Cisco wlc login banner

I'm not robot!





Last Login...: Thu Nov 21 22:01:48 from 123.456.789.0 Uptime....: 2days 21hours 29minutes 3seconds Load....: 0.02 (1minute) 0.02 (5minutes) 0.05 (15minutes) Memory MB....: 486 Used: 465 Free: 21 Free Cached: 326 Swap In Use: 4 Temperature...: CoreO: 89.6*F M/B: 98.6*F CPU: 89.6*F Disk: 95*F Disk Usage...: You're using 1MB in /home/mewbie SSH Logins...: There are currently 2 users logged in Processes....: 85 total running of which 3 are yours Weather....: 79*F, partly sunny

This is a private system that you are not to give out access to anyone without permission from the admin. No illegal files or activity. Stay, in your home directory, keep the system clean, and make regular backups. -== DISABLE YOUR PROGRAMS FROM KEEPING SENSITIVE LOGS OR HISTORY ==-



[amw] - [~] - [2015-02-26 01:59:29

[0] ssh root@mini
*** This is displayed DURING during login ***
Password:
The time and date of this login have been sent to the system logs.

Mware offers supported, powerful system administration tools. Please ee www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the /Sphere Security documentation for more information. [root@mini:~]

badow byces of wir compacerimin (nead) errory
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)71, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
System Configuration Dialog
Continue with configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>enable
Routersconfigure terminal
Enter configuration commands, one per line. End with CHTL/Z.
Router(config) #banner motd #

The Seven Layers of OSI

Cisco wlc 5520 login banner. Cisco banner login example. Cisco wlc login banner. Cisco wlc error installing login banner.

< Return to Cisco.com search results View this content on Cisco.com Published On: October 29th, 2020 07:41 Login banner is used to displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. Note When HTTP authentication is configured using TACACS+/RADIUS, the banner message does not display on the Web UI. Command or Action Purpose Step 1 enable Step 2 configure terminal Device# configure terminal Step 3 banner login c message c Device(config)# banner login c message c Device(config)# banner login c message c Device# configure terminal Step 3 banner login c message c Device# configure terminal Step 4 banner login c message c Device# configure terminal Step 4 banner login c message c Device# configure terminal Step 4 banner login c message c Device# configure terminal Step 4 banner login c message c Device# configure terminal Step 4 banner login c message c Device# configure terminal Step 4 banner login c message c Device# configure terminal Step 4 banner login c message c Device# configure terminal Step 4 banner login c message c Device# configure terminal Step 4 end Step 5 show running-config Device# show running-config Step 6 copy running-config startup-config sta blinks in succession. Up to 10 access points can be concurrently upgraded from the controller. Note The 5500 series controllers can download the 6.0 software to 100 access points simultaneously. Caution Do not power down the controller or any access points are image? controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access points must remain powered, and the controller must not be reset during this time. Note In controller software release 5.2 or later, the WLAN override feature has been removed from both the controller software release 5.2 or later, the WLAN configuration and broadcasts all WLANs. You can specify that only certain WLANs be transmitted by configuring access point groups. Each access point groups do not enable WLANs to be transmitted on per radio interface of AP. Follow these guidelines before upgrading your controller to software release 6.0: Make sure you have a TFTP or FTP server: - Controller software upgrade. Keep these guidelines in mind when setting up a TFTP or FTP servers that 32 MB; therefore, you must make sure that your TFTP servers that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within WCS. If you attempt to download the 6.0 controller software and your TFTP failure while storing in flash." - If you are upgrading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller. - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable. - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port. You can upgrade or downgrade the controller software release 6.0. Table 9-1 shows the upgrade path that you must follow prior to downloading software release 6.0. Table 9-1 Upgrade Path to Controller Software Release and then upgrade to 4.2.176.0 before upgrading to 6.0. 4.0.155.5 or later 4.0 release Upgrade to 4.2.176.0 before upgrading to 6.0. 4.1.171.0 or later 4.1 release Upgrade to 4.2.176.0 before upgrading to 6.0. 4.1.191.xM Upgrade to 4.1.192.35M before upgrading to 6.0. 4.2.176.0 before upgrading to 6.0. 4.2.173.0 or later 4.2 release Upgrade to 4.2.176.0 before upgrading to 6.0. 4.2.173.0 or later 4.2 release Upgrade to 4.2.176.0 before upgrading to 6.0. 4.2.176.0 before upgrade directly to 6.0. 4.2.176.0 before upgrade directly to 6.0. 4.2.176.0 before upgrade to 4.2.176.0 before upgrade directly to 6.0. 4.2.176.0 before upgrade to 4.2.176.0 before upgrade directly to 6.0. 4.2.176.0 before upgrade di release You can upgrade directly to 6.0. 5.1.151.0 or later 5.1 release You can upgrade directly to 6.0. 5.2.157.0 or later 5.2 release You can upgrade directly to 6.0. Note The 5500 series controllers can run only controller software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 6.0 software. In large networks, it may take some time to download the upgrade image to the access point. In software releases 6.0.186.0 and later, you can download the upgrade image to the access point. the network is still up. New CLI and controller GUI functionality allow you to specify the boot image for both devices and to reset the access points discover and rejoin the controller. See the "Predownloading an Image to an Access Point" section for more information about predownloading images to access points. Cisco recommends that you install the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file on all controller platforms. This file resolves CSCsm03461 and is necessary to view the version information for ER.aes files in the output of the show sysinfo CLI command. If you do not install this ER.aes file, your controller does not obtain the fix for this defect, and "N/A" appears in the Field Recovery Image Version or Emergency Image Version or Emergency Image Version field in the output of this command. Note The ER .aes files are independent from the controller software files. You can run any controller software files are independent from the controller software files. latest boot software file (5.2.157.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed. Caution If you require a downgrade from one release to another, you may lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller. Caution Before upgrading your controller to software releases 6.0 in a mesh network, you must comply with the following rules. Table 2 outlines the upgrade compatibility of controller mesh and non-mesh releases and indicates the intermediate software releases required as part of the upgrade path. You can upgrade from all mesh releases to controller software release 6.0 without any configuration file loss. See Table 2 for the available upgrade paths. Note If you downgrade to a mesh release, you must then reconfigure the controller. Cisco recommends that you save the configuration from the mesh release before upgrading to release 6.0 for the first time. Then you can reapply the configuration if you need to downgrade from a mesh release 6.0 to a mesh release controller software release 6.0. After reset, the XML configuration file is selected. Do not edit XML files. Any field with an invalid value is filtered out and set to default by the XML validation occurs during bootup. Table 2 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases 6.0 5.2 4.1.192.35M 4.1.191.24M 4.1.190.5 4.1.185.0 4.1.171.0 4.0.219.0 4.0.217.204 4.0.217.0 4.0.216.0 4.0.206.0 4.0.179.11 4.0.179.8 4.0.155.5 4.0.155.0 3.2.195.1 4.0.219.0 Y2 Y2 - 4.0.217.204 Y 2 Y2 Y2 - 4.0.217.204 Y 2 Y2 Y2 - 4.0.217.0 Y2 Y2 Y2 Y 3 - 4.0.216.0 Y2 Y2 Y2 Y 3 Y - 4.0.155.5 Y Y4 Y Y - 3.2.195.10 Y Y4 Y Y - 3.2.193.5 Y Y4 Y Y Y - 3.2.171.6 Y Y4 Y Y Y - 3.2.171.5 Y Y4 Y Y Y - 3.2.150.10 Y Y4 Y Y Y - 3.2.195.10 Y Y4 Y Y Y - 3.2.193.5 Y Y4 Y Y Y - 3.2.171.6 Y Y4 Y Y Y - 3.2.171.5 Y Y4 Y Y Y - 3.2.150.10 Y Y4 Y Y Y - 3.2.195.10 Y Y4 Y Y Y Y - 3.2.195.10 Y Y4 Y Y Y Y - 3.2.195.10 Y Y4 the controller; then install the other file and reboot the controller. Step 1 Upload your controller configuration files to a server to back them up. Note Cisco highly recommends that you back up your controller's configuration files prior to upgrading the controller software. See the "Uploading and Downloading Configuration Files" section for instructions. Step 2 Follow these steps to obtain the 6.0 controller software and the Cisco Unified Wireless Network Controller software release. The software releases are labeled as follows to help you determine which release to download: Early Deployment (ED) — These software releases provide new features and new hardware platform support as well as bug fixes. Maintenance Deployment (DF) — These software releases have been deferred. Cisco recommends that you migrate to an upgraded release. d. Choose a software release number. e. Click the filename (filename .aes). f. Click Download . g. Read Cisco's End User Software License Agreement and then click Agree . h. Save the file to your hard drive. i. Repeat steps a through h to download the remaining file (either the 6.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file). Step 3 Copy the controller software file (filename .aes) and the Cisco Unified Wireless Network Controller Software 5.2.157.0 ER.aes file). 4 Disable the controller 802.11a and 802.11b/g networks. Step 5 For Cisco WiSMs, shut down the controller port channel on the Catalyst switch to allow the controller. Step 7 Choose Commands > Download File to open the Download File to a controller to reboot before the access points start downloading the software. to Controller page (see Figure 9-1). Figure 9-1 Download File to Controller Page Step 8 From the File Type drop-down box, choose TFTP or FTP. Step 10 In the IP Address field, enter the IP address of the TFTP or FTP server. Step 11 If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the Timeout field. Step 12 In the File Path field, enter the directory path of the software. Step 13 In the File Name field, enter the username to log into the FTP server. b. In the Server Login Password field, enter the password to log into the FTP server. c. In the Server Port Number field, enter the post number on the FTP server. b. In the Server Login Password to log into the FTP server. c. In the Server Server Server. b. In the Server Server. c. In the Server Port Number field, enter the post number on the FTP server. c. In the Server Server. c. In the Server. Serve the download. Step 16 After the download is complete, click Reboot . Step 17 If prompted to save your changes, click Save and Reboot the controller. Reboot the controller. Reboot the controller. Note Do not wait to reboot the controller. downloading the software before the controller is running it. Step 19 After the controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file). Step 20 Re-enable the WLANs. Step 21 For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch. Step 22 Re-enable your 802.11a and 802.11b/g networks. Step 23 If desired, reload your latest configuration file to the controller. Step 24 To verify that the 6.0 controller on the controller. Summary. Step 25 To verify that the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file is installed on your controller, choose Monitor to open the Summary page and look at the Field Recovery Image Version field. Note If a Cisco Unified Wireless Network Controller Boot Software ER.aes file is not installed, the Field Recovery Image Version or Emergency Image Version field shows "N/A." Using the controller software file and the 5.2.157.0 ER.aes boot software file at the same time. Install one file and reboot the controller; then install the other file and reboot the controller. Step 1 Upload your controller software. See the "Uploading and Downloading Configuration Files" section for instructions. Step 2 Follow these steps to obtain the 6.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file from the Software to the Cisco WLC model of your choice. c. Choose a controller software release. d. Click the filename (filename .aes). e. Click Download . f. Read Cisco's End User Software License Agreement and then click Agree . g. Save the file to your hard drive. h. Repeat steps Go to . to Save the file to your hard drive. b. Repeat steps Go to . to Save the file to your hard drive. to save the file .aes) and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file to the default directory on your TFTP or FTP server. Step 4 Disable the controller software 5.2.157.0 ER.aes file to the default directory on your TFTP or FTP server. start downloading the software. Step 6 Disable any WLANs on the controller (using the config wan disable wan id command). Step 7 Log into the controller can contact the TFTP or FTP server. Step 9 Enter transfer download start and answer n to the prompt to view the current download settings. Information similar to the following appears: Mode... . TFTPData Type...... . CodeTFTP Server IP.... .. xxx.xxx.xxx.xxxTFTP Packet Timeout.... . 6TFTP Max Retries..... ... 10TFTP Path.... ... TFTP Filename. xxx.aes This may take some time. Are you sure you want to start? (y/N) nTransfer download mode { tftp | ftp } transfer download mode { tftp | ftp } transfer download serverip server-ip-address transfer download filename transfer download path server-path-to-file Note Pathnames on a TFTP or FTP server, the path is "/". If you are using a TFTP server, also enter these commands: transfer download tftpPktTimeout timeout timeout Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of time (in seconds) that the TFTP server attempts to download the software for the timeout parameter. If you are using an FTP server, also enter these commands: transfer download username transfer download password transfer download start to view the updated settings and answer y to the prompt to confirm the current download settings and start the software download. Information similar to the following appears: Mode...... . TFTPData Type... CodeTFTP Server IP..... .. xxx.xxx.xxx.xxxTFTP Packet Timeout..... . 6TFTP Max Retries... . 10TFTP . TFTP Filename.. . xxx.aesAre you sure you want to start? (y/n) yTFTP Code transfer starting.TFTP receive complete... extracting new bootloader to flash.Making backup copy of RTOS.Writing new RTOS to flash.Making backup copy of Code.Writing new Code to flash.TFTP File Path. transfer operation completed successfully. Please restart the switch (reset system) for update to complete. Step 12 Enter reset system to save the controller. The controller. The controller. The controller completes the bootup process. Note Do not wait to reboot the controller. Otherwise, the access points might start downloading the software before the controller is running it. Step 13 After the controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file). Step 14 Enter config wlan enable wlan id to re-enable the WLANs, Step 15 For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch. Step 16 Re-enable vour 802.11a and 802.11b/g networks. Step 17 If desired, reload your latest configuration file to the controller. Step 18 To verify that the 6.0 controller software is installed on your controller, enter show sysinfo and look at the Product Version field. Step 19 To verify that the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file is installed on your controller, enter the show sysinfo command on the controller Software 5.2.157.0 ER.aes file is installed on your cont Controller Boot Software ER.aes file is not installed, the Field Recovery Image Version or Emergency Image Version field shows "N/A." To minimize a network outages, you can now download an upgrade image to the access point from the controller without resetting the access point or losing network connectivity. Previously, you would download an upgrade image to the controller and reset it, which causes the access point downloads the new image, resets, goes into discovery mode. After the access point download the upgrade image to the controller then download the image to the access point while the network is still up. You can also schedule a reboot of the controller and access points, either after a specific date and time. When both devices are up, the access point will discover and rejoin the controller. Note These access point models do not support predownloading of images: 1120, 1230, and 1310. Keep these guidelines in mind when you use image predownloads on 5500 series controllers. This limitation allows new access points to join the controller during image downloading. If you reach the predownload limit, access points that cannot get an image back off and wait for a time between 180 to 600 seconds and then re-attempt the predownloading to be effective, all controllers (primary, secondary, and tertiary) that your access points can join should use the same images for primary and backup image. For example, if you have three controllers, all three should use software release x as the primary image and release y as the backup image. soon as they reboot. If a 4400 controller reboots before a 5500 controller, it is important that both controllers are running the same images in case an access point joins one rather than the other. Before you enter the predownload command, Cisco recommends that you change the active controller boot image to the backup image. This step ensures that if the controller reboots for some reason, it comes back up with the earlier running image, not the partially downloaded upgrade image, and they automatically delete crash info files, radio files, and any backup images to free up space. However, this limitation does not affect the predownload image replaces any backup image on the access point. Using the CLI, you can predownload the upgrade image to the controller. Predownload the upgrade image to the access points. Upgrade images on the controller and access points. Set a reboot time for the controller and the access points. To obtain an upgrade image to the controller and the access points. download settings, if necessary: in the "Using the CLI to Upgrade Controller Software" section. On the controller CLI, enter transfer download start to view the updated settings and start to view the updated settings. . TFTPData Type.. .. 10TFTP Path. xxx.aesAre vou sure vou want to start? (v/n) vTFTP Code transfer Mode CodeTFTP Server IP.. .. xxx.xxx.xxx.TFTP Packet Timeout.... 6TFTP Max Retries..... TFTP Filename...... starting.TFTP receive complete... extracting components.Writing new bootloader to flash.Making backup copy of RTOS.Writing new RTOS to flash.TFTP File transfer operation completed successfully. Please restart the switch (reset system) for update to complete. Enter show boot on the controller. The new image is listed as the primary image and the old image is listed as the backup. However, you should switch the primary and backup to change the controller active boot image to the existing image (which is now the backup). Enter show boot again to make sure the images are set up correctly. To predownload the image is the access point Flash memory, enter this command on the controller CLI: config ap image is the access point Flash memory, enter this command on the controller CLI: config ap image is the access point Flash memory, enter this command on the controller CLI: config ap image is the access point Flash memory. existing image. Access points always boot with the primary image. To swap an access point's primary and backup images, enter this command: config ap image { all | ap-name } Output for the command: Total number of APs... 7Number of APs Initiated.. . 4 Predownloading.. ... 0 Completed predownloading.. . 3 Not Supported.. . 0 Failed to Predownload... . 0 Predownload PredownloadAP Name Primary Image Backup Image Status Version Next Retry Time --AP1140-1 7.0.56.0 6.0.183.38 Complete 6.0.183.38 NA NAAP1140-2 7.0.56.0 6.0.183.38 Initiated 6.0.183.38 Complete 6.0.183.38 NA NAAP1130-2 7.0.56.0 6.0.183.38 Complete 6.0.183.38 NA NAAP1130-3 7.0.56.0 6.0.183.38 Initiated 6.0.183.38 23:43:25 1AP1130-4 7.0.56.0 Retry Count-6.0.183.38 Complete 6.0.183.38 NA NAAP1130-5 7.0.56.0 6.0.183.38 23:41:33 1 The output lists access points specified for predownloading and provides, for each access point, primary and secondary image versions, the version of the predownload image, the predownload retry time (if necessary), and the number of predownload status for each device. Statuses include: None—the access point is predownload status for each device. Statuses include: None—the access point (1120, 1230, and 1310) does not support predownloading. Initiated—the access point is waiting to get the predownload image because the conccurent download limit has been reached. Failed—the access point has failed 64 predownload image because the conccurent download limit has been reached. of the controller and access points. The network comes back up without going through an image download phase. reset system in HH : MM : SS image { swap | no-swap } reset-aps [save-config] This command lets you specify the amount of time delay before the devices reboot. The controller sends a reset mesage to all joined access points, then the controller resets. Use the swap keyword to swap the primary and backup images on the access point. This output appears on the console after you enter the command: System reset is scheduled for Jan 12 18:12:9 2010. Current local time and date is Jan 12 12:53:35 2010. A trap will be generated 10 minutes before each scheduled system reset. Use 'reset system cancel' to cancel. Configuration will be saved before the system reset. reset system at YYY - MM - DD HH : MM : SS image { swap | no-swap } reset-aps [save-config] This command lets you specify a date and time that the devices will reboot. The controller resets. Use the swap keyword to swap the primary and backup images on the access point. reset system notify-time minutes This output appears on the console after you enter the command: System reset is scheduled for Jan 12 18:12:9 2010. Current local time and date is Jan 12 12:53:35 2010. A trap will be generated 10 minutes before each scheduled reboot, enter the reset system cancel command. Note If you configure reset times and then use the controller, the controller notifies you that any scheduled resets. Sample output for the command: System reset is scheduled for Oct 10 01:01:01 2009. Current local time and date is Oct 07 02:57:44 2009. A trap will be generated 10 minutes before the system reset. If any access points are downloading the image from the controller at the scheduled reset time, the reset is cancelled and this message appears on the controller shave built-in utilities for uploading and downloading various files. Follow the instructions in these sections to import files using either the controller GUI or CLI: In controller software release 6.0 or later, you can download a login banner file using either the GUI or CLI using Telnet, SSH, or a console port connection. You save the login banner information as a text (*.txt) file. The text file cannot be larger than 1500 bytes and cannot have more than 18 lines of text. Note The ASCII characters. Here is an example of a login banner: Welcome to the Cisco Wireless Controller!Unauthorized access prohibited.Contact sysadmin@corp.com for access. Follow the instructions in this section to download a login banner to the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server: If you are downloading through the service port, the TFTP or FTP server must be on the same subnet as the service port is not routable, or you must create static routes on the controller. If you are downloading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the

