FCM1308L030 AIR-CT5508-K9:FCM1308L030 On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to install the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click Submit.
 - f. On the Finish and Submit page, verify that all information is correct and click Submit
 - g. When a message appears indicating that the registration is complete, click Download License . The license is emailed within 1 hour to the address that you specified.
 - h. When the email arrives, follow the instructions provided.
 - i. Copy the license file to your TFTP server.
 - j. Follow the instructions in the "Installing a License" section below to install the license on your controller.

Installing a License

You can use the controller GUI or CLI to install a license on a Cisco 5500 Series Controller.

Using the GUI to Install a License

To install a license on the controller using the controller GUI, follow these steps:

Step 1 Choose Management > Software Activation > Commands to open the License Commands page (see Figure 4-2).

Figure 4-2 License Commands Page

սիսիս						50 <u>8</u> 080	infiguration 2	ing og	n it <u>R</u> ofersin
CISCO	MONITOR	WLANS	CONTROLLOR	WIRELESS	CECUPIT*	MANAGEMENT	COMMANDIC	HELP	TEEDBACK
Management Summory F SNMP HITTP HITTPS TelevI-SSH	Cicense Action	e Comme	ands st st. st. 	C & COMMAN CONSC CONSC Ense ader Jalo	M 2				
Serial Port Lin al Management Users User Sessions			Tr an s		70				
Momt Via Wireless									
 Software Activation Fireases Firease Firsel Sommanes Firease Agent 									
▶ Tech Support	~ <				200			1	

Figure 4-3 License Commands (Install License) Page

	MONITOR W/J		NULLIN STILL	LESC SE	י אדני.:	MANA SEMEN	с соямия	NDIS LIELE					
anagement	License Com	mands					1						
Summary													
SNMP	Action		[Tristall con	isc	*							
HTTP Telact-SSH	Install license	from a file											
Serial Port	Figure to in-	stall (#p*/)	ļ			/ / d							
Local Management			`	Insta	ill License	, 11 10 - 11 11	n 9						
User Sessions													
Lugs													
Mymt Via Wireless													
Janses											58		
Loance Agant											2741		
p 3 In the File Name to I	install text box, enter the	path to the licer	nse (*.lic) on the TF	TP server.									
p 4 Click Install License not found, the license	 A message appears to e does not belong to this 	o show whether device, you do	r the license was in not have correct p	stalled succe ermissions fo	ssfully. If the r the license	e installation fail e, and so on.	s, the messa	ge provides the	e reason for the	e failure, such a	s the license	is an existing li	cense, the path wa
p 5 If the end-user licens	se agreement (EULA) ac	ceptance dialog	g box appears, read	the agreeme	ent and click	Accept to acc	ept the terms	of the agreem	ent.				
A													
Note Typically, you an	e prompted to accept the	EULA for evalu	uation, extension, a	nd rehost lice	enses. The E	EULA is also re	quired for per	manent license	es, but it is acc	epted during lice	ense general	ion.	
p 6 Save a backup copy	of all installed licenses a	as follows:											
a. From the Action d	drop-down list, choose Sa	ave License .											
b. In the File Name	to Save text box, enter th	ne path on the T	FTP server where	you want the	licenses to	be saved.							
Note You cannot save e	valuation licenses.												
c Click Save Licen	1995												
n 7 Report the controllo	н.												
n8 Follow the instruction	ns in the "Viewing Licens	ses" section to a	see the statue of the	license that	VOU installe	d.							
p 8 Follow the instruction	a is not being used by the	a controller folio	w the instructions i	n the "Choos	ing the Lice	u. nsed Feature S	et" section o	the "Activatio	n an AP-Count	Evaluation Lice	nse" section	to change the l	icense that is use
by the controller.	to not boing about by and			01000	ang tro croo		000000110	10 1001001	ganna oban	E faidatorr Eloc	100 000001	to onlinge the i	
the CLI to Install a Lice	ense												
tall a license on the contr	roller using the controller	CLI, follow thes	se steps:										
p 1 Install a license on the	he controller by entering	this command:											
se install url													
e url is tftp:// server_ip / p	ath / filename .												
Note To remove a lice	ense from the controller, e	enter the licens	e clear license_na	me comman	d. For exam	ple, you might	want to delet	an expired e	valuation licen	se or any unuse	d license. Y	u cannot delet	e unexpired evalua
licenses, the pe	ermanent base image lice	ense, or license	es that are in use by	the controlle	er.								
p 2 If you are prompted	to accept the end-user lic	cense agreeme	nt (EULA), read and	d accept the t	terms of the	agreement.							
pp 2 If you are prompted t	to accept the end-user lic	cense agreeme	nt (EULA), read and	d accept the t	terms of the	agreement.							
P 2 If you are prompted to Note Typically, you are	to accept the end-user lic	cense agreemen EULA for evalu	nt (EULA), read and uation, extension, a	d accept the t	terms of the senses. The E	agreement. EULA is also re	quired for per	manent license	es, but it is acc	epted during lice	ense general	ion.	
p 2 If you are prompted in the	to accept the end-user lic e prompted to accept the license or delete commer	cense agreemen EULA for evalu	nt (EULA), read and uation, extension, a se by entering this o	d accept the t nd rehost lice command:	terms of the senses. The E	agreement. EULA is also rei	quired for per	manent license	es, but it is acc	epted during lice	ense general	ion.	
p 2 If you are prompted in Note Typically, you are p 3 Add comments to a lise comment { add dela	to accept the end-user lic e prompted to accept the license or delete commer ete } license_name comi	e EULA for evalutions from a licens	nt (EULA), read and uation, extension, a se by entering this o	d accept the t nd rehost lice	terms of the a	agreement. EULA is also ree	quired for per	manent license	es, but it is acci	epted during lice	ense general	ion.	
p 2 If you are prompted to Note Typically, you and p 3 Add comments to a li se comment (add) dek p 4 Save a backup copy	to accept the end-user lic e prompted to accept the license or delete commer ete) license_name com or di linstalled licenses b	EULA for evaluents from a licens	nt (EULA), read and uation, extension, a se by entering this o command:	d accept the t	terms of the a	agreement. EULA is also rei	quired for per	manent license	es, but it is acci	epted during lice	ense general	ion.	
p 2 If you are prompted to Note Typically, you an p 3 Add comments to a l se comment (add dek p 4 Save a backup copy se save unt units tito?/ server ip/ p	to accept the end-user lic e prompted to accept the license or delete commer ete) license_name com of all installed licenses to ath / filename.	EULA for evalu- e EULA for evalu- nts from a licens ment_string by entering this	nt (EULA), read and uation, extension, a se by entering this o command:	d accept the t	terms of the anses. The E	agreement. EULA is also re	quired for per	manent license	es, but it is acc	epted during lice	ense general	ion.	
p 2 If you are prompted to Note Typically, you an p 3 Add comments to a l se comment { add dek p 4 Save a backup copy se save url a url is tftp:// server_/p / p p 5 Rebot the controlle	to accept the end-user lic e prompted to accept the license or delete commer ete } //cense_name com of all installed licenses t ath / filename . rr by entering this comma	Depute the series of the serie	nt (EULA), read and uation, extension, a se by entering this o command:	d accept the t	terms of the a	agreement. EULA is also rer	quired for per	manent license	as, but it is acc	epted during lice	ense general	ion.	
p 2 If you are prompted i Note Typically, you an p 3 Add comments to a I p 4 Save a backup copy se save url url is thp://server_ip/p p 5 Reboot the controlle system	to accept the end-user lic e prompted to accept the license or delete commer det) license, name com r of all installed licenses t ath / filename . r by entering this comma	e EULA for evaluation of the e	nt (EULA), read and uation, extension, a se by entering this o command:	d accept the t	terms of the a	agreement. EULA is also rer	quired for per	manent license	es, but it is acco	epted during lice	ense generat	ion.	
p 2 if you are prompted in Note Typically, you an p 3 Add comments to all p 4 Save a backup copy as eacomment (add del p 4 Save a backup copy as eace unf un is titp://server_ip/p p 5 Reboot the controlle system p 6 Follow the instruction	to accept the end-user lic e prompted to accept the license or delete commer ete) license_name com of all installed licenses t ath / filename . rr by entering this comma ns in the "Viewing Licens	EULA for evalu- the EULA for evalu- the from a licens ment_string by entering this und:	nt (EULA), read and uation, extension, a se by entering this o command:	d accept the t nd rehost lice command:	terms of the a	agreement. EULA is also ree	quired for per	manent license	as, but it is acc	epted during lice	ense general	ion.	
p 2 If you are prompted to Note Typically, you and p 3 Add comments to a l se comment (add dek p 4 Save a backup copy se save uri uri is tip// server_/p/ p p 5 Reboot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller.	to accept the end-user lic e prompted to accept the license or delete commer ette } //cense_name com of all installed licenses t ath / filename . r by entering this comma ns in the <u>"Viewing Licens</u> a is not being used by the	EULA for evalu- the EULA for evalu- the from a licens ment_string by entering this ind: ses" section to se a controller, folic	nt (EULA), read and uation, extension, a se by entering this o command: see the status of the wy the instructions i	d accept the t nd rehost lice command: e license you n the <u>"Choos</u>	terms of the anses. The B installed.	agreement. EULA is also ree	quired for per	manent license	ss, but it is acc g an AP-Count	epted during lice	anse generat	ion.	icense that is used
p 2 If you are prompted to Note Typically, you and p 3 Add comments to all see comment { add dek p 4 Save a backup copy se save url ourl is thp// server_/ip/ p p 5 Rebot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller.	to accept the end-user lic e prompted to accept the license or delete commer ete) license_name com of all installed licenses t ath / filename . rr by entering this comma ns in the <u>"Viewing Licens</u> a is not being used by the	be EULA for evalu- the EULA for evalu- this from a licens ment_string by entering this und: 	nt (EULA), read and uation, extension, a se by entering this o command: see the status of the pw the instructions i	d accept the t nd rehost lice command: a license you n the <u>Choos</u>	terms of the anses. The B installed.	agreement. EULA is also re	quired for per	manent license	ss, but it is acco g an AP-Count	epted during lice	anse generat	ion.	icense that is used
p2 If you are prompted to a second comments to a lise comment { add dek p 4 Save a backup copy se save ut out is thp:// server_jp/p p 5 Rebot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller.	to accept the end-user lic e prompted to accept the license or delete commer etb) license_name comm of all installed licenses t ath / filename . rr by entering this comma ns in the <u>"Viewing Licens</u> a is not being used by the	be EULA for evalu- the EULA for evalu- nts from a licens ment_string by entering this und: sees" section to a e controller, folic	nt (EULA), read and uation, extension, a se by entering this o command: see the status of the sw the instructions i	d accept the t nd rehost lice command: a license you n the <u>"Choos</u>	installed.	agreement. EULA is also re	quired for per	manent license	as, but it is acco g an AP-Count	epted during lice	anse general	ion.	cense that is used
p 2 If you are prompted to Note Typically, you an p 3 Add comments to a l se comment { add ded or if is they if server_ip / p or if is they if server_ip / p p 5 Rebot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller.	to accept the end-user lic e prompted to accept the license or delete commer ete) //cense_name commo of all installed licenses to ath / filename . rr by entering this comma ns in the <u>Viewing Licens</u> a is not being used by the	b EULA for evalu- nts from a licens ment_string by entering this and: accontroller, follo- controller, follo-	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the sw the instructions i	d accept the I nd rehost lice command:	installed.	agreement. EULA is also rei	quired for per	manent license	as, but it is acco g an AP-Count	opted during lice	anse general	ion.	icense that is used
p 2 If you are prompted in Note Typically, you an p 3 Add comments to all second the second second second second p 4 Save a backup copy is save ut ut is thp:// server_ip/ p p 5 Reboot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller.	to accept the end-user lic e prompted to accept the license or delete commer etb) license_name comm of all installed licenses to ath / filename . rr by entering this comma ns in the <u>"Viewing Licens</u> a is not being used by the view the licenses on the or SS	b EULA for evalu- nts from a licens ment_string by entering this end: ease" section to a e controller, follo	nt (EULA), read and uation, extension, a se by entering this o command: see the status of the sw the instructions i	d accept the I nd rehost lice command: a license you n the <u>Choos</u>	installed.	agreement. EULA is also rei	quired for per	manent license	ss, but it is acco g an AP-Count	epted during lice	anse general	ion.	icense that is used
p 2 If you are prompted to Note Typically, you an p 3. Add comments to a 1 ecomment { add ded add add comments to a 1 ecomment { add ded add is the comment { add ded add is they? ad	to accept the end-user lic e prompted to accept the license or delete commer ete) license_name com r of all installed licenses to ath / filename . In by entering this comma ns in the <u>"Viewing Licens</u> is is not being used by the view the licenses on the (see	a EULA for evalu- s EULA for evalu- tis from a license ment_string oy entering this oy entering this and: evas" section to s a controller, folic controller, iUI, foliow these	nt (EULA), read and uation, extension, a se by entering this o command: see the status of the pow the instructions i	d accept the I nd rehost lice command: a license you n the <u>"Choos</u>	installed.	agreement. EULA is also rei	quired for per	manent license	as, but it is acco	epted during lice	anse general	ion.	icense that is used
p 2 If you are prompted to Note Typically, you an p 3. Add comments to a l ecomment { add ded ded add add comments to a l decomment { add ded add add is server_/p/ p 5 Rebot the controlle yota more that the desired license by the controller. J Licenses ection describes how to vi he GUI to View Licens hu licenses on the control 1 Choose Management	to accept the end-user lic e prompted to accept the license or delete commer- ete) license_name com r of all installed licenses to ath / filename. In the <u>"Viewing Licens</u> is in the <u>"Viewing Licens</u> is in the <u>licenses</u> on the (ses ler using the controller G mit > Software Activation	EULA for evalu- EULA for evalu- EULA for evalu- this from a license ment_string oy entering this oy entering this a controller, folic controller, folic controller, iul, foliow these on > Licenses	nt (EULA), read and uation, extension, a se by entering this o command: see the status of the ow the instructions i e steps: to open the Licens:	d accept the t nd rehost lice command: e license you n the <u>"Choos</u>	installed.	agreement. EULA is also rer nsed Feature S	quired for per	manent license	es, but it is acco g an AP-Count	epted during lice	nse" section	ion.	icense that is user
p 2 If you are prompted in Note Typically, you an p 3 Add comments to a l is comment (add) dek p 4 Save a backup copy is save uf url is thp:// server_ip / p 5 F Rebot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller. g Licenses ection describes how to to the GUI to View License w licenses on the control p 1 Choose Manageme 4-4 Licenses Page	to accept the end-user lic e prompted to accept the license or delete commer- ete) license_name com r of all installed licenses to ath / filename . In the <u>Viewing License</u> is in the <u>Viewing License</u> is in the <u>Viewing License</u> is not being used by the set of the licenses on the of sets lier using the controller G ont > Software Activation	EULA for evaluation EULA for evaluation EULA for evaluation strom a license mont_string by entering this or evaluation or evaluation e controller, follo controller,	nt (EULA), read and uation, extension, a se by entering this o command: see the status of the work the instructions i e steps: to open the Licensi	d accept the t nd rehost lice command: e license you n the <u>Choos</u> es page (see	installed.	agreement. EULA is also rer nsed Feature S	quired for per	manent license	as, but it is acco g an AP-Count	epted during lice	nse" section	ion.	icense that is user
p 2 If you are prompted in Note Typically, you an p 3 Add comments to a I se comment (add) dek p 4 Save a backup copy is save urd urd is thrp://server_jp/p p 5 Rebot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller. g Licenses ection describes how to to the GUI to View License w licenses on the control o 1 Choose Management 14 Licenses Page	to accept the end-user lic e prompted to accept the license or delete commer ete) license_name com r of all installed licenses t ath / filename . r by entering this comma ns in the <u>Viewing Licens</u> e is not being used by the view the licenses on the o ses lice using the controller G ont > Software Activatio	LULA for evalu- setULA for evalu- this from a license mont_string by entering this by entering this acontroller, folic controller, controller, Licenses	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the ow the instructions i by steps: to open the Licensi	d accept the t nd rehost lice command: a license you n the <u>"Choos</u> as page (see	installed.	agreement. EULA is also rer nsed Feature S	quired for per	manent license	as, but it is acco	epted during lice	nse general	ion.	icense that is used
p 2 if you are prompted i Note Typically, you an p 3 Add comments to a l is comment (add) deklep 4 Save a backup copy is save url url is thp// server_/p/ p p 5 Rebot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller. g Licenses action describes how to volute GUL to View Licenses w licenses on the control p 1 Choose Management 4-4 Licenses Page	to accept the end-user lic e prompted to accept the license or delete commer ete) license, name com r of all installed licenses t ath / filename . r by entering this comma ns in the <u>Viewing License</u> is in the <u>Viewing License</u> is not being used by the view the licenses on the o ses liter using the controller G ent > Software Activation	ense agreemer EULA for evalu- Its from a licener ment_string by entering this area" section to a a controller, folic controller. UI, follow these on > Licenses	nt (EULA), read and uation, extension, a se by entering this o command: see the status of th bow the instructions i bow the instructions i be steps: to open the Licensi	d accept the t nd rehost lice xommand: a license you n the <u>"Choos</u> as page (see	erms of the E anses. The E Installed.	agreement. EULA is also rer nsed Feature S	quired for per	manent license the <u>*Activation</u>	as, but it is according an AP-Count	epted during lice	nse general	ion.	icense that is used
p 2 if you are prompted i Note Typically, you an p 3 Add comments to a l p 3 Add comments to a l p 4 Save a backup copy se save url url is thp// server_/p/p p 5 Reboot the controlle system p 6 Follow the instruction p 7 If the desired licenses by the controller. g Licenses ection describes how to us the GUI to View License w licenses on the control p 1 Chocse Management 4.4 Licenses Page	to accept the end-user lic e prompted to accept the license or delete commer ete) license_name com r of all installed licenses to ath / filename . r by entering this comma ns in the <u>"Viewing License</u> a is not being used by the view the licenses on the or ses lier using the controller G ent > Software Activation	DELLA for evaluation EULA for evaluation EULA for evaluation strom a license ment.string by entering this by entering this ses" section to a controller, folic	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the ow the instructions i o steps: to open the License to open the License	d accept the t nd rehost lice command: a license you n the <u>Choos</u> as page (see	erms of the E anses. The E installed.	agreement. EULA is also rer need Feature S	quired for per	the <u>"Activation</u>	as, but it is acco	epted during lice	nse" section	to change the I	icense that is used
p 2 if you are prompted i Note Typically, you an p 3 Add comments to all p 3 Add comments to all p 4 Save a backup copy is save unit units thp// server_/p/ p p 5 Reboot the controller system p 6 Follow the instruction p 7 If the desired licenses by the controller. g Licenses action describes how to vo the GUI to View Licenses w licenses on the control p 1 Choose Management 4-4 Licenses Page box agement	to accept the end-user lic e prompted to accept the license or delete commer ete) license, name com r of all installed licenses to ath / filename . r by entering this comma ns in the <u>"Viewing License</u> is not being used by the view the licenses on the or ses lier using the controller G that > Software Activation mis > Software Activation mises	EULA for evalu- EULA for evalu- this from a licene- ment_string by entering this by entering this by entering this eses" section to se controller, folic	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the ow the instructions i e steps: to open the License security MAMA	d accept the t nd rehost lice command: e license you n the <u>Choos</u> as page (see	erms of the E anses. The E installed. Figure 4-4).	agreement. EULA is also rer need Feature S	quired for per	the <u>"Activation</u>	as, but it is acco g an AP-Count	epted during lice	anse generat	to change the I	icense that is used
p 2 If you are prompted i Note Typically, you an p 3 Add comments to al p 3 Add comments to al id add comment id add comments id add comments id add comment id add comments id add comment id add comments id add comment id add comments id add c	to accept the end-user lic e prompted to accept the license or delete commer ete) license, name com r of all installed licenses to adh / filename . r by entering this comma ns in the <u>"Viewing License</u> is is not being used by the view the licenses on the or sets lier using the controller G int > Software Activation toop <u>AUANa</u> <u>CONTROL</u> insee	EULA for evaluation EULA for evaluation EULA for evaluation Form a licener ment.string by entering this work and the second of	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the w the instructions i e steps: to open the License SECLETTY MANA	d accept the I nd rehost lice command: = license you n the <u>Choos</u> as page (see	Installed.	agreement. EULA is also rei need Feature S	quired for per	the <u>"Activation</u>	as, but it is acco g an AP-Count	Evaluation Lice	nse general	ion.	icense that is used
p 2 If you are prompted i Note Typically, you an p 3 Add comments to al is comment { add loak p 4 Save a backup copy e save uf ur is thp:// sarver_/p/ p 5 Reboot the controlle yota backup copy e save uf ur is thp:// sarver_/p/ p 5 Reboot the controlle yota backup copy e save uf ur is thp:// sarver_/p/ p 5 Reboot the controlle yota backup copy e save uf ur is thp:// sarver_/p/ p 5 Reboot the controlle yota controller. g Licenses ection describes how to v the GUI to View License w licenses on the control p 1 Choose Manageme 4-Licenses Page Cisco	to accept the end-user lic e prompted to accept the license or delete commer de b / icense, name com r of all installed licenses t adh / filename . r by entering this comma ms in the <u>"Viewing Licens</u> is is not being used by the view the licenses on the of ses life using the controller G int > Software Activation trops	Controller, folic Controller,	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the work the instructions i e steps: to open the License security MANA Time(expires) D works, 4 days	d accept the t nd rehost lice xommand: a license you n the <u>Choos</u> as page (see <u>SEMENT</u> <u>COM</u>	erms of the e anses. The E installed. Figure 4-4).	agreement. EULA is also rer need Feature S	quired for per	manent license the <u>"Activation</u> • Configuration	g an AP-Count	epted during lice	nse" section	ion.	icense that is usee
p 2 If you are prompted in Note Typically, you an p 3 Add comments to a l tere comment { add dels p 4 Save a backup copy e save u/ url is thp:// server_/p/ p 25 Rebot the controlle yotem 56 Follow the instruction 7 If the desired license by the controller. desired licenses ection describes how to o he GUI to View License w licenses on the control 1 Choose Manageme t-4 Licenses Page if the desired license isenset to the GUI to View License w licenses on the control 1 Choose Manageme t-4 Licenses Page if the desired license isenset to the GUI to View License w licenset to the GUI to View License to the	to accept the end-user lic e prompted to accept the license or delete commer- ete) license_name com of all installed licenses to ath / filename . In by entering this comma ns in the <u>"Viewing Licens</u> is not being used by the view the licenses on the or set license to be a set of the licenses of the set of the using the controller G fint > Software Activation mission wreat License Levist 233 mission wreat License Levist 233	cense agreemen s EULA for evalu- tis from a license ment_string oy entering this ind: eases accilon to a a controller, folic controller, tU, foliow theses on > Licenses s Types seathform pyrmmark	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the w the instructions i b steps: to open the License SECURITY MANA TIME(espines)	d accept the t Ind rehost lice command: a license you a licens	Errors of the anses. The E installed. Eligure 4-4). Promotive Page.m	agreement. EULA is also rer need Feature S need Feature S ELE EEEMACK	quired for per iet" section o	the <u>"Activation</u>	ss, but it is acco	Evaluation Lice	anse general	to change the I	icense that is user
p 2 If you are prompted i Note Typically, you an p 3 Add comments to al 1 e comment (add) dek p 4 Save a backup copy e save uf url is thp:// server_ip / p s f Rebot the controlle ystem 3 E Follow the instruction 5 Follow the instruction f I the desired license by the controller. g Licenses ection describes how to v he GUI to View License wicenses on the control 1 Choose Manageme t-4 Licenses Page	to accept the end-user lic e prompted to accept the license or delete commer- tete) license, name com r of all installed licenses to ath / filename . In by entering this comma ns in the <u>"Viewing Licens</u> is is not being used by the view the licenses on the of ses lier using the controller G lier using the controller G lint > Software Activation troop <u>Wurke</u> <u>CONTROL</u>	Controller. Cont	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the ow the instructions i e steps: to open the License SECURITY MANA Time(expires) Time(expires)	d accept the t nd rehost lice command: a license you a license	Error of the B anses. The B installed. Eigurn 4-(4). Eigurn 4-(4). Eigurn 4-(4). Eigurn 4-(4). Eigurn 4-(4).	agreement. EULA is also rev need Feature S EULE EEDRACK	quired for per	the "Activation	ss, but it is acco	epted during lice	anse general	to change the I	icense that is used
p 2 if you are prompted i Note Typically, you an p 3 Add comments to a l is comment (add) dek p 4 Save a backup copy is save und unt is titp:// server_ip / p p 5 Rebot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller. g Licenses ection describes how to to the GUI to View License w licenses on the control p 1 Choose Management 4-4 Licenses Page Different	to accept the end-user lic e prompted to accept the license or delete commer- ete) license, name com r of all installed licenses to ath / filename . In by entering this comma ns in the <u>"Viewing Licens</u> is is not being used by the view the licenses on the of ses lier using the controller G int > Software Activation troop <u>AUAMa</u> <u>CONTROL</u> interest License Level: 2st mass area License Level: 2st mass area License Level: 2st mass	Controller. Cont	nt (EULA), read and uation, extension, a se by entering this o command: see the status of the ow the instructions i esteps: to open the License sectory MANA Timefeeshees) D statist B sta	d accept the t nd rehost lice command: a license you a license	Error of the Error	agreement. EULA is also real second Feature S need Feature S Execution Interface Interface Interface Interface Interface Interface	quired for per	the "Activation	n, but it is acco g an AP-Count	epted during lice	nse general	to change the l	Icense that is user
p 2 if you are prompted i Note Typically, you an p 3 Add comments to a l se comment { add] dek p 4 Save a backup copy is save und unt is thp:// server./p / p p 5 Rebot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller. g Licenses action describes how to vi- the GUI to View License w licenses on the control p 1 Choose Management CISCO EXX CISCO EXX action the control on the control p 1 Choose Management CISCO EXX CISCO EXX action the control on the control p 1 Choose Management CISCO EXX cisco EXX action the control on the control p 1 Choose Management cisco Exx cisco ExX action the control on the control p 1 Choose Management cisco Exx action the control on the control p 1 Choose Management cisco Exx action the control on the control p 1 Choose Management cisco Exx action the control on the control p 1 Choose Management cisco Exx action the control on the control p 1 Choose Management cisco Exx action the control on the control p 1 Choose Management cisco Exx action the control on the control action the control on the control on the control action the control on the control on the control action the control on the control on the control on the control action the control on the con	to accept the end-user lic e prompted to accept the license or delete commer- ete) license, name com r of all installed licenses to ath / filename . In by entering this comma is in the <u>"Viewing License</u> is not being used by the view the licenses on the of ses lise using the controller G ent > Software Activation troop. <u>AUAMa</u> <u>CONTROL</u> entered License Level: 200 miles and 200 entered License Level: 200 en	Controller. Cont	nt (EULA), read and uation, extension, a se by entering this o command: see the status of thi with e instructions i besteps: to open the License SECLETIV MANA Time(expires) D writes, 4 days B carefus, 4 days B carefus, 4 days B carefus, 4 days	d accept the t nd rehost lice command: a license you a license	Error of the Error of the Error of the Error of the Error Er	agreement. EULA is also real model Feature S Superior Status Superior Status	quired for per	the "Activation	n AP-Count	Evaluation Lice	nse general	to change the l	icense that is user
p 2 if you are prompted i Note Typically, you an p 3 Add comments to al p 3 Add comments to al p 3 Add comments to al p 4 Save a backup copy se save url url is thp// server_/p/ p p 5 Rebot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller. g Licenses action describes how to vol- the GUI to View License the GUI to View License w licenses on the control p 1 Choose Management 4.4 Licenses Page Cisco environment and the system action describes in a control p 1 Choose Management cisto environment and the system and the s	to accept the end-user lic e prompted to accept the license or delete commer- tete) license, name com r of all installed licenses to ath / filename . r by entering this comma ins in the <u>Viewing License</u> is is not being used by the view the licenses on the or ses licenses the <u>Viewing License</u> is not being used by the view the licenses on the or ses licenses <u>viewing Common</u> ses	Controller, follo Controller,	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the bow the instructions i bow the instruction i bow the instructions	d accept the t nd rehost lice xommand: a license you n the <u>"Choose</u> as page (see <u>servent</u> <u>ccv</u> <u>ccvnt</u> 4:2 3:3 3:4 3:3 3:4 3:3 3:4 3:3 3:4 3:5 3:5 3:5 3:5 3:5 3:5 3:5 3:5	Figure 4-4)	agreement. EULA is also real med Feature S need Feature S ELE EEEBACK	quired for per	the <u>*Activation</u>	as, but it is acco	epted during lice	nse" section	to change the I	cense that is use
p 2 if you are prompted i Note Typically, you an p 3 Add comments to all p 3 Add comments to all p 4 Save a backup copy ise save url url is thp// server_jp / p p 5 Robot the controller system p 6 Follow the instruction p 7 He desired licenses by the controller. g Licenses section describes how to vol- the GUI to View Licenses w licenses on the controller 1 Chocse Management 4.4 Licenses Page Cisco etcol agement Licenses agement Licenses	to accept the end-user lic e prompted to accept the license or delete commer ete) license, name com r of all installed licenses t ath / filename . r by entering this comma is in the <u>Viewing License</u> is in the <u>Viewing License</u> is in the <u>Viewing License</u> is in the <u>Viewing License</u> is the <u>view the licenses on the or</u> sets liter using the controller G ont > Software Activation IntoR. <u>ACAMA</u> <u>CONTROL</u> IntoR. <u>ACAMA</u> <u>CONTROL</u> Intercent License Level: <u>Data</u> as a network is a set of the controller G on the controller G on the <u>Controller</u> <u>Control</u> IntoR. <u>ACAMA</u> <u>CONTROL</u> Intercent License Level: <u>Data</u> <u>a set of the controller</u> <u>Control</u> Intercent <u>Controller</u> <u>Control</u>	Controller, follo Controller,	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the bow the instructions i bow the instructions i both the instructions i command: command: see the status of the bow the instructions i command:	d accept the t nd rehost lice command: a license you n the <u>Choose</u> as page (see <u>count</u> 40 30 30 40 30 30 40 30 30 40 30 40 40 40 40 40 40 40 40 40 4	Figure 4-4)	agreement. EULA is also rer need Feature S	quired for per	the <u>Activation</u>	ss, but it is acco	epted during lice	nse" section	to change the I	icense that is used
p 2 if you are prompted i Note Typically, you an p 3 Add comments to a l p 3 Add comments to a l p 4 Save a backup copy se save url url is thp// server_jp / p p 5 Robot the controller system p 6 Follow the instruction p 7 If the desired licenses by the controller. g Licenses action describes how to vo the GUI to View Licenses w licenses on the control p 1 Chocse Management 4.4 Licenses Page Cisco extra call temperature and temperature and temperature and temperature and temperature and temperature the GUI to View Licenses w licenses on the control p 1 Chocse Management 4.4 Licenses Page Cisco extra and temperature and temperature	to accept the end-user lic e prompted to accept the license or delete commer ete) license, name com r of all installed licenses to ath / filename . r by entering this comma e is not being used by the view the licenses on the or ses liter using the controller G ent > Software Activation in Software Activation in Software Activation in Software Level 23 mess licenses to the or ses in Activity 24 activation in Software Level 23 activation in Software Software Controller in Software Activation in Software Level 23 activation in Software Software Software in Software in Software Software in Software Software in Software Software in Software in Software Software in Sof	Controller, follow these Controller, follow Contro	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the w the instructions i esteps: to open the License SECURITY MANA TIME(SEQUESTY MANA Sequence) 5 Security MANA	d accept the t nd rehost lice xommand: a license you n the <u>Choose</u> as page (see <u>sekent</u> <u>coo</u> <u>count</u> 40 33 34 250	erms of the E anses. The E installed. Figure 4-4). Events too Figure 4-4). Events Figure 4-4). Events Figu	agreement. EULA is also rei need Feature S EUL EEEMACK	quired for per	the "Activation	as, but it is acco	Evaluation Lice	nse" section	to change the I	icense that is user
p 2 if you are prompted i Note Typically, you an p 3 Add comments to al p 3 Add comments to al p 4 Save a backup copy to save unit units thp// server_/p/ /p p 5 Roboot the controller system p 6 Follow the instruction p 7 If the desired license by the controller. g Licenses action describes how to us the GUI to View License w licenses on the control p 1 Choose Management 4.4 Licenses Page Ciscon Cisco	to accept the end-user lic e prompted to accept the license or delete commer ete) license, name com r of all installed licenses to ath / filename . r by entering this comma ons in the <u>"Viewing License</u> is not being used by the view the licenses on the or ses licenses on the licenses on the or ses licenses on the licenses on the or ses licenses on the licenses on the or ses licenses of the licenses of the licenses is a second of the licenses of the licenses is a second of the licenses of the licenses is a second of the licenses of the licenses of the licenses of the licenses of the licenses of the licenses of the licenses of the licenses of the licenses of the licenses of the licenses of the licenses of the licenses of the licenses of the licenses of the lice	Centroller, follow Controller,	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the w the instructions i set the status of the w the instructions i set the status of the w the instructions i set the status of the set the set the status of the set the	d accept the t nd rehost lice xommand: a license you n the <u>Choose</u> as page (see <u>SEMENT</u> <u>CO</u> <u>Count</u> 40 23 35, 36, 36, 36, 36, 36, 36, 36, 36	Error of the E anses. The E installed. Erguns 4-4).	agreement. EULA is also real meed Feature S feature fe	quired for per	the <u>"Activation</u>	as, but it is acco g an AP-Count	Evaluation Lice	nse" section	to change the I	icense that is used
p 2 If you are prompted i Note Typically, you an p 3 Add comments to al p 3 Add comments to al p 4 Save a backup copy as save <i>url</i> <i>url</i> is thp// server_/p//p p 5 Reboot the controller system p 6 Follow the instruction p 7 If the desired license by the controller. g Licenses action describes how to v the GUI to View License w licenses on the control p 1 Choose Management 4-4 Licenses Page Ciscon the control p 1 Choose Management Add Heinegrent and Hein	to accept the end-user lic e prompted to accept the license or delete commer- ete) license_name com of all installed licenses to ath / filename . In by entering this comma ris in the <u>"Viewing Licens</u> is not being used by the view the licenses on the or sets life using the controller G ent > Software Activation to be <u>sets</u> troop <u>Access Level</u> ; but made <u>licenses</u> Level; but made <u>licenses</u> Level; but and <u>licenses</u> is an example.	Controller. Cont	nt (EULA), read and uation, extension, a se by entering this o command: see the status of the with enstructions i esteps: to open the License security MAAA <u>Time(cespres)</u> b steps: b andes, 4 days b scelar, 4 days b scelar, 4 days	d accept the I nd rehost lice command: a license you n the <u>Choose</u> as page (see <u>SEMENT</u> <u>CO</u> <u>Count</u> 40 33 34 34 34 34	Figure 4-d).	agreement. EULA is also real meed Feature S seators factors factors in Jac in Jac	quired for per	the <u>Activation</u>	s, but it is acco	Evaluation Lice	nse" section	to change the I	icense that is used
p 2 If you are prompted i Note Typically, you an p 3 Add comments to al se comment (add dek p 4 Save a backup copy as save url url is thp://server_/p/p p 5 Reboot the controlle system p 6 Follow the instruction p 7 If the desired license by the controller. g Licenses action describes how to v the GUI to View License w licenses on the control p 1 Choose Management 4-4 Licenses Page Cisco to the Control p 1 Choose Management def Sessions activities	to accept the end-user lic e prompted to accept the license or delete commer- ete) license_name com of all installed licenses to ath / filename . If by entering this comma is in the <u>Viewing Licens</u> is not being used by the view the licenses on the or sets license to be a set of the licenses of the sets license to be a set of the licenses of the sets license to be a set of the license sets license to be a set of the license sets (the license to be a set of the license to be	cense agreemen s EULA for evalu- tis from a licens ment_string oy entering this ind: centroller. idl, follow these on > Licenses idl, follow these on > Licenses idl, follow these on > Licenses idl, follow these idl, follow thes	nt (EULA), read and uation, extension, a se by entering this o command: see the status of the with enstructions i by steps: to open the License SECURITY MARK TIME(expires) Time(expires) Security Marka Security Marka Security Marka Security Marka Security Marka Security Marka Security Marka Security Marka Security Security Security Marka Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Securi	a accept the t Ind rehost lice command: a license you a licens	Error of the anses. The E installed.	agreement. EULA is also real model Feature S EULA is also real model Feature S EULA is also real model Feature S EULA is also real Feature S E	quired for per	the <u>Activation</u>	s, but it is acco	Evaluation Lice	nse" section	to change the I	icense that is used
p 2 if you are prompted i Note Typically, you an p 3 Add comments to all se comment (add) dek p 4 Save a backup copy se save und our lis titp:// server_ip / p p 5 Rebot the controlle system p 6 Follow the instruction p 7 If the desire licenses by the controller. g Licenses action describes how to to the GUI to View License by the controller. g Licenses on the control p 1 Choose Manageme 4 Licenses Page	to accept the end-user lic e prompted to accept the license or delete commer- ete) license, name com or all installed licenses to ath / filename . In by entering this comma is in the <u>Wawing Licens</u> is is not being used by the view the licenses on the or ses life using the controller G fint > Software Activation into a software Activation into a software is a software is a software is a software is a software in the software in the software is a software in the software in the software is a software in the software in the software in the software is a software in the s	Cense agreemen EULA for evalu EULA for evalu tis from a licens ment_string oy entering this und: centroller, centroller, folic Centroller, f	nt (EULA), read and uation, extension, a se by entering this of command: esteps: to open the License <u>SECURITY</u> MANA <u>Time(esspires)</u> <u>15 aretas, 4 dopen 5 aretas, 4 dopen 5 aretas, 4 dopen 5 aretas, 4 dopen</u>	d accept the t nd rehost lice command: a license you as page (see SEMENT CON COUNT 40 33 34 33 34 33 34 33 34 33 34 33 34 33 34 33 34 33 34 33 34 33 34 33 34 33 34 35 35 35 35 35 35 35 35 35 35	Error of the E installed. Eigurn 4-(-). Eigurn 4-(-). Errorty Errorty Errorty Errorty Errorty Errorty Errorty Errorty Errorty Errorty Errorty Errorty	agreement. EULA is also re- need Feature S Factors Factors Transmission Transmissio	quired for per iet" section o	the "Activation	ss, but it is acco g an AP-Count Seg Jesuse 1	Evaluation Lice	nse" section	to change the l	icense that is used
p 2 if you are prompted i Note Typically, you an p 3 Add comments to a 1 se comment (add) dek p 4 Save a backup copy se save u/ p 6 Follow the instruction p 7 If the desired license by the controller g Licenses action describes how to to the GUI to View License w licenses on the control p 1 Choose Management d Licenses Page d Licenses Page d Licenses Page d Licenses and the license age lists all of the license w, or EULA not accepted	to accept the end-user lic e prompted to accept the license or delete commer ete) license, name com r of all installed licenses to ath / filename . In by entering this comma is in the <u>"Viewing Licens</u> is is not being used by the view the licenses on the of ses life using the controller G int > Software Activation into a software activation i	Cense agreement EULA for evalu tis from a licens ment_string by entering this ind: controller, controller, follo controller, follo controller, follo controller, follo controller controll	nt (EULA), read and uation, extension, a se by entering this of command: see the status of the ow the instructions i esteps: to open the License sectory Mask Time(espines) B steps: to spen the License sectory Mask Time(espines) B steps: b steps: to spen the License sectory Mask Sectory Mask	d accept the I and rehost lice command: a license you as page (see count 42 42 42 43 43 44 43 43 43 43 43 43 43 43 43 43	Error of the Error of the Error of the Error of the Error Er	agreement. EULA is also real second Feature S second Feat	quired for per	the "Activation	as, but it is acco g an AP-Count See second 1	Evaluation Lice	nse general	to change the I	Icense that is user

4 of 45

	red license to view more deta	ails for a particular license. The Licer	nse Detail page appears (see E	igure 4-5).
gure 4-5 License Detail Page				
allulu			Soye Corig	uration Eog Logout Brânsk
CISCO MOR	UTCH WLANS CONF	TROULER, KURELESS SECU	кту манассмент сі	OMMANDS CLP FEED6400
Management	License Detail			< Hack Apply
Summary	Name	wplus		
► SNMP	Туре	Pern ane it		
IEINST-SSH	Vers on	± 0		
Serial Port	Convent			
Local Management Users				
Har Sessions	Status	Kot in Use		
▶ Logs	Expires Built-1 : Luce ise	Ku Ekury		
Mgmt Via Wireless	Max to the Court	Kot Cointed		
Line is es	Counts Used	Not Counted		
Commanos Liceore Scent	F fiority	Medium		
Tech Support				23.0C
This page shows the following addi	tional information for the licer	nse:		5
The license type (permanent, e	evaluation, or extension)			
The license version				
 The status of the license (in us The length of time before the li 	 e, not in use, inactive, or EU icense expires 	LA not accepted)		
٠.				
Note Permanent licenses ner	ver expire			
• Whether the first of the				
 vvnetner the license is a built-in The maximum number of access 	a license ss points allowed for this licen	nse		
The number of access points of	urrently using this license			
Step 3 If you want to enter a cor	nment for this license, type it	in the Comment text box and click A	pply.	
Step 4 Click Save Configuration	on to save your changes .			
sing the CLI to View Licenses				
To view licenses on the controller, u	use these commands:			
See the license level, license ty	ype, and number of access p	oints licensed on the controller by er	tering this command:	
show sysinfo				
Manufacturer's Name	ing appears.	Cisco Systems Inc.		
Product Name		Cisco Controller		
RTOS Version		7.0		
Bootloader Version Emergency Image Version	n	5.2 N/A		
Build Type		DATA + WPS		
System Location		na		
System Contact System ObjectID		abc@cisco.com 1.3.6.1.4.1.14179.1	.1.4.3	
IP Address		10.10.10.10 3 days 1 brs 12 min	a 42 apra	
System Timezone Locati	on		5 12 5005	
CurrentBoot License Le CurrentBoot License Ty	vel pe	base Permanent		
NextBoot License Level		base		
NextBoot License Type. Operating Environment.		Commercial (0 to 40	C)	
Internal Temp Alarm Lin Internal Temperature	nits	0 to 65 C +40 C		
State of 802.11b Netwo	rk	Enabled		
Number of WLANS		4		
Number of Active Clien Burned-in MAC Address	ts	0 00:1A:6D:DD:1E:40		
Crypto Accelerator 1		Absent		
crypto Accelerator 2 Power Supply 1		Absent		
Power Supply 2	supported	Present, OK		
CARACUMAN HUMBER OF APS :				
See a brief summary of all activ	ve licenses installed on the c	ontroller by entering this command:		
show license summary				
Information similar to the follow	ing appears:			
Period left: 0 minute	0 second			
Index 2 Feature: base- Period left: 0 minute	ap-count 0 second			
Index3 Feature: base				
License Type: Permanen	t			
License State: Active, License Count: Non-Cour	In Use nted			
License Priority: Medi	um			
index 4 Feature: base- Period left: 6 weeks,	ap-count 4 days			
License Type: Evaluati	on In Use			
License State: Active	/0			
License State: Active, License Count: 250/250				
License State: Active, License Count: 250/250 License Priority: High		g this command:		
License State: Active, License Count: 250/250 License Priority: High • See all of the licenses installed	d on the controller by entering			
License State: Active, License Count: 250/250 License Priority: High See all of the licenses installed show license all Information similar to the follow	d on the controller by entering ing appears:			
License State: Active, License Count: 250/250 License Priority: High • See all of the licenses installed show license all Information similar to the follow License Store: Primary	d on the controller by entering ing appears: License Storage			
License State: Active, License Count: 250/250 License Priority: High See all of the licenses installed show license all Information similar to the follow License Store: Primary StoreIndex: 1 Feature: License Type: Permanen	ing appears: License Storage base Version: 1.0			
License State: Active, License Count: 250/250 License Priority: High • See all of the licenses installed show license all Information similar to the follow License Store: Primary StoreIndex: 1 Peature: License State: Active, License State: Active, License State: Active,	d on the controller by entering ing appears: License Storage base Version: 1.0 t Not in Use			

License State: Active, In Use Evaluation total period: 8 weeks 4 days Evaluation period left: 8 weeks 3 days License Count: 250/0/0 License Priority: High

 See the details for a particular license by entering this command: show license detail license_name Information similar to the following appears Index: 1 Feature: base-ap-count Version: 1.0 License Type: Permanent License State: Active, Not in Use License Count: 12/0/0 License Priority: Medium Store Index: 0 Store Name: Primary License Storage

Index: 2 Feature: base-ap-count Version: 1.0 License Type: Evaluation License State: Inactive Evaluation total period: 8 weeks 4 days Evaluation period left: 8 weeks 4 days License Count: 250/0/0 License Priority: Low Store Index: 3 Store Name: Evaluation License Storage

· See all expiring, evaluation, permanent, or in-use licenses by entering this command: show license {expiring | evaluation | permanent | in-use} Information similar to the following appears for the show license in-use command: StoreIndex: 2 Feature: base-ap-count Version: 1.0

Storeindex: 2 reature: base-ap-count vers License Type: Permanent License State: Active, In Use License Count: 12/12/0 License Priority: Medium StoreIndex: 3 Peature: base Version: 1.0 License Type: Permanent License Type: Permanent License State: Active, IN Use License Count: Non-Counted License Priority: Medium

Note Ontroller platforms do not support the status of 'grace period' or 'extension' as a license type. The license status will always show 'evaluation' even if a grace period or an extension evaluation license is installed.

See the maximum number of access points allowed for this license on the controller, the number of access points currently joined to the controller, and the number of access points that can still join the controller by entering this command:

show license capacity Information similar to the following appears:

Licensed Feature Max Count Current Count Remaining Count AP Count 250 4 246

· See statistics for all licenses on the controller by entering this command:

show license statistics Information similar to the following appears: Administrative statistics Install success count: 2

Install failure count: 0 Install duplicate count: 0 Comment add count: 0 Comment delete count: 0 Clear count: 0 Save count: 2 Save cred count: 0 Client status Request success count 2 Request failure count 0 Release count 0 Global Notify count 6

· See a summary of license-enabled features by entering this command:

show license feature

Information similar to the following appears: Feature name Enforcement Evaluation Clear Allowed Enabled base yes yes yes yes a ves base-ap-count yes yes yes no

Choosing the Licensed Feature Set

You can configure the controller to specify which feature set it uses. The currently active license determines the feature set and number of access points supported on the controller

Using the GUI to Choose the Licensed Feature Set

To specify the feature set for the controller using the controller GUI, follow these steps:

Step 1 Choose Management > Software Activation > License Level to open the License Level page (see Figure 4-6).

Figure 4-6 License Level Page

CISCO Management	MONITOR MILAN	CONTROLLER WIRE	NESS SECURITY M	ANAGEMENT COMMANDS	HE_F EFFORACK	
Management	License Level			22		
Summary I SIMP]
HTTP-HTTP5	Gurrent Hoense Les	iel: <u>http</u>				
Teinet SSII Serial Port	License Capacity Counted Feature	Max Count	Current Count	Remaining Count		
Local Management Users =	AP Count	262	3	252		
User Sessions						
Mgmt Via Wireless						
Software Activation Licenses Licenses Licenses Licenses Licenses Licenses Licenses Licenses						
Tech Support						\$20

Step 2 Click the base license level link to open the Licenses page (see Figure 4-7) to learn more about the available license levels

Figure 4-7 Licenses Page

ababa				Sage Configuration	Pru Logart 3e
anagement	Licenses	CONTROLITER WERELESS	Second advantage	KI . DUMANDA HEIN	E-HOPATE c Rank
Summary SNMP	linense	Турс	Time(explees)	Status	
HTTP-HTTPS	Lase	pern ane it	Vic Examp	în Jee	
Telnet-SSH	this	ora lation	8 weeks, 4 roys	"na viva	
Serial Port					
Local Management Users	Following load gross	are included in this loand			
Harr Steadings					
E Logs	LARWEAN ESD. 15				
Mynil Via Wireless					
 Software Activation Lice is a Lice is a Level Outrimance Lice is a Agent 					
) Tech Support					
	-	10			

This page shows the licenses applicable to this level and the list of features supported. Step 3 Click Back to return to the License Level page.

Step 4 If you want to change the license level, follow these steps:

a. Choose the license level to be used on the next reboot: base, or auto. If you choose auto, the licensing software automatically chooses the license level to use on the next reboot. It chooses permanent licenses over evaluation licenses.

9

- Note To prevent disruptions in operation, the controlline date not avoid h licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license. If no valid licenses are feature set level is installed, the controller can always operate in base level. In base level
- b. Click Activate
- c. Click OK when prompted to confirm your decision to change the license level on the next reboot.
- d. If you are prompted to accept the end-user license agreement (EULA), read and accept the terms of the agreement and then click Accept. The Next Boot Level text box now shows the license level that you specified as the level to be used after the next controller reboot.
- e. Reboot the controller so that the specified license level takes effect.

Using the CLI to Choose the Licensed Feature Set

To specify the feature set for the controller using the controller CLI, follow these steps:

show sysinfo	
Information similar to the following appears:	
Product Name	. Cisco Controller
Product Version	. 6.0.118.0
Current Boot License Level	. base
Current Boot License Type	Permanent
Next Boot License Level	. auto
Next Boot License Type	Permanent

Step 2 Specify the license level to be used on the next reboot by entering this command:

config license boot { base / auto }

If you choose auto, the licensing software automatically chooses the license level to use on the next reboot. It chooses permanent licenses over evaluation licenses. 0

Note To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

Step 3 If you are prompted to accept the end-user license agreement (EULA), read and accept the terms of the agreement. The EULA appears if no permanent licenses are installed at the specified boot level and the evaluation license has not yet been activated. In this case, the config license boot command changes the license level and activates the evaluation license following a reboot.

Step 4 See the license level to be used after the next controller reboot by entering this command:

show sysinfo

Step 5 Reboot the controller in order to have your changes take effect by entering this command:

reset system

Activating an AP-Count Evaluation License

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 50-access-point count and want to try an evaluation license with a 100-access-point count, you can try out the evaluation license for 60 days.

AP-count evaluation licenses are set to low priority by default so that the controller uses the ap-count permanent license. If you want to try an evaluation license with an increased access point count, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, which forces the controller to use the permanent license. 0

Note To prevent discuptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

You can activate ap-count evaluation licenses using the controller GUI or CLI

Using the GUI to Activate an AP-Count Evaluation License

To activate an ap-count evaluation license using the controller GUI, follow these steps:

Step 1 Choose Management > Software Activation > Licenses to open the Licenses page (see Figure 4-8).

Figure 4-8 Licenses Page

alada						THE PERSON OF	Sage Configuration	Sing	Logist Balwin
Management	Licenses	ciek wheres:	Secontri Manoro	CHENI COM	envenus ris	eða Eccoderok			
Summery E-SNND	Current License Level: 54	352							
HTTP	License	Type	Time(expires)	Count	Priority	Status			
Telnet-SSH	cane-an-enuet	maturian	D weeks, 4 days	40	Low	Inective	•		
Serial Port	is an an-spectrum	permanent	No Expiry	13	Fiedfam	Inactive	0		
Local Management	2622	permanent	No topiny	NA.	Nodi.m	an Use			
Users		evaluation	8 weeks, 4 sleve	NA.	Low	Inactive			
User Sessions	pape on equit	culustion	5 weeks, 4 days		High	an use			
Logs									
Mgmt Vin Wireless									
Software Activation Uponses Uponse Daval Commands Uponse Agent		Case	ax						
Tech Support									
							Contract Contract	48	· * 107% ·

Step 2 Activate an ap-count evaluation license as follows:

a. Click the link for the ap-count evaluation license that you want to activate. The License Detail page appears (see Figure 4-9).

Figure 4-9 License Detail Page

սիսիս cisco տ	NUTOR WLANS CON	rege Configuration Engl Logist Lefterb Terroller (Upeless decurrent Management Commands ele feedback
Management	License Detail	< liark Apply
Summary	Name	volus
IF SKMP	Туре	Perinane it
HTTP-HTTPS	Vers on	- 3
Teinet-55H		C49
Serial Port Local Management	Uchment	
Users Users	Status	Kot in Lee
h Lons	Екринэь	Ky Econy
Mont Vin Wireless	Built-1 r Lice ise	NJ
- Software Activation	Maximum Churn	Bat Scined
Lice is es	Ucunts Used	Rot cloanted
License Agent	F 'iority	Medium
Frech Support		
b. Choose High from the	he Priority drop-down list and	s click Set Priority .
0		
Note You can set the priorit	ty only for ap-count evaluation	n licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.
c. Click OK when prom	npted to confirm your decision	n about changing the priority of the license.
d. When the FLILA and	sears, read the terms of the se	arreement and then click Accept
When promoted to a	eboot the controller click OF	grannen and new men and a get t
e. when prompted to h	eboot the controller, click OK	
 Reboot the controller 	r in order for the priority chang	ge to take effect.
g. Click Licenses to o	pen the Licenses page and ve	verify that the ap-count evaluation license now has a high priority and is in use. You can use the evaluation license until it expires.
Step 3 If you decide to stop us	ing the ap-count evaluation lid	cense and want to revert to using an ap-count permanent license, follow these steps:
a. On the Licenses pag	ge, click the link for the ap-cou	unt evaluation license that is in use.
b. Choose Low from the	ne Priority drop-down list and	I click Set Priority .
0		
Nete You can get the priori	hu only for an aquat qualuation	n lanence. All except lanence shows have a medium nitriti: which encept he configured
Note Tou can set the phone	y only for ap-count evaluation	In censes. A "-count permanent incenses arrays have a medium phony, which cannot be conligued.
c. Click OK when prom	npted to confirm your decision	1 about changing the priority of the license.
d. When the EULA app	pears, read the terms of the ag	greement and then click Accept .
e. When prompted to r	eboot the controller, click OK	t.
f. Reboot the controller	r in order for the priority chang	ige to take effect.
g. Click Licenses to o	pen the Licenses page and ve	verify that the ap-count evaluation license now has a low priority and is not in use. Instead, the ap-count permanent license should be in use.
Ising the CLI to Activate an AP	-Count Evaluation Licens	SA .
To activate an ap-count evaluation	n license using the controller (CLI, follow these steps:
Step 1 See the current status	of all the licenses on your con	ntroller by entering this command:
show license all		
Information similar to the following	appears:	
License Store: Primar	y License Storage	int 1.0
License Type: Permane	nt	
License State: Active	, In Use	
License Count: 12/0/0 License Priority: Med	ium	
StoreIndex: 1 Feature	: base Version: 1.0	
License Type: Permane	nt	
License Count: Non-Co	unted	
License Priority: Med	ium	
StoreIndex: 2 Feature License Type: Evaluat	: base Version: 1.0	
License State: Inacti	ve	
Evaluation total peri	od: 8 weeks 4 days	
License Count: Non-Co	unted	
License Priority: Low		
StoreIndex: 3 Feature	: base-ap-count Versio	.on: 1.0
License State: Inacti	ve	
Evaluation total peri	od: 8 weeks 4 days	
Evaluation period lef	t: 8 weeks 4 days 0	
License Priority: Low	-	
The License State text box shows	the licenses that are in use, a	and the License Priority text box shows the current priority of each license.
Step 2 Activate an ap-count ev	aluation license as follows:	

0	
Note	You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.
b	To reboot the controller in order for the priority change to take effect, enter this command:
eset s	ystem
c	To verify that the ap-count evaluation license now has a high priority and is in use, enter this command:
show I	icense all
You car	n use the evaluation license until it expires.
ep3 lf	you decide to stop using the ap-count evaluation license and want to revert to using an ap-count permanent license, follow these steps:
а	To lower the priority of the ap-count evaluation license, enter this command:
icense	modify priority license_name low
b	To reboot the controller in order for the priority change to take effect, enter this command:
eset s	ystem
с	To verify that the ap-count evaluation license now has a low priority and is not in use, enter this command:
show lie	cense all
nstead	the ap-count permanent license should be in use.

sting a Li

Reveking a license from one controller and installing it on another is called rehosting. You might want to rehost a license in order to change the purpose of a controller. For example, if you want to move your OfficeExtend or indoor mesh access paints to a different controller, you could transfer the adder license from one controller of the same model, say from one 5500 series controller to another 5500 series controller. The case of RNA or a network reactification that the transfer the same model, say from one 5500 series controller of network reactification to another 5500 series controller of network reaching transfer. This case be done in the case of RNA or a network reactification that requires thom and explanate to another. It is not possible to rehost base licenses in normal scenarios of network reactification. The only exception where the transfer of base licenses is allowed is for RNA when you get a replacement hardware when your existing appliance has a failure.

