Cisco Network Building Mediator User Guide

Release 3.1.3

February, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-21272-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Network Building Mediator User Guide
© 1999–2012 Cisco Systems, Inc. All rights reserved.

Send documentation comments to cbsbu-docfeedback@cisco.com

CONTENTS

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the Cisco Network Building Mediator User Guide, Release 3.1.3.

To check for additional information about Cisco Network Building Mediator, Release 3.1.3, see the *Release Note for Cisco Network Building Mediator, Release 3.1.3*.

Table 1 summarizes the new and changed features for the Cisco Network Building Mediator User Guide, Release 3.1.3, and tells you where they are documented.

Table 1 New and Changed Features for Release 3.1.3

Feature	Description	Changed in Release	Where Documented
Enernoc Exporter Ehancements	Support for the Enernoc V2 formatter, a proprietary CSV format that includes additional configurable attributes.	3.1.3	Chapter 4, "Mediator configTOOL"
ETC/USAP Protocol	The ETC (Electronic Theatre Controls) Unison Serial Access Protocol (USAP) controls the Unison lighting control system. The standard is applied for the point-to-point command exchange between Mediator devices and the Unison system	3.1.3	Chapter 6, "Ports and Protocols"
Delphi Web Services Protocol	The Delphi Web Server provides the Banquet Event Order (BEO) service and the Meeting Space Request service. The Delphi web service that runs on the Cisco Network Building Mediator supports only the meeting space request service.	3.1.3	Chapter 6, "Ports and Protocols"
Omni Systems Metering Protocol	This protocol makes use of master-slave protocol in which the Mediator acts as a master and polls the Omnimeter to the interface to read data.	3.1.3	Chapter 6, "Ports and Protocols"

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 1 New and Changed Features for Release 3.1.3

Feature	Description	Changed in Release	Where Documented
Open Automated Demand Response (OpenADR)	Involves the dynamic management of energy usage through cooperation between power consumers, their electric utility, and the electric system operator (or the independent system operator - ISO). The OpenADR standard enables ISOs and electric utilities to continuously send signals to power consumers, which can be automatically translated into load sheds or shifts.	3.1.3	Chapter 17, "OpenADR Client Service"
TCS Basys Protocol.	Supports the TCS Basys protocol, which is a proprietary master/slave communication protocol.	3.1.3	Chapter 6, "Ports and Protocols"
Transport Layer Security (TLS) 1.0 Support	TLS 1.0 is enabled in SRNA communications that occur between Mediators as well as between a Mediator and a Mediator Manager.	3.1.3	Chapter 6, "Ports and Protocols"
The NTP (Network Transport Protocol)	The NTP ensures that the time in all of the Mediators is synchronized. This allows scheduling (for example, equipment start and stop times) and logging operations to take place when the user expects.	3.1.3	Chapter 4, "Mediator configTOOL"
IP tables and Cron Package Tools	Cron Package allows you to manage the regular background processing, while iptables allows you to setup, maintain, and inspect the tables of IP Packet filter rules in the Linux kernel.	3.1.3	Refer to the IP table and Cron Package MAN pages that are available on the ISO image.

Send documentation comments to cbsbu-docfeedback@cisco.com

Preface

This preface introduces the *Cisco Network Building Mediator User Guide* and includes the following sections:

Audience

This guide is for the experienced system administrator responsible for configuring and maintaining the Cisco Network Building Mediator.

Organization

This guide is organized as follows:

Chapter	Title	Description
New and Changed Information	New and Changed Information	Provides new and changed information for the new Cisco Network Building Mediator release.
Chapter 1	Introduction	Provides an overview of the Building Automation System (BAS), Mediator system, and Mediator Operating Environment (MOE) system software.
Chapter 2	Getting Started	Describes how to configure, upgrade, back up, and restore the Mediator.
Chapter 3	Licensing Requirements	Describes how to purchase, download, install, and verify licenses.
Chapter 4	Mediator configTOOL	Describes how to install, start, configure, and use configTOOL.

Send documentation comments to cbsbu-docfeedback@cisco.com

Chapter	Title	Description
Chapter 5	perfectHOST	Describes how to install and use perfectHOST graphical programming software to program the Cisco Network Building Mediator.
Chapter 6	Ports and Protocols	Describes how to use the configTOOL to configure communications (com) port nodes and protocols on the Cisco Network Building Mediator.
Chapter 7	KNX Deployment	Describes how to configure the KNX protocol and provides useful troubleshooting tips for configuring the KNX protocol on the Cisco Network Building Mediator.
Chapter 8	Getting Started with Mediator Web Client	Describes the overview of the Mediator web client.
Chapter 9	Managing Events	Describes how to manage events, alarms, triggers, alarm exporters, and global alarms using the Mediator web client.
Chapter 10	Managing Security	Describes how to configure and manage users, roles, and policies using the web client.
Chapter 11	Managing Trends	Describes how to configure and manage trends using the web client.
Chapter 12	Managing Schedules	Describes how to create and configure schedules that could be duplicated across an entire enterprise.
Chapter 13	Customizing HTML Pages Using Web Express	Describes how to create HTML monitor drawings using customizable widgets and graphics.
Chapter 14	Energywise Manager	Describes how to configure and view the Energywise service and energy consumption using configTOOL and the Mediator.
Chapter 15	Enterprise Navigation	Describes how to browse all the systems connected to the Mediator, navigate to different levels using the navigation tree, and monitor and control systems attached to the Mediator in real time.
Chapter 16	Global Setpoints	Describes how to monitor and modify setpoints across different devices and systems that are connected to the Mediator.
Chapter 17	OpenADR Client Service	Describes how to configure the OpenADR client service on the Mediator.

Document Conventions

This guide uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
`screen` font	Terminal sessions and information the system displays are in `screen` font.

Send documentation comments to cbsbu-docfeedback@cisco.com

Convention	Description
boldface screen font	Information you must enter is in **boldface screen** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
Option > Option	Used to select a series of menu options.
[ ]	Elements in square brackets ([ ]) are optional.

Notes use the following convention:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Cautions use the following convention:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

The documentation set for the Cisco Network Building Mediator (Mediator) includes the following documents:

- *Cisco Network Building Mediator User Guide Release 3.x.x*
- *Cisco Network Building Mediator 2500 and 5000 Hardware Installation Guide Release 3.x.x*
- *Cisco Network Building Mediator XML RPC API Guide, Release 3.x.x*
- *Cisco Network Building Mediator Quick Start Guide 3.x.x*
- *Regulatory Compliance and Safety Information for the Cisco Network Building Mediator*
- *Release Notes for Cisco Network Building Mediator Software Release 3.x*
- *Product Pointer card for Cisco Network Building Mediator 2500 and 5000*
- *Welcome Document for Cisco Network Building Mediator 2500 and 5000*

Obtaining Documentation and Submitting a Service Request

For information on obtaining 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, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (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.

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 1

Introduction

This chapter provides a detailed overview of Building Automation System (BAS), the Cisco Network Building Mediator system, and Mediator Operating Environment (MOE) system software.

This chapter includes the following sections:

Note Before you install, operate, or service the system, read the *Regulatory Compliance and Safety Information for the Cisco Network Building Mediator* document for important safety information.

Building Automation System Overview

Building Automation System (BAS) describes the functionality of the control system, which offers comprehensive and co-coordinated control of one or more major system functions required in a facility, such as the following:

- Heating, Ventilating, and Air Conditioning (HVAC) system
- Lighting system
- Security system
- Fire and Life safety system

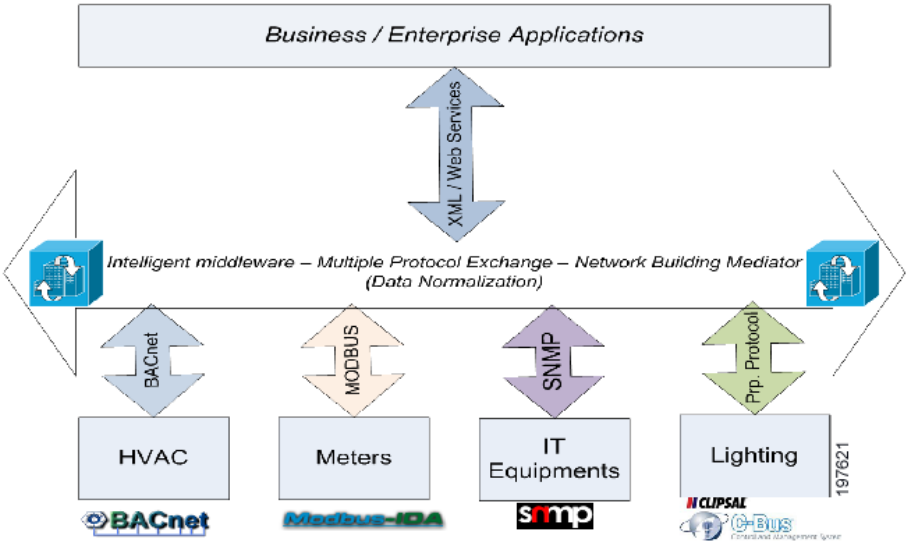
These building systems are still being installed and operated in silos for either security reasons or due to the challenges in system integration, but this reliance limits the types of applications that can emerge from the integration. In particular, it limits your ability to use BAS for your own purposes, limiting the ability to integrate BAS functions with real enterprise systems. The move to more integrated building services also requires tighter integration of the mostly heterogeneous technologies. Here evolves the need for an intelligent middleware technology that can enable businesses to integrate building infrastructure and information technology (IT) applications over a common Internet Protocol (IP) network. This intelligent middleware would aggregate, normalize, make available all data from the siloed building systems, and allow data to pass bi-directionally from the building systems to enterprise business applications through web services.