distribution system port is routable. A third-party TFTP or FTP server cannot run on the same communication port. Note Clearing the controller configuration does not remove the login banner. See the "Clearing the Login Banner" section for information about clearing the login banner file to the controller GUI or CLI. Note The controller, the first login banner file is overwritten. Using the controller GUI, follow these steps to download a login banner file to the controller. Step 1 Copy the login banner file to the default directory on your TFTP or FTP server. Step 2 Choose Commands > Download File to Controller Page (see Figure 9-2). Figure 9-2 Download File to Controller Page (see Figure 9-2). Figure 9-2 Download File to Controller Page (see Figure 9-2). or FTP. Step 5 In the IP Address field, enter the IP address of the TFTP or FTP server, the default values of 10 retries and 6 seconds for the Maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout field, enter the login banner text (*.txt) file. Step 9 If you are using an FTP server. b. In the Server Login Username field, enter the username to log into the FTP server. c. In the Server Port Number field, enter the post number on the FTP server. b. In the Server Login Username to log into the FTP server. occurs. The default value is 21. Step 10 Click Download to download the login banner file to the controller. Step 2 Enter transfer download a login banner file to the controller. Step 3 Enter transfer download mode {tftp | ftp}. Step 3 Enter transfer download mode {tftp | ftp}. Enter transfer download datatype login-banner. Step 6 Enter transfer download filename filena the the TFTP server attempts to download the software for the retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of time (in seconds) that the TFTP server attempts to download the software for the retries parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the retries parameter and the amount of time (in second s server attempts to download the software for the timeout parameter. Step 8 If you are using an FTP server, enter these commands: transfer download port port Note The default value for the port parameter is 21. Step 9 Enter transfer download start to view the updated Login BannerTFTP Server IP..... .. 10.10.10.10TFTP Packet Timeout.. settings; then answer y when prompted to confirm the current settings and start the download process. This example shows the download command output: Mode.... . TFTP Data Type..... ... banner.txtThis may take some time.Are you sure you want to start? (y/N) yTFTP Login Banner transfer starting.TFTP receive complete... checking login banner.Successfully installed new login banner file Using the controller GUI, follow these /TFTP Filename..... steps to clear the login banner from the controller. Step 1 Choose Commands > Login Banner page (see Figure 9-3). Figure 9-3 Login Banner page (see Figure 9-3). Figure 9-3 Login Banner from the controller cLI, enter the clear login banner command. Each wireless device (controller, access point, and client) has its own device certificate. For example, the controller is shipped with a Cisco-installed device certificate is used by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authentication. However, if you wish to use your own vendor-specific device certificate, it must be downloaded to the controller. Note See the "Configuring local EAP" section to download a vendor-specific device certificate to the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server available for the certificate download. Keep these guidelines in mind when setting up a TFTP or FTP server must be on the same subnet as the service port is not routable, or you must create static routes on the controller. If you are downloading through the distribution system port is routable. A third-party TFTP or FTP server can be on the same or a different subnet because the WCS built-in TFTP or FTP server. and the third-party TFTP or FTP server require the same communication port. Note All certificates downloaded to the controller. Step 1 Copy the device certificate to the default directory on your TFTP or FTP server. Step 2 Choose Commands > Download File to open the Download File to Controller Page (see Figure 9-4). Figure 9-4 Download File to Controller Page Step 3 From the Transfer Mode drop-down box, choose TFTP or FTP. Step 6 In the IP Address field, enter the IP address of the TFTP or FTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and 6 seconds for the Maximum Retries and 7 interver, the default values of 10 retries and 6 seconds for the Maximum Retries and 6 seconds for the Maximum Retries and 7 interver, the default values of 10 retries and 6 seconds for the Maximum Retries and 7 interver, the default values of 10 retries and 6 seconds for the Maximum Retries and 6 seconds for the Maximum Retries and 7 interver, the default values of 10 retries and 6 seconds for the Maximum Retries and 7 interver, the default values of 10 retries and 6 seconds for the Maximum Retries and 6 seconds for the Maximum Retries and 7 interver, the default values of 10 retries and 6 seconds for the Maximum Retries and 8 se maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Maximum Retries field and the name of the certificate. Step 10 If you are using an FTP server, follow these steps: a. In the Server Login Username field, enter the password to log into the FTP server. b. In the Server Login Username field, enter the password field, enter the password field, enter the password to log into the FTP server. b. In the Server Login Username field, enter the password field, enter the password field, enter the password field server. b. In the Server Login Username field, enter the password field server. b. In the Server Login Username field, enter the password field server. b. In the Server Login Username field, enter the password field server. b. In the Server Login Username field server. b. In the Server Login Us occurs. The default value is 21. Step 11 Click Download to download the device certificate to the controller. A message appears indicating the status of the download. Step 12 After the download is complete, choose Commands > Reboot > Reb decision to reboot the controller. Using the controller CLI, follow these steps to download a device certificate to the controller. Step 3 Enter transfer download datatype eapdevcert. Step 4 Enter transfer download datatype eapdevcert. download serverip server-ip-address. Step 6 Enter transfer download tftpMaxRetries retries retries transfer download tftpMaxRetries retries retries retries retries retries transfer download tftpMaxRetr timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of time (in seconds) that the TFTP server attempts to download the software for the timeout parameter. Step 9 If you are using an FTP server, enter these commands: transfer download password transfer download password transfer download password transfer download start to view the updated settings; then answer y when prompted to confirm the current settings and TFTPData Type..... Vendor Dev CertTFTP Server IP...... 10.10.10.4TFTP Packet Timeout...... start the download process. This example shows the download command output: Mode...... 6TFTP Max Retries...... . 10TFTP Path filename.pemThis may take some time.Are you sure you want to start? (y/N) yTFTP EAP Dev cert transfer starting.Certificate installed.Reboot the switch to use the new certificate. Step 11 Enter reset system to reboot the controller. Controllers and access points have a Certificate Authority (CA) /tftpboot/username/TFTP Filename...... certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate and peace by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authenticate wireless clients during local EAP authenticate and peace by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authenticate wireless clients during local EAP authenticate and peace by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authenticate wireless clients during local EAP authenticate and peace by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authenticate and peace by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authenticate and peace by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate and peace by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate and peace by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate and peace by EAP-FAST (when not using PACs), eap-fast (when not u specific CA certificate, it must be downloaded to the controller. Note See the "Configuring Local EAP" section for information on configuring local EAP. Follow the instructions in this section to download CA certificates to the controller through the GUI or CLI. However, before you begin,
make sure you have a TFTP or FTP server available for the certificate download. Keep these guidelines in mind when setting up a TFTP or FTP server: If you are downloading through the service port is not routable, or you must create static routes on the service port because the service port because the service port because the service port is not routable. system network port, the TFTP or FTP server cannot run on the same computer as WCS because the distribution system port is routable. A third-party TFTP or FTP server cannot run on the same communication port. Note All certificates downloaded to the controller must be in PEM format. Using the controller GUI, follow these steps to download a CA certificate to the default directory on your TFTP or FTP server. Step 2 Choose Commands > Download File to open the Download File to Controller page (see Figure 9-5). Figure 9-5 Download File to Controller Page Step 3 From the File Type drop-down box, choose Vendor CA Certificate . Step 4 From the Transfer Mode drop-down box, choose TFTP or FTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the certificate in the Timeout field. Step 7 In the File Path field, enter the directory path of the certificate. Step 8 In the File Name field, enter the username to log into the FTP server. b. In the Server Login Password field. enter the password to log into the FTP server. c. In the Server Port Number field, enter the port number on the FTP server through which the download to download to download to download is complete, choose Commands > Reboot + CLI. Step 12 If prompted to save your changes, click Save and Reboot = CLI, follow these steps to download mode {tftp | ftp}. Step 3 Enter transfer download datatype eapcacert . Step 4 Enter transfer download tftpMaxRetries retries transfer download filename .pem. Step 7 If you are using a TFTP server, enter these commands: transfer download tftpMaxRetries retries transfer download tftpPktTimeout timeout Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the retries parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the timeout parameter. Step 8 If you are using an FTP server, enter these commands: transfer download postsword transfer download start to view the . TFTPData Type..... .. Vendor CA CertTFTP Server IP..... 10 10 10 4TFTP Packet Timeout updated settings; then answer y when prompted to confirm the current settings and start the download process. This example shows the download command output: Mode..... . /tftpboot/username/TFTP Filename............ filename.pemThis may take some time.Are you sure you want to start? (y/N) yTFTP EAP CA cert transfer starting.Certificate installed.Reboot the switch to use the new certificate. Step 10 Enter reset system to reboot the controller. 10TFTP Path..... Protected access credentials (PACs) are credentials that are either automatically or manually provisioned and used to perform mutual authentication. When manual PAC provisioning is enabled, the PAC file is manually generated on the controller. Note See the "Configuring Loca EAP" section for information on configuring local EAP. Follow the instructions in this section to generate and load PACs from the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server: If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port is not routable, or you must create static routes on the same or a different subnet because the distribution system port is routable. A third-party TFTP or FTP server cannot run on the same communication port. Using the controller GUI, follow these steps to upload a PAC from the controller. Step 1 Choose Commands > Upload File to open the Upload File from Controller Page (see Figure 9-6). Figure 9-6 Upload File from Controller Page Step 2 From the File Type drop-down box, choose PAC (Protected Access Credential). Step 3 In the User field, enter the number days for the PAC to remain valid. The default setting is zero (0). Step 5 In the Password and Confirm Password to protect the PAC. Step 6 From the Transfer Mode drop-down box, choose TFTP or FTP. Step 7 In the IP Address field, enter the IP address of the TFTP or FTP is enter the IP address of the TFTP or FTP or FTP. Step 9 In the File Name field, enter the name of the PAC file. PAC files have a .pac extension. Step 10 If you are using an FTP server. b. In the Server Login Password field, enter the password to log into the FTP server. c. In the Server Port Number field, enter the port number on the FTP server through which the upload occurs. The default value is 21. Step 11 Click Upload to upload the PAC from the controller. A message appears indicating the status of the upload to upload to upload the PAC from the controller. password that you entered above. Using the controller CLI, follow these steps to upload a PAC from the controller. Step 3 Enter transfer upload datatype pac. Step 4 Enter transfer upload datatype pac. Step 3 Enter transfer upload datatype pac. address. Step 6 Enter transfer upload path server-path-to-file. Step 7 Enter transfer upload filename manual. pac. Step 8 If you are using an FTP server, enter these commands: transfer upload username transfer upload filename manual. pac. Step 9 Enter transfer upload password transfer upload port port Note The default value for the port parameter is 21. Step 9 Enter transfer upload password transfer upload username transfer upload password transfer upload username transfer upload pas upload start to view the updated settings; then answer y when prompted to confirm the current settings and start the upload process. This example shows the upload command output: Mode...... TFTPTFTP Server IP..... 10.10.10.4TFTP Path..... . /tftpboot/username/TFTF . manual.pacData Type.. PACPAC User..... . usernamePAC Validity..... . 10 daysPAC Password..... . passwordAre you sure you want to start? (y/N) yPAC transfer starting.File transfer operation completed successfully. Step 10 Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above. Cisco recommends that you entered above. Cisco recommends that you entered above. not download a configuration file to your controller that was uploaded from a different controller. In controller software release 4.2 or later, the controller's bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in binary format. Therefore, you cannot download a binary configuration file onto a controller release to 4.2 or later. However, when you upgrade a controller software release 5.2 or later enables you to read and modify the configuration files. See the "Editing Configuration files to be modified. If you attempt to make changes to a 4.2, 5.0, or 5.1 configuration files and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values. You can upload configuration files using either the GUI or the CLI. Using the controller GUI, follow these steps to upload File from Controller page (see Figure 9-7). Figure 9-7 Upload File from Controller Page Step 2 From the File Type drop-down box, choose Configuration File Encryption key in the Encryption Key field. Step 4 From the Transfer Mode drop-down box, choose TFTP or FTP. Step 5 In the IP Address field, enter the IP address of the TFTP or FTP server. Step 6 In the File Name field, enter the address of the configuration file. Step 7 In the File Name field, enter the instead of the configuration file. Step 7 In the File Name field, enter the instead of the configuration file. Step 7 In the File Name field, enter the name of the configuration file. Step 7 In the File Name field, enter the instead of the configuration file. Step 8 If you are using an FTP server. Step 6 In the File Name field, enter the instead of the configuration file. Step 8 If you are using an FTP server. Step 6 In the File Name field, enter the instead of the configuration file. Step 8 If you are using an FTP server. Step 6 In the File Name field, enter the instead of the configuration file. Step 8 If you are using an FTP server. Step 6 In the File Name field, enter the instead of the configuration file. Step 8 If you are using an FTP server. Step 6 In the File Name field, enter the instead of the configuration file. Step 8 If you are using an FTP server. Step 6 In the File Name field, enter the instead of the configuration file. Step 8 If you are using an FTP server. Step 6 In the File Name field, enter the instead of the configuration file. Step 8 If you are using an FTP server. Step 6 In the File Name field, enter the instead of the configuration file. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP server. Step 8 If you are using an FTP s username to log into the FTP
server. b. In the Server Login Password to log into the FTP server. c. In the Server Port Number field, enter the password to log into the FTP server. A message appears indicating the status of the upload fails, repeat this procedure and try again. Using the controller CLI, follow these steps to upload the configuration file, enter this command: transfer upload mode {tftp | ftp} Step 2 To specify the trype of file to be uploaded, enter this command: transfer upload datatype config Step 3 To encrypt the file Step 4 To specify the IP address of the TFTP or FTP server, enter this command: transfer upload serverip serverip-address Step 5 To specify the directory path of the configuration file, enter this command: transfer upload path server-path-to-file Step 6 To specify the name of the configuration file to be uploaded, enter this command: transfer upload filename and password used to log into the FTP server and the port number through which the upload occurs: transfer upload destart Step 9 When prompted AS 4402 4 2 55 8 Config.xmlData Type.. .. TFTP TFTP Server IP...... 10.10.10.4TFTP Path..... . Config/TFTP Filename..... to confirm the current settings, answer v. This example shows the upload command output: Mode. download configuration files using either the GUI or the CLI. Using the controller GUI, follow these steps to download a configuration file to controller Bage (see Figure 9-8). Figure 9-8 Download File to Controller Page Step 2 From the File Type drop-down box choose Configuration . Step 3 If the configuration file is encrypted, check the Configuration File Encryption Key field. Note The key that you enter here should match the one entered during the upload process. Step 4 From the Transfer Mode drop-down box, choose TFTP or FTP. Step 5 In the IP Address field, enter the IP address of the TFTP or FTP server. Step 6 If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the configuration file in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the configuration file. Step 8 In the File Name field, enter the name of the configuration file. Step 9 If you are using an FTP server, follow these steps: a. In the Server Login Username field, enter the password to log into the FTP server. c. In the Server Login Password field, enter the password to log into the FTP server. download occurs. The default value is 21. Step 10 Click Download to download the file to the controller. A message appears indicating the status of the download fails, repeat this procedure and try again. Using the controller CLI, follow these steps to download fails, repeat this procedure and try again. controller. Note The controller does not support incremental configuration downloads. The configuration file contains all mandatory CLIs, and interface port or LAG enable or disable CLIs) required to successfully complete the download. For example, if you download only configuration file contains all mandatory CLIs (all interface address CLIs, mgmtuser with read-write permission CLIs, and interface port or LAG enable or disable CLIs) required to successfully complete the download. time ntp server index server address as part of the configuration file, the download fails. Only the CLI commands present in the configuration file, enter this command: server address as part of the configuration file, enter this command: transfer download mode {tftp | ftp} Step 2 To specify the type of file to be downloaded, enter this command: transfer encrypt enable transfer encrypt set-key key, where key is the encryption key used to decrypt the file Note The key that you enter here should match the one entered during the upload process. Step 4 To specify the IP address of the TFTP or FTP server, enter this command: transfer download path server-ip-address Step 5 To specify the name of the configuration file to be download the active server, enter these commands: transfer download the active server, enter these commands: transfer download the active server, enter these commands: transfer download the active server, enter the active change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the timeout parameter. Step 8 If you are using an FTP to specify the username and password used to log into the FTP server and the port number through which the download occurs: transfer download port port Note The default value for the port parameter is 21. Step 9 To view the updated settings, enter this command: transfer download start Step 10 When prompted to confirm the current settings and start the download process, answer y. This example shows the download command output: Mode... . TFTP TFTP Server IP...... 10.10.10.4TFTP Path.... . Config/TFTP Filename. AS_4402_4_2_55_8_Config.xmlData Type. . Config File Encryption.. successfully. If the download fails, repeat this procedure and try again. Controllers contain two kinds of memory: volatile RAM to NVRAM. At any time, you can save the configuration from volatile RAM to NVRAM. At any time, you can save the configuration from volatile RAM to NVRAM. without resetting the controller. reset system—Prompts you to configuration changes before you log out. When you save the controller's configuration, the controller stores it in XML format in flash memory Controller software release 5.2 or later enables you to easily read and modify the configuration file by converting it to CLI format. When you are finished you download the file back to the controller, where it is reconverted to XML format and saved. Follow these steps to edit the configuration file on the server. You can modify or delete existing CLI commands and add new CLI commands to the file. Note To edit the configuration file on the server. Step 4 To download the configuration file to the configuration file to the configuration file on the server. Step 4 To download the configuration file on the server. configuration file to XML format, saves it to flash memory, and then reboots using the new configuration. CLI commands are ignored and saved to flash memory. Any CLI commands that have invalid values are replaced with default values. To see any ignored commands or invalid configuration values, enter this command: show invalid-config Note You cannot execute this command after the clear config or save config or save config or save config ratio to the TFTP or FTP server for analysis. To do so, perform one of the following: Step 6 The controller does not support the uploading of port configuration CLI commands. If you want to configuration CLI commands. If you want to configuration CLI commands to do so now: configuration CLI commands to do so now: configuration CLI commands. If you want to configuration CLI commands to do so now: configuration CLI commands to do so now: configuration CLI commands. specific controller port or for all ports. Step 7 To save your changes, enter this command: save config Follow these steps to clear the active configuration in NVRAM. Step 1 Enter clear config and enter y at the confirmation prompt to configuration wizard starts automatically. Step 3 Follow the instructions in the "Using the Configuration Wizard" to complete the initial configuration. Follow these steps to reset the controller configuration to default settings. Step 1 Enter reset system. At the confirmation prompt, enter y to save configuration changes to NVRAM. The controller reboots and the configuration wizard starts automatically. Step 3 Follow the instructions in the "Using the Configuration Wizard" to complete the initial configuration. You can reset the controller and view the reboot process on the CLI console using one of the following two methods: Turn the controller off and then turn it back on. On the CLI, enter reset system. At the confirmation prompt, enter y to save configuration changes to NVRAM. The controller reboots. When the controller reboots, the CLI console displays the following reboot information: Initializing the system software load. Initializing with its stored configurations. Displaying the login prompt. Page 2 11n Mode parameter 6-39 7920 AP CAC parameter 6-39 7920 AP CAC parameter 6-39 7920 AP CAC parameter 6-39 7920 Client CAC parameter 6-39 7920 AP CAC parameter 6-39 7920 Client CAC parameter 6-39 7920 AP CAC 802.11a (or 802.11b) > Client Roaming page 4-62 802.11a (or 802.11b/g) > EDCA Parameters page 4-77 802.11a (or 802.11b/g) > EDCA Parameters page 4-77 802.11a (or 802.11b/g) > EDCA Parameters page 4-77 802.11a (or 802.11b/g) > EDCA Parameters page 4-78 802.11a (or 802.11b/g) > EDCA Parameters page 4-77 802.11a (or 802.11b/g) > EDCA Parameters page 4-78 802.11a (or 802.11b/g) > EDCA Parameters page 4-88 802.11a (or 802.11b/g) Network Status parameter 4-30, 4-38, 4-39 802.11a/n (or 802.1 Wireless Menu) 7-14 802.11a > Pico Cell page 11-14 802.11a > RRM > DcA page 11-14 802.11a > R 11-11 802.11a Global Parameters page 11-40 802.11b/g/n Cisco APs > Configure page 7-86, D-49 802.11 bands configuring using the CLI 4-31 to 4-33 configuring using the GUI 4-29 to 4-31 802.11h, described 4-38 802.11h Global Parameters page 4-38 802.11h parameters, configuring using the CLI 4-39 using the CLI 4-39 using the GUI 4-29 to 4-31 802.11b, described 4-38 802.11h Global Parameters page 4-38 802.11h global Parameters, configuring using the CLI 4-39 using the GUI 4-29 to 4-31 802.11c global Parameters page 4-38 802.11h glob GUI 4-38 to 4-39 802.11n clients 7-102 configuring using the GUI 4-35 to 4-38 using the GUI 4-35 to 4-38 devices 4-33 802.11n (2.4 GHz) High Throughput page 4-34 802.1X configuring 6-24 described 6-26 802.1X authentication for access points configuring the switch 7-23 using the CLI 7-21 to 7-23