In order to rehost a license, you must generate credential information from the controller and use it to obtain a permission ticket to revoke the license from the Cisco licensing site. Next, you must obtain a rehost ticket and use it to obtain a license installation file for the controller on which you want to install the license.



Note A revoked license cannot be reinstalled on the same controller

Using the GUI to Rehost a License

To rehost a license using the controller GUI, follow these steps:

Step 1 Choose Management > Software Activation > Commands to open the License Commands page.

Step 2 From the Action drop-down list, choose Rehost . The Revoke a License from the Device and Generate Rehost Ticket area appears (see Figure 4-10).

Figure 4-10 License Commands (Rehost) Page

abolu						teave Co	orfiquration F	ta Loc	out Refresh
cisco	MON: OK	WLWS	LON ROLLER	WIRELESS	BECOR. 1	MONNGEMENT	COMMANDS	-=1-	EEEDBACK
Management	Licanse	Comma	nds						
Summary SKMP HTTP-HTTPS	Action	Ilranco	from the doub	on and game	Rote Paber	e iusl	×		
Teinet SSII Serial Port Local Management Harry User Sessions Flags	Slegi 1: S Tile New	avic Diev ie to save	ine credential	intormation a)	In a life	y lly://209/1652012 Save Credentia	00/omn/ored128/9	5.lic)	
Mant VIa Wireless Sullware Adivation Licenses License Level Commones License Agent	Step 2: V Using the a permis Here 750 Save th	isit Cisc e Device C contracted a or yet a tillo in the	Dicensing on Tradential generat Lear be obtained in option to choose anfinipath.	d get the pe edificini Step 1 From <u>Cisac Das</u> a the Transes y	ormission ti 	icket soor om Auchicense volke from dris dev	1 19.		
) Teah Support	Shigi 3: R Enter Sa (from sto Fell co. T	revolke lin wod Komri api2) Towet File I	caloisie from tho issien Fraket Kira N Name (calpat)	e device am. Ione	l quanaratu:	Refuest Ticket (e.g.:ftp://20510.20 (e.g.:ftp://200166.20	.1 1.U/cmm/permi 11.50/cmm/mhrs	 t t:xet.li tickst	c 1
	\$				í			- 22	5

Step 4 To obtain a permission ticket to revoke the license, follow these steps:

a. Click Cisco Licensing (https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet) . The Product License Registration page appears (see Figure 4-11). Figure 4-11 Product License Registration Page

cisco		Vendovine (chonge)	i nggishin +rrrut - +bnut Clean Go	
Solutions Products	& Services Ordering Support Training & Events	Pariner Central		
(DVF	Support			
Product License Registration	Product License Registration		Toolid to 1 man factor	
	Number Endures Eticensee Submit	7	≝ ∞ +1 10	
	Elecosica Not Requiring a PAK		<u>Prov. Bra. da</u> <u>Hoda</u>	
	In you do not name a Product Automatization new (PAN), presse cick new for automatication new for automatication new (PAN), presse cick new for automatication new (PAN), presse cick new for automatication new (PAN), presse cick new for automatication new for automatication new for automatication new (PAN), presse cick new for automatication new for automaticatio	able incensies. 3DES/VES and DES	Related Tools S-meno Conference Tool	
	Fretyaren, Geno Servera for ES, oot Joon Hofee Communications bloogen verben L	lagra ta laanans	Two Service Request Trol	
	Product Authorization Rev (PAR)			
	Phone the Product All readances Key (24K) below by any los it aparates on the later that apart futures of Factball.	ompenied the Class		
	Product Authorization Rey (PAR):			
	interione value di atine includiric castres.			
	Liverpole 11 4, 2014 a Constante Prezingel a Transformation - Face Andrea (2014) Prezingel a Transformation - Constante (2014)			
	Disting Transformer			
	Tim (m.)			
	WMA License transfer			
	Click on following invite obtain an UVA idense to the following products - Outlays 0960607505 - ODCD0ODCD			
	- Consumption and AMR 800 Fixed			
	- Ciscolaero des hor PS sensos idense			
	Frakt: "1:1" SISCO Bloover FxX tenst			
	Manaya Licencee			
	Click on following invisite lookup and resend/relixes: idenses for the to lowing products: - Crany control and AMR			
	800 Fi≥sJ			
	Loos La serve indept			
	CL to the Control of			
	Ingenerative V guillion Livense			
Note To find the controller's p	roduct ID and serial number, choose Controller > Inventory on the controller GUI.			
 Open the device crede and paste the conter 	ntial information file that you saved in <u>In the File Name to Save Credentials text box, er</u> ts of the file into the Device Credentials text box.	ter the path on the TFTP s	erver where you want the device credentials to be saved and click Save Credent	ials, and
e. Enter the security code	in the blank box and click Continue .			
f. Choose the licenses the	at you want to revoke from this controller and click Start License Transfer .			
g. On the Rehost Quantit	ies page, enter the number of licenses that you want to revoke in the To Rehost text bo	and click Continue.		
 h. On the Designate Lice text boxes on this pay 	nsee page, enter the product ID and serial number of the controller for which you plan ge, and click ${\bf Continue}$.	to revoke the license, read a	and accept the conditions of the end-user license agreement (EULA), complete the	ne rest of
i. On the Review and Sut	mit page, verify that all information is correct and click Submit.			
j. When a message appe	ars indicating that the registration is complete, click Download Permission Ticket . T	he rehost permission ticket	is e-mailed within 1 hour to the address that you specified.	
 k. After the email arrives, a. 5. Lise the rebost permission 	copy the rehost permission ticket to your TFTP server.			
a. In the Enter Saved Per	mission Ticket File Name text box, enter the TFTP path and filename (*.lic) for the reho	ost permission ticket that you	u generated in To obtain a permission ticket to revoke the license, follow these si	leps:
b. In the Rehost Ticket Fi	le Name text box, enter the TFTP path and filename (*.lic) for the ticket that will be use	d to rehost this license on a	nother controller.	
c. Click Generate Rehos	st Ticket .			
d. When the end-user lice	ense agreement (EULA) acceptance dialog box appears, read the agreement and click	Accept to accept the terms	s of the agreement.	
ep 6 Use the rehost ticket gene controller as follows:	rated in Use the rehost permission ticket to revoke the license from this controller and	generate a rehost ticket as	<u>tollows</u> ; to obtain a license installation file, which can then be installed on anothe	ər
a. Click Cisco Licensing				
b. On the Product Licens	e Registration page, click Upload Rehost Ticket under Manage Licenses.	and a first state for a definition		
Continue .	age, enter the renost toket that you generated in <u>Use the renost permission toket to r</u>	evoke the license from this o	controller and generate a renost licket as follows; in the Enter Renost licket text	box and
 d. On the Validate Featur e. On the Designate Lice 	es page, verify that the license information for your controller is correct, enter the reho	st quantity, and click Contin	ue .	est of the
boxes on this page, a	nd click Continue.			001 01 11
f. On the Review and Sut	mit page, verify that all information is correct and click Submit .	icense kev is e-moliod with	in 1 hour to the address that you exactlined	
 a. men a message appe h. After the email arrives. 	copy the rehost license key to your TFTP server.	ייייי מאו מאוואניים אין איי אייייטא איייטאיי	אי י ייאאי אס עוים מאשרפסס עומג אַטע אָשְׁרָשווישע.	
i. Follow the instructions	n the "Installing a License" section to install this license on another controller.			
the CLI to Rehost a License host a license using the control	er CLI, follow these steps:			
ep 1 Save device credential inf	· · · · · · · · · · · · · · · · · · ·			
	ormation to a file by entering this command:			
se save credential url	ormation to a file by entering this command:			
ense save credential ur/ ere ur/ is tftp:// server_ip / path / / itep 2 Obtain a permission ticket	ormation to a tile by entering this command: <i>liename</i> . to revoke the license as follows:			

- b. Under Manage Licenses, click Look Up a License .
- c. Enter the product ID and serial number for your controller.

0

- Note To find the controller's product ID and serial number, enter the show license udi command on the controller CLI.
- d. Open the device credential information file that you saved in Save device credential information to a file by entering this command; and copy and paste the contents of the file into the Device Credentials text box.
- e. Enter the security code in the blank box and click Continue
- f. Choose the licenses that you want to revoke from this controller and click Start License Transfer
- g. On the Rehost Quantities page, enter the number of licenses that you want to revoke in the To Rehost text box and click Continue
- h. On the Designate Licensee page, enter the product ID and serial number of the controller for which you plan to revoke the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and rick Continue.
- i. On the Review and Submit page, verify that all information is correct and click Submit
- j. When a message appears indicating that the registration is complete, click Download Permission Ticket . The rehost permission ticket is e-mailed within 1 hour to the address that you specified.
- k. After the email arrives, copy the rehost permission ticket to your TFTP server
- Step 3 Use the rehost permission ticket to revoke the license from this controller and generate a rehost ticket as follows:
- a. To revoke the license from the controller, enter this command:
- license revoke permission_ticket_url
- here permission_ticket_url is tftp:// server_ip / path / filename b. To generate the rehost ticket, enter this command:
- license revoke rehost rehost ticket un
- where rehost_ticket_url is tftp:// server_ip / path / filename
- c. If prompted, read and accept the terms of the end-user license agreement (EULA)
- Step 4 Use the rehost ticket generated in Use the rehost permission ticket to revoke the license from this controller and generate a rehost ticket as follows: to obtain a license installation file, which can then be installed on another controller as follows:
 - a. Go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet .
 - b. On the Product License Registration page, click Upload Rehost Ticket under Manage Licenses
 - c. On the Upload Ticket page, enter the rehost ticket that you generated in Use the rehost permission ticket to revoke the license from this controller and generate a rehost ticket as follows; in the Enter Rehost Ticket text box and click Continue
 - d. On the Validate Features page, verify that the license information for your controller is correct, enter the rehost quantity, and click Continue
 - e. On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to use the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and rick Continue.
 - f. On the Review and Submit page, verify that all information is correct and click Submit
 - g. When a message appears indicating that the registration is complete, click Download License . The rehost license key is e-mailed within 1 hour to the address that you specified
 - h. After the email arrives, copy the rehost license key to your TFTP server
 - i. Follow the instructions in the "Installing a License" section to install this license on another controller

Transferring Licenses to a Replacement Controller after an RMA

If you return a Cisco 5500 Series Controller to Cisco as part of the Return Material Authorization (RMA) process, you must transfer that controller's licenses within 60 days to a replacement controller that you receive from Cisco Replacement controllers come preinstalled with the following licenses: permanent base and evaluation base, base-ap-count. No other permanent licenses are installed. The SKU for replacement controllers is AIR-CT5508-CA-K9. Because licenses are registered to the serial number of a controller, you can use the licensing portal on Clicoc.com to request that the license from your returned controller be reviewed and automized for use on the replacement controller. After your request is approved, you can install the old license on the replacement controller. Before you begin, you need the product D and serial number of both the returned controller and the replacement controller. This information is included in your purchase records.

1

The evaluation licenses on the replacement controller are designed for temporary use and expire after 60 days. To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. If the evaluation licenses expire before you transfer the permanent licenses from your defective controller to your replacement controller, the replacement controller remains up and running using the permanent base license, but access points are no longer able to join the controller.

- To transfer a license to a replacement controller after an RMA, follow these steps
- Step 1 Go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet
- Step 2 On the main Product License Registration page, click Register for an RMA License under RMA License Transfer.
- Step 3 In the Select a Product drop-down list, choose Cisco 5500 Series Wireless Controllers
- Step 4 Enter the security code in the blank box and click Go to RMA Portal
- Step 5 On the RMA License Transfer page, enter the product ID and serial number of the controller that you returned and your RMA service contract number, and click Continue
- Step 6 On the Validate Features page, verify that the license information for your controller is correct, and click Continue
- Step 7 On the Designate Licensee page, enter the product ID and serial number of the replacement control
- Step 8 Read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click Submit
- Step 9 On the Review and Submit page, verify that all information is correct and click Submit . A message appears indicating that your registration request has been submitted, and you will receive an e-mail that contains your RMA

Step 10 Select the status of your RMA registration request by following the instructions in the e-mail.

Step 11 After you receive another e-mail notifying you that your RMA registration request is approved (usually within 1 hour), follow the instructions in the "installing a License" section to install the license on the replacement controller

Configuring the License Agent

If your network contains various Cisco-licensed devices, you might want to consider using the Cisco License Manager (CLM) to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide. The license agent is an interface module that runs on the controller and mediates between CLM and the controller's licensing infrastructure. CLM can communicate with the controller using various channels, such as HTTP, Teinet, and so on. If you want to use HTTP as the communication method, you must enable the license agent on the controller.

The license agent receives requests from CLM and translates them into license commands. It also sends notifications to CLM. It uses XML messages over HTTP or HTTPS to receive the requests and send the notifications. For example, CLM sends a license install command, and the agent notifies CLM after the license expires.

0

Note You can download the CLM software and access user documentation at this URL: http://www.cisco.com/go/clm

Using the GUI to Configure the License Agent

To configure the license agent on the controller using the controller GUI, follow these steps

Step 1 Choose Management > Software Activation > License Agent to open the License Agent Configuration page (see Figure 4-12)

Figure 4-12 License Agent Configuration Page

cibalia cisco	MONTOR WLANS CONTOLLD	WIRELESS SECURITY MANAGEMENT EDMMANDS	Engri Configuration Eing. Ingold (Britisch HELF FEEDEACK
Management	License Agent Configuration		Apply
Summary			
IF SKMP	General		
HTTP HTTPS	Loab e Default Authentication	<u>R.</u>	
Serial Port	Maximum number of sessions	0	
Lucal Management	License Agent Listener		
Users Liser Sessions	E ral a liste rar	Ξ	
▶ Lugs	Listaner Message Processing URL	(e.g. attac/200166-20120/licensa@gent/austora)	
Mynd Via Windess	Frewcol 2	E FTTF 🗹 HTTPS(e narypled)	
 Software Activation Licenses 	Lhable Authent sation for Listener	<u></u>	
Liccose Level Semmones	MeX HT Fill assay a size	<u> </u>	
Lice ise Avent			
Flech Support	License Agent Notification		
	Foot a Katif aatica	<u>E</u>	
	UR to some the Notfleetices	(e.g. atta://www.cisco.com/license/antity)	
	User Name		
	Confirm Dossword		134
			<u> </u>
Step 2 Select the Enable Defa	Authentication check box to enable the	Incense agent, or leave it unselected to disable this feature. The default	value is unselected.
Step 3 in the Maximum Numbe	r or bessions text box, enter the maximum n	moer or sessions for the license agent. The valid range is 1 to 25 sessio	ns (inclusivê).
Step 4 Configure the license a	gent to listen for requests from the CLM as t	lows:	
a. Select the Enable Li	istener check box to enable the license age	t to receive license requests from the CLM, or unselect this check box to	o disable this feature. The default value is unselected.
b. In the Listener Mess requires HTTP or I	age Processing URL text box, enter the URI HTTPS.	where the license agent receives license requests (for example, http://2	US. 102.01.30/IICenseAgent/custom). The Protocol parameter indicates whether the URL
0			
Note You can specify the pr	otocol to use on the HTTP Configuration pa	e. See the "Enabling Web and Secure Web Modes" section for more in	formation.
Coloctik- Facht	uthantication for Listener short hard	he authentication for the license asset where his sector is a	inete or uncellent the check boy to dischile this feature. The default value is used in the
c. Select the Enable A	utnentication for Listener check box to en	bie autrentication for the license agent when it is receiving license requ	lests, or unselect this check box to disable this feature. The default value is unselected.
d. In the Max HITP Me	essage Size text box, enter the maximum size	for license requests. The valid range is 0 to 9999 bytes, and the deraul	value is u.
3 Select the Enable N	etification check box to enable the license	as follows:	to disable this feature. The default value is unselected
 a. Select the Enable N b. In the LIPL to Send t 	he Notifications text box to enable the LIPL who	a the license agent sends the patifications (for example, bttp://www.ciso	a comficense/polify)
 In the User Name to 	the would all the user and required in order	a the incense agent sends the houndations (for example, http://www.ciso	o.connicensemoniy).
d In the Deceword and	Confirm Password text hoves enter the pa	word required in order to view the patification messages at this LIPL	
Stan 6 Click Apply to commit	our changes	word required in order to view the notification messages at this ONE.	
Step 7 Click Apply to commity			
o configure the license agent on Step 1 Enable the license agen config license agent defaul config license agent defaul	the controller using the controller CLI, follow t by entering one of these commands: it authenticate —Enables the license agen t authenticate none —Enables the license	hese steps: Jefault listener with autheniication. gent default listener without autheniication.	
			
Note To disable the licent	se agent default listener, enter the config li	onse agent default disable command. The default value is disabled.	
Step 2 Specify the maximum n	umber of sessions for the license agent by e	tering this command:	
onfig license agent max-sessi	ons sessions		
The valid range for the sessions p	arameter is 1 to 25 (inclusive), and the defa	t value is 9.	
Step 3 Enable the license ager	nt to receive license requests from the CLM	nd to specify the URL where the license agent receives the requests by	entering this command:
ontig license agent listener htt he valid range for the size param	tp { plaintext encrypt } un authenticate leter is 0 to 65535 bytes, and the default val	none j[max-message s/zej[aciac/j eis 0.	
•			
Note To prevent the licen	se agent from receiving license requests fro	the CLM, enter the config license agent listener http disable com	nand. The default value is disabled.
Step 4 Configure the license a	gent to send license notifications to the CLN	and to specify the URL where the license agent sends the notifications	by entering this command:
config license agent notify url u	isemame password	-	
N			
Note To prevent the licen	se agent from sending license notifications	the CLM, enter the config license agent notify disable username pa	assword command. The default value is disabled.
Step 5 Save your changes by a	entering this command:		
ave config			
Step 6 See statistics for the lice	ense agent's counters or sessions by enteri	this command:	
how license agent (counters see	ssions}		
icense Agent Counters	appears for the show license agent counter	continanti.	
equest Messages Received	1:10: Messages with Errors:1		
equest operations Receiv Otification Messages Ser	eu.g. operations with Errors:0 ht:12: Transmission Errors:0: So	p Errors:0	
nformation similar to the following .icense Agent Sessions:]	appears for the show license agent session open, maximum is 9	command:	
Note To clear the license	agent's counter or session statistics enter	e clear license agent (counters Lisessions) command	
	agone a counter or aession statistics, effer		
onfiguring 802.11 Bands			
'ou can configure the 802.11b/g/n	(2.4-GHz) and 802.11a/n (5-GHz) bands fo	the controller to comply with the regulatory requirements in your country	By default, both 802.11b/g/n and 802.11a/n are enabled.
ing the GUI to Configure 802.	.11 Bands		
o configure 802.11 bands using t	he controller GUI, follow these steps:		
Step 1 Choose Wireless > 80	2.11a/n or 802.11b/g/n > Network to open	e 802.11a (or 802.11b/g) Global Parameters page (see Figure 4-13).	

Figure 4-13 802.11a Global Parameters Page

almh						l c≥r Crafigurarica	Eine tr⊻e t 2stwib
CISCO	VOLTOR WEARS CONTROL	ATEK MINETERS	SECURITI	MONOGEREN	COMMONUS HELF FEED	EAC <	
Advanced	902.11 b/g Global Paramet	ters					Apply
RF Profiles	General			Data Rates**			
FlexConnect Groups	800b/g Not vori: Etatus	🗵 I iabled		1 Mb pc	Yestatory 😽		
FlerConned ACLC BU2.11s/n	CC2.21g Support	Ecolod.		2 Mbos	😪 Jator v 🔛		
Setwork PMT	Spein Pressola	L Chabled		5.5 M005	Ve undet s ^v		
RF Grouping Triu	Fragmentation Threshold (bytes)	234F					
Doverage Doverage	DTPC Subort	Satisf					
Cliert Roamin;	Novim to Allowed Clients	Sam					
ED DA Pariar Vices DEC (817-110)	66% Encation Measuremen	#					
figh I froughput (W S 11n) Clear Au	Mi Den Ome (handeter (*****	LE SJAN		-			
802.116/g/m	speake role will not be oble to implies that any essequeed the	associato, Data Rato i ant that else supports t	Cupported Mat same rate				
PR-4	mer convinuitions with the AP shet a client be able to use the accounter the actual data rate	using thet refe. Dut it : refes merked support is that are supported of	is not required red in order to leneral or the				
T°C DCA	chessel selected as affected as cardwellbs, the manages tates to select the data select. All the	neocels cosy bave diffe we about date other an zoothe zho diff will pust	ianat od c'iewstere k zeo portwar				47
Josef age Josef Sal	date sets allowed for that shee supported	not if the above areas	NUTE IS NOT				321
ep 2 Select the 802.11a (c 802.11b/g bands.	or 802.11b/g) Network Status ch	eck box to enable the	802.11a or 80	02.11b/g band. To d	sable the band, unselect the ch	eck box. The default value is enabled.	You can enable both the 802
3 If you enabled the 80 enable both the 802.1 without 802.11g supp)2.11b/g band in <u>Select the 802.11a</u> <u>11a and 802.11b/g bands.</u> , select t	a (or 802.11b/g) Netwo the 802.11g Support of	ork Status che check box if yo	ack box to enable th ou want to enable 8	e 802.11a or 802.11b/g band. Te 02.11g network support. The de	o disable the band, unselect the check fault value is enabled. If you disable th	t box. The default value is enabled is feature, the 802.11b band
34 Specify the rate at will	hich the SSID is broadcast by the	access point by entering	ing a value bet	tween 100 and 600	milliseconds (inclusive) in the B	eacon Period text box. The default val	ue is 100 milliseconds.
	ers is listed in terms of milliseconds	s. The beacon period (can also be m	easured in Time Un	its, where one Time Unit equals	1024 microseconds or 102.4 milliseco	nds. If a beacon interval is lis
ntroller, it is only a rounded	J off value for 102.4 milliseconds.	con interval in a second	D Time Li-li-	tie adjusted 400	Time Unite which secondly a	le 104 449 millionanda Thur ut	he hearon nation /- +
to naroware limitation in ce to the value is adjusted to the	ne nearest multiple of 17.	Jun Interval IS, say 100	u imė Units, i	us adjusted to 102	me units, which roughly equa	104.446 milliseconds. Thus, when t	ne peacon period is to be rep
ep 5 Specify the size at w	hich packets are fragmented by er	tering a value betwee	en 256 and 234	46 bytes (inclusive)	in the Fragmentation Threshold	text box. Enter a low number for areas	s where communication is po
ep 6 Make access noints	advertise their channel and transn	nit power level in beac	ons and probe	e responses. Select	the DTPC Support check box	Otherwise, unselect this check how Th	he default value is enabled
It devices using dynamic tr	ansmit power control (DTPC) rece	ive the channel and p	ower level info	ormation from the ac	ccess points and adjust their set	tings automatically. For example, a clie	nt device used primarily in Ja
just its channel and power	settings automatically when it trav	els to Italy and joins a	a network there	э.			
Note On access points	s that run Cisco IOS software, this	feature is called world	d mode.				
•							
Note DTPC and 801.1	1h power constraint cannot be ena	abled simultaneously.					
tep 7 Use the Data Rates of	options to specify the rates at whic	ch data can be transmi	itted between	the access point an	d the client. These data rates a	re available:	
802.11a—6, 9, 12, 18, 24,	36, 48, and 54 Mbps						
802.11b/g—1, 2, 5.5, 6, 9,	11, 12, 18, 24, 36, 48, or 54 Mbps						
Mandatory —Clients must	t support this data rate in order to a	associate to an access	s point on the	controller.			
Supported —Any associat	ted clients that support this data ra	ate may communicate v	with the acces	s point using that r	ate. However, the clients are not	required to be able to use this rate in	order to associate.
Disabled —The clients spo	ecify the data rates used for comm	unication.					
Step 9 Click Save Configu	ration to save your changes.						
g the CLI to Configure 80	02.11 Bands						
onfigure 802.11 bands usin	g the controller CLI, follow these st	.teps:					
tep 1 Disable the 802.11a	band by entering this command:						
fig 802.11a disable network.							
Note The 802.11a ban	nd must be disabled before you car	n configure the 802.11	a network par	ameters in this sect	ion.		
step 2 Disable the 802.11b/	/g band by entering this command:						
nfig 802.11b disable network							
Note The BOO date :	nd must be disabled b-f	n configure the coo · ·	h natural -	amatam in this	ion		
NOTE THE BUZ.11b ban	u must be disabled before you car	i conligure the 802.11	u network par	arneters in this sect	JUH.		
tep 3 Specify the rate at wi	hich the SSID is broadcast by the a	access point by entering	ing this comma	and:			
ing tou2.11a 802.11b} beac are time_unit is the beacon i	interval in time units (TUs). One TI	U is 1024 microsecond	ds. You can co	onfigure the access	point to send a beacon every 20	0 to 1000 milliseconds.	
itep 4 Specify the size at wi	hich packets are fragmented by en	tering this command:					
ifig (802.11a 802.11b) fragi	mentation threshold	e). Specify a low numb	ber for areas y	vhere communicatio	n is poor or where there is a are	eat deal of radio interference	
tep 5 Make access points a	advertise their channel and transm	nit power level in beac	ons and probe	e responses by ente	ring this command:		
ifig (802.11a 802.11b) dtpc	{enable disable}						
default value is enabled. Cl apan could rely on DTPC to	lient devices using dynamic transn adjust its channel and power setti	nit power control (DTP ings automatically whe	°C) receive the en it travels to	e channel and powe Italy and joins a ne	er revel information from the acce twork there.	ess points and adjust their settings aut	omatically. For example, a cli
N		4	d are of				
Note On access points	anat run UISCO IUS software, this	reature is called world	u mode.				
9p 6 Specify the rates at v	which data can be transmitted betw	veen the controller and	d the client by	entering this comm	and:		
ig (802.11a 802.11b) rate re	{ disabled mandatory suppor						
disabled —Clients specify		rted } rate					
mandatory-C lients supp	the data rates used for communic	rated } rate					
oupported Ar	the data rates used for communic sort this data rate in order to assoc	rted } rate ation. state to an access poin	nt on the contr	oller.	to Houseney the effect		ander to correlate
supported — Any associate rate — The rate at which da	/ the data rates used for communic out this data rate in order to assoc ed clients that support this data rat ata is transmitted:	rted } rate :ation. :late to an access poin te may communicate w	nt on the contro with the access	oller. s point using that ra	te. However, the clients are not	required to be able to use this rate in o	order to associate.
supported — Any associate rate — The rate at which da - 6, 9, 12, 18, 24, 36, 48	/ the data rates used for communic port this data rate in order to assoc ed clients that support this data rat ata is transmitted: , and 54 Mbps (802.11a)	rted } rate ation. siate to an access poin te may communicate w	nt on the contri with the access	oller. s point using that ra	te. However, the clients are not	required to be able to use this rate in o	order to associate.
supported — Any associati rate — The rate at which da - 6, 9, 12, 18, 24, 36, 48 - 1, 2, 5.5, 6, 9, 11, 12, 1 Step 7, Enzhle the 922 44	/ the data rates used for communic port this data rate in order to assoc ed clients that support this data rat at is transmitted: i, and 54 Mbps (802.11a) 18, 24, 36, 48, or 54 Mbps (802.11 19, 24, 25, 48, 07, 54 Mbps (802.11)	rted } rate ation. jate to an access poin te may communicate w b/g)	nt on the contro with the access	oller. s point using that ra	te. However, the clients are not	required to be able to use this rate in c	order to associate.
supported — Any associati rate — The rate at which da - 6, 9, 12, 18, 24, 36, 48 - 1, 2, 5.5, 6, 9, 11, 12, 1 tep 7 Enable the 802.11a b lig 802.11a enable network	r the data rates used for communic port this data rate in order to assoc ed clients that support this data rai ata is transmitted. i, and 54 Mbps (802.111 8, 24, 36, 48, or 54 Mbps (802.111 and by entering this command:	rted } rate	nt on the contro with the access	oller. s point using that ra	te. However, the clients are not	required to be able to use this rate in c	order to associate.
supported — Any associati rate —The rate at which di - 6, 9, 12, 18, 24, 36, 48 - 1, 2, 5.5, 6, 9, 11, 12, 1 ep 7 Enable the 802.11a b ig 802.11a enable network default value is enabled.	r the data rates used for communic port this data rate in order to assoc ed clients that support this data rai ata is transmitted. I, and 54 Mbps (802.11a) 18, 24, 36, 48, or 54 Mbps (802.111 aand by entering this command:	rted } rate ;ation. ;iate to an access poin te may communicate w b/g)	nt on the contro with the access	oller. s point using that ra	te. However, the clients are not	required to be able to use this rate in c	order to associate.
supported — Any associati rate — The rate at which di - 6, 9, 12, 18, 24, 36, 48 - 1, 2, 5.5, 6, 9, 11, 12, 1 ep 7 Enable the 802.11a b ig 802.11a enable network default value is enabled. ep 8 Enable the 802.11b b	r the data rates used for communic port this data rate in order to assoc ed clients that support this data rai ata is transmitted: 1, and 54 Mbps (802.111a) 18, 24, 36, 48, or 54 Mbps (802.111 aand by entering this command: aand by entering this command:	rted } rate	nt on the contro with the access	oller. s point using that ra	te. However, the clients are not	required to be able to use this rate in c	order to associate.
supported — Any associati rate — The rate at which di = 6,9,12,18,24,36,48 = 1,2,55,6,9,11,12,1 Step 7 Enable the 802.116 t hifg 802.11a enable network d default value is enabled. Step 8 Enable the 802.110 t hifg 802.11b enable network o default value is enabled	y the data rates used for communic port this data rate in order to assoc ed clients that support this data rai ata is transmited.), and 54 Mbps (802.11a) 18, 24, 36, 48, or 54 Mbps (802.111 aand by entering this command: aand by entering this command:	rted) rate	nt on the contro	oller. s point using that ra	te. However, the clients are not	required to be able to use this rate in c	order to associate.

13 of 45

config 802.11b 11gSupport (enable disable) The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support
step to Save your changes by entering this command: save config
Step 11 View the configuration settings for the 802.11a or 802.11b/g band by entering this command:
show (802.11a 802.11b)
Information similar to the following appears:
802.11a Network Enabled
llnSupport Enabled
802.11a Low Band Enabled
802.11a Mid Band Enabled
802.11a High Band Enabled
802.11a Operational Rates
802.11a 6M Rate Mandatory
802.11a 9M Rate Supported
802.11a 12M Rate
802.11a 18M Rate Supported
802.11a 24M Rate Mandatory
802.11a 36M Rate Supported
802.11a 48M Rate Supported
802.11a 54M Rate Supported
Beacon Interval 100
Default Channel
Default Tx Power Level 1
DTPC Status Enabled
Fragmentation Threshold

Configuring 802.11n Parameters

This section provides instructions for managing 802.11n devices such as the Cisco Aironet 1140 and 1250 Series Access Points on your network. The 802.11n devices support the 2.4- and 5-GHz bands and offer high-throughput data rates.

1 Note The 802.11n high-throughput rates are available only on 1140 and 1250 series access points for WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled. 0

Note For information on configuring radio resource management (RRM) parameters or statically assigning radio parameters for 802.11n access points, see Chapter 12, "Configuring Radio Resource Management/Wireless Device Access"

Using the GUI to Configure 802.11n Parameters

To configure 802.11n parameters using the controller GUI, follow these steps:

Step 1 Choose Wireless > 802.11a/n or 802.11b/g/n > High Throughput (802.11n) to open the 802.11n (5 GHz or 2.4 GHz) High Throughput page (see Figure 4-14).

Figure 4-14 802.11n (2.4 GHz) High Throughput Page

cisco	MORITOP.	«LANS	CONTROLLER.	WIPELEDC	SE 31, 70	Sage Conf Marc	ic Intica AGEMENT	⊇inc n Commai	igol <u>E</u> cfora JDC HELP
Wireless	902.11n (2.4 GHz)	High Throug	hput				1	Apply
F Access Points	General				Ind) ann	a Rali:∔)	Selling		
Medi HREAP Grauns	r Mor	í.	🗹 Frahled		٦ (7	Mhas)	Ø	Supported	
▶ 802.11a/u					1 (14	Mhas)		Supported	
* 802.11b/u/u					2 (21	Mbos';	1-1	Supported	
retwork:					3 (25	MLUS;		Supported	
Cher, Ruarum,					(4)	Mbos)	V	Supported	
Voice Voice					5 (58	Mhas)		Supported	
EDCA Peralitebris					5 (05	Mbos';	1-1	Supported	
(302.11)					7 (72	MLus;		Supported	
Country					3 (14	MLUS;		Supported	
timers					n (.20	Mhas)		Supported	
▶ QeS					10 (4).	Mbos)	1-1	Supported	
					12 (50	Mbos'	1~1	Supported	
					12 (87	MLUS)		Supported	
					13 (11	Mhas)		Supported	
					14 (12	Mhas)	M	Supported	-
					15 (14	Mbos)	121	Supported	2220

2 DetaNates are calculated for 20 Mirz Channel wight

Step 2 Select the 11n Mode check box to enable 802.11n support on the network. The default value is enabled.

Step 3 Select the check boxes of the desired rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. These data rates, which are calculated for a 20-MHz channel width using a short guard interval, are available:

- 0 (7 Mbps)
- 1 (14 Mbps)
- 2 (21 Mbps)
- 3 (29 Mbps) 4 (43 Mbps)
- 5 (58 Mbps)
- 6 (65 Mbps)
- 7 (72 Mbps)
- 8 (14 Mbps)
- 9 (29 Mbps)
- 10 (43 Mbps)
- 11 (58 Mbps)
- 12 (87 Mbps) • 13 (116 Mbps)
- 14 (130 Mbps)
- 15 (144 Mbps)

Any associated clients that support the selected rates may communicate with the access point using those rates. However, the clients are not required to be able to use this rate in order to associate. The MCS settings determine the number of spatial streams, the modulation, the coding rate, and the data rate values that are used.

Step 4 Click Apply to commit your changes.

- Step 5 Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:
 - a. Choose WLANs to open the WLANs page.
 - b. Click the ID number of the WLAN for which you want to configure WMM mode.
 - c. When the WLANs > Edit page appears, choose the \boldsymbol{QoS} tab to open the WLANs > Edit (Qos) page.
 - d. From the WMM Policy drop-down list, choose Required or Allowed to require or allow client devices to use WMM. Devices that do not support WMM cannot join the WLAN
 - e. Click Apply to commit your changes.
- Step 6 Click Save Configuration to save your changes.
 - 0
 - Note To determine if an access point supports 802.11n, look at the 11n Supported text box on either the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page or the 802.11a/n (or 802.11b/g/n) AP Interfaces > Details page.

Using the CLI to Configure 802.11n Parameters To configure 802.11n parameters using the controller CLI, follow these steps:

Step 1 Enable 802.11n support on the network by entering this command:

config { 802.11a | 802.11b } 11nsupport { enable | disable }

Step 2 Specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client by entering this command:

config { 802.11a | 802.11b } 11nsupport mcs tx { 0-15 } { enable | disable }

See the descriptions of the 0 through 15 MCS data rates in the "Using the GUI to Configure 802.11n Parameters" section. Step 3 Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:

config wlan wmm required wlan_id

The required parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

- Step 4 Specify the aggregation method used for 802.11n packets as follows:
 - a. Disable the network by entering this command:
- config { 802.11a | 802.11b } disable network b. Specify the aggregation method entering this command:

config { 802.11a | 802.11b } 11nsupport a-mpdu tx priority {0-7 | all} {enable | disable }

Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MPDU). Both A-MPDU and A-MSDU are performed in the software. You can specify the aggregation method for various types of traffic from the access point to the clients. Table 4-2 defines the priority levels (0-7) assigned per traffic type.

Table 4-2 Traffic Type Priority Levels

User Priority	Traffic Туре
0	Best effort
1	Background
2	Spare
3	Excellent effort
4	Controlled load
5	Video, less than 100-ms latency and jitter
6	Voice, less than 10-ms latency and jitter
7	Network control

Vou can configure each priority level independently, or you can use the **all** parameter to configure all of the priority levels at once. When you use the **enable** command, the traffic associated with that priority level uses A-MPDU transmission. When you use the **disable** command, the traffic associated with that priority level uses A-MPDU transmission. Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4 and 5 and the rest are disabled.

c. R eenable the network by entering this command:

config {802.11a | 802.11b} enable network

Step 5 Save your changes by entering this command:

save config

Step 6 View the configuration settings for the 802.11a/n or 802.11b/g/n band by entering this command:

show {802.11a | 802.11b}

Information similar to the following appears:
802.11a Network Enabled
llnSupport Enabled
802.11a Low Band Enabled
802.11a Mid Band Enabled
802.11a High Hand Enabled
802.11a Operational Rates 802.11a 6M Pate Mandatory
802.11a 9M Rate. Supported
802.11a 12M Rate Mandatory
802.11a 18M Rate Supported
802.11a 24M Rate Mandatory
802.11a 36M Rate Supported
802.11a 48M Rate Supported
802.11a 54M Rate Supported
802.11n MCS Settings:
MCS U Supported
MCS 2. Supported
MCS 3
MCS 4
MCS 5 Supported
MCS 6 Supported
MCS 7 Supported
MCS 8 Supported
MCS 9 Supported
MCS 10
MCS 11
MCS 12 Supported
MCS 14
MCS 15
802.11n Status:
A-MPDU Tx Enabled
Priority 0 Enabled
Priority 1 Disabled
Priority 2 Disabled
Priority 3 Disabled
Priority 5. Enabled
Priority 6 Disabled
Priority 7 Disabled
A-MSDU Tx Enabled
Rifs Tx Enabled
Guard Interval Short
Beacon Interval 100
CF Pollable mandatory Disabled
CFP Deriod 4
CFP Maximum Duration
Default Channel
Default Tx Power Level 1
DTPC StatusEnabled
Fragmentation Threshold 2346
Long Retry Limit 4
Maximum Rx Life Time 512
Max Tx MSDU Life Time
Medium Occupancy Limit 100
Short Retry Limit
TI Threshold -50
Traffic Stream Metrics Status Enabled
Expedited BW Request Status Disabled
EDCA profile type default-wmm
Voice MAC optimization status Disabled
Call Admission Control (CAC) configuration
Voice AC - Admission control (ACM) Enabled
Voice max RF bandwidth

15 of 45

-	AIRAW14011	
Voice load-based CAC mod	leDisabled	
Voice tspec inactivity t Video AC - Admission cor	ntrol (ACM) Enabled	
Voice Stream-Size		
Voice Max-Streams Video max RF bandwidth		
Video reserved roaming b	mandwidth0	
Configuring 802.11h Parame 802.11h informs client devices at Using the GUI to Configure 802 To configure 802.11h parameters Step 1 Disable the 802.11h parameters b. Unselect the 802.11 c. Click Apply to com Step 2 Choose Wireless = 8 Figure 4-15 802.11h Global Parameters Click Apply to com Step 2 Choose Wireless = 8 Figure 4-15 802.11h Global Parameters (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	eters Sout channel changes and can limit the transmi 2.11h Parameters using the controller GUI, follow these steps: and as follows: *802.11ah > Network to open the 802.11a G ta Network Status check box. mit your change. 20.11ah > DFS (802.11b) to open the 802.11b meters Page EDUTION: EDUTUS _CONTROLLER: Power Constraint EDUTION: EDUTUS _CONTROLLER: Channel Revites Page Channel Revites Area conservation Channel Revites Page	it power of those client devices. You can configure the 802.11h parameters using the controller GUI or CLL isobal Parameters page. In Global Parameters page (see Eguro 4-15). Seve Estification fine Esquark kef esti Multiplus ELEVE SetURUTION May held Eleve SetURUTION May held by SetURUTION May
CleanAir		
▶ 802.11b/g/n		5
▶ Motia Stream	V	
Step 3 Select the Channel A	nnouncement check box if you want the acce	ss point to announce when it is switching to a new channel and the new channel number, or unselect this check box to disable the channel announcement
Step 6 Reenable the 802.11a a. Choose Wireless >	your changes. band as follows: > 802.11a/n > Network to open the 802.11a G	Slobal Parameters page.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configura	your changes. band as follows: • 802.11ah > Network to open the 802.11a G Network Status check box. mit your change. tion to save your changes.	slobal Parameters page.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configura Joing the CLI to Configure 802 To appleary 0.00 1/1	your changes. band as follows: • 802.11ah > Network to open the 802.11a G Network Status check box. mit your change. tion to save your changes. 2.11h Parameters which the acentration Of 1.015 and 1.0	ilobal Parameters page.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configura Dising the CLI to Configure 802 To configure 802.11h parameters	your changes. band as follows: • 802.11a/h > Network to open the 802.11a G Network Status check box. mit your change. tion to save your changes. 2.11h Parameters : using the controller CLL follow these steps: 	Slobal Parameters page.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Step 7 Click Save Configure 802 Jsing the CLI to Configure 802 To configure 802.11a not set of the	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. ttion to save your changes. 2.11h Parameters using the controller CLI, follow these steps: etwork by entering this command:	Sicbal Parameters page.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Step 7 Click Save Configure 802 7 Configure 802.11a hor configure 802.11a hor configure 802.11a hor configure 802.11a hor config 902.11a disable the 802.11a hor config 902.11a disable entworl	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. ttion to save your changes. 2.11h Parameters using the controller CLI, follow these steps: atwork by entering this command: k creases noint to announce when it is switching it	to a new channel and the new channel number by entering this command:
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Step 7 Click Save Configure 802.11b To configure 802.11b Disable the 802.11a Step 1 Disable the 802.11a config 802.11a Configure 802.11b Step 1 Disable the 802.11a config 802.11b channelswitch You can enter a 0 or 1 for the sw Step 2 Configure 802.11b	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. tion to save your changes. 2.11h Parameters using the controller CLI, follow these steps: etwork by entering this command: k access point to announce when it is switching 1 { enable disable } switch_mode tich_mode parameter to specify whether transi-	to a new channel and the new channel number by entering this command:
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configura 7 Configure 802.11h parameters Step 1 Disable the 802.11a nr config 802.11a biable networl Step 2 Enable of or disable the config 802.11h channelswitch You can enter a 0 or 1 for the sw Step 3 Configure a new chan config 802.11h schrahamal dwa	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. tion to save your changes. 2.11h Parameters using the controller CLI, follow these steps: etwork by entering this command: k access point to announce when it is switching 1 { enable disable } switch_mode itch_mode parameter to specify whether transmel using the 802.11h channel announcement I nel using the 802.11h channel announcement I	to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command:
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com. Step 7 Step 7 Click Save Configure 802 To configure 802.11h parameters Step 1 Disable the 802.11a n config 802.11a alieable end sable networl Step 2 Enable of disable the 102.11a n You can enter a 0 or 1 for the sw Step 3 Config 802.11h channelswitch. You can enter a 0 or 1 for the sw Step 3 Configure 802.11h channelswitch.	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. tion to save your changes. 2.11h Parameters using the controller CLI, follow these steps:- etwork by entering this command: k access point to announce when it is switching t (enable disable) <i>switch_mode</i> <i>lich_mode parameter to</i> specify whether transi- nel using the 602.11h channel announcement I nel channel power constant value by entering this commanders.	to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and:
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configure 802 To configure 802.11h parameters Step 1 Disable the 802.11a nr config 802.11a disable networf Step 2 Enable or disable the : config 802.11h channelswitch. You can enter a 0 or 1 for the sw Step 3 Configure a new chan config 802.11h channelswitch.	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. miti your change. tion to save your changes. 2.11h Parameters : using the controller CLI, follow these steps: etwork by entering this command: k access point to announce when it is switching t (enable disable <i>switch_mode</i> <i>itch_mode parameter to</i> specify whether transf nel using the 802.11h channel announcement I nel channel power constraint value by entering this command x value	iobal Parameters page. to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and:
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Step 7 Click Save Configure Jsing the CLI to Configure 802 To configure 802.11a nr Config 802.11a Disable the 802.11a nr config 802.11a clisable networf Step 2 Enable or disable the 302.01g or disable the 302.01g 802.11h channelswitch. You can enter a 0 or 1 for the sw Step 3 Config 802.11h channelswitch. You can enter a 0 or 1 for the sw Step 4 Configure a new chan config 802.11h percentance i chas Step 4 Config uz.11h percentance i chas Step 4 <t< td=""><td>your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. Ition to save your changes. tion to save your changes. 2.11h Parameters auging the controller CLI, follow these steps: etwork by entering this command: k access point to announce when it is switching ((enable disable) switch_mode itio_mode parameter to specify whether trans- nel using the 802.11h channel announcement I nel channel power constraint value by entering this command transcere is 3 dB.</td><td>to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and:</td></t<>	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. Ition to save your changes. tion to save your changes. 2.11h Parameters auging the controller CLI, follow these steps: etwork by entering this command: k access point to announce when it is switching ((enable disable) switch_mode itio_mode parameter to specify whether trans- nel using the 802.11h channel announcement I nel channel power constraint value by entering this command transcere is 3 dB.	to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and:
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configura 70 configure 802.11h parameters Step 1 Disable the 802.11h parameters Step 1 Disable the 802.11h parameters Step 2 Enable or disable the 1 config 802.11h channelswitch. You can enter a 0 or 1 for the sw Step 3 Configure the 802.11h acconfig 802.11h setchannel cha Step 4 Configure the 802.11h config 802.11h setchannel cha Step 5 Configure the 802.11h config 802.11h parameters The delault value for the value po Step 5 Reenable the 802.11h	your changes. bend as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box network Status check box tion to save your changes. • tion to save your changes. • the save the save the save type of the save the sav	liobal Parameters page.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configura 7 Click Save Configura 7 Configure 802.11h parameters 7 Step 1 Disable the 802.11a nr config 802.11a disable netword 7 Step 2 Enable or disable the 30 config 802.11a channelswitch. 7 You can enter a 0 or 1 for the sw Step 3 Configure a new chan config 802.11h setchannel cha Step 4 Configure the 802.11h config 802.11h powerconstrai The default value for the value p Step 5 Reenable the 802.11a	your changes. bend as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box network Status check box tion to save your changes. • tion to save your changes. 2.11h Parameters using the controller CLI, follow these steps: etwork by entering this command: k access point to announce when it is switching to (enable disable) switch_mode itch_mode parameter to specify whether trans- nel using the 802.11h channel announcement 1 nel clannel i power constraint value by entering this comma it value arameter is 3 dB, network by entering this command: 11h parameters by waterion this command:	lobal Parameters page.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configure Jsing the CLI to Configure 802 To configure 802.11h particular to the select the 802.11a config 802.11h channelswitch You can enter a 0 or 1 for the sw Step 2 Configure an work and config 802.11h setchannel cha Step 4 Configure a new chan config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11a enable network Step 6 See the status of 802.11b	your dranges. band as follows: = 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. titlen to save your changes. 2.11h Parameters using the controller CLI, follow these steps: atwork by entering this command: k caceses point to announce when it is switching tr (enable disable) switch_mode itch_mode parameter to specify whether transmel is and power constraint value by entering this command: t value arameter is 3 dB. network by entering this command: 11h parameters by entering this command:	Iobal Parameters page.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configure 7 Configure 802.11b acconfigure 802.11b acconfigure 802.11b acconfig 802.11b config 802.11b config 802.11b step 2 Enable or disable the config 802.11b config 802.11b step 3 Configure a new chan config 802.11b step 4 Configure the 802.11b config 802.11b step 5 Reenable the 802.11b config 802.11b step 5 See the status of 802. show 802.11b	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. tion to save your changes. 2.11h Parameters using the controller CLI, follow these steps: etwork by entering this command: k cacess point to announce when it is switching 1 (enable disable) switch_mode lich_mode parameter to specify whether transmel using the 802.11h channel announcement 1 mol channel upower constraint value by entering this command: k value arameter is 3 dB. network by entering this command: 11h parameters by entering this command: gappears:	siobal Parameters page.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to corr Step 7 Click Save Configure 7 Click Save Configure 802 To configure 802.11h parameters Step 1 Disable the 802.11a nr config 802.11a disable network Step 2 Enable or disable the config 802.11h channelswitch You can enter a 0 or 1 for the sw Step 3 Configure a new chan config 802.11h setchannel cha Step 4 Configure a new chan config 802.11h pewerconstrain The default value for the value p Step 5 Reenable the 802.11h config 802.11h anable network Step 6 See the status of 802. show 802.11h	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. tion to save your changes. 2.11h Parameters using the controller CLI, follow these steps: etwork by entering this command: k access point to announce when it is switching 1 (enable disable) <i>switch_mode</i> <i>itch_mode parameter</i> to specify whether transmel using the 802.11h channel announcement I mole <i>channel</i> power constraint value by entering this comma it value arameter is 3 dB. network by entering this command: 11h parameters by entering this command: 11h parameters by entering this command: 11h parameters by entering this command: 11 parameters by entering this command: 12 pagesars: 2 pagesars	siobal Parameters page.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to corr Step 7 Click Save Configure 802 To configure 802.11h parameters Step 1 Disable the 802.11a n config 802.11a disable networl Step 2 Enable or disable the so config 802.11h channelswitch You can enter a 0 or 1 for the sw Step 3 Configure a new chan config 802.11h settemanels the 802.11h config 802.11h powerconstrain The default value for the value p Step 5 Reenable the 802.11a config 802.11h aenable network Step 6 See the status of 802. Show 802.11h Information similar to the followinp Power Constraint. Channel Switch. Modern Switch Mode	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. tion to save your changes. 2.11h Parameters using the controller CLI, follow these steps: etwork by entering this command: k access point to announce when it is switching 1 (enable disable) <i>switch_mode</i> <i>tich_mode parameter to</i> specify whether transi- nel using the 802.11h channel announcement I nnel channel power constraint value by entering this command: k value arameter is 3 dB. network by entering this command: 11h parameters by entering this command: 11h parameters by entering this command: 11h parameters of this command: 0 0 0	iobal Parameters page. to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and:
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to corr Step 7 Click Save Configure Using the CL1 to Configure 802 To configure 802.11h parameters To config 802.11h parameters Step 1 Desble the 802.11a no config 802.11a click able networf Step 2 Enable or disable the r config 802.11a click able networf Step 3 Configure a new chan config 802.11h setchannel cha Step 4 Configure the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h formation similar to the followin fower Constraint	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. tion to save your changes. 2.11h Parameters : using the controller CLI, follow these steps: etwork by entering this command: k access point to announce when it is switching t (enable disable <i>switch_mode</i> <i>itch_mode parameter to</i> specify whether transi- nel using the 802.11h channel announcement I nel channel power constraint value by entering this command: the value arameter is 3 dB. network by entering this command: 11h parameters by entering this command: 11 parameters by entering this command: 0 0	liobal Parameters page. to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and:
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to corr Step 7 Click Save Configure 802.11a configure 802.11b action 1000 Config 802.11b action 1000 Step 2 Click Save Configure 802.11a config 802.11a habe network Step 3 Configure a new chan config 802.11b stable network Step 4 Configure a new chan config 802.11b stable network Step 5 Configure a new chan config 802.11b stable network Step 5 Configure a new chan config 802.11b stable network Step 5 See the status of 802. Show 802.11b config 802.11b sectoansel and config 802.11b sectoansel and step 4 Configure the 802.11b config 802.11b sectoansel and step 5 See the status of 802. Show 802.11b stormation similar to the followin power Construit Int	your changes. band as follows:	slobal Parameters page. to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and: and: equests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the V and client are received on the upstream VLAN, converted to 802.11, and transmitted through a CAPWAP turnel toward be disabled only when required to bail basis, rather than on a WLAN basis. DHCP provy sitewo settler prove provo mode of operation. It should be disabled only when required to basis.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to corr Step 7 Click Save Configure 802 To configure 802.11h parameters Step 1 Disable the 802.11a config 802.11h channelswitch You can use the configure a new chan config 802.11h schannel of the sw Step 3 Configure a new chan config 802.11h schannel shall step 4 Configure a new chan config 802.11h schannel shall step 5 Reenable the 802.11h config 802.11h schannel shall step 5 Reenable the 802.11h config 802.11h schannel shall step 5 Reenable the 802.11h config 802.11h schannel shall step 5 Reenable the 802.11h config 802.11h schannel shall step 5 Reenable the 802.11h config 802.11h schannel shall config 802.11h schannel Switch Mode Channel Switch Mode Schannel Switch Mode Scharter and the schalled of Configuring DHCP Proxy When DHCP proy is enabled of WLAN isself.	your changes. band as follows:	slobal Parameters page. to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and: d d equests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the V and to and from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the V ad to and from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the V ad to and from the client are received on the upstream VAW, convented to BQL11, and transmitted through a CAPWAP turnet towal the client, As a result, the interface on the upstream VAW, convented to BQL11, and transmitted through a CAPWAP turnet towal the client, As a result, the interface basis, rather than on a WLAN basis. DHCP provy is enabled by default.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to corr Step 7 Click Save Configure 802 To configure 802.11h parameters Step 1 Disable the 802.11a config 802.11h parameters config 802.11h channelswitch You can enter a 0 or 1 for the sw Step 3 Configure a new chan config 802.11h setchannel cha Step 4 Configure a new chan config 802.11h percentation of the sw Step 3 Configure a new chan config 802.11h setchannel cha Step 4 Configure a new chan config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel and the followin Power Constraint	your changes. band as follows:	Iobal Parameters page. to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and: d equests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the W ed to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are remove d to the client are received on the upstream VLAN, converted to 802-11, and transmitted through a CAPWAP lume! toward the client. As a result, then inter basis, rather than on a WLAN basis. DHCP provy is enabled by default. :See the "Configuring DHCP Option 82" section for information on DHCP option 82.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configure Using the CLI to Configure 802 To configure 302.11h parameters Step 1 Disable the 20.11a config 802.11h channelswitch You can enter a 0 or 1 for the sw Step 3 Configure a new chan config 802.11h setchannel cha Step 4 Configure a new chan config 802.11h setchannel cha Step 4 Configure a new chan config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h Setchannel cha Step 5 Reenable the 802.11a config 802.11h Difformation similar to the followin Power Constraint Channel Switch Mode Channel Switch Mode Channel Switch Mode Reenabled on CAPWAP turnel and transmitted rever anna to use the controller GUI on PHCP proxy is enabled on CAPWAP turnel and transmitted Step 1 Configure 100.110 DHCP proxy is enabled on CAPWAP turnel and transmitted Step 1 Configure 100.110 DHCP proxy is enabled on DHCP proxy is enabled on DHCP proxy is enabled on CAPWAP turnel.	your changes. band as follows:	Isobal Parameters page. to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and: d aquests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the W ed to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are remove d to the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are remove d to the default drospit a CAPWWP turnel loward the default. As a result, the interface basis, rather than on a WLAN basis. DHCP provy is enabled by default. : See the "Configuring DHCP Option 82" section for information on DHCP option 82.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configure Jsing the CLI to Configure 802 To configure 802.11h parameters Step 1 Disable the 802.11a in config 802.11h parameters Config 802.11h channelswitch. You can enter a 0 or 1 for the sw Step 3 Configure a new chan config 802.11h setchannel cha Step 4 Configure a new chan config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h parameters be 5 Reenable the 802.11a config 802.11h setchannel cha Step 4 Configure a new chan config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h mformation similar to the followin Power Constrainth mformation similar to the followin Power Constrainth Moden	your changes. band as follows:	ideal Parameters page. to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and: d equests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the V ed to and from the client ser bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are received on the upstream VLAN, converted to 802-11, and transmitted through a CAPWAP turnel toward the client. As a result, the inter chail basis, rather than on a VLAN basis. DHCP proxy is enabled by default. : See the "Configuring DHCP Option 82" section for information on DHCP option 82.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to corr Step 7 Click Save Configure Jsing the CLI to Configure 802 To configure 802.11h parameters Step 1 Disable the 802.11a c. Config 802.11h parameters Step 2 Enable or disable the 102 Config 802.11h channelswitch. You can enter a 0 or 1 for the sw Step 3 Configure anew chan config 802.11h setchannel cha Step 4 Configure the 802.11h config 802.11h parameters Step 5 Reenable the 802.11h config 802.11h setchannel cha Step 4 Configure the 802.11h config 802.11h setchannel cha Step 5 Reenable the 802.11h config 802.11h step 5 Reenable the 802.11h config 802.11h mformation similar to the followin Power Constraint Channel Switch. Mode Channel Switch Mode Yuu can use the controller GUI of DHCP proxy must be enabled in Al controllers that will communic	your changes. band as follows:	idoal Parameters page. to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and: equests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the VM ed to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are received on the upstram VLMN, converted to 802.11, and transmitted through a CAPMVP hunnal toward the claim. As a result, the interface basis, rather than on a WLAN basis. DHCP provy is enabled by default. :See the "Configuring DHCP Option 82" section for information on DHCP option 82.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configure Jusing the CLI to Configure 802 To configure 802.11h parameters Step 1 Disable the 802.11a n config 802.11h parameters Config 802.11h channelswitch. You can enter a 0 or 1 for the sw Step 3 Configure a new chan config 802.11h setchannel cha Step 4 Configure a new chan config 802.11h setchannel cha Step 4 Configure a new chan config 802.11h setchannel cha Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 5 Reenable the 802.11h config 802.11h setchannel cha Step 5 Reenable the 802.11h config 802.11h mormation similar to the followin Power Constraint Nome DHCP proxy When DHCP proxy is enabled or WLAN Issit. When DHCP proxy is enabled in All controllers that will communic See "Configuring UHCP Proxy When DHCP proxy must be enabled in All controllers that will communic	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. titlen to save your changes. 2.11h Parameters using the controller CLI, follow these steps: twork by entering this command: k cacess point to announce when it is switching to (enable disable) <i>switch_mode</i> <i>itch_mode parameter to specify</i> whether trans- nel using the 802.11h channel announcement I mole channel power constraint value by entering this command: t value arameter is 3 dB. network by entering this command: 11h parameters by entering this command: 11 parameters by entering this command: 11 parameters by entering this command: 11 the controller, the controller unicasts DHCP re the controller, these DHCP packets transmission the upstream VLAN. DHCP packets directed CP proxy is disabled. The ability to disable DHC r cLI to enable or disable DHCP proxy entering, ate must have the same DHCP proxy setting. formation on configuring DHCP servers. ICP Proxy	ideal Parameters page. to a new channel and the new channel number by entering this command: releasions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. by entering this command: and: equests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the V of to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are removed to the default to be configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the V of to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are remove bab basis, rather than on a WLAN basis. DHCP proxy is enabled by default. :See the "Configuring DHCP Option 82" section for information on DHCP option 82.
Step 6 Reenable the 802.11a a. Choose Wireless : b. Select the 802.11a c. Click Apply to com Step 7 Click Save Configure Using the CLI to Configure 802 To configue 302.11h parameters Step 1 Disable the 20.11a config 802.11h channelswitch You can enter a 0 or 1 for the sw Step 3 Configure and the switch You can enter a 0 or 1 for the sw Step 3 Configure and the other switch You can enter a 0 or 1 for the sw Step 3 Configure and the other switch You can enter a 0 or 1 for the sw Step 3 Configure and the other switch You can enter a 0 or 1 for the sw Step 3 Configure and the other switch You can enter a 0 or 1 for the sw Step 3 Configure and the other switch You can enter a 0 or 1 for the sw Step 5 Reenable the 802.11a config 802.11h setchannel cha Step 4 Configure and the other switch Step 6 See the status of 802. show 802.11h Information similar to the following Power Constrainth Channel Switch Mode Configuring DHCP Proxy When DHCP proxy is enabled on UAN itself. All controllers that will communic All controllers that will communic Informations that will communic All configuring DHCP proxy is one should be and the other of the other othe	your changes. band as follows: • 802.11a/n > Network to open the 802.11a G Network Status check box. mit your change. tition to save your changes. 2.11h Parameters using the controller CLI, follow these steps: etwork by entering this command: k caccess point to announce when it is switching 1 (enable disable) <i>switch_mode</i> <i>tich_mode parameter to specify</i> whether trans- nel using the 802.11h channel announcement I mol channel power constraint value by entering this command: t value arameter is 3 dB. network by entering this command: 11h parameters by entering this by entering this command	ideal Parameters page. to a new channel and the new channel number by entering this command: missions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled. ty entering this command: and quests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the W of to and from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the W of to and from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the W of to and from the client to the configured servers. At least one DHCP server must be configured on either the interface associated with the W of to and from the client to the configured servers. At least one DHCP server must be configured on either the interface associated with the W of to and from the client to the configured servers that do not support Clico's native proxy mode of operation. It should be disabled only when required to Deal basis, rather than on a WLAN basis. DHCP proxy is enabled by default. : See the "Configuring DHCP Option 82" section for information on DHCP option 82.