Send documentation comments to cbsbu-docfeedback@cisco.com

The core function of the BAS is to keep the building climate within a specified range, provide lighting based on an occupancy schedule, monitor system performance and device failures, and provide e-mail or text notifications to building engineering staff. The BAS functionality reduces building energy and maintenance costs when compared to a non-controlled building.

Figure 1-1 displays a typical Cisco Network Building Mediator(Mediator) integration architecture.

Figure 1-1 Cisco Network Building Mediator Integration Architecture



Mediator System Overview

The Mediator provides a network-based framework, which allows the convergence of multiple disparate building systems onto an IP network, resulting in improved efficiency and greater energy savings.

A Mediator system includes hardware and software components. The Mediator is a hardware component; configTOOL, perfectHOST, and Mediator web client are the software components of the system.

- configTOOL—The software used to configure the Multi-Protocol Exchange (MPX) of the Mediator.
- perfectHOST—The graphical programming software used to program the Cisco Building Intelligence controllers.
- Mediator web client—A suite of advanced system software tools used to configure, program, and monitor the Mediator.

Warning **Installation of the equipment must comply with local and national electrical codes.**

Figure 1-2 displays a typical Mediator system architecture.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 1-2 Mediator System Architecture

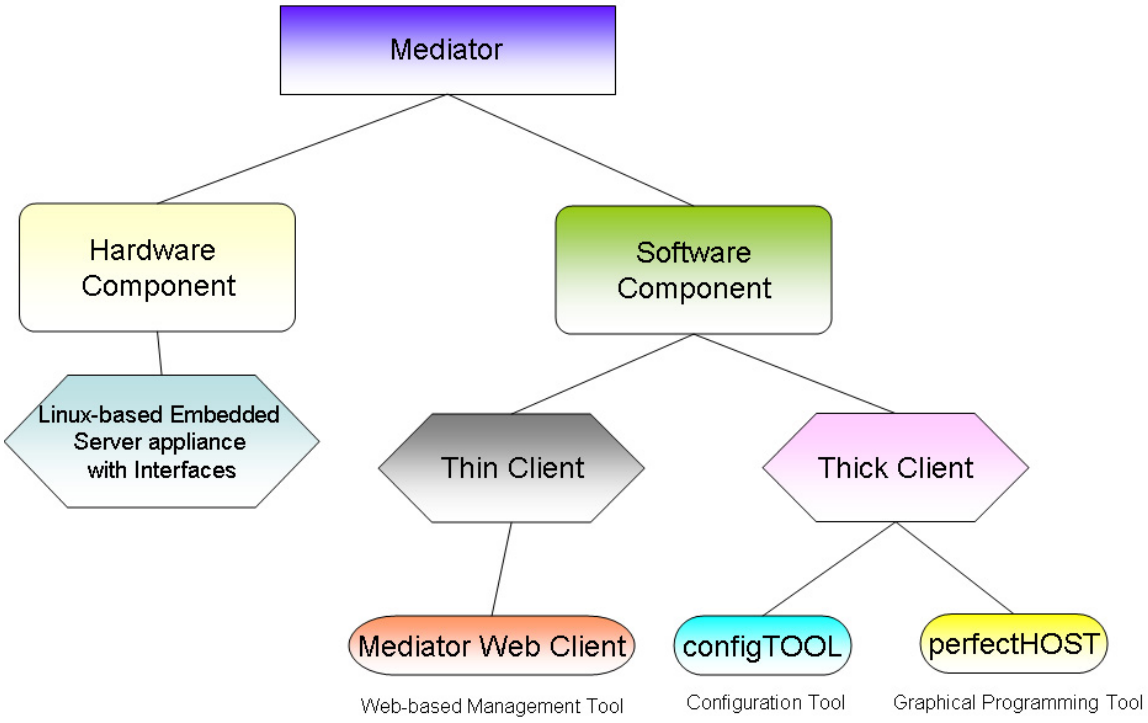
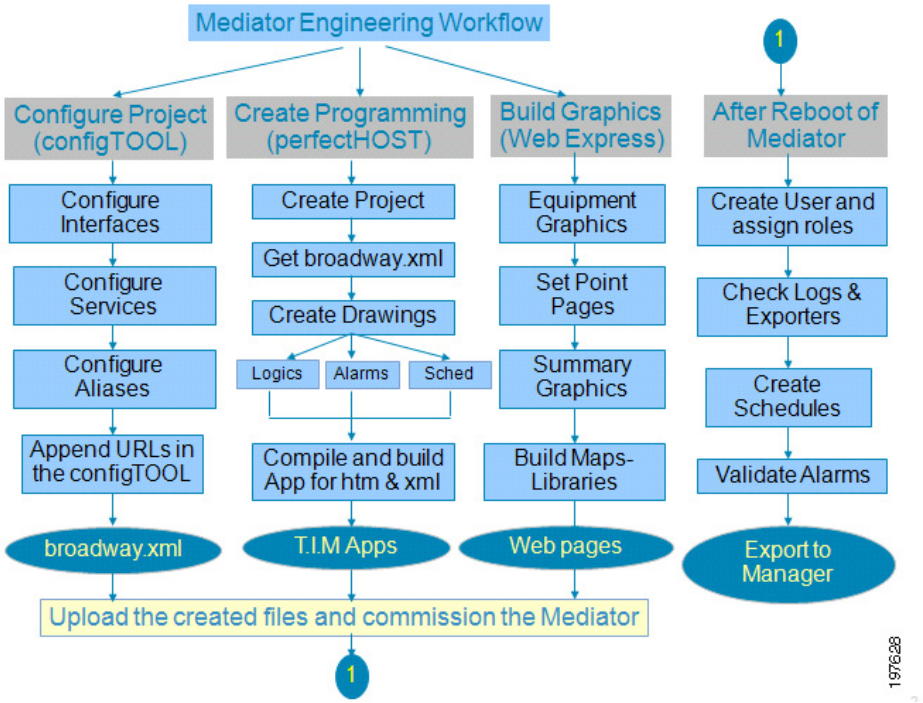


Figure 1-3 displays a typical Mediator engineering workflow.

Figure 1-3 Mediator Engineering Workflow



Send documentation comments to cbsbu-docfeedback@cisco.com

Mediator Framework Overview

Mediator Framework is the software application that provides the core function of the Mediator. The Mediator Framework gives the Mediator its Multi-Protocol Exchange capabilities, including the following:

- Assembling a running system from configuration data.
- Getting and setting values.
- Processing raw data.
- Presenting data from disparate sources in a uniform format.
- Making data easily available to you.
- Providing services such as data logging and HTTP services.
- Providing an environment for custom system configuration.
- Providing an environment for developing custom solutions.

A key feature of the Mediator Framework architecture is Dynamic System Configuration (DSC). DSC allows the Mediator Framework to assemble a system that includes only the program code required by a particular site configuration.

The Mediator Framework provides the structure upon which represented site systems are built. It provides the following functionality, allowing the Mediator to configure any site:

- Assembly of the system from configuration data.
- The operating environment in which that system runs.
- The existing framework can be modified or extended without shutting the system down.

The Mediator Framework represents a site by assembling a tree structure of objects called nodes. Nodes are software abstractions that represent the relationships between objects in the system. A node is a named object that exchanges information with other nodes.

For example, an RS-232 port, a Modbus line handler, a data point, and so on are named objects which support the exchange of information with other nodes.

The Mediator Framework structures nodes hierarchically. In the Mediator Framework terminology, a child node is a node that has a subordinate relationship to another node (for example, a Modbus handler configured under a COM port). The node to which a child is subordinate is called a parent node. The child nodes that the Mediator Framework automatically inserts under the parent nodes are called inherent child nodes.

The Mediator Framework creates a global name space on the Mediator in the form of a URL structure that resembles a file path made up of objects with parent-child relationships.

For example, the file:

/interfaces/com1/modbus/meter_1/*max.kW*

uniquely identifies a data point *max.kW* as a node whose parent node is a Veris meter personality, whose parent node is a Modbus line handler, whose parent node is com1, whose parent node is the interfaces anchor, whose parent node is the host device.

Send documentation comments to cbsbu-docfeedback@cisco.com

The top level (root) of the node tree is the host, and is represented by a forward slash (/). In the standard system, the host is a Mediator device. Because every node has a name and a parent going up to the root node in the name space, the Mediator Framework can look up any node on the Mediator host by its URL name. The nodes at the level immediately under the root are called anchors. The configTOOL has three anchor nodes representing the three main node categories of the Mediator Framework:

1. Interfaces—Interface nodes include the I/O ports and sensors of the Mediator, and the devices connected to them.
2. Services—Service nodes support data exchange (for example, the Logger, network services such as the HTTP server, and so on.)
3. Aliases—Alias nodes are used to assign alternative names to other nodes. Aliases allow you to assign a meaningful name to any node in the system. In addition, you can use aliases to group into a single folder related nodes that reside in different parts of the node tree.

The Mediator software includes two files that determine the operating parameters:

- The configuration file
- The configuration database

The configuration file is an XML file that describes the system configuration. The configTOOL generates this file after you finish and saves the entries specifying the configuration. At system startup, the Mediator Framework parses the configuration file and uses the information it contains to configure all of the nodes in the system.

Note The standard Mediator software includes a generic configuration file that allows the Mediator Framework to configure a minimal running system if configTOOL is not used to generate a configuration file.

The configuration database is an XML file that contains the NodeDefs (the node definitions) that specify the capabilities and requirements for each node. When you configure a node, configTOOL uses the information in the configuration database file to list the available options based on matching parent node capabilities to the requirements of child node.

The configTOOL allows you to edit the configuration file.