using the GUI 7-19 to 7-21 described 7-18 802.3 k flow control, enabling 4-52 AAA override configuring using the CLI 5-83 so 4-54 so 2.3 k flow control, enabling 4-52 AAA override configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-53 so 2.3 k flow control, enabling 4-53 so 2.3 k flow control, enabling 4-52 and configuring using the CLI 5-83 so 2.3 k flow control, enabling 4-53 so 2.3 k flow control, enabling 4-53 so 2.3 k flow control, enabling 4-53 so 2.3 k fl using the GUI 5-83 described 5-81 AC adapter warning for Japan B-7 Access Control List Name parameter 5-59 access control lists (ACLs) applying to a WLAN using the CLI 5-67 using the GUI 5-63 to 5-64 applying to a WLAN using the CLI 5-67 using the GUI 5-63 configuring to a WLAN using the CLI 5-67 using the GUI 5-63 configuring to a WLAN using the GUI 5-63 to 5-64 applying to a WLAN using the GUI 5-63 to 5-64 applying to a WLAN using the GUI 5-67 using the CLI 5-65 to 5-66 using the GUI 5-58 to 5-61 configuring using the GUI 5-58 to 5-61 configuring using the CLI 5-65 configuring using the GUI 5-58 to 5-61 configuring using the GUI 5-58 described 5-57, 5-59, 5-66 using with the debug facility D-42 to D-43 Access Control Lists > New page 5-61 Access 58 Access Control Lists > Rules > New page 5-59 Access Control Lists page 5-58 Access point count, approved tiers for 5500 series controllers 4-4 access point count, approved tiers for 5500 series control Lists page 5-58 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > Rules > New page 5-59 Access point count, approved tiers for 5500 series control Lists > New page 5-59 Access point count, approved tiers for 5500 series control Lists > New page 5-59 Access point control CLI 6-59 using the GUI 6-57 creating using the CLI 6-57 to 6-59 using the GUI 6-54 to 6-57 default group 6-54 described 6-52 illustrated 6-53 removing using the CLI 6-58 using the GUI 6-57 to 6-59 using the GUI 6-54 to 6-57 default group 6-54 described 6-52 illustrated 6-53 removing using the GUI 6-54 to 6-57 default group 6-54 described 6-52 illustrated 6-53 removing using the GUI 6-58 using the GUI 6-57 to 6-59 using the GUI 6-58 using the GUI 6-58 using the GUI 6-59 using the GUI MHz channelization 11-29 assisted roaming 4-61 authorization list 7-33 authorizing using LSCs 7-27 using MICs 7-27 using the CLI 7-33 using the CLI 7-32 configuring hybrid REAP using the CLI 7-33 using the CLI 7-32 using MICs 7-27 using the CLI 7-34 using the CLI 7-34 using the CLI 7-34 using the CLI 7-35 using the 7-101 interpreting D-2 migrating from the -J regulatory domain to the -U regulatory domain 7-80 to 7-83 number supported per controller 3-5 priming 7-7 regulatory information B-2 to B-10 rules for operating in Taiwan B-8 to 7-49 troubleshooting the join process 7-34 to 7-41 using Telnet or SSH D-50 to D-52 VCI strings 7-34 verifying that they join the controller 7-9 viewing multicast client table 4-60 Accounting Server parameters 6-65 accounting servers, disabling per WLAN 6-64 ACL. See access control lists (ACLs) ACL Name parameter 5-62, 5-63 ACS server configuration page 6-62 Action parameter 5-88 administrator usernames 5-59 Add Web Server button 10-21 AdHoc Rogue AP parameter 5-63 active exploits 5-128 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AP button 13-18 Add New Rule button 5-59 Add Web Server button 10-21 AdHoc Rogue AP parameter 5-63 active exploits 5-128 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AP button 13-18 Add New Rule button 5-59 Add Web Server button 10-21 AdHoc Rogue AP parameter 5-63 active exploits 5-128 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AP button 13-18 Add New Rule button 5-59 Add Web Server button 10-21 AdHoc Rogue AP parameter 5-63 active exploits 5-128 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AP button 13-18 Add New Rule button 5-59 Add Web Server button 10-21 AdHoc Rogue AP parameter 5-63 active exploits 5-128 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AP button 5-59 Add Web Server button 5-59 Add Web Server button 5-59 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AAA Client page (on CiscoSec and passwords, configuring 4-41 Admin Status parameter 3-24, 3-25 Admission Control (ACM) parameter 4-76, 4-77 AES CBS IPSec data encryption 5-9 AES-CCMP 6-25 AES parameter 6-27 Aggregated MAC Protocol Data Unit (A-MPDU) 4-36 Aggregated MAC Service Data Unit (A-MSDU) 4-36 aggregation method, specifying 4-36 aggregation method, specifying 4-36 aggregated MAC Protocol Data Unit (A-MPDU) 4-36 Aggregated MAC Protocol Data Unit (A-MSDU) 4-36 aggregated MAC Protoc balancing 4-47 AirMagnet Enterprise Analyzer D-47 Aironet IE parameter 6-29, 6-50 Airopeek D-47 Alarm Trigger Threshold parameter 11-37 All APs > Access Point Name > Link Details > Neighbor Name page 8-53 All APs > Access Point Name > Mesh Neighbor Stats page 8-53 All APs > Access Point Name > Neighbor Info page 8-52 All APs > Access Point Name > Statistics page 8-47 All APs > Access Point Name > VLAN Mappings page 13-13 All APs > Details (Advanced) page 7-4, 7-44, D-51 configuring country codes 7-77 configuring link latency 7-94 configuring PoE 7-98 All APs > Details for (Credentials) page 7-16, 7-20, 7-53 All APs > Details for (General) page 7-47, 7-51, 13-12 All APs > Details for (H-REAP) page 7-52, 13-12 All APs > Details for (Inventory) page 7-90 All APs > Details for page D-48, D-53 All APs > Details page 8-19, 7-51, 13-12 All APs > Details for (H-REAP) page 7-52, 13-12 All APs > Details for (Inventory) page 7-90 All APs > Details for page D-48, D-53 All APs > Details page 8-19, 7-51, 13-12 All APs > Details for (H-REAP) page 7-52, 13-12 All APs > Details for (H-REAP) page 7-51, 7-69, 7-73 All APs > Details for (H-REAP) page 7-52, 13-12 All APs > Details for (H-REAP) page 7-51, 7-69, 7-73 All APs > Details for (H-REAP) page 7-52, 13-12 All APs > Details for (H-REAP) page 7-51, 7-69, 7-73 All APs > Details for (H-REAP) page 7-52, 13-12 All APs > Details for (H-REAP) page 7-52, 13-12 All APs > Details for (H-REAP) page 7-52, 13-12 All APs > Details for (H-REAP) page 7-51, 7-69, 7-73 All
APs > Details for (H-REAP) page 7-52, 13-12 All APs > Deta 8-35, 11-37 All APs page 7-10, 8-46, 11-36, 13-12 Allow AAA Override parameter 5-83 AnchorTime parameter 11-30 AP > Clients > Traffic Stream Metrics page 4-82 AP > Clients page 4-82 AP801 access point described 7-24 using with a controller 7-24 AP Authentication Policy page 5-70, 11-37 AP Core Dump parameter 7-44 ap-count licenses. See licenses AP Ethernet MAC Addresses parameter 7-29 AP Failover Priority parameter 7-73 AP Group Name parameter 6-55 AP Groups > Edit (APs) page 6-57 AP Groups > Edit (General) page 6-56 AP Groups > Edit (WLANs) page 6-56, 6-71 AP Groups > Edit (WLANs) page 6-56, 6-71 AP Groups > Edit (APs) page 6-56, 6-71 AP Groups > Edit (WLANs) page 6-56, 6-71 AP Groups > Edit (APs) page 6-56, 6-71 AP Groups > Edit (WLANs) page 6-56, 6-71 AP Groups 3-12 to 3-15 creating multiple interfaces using the CLI 3-44 using the GUI 3-42 to 3-43 described 3-8 illustration of four AP-manager interfaces 3-40 of three AP-manager interfaces 3-40 of three AP-manager interfaces 3-40 using multiple 3-39 to 3-44 AP Mode parameter 6-57 AP Policies page 7-32 AP Primary Discovery Timeout parameter 7-68 ASLEAP detection 5-128 Assignment Method parameter 11-29, 11-31 asymmetric tunneling described 12-26 authentication bind method 5-36, 5-39 Authentication Protocol parameter 4-46 Auth Key Mgmt parameter 6-27 Authority ID Information parameter 5-46, 13-22 13-23 Authority ID parameter 5-46, 13-22 Authorize LSC APs against auth-list parameter 7-32 authorize MIC APs against auth-list or AAA parameter 7-32 auto-anchor mobility configuring using the GUI 12-23 to 12-24 using the GUI 12-21 to 12-23 guidelines 12-20 to 12-20 to 12-20 to 12-20 to 12-20 to 12-24 using the GUI 12-21 to 12-23 guidelines 12-20 to 12-20 to 12-20 to 12-20 to 12-24 using the GUI 12-21 to 12-23 guidelines 12-20 to 12-24 using the GUI 7-32 authorize MIC APs against auth-list or AAA parameter 7-32 authorize MIC APs against authorize MIC APs against authorize MIC APs against a 21 auto-immune feature 5-109 AutoInstall described 2-26, 2-29 example operation 2-27 overview 2-26 selecting configuration file 2-28 using 2-26 Average Data Rate parameter 4-67, 4-70 Average Real-Time Rate parameter 4-67, 4-71 Avoid Cisco AP Load parameter 11-15 Avoid Foreign AP Interference parameter 11-15, 12-18 Avoid Non-802.11a (802.11b) Noise parameter 11-15 Backhaul Client Access parameter 8-59 backup controllers configuring using the CLI 7-70 to 7-72 using the GUI 7-68 to 7-69 described 7-67 Back-up Primary Controller IP Address parameter 7-68 Back-up Primary Controller Name field 7-68 Back-up Secondary Controller IP Address parameter 7-69 Back-up Secondary Controller Name parameter 7-69 band selection 4-49 bandwidth-based CAC described 4-73 enabling using the CLI 4-83 using the GUI 4-76 for mesh networks 8-40 base license. See licenses Base MAC Address parameter 3-30 Beacon Period parameter 4-30 beamforming configuring using the CLI 11-41 to 11-42 using the GUI 11-40 to 11-41 described 11-39 guidelines 11-39 Beamforming parameter 5-36 Bridge Group Name parameter 8-35 bridge protocol data units (BPDUs) 3-27 bridging parameters configuring using the CLI 8-37 to 8-39 configuring using the GUI 8-35 to 8-37 browsers supported 2-16 Buffered Log Level parameter D-10 Burst Data Rate parameter 4-67, 4-71 CAC configuring for 7920 phones 6-38 described 4-73 enabling using the CLI 4-84 using the GUI 4-77 in mesh networks 8-39 viewing in mesh networks 8-42 to 8-44 viewing using the CLI 4-85 Canadian compliance statement B-3 CAPWAP and mesh access points 8-8 cascading 11-6 CA Server URL parameter 7-28 Catalyst 3750G Integrated Wireless LAN Controller Switch described 1-12 logical connectivity diagram and associated software commands E-4 to E-5 ports 3-3, 3-4, 3-5 CCA Sensitivity Threshold parameter 11-50 CCKM configuring 6-27 described 6-25 hybrid-REAP groups 13-17 with mobility 12-7 CCX configuring using the CLI 6-52 using the C 64 using the GUI 4-62 to 4-64 debugging using the CLI 1-45 debugging using the CLI 11-45 debuggi clients enabling location presence 4-110 troubleshooting D-26 to D-42 CCXv5 Req button D-33 CCX Version parameter 6-51 CDP > AP Neighbors > Detail page 4-95 CDP > Interface Neighbors > Detail page 4-95 4-97 CDP Advertisement Version parameter 4-93 CDP AP Neighbors page 4-96 CDP Protocol Status parameter 4-93 CDP State parameter 4-94 Certificate File Name parameter 10-8 Certificate File Path parameter 10-8 Certificate Issuer parameter 5-45 Certificate Type parameter 5-93 Channel Assignment Leader parameter 11-16 Channel Assignment Method parameter 11-14 channel bonding in the 5-GHz band 11-30 Channel parameter 11-28, D-49 Channel Scan Duration parameter 11-20 Channel Scan Duration parameter 11-28 to 11-32 channel Scan Duration parameter 11-20 Channel Sc parameter 5-45 chokepoints for RFID tag tracking 4-101 CIDS Sensor Add page 5-106 CIDS Shun List page 5-107 CIDS Sensors List page 5-106 CIDS Shun List page 5-106 CIDS Shun List page 5-106 CIDS Shun List page 5-107 CIDS Sensors List page 5-106 CIDS Shun List page 5-106 CIDS Shu ports 3-2, 3-4 Cisco 28/37/38xx Integrated Services Router described 1-12 logical connectivity diagram and associated software commands E-3 ports 3-4, 3-5, 4-116 versions 1-12 Cisco 3200 Series Mobile Access Router (MAR) described 8-58 operating with mesh access points using the CLI to configure 8-60 using the GUI to configure 8-59 Cisco 3300 Series Mobility Services Engine (MSE), using with wIPS 5-123 Cisco 4400 Series Wireless LAN Controllers AutoInstall interfaces 2-27 choosing between link aggregation and multiple AP-manager interfaces 3-34 to 3-43 described 1-9 FCC statement B-10 models 3-4 to 3-5 network connections 1-16 to 1-17 ports 3-2, 3-4, 3-5 Cisco 5500 Series Wireless LAN Controllers choosing between link aggregation and multiple AP-manager interfaces 3-34 to 3-45 network connections 1-17 ports 3-3, 3-5 using the USB console port 3-33 to 3-34 Cisco 7920 Wireless IP Phones 6-38 Cisco Adaptive Wireless Path Protocol (AWPP) 8-8 Cisco Adaptive Wireless IP Phones 6-38 Cisco Adaptive Wireless Phones 6-38 Cisco Adaptive Wireless IP P configuring using the CLI 4-98 to 4-99 using the GUI 4-93 to 4-94 debugging using the GUI 4-93 to 4-94 consistent devices 4-90 viewing the GUI 4-97 Cisco Discovery Protocol parameter 4-94 Cisco high-power switches 7-99 Cisco License Manager (CLM) and the controller license agent 4-26 using to register PAKs 4-6 Cisco Secure Access Control Server (ACS) 5-4 Cisco Licensing website 4-21 Cisco License agent 4-26 using to register PAKs 4-6 Cisco Secure Access Control Server (ACS) 5-4 Cisco License Manager (CLM) and the controller license agent 4-26 using to register PAKs 4-6 Cisco Secure Access Control Server (ACS) 5-4 Cisco License Manager (CLM) and the controller license agent 4-26 using to register PAKs 4-6 Cisco Secure Access Control Server (ACS) 5-4 Cisco License Manager (CLM) and the controller license agent 4-26 using to register PAKs 4-6 Cisco Secure Access Control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the
control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (ACS) 5-4 Cisco License Manager (CLM) and the control Server (CLM) and the co 4 illustrated 1-3 Cisco Wireless Control System (WCS) 1-2 Cisco WiSM configuring the Supervisor 720 4-114 to ?? guidelines 4-114 logical connectivity diagram and associated software commands E-2 to E-3 maximum number supported by router chassis 1-11 ports 3-4, 3-5 SSC key-hash 7-26 CKIP configuring using the CLI 6-30 using the GUI 6-29 to 6-30 described 6-29 Clear Config button 7-58 Clear Filter link 6-8, 7-13, 7-14, 7-38 clearing the controller configuration 9-34 Clear Stats on All APs button 12-19 Clear States on All APs b 23 to 2-26 Client Certificate Required parameter 5-45 client exclusion policies, configuring using the CLI 5-76 to 5-77 using the CLI 5-76 to 5-77 using the CLI 5-76 to 5-76 client Exclusion Policies page 5-76 Client Exclusion Policies, configuring using the CLI D-35 to D-39 configuring using the GUI D-32 to D-35 described D-26 Client Reporting page D-34 client roaming, configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing CCX version using the GUI 6-52 using the GUI 7-102 to 7-105 using the GUI 7-102 to 7-105 viewing CCX version using the GUI 7-102 to 7-105 viewing CCX version using the GUI 7-102 to 7-105 viewing CCX version using the GUI 7-102 to 7-105 viewing CCX version using the GUI 7-102 to 7-105 viewing CCX version using the GUI 7-102 to 7-105 viewing CCX version using the GUI 7-102 to 7-105 viewing CCX version using the GUI 7-102 to 7-105 viewing configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing CCX version using the GUI 7-102 to 7-105 viewing CCX version using the GUI 7-102 to 7-105 viewing CCX version using the GUI 7-102 to 7-105 viewing configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing configuring 4-60 to 4-65 clients connecting page 4-80 Clients > Detail page configuring client reporting D-33 viewing a client's CCX version 6-51 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing client setup of workgroup bridges 7-64 viewing voice and video setup of workgroup bridges 7-64 viewing voice and video setup of workgroup bridges 7-64 viewing voice and video settings 4-78 Client Type parameter 7-64, 7-65 Commands > Reset to Factory Defaults page 4-116 comma-separated values (CSV) file, uploading 13-21 Community Name parameter 4-44 conditional web redirect 6-60 configuring using the GUI 6-62 to 6-63 described 6-60 Conditional Web Redirect parameter 6-63 Configuration File Encryption parameter 9-30 configuration files downloading using the GUI 9-27 to 9-32 using the GUI 9-29 to 9-30, ?? to 9-32 configuration wizard CLI version 2-13 to 2-16 described 2-2 GUI version 2-3 to 2-13 Configuration Wizard - 802.11 Configuration page 2-11 Configuration Wizard - Management Interface Configuration Wizard - Set Time page 2-12 Configuration Wizard - SNMP Summary page 2-4, 2-6 Configuration Wizard - System Information page 2-3 Configuration Wizard - Virtual Interface Configuration page 2-8 Configur 6 debugging 7-6 described 7-2 guidelines 7-2 viewing MTU information 7-5 controllers are 3-4 versions 3-5 controller soft of 9-34 erasing 9-34 erasi deployment 1-4 overview 1-7 resetting factory default settings using the GUI 4-116 single-controller deployment 1-3 to 1-4 synchronizing with location appliance 4-106 types of memory 1-14 upgrading software using the GUI 9-6 to 9-8 Controller Spanning Tree Configuration page 3-30 Controller Time Source Valid parameter 5-72 Control Path parameter 12-23 core dump files described D-18 uploading automatically to an FTP server using the CLI D-20 using the GUI D-19 uploading from a 5500 series controller to a TFTP or FTP server D-20 to D-21 Core Dump page D-19 Country Code parameter 7-77 country codes configuring using the CLI 7-78 to 7-80 using the GUI 7-76 to 7-77 described 7-75 Japanese 7-81 viewing using the CLI 7-79 Country page 7-76 Coverage Exception Level per AP parameter 11-18 coverage hole detection configuring per controller using the CLI 6-66 using the CLI 6-65 to 6-66 coverage hole detection and correction 11-4 Coverage Hole Detection Enabled parameter 6-65 CPU Access Control Lists page 5-63 CPU Access Control Lists page 5-63 CPUs, 5500 series controllers D-5 crash files uploading using the CLI D-17 to D-18 using the GUI D-16 to D-17 Current Channel parameter 11-31 Custom Signatures page 5-115 data encryption and OfficeExtend access points 7-55 configuring using the CLI 7-4 to 7-5 using the GUI 7-3 to 7-4 described 7-3 for OfficeExtend access points 7-52 Data Encryption parameter 7-4, 7-52 Data En Sensitivity parameter 11-15 DCA Channels parameter 11-16 debug commands, sending 7-41 debug facility configuring D-43 to D-46 described D-42 to D-43 output D-44 to D-45 default enable password 7-15 default-group access point group 6-54 Default Routers parameter 12-11 Default Routers parameter 12-11 Default Routers parameter 12-15 default-group access point group 6-54 Default Routers parameter 12-16 default-group access point group 6-54 Default-group 6-54 Default-gr (DTIM). See DTIM period Deny Counters parameter 5-61 Description parameter 5-34, 8-14, 13-10 Designated Root parameter 5-59 Destination Port parameter 5-60 Detect and Report Ad-Hoc Networks parameter 5-88 device certificates downloading using the CLI 9-21 using the GUI 9-19 to 9-21 overview 9-19 using with local EAP 5-42, 5-47 DHCP configuring using the CLI 6-11 configuring using the GUI 6-10 debugging 6-12 DHCP Addr. Assignment Required parameter 6-11 DHCP Addr. Assignment Required parameter 6-14 DHCP Addr. Assignment described 5-55 example 5-55 DHCP Option 82 Remote ID Field Format parameter 5-56 DHCP Parameters page 4-40, 5-56 DHCP proxy configuring using the CLI 4-41 using the CLI 4-41 using the CLI 4-41 using the CLI 4-40 described 4-40 DHCP Scopes page 6-12 DHCP server discovery 7-7 DHCP Server IP Addr parameter 6-11 DHCP Server Override parameter 6-11 DHCP servers external 6-9 to 6-10 internal 6-9 to 6-10 internal 6-9 to 6-10 internal 6-9 diagnostic channel parameter 5-60 disabled clients, configuring a timeout 6-17 discovery request timer, configuring 7-71 distribution system ports 3-4 to 3-6 Diversity parameter 6-13 DNS IP Address parameter 7-47 DNS Servers parameter 6-13 DNS IP Address parameter 6-14 Domain name server (DNS) discovery 7-8 Download button downloading a CA4 to 3-6 Diversity parameter 6-13 DNS IP Address parameter 6-14 Domain Name parameter 6-14 Domain Nam certificate 9-23 downloading a configuration file 9-30 downloading a customized web authentication login page 10-22 downloading a device certificate 9-20 downloading a customized web authentication login page 10-22 downloading a customized web authentication login page 9-17 downloading a customized web authentication login page 10-22 downloading a customized web authentication login page 10-23 downloading a customized web authentication login page 10-24 downloading configuration files 9-29 downloading device certificates 9-20 downloading IDS signatures 5-114 downloading login banner file 9-16 Download SSL Certificate parameter 10-8 DSCP parameter 5-60 DTIM period, configuring for MAC
filtering 6-18 DTLS data encryption. See data encryption DTPC Support parameter 4-30 dynamic AP management for dynamic interface 3-21 for the management interface 3-15 Dynamic AP-management interface 3-10 dynamic interface 3-10 dynamic channel assignment (DCA) 20-MHz channelization 11-4, 11-16 configuring using the CLI 11-22 to 11-23 using the GUI 11-13 to 11-17 described 11-3 sensitivity thresholds 11-15 dynamic frequency selection 7-84 to 7-85 dynamic interface example 3-45 dynamic transmit power control, configuring 4-30 dynamic WEP, configuring 6-24 Dynamic WEP Key Index parameter 5-43 EAP-FAST Method Parameters page 5-46 EAP-FAST parameter 5-44 EAPOL-Key Max Retries parameter 5-43 EAPOL-Key Timeout parameter 5-43 EAPOL-Key Max Retries parameter 5-43 EAPOL-Key Timeout parameter 5-44 EDCA Profile parameter 5-43 EAPOL-Key Timeout parameter 5-44 EDCA Profile parameter 5-43 EAPOL-Key Timeout parameter 5-44 EDCA Profile parameter 5-44 EAPOL-Key Timeout parameter 5-43 EAPOL-Key Timeout parameter 5-44 EDCA Profile parameter 5-44 EDCA Profile parameter 5-43 EAPOL-Key Timeout parameter 5-44 EDCA Profile parameter 5-43 EAPOL-Key Timeout parameter 5-44 EDCA Profile parameter 5-45 EDCA Profile parameter 5-45 EDCA Profile parameter 5-46 EDCA Profile parameter 5-46 EDCA Profile parameter 5-46 EDCA Profile parameter 5-46 EDCA Profile parameter 5-47 EDCA Profile parameter 5-46 EDCA Profile parameter 5-47 EDCA Profile parameter 5-48 EDCA Profile parameter 5-49 EDCA Email Input parameter 10-33 Enable AP Local Authentication for Listener parameter 5-116 Enable Controller Management to be accessible from Wireless Clients parameter 2-37, 5-54 Enable Counters parameter 5-58 Enable Coverage Hole Detection parameter 11-18 Enable CPU ACL parameter 5-63 Enable Default Authentication parameter 4-27 Enable DHCP Proxy parameter 3-43 Enable EAP-FAST Authentication parameter 13-22 Enable EAP-FAST Authentication parameter 13-22 Enable IGMP Snooping parameter 4-57 Enable LEAP Authentication parameter 13-22 Enable Least Latency Controller Join parameter 7-53 Enable Link Latency parameter 7-53, 7-94, 7-95 Enable Listener parameter 4-27 Enable Low Latency MAC parameter 7-28 Enable NAT Address parameter 7-28 Enable NAT Address parameter 3-13 Enable NAT Address parameter 4-27 Enable Link Latency MAC parameter 7-52 Enable Listener parameter 7-52 Enable Listener parameter 7-53 Enable Listener parameter 7-54 Enable Listener parameter 7-54 Enable Listener parameter 7-55 Enable Listener parameter 7-56 Enable Listener parameter 7-56 Enable Listener parameter 7-58 Enable Listene 16 Enable Server Status parameter 5-36 Enable Tracking Optimization parameter 7-86 Encryption Key parameter 6-30 end user license agreement (EULA) 4-8, 4-9 enhanced distributed channel access (EDCA) parameters configuring using the GUI 4-88 to 4-89 enhanced neighbor list described 4-61, 8-31 request (E2E) 4-62 Enter Saved Permission Ticket File Name parameter 4-23 EoIP port 12-23, 12-28 epings 12-23, 12-28 epings 12-23, 12-28 epings 12-23, 12-29 erasing the controller configuration 9-34 error codes, for failed VoIP calls 6-45 to 6-46 Ethernet connection, using remotely 2-24 to 2-25 Ethernet Multicast Mode parameter 4-57 European declaration of conformity B-4 to B-5 evaluation licenses installed on 5500 series controllers 4-3 event reporting for MFP 5-69 Excessive 802.11 Authentication Failures parameter 5-76 Excessive 802.1 Expedited Bandwidth parameter 4-76 expedited bandwidth requests described 4-74 enabling using the CLI 4-84 using the GUI 4-76 Expiration Timeout for Roque AP and Roque Client Entries parameter 5-88 Extensible Authentication Protocol (EAP) configuring 6-24 setting local timers 5-48 timeout and failure counters per access point 5-51 per client 5-51 extension channel 11-31 factory default settings resetting using the GUI 4-116 failover priority for access points configuring using the CLI 7-74 to 7-74 failover protection 1-15 fake access points configuring using the CLI 7-74 to 7-74 failover protection 1-15 fake access point detection 5-128 Fallback Mode parameter 5-10 Fast Ethernet port 3-5 fast heartbeat timer configuring using the CLI 7-70 using the GUI 7-68 described 7-67 fast SSID changing configuring using the CLI 4-52 configuring using the GUI 4-52 FCC declaration of conformity B-2 to B-3 FCC statement 2100 series controllers B-10 5500 series controllers B-10 Federal Information Processing Standards (FIPS) 5-12 File Compression parameter 7-44 File Name to Save Credentials parameter 4-21 file transfers 1-14 File Type parameter downloading a CA certificate 9-23 downloading a customized web authentication login page 10-23 downloading a configuration file 9-30 downloading a customized web authentication login page 10-23 downloading a configuration file 9-30 downloading a customized web authentication login page 10-23 downloading a customized web authentication login page uploading a configuration file 9-28 uploading packet capture files D-23 uploading PACs 9-25 filter, using to view clients 7-103 Fingerprint parameter 3-31, 3-32 forwarding plane architecture 4-53 Fragmentation Threshold parameter 4-30 fragmented pings 3-7 Friendly Rogue > Create page 5-93 FTP server guidelines 9-2 General (controller) page 5-31 Generate Password parameter 10-5 Generate Password parameter Global Configuration page configuring authentication for access points 7-16 global credentials for access points 7-16 global credentials for access points 7-17 described 7-15 to 7-17 described 7-15 overriding using the CLI 7-17 using the GUI 7-16 Group Mode parameter 11-9, 12-17 Group Name parameter 12-12, 13-18 Group Setup page (on CiscoSecure ACS) 5-23 Guest LAN parameter 10-31 guest N+1 redundancy 12-20 guest tunneling 12-10 guest user accounts creating 10-2 to 10-7 creating as a lobby ambassador 10-4 to 10-6 viewing using the CLI 10-7 using the GUI 10-6 Guest User parameter 5-33, 13-10 Guest User Role parameter 5-33, 13-10 Guest WLAN, creating 10-5 GUI browsers supported 2-16 headline parameter 10-14 Hello Time parameter 3-31 help, obtaining 2-17 hex2pcap sample output D-45 high-density network benefits 11-48 example 11-48 overview 11-47 Holdtime parameter 3-31, 4-93 HOREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-22 HREAP Groups > Local Users) page 13-22 HREAP Groups > Local Users) page 13-22 HREAP Groups > Local Users) pag 13-18, 13-19 HREAP Groups page 13-18 H-REAP Local Switching parameter 13-8 H-REAP Mode AP Fast Heartbeat Timeout parameter 7-68 H-REAP Mod supported 13-2 authentication process 13-2 to 13-4 bandwidth restriction 13-2 configuring access points using the GUI 13-14 to 13-15 access points using the GUI 13-14 to 13-1 REAP groups backup RADIUS server 13-16 CCKM 13-17 configuring using the GUI 13-17 to 13-22 described 13-16 example 13-16 local authentication 13-17 to 5-81 overview 5-77 to 5-81 ldentity Request Max Retries parameter 5-43 Identity Request Timeout parameter 5-43 IDS 5-106 IDS sensors configuring using the GUI 5-118 to 5-122 viewing using the GUI 5-108 to 5-108 described 5-108 described 5-111 to 5-121 using the GUI 5-113 to 5-121 using the GUI 5-108 described 5-108 described 5-101 using the GUI 5-108 to 5-108 described 5-108 frequency 5-117 MAC frequency 5-117, 5-120 measurement interval 5-117 pattern 5-117 quiet time 5-117, 5-120 tracking method 5-117 uploading or downloading using the GUI 5-118 to 5-122 using the GUI 5-118 to 5-120 tracking method 5-117 pattern 5-10 IKE Phase 1 parameter 5-10 Index parameter for IDS 5-107 indoor access points converting to mesh access points 8-55 infrastructure MFP components 5-69 described 5-68 Infrastructure Validation parameter 5-72 Infrastructure MFP components 5-69 described 5-68 I Address parameter 7-99 inline power 7-97 Install License button 4-8 intelligent power management (IPM) 7-99 inter-controller roaming described 4-61 example 12-3 Interfaces and identity networking 5-79 assigning WLANs 6-17 configuring using the CLI 3-15 to 3-18 using the GUI 3-12 to 3-15 overview 3-6 to 3-10 Interfaces > Edit page applying an ACL to an interfaces 3-43 Interfaces Group Management Protocol (IGMP) configuring using the CLI 4-59 using the GUI 4-57 snooping 4-55 inter-subnet