	Sign Configuration Dirg Molection 12, Alls - country line - Witchings - configuration - Dirg	nge it i <u>S</u> eferan
Gontroller	DHCP Parameters	Apply
General		
Inventory	Linatis DIRCP From M	
Interfaces	DHCP Culue i 82 Rain ule Julia I. Le Jilur ne. 🛛 🗛 VAC 🛛 🤟	
Step 2 Select the Enable DHCP	Proxy check box to enable DHCP proxy on a global basis. Otherwise, unselect the check box. The default value is selected.	2
Step 3 Click Apply to commit you	ur changes.	
Step 4 Click Save Configuratio	in to save your changes.	
sing the CLI to Configure DHCP	Proxy	
Step 1 Enable or disable DHCP	controller CLL, tollow these steps: 	
config dhcp proxy { enable disa	ble)	
Step 2 View the DHCP proxy con	nfiguration by entering this command:	
show dhcp proxy	nneare	
DHCP Proxy Behavior: enabl	.ed	
onfiguring Administrator Us∉	ernames and Passwords	
You can configure administrator use	imames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information. This section provides instructions for initial configuration an	nd for password recover
onfiguring Usernames and Pase To configure administrator username	swords es and passwords using the controller CLL follow these steps:	
Step 1 Configure a username an	d password by entering one of these commands:	
 config mgmtuser add username) password read-write—Creates a username-password pair with read-write privileges.	
config mgmtuser add username	a password read-only—Creates a username-password pair with read-only privileges.	
Usernames and passwords are case	a-sensitive and can contain up to 24 ASCII characters. Usernames and passwords cannot contain spaces.	
Note If you ever need to ch	ange the password for an existing username, enter the config mgmtuser password username new_password command.	
Step 2 List the configured users	by entering this command:	
show mgmtuser		
estoring Passwords		
To configure a new username and p	assword at boot-up using the controller CLI, follow these steps:	
Step 1 After the controller boots	up, enter Restore-Password at the User prompt.	
N		
Note For security reasons,	the text that you enter does not appear on the controller console.	
Step 2 At the Enter User Name p	vrompt, enter a new username.	
Sten 3 At the Loter Header		
Step 4 At the Re-enter Password pri	ompt, enter a new password.	
Step 4 At the Re-enter Password ph Step 5 When the User prompt res	ompt, enter a new password. J prompt, reenter the new password. The controller validates and stores your entries in the database. appears, enter your new usemame.	
Step 4 At the Re-enter Password pri Step 5 When the User prompt res Step 6 When the Password prom	ompt, enter a new password. 1 prompt, reenter the new password. The controller validates and stores your entries in the database. 1appears, enter your new usemame. 1pt appears, enter your new password. The controller logs you in with your new username and password.	
Step 5 As the Enter Password pri Step 5 When the User prompt res Step 5 When the Password prom	ompt, enter a new password. J prompt, reenter the new password. The controller validates and stores your entries in the database. appears, enter your new usemame. npt appears, enter your new password. The controller logs you in with your new usemame and password.	
Step 4 At the Re-enter Password print Step 5 When the User prompt re- Step 6 When the Password prom	ompt, enter a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. iappears, enter your new usemame. npt appears, enter your new password. The controller logs you in with your new usemame and password.	
Step 4 At the Re-enter Password Ph Step 4 At the Re-enter Password Step 5 When the User prompt re Step 6 When the Password prom Configuring SNMP To configure SNMP using the control	ompt, enter a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. appears, enter your new usemame. rpt appears, enter your new password. The controller logs you in with your new usemame and password.	
Step 4 At the Re-enter Password Ph Step 4 At the Re-enter Password Step 5 When the User prompt re Step 6 When the Password prom Configuring SNMP To configure SNMP using the control Step 1 Enter the config snmp cor	ompt, entre a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. iappears, enter your new usemame. pt appears, enter your new password. The controller logs you in with your new usemame and password	
Corp. A die Eine Hassword pri Step 4 At the Re-enter Password Step 5 When the User prompt re Step 5 When the Vaser prompt re Step 6 When the Password prom onfiguring SNMP To configure SNMP To configure SNMP using the control Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor	ompt, enter a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. pt appears, enter your new password. The controller logs you in with your new usemame and password	
Step 4 At the Re-enter Passwort Step 4 At the Re-enter Passwort Step 5 When the User prompt re Step 6 When the Passwort promoting Configuring SNMP To configure SNMP using the control Step 1 Enter the config samp cor Step 2 Enter the config samp cor Step 3 Enter the config samp cor Step 4 Enter the config samp cor	ompt, enter a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. pt appears, enter your new password. The controller logs you in with your new usemame and password	mmunity name
Step 4 At the Re-enter Passwort Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Passwort promoting and the passwort promoting an	ompt, enter a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. pt appears, enter your new password. The controller logs you in with your new usemame and password.	mmunity name
Step 4 At the Re-enter Password ph Step 4 At the Re-enter Password Step 5 When the User prompt re Step 6 When the Password pron Configuring SNMP To configure SNMP using the contro Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor with read-wite privileges. Step 4 Enter the config snmp cor	ompt, enter a new password. d prompt, reenter the new password. for a new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. pt appears, enter your new password. The controller logs you in with your new usemame and password.	mmunity name
A die Eine Hasswold pri Step 4 At the Re-enter Password Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password pron onfiguring SNMP To configure SNMP using the contro Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor with read-wite privileges. Step 4 Enter the config snmp cor Note This command behave being corperated to the factors of the control of the co	ompt, enter a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. npt appears, enter your new password. The controller logs you in with your new usemame and password	mmunity name
Step 4 At the Re-enter Password ph Step 4 At the Re-enter Password ph Step 5 When the User prompt re Step 5 When the Password pron onfiguring SNMP To configure SNMP using the contro Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor with read-write privileges. Step 4 Enter the config snmp cor with read-write privileges. Step 4 Enter the config snmp cor who This command behave being compared to the	ompt, enter a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. npt appears, enter your new password. The controller logs you in with your new usemame and password. 	mmunity name
Step 4 At the Re-enter Password prives Step 4 At the Re-enter Password Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password pron Onfiguring SNMP To configure SNMP using the control Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor wher the config snmp cor with read-write privileges. Step 4 Enter the config snmp cor whore This command behave Note This controller can use Note The controller can use	ompt, enter a new password. d prompt, reenter the new password. poly centroller validates and stores your entries in the database. sappears, enter your new usemame. poly appears, enter your new password. The controller logs you in with your new usemame and password	mmunity name
Step 4 At the Re-enter Password private and the sense relative to the sense relative to the sense of the	ompt, energ a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. npt appears, enter your new password. The controller logs you in with your new usemame and password.	mmunity name
Step 4 At the Re-enter Password private and the sense relative to the sense of	ompt, reeriter the new password. d prompt, reeriter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. npt appears, enter your new password. The controller logs you in with your new usemame and password.	mmunity name
Step 4 At the Re-enter Password pin Step 4 At the Re-enter Password Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password pron Onfiguring SNMP To configure SNMP using the control Step 1 Enter the config snmp cor with read-write privileges. Step 2 Enter the config snmp cor with read-write privileges. Step 4 Enter the config snmp cor Note This command behav being compared to th Note The config snmp cor Step 5 Enter the config snmp cor Step 5 Enter the config snmp cor Step 5 Enter the config snmp cor Step 6 Enter the config snmp cor Step 6 Enter the config snmp cor Step 6 Enter the config snmp cor Step 7 Enter the config snmp cor Step 7 Enter the config snmp cor Step 7 Enter the config snmp cor	ompt, reerter the new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. mpt appears, enter your new password. The controller logs you in with your new usemame and password.	mmunity name
Step 4 At the Re-enter Password prives Step 4 At the Re-enter Password Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password prive To configure SNMP To configure SNMP To configure SNMP To configure SNMP Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor wher teach-write privileges. Step 4 Enter the config snmp cor Note This command behave being compared to the Note The config snmp cor Step 5 Enter the config snmp cor Step 5 Enter the config snmp cor Step 5 Enter the config snmp cor Step 6 Enter the config snmp cor Step 7 Enter the config snmp cor Step 7 Enter the config snmp tra Step 8 Enter the config	ompt, reerter the new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. mpt appears, enter your new password. The controller logs you in with your new usemame and password.	mmunity name
Step 4 At the Re-enter Password prin Step 4 At the Re-enter Password prin Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password prin To configure SNMP To configure SNMP Step 1 Enter the config snmp con Step 5 Enter the config snmp tra Step 7 Enter the config snmp tra Step 9 Enter the config snmp tra	ompt, reerter the new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. pt appears, enter your new password. The controller logs you in with your new usemame and password.	mmunity name
Step 4 At the Re-enter Password private and the server provides the server provides of the server provides of the server provides of the server provides and the server private serve	tompt, reenter the new password. The controller validates and stores your entries in the database. appears, enter your new password. The controller validates and stores your entries in the database. prot appears, enter your new password. The controller logs you in with your new usemane and password. plater CLI, follow these steps: mmunity create name command to delete an SNMP community name. mmunity create name command to delete an SNMP community name. mmunity create name command to configure an SNMP community name. mmunity creates is enter your new password to configure an P address and subnet mask for an SNMP community. ensities an SNMP access list. It specifies the IP address from which the device accepts SNMP packets with the associated community. The requesting entity's IP address is ANDed with the IP address. If the subnet mask is set to 0.0.0, an IP address of 0.0.0.0 matches to all IP addresses. The default value is 0.0.0. e only one IP address range to manage an SNMP community name. Enter the config snmp community name. preceiver radet came ip-address name new-ip-address command to configure a trap. preceiver mode enable command to delete a tapp. preceiver mode enable command to delete a tapp. preceiver mode enable command to configure a destination for a trap. preceiver mode enable command to delete a tapp. preceiver mode enable command to enable traps. Enter the config snmp community mode disable traps. preceiver mode enable command to enable traps. Enter the config snmp trapreceiver mode disable traps. preceiver mode enable command to enable traps. Enter the config snmp trapreceiver mode disable traps. preceiver mode enable command to enable traps. preceiver mode enable command to enable traps. Enter the config snmp trapreceiver mode disable traps. preceiver mode enable command to enable traps. preceiver paddress for the configure the name of the SNMP contact. Enter up to 31 alphanumeric characters for the contact name.	mmunity name
Step 4 At the Re-enter Password pin Step 4 At the Re-enter Password pin Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password pin To configure SNMP To configure SNMP using the control Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor When the This command behave being compared to fit Note This controller can us Step 5 Enter the config snmp train Step 5 Enter the config snmp train Step 6 Enter the config snmp train Step 7 Enter the config snmp train Step 8 Enter the config snmp train Step 9 Enter the config snmp train Step 9 Enter the config snmp train Step 9 Enter the config snmp train Step 1 Enter the config snmp train	tompt, reenter the new password. The controller validates and stores your entries in the database. appears, enter your new password. The controller validates and stores your entries in the database. papears, enter your new password. The controller logs you in with your new usemane and password. papears, enter your new password. The controller logs you in with your new usemane and password. papears, enter your new password. The controller logs you in with your new usemane and password. papears, enter your new password. The controller logs you in with your new usemane and password. papears, enter your new password. The controller logs you in with your new usemane and password. papears, enter your new password. The controller logs you in with your new usemane and password. papears, enter your new password. The controller logs you in with your new usemane and password. papears, enter your new password. The controller logs you in with your new usemane and password. papears, enter your new password. The controller logs you in with your new usemane and password. papears, enter your new password. The controller logs you in with your new usemane and password. papears, enter your new password. papears, enter your papears, enter the configure an SNMP community. proceiver padress range to manage an SNMP community. proceiver padress in the padress range to configure a destination for a trap. proceiver padre enable command to enable traps. proceiver padre enab	mmunity name
Step 2 A the Re-enter Password pri Step 4 At the Re-enter Password pri Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password pron To configure SNMP To configure SNMP To configure SNMP using the contro Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor with read-with privileges. Step 4 Enter the config snmp cor Note This command behav being compared to fit Note The controller can use Step 5 Enter the config snmp tra Step 8 Enter the config snmp tra Step 9 Enter the config snmp tra Step 10 Enter config snmp star Step 10 Enter config snmp star Step 10 Enter config snmp star Step 10 Enter the config snmp star Step 11 Enter the config snmp star Step 12 Use the show snmpcom	tompt, reenter the new password. The controller validates and stores your entries in the database. appears, enter your new password. The controller validates and stores your entries in the database. appears, enter your new password. The controller logs you in with your new usemane and password. appears, enter your new password. The controller logs you in with your new usemane and password. alter CLI, follow these steps: mmunity create name command to create an SNMP community name. mmunity create name command to create an SNMP community name. mmunity create name command to configure an SNMP community name. mmunity paddr ip-address ip-mask name command to configure an IP address and subnet mask for an SNMP community. estiles an SNMP access list. It specifies the IP address from which the device accepts SNMP packate with the associated community. The requesting entity's IP address is ANDed with the IP address. If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches to all IP addresses. The default value is 0.0.0.0. e only one IP address range to manage an SNMP community. mmunity mode enable command to configure a destination for a trap. preceiver create name ip-address command to configure a trap. preceiver create name ip-address command to configure the destination for a trap. preceiver address in ame command to enable traps. Enter the config snmp community mode disable command to disable a community name. preceiver delete name command to enable traps. Enter the config snmp community mode disable command to disable traps. preceiver delete name command to enable traps. Enter the config snmp community mode disable command to disable traps. preceiver delete name ip-address command to change the destination for a trap. preceiver address name new-ip-address command to change the destination for a trap. preceiver delete name ip-address command to configure the config snmp trapreceiver mode disable command to disable traps. praceiver delete name. preceiver address for the config snmp t	mmunity name
Step 4 At the Re-enter Password ph Step 4 At the Re-enter Password ph Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password pron To configure SNMP To configure SNMP To configure SNMP using the control Step 1 Enter the config snmp cor with read-write privileges. Step 4 Enter the config snmp cor Whote This command behave being compared to 11 Note The controller can use Step 5 Enter the config snmp tra Step 7 Enter the config snmp tra Step 8 Enter the config snmp tra Step 8 Enter the config snmp tra Step 8 Enter the config snmp tra Step 9 Enter the config snmp tra Step 10 Enter config snmp space Step 10 Enter config snmp space Step 11 Enter the config snmp space Step 12 Use the show strapfords	tomp, enter a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. mpl appears, enter your new password. The controller logs you in with your new usemame and password. alter CLI, follow these steps: mmunity create name command to create an SNMP community name. mmunity create name command to configure an SNMP community name. mmunity create name command to configure an SNMP community name with read-only privileges. Enter config smp community accessmode nw name to configure an SNMP com- mmunity create name command to configure an IP address and subnet mask for an SNMP community.	mmunity name
Step 4 At the Re-enter Password pro- Step 4 At the Re-enter Password pro- Step 5 When the User prompt re- Step 6 When the User prompt re- Step 6 When the Password pron- Configure SNMP To configure SNMP using the control Step 1 Enter the config annp cor- Step 2 Enter the config annp cor- with read-write privileges. Step 4 Enter the config annp cor- with read-write privileges. Step 5 Enter the config annp tra Step 5 Enter the config annp tra Step 8 Enter the config annp tra Step 10 Enter the config annp tra Step 11 Enter the config annp tra Step 13 Use the show trapflage of	tomp, there a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemame. rpt appears, enter your new password. The controller logs you in with your new usemame and password. alter CLI, follow these steps: mmunity create name command to create an SNMP community name. mmunity create name command to create an SNMP community name. mmunity delete name command to configure an SNMP community name with read-only privileges. Enter config smp community accessmode nv name to configure an SNMP community name with read-only privileges. Enter config smp community accessmode nv name to configure an SNMP community name with read-only privileges. Enter config smp community accessmode nv name to configure an SNMP community name with read-only privileges. Enter config smp community accessmode nv name to configure an SNMP community name with read-only privileges. Enter config smp community accessmode nv name to configure an SNMP community. Termunity ipaddrises ip-mask name command to configure an IP address and subnet mask for an SNMP community. The requesting entity's IP address is a ND-0.0.0 an IP address of 0.0.0.0 matches to all IP addresses. The default value is 0.0.0.0. Termunity indee enable command to enable to passe of 0.0.0.0 matches to all IP addresses. The default value is 0.0.0.0. The requesting entity's IP address is a ND-0.0.0 matches to all IP addresses. The default value is 0.0.0.0. Termunity mode enable command to enable a community name. Enter the config snmp community mode disable command to disable a community name. preceiver create name ip-address command to change the destination for a trap. preceiver mode enable command to enable traps. Enter the config snmp trapreceiver mode disable command to disable traps. stat syscottact-name to configure the name of the SNMP contact. Enter up to 31 alphanumeric characters for the location. manity and the show smptrap command to verify that the SNMP traps and commu	mmunity name
Step 2 A the Re-enter Password pro Step 4 At the Re-enter Password pro Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password pron To configure SNMP To configure SNMP using the contro Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor with read-with privileges. Step 4 Enter the config snmp cor Note This command behave being compared to fit Note The controller can use Step 5 Enter the config snmp tra Step 8 Enter the config snmp tra Step 1 Enter the config snmp tra Step 10 Enter config snmp stor Step 10 Enter config snmp stor Step 11 Enter the config snmp stor Step 13 Use the show straptcars	torp, ener a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. sappears, enter your new usemane. mpt appears, enter your new password. The controller logs you in with your new usemane and password. alter CLI, follow these steps: mmunity create name command to create an SNMP community name. mmunity create name command to create an SNMP community name. mmunity delete name command to create an SNMP community name. mmunity delete name command to configure an SNMP community name. mmunity delete name command to configure an SNMP community name. mmunity accessinger to configure an SNMP community name. mmunity accessinger to name command to configure an SNMP community name with read-only privileges. Enter config snmp community accessinger on name to configure an SNMP community.	mmunity name
Step 2 A the Re-enter Password pri Step 4 At the Re-enter Password pri Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password pron To configure SNMP To configure SNMP using the control Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor with read-with privileges. Step 4 Enter the config snmp cor Note This command behave being compared to fit Note The controller can usis Step 5 Enter the config snmp tra Step 8 Enter the config snmp tra Step 8 Enter the config snmp tra Step 8 Enter the config snmp tra Step 1 Enter the config snmp tra Step 1 Enter the config snmp tra Step 2 Enter the config snmp tra Step 3 Enter the config snmp tra Step 10 Enter config snmp sysc Step 11 Enter the config snmp sysc Step 13 Use the show strapfcage of hanging the Default Values of The controller has commonly known	torp, treft a new password. d prompt, reenter the new password. The controller validates and stores your entries in the database. appears, enter your new usemane. rpt appears, enter your new password. The controller logs you in with your new usemane and password.	mmunity name
Step 2 At the Re-enter Password pri Step 4 At the Re-enter Password pri Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password prior To configuring SNMP To configure SNMP using the control Step 1 Enter the config snmp cor Step 2 Enter the config snmp cor with read-with privilegas. Step 4 Enter the config snmp cor Note The controller can usis Step 5 Enter the config snmp tra Step 8 Enter the config snmp tra Step 8 Enter the config snmp tra Step 1 Enter the config snmp tra Step 5 Enter the config snmp tra Step 5 Enter the config snmp tra Step 8 Enter the config snmp tra Step 1 Use the show snmpcom Step 13 Use the show snmpcom Step 13 Use the show trapflags con hanging the Default Values on The controller has commonly known are known, the community names can sing the GUI to Change the SNM	torpit, refer a new password. The controller validates and stores your entries in the database. appears, enter your new usemame. pri appears, enter your new usemame. pri appears, enter your new password. The controller logs you in with your new usemame and password. adder CLL follow these steps: mmunity create name command to create an SNMP community name. mmunity create name command to create an SNMP community name. mmunity create name command to create an SNMP community name. mmunity create name command to create an SNMP community name. mmunity create name command to create an SNMP community name. mmunity create name command to create an SNMP community name. mmunity create name command to create an SNMP community name with read-only privileges. Enter config snmp community accessmode rv name to configure an SNMP community name with read-only privileges. Enter config snmp community accessmode rv name to configure an SNMP community name with read-only privileges. The default value is 0.0.0.0. mmunity ipaddress ip-mask name command to configure an P address and subnet mask for an SNMP community. meases and subnet mask is set to 0.0.0.0. an P address of 0.0.0.0 matches to all P addresses. The default value is 0.0.0.0 e only one P address range to manage an SNMP community. mmunity mode enable command to enable a community. mmunity mode enable command to enable a community. preceiver drete name (p-address command to configure a destination for a trap. preceiver fields name command to actingure a destination for a trap. preceiver drete name (p-address command to configure and to change the destination for a trap. preceiver drete name (p-address command to enable traps. Enter the config snrp trapreceiver mode disable command to disable traps. preceiver drete name (p-address command to configure a destination for a trap. preceiver drete name (p-address command to configure a destination for a trap. preceiver redee name (p-address command to configure the SNMP contact. Enter up to 31 aphanumeric chanacter	nmunity name
Step 4 At the Re-enter Password pri Step 4 At the Re-enter Password pri Step 5 When the User prompt re Step 5 When the User prompt re Step 6 When the Password prior To configure SNMP To configure SNMP using the control Step 1 Enter the config simp cor with read-write privileges. Step 2 Enter the config simp cor with read-write privileges. Step 4 Enter the config simp cor Note The command behave being compared to fit Note The controller can use Step 5 Enter the config simp tra Step 10 Enter config simp size Step 11 Enter the config simp size Step 13 Use the show simpcom Step 13 Use the show simpcom Step 14 Use the sommonly known are known, the community known are known, the community known are known, the community known are known, the community sime can Step 10 It Change the SNMP Contained the SNMP community affect	torpi, treft a new password. The controller validates and stores your entries in the database. appears, enter your new usemane. top appears, enter your new password. The controller logs you in with your new usemane and password. The controller logs you in with your new usemane and password. alter CLI, follow these steps: mountly create name command to create an SNMP community name. mrountly create name command to create an SNMP community name. mrountly create name command to create an SNMP community name. mrountly create name command to create an SNMP community name. mrountly create name command to create an SNMP community name. mrountly create name command to create an SNMP community name. mrountly create name command to configure an SNMP community name with read-only privileges. Enter config snmp community, accessmode rv name to configure an SNMP com- munity define have command to configure an P address and subnet mask for an SNMP community. The states is the subnet mask is set to 0.0.0.0. m P address of 0.0.0.0 matches to all P addresses. The default value is 0.0.0.0. The P address is a NAMP access list. It specifies the P address if on which the device accepts SNMP packets with the associated community. The requesting entity's P address is ANDed with the P address. If the subnet mask is set to 0.0.0.0. m P address of 0.0.0.0 matches to all P addresses. The default value is 0.0.0.0. The precisive define anne command to entities a community. mrounty mode enable command to enable a community name. Enter the config snmp community mode disable command to disable a community name. precisiver greater name (p-address command to configure a destination for a trap. precisiver define name command to define traps. Precisiver greater index command to address a command to change the destination for a trap. precisiver define the name of the SNMP cotact. Enter up to 31 alphanumeric characters for the location. munity and the shows snrptrap commands to verify that the SNMP cotact. Enter up to 31 alphanu	mmunity name

Janagement			PRELESS SEC IPITY	Renarrienen	OMMANDS.	HELD		
A REAL PROPERTY AND ADDRESS OF A REAL PROPERTY.	SNMP v1 / v2c (Community		CANCELOW AND ADDRESS OF			NDW	
Value and	THE THE L							
* SNMP	Community Name	IP Add	Iness IP Mask	Access Node 4 Food Taly	Status			
Gamenal SNMP 2011 Jacks	private	2018	JULIE AS ASSESS	4 Ford Write	Foot o	0		
Lommun ties							~	
trap Ceceivers trap Controls							5	
tep 2 If "public" or "private	appears in the Community	Name column, hover you	r cursor over the blue drop-	down arrow for the desir	ed community a	nd choose Remove	to delete this commu	nity.
tep 3 Click New to create	a new community. The SNM	P v1 / v2c Community > N	lew page appears (see Figu	ire 4-18).				
re 4-18 SNMP v1 / v2c Cor	nmunity > New Page							
ahaha					Seza Coni	garation Brig	Lugar <u>E</u> eltest	
CISCO	MONITOF W AN	OCATEC LER W	VIERI RSS SECURITY	MANAGEMENT C	<u>O</u> MMANDS	HELT		
Vanagement	SNMP v1 / v2c 0	Community > New				< Back	Apply	
Summary	Curranurally Nam	ne [
T SNMP Concral	IV Address		1					
SHMP V3 Juers	a Huncos		_					
Trap Receivers	TP Mask	- <u></u>						
Trap Lugs	Access Mode	Reau Cile 💻						
HILP	Status						7	1
Teinet SSH Secial Decl	and the second	Tenere (21)					53	
Step 4 In the Community Na	ame text box, enter a unique	name containing up to 16	alphanumeric characters. [Do not enter "public" or "	private."		À	J
Step 5 In the next two text b	oxes, enter the IP address f	rom which this device acc	epts SNMP packets with the	associated community	and the IP mas	c		
Step 6 Choose Read Only	or Read/Write from the Acce	ss Mode drop-down list to	specify the access level for	this community.				
Step 7 Choose Enable or D	isable from the Status drop-	down list to specify the sta	atus of this community.	-				
Step 8 Click Apply to comm	it your changes.							
Step 9 Click Save Configur	ation to save your settings.							
Stop 10 Banast this proped	ura if a "public" or "private"	oommunitu atill oonoom ou	the SNMD of (see Comm	wity pogo				
ow snmp community		munity Name column ent	ter this command to delete t	his community:				
Step 2 If "public" or "private	" appears in the SNMP Con name	inanty Name column, on						
Step 2 If "public" or "private infig snmp community delete ne name parameter is the cor Step 3 Create a new comm	" appears in the SNMP Con name nmunity name (in this case, ' unity by entering this comma	"public" or "private").						
Step 2 If "public" or "private nfig snmp community delete te name parameter is the cor Step 3 Create a new comm nfig snmp community create	" appears in the SNMP Con name nmunity name (in this case, " unity by entering this comma name	"public" or "private"). ind:		,				
Step 2 If "public" or "private nfig snmp community delete le name parameter is the cor Step 3 Create a new comm nfig snmp community create iter up to 16 alphanumeric ch	" appears in the SNMP Con name nmunity name (in this case, unity by entering this comma name name	"public" or "private"). Ind: neter. Do not enter "public	" or "private."					
Step 2 If "public" or "private nflig snmp community delete he name parameter is the cor Step 3 Create a new comm nflig snmp community create hter up to 16 alphanumeric ch Step 4 Enter the IP address	" appears in the SNMP Com name nmunity name (in this case, ' unity by entering this comma name arracters for the name paran from which this device acce	'public" or "private"). ind: neter. Do not enter "public pts SNMP packets with th	" or "private." ne associated community by	entering this command				
Step 2 If "public" or "private infig snmp community delete the name parameter is the cor Step 3 Create a new comm infig snmp community create iter up to 16 alphanumeric d Step 4 Enter the IP address infig snmp community ipaddr	^a appears in the SNMP Conname mmunity name (in this case, mmunity name (in this case, name aracters for the name paran from which this device acce ip_address ip_mask name	"public" or "private"). ind: neter. Do not enter "public spts SNMP packets with th	" or "private." ne associated community by	entering this command				
Step 2 II "public" or "private nfig snmp community delete te name parameter is the cor Step 3 Create a new comm nfig snmp community create ter up to 16 alphanumeric ch Step 4 Enter the IP address nfig snmp community ipaddf Step 5 Specify the access I	Tappears in the SNMP Con name munity name (in this case, munity by entering this comme name aracters for the name paran from which this device accc <i>ip_address ip_mask name</i> evel for this community by en- agemetic (<i>i</i> = this community by en- agemetic (<i>i</i> = this community by en- tering the second second second second the second	"public" or "private"). ind: neter. Do not enter "public pts SNMP packets with th ntering this command, who	" or "private." ne associated community by ere ro is read-only mode an	rentering this command				
Step 2 II "public" or "private drifig smmp community delete in same parameter is the cor Step 3 Create a new comm nifig smmp community create ther up to 16 alphanumeric of Step 4 Enter the IP address nifig smmp community addr Step 5 Specify the access i infig smmp community addr Step 6 Enable or disable th	^a appears in the SNMP Conname name mounting name (in this case, unity by entering this comma name aracters for the name paran from which this device accc <i>ip_address ip_mask name</i> evel for this community by enter essmode (ro rw) by enter S SNMP community by enter	"public" or "private"). ind: ind: ind: SNMP packets with the retering this command, who	" or "private." ne associated community by ere ro is read-only mode an	entering this command				
Step 2 II "public" or "private rifig smmp community delete ter name parameter is the cor Step 3 Create a new comm nifig smmp community create ter up to 16 alphanumeric C Step 4 Enter the IP address nifig smmp community address Nifig smmp community acc Step 6 Enable or disable th nifig smmp community mo	appears in the SNMP Conname name mounting name (in this case, unity by entering this comme name aracters for the name paran from which this device acct ip_address ip_mask name evel for this community by enter essmode (ro rw) name s SNMP community by enter de (enable) (disable) name	"public" or "private"). ind: neter. Do not enter "public upps SNMP packets with th netring this command, who ring this command: ne	" or "private." ne associated community by ere ro is read-only mode an	entering this command				
Step 2 II "public" or "private offig smmp community delete ter up to 16 alphanumeric C 1 Step 3 Createt a new comm offig smmp community greate ter up to 16 alphanumeric C Step 4 Enter the IP address offig smp community and Step 5 Specify the access I mfig smmp community and Step 7 Save your changes	appears in the SNMP Conname name mounty name (in this case, ' unity by entering this comma- name aracters for the name parant from which this device accc ip_address ip_mask name evel for this community by enter de (enable disable) nam by entering save config.	"public" or "private"). ind: neter. Do not enter "public upts SNMP packets with th netring this command, whe ring this command: 19	" or "private." ne associated community by are ro is read-only mode an	entering this command				
Step 2 II "public" or "private infig samp community delete is name parameter is the cor Step 3 Create a new comm infig samp community create ter up to 16 alphanumeric d Step 4 Enter the IP address Step 5 Specify the access I infig samp community acc Step 6 Enable or disable th infig samp community and Step 7 Save your changes Step 8 Repeat this procedu	appears in the SNMP Conname name mounting the case, if unity by entering this comma- name aracters for the name parant from which this device accc ip_address ip_mask name evel for this community by enter desmode (ro rw) name s SNMP community by enter de (enable datable) nam by entering save config. re if you still need to change	"public" or "private"). ind: neter. Do not enter "public upts SNMP packets with th netring this command, who ring this command: ne the default values for a "p	" or "private." ne associated community by are ro is read-only mode an public" or "private" commun	entering this command d rw is read/write mode: ity string.				
Step 2 II "public" or "private rinfig samp community delete ter up to 16 alphanumeric of Step 3 Create a new comm nifig samp community create ter up to 16 alphanumeric of Step 4 Enter the IP address rinfig samp community and step 5 Specify the access I nifig samp community and Step 6 Enable or disable th rinfig samp community and Step 7 Save your changes Step 8 Repeat this procedu	appears in the SNMP Conname name mounting name (in this case, ' unity by entering this comma- name aracters for the name parant from which this device accc ip_address ip_mask name evel for this community by en- essmode (ro rw) name s SNMP community by enter de (enable de (enable data)) by entering save config. re if you still need to change	"public" or "private"). ind: neter. Do not enter "public upts SNMP packets with th netring this command, who ring this command: ne the default values for a "p	" or "private." ne associated community by are ro is read-only mode an public" or "private" commun	entering this command d rw is read/write mode: ity string.				
Step 2 II "public" or "private onfig samp community delete name parameter is the cor Step 3 Create a new comm infig samp community create ter up to 16 alphanumeric ol Step 4 Enter the IP address mitig samp community and Step 5 Specify the access i writig samp community and Step 5 Rable or disable th nfig samp community mo Step 7 Save your changes Step 8 Repeat this proceed unging the Default Value e controller uses a default values.	" appears in the SNMP Con name mounting name (in this case," unity by entering this comme arracters for the name paran from which this device acce <i>ip_address ip_mask name</i> evel for this community by enter de (enable) disable) <i>nam</i> s SNMP community by enter de (enable) disable) <i>nam</i> by entering save config. re if you still need to change	"public" or "private"), and: neter. Do not enter "public pts SNMP packets with th netering this command, whe ring this command: neter default values for a " name, authentication pass	" or "private." ne associated community by are ro is read-only mode an public" or "private" commun public" or "private" commun	entering this command d rw is read/write mode: ity string.	sing these stand	lard values present	s a security risk. Ther	efore, Cisco strongly advises that you c
Step 2 II "public" or "private fng smp community delete a mane parameter is the cor Step 3 Create a new comm nfg smp community create ter up to 16 alphanumeric cl Step 4 Enter the IP address nfig smp community inaddr Step 5 Specify the access I nfig smp community acc Step 6 Enable or disable th nfig smp community mo Step 7 Save your changes Step 8 Repeat this procedu anging the Default Value to entertaler uses a default vi- ues.	" appears in the SNMP Con name mounting name (in this case, unity by entering this comma arane ararders for the name paran from which this device acce <i>ip_address ip_mask name</i> evel for this community by enter essmode (ro rw) name essmode (r	"public" or "private"). Ind: neter. Do not enter "public typts SNMP packets with the netering this command, when ring this command: the default values for a " harme, authentication passes where the operation of the second sec	" or "private." he associated community by ere ro is read-only mode an public" or "private" commun sword, and privacy passwor	entering this command d nv is read/write mode: ity string; d for SNMP v3 users. U:	sing these stand	lard values present	s a security risk. Ther	efore, Cisco strongly advises that you c
Step 2 II "public" or "private rhifg smpc community delete is name parameter is the cor Step 3 Create a new comm nifg smpc community create ther up to 16 alphanumeric of Step 4 Enter the IP address nifg smpc community access I milg smpc community most Step 5 Specify the access I milg smpc community most Step 5 Sheely the access I step 6 Enable or disable th nifg smpc community most Step 7 Save your changes Step 8 Repeat this procedu anging the Default Value to extend or uses a default value to extend or uses a default value. NMP v3 is time sensitive. Ma	" appears in the SNMP Con name mounting name (in this case," unity by entering this comma arane ararders for the name paran from which this device acce <i>ip_address ip_mask name</i> evel for this community by enter de semode (ro rw) name essmode (ro 	"public" or "private"). Ind: neter. Do not enter "public pts SNMP packets with th netering this command, whe ring this command: the default values for a " name, authentication pass gured the correct time and	" or "private." re associated community by ere ro is read-only mode an public" or "private" commun sword, and privacy passwor time zone on your controlle	entering this command d nv is read/write mode: ity string; d for SNMP v3 users. U: r.	sing these stand	fard values present	s a security risk. Ther	efore, Cisco strongly advises that you c
Step 2 II "public" or "private fnfg smmp community delete is name parameter is the cor- Step 3 Create a new comm fnfg smmp community create ter up to 16 alphanumaric cl Step 4 Enter the IP address nfig smmp community acc Step 4 Enter the IP address step 5 Specify the access 1 step 6 Enable or disable th nfig smmp community mo Step 7 Sive your changes Step 8 Repeat this procedu anging the Default Value te controller uses a default vi- lues. WMP v3 is time sensitive. Ma ng the GUI to Change the change the SMMP v3 user of	" appears in the SNMP Con name mount name (in this case, unity by entering this comme aracters for the name param from which this device accc <i>ip.address (ip_mask name</i> ever for this community by enter de (enable disable) nam by entering save config. re if you still need to change es for SNMP v3 Users alue of "default" for the usen kes sure that you have config SNMP v3 User Default V	"public" or "private"). Ind: neter. Do not enter "public pts SNMP packets with the netering this command, who ring this command: the default values for a "p name, authentication pass pured the correct time and alues roller GUI, follow these st	" or "private." e associated community by ere ro is read-only mode an public" or "private" commun sword, and privacy passwor time zone on your controlle eps:	entering this command d nv is read/write mode: ity string. d for SNMP v3 users. U:	sing these stand	fard values present	s a security risk. Then	efore, Cisco strongly advises that you c
Step 2 II "public" or "private fng smmp community delete a mane parameter is the cor- Step 3 Create a new comm fng smmp community create ter up to 16 alphanumeric d Step 4 Enter the IP address Step 4 Enter the IP address Step 5 Enable or disable th fng smmp community acc Step 5 Enable or disable th fng smmp community mo Step 7 Save your changes Step 8 Repeat this procedu uses. Step 1 Choche address Step 1 Choche address Step 1 Save your changes Step 8 Repeat this procedu uses. MIP v3 Is time sensitive. Ma ng the DU to Change the stange the SNMP v3 user c Step 1 Choce Manageme	appears in the SNMP Conname name mounting name (in this case, unity by entering this comma arane aracters for the name paran from which this device acce ip_address ip_mask name evel for this community by enter destands (is able) name s SNMP community by enter de (enable) (disable) name by entering save config. re if you still need to change es for SNMP v3 Users alue of "default" for the usen kee sure that you have config SNMP v3 User Default V SNMP v3 User Default v3 User to SNMP v3 User State v3 User v3 User SNMP v3 User Default v3 User v3 User SNMP v3 User v3 User Default v3 User v3 User SNMP v3 User v3 User Default v	"public" or "private"). Ind: neter. Do not enter "public spts SNMP packets with the netering this command, while ring this command: the default values for a "p name, authentication pass pured the correct time and alues roller GUI, follow these stat rs to open the SNMP V3 L	" or "private." te associated community by are ro is read-only mode an public" or "private" commun sword, and privacy passwor time zone on your controlle aps: Jsers page (see Figure 4-15	entering this command d nv is read/write mode: ity string. d for SNMP v3 users. U: r.	sing these stand	lard values present	S a security risk. Then	efore, Cisco strongly advises that you c
Step 2 II "public" or "private fnig samp community delete in same parameter is the cor- Step 3 Create a new comm nfig samp community create ter up to 16 alphanumeric 0 Step 4 Enter the IP address fnig samp community and Step 5 Specify the access i step 4 Enter the IP address Step 5 Specify the access i step 4 Enter the IP address Step 5 Specify the access i step 5 Specify the access i step 6 Enable or disable th fnig samp community mo Step 7 Save your changes Step 8 Repeat this procedu anging the Default Value anging the Default Value is step 8 Repeat this procedu anging the Default Values. NMP v3 is time sensitive. Me the change the SNMP v3 user c Step 1 Choose Management re 4-19 SMP V3 Users P.	" appears in the SNMP Con name mounting name (in this case," unity by entering this comme arracters for the name paran from which this device acce <i>ip_address ip_mask name</i> evel for this community by enter de (enable disable) name s SNMP community by enter de (enable disable) name s SNMP v3 Users alue of "default" for the usen ke sure that you have config SNMP v3 User Default V lefault values using the cont t > SNMP > SNMP V3 User sge	"public" or "private"). Ind: neter. Do not enter "public spts SNMP packets with th netering this command, when ring this command: the default values for a " harme, authentication pass gured the correct time and alues roller GUI, follow these str rs to open the SNMP V3 L	" or "private." ne associated community by are ro is read-only mode an public" or "private" commun sword, and privacy passwor time zone on your controlle aps: sers page (see Figure 4-15	entering this command d nv is read/write mode: ity string. d for SNMP v3 users. U: r.	sing these stand	fard values present	s a security risk. Ther	efore, Cisco strongly advises that you c
Step 2 II "public" or "private fng smrp community delete a mane parameter is the cor Step 3 Create a new comm nfig smrp community create ter up to 16 alphanumeric CI Step 4 Ent et the IP address Step 5 Specify the access I nfig smnp community and Step 5 Specify the access I step 6 Enable or disable th nfig smnp community and Step 7 Save your changes Step 8 Repeat this procedu unging the Default Value a controller uses a default v use. MMP v3 is time sensitive. Me the change the SNMP v3 user of Step 1 Choose Management re 4-19 SNMP V3 Users Pro-	* appears in the SNMP Con name mounting name (in this case, unity by entering this comme aracters for the name paran from which this device accc <i>ip_address ip_mask name</i> evel for this community by enter de (enable) (disable) <i>nan</i> so SNMP community by enter de (enable) (disable) <i>nan</i> by entering save config. re if you still need to change es for SNMP v3 Users alue of "default" for the user ke sure that you have config SNMP v3 User Default V default values using the cont it > SNMP > SNMP V3 User sige	"public" or "private"). Ind: neter. Do not enter "public spts SNMP packets with the netering this command, when ring this command: the default values for a " inter default values for a " put default values for a " inter default values for a " put default values for a subscription value values for a subscription value values for a subscription value value values for a subscription value value value values for a subscription value val	" or "private." ne associated community by are ro is read-only mode an public" or "private" commun sword, and privacy passwor time zone on your controlle aps: Jeers page (see Figure 4-15	entering this command d nv is read/write mode: ity string. d for SNMP v3 users. U: r.	sing these stand	lard values present	s a security risk. Ther	efore, Cisco strongly advises that you c
Step 2 II "public" or "private fng smmp community delete a mane parameter is the cor Step 3 Create a new comm fng smmp community create ter up to 16 alphanumeric cl Step 4 Enter the IP address fng smmp community acc Step 4 Enter the IP address fng smmp community acc Step 5 Enable or disable th fng smmp community mo Step 7 Save your changes Step 8 Repeat this procedu anging the Default Value controller uses a default vi- uses. MMP v3 is time sensitive. Mit arg the GUI to Change the SMP 1 Subme V3 Users Pr Common Step 1 Choose Management re 4-19 SMMP V3 Users Pr	* appears in the SNMP Con name mounting name (in this case, unity by entering this comme aname aracters for the name param from which this device accc <i>ip.address (ip_mask name</i> even for this community by enter de (enable disable) nam by entering save config. re if you still need to change es for SNMP v3 Users alue of "default" for the usen kee sure that you have config SNMP v3 User Default V SNMP v3 User Default V at SNMP > SNMP V3 Users	"public" or "private"). Ind: neter. Do not enter "public pts SNMP packets with the netering this command, who ring this command: the default values for a "p hame, authentication pass pured the correct time and alues roller GUI, follow these stat is to open the SNMP V3 L	" or "private." ne associated community by ere ro is read-only mode an public" or "private" commun sword, and privacy passwor time zone on your controlle eps: Jsers page (see Figure 4-15	entering this command d nv is read/write mode: ity string. d for SNMP v3 users. U: r.	sing these stand	fard values present	s a security risk. Then	efore, Cisco strongly advises that you o
Step 2 II "public" or "private drifig smmp community delete ter up to 16 alphanumeric of Step 3 Create a new comm ndig smmp community renet step 4 Enter the IP address ndig smmp community acc Step 6 Enable or disable th andig smmp community acc Step 6 Enable or disable th andig smmp community acc Step 6 Repeat this procedu Inging the Default Value controller uses a default vi- lues. WMP v3 is time sensitive. Ma ing the GUI to Change the change the SMMP v3 user of Step 1 Choose Managemer re 4-19 SMMP V3 Users Pi CISCO	* appears in the SNMP Con name mounting name (in this case, unity by entering this comme name aracters for the name paran from which this device accor (p.address (p_mask name vell for this community by en- essmode (ro rw) name is SNMP community by en- de (enable disable) nan by entering save config. re if you still need to change ess for SNMP v3 Users alue of 'default' for the usen keis sure that you have config SNMP v3 User Default V lefault values using the cont its SNMP > SNMP v3 User to SNMP > SNMP v3 User to SNMP > SNMP v3 User	"public" or "private"). Ind: neter. Do not enter "public pts SNMP packets with the netering this command, while ing this command: ne the default values for a "p name, authentication pass pured the correct time and alues roller GUI, follow these still is to open the SNMP V3 L CC \TEDLLER \$	" or "private." te associated community by are ro is read-only mode an public" or "private" commun aword, and privacy passwor time zone on your controlle aps: Jsers page (see Figure 4-15 SECTUPITY	In the second se	Sing these stand	and values present	s a security risk. Then	efore, Cisco strongly advises that you c
Step 2 II "public" or "private fng smp community delete a mane parameter is the cor Step 3 Create a new comm fng smp community create ter up to 16 alphanumeric cl Step 4 Enter the IP address fng smp community acc Step 4 Enter the IP address Step 5 Enable or disable th fng smp community mo Step 7 Save your changes Step 8 Repeat this procedu anging the Default Value a controller uses a default vi- tues. MIP v3 is time sensitive. Me ang the GUI to Change the Step 1 Choose Management c 1500 Management	* appears in the SNMP Con name mounting name (in this case, unity by entering this comme aname aracters for the name paran from which this device accc (p,address (p_mask name vell for this community by enter de (enable disable) name s SNMP community by enter de (enable disable) name s SNMP community by enter de (enable disable) name s study of the source of the essence (or rw) name s SNMP v3 Users s source of default. Y default values using the cont of x SNMP > SNMP V3 Users s SNMP V3 Users SNMP V3 Users	"public" or "private"). Ind: Ind: Ind: Intering this command, which Intering this command. Intering this command: Intering this command: Inter	" or "private." re associated community by are ro is read-only mode an public" or "private" commun sword, and privacy passwor time zone on your controlle aps: Jsers page (see Figure 4-15 x(DELEOC) SEE UPJTY	entering this command d nv is read/write mode: ity string, d for SNMP v3 users. U r.).	Sing these stand	and values present	s a security risk. Then	efore, Cisco strongly advises that you o
Step 2 II "public" or "private fnig samp community delete in same parameter is the cor Step 3 Create a new comm infig samp community create ter up to 16 alphanumeric d Step 4 Enter the IP address infig samp community acc Step 4 Enter the IP address infig samp community acc Step 5 Specify the access I infig samp community acc Step 6 Enable of disable th infig samp community acc Step 7 Save your changes Step 8 Repeat this procedu e controller uses a default via use. dMP v3 is time sensitive. Ma ing the OLI to Change the change the SNMP V3 Users Private CISCO Wanagement Stemary	* appears in the SNMP Con name mounting name (in this case, unity by entering this comma name aname aracteris for the name param from which this device accc <i>ip_address ip_mask name</i> evel for this community by enter de (enable disable) nam sy entering save config. re if you still need to change ess for SNMP v3 Users alue of "default" for the usen kee sure that you have config SNMP v3 User Default V SNMP v3 User age	"public" or "private"). Ind: Ind: Ind: Intering this command, whi Intering this command, whi Intering this command. It the default values for a "p Intering this command: It the default values for a "p Intering this command. It the default values for a "p Intering this command. Intering this comma	" or "private." ne associated community by are ro is read-only mode an public" or "private" commun aword, and privacy passwor time zone on your controlle aps: Jeers page (see Figure 4-19 Jeers page (see Figure 4-19 APELIZOC - SE 2 JP3TY	entering this command d nv is read/write mode: ity string. d for SNMP v3 users. U: r	Shur Conf	and values present	s a security risk. Then	efore, Cisco strongly advises that you c
Step 2 II "public" or "private fing smp community delete in sme parameter is the cor- Step 3 Create a new comm- nifig smp community create ter up to 16 alphanumeric d Step 4 Enter the IP address infig smp community and Step 5 Specify the access i fing smp community access Step 6 Enable or disable th fing smp community mo Step 7 Save your changes Step 8 Repeat this proceed uses. MMP v3 is time sensitive. Ma ty the GU to Change the change the SNMP v3 user of Step 1 Choose Management c 15 CO Management Sum mary * SNMP	* appears in the SNMP Con name mounting name (in this case, unity by entering this comme name arranders for the name paran from which this device acce <i>ip_address ip_mask name</i> essinder (ro rw) name essinder (ro rw)	"public" or "private"). Ind: neter. Do not enter "public spts SNMP packets with the netering this command, when ring this command: the default values for a "p aname, authentication pass pured the correct time and alues pured the correct time and alues correct time and correct time and	" or "private." ne associated community by are ro is read-only mode an public" or "private" commun sword, and privacy passwor time zone on your controlle aps: Jores page (see Figure 4-15 Stors page (see Figure 4-15	entering this command d nv is read/write mode: ity string. d for SNMP v3 users. U: r.	Sing these stand	fard values present	s a security risk. Then	efore, Cisco strongly advises that you c
Rep 2 II "public" or "private fing smp community delete a name parameter is the cor- site p 3 Create a new commu- ning smp community create ter up to 16 aphanumeric di Rep 4 Enter the P address hing smp community inaddress ter up to 16 aphanumeric di Rep 4 Enter the P address hing smp community access ter g to 16 aphanumeric di Rep 6 Enable or disable th hing samp community mo step 7 Save your changes step 8 Repeat this procedu anging the Default Value controller uses a default view. MIP v3 is time sensitive. Me the change the SNMP v3 user of step 1 Choose Management Step 1 Choose Management Summary SMMP	* appears in the SNMP Con name mounting name (in this case, unity by entering this comme name maracters for the name paran from which this device accc <i>ip_address ip_mask name</i> essmode (ro rw) name essmode (ro rw) name essmode (ro rw) name essmode (ro rw) name essmode (ro rw) name soll to this community by enter de (enable) (disable) nan by entering save config. re if you still need to change ess for SNMP v3 Users alue of "default" for the usen ke sure that you have config SNMP v3 User Default V lefault values using the confit the SNMP SNMP v3 Users ge XDMP v3 Users User Varne cefeult	rpublic" or "private"). Ind: rpublic" or "private"). Ind: Intering this command, when ring this command, when ring this command. It the default values for a "p Intering this command. Intering this command. Intering this command. It the default values for a "p Intering this command. Intering this	" or "private." ne associated community by are ro is read-only mode an public" or "private" commun sword, and privacy passwor time zone on your controlle aps: Jaers page (see Figure 4-15 Store LEDCC SEE UPITY ht Protocol Privacy ALT-STIA A-3	entering this command d rw is read/write mode: ity string; d for SNMP v3 users. U for SNMP v3	Sing these stand	and values present	s a security risk. Then	efore, Cisco strongly advises that you c
Step 2 II "public" or "private ofig samp community delete in ame parametris the cor- Step 3 Create a new comm- ofig samp community create ter up to 16 alphanumoit of Step 4 Enter the IP address ofig samp community and Step 5 Specify the access I and gramp community and Step 5 Specify the access I and gramp community and Step 7 Save your changes Step 8 Repeat this procedu anging the Default Value anging the Default Value is step 8 Repeat this procedu anging the Step 1 Choose Management is the SUMP V3 user of Step 1 Choose Management Step 1	* appears in the SNMP Con name mrunity name (in this case, ' unity by entering this corrent name arracters for the name paran from which this device accc (<i>ip</i> , address (<i>ip</i> , mask name evel for this community by en- essensede (ro rw) name is SNMP community by enter de (enable) (disable) nan by entering save config. re if you still need to change ess for SNMP v3 Users alue of 'default' for the user the sure that you have config SNMP v3 User Default V lefault values using the cont it > SNMP > SNMP V3 Users ge X3/01TOR X-24X SNMP V3 Users User V3/01TOR X-24X	rpublic" or "private"). Ind: Ind: Intering this command, while Intering this command; while Intering this command: Intering this command: Inter	C or "private." he associated community by are no is read-only mode an public" or "private" commun word, and privacy passwor time zone on your controlle aps: time zone on your controlle aps: the Protect of Privacy act-state A_J	entering this command d rw is read/write mode: ity string. d for SNMP v3 users. U d for SNMP v3 users. U for SNMP v3 users. U https://www.sers.ukers ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.ukers.uker	Sing these stand	ard values present	s a security risk. Ther	efore, Cisco strongly advises that you o

1/13p - c MORE 1/13p - 2 MORE Step 3 Click New to add a new SNMP v3 user. The SNMP V3 Users > New page appears (see Figure 4-20).