Mediator Operating Environment (MOE) System Software

The Mediator Operating Environment (MOE) system software is based on the current Linux kernel. Linux is a UNIX-like, open-source, fully featured operating system that provides true multitasking, multithreading, virtual memory, shared libraries, demand loading, shared copy-on-write executables, sophisticated memory management, loadable device driver modules, and TCP/IP networking. It allows the Mediator to run multiple services and protocols simultaneously and still respond to events generated in the network environment. Linux supports a broad range of open and secure networking capabilities.

In the event of a system failure, its full-journaling file system restores the data on the disk to its pre-failure configuration. It also recovers unsaved data and stores it in the location where it would have gone if the system had not failed.

The Mediator software consists of two main components, the MOE (operating system) and the Mediator Framework (application).

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 2

Getting Started

This chapter describes how to upgrade the Cisco Network Building Mediator (Mediator) and perform preliminary tasks, such as configuring network settings and modifying user accounts.

This chapter includes the following sections:

Note Before you install, operate, or service the system, read the *Regulatory Compliance and Safety Information for the Cisco Network Building Mediator* document for important safety information.

Prerequisites

This section includes the following topics:

Power Supply Requirements

You need a 24 VAC/VDC Power Supply to power on the Mediator.

Caution Use a UL/CSA/IEC 60950 Limited Power Source (LPS) or Class 2 certified approved power supply.

Send documentation comments to cbsbu-docfeedback@cisco.com

Warning **The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.**

Hardware Requirements

- 600 MHz Intel Pentium III processor (or equivalent)
- Windows 2000 SP2 or Windows XP
- 256 MB RAM (512 MB recommended)
- 800 MB available disk space
- Serial console cable (to connect between the PC Com1 port and the Mediator console port)

Other Requirements

Before you initiate the installation process, you must ensure the following:

- You have access to a third-party terminal communications utility such as HyperTerminal or PuTTy.

  When you connect to the Mediator using a third-party utility, use the following baud rates:
  - For Cisco Network Building Mediator 2400 and 4800, the baud rate is 38400 per second.
  - For Cisco Network Building Mediator 2500 and 5000, the baud rate is 115200 per second.
- You have access to the latest image file available on Cisco.com.
- Internet Explorer 7.0 and 8.0, or Mozilla Firefox 3.5 and later.

Caution Do not open or remove the chassis cover or operate the unit without the cover installed.
Do not remove or reapply the thermal conductive pad that connects the heat sink to the CPU. Improper thermal pad contact can cause the CPU to overheat and produce intermittent failure. Removal of the thermal pad can cause the CPU to shut down.

Note If you are unable to resolve a problem with the product, contact the Cisco Technical Assistance Center (TAC) for assistance and further instructions.

Setting Up the Mediator

This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Connecting Power to the Mediator

The Mediator operates on 24 VAC or 24 VDC power and is shipped with a 24 VDC power supply (100 VDC-240 VDC input).

This section describes how you must connect the Mediator to the DC and AC power and includes the following topics:

Connecting to DC Power

This section includes the following topics:

Mediator 2400 and 4800

The 24 VDC power supply is connected to the uppermost screw terminal and the GND terminal using 18-24 AWG wire. The positive (+) transformer wire should be connected to the uppermost terminal, and the negative (-) wire should be connected to the GND terminal. The Mediator is shipped with the leads of the power supply screwed on to the terminal block. To power on the Mediator, plug the terminal block into the Mediator socket.

Mediator 2500 and 5000

The power supply uses a plug type connector instead of a terminal block. To power on the Mediator, connect the power supply to the power jack on the Mediator.

Connecting to AC Power

This section includes the following topics:

Mediator 2400 and 4800

The AC leads of a 24 VAC class 2 transformer (minimum 40 VA) are connected to the two uppermost screw terminals using 18 - 24 AWG wire. If the transformer has a ground lead, then it is connected to the GND terminal.

Mediator 2500 and 5000

The AC leads of a 24 VAC class 2 transformer (minimum 40 VA) are connected to the two AC screw terminals using 18 - 24 AWG wire.

Tighten the screws using the following terminal torque specifications:

- (N-m) 0.3 – 0.5
- (in-lbs.) 2.7 – 4.4

Send documentation comments to cbsbu-docfeedback@cisco.com

Monitoring the Mediator

This section includes the following topics:

LED Codes for the Mediator 2400 and 4800

Table 2-1 provides a description of the LED codes used by Mediator 2400 and 4800.

Table 2-1 LED Codes for Mediator 2400 and 4800

LED Code	Status	Description
Power LED		
None	Power off Initializing the rebooting	The Mediator is not powered on. The Mediator is initializing. The Mediator is rebooting.
Green flash	Power on	The Mediator is powered on.
Status LED		
One long flash followed by a pause.	Idle	The Mediator is booted up and running, but the framework is not running.
Two short flashes followed by a pause.	Installing	The Mediator Framework is starting for the first time and is installing itself.
Three long flashes followed by a pause.	Running	The Mediator Framework is running normally.
Four short flashes followed by a pause.	Error	The Mediator Framework is running, but errors are present. Check the Message Log for details.
Three short flashes followed by three long flashes, followed by three short flashes, followed by a pause.	Emergency	The Mediator Framework has stopped running for at least two minutes.

LED Codes for the Mediator 2500 and 5000

Table 2-2 provides a description of the LED codes used by the Mediator 2500 and 5000.

Table 2-2 LED Codes for Mediator 2500 and 5000

LED Code	Status	Description
Power LED		
None	Power off	The Mediator is not powered on.
Solid Yellow	Power on	The Mediator is powered on.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 2-2 LED Codes for Mediator 2500 and 5000 (continued)

LED Code	Status	Description
Status LED		
White flashes	Idle	The Mediator is booted up and running, but the framework is not running.
Continuous green flashes	Installing	The Mediator Framework is being installed.
Short blue flashes	Configuring	The Mediator Framework is being configured.
Blue flashes	Initiating	The Mediator Framework is starting for the first time.
Continuous short and long green flashes	Running	The Mediator Framework is running.
Continuous red flashes	Error	The processors are not communicating with one another.
None	Off	The co-processor firmware is not loaded.
Sequential red, green, and blue flashes	Installing	The co-processor firmware is being loaded.

Configuring the Mediator

While the initial login to the Mediator must be done through the Mediator console port, you can also configure the Mediator remotely. To configure the Mediator remotely, you can use any third-party terminal communication utility.

Note For Mediator 2500 and 5000, both the initial login and the configuration, can be done remotely.

Table 2-3 lists the utilities that you can use to configure the Mediator remotely.

Table 2-3 Options to configure the Mediator

Configuration Method	Type of Utility
Console port	HyperTerminal (allows you to log in to the Mediator Linux command line when you connect the PC to the Mediator console port using the null modem cable supplied with each Mediator).
Remote	PuTTY or any SSH Client (allows you to log in to the Mediator Linux command line by connecting with a Mediator over the Internet).

The first time you log in to the Mediator 2400 and 4800, you could be forced to change the default administrator password. This does not occur when you log in to the Mediator 2500 and Mediator 5000 for the first time.

Send documentation comments to cbsbu-docfeedback@cisco.com

You can also configure the network settings when you log in to the Mediator for the first time.

To configure the Mediator using HyperTerminal, perform the following steps:

Step 1 Connect a PC to the console port of the Mediator using a null modem cable.

Step 2 Launch HyperTerminal.

A New Connection - HyperTerminal window appears with the Connection Description dialog box.

Step 3 In the Name text box, enter a name for the new connection, and click **OK**.

The Connect To dialog box appears.

Step 4 From the Connect using drop-down list, choose the COM port used to connect to the Mediator.

The COM Properties dialog box appears.

Step 5 Click **Restore Defaults**. The default values for the text boxes in the COM properties dialog box are as follows:

- Bits per second - 38400

Note For Cisco Network Building Mediator 2500 and 5000, the default value is 115200 bits per second.

- Data bits - 8
- Parity - None
- Stop bits - 1
- Flow control - None

Step 6 Click **Apply**, and then click **OK**.

Step 7 Choose **File > Save As**, and save the HyperTerminal session to the desktop.

You can now launch HyperTerminal from the desktop.

Step 8 Press **Enter** twice.

The Mediator system login prompt appears.

Step 9 Enter **mpxadmin** and press **Enter** when prompted for the username and password.

Note For Mediator 2500 and 5000, prior to using the mpxconfig utility, perform the following steps:

a. Enter **./firstboot** (wait for command prompt to return).

b. Enter the **reboot** command.

After the Mediator reboots, log in to the Mediator and continue to Step 10.

Step 10 Enter **mpxconfig** and press **Enter**.

Tip We recomend you enter *export TERM=vt100* on bash before you use the mpxconfig utility.

Step 11 When the mpxconfig utility launches. By default, the Global settings are highlighted.

Send documentation comments to cbsbu-docfeedback@cisco.com

The mpxconfig utility allows you to configure the network settings and set the date and time.

Step 12 Press **Enter**.

The Global settings text boxes appear.

Step 13 In the Global settings text boxes, enter the hostname, domain, gateway, name server, proxy server, and location.

By default, the IP forwarding status is disabled. Press **Spacebar** to enable the IP forwarding status.

Step 14 Press **Enter** to save changes in the global settings and return to the main menu.

Step 15 Press **ESC** to cancel the changes.

Step 16 Navigate to Ethernet port 0, and press **Enter**.

The Ethernet port selection option appears.

Step 17 Press **Spacebar** to enable or disable DHCP.

Step 18 Scroll down to change the IP address and Net mask.

You can also press **Tab** to move the cursor between text boxes.

Step 19 To return to the main menu, press **Enter**.

Step 20 Repeat Step 16 to Step 19 to configure Ethernet port 1.

Step 21 Scroll down to System Date and Time and press **Enter**.

The System Date and Time settings option appears.

Step 22 Press **Spacebar** to select the appropriate time zone.