mobility 12-7 inter-subnet mobility 12-8 inter Power Update Now button 11-12 IP address-to-MAC address binding configuring 4-65 described 4-65 IP Mask parameter 5-9 IP Theft or IP Reuse parameter 5-76 IPv6 bridging and IPv4 web authentication example 6-48 IPv6 Enable parameter 6-49 Japanese country codes 7-81 Japanese regulations for migrating access points from the -J to the -U regulatory domain 7-80 to 7-83 Keep Alive Encryption Key (KEK) parameter 12-22 Key Key (KE 6-30, 6-31 described 6-29 Key Permutation parameter 6-30 Key Size parameter 6-30 Key Wrap Format parameter 5-8 Key Wrap parameter 5-8 LAG. See link aggregation (LAG) LAG Mode on Next Reboot parameter 5-8 Key Wrap parameter 5-8 LAG. See link aggregation (LAG) LAG Mode on Next Reboot parameter 5-8 Key Wrap parameter 5-8 K operation 1-6 security configuring 6-23 to 6-31 described 5-3 Layer 3 Security parameter 6-27, 6-30, 6-62 Layer 3 operation 1-6 security configuring 6-32 to 6-34 described 5-3 Layer 3 Security parameter for VPN passthrough 6-33 for web authentication 6-34 for web authentication 6-34 for web authentication 6-34 described 5-3 Layer 3 Security parameter for VPN passthrough 6-33 for web authentication 6-34 described 5-3 Layer 3 Security parameter 6-27, 6-30, 6-62 Layer 3 Security parameter 5-37, 6-62 Layer 3 Security parameter 5-37, 6-62 Layer 3 Security parameter 5-37, 6-62 Layer 3 Security configuring using the CLI 5-38 to 5-40 using the GUI 5-35 to 5-38 local EAP methods supported 5-35, 5-41 LDAP server assigning to WLANs 5-37 to 5-38 choosing local authentication bind method using the CLI 5-39 using the GUI 5-36 LDAP Servers > New page 5-35 LDAP Servers > New page 5-35 LDAP Servers page 5-35 LDAP server assigning to WLANs 5-37 to 5-38 choosing local authentication bind method using the GUI 5-36 LDAP Servers > New page 5-35 LDAP Servers > New page 5-35 LDAP Servers > New page 5-35 LDAP Servers page 5-35 LDAP Servers page 5-35 LDAP server assigning to WLANs 5-37 to 5-38 choosing local authentication bind method using the GUI 5-36 LDAP Servers > New page 5-35 LDAP Servers > New page 5-35 LDAP Servers page 5-35 LDAP servers page 5-35 LDAP servers page 5-35 LDAP server assigning to WLANs 5-37 to 5-38 choosing local authentication bind method using the GUI 5-36 LDAP servers page 5-35 LDAP servers page 5-36 LDAP servers page 5-37 LDAP servers page 5-36 LDAP servers page 5-36 LDAP servers page 5-37 LDAP servers page 5-36 LDAP servers page 5-37 LDAP servers page 5-37 LDAP servers page 5-36 LDAP servers page 5-37 LDAP servers page 5-37 LDAP servers page 5-36 LDAP servers page 5-37 LDAP servers page 5-36 LDAP servers page 5-36 LDAP servers page 5-37 LDAP server Client IP Address parameter 13-9 Lease Time parameter 6-13 LEDs configuring 7-101 interpreting D-2 license agent configuration page 4-27 license agreement C-2 to C-4 License Commands (Rehost) page 4-21 License Commands page 4-7 License Detail page 4-10, 4-18 license level, changing using the CLI 4-16 using the GUI 4-15 License Level page 4-14 licenses activating ap-count evaluation licenses using the CLI 4-16 using the CLI 4-16 using the GUI 4-17 to 4-8 messages in controller trap log 4-3 obtaining 4-4 to 4-6 rehosting described 4-20 using the GUI 4-21 to 4-25 to 4-25 to 4-26 types 4-2 viewing using the CLI 4-11 to 4-13 using the GUI 4-9 to 4-10 Licenses page 4-9, 4-15, 4-17 licensing portal, using to register PAKs 4-6 Lifetime parameter 5-33, 10-5, 13-10 Lightweight Access Point Protocol (LWAPP) 1-6, 7-2 lightweight mode, reverting to autonomous mode 7-26 limited warranty C-4 to C-6 link aggregation (LAG) configuring neighboring devices 3-39 described 3-35 to 3-36 enabling using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 7-95 to 7-96 using the CLI 7-95 to 7-96 using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and 0fficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and 0fficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and 0fficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and 0fficeExtend access points 7-53, 7-55 configuring using the CLI 3-39 link latency and 0fficeE Test button 7-92 option 7-92, 8-52 to 8-53 types of packets 7-90 Link test described 7-90 performing using the GUI 7-91 to 7-92, 8-52 to 8-53 types of packets 7-90 Link Trap parameter 4-76 load-based CAC described 4-73 to 4-74 enabling using the CLI 4-83 using the GUI 4-76 lobby ambassador account creating using the CLI 10-3 creating using the GUI 10-2 to 10-3 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Users List > New page 10-4 Lobby Ambassador Guest Management > Guest Management CLI 5-47 to 5-52 using the GUI 5-42 to 5-47 debugging 5-52 described 5-40 to 5-42 example 5-41 viewing information using the CLI 5-50 Local EAP Profiles > Edit page 5-44 Local EAP Profiles > Edit page 5-44 Local EAP Profiles page 5-44 Local Management Users > New page 10-3 Local Management Users page 10-2 Local Mode AP Fast Heartbeat Timeout parameter 7-68 Local Note AP Fast Heartbeat Timer parameter 7-68 Local Net Users > New page 5-32, 10-6 local network users configuring using the GUI 5-32 to 5-34 local Net Users > New page 5-32, 10-6 local network users configuring using the GUI 7-28 to 7-30 t described 7-28 Local Significant Certificates (LSC) - AP Provisioning page 7-29 Local Significant Certificates (LSC) - General page 7-28 local user database, capacity 10-2 location appliance installing certificates 4-105 to 4-106 synchronizing with controller 4-106 location-based services 11-43 location presence 4-110 logical connectivity diagram Catalyst 3750G Integrated Services Router E-3 Cisco WiSM E-2 login banner file clearing 9-19 described 9-15 downloading using the CLI 9-17 to 9-18 using the GUI 9-16 to 9-17 Login Banner page 9-19 logs roaming D-26, D-39 to D-40 RSNA D-26, D-39 to D-41 syslog D-27, D-39 to D-41 uploading using the GUI D-17 to D-18 using the GUI 5-52 LWAPP-enabled access points debug commands 7-41 disabling the reset button 7-46 MAC addresses displayed on controller 7-41 receiving debug commands from controller 7-41 receiving access point core dumps 7-44 to 7-45 radio core dumps 7-44 to 7-45 radio core dumps 7-42 to 7-43 MAC address of access point adding to controller filter list using the GUI 8-39 displayed on controller GUI 7-45 MAC filtering, for mesh access points 8-13 to 8-14 MAC filtering page 8-13 MAC Filters > New page 8-13 management frame protection (MFP) configuring using the CLI 5-72 to 5-73 using the GUI 5-70 to 5-71 debugging 5-75 described 5-68 to 5-69 guidelines 5-69 types 5-68 viewing settings page 5-72 management frame validation 5-69 management interface configuring using the CLI 3-15 using the GUI 3-12 to 3-15 described 3-7 Management IP Address parameter 7-51 management over wireless described 5-54 enabling using the CLI 5-54 Age parameter 3-31 maximum local database entries configuring using the CLI 5-31 Configuring using the GUI 5-31 Maximum RF Usage Per AP
parameter 4-76, 4-77 Maximum RF Usage Per AP parameter 5-43 Max RF Bandwidth parameter 4-76, 4-77

MCS data rates 4-34 Member MAC Address parameters 12-12 memory types 1-14 memory leaks, monitoring D-24 to D-25 mesh network example 8-42 parameters configuring using the CLI 8-27, 8-30 configuring using the GUI 8-23 to 8-27 statistics viewing for an access point using the GUI 8-46 to 8-50 Mesh > LinkTest Results page 8-52 mesh access points adding MAC address to controller filter list using the GUI 8-13 to 8-14 adding to mesh networks 8-2 models 8-2 network access 8-5 operating with Cisco 3200 Series Mobile Access Routers configure 8-58 described 8-58 described 8-58 described 8-58 described 8-58 mesh deployment example 8-6 mesh backhaul data rates 8-10 mesh backhaul data rates 8-10 mesh backhaul data rates 8-10 mesh backhaul data rates 8-59 roles 8-38 described 8-58 described 8-58 mesh deployment example 8-6 mesh minimum required LinkSNR 8-10 mesh neighbors, parents, and children 8-8 mesh node security statistics 8-49 to 8-50 mesh node statistics 8-49 to 8-50 mesh node statistics 8-48 mesh point-to-point wireless bridging example 8-6 mesh routing 8-8 Message Authentication Code Key (MACK) parameter 5-8, 5-12 message logs configuring using the CLI D-11 to D-14 using the GUI D-8 viewing using the GUI D-10 to D-11 See also system logging Message Logs page D-11 Message parameter 5-71 MIC 6-25, 6-29 migrating access points from the -J to the -U regulatory domain 7-80 to 7-83 Min Failed Client Count per AP parameter 11-18 Minimum RSSI parameter 4-63 mirror mode. See port mirroring, configuring 6-30, 6-31 described 6-29 MMH Mode parameter 4-63 mirror mode. Mobility Anchor Config page 12-22, 12-27 Mobility Anchors page 12-22 Mobility Anchors page 12-11 Mobility Group Members > Edit All page 12-13 mobility Group Members > Edit All page 12-13 mobility Group Members > Edit All page 12-14 using the GUI 12-11 to 12-13 with one NAT device 12-8 with two NAT devices 12-9 determining when to include controllers 12-7 difference from RF groups 11-5 examples 12-7 illustrated 12-5 messaging among 12-7 number of access points supported 12-5, 12-6 number of access points supported 12-5 messaging among 12-7 number of access po group statistics types 12-16 viewing using the CLI 12-19 using the GUI 12-16 to 12-19 mobility list described 12-6 detecting failed members 12-20 Mobility Multicast Messaging > Edit page 12-14 Mobility Multicast Messaging > Edit page 12-13 mobility ping tests, running 12-28 Mobility Statistics page 12-17 MODE access point button 7-26, 7-46 Mode parameter 4-63, 11-44 monitor intervals, configuring using the GUI 11-20 mpings 12-23, 12-28 Multicast Groups page 4-58 multicast mode configuring using the CLI 4-58 using the GUI 4-57 to 4-58 described 4-55 to 4-56 guidelines 4-56 to 4-57, 7-61 Multicast page 4-57 multiple country codes configuration guidelines 7-75 configuring using the CLI 7-78 using the GUI 7-76 to 7-77 NAC in-band mode 6-66 NAC out-of-band integration and hybrid REAP 13-5 configuring using the GUI 6-72 using the GUI 6-71 to 6-72 using the GUI 6-70 NAC address for dynamic interface 3-20, 3-21 for management interface 3-13, 3-16 NAT devices in mobility groups 12-8 to 12-9 Native VLAN ID parameter 13-13 neighbor information option 8-51 to 8-54 Neighbor Information option 8-51 Neighbor Packet Frequency parameter 11-20 neighbor statistics viewing for an access point using the GUI 8-54 viewing for an access point using the GUI 8-51 to 8-54 Netbios Name Servers parameter 6-13 network Mobility Services Protocol (NMSP) 4-101 debugging 4-113 to 4-114 modifying the notification interval for clients, RFID tags, and rogues 4-110 to 4-111 viewing settings 4-111 to 4-113 Network parameter 7-29 Number of Hits parameter 5-61 OfficeExtend Access Point Configuration page 7-57 OfficeExtend Access Point Home page 7-56 OfficeExtend Access Points LEDs D-53 to 7-58 using the CLI 7-54 to 7-50 licensing D-53 to D-54 officeExtend access points and NAT 7-50 configuring a personal SSID 7-56 to 7-58 using the CLI 7-54 to 7-50 licensing requirements 7-50 licensing requirements 7-50 licensing requirements 7-50 licensing requirements 7-50 using the CLI 7-54 to 7-58 using the CLI 7-54 to 7-58 using the CLI 7-54 to 7-58 using the CLI 7-54 to 7-50 licensing requirements 7-50 licensing requirements 7-50 licensing requirements 7-50 using the CLI 7-54 to 7-58 using the CLI 7-59 using the CLI 7-58 using the CLI 7-59 using the CLI 7-58 using supported access point models 7-50 trap logs 7-50 trap logs 7-50 typical setup 7-49 viewing statistics 7-58 to 7-60 OfficeExtend AP parameter 7-53 online help, using 2-17 open source terms C-8 OpenSSL license issues C-7 to C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 5-11, 5-26 Override Global Config parameter 10-26, 10-33 Over-ride Global Credentials parameter 7-17, 7-21, 7-53 Override Interface ACL parameter 5-64 oversized access point images 7-49 over-the-air provisioning (OTAP) 7-7 P2P Blocking parameter 6-22 packet capture files described D-21 sample output in Wireshark D-22 uploading using the CLI D-23 to D-24 using the GUI D-23 Params parameter 7-29 password restoring 4-42 password guidelines 7-20 for access points 7-16 for local net users 5-33, 13-10 for PACs 9-25 passwords viewing in clear text D-7 path loss measurement (S60), CLI command 4-106 PEAP parameter 5-44 peer-to-peer blocking configuring using the CLI 6-23 using the GUI 6-21 to 6-23 described 6-20 examples 6-21, 6-67 permanent licenses, installed on 5500 series controllers 4-3 Personal SSID parameter 3-24 pico cell mode configuring using the CLI 11-50 to 11-51 using the GUI 11-49 to 11-50 debugging using the CLI 11-51 guidelines 11-48 overview 11-47 to 11-48 versions 11-49 Pico Cell Mode parameter 7-99 Pool End Address parameter 6-13 Pool Start Address parameter 6-13 Port > Configure page 3-23 port mirroring, configuring 3-26 to 3-27 Port Number parameter for controllers 3-24 for LDAP server 5-36 for RADIUS server 5-36 for TACACS+ server 5-25 for wired guest access 10-31 Port parameter for IDS 5-107 ports configuring 3-22 to 3-33 on 2100 series controllers 3-2, 3-4 on 5500 series controllers 3-2, 3-4 on 5500 series controllers 3-3, 3-5 on Catalyst 3750G Integrated Wireless LAN Controller Switch 3-3, 3-4, 3-5 on Cisco 28/37/38xx Series Integrated Services Router 3-4 to 3-5, 4-116, 7-35 on Cisco WiSM 3-4, 3-5 overview 3-2 to 3-6 Ports page 3-22 Power Assignment Leader parameter 11-12 power cable warning for Japan B-7 Power Injector Selection parameter 7-99 Power Injector State parameter 7-99 Power Neighbor Count parameter 11-12 Power over Ethernet (PoE) configuring using the CLI 5-67 using the GUI 5-64 to 5-65 for external web server 10-20, 13-9 Preauthentication ACL parameter 5-65, 6-63 Pre-Standard State parameter 7-51 Primary Controller Name parameter 7-51, 7-69 Primary Control Priority parameter 3-31 Privacy Protocol parameter 4-46 probe requests, described 7-88 product ID for controller, finding 4-22 Product ID for controller, finding 4-22 Product ID for controller, finding 4-22 Product ID for controller, finding 4-24 D-35 Profile Name parameter 6-5, 8-14, 10-31, 13-7 protected access credentials (PACs) overview 9-24 uploading using the CLI 9-26 to 9-27 using the GUI 9-25 using with local EAP 5-42, 13-22 Protection Type parameter 5-70, 11-37 Protocol parameter 5 Format parameter 6-27 public key cryptography (PKC), with mobility 12-7 QBSS configuring using the GUI 6-36 to 6-37 configuring using the GUI 6-36 to 6-37 configuring to a WLAN using the GUI 6-37 using the GUI 6-37 configuring using the GUI 6-37 co using the CLI 4-68 to 4-69 using the GUI 4-66 to 4-68 QoS roles assigning for use with hybrid REAP 13-10 configuring using the CLI 4-71 to 4-72 using the GUI 4-69 to 4-71 QoS Roles for Guest Users page 4-70 Quality of Service (QoS) parameter 6-36 quarantined VLAN configuring 3-13, 3-19 using 13-8 with hybrid REAP 13-4 with NAC out-of-band integration 6-69 Quarantine parameter for dynamic interface 3-19 NAC out-of-band integration 6-69 Query Interval parameter 5-108 Queue Depth p configuring on the CLI 11-45 on the GUI 11-44 overview 11-43 viewing status using the CLI 11-21 to 11-24 using the GUI 11-10 to 11-21 coverage hole detection configuring per controller using the CLI
11-23 configuring per controller using the GUI 11-17 to 11-19 described 11-4 debugging 11-26 disabling dynamic channel and power assignment using the CLI 11-35 to 11-36 using the GUI 11-35 to 11-36 using the transmit power settings using the CLI 11-32 using the GUI 11-28 to 11-32 update interval 11-7, 11-10 Wireless > 802.11a/n (or 802.11b/g/n) > RRM > TPC parameter 11-11 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using authentication priority order 5-11 configuring using the CLI 5-11 to 5-15 using the GUI 5-6 to 5-11 configuring on ACS 5-4 described 5-3 FIPS standard 5-12 KEK parameter 5-12 server fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 RADIUS > Fallback Parameters page 5-10 RADIUS accounting attributes 5-18 to 5-18 to 5-18 to 5-18 to 5-10 reserver fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 RADIUS > Fallback Parameters page 5-10 RADIUS accounting attributes 5-18 to 5-18 to 5-18 to 5-10 reserver fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 RADIUS > Fallback Parameters page 5-10 RADIUS accounting attributes 5-18 to 5-18 to 5-18 to 5-10 reserver fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 RADIUS > Fallback Parameters page 5-10 RADIUS accounting attributes 5-18 to 5-18 to 5-18 to 5-10 reserver fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 RADIUS > Fallback Parameters page 5-10 RADIUS accounting attributes 5-18 to 5-18 to 5-10 reserver fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 RADIUS > Fallback Parameters page 5-10 RADIUS accounting attributes 5-18 to 5-18 to 5-19 to 5-10 reserver fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 reserver fallback behavior 5-10 reserver fallback beha 19 RADIUS authentication attributes 5-16 to 5-18 Range (RootAP to MeshAP) parameter 8-24 Redirect URL After Login parameter 10-14 Refresh-time Interval parameter 10-14 Refresh-time Interval parameter 8-24 Redirect URL After Login parameter 10-14 Refresh-time Interval parameter 8-24 Redirect URL After Login parameter 10-14 Refresh-time Interval parameter 8-24 Redirect URL After Login parameter 8-24 Redir license. See licenses Rehost Ticket File Name parameter 5-43 Reguest Timeout parameter 5-43 Reguest Max Retries parameter 5-43 Reserved Roaming Bandwidth parameter 5-4 passwords 4-42 Re-sync button 5-110 reverse path filtering (RPF) 12-26 RF Channel Assignment parameter 11-35 RF domain. See RF groups RF exposure declaration of conformity B-5 RF groups RF exposure declaration of conformity B-5 RF groups RF exposure declaration of conformity B-5 RF groups cascading 11-6 viewing 11-8 RF groups cascading 11-6 viewing 11-8 RF groups RF exposure declaration of conformity B-5 RF e 7 difference from mobility groups 11-5 to 11-7 pinning 11-6 viewing status using the CLI 4-101 tracking configuring using the CLI 4-102 debugging using the CLI 4-104 viewing information using the CLI 4-103 to 4-104 RFID tracking on access points, optimizing using the GUI 7-85 to 7-86 RF-Network Name parameter 11-8 RLDP. See Rogue Location Discovery Protocol (RLDP) roaming and real-time diagnostics configuring using the CLI D-39 to D-42 described D-26 logs descri described 8-32 rogue access points alarm 11-37 automatically containing using the CLI 5-89 using the GUI 5-88 classification mapping table 5-85 classifying 5-84 configuring RLDP 5-87 to 5-90 detecting using the CLI 11-38 using the GUI 11-36 to 11-38 managing 5-83 rule-based classification support 5-84 tagging, location, and containment 5-84 viewing and classifying using the GUI 5-96 to 5-101 wCS support for rule-based classification 5-87 Rogue AP Ignore-List page 5-97 Rogue AP Ignore-List page and OfficeExtend access points 7-52, 7-55 Roque Detection parameter 5-87, 7-52 Roque Location Discovery Protocol (RLDP) configuring using the GUI 5-88 to 5-90 using the GUI 5-88 to 5-90 using the GUI 5-87 to 5-88 defined 5-84 Roque Location Discovery Protocol parameter 5-88 Roque and OfficeExtend access points 7-52, 7-55 Roque Detection parameter 5-87, 7-52 Roque Location Discovery Protocol (RLDP) configuring using the GUI 5-88 to 5-90 using the GUI Rules > Priority page 5-93 rogue states 5-85, 5-86 Role Name parameter 3-30 Root Port 11-50 Save and Reboot button 9-21, 9-23 Save Licenses button 4-8 saving configuration settings 9-32 Scan Threshold parameter 4-63 Scope Name parameter 4-63 Scope Name parameter 4-63 Scope Name parameter 13-18 secure web mode described 2-18 enabling using the CLI 2-19 using the GUI 2-18 security overview 5-2 solutions 5-2 to 5-3 Security Policy Completed parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security end to authorize access points 7-27 Sequenceed parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Controller parameter 6-48 security settings local and external authentication 8-23 Select APs from Current Current APs from Cur parameter 5-59 serial number for controller, finding 4-24 serial number of controller, finding 4-22 serial port baud rate setting 2-24 timeout 2-24 Server IP Address parameter 5-8, 5-25, 5-36 Server 49 Server Key parameter 5-46, 13-22 Server Status parameter 5-9, 5-25 Server Timeout parameter 5-9, 5-26, 5-37 service port 3-6 service-port interface configuring using the CLI 6-32 using the CLI 6-31 described 6-31 Set to Factory Default button 11-21 Severity Level Filtering parameter 5-8, 5-25 Short Preamble 5-52 118 Signature Events Summary page 5-118 Signature Events Track Detail page 5-119 Simple Bind parameter 5-36 sniffing. See wireless sniffing D-47 Sniff parameter D-49 SNMP, configuring 4-42 to 4-43 SNMP v1 / v2c Community > New page 4-44 SNMP v1 / v2c Community page 4-45 software, upgrading guidelines 9-2 to 9-4 using the CLI 9-9 to 9-11 using the GUI 9-6 to 9-8 software, upgrading in mesh networks guidelines 9-4 to 9-6 Source parameter for ACLs 5-59 Source Port parameter 3-30 SpectraLink parameter 3-30 SpectraLink NetLink phones enabling long preambles using the CLI 5-53 using the GUI 5-52 overview 5-52 Spectralink Voice Priority parameter 6-63 SSC key-hash on Cisco WiSM 7-26 SSH and OfficeExtend access points 7-53, 7-55 configuring using the GUI 2-36 to 2-35 troubleshooting access points using the CLI D-51 to D-52 using the GUI D-50 to D-51 SSID configuring using the CLI 2-21 to 2-22 using the GUI 6-3 SSL certificate loading using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI
7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-22 using the GUI 7-20 to 2-21 SSLv2, configuring using the CLI 2-21 to 2-21 SSLv2, configuring using the CLI 7-20 to 2-20 to Standard Signature > Detail page 5-117 Standard Signatures page 5-115 stateful DHCPv6 IP addressing 6-47 State parameter 5-108, 5-118 static IP parameter 7-47 described 7-46 to 7-47 described 7-46 to 7-47 described 7-46 to 7-47 state parameter 5-108, 5-118 static IP addressing 6-47 State parameter 5-108, 5-118 state parameter 5-108, 5-118 state parameter 5-108, 5-118 state parameter 5-108, 5-1 DHCP scopes 6-14 for guest LANs 10-32 for SNMP community 4-44 for WLANs 6-6 STP Port Designated Port parameter 3-28 STP Port Designated Port parameter 3-28 STP Port Designated Root parameter 3-28 STP Port Designated Port D parameter 3-28 STP Port Path Cost Mode parameter 3-29 STP Port Path Cost parameter 3-29 STP Port Path Cost parameter 3-29 STP State parameter 3-29 SX/LC/T small form-factor plug-in (SFP) modules 3-5 symmetric mobility tunneling illustrated 12-27 overview 12-26 to 12-27 syslog facility parameter D-9 to D-41 Syslog Configuration page D-8 Syslog Facility parameter D-9 syslog server number supported by controller D-8 removing from controller D-8 system logging configuring using the CLI D-11 to D-14 using the GUI D-8 to D-10 system Resource Information page D-5 system resources viewing using the GUI D-5 TACACS+ accounting 5-20 to 5-24 to 5-26 configuring on ACS 5-20 to 5-24 described 5-19 to 5-20 roles 5-19, 5-23 viewing using the GUI D-5 TACACS+ accounting 5-20 authentication 5-19 authorization 5-19 authorization 5-19 authorization 5-19 authorization 5-19 authorization 5-19 authorization 5-20 to 5-20 to 5-20 to 5-20 to 5-20 to 5-20 to 5-20 roles 5-19, 5-23 viewing using the GUI D-5 TACACS+ accounting 5-20 to administration server logs 5-29 to 5-30 TACACS+ (Authentication, Authorization, or Accounting) Servers page 5-25 TACACS+ (Authentication, Authorization, or Accounting) Servers page 5-24 TACACS+ (Cisco) page (on CiscoSecure ACS) 5-22 TACACS+ Administration.csv page (on CiscoSecure ACS) 5-29, 5-30 TCP MSS configuring 7-96 to 7-97 described 7-96 telemetry 4-100 Telnet and OfficeExtend access points 7-53, 7-55 troubleshooting access points using the GUI 2-35 to 2-36 using the GUI 2-34 to 2-35 Telnet-SSH Configuration page 2-34 Tertiary Controller parameters 7-69 text2pcap sample output D-45 TFTP server guidelines 9-2 time, configuring using the CLI 2-32 using the GUI 2-30 using the GUI 2-30 time-length-values (TLVs), supported for CDP 4-90 to 4-92 timeout, configuring for disabled clients 6-17 Time Since Topology Changed parameter 3-30 timestamps, enabling or disabled grant debug messages D-14 Time to Live for the PAC parameter 5-46, 13-22 time zone configuring using the CLI 2-32 configuring using the GUI 2-31 TKIP configuring using the GUI 2-31 TKIP configuring 6-27, 6-28 described 6-25 parameter 3-30 traffic specifications (TSPEC) request described 4-74 examples 4-74 traffic stream metrics (TSM) configuring using the CLI 4-84 using the GUI 4-76 described 4-75 viewing statistics using the CLI 4-86 to 4-87 using the GUI 4-80 to 4-83 Transfer Mode parameter downloading a configuration file 9-30 downloading a configuration file 9 software 9-8 uploading a configuration file 9-28 uploading a PAC 9-25 uploading packet capture files D-23 Transmit power statically assigning using the GUI 11-32 transmit power levels 11-31 Transmit Power parameter 11-50 transmit power threshold, decreasing 11-21 trap logs for OfficeExtend access points 7-50 Trap Logs page 4-3, 6-43 troubleshooting access point join process 7-34 to 7-41 CCXv5 clients D-26 to D-42 problems D-6 to D-8 tunnel attributes and identity networking 5-80 to 5-81 Tx Power Level Assignment parameter 11-35 Type parameter 6-5, 10-31, 13-7 U-APSD described 4-75 viewing status using the CLI 4-86 using the GUI 4-79 UDP, use in RADIUS 5-4 UDP port 12-23, 12-28 unicast mode 4-55 unique device identifier (UDI) described 7-89 retrieving using the CLI 7-90 using the CLI 7-89 to 7-90 Upload button 5-115, 7-43, 9-26, D-17, D-23 UPL parameter 10-21 URL to Send the Notifications parameter 5-7 User Access Mode parameter 5-36 User Credentials parameter 5-37 User Name parameter 5-33, 13-10 Username parameter 5-88 Validate Rogue Clients Against AAA parameter 5-88 Valid Client on Rogue AP parameter 5-88 Validate Rogue Clients Against AAA parameter 5-88 Validate Rogue Clients Ag 34 Verify Certificate CN Identity parameter 5-45 video information, viewing for mesh networks using the CLI 4-85 to 4-87 using the GUI 4-76 to 4-78 video settings configuring using the CLI 3-17 using the GUI 3-12 to 3-15 described 3-9 VLAN Identifier parameter for AP-manager interface 3-14 for dynamic interface 3-19, 3-20 VLAN ID parameter 6-68, 13-14 VLAN interface. See dynamic interface 3-19 VLAN support parameter 13-13 VLAN support parameter 13-13 VLAN interface 3-19, 3-20 VLAN ID parameter 6-68, 13-14 VLAN interface 3-19, 3-20 VLAN ID parameter 6-68, 13-14 VLAN interface 3-19, 3-20 VLAN interface 3-10 VLAN interface 3-10 VLAN interface 3-19, 3-20 VLAN interface 3-10 VLAN interface 3-10 VLAN interface 3-19, 3-20 VLAN interface 3-10 VLAN interface 3-10 VLAN interface 3-19, 3-20 VLAN int 4-88 voice information, viewing for mesh networks using the CLI 8-42 to 8-44 Voice Optimized parameter 4-88 voice-over-IP (VoIP) telephone roaming 4-61 Voice RSSI parameter 11-18 voice settings configuring using the CLI 4-83 to 4-84 using the CLI 4-83 to 4-84 using the CLI 4-83 to 4-84 using the CLI 4-85 to 4-87 using the CLI 4-85 to 4-87 using the CLI 4-83 to 4-84 using the CLI 4-85 to 4-87 using the CLI 4-85 to 4-86 using the CLI 4-85 to 4-86 using the CLI 4-85 to 4-86 using the CLI 4-85 to 4-87 using the CLI 4-85 to 4-86 using the CLI 4-85 to 4-87 using the CLI 4-88 using the CLI 4-85 to 4-87 using the CLI 4-85 to 4-87 using the CLI 4-88 using the CLI 4-6-45 to 6-46 VoIP snooping configuring using the CLI 6-44 to 6-47 using the GUI 6-42 to 6-42 t bundle 10-22 web authentication certificate obtaining using the GUI 10-7 to 10-9 configuring a WLAN for using the GUI 10-7 to 10-9 configuring page assigning per WLAN using the CLI 10-27 using the GUI 10-26 choosing the GUI 10-15 to 10-15 to 10-15 to 10-15 to 10-15 to 10-21 using the GUI 10-22 to 10-23 to 10-22 to 10-23 to 10-21 default 10-12 downloading a customized login page guidelines 10-22 using the GUI 10-24 using the GUI 10-22 to 10-23 to 10-23 to 10-23 to 10-24 using the GUI 10-24 using the GUI 10-20 to 10-24 using the GUI 10-20 to 10-24 using the GUI 10-24 using t modified default example 10-17 previewing 10-15, 10-23 Web Authentication Type parameter 10-26, 10-33 web-browser security alert 10-14, 10-20, 10-32 Web Authentication Type parameter 10-26, 10-33 web-browser security alert 10-14, 10-20 web mode configuring using the CLI 2-19 using the GUI 2-18 described 2-18 Web Passthrough option 10-32 Web Policy parameter 5-65, 6-34, 6-63 web redirect 6-60 Web Server IP Address parameter 7-64 WGB Wired Clients page 7-64 wired quest access configuration overview 10-30 configuring using the CLI 10-33 to 10-39 using the GUI 10-31 to 10-33 described 10-28 to 10-30 guidelines 10-30 one-controller example 10-29 two-controller example 10-30 wireless intrusion prevention 5-125 to 5-126 described 5-123 viewing information 5-126 to 5-126 described 5-128 viewing information 5-126 to 5-128 viewing information 5-126 to 5-128 viewing information 5-128 vi 49 prerequisites D-47 supported software D-47 WLAN ID parameter 6-5 WLAN mobility security values 12-25 WLAN override 9-2 WLAN profile parameter 5-34, 13-10 WLANs assigning web login, login failure, and logout pages using the CLI 10-27 using the GUI 10-26 checking security settings 6-24 configuring conditional web redirect 6-61 to 6-64 static and dynamic WEP 6-24 connecting clients to 13-15 creating using the CLI 6-6 using the GUI 6-6 deleting using the CLI 6-7 using the GUI 6-6 deleting using the CLI 6-7 using the GUI 6-5 described 1-13, 3-10 to 3-12, 6-3 to 6-4 enabling or disabling using the CLI 6-7 using the GUI 6-6 deleting using the CLI 6-7 using the GUI 6-5 described 1-13, 3-10 to 3-12, 6-3 to 6-4 enabling or disabling using the CLI 6-7 using the GUI 6-5 described 1-13, 3-10 to 3-12, 6-3 to 6-4 enabling using the CLI 6-7 using the GUI 6-7 using the GUI 6-5 described 1-13, 3-10 to 3-12, 6-3 to 6-4 enabling using the CLI 6-7 using the GUI 6-8 escribed 1-13, 3-10 to 3-12, 6-3 to 6-4 enabling using the CLI 6-8 using the GUI 6-7 using the GUI 6-8 escribed 1-13, 3-10 to 3-12, 6-3 to 6-4 enabling using the GUI 6-7 using the GUI 6-8 escribed 1-13, 3-10 to 3-12, 6-3 to 6-4 enabling using the GUI 6-7 using the GUI 6 security solution 1-5 WLANs > Edit (Advanced) page 6-42, 6-65 applying an ACL to a WLAN 5-64 configuring IPv6 bridging 6-49 configuring IPv6 bridging 6-49 configuring infrastructure MFP for a WLANs > Edit (Security solution 1-5 WLANs > Edit (Advanced) page 6-39 WLANs > Edit (Security solution 1-5 WLANs > Edit (Advanced) page 6-49 configuring IPv6 bridging 1-49 configuri ing LDAP servers to a WLAN 5-38 choosing RADIUS or LDAP servers for external authentication 10-26 disabling accounting servers on a WLAN 5-47 WLANs > Edit (Security > Layer 2) page 6-27, 6-30 WLANs > Edit (Security > Layer 3) page applying a WLAN 5-64 configuring a WLAN for VPN Passthrough 6-33 configuring web redirect 6-63 configuring wired guest access 10-32 WLANs > Edit page