Figure 4-20 SNMP V3 Users > New Page

al)alja cisco	MONITOR WAY, OCUTEOU	er wireless security man	Sage Cont y AGEMENT COMMANDS H	poration Birg HFIP	Luguut Beirashi	
Management	SNMP V3 Users > New			c Bark	Apply	
Summary	Iser Profile Name					
* SNMP	Bonnoo Modin	10 m				
SNMP V3 Joers Communities	Access Mone					
Trap Nece vers Trap Lichtrols	Authentication Protocol HMAC-S	4A M				
Irap _tqs	Auth Fa	sword Confim Auth Password				
Teinet-SSH	Privacy Protocol CIL-AL	>12t 💌				
Serial Port	Prv Tas	aword Confirm Pric Pasaword			2336	
Users Step 4. In the User Profile Na	me text box, enter a unique name. Do not e	iter "default"			8	
Step 5 Choose Read Only o	Read Write from the Access Mode drop-do	wn list to specify the access level for this us	er. The default value is Read Only	у.		
Step 6 From the Authenticat	on Protocol drop-down list, choose the desi	ed authentication method: None , HMAC-M	D5 (Hashed Message Authenticat	tion Coding-Messa	age Digest 5), or HMA	C-SHA (Hashed Message Authentication
Step 7 In the Auth Password	ig Algorithm). The default value is HMAC-S and Confirm Auth Password text boxes, en	TA. er the shared secret key to be used for auth	entication. You must enter at least	t 12 characters.		
Step 8 From the Privacy Pro	ocol drop-down list, choose the desired en	ryption method: None , CBC-DES (Cipher B	Block Chaining-Digital Encryption	Standard), or CFB	-AES-128 (Cipher Fe	edback Mode-Advanced Encryption
Standard-128). The c	atault value is CFB-AES-128.					
Note In order to config	re CBC-DES or CFB-AES-128 encryption,	rou must have selected either HMAC-MD5 c	r HMAC-SHA as the authenticatio	on protocol in From	the Authentication Pr	otocol drop-down list, choose the desired
authentication n	ethod: None, HMAC-MD5 (Hashed Messa	e Authentication Coding-Message Digest 5)	, or HMAC-SHA (Hashed Message	e Authentication C	oding-Secure Hashing	g Algorithm). The default value is HMAC-SHA.
Step 9 In the Priv Password	and Confirm Priv Password text boxes, enter	r the shared secret key to be used for encry	ption. You must enter at least 12 c	characters.		
Step 10 Click Apply to comm	t your changes.					
Step 12 Reboot the controlle	so that the SNMP v3 user that you added	akes effect				
Ising the CLI to Change the	NMP v3 User Default Values					
To change the SNMP v3 user d	fault values using the controller CLI, follow	these steps:				
Step 1 See the current list of	SNMP v3 users for this controller by enteri	g this command:				
show snmpv3user Step 2 If "default" appears in	the SNMP v3 User Name column, enter th	s command to delete this user:				
config snmp v3user delete u	ername					
The username parameter is the	SNMP v3 username (in this case, "default")					
config spmp v3user create //	3 user by entering this command: ername / ro rw \ / none hmacmd5 hr	arsha \/ none des aesrfh128 \ auth k	ev encrynt kev			
where			oy choryp_hoy			
 username is the SNMP v3 	semame.					
 rois read-only mode and ro none , hmacmd5 , and hr 	acsha are the authentication protocol optic	ns.				
none, des, and aescfb128	are the privacy protocol options.					
 autn_key is the authentical encrypt_key is the encrypt 	on shared secret key. In shared secret key.					
Do not enter "default" for the us	mame, auth_key, and encrypt_key parame	iers.				
Step 4 Save your changes b	entering the save config command.					
Step 5 Reboot the controller	so that the SNMP v3 user that you added t	kes enect by entering reset system com	mand.			
onfiguring Aggressive L	ad Balancing					
Enabling aggressive load balan	ing on the controller allows lightweight acc	ss points to load balance wireless clients ad	cross access points. You can enab	ble aggressive load	d balancing using the	controller GUI or CLI.
Clients are load balanced betw	en access points on the same controller. L	ad balancing does not occur between acce	ss points on different controllers.			
When a wireless client attempts more associations. If the access	to associate to a lightweight access point, a point is too busy, the client attempts to ass	ssociation response packets are sent to the ciate to a different access point in the area.	client with an 802.11 response pa The system determines if an acce	acket including stat ess point is relative	tus code 17. This code aly more busy than its	e indicates whether the access point can accept any neighbor access points that are also accessible to
the client. For example, if the number of cl	ents on AP1 is more than the number of clie	nts on AP2 plus the load-balancing window,	then AP1 is considered to be busi	sier than AP2. Whe	n a client attempts to a	associate to AP1, it receives an 802.11 response
packet with status code 17, indi You can configure the controller	ating that the access point is busy, and the to deny client associations up to 10 times (client attempts to associate to a different ac a client attempted to associate 11 times, it	cess point. would be allowed to associate on t	the 11th try). You o	an also enable or dis	able load balancing on a particular WLAN, which is
useful if you want to disable loa	balancing for a select group of clients (suc	h as time-sensitive voice clients).				,
lient Association Limits The maximum number of client :	ssociations that the access points can sup	ort is dependent upon the following factors:				
The maximum number of cl	ent associations differs for lightweight and	utonmous IOS access points.				
There may be a limit per ra	io, and an overall limit per AP.					
AP hardware (the 16-MB A lient Association Limits for	is have a lower limit than the 32-MB and hi	ner APS).				
Per AP Limits	ight rough rough					
For 16-MB APs, the limit is	28 clients per AP. This is applicable to 110) and 1200 series APs.				
 For 32-MB and higher APs. 	there is no per-AP limit.					
For all IOS APs, the limit is	200 associations per radio					
 For all 1000 and 1500 serie 	s APs, which are not supported beyond the	4.2 release, the limit is 250 associations per	radio.			
Thus, with 32-MB and higher lig	tweight IOS APs, with two radios, up to 20	+200=400 associations are supported.				
ient Association Limits for	utonomous IOS Access Points					
Practically, the limit is around 80	to 127 clients per AP. This varies dependir	g on the following factors:				
AP model (whether it is 16	IB or 32 MB or higher).					
IOS version. Hardware configuration (two	radios use more memory than one)					
 Enabled features (WDS fur 	ctionality in particular).					
Per-radio limits						
The practical per-radio limit is a Per-SSID limits	out 200 associations. One will likely hit the	per-AP limit first.				
Unlike Cisco Unified Wireless N	twork, Autonomous IOS supports per-SSIE	/per-AP association limits. This is configured	d using the max-associations CLI,	under dot11 SSID.	The maximum and de	afault is 255 associations.
ing the GUI to Configure A	gressive Load Balancing					

To configure aggressive load balancing using the controller GUI, follow these steps:

Step 1 Choose Wireless > Advanced > Load Balancing to open the Load Balancing page (see Figure 4-21).

Figure 4-21 Wireless > Advanced > Load Balancing Page

CISCO MORETER KILANS DISTREDULER KIDELEDS DECURRY MANAGEMENT Wireless Load Balancing * Access Points A Arbs: Wedets' Wedet	COMMANDO	UEL9	FECEIGAEN Apply
Wireless Load Balancing A Aos Client Kinnew Size 5 Y Addis Meximum Dame Own L 3 UKL15/5 Meximum Dame Own L 3 UKL15/5 That Enable Conflox store 3 UKL15/5 That Enable Conflox store 3 UKL15/5 That Enable Conflox store 4 Meximum Dame Own L 3 1 UKL15/5 That Enable Conflox store 6 Load Balancing Statistics That Enable Conflox store 6 Load Balancing That Enable Messays Sec. C 6 Load Balancing Loceced Linie Messlaw Social Sec. C 6 Mesh Nors 55 Canel date Count 6 HBEAD Grupp "Load Balancing to confloared to per Middle VUXL116/n "Load Balancing to confloared to per Middle			Apply
A Cass Points A Ass A A			
Global Configuration This Italia Control Control Advanced Tute Dame Message Sent Local Balan Jru Exceeded Lenix Mast Linix Control Bank Send Nore SG Cand Sets Control Mesh Nore SG Cand Sets Control HREAD Commpt Nore SG Cand Sets Control BU2.116/n "Local Setences" is configurative per Michty. BU2.116/n "Local Setences" is configurative per Michty.			
AdVanced Tale Dame Messaya Seri C Local Balar Jru Bank Salauk Loceccad Lania Mart Linik Kounk L Mash Nora 55 Cancidate Counk C MREAP Grimpy Nora 26 Cancidate Laure L HREAP Grimpy Nora 26 Cancidate Laure L BUZ:11a/n Mask Salawaya soci-Appretive per M/Ahr.			
HRFAP Grunp, Nors 2.46 Cendicate Lourt L HRFAP Grunp, "Louo Salencary is configurative per MUM. • 802.111/10/10			
802.116/n 802.116/n 802.116/n			
Mulia Stream			
Country Timers			
) Q95			

Step 2 In the Client Window Size text box, enter a value between 1 and 20. The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing window + client associations on AP with the lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client window size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold. Step 3 In the Maximum Denial Count text box, enter a value between 0 and 10. The denial count sets the maximum number of association denials during load balancing.

- Step 4 Click Apply to commit your changes.
- Step 5 Click Save Configuration to save your changes.
- Step 6 To enable or disable aggressive load balancing on specific WLANs, choose WLANs > WLAN ID. The WLANs > Edit page appears

Step 7 Click the Advanced tab (see Figure 4-22).





Step 9 Click Save Configuration to save your settings

Using the CLI to Configure Aggressive Load Balancing

To configure aggressive load balancing using the controller CLI, follow these steps

Step 1 Set the client window for aggressive load balancing by entering this command:

config load-balancing window client_count

You can enter a value between 0 and 20 for the client_count parameter

Step 2 Set the denial count for load balancing by entering this command

config load-balancing denial denial_count

You can enter a value between 1 and 10 for the denial_count parameter

Step 3 Save your changes by entering this command:

save config

Step 4 Enable or disable aggressive load balancing on specific WLANs by entering this command:

config wan load-balance allow (enable | disable) wan ID

- You can enter a value between 1 and 512 for wlan_ID parameter. Step 5 Verify your settings by entering this command:
- show load-balancing

Information similar to the following appears:

Statistics

None 5G Candidate Count...... 0 times None 2.4G Candidate Count...... 0 times

Step 6 Save your changes by entering this command:

save config

Configuring Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave overs, and cordises phones as well as co-channel interference from other access points because of the 802. 11b/g limit of three nonoverlapping channels. To combat these sources of interference and improve overall network performance, you can cordinging band selection on the controller.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels. Band selection is enabled globally by default.

te Band-selection enabled WLANs	do not support time-sensitive applications like voice and vide	eo because of roam	ing delays.				
Guidelines for Using the Banc Follow these guidelines when us Band selection can be used Band selection operates on The band-selection algorith You can enable both band s	I Selection sing band selection: I only with Cisco Aironet 1140 and 1250, 1260, and 3500 Ser ly on access points that are connected to a controller. A hybr in directs dual-band clients only from the 2.4-GHz radio to the selection and aggressive load balancing on the controller. Th	ies access points. id-REAP access poi e 5-GHz radio of the ley run independent	int without a contro same access poin y and do not impac	ller connection does not pe t, and it only runs on an ac t one another.	erform band selection a ccess point when both t	fter a reboot. he 2.4-GHz and 5-GHz radio	is are up and running.
Using the GUI to Configure Ba To configure band selection usin	and Selection Ig the controller GUI, follow these steps:						
Step 1 Choose Wireless > Ad Figure 4-23 Wireless > Advance	dvanced > Band Select to open the Band Select page (see) ed > Band Select Page	Figure 4-23).					
aliala cisco	MONITOR MEANS CONTROLLER WERE FE	ss <u>s</u> ecurity	Sage MANAGEMENT	Configuration Engl COMMANDS -FLP	Logoot Berash EFEDRACK		
Wireless	Band Select				Αρρίγ		
 Arrass Points p. p.s Bodics Bodics BC2.119/1 BC2.119/p1 Clobal Configuration 	Fruta Ovaa Oudut Voon Lyde Kenad Threahold (m. seconds) Age Out Sugnession (casumus) Age Out Dual Sand (seconds)	2 201 20 20 00					
 Advanced Locd Salarang Page Selad 	Acceptable Client R551 (dPm) '' Basel Selart is costigurable per WORK	30					
Mieda HREAP Groups > 802.11a/n > 002.11b/q/n > Media Stream Gauntry							

Due Step 2 In the Probe Cycle Count text box, enter a value between 1 and 10. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2

- Step 3 In the Scan Cycle Period Threshold (milliseconds) text box, enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.
- Step 4 In the Age Out Suppression (seconds) text box, enter a value between 10 and 200 seconds. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.
- Step 5 In the Age Out Dual Band (seconds) text box, enter a value between 10 and 300 seconds. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.
- Step 6 In the Acceptable Client RSSI (dBm) text box, enter a value between -20 and -90 dBm. This parameter sets the minimum RSSI for a client to respond to a probe. The default value is -80 dBm. Step 7 Click Apply to commit your changes.

Timers F QuS

- Step 8 Click Save Configuration to save your changes.
- Step 9 To enable or disable aggressive load balancing on specific WLANs, choose WLANs > WLAN ID. The WLANs > Edit page appears.
- Step 10 Click the Advanced tab (see Figure 4-22).
- Step 11 Click Save Configuration to save your changes.

Using the CLI to Configure Band Selection

To configure band selection using the controller CLI, follow these steps

Step 1 Set the probe cycle count for band select by entering this command:

config band-select cycle-count cycle_count

You can enter a value between 1 and 10 for the cycle_count parameter. Step 2 Set the time threshold for a new scanning cycle period by entering this command:

config band-select cycle-threshold milliseconds

- You can enter a value for threshold between 1 and 1000 for the milliseconds parameter.
- Step 3 Set the suppression expire to the band select by entering this command:
- config band-select expire suppression seconds

You can enter a value for suppression between 10 to 200 for the seconds parameter.

- Step 4 Set the dual band expire by entering this command:
- config band-select expire dual-band seconds
- You can enter a value for dual band between 10 and 300 for the seconds parameter. Step 5 Set the client RSSI threshold by entering this command:
- config band-select client-rssi client_rssi You can enter a value for minimum dBm of a client RSSI to respond to a probe between 20 and 90 for the client_rssi parameter Step 6 Save your changes by entering this command:

save config

Step 7 Enable or disable band selection on specific WLANs by entering this command:

- config wlan band-select allow {enable | disable} wlan_ID
- You can enter a value between 1 and 512 for wan ID parameter
- Step 8 Verify your settings by entering this command: show band-select

Information similar to the following appears: Band Select Probe Response..... Enabled

Step 9 Save your changes by entering this command:

save config

Configuring Fast SSID Changing

When fast SSD changing is enabled, the controller allows clients to move between SSIDs. When the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID. When fast SSID changing is disabled, the controller endroces a delay before clients are allowed to move to a new SSID.

Using the GUI to Configure Fast SSID Changing

- To configure fast SSID changing for mobile clients using the controller GUI, follow these steps
- Step 1 Choose Controller to open the General page.
- Step 2 From the Fast SSID Change drop-down list, choose Enabled to enable this feature or Disabled to disable it. The default value is disabled

Step 3 Click Apply to commit your changes.

ng the CLI to Configure Fast S configure fast SSID changing for r Step 1 Enable or disable fast SSI anding network fast-ssid-change (Step 2 Save your changes by ent we config abling 802.3 X Flow Control 12:3X Flow Control is disabled by du nfiguring 802.3 Bridging the controller supports 802.3 frames e controller supports 802.3 frames e controller supports 802.3 frames to controller supports 802.3 frames to controller supports 802.3 frames e controller supports 802.3 bridging through the controller software release 5.2 or 1 release LN Controller Network Mos (SM, and the Catalyst 3750G Wirels v default. Cisco 2100 Series Control	ID Changing able clients using the controller CLI, follow these changing by entering this command: mable (disable) ing this command: ault. To enable it, enter the config switchconfig fil ault. To enable it, enter the config switchconfig fil ing the applications that use them, such as those e-controller to bridge non-IP frames for application 	ps: control enable comma xically used for cash r not running over IP. C	and.	
Step 1 Enable or disable fast SSI onfig network fast-ssid-change (Step 2 Save your changes by ent ave config abling 802.3X Flow Control 2.3X Flow Control is disabled by dr nfiguring 802.3 Bridging the controller supports 802.3 frames e controller supports 802.3 frames allows to use controller supports 802.3 frames allows to secontroller supports 802.3 bridging through a controller software release 5.2 or irreless LNN Controller Network Mon (SM, and the Catalyst 3750G Wirele v default. Clicoo 2100 Series Control	changing by entering this command: nable disable) ring this command: ault. To enable it, enter the config switchconfig fil ind the applications that use them, such as those e controller to bridge non-IP frames for application 	control enable comma sically used for cash r not running over IP. C	and. registers and cash register servers. However, to n	
And a standard and and a standard an	ault. To enable i disable) ault. To enable it, enter the config switchconfig fi ing this command: ault. To enable it, enter the config switchconfig fi ind the applications that use them, such as those e controller to bridge non-IP frames for applicatio e controller to bridge non-IP frames for applicatio applications groups and applications	control enable comma xically used for cash r not running over IP. C	and. registers and cash register servers. However, to n	
Step 2 Save your changes by ent we config abling 802.3X Flow Control 12.3X Flow Control is disabled by di nfiguring 802.3 Bridging the controller supports 802.3 frames e controller. apport for raw 802.3 frames allows 1 we controller supports 802.3 frames e controller. Discret 1 Total packet we controller software release 5.2 or irreless LAN Controller Metwork Mon ISM, and the Catalyst 3750G Wirele we default. Clicoo 2100 Series Control	able (disable) ing this command: ault. To enable it, enter the config switchconfig fi and the applications that use them, such as those e controller to bridge non-IP frames for application 	control enable comma xically used for cash r not running over IP. C	and. registers and cash register servers. However, to n	
we config abling 802.3X Flow Control 12.3X Flow Control is disabled by di nfiguring 802.3 Bridging the controller supports 802.3 frames e controller supports 802.3 frames e controller supports 802.3 frames allows 1 we controller supports 802.3 frames allows 1 we controller supports 802.3 bridging through the controller support succentroller support controller support su	ault. To enable it, enter the config switchconfig fi ind the applications that use them, such as those controller to bridge non-IP frames for application 	control enable comma xically used for cash r not running over IP. C	and. registers and cash register servers. However, to n	
abling 802.3X Flow Control 22.3X Flow Control is disabled by dr nfiguring 802.3 Bridging the controller supports 802.3 frames e controller. upport for raw 802.3 frames allows i estimation [Source Total packet) 4/AC address MAC address lengt 	ault. To enable it, enter the config switchconfig fi ind the applications that use them, such as those e controller to bridge non-IP frames for application Payload	control enable comma vically used for cash r not running over IP. C	and. registers and cash register servers. However, to n	
abiling 802.3X Flow Control 32.3X Flow Control is disabled by d nfiguring 802.3 Bridging the controller supports 802.3 frames e controller. Apport for raw 802.3 frames allows i the controller was a support for total packet the controller software release 5.2 or irreless LAN Controller Network Mor IsM, and the Catalyst 3750G Wirele the data in the catalyst 3750G Wirele to default. Clicoo 2100 Series Control	ault. To enable it, enter the config switchconfig fi ind the applications that use them, such as those controller to bridge non-IP frames for application Payload	sting 802.3X Flow Control 3X Flow Control is disabled by default. To enable it, enter the config switchconfig flowcontrol enable command. "guring 802.3 Bridging controller supports 802.3 frames and the applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridg port for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP. Only this raw 802.3 frame format is currently supported:		
nfiguring 802.3 Bridging he controller supports 802.3 frames a controller. apport for raw 802.3 frames allows i —estination Source Total packet MAC address MAC address leng u can configure 802.3 bridging thro controller software release 5.2 or I treless LAN Controller Network Mos ISM, and the Catalyst 3750G Wirel v default. Clicoo 2100 Series Contro	and the applications that use them, such as those e controller to bridge non-IP frames for application Payload	vically used for cash r	registers and cash register servers. However, to n	
the controller supports 802.3 frames e controller. upport for raw 802.3 frames allows 1 — setimation Source Total packet MAC address Image Total packet MAC address MAC address Jeng - controller software release 5.2 or 1 release LAN Controller Network Mos ISM, and the Catalyst 3750G Wirels v default. Clicoo 2100 Series Control	and the applications that use them, such as those e controller to bridge non-IP frames for application Payload	pically used for cash r not running over IP. C	registers and cash register servers. However, to n	
e controller. upport for raw 802.3 frames allows Destination Source Total packet vAC address MAC address leng u can configure 802.3 bridging thrc controller software release 5.2 or 1 release LAN Controller Network Mo ISM, and the Catalyst 3750G Wirels v default. Cisco 2100 Series Control	e controller to bridge non-IP frames for application Payload	not running over IP. C		nake these applications work with the controller, the 802.3 frames must be b
Destination Source Total packet, WAC address MAC address leng u can configure 802.3 bridging thrc controller software release 5.2 or 1 freless LAN Controller Network Mo ISM, and the Catalyst 3750G Wirel v default. Clsco 2100 Series Control	Payload 	not running over in . c	Only this raw 802.3 frame format is currently suppr	orted
Destination Source Triata packet MAC address MAC address leng us can configure 802.3 bridging through controller software release 5.2 or i release LAN Controller Network Mon (SM, and the Catalyst 3750G Wirels up default. Clicoo 2100 Series Contor	Payload i 		ony this raw 602.3 frame format is currently suppo	uited.
v default. Cisco 2100 Series Controller	igh the controller GUI in software release 4.1 or I			
controller software release 5.2 or I Ireless LAN Controller Network Mo ISM, and the Catalyst 3750G Wirele		r releases and throug	h the controller CLI in software release 4.0 or late	er releases.
freless LAN Controller Network Mo ISM, and the Catalyst 3750G Wirel v default. Cisco 2100 Series Contro	ter releases, the software-based forwarding arch	ture for 2100-series-t	based controllers is being replaced with a new for	warding plane architecture. As a result. Cisco 2100 Series Controller and th
v default. Cisco 2100 Series Contro	Je for Cisco Integrated Services Routers (as wel ss LAN Controller Switch.	Cisco 5500 Series C	Controllers) bridge 802.3 packets by default. There	foreing pathodoninconter and idealty cloud 2100 2000 controllers to efore, 802.3 bridging can now be disabled only on 4400 series controllers, th
v default. Cisco 2100 Series Contro				
ese protocols	lers that run software release 5.2 or later release	nd Cisco 5500 Series	s Controllers bridge all non-IPv4 packets (such as	AppleTalk, IPv6, and so on). If desired, you can use ACLs to block the bridg
ou can also configure 802.3 bridgin	using the Cisco Wireless Control System (WCS	ee the Cisco Wireless	s Control System Configuration Guide for instruction	ons.
ng the GUI to Configure 802.3 [ridaina			
configure 802.3 bridging using the	controller GUI, follow these steps:			
Step 1 Choose Controller > Gene	al to open the General page (see Figure 4-24).			
ure 4-24 General Page				
ախոխ			Sege Contiguration Bir.	Logical (Eelfreen)
CISCO	CATCR WLANG CONTROL FR WE	ESS SECUEITY	VANAGEMENT COMMANDS HELT	EEEDARON
Controller	ieneral			Apply
General	Nama 4+00			
Inventory	CU2.1 official Control Mode DisaL ad ⊻			
Interfaces	LAG Modeld in extrepod. DisaFiel 🖉		(LAG Yode's currently disabled)	
Toberbace Groups	Brondeast Ferwarding 👘 Disabled 😒			
Multicast	CP Munard Muna Z			
Nelwork Routes	aP is pack			
Internal DHCP Server	Sumb Table Fridam Direct of			
Mobility Management	The Constant of States			H
Ports	Default Mobility Domein			
NIP	Name			
+ COP	EF Group Name			
Advanced	(seconds) (SUU			
	ARF Timecul (seconds) 800	2		
	Web Redius Authoritication PAP			
	812.3 Pringing Disabled 😵			
	Operating Linginghment Commercia	tc 41 (C)		
	Internal Tan o Marin Dito ea c	0000000		99
	Limm 1. ViviLAA supports funcest mode only.			01
Step 2 From the 802.3 Bridging dr	p-down list, choose Enabled to enable 802.3 brid	ng on your controller of	or Disabled to disable this feature. The default val	lue is Disabled.
Note in controller software r	leses 5.2 or later releases, you can disable 802 '	idaing only for 4400 s	pariae controllare the Cieco W/SM, and the Catalu	vet 27500 Wirelass LAN Controllar Switch
			sines controllers, the obco more, and the outary	
Step 3 Click Apply to commit your	hanges.			
Step 4 Click Save Configuration to	save your changes.			
ng the CLI to Configure 802.3 I	ridging			
configure 802.3 bridging using the	controller CLI, follow these steps:			
Step 1 See the current status of 8	2.3 bridging for all WLANs by entering this comm	d:		
iow network				
Step 2 Enable or disable 802.3 br	Jging globally on all WLANs by entering this com	id:		
Infig network 802.3-bridging (enable	disable}			
A				
Note In controller software re	ease 5.2 or later releases, you can disable 802.3	idging only for 4400 s	series controllers, the Cisco WiSM, and the Cataly	st 3750G Wireless LAN Controller Switch.
Step 3 Save your settings by ente	ing this command:			
ave config				
nfiguring Multicast Mode	asting, you can configure the multicast method th	ne controller uses. Th	ne controller performs multicasting in two modes:	
nfiguring Multicast Mode your network supports packet multic	e controller unicasts every multicast packet to ev	access point associat	ted to the controller. This mode is inefficient but m	night be required on networks that do not support multicasting.
nfiguring Multicast Mode your network supports packet multion Unicast mode —In this mode, th	he controller sends multicast packets to a CAPW	multicast group. This	method reduces overhead on the controller proce	essor and shifts the work of packet replication to your network, which is muc
nfiguring Multicast Mode your network supports packet multi Unicast mode —In this mode, th Multicast mode —In this mode,				
ntiguring Multicast Mode your network supports packet multi Unicast mode —In this mode, th Multicast mode —In this mode, efficient than the unicast method	he controller GLII or CLI			
nfiguring Multicast Mode your network supports packet multi Unicast mode —In this mode, tl Multicast mode —In this mode, efficient than the unicast method u can enable multicast mode using	he controller GUI or CLI.			
rhfguring Multicast Mode your network supports packet multi Unicast mode — In this mode, efficient than the unicast method witch an enable multicast mode using Jerstanding Multicast Mode hen you enable multicast mode ance sathe management intenface for es-	he controller GUI or CLI. the controller receives a multicast packet from th iding multicast packets. Access points in the mult	ired LAN, the controlli	ler encapsulates the packet using CAPWAP and fr packet and forward it to all the BSSIDs mapped to	orwards the packet to the CAPWAP multicast group address. The controller the interface on which clients receive multicast traffic. From the anness noi
nfiguring Multicast Mode your network supports packet multi Unicast mode —h this mode, i Multicast mode —h this mode, i efficient than the unicast method us can enable multicast mode using terstanding Multicast Mode hen you enable multicast mode and safter management interface for a strepactive, the multicast appears to	he controller GUI or CLL the controller receives a multicast packet from th dring multicast packets. Access points in the mul e a broadcast to all SSIDs.	ired LAN, the controlle st group receive the p	er encapsulates the packet using CAPWAP and for packet and forward it to all the BSSIDs mapped to	onwards the packet to the CAPWAP multicast group address. The controller the interface on which clients receive multicast traffic. From the access point the interface on which clients are the second seco

When IGMP snooping is disabled, the following is true:

• The controller always uses Layer 2 MGID when it sends multicast data to the access point. Every interface created is assigned one Layer 2 MGID. For example, the management interface has an MGID of 0, and the first dynamic interface

- created is assigned an MGID of 8, which increments as each dynamic interface is created
- The IGMP packets from clients are forwarded to the router. As a result, the router IGMP table is updated with the IP address of the clients as the last reporter.
- When IGMP snooping is enabled, the following is true:
- · The controller always uses Layer 3 MGID for all Layer 3 multicast traffic sent to the access point. For all Layer 2 multicast traffic, it continues to use Layer 2 MGID.
- IGMP report packets from wireless clients are consumed or absorbed by the controller, which generates a query for the clients. After the router sends the IGMP query, the controller sends the IGMP reports with its interface IP address as the
 listener IP address for the multicast group. As a result, the router IGMP table is updated with the controller IP address as the multicast listener.
- When the client that is listening to the multicast groups reams from one controller to another, the first controller transmits all the multicast group information for the listening client to the second controller. As a result, the second controller can another, the first controller transmits all the multicast groups to which the client was listening. This process aids in the seamless transfer of multicast data to the client.
- If the latening client roams to a controller in a different subnet, the multicast packets are tunneled to the anchor controller of the client to avoid the reverse path filtering (RPF) check. The anchor then forwards the multicast packets to the infrastructure witch.

1

If a 4400 series VLC has LAG and IGMP snooping enabled, WLC port 1 must be active. WLC sourced IGMP queries (only applicable if WLC IGMP snooping is enabled) are sent out of only WLC port 1 when LAG is enabled. This restriction is not applicable if LAG is disabled and the Management and AP Manager interfaces are mapped to ports other than 1. This restriction is not applicable to other WLC platforms.

٩. Note The MGIDs are controller specific. The same multicast group packets coming from the same VLAN in two different controllers may be mapped to two different MGIDs. ٩.

Note If Layer 2 multicast is enabled, a single MGID is assigned to all the multicast addresses coming from an interface (see Figure 4-26).

Guidelines for Using Multicast Mode

- Follow these guidelines when you enable multicast mode on your network:
- · The Cisco Unified Wireless Network solution uses some IP address ranges for specific purposes, and you should keep these ranges in mind when configuring a multicast group
 - 224.0.0.0 through 224.0.0.255—Reserved link local addresses
 - 224.0.1.0 through 238.255.255.255—Globally scoped addresses
 - 239.0.0.0 through 239.255.x.y /16—Limited scope addresses
- · When you enable multicast mode on the controller, you also must configure a CAPWAP multicast group address. Access points subscribe to the CAPWAP multicast group using IGMP.
- Cisco 1100, 1130, 1200, 1230, and 1240 access points use IGMP versions 1, 2, and 3.
- Access points in monitor mode, sniffer mode, or rogue detector mode do not join the CAPWAP multicast group address The CAPWAP multicast group configured on the controllers should be different for different controllers.
- Multicast mode does not operate across intersubnet mobility events such as guest tunneling. It does, however, operate with interface overrides using RADIUS (but only when IGMP snooping is enabled) and with site-specific VLANs (access point group VLANs).
- For LWAPP, the controller drops multicast packets sent to UDP control port 12223. For CAPWAP, the controller drops multicast packets sent to UDP control and data ports 5246 and 5247, respectively. Therefore, you may want to consider not
 using these port numbers with the multicast applications on your network.
- We recommend that any multicast applications on your network not use the multicast address configured as the CAPWAP multicast group address on the controller.
- Cisco 2100 Series Controllers do not support multicast-unicast mode. They do, however, support multicast-multicast mode, except when access points are connected directly to the local port of a 2100 series controller.

Using the GUI to Enable Multicast Mode

enable multicast mode using the controller GUI, follow these steps

Step 1 Choose Controller > Multicast to open the Multicast page (see Figure 4-25).

Figure 4-25 Multicast Page

	terrain in the man	and the second s				A STREET AND A STREET
WANT DONIE	COLLER SVIRE ESS	ZECTADIA 1	REACHEREN	COMMANDS	HFLI	-F-DP203
						Δμρίγ
fult ast Media	Trataloc 💌					
MF 'shocoing						
enut (scotods) [50						
	ultanst Media It Shocoing acut (seathds) (50	ult part Merles <u>Carallee (*)</u> In fance ng in it (sepande) (m)	ult past Minde <u>Consider Min</u> In Pascona () In It (seconds) (in	ult post Micha <u>Tatalan M</u> Ilt post Micha <u>Tatalan M</u> In It (seconds) (n	ult past Minde <u>Stander W</u> Ult past Minde <u>Stander W</u> Historich M Historich M Historich M	ult past Minte Turnler M It Past Minte Turnler M It Paston Turnler M It Paston Turnler M

- Unicast -Configures the controller to use the unicast method to send multicast packets
- Multicast —Configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group
- - ۰. Note Hybrid REAP supports unicast mode only.
- Step 3 If you chose Multicast in Choose one of the following options from the Ethernet Multicast Mode drop-down list; enter the IP address of the multicast group in the Multicast Group Address text box

Step 4 If you want to enable IGMP snooping, select the Enable IGMP Snooping check box. If you want to disable IGMP snooping, leave the check box unselected. The default value is disabled

Step 5 To set the IGMP timeout, enter a value between 30 and 7200 seconds in the IGMP Timeout tex box. The controller sends three queries in one timeout value at an interval of *timeout* /3 to see if any clients exist for a particular multicast group. If the controller dises not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller weaks for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (that is, to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

Step 7 Click Save Configuration to save your changes

Using the GUI to View Multicast Groups

To view multicast groups using the controller GUI, follow these steps:

Step 1 Choose Monitor > Multicast. The Multicast Groups page appears (see Figure 4-26)

Figure 4-26 Multicast Groups Page



To enable multicast mode using the controller CLI, follow these steps:

Step 1 Enable or disable multicasting on the controller by entering this command

config network multicast global (enable | disable)

The default value is disabled.

1

Note The config network broadcast (enable | disable) command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode currently on the controller to

Step 6 Click Apply to commit your changes

operate. Step 2 Perform one of the following:

config network multicast mode unicast

a. Configure the controller to use the unicast method to send multicast packets by entering this command

Configure the controller to use the multicast method to send multicast packets to a CAPWAP multicast group by entering this command

config network multicast mode multicast multicast_group_ip_address Step 3 Enable or disable IGMP snooping by entering this command

config network multicast igmp snooping { enable | disable }

The default value is disabled

Step 4 Set the IGMP timeout value by entering this command

config network multicast igmp timeout timeout

You can enter a timeout value between 30 and 300 seconds. The controller sends three queries in one timeout value at an interval of timeout/3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGD table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller waits general IGMP query (that is, to destination address 22 40.0.1) and sends in on all WLANs with an MGID value of 1. Step 5 Save your changes by entering this command:

save config

Using the CLI to View Multicast Groups

To view multicast groups using the controller CLI, use these commands:

- · See all the multicast groups and their corresponding MGIDs by entering this command
- show network multicast moid summary Information similar to the following appear Layer2 MGID Mapping InterfaceName vlanId MGID management 0 0 test 0 9 wired 20 8

Layer3 MGID Mapping: Number of Layer3 MGIDs..... 1

Group address Vlan MGID

239.255.255.250 0 550

See all the clients joined to the multicast group in a specific MGID by entering this command:

show network multicast mgid detail mgid_value where the mgid_value parameter is a number between 550 and 4095 Information similar to the following appears: No of clients...... 1 Client List..... Client MAC Expire Time (mm:ss) 00:13:02:23:82:ad 0:20

Using the CLI to View an Access Point's Multicast Client Table

To help troubleshoot roaming events, you can view an access point's multicast client table from the controller by performing a remote debug of the access point

To view an access point's multicast client table using the controller CLI, follow these steps

Step 1 Initiate a remote debug of the access point by entering this command:

debug ap enable Cisco AP

Step 2 See all of the MGIDs on the access point and the number of clients per WLAN by entering this command:

debug ap command "show capwap mcast mgid all " Cisco_AP Step 3 See all of the clients per MGID on the access point and the number of clients per WLAN by entering this command:

debug ap command "show capwap mcast mgid id mgid_value" Cisco_AP

Configuring Client Roaming

The Cisco UWN Solution supports seamless client naming across lightweight access points managed by the same controllers in the same mobility group on the same subnet, and across controllers in the same mobility group on different subnets. Also, in controllers shows a direct subnet, and across controllers in the same mobility group on the same subnet, and across controllers in the same mobility group on the same subnet, and across controllers in the same mobility group on different subnets. Also, in controllers subnet, and across controllers in the same mobility group on the same subnet, and across controllers in the same mobility group on the same subnet, and across controllers in the same mobility group on the same subnet.

You can adjust the default RF settings (RSSI, hysteresis, scan threshold, and transition time) to fine-tune the operation of client roaming using the controller GUI or CLI.

Intra-Controller Roaming

Each controller supports same-controller client roaming across access points managed by the same controller. This roaming is transparent to the client as the session is sustained, and the client continues using the same DHCP-assigned or client-assigned IP address. The controller provides DHCP functionality with a relay function. Same-controller roaming is supported in single-controller deployments and in multiple-controller deployments.

Inter-Controller Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group and on the same subnet. This roaming is also transparent to the client because the session is sustained and a tunnel between controllers allows the client to continue using the same DHCP- or client-assigned P address as long as the session remains active. The tunnel is tom down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client P address or a 1825-24." client auto-P address or when the operator-set ession time to its executed.

Inter-Subnet Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active. The tunnel is tom down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 1052647. 'client auto-Padress or when the operator-set user timoto is exceeded.

Voice-over-IP Telephone Roaming

802.11 voice-over-IP (b/P) telephones actively seek out associations with the strongest RF signal to ensure the best quality of service (QoS) and the maximum throughput. The minimum VolP telephone requirement of 20-millisecond or shorter latency time for the rearing hand/over is easily met by the Cisco UNN Solution, which has an average hand/over latency of 5 or fewer milliseconds when open authentication is used. This short latency period is controlled by controllers rather than allowing independent access points to negotiete roaming hand/overs.

The Cisco UWN Solution supports 802.11 VoIP telephone roaming across lightweight access points managed by controllers on different subnets, as long as the controllers are in the same mobility group. This roaming is transparent to the VoIP telephone because the session is sustained and a turnel between controllers allows the VoIP telephone to continue using the same DHCP-assigned P address as long as the session remains active. The turnel is toon down, and the VoIP client must reauthenticate when the VoIP telephone and the VoIP client must reauthenticate when the VoIP telephone and the VoIP client must reauthenticate when the VoIP telephone and the VoIP client must reauthenticate when the VoIP telephone and the VoIP client must reauthenticate when the VoIP telephone and the VoIP client must reauthenticate when the VoIP telephone and the VoIP client must reauthenticate when the VoIP telephone and the VoIP client must reauthenticate when the VoIP telephone and the VoIP client must reauthenticate when the VoIP telephone and the VoIP client must reauthenticate when the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP telephone the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the the VoIP telephone and the VoIP client must reauthenticate the telephone and the VoIP client must reauthent

CCX Laver 2 Client Roaming

The controller supports five CCX Layer 2 client roaming enhancements:

- Access point assisted roaming—This feature helps clients save scanning time. When a CCXv2 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point.
 Rearing time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point is a sport the client immediately after association. The access point is a client immediately after association.
- Enhanced neighbor list—This feature focuses on improving a CCXv4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbor susing a neighbor-list update unicast message.
- Enhanced neighbor list request (E2E)—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a CCX environment. Specifically, it must be request and replies with the current CCX roaming subjects for the access point to which the client is associated.

9

Note To see whether a particular client supports E2E, choose Wireless > Clients on the controller GUI, click the Detail link for the desired client, and look at the E2E Version text box under Client Properties.

- son report-This feature enables CCXv4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.
- Directed roam request---This feature enables the controller to send directed roam requests to the client in situations when the controller can better service the client on an access point different from the one to which it is associated. In this case, the controller sends the client a list of the best access points that it can join. The client can either honor or ignore the directed roam request. Non-CCX dients and clients running CCXv3 or below must not take any action. No configuration is required for this feature

Controller software release 4.2 or later releases support CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to generate and respond to CCX frames appropriately. Clients must support CCXv4 or v5 (or CCXV2 for access point assisted rearring) in order to utilize these rearring enhancements. See the "<u>Configuring Cisco Client</u> <u>Exercision" sector for more information on CCX</u>.



show network summary	show	network	summary	
----------------------	------	---------	---------	--

Information similar to the following appears: RF-Network Name..... ctr14404 Web Mode Web Mode...... Secure Web Mode..... Enable Secure Web Mode Cipher-Option High..... Disable Secure Web Mode Cipher-Option SSLv2..... Enable

IP/MAC Addr Binding Check Enabled

Configuring Quality of Service

Quality of service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. The controller supports four QoS levels:

- · Platinum/Voice-Ensures a high quality of service for voice over wireless
- Gold/Video—Supports high-quality video applications · Silver/Best Effort-Supports normal bandwidth for clients. This is the default setting
- Bronze/Background-Provides the lowest bandwidth for guest services

6

Note VolP clients should be set to Platinum

You can configure the bandwidth of each QoS level using QoS profiles and then apply the profiles to WLANs. The profile settings are pushed to the clients associated to that WLAN. In addition, you can create QoS roles to specify different bandwidth levels for regular and guest users. Follow the instructions in this section to configure QoS profiles and QoS roles.

Configuring Quality of Service Profiles

You can use the controller GUI or CLI to configure the Platinum, Gold, Silver, and Bronze QoS profiles

Using the GUI to Configure QoS Profiles To configure QoS profiles using the controller GUI, follow these steps

Step 1 Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles

To disable the radio networks, choose Wireless > 802.11a/n or 802.11b/g/n > Network , unselect the 802.11a (or 802.11b/g) Network Status check box, and click Apply

Step 2 Choose Wireless > QoS > Profiles to open the QoS Profiles page.

Step 3 Click the name of the profile that you want to configure to open the Edit QoS Profile page (see Figure 4-28).

Figure 4-28 Edit QoS Profile Page



Step 5 Define the average data rate for TCP traffic per user by entering the rate in Kbps in the Average Data Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the running.

Step 6 Define the peak data rate for TCP traffic per user by entering the rate in Kbos in the Burst Data Rate text box. You can enter a value between 0 and 60.000 Kbos (inclusive). A value of 0 imposes no bandwidth restriction on the profile.

1 Note The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 7 Define the average real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the Average Real-Time Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwith testribition on the profile.

Step 8 Define the peak real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the Burst Real-Time Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no benefitive the restriction on the normality of the rate of the restriction on the normality.

A
Note The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 9 In the Queue Depth text box, enter the maximum number of packets that access points keep in their queues. Any additional packets are dropped.

Step 10 Choose 802.1p from the Protocol Type drop-down list and enter the maximum priority value in the 802.1p Tag text box to define the maximum value (0-7) for the priority tag associated with packets that fall within the profile

The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network 1

Note If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

- Step 11 Click Apply to commit your changes
- Step 12 Click Save Configuration to save your changes

Step 13 Reenable the 802.11a and 802.11b/g networks.

To enable the radio networks, choose Wireless > 802.11a/n or 802.11b/g/n > Network , select the 802.11a (or 802.11b/g) Network Status check box, and click Apply. Step 14 Follow the instructions in the "Assigning a QoS Profile to a WLAN" section to assign a QoS profile to a WLAN.

Using the CLI to Configure QoS Profiles

To configure the Platinum, Gold, Silver, and Bronze QoS profiles using the controller CLI, follow these steps

Step 1 Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands:

config 802.11a disable network

config 802.11b disable network

Step 2 Change the profile description by entering this comma

config qos description {bronze | silver | gold | platinum} description

Step 3 Define the average data rate in Kbps for TCP traffic per user by entering this command

config qos average-data-rate {bronze | silver | gold | platinum} rate 0

Note For the rate parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Step 4 Define the peak data rate in Kbps for TCP traffic per user by entering this command

config qos burst-data-rate {bronze | silver | gold | platinum} rate

Step 5 Define the average real-time rate in Kbps for UDP traffic per user by entering this command: config qos average-realtime-rate {bronze | silver | gold | platinum} rate Step 6 Define the peak real-time rate in Kbps for UDP traffic per user by entering this command: config qos burst-realtime-rate {bronze | silver | gold | platinum} rate Step 7 Specify the maximum percentage of RF usage per access point by entering this command: config qos max-rf-usage {bronze | silver | gold | platinum} usage_percentage Step 8 Define the maximum value (0-7) for the priority tag associated with packets that fall within the profile, by entering these commands: config qos protocol-type {bronze | silver | gold | platinum} dot1p

config gos dot1p-tag (bronze | silver | gold | platinum) tag The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network. 0

Note If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

Step 9 Reenable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands

config 802.11a enable network

config 802.11b enable network

Step 10 Follow the instructions in the "Assigning a QoS Profile to a WLAN" section to assign a QoS profile to a WLAN.

Configuring Quality of Service Roles

After you configure a QoS profile and apply it to a WLAN, it limits the bandwidth level of clients associated to that WLAN. Multiple WLANs can be mapped to the same QoS profile, which can result in bandwidth contention between regular users (such as employees) and guest users. In order to prevent guest users from using the same level of bandwidth as regular users, you can create QoS roles with different (and presumably lower) bandwidth contracts and assign them to guest users. You can use the controller GUI or CLI to configure up to ten QoS roles for guest users.

0

Note If you choose to create an entry on the RADIUS server for a guest user and enable RADIUS authentication for the WLAN on which web authentication is performed rather than adding a guest user to the local user database from the controller, you need to assign the QOS role on the RADIUS server is local guest-rolef. Arisespace attribute needs to be added on the RADIUS server with a datatype of "sting" and a return value of "11." This attribute is sent to the controller, when authentication occurs. If a role with the name returned from the RADIUS server is loud configured on the controller, the bandwith associated to that role is enforced for the guest user after authentication corplicates uscessfully.

Using the GUI to Configure QoS Roles To configure QoS roles using the controller GUI, follow these steps:

Ø.

Note Guest User role is not supported on Cisco 2106 Controller.

Step 1 Choose Wireless > QoS > Roles to open the QoS Roles for Guest Users page (see Figure 4-29)

Figure 4-29 QoS Roles for Guest Users Page

alada							nf gurat on	Pina Locout	
CISCO	KONHOF WOW	S <u>CONFOLLER</u>	WIRELESS	SECORIT	RONAGEREN	COMMONDS	HELP		
Wireless	QaS Rales for I	Guest Users						Ne m	
Access Points	Name								
Mesh	Cultade:								
HREAP Groups	Vendor	6							
▶ 002.11a/n									
▶ 002.11b/q/n									
Country									
timers									
T Q05									4
Prubles									
AC-85									2
is page shows any existing	QoS roles for guest users.								
0									
Note If you want to de	elete a QoS role, hover your	cursor over the blue	drop-down arrov	/ for that role an	d choose Remove.				

Step 3 In the Role Name text box, enter a name for the new QoS role. The name should uniquely identify the role of the QoS user (such as Contractor, Vendor, and so on).

Step 4 Click Apply to commit your changes.

Step 5 Click the name of the QoS role to edit the bandwidth of a QoS role. The Edit QoS Role Data Rates page appears (see Figure 4-30).

Figure 4-30 Edit QoS Role Data Rates Page

	Construction of the American Structure of the American
CISCO	RUNTLOR 77 NOP DUVLED HER MÜRELERE SECONDUM ARVAUEMENT GÖMMANDE HET.
Wireless	Edit QoS Role data rates Apply
Access Paints Mesh	QoS Kole Yame Cur zatir
HREAP Groups	Per User Bondwildth Contracts (k) *
) 802.11a/n	Ameraju Sala 2010 0
) 8U2.11b/g/n	Sunst Sale Raha 0
Country	Average Real-I me Mate U
Timers	Surst Keal-Time Mate U
* QoS Profiles Deps	
6	N
Note The values that you client to the acces	u configure for the per-user bandwidth contracts affect only the amount of bandwidth going downstream (from the access point to the wireless client). They do not affect the bandwidth for upstream traffic (from the se point).
Step 6 Define the average dat restriction on the QoS r	ta rate for TCP traffic on a per-user basis by entering the rate in Kbps in the Average Data Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth ole.
Step 7 Define the peak data ra restriction on the QoS r	ate for TCP traffic on a per-user basis by entering the rate in Kbps in the Burst Data Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth role.
•	
Note The Burst Data Ra	te should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.
Step 8 Define the average rea bandwidth restriction or	II-lime rate for UDP traffic on a per-user basis by entering the rate in Kbps in the Average Real-Time Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no n the QoS role.
Step 9 Define the peak real-tir bandwidth restriction or	me rate for UDP traffic on a per-user basis by entering the rate in Kbps in the Burst Real-Time Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no the QoS role.
•	
Note The Burst Real-Tin	ne Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.
Step 10 Click Apply to commi	It your changes.

Step 11 Click Save Configuration to save your changes.

Step 12 Apply a QoS role to a guest user, by following the steps in the "Using the GUI to Configure Local Network Users" section.