Step 23 Scroll down to set the date and time

Step 24 To return to the main menu, press **Enter**.

Step 25 Press **Esc** to exit.

The mpxconfig window appears.

Step 26 Press **Enter** to save the changes or press **ESC** to discard the changes.

Step 27 Type **R** to reboot the system or press any other key to exit.

Note Changes to the network settings are not effective until you reboot the Mediator.

Upgrading the Mediator

This section describes the procedures for upgrading the Mediator Operating Environment (MOE) and the Mediator Framework.

Note This section is not necessary if the Mediator is already running the latest MOE and Mediator Framework. To verify the MOE and Mediator Framework, see the "Verifying the Mediator Framework and MOE" section on page 2-15.

This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Downloading the Image File

Before you begin the upgrade process, you must download the latest image file from Cisco.com.

To download the image file, perform the following steps:

Step 1 Log in to Cisco.com to download the image file.

If you are not a registered user of Cisco.com, obtain your Cisco.com user ID from the following website: http://tools.cisco.com/RPF/register/register.do

Step 2 Download the image file to a folder location on your local system.

Extracting the Image File Contents

After you download the image file on to your local system, you must extract the image file contents using any Zip file utility such as WinZip. You cannot copy the image file to the Mediator until you extract the image file contents.

Table 2-4 lists the details on the extracted image file contents.

Table 2-4 CCO Distribution Matrix

Hardware/Tools	Software Version	File Category	File Name	Contents
5000	3.1.3-1	Installation Software	NBM5000-SW-3.1.3-1-K9.iso	• MANIFEST • cisco.nbm-5000-moe-1.21-fw-3.1.3-1 • cisco.nbm-5000-moe-1.21-fw-3.1.3-1.md5
5000	3.1.2-6	Installation Software	NBM5000-SW-3.1.2-6v2-K9.iso	• MANIFEST • cisco.nbm-5000-moe-1.21-fw-3.1.2-6 • cisco.nbm-5000-moe-1.21-fw-3.1.2-6.md5

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 2-4 CCO Distribution Matrix (continued)

Hardware/Tools	Software Version	File Category	File Name	Contents
4800	3.1.3-1	Installation Software	NBM4800-SW-3.1.3-1-K9.iso	• NBM4800-SW-3.1.3-1-K9.tx • cisco.nbm-4800.Release3.1.3-1.tgz • moe-3.0.4to3.0.9-upgrade.tgz • moe-3.0.9.tgz • netinstall-1.0.1.tgz • version.txt
4800	3.1.2-6	Installation Software	NBM4800-SW-3.1.2-6v2-K9.iso	• NBM4800-SW-3.1.2-6-K9.txt • cisco.nbm-4800.Release3.1.2-6.tgz • moe-2.5.1to3.0.8-upgrade.tgz • moe-3.0.4to3.0.8-upgrade.tgz • moe-3.0.8.tgz • netinstall-1.0.1.tgz • version.txt
2500	3.1.3-1	Installation Software	NBM2500-SW-3.1.3-1-K9.iso	• MANIFEST • cisco.nbm-2500-moe-1.21-fw-3.1.3-1 • cisco.nbm-2500-moe-1.21-fw-3.1.3-1.md5
2500	3.1.2-6	Installation Software	NBM2500-SW-3.1.2-6v2-K9.iso	• MANIFEST • cisco.nbm-2500-moe-1.21-fw-3.1.2-6 • cisco.nbm-2500-moe-1.21-fw-3.1.2-6.md5
2400	3.1.3-1	Installation Software	NBM2400-SW-3.1.3-1-K9.iso	• NBM2400-SW-3.1.3-1-K9.tx • cisco.nbm-2400.Release3.1.3-1.tgz • moe-3.0.4to3.0.9-upgrade.tgz • moe-3.0.9.tgz • netinstall-1.0.1.tgz • version.txt

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 2-4 CCO Distribution Matrix (continued)

Hardware/Tools	Software Version	File Category	File Name	Contents
2400	3.1.2-6	Installation Software	NBM2400-SW-3.1.2-6v2-K9.iso	• NBM2400-SW-3.1.2-6-K9.txt • cisco.nbm-2400.Release3.1.2-6.tgz • moe-2.5.1to3.0.8-upgrade.tgz • moe-3.0.4to3.0.8-upgrade.tgz • moe-3.0.8.tgz • netinstall-1.0.1.tgz • version.txt
configTOOL	3.1.2-2	Configuration Software	configtool_install_3_1_2-2.exe	NA
perfectHost	8.00.03	Programming Software	phwsetup.exe	NA

Send documentation comments to cbsbu-docfeedback@cisco.com

Copying the Image File to the Mediator

Table 2-5 describes the different methods you can use to copy the image file to the Mediator.

Table 2-5 Copying Image Files to the Mediator

Mediator Model	Method	Instructions
Mediator 2400/4800	SFTP or SCP File Transfer Client	Follow these steps: **a.** Open the SFTP or SCP File Transfer Client and enter the IP address of the Mediator in the Host Name text box. **b.** Enter **mpxadmin** in the Username and Password text boxes, and click **Login**. **c.** To copy a file from your PC to the Mediator, select the file from the left pane and place it in the appropriate directory in the right pane. **d.** Use the following directories: – Use the /usr/lib directory for the Mediator Framework upgrade file. – Use the **/** directory for the MOE upgrade file.
Mediator 2500/5000	SFTP or SCP File Transfer Client	Follow these steps: **a.** Open the SFTP or SCP File Transfer Client and enter the IP address of the Mediator in the Host Name text box. **b.** Enter **mpxadmin** in the Username and Password text boxes, and click **Login**. **c.** To copy a file from your PC to the Mediator, select the file from the left pane and place it in the /home/mpxadmin directory in the right pane.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 2-5 Copying Image Files to the Mediator (continued)

Mediator Model	Method	Instructions
Mediator 2500/5000	Universal Serial Bus (USB) Flash Drive	Follow these steps: **a.** Plug the USB Flash Drive into a USB socket on the Mediator. **b.** Connect to the Mediator using any third-party terminal communications utility or an SSH client. **c.** Enter **mpxadmin** in the Username and Password text boxes, and click **Login**. **d.** Enter **mount /dev/sdb1 /mnt** to mount the file system of the USB Flash device. **e.** Enter **cp /mnt/***install image* **/home/mpxadmin** to copy the new image file to the /home/mpxadmin directory.
Mediator 2500/5000	wget	Follow these steps: **a.** Connect to the Mediator using any third-party terminal communications utility or an SSH client. **b.** Enter **mpxadmin** in the Username and Password text boxes, and click **Login**. **c.** Enter **wget *http*** *server URL* ***image file name***.

Upgrading the Mediator 2400 and 4800

You can upgrade either the Mediator Framework or the Mediator Operating Environment (MOE) and the Mediator Framework.

Caution All image files are saved under the /var/mpx/www/http/images directory. Before you begin with the upgrade procedure, you must back up the entire folder. It is important that after you complete the upgrade procedure, you must restore the folder under the /usr/lib/broadway/opt/rz/omega/html/images directory to save all the customized images.

This section describes the procedure you can use to install or upgrade the Mediator Framework or the MOE and includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Mediator Framework

Before you begin with the upgrade procedure, verify that the Mediator is running a MOE that is compatible with the Mediator Framework that you want to upgrade.

For details on the MOE compatibility, see the Software Compatibility Matrix that is available in *Release Notes for the Cisco Network Building Mediator*.

To upgrade the Mediator Framework perform the following steps:

Step 1 Connect to the Mediator using an SCP and SSH client such as WinSCP and PuTTY.

Both the username and the password are mpxadmin.

Step 2 Copy the cisco.nbm-3.x.tgz file to the /usr/lib directory on the Mediator.

Step 3 Enter **init 2** to shut down the Mediator Framework.

Step 4 Enter the **cd /var/mpx/config** command.

Step 5 Enter the **mv broadway.xml broadway.orig.xml** command.

Step 6 Enter the **cd /usr/lib** command.

Step 7 Enter **ls** to view the list of files in the current working folder.

Step 8 Enter **rm -rf broadway** to remove the existing broadway folder.

Step 9 Enter **tar -xzvf cisco.nbm-3.x.tgz** to unzip the file and recreate the broadway folder.

Step 10 Enter **cd broadway** to navigate to the new broadway folder.

Step 11 Enter the **./install cisco.nbm** command.

Step 12 (Optional) Enter **./install -d cisco.nbm** to view the installation steps.

Upon the completion of installation process, you are prompted to enter the next command.

Step 13 Enter the **cd /var/mpx/config** command.

Step 14 Enter the **mv broadway.orig.xml broadway.xml** command.

Step 15 Enter **init 3** to restart the Mediator Framework.

Step 16 Enter **msglog_viewer -f** to watch the message logs.

Step 17 To verify that the appropriate Mediator Framework has been installed, see the "Verifying the Mediator Framework and MOE" section on page 2-15.

MOE and Mediator Framework

Before you begin with the upgrade procedure, check the MOE version that is currently running on the Mediator to determine which MOE upgrade file you must use.

For example, if the Mediator is running a MOE version 2.5.1, then use the moe-2.5.1 to 3.0.9-upgrade.tgz file or if the Mediator is running a MOE version 3.0.4, then use the moe-3.0.4to3.0.9-upgrade.tgz file.

To check the MOE version, log in to the Mediator Web Client and browse to the System page.

To upgrade the MOE and the Mediator Framework, perform the following steps:

Step 1 Connect to the Mediator using an SCP and SSH client such as WinSCP and PuTTY.

Send documentation comments to cbsbu-docfeedback@cisco.com

Both the username and the password are **mpxadmin**.

Step 2 Copy the **c**isco.nbm-3.x.tgz file to the /usr/lib directory on the Mediator.