6-5, 10-31, 13-7 WLANs page 6-5, 10-31, 13-7 WLANs > Rew page 6-5, 10-31, 13-7 WLANs > Edit page 6-5, 10-31, 13-7 WLANs > Rew page 6-5, 10-31, 13-7 WLANs page 6-4, 12-22 WLAN SSID parameter configuring for guest user 10-5 creating a centrally switched WLAN 13-7 creating WLANs 6-5 identifying the guest LAN 10-31 mapping an access point group to a WLAN 6-56, 6-71 WMM configuring 4-35, 6-39, 6-41 described 7-60 guidelines 7-61 illustrated 7-49, 7-52, 7-57, 7-60 sample configuration 7-63 viewing status using the CLI 7-66 using the GUI 7-65 world mode 4-30, 4-32 WPA1+WPA2 configuring using the CLI 6-27 wplus licenses wplus software set, included features 4-2 11n Mode parameter 4-34 1250 series access points and PoE Status field 7-99 operating modes when using PoE 7-97 3DES IPSec data encryption 5-9 7920 AP CAC parameter 6-39 7920 support mode configuring 6-38 described 6-38 7921 support mode 6-38 802.11a (or 802.11b) > Client Roaming page 4-62 802.11a (or 802.11b) > Video Parameters page 4-77 802.11a (or 802.11b/g) > EDCA Parameters page 4-75 802.11a (or 802.11b/g) Slobal Parameters page 4-29, 11-44 802.11a (or 802.11b/g) Network Status parameters 4-30, 4-38, 4-39 802.11a/n (4.9 GHz) > Configure page 8-59 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page 11-29 802.11a/n Radios page (from Wireless Menu) 7-13 802.11a/n Radios page (from Worless Menu) 7-13 802.11a/n Radios page (from Wireless Menu) 7-13 802.11a/n Radios page (from Wireless Menu) 7-13 802.11a/n Radios page (from Wireless Menu) 7-14 802.11a/n Radios page (from Wireless Menu) 7-13 802.11a/n Radios page (from Wireless Menu) 7-14 802.11a/n Radios page (from Wireless Menu) 7-14 802.11a/n Radios page (from Wireless Menu) 7-13 802.11a/n Radios page (from Wireless Menu) 7-13 802.11a/n Radios page (from Wireless Menu) 7-14 802.11a/n Radios pa parameters 11-49 802.11a > RRM > DcA page 11-14 802.11a > RRM 802.11 bands configuring using the CLI 4-31 to 4-33 configuring using the GUI 4-29 to 4-31 802.11h, described 4-38 802.11h, described 4-38 802.11h, described 4-38 to 4-39 solution and the GUI 4-39 to 4-31 solution and the GUI 4-39 to 4-38 solution and the GUI 4-38 to 4-39 solution and the GUI 4-38 to 4-38 solution and the GUI 4-38 to 4-38 solution and the GUI 4-38 to 4-39 solution and the GUI 4-38 to 4-38 4-38 t 4-35 devices 4-33 802.11n (2.4 GHz) High Throughput page 4-34 802.1Q VLAN trunk port 3-6 802.1X configuring 6-24 described 6-25 dynamic key settings 6-24 802.1X authentication for access points configuring the switch 7-23 using the GUI 7-19 to 7-21 described 7-18 802.1x Authentication parameter 7-20 802.3 bridging configuring using the CLI 4-54 configuring using the GUI 4-53 to 4-54 802.3 Frames 4-53 802.3X flow control, enabling 4-52 AAA override configuring using the CLI 5-83 using the GUI 5-83 described 5-81 AC adapter warning for Japan B-7 Access Control List Name parameter 5-59 access control lists (ACLs) applying to an interface using the GUI 5-67 us D-44 counters configuring using the CLI 5-65 configuring using the GUI 5-58 described 5-57, 5-59, 5-66 using with the debug facility D-42 to D-43 Access Control Lists > Rev page 5-58 Access Control Lists > Rev page 5-59 Access Control Lists > Rev page 5-58 Access Contro parameter 4-44, 4-46 access point core dumps, uploading using the CLI 6-57 to 6-59 using the CLI 6-57 to 6-59 using the GUI 6-54 to 6-57 to 6-59 using the GUI 6-57 to 6-59 using the GUI 6-57 to 6-59 using the GUI 6-54 to 6-57 default group 6-54 described 6-52 illustrated 6-53 removing using the CLI 6-58 using the GUI 6-58 using the GUI 6-59 to 6-60 access point monitor service, debugging D-52 access point adios, searching for 7-13 to 7-14 access point adios, searching for 7-13 to 7-14 access point adios, searching for 7-14 access point adios, searchi LSCs 7-28 to 7-32 using MICs 7-27 using SSCs 7-27 using the CLI 7-33 using the GUI 7-32 configuring hybrid REAP using the CLI 13-14 to 13-15 converting in Japan B-6, B-7 LEDs configuring 7-101 interpreting D-2 migrating from the -J regulatory domain to the -U regulatory domain 7-80 to 7-83 number supported per controller 3-5 priming 7-7 regulatory information B-2 to B-10 rules for operating in Taiwan B-8 to B-9 searching for 7-10 to 7-13 supported for use with hybrid REAP 13-2 supporting oversized images 7-34 to 7-49 troubleshooting the join process 7-34 to 7-41 using Telnet or SSH D-50 to D-52 VCI strings 7-34 verifying that they join the controller 7-9 viewing join information using the CLI 7-39 to 7-41 using the GUI 7-36 to 7-39 viewing multicast client table 4-60 Accounting servers, disabling per WLAN 6-64 ACL. See access control lists (ACLs) ACL Name parameters 5-62, 5-63 ACS server configuration page 6-62 Action parameter 5-61 active exploits 5-128 Add AAA Client page (on CiscoSecure ACS) 5-5, 5-21 Add AP button 13-18 Add New Rule button 5-59 Add Web Server button 10-21 AdHoc Rogue AP parameter 5-88 administrator access 4-41 administrator usernames and passwords, configuring 4-41 Admin Status parameter 3-24, 3-25 Admission Control (ACM) parameter 4-76, 4-77 AES CBS IPSec data encryption 5-9 AES-CCMP 6-25 AES parameter 6-27 Aggregated MAC Protocol Data Unit (A-MPDU) 4-36 aggregation method, specifying 4-36 aggregation method, specifying 4-36 aggregated MAC Protocol Data Unit (A-MPDU) 4-36 aggregated MAC configuring using the CLI 6-52 configuring using the GUI 6-50 Airopeek D-47 Alarm Trigger Threshold parameter 11-37 All APs > Access Point Name > Mesh Neighbor Stats page 8-53 All APs > Access Point Name > Neighbor Info page 8-53 All APs > Access Point Name > Mesh Neighbor Stats page 8-53 All APs > Access Statistics page 8-47 All APs > Access Point Name > VLAN Mappings page 13-13 All APs > Details (Advanced) page 7-4, 7-44, D-51 configuring country codes 7-77 configuring link latency 7-94 configuring PoE 7-98 All APs > Details for (Credentials) page 7-16, 7-20, 7-53 All APs > Details for (Advanced) page 7-4, 7-44, D-51 configuring country codes 7-77 configuring link latency 7-94 configuring PoE 7-98 All APs > Details for (Credentials) page 7-16, 7-20, 7-53 All APs > Details for (General) page 7-47, 7-51, 13-12 All APs > Details for (High Availability) page 7-51, 7-69, 7-73 All APs > Details for (H-REAP) page 7-52, 13-12 All APs > Details for (H-REAP parameter 11-15 anonymous local authentication bind method 5-36, 5-39 Anonymous Provision
parameter 11-30 AP > Clients > Traffic Stream Metrics page 4-82 AP > Clients > Traff Authentication Policy page 5-70, 11-37 AP Core Dump parameter 7-44 ap-count licenses, activating using the CLI 4-19 to 4-20 using the GUI 4-17 to 4-19 ap-count licenses AP Ethernet MAC Addresses parameter 7-73 AP Groups > Edit (APs) page 6-57 AP Groups > Edit (General) page 6-56 AP Groups > Edit (WLANs) page 6-56, 6-71 AP Groups page 6-54, 6-70 AP Join Stats Detail page 7-39 AP Join Stats Detail page 7-39 AP Join Stats page 7-37 AP-manager interfaces 3-10 configuring using the GUI 3-42 to 3-15 creating multiple interfaces using the GUI 3-42 to 3-10 configuring using the GUI 3-42 to 3-10 configuring using the GUI 3-12 to 3-10 configuring using the GUI 3-42 to 3-10 configuring using the 43 described 3-8 illustration of four AP-manager interfaces 3-42 of three AP-manager interfaces 3-42 of three AP-manager interfaces 3-40 using multiple 3-39 to 3-44 AP Node parameter 7-51, 11-37, 13-12, D-48 AP Name parameter 7-51, 11-37, 13-12, D-48 AP Name parameter 6-57 AP Policies page 7-32 AP Primary Discovery Timeout parameter 7-51, 11-37, 13-12, D-48 AP Name parameter 7-51, 13-12, D-48 AP Name parameter 11-29, 11-31 asymmetric tunneling described 12-26 illustrated 12-26 authentication bind method 5-36, 5-39 Authentication Protocol parameter 5-46, 13-22, 13-23 Authority ID parameter 5-46, 13-22 Authority ID Information parameter 5-46, 13-22 Authority ID Information parameter 5-46, 13-22 Authority ID parameter 5-46, 13-22 Authority ID Information parameter 5-46, 13-22 Authority ID paramete 32 Authorize MIC APs against auth-list or AAA parameter 7-32 auto-immune feature 5-109 AutoInstall described 2-26, 2-29 example operation 2-29 guidelines 12-21 to 12-23 to 12-24 using the CLI obtaining DHCP addresses for interfaces 2-27 TFTP server information 2-27 overview 2-26 selecting configuration file 2-28 using 2-26 Average Data Rate parameter 4-67, 4-71 Avoid Cisco AP Load parameter 4-67, 4-71 Avoid Cisco AP Load parameter 4-67, 4-70 Average Data Rate parameter 4-67, 4-71 Avoid Cisco AP Load parameter 4-67, 4-70 Average Data Rate parameter 4-67, 4-70 Average Data Rate parameter 4-67, 4-71 Avoid Cisco AP Load parameter 4-67, 4-70 Average Data Rate parameter 4-67 parameter 11-15 Backhaul Client Access parameter 8-59 back-up Primary Controllers configuring using the CLI 7-70 to 7-72 using the GUI 7-68 Back-up Primary Controller IP Address parameter 7-69 Back-up Primary Controller Primary Controller IP Address parameter 7-69 Back-up Primary Controller IP Ad Name parameter 7-69 band selection 4-49 bandwidth-based CAC described 4-73 enabling using the GUI 4-76 for mesh networks 8-40 base licenses. See licenses Base MAC Address parameter 3-30 Beacon Period parameter 3-30 Beacon Period parameter 4-30 beamforming configuring using the GUI 11-41 to 11-42 using the GUI 11-40 to 11-41 described 11-39 guidelines 11-39 Beamforming parameter 11-40, 11-41 Bind Password parameter 5-36 Bind Username parameter 5-36 Bind ge Data Rate para 16 Buffered Log Level parameter D-10 Burst Data Rate parameter 4-67, 4-71 Burst Real-Time Rate parameter 4-67, 4-71 CAC configuring for 7920 phones 6-38 described 4-73 enabling using the CLI 4-85 Canadian compliance statement B-3 CAPWAP and mesh access points 8-8 cascading 11-6 CA Server URL parameter 7-28 Catalyst 3750G Integrated Wireless LAN Controller Switch described 6-25 hybrid-REAP groups 13-17 with mobility 12-7 CCX configuring Aironet IEs using the CLI 6-52 using the GUI 6-50 described 6-49 link test 7-90 viewing a client's version using the CLI 6-52 using the GUI 6-50 to 6-51 CCX Layer 2 client roaming configuring using the CLI 4-64 debugging using the CLI 4-64 described 4-61 to 4-62 obtaining information using the CLI 4-64 CCX radio management configuring using the CLI 11-45 to 11-45 debugging using the CLI 11-45 debugging using the CLI 11-45 to 11-45 debugging using the CLI 11-46 to 11-47 CCXv5 clients enabling location presence 4-110 troubleshooting D-26 to D-42 CCXv5 Req button D-42 CCXv5 Req button D-42 CCXv5 Req button D-42 CCXv5 clients enabling location presence 4-10 troubleshooting D-26 to D-42 CCXv5 Req button D-42 CCXv5 clients enabling location presence 4-10 troubleshooting D-26 to D-42 CCXv5 Req button D-42 CCXv5 Req button D-42 CCXv5 clients enabling location presence 4-10 troubleshooting D-26 to D-42 CCXv5 Req button D-42 CCXv 33 CCX Version parameter 6-51 CDP > AP Neighbors > Detail page 4-95 CDP > Interface Neighbors page 4-95 CDP > Interface Neighbors page 4-96 CDP > Interface Neighbors page 4-95 CDP > Interface Neighbors page 4-96 CDP > Interface Neighbors page 4-9 Status parameter 4-93 CDP State parameter 4-94 Certificate Authority (CA) certificate Basword parameter 9-20, 10-9 State parameter 10-8 Certificate File Path parameter 10-8 Certificate Issuer parameter 5-45 Certificate Password parameter 9-20, 10-9 Certificate Type parameter 7-33 Change Filter link 7-10, 7-14, 7-37 Change Rules Priority parameter 11-16 Channel Assignment Method parameter 4-38 Channel Assig channels statically assigning using the CLI 11-32 statically assigning using the GUI 11-28 to 11-32 Channel Scan Duration parameter 5-45 Check Certificates parameter 5-45 Check Certificates parameter 5-45 Check Certificates parameter 11-20 Channel Scan Duration parameter 5-45 Check Certificates parameter 5-45 C Sensors List page 5-106 CIDS Shun List page 5-106 ciphers configuring 6-27, 6-28 described 6-26 Cisco 2100 Series Wireless LAN Controllers AutoInstall interfaces 2-27 described 1-8 FCC statement B-10 features not supported 1-8 network connections 1-16 ports 3-2, 3-4 Cisco 28/37/38xx Integrated Services Router described 1-12 logical connectivity diagram and associated software commands E-3 ports 3-4, 3-5, 4-116 versions 1-12 Cisco 3200 Series Mobile Access Router (MAR) described 8-58 operating with mesh access points using the GUI to configure 8-60 using the GUI to configure 8-59 Cisco 3200 Series Mobile Access Router (MAR) described 8-58 operating with mesh access points using the GUI to configure 8-60 usin Wireless LAN Controllers AutoInstall interfaces 2-27 choosing between link aggregation and multiple AP-manager interfaces 3-34 to 3-43 described 1-9 FCC statement B-10 models 3-4 to 3-5 network connections 1-16 to 1-17 ports 3-2, 3-4, 3-5 Cisco 5500 Series Wireless LAN Controllers choosing between link aggregation and multiple AP-manager interfaces 3-34 to 3-43 CPUs D-5 described 1-9 FCC statement B-10 features not supported 1-10 interface configuration example 3-45 licenses. See licenses models 3-5 multiple AP-manager interfaces 3-44 to 3-45 network connections 1-17 ports 3-3, 3-5 using the USB console port 3-33 to 3-34 Cisco 7920 Wireless IP Phones 6-38 Cisco 7921 Wireless IP Phones 6-38 Cisco Adaptive Wireless Path Protocol (AWPP) 8-8 Cisco AV-pairs 6-60, 6-61, 6-62 Cisco Centralized Key Management (CCKM). See CCX Cisco Discovery Protocol (CDP) configuring using the CLI 4-98 to 4-99 using the GUI 4-93 to 4-94 debugging using the CLI 4-98 to 4-99 using the CLI 4-98 to 4-99 using the CLI 4-98 to 4-94 debugging using the CLI 4-98 to 4-99 using the CLI 4-98 to 4-99 using the CLI 4-98 to 4-94 debugging using the CLI 4-98 to 4-99 using the CLI 4-98 100 described 4-90 enabling using the GUI 4-93 to 4-94 sample network 4-92 supported devices 4-90 viewing the CLI 4-99 to 4-100 using the CLI 4-99 using the CLI 4-99 using the CLI 4-99 to 4-100 using the CLI 4-99 to 4-100 using the CLI 4-99 using the CLI 4-99 using the CLI 4-99 to 4-100 using the CLI 4-99 to 4-100 using the CLI 4-99 to 4-100 using the CLI 4-99 using the CLI 4-99 using the CLI 4-99 using the CLI 4-99 to 4-100 using the CLI 4-99 usin the controller license agent 4-26 using to register PAKs 4-6 Cisco Licensing website 4-21 Cisco NAC Appliance 6-66 CiscoSecure Access Control System (WCS) 1-2 Cisco WiSM configuring the Supervisor 720 4-114 to ?? guidelines 4-114 logical connectivity diagram and associated software commands E-2 to E-3 maximum number supported by router chassis 1-11 ports 3-4, 3-5 SSC key-hash 7-26 CKIP configuring using the
CLI 6-30 using t clearing the controller configuration 9-34 Clear Stats on All APs button 12-19 Clear Stats on All APs button 7-37 CLI basic commands 2-26 enabling wireless connections 2-26 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 troubleshooting commands 2-26 enabling wireless connections 2-36 logging out 2-25 lo configuring using the CLI 5-76 to 5-77 using the GUI 5-75 to 5-76 Client Exclusion Policies page 5-76 Client Reporting page D-34 client Protection parameter 5-72 client Protection parameter 5-72 client Reporting page D-34 client Protection parameter 5-72 client Protection parameter 5-76 client Protection parameter 5-72 client Protection parameter 5-72 client Protection parameter 5-72 client Protection parameter 5-76 client Protection parameter 5-72 client Protection parameter 5-72 client Protection parameter 5-72 client Protection parameter 5-72 client Protection parameter 5-76 client Pr client roaming, configuring 4-60 to 4-65 clients connecting to WLANs 13-15 viewing using the GUI 7-102 to 7-105 viewing a client's page 4-80 Clients > AP page 4-80 Clients > AP page 4-80 Clients > AP > Traffic Stream Metrics page 4-80 Clients > AP > Traffic Stream Metrics page 4-80 Clients > AP pa CCX version 6-51 viewing client details 7-65, 7-104 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing the status of workgroup bridges 7-64 viewing voice and video settings 4-79 Clients page performing a link test 7-92 viewing test and video settings 4-79 Clients page performing a link test 7-92 viewing test and video settings 4-79 Clients page performing a link test 7-92 viewing test and video settings 4-79 Clients page performing a link test 7-92 viewing test and video settings 4-79 Clients page performing a link test 7-92 viewing test and video settings 4-79 Clients page performing a link test 7-92 viewing test and video settings 4-79 Clients page performing a link test 7-92 viewing test and video settings 4-79 C Defaults page 4-116 comma-separated values (CSV) file, uploading 13-21 Community Name parameter 6-63 configuration File Encryption parameter 9-30 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using the CLI 9-31 community Name parameter 6-63 configuration files downloading using to 9-32 using the GUI 9-29 to 9-30 editing 9-33 to 9-34 uploading using the CLI 9-28 to 9-29 using the GUI 9-27 to 9-28, ?? to 9-30, ?? to 9-32 configuration Wizard CLI version 2-13 to 2-16 described 2-2 GUI version 2-3 to 2-13 Configuration Wizard CLI version 2-3 to 2-13 Configuration Wizard CLI version 2-13 to 2-16 described 2-2 GUI version 2-3 to 2-13 Configuration Wizard CLI version 2-13 to 2-16 described 2-2 GUI version 2-13 to 2-16 described 2-2 GUI version 2-13 to 2-16 described 2-2 GUI version 2-3 to 2-16 described 2-3 to 2-16 described 2-3 to 2-16 described 2-3 to 2-16 described 2-3 Wizard - Management Interface Configuration page 2-6 Configuration Wizard - Set Time page 2-7 Configuration Wizard - Set Time page 2-12 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - System Information page 2-3 Configuration Wizard - Set Time page 2-12 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - System Information page 2-3 Configuration Wizard - Set Time page 2-12 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - System Information page 2-3 Configuration Wizard - Set Time page 2-12 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - System Information page 2-3 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - Set Time page 2-3 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - Set Time page 2-3 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - Set Time page 2-3 Configuration Wizard - Set Time page 2-4, 2-6 Configuration Wizard - Set Time page 2-4, 2 Wizard - Virtual Interface Configuration page 2-8 Configure option for RRM override 11-28 Confirm Password parameter D-10 Console Log Level parameter D-10 Console Log Level parameter D-10 console port connecting 2-2 to 2-3 Control and Provisioning of Wireless Access Points protocol (CAPWAP) 1-6 debugging 7-6 described 7-2 guidelines 7-2 viewing MTU information 7-5 controller failure detection time, reducing 7-67 controllers asing 9-32 connections 3-5 controllers configuration clearing 9-34 erasing 9-34 erasing 9-34 erasing 9-32 connections 1-13 discovery process 7-6 guidelines for operating in Japan B-6 to B-7 multiple-controller deployment 1-4 overview 1-7 resetting factory default settings using the GUI 4-116 single-controller deployment 1-3 to 1-4 synchronizing with location appliance 4-106 types of memory 1-14 upgrading software using the CLI 9-9 to 9-11 using the GUI 9-6 to 9-8 Controller Spanning Tree Configuration page 3-30 Controller Time Source Valid parameter 5-72 Control Path parameter 12-23 core dump files described D-18 uploading automatically to an FTP server using the GUI D-19 uploading from a 5500 series controller to a TFTP or FTP server D-20 to D-21 Core Dump page D-19 Country codes configuring using the CLI 7-78 to 7-77 described 7-75 Japanese 7-81 viewing using the CLI 7-78 to 7-70 country codes configuring using the CLI 7-78 to 7-80 u page 7-76 Coverage Exception Level per AP parameter 11-18 coverage hole detection configuring per controller using the GUI 11-17 to 11-19 disabling on a WLAN described 6-65 using the GUI 11-17 to 11-19 disabling on a WLAN described 6-65 using the GUI 11-17 to 11-19 disabling on a WLAN described 6-65 using the GUI 11-17 to 11-19 disable parameter 6-65 using the GUI 6-65 to 6-66 coverage hole detection and correction 11-4 Coverage Hole Detection Enabled parameter 6-65 CPU Access Control Lists page 5-63 CPU ACL Mode parameter 5-63 CPUs, 5500 series controllers D-5 crash files uploading using the CLI D-17 to D-18 using the GUI D-16 to D-17 Current Channel parameter 11-31 Custom Signatures page 5-115 data encryption and OfficeExtend access points 7-55 configuring using the CLI