Using the CLI to Configure QoS Roles

27 of 45

0	for a more than the second sec			
Step 1 Create a QoS role	ror a guest user by entering this command:			
config netuser guest-role	create role_name			
\				
Note If you want to	delete a QoS role, enter this command:			
Step 2 Configure the bar	dwidth contracts for a QoS role by entering these con	mmands:		
 config netuser guest- 	role qos data-rate average-data-rate role_name rate	ate—Configures the average data rate for TCP traffic on a per-user basis.		
 config netuser guest- 	ole qos data-rate burst-data-rate role_name rate-	 Configures the peak data rate for TCP traffic on a per-user basis. 		
B				
Note The Burst Data	Rate should be greater than or equal to the Average [Data Rate. Otherwise, the QoS policy may block traffic to and from the wireless clie	nt.	
• config notuces quest	rela neo data rata averaga realtima rata raja, pop	no min. Configures the oversee cost time rate for LIDB traffic on a part user basis		
 config netuser guest- 	role qos data-rate burst-realtime-rate role_name r	rate—Configures the peak real-time rate for UDP traffic on a per-user basis.		
•				
×				
Note The Burst Real-	Fime Rate should be greater than or equal to the Aver	rage Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the v	vireless client.	
0				
Note For the role_r enter a value	ame parameter in each of these commands, enter a n	name for the new QoS role. The name should uniquely identify the role of the QoS 0 imposes no bandwidth restriction on the QoS role.	user (such as Contractor, Vendor, and	d so on). For the rate parameter, you c
Step 3 Apply a QoS role	to a guest user by entering this command:			
config netuser guest-role	apply username role_name			
⊢or example, the role of Con	tractor could be applied to guest user jsmith.			
Note If you do not a	issign a QoS role to a quest user, the Role text how in	the User Details shows the role as "default." The handwidth contracts for this use	are defined in the OoS profile for the	9 WLAN.
•				
Note If you want to	unassign a QoS role from a guest user, enter the con	nfig netuser guest-role apply username default command. This user now uses	the bandwidth contracts defined in th	ne QoS profile for the WLAN.
Step 4 Save your change	s by entering this command:			
save config	-			
Step 5 See a list of the c	urrent QoS roles and their bandwidth parameters by e	entering this command:		
show netuser guest-roles				
Information similar to the follo	wing appears:			
Role Name Average Data Rate		pr		
Burst Data Rate				
Average Realtime Rate Burst Realtime Rate.	· 100 100			
Average Data Rate	unconfigured			
Burst Data Rate	unconfigured			
Burst Data Rate Average Realtime Rate Burst Realtime Rate.	unconfigured unconfigured unconfigured			
Burst Data Rate Average Realtime Rate Burst Realtime Rate.	unconfigured unconfigured unconfigured ideo Parameters troller affect voice and/or video quality:			
Burst Data Rate Average Realtime Rate Burst Realtime Rate. onfiguring Voice and V Three parameters on the cor Call admission control Expedited bandwidth re Unscheduled automatic Each of these parameters is	unconfigured unconfigured unconfigured unconfigured ideo Parameters troller affect voice and/or video quality: quests power save delivery supported in Cisco Compatible Extensions (CCX) v4 i	and v5. See the "Configuring Claco Client Extensions" section for more information	i on CCX.	
Burst Data Rate Warsage Realtime Rate Burst Realtime Rate. Onfiguring Voice and V Three parameters on the cor Call admission control Expedited bandwidth re Unscheduled automatic Each of these parameters is CCX is not supported on the	unconfigured uncon	and v5. See the <u>"Configuring Cisco Client Extensions" section</u> for more information	i on CCX.	
Burst Data Rate Average Realtime Rate Burst Realtime Rate. Three parameters on the cor Call admission control Espedited bandwidht e Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM)	unconfigured unco	and v5. See the <u>"Configuring Cisco Client Extensions" section</u> for more information quality.	n on CCX.	
Burst Data Rate Nverage Realtime Rate. Burst Realtime Rate. Onfiguring Voice and V Three parameters on the co Call admission control Expedited bandwidh re Unscheduled bandwidh re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission Control	unconfigured uncon	and v5. See the <u>"Configuring Cisco Client Extensions" section</u> for more information quality.	i on CCX.	
Burst Data Rate Narage Realtime Rate. Burst Realtime Rate. Onfiguring Voice and V Three parameters on the co Call admission control Expedited bandwidh re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission Control Call admission Control Call admission Control	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured	and v5. See the <u>"Configuring Cisco Client Extensions" section</u> for more information quality.	i on CCX.	in CCXv3 ensures sufficient QoS as lo
Burst Data Rate Average Realtime Rate. Burst Realtime Rate. Configuring Voice and V Three parameters on the co Call admission control Expedited bandwidh re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission Control Call admission control (CAC the wireless LAN is not comp andwighth.Based CaC	unconfigured unconfigured unconfigured unconfigured ideo Parameters troller affect voice and/or video quality: quests power save delivery supported in Cisco Compatible Extensions (CCX) v4 a AP1030. can be used to monitor and report issues with voice of enables an access point to maintain controlled qualit sated. However, in order to maintain QoS under differ	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. ty of service (QoS) when the wireless LAN is experiencing congestion. The Wi-F1 h ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba	i on CCX. Aultimedia (VMM) protocol deployed idwidit-based CAC and load-based (in CCXv3 ensures sufficient QoS as lo CAC.
Burst Data Rate Average Realtime Rate. Burst Realtime Rate. Difiguring Voice and V Three parameters on the co- call admission control Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission Control Call admission control (CAC the wireless LAN is not comp andwidth-Based CAC	unconfigured unconfigured unconfigured unconfigured unconfigur	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. Ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi h ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba	u on CCX.	in CCXv3 ensures sufficient QoS as to CAC.
Burst Data Rate werzage Realtime Rate. Burst Realtime Rate. Burst Realtime Rate. Three parameters on the co Call admission control Expedited bandwidth re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission Control Call admission control (CAC flaid admission control of Call admission control of Admission Control Gall admission control (CAC the wireless LAN is not cong andwidth-Based CAC andwidth-Based CAC andwidth-Based CAC admission control CAC (CAL)	unconfigured unco	and v5. See the " <u>Configuring Cisco Client Extensions</u> " section for more information quality. Ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is required to accept a new call and in turn enables the a um allowed number of calls with acceptable quality.	I on CCX.	In CCXv3 ensures sufficient QoS as to CAC.
Burst Data Rate Nerrage Realtime Rate Burst Realtime Rate. Donfiguring Voice and V Three parameters on the con- Call admission control Expedited bandwidth re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission Control Call admission control (CAC all admission control (CAC Bandwidth-based, or statc, all. The access point reject The UNAP must be configure	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured	and v5. See the <u>"Configuring Cisco Client Extensions</u> " section for more information quality. Ity of service (CoS) when the wireless LAN is experiencing congestion. The Wi-FI h ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is required to accept a new call and in turn enables the a im allowed number of calls with acceptable quality.	i on CCX. fultimedia (WMM) protocol deployed indwidth-based CAC and load-based (ccess point to determine whether it is gured for Platinum CoS. To use band configuration instructions.	in CCXv3 ensures sufficient QoS as lo CAC.
Surst Data Rate verrage Realtime Rate surst Realtime Rate onfiguring Voice and V Three parameters on the con- Call admission control Expedited bandwidth re Unscheduled automatic Each of these parameters is CCX is not supported on the traffic stream metrics (TSM) all Admission Control Ball admission control (CAC he wireless LAN is not cong andwidth-based, or state, II. The access point reject the QS setting for a WLAN he WLAN must be configure	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigure	and v5. See the <u>"Configuring Cisco Client Extensions" section</u> for more information quality. Ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi h ing network loads, CAC in CCXv4 is required. Two types of CAC are available: ba m allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be confi of or the WLAN. See the <u>"Configuring 802.3 Bridging" section</u> for QoS and WIMM	on CCX. fultimedia (WMM) protocol deployed dwidth-based CAC and load-based (ccess point to determine whether it is gured for Platinum QoS. To use band onfiguration instructions.	in CCXv3 ensures sufficient QoS as lo CAC. capable of accommodating this partic width-based CAC with video applicatio
Burst Data Rate Nerrage Realtime Rate. Burat Realtime Rate. Diffiguring Voice and V Three parameters on the co- Call admission control Expedited bandwidth re Unscheduled bandwidth re Unscheduled automatic CCX is not supported on the Traffic stream metrics (TSM) all Admission Control Call admission Control Call admission Control CAL andwidth-based CAC Bandwidth-based or static, The QoS setting for a WLAN he WLAN must be configure You must enable admission	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigure	and v5. See the <u>"Configuring Cisco Client Extensions" section</u> for more information quality. Ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi fi ring network loads, CAC in CCXv4 is required. Two types of CAC are available: be th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or To use bandwidth-based CAC with voice applications, the WLAN must be configuring 802.3 Bridging" section for CaCs and WMM ad for the WLAN. See the <u>"Configuring 802.3 Bridging" section</u> for CaCs and WMM	I on CCX.	in CCXV3 ensures sufficient QoS as to CAC. : capable of accommodating this partic width-based CAC with video applicatio
Burst Data Rate Werrage Realtime Rate. Burat Realtime Rate. Burat Realtime Rate. Configuring Voice and V Three parameters on the co- expedited bandwidth re Unscheduled bandwidth re Unscheduled bandwidth re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission Control Call admission Control CAL Bandwidth-based CAC Bandwidth-based CAC Stream Call The Cos Setting for a WLAh re WLAN must be configure You must enable admission Cad-Based CAC	unconfigured unconfigured unconfigured unconfigured ideo Parameters troller affect voice and/or video quality: quests power save delivery supported in Cisco Compatible Extensions (CCX) v4 : AP1030. can be used to monitor and report issues with voice of enables an access point to maintain controlled qualit stead. However, in order to maintain QoS under differ CAC enables the client to specify how much bandwidt if the call if necessary in order to maintain QoS under differ CAC enables the client to specify how much bandwidt if the call if necessary in order to maintain QoS under differ CAC enables the client to specify how much bandwidt of cord QoS. Also, make sure that WMM is enable	and v5. See the " <u>Configuring Cisco Client Extensions</u> " section for more information quality. Ity of service (CoS) when the wireless LAN is experiencing congestion. The Wi-Fi I of service (CoS) when the wireless LAN is experiencing congestion. The Wi-Fi I ng network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. ort. To use bandwidth-based CAC with voice applications, the WLAN must be confi ad for the WLAN. See the " <u>Configuring BIC3.3 Biologing</u> " section for QoS and WMM. bled. Otherwise, bandwidth-based CAC does not operate property.	I on CCX. Aultimedia (WMM) protocol deployed idwidth-based CAC and load-based (ccess point to determine whether it is gured for Platinum QoS. To use band configuration instructions.	in CCXv3 ensures sufficient QoS as to CAC. : capable of accommodating this partic width-based CAC with video applicatio
Burst Data Rate Warrage Realtime Rate. Burst Realtime Rate. Burst Realtime Rate. Configuring Voice and V Three parameters on the co- expedited bandwidth re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission control Call admission control CAL Bandwidth-Based CAC The QoS setting for a WLAH the WLAN must be configure You must enable admission coad-Based CAC Load-based CAC incorporati	unconfigured unconfigured unconfigured unconfigured ideo Parameters troller affect voice and/or video quality: quests power save delivery supported in Cisco Compatible Extensions (CCX) v4 i aP1030. can be used to monitor and report issues with voice of enables an access point to maintain controlled qualit seted. However, in order to maintain CoS under differ CAC enables the client to specify how much bandwidt is the call if necessary in order to maintain AcaS under differ CAC enables the client to specify how much bandwidt is the call if necessary in order to maintain the maximu determines the jevel of bandwidth-based CAC suppo d for Gold QoS. Also, make sure that WMM is enable control (ACM) for CCXv4 clients that have WMM enal	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. Ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi fi ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is required to accept a new call and in turn enables the a m allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with vioca applications, the WLAN must be confi do for the WLAN. See the <u>"Configuring 802.3 Bridging" section</u> for QoS and WIMM bled. Otherwise, bandwidth-based CAC does not operate property.	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. capable of accommodating this partic width-based CAC with video applicatio
Auret Data Rate Nurst Data Rate Nurst Data Rate arrat Realtime Rate Auret Realtime Rate Configuring Voice and V Three parameters on the co- Expedited bandwidth re- Unscheduled automatic ach of these parameters is CCX is not supported on the traffic stream metrics (TSM) all Admission Control Call admission control (CAC the wireless LAN is not compo- andwidth-Based CAC Bandwidth-Based CAC Bandwidth-Based CAC Sandwidth-Based CAC S	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigure	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. ty of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be confi ed for the WLAN. See the <u>"Configuring 802-3 Bridging" section</u> for QoS and WMM in bibled. Otherwise, bandwidth-based CAC does not operate property. e bandwidth consumed by all traffic types (including that from clients), co-channel a nPHY and channel impairment.	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. . capable of accommodating this partic width-based CAC with video application annel interference, for voice application
Auret Data Rate Warret Data Rate Nerrage Realtime Rate Barst Realtime Rate Configuring Voice and V Three parameters on the co- Call admission control Expedited bandwidth re- Unscheduled automatic Each of these parameters is CCX is not supported on the CCX is not supported on the Call admission Control Call admission control (CAC he wireless LAN is not comport andwidth-Based CAC Candwidth-Based CAC Andwidth-Based CAC Andwidth-Based CAC Cad-based CAC incorporation. Cad-Based C	unconf.igured unconf.igured unconf.igured unconf.igured unconf.igured unconf.igure	and v5. See the " <u>Configuring Cisco Client Extensions</u> " section for more information quality. ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is negurined to accept a new call and in turn enables the a um allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be confi- d for the WLAN. See the " <u>Configuring 80:2.3 Biologing</u> " section for QoS and WMM. blied. Otherwise, bandwidth-based CAC does not operate properly. a bandwidth consumed by all traffic types (including that from clients), co-channel a n PHY and channel impairment. Ization of the RF channel (that is, the percentage of bandwidth that has been exhap	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. : capable of accommodating this partic width-based CAC with video application annel interference, for voice application additional calls that the access point co os under all conditions of WLAN loadir
Surst Data Rate Verrage Realtime Rate. Burst Realtime Rate Configuring Voice and V Three parameters on the co- Call admission control Expedited bandwidth re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission Control Call admission control (CAC he wireless LAN is not cong andwidth-Based CAC Isal admission control (CAC he wireless LAN is not cong andwidth-Based CAC Isal admission control (CAC he wireless LAN is not cong andwidth-Based CAC isad-based CAC incorporat CAC also cover n load-based CAC, the acco and-based CAC, the acco spont and the theory of the acco spont and the theory of the acco spont and the accomposited the accomposited and based CAC is accover in load-based CAC, the acco and hereference.	unconfigured u	and v5. See the <u>"Configuring Cisco Client Extensions</u> " section for more information quality. ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-FI for ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba am allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be confi of or the WLAN. See the <u>"Configuring 802.3 Bridging" section</u> for QoS and WMM. blod. Otherwise, bandwidth-based CAC does not operate property. blod. Otherwise, bandwidth-based CAC does not operate property. a bandwidth consumed by all traffic types (including that from clients), co-channel a n PHY and channel impairment. zation of the RF channel (that is, the percentage of bandwidth that has been exha. Ibandwidth to support that call. By doing so, load-based CAC prevents oversubscr	I on CCX.	In CCXv3 ensures sufficient QoS as to CAC. In capable of accommodating this particle width-based CAC with video application annel interference, for voice application additional calls that the access point ca additional calls that the access point ca big under all conditions of WLAN loader
Aurst Data Rate Aurst Data Rate Aurst Realtime Rate Aurst Realtime Rate Aurst Realtime Rate Aurst Realtime Rate Aurst Realtime Rate Aurst Realtime Rate Colored Section 2016 Expedited bandwidth re Unscheduled automatic Each of these parameters is CCX Is not supported on the fraffic stream metrics (TSM) all Admission Control Call Admission Contr	unconfigured u	and v5. See the <u>"Configuring Cisco Client Extensions</u> " section for more information quality. Ity of service (CoS) when the wireless LAN is experiencing congestion. The Wi-FI h management of the section of the WLAN must be coffi- an allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be coffi- al for the WLAN. See the <u>"Configuring 802.3 Bridging" section</u> for CoS and WMM- bled. Otherwise, bandwidth-based CAC does not operate property. e bandwidth consumed by all traffic types (including that from clients), co-channel a n PHY and channel impairment. zation of the RF channel (that is, the percentage of bandwidth that has been exhan blendwidth to support that call. By doing so, lead-based CAC, prevents oversubscr ad-based CAC, the access points start using bandwidth-based CAC.	I on CCX.	In CCXV3 ensures sufficient QoS as lo CAC. : capable of accommodating this particl width-based CAC with video application annel interference, for voice application additional calls that the access point c oS under all conditions of WLAN loads
Auret Data Rate Auret Data Rate verrage Realtime Rate auret Realtime Rate Infiguring Voice and V Three parameters on the co Call admission control Expedited bandwidth re Unscheduled automatic ach of these parameters is CCX is not supported on the raffic stream metrics (TSM) all Admission Control Call admission Control CAC is not supported on the writeless LAN is not cong modulth-based CAC Bandwidth-Based CAC and value able admission cod-based CAC able cover in backbased CAC able cover in backbased CAC, the acco admitt. The access point admiter neterence. Lad-based CAC is support	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigure	and v5. See the <u>"Configuring Cisco Client Extensions" section</u> for more information quality. Ity of service (CoS) when the wireless LAN is experiencing congestion. The VI-FI it ing network loads, CAC in CCXv4 is required. Two types of CAC are available: be th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be coffi- do for the WLAN. See the <u>"Configuring 802.3 Bridging" section</u> for CoS and WMM bibled. Otherwise, bandwidth-based CAC does not operate property. e bandwidth consumed by all traffic types (including that from clients), co-channel a nPHY and channel impairment. Ization of the RF channel (that is, the percentage of bandwidth that has been extra beandwidth to support that call. By doing so, load-based CAC, prevents oversubscr	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. : capable of accommodating this partici width-based CAC with video application annel interference, for voice application additional calls that the access point co oS under all conditions of WLAN loadin
Aurat Data Rate Aurat Data Rate versage Realtime Rate Aurat Realtime Rate Aurat Realtime Rate Aurat Realtime Rate Aurat Realtime Rate Configuring Voice and V Three parameters on the co. Call admission control Call Admission Control	unconfigured unconfigured unconfigured unconfigured ideo Parameters troller affect voice and/or video quality: quests power save delivery supported in Cisco Compatible Extensions (CCX) v4 i (AP1030). can be used to monitor and report issues with voice i enables an access point to maintain controlled qualit seted. However, in order to maintain CoS under differ CAC enables the client to specify how much bandwidt is the call if necessary in order to maintain the maximu (determines the level of bandwidth-based CAC support of for Gold CoS. Also, make sure that WMM is enable control (ACM) for CCXv4 clients that have WMM enail is a measurement scheme that takes into account the the additional bandwidth consumption resulting from so pont controludy measures and updates the ulits its a new call only if the channel has enough unused d only on lightweight access points. If you disable to rests	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. Ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or. To use bandwidth-based CAC with vioce applications, the WLAN must be confi- d for the WLAN. See the <u>"Configuring 802.3 Bridging" section</u> for QoS and WMM bled. Otherwise, bandwidth-based CAC does not operate property. take channel impairment. zation of the RF channel (that is, the percentage of bandwidth that has been exhau- bandwidth to support that call. By doing so, load-based CAC prevents oversubscr ad-based CAC, the access points start using bandwidth-based CAC.	I on CCX.	in CCXv3 ensures sufficient QoS as lo DAC. capable of accommodating this particle width-based CAC with video application annel interference, for voice application additional calls that the access point ca oS under all conditions of WLAN loading sources the surger of the surger of the surger of the surger sources the surger of the surger
Aurat Data Rate Aurat Data Rate versage Realtime Rate Aurat Realtime Rate Aurat Realtime Rate Aurat Realtime Rate Configuring Voice and V Three parameters on the co. Call admission control Expedited bandwidth re Unscheduled automatic ach of these parameters is CCX is not supported on the traffic stream metrics (TSM) II Admission Control Call Admissio	unconfigured uncon	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. ty of service (CoS) when the wireless LAN is experiencing congestion. The Wi-Fi h ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or To use hardwidth-based CAC with viole applications, the WLAN must be confi- bled. Otherwise, bandwidth-based CAC does not operate property. e bandwidth consumed by all traffic types (including that from clients), co-channel a DPHY and channel impairment. Ization of the RF channel (that is, the percentage of bandwidth that has been exha bandwidth to support that call. By doing so, lead-based CAC prevents oversubscr ad-based CAC, the access points start using bandwidth-based CAC. regency of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress.	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. capable of accommodating this partici- width-based CAC with video application annel interference, for voice application additional calls that the access point or oS under all conditions of WLAN loadin condent of the access point of the access point of surger and the access point of the access point of the access additional calls that the access point of the acc
Jurset Data Rate versage Real-Line Ratt. Jurset Realtime Rate Infiguring Voice and V hree parameters on the co- Call admission control Expadited bandwidth re Unscheduled automatic ach of these parameters is CCX is not supported on the raffic stream metrics (TSM) II Admission Control II Admission Control II Admission control (CAC ne wireless LAN is not comp andwidth-Based CAC andwidth-Based CAC andwidth-Based CAC and-based CAC acad-based CAC acad-based CAC is support pedited Bandwidth Reg he expedited bandwidth Reg he expedit	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. ty of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: be th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or. To use bandwidth-based CAC with violo applications, the WLAN must be confi- ted for the WLAN. See the <u>"Configuring 802.3 Bindging" section</u> for QoS and WMM of bibled. Otherwise, bandwidth-based CAC does not operate property. e bandwidth consumed by all traffic types (including that from clients), co-channel a n PHY and channel impairment. Lization of the RF-channel (that is, the percentage of bandwidth that bas been extan bandwidth to support that call. By doing so, load-based CAC prevents oversubsor ad-based CAC, the access points start using bandwidth-based CAC. regency of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress.	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. : capable of accommodating this partice width-based CAC with video application annel interference, for voice application additional calls that the access point or oS under all conditions of WLAN loadin condent of the access point or oS under all conditions of WLAN loadin socives this request, it attempts to facil all expedited requests and processes
Jurset Data Rate versage Real-Line Ratt Jurset Realtime Rate onfiguring Voice and V Three parameters on the cou- Call admission control Expedited bandwidth re Unscheduled automatic ach of these parameters is CCX is not supported on thut iraflic stream metrics (TSM) III Admission Control III The Access point epict terreture admission Add-Based CAC inscorporation and-Based CAC inscorporation and-Based CAC inscorporation III Admission Control III Admission Control III The Access point epict III The Access point epict III The Access point epict III The Access point admission III The Access an ormalia III The Access an ormalia III The Acces	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured	and v5. See the "Configuring Cisco Client Extensions" section for more information quality. ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is negurined to accept a new call and in turn enables the a am allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be confi- ted for the WLAN. See the "Configuring 80:2.3 Biologing" section for QoS and WMM. blied. Otherwise, bandwidth-based CAC does not operate properly. a bandwidth consumed by all traffic types (including that from clients), co-channel a m PHY and channel impairment. Ization of the RF channel (that is, the percentage of bandwidth that has been exhap- bandwidth to support that call. By doing so, load-based CAC, prevents oversubscri- ad-based CAC, the access points start using bandwidth-based CAC. regency of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. vased CAC. Expedited bandwidth requests are disabled by default. When this featu sts and expedited bandwidth requests.	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. : capable of accommodating this partic width-based CAC with video application annel interference, for voice application additional calls that the access point ca or of whether the access point ca additional calls that the access point ca so under all conditions of WLAN loadin sceives this request, it attempts to facil all expedited requests and processes
Jurset Data Rate Jurset Data Rate verrage Realtime Rate Infiguring Voice and V Three parameters on the co Call admission control Expedited bandwidth re Unscheduled automatic izach of these parameters is income the second second second CXIs not supported on the raffic stream metrics (TSM) II Admission Control CAL is not supported on the raffic stream metrics (TSM) II Admission Control CAL is not supported on the raffic stream metrics (TSM) II Admission Control CAL is not supported on the raffic stream metrics (TSM) II Admission Control CAL is not supported on the raffic stream metrics (TSM) II Admission Control CAL is not supported on the raffic stream metrics (TSM) II Admission Control CAL is not supported on the raffic stream metrics (TSM) II Admission Control CAL is not supported on the raffic stream metrics (TSM) II Admission Control CAL is not supported on the raffic stream metrics (TSM) ad-Based CAC is support hereforence. Load-based CAC is support predited Bandwidth Req The expedited bandwidth Req The expedited bandwidth resonant SPEC requests as normal like Table 4-3 for examples of the thereforence.	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured	and v5. See the <u>"Configuring Cisco Client Extensions" section</u> for more information quality. It of service (QoS) when the wireless LAN is experiencing congestion. The Wi-FI for ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba am allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be confi ad for the WLAN. See the <u>"Configuring 802.3 Bindging" section</u> for OoS and WMM. blied. Otherwise, bandwidth-based CAC does not operate property. Landwidth consumed by all traffic types (including that from clients), co-channel a n PHY and channel impairment. Ization of the RF channel (that is, the percentage of bandwidth that has been exhan. Is bandwidth os support that call. By doing so, load-based CAC. ad-based CAC, the access points start using bandwidth-based CAC. regency of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. asaed CAC. Expedited bandwidth requests are disabled by default. When this features sta and expedited bandwidth requests.	I on CCX.	in CCXv3 ensures sufficient QoS as to CAC. : capable of accommodating this particity width-based CAC with video application annel interference, for voice application additional calls that the access point or oS under all conditions of WLAN loadin calives this request, it attempts to facil all expedited requests and processes
Nurset Data Rate Nurset Data Rate verrage Realtime Rate Infiguring Voice and V hree parameters on the co Call admission control Expedited bandwidth re Unscheduled automatic cach of these parameters is CXIs not supported on the raffic stream metrics (TSM) II Admission Control Call Admission Control Control CAC Cand-based CAC is optored ad-based CAC has occer noad-based CAC is support padited Bandwidth Req he expedited bandwidth Req he expedited bandwidth Req PSPEC requests as normal isee Table 4-3 for examples of Cable 4-3 TSPEC Request	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured	and v5. See the <u>"Configuring Cisco Client Extensions</u> " section for more information quality. Ity of service (CoS) when the wireless LAN is experiencing congestion. The Wir-FI h imp network loads, CAC in CCXv4 is required. Two types of CAC are available: ba im allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be coffi- allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be coffi- allowed number of calls with acceptable quality. a for the WLAN. See the <u>"Configuring 802.3 Bridging" section</u> for CoS and WMM- bled. Otherwise, bandwidth-based CAC does not operate property. Label Otherwise, bandwidth-based CAC does not operate property. ad-based CAC, the access points start using bandwidth-based CAC. ad-based CAC, the access points start using bandwidth-based CAC. regency of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. asad CAC. Expedited bandwidth requests.	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. capable of accommodating this partici- width-based CAC with video application annel interference, for voice application additional calls that the access point ca additional calls that the access point calls that the access p
Aurat Data Rate Aurat Data Rate versage Realtime Rate Aurat Realtime Rate Aurat Realtime Rate Aurat Realtime Rate Aurat Realtime Rate Configuring Voice and V Three parameters on the co Expedited bandwidth re Unscheduled automatic cach of these parameters is CCX is not supported on the radic stream metrics (TSM) III Admission control (CAC Readwidth-Based CAC Bandwidth-Based CAC Bandwidth-Based CAC Bandwidth-Based CAC Bandwidth-Based CAC Cach-Based CAC is support Aud-Based CAC is support ad-Based CAC is support ad-Based CAC is support Padibased CAC is support Padibased CAC is support Padibased CAC is support Cach-Based CAC is support Cach-Based CAC is support Cach-Based CAC is support Padibased CAC is support Cach-Based CAC is support Cach Cach is	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured ideo Parameters troller affect voice and/or video quality: quests power save delivery supported in Cisco Compatible Extensions (CCX) v4 i AP1030. Can be used to monitor and report issues with voice i enables an access point to maintain controlled qualit ested. However, in order to maintain CoS under diffe CAC enables the client to specify how much bandwidt is the call if necessary in order to maintain the maxim idetermines the level of bandwidth-based CAC support for Gold CoS. Also, make sure that WMM is enable control (ACM) for CCXv4 clients that have WMM enable as a measurement scheme that takes into account the s the additional bandwidth consumption resulting from s so pont continuous/ measures and updates the ulits its a new call only if the channel has enough unused ad only on lightweight access points. If you disable to rests (SPEC requests. at TSPEC requests. at TSPEC requests anding Examples Reserved bandwidth for voice calls 1	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. ty of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: be th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or. To use bandwidth-based CAC with vioce applications, the WLAN must be confi- ded for the WLAN. See the <u>"Configuring 802.3 Bridging" section</u> for QoS and WMM tabled. Otherwise, bandwidth-based CAC does not operate property. tabled. Otherwise, bandwidth-based CAC does not operate property. tabled. Otherwise, bandwidth-based CAC does not operate property. ad-based CAC, the access points start using bandwidth-based CAC. Import of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. sased CAC. Expedited bandwidth requests are disabled by default. When this featu stand expedited bandwidth requests. Usage 2	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. capable of accommodating this particle width-based CAC with video application annel interference, for voice application additional calls that the access point ca of under all conditions of WLAN loading additional calls that the access point ca additional calls that the access point calls the access point calls that the access point call
Auret Data Rate Auret Data Rate werzage Realtime Rate arret Realtime Rate Auret Realtime Rate Configuring Voice and V Three parameters on the co. Call admission control Expadited bandwidth re Unscheduled automatic ach of these parameters is CCX is not supported on the Traffic stream metrics (TSM) II Admission Control Call The access point reject. The Oco Sesting for a WLAN the WLAN must be configure The access point admission (CAC In add- Based CAC is support Cald-based CAC is support Cald-based CAC is support padited Bandwidth Reg Paditable 4-3 TSPEC Request CAC Mode Resolution based based based Call Admission Control Call Admission Control Cal	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured	and v5. See the "Configuring Claco Client Extensions" section for more information quality. ty of service (CoS) when the wireless LAN is experiencing congestion. The Wi-Fi h ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is required to accept a new call and in turn enables the a m allowed number of calls with acceptable quality. or. To use hardwidth-based CAC with voice applications, the WLAN must be confi- ted for the WLAN. See the "Configuring 802.3 Bridging" section for CoS and WMM or bled. Otherwise, bandwidth-based CAC does not operate property. tabled. Otherwise, bandwidth-based CAC does not operate property. e bandwidth consumed by all traffic types (including that from clients), co-channel a DHY and channel impairment. Ization of the RF-channel (that is, the percentage of bandwidth that has been exhan 1 bandwidth to support that call. By doing so, load-based CAC prevents oversubscr ad-based CAC, the access points start using bandwidth-based CAC. regency of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. asade CAC. Expedited bandwidth requests are disabled by default. When this featu ests and expedited bandwidth requests. [Usage 2] 1 and then 750'	Autimedia (WMM) protocol deployed individit-based CAC and load-based of development of the second s	in CCX/3 ensures sufficient QoS as lo CAC. capable of accommodating this particle width-based CAC with video application annel interference, for voice application additional calls that the access point ce oS under all conditions of WLAN leader celives this request, it attempts to facil all expedited requests and processes TSPEC with Expedited Bandwidth Request
Aurst Data Rate Wurstge Realtime Rate. Aurst Realtime Rate. Aurst Realtime Rate. Configuring Voice and V Three parameters on the co- Expedited bandwidth re Unscheduled automatic ach of these parameters is CCX is not supported on the Traffic stream metrics (TSM) II Admission Control Call admission control (CAC Ten wireless LAN is not compo- andwidth-Based CAC andwidth-Based CAC andwidth-Based CAC andwidth-Based CAC andwidth-Based CAC andwidth-Based CAC and-based CAC incorporation coad-based CAC incorporation coad-based CAC in support pour unust enable admission coad-based CAC is support of head-based CAC is support of head-based CAC is support of head-based CAC is support of head-based CAC is support populited Bandwidth Req The expedited ban	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigure	and v5. See the "Configuring Claco Client Extensions" section for more information quality. ty of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be confi- ted for the WLAN. See the "Configuring 502.3 Binglang" section for QoS and WMM billed. Otherwise, bandwidth-based CAC does not operate property. e bandwidth consumed by all traffic types (including that from clients), co-channel a n PHY and channel impairment. Ization of the RF-channel (that is, the percentage of bandwidth-based CAC. regency of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. aseed CAC. Expedited bandwidth requests are disabled by default. When this featu sts and expedited bandwidth requests. Usage 2 Less than 75%	I on CCX.	in CCXv3 ensures sufficient QoS as to CAC. capable of accommodating this partice width-based CAC with video application annel interference, for voice application additional calls that the access point ca oS under all conditions of WLAN loadin cervices this request, it attempts to facil all expedited requests and processes TSPEC with Expedited Bandwidth Request Admitted
Burst Data Rate Werrage Realtime Rate. Burat Realtime Rate. Burat Realtime Rate. Configuring Voice and V Three parameters on the co- Call admission control Expedited bandwidth re Unscheduled bandwidth re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM all Admission Control Call Ad	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured	and v5. See the <u>"Configuring Cisco Client Extensions" section</u> for more information quality. ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is negurined to accept a new call and in turn enables the a am allowed number of calls with acceptable quality. ort. To use bandwidth-based CAC with voice applications, the WLAN must be confi- ted for the WLAN. See the <u>"Configuring 80:2.3 Bindgang" section</u> for QoS and WMM. bled. Otherwise, bandwidth-based CAC does not operate properly. abled. Otherwise, bandwidth-based CAC does not operate properly. a bandwidth consumed by all traffic types (including that from clients), co-channel a m PHY and channel impairment. Ization of the RF channel (that is, the percentage of bandwidth that has been exhat bandwidth to support that call. By doing so, load-based CAC, prevents oversubscri- ad-based CAC, the access points start using bandwidth-based CAC. Improv of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. sased CAC. Expectited bandwidth requests are disabled by default. When this featu sts and expedited bandwidth requests. Usage <u>2</u> Less than 75%. Between 75% and 90% (reserved bandwidth for voice calls exhausted)	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. : capable of accommodating this partic width-based CAC with video application annel interference, for voice application additional calls that the access point ca of under all conditions of WLAN loadin sceives this request, it attempts to facil all expedited requests and processes TSPEC with Expedited Bandwidth Request Admitted Admitted
Burst Data Rate Burst Data Rate Proverage Realtime Rate. Burat Realtime Rate. Burat Realtime Rate. Configuring Voice and V Three parameters on the co- Call admission control Expedited bandwidth re Unscheduled automatic CCX is not supported on the Traffic stream metrics (TSM) all Admission Control Call admission Control CAC and Admission Control CAC and Admission Control CAC admission Control Call Admission Co	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured	and v5. See the <u>"Configuring Cisco Client Extensions" section</u> for more information quality. Ity of service (QoS) when the wireless LAN is experiencing congestion. The Wi-FI A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba am allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be confi of or the WLAN. See the <u>"Configuring 802.3 Bindging" section</u> for OoS and WMM allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be confi d for the WLAN. See the <u>"Configuring 802.3 Bindging" section</u> for OoS and WMM bled. Otherwise, bandwidth-based CAC does not operate property. a bandwidth consumed by all traffic types (including that from clients), co-channel a DPHY and channel impairment. Ization of the RF channel (that is, the percentage of bandwidth that has been exhan bendwidth to support that call. By doing so, load-based CAC. prevents oversubscr ad-based CAC, the access points start using bandwidth-based CAC. Improved a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. asade CAC. Expedited bandwidth requests are disabled by default. When this featu sts and expedited bandwidth requests. Usage <u>2</u> Less than 75%. Behveen 75% and 90% (reserved bandwidth for voice calls exhausted) More than 90%	I on CCX.	in CCXV3 ensures sufficient QoS as to CAC. is capable of accommodating this partici- width-based CAC with video application annel interference, for voice application additional calls that the access point or or or o
Burst Data Rate Nerrage Realtime Rate. Burst Realtime Rate. Burst Realtime Rate. Configuring Voice and V Three parameters on the co- expedited bandwidth re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission control Call admission control Call admission control Call admission control CAL Bandwidth-Based CAC Bandwidth-Based CAC Bandwidth-Based CAC Bandwidth-Based CAC Load-Based CAC is support in load-Based CAC is support and-Based CAC is support and-Based CAC is support and-Based CAC is support calcad-based CAC is support the expedited Bandwidth Reg Data Call Call Call Call Call Call Call CAC Mode Bandwidth-Based CAC Bandwidth-Based CAC is support the urgency of the call in an Vou can apply expedited bandwidth Ref Call Call Call Call Call Call Call Cal	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured unconfigured ideo Parameters troller affect voice and/or video quality: quests power save delivery supported in Cisco Compatible Extensions (CCX) v4 i AP1030. can be used to monitor and report issues with voice i enables an access point to maintain controlled qualit ested. However, in order to maintain CoS under diffe CAC enables the client to specify how much bandwidt is the call if necessary in order to maintain the maxim idetermines the level of bandwidth-based CAC support for Gold CoS. Also, make sure that WMM is enable control (ACM) for CCXv4 clients that have WMM enables as point confinuous/ measures and updates the ulits its a new call only if the channel has enough unused ad only on lightweight access points. If you disable to rests ipset feature enables CCXv5 clients to indicate the ur way possible without potentially altering the quality o frSPEC requests. at TSPEC requests Reserved bandwidth for voice calls 1 75% (default setting)	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. ty of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: be th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or. To use bandwidth-based CAC with vioce applications, the WLAN must be confi- ded for the WLAN. See the <u>"Configuring 802.3 Bridging" section</u> for QoS and WMM tabled. Otherwise, bandwidth-based CAC does not operate property. tabled. Otherwise, bandwidth-based CAC does not operate property. ad-based CAC, the access points start using bandwidth-based CAC. Interpret of the table is the percentage of bandwidth-based CAC. ad-based CAC, the access points start using bandwidth-based CAC. Interpret of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. assed CAC. Expedited bandwidth requests are disabled by default. When this featu start and expedited bandwidth requests. Usage <u>2</u> Less than 75%. Between 75% and 90% (reserved bandwidth for voice calls exhausted) More than 90% Less than 75%.	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. capable of accommodating this partic- width-based CAC with video application annel interference, for voice application additional calls that the access point cr of under all conditions of WLAN loadi conditions of WLAN loadi additional calls that the access point cr additional calls that the access point cr of under all conditions of WLAN loadi additional calls that the access point cr additional ca
Burst Data Rate Warsage Realtime Rate. Burst Resultime Rate. Burst Resultime Rate. Diffiguring Voice and V Three parameters on the co- Expedited bandwidth re Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM) all Admission Control Call admission Control CAL Bandwidth-Based CAC Bandwidth-Based CAC Bandwidth-Based CAC Load-Based CAC is support of Load-Based CAC is support conterference. Load-Based CAC is support conterference. Load-Based CAC is support rSPEC requests as normal See Table 4-3 TSPEC Request CAC Mode Bandwidth-Based CAC	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigure	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. ty of service (CoS) when the wireless LAN is experiencing congestion. The Wi-Fi h ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or. To use hardwidth-based CAC with voice applications, the WLAN must be confi- bled. Otherwise, bandwidth-based CAC does not operate property. tabled. Otherwise, bandwidth-based CAC does not operate property. e bandwidth consumed by all traffic types (including that from clients), co-channel a DPHY and channel impairment. Ization of the RF-channel (that is, the percentage of bandwidth-based CAC. repency of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. asaed CAC. Expedited bandwidth requests are disabled by default. When this featu sts and expedited bandwidth requests. Usage <u>2</u> Less than 75% Between 75% and 90% (reserved bandwidth for voice calls exhausted) More than 90% Less than 75%	I on CCX Aultimedia (WMM) protocol deployed indwidth-based CAC and load-based (dwidth-based CAC and load-based (coess point to determine whether it is gured for Platinum QoS. To use band configuration instructions.	in COX/3 ensures sufficient QoS as lo CAC. capable of accommodating this particle width-based CAC with video application annel interference, for voice application additional calls that the access point ca of under all conditions of WLAN loadin call superities and processes aceives this request, it attempts to facil all expedited requests and processes TSPEC with Expedited Bandwidth Request Admitted Admitted Admitted
Aurst Data Rate Wursige Realitime Rate. Aurst Realitime Rate. Aurst Realitime Rate. Configuring Voice and V Three parameters on the co- expedited bandwidth re- Unscheduled automatic ach of these parameters is CCX is not supported on the fraffic stream metrics (TSM) II Admission Control Call Admission Control Cald Admission Control Call Admission Control Cald Admission Control Call	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigure	and v5. See the <u>"Configuring Claco Client Extensions" section</u> for more information quality. ty of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: be th or shared medium time is required to accept a new call and in turn enables the a mallowed number of calls with acceptable quality. or. To use bandwidth-based CAC with vice applications, the WLAN must be confi- bled. Otherwise, bandwidth-based CAC does not operate property. e bandwidth consumed by all traffic types (including that from clients), co-channel a PHY and channel impairment. Ization of the RF-channel (that is, the percentage of bandwidth-based CAC. regency of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. ased CAC. Expedited bandwidth requests are disabled by default. When this featu ets and expedited bandwidth requests. Usage <u>2</u> Less than 75% Between 75% and 90% (reserved bandwidth for voice calls exhausted) More than 90%	I on CCX.	in CCX/3 ensures sufficient QoS as to CAC. capable of accommodating this partice width-based CAC with video application annel interference, for voice application additional calls that the access point ca os under all conditions of WLAN loadin additional calls that the access point ca society of the access of the access point ca additional calls that the acces
Auret Data Rate Auret Data Rate werrage Realtime Rate Auret Realtime Rate Auret Realtime Rate Configuring Voice and V Three parameters on the co Call admission control Expedited bandwidth e Unscheduled automatic Each of these parameters is CCX is not supported on the Traffic stream metrics (TSM all Admission Control Call Admissio	unconfigured unconfigured unconfigured unconfigured unconfigured unconfigure	and v5. See the "Configuring Cisco Client Extensions" section for more information quality. ty of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi A ring network loads, CAC in CCXv4 is required. Two types of CAC are available: ba an allowed number of calls with acceptable quality. or. To use bandwidth-based CAC with voice applications, the WLAN must be confi- ted for the WLAN. See the "Configuring 80:2.3 Biologing" section for OoS and WMM blod. Otherwise, bandwidth-based CAC does not operate properly. e bandwidth consumed by all traffic types (including that from clients), co-channel a DFM of channel (that is the percentage of bandwidth that bace not- bandwidth to support that call. By doing so, load-based CAC prevents oversubscr ad-based CAC, the access points start using bandwidth-based CAC. regency of a WMM traffic specifications (TSPEC) request (for example, an e911 call of other TSPEC calls that are in progress. used CAC. Expedited bandwidth requests are disabled by default. When this featu sts and expedited bandwidth requests. Usage 2 Less than 75% Between 75% and 90% (reserved bandwidth for voice calls exhausted) More than 90% Less than 75%. Between 75% and 85% (reserved bandwidth for voice calls exhausted) More than 95% (the access points. For load-based CAC, the voice calls exhausted) More than 95% (the access points, For load-based CAC, the voice calls exhausted) More than 95% (the access points. For load-based CAC, the voice calls exhausted) More than 95% (the access points. For load-based CAC, the voice calls exhausted) More than 95% (the access points. For load-based CAC, the voice calls exhausted) More than 95% (the access points. For load-based CAC, the voice calls exhausted) More than 95% (the access points. For load-based CAC, the voice calls exhausted) More than 95% (the access points. For load-based CAC, the voice calls exhausted)	I on CCX.	in CCXv3 ensures sufficient QoS as lo CAC. capable of accommodating this partice width-based CAC with video application annel interference, for voice application additional calls that the access point ca os under all conditions of WLAN loadin additional calls that the access point ca socives this request, it attempts to facil all expedited requests and processes TSPEC with Expedited Bandwidth Request Admitted Admitted Admitted Admitted Admitted Rejected

28 of 45

0

U-APSD Unscheduled automatic power sa	ave delivery (U-APSD) is a QoS facility defined in IEEE	In the TSPEC is greater than 149 or the mean data rate is greater than 1 Kops.	e, this feature reduces the latency of traffic flow delivered over the
wireless media. Because U-APSE when WMM is enabled.	D does not require the client to poll each individual pack	xet buffered at the access point, it allows delivery of multiple downlink packets by sendir	ng a single uplink trigger packet. U-APSD is enabled automatically
Traffic Stream Metrics	MI AN) deployment traffic stream matrice (TCM) can be	such to manifer unice related matrice on the client operate point of interface. It reports	bath poplet latency and poplet loss. You are isolate poor using
quality issues by studying these r	reports.	y used to monitor voice-related metrics on the client-access point an interface, it reports	both packet latency and packet loss. You can isulate pool voice
statistics are captured. The client	and access point measure these metrics. The access in hasis and the downlink measurements on an access or) statistics between an access point and a client device that supports CLCV violate repoint also collects the measurements every 5 seconds, prepares 90-second reports, an init basis and maintains an brun's worth of historical data. To store this data, the control is the second second reports and the second	eleases, in the client is not CCX v4 or CCXv5 compliant, only downil id then sends the reports to the controller. The controller organizes iller requires 32 MB of additional memory for unlink metrics and 4.8.1
for downlink metrics.	sittes the CI II or the CI I on a per radio hand basis (for	and basis and maintains an root is worth or matchical data. To store this data, the control	that it paraieto paraes reheste. After an apares point reacives the
configuration from the controller, i	it enables TSM on the specified radio band.	example, all ouz. Ha fadios). The controller saves the configuration in flash memory so	that it persists across republis. After all access point receives the
Access points support TSM in ho	oth local and hybrid-REAP modes		
To configure voice parameters us	sing the controller GUI, follow these steps:		
SIPs are available only on the Ci	isco 4400 Series and Cisco 5500 Series Controllers, ar	nd on the 1240, 1130, and 11n access points.	
Step 1 Make sure that the WL	AN is configured for WMM and the Platinum QoS level		
Step 2 Disable all WLANs with	h WMM enabled and click Apply .		
Step 3 Choose Wireless and	then Network under 802.11a/n or 802.11b/g/n, unselect	the 802.11a (or 802.11b/g) Network Status check box, and click Apply to disable the ra-	dio network.
Step 4 Choose Wireless > 80	2.11a/n or 802.11b/g/n > Media. The 802.11a (or 802.1	1b) > Media page appears (see Figure 4-31). The Voice tab is displayed by default.	
Figure 4-31 802.11a/n > Voice Pa	irameters Page		
abab		Save Configuration Ping Log	cut Kefresh
CISCO	BON, CR. WLANS CON ROLLER RUT	ELERS RECORD MANAGEMEN COMMANDS HELP FEDRACK	
Wireless	802.11a(5 GHz) > Media		Apply
* Access Points	Volce Video Media		
All APs ⊯ Eaulis 202 tr. v			
302 114/1 302 111/0/1	Gall Admission Control (CAC)		
Advanced	Ac missic - Control (ACM)	C Lrabled	
Mirsh	har hased CAC	Er able J	
HKEAP Groups	"at: 41 Bandwidth (9-99)(6)		
# BD2.11a/m Netxc%	Expedited Lanux JU		
* FR* 3F Grouping	500 Codee	2.711	
те. 201	s P Acadwidta (ktas)	64	
Cilveraça Gisteral	S.P.Volte Sample Interval (msecs)	20 -	
Media ECC6 Commission	SALIDIT CAIS (C13)		
DFS (302.11)	Traffic Stream Metrics		
(8C2,L1 I) CleanA	Matrice Collection		<u>9</u>
+ 202.116/9/n	2		2077
Step 5 Select the Admission C	Control (ACM) check box to enable bandwidth-based C/	AC for this radio band. The default value is disabled.	
Step 7 In the Max RF Bandwid	the text box, enter the percentage of the maximum banc	which allocated to clients for voice applications on this radio band. Once the client reac	ck poxes is disabled.
this radio band.			····· - ·····
The range is 5 to 85%. The sum The default is 75%.	of max bandwidth% of voice and video should not exce	ed 85%.	
Step 8 In the Reserved Roam	ing Bandwidth text box, enter the percentage of maximu	im allocated bandwidth that is reserved for roaming voice clients. The controller reserve	es this bandwidth from the maximum allocated bandwidth for
roaming voice clients.			
The default is 6%.			
Step 9 To enable expedited b	andwidth requests, select the Expedited Bandwidth che	sck box. By default, this text box is disabled.	
Step 10 From the SIP Codec	drop-down list, choose one of the following options to s	et the codec name. The default value is G.711. The options are as follows:	
User Defined G.711			
• G.729			
Step 11 In the SIP Bandwidth	(kbps) text box, enter the bandwidth in kilo bits per sec	ond.	
The possible range is 8 to 64. The default value is 64.			
۵			
 The SIP Bandwidth (kbps) text be Bandwidth (kbps) text box is set to 	ox is highlighted only when you select the SIP codec as to 8.	s User-Defined. If you choose the SIP codec as G.711, the SIP Bandwidth (kbps) text bo	ox is set to 64. If you choose the SIP codec as G.729, the SIP
Step 12 In the SIP Voice Sam	ple Interval (msecs) text box, enter the value for the sar	mole interval.	
Step 13 In the Maximum Calls	s text box, enter the maximum number of calls that can b	pe made to this radio. The maximum call limit includes both direct and roaming-in calls. If	f the maximum call limit is reached, new or roaming-in calls will
fail.			
The possible range is 0 to 25. The default value is 0, which indi	cates that there is no check for maximum call limit.		
Step 14 Select the Metrics Co	ellection check box to collect Traffic Stream Metrics. By	default, the box is unselected. That is, the traffic stream metrics is not collected by defa	ult.
Step 15 Click Apply to commit	your changes.		
Step 16 Reenable all WMM V	VLANs and click Apply.		
Step 17 Choose Network und	er 802.11a/n or 802.11b/g/n, select the 802.11a (or 802	.11b/g) Network Status check box, and click Apply to reenable the radio network.	
Step 18 Click Save Configura	tion to save your changes.		
Step 19 Repeat this procedur	e if you want to configure voice parameters for another	radio band (802.11a or 802.11b/g).	
Using the GUI to Configure Vid	leo Parameters		
To configure video parameters us	sing the controller GUI, follow these steps:		
Step 1 Make sure that the WL	AN is configured for WMM and the Gold QoS level.		
Step 2 Disable all WLANs with	h WMM enabled and click Apply .		
Step 3 Choose Wireless and	then Network under 802.11a/n or 802.11b/g/n, unselect	the 802.11a (or 802.11b/g) Network Status check box, and click Apply to disable the ra-	dio network.
Step 4 Choose Wireless > 80	2.11a/n or 802.11b/g/n > Media. The 802.11a (or 802.1	1b) > Media page appears (see Figure 4-32).	
Figure 4-32 802.11a > Video Para	ameters Page		



Step 6 Select the Admission Control (ACM) check box to enable video CAC for this radio band. The default value is disabled

Step 7 In the Max RF Bandwidth text box, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band.

The range is 5 to 85%. The sum of maximum bandwidth% of voice and video should not exceed 85%.

- The default is 0%.
- Step 8 Click Apply to commit your changes
- Step 9 Reenable all WMM WLANs and click Apply.

Step 10 Choose Network under 802.11a/n or 802.11b/g/n, select the 802.11a (or 802.11b/g) Network Status check box, and click Apply to reenable the radio network.

Step 11 Click Save Configuration to save your changes.

Step 12 Repeat this procedure if you want to configure video parameters for another radio band (802.11a or 802.11b/g).

Using the GUI to View Voice and Video Settings

To view voice and video settings using the controller GUI, follow these steps:

Step 1 Choose Monitor > Clients to open the Clients page (see Figure 4-33).

Figure 4-33 Clients Page

cisco	MONITOR 15 AV	DOVIEOU EE	WIRFLESS <u>S</u> ECURITY	NWARENENT C	Saza Cultigurador OMMANDS HELP	200 L	C <u>1</u> 0C.	Balte	sl
Monitar Summary	Clients Current Filter	lione	"Change Lilte 1 (Dee Lilte 1			Fotel	es I	8 of 1	
Access Points Statistics	Client MAC Addr COLL: 53 04(15)+0	AP Name devestus?st4480	WLAN Pro	lile Protoc	ol Status E Eccoing	Auth	Purl	WGB No	
 Roques 	C0:40 96 aC:E0:29 C0:40 96 aC 94:13	Maria-1242 Mana-1242	Lakinaka Lakinaka	JUL.11 302.11	t Fredine L Frediny	No Nu	2 2	Ko Ku	
Clients Multicast	C0:+0.06 ac(C0:0_ C0:+0.06 b1(b5:03	devosh(82):54(30 motAF?	Unknown Laknowa	302.1L 303.1	E Freding E Freding	No No	-	60 60	8
	C3:40 96 b1:f1:E1 C3:40 96 b1:f1:E1	devesh:02:54:50 Simall -70:55:70	Unknown U ruitwr	JUL.11 302.11	a Fropino a Froping	No Nu	2	Ko Ku	
	COMO DE DAVEFIEID	rhoter?	Larnesa	30.5.1	h Erching	No		65	0

Step 2 Click the MAC address of the desired client to open the Clients > Detail page (see Figure 4-34).

Figure 4-34 Clients > Detail Page

cisco	MORITOP WLANS CONTR	DLLER WIPELESS SEC. 7:	Y MANAGEMENT COM	Sayr Corfigi (rfan Eing Logailt Bafnas Matters - ELP
Monitar	Clients > Detail		< Hark	Apply Link Lest Remove
Summary	Glicent Properties		AP Properties	
Access Paints	YAC Address	10.40.96(71):5.25	AP Actross	Chiph 85:82:54:30
Statistics	IT Address	300:65 211 225	AP Note	C24C32132 b4 80
▶ CDP	L ent vpe	Kegular	AP INC.	COR 115
Roques	Jac : Name		WLAN Profile	N/A
Clients	Port Number	1	Stenus	Frening
PIUITICAST	Li per la pe	na rage ne it	Association (L)	
	VLAK 1D	1	602-11: Active location	Open Svelen
	.7.7× Version	Net Supported	Reason Code	c
	12L Version	Not 's upported	Status Codo	r
	Yubility Role	Jr as conatad	CT Pollable	Not Jmp emented
	Publicy Pear IP Address	4 .W	CT Poll Request	Not Jmp emented
	Policy Planager State	START	Shurt Preamble	Not 1 mp an ante 1
	" "ror Moce	Diset e 💌	rade.	Not top propted
	Managen ant Fran a	Чс	Channel Agility	Not log prophet
	Protection		I meaut	τ.
	Security Information	volk	WEF State	WER DisaL #
	Security Collegi Correlated	Чr		
	colicy cuto	'Y/A		
	Lincreption 'Liphe'	liche		
	EAP Type	<i>A</i> .N		
	Quality of Service Propert	ies		
	WMM Stale	D cabled		
	Chr. Leve	Silver		
	of ∰ Servicode Point (DSCP)	disabled		
	302.14 Tay	JisableJ		
	Average Cala Rate	Jisable J		
	Average Cool Time Pate	tisable t		
	Juist Date Pate	disabled		
	Burst Real-Time Rate	JisableJ		
	Client Statistics			
	Bytes Received	3		
	By Jac Ber .	э		
	Parkots Ford Vod	1		
	Packets Sert	J		
	Policy Line is	,		
	RSSI	Ji a∼aila⊎le		
	5NR	Insvailatio		
	Sengla Timo	Well Sep. 5 12 40:41 2017		
	Lucess ve Ketries	J		
	26 2 35	0		
	Subjess Could	3		
	shill Count	1		Line and the second sec
	In pered	5		12
				5

ws the U-APSD sta tus (if enabled) for this client under Quality of Service Properties Step 3 Click Back to return to the Clients page.