Step 3 Copy the moe-*version*to3.0.9-upgrade.tgz file to the / directory on the Mediator.

Step 4 Enter **init 2** to shut down the Mediator Framework.

Step 5 Enter the **cd /var/mpx/config** command.

Step 6 Enter the **mv broadway.xml broadway.orig.xml** command.

Step 7 Enter the **cd /** command.

Step 8 Enter the **tar -xzvf moe-*version*to3.0.9-upgrade.tgz** command.

Step 9 Enter the **cd /usr/lib** command.

Step 10 Enter **rm -rf broadway** to remove the existing broadway folder.

Step 11 Enter **tar -xzvf cisco.nbm-3.x.tgz** to unzip the file and recreate the broadway folder

Step 12 Enter **cd broadway** to navigate to the new broadway folder.

Step 13 Enter the **./install cisco.nbm** command.

Step 14 (Optional) Enter **./install -d cisco.nbm** to view the installation steps.

Upon the completion of installation process, you are prompted to enter the next command.

Step 15 Enter the **cd /var/mpx/config** command.

Step 16 Enter the **mv broadway.orig.xml broadway.xml** command.

Step 17 Enter **reboot** to reboot the system.

Step 18 Re-connect to the Mediator using an SSH client.

Step 19 Enter **mpxadmin** for both, the username and the password.

Step 20 Enter **msglog_viewer -f** to watch the message log.

Step 21 To verify that the appropriate Mediator Framework and MOE have been installed, see the "Verifying the Mediator Framework and MOE" section on page 2-15.

Upgrading Mediator 2500 and 5000

Cisco Network Building Mediator 2500 and Cisco Network Building Mediator 5000 includes an **nbm_install** command that installs or upgrades the Mediator Operating Environment (MOE) and Mediator Framework.

To use the **nbm_install** command, the Mediator must download the image file from Cisco.com.

Caution The **nbm_install** command backs up certain configuration data such as the location, hostname, and the domain name, which gets restored after the install process. We recommend that the configuration data is manually backed up before the installation and restored later. To back up and restore the data manually, see the "Backing Up the Mediator" section on page 2-16 and the "Restoring the Mediator" section on page 2-16.

This section describes the procedure you use to install or upgrade the Mediator Operating Environment and the Mediator Framework.

Send documentation comments to cbsbu-docfeedback@cisco.com

To install the new operating system and the Mediator Framework, follow these steps:

Step 1 Connect to the Mediator using an SCP and SSH client such as WinSCP and PuTTY.

Both the username and the password are mpxadmin.

Step 2 Copy the new image to the /home/mpxadmin directory. Verify that the correct image has been transferred to this directory.

Step 3 Enter the **cd /home/mpxadmin** command.

Step 4 Enter **ls** to view the list of files in the current working directory. This helps to ensure that the transferred file is available in the /home/mpxadmin directory.

Step 5 Enter the **nbm_install** *image file name* command to install the new MOE and Mediator Framework.

The installation process causes the Mediator to enter a state which will terminate your current SSH session. Wait approximately 15 minutes for the installation to complete and re-establish the SSH connection.

Note Ensure that the power supply to the Mediator is not interrupted during the upgrade process.

Step 6 Enter **mpxadmin** for both the username and password.

Step 7 Enter the **./firstboot** command.

Step 8 Enter the **reboot** command.

Step 9 Re-connect to the Mediator using an SSH client.

Step 10 Enter **mpxadmin** for both, the username and the password.

Step 11 Enter **msglog_viewer -f** to watch the message log.

Step 12 To verify that the appropriate Mediator Framework and MOE has been installed, see the "Verifying the Mediator Framework and MOE" section on page 2-15.

Verifying the Mediator Framework and MOE

To verify the Mediator Framework and MOE, perform the following steps:

Step 1 Open a web browser on your PC and enter the URL for the Mediator. Be sure to include the "s" in https:// to connect your browser to the secure URL.

Step 2 Enter the default username and password in the Username and Password text boxes.

Both the default username and password are mpxadmin.

Step 3 Click **System**. On the Status tab, the Framework version text box displays the new image number that you have installed. If you have upgraded the MOE, then verify the correct version of the MOE.

Send documentation comments to cbsbu-docfeedback@cisco.com

Backing Up and Restoring the Mediator

This section includes the following topics:

Backing Up the Mediator

The backup function saves all of your applications, HTTP files, schedules, trends, and persistent data in a compressed archive file (.tgz), which is stored locally on the hard disk of your PC.

To back up a Mediator, perform the following steps:

Step 1 In the Mediator web client homepage, click **System**.

Step 2 Click the **Backup/Restore** tab.

The Backup/Restore tab appears.

Step 3 Click **Backup**.

The file download dialog box appears prompting you to open or save the backup file, mediator_backup.tgz.

Step 4 Click **Save**.

The file is saved on your local drive.

Restoring the Mediator

You can reverse the backup operation by using the restore function of the Mediator. The restore function takes the compressed archive file (.tgz) from the hard drive of your PC and restores the data to the Mediator.

If you modify the compressed archive file (.tgz) name on the hard drive of your PC, the restore function does not restore the data back to the Mediator.

Note We recommend that you restart the Mediator Framework to view the restored data on the web client. If you do not restart the Mediator Framework, the restored data will not appear on the web client, although it is restored to the Mediator.

To restore the Mediator, perform the following steps:

Step 1 In the Mediator web client homepage, click **System**.

Step 2 Click the **Backup/Restore** tab.

The Backup/Restore tab appears.

Step 3 Click **Browse** and navigate to the folder on your PC where the backup file is stored.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 Click **Restore**.

The files are restored to the Mediator and a message indicating the operation is successful is displayed.

Step 5 Launch PuTTY from your PC.

Step 6 In the PuTTY configuration window that appears, enter the Mediator IP address in the Host Name text box. The Username and Password text boxes appear.

Step 7 Enter **mpxadmin** in both, the Username and Password text boxes.

Step 8 Enter **init 2**, and press **Enter**.

Step 9 Enter **init 3**, and press **Enter**.

Step 10 The backup of the Mediator is restored.

Restoring a Single File

While you can back up and restore the Mediator files, you are also allowed to restore a single file. To restore a specific file from the Mediator backup files, ensure that you know the appropriate Persistant Data Object (PDO) file name.

Tip From the Mediator web client, navigate to the specific node on the node browser to check the appropriate PDO file name.

To restore the single file, perform the following steps:

Step 1 Perform step1 to step 7 of the "Restoring the Mediator" section on page 2-16.

Step 2 Enter **tar -xzf backupFilename.tgz pdoFilename.dat.1** to extract the specific file.

Step 3 Enter **init 2** to shutdown the Mediator Framework.

Step 4 Enter **pdoFilename.dat.1 to /var/mpx/config/persistent/** to copy the file to the Mediator.

Step 5 Enter **init 3** to restart the Mediator Framework.

The file is restored.

Configuring the Mediator Settings

You can use the Mediator web client to view and modify the Mediator network settings.

To customize the Mediator network settings, perform the following steps:

Step 1 In the Mediator web client, click **System**.

Step 2 Click the **Status** tab.

The Status tab appears. This tab displays the Mediator information.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note Text that appears in a grey color is auto generated and cannot be modified.

Step 3 On the Status tab, perform the following steps:

a. The Model text box displays the platform version of the Mediator.

b. The MOE Version text box displays the MOE version of the Mediator.

c. The Framework Version text box displays the Mediator Framework version.

d. In the Location text box, enter the location of your Mediator.

e. In the Hostname text box, enter the name of the host Mediator.

f. In the Domain Name text box, enter the name of the domain.

g. In the Gateway text box, enter the gateway IP address.

h. In the Name Server, enter the IP address of the server.

i. In the Proxy Server text box, enter the name of the proxy server.

j. In the License Status text box, the status of the license is displayed. This text box displays Enabled if a license is uploaded. Otherwise the text box is disabled and displays Disabled.

k. The Intermediate Protocols text box displays Supported if protocols were supported. Otherwise the text box is disabled and displays Unsupported. The intermediate protocols are loaded into your Mediator when you procure the license with intermediate protocols.

l. The Advanced Protocols text box displays Supported if advanced protocols are supported. Otherwise the text box is disabled and displays Unsupported. The advanced protocols are loaded into your Mediator when you procure the license with advanced protocols.

m. The Point Limit text box displays the maximum number of points that are available to you for configuration. By default the text box is disabled and displays 0. You obtain the points limit when you procure the license.

n. The Points Available text box displays the remaining number of points that are available to you. The number of points available decreases as you configure the points.

o. In the Upload License text box, click **Browse** to upload the license.

p. Set the text box options in the Ethernet columns as follows:

- MAC Address: Enter the Ethernet MAC address.
- DHCP: Displays the status of the Ethernet Dynamic Host Configuration Protocol (DHCP). Choose from the drop-down list to enable or disable the DHCP.
- IP Address: Enter the IP address of the Mediator.
- IP Netmask: Enter the IP Netmask address of the Mediator.

q. Click **Save** to save the changes you made.

r. Click **Reboot** to reboot the Mediator.

s. (Optional) Click **Save/Reboot** to save and reboot the Mediator.

Send documentation comments to cbsbu-docfeedback@cisco.com

Modifying User Accounts

The tasks described in this section enable you to create passwords and modify the profile of an existing user. These tasks are restricted to privileged users as determined by your administrator.

This section includes the following topics:

Username Guidelines

You need to configure a username with strong characteristics. To configure a username with strong characteristics, you must know the defined username security guidelines.

The username should have strong characteristics, such as the following:

- At least eight characters.
- Not more than eighty characters.
- Contain both upper and lowercase characters (Aa - Zz).
- Contain numbers (0- 9).
- Not contain printable or non-printable characters (such as [!"#$%&'()*+,\-./:;<=>?@[\]^_`{|}~\\].