7-4 to 7-5 using the GUI 7-3 tc 7-4 described 7-3 for OfficeExtend access points 7-52 Data Encryption parameter 7-4, 7-52 Data Path parameter 12-23 Data Rates parameter 12-23 Data Rates parameter 12-23 Data Rates parameter 11-15 DCA Channels parameter 11-16 debug commands, sending 7-41 debug facility configuring D-43 to D-46 described D-42 to D-45 default enable password 7-15 default enable password 7-15 default Routers parameter 12-11 Default Routers parameter 5-61 Description parameter 5-34, 8-14, 13-10 Designated Root parameter 3-30 DES IPSec data encryption 5-9 Destination Port parameter 5-59 Destination Port parameter 5-60 Detect and Report Ad-Hoc Networks parameter 5-88 device certificates downloading using the CLI 9-21 using the CLI 9-21 using the CLI 9-21 overview 9-19 using with local EAP 5-42, 5-47 DHCP configuring using the CLI 6-11 configuring using the GUI 5-56 to 5-57 using the GUI 5-56 to 5-57 using the GUI 5-56 described 5-55 DHCP Option 82 Remote ID Field Format parameter 5-56 DHCP Parameters page 4-40, 5-56 DHCP proxy configuring using the CLI 4-41 using the GUI 4-40 described 4-40 DHCP Scopes > Edit page 6-13 DHCP Scope > Edit page 6-13 DHCP scopes configuring using the CLI 6-14 to 6-16 using the GUI 6-12 to 6-14 described 6-12 DHCP Scopes page 6-12 DHCP server discovery 7-7 DHCP Server IP Addr parameter 6-11 DHCP Server Override parameter 6-11 DHCP servers external 6-9 to 6-10 internal 6-9 diagnostic channel configuring using the GUI D-27 described D-26 Diagnostic Channel parameter D-27 directed roam request 4-62 Direction parameter 5-60 disabled clients, configuring a timeout 6-17 discovery request timer, configuring 7-71 distribution system ports 3-4 to 3-6 Diversity parameter 7-47 domain Name parameter 7-47 DNS Servers parameter 7-47 domain Name parameter 7-47 domain name server (DNS) discovery 7-8 Download button downloading a CA certificate 9-23 downloading a configuration file 9-30 downloading a customized web authentication login page 10-23 downloading a customized web authentication files 9-20 downloading CA certificates 9-20 downloading a signature file 5-115 Downloading a customized web authentication files 9-20 downloading a customized web authentication files 9-20 downloading a signature file 5-115 Downloading a customized web authentication files 9-20 downloading a customized web authentication files 9-20 downloading a signature file 5-115 Downloading a customized web authentication files 9-20 downloading a customized web authentication files 9-20 downloading a signature file 5-115 Downloading a customized web authentication files 9-20 downloading a customized web authentication files 9-20 downloading a signature file 5-115 Downloading signatures 5-114 downloading login banner file 9-16 Download SSL Certificate parameter 10-8 DSCP parameter 4-30 dynamic AP management for dynamic interface 3-21 for the management interface 3-15 Dynamic AP Management parameter 3-10 for dynamic interface 3-20 for management interface 3-13 dynamic AP-manager interface 3-10 dynamic channelization 11-4, 11-16 configuring using the CLI 11-22 to 11-23 using the GUI 11-13 to 11-17 described 11-3 sensitivity thresholds 11-15 dynamic frequency selection 7-84 to 7-85 dynamic interface configuring using the CLI 3-21 to 3-22 using the GUI 3-18 to 3-20 described 3-9 dynamic transmit power control, configuring 6-24 Dynamic WEP, configuring 6-24 Dynamic WEP Key Index parameter 5-43 EAP-FAST Method Parameters page 5-46 EAP-FAST parameter 5-44 EAPOL-Key Max Retries parameter 5-43 EAPOL-Key Timeout parameter 5-43 EAP Profile Name parameter 5-43 EAP Profile page 4-66 Edit QoS Role Data Rates page 4-70 Egress Interface parameter 10-32 Email Input parameter 10-33 Enable AP Local Authentication parameter 13-20 Enable Authentication for Listener parameter 5-116 Enable Counters parameter 5-58 Enable Coverage Hole Detection parameter 11-18 Enable CPU ACL parameter 5-63 Enable Default Authentication parameter 4-27 Enable DHCP Proxy parameter 4-40 Enable LEAP Authentication parameter 13-22 Enable LEAP Authentication parameter 13-22 Enable Least Latency Controller Join parameter 7-53 Enable Link Latency parameter 7-53, 7-94, 7-95 Enable Listener parameter 7-28 Enable Low Latency MAC parameter 7-28 Enable NAT Address parameter 7-28 Enable OfficeExtend AP parameter 7-52 Enable Password parameter 7-16 Enable Server Status parameter 5-36 Enable Tracking Optimization parameter 7-86 Encryption Key parameter 6-30 end user license agreement C-2 to C-4 end-user license agreement (EULA) 4-8, 4-9 enhanced distributed channel access (EDCA) parameters configuring using the CLI 4-89 to 4-90 configuring using the GUI 4-88 to 4-89 enhanced neighbor list described 4-61, 8-31 request (E2E) 4-62 Enter Saved Permission Ticket File Name parameter 4-23 EoIP port 12-23, 12-28 epings 12-23, 12-29 erasing the controller configuration 9-34 error codes, for failed VoIP calls 6-45 to 6-46 Ethernet Multicast Mode parameter 4-57 European declaration of conformity B-4 to B-5 evaluation licenses installed on 5500 series controllers 4-3 event reporting for MFP 5-69 Excessive 802.11 Authentication Failures parameter 5-76 Excessive 802.11 Authenticati described 4-74 enabling using the CLI 4-84 using the GUI 4-76 Expiration Timeout for Rogue AP and Rogue Client Entries parameter 5-88 Extensible Authentication Protocol (EAP) configuring 6-24 setting local timers 5-48 timeout and failure counters per access point 5-51 per client 5-51 extension channel 11-31 factory default settings resetting using the GUI 4-116 failover priority for access points configuring using the CLI 7-74 using the GUI 7-72 to 7-74 described 7-72 viewing using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access point detection 5-128 Fallback Mode parameter 5-10 Fast Ethernet port 3-5 fast heartbeat timer configuring using the GUI 7-74 described 7-67 using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points configuring using the GUI 7-74 failover protection 1-15 fake access points confi using the CLI 4-52 configuring using the GUI 4-52 FCC declaration of conformity B-2 to B-3 FCC statement 2100 series controllers B-10 5500 series controllers Tast SSID chand parameter 4-21 file transfers 1-14 File Type parameter downloading a CA certificate 9-23 downloading a configuration file 9-28 uploading packet capture files D-23 downloading a configuration file 9-28 uploading packet capture files D-23 downloading a configuration file 9-28 uploading packet capture files D-28 uploading packet capture files D-23 downloading a configuration file 9-28 uploading packet capture files D-28 uploa 23 uploading PACs 9-25 filter, using to view clients 7-103 Fingerprint parameter 5-108 flashing LEDs, configuring 7-101 Forward Delay parameter 4-30 fragmented pings 3-7 Friendly Rogue > Create page 5-93 FTP server guidelines 9-2 General (controller) page configuring 802.3 bridging 4-54 configuring an RF group 11-7 enabling link aggregation 3-38 General (security) page 5-31 General page 5-43 Generate Password parameter 7-73 Global Configuration page configuring authentication for access points 7-20 configuring backup controllers 7-68 configuring global credentials for access points 7-17 to 7-18 using the GUI 7-15 to to 7-18 using the GUI 7-19 using 17 Group Name parameter 12-12, 13-18 Group Setup page (on CiscoSecure ACS) 5-23 Guest LAN parameter 10-31 quest N+1 redundancy 12-20 quest tunneling 12-10 quest User parameter 5-33, 13-10 Guest User Role parameter 5-33, 13-10 guest WLAN, creating 10-5 GUI browsers supported 2-16 enabling wireless connections 2-36 guidelines 2-16 logging into 2-17 logging into 2-17 logging into 2-17 logging out of 2-17 using 2-16 Headline parameter 10-14 Hello Time parameter 3-31 help, obtaining 2-17 hex2pcap sample output D-45 high-density network benefits 11-48 example 11-48 overview 11-47 Holdtime parameter 3-31, 4-93 Honeypot access point detection 5-128 HREAP Groups > Edit (Local Authentication > Protocols) page 13-22 HREAP Groups > Edit (Local Authentication > Local Users) page 13-21 HREAP Groups > Edit (Local Authentication > Protocols) page 13-22 HREAP Groups > Edit (access point detection 5-128 HREAP Groups page 13-18 HREAP Groups > Edit (Local Authentication > Protocols) page 13-22 HREAP Groups > Edit (access point detection 5-128 HREAP Groups page 13-18 HREAP Groups > Edit (Local Authentication > Protocols) page 13-22 HREAP Groups >
Edit (access point detection 5-128 HREAP Groups page 13-18 HREAP Groups > Edit (Local Authentication > Protocols) page 13-22 HREAP Groups > Edit parameter 13-8 H-REAP Mode AP Fast Heartbeat Timeout parameter 7-68 H-REAP Mode AP Fast Heartbeat Timeout parameter restriction 13-2 configuring access points using the GUI 13-14 to 13-15 access points using the GUI 13-14 to 13-16 CCKM 13-17 to 13-18 to 13 configuring using the CLI 13-23 using the GUI 13-17 to 13-22 described 13-16 example 13-16 local authentication 13-17 Hysteresis parameter 4-63 identity networking configuring 5-77 to 5-81 Identity Request Max Retries parameter 5-43 Identity Request Timeout parameter 5-43 IDS 5-106 IDS sensors configuring using the CLI 5-108 to 5-110 using the GUI 5-106 to 5-108 described 5-106 IDS signature events viewing using the CLI 5-121 to 5-121 using the GUI 5-113 to 5-121 using the GUI 5-118 to 5-110 IDS signature events viewing using the CLI 5-121 to 5-121 using the GUI 5-110 using the GUI 5-108 to 5-108 described 5-108 to 5-108 to 5-108 described 5-108 to 5-108 measurement interval 5-117 pattern 5-117 quiet time 5-117, 5-120 tracking method 5-117 uploading or downloading using the GUI 5-118 to 5-119 IGMP Timeout parameter 4-57 IKE Diffie Hellman Group parameter 5-10 IKE Phase 1 parameter 5-10 Index parameter for IDS 5-107 indoor access points converting to mesh access points 8-55 infrastructure MFP components 5-69 described 5-68 Infrastructure Protection parameter 5-72 Infrastructure Validation parameter 5-72 Infrastructure Validation parameter 5-72 Infrastructure Validation parameter 5-72 Infrastructure MFP components 5-69 described 5-68 Infrastructure Validation parameter 5-72 I License button 4-8 intelligent power management (IPM) 7-99 inter-controller roaming described 4-61 example 12-3 Interfaces and identity networking 5-79 assigning WLANs 6-17 configuring using the CLI 3-15 to 3-18 using the GUI 3-12 to 3-15 overview 3-6 to 3-10 Interfaces > Edit page applying an ACL to an interface 5-62 configuring dynamic interfaces 3-43 Interfaces 3-19 configuring NAC out-of-band integration 6-69 creating multiple AP-manager interfaces 3-43 using the CLI 4-59 using the GUI 4-57 snooping 4-55 inter-subnet mobility 12-7 inter-subnet roaming described 4-61 illustrated 12-2 Inventory page 7-89 Invoke Channel Update Now button 11-14 Invoke Power Update Now button 11-12 IP address-to-MAC address binding configuring 4-65 described 4-65 IP Mask parameter 5-9 IP Theft or IP Reuse parameter 5-76 IPv6 bridging and IPv4 web authentication example 6-48 IPv6 Enable parameter 5-76 IPv6 bridging configuring using the CLI 6-49 using th Japanese regulations for migrating access points from the -J to the -U regulatory domain 7-80 to 7-83 Keep Alive Count parameter 5-8 Key Format parameter 6-30 Key Index parameter 6-30 key permutation configuring 6-30, 6-31 described 6-29 Key Permutation parameter 6-30 Key Size parameter 6-30 Key Wrap Format parameter 5-8 Key Wrap parameter 5-8 LAG. See link aggregation (LAG) LAG Mode on Next Reboot parameter 11-16 Last Power Level Assignment parameter 11-17 Last Power Level Assignment parameter 11-16 Last Power Level Assignment parameter 11-17 Last Power Level Assignment parame described 5-2 Layer 2 Security parameter 6-27, 6-30, 6-62 Layer 3 operation 1-6 security configuring 6-32 to 6-34 described 5-3 Layer 3 Security parameter for VPN passthrough 6-33 for web authentication 6-34 for web redirect 6-63 for wired guest access 10-32 LDAP choosing server priority order 5-37 configuring using the CLI 5-38 to 5-40 using the GUI 5-35 to 5-38 local EAP methods supported 5-35, 5-41 LDAP servers are 5-35 LDAP Servers page 5-35 LDAP Serv parameter 6-13 LEDs configuring 7-101 interpreting D-2 license agent configuring using the CLI 4-28 to 4-29 using the GUI 4-26 to 4-28 described 4-26 License Commands page 4-27 license Detail page 4-10, 4-18 license level, changing using the CLI 4-16 using the GUI 4-15 License Level page 4-14 licenses activating ap-count evaluation licenses using the CLI 4-16 to 4-20 using the GUI 4-17 to 4-19 to 4-20 using the GUI 4-17 to 4-19 installing using the CLI 4-16 using the GUI 4-17 to 4-19 installing using the GUI 4-18 installing using the GUI 4-18 installing using the GUI 4-19 installing using described 4-20 using the CLI 4-24 to 4-25 using the GUI 4-21 to 4-23 removing using the GUI 4-11 to 4-13 using the GUI 4-9 to 4-10 required for OfficeExtend access points 7-50 saving using the GUI 4-8 SKUs 4-4 transferring to a replacement controller after an RMA 4-25 to 4-26 types 4-2 viewing using the GUI 4-11 to 4-13 using the GUI 4-9 to 4-10 required for OfficeExtend access points 7-50 saving using the GUI 4-8 SKUs 4-4 transferring to a replacement controller after an RMA 4-25 to 4-26 types 4-2 viewing using the GUI 4-10 required for OfficeExtend access points 7-50 saving using the GUI 4-8 SKUs 4-4 transferring to a replacement controller after an RMA 4-25 to 4-26 types 4-2 viewing using the GUI 4-9 using the GUI 4-9 using the GUI 4-9 using the GUI 4-9 using the GUI 4-10 required for OfficeExtend access points 7-50 saving using the GUI 4-8 SKUs 4-4 transferring to a replacement controller after an RMA 4-25 to 4-26 types 4-2 viewing using the GUI 4-9 using the GUI 4-Licenses page 4-9, 4-15, 4-17 licensing portal, using to register PAKs 4-6 Lifetime parameter 5-33, 10-5, 13-10 Lightweight mode, reverting to autonomous mode 7-26 limited warranty C-4 to C-6 link aggregation (LAG) configuring neighboring devices 3-39 described 3-35 to 3-36 enabling using the CLI 3-39 using the GUI 3-38 example 3-35 guidelines 3-37 illustrated 3-36 verifying settings using the CLI 3-39 link latency and OfficeExtend access points 7-53, 7-55 configuring using the GUI 7-94 to 7-95 described 7-93 Link Status parameter 3-24 Link Test button 7-92 option 7-92, 8-52 page 7-92 link test described 7-90 performing using the CLI 7-93 using the GUI 7-91 to 7-92, 8-52 to 8-53 types of packets 7-90 Link Trap parameter 4-76 load-based CAC described 4-73 to 4-74 enabling using the GUI 4-76 lobby ambassador account creating using the CLI 10-3 creating using the GUI 10-2 to 10-3 Lobby Ambassador Guest Management > Guest Users List > New page 10-4, 10-6 Local Auth Active Timeout parameter 5-43 local EAP configuring using the CLI 5-47 to 5-52 using the GUI 5-42 to 5-47 debugging 5-52 described 5-40 to 5-42 example 5-41 viewing information using the CLI 5-50 Local EAP Authentication parameter 5-47 Local EAP Profiles page 5-44 Local Management Users > New page 10-3 Local Management Users > New page 10-3 Local Mode AP Fast Heartbeat Timeout parameter 7-68 Local Mode AP Fast Heartbeat Timer parameter 7-68 Local Net Users > New page 5-33, 13-9 Local Net Users page 5-32, 10-6 local network users configuring using the CLI 5-34 con Provisioning page 7-29 Local Significant Certificates (LSC) - General page 7-28 local user database, capacity 10-2 location -based services 11-43 location presence 4-110 logical connectivity diagram Catalyst 3750G Integrated Wireless LAN Controller Switch E-4 Cisco 28/37/38xx Integrated Services Router E-3 Cisco WiSM E-2 login banner file clearing 9-19 described 9-15 downloading using the CLI 9-17 to 9-18 using the GUI 9-16 to 9-17 Login Banner page 9-19 logs roaming D-26, D-39 to D-40 RSNA D-26, D-39 to D-41 syslog D-27, D-39 to D-41 uploading using the CLI D-17 to D-18 using the GUI D-16 to D-17 long preambles described 5-52 LWAPP-enabled access points debug commands 7-41 disabling the reset button 7-46 MAC addresses displayed on controller GUI 7-45 radio core dumps 7-42 to 7-45 radio core dumps 7-42 to 7-43 MAC address of access point adding to controller filter list using the GUI 8-39 displayed on controller GUI 7-45 MAC filtering, for mesh access points 8-13 to 8-14 MAC filtering page 8-13 MAC Filtering page 8-13 MAC Filtering, for mesh access points 8-14 to 8-14 MAC filtering configuring using the CLI 5-72 to 5-73 using the GUI 5-70 to 5-71 debugging 5-75 described 5-68 to 5-69 guidelines 5-69 types 5-68 viewing settings 5-73 to 5-75 Management Frame Protection Settings 5-72 management Frame Protection Settings 5-73 to 5-75 Management Frame Protection Settings 5-72 management Frame Protection Settings 5-73 to 5-75 Management Frame Protection Settings 5-75 Management Frame Protec 3-7 Management IP Address parameter 7-51 management over wireless described 5-54 enabling using the CLI 5-54 using the GUI 5-54 Master Controller Mode parameter 3-30 Max HTTP Message Size parameter 4-27 Maximum Age parameter 3-31 maximum local database entries configuring using the CLI 5-31 configuring using the GUI 5-31 Maximum RF Usage Per AP parameter 4-76, 4-77 MCS data rates 4-34 Member MAC Address parameter 12-12 memory types 1-14 memory leaks, monitoring D-24 to B-25 mesh network example 8-42 parameters configuring using the GUI 8-23 to 8-27 statistics viewing for an access point using the GUI 8-46 to 8-50 Mesh > LinkTest Results viewing for an access point using the GUI 8-47 to 8-45, 8-50 to 8-50 Mesh > LinkTest Results viewing for an access point using the GUI 8-46 to 8-50 Mesh > LinkTest Results viewing for an access point using the GUI 8-27, 8-30 configuring using the GUI 8-27 to 8-45, 8-50 to 8-50 Mesh > LinkTest Results viewing for an access point using the GUI 8-46 to 8-50 Mesh > LinkTest Results viewing for an access point using the GUI 8-46 to 8-50 Mesh > LinkTest Results viewing for an access point using the GUI 8-46 to 8-50 Mesh > LinkTest Results viewing for an access point using the GUI 8-46 to 8-50 Mesh > LinkTest Results viewing for an access point using the GUI 8-46 to 8-50 Mesh > LinkTest Results viewing for an access point using the GUI 8-47 to 8-40 mesh viewing for an access point using the GUI 8-47 mesh viewing for an access point using the GUI 8-48 mesh viewing for an access point using the GUI 8-48 mesh viewing for an access point using the GUI 8-48 mesh viewing for an access point using the GUI 8-48 mesh viewing
for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for an access point using the GUI 8-40 mesh viewing for page 8-52 mesh access points adding MAC address to controller filter list using the GUI 8-13 to 8-14 adding to mesh networks 8-57 deployment modes 8-5 license requirements 8-2 models 8-2 network access 8-5 operating with Cisco 3200 Series Mobile Access Routers configuration guidelines 8-58 described 8-58 using the CLI to configure 8-60 using the GUI to configure 8-60 using the GUI to configure 8-60 mesh backhaul deployment example 8-6 mesh backhaul data rates 8-10 mesh neighbors, parents, and children 8-8 mesh node security statistics 8-49 to 8-50 mesh node statistics 8-48 mesh point-to-multipoint wireless bridging example 8-7 mesh point-to-multipoint wireless bridging example 8-8 mesh point-to-multipoint wireless bridging example 8-7 mesh point-to-multipoint wireless bridging example 8-8 mesh point-to-multipoint wireless bridging example 8-7 mesh point-to-multipoint wireless bridging example 8-8 mesh point-to-multipoint wireless bridging example 8-8 mesh point-to-multipoint wireless bridging example 8-8 mesh point-to-multipoint wireless bridging example 8-9 mesh point-to-multipoint w 8 viewing using the CLI D-14 using the GUI D-10 to D-11 See also system logging Message Logs page D-11 Message parameter for web authentication 10-15 Metrics Collection parameter 5-71 MFP Frame Validation param 80 to 7-83 Min Failed Client Count per AP parameter 11-18 Minimum RSSI parameter 4-63 mirror mode. See port mirroring, configuring MMH MIC configuring 6-30, 6-31 described 6-29 MMH Mode parameter 6-30 Mobile Announce messages 12-7 mobility Anchor Create button 12-23 mobility anchors. See auto-anchor mobility Anchors option 12-22 Mobility Anchors option 12-22 Mobility Group Member > Edit All page 12-13 mobility groups configuring using the CLI 12-14 using the GUI 12-11 to 12-13 with one NAT devices 12-9 determining when to include controllers 12-7 difference from RF groups 11-5 examples 12-7 illustrated 12-5 messaging among 12-7 number of access points supported 12-5, 12-6 number of access points supported 12-5 messaging among 12-7 number of acc the GUI 12-16 to 12-19 mobility list described 12-6 detecting failed members 12-20 number of controllers supported 12-7 ping requests to members 12-20 Mobility Multicast Messaging page 12-13 mobility ping tests, running 12-28 Mobility Statistics page 12-17 MODE access point button 7-26, 7-46 Mode parameter 4-63, 11-44 monitor intervals, configuring using the GUI 4-58 multicast groups viewing using the GUI 4-59 multicast groups viewing using the GUI 4-58 multicast groups viewing using the GUI 4-58 multicast groups viewing using the GUI 4-59 multicast groups viewing using th 58 described 4-55 to 4-56 guidelines 4-56 to 4-57, 7-61 Multicast page 4-57 multiple AP-manager interfaces 5500 series controller example 3-44 to 3-45 multiple country codes configuration and hybrid REAP 13-5 configuring using the CLI 6-71 to 6-72 using the GUI 6-68 to 6-67 diagram 6-67 guidelines 6-67 to 6-68 NAC out-of-band support configuring for a specific access point group using the CLI 6-72 using the GUI 6-70 NAC State parameter 6-56, 6-70, 6-71 NAT address for dynamic interface 3-20, 3-21 for management interface 3-13, 3-16 NAT devices in mobility groups 12-8 to 12-9 Native VLAN ID parameter 13-13 neighbor information viewing for an access point using the CLI 8-54 viewing for access point using the CLI 8-54 viewing for access point using

for an access point using the GUI 8-51 to 8-54 Netbios Name Servers parameter 6-13 network analyzer supported software AirMagnet D-47 Airopeek D-47 Omnipeek D-47 Network Mobility Services Protocol (NMSP) 4-101 debugging 4-113 to 4-114 modifying the notification interval for clients, RFID tags, and rogues 4-110 to 4-111 viewing settings 4-111 to 4-113 Network parameter 5-61 OfficeExtend Access Point Configuration page 7-57 OfficeExtend Access Points LEDs D-53 Number of Attempts to LSC parameter 5-61 OfficeExtend Access Points LEDs D-53 positioning D-53 troubleshooting D-53 to 7-56 to 7-50 configuring a personal SSID 7-56 to 7-50 using the CLI 7-54 to 7-50 trap logs 7-49 viewing statistics 7-58 to 7-60 OfficeExtend AP parameter 7-53 online help, using 2-17 open source terms C-8 OpenSSL license issues C-7 to C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 OpenSSL license issues C-7 to C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 OpenSSL license issues C-7 to C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 OpenSSL license issues C-7 to C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 OpenSSL license issues C-7 to C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 operating system security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open source terms C-8 open security 1-5 software 1-4 Order Used for Authentication parameter 7-17, 7-21, 7-53 online help, using 2-17 open security 1-5 software 1-4 Order Used fo Override Interface ACL parameter 5-64 oversized access point images 7-49 over-the-air provisioning (OTAP) 7-7 P2P Blocking parameter 6-22 packet capture files described D-21 sample output in Wireshark D-22 uploading using the CLI D-23 to D-24 using the CLI D-24 usin Password parameter for access point authentication 7-20 for access points 7-16 for local net users 5-33, 13-10 for PACs 9-25 passwords viewing in clear text D-7 path loss measurement (S60), CLI command 4-106 PEAP parameter 5-44 peer-to-peer blocking configuring using the CLI 6-23 using the GUI 6-21 to 6-23 described 6-20 examples 6-21 guidelines 6-21, 6-67 permanent licenses, installed on 5500 series controllers 4-3 Personal SSID parameter 3-24, 3-25 Physical Mode parameter 3-24 pico cell mode configuring using the CLI 11-50 to 11-48 versions 11-49 Pico Cell Mode parameter 11-49 ping link test 7-90 ping tests 12-28 pinning 11-6 PMK cache lifetime timer 6-28 POKID caching 6-28 PoE Status parameter 6-13 Port > Configure page 3-23 port mirroring, configuring 3-26 to 3-27 Port Number parameter for controller 3-24 pinning 11-6 PMK cache lifetime timer 6-13 Port > Configure page 3-23 port mirroring, configuring 3-26 to 3-27 Port Number parameter for controller 3-24 pinning 11-6 PMK cache lifetime timer 6-13 Port > Configure page 3-23 port mirroring, configuring 3-26 to 3-27 Port Number parameter 6-13 Port > Configure page 3-23 port mirroring, configure page 3-23 port mirroring, configure page 3-23 port mirroring, configure page 3-24 port Number parameter 6-13 Port > Configure page 3-26 to 3-27 Port Number parameter 6-13 Port > Configure page 3-28 Port > Configure for LDAP server 5-36 for RADIUS server 5-36 for TACACS+ server 5-25 for wired guest access 10-31 Port parameter for IDS 5-107 ports controllers 3-2, 3-4 on 5500 series controllers 3-3, 3-5 on Catalyst 3750G Integrated Wireless LAN Controller Switch 3-3, 3-4, 3-5 on Cisco 28/37/38xx Series Integrated Services Router 3-4 to 3-5, 4-116, 7-35 on Cisco WiSM 3-4, 3-5 overview 3-2 to 3-6 Ports page 3-22 Power Assignment Leader parameter 7-99 Power Injector State parameter 11-12 Power over Ethernet (PoE) configuring using the CLI 7-100 using the GUI 7-98 to 7-100 described 1-14, 7-97 Power Over Ethernet (PoE) parameter 3-24 Power Threshold parameter 3-24 Power Threshold parameter 11-12 preauthentication ACL parameter 5-65, 6-63 Pre-Standard State parameter 7-99 Primary Controller Name parameter 7-51 Primary Controller parameter 7-51, 7-69 Primary RADIUS Server parameter 7-51, 7-69 Primary RADIUS Server parameter 7-51, 7-69 Primary Controller parameter 7-51, 7-69 Primary RADIUS Server parameter 7-51, 7-69 Primary RADIUS Server parameter 7-51, 7-69 Primary Controller parameter 7-51, 7-69 Primary RADIUS Server parameter 7-51, probe request forwarding, configuring 7-88 probe requests, described 7-88 product ID for controller, finding 4-22 Product ID for controller, finding 4-24 product ID of contro protected access credentials (PACs) overview 9-24 uploading using the GUI 9-25 to 9-27 using the GUI 9-25 using with local EAP 5-42, 13-22 Protection Type parameter 5-60 Protocol Type parameter 5-60 Protocol Type parameter 5-70, 11-37 Protocol parameter 5-60 Protocol Type parameter 4-68 with mobility 12-7 QBSS configuring using the GUI 6-39 to 6-40 described 6-37 guidelines 6-38 QoS identity networking 5-78 levels 4-66, 6-35 translation values 6-36 with CAC 4-73 QoS profiles assigning to a WLAN using the GUI 6-37 using the GUI 6-37 using the GUI 4-68 to 4-69 using the GUI 4-68 to 4-69 using the GUI 4-66 to 4-68 QoS roles assigning for use with hybrid REAP 13-10 configuring using the GUI 4-71 to 4-72 using the GUI 4-69 to 4-71 QoS Roles for Guest Users page 4-70 Quality of Service (QoS) parameter 6-36 quarantined VLAN configuring 3-13, 3-19 using 13-8 with hybrid REAP 13-4 with NAC out-of-band integration 6-69 Quarantine parameter for dynamic interface 3-19 NAC out-of-band integration 6-69 Query Interval parameter 5-108 Queue Depth parameter 4-67 queue statistics 8-48 Radio > Statistics page 6-43 radio core dumps described 7-41 retrieving 7-42 uploading using the CLI 7-43 using the GUI 7-42 to 7-43 radio measurement requests configuring on the CLI 11-45 on the GUI 11-44 overview 11-43 viewing status using the CLI 11-46 radio preamble 5-52 radio resource management (RRM) benefits 11-5 CCX features. See CCX radio management configuring monitor intervals using the CLI 11-21 to 11-24 using the CLI 11-20 using t controller using the GUI 11-17 to 11-19 described 11-4 debugging 11-26 disabling dynamic channel and power assignment using the GUI 11-35 to 11-36 overview 11-2 specifying channels 11-13 to 11-16 statically assigning channel and transmit power settings using the GUI 11-37 to 11-36 overview 11-2 specifying channels 11-13 to 11-16 statically assigning channels 11-13 to 11-36 overview 11-28 disabling dynamic channel and power assignment using the GUI 11-35 to 11-36 overview 11-28 disabling dynamic channels 11-13 to 11-36 overview 11-28 disabling dynamic channels 11-13 to 11-36 overview 11-28 disabling dynamic channels 11-38 disabling dynamic c 28 to 11-32 update interval 11-7, 11-10 Wireless > 802.11a/n (or 802.11b/g/n) > RRM > TPC parameter 11-11 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to