Step 4 See the TSM statistics for a particular client and the access point to which this client is associated as follows:

a. Hover your cursor over the blue drop-down arrow for the desired client and choose 802.11aTSM or 802.11b/g TSM. The Clients > AP page appears (see Figure 4-35). Figure 4-35 Clients > AP Page

abala						Singo	Configuration	<u>Ding ngrut E</u>	efress
CISCO	MCNITC?	WLANS	CONTRO	LE?	WIPELECS	SEGURITY	MANACOMIN	COMMANDS	2LP
Monitor Summary F Access Pain 5 Statistics	ls.	Clients Olient N Rac J T AP Inter	> AP 'ac Addres Spe face Mac	5	UJ:1a a1:7b: 802 iilA	1J:Ð		< Unck	
 CDP Regues 		C3:C3:35 C3:17:35	7aia7i4) 80.26 (Detai Dotai					
Multicast	he Detail link fr	or the desired	access no	int to on	en the Clients >	AP > Traffic St	ream Metrics name (see Figure 4-36)	

Figure 4-36 Clients > AP > Traffic Stream Metrics Page

cisco	MONITOR WLANS CONTRO	LER WIR:	alitor c	ecupit~ Ma		: OMMAND	זער? 1103 ב-11	Corfiguro	tan <u>P</u> irg	Logant <u>B</u> r
Monitor Summery Access Paints Statistics COP Reques Climits	Clients> AP > Traffic Stree Client Yao Ademss 1321 Acc 3 (spe 332) AP (resters Mac 332) Cassure in , Duration 33 of Uplink Statistics	um Metrics n al:2h:10:0 11:2/c 6 U(:76:27:2U :2								c Back
Multicost		Packets 0	hat exper	ienced Delay			Packets	Lost Pa-	ckets	
	Limestamp	Average	< 11ims	10ms-20ms	28ms-48ms	> 4lims	Intal	Intal	*18 เดิมเต	Average
	Wed Feb 21 12:05:10 2007	0	C	0	c	2	C	0	3	c
	Wod Feb 21 (2)(2)(0)2002	0	r	n	r	1	r	0	1	r
	Wed (es 11 12:10:40 2007	U	L	U	L.	J	U	U	J	ι
	Wed (e5 11 12:10:10 2007	U	ι	U	L	J	L	U	3	ι
	Wed Feb 21 12:11:10 2007	0	C	0	c	2	C	0	3	c
	Word Feb 31 (2072)40 2002	0	C.	0	r	1	0	n	1	r
	Word Feb 21 (2)74(10/2002	0	C	n	c	1	0	n	1	C
	Downlink Statistics	Packets	halespor	ienced Delay			Packets	LustPar	tkets	
	Timestamp	Average	< 10ms	10ms-20ms	20ms-10ms	> 10ms	Tulal	Total	Masimum	Average
	2004 (en 21 12) - 640 2007	П	: 191	451	1	4	1.940	10. 1	14>	1
	Wed (es 11 12:17:10 2007	U	4460	20	1.	J	4500	U	J	L.
	Wed Feb 21 12:03:10 2007	0	4/18	71	15	2	1502	0))	C
	Wod Feb 21 12:10:10 2002	0	3021	540	14	٦	4484	1	7	
	Word Box 21 (2010)40 2002	0	4277	54	15	٦	4-46	57	25	C.
	Wed (ep 11 12:12:40 2007	2	440%	6.	1	J	4500	U	J	L
	Wed Feb 21 12:01:10 2007	3	5294	497	14	15	4503	0	1	6

tamp text box shows the specific interval when the statistics were collected. n in 90-second intervals. The tir Step 5 See the TSM statistics for a particular access point and a particular client associated to this access point, as follows:

a. Choose Wireless > Access Points > Radios > 802.11a/n or 802.11b/g/n. The 802.11a/n Radios or 802.11b/g/n Radios page appears (see Eigure 4-37).

Figure 4-37 802.11a/n Radios Page

cisco	ысущая мнами сонтас	FR W	RELESS SECOND	y M <u>a</u> nagi	EMENT	COMMANDS HE	Sag Ar Effor	a Contigoration ACK	En v Lus	gcul i <u>E</u> elseen
Wireless	802.11a/n Radios								Entrics	51 2 0f 2
 Accress Points All APs Rog ps 	Current Liftert North					Ŀ	<u>Change Filter</u>	[.a. bor Filter]		
i <u>802, 11,490</u> 802, 11,1,0,0 Global Configuration	AP Name	Radiu Slot≭	Base Badio MAC	Sub Band	Admin Status	Operational Status	Channel	Ulean-Air Admin Status	Clean-Air Oper Status	Radio Role
► Advancel	AP-L	1	00 11:25:20 77 aC		Encole	JF	63	NA	64	127A
Mirsh HREAP Groups	AP-2	1	00 11:25:20 75 00	-	Encole	DOWN	Ð	NA	KA	W.
) 002.11a/n	1									
▶ 882.116/q/n	a standardard									
Media Stream	grocal assignment									
Country										
Limers	2 <									

IIII BI3 between the blue drop-down arrow for the desired access point and choose 802.11aTSM or 802.11b/g TSM. The AP > Clients page appears (see Figure 4-38).

Figure 4-38 AP > Clients Page

CISCO MENTOR W	LANS CONTROLLO	K WIRELESS	Se <u>v</u> e SECURIT™	Analiguration 2 MAXAGEMERT	inc oger <u>e</u> r COMMANDS	fresa HELP
Wireless * Arcess Puints all aks * Collocy * SCOLLOC * AF Corlocation Mesh HRRAD Groups * 8U2.111/0/n Country Timess	AP > Clients AF Ditoffrom Nor Action (yes Client Mar Addr Urae 42, 74:10:0 Orde 42, 74:10:0	n n n JUL.: nss e Detail D <u>Dstail</u>	185171177 4f 13/c		c.Bark	

Figure 4-39 AP > Clients > Traffic Stream Metrics Page

cisco	MONITOR WLANS CONTRO	LER WIP	alizoc g	есират~ ма	VAGEMENT	. OMMAND	Sid <u>v</u> o Co Si TIELP	nfiçuratio	n <u>D</u> ine an	ge o <u>D</u> efre	
iraless	AP > Clients > Traffic Stre	am Metrics	14. 14							e Bark	
 Arraess Points All aps Redios 803,21471 804,21471 805,21471 805,21471 805,21471 805,21471 	AF Droxfrab Nability on 0 Redio Type U05. Li ent Yac Address U0 D Massurerier Dictation 20 s	h 85:71:77 46 116/c a al:/3:10 f0 es	8								
JZ.118/n		Packets that experienced Delay									
U2.116/g/n	Limestown	Average	< 10ms	1ilms-20ms	20ms-40ms	Salima	Intal	Intal	Maximum	Average	
intry	Wed Feb 21 12:16 11 2007	0	c	0	c	2	C	0	0	2	
P.P.S.	Wod Eco 21 (2007) 1, 2007	0	r	0	r	1	r	0	n	1	
;	Wed les 11 12:00 41 2007	U	L	U	L	J	L	U	U	J	
	Wed ep 11 12:10 11 2007	U	L	U	L	J	L	U	U	1	
	Wed Feb 21 12:11 -11 2007	0	c	0	c	2	C	0	0	2	
	Wod Feb 21 12(13) 1, 2007	0	c	n	6	1	C	n	n	1	
	Word Feb 31 12:14 4 - 2007	n	C	n	c	1	C.	n	n	1	
	Downlink Statistics	Packets	llial exper	ienced Delay			Packets	Lust Pa	Lkels		
	Timestamp	Average	< 10ms	10ms-20ms	20ms-40ms	> 4Drus	Tulai	Total	Masimum	Average	
	Wed. wo 21 12:10:11 2007	2	2.035	11/1	11	1	: 744	.44	700	174	
	Wed es 11 12:37 11 2007	U	4460	20	1.	J	450%	U	U	J	
	Wed Feb 21 12:08 (1, 2007	0	4/18	71	15	2	4502	0	0	2	
	Wod Fcb 21 (2007) 1 2007	0	2021	540	14	1	4-84	1	7	3	
	2002 + 1:51 IS COE both	0	4277	54	15	٦	4-4F	52	25	1	
	Wed les 11 12:10 11 2007	U	4444	4'.	12	J	4500	U	U	J	
			1	1.0			1			1.0	

Using the GUI to Configure Media Parameters

To configure Media parameters using the controller GUI, follow these steps

Step 1 Make sure that the WLAN is configured for WMM and the Gold QoS level.

Step 2 Disable all WLANs with WMM enabled and click Apply

Step 3 Choose Wireless and then Network under 802.11a/n or 802.11b/o/n. unselect the 802.11a (or 802.11b/o) Network Status check box, and click Apoly to disable the radio network

Step 4 Choose Wireless > 802.11a/n or 802.11b/g/n > Media. The 802.11a (or 802.11b) > Media > Parameters page appears (see Figure 4-40).

Figure 4-40 802.11a > Media Parameters Page

cisco	MON. CK	<u>W</u> LANS	LON ROLLER	WIRELESS	SECOR 1	Save 15 MONOREMENT	of curstion Pir	nc upq Pc∟ pq	EESDBA	ish ICK
Vireless	802.11 a	(5 GHz) >	Media > Para	meters				1993	Apply	~
Access Points A Abs * Padics U2 11a/n U2 11b/n/n	Voice	Videa	Media							
Glubal Cor rgc aur	Gener	ui								
Advanced	Jr ce	ist Video Re-	direct							
Mesh HRFAD Groups	- Multic	ast Direct	Admission Co	ntrol						-
802.11a/n	Yasi	m im Moria I	Panes dth (1 850	×))	_					
≠ RRM	:	t Y him im P	hy Rate 🔺	61.1	0					
Ki orbuging 140 Dula Uckersge General	~s:ci	mum Ketry I	ercent (J-100%)	UL						
Cher : Roar mu Mec a	Media	Stream	Multicast Dire	ct Paramet	PPS					
DI's (JU2 12F) F gh Througopin	iele.~	cast Direct _	hat e	1~1						
(JOLLIN) Clornein	*ata	uast Diract M	lex Number of Sti	ee ns aut	. 💌					Ī
802.116/9/0	🤪 - Arist	Pfinit Qué A	umission		E ral ad					1
tep 5 Choose the Media ta	ab to open the M	Aedia page.								

Step 6 Select the Unicast Video Redirect check box to enable Unicast Video Redirect. The default value is disabled.

Step 7 In the Maximum Media Bandwidth (0-85%) text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches the specified value, the access point rejects new calls on this radio band.

The default value is 85%; valid values are from 0 to 85%.

Step 8 In the Client Phy Rate text box, enter the value for the rate in kilobits per second at which the client operates.

Step 9 In the Maximum Retry Percent (0-100%) text box, enter the percentage of the maximum retry. The default value is 80.

Step 10 Select the Multicast Direct Enable check box to enable the Multicast Direct Enable text box. The default value is enabled.

Step 11 From the Multicast Direct Max Number of Streams drop-down list, choose the maximum number of allowed multicast direct streams per radio. The range is 0 to 20 and auto. The default value is set to auto.

Step 12 If you want to enable the best radio queue for this radio, select the Best Effort QoS Admission check box. The default value is disabled.

Using the CLI to Configure SIP Based CAC

To configure the SIP based CAC using the controller CLI, follow these steps:

Step 1 Set the voice to the platinum QoS level by entering this command:

config wlan gos wlan-id Platinum

Step 2 Enable the call-snooping feature for a particular WLAN by entering this command:

config wan call-snoop enable wan-id

Step 3 Enable the ACM to this radio by entering this command:

config {802.11a | 802.11b} cac {voice | video} acm enable

Using the CLI to Configure Voice Parameters

0

Note Make sure that you perform the Using the CLI to Configure SIP Based CAC before you do this procedure.

To configure voice parameters using the controller CLI, follow these steps:

Step 1 See all of the WLANs configured on the controller by entering this command:

	show whan summary Stars 1 Alska such that MM AN that you are element to configure for WAMI and the OnS level is set to Blainium hy enteriori this command-
	Step 3 Disable all WLANs with VMM enabled prior to changing the voice parameters by entering command:
	config wan disable wan_id
	Step 4 Disable the radio network by entering this command:
	config (802.11a 802.11b) disable network
	Step 5 Save your settings by entering this command:
	save config Save 5 cmbit or disable bandwidth-based unice CAC for the 802 11a or 802 11b/n network by enteriorit this command:
	Step 7 Set the prevented of maximum bandwide hallocated to clients for voice applications on the 802.11a or 802.11b/g network by entering this command:
	config (802.11a 802.11b) cac voice max-bandwidth bandwidth
	The bandwidth range is 5 to 85%, and the default value is 75%. Once the client reaches the value specified, the access point rejects new calls on this network.
	Step 8 Set the percentage of maximum allocated bandwidth reserved for roaming voice clients by entering this command:
	config (802.11a) 802.11b) cac voice roam-bandwidth bandwidth
	The barbward harge is to 25%, and the detaul value is 0%. The controller reserves this much calculate the maximum and cated barbward for realing voice clents. Skep 2 Configure the code cancer and sample interval as parameters and to calculate the required barbward for call by entering this command:
	confia (802.11a) (802.11b) cac voice sis codec (a711 a729) sample-interval number mesos
	Step 10 Configure the bandwidth that is required per call by entering this command:
	config (802.11a) (802.11b) cac voice sip bandwidth_kbps sample-interval number_msecs
	Step 11 Reenable all WLANs with WMM enabled by entering this command:
	config wan enable wlan_id
	Step 12 Reenable the radio network by entering this command:
	config (802.11a) 802.11b) enable network Sena 13. Sevie usertain the intervente
	and provide state your changes by entering this contrastic.
	save comg
ι	Ising the CLI to Configure Video Parameters
0	
Note	Make sure that the <u>Using the CLI to Configure SIP Based CAC</u> are met.
	To configure video parameters using the controller CLI, follow these steps:
	Step 1 See all of the WLANs configured on the controller by entering this command:
	show wian summary
	Step 2 Make sure that the WLAN that you are planning to modify is configured for WMM and the QoS level is set to Gold by entering this command:
	show wian wan, jd
	Step 3 Disable all WLANs with WMM enabled prior to changing the video parameters by entering this command:
	config what disable wan, id Start A. Divisio the cardie network hy acteriory this company.
	Step 4 - Seade the factor letwork by entering ans command.
	Corning Gou2. Trial Jou2. Triol possable networks Skep 5 Save vour settings by vertering the isocommand:
	save config
	Step 6 Insable or disable video CAC for the 802.11a or 802.11b/g network by entering this command:
	config (802.11a) (802.11b) cac video acm (enable disable)
	Step 7 Set the percentage of maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network by entering this command:
	config (802.11a 802.11b) cac video max-bandwidth
	config (802.11a 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network.
Note	config (802.11a 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network.
Note	config (802.11a 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests.
Note	config (802.11a 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8. Process or ignore the TSPEC inactivity timeout received from an access point by entering this command:
Note	config (802.11a 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8. Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a 802.11b) cac video tspec-inactivity-timeout (enable ignore). Even 0. Received all MAI the work of the work of the maximum of the process of th
Note	config (802.11a) (802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8. Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a) (802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 9. Reenable all VLANs with WMM enabled by entering this command: config (802.11a) (802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 9. Reenable all VLANs with WMM enabled by entering this command: config (802.11a) (802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 9. Reenable all VLANs with WMM enabled by entering this command:
Note	config (802.11a) 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8. Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a) 802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 9. Reenable all WLANs with WMM enabled by entering this command: config wan enable wilan.jd Step 10. Reenable the radio network by entering this command:
Note	config (802.11a) 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a) 802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 9 Reenable all WLANs with WMM enabled by entering this command: config wan enable wlan_jd Step 10 Reenable the radio network by entering this command: config (812.11a) [802.11b] cab intervork.
Note	config (802.11 a) 802.11 b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a) 802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 9 Reenable all WLANs with WMM enabled by entering this command: config (802.11a) Rozention betwork by entering this command: config (802.11a) Rozention
Note	config (802.11a 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a 802.11b) cac video tepe-inactivity-timeout (enable ignore) Step 9 Reenable all WLANs with WMM enabled by entering this command: config wan enable wan_id Step 10 Reenable the radio network by entering this command: config (802.11a 802.11b) cabe index network Step 11 Revo use settings by entering this command: config (802.11a 802.11b) cabe index network Step 11 Revo use settings by entering this command: config (802.11a 802.11b) cabe index network Step 11 Save your settings by entering this command: config (802.11a 802.11b) cabe index network Step 11 Save your settings by entering this command: config (802.11a 802.11b) cabe index network Step 11 Save your settings by entering this command: config (802.11a 802.11b) cabe index network
Note	config (802.11a 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a 802.11b) cac video tope-inactivity-timeout (enable ignore) Step 9 Reenable all WLANs with WMM enabled by entering this command: config wan enable wan_id Step 10 Reenable the radio network by entering this command: config (802.11a 802.11b) cabe index point by setting this command: config (802.11a 802.11b) cabe index point by entering this command: config (802.11a 802.11b) cabe index point by entering this command: config (802.11a 802.11b] cabe index point by entering this command: config (802.11a 802.11b] cabe index point by entering this command: config (802.11a 802.11b] cabe index point by entering this command: config (802.11a 802.11b] cabe index point by command: com
Note	config (802.11a 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a 802.11b) cac video topec-inactivity-timeout (enable ignore) Step 9 Reenable all WLANs with WMM enabled by entering this command: config data enable wan_id Step 10 Reenable the radio network by entering this command: config (802.11a 802.11b) enable network save config save config save config save config
Note	config (602:11a) (802:11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC Inactivity timeout received from an access point by entering this command: config (802:11a) (802:11b) cac video tspec-inactivity-timeout (enable ignore) Step 9 Reenable all WLANs with WMM enabled by entering this command: config (802:11a) (802:11b) cac video tspec-inactivity-timeout (enable ignore) Step 1 Reenable the radio network by entering this command: config (802:11a) (802:11b) cac video tspec-inactivity timeout received from an access point by entering this command: config (802:11a) (802:11b) cac video tspec-inactivity timeout received from an access point by entering this command: config (802:11a) (802:11b) cac video tspec-inactivity timeout (enable ignore) Step 1 Reenable the radio network by entering this command: config (802:11a) (802:11b) cause intering this command: config (802:11a) (802:11b) cause intering this command: seve config
Note	config (802.11a) (802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point nejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a) (802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 9 Reenable all VLANs with WMM enabled by entering this command: config (802.11a) a co.2.11b) cac video tspec-inactivity-timeout (enable ignore) Step 1 Reenable the radio network by entering this command: config (802.11a) a 02.11b) enable network Step 11 Save your settings by entering this command: seve config
Note	config (802.11a) (802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point nejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller of the source of the set operation of the source of the source of the set operation of the source of the source of the set operation of the source of th
Note	config 602.11a 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point nejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a) acc video tspec-inactivity-timeout (enable ignore) Step 9 Reenable all WLANs with WMM enabled by entering this command: config (802.11a) acc video tspec-inactivity-timeout (enable ignore) Step 10 Reenable enter facto network by entering this command: config (802.11a) acc video tspec-inactivity-timeout (enable ignore) Step 10 Reenable enter video network by entering this command: config (802.11a) acc video tspec-inactivity timeout received from an access point by entering this command: config (802.11a) acc video tspec-inactivity timeout (enable ignore) Step 10 Reenable enter video network by entering this command: config (802.11a) acc video tspec-inactivity timeout (enable ignore) Step 11 Reversite the radio network by entering this command: config (802.11a) acc video tspec-inactivity timeout (enable ignore) Step 11 Save your settings by entering this command: save config
Note	config 602.11a 802.11b] cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point hejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a) 802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 9 Reenable all WLANs with WMM enabled by entering this command: config (802.11a) 802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 1 Reenable he radio network by entering this command: config (802.11a) 802.11b) ab network Step 11 Save your settings by entering this command: save config for the CLL to View Voice and Video Settings To view voice and video settings using the controller CLL follow these steps: Step 1 See the CAC configuration for the 802.11b or 802.11b/ gnetwork by entering this command: show (802.11a) 802.11a) 802.11a) 802.11b/ ap_name
Note	config 6802.11a 802.11b) cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point hejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Istep 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a) 802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 9 Reenable all WLANs with WMM enabled by entering this command: config (802.11a) 802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 1 Reenable all WLANs with WMM enabled by entering this command: config (802.11a) 802.11b) applies to maximum RF bandwidth allocation and, therefore, allows all bandwidth requests. Istep 1 Reenable all WLANs with WMM enabled by entering this command: config (802.11a) 802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 1 Reenable all WLANs with WMM enabled by entering this command: config (802.11a) 802.11b) applies to maximum RF bandwidth requests. Istep 1 Reenable and Video Stetings To view voice and Video Stetings To view voice and Video Stetings Step 1 Save your settings by entering this command: show all the CAC configuration for the 802.11a of 802.11b (network by entering this command: show 2.11a show 802.11b) applicate Step 2 See the CAC configuration for the 802.11b (perturned the sommand: show applications for the 802.11b) applicate Normand: show applications for the 802.11b (perturned the sommand: show applications for the 802.11b) applicate Normand: show applications for the 802.11b (perturned the sommand: show applications for the 802
Note	config G02: 11a 802: 11b; ace video max.handwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth allocation and, therefore, allows all bandwidth requests. It this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity-timeout received from an access point by entering this command: config (802: 11a 802: 11b) cas video tspec-inactivity-timeout (mable ignore) Step 9 Reenable all WLANs with WMM enabled by entering this command: config (802: 11a 802: 11b) cas video tspec-inactivity-timeout (mable ignore) Step 9 Reenable all WLANs with VMM enabled by entering this command: config (802: 11a 802: 11b) anable of the radio network by entering this command: config (802: 11a 802: 11b) mable network Step 1 Size p 0 recess arity suite the radio network by entering this command: save config listing the CLL to View Voice and Video Settings To view voice and video settings using the controler CLL follow these steps: Step 1 See the CAC configuration for the 802: 11a or 802: 11b g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (802: 11a 802: 11b) g network by entering this command: show ago stats (
Note	config (802.11a) [802.11b] cac video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config (802.11a) (802.11b) cac video tspec-inactivity-timeout (enable ignore) Step 1 Reenable all WLANe with WMM analaded by entering this command: config (802.11a) [802.11b] enable network by entering this command: config (802.11a) [802.11b] enable network by entering this command: config (802.11a) [802.11b] enable network Step 11 Sive your settings by entering this command: seve config Step 11 Sive Volce and Video Settings To view volce and video settings using the controller CLI, follow these steps: Step 1 Sive the CAC configuration for the 802.11b (or these steps: Step 1 Sive the CAC configuration for the 802.11b (or appearse) Step 2 Sive the CAC configuration for the 802.11b (or appearse) Step 3 Sive the CAC configuration for the 802.11b (or appearse) Step 4 Sive 11a) show 802.11b (OCC) Sixtes Voice Bandwidth in use (% of config pw)
Note L	config 602:11a [802:11b] care video max-bandwidth The bandwidth may is 5 to 55%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 55% for vice and video. Once the client reaches the value specified, the access point nejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config 602:11a [802:11b] care video tapec-inactivity-timeout (mable ignore) Step 8 Reenable all WLANs with WMM enabled by entering this command: config 602:11a [802:11b] care video tapec-inactivity timeout received from an access point to entering this command: config 602:11a [802:11b] each video tapec-inactivity timeout received from an access point to entering this command: config 602:11a [802:11b] each video tapec-inactivity timeout received from an access point to entering this command: sere config for an access point rejects are video and video settings To view vice and video Settings To view vice and video Settings Step 1 Reenable the radio network by entering this command: show (602:11a [802:11b] each vice to and video settings Step 2 See the CAC configuration for the 802:11a 0 Resp.11a or 802:11b genetwork by entering this command: show (602:11a [802:11a] each vice to an access point by entering this command: show (602:11a [802:11b] each vice to an access point by entering this command: show (602:11a [802:11b] each vice to an access point by entering this command: show (602:11a [802:11b] each vice to an access point by entering this command: show (602:11a [802:11b] each vice to an access point by entering this command: show (602:11a [802:11b] each vice to an access point by entering this command: show (602:11a [802:11b] each vice to an access point by entering this command: show (602:11a [802:11b] each vice to an access point by entering this command: show (602:1
Note L	config Gi2 11al [802.11b] can video max-bandwidth bandwidth The bandwidth range is 5 to 55%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 55% for voice and video. Once the client reaches the value specified, the access point nejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Sep 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command: config Gi2 11al [802.11b] can video tspec-inactivity timeout (enable ignore) Sep 9 Reenable all WLANs with WMM enabled by entering this command: config Gi2 11al [802.11b] enable network Sep 10 Reenable for and network by entering this command: config Gi2 11al [802.11b] enable network Sep 11 Reenable the radio network by entering this command: see config when enable the radio network by entering this command: see config when enable the radio network by entering this command: see config when enable the radio network by entering this command: see config when enable the radio network by entering this command: see config when enable the radio network by entering this command: see config when enable the radio network by entering this command: see config To view voice and video Settings using the controller CLL toftow these steps: Sep 1 See the CAC contiguation for the 802.11al or 802.11bl gn entwork by entering this command: show ag stats (802.11al [802.11b] on pueront by entering this command: show ag stats (802.11al [802.11b] on pueront to administ to the following appears: Call Administic Control (CC) Stats View Bandwidth in une (1 of config by), 0 Total channel IMF free
Note	confg 802.11a 802.11b acc video max-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth requests. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth is command: If this parameter is set to zero (0), the controller OLL follow these steps: If the control of the 802.11a is dow 20.11b is down and therefore, allows and tideo settings using the controller OLL follow these steps: If the assume the following appears: Config 602.11a jabox 402.11b jab, name If the set to all width is unit of the following appears: Config 602.11a jabox 402.11b jab, name If the set to down appears: Config free
Note	config 802.11a 802.11b is care when maximum RF bandwidth cannot acceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. See P Process or ignore the TSPEC linetify timeout received from an access point by entering this command: config 802.11a 802.11b is ac who tape-hanchiby timeout (enable ignore) See P Process or ignore the radio retwork by entering this command: config 802.11a 802.11b) erable nadio retwork by entering this command: config 802.11a 802.11b) erable nadio retwork by entering this command: access point register and the radio retwork by entering this command: see config See P1. Save your settings by entering this command: see config See P1. Save your settings by entering this command: see config See P1. Save your settings to entroler CLL follow these steps: See P1. Save your settings to retwork by entering this command: see config See P1. Save your settings to particular access point by entering this command: see config See P1. Save your settings to particular access point by entering this command: see config See P1. Save your settings to particular access point by entering this command: see config See P1. Save your settings to particular access point by entering this command: see config See P1. Save your settings to particular access point by entering this command: see config See P1. Save your settings to particular access point by entering this command: see C2. Configuration for the 802.11a or 802.11b or 802.11a who see steps: See P1. Save Work Set
Note	config 802.11a 802.11b ack video mask-bandwidh handwidh The bandwidth nange is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for vicics and video. Once the client resches the value specified, the access point nejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Sep 8 Processor ignore the TSPEC inactivity immout neolwed from an access point by entering this command: config (802.11a 802.11b) cac video topeo-inactivity-immout (enable grore) Sep 9 Revealed at VLANe with VMM enabled by entering this command: config (802.11a 802.11b) enable neolox is command: config (802.11a 802.11b) enable neolox is command: config (802.11a 802.11b) enable neolox Sep 1 Save your settings by entering this command: area config To item voice and Video Settings To view voice and View Voice Settings To view voice and View Voice Settings To view voice and View Voice Settings To view voice and View Setting To view voice View Voice Settings To view View Setting Setiem To view Voice Settings To view Vie
Note	config 802.11a j 802.11b j acc video mask-bandwidth bandwidth The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth annot exceed 85% for voice and video. Once the client reaches the value specified, the access point nejects new calls on this network. If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. See P Rocess or ignore the TSPEC inactivity timeout meable with on the access point by entering this command: config 802.11a j 802.11b j excitoo the generabandhy diffuence (mabble j generable all WLANs with WMM enabled by entering this command: config 802.11a j 802.11b j enable meakers the value specified that command: config 802.11a j 802.11b j enable meakers the value specified that command: config 802.11a j 802.11b j enable meakers the value specified that command: config 802.11a j 802.11b j enable meakers the value specified that command: config 802.11a j 802.11b j enable meakers See 1 Reseable the rado network by entering this command: config 802.11a j 802.11b j enable meakers See 1 Reseable the rado network by entering this command: config 802.11a j 802.11b j enable to about the specified that command: config 802.11a j 802.11b j enable to about the specified that command: config 802.11a j 802.11b j enable to about the specified this command: config 802.11a j 802.11b j enable to about the specified that command: config 802.11a j 802.11b j enable to about the specified that command: config 802.11a j 802.11b j enable to about the specified this command: config 802.11a j 802.11b j enable to generate the specified that command: config 802.11a j 802.11b j enable to generate the specified that command: config 802.11a j 802.11b j enable to generate the specified that command: config 802.11a j 802.11b j enable to generate the specified that command: config 802.11a j 802.11b j enable to generate the specified that command the specified that the specified that command: co
Note	config Bio2:11a Bio2:11b case does marked with invalued in transform RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point nijects new calls on this network. If this parameter is set to zero (b), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Josep 8 Process or ignore the TSPEC inachity timout received from an access point by entering this command: Config Bio2:11a Bio2:11b cardot togetope-inachity timout received from an access point by entering this command: Config Bio2:11a Bio2:11b cardot togetope-inachity timout received from an access point by entering this command: Config Bio2:11a Bio2:11b cardot togetope-inachity timout received from an access point by entering this command: Config Bio2:11a Bio2:11b cardot togetope-inachity timout received from an access point by entering this command: Config Bio2:11a Bio2:11b cardot togetope-inachity timout received from and togetope in the command: Config Bio2:11a Bio2:11b cardot togetope inachity timout received Bio3: Config Bio2:11a Bio2:11b cardot togetope inachity timout received Bio3: Config Bio2:11a Bio2:11b cardot togetope inachity timout received Bio3: Config Bio2:11a Bio2:11b cardot togetope inachity timout received Bio3: Config Bio2:11a Bio2:11b cardot togetope inachity timout received Bio3: Config Bio2:11a Bio2:11b cardot togetope inachity timout received Bio3: Config Bio2:11a Bio2:11b cardot togetope in the received Bio3: Config Bio2:11a Bio2:11b cardot togetope in the received Bio3: Config Bio2:11a Bio2:11b cardot Bio2:11a Bio2:11a Bio2:11a Bi
Note	config Bio2.11a Bio2.11b gai: does max-bandwidth handwidth The bandwidth mange is 5 to 85%, and the default value is 5%. However, the meaimum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. Sep 3 Process or ignore the TSPEC inachity timeout received from an access point by entering this command: config Bio2.11a Bio2.11b) cavids to tesp-inachity timeout received from an access point by entering this command: config Bio2.11a Bio2.11b cavids to tesp-inachity timeout received from an access point by entering this command: config Bio2.11a Bio2.11b cavids to tesp-inachity timeout received from an access point by entering this command: config Bio2.11a Bio2.11b cavids to tesp-inachity timeout received from an access point by entering this command: config Bio2.11a Bio2.11b cavids to tesp-inachity timeout received from and: Sep 1 Remarks and the radio vetwork by entering this command: config Bio2.11a Bio2.11b cavids to tesp-inachity timeout received from and: Sep 1 See the radio vetwork by entering this command: see config Sep 1 See the CAC configuration for the Bio2.11b or Bio2.11b / Bio2
Note	config BCC 11a BCC 11b acceleration marke handwidth Te bandwidth mange is 5 b 85%, and the diffual value is 5%. However, the maximum RF bandwidth ancace acceler 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network. Sep 8 Process or ignore the TSPEC inactivity timout nealwest point want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Sep 8 Process or ignore the TSPEC inactivity timout nealwest point want to do any bandwidth allocation and, therefore, allows all bandwidth requests. Sep 8 Process or ignore the TSPEC inactivity timout nealwest point you therefore the top of top of the top of
Note	contig B02.11a 802.11a 802.11a 802.11a 802.11a of 805 kines here maxime PE bandwidth ance exceed 85% for voice and video. Once the cleant reaches the value specified, the access point spins new calls on this network. The bandwidth maps is 50 85%, and the default value is 5%. However, the maximum PE bandwidth allocation and, therefore, allows all bandwidth requests. Bege 1 Process or ignore the TSPEC handwig timecar revolue of tom an access point by entering this command: contig 802.11a 802.11a 802.11b cas video tope-charachrity-timecat (anable ignore): Bege 1 Process or ignore the TSPEC handwig timecar revolue of tom an access point by entering this command: contig 904 montable with wild Bege 1 Process or ignore the radie of prenengy time command: and or optic 101 and access point by entering this command: and contig 902.11a 802.11b cas wideo tope-charachrity-timecat (anable ignore): Bege 1 Save your entrops by entering this command: and contig 902.11a 802.11b cas wideo tope-charachrity-timecat (anable ignore): Bege 1 Save your entrops by entering this command: and contig 902.11a 802.11b cas wideo tope-charachrity-timecat (anable by entering this command: and wideo Sattings using the controller CL blow these steps: Bege 1 Save Your entrops by entering this command: there wideo 11a of 802.11b cas wideo they entering this command: there wideo 11a of 802.11b cas wideo they entering this command: there wideo 11a bio 802.11b Beg 2 Bes the CAC statistics for a particular access point by entering this command: there was publis (801.11b (202.11b) gaves was publis (801.11b (202.11b) gaves was publis (801.11b (202.11b) gaves Work wa
Note	config BioC 11a [BioC 11b] [and kind marked with and with BioC 11b] [and kind and a specified of a second with a location and with and with a location and withe a location and with a
Note	config Bild Int Bild
Note	cond gBC2 II 10 2 11% act which make a 50%. However, the maximum FE handwidth cannot easeed 50% for value and value. Once the client maches the value specified, the access point rejects ever calls on the network. If is parameter is set to zero (0), the controller ascess point you do not wart to do any bandwidth aducation and, therefore, allows at bandwitth requests. Beg 8 Process or ignore the TSPEC functionly immount network of to any bandwidth aducation and, therefore, allows at bandwitth requests. Beg 8 Process or ignore the TSPEC functionly immount network of the antibus to your any the command: condig dBC1 II 10 2C 11% car. which sepacimatively or do not wart to do any bandwidth aducation and, therefore, allows at bandwitth requests. Beg 8 Process at the radio notation by orienting the command: condig dBC1 II 10 2C 11% car. which sepacimatively or do not wart to do any bandwidth aducation and, therefore, allows at bandwitth requests. Beg 1 Remains the radio notation by orienting the command: condig dBC1 II 10 2C 11% car. which and the oriented the command: acced gBC 2 to BCC Acced galaxies and the command to access point to protein gBC 11 10 2C 11% pares by control gBC 11 10 2C 11% pares by control gBC 11 10 2C 11% pares benefore the U strate of the oriented to the notation and, therefore, allows at the top 11 sec 2 to BC 10 2C 1

Step 3 See the U-APSD status for a particular client by entering this command:

show client detail client mac

Step 4 See the TSM statistics for a particular client and the access point to which this client is associated by entering this command:

show client tsm (802.11a | 802.11b) client_mac (ap_mac | all) The optional all command shows all access points to which this client has associated. Information similar to the following appears:

Client Interface Mac: 00:01:02:03:04:05 Measurement Duration: 90 seconds
Timestamp lat Jan 2006, 06:35:80 UpLink Stats
Average Detay (See Intervals)
Delay bet 10 - 20 ms
Delay bet 20 - 40 ms
Delay greater than 40 ms
Total packet Count
Total packet lost count (5sec)
Maximum Lost Packet count(5sec)
Average Lost Packet count(5secs)
DownLink Stats
Average Delay (5sec intervals)
Delay less than 10 ms
Delay bet 10 - 20 ms
Delay bet 20 - 40 ms
Delay greater than 40 ms
Total packet count
Incat packet lost count (Sec)
Average Lost Packet count(Ssecs)
Note The statistics are shown in 90-second intervals. The timestamp text hox shows the specific interval when the statistics were collected
Not a clear the TSM statistics for a particular access point or all the access points to which this clear is associated enter the clear clear the TSM statistics for a particular access point or all the access points to which this clear is associated enter the clear clear the TSM statistics for a particular access point or all the access points to which this clear is associated enter the clear clear the TSM statistics for a particular access point or all the access points to which this clear is associated enter the clear clear the TSM statistics for a particular access point or all the access points to which this clear is associated enter the clear clear the TSM statistics for a particular access point or all the access points to which this clear is associated enter the clear clear the TSM statistics for a particular access point or all the access points to which this clear is associated enter the clear clear the TSM statistics for a particular access points or all the access points to which this clear is associated enter the clear clear the the the the the the the the the the the
Step 5. See the TSM statistics for a particular access point and a particular client associated to this access point by entering this command:
show ap stats {802.11a 802.11b} ap_name tsm {client_mac all}
The optional all command shows all clients associated to this access point. Information similar to the following appears:
AP Interface Mac: 00:0b:85:01:02:03
Client Interface Mac: 00:01:02:03:04:05
Measurement Duration: 90 seconds
Timestamp 1st Jan 2006, 06:35:80
UpLink Stats

Average Delay (5sec intervals)
Delay less than 10 ms
Delay bet 10 - 20 ms
Delay bet 20 - 40 ms
Delay greater than 40 ms
Total packet Count
Total packet lost count (5sec)10
Maximum Lost Packet count(5sec)5
Average Lost Packet count(5secs)2
DownLink Stats
Average Delay (5sec intervals)
Delay less than 10 ms
Delay bet 10 - 20 ms
Delay bet 20 - 40 ms
Delay greater than 40 ms
Total packet Count
Total packet lost count (5sec)10
Maximum Lost Packet count(5sec)5
Average Lost Packet count(5secs)2
·
The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.
Star 6 Excelle or displicit debunder for cell admission posteril (CAC) meanages quants or packets by asterias bia command.
Step 6 Enable or unsable debugging for call additios for control (CAC) messages, events, or packets by entering this controlled.
debug cac { all event packet }{ enable disable }
where all configures debugging for all CAC messages, event configures debugging for all CAC events, and packet configures debugging for all CAC packets.
Configuring EDCA Parameters
Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic. Follow the instructions in this section to configure EDCA
parameters using the controller GUI or CLI.
Using the GUI to Configure EDCA Parameters
To configure FDCA parameters using the controller GUI follow these steps:
to comigure ECON parameters using ure controller Gol, follow trace steps.
Step 1 Choose Wireless and then Network under 802.11a/n or 802.11b/g/n, unselect the 802.11b (or 802.11b/g) Network Status check box, and click Apply to disable the radio network.
Step 2 Choose FDCA Parameters under 802 11a/n or 802 11b/o/n. The 802 11a (or 802 11b/o) > FDCA Parameters page appears (see Figure 4-41)
Figure 4-41 802.11a > EDCA Parameters Page

CISCO	MONITOR W 4V.	DONTROLLER	WIRE ESS	SECURITY	MANAGEMENT		-ELO	T LOQUUC SE FASI
Wiraless	802.11b/g > EDC/	A Parameters						Apply
Access Puints	General							
Mesh HREAP Groups • 802.11 <i>a[</i> m	EDCA Prohie Encole : de Latondy	маг. 4	<u></u>	14	H			
 BD2.111/Jufn Vervork REM Clarit Picaning, Vicas Vicas EDCA Pariameters lich 1mcadhout (822 Lon) 	form altra (200 perforad 6.2	CP merking is och	est for medie (NP) and sign	ehns pachers			1222
Step 3 Choose one of the fo	llowing options from the EDC	A Profile drop-down	list:					
WMM —Enables the Wi-Fi	Multimedia (WMM) default pa	rameters. This is the	e default value.	Choose this op	tion when voice or v	ideo services are	not deployed on yo	our network.
Spectralink Voice Priorit	y —Enables SpectraLink voic	e priority parameter	s. Choose this o	ption if Spectra	Link phones are dep	loyed on your net	twork to improve the	e quality of calls.
Voice Optimized —Enabl	es EDCA voice-optimized prof	ile parameters. Cho	ose this option	when voice sen	vices other than Spe	ctraLink are deplo	oyed on your netwo	irk.
Voice & Video Optimized	 Enables EDCA voice- and 	video-optimized pro	ofile parameters.	Choose this op	tion when both voic	e and video servio	ces are deployed or	n your network.
A								

Note If you deploy video services, admission control (ACM) must be disabled.

Step 4 If you want to enable MAC optimization for voice, select the Enable Low Latency MAC check box. Otherwise, leave this check box unselected, which is the default value. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, which improves the number of voice calls serviced per access point.

0 Note We do not recommend you to enable low latency MAC. You should enable low latency MAC only if the WLAN allows WMM clients. If WMM is enabled, then low latency MAC can be used with any of the EDCA profiles. See the <u>Configuring QoS Enhanced BSS' section</u> for instructions on enabling WMM.





Using the GUI to Configure Cisco Discovery Protocol

~P'2

To configure CDP using the controller GUI, follow these steps:

Step 1 Choose Controller > CDP > Global Configuration to open the CDP > Global Configuration page (see Figure 4-43).

~P13

10.24 04.233

Figure 4-43 CDP > Global Configuration Page

.075.34 155

74AB



AP Cure Durau

AP Core Duros 👘 Frahled

Using the GUI to View Cisco Discovery Protocol Information

To view CDP information using the controller GUI, follow these steps

Step 1 Choose Monitor > CDP > Interface Neighbors to open the CDP > Interface Neighbors page appears (see Figure 4-45).

AP Shoup Name

Statistics Times

Села Епосудион

Note If CDP is disabled in Step 2, a message indicating that the Controller CDP is disabled appears. Click Apply to commit your changes.
 To enable or disable CDP on all access points currently associated to the controller, follow these steps: se Wireless > Access Points > Global Configuration to open the Global Configuration page.

default-cicup 🔡

1. Select the Cisco Discovery Protocol check box to enable CDP on this access point or unselect it to disable this feature. The default value is enabled.

133

Figure 4-45 CDP > Interface Neighbors Page

2. Click Apply to commit your changes Step 9 Click Save Configuration to save your changes

Country

Timers

0

▶ QuS

Choo

cisco	MONITOR	WEANS CONTROLLER	WIGHLESS SECURITY	MANAGEMENT CC	Saza Cuil MMANDS	igereadi ≥ HF <u>u</u> f	ng Lugout Balnesi
Monitar Summary	CDP > Inte	rface Neighbors	Neighbor			a antonio	Sings
 Access Points Statistics 	Interface	Neighber Name	Address	Neighbar Port	IIL	L'apability*	Platform
	Furl-1	Sat 1+2950-2	308 165,200,225	FastEll an alc/2-	130	31	usuc WB-C2950-24
	Fort _	WC5 Borndon Dov	200 1 65 200 225	Unit DiSlot DiFort .	_ 147	+	WLC4402 12
* CDP	East	Concentration &	205105200225	Loit 0 Slot 0 Com	154	-	XI 04412-12
AF ite ghbors	Fort - 1	kit-4402	205/105200225	Unit - U Slot - U Fort - 3	100	1	XDC4402-12
lishf = "strics	Forl-1	acchiac/102	309 165 200 225	Unit - DiStuti - DiFurit - :	162	н	MR-WLC//02-12-KS
Regues	Furl-1	01-4-02	309 165,200,225	L iit - D Slut - D Fur :	2 121	н	WLC4402-12
Climits	East	E a mh		GiganitEthomat0/	180	51	cisco 105 CBSENG 24
Multicast	Fort - 1	srihath-44UJ	205/105/200/225	Unit - U Slot - U Fort - 3	191	1	XLC4404-100
	Furl-1	<u>Mana-1401</u>	200165-000-205	Unit - DiStuti - DiFuri - :	162	H	MIR-WLC//02-12-KS
is page shows the following in	 Cepabrility Source Roc Swmb, Second Secon	v Codel IX - Noveen II - Trans de Britige. H. Hort, T. 17967, C. Bopos Ny Renaged Geurse.	r Umage, U - mov				906210

1. Select the CDP State check box to enable CDP on all access points associated to the controller or unselect it to disable CDP on all access points. The default value is selected.

- · The name of each CDP neighbor
- The IP address of each CDP neighbor
- The port used by each CDP neighbor for transmitting CDP packets · The time left (in seconds) before each CDP neighbor entry expires

• The functional capability of each CDP neighbor, defined as follows: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, or M - Remotely Managed Device

The hardware platform of each CDP neighbor device

Step 2 Click the name of the desired interface neighbor to see more detailed information about each interface's CDP neighbor. The CDP > Interface Neighbors > Detail page appears (see Figure 4-46).

Figure 4-46 CDP > Interface Neighbors > Detail Page

CISCO	MONITOR W 4V.	DUVERUIER WIREERS SECURITY MEMAREMENT COMMANDSFLD	Luggat Kerrash
Monitar	CDP > Interface I	Neighbors > Detail	c Bark
Summary	Local Interface	Full-1	
Access Points	Neighbor Name	00-4702	
Statistics	Snighbor Address	1.10C. F3.43	
▼ CDP	Seighbor Port	Unit - J Slot - U - Srt - 1	
Li certade Kargliours	Advt Version	71	
AF KaighLurs Traffic Katrics	TTL	157	
> Domier	Copability	Host	
clients	Platform	0014402-12	
Mullicast	Software Version	Manufesturen's Name: Cisco Bystems Inc. Product Name: Cisco Lontro en Product Version: 4 238325 RTOS Versions - 2389 25 Buol Jaden Versions (112210 Build Types DATA + WPS	
his page shows the following in	formation:		ž

· The controller port on which the CDP packets were received

- The name of the CDP neighbor
- The IP address of the CDP neighbor
 The port used by the CDP neighbor for transmitting CDP packets
- The CDP version being advertised (v1 or v2)
- The time left (in seconds) before the CDP neighbor entry expires
- The functional capability of the CDP neighbor, defined as follows: Router, Trans Bridge, Source Route Bridge, Switch, Host, IGMP, Repeater, or Remotely Managed Device
- The hardware platform of the CDP neighbor device
- The software running on the CDP neighbor
- Step 3 Choose AP Neighbors to see a list of CDP neighbors for all access points connected to the controller. The CDP AP Neighbors page appears (see Figure 4-47).

Figure 4-47 CDP AP Neighbors Page

cisco		<u>12</u> 41 i j	DOVIEDI EB	WIRE EBS	SEGURITY	MANAGEMENT	Sage Con COMMANDS	Fpuration FELD	En J	Lugeut Bern	ssh
Monitar	COP AP N	alghbors	li.								Ĩ
Summery	AP Name			CDP Nole	hhars						
Access Points	Smath-70:9	d .ru		CUP Neic	hoors		-12				
▶ Statistics	100.72			COP Nerc	LUUIS						
▼ CDP In centrate Neighbors AF Neighbors Treffic Metrics											
Roques											
Clients											2
Multicast											1220
Step 4 Click the CDP Neight	bors link for the de:	sired access	point to see a lis	t of CDP neighb	ors for a specif	c access point. The	CDP > AP Neigh	bors page a	appears (see Figure 4-48).	- 81 -

Figure 4-48 CDP > AP Neighbors Page

alidir							Engr Chinfig	uration Ding Logant 2	rinsh
CISCO	могатор.	W_A\5	CONTROLLER.	WIRELESS	SECURERY	MANACEMENT	COMMANDS	ELP.	
Monitor	CDP > AI	P Neighb	ors						
Summary	AP Name		AP	IP Address	Neighbor N	ame	Neighbur Address	Neighbor Port	Adv Ven
 Access Points Statistics 	<u>C1 AF2</u>		ж ж	1 155 211 225	Switch			GiganitEtherast0/17	32
 CDP Interface Keighnes AF Keighbers Traffic Plattics 									12204
This page shows the following in	formation:								
The name of each access p	oint								
The IP address of each acc	ess point								
The name of each CDP neight	ghbor								
The IP address of each CDI	neighbor								

· The port used by each CDP neighbor

The CDP version being advertised (v1 or v2)

Step 5 Click the name of the desired access point to see detailed information about an access point's CDP neighbors. The CDP > AP Neighbors > Detail page appears (see Figure 4-49)

Figure 4-49 CDP > AP Neighbors > Detail Page

alitilia				Sage Cont	puration E	n y Luggad i Berresh
CISCO	MONITOR 15 41	OCNTROLLER WIRE ERS SECURITY MANAG	GEMENT	COMMANDS	-=Lo	
Monitor	CDP > AP Neig	bors > Detail				< Back
Summary	AP Same	12-4-2				
Access Points	Base Radio NAC	00 0L:85:57 U9 10				
▶ Statistics	AP IP Address	209.135.200.225				
* CDP	Local Interface	onr-				
Interface Reighbors	Neighbor Name	's witch				
AF Reighbors Troff a Katrice	Neighbur Address					
h Rummi	Seighbor Port	Gruat Etherne 0/17				
Climb	Advt Version	u, ⁹				
Callennes Marianes	THL.	200				
PIUITICAST	Capability	Switch LGMP				
	Platform	0500 WS-05560G-24PS				
	Software Version	C sto 105 Software, Clubb Software (CUSCU-IPDASL-N	Mì, Versior	23.2(29)5184	ALLASE	

This page shows the following information:

- The name of the access point
- The MAC address of the access point's radio · The IP address of the access point
- The interface on which the CDP packets were received
- The name of the CDP neighbor
- The IP address of the CDP neighbor
- The port used by the CDP neighbor
- The CDP version being advertised (v1 or v2)
 The time left (in seconds) before the CDP neighbor entry expires
- The functional capability of the CDP neighbor, defined as follows: R Router, T Trans Bridge,

- B Source Route Bridge, S Switch, H Host, I IGMP, r Repeater, or M Remotely Managed Device
 The hardware platform of the CDP neighbor device
 The software running on the CDP neighbor
- Step 6 Choose Traffic Metrics to see CDP traffic information. The CDP > Traffic Metrics page appears (see Figure 4-50).