Note Usernames such as “Cisco” and “mpxadmin” are not allowed and are rejected if you try to configure these usernames.

Password Guidelines

You need to configure a password with strong characteristics. To configure a password with strong characteristics, you must know the defined password security guidelines.

The password should have strong characteristics, such as the following:

- Contain characters from at least three of the four character groups that are uppercase (A-Z), lowercase (a-z), number (0-9), and punctuation characters ([!"#$%&'()*+,\-./:;<=>?@[\]^_`{|}~\\]).

Note Other characters than those mentioned in this section will not be accepted/configured.

- Contain characters that are repeated not more than twice.

  For example: If the password is bangalore, it is approved because the character b is not repeated twice. But if the password is pppusrpasswd, it is rejected because the character p is repeated more than twice.
- Should not be any variation of Cisco or mpxadmin. For example: C!sco, cisc0.
- Should not be a repeat of your username. For example: a testuser user cannot have testuser as the password.
- Should not be the reverse of a username.

Send documentation comments to cbsbu-docfeedback@cisco.com

Recovering the Mediator Password

If the administration credentials are lost, you can reset the default password. This section describes the procedures to recover the default password of the Mediators, and includes the following topics:

Note See the "Username Guidelines" section on page 2-19 and the "Password Guidelines" section on page 2-19, when you create a new username and password.

Mediator 2400 and 4800 Password Recovery

To recover the Mediator 2400 and 4800 password, perform the following steps:

Step 1 Perform Step 1 to Step 8 described in the "Configuring the Mediator" section on page 2-5.

Step 2 Power on the Mediator.

Step 3 Press **Enter** twice.

The Mediator system login prompt appears.

Step 4 To enter the menu, press **ESC**.

The prompt appears; press **ESC** again.

Step 5 Press the **e** key.

Step 6 Scroll down to choose the kernel line.

You can also press **Tab** to move the cursor between text boxes.

Step 7 Press the **e** key.

Step 8 Enter the word **single** at the end of the kernel line.

Step 9 Press **Enter**.

Step 10 Press the **b** key.

The Mediator device should start up in single-user mode without having to re-enter a password.

Step 11 Enter the **cd /usr/lib/broadway/tools** command.

Step 12 Enter **passwd**, and press **Enter**.

You are prompted to change the default username and password.

Step 13 Enter **y** to proceed.

Step 14 Enter the new username and password in the appropriate text boxes.

Mediator 2500 and 5000 Password Recovery

To recover the Mediator 2500 and 5000 password, you must be connected to the Mediator through the console port.

To recover the password, perform the following steps:

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 1 Perform Step 1 to Step 8 described in the "Configuring the Mediator" section on page 2-5.

Step 2 Power cycle the Mediator.

Step 3 Press **Enter** during the 5 second boot loader countdown so that the boot loader remains active.

Step 4 Enter the **setenv autoexec password_rese**t command.

Step 5 Enter the **saveenv** command.

Step 6 Enter the **run ramboot** command.

The Mediator system should start up in ramdisk mode.

Step 7 Log in using **root** as the username and no password.

Step 8 Enter **password_reset** to reset the password.

Step 9 Enter the **reboot** command.

The Mediator system reboots and the password is reset to the default password.

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 3

Licensing Requirements

The Mediator provides you with a flexible, pay-as-you-grow licensing mechanism, that allows you to add additional functionality as required. Licensing allows you to access specified features on the Mediator after you install the appropriate license for that feature. You can use these features only after the relevant licenses are installed.

While feature licenses allow you to use the features, the Global Management license enables the Mediator to communicate with the Mediator Manager. If the Global Management license is not enabled on the Mediator, then that Mediator cannot communicate with the Mediator Manager.

This chapter describes the Mediator licensing terms, how to purchase licenses, how to download and install licenses. It includes the following sections:

General Information on Licenses

This section describes general information about licenses and includes the following topics:

Licensing Terminology

The following terms are used in this section:

- Product Authorization Key (PAK)—A serial number included with the Mediator. The PAK is printed on the Software License Claim Certificate that ships with the Mediator. The PAK is the source of entitlement to a license key.

Send documentation comments to cbsbu-docfeedback@cisco.com

- License—Permission to use a particular feature through a license file. This permission is limited to the number of users and time span of usage.
- License file—A Mediator-specific unique, CRC-protected XML file that specifies the licensed features.
- Support—If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco Systems, contact Cisco Technical Support (TAC) at the following URL: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Licenses Types

The Mediator provides a flexible, pay-as-you-grow licensing mechanism that gives you the option to add additional points and protocols as required.

There are three types of licenses:

- Point licenses—Each Mediator comes with a certain number of built-in points that can be configured per appliance. Additional licenses can be purchased to increase the number of points.
- Protocol licenses—Each Mediator comes with a certain set of built-in protocols. Additional protocol licenses may be purchased based on the requirements of the project.
- Global Management license—You can purchase this license to enable the Mediators to communicate with the Mediator Manager.

Product Configurations

Table 3-1 describes the Mediator product configurations.

Table 3-1 Product Configuration

Product Name	Part Number	Description
Cisco Network Building Mediator 2400	NBM2400-K9	Designed for branch and retail. Supports up to 1000 points
Cisco Network Building Mediator 2500	NBM2500-K9	Designed for branch and retail. Supports up to 1000 points
Cisco Network Building Mediator 4800	NBM4800-K9	Designed for enterprise and campus. Supports up to 5000 points.
Cisco Network Building Mediator 5000	NBM5000-K9	Designed for enterprise and campus. Supports up to 5000 points.

Note A point is a generic term used to describe a single item of information in a building control system. For example, the temperature of a room, duct pressure of an air handling unit (AHU) and the chiller water flow rate are examples of points. The number of points needed in a particular project may be provided by the customer, project consultant or a partner.

Send documentation comments to cbsbu-docfeedback@cisco.com

Ordering Information

Table 3-2 describes the licensing ordering information for the Mediator.

Table 3-2 Licensing Ordering Information

Product Name	Part Number
Cisco Network Building Mediator 5000-Global Management	NBM5000-MGMT
Cisco Network Building Mediator 5000-Includes 5000 Points	NMB5000-K9
Cisco Network Building Mediator 5000-Add 1000 Points	NBM5000-PL
Cisco Network Building Mediator 5000-Intermediate Protocol	NBM5000-INT
Cisco Network Building Mediator 5000-Advanced Protocols	NBM5000-ADV
Cisco Network Building Mediator 4800-Global Management	NBM4800-MGMT
Cisco Network Building Mediator 4800-Includes 2000 Points	NBM4800-K9
Cisco Network Building Mediator 4800-Add 1000 Points	NBM4800-PL
Cisco Network Building Mediator 4800-Intermediate Protocols	NBM4800-INT
Cisco Network Building Mediator 4800-Advanced Protocols	NBM4800-ADV
Cisco Network Building Mediator 2500-Global Management	NBM2500-MGMT
Cisco Network Building Mediator 2500-Includes 250 Points	NBM2500-K9
Cisco Network Building Mediator 2500-Add 250 Points	NBM2500-PL
Cisco Network Building Mediator 2500-Intermediate Protocols	NBM2500-INT
Cisco Network Building Mediator 2400-Global Management	NBM2400-MGMT
Cisco Network Building Mediator 2400-Includes 250 Points	NBM2400-K9
Cisco Network Building Mediator 2400-Add 250 Points License	NBM2400-PL
Cisco Network Building Mediator 2400-Intermediate Protocols	NBM2400-INT

Licenses for Points

All points on the Mediator do not require a license. While protocol points require that you have a specified license, the following points do not require a license:

- Aliases
- Virtual Points
- Alarms
- Logs
- Trends

Purchasing Licenses

You can purchase your license either through your reseller or through Cisco Systems. There are two options to purchase the Mediator license:

Send documentation comments to cbsbu-docfeedback@cisco.com

- With base product—Applies to a new Mediator order. In this option, you should purchase the license as a configurable option when you order the Mediator. In this case, the Software License Claim Certificate is shipped along with the Mediator.

Note Please contact your reseller or Cisco account representative for details on the ordering process.

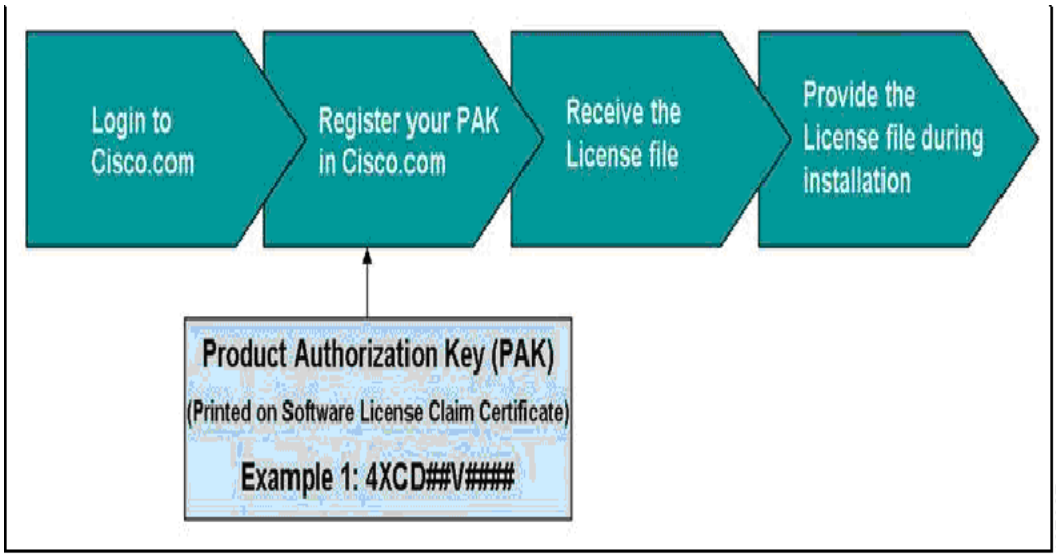
- Standalone—Applies to a license that is ordered separately at a subsequent point of time. In this option, you purchase the license as a standalone spare. You can choose to order the license for a physical or electronic delivery. In the case of a physical delivery, the Software License Claim Certificate is shipped in hard copy form to your mailing address. If you choose an electronic delivery, a soft copy of the Software License Claim Certificate is e-mailed to you.