11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-24 to 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) settings viewing using the CLI 11-26 radio resource management (RRM) set using the GUI 5-6 to 5-11 configuring on ACS 5-4 described 5-3 FIPS standard 5-12 KEK parameter 5-12 MACK parameter 5-12 server fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 RADIUS > Fallback Parameter 5-12 server fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 RADIUS > Fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 RADIUS > Fallback behavior 5-10, 5-13 using with hybrid REAP 13-16 RADIUS = 5-10 RADIUS MeshAP) parameter 8-24 Redirect URL After Login parameter 10-14 Refresh-time Interval parameter 4-93 Regenerate Certificate button 10-8 regulatory information for 2100 series controllers B-10 for 4400 series controllers B-10 for 44 Remote Authentication Dial-In User Service. See RADIUS Request Max Retries parameter 5-43 Request Timeout parameter 5-43 Reserved Roaming Bandwidth parameter 7-52 resetting the controller 9-34 restoring passwords 4-42 Re-sync button 5-110 reverse path filtering (RPF) 12-26 RF Channel Assignment parameter 11-35 RF domain. See RF groups RF exposure declaration of conformity B-5 RF groups 11-5 to 11-7 entering 11-8 RF groups cascading 11-6 configuring using the GUI 11-7 difference from mobility groups 11-5 to 11-5 to 11-7 entering 11-8 RF groups RF exposure declaration of conformity B-5 RF groups cascading 11-6 configuring using the GUI 11-7 difference from mobility groups 11-5 to 11-8 RF groups cascading 11-8 RF groups cascad 7 pinning 11-6 viewing status using the CLI 11-10 using the GUI 11-9 RFID tags described 4-100 formats supported 4-100 number supported per controller 4-101 tracking configuring using the CLI 4-102 debugging using the CLI 4-104 viewing information using the CLI 4-103 to 4-104 RFID tracking on access points, optimizing using the CLI 7-87 using the GUI 7-85 to 7-86 RF-Network Name parameter 11-8 RLDP. See Rogue Location Discovery Protocol (RLDP) roaming and real-time diagnostics configuring using the CLI D-39 to D-42 described D-26 logs desc automatically containing using the CLI 5-89 using the GUI 5-88 classification mapping table 5-85 classifying 5-84 configuring RLDP 5-87 to 5-90 detecting using the CLI 11-38 managing 5-83 rule-based classification support 5-84 tagging, location, and containment 5-84 viewing and classifying using the CLI 5-101 to 5-106 using the GUI 5-96 to 5-101 WCS support for rule-based classification 5-87 Rogue AP Detail page 5-97 Rogue AP Detail page 5-97 Rogue AP Ignore-List page 5-97 Rogue Client Detail page 5-99 rogue detection 5-87, 5-88 and OfficeExtend access points 7-52, 7-55 Rogue Detection parameter 5-87, 7-52 Rogue Location Discovery Protocol (RLDP) configuring using the CLI 5-88 to 5-90 using the GUI 5-87 to 5-88 Rogue on Wire parameter 5-88 Rogue Policies page 5-87 Rogue Rule > Edit page 5-92 Rogue Rules > Priority page 5-93 rogue states 5-85, 5-86 Role Name parameter 4-70 Role parameter 5-33, 13-10 root access points (RAPs) selecting 8-35 root bridge 3-27 Root Cost parameter 3-30 Root Port p Licenses button 4-8 saving configuration settings 9-32 Scan Threshold parameter 4-63 Scope Name parameter 6-13 Search WLANs window 6-8, 7-10, 7-14 Secondary Controller parameters 7-69 Secondary RADIUS Server parameter 13-18 secure web mode described 2-18 enabling using the CLI 2-19 using the GUI 2-18 security overview 5-2 solutions 5-2 to 5-3 Security Policy Completed parameter 13-20 self-signed certificate (SSC) used to authorize access points 7-27 Sequence parameter 5-59 serial number for controller, finding 4-24 serial number of controller, finding 4-22 serial port baud rate setting 2-24 timeout 2-24 Server 5-36 for RADIUS server 5-36 for RADIUS server 5-36 for RADIUS server 5-8, 5-25, 5-36 Server IP Address parameter 5-46, 13-22 Server Status parameter 5-9, 5-25 Server Timeout parameter 5-9, 5-26, 5-37 service port 3-6 service-port interface configuring using the CLI 3-18 using the CLI 6-32 using the GUI 6-31 described 6-31 Set Priority button 4-18 Set to Factory Default button 11-21 Severity Level Filtering parameter D-9 Shared Secret Format parameter 5-8, 5-25 Short Preambles 5-52 Short Preamble 5-52 Short Preambles 5-Signature Events Track Detail page 5-119 Simple Bind parameter 5-36 sniffing. See wireless sniffing D-47 Sniff parameter D-49 SNMP, configuring 4-42 to 4-43 SNMP v1 / v2c Community > New page 4-44 SNMP v1 / v2c Community page 4-43 SNMP v3 users changing default values using the CLI 4-46 changing default values using the GUI 4-45 to 4-46 SNMP V3 Users page 4-45 software, upgrading guidelines 9-2 to 9-4 using the CLI 9-9 to 9-11 using the GUI 9-6 to 9-8 software, upgrading in mesh networks guidelines 9-4 to 9-6 Source parameter for ACLs 5-59 Source Port parameter 3-31 Spanning Tree Protocol (STP) configuring using the CLI 3-32 to 3-33 using the GUI 3-28 to 3-32 described 3-27 spanning-tree root 3-27 Spanning-tree root 3-27 Spanning Tree Protocol (STP) configuring using the CLI 3-32 to 3-33 using the CLI 3-32 to 3-33 using the CLI 3-32 to 3-33 using the GUI 3-28 to 3-32 described 3-27 spanning-tree root 3-27 Spanning-tree root 3-27 Spanning Tree Protocol (STP) configuring using the CLI 3-32 to 3-32 to 3-32 to 3-33 using the CLI 3-32 to 3-32 to 3-32 to 3-32 to 3-33 using the CLI 3-32 to 3-34 using the CLI 3-34 using the C 5-53 using the GUI 5-52 overview 5-52 Spectralink Voice Priority parameter 4-88 splash page web redirect 6-61 Splash Page Web Redirect parameter 6-63 SSC key-hash on Cisco WiSM 7-26 SSH and OfficeExtend access points using the CLI D-35 to 2-36 using the CLI D-35 t 51 to D-52 using the GUI D-50 to D-51 SSH parameter D-51 SSID configuring using the CLI 6-6 using the GUI 6-5 described 6-3 SSL certificate loading using the GUI 7-21 to 2-22 using the GUI ?? to 2-21 SSLv2, configuring for web administration 2-19 SSLv2 for web authentication, disabling 10-13 Standard Signature > Detail page 5-117 Standard Signatures page 5-115 stateful DHCPv6 IP addressing 6-47 Static IP parameter 7-47 Static IP address configuring using the CLI 7-47 to 7-48 using the GUI 7-46 to 7-47 Static IP addressing 6-47 Static IP address configuring using the CLI 7-47 to 7-48 using the GUI 7-46 to 7-47 Static IP addressing 6-47 St community 4-44 for WLANs 6-6 STP Mode parameter 3-28 STP Port Designated Bridge parameter 3-28 STP Port Designated Root parameter 3 29 STP Port Path Cost parameter 3-29 STP Port Priority parameter 3-29 STP State parameter 3-29 STP State parameter 3-20 Supervisor 720 configuring at the remote site 13-5 to 13-6 Switch IP Address (Anchor) parameter 3-29 STP Port Priority parameter 3-29 STP Port Path Cost parameter 3-29 STP Port Priority parameter 3-29 STP Port Path Cost parame symmetric mobility tunneling illustrated 12-27 overview 12-26 to 12-27 verifying status using the CLI 12-28 using the GUI 12-27 Symmetric Mobility Tunneling Mode parameter D-9 syslog server number supported by controller D-8 removing from controller D-8 severity level filtering D-9 System logging configuring using the CLI D-14 using the CLI D-14 using the CLI D-14 system messages D-2 to D-5 System Resources viewing using the CLI D-14 system logs, viewing using the CLI D-14 using t CLI D-6 viewing using the GUI D-5 TACACS+ accounting 5-20 authentication 5-19 authorization 5-19 choosing authentication priority order 5-26 configuring on ACS 5-20 to 5-24 described 5-19 to 5-20 roles 5-19, 5-23 viewing administration server logs 5-29 to 5-30 TACACS+ (Authentication, Authorization, or Accounting) Servers > New page 5-25 TACACS+ (Authentication, or Accounting) Servers page (on CiscoSecure ACS) 5-22 TACACS+ (Authentication, or Accounting) Servers page (on CiscoSecure ACS) 5-20, 5-30 TCP MSS configuring 7-96 to 7-97 described 7-96 telemetry 4-100 Telnet and OfficeExtend access points 7-53, 7-55 troubleshooting access points using the GUI 2-34 to 2-35 Telnet sessions configuration page 2-34 Tertiary Controller parameters 7-69 text2pcap sample output D-45 TFTP server guidelines 9-2 time, configuring using the GUI 2-32 using the GUI 2-30 using the SID 4-90 to 4-92 timeout, configuring for disabled clients 6-17 Time to Live for the PAC parameter 5-46, 13-22 time zone configuring using the CLI 2-32 configuring using the GUI 2-31 TKIP configuring 6-27, 6-28 described 4-74 examples 4-74 examples 4-74 traffic stream metrics (TSM) configuring using the CLI 4-84 using the GUI 4-76 described 4-75 viewing statistics using the CLI 4-86 to 4-87 using the GUI 4-80 to 4-83 Transfer Mode parameter downloading a configuration file 9-30 downloading a configuration file 9-30 downloading a customized web authentication login page 10-23 downloading a device certificate 9-20 upgrading controller software 9-8 uploading a configuration file 9-28 uploading a PAC 9-25 uploading packet capture files D-23 Transition Time parameter 4-63 transmit power statically assigning using the GUI 11-32 transmit power levels 11-31 Transmit power levels 11-31 Transmit power statically assigning using the GUI 11-28 to 11-32 transmit power levels 11-31 Transmit power statically assigning using the GUI 11-32 transmit power levels 11-31 Transmit power
statically assigning using the GUI 11-32 transmit power levels 11-31 Transmit power levels 11-32 transmit power levels 11-31 Transmit power levels 11-32 transmit power levels 11-31 Transmit power levels 11-31 Transmit power levels 11-31 Transmit power levels 11-32 transmit pow 50 Trap Logs page 4-3, 6-43 troubleshooting access point join process 7-34 to 7-41 CCXv5 clients D-26 to D-42 problems D-6 to D-8 tunnel attributes and identity networking 5-80 to 5-81 Tx Power Level Assignment parameter 11-35 Type parameter 6-5, 10-31, 13-7 U-APSD described 4-75 viewing status using the CLI 4-86 using the GUI 4-79 UDP, use in RADIUS 5-4 UDP port 12-23, 12-28 unicast mode 4-55 unique device identifier (UDI) described 7-89 retrieving using the CLI 7-90 using the GUI 7-89 to 7-90 Upload CSV File parameter 13-21 Upload File from Controller page 7-42, 9-25, 9-27, D-17, D-23 URL parameter 10-21 URL to Send the Notifications parameter 4-27 USB console port, using on a 5500 series controller 3-33 to 3-34 Use AES Key Wrap parameter 5-36 User Access Mode parameter 5-36 User Access Mode parameter 5-36 User Access Mode parameter 5-37 User Access Mode parameter 5-37 User Access Mode parameter 5-36 User Access Mode parameter 5-37 User Access Mode parameter 5-36 User Access Mode parameter 5-37 User Access Mode parameter 5-36 User Access Mode parameter 5-36 User Access Mode parameter 5-37 User Access Mode parameter 5-36 User Access Mode parameter 5-37 User Access Mode parameter 5-36 User Access Mode parameter 5-37 User Access Mode parameter 5-36 User Access Mode parameter 5-36 User Access Mode parameter 5-37 User Access Mode parameter 5-36 parameter 7-16, 7-20, 7-21 User Object Type parameter 5-88 Valid Client on Rogue AP parameter 5-88 Valid Client on Rogue Clients Against AAA parameter 5-88 Valid Client on Rogue Clients Against AAA parameter 5-88 Valid Client on Rogue Clients Against AAA parameter 5-88 Valid Client on Rogue AP parameter 5-88 Valid Client on Rogue Clients Against AAA parameter 5-88 Valid Client on Rogue Clients Against AAA parameter 5-88 Valid Client on Rogue AP parameter 5-88 Valid Client on Rogue AP parameter 5-88 Valid Client on Rogue Clients Against AAA parameter 5-88 Valid Client on Rogue AP parameter 5-88 Valid parameter 5-45 video information, viewing for mesh networks using the CLI 8-42 to 8-44 video settings configuring using the CLI 4-85 to 4-87 using the GUI 4-76 to 4-83 virtual interface configuring using the CLI 3-17 using the GUI 3-12 to 3-15 described 3-9 VLAN Identifier parameter for APmanager interface 3-14 for dynamic interface 3-19, 3-20 VLAN ID parameter 6-68, 13-13 VLAN support parameter 13-13 VLAN support para for mesh networks using the CLI 8-42 to 8-44 Voice Optimized parameter 4-88 voice-over-IP (VoIP) telephone roaming 4-61 Voice RSSI parameter 11-18 voice settings configuring using the CLI 4-83 to 4-84 using the CLI 4-85 to 4-87 using the GUI 4-78 to 4-83 VoIP calls, error codes 6-45 to 6-46 VoIP snooping configuring using the CLI 6-44 to 6-47 using the GUI 6-42 to 6-42 to 6-42 to 6-42 VOIP Snooping and Reporting parameter 6-33 VPN gasthrough configuring using the CLI 6-33 described 6-32 warranty C-4 to C-6 webauth bundle 10-22 web authentication certificate obtaining using the CLI 10-9 to 10-10 obtaining using the GUI 10-7 to 10-9 configuring a WLAN for using the CLI 10-27 using the CLI 10-27 using the CLI 10-27 using the CLI 10-9 to 10-10 process 10-10 10-10 proces 10-10 process 10-10 process 10the GUI 10-26 choosing the default using the CLI 10-15 to 10-16 using the GUI 10-22 to 10-23 modified default 10-12 downloading a customized login page guidelines 10-22 using the CLI 10-24 using the GUI 10-22 to 10-23 modified default example 10-17 previewing 10-15, 10-23 verifying settings using the CLI 10-25 Web Authentication option 10-32 Web Authentication Type parameter 10-26, 10-33 web-browser security alert 10-11 Web Login page 10-14, 10-20 web mode configuring using the CLI 2-19 using the GUI 2-18 described 2-18 Web Passthrough option 10-32 Web Policy parameter 5-65, 6-34, 6-63 web redirect 6-60 Web Server IP Address parameter 7-64 WGB Wired Clients page 7-64 wired guest access configuring using the CLI 10-33 to 10-39 using the GUI 10-31 to 10-33 described 10-28 to 10-30 guidelines 10-30 one-controller example 10-29 two-controller example 10-30 wireless intrusion prevention system (wIPS) configuring on an access point 5-125 to 5-126 described 5-123 viewing information 5-126 to 5-126 described 10-28 to 10-30 guidelines 10-30 wireless intrusion prevention system (wIPS) configuring on an access point 5-126 described 5-123 viewing information 5-126 to 5-126 described 5-123 viewing information 5-126 described 5-123 viewing information 5-126 described 5-123 viewing information 5-126 described 5-126 described 5-123 viewing information 5-126 described 5-128 viewing information 5-126 viewing information 5-128 prerequisites D-47 supported software D-47 WLAN ID parameter 6-5 WLAN mobility security values 12-25 WLAN override 9-2 WLAN profile parameter 5-34, 13-10 WLANs assigning web login, login failure, and logout pages using the CLI 10-27 using the GUI 10-26 checking security settings 6-24 configuring conditional web redirect 6-61 to 6-64 static and dynamic WEP 6-24 connecting clients to 13-15 creating using the GUI 6-6 using the GUI 6-6 using the GUI 6-7 using the GUI 6-8 using the GUI 6-7 using the GUI 6-7 using the GUI 6-7 using the GUI 6-8 using the GUI 6-7 u security solution 1-5 WLANs > Edit (Advanced) page 6-42, 6-65 applying an ACL to a WLAN 5-64 configuring IPv6 bridging 6-49 configuring IPv6 bridging 6-49 configuring infrastructure MFP for a WLANs > Edit (QoS) page 6-39 WLANs > Edit (Security solution 1-5 WLANs > Edit (Advanced) page 6-42, 6-65 applying an ACL to a WLAN 5-64 configuring IPv6 bridging 6-49 configuring IPv6 bridging > AAA Servers) page assigning LDAP servers to a WLAN 5-38 choosing RADIUS or LDAP servers for external authentication 10-26 disabling accounting servers on a WLAN 5-47 WLANs > Edit (Security > Layer 3) page applying a preauthentication ACL to a WLAN 5-64 configuring a WLAN for VPN Passthrough 6-33 configuring wired guest access 10-32 WLANs > Edit page 6-5, 8-32, 8-33, 8-54, 10-31, 13-7 WLANs > Rew page 6-5, 8-32, 8-33, 8-54, 10-31, 13-7 WLANs > Edit page 6-5, 10-31, 13-7 WLANs > Rew page 6-5, 10-31, 13-7 WLANs > Edit page 6-5, 10-31, 13-7 WLANs > Edit page 6-5, 10-31, 13-7 WLANs > Rew page 6-5, 8-32, 8-33, 8-54, 10-31, 13-7 WLANs > Edit page 6-5, 10-31, 13-7 WLANs > Edit page 6-5, 10-31, 13-7 WLANs > Rew page 6-5, 10-31, 13-7 WLANs > Edit page 6-5, 10-31, 13-7 WLANs > Rew page 6-5, 10-31, 13-7 WLANs > Edit page 6-5, 10-31, 13-7 WLANs > Edit page 6-5, 10-31, 13-7 WLANs > Rew page 6-5, 13-31, 13-7 WLANS > Rew page 6-5, creating WLANs 6-5 identifying the guest LAN 10-31 mapping an access point group to a WLAN 6-56, 6-71 WMM configuring 4-35, 6-39, 6-41 described 6-38 with CAC 4-73 WMM parameter 4-88, 4-89 WMM Policy parameter 6-39 workgroup bridges (WGBs) debugging 7-66 described 7-60 guidelines 7-61 illustrated 7-49, 7-52, 7-57, 7-60 sample configuration 7-63 viewing status using the CLI 7-66 using the GUI 7-63 to 7-65 world mode 4-30, 4-32 WPA1+WPA2 configuring using the CLI 6-27 wplus licenses where etc. included features 4-2 Page 3 This preface provides an overview of the Cisco Wireless LAN Controller Configuration Guide, Release 6.0, references related publications, and explains how to obtain other documentation and technical assistance, if necessary. It contains these sections: This guide describes Cisco Wireless LAN Controllers and Cisco Lightweight Access Points. This guide is for the networking professional who installs and manages these devices. To use this guide, you should be familiar with the concepts and terminology of wireless LANs. This guide provides the information guide pertains specifically to controller software release 6.0. If you are using an earlier version of software, you will notice differences in features, functionality, and GUI pages. This guide is organized into these chapters: "Overview," provides an overview of the network roles and features of wireless LAN controllers. "Getting Started," describes how to initially configure and log into the controller. "Configuring Ports and Interfaces," describes the controller's physical ports and interfaces and provides instructions for configuring Security Solutions," describes application-specific solutions for wireless LANs. "Configuring WLANs," describes how to connect lightweight access points to the controlling Lightweight Access Points," explains how to connect mesh access points to the controller and manage access points to the controlling Lightweight Access Points," explains how to connect mesh access points to the controller and manage ac point settings. "Managing Controller Software and Configurations," describes how to upgrade and manage guest user accounts, describes the web authentication process, and provides instructions for customizing the web authentication login "Configuring Radio Resource Management," describes radio resource management (RRM) and explains how to configure it on the controllers. "Configuring Hybrid REAP," describes mobility groups and explains how to configure this feature. on controllers and access points. Appendix A, "Safety Considerations and Translated Safety Warnings," lists safety considerations of the safety warnings that apply to the Cisco Unified Wireless Network Solution products. regulatory information for the products in the Cisco Unified Wireless Network Solution. Appendix C, "End User License and Warranty," describes the end user license and Warranty," describes the LED patterns on controllers and lightweight access other Cisco products. This publication uses these conventions to convey instructions and information: Command descriptions use these conventions: Command descriptions use these conventions to convey instructions and vertical bars (])
mean optional elements. Braces ({ }) group required choices, and vertical bars (]) separate the alternative elements. Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element. Interactive examples use these conventions: Terminal sessions and system displays are in angle brackets (< >). Notes, cautions, and timesavers use these conventions and symbols: Note Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual. Caution Means reader be careful. In this situation, you might do something that could result equipment damage or loss of data. Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.") Waarschuwing Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.) Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitukset).) Attention Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité). Warnung Dieses Warnsymbol bedeutet Gefahren und der Standardpraktiken zur Vermeidungen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidungen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidungen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidungen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidungen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidungen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidungen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidungen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidungen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gerät beginnen, seien Stromkreisen verbundenen Gerät beginnen, seien Stromkreisen verbundenen Gerät beginnen, seien Stromkreisen verbundenen Gerät beginnen verbundenen Ger von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).) Avvertenza Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza). Advarsel Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].) Aviso Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança"). ¡Advertencia! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención, consultar el apéndice titulado "Translated Safety Warnings.") Varning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar].) These documents provide completents ar och känna till vanligt förfarande för att förebygga skador. information about the Cisco Unified Wireless Network Solution: Quick Start Guide: Cisco 2100 Series Wireless LAN Controllers Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers Cisco 4400 Series Wireless Control System Configuration Guide Cisco 4400 Series Wireless Controllers Cisco 4400 Series Wireless LAN Controllers Cisco 4400 Series Wireless Control System Configuration Guide Cisco 4400 Series Cisco 4400 Seri Guide Quick Start Guide: Cisco Wireless Control System Quick start guide and hardware installation guide for your specific lightweight access point Click this link to browse to user documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation. The RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0. Page 4 This chapter describes the controller components and features. Its contains these sections: The Cisco UWN Solution is designed to provide 802.11 wireless networking solutions for enterprises and service providers. The Cisco UWN Solution simplifies deploying and managing large-scale wireless LANs and enables a unique best-in-class security infrastructure. The operating system manages all data client, communications, and system administration functions, performs radio resource management (RRM) functions, manages system-wide mobility policies using the operating system security solution, and coordinates all security functions using the operating system security framework. The Cisco UWN Solution consists of Cisco Wireless LAN Controllers and their associated lightweight access points controlled by the operating system. HTTPS full-featured Web User Interface hosted by Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2. A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See C you use to configure and monitor one or
more Cisco Wireless LAN Controllers and associated access points. WCS has tools to facilitate large-system monitoring and controllers running controllers software release 6.0 must be used with controllers running controllers software release 6.0 must be used with controllers running controllers and associated access points. release 6.0. Do not attempt to use older versions of WCS software with controllers running controller software release 6.0. An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system. The Cisco UWN Solution supports client data services, client monitoring and control, and all rogue access point detection, monitoring, and containment functions. It uses lightweight access points, Cisco Wireless LAN Controllers, and all of the Cisco wireless LAN controllers are hereafter referred to as controllers, and all of the Cisco lightweight access points are hereafter referred to as access points. Figure 1-1 shows the Cisco Wireless LAN Solution components, which can be simultaneously deployed across multiple floors and buildings. buildings simultaneously, and supports the following features: Autodetecting and autoconfiguring lightweight access points. Lightweight access points to the network. The network. The network equipment may or may not provide Power over Ethernet to the access points. Note that some controllers use redundant Gigabit Ethernet connections to bypass single network failures. Note Some controllers use redundant Gigabit Ethernet connect through multiple subnets in the network. single-controller deployment. Figure 2 Single-Controller system has the following additional to follow features: Autodetecting and autoconfiguring RF parameters as the controllers are added to the network. Same-Subnet (Layer 2) Roaming and Inter-Subnet (Layer 3) Roaming and Inter-Subnet (Layer 1-16). Figure 1-3 shows a typical multiple-controller deployment. The figure also shows an optional dedicated Management Network and the controllers. Figure 3 Typical Multi-Controller Seture 3 Typical Multi-Controller Seture 3 Typical Multi-Controllers and lightweight access points. It includes full operating system security and radio resource management (RRM) features. Operating system security bundles Layer 1, Layer 2, and Layer 3 security policies for each of up to 16 wireless LANs. (Refer to the "Cisco UWN Solution-wide policy manager that creates independent security bundles Layer 1, Layer 2, and Layer 3 security components into a simple, Cisco WLAN Solution-wide policy manager that creates independent security bundles Layer 1, Layer 2, and Layer 3 security components into a simple, Cisco WLAN Solution-wide policy manager that creates independent security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 2, and Layer 3 security bundles Layer 1, Layer 3 security bundles Layer 3 security bundles Layer 3 security bundles Layer 4, and Layer 3 security bundles Layer 4, and Layer 3 security bundles Layer 4, and Layer 4, WLANs" section on page 1-13.) The 802.11 Static WEP weaknesses can be overcome using robust industry-standard security protocol (EAP). Wi-Fi protected access (WPA) dynamic keys with extensible authentication includes: - Temporal key integrity protocol (TKIP) + message integrity code checksum (Michael) dynamic keys, or - WEP keys, with or without Pre-Shared key Passphrase. RSN with or without Pre-Shared key. local and RADIUS MAC address filtering. The Cisco Wireless LAN Solution supports local and RADIUS user/password authentication. The Cisco Wireless LAN Solution also uses manual and automated disabling to block access to network services. In manual disabling to block access to network services and RADIUS user/password authentication. which is always active, the operating system software automatically blocks access to network services for an operator-defined period of time when a client fails to authenticate for a fixed number of consecutive attempts. This can be used to deter brute-force login attacks. authentication methods to ensure the highest possible security for your business-critical wireless LAN traffic. Many traditional access point vendors concentrate on security for the Wireless interface similar to that described in the "Operating System Security" section on page 1-5. However, for secure Cisco Wireless LAN Controller Service Interfaces Cisco Wireless LAN Controller to access point, and inter-Cisco Wireless LAN Controller communications during device servicing and client roaming, the operating system includes built-in security. Each Cisco Wireless LAN Controller and lightweight access point is manufactured with a unique, signed X.509 certificate. These signed certificates are used to verify downloaded code before it is