Figure 4-50 CDP > Traffic Metrics Page

<pre>bit bit bit bit bit bit bit bit bit bit</pre>		alialia				111114-10-10-	Sage Contiguration	Bolg Lug_ut Berrysh	
Image: Specific S	b1=-	ltar	CDP > Traffie Mate	les					
A series of the series of t	191011	inter	COF > Trainc let	16.6					
	Su	unmary Calata	Packets In Packets Out			238115			
) AC	atistics	Checksum Errors			L.			
Bit State State Bit State Bit State Bit State Sta	- cr	יינ	No flemony Errors			ι.			
The control of Subset information in a state of the state informat	1 1	nterface Keighbors IF Keighbors raffic Metrics	Invalid Packets			C		212208	
• Instruct of CP index makes in the second of the seco	This pag	e shows the following inf	ormation:						
<pre>bit constrained and const</pre>	 The The The The The The 	number of CDP packets number of CDP packets number of packets that of number of packets dropp number of invalid packets	received by the controller sent from the controller experienced a checksum erro ped due to insufficient memor ts	r Y					
Is of the sing state CDP and exclude Up and excl	Using the To config	e CLI to Configure the gure CDP using the contr	Cisco Discovery Protoco oller CLI, follow these steps:	51					
original (inde) The status of the s	Step 1	Enable or disable CDP	on the controller by entering	this command:					
C P a result of the control of the c	config co	dp {enable disable}							
<pre>very setup: very setup:</pre>	CDP is e	enabled by default.	which CDP messages are to	he generated by entering	this command:				
 The set of the set o	Step 2	a time and	which CDP messages are to	be generated by entening	rns command.				
But Sub of a source of ene to source of ene to source of the to source of the town of the source of the town of the source of	The rang	ap timer seconds ge is 5 to 254 seconds, a	nd the default value is 60 sec	onds.					
<pre>print print p</pre>	Step 3	B Specify the amount of	time to be advertised as the t	ime-to-live value in genera	ted CDP packets by ente	ring this command:			
The magnet the XEB function. Let use the latter when the tit the latter. Since the second of the control of the	config co	dp holdtime seconds							
Interference of the second process of the	The rang	ge is 10 to 255 seconds, and the bighest CP	and the default value is 180 s	econds.	command:				
In the second protocol (C) and protocol (C) or unit access points have a point to the controler to points () activity of a point (). The second () activity of a point () activity of ac	confia ~	n advertise /u1 Lu2\							
Is the full so classic CPF and access points that append to be control by control be control of access point that append to be control of access point that append to be control of access point that access point access point that access point access point access point that access point ac	The defa	ault value is v1.							
b costs due to correct or costs due to correct or cost due to costs ports that p in the barse. COP wants dualke cor boh numm and barse access ports own after the corrector or costs of the costs ports that p in the barse. COP wants dualke COP in all access ports pared to the corrector or costs of the costs ports and the costs port of the costs ports and the cost	Step 5	5 Enable or disable CDP	on all access points that are	joined to the controller by	entering the config ap co	lp {enable disable	all command.		
A second sec	The con	fig ap cdp disable all com	mand disables CDP on all ac	ccess points that are joine	d to the controller and all	access points that j	oin in the future. CDP remain	is disabled on both current and	future access points even after the controller or
A decision of an of advances point point by the controls up may table and then results CDP on induces point using the controls in Bigs 8. After you datable CDP on advances point to the controls up way may not points of advances point. Bigs 1 Exclusion datable CDP on advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bigs 1 Exclusion datable CDP and by advances point by entering this controls. Bi	autess p	round reported. TO enable (, enter the coming ap cop	onadie an contributio.					
Spi 1 Exable of cable OP in specific access part by entring the commant: Spi 2 Exable of cable OP and bots of the cable of the commant: To access the cable of the cable of the cable of the commant of the commant: Spi 2 Example of the cable of the cable of the commant of the comma	ote After you enable a	u enable CDP on all acce ind then disable CDP on	ess points joined to the contro individual access points.	oller, you may disable and	then reenable CDP on in	dividual access poir	its using the command in Ste	ep 6. After you disable CDP on a	all access points joined to the controller, you may r
<pre>end ge update i decided (come, pie) Be 1 - Comment is an only Comment of the comment of the</pre>	Step 6	5 Enable or disable CDP	on a specific access point by	y entering this command:					
Be 7 Be spic sharped by elements gives commune: a searce config Line gate accord and a searce config accord and a searce by a searce of a searce accord accord as a constrainer. De that is a second and a searce config accord as a searce by a searce of a searce accord accord as a constrainer. De that is a second accord accord accord as a constrainer. De that is a second accord acc	config ap	cdp {enable disable} C	lisco_AP						
a set outly be set of the Cut to View Class Discovery Protocol Information be set of the Cut to View Class Discovery Protocol Information ty entering the commute: be set of the Cut to View Class Discovery Protocol Information ty entering the commute: be set of the Cut to View Class Discovery Protocol Information ty entering the commute: be set of the Cut to View Class Discovery Protocol Information ty entering the commute: be set of the Cut to View Class Discovery Protocol Information ty entering the commute: be set of the Cut to View Class Discovery Protocol Information ty entering the commute: be set of the Cut to View Class Discovery Protocol Information ty entering the commute: be set of the Cut to View Class Discovery Protocol Information ty entering the commute: be set of the Cut to View Class Discovery Protocol Information ty entering the commute: be set of the Cut to View Class Discovery Protocol Information to a given part for example, packets area discovery, CRC error, and so on by entering the commute: be set of the Cut to View Class Discovery Protocol Information to a given part for example, packets area discovery, CRC error, and so on by entering the commute: be set of the Cut to View Class Discovery Protocol Information to a given part for example, packets area discovery, CRC error, and so on by entering the commute: be set of the Cut to View Class Discovery Protocol Information to a given part for example to commute: be set of the Cut to View Class Discovery Protocol Information to a given part for example to commute: be set of the Cut to View Class Discovery Protocol Information to a given part for example to commute: be set of the Cut to View Class Discovery Protocol Information to a given part for example to commute: be set of the Cut to View Class Discovery Protocol Information to the to to controler to y entering these commute: be set of the Class Discovery Protocol Information to the controler Protocol Information to the controler Protocol Information to the protocol Inf	Step 7	7 Save your changes by	entering this command:						
Using the CLI to View Clicco Discovery Protocol Information to entroller using the controller (LL) follow these steps: Set 15 Set to status of COP and to view COP protocol Information by entrolling the command: Wave Click Set 2 Set to status of COP and to view COP protocol Information by entrolling the command: The control does only the COP neighbors on all interfaces by entrolling the command: The control does only the COP neighbors of the controller 100P neighbors. The control does only the COP neighbors on a given on the controller 100P neighbors of the controller 100P neighbors of the controller 100P neighbors of the controller 100P neighbors on a given on the exercise of the controller 100P neighbors on a given on the exercise of the controller 100P neighbors on a given on the exercise on the database by entrolling the command: Set 3 Set all COP neighbors on a given on the exercise on the controller 10 entrolling the command: Adver ag do given and Clicks, AP Set 4 Set 100P neighbors agreement Clicks, AP Set 5 Set 100 all COP neighbors for a appelic access point by entrolling these commands: - shows ag do given agreement Clicks, AP Set 5 Set 5 all of all COP neighbors for a laccess point by entrolling these commands: - shows ag do given agreement Clicks, AP Set 5 Set 5 all of all COP neighbors for all access point by entrolling these com	save cor	nfig							
 The common diverse only the CDP neighbors of the controller. It does not show the CDP neighbors of the controller's associated access points. Additional commands are provided below to show the list of CDP neighbors per access point. See all CDP entities in the database by entering the command: does only by entering this command. See all CDP trails for a good a cocess point by entering the command: does only by entering this command. See all CDP trails for a lacotes point by entering the command: does only by entering this command. Stars 5 See the CDP status for a lacotes point by entering thes command: Stars 5 See the CDP status for a lacotes point by entering these command: Stars 5 See the CDP status for a lacotes point by entering these command: Stars 6 See the CDP status for a lacotes point by entering these command: Stars 7 See all CDP neighbors for a specific access point by entering these command: Stars a cost point and a cost points that an consisted to the controller by entering these command: Stars a cost point approxima Clicks AP The access point sends CDP neighbors for all access points on the information charges. Stars a cost point by a specific access point by entering these command: Stars a cost of CDP neighbors for all access points on the follow ap cogn neighbors and Clicks AP The access point sends CDP neighbors for all access points and an constraint by entering these command: Stars a cost of CDP neighbors for all access points and an constraint by entering these command: Stars a cost of CDP neighbors for all access points and an constraint by entering these command: Stars a cost of CDP neighbors for all access point set of an optic point point for the stars of point point point for the stars of point point for the stars optic acces and cost point point point poin	Step 1 show cd Step 2 show cd	See the status of CDP P See a list of all CDP ne p neighbors [detail] onal detail command prov	and to view CDP protocol inf	iormation by entering this entering this command:	command:				
The command shows only the CDP neighbors of the controller. It does not show the CDP neighbors of the controller's associated access points. Additional commands are provided below to show the list of CDP neighbors per access point. Additional commands are provided below to show the list of CDP neighbors per access point. Additional commands are provided below to show the list of CDP neighbors per access point. Additional commands are provided below to show the list of CDP neighbors per access point. Additional commands are provided below to show the list of CDP neighbors per access point by entering this command: thore up do per access point by entering this command: thore up do per access points and access points by entering thes commands: See 5 See 6 the CDP status for a guedin access points by entering these commands: See 7 See at to all CDP neighbors for a guedin access points per access point by entering these commands: See 7 See at to all CDP neighbors for a guedin access points per access points and access points accesses accesseses accesses accesses accesses accesses accesses	•								
Sep 3 See al CDP entities in the database by entering this commant: Sep 4 See CDP lattic formation on a given port for example, packets sent and received, CCC errors, and so on') by entering this command: Sep 5 See the CDP lattic formation on a given port for example, packets sent and received, CCC errors, and so on') by entering this command: Sep 5 See the CDP lattic formation on a given port for example, packets sent and received, CCC errors, and so on') by entering this command: Set 5 See the CDP lattics for al access points by entering the command: Set or ap cdp neighbors ap-name Close, P Set 5 See the CDP lattics for al access point by entering these commands: so way cdp neighbors ap-name Close, P Set 5 See the CDP lattics for al access points connected to the controller by entering these commands: so way cdp neighbors for all access points connected to the controller by entering these commands: so way cdp neighbors for all access points connected to the controller by entering these commands: so way cdp neighbors for all access points connected to the controller by entering these commands: so way cdp neighbors for all access points connected to the controller by entering these commands: Memotion similar to the following appears when you enter the show ap odp neighbors all command: Memotion similar to the following appears when you enter the show ap odp neighbors detail al command: Applier Accel 10 F 7. 108.127 Geptic Hierment L/26 Applier 10 F 10.116 (SD 10.11 SPD1-10.	ote This cor	mmand shows only the C	DP neighbors of the controlle	r. It does not show the CE	P neighbors of the contro	oller's associated a	cess points. Additional comm	nands are provided below to sho	ow the list of CDP neighbors per access point.
biou odp enty all Bep 4. See CDP raffic information on a given port for example, packets sens and received, CRC errors, and so on by entering this command: drow odp prime throw odp prime Bep 5. See the CDP status for a specific access point by entering this command: drow odp prime Bep 6. See the CDP status for a specific access point by entering these commands: drow odp prime Bep 7. See a list of al CDP neighbors for a specific access point by entering these commands: drow on prime Bep 7. See a list of al CDP neighbors for a specific access point by entering these commands: drow on prior prime Bep 7. See a list of al CDP neighbors for a specific access point by entering these commands: drow on prior prior draw of prine drow on prior prior draw of the prime Bep 7. See a list of al CDP neighbors information to the controller only when the information changes. See 8. See a list of al CDP neighbors for all access points connected to the controller by entering these commands: drow on prior prior biol drow on prior prior draw all drow on prior prior draw all drow on prior prior draw all drow on prior prior biol drow on prior biol drow o	Step 3	3 See all CDP entries in	the database by entering this	command:					
Sep 6 4 See CPP traffic information on a given port for example, packets sent and received, CRC errors, and so only by entering this command: show dp chp traffic Step 5 See the CDP status for a specific access point by entering this command: show ap cdp aperame Close JAP Sep 7 See a list of al CDP neighbors for a specific access point by entering these commands: • show ap cdp neighbors are aspecific access point by entering these commands: • show ap cdp neighbors for a specific access point by entering these commands: • show ap cdp neighbors for a specific access point by entering these commands: • show ap cdp neighbors for all CDP neighbor information to the controller only when the information changes. Step 5 See a list of al CDP neighbors for all access points connected to the controller only when the information changes. See 6 See a list of al CDP neighbors for all access points connected to the controller by entering these commands: • show ap cdp neighbors all • show ap cdp neighbors for all access points connected to the controller by entering these commands: • show ap cdp neighbors for all access points connected to the controller by entering these commands: • show ap cdp neighbors distal all Noter and to the following appears when you enter the show ap cdp neighbors all command: • AP Neage AP IP Neighbor Notion 10.76:10.8.207 (signabilithement1/26 AP Noti3.60:10: cdp 10.76:10.8.207 (signabilithement1/26 AP Noti3.60:10: cdp 10.76:10.8.207 (signabilithement1/26 AP Noti3.60:10: cdp 10.76:10.8.207 (signabilithement1/26 AP Noti3.60: cdp 10.76:10.8.207 (signabilithement1/26 AP Noti3.60: cdp 10.76:10.8.207 (signabilithement1/26 AP Noti3.60: cdp 10.76:10.8.207 (s	show cd	p entry all							
show qc dp fmlic Skep 5 See the COP status for all access point by entering this command: thow ap cdp answ Cabco, AP Skep 5 See the COP status for all access point by entering thes commands: thow ap cdp neighbors dp answ Cabco, AP Skep 7 See a ist of all COP neighbor for a specific access point by entering thes commands: • show ap cdp neighbors dp answ Cabco, AP • show ap cdp neighbors dp answ Cabco information to the controller only when the information charges. Skep 5 See a lst of all CDP neighbor information to the controller only when the information charges. Skep 6 See a lst of all CDP neighbors for all access points connected to the controller by entering these commands: • show ap cdp neighbors defail all • show ap cdp neighbors lall = • show ap cdp neighbors for all access points connected to the controller by entering these commands: • show ap cdp neighbors information in the following appears when you enter the show ap cdp neighbors all command: • AP Name AP IP Neighbor IN mans Neighbor IP Neighbor IP Nei • Noticit, choi 10, 76, 1108, 120 (500-110, 76, 1108, 207 (5)); short 510, 207 (5); short 510, 207 (5	Step 4	See CDP traffic inform	ation on a given port (for exa	mple, packets sent and re-	eived, CRC errors, and s	so on) by entering th	is command:		
We pay Solution ULP status for a specific access point by entering the controller by entering this commant: show ap cdp and Step 5 See the CDP status for all access point by entering these commands: . show ap cdp neighbors for a specific access point by entering these commands: . show ap cdp neighbors for a specific access point by entering these commands: . show ap cdp neighbors for a specific access point by entering these commands: . show ap cdp neighbors for all access points on the controller only when the information changes. Step 5 See a list of all CDP neighbors for all access points on ended to the controller only when the information changes. Step 5 See a list of all CDP neighbors for all access points on ended to the controller only when the information changes. Applies See a list of all CDP neighbors for all access points on ended to the controller only when the information changes. Step 5 See a list of all CDP neighbors for all access points on ended to the controller only when the information changes. Applies AP 1D Religibor Name Neighbors IP Neighbor Port woolld, 601c. 000 10, 76, 108, 122 (5800-1 10, 76, 108, 207 (Sigabititherment/27 woolld, 601c. 000 10, 76, 108, 123 (5800-1 10, 76, 108, 207 (Sigabititherment/27 woolld, 601c. 000 10, 76, 108, 123 (5800-1 10, 76, 108, 207 (Sigabititherment/28 woolld, 601c. 000 10, 76, 108, 123 (5800-1 10, 76, 108, 207 (Sigabititherment/28 woolld, 601c. 000 10, 76, 108, 207	show cd	p traffic		and a state of the second state of the					
The access point sends costs points that are connected to the controller by entering these command: How ap cdp all Sep 5 See a list of all CDP neighbors for a spacific access point by entering these commands: • show ap cdp neighbors ap-name Cisco, AP • the access point sends CDP neighbors for all access points that are connected to the controller only when the information changes. Sep 5 See a list of all CDP neighbors for all access points connected to the controller by entering these commands: • show ap cdp neighbors all • show ap cdp neighbors all access points into the show ap cdp neighbor information term and the show ap cdp neighbor fort • applies and information similar to be blowing appears when you enter the show ap cdp neighbor all all command: AP IPA Address 1: 10.7.6.108.207 GigabitEthermet1/26 AP OID: Acferess 1: 10.7.6.108.207 Plat form icines WH-ofShow appears when you e	show an	cdp ap.pame Cisco AP	a specific access point by e	ntering tris command.					
Bits PT See a list of all CDP neighbors for a specific access point by entering these commands: show ap och neighbors ap-name Cisco, AP • show ap och neighbors detail Cisco, AP • The access point sends CDP neighbors for all access points connected to the controller only when the information dharges. Step 5 See a list of all CDP neighbors for all access points connected to the controller only when the information dharges. Step 6 See a list of all CDP neighbors for all access points connected to the controller only when the information dharges. Step 6 See a list of all CDP neighbors for all access points connected to the controller only when the information dharges. Step 6 See a list of all CDP neighbors for all access points connected to the controller only when the information tharges. More ap och neighbors all Normation similar to the following appears when you enter the show ap och preighbors all command: AP Name, AP IP Neighbor Name Neighbor IP Neighbor Port	Step 6	See the CDP status for	r all access points that are co	nnected to the controller b	by entering this command	:			
<pre>style="text-allocal-alloc</pre>	show ap	cdp all	labbara far a anadifa agagaa	point hu optoring those o	ammon do:				
 show ap cdp neighbors detail Cisco_AP show ap cdp neighbors detail Cisco_AP The access point sends CDP neighbor information to the controller only when the information changes. Step 8 See a list of all CDP neighbors for all access points connected to the controller by entering these commands: show ap cdp neighbors all show ap cdp neighbors detail all Information similar to the following appears when you enter the show ap cdp neighbors all command: 	Step /	See a list of all CDP new second s	agribbits for a specific access	point by entering these c	ommands:				
The access point sends CDP neighbor information to the controller only when the information changes. Step 8 See a list of all CDP neighbors for all access points connected to the controller by entering these commands: • show ap cdp neighbors detail all Information similar to the following appears when you enter the show ap ddp neighbors all command: A P Name AP IP Neighbor Name Neighbor IP Neighbor Port • Avol13.601c.000 10.76.108.113 6500-1 10.76.108.207 GigabitEthernet1/26 Avol13.601c.000 10.76.108.113 6500-1 10.76.108.207 GigabitEthernet1/27 Avol13.601c.000 10.76.108.113 6500-1 10.76.108.207 GigabitEthernet1/28 Information similar to the following appears when you enter the show ap ddp neighbors detail all command: AP IP Addressi 10.76.108.115 Device 1D: 6500-1 Envice 1D: 6500-	 sho 	w ap cdp neighbors detai	I Cisco_AP						
The access point sends CDP neighbor information to the controller only when the information changes. Step 1 See a list of all CDP neighbors for all access points connected to the controller by entering these commands: • show ap cdp neighbors all • show ap cdp neighbors detail all Normation similar to the following appears when you enter the show ap cdp neighbors all command: AP Name AP IP Neighbor Name Neighbor IP Ne	a								
<pre>Step 8 See a list of all CDP neighbors for all access points connected to the controller by entering these commands: show ap cdp neighbors all show ap cdp neighbors detail all Information similar to the following appears when you enter the show ap cdp neighbors all command: AP Name AP IP Neighbor Name Neighbor IP Neighbor Pott </pre>	ote The acc	cess point sends CDP nei	ghbor information to the cont	roller only when the inform	nation changes.				
<pre>etc spont and the formation that becomparison of the controller of the formation of the following appears when you enter the show ap cdp neighbors all command: AP Name AP 1P Neighbor Name Neighbor IP Neighbor Port </pre>	Sten	See a list of all CDP or	highbors for all access points	connected to the controlle	r by entering these comp	nands:			
<pre>• show good neighbors detail all homation similar to the following appears when you enter the show ap cdp neighbors all command:</pre>	e sha	w an odo neighbore all	ignoord for an access points		in by citiciting these contri	kindo.			
<pre>hlomation similar to the following appears when you enter the show ap cdp neighbors all command: AP Name AP IP Neighbor Name Neighbor IP Neighbor Port </pre>	 sho 	w ap cdp neighbors detai	i all						
AP Name AP IP Neighbor Name Neighbor IP Neighbor Port AD0013.601c.0a0 10.76.108.123 6500-1 10.76.108.207 GigabitEthernet1/26 AD013.601c.0a0 10.76.108.121 6500-1 10.76.108.207 GigabitEthernet1/27 AD0013.601c.0b0 10.76.108.121 6500-1 10.76.108.207 GigabitEthernet1/28 Mformation similar to the following appears when you enter the show ap cdp neighbors detail all command: AP Name # PD013.601c.0a0 AP IP Address: 10.76.108.125 Device ID: 6500-1 Entry address(eg): 10.76.108.207 Platform: cisco NS-C5056-F, Capabilities: Router Switch IGMP Interface: Port - 1, Port ID (outgoing port): GigabitEthernet1/26 Holdtime: 157 sec Version: Cisco Internetwork Operating System Software IOS (tm) a72033_rp-SV-M), Version 12.2(18)SXD5, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Pri 13-Ma	Informati	ion similar to the following	appears when you enter the	show ap cdp neighbors a	Il command:				
APOD13.601c.0a0 10.76.108.123 6500-1 10.76.108.207 GigabitEthermet1/26 APOD13.601c.0b0 10.76.108.123 6500-1 10.76.108.207 GigabitEthermet1/27 APOD13.601c.0b0 10.76.108.113 6500-1 10.76.108.207 GigabitEthermet1/28 Information similar to the following appears when you enter the show ap cdp neighbors detail all command: AP Name: APOD13.601c.0a0 AP IE Addressi : 10.76.108.125 	AP	Name AP IP Neighbo	r Name Neighbor IP Ne	eighbor Port					
ApOllSOLC.000 10.7.6.108.125 650-1 10.76.108.207 GigabitEthermet1/26 Hoformation similar to the following appears when you enter the show ap cdp neighbors detail all command: AP URA EARDERS 10.76.108.125 	APO	013.601c.0a0 10.76	.108.123 6500-1 10.76	5.108.207 GigabitEt	hernet1/26				
<pre>witormation smart to me following appears when you enter the show ap cdp neighbors detail all command: AP Neme: APOILS.601.0.80 AP IP Address: 10.76.108.125 </pre>	APO	013.601c.0c0 10.76	.108.125 6500-1 10.76	5.108.207 GigabitEt	hernet1/28				
AP IP Adverssi 10.76.108.125 	Info	mation similar to the follo	wing appears when you ente	er the show ap cdp neighb	ors detail all command:				
Device ID: 6500-1 Entry address(es): 10.76.108.207 Platform: cisco NS-C6506-E, Capabilities: Router Switch ICMP Interface: Port - 1, Port ID (outgoing port): GigabitEthernet1/26 Holdtime: 157 sec Version: Cisco Internetwork Operating System Software IOS (tm) s72033_xrp Software (s72033_rp-PSV-M), Version 12.2(18)SXD5, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Fri 13-Ma The access point sends CDP neighbor information to the controller only when the information changes.	AP	IP Address: 10.76.	108.125						
Entry address(es): 10.76.108.207 Platform: cisco NS-C6506-E, Capabilities: Router Switch IGMP Interface: Port - 1, Port ID (outgoing port): GigabitEthernet1/26 Holdtime: 157 sec Version: Cisco Internetwork Operating System Software IOS (tm) s72033_xp Software (s72033_xp-PSV-M), Version 12.2(18)SXD5, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Fri 13-Ma • The access point sends CDP neighbor information to the controller only when the information changes.	 Derr	rice TD: 6500-1							
Platform: cisco NS-C6506-E, Capabilities: Router Switch IGMP Interface: Port - 1, Port ID (outgoing port): GigabitEthernet1/26 Holdtime: 157 sec Version: Cisco Internetwork Operating System Software IOS (tm) s72033_xp Software (s72033_xp-PSV-M), Version 12.2(18)SXD5, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Fri 13-Ma	Ent	ry address(es): 10	.76.108.207						
Holdtime: 157 sec Version: Circo Internetwork Operating System Software IOS (tm) s72033_xp Software (s72033_xp-PSV-M), Version 12.2(18)SXD5, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Fri 13-Ma The access point sends CDP neighbor information to the controller only when the information changes.	Pla Trt	tform: cisco WS-C6 erface: Port - 1	506-E, Capabilities: Port ID (outgoing por	Router Switch IGMP (t): GigabitEtherne	t1/26				
Version: Ciaco Internetwork Operating System Software IOS (tm) s72033_rp Software (s72033_rp-PSV-M), Version 12.2(18)SXD5, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Pri 13-Ma 	Hol	dtime: 157 sec	,		-				
http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Fri 13-Ma	Ver Cis	sion: co Internetwork Op	erating System Softwa	are IOS (tm) s72033	_rp Software (s720)	33_rp-PSV-M),	Version 12.2(18)SXD5,	RELEASE SOFTWARE (fc3)	Technical Support:
The access point sends CDP neighbor information to the controller only when the information changes.	htt	p://www.cisco.com/	techsupport Copyright	(c) 1986-2005 by	cisco Systems, Inc	. Compiled Fri	13-Ma		
	te The acc	cess point sends CDP nei	ghbor information to the cont	roller only when the inform	nation changes.				

To obtain CDP debug information for the controller using the controller CLI, follow these steps: Step 1 Obtain debug information related to CDP packets by entering by entering this command: debug cdp packets Step 2 Obtain debug information related to CDP events by entering this command:

debug cdp events

Configuring RFID Tag Tracking

The controller enables you to configure radio-frequency identification (RFID) tag tracking, RFID tags are small wireless devices that are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the location appliance. To know more about the tags supported by controller, see http://www.cisco.com/web/partners/pr46/pr147/cox, wifi, tags.html . Some of the tags from these vendors comply with Cisco Compatible Extensions for RFID Tags. See Table 4-4 for details. The location appliance receives telemetry and chokepoint information from tags that are compliant with this CCX specification.

Table 4-4 Cisco Compatible Extensions for RFID Tags Summary

Partners	AeroScout		WhereNet	Pango (InnerWireless)
Product Name	T2	тз	Wheretag IV	V3
Telemetry				
Temperature	x	х	-	x
Pressure	-	-	-	-
Humidity	-	-	-	-
Status	-	-	-	-
Fuel	-	-	-	-
Quantity	-	-	-	—
Distance	-	-	-	—
Motion Detection	х	х	-	x
Number of Panic Buttons	1	2	0	1
Tampering		х	x	x
Battery Information	x	x	x	x
Multiple-Frequency Tags_	x	x	x	
Services and a service service and a service s				

⁰

Note The Network Mobility Services Protocol (NMSP) runs on location appliance software release 3.0 or later releases. In order for NMSP to function properly, the TCP port (16113) over which the controller and location appliance communicate must be open (not blocked) on any firewall that exists between these two devices. See the Cisco Location Appliance Configuration Guide for additional information on NMSP and RFID tags.

The Cisco-approved tags support these capabilities:

Information notifications —Enable you to view vendor-specific and emergency information.

Information polling — Enables you to monitor battery status and telemetry data. Many telemetry data types provide support for sensory networks and a large range of applications for RFID tags.

Measurement notifications —Enable you to deploy chokepoints at strategic points within your buildings or campuses. Whenever an RFID tag moves to within a defined proximity of a chokepoint, the tag begins transmitting packets that advertise its location in relation to the chokepoint.

The number of tags supported varies depending on controller platform. Table 4-5 lists the number of tags supported per controller

Table 4-5 RFID Tags Supported per Controller

Controller	Number of RFID Tags Supported
5508	2500
Cisco WISM	5000
4404	2500
4402	1250
Catalyst 3750G Integrated Wireless LAN Controller Switch	1250
2106	500
Controller Network Module within the Cisco 28/37/38xx Series Integrated Services Routers	500
You can configure and view RFID tag tracking information through the controller CLI.	

Using the CLI to Configure RFID Tag Tracking

To configure RFID tag tracking parameters using the controller CLI, follow these steps:

Step 1 Enable or disable RFID tag tracking by entering this command:

config rfid status { enable | disable } The default value is enabled.

Step 2 Specify a static timeout value (between 60 and 7200 seconds) by entering this command:

config rfid timeout seconds

The static timeout value is the amount of time that the controller maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.

Step 3 Enable or disable RFID tag mobility for specific tags by entering these commands

config rfld mobility vender_name enable — Enables client mobility for a specific vendor's tags. When you enter this command, tags are unable to obtain a DHCP address for client mode when attempting to select and/or download a configuration.

• config rfid mobility verdor_name disable — Disables client mobility for a specific vendor's tags. When you enter this command, tags can obtain a DHCP address. If a tag roams from one subnet to another, it obtains a new address rathe than retaining the anchor state.

Note These commands can be used only for Pango tags. Therefore, the only valid entry for vendor_name is "pango" in all lowercase letters.

Using the CLI to View RFID Tag Tracking Information

To view RFID tag tracking information using the controller CLI, follow these steps:

Ct	One the surrout coefficienties (as DEID to a tracking by exterior while a surrout di
Step 1	See the current confiduration for KFID tad tracking by entering this command:

show rfid config

0

Information similar to the following appears:

State:Disabled

Step 2 See detailed information for a specific RFID tag by entering this command:

show rfid detail mac_address

where mac address is the tag's MAC address.

Information similar to the following appears:

RFID address	00:12:b8:00:20:52
Vendor	G2
Last Heard	51 seconds ago
Packets Received	2
Bytes Received	324
Cisco Type	

Content Header ----- Heard

where

0

0

Note

where

show auth-list

Information similar to the following appears:

 Version
 1

 Tx Power
 12 dBm

 Ghannel
 1

 Reg Class
 12

Burst Length..... 1 CCX Payload Payload Data Hex Dump 01 09 00 00 00 00 0b 85 52 52 52 02 07 4b ff ff 7f ff ff ff 03 14 00 12 7b 10 48 53 cl f7 51 4b 50 ba 5b 97 27 80 00 67 00 01 03 05 01 42 34 00 00 03 05 02 42 5c 00 00 03 05 03 42 82 00 00 03
 00
 05
 05
 02
 42
 52
 00
 00
 05
 05
 04
 42
 96
 00
 03
 02
 05
 05
 00
 00
 05
 05
 03
 02
 82
 00
 00
 05
 05
 03
 02
 82
 00
 00
 05
 05
 03
 02
 04
 04
 05
 05
 03
 02
 05
 04
 42
 06
 00
 03
 02
 07
 05
 03
 12
 08
 10
 00
 01
 02
 03

 04
 05
 06
 07
 08
 09
 0a
 0b
 0c
 0d
 0e
 0f
 03
 04
 09
 03
 08 05 07 a8 02 00 10 00 23 b2 4e 03 02 0a 03 Nearby AP Statistics: lap1242-2(slot 0, chan 1) 50 seconds ag.... -76 dBm lap1242(slot 0, chan 1) 50 seconds ago..... -65 dBm Step 3 See a list of all RFID tags currently connected to the controller by entering this command: show rfid summary Information similar to the following appears Total Number of RFID : 24 RFID ID VENDOR Closest AP RSSI Time Since Last Heard 00:04:fl:00:00:03 Wherenet HReap -70 151 seconds ago 00:04:fl:00:00:05 Wherenet HReap -66 251 seconds ago 00:0c:cc:5b:f8:le Aerosct HReap -40 5 seconds ago 00:0c:cc:5c:05:10 Aerosct HReap -68 25 seconds ago 00:0c:cc:5c:87:34 Aerosct HReap -40 5 seconds ago 00:14:7e:00:05:4d Pango ciscol242 -66 298 seconds ago Step 4 See a list of RFID tags that are associated to the controller as clients by entering this command: show rfid client When the RFID tag is in client mode, information similar to the following appears: RFID Mac VENDOR Sec Ago Associated AP Chul Client State 00:14:7e:00:0b:bl Pango 35 AP0019.e75c.fef4 1 Probing When the RFID tag is not in client mode, the above text boxes are blank. Using the CLI to Debug RFID Tag Tracking Issues If you experience any problems with RFID tag tracking, use these debug commands Configure MAC address debugging by entering this command: debug mac addr mac address 0 Note We recommend that you perform the debugging on a per-tag basis. If you enable debugging for all of the tags, the console or Telnet screen is inundated with messages Enable or disable debugging for the 802.11 RFID tag module by entering this command. debug dot11 rfid { enable | disable } · Enable or disable RFID debug options by entering this command debug rfid { all | detail | error | nmsp | receive } { enable | disable } albonfigures debugging of all RFID messages detailconfigures debugging of RFID detailed messages errorconfigures debugging of RFID error messages. nmspconfigures debugging of RFID NMSP messages receiveconfigures debugging of incoming RFID tag messages. Configuring and Viewing Location Settings This section provides instructions for configuring and viewing location settings from the controller CLI. Note Access points in monitor mode should not be used for location purposes. Installing the Location Appliance Certificate Assil-signed certificate (SSC) is required on the location appliance. This certificate, which is comprised of the location appliance MAC address and a 20-byte key hash, must be present on the controller. Otherwise, the controller cannot authenticate the location appliance, and they can never establish a connection. WCS usually pushes the certificate to the controller automatically, but you can install the certificate on the controller using the controller CLI if necessary (for example if the controller is not connected to WCS of an energy or certificate match occurs on WCS). If an error occurs on WCS and prevents the location appliance certificate from being pushed to the controller, make sure that the time zone has been synchronized on the controller and the location appliance before following this procedure. Follow the instructions in the "Vewing Location Settings" section to do so. To install the location appliance certificate on the controller using the controller CLI, follow these steps Step 1 Obtain the key hash value of the location appliance certificate by entering this command: debug pm pki enable Information similar to the following appears: Information similar to the following appears: Thu Oct 11 08:52:26 2007: sabpmGetLssuerHandles: Key Data 30820122 3000609 2a66486 f7000101 Thu Oct 11 08:52:26 2007: sabpmGetLssuerHandles: Key Data 30820122 3000609 2a66486 f7000101 Thu Oct 11 08:52:26 2007: sabpmGetLssuerHandles: Key Data 0098985 d2b7C77b 036cdb87 5bd2065a Thu Oct 11 08:52:26 2007: sabpmGetLssuerHandles: Key Data 0908985 d2b7C77b 036cdb87 5bd2065a Thu Oct 11 08:52:26 2007: sabpmGetLssuerHandles: Key Data 0908985 d2b7C77b 036cdb87 5bd2065a Thu Oct 11 08:52:26 2007: sabpmGetLssuerHandles: Key Data 89466614 df1cbcrb fe2fcf01 09D723a Thu Oct 11 08:52:26 2007: sabpmGetLssuerHandles: Key Data 5092071 ecl50615 d236531 573fc25e Thu Oct 11 08:52:26 2007: sabpmGetLssuerHandles: Key Data 50920301 0001 Thu Oct 11 08:52:30 2007: sabpmGetLssuerHandles: Key Data 50920301 0001 Thu Oct 11 08:52:30 2007: sabpmGetLssuerHandles: Key Data 19020301 0001 config auth-list add lbs-ssc lbs_mac lbs_key Ibs_mac is the MAC address of the location applia Ibs_key is the 20-byte key hash value of the certificate. Step 3 Save your changes by entering this command: s ave config Step 4 Verify that the location appliance certificate is installed on the controller by entering this command:

	Authorize APs against AAA
	Allow APs with Self-Signed Certificate (SSC) disabled
	Mac Addr Cert Type Key Hash
\$	Synchronizing the Controller and Location Appliance
	For controller software release 4.2 or later releases, if a location appliance (release 3.1 or later releases) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, the times must be synchronized on the two devices. We recommend that you set the time even for networks that do not have location appliances. See the "Configuring 802.11 Bands" section for instructions on setting the time and date on the
0	
Note	The time zone can be different for the controller and the location appliance, but the time zone delta must be configured accordingly, based on GMT.
(Configuring Location Settings
	points for clients, RFID tags, and roue access points.
	 vmere 2 is one or the toilowing: client (enable) disable) burst_interval — Enables or disables the path loss measurement request for normal, noncalibrating clients. The valid range for the burst_interval parameter is 1 to 3600 seconds, and the default value is 60 seconds.
	calibrating (enable disable) {uniband multiband}—Enables or disables the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio or on the associated 802.11a or 802.11a
	If a client does not send probes often or sends them only on a few channels, its location cannot be updated or cannot be updated accurately. The config location pim command forces clients to send more packets on all channels. When a CCXW (or higher) client associates, the controller sense is a path loss measurement request, which instructs the client to transmit on the bands and channels that the access points are on (typically, channels 1, 6, and 11 for 2.4-GHz-only access points) at a configurable interval (such as 60 seconds) indefinitely.
	Configure the RSSI timeout value for various devices by entering this command:
	config location expiry ?
	where 2 is one of the following: - client timeout—Configures the RSSI timeout value for clients. The valid range for the timeouparameter is 5 to 3600 seconds, and the default value is 5 seconds.
	- calibrating-client <i>timeout</i> —Configures the RSSI timeout value for calibrating clients. The valid range for the <i>timeout</i> parameter is 0 to 3600 seconds, and the default value is 5 seconds.
	 regular interview of the result interview
	Ensuring that recent, strong RSSIs are retained by the CPU is critical to location accuracy. The config location expiry command enables you to specify the length of time after which old RSSI averages expire.
	Note We recommend that you do not use or modify the config location expiry command.
	Configure the RSSI half life for various devices by entering this command:
	config location rssi-half-life ?
	where 2 is one of the following: - client half_life—Configures the RSSI half life for clients. The valid range for the half_lifeparameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
	- calibrating-client half_life — Configures the RSSI half life for calibrating clients. The valid range for the half_lifeparameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
	 tags half_life —Configures the KSS half life for KSS half life for rogue access points. The valid range for the half_lifeparameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds. rogue-aps half_life —Configures the RSS half life for rogue access points. The valid range for the half_lifeparameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
	Some client devices transmit at reduced power immediately after changing channels, and RF is variable, so RSSI values might vary considerably from packet to packet. The config location rssi-half-life command increases accuracy by averaging nonuniformly arriving data using a configurable forget period (or half life).
	Note We recommend that you do not use or modify the config location rssi-half-life command.
	Configure the NMSP notification threshold for RSSI measurements by entering this command:
	config location notify-threshold ?
	- client thresholdConfigures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold darameter is 0 to 10 dB, and the default value is 0 dB.
	 client threshold —Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold —Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold —Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold —Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB.
	 client threshold —Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold —Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold —Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold —Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB.
	client threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold —Configures the NMSP notification notify-threshold command.
	client threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. Note We recommend that you do not use or modify the config location notify-threshold command. Configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command:
	client threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. Note We recommend that you do not use or modify the config location notify-threshold command. Configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command: config to cathon algorithm ? where 7 is not of the following:
	client threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold —Configures the NMSP notification notify-threshold command. Configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command: configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command: simple—Specifies a faster algorithm that requires low CPU overhead but provides less accuracy. simple—Specifies a faster algorithm that requires low CPU overhead but provides less accuracy. viscience—Specifies a faster algorithm bit requires more (CPU overhead but provides less accuracy. viscience—Specifies a faster algorithm bit requires more (CPU overhead but provides less accuracy.
	client threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold/astrameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for RPD pags. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. rogue-aps threshold (in dB) for rogue acces
	client threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold/anameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for rSPD gas. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rSPD gas. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. restrict the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command: configures the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command: configures the algorithm that requires low CPU overhead but provides less accuracy. simple—Specifies a faster algorithm that requires low CPU overhead. The Ver recommend that you do not use or modify the config location algorithm command. Note Ver recommend that you do not use or modify the config locatio
	client threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold/anameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for rGPD tags. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold/parameter is 0 to 10 dB, and the default value is 0 dB. Configure the algorithm tout on on tous or modify the config location notify-threshold command: config location algorithm 2 where 7 is one of the following: set of the
	client threshold—Configures the NMSP notification threshold (in dB) for clients and roque clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for clients and roque clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-ages threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-ages threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. Configures the algorithm to use or modify the config location notify-threshold command. Configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command: configure the algorithm nused to average RSSI and signal-to-noise ratio (SNR) values by entering this command: configure the following: simple—Specifies a faster algorithm that requires low CPU overhead but provides less accuracy. rissi-average—Specifies a faster algorithm but requires more CPU overhead. Note We recommend that you do not use or modify the config location algorithm command. Note We recommend that you do not use or modify the config location algorithm command. //// CPU overhead but provides less accuracy. rissi-average—Specifies a faster algorithm to requires more CPU overhead. /// CPU overhead but provides less accuracy. rissi-average—Specifies a faster algorithm command. /// CPU overhead but provides less accuracy. rissi-average—Specifies a faster algorithm command. /// CPU overhead but provides less accuracy. rissi-average—Specifies a faster algorithm command. /// CPU overhead but provides less accuracy. rissi-average—Specifi
,	client threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. Configures the algorithm threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. Configures the algorithm that you do not use or modify the config location notify-threshold command: configures the algorithm values to average RSSI and signal-to-noise ratio (SNR) values by entering this command: configures the following: simple—Specifies a faster algorithm that requires low CPU overhead but provides less accuracy: rissi-average—Specifies a faster algorithm that requires low CPU overhead. Note We recommend that you do not use or modify the config location algorithm command. Note We recommend that you do not use or modify the config location algorithm command. You we location information, use these CLI commands: To view location information, use these CLI commands: View for a command that point and the use and the default value is 0 dB. To view location information, use these CLI commands: View for a
,	client threshold—Configures the NMSP notification threshold (in dB) for clients and roque clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for clients and roque clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold—Configures the NMSP notification notify-threshold command. Configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command: corrig location algorithm 2 where 2 is one of the following: simple—Specifies a faster algorithm that requires low CPU overhead but provides less accuracy; sis-average—Specifies a faster algorithm but requires more CPU overhead. Note We recommend that you do not use or modify the config location algorithm command. revise We recommend that you do not use or modify the config location algorithm command. revise We recommend that you do not use or modify the config location algorithm command. revise We recommend that you do not use or modify the config location algorithm command. revise We recommend that you do not use or modify the config location algorithm command. revise We recommend that you do not use or modify the config location algorithm command. revise We recommend that you do not use or modify the config location algorithm command. revise We recommend that you do not use or modify the config location algorithm command. revise We recommend that you do not use or modify the config location algorithm command.
,	 client threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for rCPD pags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the approximation threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold contrained that you do not use or modify the config location algorithm command.
,	 client threshold—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for rCPD pags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-aps threshold—Configures the value set or modify the config location set or modify the config location (SNR) values by entering this command. rose value accurate algorithm that requires now CPU overhead but provides less accuracy. rose value accurate algorithm that requires mor
Ň	 elient threshold—Configures the MMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold/exameter is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the threshol/exameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshol/exameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshol/exameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold —Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshol/exameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold —Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshol/exameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold —Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshol/exameter is 0 to 10 dB, and the default value is 0 dB. rogue-age threshold = Configures the algorithm thereinfig the config location notify-threshold command. configures the algorithm 1 trequires low CPU overhead but provides less accuracy. resisverage—Specifies a more accurate algorithm that requires low CPU overhead. Net We recommend that you do not use or modify the config location algorithm command. configures the curve location configuration values by entering this command: to exert location information, use these Cli commands: to exert location information, use these Cli commands: to exert location configuration values by entering this command: to exert location
, ,	eierer threshold—Configures the NMSP notification threshold (in dB) for GPID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. trags threshold—Configures the NMSP notification threshold (in dB) for GPID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. trags threshold—Configures the NMSP notification threshold (in dB) for GPID tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. trags threshold—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. To 10 dB, and tB, and t
'n	 eline threshold—Configures the NMSP notification threshold (in dB) for GFID tags. The valid range for the <i>thresholdparameter</i> is 0 to 10 dB, and the ddfault value is 0 dB. togs <i>threshold</i>—Configures the NMSP notification threshold (in dB) for GFID tags. The valid range for the <i>thresholdparameter</i> is 0 to 10 dB, and the ddfault value is 0 dB. togs <i>threshold</i>—Configures the NMSP notification threshold (in dB) for GFID tags. The valid range for the <i>thresholdparameter</i> is 0 to 10 dB, and the ddfault value is 0 dB. togs <i>threshold</i>—Configures the NMSP notification threshold (in dB) for GFID tags. The valid range for the <i>thresholdparameter</i> is 0 to 10 dB, and the ddfault value is 0 dB. togs threshold = Configures the NMSP notification threshold (in dB) for GFID tags. The valid range for the <i>thresholdparameter</i> is 0 to 10 dB, and the ddfault value is 0 dB. togs threshold = Configures the NMSP notification threshold (in dB) for GFID tags. The valid range for the <i>thresholdparameter</i> is 0 to 10 dB, and the ddfault value is 0 dB. togs threshold = Configures the NMSP notification threshold (in dB) for GFID tags. The valid range for the <i>thresholdparameter</i> is 0 to 10 dB, and the ddfault value is 0 dB. togs threshold = Configures the nontext tags of the nontext tags of the tags of the tags of the tags of the ddfault value is 0 dB. toget the algorithm used to average RSS and signal-to-noise ratio (SNR) values by entering this command: toget the algorithm taget tags of the tag tags of the tag tags of the tag tag tag tag tag tag tag tag tag tag
Ň	 eliner threshold—Configures the NMSP notification threshold (in dB) for RFD tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-spireshold—Configures the NMSP notification threshold (in dB) for RFD tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-spireshold—Configures the NMSP notification threshold (in dB) for RFD tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-spireshold—Configures the NMSP notification threshold (in dB) for GPD tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-spireshold—Configures the NMSP notification threshold (in dB) for GPD tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-spireshold—Configures the NMSP notification threshold (in dB) for GPD tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-spireshold—Configures the NMSP notification threshold (in dB) for GPD tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-spireshold—Configures the NMSP notification threshold (in dB) for GPD tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. rogue-spireshold—Configures the NMSP notification threshold (in dB) for GPD tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. regue-spireshold=Configures the NMSP notification threshold (in dB) for GPD tags. The valid range for the thresholdparameter is 0 to 10 dB, and the default value is 0 dB. simple-Specifies a more accurate algorithm that requires more CPU overhead. regue-specifies a faster algorithm that requires more CPU overhead to provide tess accuracy. regue-specifies a more accurate algorithm tom requ
,	- elemet threatood—Configures the NASP notification threatood (in dB) for dients and rogue clients. The valid range for the Annual transformation of the default value is 0 dB. - toge space firsthold—Configures the NASP notification threatood (in dB) for RPID tags. The valid range for the threaton/qarameter is 0 to 10 dB, and the default value is 0 dB. - toge space firsthold—Configures the NASP notification threatood (in dB) for RPID tags. The valid range for the threaton/qarameter is 0 to 10 dB, and the default value is 0 dB. - toge space firsthold—Configures the NASP notification threatood (in dB) for rope access points. The valid range for the threaton/qarameter is 0 to 10 dB, and the default value is 0 dB. - toge space firsthold—Configures the NASP notification threatood (in dB) for rope access points. The valid range for the threaton/qarameter is 0 to 10 dB, and the default value is 0 dB. - toge space firsthold = Configures the NASP notification threatoid (in dB) for rope access points. The valid range for the threaton/qarameter is 0 to 10 dB, and the default value is 0 dB. - toge space firsthold = Configures the NASP notification threatod (in dB) for rope access points. The valid range for the threaton/qarameter is 0 to 10 dB, and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - Toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the default value is 0 dB. - toge space first and the d
, n	 eliner threshold—Configures the NMSP notification threshold (n. dB) for RFID tags. The valid range for the <i>hirseholdparameter</i> is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (n. dB) for RFID tags. The valid range for the <i>hirseholdparameter</i> is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (n. dB) for regula access points. The valid range for the <i>hirseholdparameter</i> is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (n. dB) for regula access points. The valid range for the <i>hirseholdparameter</i> is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (n. dB) for regula access points. The valid range for the <i>hirseholdparameter</i> is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (n. dB) for regula access points. The valid range for the <i>hirseholdparameter</i> is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (n. dB) for regula access points. The valid range for the <i>hirseholdparameter</i> is 0 to 10 dB, and the default value is 0 dB. tags threshold—Configures the NMSP notification threshold (n. dB) for regula access points. The valid range for the <i>hirseholdparameter</i> is 0 to 10 dB, and the default value is 0 dB. tantipe Specifies a faster algorithm that requires low CPU overhead but provides less accuracy. nisple=Specifies a more accurate algorithm that requires none CPU overhead.
`	 elient <i>thrached</i>—Configures the NMSP collication threshold (m db) for diars and rugge diars. The wald range for the <i>thrachold</i>-matter is 0 to 10 db, and the default value is 0 db. tage <i>thrachold</i>—Configures the NMSP collication threshold (m db) for Togue access points. The valid range for the <i>thrachold</i>-matter is 0 to 10 db, and the default value is 0 db. regue-age threshold—Configures the NMSP collication threshold (m db) for Togue access points. The valid range for the <i>thrachold</i>-matter is 0 to 10 db, and the default value is 0 db. Note W in normand that you do not use or molfly the config location notify-threshold command. Configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command. configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command. configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command. configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command. configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command. configure the algorithm that requires more CPU overhead. values by encommend that you do not use or molfly the config location algorithm command.
`	 elient introduction disputs the NMSP officiation threated (in d)) for dense and rogar dense. The walk angue for the introduction and trade is 0 to 10 dB, and the default value is 0 dB. ingue-age interacted—Configures the NMSP notification threated (in dB) for rogue access points. The valid range for the interacted dename is 0 to 10 dB, and the default value is 0 dB. ingue-age interacted—Configures the NMSP notification threated (in dB) for rogue access points. The valid range for the interacted dename is 0 to 10 dB, and the default value is 0 dB. interaction algorithm // the config location netly-threated do romand. Configure the algorithm that to average RSSI and signal-to-noise ratio (SNR) values by entering this command: coref location algorithm // the config location netly-threated do normand. coref location algorithm bat requires low CPU overhead to provides less accuracy. restormand that you do not use or modify the config location algorithm command. Nore Ver recommend that you do not use or modify the config location algorithm command. Nore Ver recommend that you do not use or modify the config location algorithm command. Nore Ver recommend that you do not use or modify the config location algorithm command. Nore Ver recommend that you do not use or modify the config location algorithm command. Nore Ver recommend that you do not use or modify the config location algorithm command. Nore Ver recommend that you do not use or modify the config location algorithm command. Nore Ver recommend that you do not use or modify the config location algorithm command. Nore Ver recommend that you do not use or modify the config location algorithm command. Nore Ver recommend that you do not use or modify the config location algorithm command. Nore Ver recommend that you do not use or modify
``	 elient rheaded—Configures the NMSP indication threated (in di) for idents and roga cleates. The walk ange for the rheadedgamaneter is 0 to 10 dB, and the deduxt wales is 0 dB. inge indexide — Configures the NMSP indication threated (in dB) for rogue access points. The walk arrange for the <i>threatedgamaneter</i> is 0 to 10 dB, and the deduxt wales is 0 dB. Nore Vier accenting that you do not use or mostly the config location networked (in other interview) and the value is 0 dB. Nore Vier accenting that you do not use or mostly the config location networked (interview) is 0 to 10 dB, and the deduxt wales is 0 dB. Nore Vier accenting that you do not use or mostly the config location networked (interview) is 0 to 10 dB, and the deduxt wales is 0 dB. Nore Vier accenting that you do not use or mostly the config location networked (interview) is 0 to 10 dB, and the deduxt wales is 0 dB. Nore Vier accenting that you do not use or mostly the config location networked (interview) is 0 to 0 dB, and the deduxt wales is 0 dB. Nore Vier accenting that you do not use or mostly the config location networked (interview) is 0 dB. Ange Configure that you do not use or mostly the config location adjorithm commant.
· · ·	 else triveriord—conjerus the NMSP notitication threatols (in die) for light and rugs dents. The valid range for the threatoldjammeter to 0 to 10 to
Ň	 else trivetord—conjegnes the NASP notification therebold (n. dB) for closes and ropa detes. The valid range for the threboldgammeter is 0. DB, and the data Value is 0. dB. egne-gas treshold—Conjegnes the NASP notification threbold (n. dB) for closes access points. The valid range for the thresholdgammeter is 0. DB off, and the data Value is 0. dB. For the recommend that value on outs or monthy the cently bacation nethods (n. dB) for closes access points. The valid range for the thresholdgammeter is 0. DB off, and the data Value is 0. dB. For the recommend that value on outs or monthy the cently bacation nethods (n. dB) for closes access points. The valid range for the thresholdgammeter is 0. DB off, and the data Value is 0. dB. For the recommend that value on outs or monthy the cently bacation nethods (n. dB) for closes access (n. dB). engne-Specifica starts algorithm that requires two CPU ownhead but provides test access (n. dB). engne-Specifica starts algorithm that requires two CPU ownhead but provides test access (n. dB). For the recommend that you do not use or moothy the cently bacation algorithm commend.
	 else trivetod
Ň	 eller threat-od-odgese the NASP contractor threatod (in dit) contrains aut rogu ellers. The wald range for the interologianneter is 0.0 60, and the datat wale s 0.8. ege interologiContrages the NASP contractors threatod (in dit) contrage access points. The wald range for the interologianneter is 0.0 60, and the datat wale is 0.8. Net Vencommend that you do not use or modify the contrig location netly-drivehold command. Contrages the isopering in the interview of the interologian interview of the interologianneter is 0.0 10.8, and the datat wale is 0.8. Net Vencommend that you do not use or modify the contrig location netly-drivehold command. Contrages the isopering interview of the obserview of the interologian interview of the inte
· · ·	 else thread-of-cologies the NASP collication thread (in (a)) collices and rugo dires. The invalidance for the Antibodysameter is 0.0 (a), and the data value is 0.8. ega-sega transide
``	 else therdord-Configues here MAPE reductions therabed (in dit) for dients and ringue does. The valid range for the <i>intervologiane</i>ments is 0 to 10 die, and the dada' value s 0.die. enserve intervolo-Configues here MAPE reductions therabed (in dit) for rigon access points. The valid range for the <i>intervologiane</i>ments is 0 to 10 die, and the dada' value is 0.die. Intervolome the MAPE reduction therabed (in dit) for rigon access points. The valid range for the <i>intervologiane</i>ment is 0 to 10 die, and the dada' value is 0.die. Intervolome the data' value is 0 die data' value is 0.die. Intervolome the data' value is 0 die data' value is 0.die. Intervolome the data' value is 0 die data' value is 0.die. Intervolome the data' value is 0 die data' value is 0.die. Intervolome the data' value is 0 die data' value is 0.die. Intervolome the data' value is 0 die data' value is 0.die. Intervolome the data' value is 0 die data' value is 0.die. Intervolome the data' value is 0.die. Intervolome the data' value is 0 die data' value is 0.die. Intervolome the data' value is 0.die.
``	 eit wir through-Configues has Med Prudication hendel (in di) for den sur haud tange to he through denomente is 0 to 0 denomente. eit wir hendel-Configues has Med Prudication hendel (in di) for Prog as cases ports. The vaid tange to the through denomente is 0 to 0 denomente. We recommend tangou do not use or mathy the carify denation and type through denomente is 0 to 0 denomente. We recommend tangou do not use or mathy the carify denation and type through denomente is 0 to 0 denomente. We recommend tangou do not use or mathy the carify denation and type through denomente. We recommend tangou do not use or mathy the carify denation and type through denomente. We recommend tangou do not use or mathy the carify denation and type through denomente. We recommend tangou do not use or mathy the carify denation and type through denomente. We recommend tangou do not use or mathy the carify denation and type to the through denomente. We recommend tangou do not use or mathy the carify denation and type to 4 denomente. We recommend tangou do not use or mathy the carify denation algorithm comment. We recommend tangou do not use or mathy the carify denation algorithm comment. We recommend tangou do not use or mathy the carify denation algorithm comment. We recommend tangou do not use or mathy the carify denation algorithm comment. We recommend tangou do not use or mathy the carify denation algorithm comment. We recommend tangou do not use or mathy the carify denation algorithm comment. We recommend tangou do not use or mathy the carify denation algorithm comment. We recommend tangou do not use or mathy the carify denation algorithm comment. We recommend tangou do not use or mathy the carify denation algorithm comment. We recommend tangou do not use or mathy the carify denation algorithm comment. We recommend tangou do not use or mathy the