Note Irrespective of the number of licenses purchased, you receive a single claim certificate with a single PAK at any point of purchase. The license registration website is linked with the sales order database, therefore, all the licenses that you have ordered are enabled in the license file.

Downloading Licenses

A typical licensing workflow is shown in Figure 3-1.

Figure 3-1 Licensing Workflow



Based on the option you select to purchase your license, you receive a Software License Claim Certificate.

To download the license file, you need to register your Mediator at Cisco.com. To register your Mediator, it is necessary to have the following:

- The PAK—This is printed on the Software License Claim Certificate.

  For example, 4XCD##V####

- The MAC address of the Mediator—This is the address of the ETH 0 Port of you Mediator. To view this address, log in to the Mediator web client, and click **System**.

Send documentation comments to cbsbu-docfeedback@cisco.com

To download the license files for a Mediator, perform the following steps:

Step 1 Log in to Cisco.com to register your license.

If you are not a registered user of Cisco.com, obtain your Cisco.com user ID from the following website: http://tools.cisco.com/RPF/register/register.do

After you have obtained your Cisco.com user ID, log in to Cisco.com to get your license file from the following website: http://www.cisco.com/go/license

Step 2 Register your Mediator with Cisco.com using the Product Authorization Key (PAK) and the MAC address of the Mediator (ETH 0 Port) to obtain your license file.

After you have registered your Mediator with Cisco.com, you receive the license file through e-mail.

Step 3 Save the license file to a folder location on your local disk.

Note Alternatively, you can send an e-mail message to the Cisco Licensing support team at licensing@cisco.com. You need to provide the Product Serial No., MAC address of the Mediator, and the PAK in your e-mail message to the Cisco Licensing support team. Once the licensing team receives the necessary details, you receive the license file through e-mail.

Installing Licenses

To install the Mediator license, perform the following steps:

Step 1 Launch an Internet browser (for example, Internet Explorer) and connect to the Mediator using the IP address previously configured.

The Mediator web client homepage appears.

Step 2 Click **System**.

The System pane appears.

Step 3 Click the **Status** tab.

Note By default, the License Status text box reads Disabled if a license has not been installed.

Step 4 To upload a license, click **Browse**.

Step 5 Navigate to the license file on your local disk.

Step 6 Click **Open**.

Step 7 Click **Upload License** to upload the license file to the Mediator.

When the file upload is complete, the file upload dialog box closes.

Note If you upload an inappropriate license file,a message box stating that the uploaded file is invalid appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 8 Click **Reboot**.

Note We recommend you restart the Mediator to enable the new license. Until you reboot, the license is not enabled.

Step 9 To verify the license status, click **Refresh**.

The updated licensing information appears in the License Status text box and the text box reads Enabled.

If you encounter any errors, repeat Step 1 to Step 6 to license your Mediator.

Verifying Licenses

After you install the Mediator license, you can verify the details of the licenses that you have ordered.

To see the details for the installed licenses, perform the following steps:

Step 1 Launch an Internet browser (for example, Internet Explorer) and connect to the Mediator using the IP address of the Mediator.

The Mediator web client homepage appears.

Step 2 Click **System**. The System pane appears.

Step 3 Click the **Status** tab.

The Status tab displays the licensing details as follows:

- License Status—Reads Enabled if a license has been installed.
- Intermediate Protocols—Reads Supported if an intermediate protocol license has been installed.
- Advanced Protocols—Reads Supported if an advanced protocol license has been installed.
- Global Management—Reads Enabled if the global management license has been installed.
- Point Limit—Displays the number of points that can be used on your Mediator with the existing licenses installed.
- Points Available—Displays the number of available points yet to be used on your Mediator.

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 4

Mediator configTOOL

This chapter describes how to start, configure and use the Cisco Network Building Mediator configTOOL (configTOOL), and includes the following topics:

Overview

The configTOOL software is used to configure the system settings, protocols, and services on the Mediator.

The configTOOL includes the following features:

- Aliases—Are used to assign alternative names to other nodes within the network.
- Interfaces—Represent the physical interfaces on the Mediator that connected to devices.
- Services—Utilities on the Mediator such as alarms, controls, logger, network, status, and time.

Send documentation comments to cbsbu-docfeedback@cisco.com

Installing configTOOL

This section includes the following topics:

Prerequisites

It is necessary that you install the Mediator configTOOL on your workstation.

For a PC running the configTOOL, we recommend that you use Windows-based platforms (95 or later) with 2 GB of RAM and 10 GB of free disk space.

Installation Instructions

To install this software, access Cisco.com at the following website:

http://www.cisco.com/en/US/products/ps10454/index.html

This software is available in the Support section at this website.

Note To download this software, you need to have a valid CCO username and password.

To download and install the software on your workstation, perform the following steps:

Step 1 Click **Download Software**.

Step 2 Choose **Smart Connected Building Software > Cisco Network Building Mediator**.

Step 3 Choose the appropriate hardware platform.

Step 4 Click **Network Building Mediator Configuration Software** to download the configTOOL.

Step 5 Select the appropriate release, click the release number, and then click **Download Now**.

Step 6 On the Download Cart window that appears, click **Proceed With Download**.

The Cisco End User Software License Agreement page appears.

Step 7 Click **Agree** to accept the software download rules specified in the Cisco's End User Software License Agreement page. Click **Disagree** to cancel the download process.

The download software page appears with two options to download the configTOOL: Download Manager Option and Non-Java Download Option.

Step 8 Click **Non-Java Download Option** to proceed with the download.

Note The Download Manager Option requires a working Java version of 1.4.2.xx and later. If you choose this option to download the configTOOL software, the file is saved on your PC and you are allowed to run this file to install this software.

Step 9 Click **Download URL** to download the configTOOL.

The file download dialog box appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 10 Click **Run**.

You see the welcome message in the configTOOL Installer window.

Step 11 Click **Next** and follow the instructions to install the configTOOL. Alternatively, click **Cancel** to cancel the download process.

Step 12 Once you install the configTOOL, you can launch this application by choosing **Start > All Programs > Cisco Systems > Cisco Systems Network Building Mediator configTOOL**.

Starting configTOOL

To start the configTOOL, double-click the configTOOL shortcut icon on your desktop, or choose **Start > All Programs > Network Building Mediator configTOOL**.

configTOOL Interface

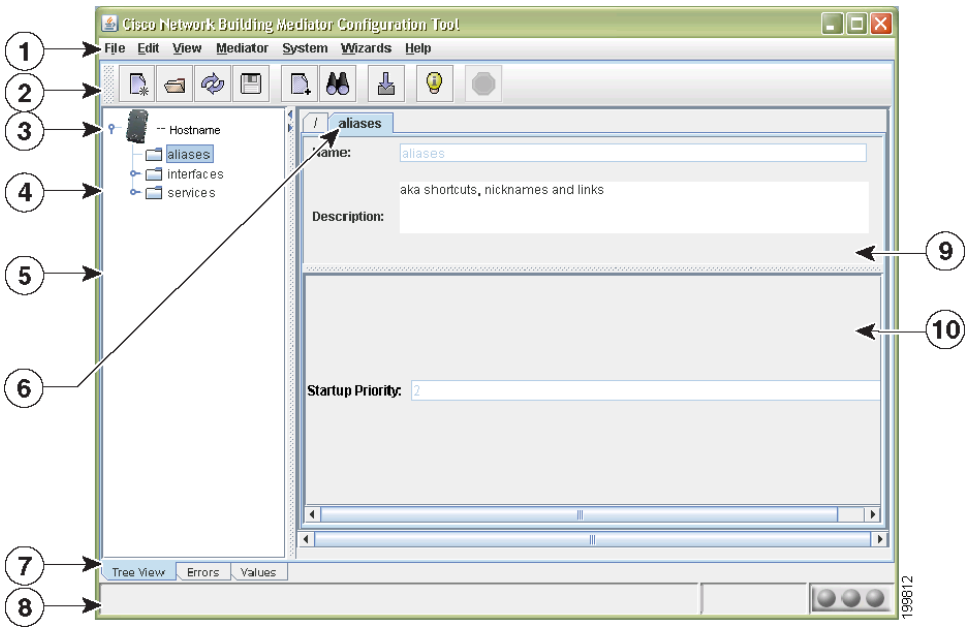
This section describes the different elements of the configTOOL interface and includes the following topics:

About Interface Elements

This section describes the configTOOL window with area titles, panes, and information areas (see Figure 4-1).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 4-1 configTOOL Interface



1	Menu bar. Use the commands in these menus to create, access, and save the Mediator configuration files.
2	Toolbar. Use eight of the most frequently used commands without using the menus.
3	Node tree. You can view a node tree representation of the selected Mediator configuration.
4	Expand/collapse switch. You can expand or collapse individual nodes within a tree.
5	Node tree pane. You can view a node tree representation of the selected Mediator configuration and access individual nodes.
6	configTOOL tabs. You can view and edit the current configuration of the nodes selected in the node tree pane.
7	View selection tabs. You can view and edit the current configuration of the nodes selected in the node tree pane.
8	Status bar. You can view messages and graphics that indicate the status of activity in the currently selected Mediator.
9	Name and Description text boxes. You can enter the name of the selected node and description of the selected node to identify the purpose of the selected node.
10	Parameter text box. You can enter or choose the configurable parameters for the selected node and protocol.