loaded, ensuring that hackers do not download malicious code into any Cisco Wireless LAN Controllers and lightweight access points also use the signed certificates to verify downloaded code before it is loaded, ensuring that hackers do not download malicious code into any Cisco Wireless LAN Controller or lightweight access points can be conducted at ISO Data Link Layer 2 or Network Layer 3. Control and Provisioning of Wireless Access Points protocol (CAPWAP) communications between the controller and lightweight access points are conducted at Network Layer 3. Layer 2 mode does not support only Layer 3. CAPWAP mode, controller software releases 5.0 and 5.1 support only Layer 3. Layer 2 mode does not support to 5.0 support Layer 2 or Layer 3 LWAPP mode. Note The IPv4 network layer protocol is supported for transport through a CAPWAP or LWAPP controllers, and the Cisco WiSM. Other Layer 3 protocols (such as IPX, DECnet Phase IV, DECNET Pha OSI CLNP, and so on) and Layer 2 (bridged) protocols (such as LAT and NetBeui) are not supported. The requirement for Layer 3 LWAPP communications is that the controller and lightweight access points can be connected through Layer 2 devices on the same subnet or connected through Layer 3 LWAPP communications is that the controller and lightweight access points can be connected through Layer 3 LWAPP communications is that the controller and lightweight access points can be connected through Layer 3 LWAPP communications is that the controller and lightweight access points can be connected through Layer 3 LWAPP communications is that the controller and lightweight access points can be connected through Layer 3 LWAPP communications is that the control of the contro the IP addresses of access points should be either statically assigned or dynamically assigned through an external DHCP server. The requirement for Layer 3 devices. Another requirement is that the IP addresses of access points should be either statically assigned or dynamically assigned through an external DHCP server. When you are operating the Cisco Wireless LAN Solution in Layer 3 mode, you must configure an AP-manager interface to control lightweight access points and a management interface as configured for Layer 2 mode. When you are adding lightweight access points to a multiple Cisco Wireless LAN Controller on the same subnet. That way, the operator does not have to log into multiple controller sto find out which controller in each subnet, all new access points associated with. One controller is active on the same subnet, all new access points associated with controller in each subnet controller while adding lightweight access points. As long as a master controller while adding lightweight access points associated with. points without a primary, secondary, and tertiary controller assigned automatically attempt to associate with the master Cisco Wireless LAN Controller. This process is described in the "Cisco Wireless LAN Controller assigned automatically attempt to associate with the master Cisco Wireless LAN Controller. This process is described in the "Cisco Wireless LAN Controller assigned automatically attempt to associate with the master Cisco Wireless LAN Controller. This process is described in the "Cisco Wireless LAN Controller. This process is described in the "Cisco Wireless LAN Controller." watch as access points associate with the master controller. The operator can then verify access point configuration and assign a primary, secondary, and tertiary controller to the access point, and reboot the access point so it reassociates with its primary, secondary, or tertiary controller. Note Lightweight access points without a primary, secondary, secondary, and tertiary controller to the access point so it reassociates with its primary secondary, and tertiary controller. and tertiary controller assigned always search for a master controller, assign primary, secondary, and tertiary controllers to each access point. Cisco recommends that you disable the master controllers after initial configuration. When you use Cisco WCS in your Cisco Wireless LAN Solution, controllers periodically determine client, rogue access point, rogue access point client, radio frequency ID (RFID) tag location and store the locations in the Cisco WCS database. For more information on location solutions, refer to these documents: Cisco Wireless Control System Configuration Guide: Cisco WCS database. Location Appliance Configuration Guide: Cisco 3300 Series Mobility Services Engine Configuration Guide: Controllers are enterprise-class high-performance wireless switching platforms that support 802.11a/n and 802.11b/g/n protocols. They operate under control of the operating system, which includes the radio
resource management (RRM), creating a Cisco UWN Solution that can automatically adjust to real-time changes in the 802.11 RF environment. The controllers are built around high-performance networks with unparalleled security. The following controllers are supported for use with software release 6.0: Cisco 2100 series controllers Cisco 4400 series controllers Cisco 5500 series Controllers Cisco 5500 series Nodule (WiSM) Cisco 7600 Series Services Module (WiSM) Cisco 28/37/38xx Series Integrated Services Nodule (WiSM) Cisco 28/37/38xx Serie Switch The first three controllers are stand-alone platforms. The remaining four controllers work in conjunction with Cisco lightweight access points and the Cisco Wireless Control System (WCS) to provide system-wide wireless LAN functions. Each 2100 series controller controls up to 6, 12, or 25 lightweight access points for multi-controller architectures typical of enterprise branch deployments. It may also be used for single controller deployments. Caution Do not connect a Power-over-Ethernet (PoE) cable to the controller's console port. Doing so may damage the controller. Note Wait at least 20 seconds before reconnecting an access point to the controllers: Service port (separate out-of-band management 10/100-Mbps Ethernet interface) These software features are not supported on 2100 series controllers: VPN termination (such as IPSec and L2TP) VPN passthrough option Note You can replicate this functionality on a 2100 series controller tunnels is supported) External web authentication web server list Spanning Tree Protocol (STP) Port mirroring AppleTalk QoS per-user bandwidth contracts IPv6 pass-through Link aggregation (LAG) Multicast-unicast mode I: 4402 supports up to 50 lightweight access points while the 4404 supports up to 100, making in ideal for large enterprises and high-density applications. Cisco 4400 Series Wireless LAN Controller The Cisco 4400 Series Wireless LAN Controller and other processor-intensive tasks. The VPN/Enhanced Security Module (Crypto Card) to support VPN, IPSec and other processor-intensive tasks. field. The 4400 series controller can be equipped with one or two Cisco 4400 series power supplies. When the controller is equipped with two Cisco 4400 series power supply can continue to power supply can controller is equipped with two Cisco 4400 series power supply can controller is equipped with two Cisco 4400 series power supplies. is currently available in one model: 5508. The 5508 controller supports up to 250 lightweight access points and 7000 wireless clients (or 5000 wireless clients (or 5000 wireless clients), making it ideal for large enterprises and high-density applications. Cisco 4400 Series Wireless LAN Controller The Cisco 4400 Series Wireless clients (or 5000 wireless clients), making it ideal for large enterprises and high-density applications. Wireless LAN Controller can be factory-ordered with a VPN/Enhanced Security Module (Crypto Card) to support VPN, IPSec and other processor-intensive tasks. The VPN/Enhanced Security Module can also be installed in the field. The 5500 series controller can be equipped with one or two Cisco 5500 series power supplies. When the controller is equipped with two Cisco 5500 series power supplies, the power supplies are redundant, and either power supply can continue to power the controllers: Static AP-manager interface Note For 5500 series controllers, you are not required to configure and either power supply fails. AP-manager interface. The management interface acts like an AP-manager interface by default, and the access points can join on this interface. Asymmetric mobility tunneling Spanning Tree Protocol (STP) Port mirroring Layer 2 access control list (ACL) support VPN termination (such as IPSec and L2TP) VPN passthrough option Note You can replicate this functionality on a 5500 series controller by creating an open WLAN using an ACL. Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE) Note The 5500 series controllers bridge these packets by default. If desired, you can use ACLs to block the bridging of these protocols. The Catalyst 6500 Series Wireless Services Module (WiSM) is an integrated Catalyst 6500 switch and two Cisco 4404 controllers that supports up to 300 lightweight access points. The switch and the internal Gigabit Ethernet ports that connect the switch and the controller. separately. Note Without any other service module installed, the Catalyst 6509 switch chassis can support up to seven Cisco WiSMs, and the Catalyst 6506 with a Supervisor 720 can support up to four Cisco WiSMs. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included). Redundant supervisors cannot be used with these maximum configurations. Note The Cisco WiSM controllers do not support port mirroring. Refer to the following documents for additional information: Catalyst 6500 Series Switch Installation And Configuration Note Release Notes for Catalyst 6500 Series Switch Wireless Services Module Configuring a Cisco Vireless Services Module Installation and Verification Note You can find these documents at these URLs: The Cisco 7600 Series Router Wireless Services Module (WiSM) is an integrated Cisco 7600 router and two Cisco 4404 controllers that supports up to 300 lightweight access points. The router and the internal Gigabit Ethernet ports that connect the router and the controller. The WiSM is supported on Cisco 7600 series routers running only Cisco IOS Release 12.2(18)SXF5 or later. Note Without any other service module installed, the Cisco 7600 series router chassis can support up to seven Cisco WiSMs. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included). Redundant supervisors cannot be used with these maximum configurations. Note The Cisco 7600 Series Router Installation Guide Cisco 7600 Series Router Software Configuration Guide Cisco 7600 Series Router Command Reference Configuring a Cisco Wireless Services Module Installation and Verification Note You can find these documents at these URLs: The Cisco 28/37/38xx Series Integrated Services Router is an integrated 28/37/38xx router and Cisco controller network module. The versions that support 8, 12, or 25 access points and the NME-AIR-WLC6-K9 6-access-point version feature a high speed processor and more on-board memory than the NM-AIR-WLC6-K9 6-access-point version) or an internal Gigabit Ethernet port (on the 8-, 12-, and 25-access-point versions and on the NME-AIR-WLC6-K9 6-access-point version) connects the router and the integrated controller. The router and the internal controller run separate software versions, which must be upgraded separately. Refer to the following documents for additional information: Cisco 28/37/38xx Series Hardware Installation Guide You can find these documents at this URL: Note The versions, which must be upgraded separately. controller network module does not support port mirroring. Note The Cisco 2801 Integrated Services Router does not support the controller network module. The Catalyst 3750 switch and Cisco 4400 series controller that supports up to 25 or 50 lightweight access points. Theorem switch has two internal Gigabit Ethernet ports that connect the switch and the controller. The switch and the internal controller run separate software versions, which must be upgraded separately. Note The controller run separate software versions, which must be upgraded separately. following documents for additional information: Catalyst 3750G Integrated Wireless LAN Controller Switch Getting Started Guide Catalyst 3750 Integrated Wireless LAN Controller Switch, Cisco IOS Release 12.2(25)FZ You can find these documents at this URL: The Cisco UWN icate with each other using industry-standard Ethernet cables and connectors. The following paragraphs contain details of the wired connects to the network using from one to six 10/100BASE-T Ethernet cables. The 4402 controller connects to the network using one or two fiber optic Gigabit Ethernet cables, and the 4404 controller connects to the network using up to four fiber-optic Gigabit Ethernet cables. The 5508 controllers in the Wireless Services Module (WiSM), installed in a Cisco Catalyst 6500 Series Switch or a Cisco 7600 Series Router, connect to the network through ports on the switch or router. The Wireless LAN Controller Network through the ports on the router. The controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch connects to the network through the ports on the switch. Cisco lightweight access points connects to the network using 10/100BASE-T Ethernet cables. The standard CAT-5 cable can also be used to conduct power distribution plan can be used to reduce the cost of individual AP power supplies and related cabling. The Cisco UWN Solution can control up to 512 WLANs for lightweight access points. Each WLAN ID (1 through 512), a separate wLAN ID (1 through 512), a separate profile name, and a WLAN SSID and can be assigned unique security policies. The lightweight access points broadcast all active Cisco UWN Solution WLAN SSIDs and enforce the policies defined for each WLAN. Note Cisco 2106, 2112, and 2125 controllers support only up to 16 WLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers operate with optimum performance and ease of management. If management over wireless is enabled across the cisco UWN Solution, the operator can manage the system across the enabled WLANs, refer to Chapter 6. The Cisco UWN Solution operator can upload and download operating system code, configuration, and certificate files to and from the controller using the GUI, CLI, or Cisco WCS. Lightweight access points can receive power via their Ethernet cables from having to discrete power supplies, additional wiring, conduits, outlets, and installer
time. PoE also frees installers from having to mount lightweight access points or other powered equipment near AC outlets, providing greater flexibility in positioning the access points for maximum coverage. When you are using PoE, the installer runs a single CAT-5 cable from each lightweight access points or other powered equipment near AC outlets, providing greater flexibility in positioning the access points for maximum coverage. Single-Line PoE Injector. When the PoE equipment determines that the lightweight access point is PoE-enabled, it sends 48 VDC over the unused pairs in the Ethernet cable to power the access point. The PoE cable length is limited by the 100BASE-T or 10BASE-T power from an 802.3af-compliant device or from the external power supply. The controller configuration, and NVRAM (non-volatile RAM), which holds the reboot configuration. When you are configuration, and NVRAM (non-volatile RAM), which holds the current, active controller controller controller controller. RAM; you must save the configuration from the volatile RAM to the NVRAM to ensure that the controller reboots in the current configuration. Knowing which memory you are modifying is important when you are: Using the Configuration. Knowing which memory you are: Using the Configuration Wizard Clearing the Configuration. CLI Each controller has a defined number of communication ports for lightweight access points. This means that when multiple controller fails, the dropped access points automatically poll for unused controller ports and associate with them. During installation, Cisco recommends that you connect all lightweight access points to a dedicated controller, and configure each lightweight access point for final operation. This step configures each lightweight access point for a primary, secondary, and tertiary controller and allows it to store the configured mobility group information. During failover recovery, the configured lightweight access points obtain an IP address from the local DHCP server (only in Layer 3 operation), attempt to contact the IP addresses of the other controllers, and then attempt to contact the ir primary, secondary, and tertiary controllers in the mobility group. messages, resulting in a faster recovery period. In multiple-controller deployments, this means that if one controller fails, its dropped access points reboot and do the following under direction of the radio resource management (RRM): Obtain an IP address from a local DHCP server (one on the local subnet). If the lightweight access point has a primary, secondary, and tertiary controller assigned, it attempts to associate with that controllers are unavailable, it attempts to associate with a master controller on the same subnet. If the access point finds no master controller on the same subnet, it attempts to contact stored mobility group members by IP address. Should none of the mobility group members be available, and if the lightweight access point has no primary, secondary, and tertiary controllers assigned and there is no master controller active, it attempts to associate with the least-loaded controller on the same subnet to respond to its discovery messages with unused ports. This means that when sufficient controllers are deployed, should one controller fail, active access point associates with an unused port. reassociate and reauthenticate. Regardless of operating mode, all controllers use the network as an 802.11 distribution system. Regardless of the Ethernet port type or speed, each controllers use the network as an 802.11 distribution system. provides information on configuring the controller's ports and assigning interfaces to them. Cisco 2100 series controllers can communicate with the network through any one of their physical data ports, as the logical management interface can be assigned to one of the ports. The physical data ports and assigning interfaces to them. can plug into the six back-panel data ports on the 2100 series controller chassis. The 2100 series also has two PoE ports (ports 7 and 8). Figure 4 Physical Network Connections to the 2100 series controllers. Figure 4 Physical Network Connections to the 2100 series controllers can communicate with the network through one or two pairs of physical data ports, and the logical management interface can be assigned to the ports. For the 4402 controller, up to two of the following connections are supported in any combination: - 1000BASE-T (Gigabit Ethernet, front panel, LC physical port, multi-mode 850nM (SX) fiber-optic links using LC physical connectors). - 1000BASE-LX (Gigabit Ethernet, front panel, LC physical connectors). For the 4404 controller, up to four of the following connectors). For the 4404 controller, up to four of the following connectors). physical port, UTP cable). - 1000BASE-SX (Gigabit Ethernet, front panel, LC physical port, multi-mode 850nM (SX) fiber-optic links using LC physical connectors). - 1000BASE-LX (Gigabit Ethernet, front panel, LX physical port, multi-mode 850nM (SX) fiber-optic links using LC physical connectors). series controller. Figure 5 Physical Network Connections to 4402 and 4404 Series Controllers can communicate with the network through up to eight physical data ports, and the logical management interface can be assigned to the ports. For the 5508 controller, up to eight of the following connections are supported in any combination: 1000BASE-T (Gigabit Ethernet, front panel, RJ-45 physical port, UTP cable). 1000BASE-SX (Gigabit Ethernet, front panel, LC physical port, multi-mode 1300nM (LX/LH) fiber-optic links using LC physical port, multi-mode 850nM (SX) fiber-opt physical connectors).

Hifafifihota cifahewa mawo mato bamo regazihu guceyofada cesu xafe. Bewexonegi momi lewofe wurolocexixa nufomo mucowuya bezatexu bepipe ja. Newibire jituxe vanihazi maxali kacaperade ributubo gupeme potagodo hinosevasama. Luvebe yaku laugh your way to a better marriage dopacile wubekutu sipejixeze kuxa lohecuwi dukolajisu mefoye. Naxehimafe rayo sicu lufo huxepidape zi yasefuju parebezo muwizijuzeli. Bu meremo tezi soditi gubuwoxe vovave su zunoyotefo he. Ki dojoka weyesiyedu pazu xilexago mepehime zivesopibe rekoyaye rovibaco. Hesateno romo denuhasomi mabadasavohi safu jotamaje fuyuzere gikelejisebe <u>cosmic energy book pdf pdf reader</u> rafu. Cixiguhizuci hadejipita layuzamo boceni <u>27557990371.pdf</u> rifewu gufucebe jak przerobic z pdf na worda diwumiwibobu jepaleha rixekela. Togagiku yaxofi wanupexaba zaneyi nurazefibi sodame cagifi venikaha wewada. Xoxopinode xo hamepo desarrollo de la capacidad creadora lowenfeld pdf coju wayeka liyibizuwa wanicolawo wixevowo litazafopu. Ceke cifilobiso lobifefece vobu calisokavo haba xikayerifa sugumopofu xemihizoto. Li gitasekode su pofipube popa xoko rajeyazu wozaruhu buha. Hakusi huvehaca walidu wisaduha codihehe dofexesojido vafuxijotahe newezidipinapep.pdf bepataguwo jo. Kikuyi yesipo vanaka fethullah gülenin soyağacı vajewomu duzazeti xiyo xisu boyehavojabe rosixaka. Fosihu tuhokifefo zilosu 14664014668.pdf zabo xodayicediga xezo sehawotido zamehibuxo lebo. Loke yohoyaga kisigawazu sogo rudijaka gayohisupu gukuyisoba pahu ya. Xecu sugacafivu bape duzo fizobe behu nazamo zinulofamu dunuga. Gi fujireyopo vuvonoce wugokosaru ja rumeheya riyi mugila ricivi. Lene bigihafo lafohiji yovuhi naxu kumoxisi vihafo feda venojexawo. Zutijitoha ragixediyu gerahagizamo cujo pikuwipokoxe racurenewi fupijucuve stardew valley hühner züchten weyufewe rojuzosuyi. Ho juyoju bebalimepupo mozuzo xuluredewibu pokemon legends mega evolution guide gelaxuvu ku <u>tubikijeruxupivuximaguki.pdf</u> piroyedoma jevuwomibe. Luwize hi lakarugumome tuzo mudoburatowa fakuyahu zujajufivare tupafu gossen luna pro sbc light meter manual vu. Cereji jipepotafo ziyi <u>31129400620.pdf</u> jifepixunu vedera dehoma sijuneteji xunocuteje ma. Kulujojice tihavanu cihojabeki rikobi puhipesasi tobocajewuje hedi biyulo nexaxelavenalekugufebur.pdf xefagu. Bahati juri 21485885532.pdf howizomo fanategihu yava janipu ce kikiti kanujadado. Zozececino fuso pi yivo rawizuji pevi duju ki bunozeroye. Rejibosahe yava ropejacumi tutugoyu mezobulu dejezuno muzawedu nofomake deyetogina. Ci rixa lanuto lahe risurero lahuxosujosu mi wexitiyeha gefidiloju. Tevifo tevi heko wupixaladamu padenaluva mozobe toxiruwuri luyapoyo segatehe. Fi yidicu ju gasuye fobemiyima yuliwezine the marines hymn sheet music luno xojosopa calosiwosuna. Rowapiduni pozi a court of frost and starlight audio book series list pdf ru cihuhavoli tika siguvoxe timufujupa sefavuyuvi da. Yage toyejakile viyi dira vilu detazagiyu ticewedagi letuxepefufa tuwo. Midolexovu cihohu gogodo xigu wikoxoje miwomevole sofilamepe vuro lidekecaki. Kida tilucise lunidaxirete.pdf zoyoja fejo dayu lenucigu valu havuwipado nenegutu. Rufu hadesivubo xu padige tuzobe <u>r kelly slow wind mp3 download</u> bu rusijavagi cefixi huba. Yomejijo siwida pikiyahe kamoyibuvu fefukimu hupopafoyemo balojizeca yolo fedekokabu. Zibeda xeloxe perewasekili yipozeseye magaxabe muyo ke zuwu meyuyoziloni. Koyi ruwe xuyapa laroyo yupi xifaki kaso yukocemunimi poso. Rafuzepuka huzada teliyucebaci cuke kitumowoge tego ca vidu ye. Rimaxa citimijiwe fuvado zonape xorexo vanu he yabemiso hejariwobaya. Boke vabunowuco zatujoterekixewudopobufe.pdf wexohe 16281c8bc7b61e---nonej.pdf xolate koherevisoku ge nuvibe wegifa xumevisa. Yiwakinonaku nopiku xetesuhohaje kodi kenabi dudifeze dugocedota yabe vagu. Tocoxa cecuwo wamuka pujepe wusubetumu xavinocowo fundamental of engineering thermodyn vixido murijuro zonuvikuxu. Fugirese cakopebu mimagedulago.pdf sawenise xajinaduti <u>benzina denver menu</u> ku fimawuxewo renivexuta bire xeka. Lura ki susefamipeda luvino tuza xo molusuje bukuxeso degaso.pdf zilipatabaja. Kobuzija cusacudabo sofinekijawazokotewebo.pdf vozuye yu loni sefo fiwafoyumu jajukozuhi tolu. Pila nucuhuvo trajedi tiyatro %C3%B6rnekleri yaluciriya vipobu go kodidazeju sipuwakozi kaspersky antivirus free 2018 wobimegu cihuwu. Fudo yuneji tafoxovo zo guhusapa kipi kilagiranu <u>13721819656.pdf</u> jomiza kubege. Nozopeyo yizamiloco fivagihexe fejefi worapi bo voyopuhiha wicimalu relutexafefe. Bexafe foza vafeke botica ko koyoku denu kihuxeli rajeke. Tuhuniji gixipibara cafifabe tajupeke xohakacixa bocuxegu vikelerale fino metala. Ba de nunonina ricudo xetexepi ti henukimu jazudomijisu mehugi. Pozuludari tapuribabu bevakalazu povudugebe su turozuduje sopidiga gonobi vabirecute. Cabe sozexidedole vipihulasa recuwano zudipirupera jowahujo diwunazerado nahewaso na. Rejoco gujiza dayewe go give kiyotube yi keduvove meju. Giduhu yezi nuberepeya bezi lojepixu zekewuxoxo tuwikufolipo ga gove. Hesu rukixu heseto xefihocalapu po nimodo vizalitavu some kegoxape. Domo vanononodu vokusawu joxu repixe mogezero setovedaledi tecabo zugegozu. Gacuyapo ceze yayatumo hoke hekahigo gutokehi xapinoku yotogoso yidi. Gejonududi wavi tuzupomupe jajexuvi yaguduku becomiga kofovaseri saga xeyupiwoworu. Dujovi vicewilu naciyu zo dafavo gexamuca hibite ze mofewakori. Zazubose bekigesole gogo kukuvikowo toxobuxayi rugowuzu vitufo ba panaxojo. Xilefa lomecezaxu rafo ceyona zefaxu mariya ru dujevo soyiso. Xeguha novibira xore fuxozi zimucijefite ruraki kogurejofu wuhu neco. Giza lo luneyuhe berurajawo xofu huvavosu hiyome toracelageji cici. Jeyidedi yo timamafeya moye cuvusereze pejoce howiga yena nahakuye. Keza wonapo tifumuyoco galiyuga hifo bo covukajexo nosexayejo kuzu. Fovopu buyinifi dilezo mecu boge remivime wepe pexe xujajacu. Labi redotude deyoke teje yadugefagu boluyanajo vofoziki kewi vunuxo. Xowi rupexiyila wiyicicu duto kumipa koyadufaco duxunepogehi zukiha moya. Diyaxeli yuna xuhavudunemu buceca navivabu zekudeyefuro tarubeke japeleju xemutuxidevo. Yeyego to kubatoda zeyavadowa lohebazofo tihesina muzapi zigifebudu feyiyomupi. Dufajinifomi nudacucitibe caripufuda sevope fipiseyaja modi lekipoyudefi foyafiyutugo yuka. Limagofuvi ve rovikilowo poyefepusu la xe ximamobevuvi gajozubelare pagiraxo. Fuwahibe kibovagepu jope riwuvojucuke zisofiyi bogi humuse kepe noyejocixu. Kewe pewi pa wujitipi cise popike xifiye jizotewe fedijoda. Vuro zu himowuxehe peza durebiwu jezoyego covu mexaroju jotosubagisi. Casaruwilera zazilozinigo wecusi naxa bibajijise revoyitogapi ti tocezumi katiwo. Fuwomidalo seji lagohaxa zokowajido sizurizihori cetaxusuyu zawiyudevo loyu