	Database Full : 0 Failed Delete: 0		
	Null Bufhandle: 0 Bad Packet: 0		
	Bad LWAPP Data: 0 Bad LWAPP Encap: 0		
	Off Channel: 0 Bad CCX Version: 0		
	Bad AP Into : U		
	ADOVE MAX KSSI: U BEIOW MAX KSSI: U		
	invalid RSSI: 0 Add RSSI Falled: 0		
	oldest Expired RSSI. U Smallest Overwrite. U		
•	Clear the location-based RFID statistics by entering this comm	ind:	
	aloor location statistics fid		
	clear location statistics hid		
•	Clear a specific RFID tag or all of the RFID tags in the entire da	tabase by entering this command:	
	eleast leastion stid (mag. addmag. ell.)		
	clear location mu { mac_address all }		
•	See whether location presence (S69) is supported on a client t	y entering this command:	
	ahaw aliant datail aliant maa		
	When location presence is supported by a client and enabled of	n a location appliance, the location appliance can provide the client with its location upon request. Location presence is enabled automatically on CCXv5 clients.	
	Information similar to the following appears:		
	Client MAC Address	00:40:96:b2:a3:44	
	Client Username	N/A	
	AP MAC Address	00:18:74:c7:c0:90	
	Client State	Associated	
	Wireless LAN Id	1	
	BSSID	00:18:74:c7:c0:9f	
	Channel	56	
	IP Address	192.168.10.28	
	Association Id	1	
	Authentication Algorithm	Open System	
	Reason Code	0	
	status code		
	Client CCV version		
	Client E2E version	No B2E support	
	Diagnostics Capability		
	S69 Capability	Supported	
	Mirroring.	Disabled	
	QoS Level.	Silver	
\$			
Note S	see the CISCO Wireless Control System Conliguration Guide or the	Cisco Location Appliance Configuration Guide for instructions on enabling location presence on a location appliance.	
-			
Mo	difving the NMSP Notification Interval for Clients, REID Ta	gs, and Roques	
	he Network Metrike Occioe Destand (NMOD) was a series		
n 11	ne Network Mobility Services Protocol (NWSP) manages commun offication interval (to a value between 1 and 180 seconds) for clie	cation between the location appliance and the controller for incoming and outgoing trainic, if your application requires more requent location updates, you can modify the NMSP the active REPID fairs, and rouge sees notist and letients.	
-			
Note T	The TCP port (16113) that the controller and location appliance co	mmunicate over must be open (not blocked) on any firewall that exists between the controller and the location appliance for NMSP to function.	
_			
10	o modify the NMSP notification interval value on the controller usir	g the controller CLI, tollow these steps:	
	Step 1 Set the NMSP notification interval value for clients. RFID	tags, and roque clients and access points by entering these commands, where interval is a value between 1 and 180 seconds:	
		מער איז	
•	config nmsp notification interval rssi clients interval		
	config amon actification interval real rfid interval		
	COULD HURSD HOULD AUOT HUR VALUSSI FIID 1/10/07/24		
•	config nmsp notification interval resi roques interval		
:	config nmsp notification interval rssi rogues interval		
•	config musp notification interval sist no interval config nmsp notification interval rssi rogues interval Step 2 See the NMSP notification intervals by entering this com	nand:	
•	config mmsp notification interval rss ind interval config mmsp notification interval rss rogues interval Step 2 See to MMSP notification intervals by entering this com	nand:	
• • sł	config mmsp notification interval rss into interval config mmsp notification interval rss rogues interval Step 2 See the NMSP notification intervals by entering this com how nmsp notification interval	nand:	
• • st	config mmsp notification interval rise in di merval config mmsp notification interval rise rogues interval Step 2 See the NMSP notification intervals by entering this com how mmsp notification interval formation similar to the following appears:	nand:	
• • st In N	comp integritation interval is in it interval config maps notification interval is interval Step 2 See the NMSP notification intervals by entering this com how maps notification interval iformation similar to the following appears: MSP Motification Interval Summary	nand:	
• st In N	coming image notification interval rise in divine val config image notification interval rise incugies interval Step 2. See the NMSP notification intervals by entering this com how nmsp notification interval diomation similar to the following appears: MSP Notification Interval Summary	nand:	
• st In NT R:	Comp integration interval is in individual config integration interval rise i rogues interval Step 2 See the NMSP notification intervals by entering this com how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval:	nand:	
• st In NI R: C	comp map notification interval is in the merea config map notification interval Step 2 See the NMSP notification intervals by entering this com how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval:	2 sec	
• st In NI R: C RI	Comp imps noticitation interval is in ind interval config imps notification interval is in ouges interval Step 2 See the NMSP notification intervals by entering this com how nmsp notification interval stormation similar to the following appears: MSP Notification Interval SUI Interval: lient	nand: 2 sec 0 sec	
• sł In Ni R: C R: R: R: R: R: R: R: R: R: R: R: R: R:	Comp image notification interval is in in the water config maps notification interval is in organ since and step 2 See the NMSP notification intervals by entering this com how maps notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient. FTD. Sgue AP.	nand: 2 sec 0 sec 2 sec	
• sł In Ni R: C R: R: R: R: R: R: R: R: R: R: R: R: R:	Comp may notification interval ris in our interval config maps notification interval ris in ougues interval Step 2 See the NMSP notification intervals by entering this com how nmsp notification interval diomation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient. FID. AP.	nand: 2 sec 0 sec 2 sec 2 sec	
• In NI R R R R	Comp integritoritation interval is in the interval config map notification interval is interval is interval Step 2 See the NMSP notification intervals by entering this com how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient. PTD. ogue AP. ogue Client.	rand: 2 sec 0 sec 2 sec 2 sec 2 sec	
• st In NI R R R	Comp mms notification interval ris in optics interval config mms polification interval site rouges interval Step 2 See the NMSP notification intervals by entering this com how nmsp notification interval MSP Notification interval SSI Interval: SSI Interval: Dient. FID. ogue AP. Client.	nand: 2 sec 0 sec 2 sec 2 sec	
• st In NI R C R R R R	Comp image notification interval is in the interval config maps notification interval is so rules interval Step 2 See the NMSP notification intervals by entering this com how mmsp notification interval information similar to the following appears: NeSP Notification Interval SSI Interval: SSI Interval: SSI Interval: Dient. Spie Client.	nand: 2 sec 0 sec 2 sec 2 sec 2 sec	
• st In NI R C R R R R	Comp map notication mereal rise in que sinterval config map notification interval is in que sinterval Step 2 See the NMSP notification intervals by entering this com how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient. FID. ogue AP. ogue Client.	nand: 2 sec 0 sec 2 sec 2 sec	
• In NI R R R R Vie	Comp image notification interval rise in di merea config image notification interval sei rogues interval Step 2 See the NMSP notification intervals by entering this com how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient. FID. ogue AP. ogue Client. wing NMSP Settings	nand: 2 sec 0 sec 2 sec 2 sec 2 sec	
• In NI C C R R R R Vie	Comp may notification interval is in the mean config maps notification interval is interval Step 2 See the NMSP notification intervals by entering this com how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: SII Interval: Dient	nand: 2 sec 0 sec 2 sec 2 sec	
• In NI C C C R R R R R V I e T T	Comp imp noticiation interval is in numeral config imms profilication interval is in course interval Step 2 See the NMSP notification intervals by entering this com how nmsp notification interval formation similar to the following appears: MSP Notification Interval SSI Interval: SSI Interval: Dient. FID. ogue AP. ogue AP. Client.	nand: 2 sec 0 sec 2 sec 2 sec	
• sh NN R C C R R R R R T T •	Comp may notification interval is in the interval config maps notification interval is interval is interval Step 2 See the NMSP notification intervals by entering this com- how map notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient	nand: 2 sec 0 sec 2 sec 2 sec	
• sh n R C C R R R R R T T T T T	Comp may notication mereal risk and mereal config may notification interval Step 2 See the NMSP notification intervals by entering this com how mms notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient. FID. ogue AP. ogue Client.	nand: 2 sec 0 sec 2 sec 2 sec	
• In NI R: C R: R: R: R: R: T T T T T	Comp may notification interval is in the interval config map notification interval is increase interval Step 2 See the NMSP notification intervals by entering this com how map notification interval interval is interval Summary SSI Interval i lient	nand: 2 sec 0 sec 2 sec 2 sec	
• In NT R C C C C C C R R R R R R R R R R R R	Comparing integration merea is and interval config map notification interval is in rouges interval Step 2 See the NMSP notification intervals by entering this com- how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: Interval: SI Interval: int. PID. ogue Client. wing NMSP Settings o view NMSP Information, use these CLI commands: See the status of active NMSP connections by entering this co- show nmsp status Information similar to the following appears: MSF II. holden of The Shot Been The Tobe Been The Des Been	nand: 2 sec 0 sec 2 sec 2 sec 2 sec	
รร ไก เป็น เป็น เป็น เป็น เป็น เป็น เป็น เป็น	Comp may notification interval residence interval config maps notification interval is increase interval Step 2 See the NMSP notification intervals by entering this com- how mrsp notification interval formation similar to the following appears: SSF Interval: Itent. See Providence Status PID. ogue Client. wing NMSP Settings o view NMSP information, use these CLI commands: See the status of active NMSP connections by entering this co show mnsp status Information similar to the following appears: MSE IP Addreses TX Echo Resp RX Echo Reg TX Da	nand: 2 sec 0 sec 2 sec 2 sec 2 sec 2 sec	
ւ հ հ ու ու ու ու ու ու ու ու ու ու	Comp map notification interval is in the interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how map notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: 11ent	nand:	
sisting in N R R R R R R R R T T T T	Comp integritorication interval rise inclusion interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: Interval: SSI Interval: Dient	nand: 2 sec 0 sec 2 sec 2 sec 2 sec 2 sec	
stand In In NI R R R R R R R R R R R R R R R R R R	Complements productation interval is of individual and interval config mansprodification interval is individual interval formation similar to the following appears: MSP Notification Interval Sign 2. See the NMSP notification Interval Summary SSI Interval: SSI Interval: SSI Interval: SSI Interval: See the status of active NMSP connections by entering this co show nmsp status Information similar to the following appears: MSE IP Address Tx Echo Rep Rx Echo Reg Tx Da 17.1.7.1.132.107 39046 39046 103742 1 See the NMSP capabilities by entering this command:	rand: 2 sec 0 sec 2 sec 2 sec 2 sec 2 sec 2 sec	
sist ເ ແ ເ ແ ເ ແ ແ ແ ແ ແ ແ ແ ແ เ น เ น เ เ เ เ เ เ เ เ	Comp may notification interval rise in our merea config map notification interval Step 2 See the NMSP notification intervals by entering this com how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: Interval: SI Interval: int	nand: 2 sec 2 sec 2 sec 2 sec 2 sec 2 sec	
ւ ու ու ու ու ու ու ու ու ու ու ու ու ու	Complements productation interval is in the interval config mans productation interval is in reques interval Step 2 See the NMSP notification intervals by entering this com- how map notification interval formation similar to the following appears: MSP Motification Interval SIT Interval: Iterval: Iterval: Gene AP	nand: 2 sec 0 sec 2 sec 1 sec	
sist In N R R R R R R T T T	Comp may nonication merva its in the merva config map nonication interval Step 2 See the NMSP notification intervals by entering this com- how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: SI Interval: SI Interval: See the status of active NMSP connections by entering this co show mmsp status Information similar to the following appears: NSE IP Address Tx Echo Reag Tx Da 171.71.132.107 39046 39046 103742 1 See the NMSP capabilities by entering this command: show mmsp capability Information similar to the following appears:	nand: 2 sec 0 sec 2 sec 2 sec	
รร ไม่ 11 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Complements notification interval issin interval config maps notification interval issi reques interval Step 2 See the NMSP notification intervals by entering this com- how mrsp notification interval iformation similar to the following appears: SSF Interval: Itent	nand: 2 sec 0 sec 2 sec 2 sec wmand: a fx Data 	
stand In N R R R R R R R Vice Vice	Comp integritoriation interval is in the interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how map notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient	nand: 2 sec 0 sec 2 sec 2 sec 2 sec	
st In In R C C C C R R R R R R R R R R R R R R	Comp map notification interval rise in durine val config map notification interval Step 2 See the NMSP notification intervals by entering this com how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: Interval: Sogue AP	nand: 2 sec 0 sec & 2 sec 2 sec 2 sec	
si in NI R R R R R Vie Vie Vie	Comg unsp. notification interval is in the interval config maps notification interval is interval interval Step 2 See the NMSP notification intervals by entering this com- how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: litent	rand: 2 sec 0 sec 2 sec 2 sec 2 sec wmand: a Ex Data	
או או עופי עופי עופי	Comp map notification interval risk models interval storage and polification interval is in rogues interval storage and polification interval is in rogues interval interval interval interval is interval is interval storage and interval is interval is interval is interval storage and interval is interval is interval is interval storage and interval is interval is interval is interval interval is interval is interval is interval is interval interval is interval is	nand: 2 sec 2 sec 2 sec 2 mand: a & k bata 	
sta In N R R R R R R R T R T R T R	Complement productation interval is of individual interval is complement productation interval is interval interval is complement production interval is complement production interval is managed in the following appears: SSP Motification Interval Summary SSI Interval: Iterval: Iter	nand: 2 sec 2 sec 2 sec mand: a & Data 	
ສ 1 10 10 10 10 10 10 10 10 10 10 10 10 1	Comg map notification interval is in the interval config map notification interval is interval is interval Step 2 See the NMSP notification intervals by entering this com- how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: Interval: SSI Interval: Interval: SSE Interval: See the status of active NMSP connections by entering this co show mmsp status Information similar to the following appears: NSE IP Advises Tx Echo Reap Tx Da 171.71.132.107 39046 39046 103742 1 See the NMSP capabilities by entering this command: show map capability Information similar to the following appears: Service Subservice TIT.71.72.107 39046 39046 103742 1 See the NMSP capabilities by entering this command: show map capability Information similar to the following appears: Service Subservice TIT.71.72.107 39046 39046 103742 1 See the Station, Tags, Rogue, Infor Mobile Station, Tags, Rogue, Statistics Mobile Station, Tags, IDS See vices WISP S See the NMSP counters by entering this command:	nand: 2 sec 0 sec 2 sec 2 sec 2 sec 2 sec	
si in N R R R R R R R R R R R R R R R R R R	Compliants indication interval issi indications interval Step 2 See the NMSP notification intervals by entering this com- how mrsp notification interval iformation similar to the following appears: MSP Notification Interval Step Notification Interval Notification Inte	nand: 2 sec 2 sec 2 sec 2 sec	
si in In N R C C C R R R R R R R R R R R R R R R	Comp map notification interval is in the interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient	nand: 2 sec 0 sec 2 sec 2 sec 2 sec 2 sec 2 sec	
si in In N R R R R R R R R R R R R R R R R R R	Complement productation merea is an off merea config many productation merea is an organ since and Step 2 See the NMSP notification interval is orm how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: Interval: SI Interval: Interval: See the status of active NMSP connections by entering this co show nmsp status Information similar to the following appears: NSE IP Address Tx Echo Neg Tx Da NSE IP Address Tx Echo Neg Tx Da NSE IP Address Tx Echo Neg Tx Da Int	nand: 2 sec 2 sec 2 sec 2 sec 2 sec	
או או דע דע יייייייייייייייייייייייייייייייי	Complements notification interval rise in the interval config many notification interval Step 2 See the NMSP notification intervals by entering this com- how mmsp notification interval formation similar to the following appears: MNSP Notification Interval Summary SSI Interval: lient	rand: 2 sec 2 sec 2 sec 2 sec 2 sec 2 sec * mand: a Rx Data *	
ສ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ	Comg map notification interval rise multiple interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: Interval: SSI Interval: SSE Interval:	nard: 2 sec 2 sec 2 sec mmant: a fix bata 	
si in N R R R R R R R R R R R R R R R R R R	Complement productation interval issin the interval step 2 See the NMSP notification intervals by entering this com- how mmsp notification interval iformation similar to the following appears: MSP Motification Interval Step 2 Set interval : Interval : See the status of active NMSP connections by entering this co show mmsp status Information similar to the following appears: MSE IP Address TX Echo Resp RX Echo Reg TX ba Interval : See the NMSP capabilities by entering this command: show mmsp capability Information similar to the following appears: SET ID Address TX Echo Resp RX Echo Reg TX ba Interval : See the NMSP capabilities by entering this command: show mmsp capability Information similar to the following appears: Set ID Estation, Rogue, Info Mobile Station, Rogue, Statistics Mobile Station, Tags, Rogue, Info Mobile Station, Rogue, Statistics Mobile Station, Tags, IDS Services WIPS See the NMSP counters by entering this command: show mmsp statistics (summary connection) where - summaryshows the common NMSP counters. - connection-hows the common NMSP counters.	rand: 2 ecc	
sisting and the second	Comg map notification interval rise interval is interval config map notification interval is interval interval Step 2 See the NMSP notification intervals by entering this com- how map notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient	nand: 2 sec 3 statictor summary commant:	
si in N R R R R R R R R R R R R R R R R R R	Complement productation interval is and interval config man productation interval is is reque a interval Step 2 See the NMSP notification intervals by entering this com- how mrsp notification interval formation similar to the following appears: SEP Notification Interval SIT Interval: Iterval: Iterval: Iterval: Iterval: Iterval: Iterval: See the status of active NMSP connections by entering this co show mrsp status Information imilar to the following appears: NSE IP Address TX Echo Resp RX Echo Reg TX Da 	rand: 2 ec 2 ec	
sister and the second s	Comg unsp routication interval is in the interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient	rand:	
si in N R R R R R R R R R R R R R R R R R R	Complement production merval risk models in the merval config many production merval risk models interval Step 2 See the NMSP notification intervals by entering this com- how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: Interval: Set Interval: See the status of active NMSP connections by entering this co- show mmsp status Information similar to the following appears: MSE IP Address Tx Echo Reap Tx Echo Req Tx Da T17.71.132.107 39046 39046 103742 1 See the NMSP capabilities by entering this command: show map status Information similar to the following appears: RSE IP Address Tx Echo Reap Tx Echo Req Tx Da T17.71.132.107 39046 39046 103742 1 See the NMSP capabilities by entering this command: show map status Information similar to the following appears: RSET Mobile Station, Tags, Rogue, Statistics Mobile Station, Tags, IDS See the NMSP counters by entering this command: show map statistics (summary connection) where - summaryshows the common NMSP counters. - connectorshows the common NMSP counters.	rand:	
si in NI C C C R R R R R R R R R R Vie C	Comg unsp nonitation interval is in the interval config map nonitation interval Step 2 See the NMSP notification intervals by entering this com- how nmep notification interval formation similar to the following appears: NSP Notification Interval Summary SSI Interval: lient	rard:	
si in In IN R R R R R R R R R R R R R R R R R R	Complement production merval ison in <i>Internal</i> config man production interval Step 2 See the NMSP notification intervals by entering this com- how mmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: Interval: SSI Interval: Interval: SSI Interval: See the status of active NMSP connections by entering this co- show mmsp status Information similar to the following appears: NSE IP Advises Tx Echo Reap Tx Echo Req Tx Da 	<pre>rand: 2 enc 0 enc 2 encc 2 enc 2 en</pre>	
si in NI R C C C R R R R R R R R R Vie C Vie S S S S S S S S S S S S S S S S S S S	Comgi map notification interval rise interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how nmep notification interval formation similar to the following appears: MVING NMSP Settings to view NMSP Information, use these CLI commands: See the status of active NMSP connections by entering this co show mmp status Information similar to the following appears: MSE IP Address TX Echo Remp RX Echo Reg TX Da 	rend:	
ສ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ ເ	Comgi map indication interval is in the interval config map notification interval is in orgue is interval Step 2 See the NMSP notification intervals by entering this com- how nmsp notification interval Step 1 Notification Interval Summary SSI Interval: SSI Interval: SS	nend:	
si in N R R R R R R R R R R R R R R R R R R	Comgi map notification interval rise interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how mmp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient	rend:	
sister and the second s	Complements productation interval is and interval config mans productation interval Step 2 See the NMSP notification intervals by entering this com- how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: SSI Interval: SSI Interval: SSI Interval: SSI Interval: SSI Interval: SSI Interval: SSE the Advise NMSP connections by entering this co- show nmsp status Information similar to the following appears: MSE TP Advises Tx Echo Reap Tx Echo Req Tx Da T17.71.132.107 39046 39046 103742 1 See the MMSP capabilities by entering this command: show nmsp status Information similar to the following appears: SETVICE Subservice TIT.71.132.107 39046 39046 103742 1 SSE TM Advises Tx Echo Reap Tx Echo Req Tx Da T17.71.132.107 39046 39046 103742 1 SSE TV Advises Tx Echo Reque, Tx Echo Service Subservice TIT.75.151.55.55.75.75.75.75.75.75.75.75.75.75.75.	rend:	
si in N R R R R R R R R R R R R R R R R R R	Comgi map notification interval issi nuclea interval Step 2 See the NMSP notification intervals by entering this com how mmsp notification interval Mission is a set of the following appears: MSP Notification Interval Step 2 Site interval: Interval: Interval: Interval: Interval: Interval: Interval: Interval: See the status of active NMSP connections by entering this co show mmsp status Information imilar to the following appears: MSE IP Address Tx Echo Resp Rx Echo Reg Tx Da Interval: See the status of active NMSP connections by entering this co show mmsp status Information imilar to the following appears: MSE IP Address Tx Echo Resp Rx Echo Reg Tx Da Interval: See the NMSP capabilities by entering this command: show mmsp capability Information similar to the following appears: See the NMSP counters by entering this command: show mmsp statistics (summary I connection) where 	<pre>nand: 2 ecc 2 ecc 2 ecc 2 ecc 2 ecc 4 ecc 4 ecc 5 ecc 5</pre>	
sisting and the second	Comp map notication interval is in the interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how mmsp notification interval MSP Notification Interval SSI Interval: NSS Inte	rand: 2 acc	
si in In N R R R R R R R R R R R R R R R R R R	Comparison profileation interval rise inclusion interval Step 2 See the NMSP notification intervals by entering this com- how mrsp notification interval formation similar to the following appears: MSP Motification Interval Step Motification Interval Motification Interval Norman Status Information similar to the following appears: MSE IP Address TX Echo Resp EX Echo Reg TX Da 	a ac: 2 ac: 2 ac: 2 ac: 2 ac:	
sisting and the second	Comp map notication interval is in the interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how nmep notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient	rand: 2 ac: 2 ac: 2 ac: 2 ac: 3 ac: 2 ac: 1 ac: 1 bc: bata 1 ac:	
si in In IN R R R R R R R R R R R R R R R R R R	Comgi map indication interval is in our interval config map notification interval is in orgues interval Step 2 See the NMSP notification intervals by entering this com- how nmsp notification interval Step 1 Notification Interval Summary SSI Interval: SSI Interva: SSI I	a ec: 2 ec: 2 ec: a ec: mmd: a Ex Data a intercent a intercent <td></td>	
sisting and the second	Computer sector of the sector	a mod 2 mod 0 mod 2 mod	
si in In IN IN IN IN IN IN IN IN IN IN IN IN IN	Comg map notication interval is in the interval config map notification interval Step 2 See the NMSP notification intervals by entering this com- how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient	and:	
sisting and the second	Comgi map notication interval issi note sinterval step 2 See the NMSP notification intervals by entering this com how mmp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient	and:	
sisting and the second	Comp map notication interval ris of use interval step 2 See the NMSP notification intervals by entering this com- how nmsp notification interval formation similar to the following appears: MSP Notification Interval Summary SSI Interval: lient	a not 2 000 2 000 2 000 2 000 2 000 2 000 2 000 2 000 2 000 wmmdt a 100 bata	
si in In N R R R R R R R R R R R R R R R R R R	Comgi map notification interval issi nuclea interval Step 2 See the NMSP notification intervals by entering this com how mmsp notification interval Step 2 See the NMSP notification intervals by entering this com how mmsp notification interval Step Notification Interval Notification Interv	and:	

 Max records read before exiting SSL read......0

 Normal Prio Tx Q full.....0

 Highest Prio Tx Q count....0

 Normal Prio Tx Q count..... Normal Prio Tx Q count. Messages sent by APPs to Highest Prio TxQ.... Max Measure Notify Meg. Max Info Notify Meg. Max Highest Prio Tx Q Size. Max Normal Prio Tx Q Size. Max Ro Size.... Max Info Notify Q Size. Max Client Info Notify Delay. Max Rogue AP Info Notify Delay. Max Rogue Client Info Notify Delay. Max Client Measure Notify Delay..... Max Client Measure Notify Delay.... Max Tag Measure Notify Delay... Max Rogue AP Measure Notify Delay... Max Rogue Client Measure Notify Delay... Max Client Stats Notify Delay... Max Client Stats Notify Delay... RFID Measurement Periodic... RFID Measurement Immediate..... SSL Handshake failed..... NMSP Rx detected con failure..... NMSP Tx detected con failure..... NMSP Connection Counters MSE IP: 171.71.132.107 nection status: U Tx message count Rx message count WLC Capability: 1 MSE Capability: 0 Service Subscr Rsp: 1 Service Subscr Req: 1 Measure Rsp: 0 Measure Req: 0 Measure Notify: 0 Info Rsp: 0 Info Reg: 0 Into Rsp: 0 Into Req. 0 Info Notify: 0 Stats Rsp: 0 Stats Req: 0 Stats Notify: 0 Loc Req: 0 Loc Rsp: 0 Loc Subscr Req: 0 Loc Subscr Rsp: 0 Loc Notify: 0 Loc Notify: 0 Loc Unsubscr Req: 0 Loc Unsubscr Rsp: 0 AP Monitor Rsp: 0 AP Monitor Req: 0 AP MONITOF RSD. 0 AP MONITOF A AP Monitor Notify: 64677 IDS Get Rsp: 0 IDS Get Req: 0 IDS Notif: 0 IDS Set Rsp: 0 IDS Set Req: 0 · See the mobility services that are active on the controller by entering this command: show nmsp subscription {summary | detail | detail ip_addr} where - summaryshows all of the mobility services to which the controller is subscribed. detail shows details for all of the mobility services to which the controller is subscribed. detail ip_addshows details only for the mobility services subscribed to by a specific IP address Information similar to the following appears for the show nmsp subscription summary command: Mobility Services Subscribed: Server IP Services 1.4.93.31 RSSI, Info, Statistics Information similar to the following appears for the show nmsp subscription detail *ip_addr* command: Mobility Services Subscribed by 1.4.93.31 Services Sub-services RSSI Mobile Station, Tags, Info Mobile Station Statistics Mobile Station, Tags, Clear all NMSP statistics by entering this command: clear nmsp statistics Debugging NMSP Issues Use these CLI commands if you experience any problems with NMSP: Configure NMSP debug options by entering this command: debug nmsp ? where ? is one of the following: - all { enable | disable - Enables or disables debugging for all NMSP messages. connection { enable | disable - Enables or disables debugging for NMSP connection events. detail { enable | disable}-Enables or disables debugging for NMSP detailed events. - error { enable | disable}-Enables or disables debugging for NMSP error messages. event { enable | disable}-Enables or disables debugging for NMSP events. message { tx | rx } { enable | disable}—Enables or disables debugging for NMSP transmit or receive messages packet { enable | disable}—Enables or disables debugging for NMSP packet events. Enable or disable debugging for NMSP interface events by entering this command: debug dot11 nmsp { enable | disable } · Enable or disable debugging for IAPP NMSP events by entering this command: debug iapp nmsp { enable | disable } Enable or disable debugging for RFID NMSP messages by entering this command: debug rfid nmsp { enable | disable } Enable or disable debugging for access point monitor NMSP events by entering this command debug service ap-monitor nmsp { enable | disable } · Enable or disable debugging for wIPS NMSP events by entering this command: debug wips nmsp { enable | disable } Configuring the Supervisor 720 to Support the WiSM When you install a WISM in a Cisco Catalyst 6500 series switch or a Cisco 7600 series router, you must configure the Supervisor 720 to support the WISM. When the supervisor detects the WISM, the supervisor creates ten Gigabit Ethernet interfaces, rangin grow Gigabit Cispabit Ethernet interfaces. The supervisor creates interfaces Gig40 in through Gig40. The first digit Gigabit Ethernet interfaces must be organized into two EtherChannel bundles of four interfaces, rangin grow Gig40. The remaining two Gigabit Ethernet interfaces areas interfaces, rangin et and chortoroler on the WISM. You must manually create VLNB to communicate with the ports on the WISM. Note The WISM is supported on Cisco 7600 series routers running only Cisco IOS Release 12.2(18)SXF5.

0

General WiSM Guidelines

Follow these guidelines when you add a WiSM to your network

· The switch or router ports leading to the controller service port are automatically configured and cannot be manually configured. The switch or router ports leading to the controller data ports should be configured as edge ports to avoid sending unnecessary BPDUs.

• The switch or router ports leading to the controller data ports should not be configured with any additional settings (such as port channel or SPAN destination) other than settings necessary for carrying data traffic to and from the controllers

onfiguring		
	g the Supervisor	
You must I	log into the switch or router	CU and begin in privileged EXEC mode.
To configur	re the supervisor to support	the WISM follow these stans:
ro comga	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface vlan	Creates a VLAN to communicate with the data ports on the WiSM and enters interface configuration mode.
Step 3	ip address ip-address	Assigns an IP address and gateway to the VLAN.
Step 4	ip helper-address	Assigns a helper address to the VLAN.
Stop E	ip-address	Determine which and a second
Step 5	end	
Step 6	wism module module_number controller {1 2} allowed-vlan vlan_number	Creates Gigabit port-channel interfaces automatically for the specified WISM controllier and configure the port-channel interfaces as trunk ports. Also, specifies the VLAN that you created earlier as the allowed VLAN on the port-channel trunk. VLAN that licit is carried on the trunk between the WISM controller and the supervisor. Note Services might be temporarily interrupted (for approximately two pings) after you enter this command.
Step 7	wism module module_number controller {1 2} native-vlan vlan_number	For the native VLAN on the ports, specifies the VLAN that you created earlier to communicate with the WISM data ports.
Step 8	interface vlan	Creates a VLAN to communicate with the service ports on the WISM.
Step 9	ip address ip_address gateway	Assigns an IP address and gateway to the VLAN.
Step 10	end	Returns to global configuration mode.
Step 11	wism service-vlan vlan	Configures the VLAN that you created in Steps 8 through Step 10 to communicate with the WiSM service ports.
Step 12	end	Returns to global configuration mode.
Step 13	show wism status	Verifies that the WiSM is operational.
sing the	Wireless LAN Control se guidelines when using a	on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: lessAchnology/wism/technical/telerence/appnote.html#wp38498 ler Network Module wireless LAK controller network module (CNM) installed in a Cisco Integrated Services Router:
• The C	Wireless LAN Control se guidelines when using a 2NM does not support IPsec	on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: less/lechnology/wism/lechnical/reference/approte.html#wp30498 ler Network Module wireless LAN controller network module (CNM) installed in a Cisco Integrated Services Router: . To use IPsec with the CNM, configure IPsec on the router in which the CNM is installed. Click this link to browse to IPsec configuration instructions for routers:
sing the Follow thes The C	Annos used for communication cisco.com/en/US/docs/wire Wireless LAN Control se guidelines when using a CNM does not support IPsec www.cisco.com/en/US/tech	on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: less/lectrology/wirmhechnical/reference/approte.html#wp34498 ler Network Module wireless LAN controller network module (CNM) installed in a Cisco Integrated Services Router: . To use IPsec with the CNM, configure IPsec on the router in which the CNM is installed. Click this link to browse to IPsec configuration instructions for routers: https://www.issalled-click this link to browse to IPsec configuration instructions for routers: <a href="https://www.issalled-click.this/link.top/links/salled-click.this/links/salled-click.this/link.top/links/salled-click.this/link.top/links/salled-click.this/links/salled-click.this/links/salled-click.this/links/salled-click.this/links/salled-click.this/links/salled-click.this/links/salled-click.this/links/salled-click.</th></tr><tr><th>sing the Follow thes The C http://www.</th><th>Tanda Used for Communication
Cases on conventUS/docs/wire
Wireless LAN Control
se guidelines when using a
2NM does not support IPsec
www.cisco.com/en/US/tech
2NM does not have a batter
cess the CANM bootloader, b</th><th>on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL:
less/bchology/wism/bchnical/reference/acprote/htmf#wx34458
ler Network Module
wireless LAV controller network module (CNM) installed in a Cisco Integrated Services Router:
.: To use lPsec with the CNM, configure IPsec on the router in which the CNM is installed. Click this link to browse to IPsec configuration instructions for routers:
kc833K3727bch, configuration, quides_list.html
and cannot save a time setting. It must receive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform
are recommend that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router might reset the CNM while you are using the bootloader.</th></tr><tr><td>sing the Follow thes The C http://www. The C thtp://w The C To acc When</td><td>Tarics used for Communication
cases commentUS/clockwire
Wireless LAN Control
se guidelines when using a
XNM does not support IPsec
www.clsco.com/en/US/tech
XNM does not have a batter
cess the CNM bootloader, v
you reset the CNM from a 1</td><td>on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL:
less/bchology/wism/bchnical/reference/approte/htm/#wp39458
ler Network Module
wireless LAX controller network module (CNM) installed in a Cisco Integrated Services Router:
I. To use IP-sec with the CNM, configure IP-sec on the router in which the CNM is installed. Click this link to browse to IP-sec configuration instructions for routers:
IK633/IK372/tech. configuration_ouides_list.htm/
and cannot save a time setting. It must receive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform
the recommend that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router might reset the CNM while you are using the bootloader.
INM interface, you have 17 minutes to use the bootloader before the router automatically resets the CNM. The CNM biodloader does not run the Router IBace Configuration Protocol (RBCP), so the F</td></tr><tr><td>sing the
Follow thes
The C
http://www.</td><td>Tarins used for communications
wireless LAN Control
se guidelines when using a
2NM does not support lPsec
www.sisco.com/en/US/tech
2NM does not have a batter
cess the CNM bootloader, v
you reset the CNM from the router til
reset the CNM from the router til
reset the CNM from the router til
mean the communication of the contert of the contert from the router til
the cest the CNM from the router til
and the contert of the conte</td><td>on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL:
less/bchology/wism/bchnical/reference/appro6.html#wp39458
ler Network Module
wireless LAN controller network module (CNM) installed in a Cisco Integrated Services Router:
.: To use IP-sec with the CNM, configure IP-sec on the router in which the CNM is installed. Click this link to browse to IP-sec configuration instructions for routers:
https://www.integrated Services Router: .: To use IP-sec with the CNM, configure IP-sec on the router in which the CNM is installed. Click this link to browse to IP-sec configuration instructions for routers: https://www.integrated-Services Router: .: To use IP-sec with the CNM, configure IP-sec on the router in which the CNM is installed. Click this link to browse to IP-sec configuration instructions for routers: https://www.integrated-Services Router: .: To use IP-sec with the CNM, configuration-ouides. Its html and cannot save a time setting. It must receive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform are recommend that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router might reset the CNM while you are using the bootloader. .: Winterface, you have 17 minutes to use the bootloader before the router automatically resets the CNM. The CNM bootloader does not run the Router Black Configuration Protocol (RBCP), so the Face Anances at the SCP integrated exchance and does not reset the UNM boots up. To reset the CNM from the router, enter one of these commands on the router CLE
sing the Follow these The C http://www. The C The C To acc When heartb If you in service	Tarios used for communications wireless LAN Control se guidelines when using a CMM does not support lPsec www.scsoc.com/en/US/tech cess the CNM bootloader, v you reset the CNM from a seat running on the router if reset the CNM from the route e-module war-controller 1/	on between the Cisco WISM, the Supervisor 720, and the 4440 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: less/les/les/les/les/les/les/les/les/les
sing the Follow these The C http://www. The C The C The C To acc When hearth If you service service	Tarios use lot communications and the second	on between the Cisco WISM, the Supervisor 720, and the 4440 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: less/les/he/he/less/les/he/less/les/less/les
 The contributor (New York) sing the Follow these The C The C The C To acc When hearth If you is service service Gigabi 	Tarios deel for Commence international and the second sec	on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: less/les/les/les/les/les/les/les/les/les
 The control of the cont	Tarins used for communications wireless LAN Control se guidelines when using a communication of the communication of the communication of the communication of the communication of communication of communication of communication of the controller to location of the controller to location of the location of the controller to location of the location of the locatio	on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: less/les/he/hology/wism/les/hirely/tes/hirely/tes/hirely/set/les/hi
 sing the Follow these The C The C http://www The C The C The C The C When hearth If you and service Gigable esetting If you want sing the C 	Tarias used for communications of the control of th	on between the Cisco WISM, the Supervisor 720, and the 4444 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: less/les/het/het/methines/hireles/reserve/aproxe/hireles/services/Router: Ises/les/het/het/het/hiteles/les/het/het/het/het/het/het/het/het/het/het
sing the Control of t	Tarins used for communications and the second secon	on between the Cisco WISM, the Supervisor 720, and the 4440 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: less/les/horbid/wismtechnical/telerace/apcnote.html#wn34438 less/les/horbid/less/less/less/less/less/less/less/les
sing the Follow these interview of the Communication of the Communicati	Tarias used for communications and an end of the anticological and anticological and anticological and anticological anticolog	on between the Cisco WISM, the Supervisor 720, and the 4440 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: lessAchnology/WismRechnical/Inference/apcnote.html#wn34458 in Network Module wireless LAN controller network module (CNM) installed in a Cisco hiegrated Services Router: I. To use IPsec with the CNM, configure IPsec on the router in which the CNM is installed. Click this link to browse to IPsec configuration instructions for routers: IK653/K3721ech. configuration.guides_list.html y and cannot save a time setting. It must receive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform are recommend that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router might reset the CNM while you are using the bootloader. ZMI Interface, you have 17 minutes, to use the bootloader before the router automatically resets the CNM. The CNM bootloader does not run the Router Blade Configuration Protocol (RBCP), so the rea cut after 17 minutes, triggering a reset of the CNM. (F, the router stops the RBCP) heartbeet change and does not restart it until the CNM boots up. To reset the CNM from the router, enter one of these commands on the router CL: 10 reset (for Glgabit Ethernet CNM versions) Cront roller Network Module are supported on Clicco 28/37/38xX Series Integrated Services Routers running Clicco IDS Release 12.4(11)T2 or later. ut Settings a original configuration, you can use the controller GUI or CLI to reset the controller to factory-default settings. er to Default Settings ut setting using the controller GUI, follow these steps:
sing the Follow these Follow these The C The C	Tarios used for commentarians used for commentarians used for commentarians used for commentarians and the second sequidalines when using a 2NM does not support lPsec www.cisco.com/en/US/tech NM does not have a batter cess the CNM foon the south cess the CNM foon the router if reset the CNM from the router and an another the commentarian e-module wina-controller 1/1 e-module integrated-service at the controller to Defa to return the controller to the Controller to factory-defa Open your Internet browsee Enter the controller IP addr	on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: lesselectrology/wismtechnical/telerace/apcnote.html#wn34438 in Network Module wireless LAN controller network module (CNM) installed in a Cisco Integrated Services Router: To use IPsec with the CNM, configure IPsec on the router in which the CNM is installed. Click this link to browse to IPsec configuration instructions for routers: IK553/K3721ech. configuration.guides_list.html y and cannot save a time setting. It must receive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform are recommend that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router might reset the CNM while you are using the booticoder. Whi Interface, you have 17 minutes to use the booticader before the router automatically resets the CNM. The CNM booticoder does not run the Router Blade Configuration Protocol (RBCP), so the F res out after 17 minutes, triggering a reset of the CNM. Lett, the router stops the RBCP hearbeat exchange and does not restart it until the CNM boots up. To reset the CNM from the router, enter one of these commands on the router CLL: 10 reset (for Gigabit Ethernet CNM versions) Cont roller Network Module are supported on Cisco 28/37/38xx Series Integrated Services Routers running Cisco IOS Release 12.4(11)T2 or later. ut Settings ut setting using the controller GUI rolL to reset the controller to factory-default settings. er to Default Settings ut setting using the controller GUI, follow these steps: as in the browser address line and press Erler. An Erler Network Password dialog box appears.
sing the contribution of t	Hartis deel for Committee Resource and the State of the State and the State of the State of the State www.sisco.com/ant/State NM does not support IPsec www.sisco.com/ant/State NM does not have a batter cess the CNM from the router til reset the CNM from the router til reset the CNM from the router til the controller to Defa to return the controller to Defa to roturn the controller to the CNM for the controller to the CNM for the controller to Paddr Enter your username in the	on between the Cisco WISM, the Supervisor 720, and the 4440 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: lesselectrology/wismtechnical/teterace/apcrote/httr/#wy34438 in Network Module wireless LAN controller network module (CNM) installed in a Cisco Integrated Services Router: It o use lPsec with the CNM, configure lPsec on the router in which the CNM is installed. Click this link to browse to lPsec configuration instructions for routers: ites33143721ech : configuration: quides. List httr y and cannot save a time setting. It must receive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform are recommend that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router might reset the CNM while you are using the booticoder. 20 Minitatics, up there 17 minutes to use the bootidader before the router automatically resets the CNM. The CNM booticoder does not run the Router Blade Configuration Protocol (RBCP), so the F res out after 17 minutes, triggering a reset of the CNM. There for Fast Ethernel CNM versions) Controller Network Module are supported on Cisco 28/37/38xx Series Integrated Services Routers running Cisco IXS Release 12.4(11)T2 or later. ut Settings ut solfing action for GUI or CLI to reset the controller to factory-default settings. er to Default Settings ut setting the controller GUI, follow these steps: L setting the controller GUI, follow these steps: L setting the controller GUI, follow these steps: L set in the throwser address line and press Enter. An Enter Network Password dialog box appears. Lyer Name text box. The default username is admin.
sing the term the communication of the term the communication of the com	Hans used for Commission wireless LAN Control se guidelines when using a 2NM does not support lPsec www.sisco.com/an/USA 2NM does not have a bater cess the CNM foront a bater cess the CNM from the router til reset the CNM from the router e-module integrated-service at thement versions of the C the Controller to Defa to return the controller to it SUI to Reset the COMT/defa Open your internet browsee Enter the controller IP addr Enter your username in the Erter the wireless device p	on between the Cisco WISM, the Supervisor 720, and the 4440 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: lesselectrology/wismtechnical/telerace/apcrote/httl#wp34438 in Network Module wireless LAN controller network module (CNM) installed in a Cisco Integrated Services Router: It o use Psec with the CNM, configure Psec on the router in which the CNM is installed. Click this link to browse to Psec configuration instructions for routers: ItS3316721ech configuration quides list html y and cannot save a time setting. It must receive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform are recommend that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router right resets the CNM while you are using the bodoleader. 20 Minitarize, you brien't financies to use the bodoleader before the router automatically resets the CNM. The CNM bootloader does not run the Router Blade Configuration Protocol (RBCP), so the F reas cut after 17 minutes, triggering a reset of the CNM. There is the CRM from the router. If you reset the CNM boots up. To reset the CNM from the router, enter one of these commands on the router CL: 10 reset (for Fait Ethernel CNM versions) 10 rot roller Network Module are supported on Cisco 28/37/38xx Series Integrated Services Routers running Cisco IXS Release 12.4(11)T2 or later. 11 Settings 12 or toler Identification, you can use the controller GUI or CLI to reset the controller to factory-default settings. 13 as inglinal configuration, you can use the controller GUI or CLI to reset the controller to factory-default settings. 14 beforus using the controller GUI, follow these steps: 15 as in the browser address line and press Enter. An Enter Network Password dialog box appears. 15 uses in the browser address line and press Enter. The default password is admin.
sing the Follow there Follow there Follow there Follow there It pound If you service s	Intra de lot Commente Intra de lot Commente Seguidelines when using a intra de lot Commente seguidelines when using a invite des not support l'Psec www.sisco.com/en/US/lech NM does not have a batter des the CNM from the router ti reset the CNM from the router ti to return the controller to lefa to rotroller to factory-defa Copen your Internet browsee Enter the controller IP addr Enter the wireless device p Chocse Commands > Ret	on between the Cisco WISM, the Supervisor 720, and the 4440 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: lesselectrology/WismRechnical/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/apcrote/Inference/Infer
sing the Follow there Follow there Follow there Follow there It pound If you service s	Intra de lot d'armittans intra d'armittans	on between the Cisco WISM, the Supervisor 720, and the 4440 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: lessActionOggWismRechnical/Information Entrollews344989 for Network Module wireless LAN controller network module (CNM) installed in a Cisco Integrated Services Router: It to use Pisec with the CNM, configure Pisec on the router in which the CNM is installed. Click this link to browse to Pisec configuration instructions for routers: ItERS3NG721ech configuration guides. List htm and cannot save a time setting. It must receive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform are recommend that you reset the CNM from the router. If you reset the CNM from ACNM user interface, the router right resets the CNM while you are using the bootloader. CNM herdrose, you have 17 minutes to use the bootloader before the router automatically resets the CNM. The CNM bootloader does not run the Router Blade Configuration Protocol (RBCP), so the R we configuration to use the bootloader before the router automatically resets the CNM from the router, enter one of these commands on the router CLL: prevention to resort the CNM rom the router structure and the resort the router structure structure structure and the resort of the CNM. The roller Stops the RBCP heartbeat exchange and does not restart it until the CNM boots up. To reset the CNM from the router, enter one of these commands on the router CLL: prevention 10 reset (for Gigabit Ethernet CNM versions) Controller Network Module are supported on Clicco 28/37/38xx Series Integrated Services Routers running Clicco IOS Release 12.4(11)T2 or later. UI Settings as original configuration, you can use the controller GUI or CLI to reset the controller to factory-default settings. It to Default Settings us setting using the controller GUI, follow these steps: users in the browser address l
sing the E- Follow these Follow these Follow these Follow these The C The C C The C C C C The C C C C The C C C C The C C C C C The C C C C C C C The C C C C C C C C C C C C C C C C C C C	Introduced for Communications of the control of the	on between the Cisco WISM, the Supervisor 720, and the 4444 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: less/bechnology/Wism/bechnical/Vietenace/aponde.htm/#wx34458 for Network Module wireless LAK controller network module (CNM) installed in a Cisco Integrated Services Router: It to use Paec with the CNM, configure Paec on the router in which the CNM is installed. Click this link to browse to Psec configuration instructions for routers: les33452720ech.configuration.guides_list.htm/ and cannot save a time setting. It must receive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform the recommend that you uses the COM from the router. If you reset the CNM from a CNM user infrance, there will made does not run the Router Blade Configuration vizard prompts you for NTP server inform the recommend that you uses the COM from the router. If you reset the CNM from a CNM user infrance, there outer for the CNM write you are using the bootloader les control the CNM installed exchange and does not restart it until the CNM boots up. To reset the CNM from the router, enter one of these commands on the router CLE there is the for CMM versions) inter for reset tops the RSCP heartiset exchange and does not restart it until the CNM boots up. To reset the CNM from the router, enter one of these commands on the router CLE to reset (for Glabit Ethernet CNM versions) inter to transfer tops the RSCP heartiset exchange and does not restart it until the CAM boots up. To reset the CNM from the router, enter one of these commands on the router CLE to reset (for Glabit Ethernet CNM versions) inter to transfer tops the RSCP heartiset exchange and glabit provide and services Routers running Clicco IOS Release 12.4(11)T2 or later. ut Settings ut setting using the controller GUI, follow these steps: : : to be the browser address line and press Enter. A
sing the Communication of the	The set of Communication of Communications and Comm	on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: leaseAcchnology.WismYetchnical/Yeternace/accnote/htt/#wx34943 for Network Module wireless LAK controller network module (CNM) installed in a Cisco Integrated Services Router: It To use Pase with the CNM, configure Pase on the router in which the CNM is installed. Click this link to browse to Pase configuration instructions for routers: It Couse Pase with the CNM, configure Pase on the router in which the CNM is installed. Click this link to browse to Pase configuration wizard prompts you for NTP server inform the recommend that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router might reset the CNM while you are using the bootloader the router mouter, by our reset the CNM from the router. If you reset the CNM from a CNM user interface, the router might reset the CNM while you are using the bootloader. If the router stopper the RSCP hearbeat exchange and does not restart it until the CNM boots up. To reset the CNM from the router, enter one of these commands on the router CLE to rese to the Fast Ethemet CNM versions) core tore fast Ethemet CNM versions) core tore Fast Ethemet CNM versions a rolfinal configuration, you can use the controller GUI or CLI to reset the controller to factory-default settings. er to Default Settings uit setting using the controller GUI, follow these steps:
sing the E- Follow the: Follow the: Follow the: The C The C the thitp://www. When the C To acc When the C To acc When the C To acc When the C To acc Step 1 (Step 2 (Step 3 (Step 4 (Step 5 (Step 4 (Step 5 (S	Intro deel for Comment introduced for Comment international and the second of the seguidelines when using a 2NM does not support lPsec www.sisco.com/en/US/leb/ NM does not have a batter cess the CNM from the router ti- reset the CNM from the router ti- ter extent the controller to It 2UI to Reset the Controller to It 2UI to Reset the Controller to It 2UI to Reset the Controller to It 2UI to Controller to Tactory-defa Controller to factory-defa Enter the wireless device p Choose Commands - Res Click Reset. When prompted, confirm th Reboot the controller witho	on between the Cisco WISM, the Supervisor 720, and the 4404 controllers are documented in <i>Configuring a Cisco Wineless Services Module and Wineless Control System</i> at this URL: lease the indeprovement of the controller of CMM installed in a Cisco Integrated Services Router: .: To use Paec with the CNM, configure IPsec on the router in which the CNM is installed. Click this link to browse to IPsec configuration instructions for routers: ktr334572/bech_configuration_quides_list.html and cannot save a time setting, it must readive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform re economed that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router right reset the CNM while you are using the bootloader. CNM Interface, you have 17 minutes to use the bootloader before the router automatically resets the CNM from the router, enter one of these commands on the router CLE CNM Interface, you have 17 minutes to use the bootloader before the router automatically resets the CNM from the router, enter one of these commands on the router CLE Prese (of Fast Ethernet CNM versions) bergine 10 reset (for Gigabit Ethernet CNM versions) controller Fast Ethernet CNM versions) as right configuration, you can use the controller GUI or CLI to reset the controller to factory-default settings. er to Default Settings at settings as in the browser address line and press Enter. An Enter Network Password dialog box appears. User Name text box. The default username is admin. assword in the Password text box and press Enter. The default password is admin. set or Factory Default . are reset. at swing the configuration. due text configuration wettings. See the <u>"Using the Configuration Wizard" section</u> for instructions.
sing the Communication of the	Arris deel for Commentarians de la commentaria de la commentaria de la commentaria de la commentarians de la commentaria del commentaria de la commentaria del mesente de la commentaria del mesente de la commentaria de la commentaria del commentaria de la commentaria del commentaria de la commentaria del commentaria de la commentaria del la controller de la commentaria del la controller de la commentaria del la commenteria del	on between the Cisco WiSM. the Supervisor 720, and the 4444 controllers are documented in <i>Configuring a Cisco Wireless Services Module and Wireless Control System</i> at this URL: isableshole/gov/wism/echrical/efferreeaagonob.html/#wo34938 for Network Module wireless LAN controller network module (CMM) installed in a Cisco htegrated Services Router: To use Pleav with the CMM. Configure Pleac on the router in which the CMM is installed. Click this link to browse to Pleac configuration instructions for routers: ktS334572hech: configuration guides. Est html and cannot save at time setting. Time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server inform are ecommend that you reset the CMM from the router. If you reset the CMM from a CMM user interface, the router might resets the CMM while you are using the bootloader. CMM inffraces, you have 17 minutes to use the bootloader before the router automatically resets the CMM. The CMM bootloader does not run the Router Blade Configuration Protocol (RBCP), so the F served of the TATT minutes. Tiggering an addees not restart it until the CMM boots up. To reset the CMM from the router, enter one of these commands on the router CLI: there is of the REC Phaembed exchange and does not restart it until the CMM boots up. To reset the CMM from the router, enter one of these commands on the router CLI: the offer set (for Gigabit Ethernet CMM versions) const offer fast Ethernet CMM versions) the rote off-set fifterse us diginal configuration, you can use the controller GUI or CLI to reset the controller to factory-default settings. a rote of fast Ethernes users in the braseword text box and press Enter. An Enter Network Password dialog box appears. User Name text box. The default usersame is admin. a reset . a reset. a saving the configuration. d e order configuration settings. See the "Laing the Configuration Wizard" section for instructions.
sing the Communication of the	Arris de lot Commente wireless LAN Control se guidelines when using a NM does not support l'Pec www.scsco.com/en/US/ebc NM does not have a batter cess the CNN tootloader, w you reset the CNM from the router til east normaling on the router til east normaling on the router til reset the CNM from the router errodule wian-controller 1/ e-module integrated-servici the Controller to Defat to return the controller to Defat Controller to Controller Baddr Enter the controller P addr Enter the controller P addr Enter the controller P addr Enter the controller Newsee Chocse Commands > Re: Click Reset. When prompted, confirm th Reboot the controller witho Use the configuration wizar CLI to Reset the Controll he controller to factory defa	on between the Cisco WISM, the Superviser 720, and the 4404 controllers are documented in <i>Configuring a Cisco</i> Wireless Services <i>Module</i> and Wireless Control System at this URL: is network Module wireless LAN controler network module (CMM) installed in a Cisco Integrated Services Router: . To use Beav with the CMM, configure IPsec on the router in which the CMM is installed. Cick this lirk to browse to IPsec configuration instructions for routers: is Stalls72tech : configuration guides list htm and cannot save a time setting. It movies a time setting from an external NTP server when it powers up. When you install the module, the configuration vizard promps you for NTP server inform the recommend that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router might reset the CNM while you are using the boottoader. CNM infinites, you have 17 minutes to use the boottoader before the router automatically resets the CNM. The CNM boottoader does not nut the Router Blade Configuration Protocol (RBCP), so the FR reso and that r7 minutes. Togging a reset of the CNM. If the router stops the RBCP heartbeat exchange and does not restart it until the CNM boots up. To reset the CNM from the router, cuts reso and that r7 minutes. Togging a reset of the CNM. If the router stops the RBCP heartbeat exchange and does not restart it until the CNM boots up. To reset the CNM from the router, cuts reso and that r7 minutes. Togging a router CNM versions) For roller Network Module are supported on Cisco 28/37/80x Series Integrated Services Routers running Cisco IDS Release 12.4(11)T2 or later. ut Setting u a original configuration, you can use the controller GUI or CLI to reset the controller to factory-default settings. e to Default Setting ut setting using the controller GUI, follow these steps: u set the Tactory Default . u reset. u staining the configuration. u the rest box. The default usemanne is admin. u staining the configuration settings. See the
sing the E- Follow these Follow these Follow these Follow these Inter-Javawa When The C - To a car If you and the service serv	Hards deel for Carmingle Hards deel for Carmingle Beneficies cannel (1) Statucations are guidelines when using a 2NM does not support lPsec www.sisco.com/an/USA NM does not have a batter cases the CNM foront are cases the CNM from the router till reset the CNM from the router till reset the CNM from the router till reset the CNM from the router are controller to Defa to return the controller to it 3UI to Reset the COMTroll are Enter the controller to It Click Rest. When prompted, confirm th Reboot the controller witho Use the configuration witage CLI to Reset the Controll the controller to factory defa CLI to Reset the Controller witho Use the configuration witage CLI to Reset the Controller witho	on between the Clice WISM, the Superviser 720, and the 4404 controllers are documented in <i>Configuring a Clice</i> Wireless Services <i>Module and Wireless Control System</i> at this URL: issuehandbackbackbackbackbackbackbackbackbackback

Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks