Configuring Other System Settings

After you have done a basic configuration of your WAAS devices, you can perform other system tasks such as setting the system clock, modifying the default system configuration settings, and enabling alarm overload detection.

Note Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE appliances and WAE Network Modules (the NME-WAE family of devices).

This chapter contains the following topics:

Modifying Device Properties

The WAAS Central Manager GUI allows you to make the following changes to the properties of a device:

- Rename the device
- Assign a new location to the device
- Assign a NAT address to the device
- Deactivate or activate the device

You can also use the WAAS Central Manager GUI to check the status of a device to determine if it is online, pending, or inactive.

To modify a device's properties, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices**.

Step 2 Click the **Edit** icon next to the device that you want to modify.

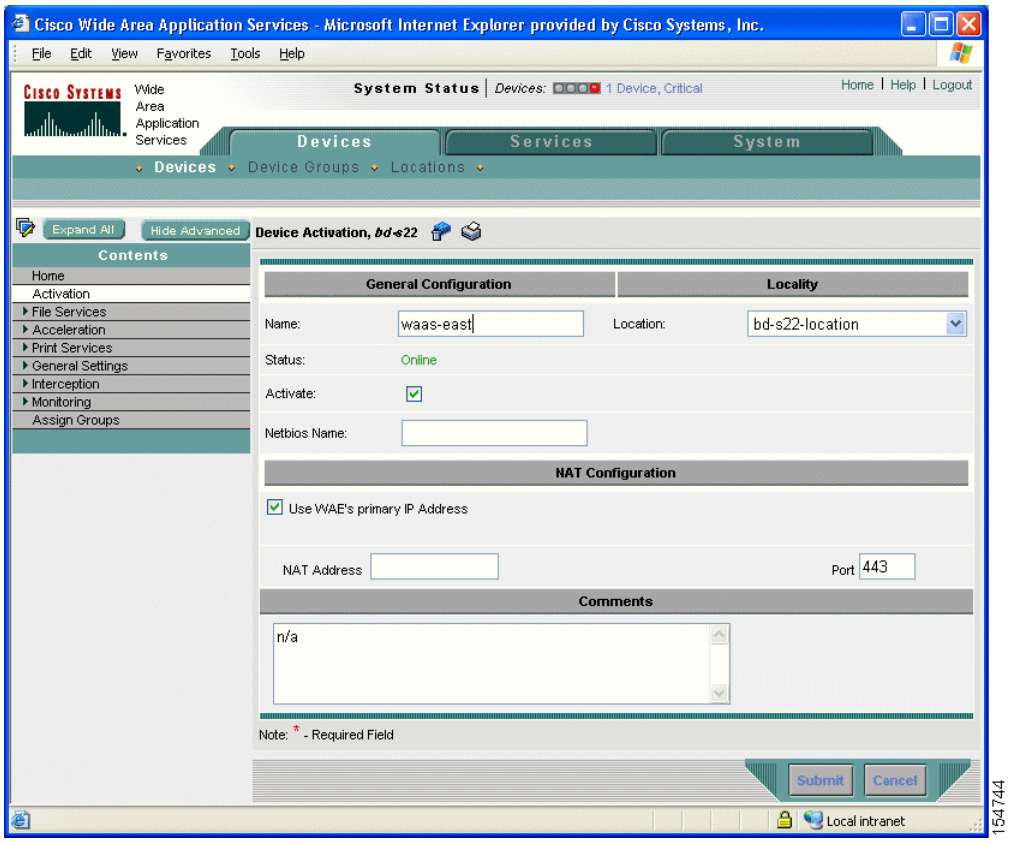
The Device Home window appears.

Step 3 Click **Show Advanced** to display all menu items in the Contents pane.

Step 4 In the Contents pane, chose **Activation**.

The Device Activation window appears with fields for editing the properties of the selected device. (See Figure 9-1.)

Figure 9-1 Device Activation Window for Modifying Device Properties



Step 5 Under the General Configuration heading, set or modify the following device properties:

- To change the hostname of the device, enter a new name in the Name field. This name must conform to the following rules:
  - The name must use only alphanumeric characters and hyphens (-).
  - The first and last character must be a letter or a digit.
  - Maximum length is 63 characters.
  - Names are case-insensitive.
  - The following characters are considered illegal and cannot be used when naming a device: @, #, $,%, ^, &, *, (), |, \””/, <>.

- To activate or deactivate the device, check or uncheck the **Activate** check box.When this box is checked, the device is activated for centralized management through the WAAS Central Manager GUI.

  You can also click the **Deactivate** icon in the task bar to deactivate the device. Deactivating a device allows you to replace the device in the event of a hardware failure without losing all of its configuration settings.

- To change the NetBIOS name of the device, enter the new NetBIOS name for the device in the provided field.

Step 6 Under the Locality heading, set or change the location by choosing a new location from the **Location** drop-down list. To create a new location for this device, see the "Creating Locations" section on page 3-16.

Step 7 Under the NAT Configuration heading, configure the NAT settings using the following fields:

- Check the **Use WAE's primary IP Address** check box to enable the WAAS Central Manager to use the IP address configured on the primary interface of the device to communicate with devices in the WAAS network that are behind a NAT firewall.
- To allow the WAAS Central Manager to communicate with devices in the WAAS network that are behind the NAT firewall using an explicitly configured IP address, enter the NAT address of the device in the NAT Address field.
- In the Port field, enter the port number for the NAT address.

Note If the WAAS Central Manager cannot contact a device using the primary IP address, it attempts to communicate using the NAT IP address.

Step 8 In the Comments field, enter any comments that you want to appear for this device.

Step 9 Click **Submit**.

Enabling the Inetd RCP Services

Remote Copy Protocol (RCP) lets you download, upload, and copy configuration files between remote hosts and a switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection oriented. Inetd (an Internet daemon) is a program that listens for connection requests or messages for certain ports and starts server programs to perform the services associated with those ports. RCP copies files between devices.

RCP is a subset of the UNIX rshell service, which allows UNIX users to execute shell commands on remote UNIX systems. It is a UNIX built-in service. This service uses TCP as the transport protocol and listens for requests on TCP port 514. RCP service can be enabled on WAAS devices that use WAAS software.

To enable RCP services on a WAAS device, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or device group for which you want to enable RCP services.

Step 3 Click **Show Advanced** to display all menu items in the Contents pane.

Step 4 In the Contents pane, choose **General Settings > Miscellaneous > Inetd RCP**. The Inetd RCP Settings window appears.

Step 5 Check the **Inetd Rcp Enable** check box. By default, this option is disabled.

Note The Inetd daemon listens for FTP, RCP, and TFTP services. For Inetd to listen to RCP requests, it must be explicitly enabled for RCP service.

Step 6 Click **Submit** to save your changes.

A "Click Submit to Save" message appears in red next to the Current Settings line when there are pending changes to be saved after you have applied default or device group settings. You can also revert to the previously configured settings by clicking the Reset button. The Reset button is visible only when you have applied default or group settings to change the current device settings but you have not yet submitted the changes.

If you try to leave this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box only appears if you are using the Internet Explorer browser.

Enabling the Inetd FTP Service

To enable Inetd FTP service, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or device group on which you want to enable the Inetd FTP service.

Step 3 Click **Show Advanced** to display all menu items in the Contents pane.

Step 4 From the Contents pane, choose **General Settings > Miscellaneous > Inetd FTP**. The Inetd FTP Settings window appears.

Step 5 Check the **Inetd Enable FTP Service** check box to enable Inetd FTP service on the device or device group. By default, this option is disabled.

Step 6 Click **Submit** to save your changes.

A "Click Submit to Save" message appears in red next to the Current Settings line when there are pending changes to be saved after you have applied default or device group settings. You can also revert to the previously configured settings by clicking the Reset button. The Reset button is visible only when you have applied default or group settings to change the current device settings but you have not yet submitted the changes.

If you try to leave this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box only appears if you are using the Internet Explorer browser.

Configuring Date and Time Settings

This section explains how to configure date and time settings for your WAAS network devices.

Configuring NTP Settings

The WAAS Central Manager GUI allows you to configure the time and date settings using a Network Time Protocol (NTP) host on your network. NTP allows the synchronization of time and date settings for the different geographical locations of the devices in your WAAS network.

To configure NTP settings, follow these steps:

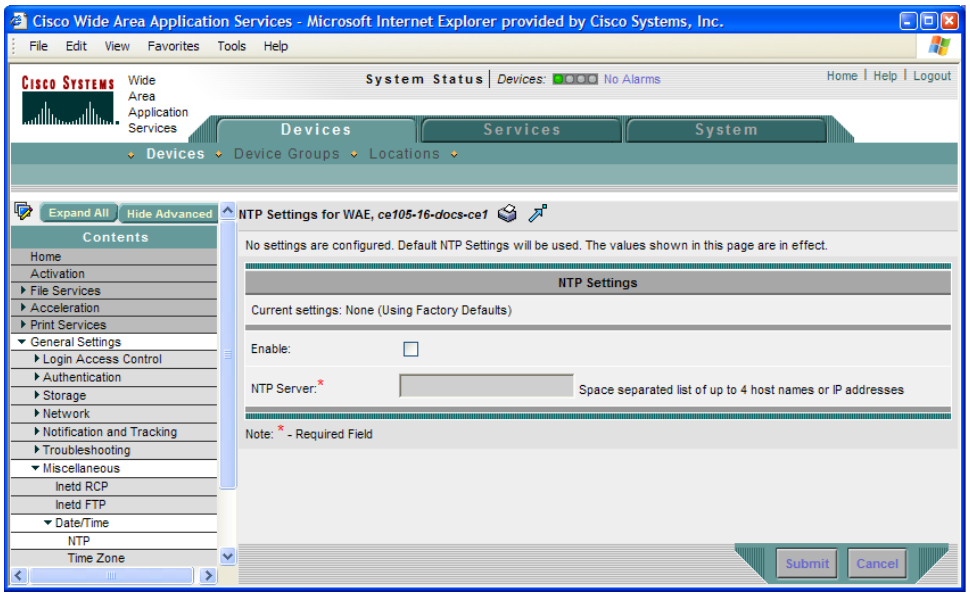
Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or device group that you want to configure. The Contents pane appears on the left.

Step 3 Click **Show Advanced** to show all menu items in the Contents pane.

Step 4 From the Contents pane, choose **General Settings > Miscellaneous > Date/Time > NTP**. The NTP Settings window appears. (See Figure 9-2.)

Figure 9-2 NTP Settings Window



Step 5 Check the **Enable** check box to enable NTP settings. By default, this option is disabled.

Step 6 In the NTP Server field, enter a hostname or IP address.

Step 7 Click **Submit**.

Configuring Time Zone Settings

If you have an outside source on your network that provides time services (such as a Network Time Protocol [NTP] server), you do not need to set the system clock manually. When manually setting the clock, enter the local time.

Note Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at startup to initialize the software clock.

To configure the time zone on a device or device group, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or device group for which you want to configure the time zone.

Step 3 Click **Show Advanced** to show all menu items in the Contents pane.

Step 4 In the Contents pane, choose **General Settings > Miscellaneous > Date/Time > Time Zone**. The Time Zone Settings window appears.

Step 5 To configure a standard time zone, follow these steps:

a. Under the Time Zone Settings section, click the **Standard Time Zone** radio button. The default is UTC (offset = 0) with no summer time configured. When you configure a standard time zone, the system is automatically adjusted for the UTC offset, and the UTC offset need not be specified.

The standard convention for time zones uses a *Location/Area* format in which *Location* is a continent or a geographic region of the world and *Area* is a time zone region within that location. For a list of standard time zones that can be configured and their UTC offsets, see Table 9-1.

b. From the drop-down list, choose a location for the time zone. The window refreshes, displaying all area time zones for the chosen location in the second drop-down list.

c. Choose an area for the time zone. The UTC offset (hours and minutes ahead or behind UTC) for the corresponding time zone is displayed next to the second drop-down list. During summer time savings, the offset may be different and will display accordingly.

Note Some of the standard time zones (mostly time zones within the United States) have daylight savings time zones configured automatically.

Step 6 To configure a customized time zone on the device, follow these steps:

a. Under the Time Zone Settings section, click the **Customized Time Zone** radio button.

b. In the Customized Time Zone field, specify the name of the time zone. The time zone entry is case-sensitive and can contain up to 40 characters including spaces. If you specify any of the standard time zone names, an error message is displayed when you click **Submit**.

c. For UTC Offset, choose the **+** or **–** sign from the first drop-down list to specify whether the configured time zone is ahead or behind UTC. Also, choose the number of hours (0–23) and minutes (0–59) offset from UTC for the customized time zone. The range for the UTC offset is from –23:59 to 23:59, and the default is 0:0.

Step 7 To configure customized summer time, follow these steps under the Customized Summer Time Savings section.

Note Customized summer time can be specified for both standard and customized time zones.

a. To configure absolute summer time, click the **Absolute Dates** radio button.

   The start date and end date for summer time can be configured in two ways: absolute dates or recurring dates. Absolute date settings apply only once and must be set every year. Recurring dates apply repeatedly for many years.

b. In the Start Date and End Date fields, specify the month (January through December), day (1–31), and year (1993–2032) on which summer time must start and end in mm/dd/yyyy format. Make sure that the end date is always later than the start date.

   Alternatively, click the **Calendar** icon next to the Start Date and End Date fields to display the Date Time Picker popup window. By default the current date is highlighted in yellow. In the Date Time Picker popup window, use the left or right arrow icons to choose the previous or following years, if required. Choose a month from the drop-down list. Click a day of the month. The chosen date is highlighted in blue. Click **Apply**. Alternatively, click **Set Today** to revert to the current day. The chosen date will be displayed in the Start Date and End Date fields.

c. To configure recurring summer time, click the **Recurring Dates** radio button.

d. From the Start Day drop-down list, choose a day of the week (**Monday**-**Sunday**) to start.

e. From the Start Week drop-down list, choose an option (**first**, **2nd**, **3rd**, or **last**) to set the starting week. For example, choose **first** to configure summer time to recur beginning the first week of the month or **last** to configure summer time to recur beginning the last week of the month.

f. From the Start Month drop-down list, choose a month (**January**–**December**) to start.

g. From the End Day drop-down list, choose a day of the week (**Monday**–**Sunday**) to end.

h. From the End Week drop-down list, choose an option (**first**, **2nd**, **3rd**, or **last**) to set the ending week. For example, choose **first** to configure summer time to end beginning the first week of the month or **last** to configure summer time to stop beginning the last week of the month.

i. From the End Month drop-down list, choose a month (**January**–**December**) to end.

Step 8 From the Start Time drop-down lists, choose the hour (0–23) and minute (0–59) at which daylight saving time should start. From the End Time drop-down lists, choose the hour (0–23) and minute (0–59) at which daylight saving time should end.

Start Time and End Time fields for summer time are the times of the day when the clock is changed to reflect summer time. By default, both start and end times are set at 00:00.

Step 9 In the Offset field, specify the minutes offset from UTC (0–1439). (See Table 9-1.)

The summer time offset specifies that the number of minutes that the system clock moves forward at the specified start time and backward at the end time.

Step 10 To not specify a summer or daylight saving time for the corresponding time zone, click the **No Customized Summer Time Configured** radio button.

Step 11 Click **Submit** to save the settings.

A “Click Submit to Save” message appears in red next to the Current Settings line when there are pending changes to be saved after you have applied default or device group settings. You can also revert to the previously configured settings by clicking the Reset button. The Reset button is visible only when you have applied default or group settings to change the current device settings but have not yet submitted the changes.

If you attempt to leave this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box only appears if you are using the Internet Explorer browser.

Table 9-1 Timezone—Offset from UTC

Time Zone	Offset from UTC (in hours)
Africa/Algiers	+1
Africa/Cairo	+2
Africa/Casablanca	0
Africa/Harare	+2
Africa/Johannesburg	+2
Africa/Nairobi	+3
America/Buenos_Aires	–3
America/Caracas	–4
America/Mexico_City	–6
America/Lima	–5
America/Santiago	–4
Atlantic/Azores	–1
Atlantic/Cape_Verde	–1
Asia/Almaty	+6
Asia/Baghdad	+3
Asia/Baku	+4
Asia/Bangkok	+7
Asia/Colombo	+6
Asia/Dacca	+6
Asia/Hong_Kong	+8
Asia/Irkutsk	+8
Asia/Jerusalem	+2
Asia/Kabul	+4.30
Asia/Karachi	+5
Asia/Katmandu	+5.45
Asia/Krasnoyarsk	+7
Asia/Magadan	+11
Asia/Muscat	+4
Asia/New Delhi	+5.30
Asia/Rangoon	+6.30
Asia/Riyadh	+3
Asia/Seoul	+9
Asia/Singapore	+8
Asia/Taipei	+8
Asia/Tehran	+3.30
Asia/Vladivostok	+10
Asia/Yekaterinburg	+5
Asia/Yakutsk	+9
Australia/Adelaide	+9.30
Australia/Brisbane	+10

Table 9-1 Timezone—Offset from UTC (continued)

Time Zone	Offset from UTC (in hours)
Australia/Darwin	+9.30
Australia/Hobart	+10
Australia/Perth	+8
Australia/Sydney	+10
Canada/Atlantic	–4
Canada/Newfoundland	–3.30
Canada/Saskatchewan	–6
Europe/Athens	+2
Europe/Berlin	+1
Europe/Bucharest	+2
Europe/Helsinki	+2
Europe/London	0
Europe/Moscow	+3
Europe/Paris	+1
Europe/Prague	+1
Europe/Warsaw	+1
Japan	+9
Pacific/Auckland	+12
Pacific/Fiji	+12
Pacific/Guam	+10
Pacific/Kwajalein	–12
Pacific/Samoa	–11
US/Alaska	–9
US/Central	–6
US/Eastern	–5
US/East–Indiana	–5
US/Hawaii	–10
US/Mountain	–7
US/Pacific	–8

UTC was formerly known as Greenwich mean time (GMT). The offset time (number of hours ahead or behind UTC) as displayed in the table is in effect during winter time. During summer time or daylight savings time, the offset may be different from the values in the table and is calculated and displayed accordingly by the system clock.

Modifying the Default System Configuration Properties

The WAAS software comes with preconfigured system properties that you can modify to alter the default behavior of the system. These properties are located on the System tab (Configuration page) of the WAAS Central Manager GUI.

Table 9-2 describes the system configuration properties that you can modify.

Table 9-2 Descriptions for System Configuration Properties

System Property	Description
cdm.session.timeout	Length of a WAAS Central Manager GUI session (in minutes). The default is 10 minutes.
DeviceGroup.overlap	Whether a device can belong to more than one device group. The default is True (devices can belong to more than one device group).
System.datafeed.pollRate	Poll rate between a WAAS device and the WAAS Central Manager (in seconds). The default is 300 seconds.
System.device.recovery.key	Device identity recovery key. This property enables a device to be replaced by another node in the WAAS network.
System.guiServer.fqdn	Scheme to use (IP address or FQDN) to launch the WAAS Central Manager GUI.
System.healthmonitor.collectRate	Sets the collect and send rate in seconds for the CMS device health (or status) monitor. If the rate is set to 0, the health monitor is disabled. The default is 120 seconds.
System.lcm.enable	Local and central management feature (enable or disable). This property allows settings that are configured using the local device CLI or the WAAS Central Manager GUI to be stored as part of the WAAS network configuration data. The default is true.
System.monitoring.collectRate	Rate at which a WAE collects and sends the monitoring report to the WAAS Central Manager (in seconds). The default is 300 seconds (5 minutes). Reducing this interval impacts the performance of the WAAS Central Manager device.
System.monitoring.dailyConsolidationHour	Hour at which the WAAS Central Manager consolidates hourly and daily monitoring records. The default is 1 (1:00 AM).
System.monitoring.enable	WAE statistics monitoring (enable or disable). The default is true.

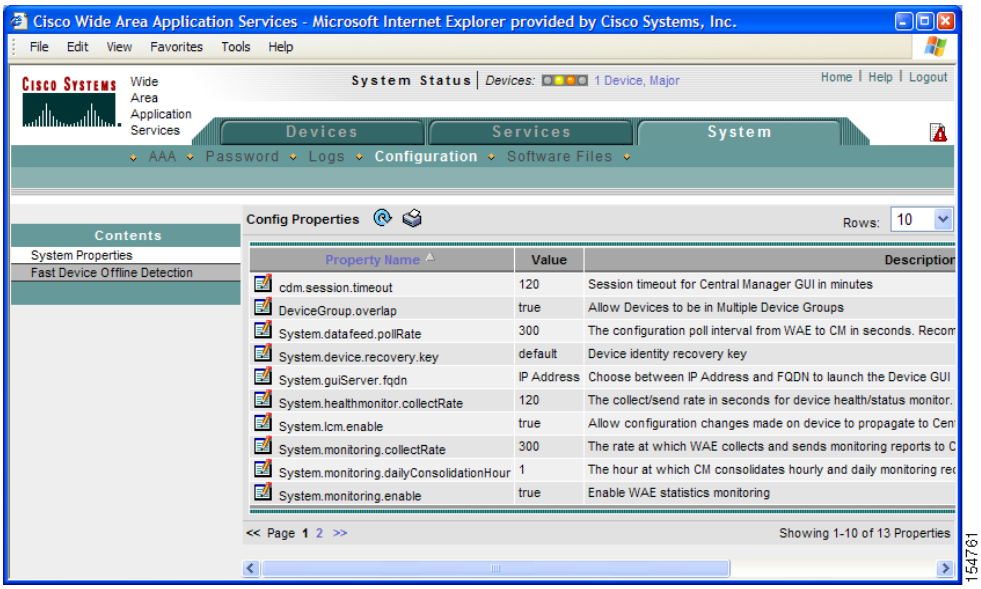
Table 9-2 Descriptions for System Configuration Properties (continued)

System Property	Description
System.monitoring.monthlyConsolidationFrequency	How often (in days) the WAAS Central Manager consolidates daily monitoring records into monthly records. If this setting is set to 1, the WAAS Central Manager checks if consolidation needs to occur every day, but only performs consolidation if there is enough data for consolidation to occur. The default is 14 days. When a monthly data record is created, the corresponding daily records are removed from the database. Consolidation occurs only if there is at least two calendar months of data plus the consolidation frequency days of data. This ensures that the WAAS Central Manager always maintains daily data records for the past month and can display data on a day level granularity for the last week. For example, if data collection starts on February 2nd, 2006 and System.monitoring.monthlyConsolidationFrequencyis set to 14, then the WAAS Central Manager checks if there is data for the past two calendar months on the following days: Feb 16th, March 2nd, March 16th, and March 30th. No consolidation will occur because there is not enough data on these days. On April 13th, however, two calendar months of data exists. The WAAS Central Manager then consolidates data for the month of February and deletes the daily data records for that month.
System.monitoring.recordLimitDays	Maximum number of days of monitoring data to maintain in the system. The default is 1825 days.
System.print.driverFtpTimeout	Maximum number of seconds to wait for printer driver files to transfer by FTP. The range is 10 to 1800 seconds. The default is 600 seconds.
System.rpc.timeout.syncGuiOperation	Timeout in seconds for the GUI synchronization operations for the Central Manager to WAE connection. The default is 50 seconds.

To view or modify the value of a system property, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **System > Configuration**. The Config Properties window appears. (See Figure 9-3.)

Figure 9-3 Config Properties Window



Step 2 Click **Page 2** to see the second page of this window.

Step 3 Click the **Edit** icon next to the system property that you want to change. The Modifying Config Property window appears.

Step 4 From a drop-down list, enter a new value or choose a new parameter, depending on the system property that you want to change.

Step 5 Click **Submit** to save the settings

Configuring Faster Detection of Offline WAAS Devices

You can detect offline WAAS devices more quickly if you enable the fast detection of offline devices. A WAAS device is declared as offline when it has failed to contact the WAAS Central Manager for a getUpdate (get configuration poll) request for at least two polling periods. (See "About Faster Detection of Offline Devices" section on page 9-13 for more information about this feature.)

To configure fast detection of offline WAAS devices, follow these steps:

Step 1 From the WAASA Central Manager GUI, choose **System > Configuration**. The Config Properties window appears.

Step 2 In the Contents pane, choose **Fast Device Offline Detection**. The Configure Fast Offline Detection window appears.

Note The fast detection of offline devices feature is in effect only when the WAAS Central Manager receives the first UDP heartbeat packet and a getUpdate request from a device.

Step 3 Check the **Enable** check box to enable the WAAS Central Manager to detect the offline status of devices quickly.

Step 4 In the Heartbeat Rate (Seconds) field, specify how often devices should transmit a UDP heartbeat packet to the WAAS Central Manager.

Step 5 In the Heartbeat Fail Count field, specify the number of UDP heartbeat packets that can be dropped during transmission from devices to the WAAS Central Manager before a device is declared offline.

Step 6 In the Heartbeat UDP Port field, specify the port number using which devices will send UDP heartbeat packets to the primary WAAS Central Manager.

The Maximum Offline Detection Time field displays the product of the failed heartbeat count and heartbeat rate.

Maximum Offline Detection Time = Failed heartbeat count * Heartbeat rate

If you have not enabled the fast detection of offline devices feature, then the WAAS Central Manager waits for at least two polling periods to be contacted by the device for a getUpdate request before declaring the device to be offline. However, if you enable the fast detection of offline devices feature, then the WAAS Central Manager waits until the value displayed in the Maximum Offline Detection Time field is exceeded.

If the WAAS Central Manager receives the Cisco Discovery Protocol (CDP) from a device, then the WAAS Central Manager GUI displays the device as offline after a time period of 2* (heartbeat rate) * (failed heartbeat count).

Step 7 Click **Submit**.

About Faster Detection of Offline Devices

Communication between the WAAS device and WAAS Central Manager using User Datagram Protocol (UDP) allows faster detection of devices that have gone offline. UDP heartbeat packets are sent at a specified interval from each device to the primary WAAS Central Manager in a WAAS network. The primary WAAS Central Manager tracks the last time that it received a UDP heartbeat packet from each device. If the WAAS Central Manager has not received the specified number of UDP packets, it displays the status of the nonresponsive devices as offline. Because UDP heartbeats require less processing than a getUpdate request, they can be transmitted more frequently, and the WAAS Central Manager can detect offline devices much faster.

You can enable or disable this feature, specify the interval between two UDP packets, and configure the failed heartbeat count. Heartbeat packet rate is defined as the interval between two UDP packets. Using the specified heartbeat packet rate and failed heartbeat count values, the WAAS Central Manager GUI displays the resulting offline detection time as a product of heartbeat rate and failed heartbeat count. If the fast detection of offline devices is enabled, the WAAS Central Manager detects devices that are in network segments that do not support UDP and uses getUpdate (get configuration poll) request to detect offline devices.

By default, the feature to detect offline devices more quickly is not enabled.

Configuring Alarm Overload Detection

WAAS devices can track the rate of incoming alarms from the Node Health Manager. If the rate of incoming alarms exceeds the high-water mark (HWM), then the WAAS device enters an alarm overload state. This situation occurs when multiple applications raise alarms at the same time to report error conditions. When a WAAS device is in an alarm overload state, the following occurs:

- SNMP traps for subsequent alarm raise and clear operations are suspended. The trap for the raise alarm-overload alarm and the clear alarm-overload alarm are sent; however, traps related to alarm operations between the raise alarm-overload alarm and the clear alarm-overload alarm operations are suspended.
- Alarm overload raise and clear notifications are not blocked. The alarm overload state is communicated to SNMP and the Configuration Management System (CMS). However, in the alarm overload state, SNMP and the CMS are not notified of individual alarms. The information is only available by using the CLI.
- The WAAS device remains in an alarm overload state until the rate of incoming alarms decreases to the point that the alarm rate is less than the low-water mark (LWM).
- If the incoming alarm rate falls below the LWM, the WAAS device comes out of the alarm overload state and begins to report the alarm counts to SNMP and the CMS.

When the WAAS device is in an alarm overload state, the Node Health Manager continues to record the alarms being raised on the WAAS device and keeps a track of the incoming alarm rate. Alarms that have been raised on a WAAS device can be listed using the **show alarm** CLI commands that are described in the *Cisco Wide Area Application Services Command Reference.*

To configure alarm overload detection for a WAAS device (or device group), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**). The Devices (or Device Groups) window appears.

Step 2 Click the **Edit** icon next to the device (or device group) for which you want to configure the alarm overload state.

Step 3 Click **Show Advanced** to display all menu items in the Contents pane.

Step 4 In the Contents pane, choose **General Settings > Notification and Tracking > Alarm Overload Detection**. The Alarm Overload Detection Settings window appears.

Step 5 Uncheck the **Enable Alarm Overload Detection** check box if you do not want to configure the WAAS device (or device group) to suspend alarm raise and clear operations when multiple applications report error conditions. This check box is checked by default.

Step 6 In the Alarm Overload Low Water Mark (Clear) field, enter the number of incoming alarms per second below which the WAAS device comes out of the alarm overload state.

Low-water mark is the level up to which the number of alarms must drop before alarms can be restarted. The default value is 1. The low-water mark value should be less than the high-water mark value.

Step 7 In the Alarm Overload High Water Mark (Raise) field, enter the number of incoming alarms per second above which the WAAS device enters the alarm overload state. The default value is 10.

Step 8 Click **Submit** to save the settings.

To configure alarm overload detection from the CLI, you can use the **alarm overload-detect** global configuration command.