Using Interface Elements

This section describes how to use the configTOOL interface and includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Node Tree Right-Click Menu

When you right-click a node in the node tree pane, the node tree right-click menu appears.

Table 4-1 describes the node tree right-click menu options and the associated tasks.

Table 4-1 Right-Click Menu Options

Command	Allows you to ...
Find	Find a node in the node tree
Add	Add a node to the configuration.
Edit	Display the data entry form of the selected node when the Synchronize Forms option is deselected.
Delete	Delete the selected node from the configuration.
Copy Node Path	Copy the path of a selected node to the appropriate text box in a data entry form.
Expand From Here	Expand the node tree to the show the child nodes of the selected node.
Collapse From Here	Collapse the node tree to hide the child nodes of the selected node.
Output From Here	Display or save the XML code segment of the configuration file.
Get Value	Display the current numerical value of the selected node.
Create Alias In	Create an alias directly under the selected node.
System	Open a submenu with the following commands. • Edit Node Def: This is a tool intended to assist developers and should not be changed without consulting Cisco TAC. • Import Configuration Fragment: Import a saved XML code segment. The nodes represented in the XML segment get imported as child nodes under the selected node.
Graph Point	Display a running graph of the value of the selected node.

configTOOL Tabs

The configTOOL tab (see Figure 4-2) contains the data entry text boxes, in which you enter and edit node configuration parameters. The data entry text boxes are typical Windows application controls. A text box labelled in red indicates that the text box entry is mandatory.

The tab is divided into two parts, the upper area and the lower area.

- The upper area contains the data entry text boxes for name and description of the selected node.

  For some nodes, the Name text box is disabled indicating that you cannot change it.

- The lower area contains the data entry text box appropriate for the selected node that you are configuring.

Send documentation comments to cbsbu-docfeedback@cisco.com

For some nodes, the data entry text boxes have a default entry that you can change; and for some, the data entry text boxes are disabled indicating that you cannot change it. For some nodes, the pane does not have any data entry text boxes.

In some cases, a wizard guides you through the node configuration procedure.

Some text boxes prompt you to enter the node path. The text box may be in the form of a data entry text box, where you use the Copy Node Path command to insert the entry.

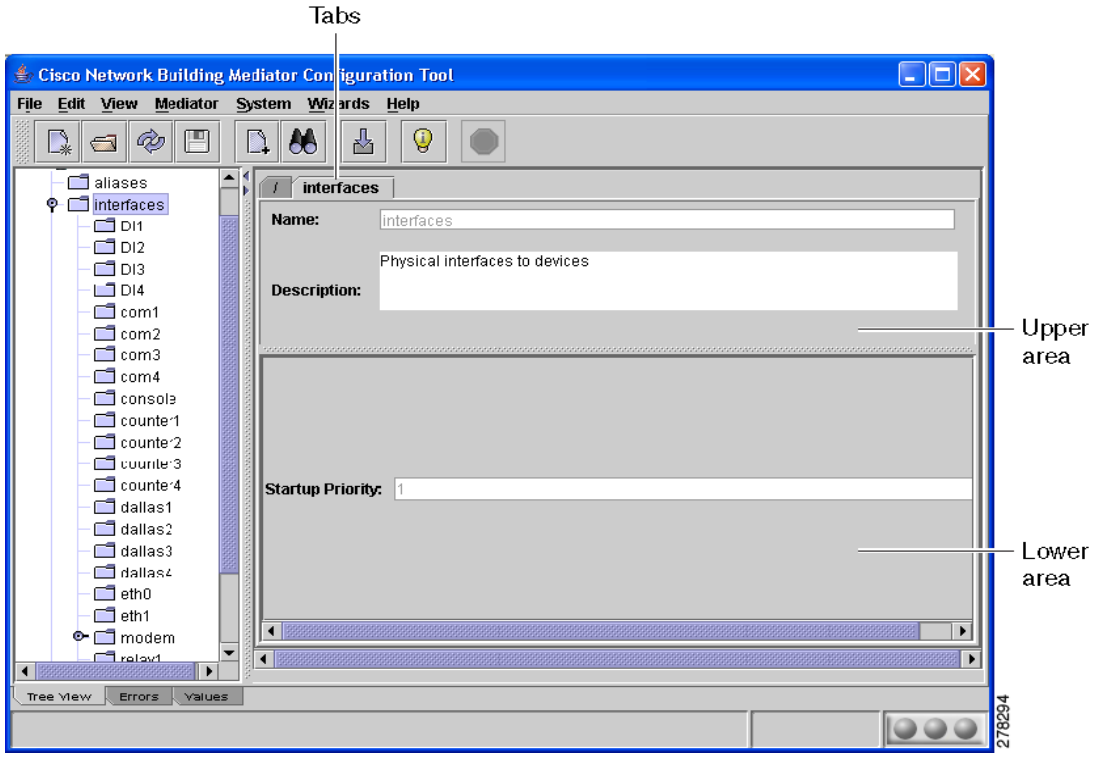
To complete the tab text boxes, perform the following steps:

Step 1 In the node tree pane, expand or collapse the node tree to list the interface nodes.

Step 2 Click the node you want to configure.

The tab appears in the right pane of the window. The default name and description of the connected device appear in the upper area (see Figure 4-2).

Figure 4-2 Mediator configuration Tool Window



Note The tab appears automatically if the Synchronize Forms option under View > Options is selected. If the Options check box is selected, use the Edit function to display the form.

You can enter a new name and description to identify the selected node. When you rename a node, the updated name replaces the default name in the node tree.

Note The screen tooltip appears when you position the cursor over the node in the node tree. In this example, you cannot change the default name.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 3 Right-click the node you want to configure, and then choose **Add** (see Node Tree Right-Click Menu, page 4-5).

Step 4 From the Available Devices dialog box that appears, choose **periodic value driver (driver)**, and click **OK**.

A new child node appears under the selected node in the node tree.

The data entry text boxes of the newly added child node appear on the driver tab within the tab. The default name and description text box of the node appear in the upper area of the driver tab; and other mandatory and optional entry text boxes appear in the lower area.

Step 5 In the Name text box, enter the new name.

Step 6 In the Description text box, enter the new description.

Note The description entered in this text box appears in the tooltip, which appears when you position the cursor over or near the node in the node tree.

Step 7 In the lower area of the driver tab, enter the appropriate parameters in the data entry text boxes.

View Selection Tabs

The view selection tabs, located at the bottom of the configTOOL window, allow you to view all the options that contain different information on the node tree pane and the data entry pane. This section describes each of these tabs and includes the following topics:

- Accessing the Node Tree, page 4-7
- Accessing the Errors View, page 4-7
- Accessing the Values View, page 4-7

Accessing the Node Tree

The node tree is the default view of the configTOOL window. You can click the Tree View tab to return to this view from another view.

Accessing the Errors View

When you click the Errors tab, the configTOOL window displays the Errors view. The Errors view displays a list of error messages the Mediator has generated during the current session. The Errors view is a diagnostic tool intended to assist developers and technicians.

Accessing the Values View

When you click the Values tab, the configTOOL window displays the Values view. The Values view displays the list of values of the nodes currently configured for logging.

Status Bar

The Status bar is located at the bottom of the configTOOL window (see Figure 4-3). The Mediator uses this area to display messages and graphics that indicate the status of activity in the currently selected Mediator.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Status bar contains three areas:

- The Status Message area is located on the left. Here the configTOOL displays messages that tell you about operations in progress. For example, when you open an existing Mediator, it displays the message Opening configuration.
- The Progress Indicator area is located in the middle. A blue rectangle sweeps back and forth in the area while an operation is in progress.
- The Online/Offline indicator is located on the right. When the Mediator is online, the indicator is green; and when it is offline, the indicator is red.

Figure 4-3 Status Bar

Mediator Units Window

The Mediator Units window is a frequently used feature of the configTOOL. It appears when you initiate either of the following two operations:

- When you open the configuration file of a Mediator in a network while running the configTOOL.

  You can perform this task by choosing File > Open Mediator > From Network.

Note When opened this way, the window title bar displays the label Open Mediator Configuration.

- When you save the configuration file and restart the Mediator.

  You can perform this task by choosing File > Save As.

Note When opened this way, the window title bar displays the label Save Mediator Configuration.

The sections describe the controls included in the Mediator Units window. These include the toolbar located in the upper right-hand corner of the window, and a right-click menu. In addition, the Restart Mediator drop-down list appears in the lower left corner of the window when you choose File > Save As.

This section includes the following topics:

- Mediator Units Window Toolbar, page 4-8
- Mediator Units Window Right-Click Menu, page 4-9
- Using the Mediator Units Window to Restart the Mediator, page 4-10

Mediator Units Window Toolbar

The Mediator Units window toolbar contains six tools representing tools that perform configuration file management functions. However, at any given point in time, the toolbar displays only five tools.

- When the window title bar contains the label Open Mediator Configuration, the first tool allows you to open files.

Send documentation comments to cbsbu-docfeedback@cisco.com

- When the window title bar contains the label Save Mediator Configuration, the first tool allows you to save files.

Table 4-2 describes these tools and its associated tasks.

Table 4-2 Toolbar Description

Tool	Tool Name	Allows you to...
	Open Mediator Configuration	Open a Mediator configuration file from a file stored on the hard disk of your computer (or on a computer you can access over the network).
	Save Mediator Configuration	Save a Mediator configuration file to the hard disk of your computer (or to a computer you can access over the network).
	Search the Network for Mediator Configurations	Find and download the configuration file of any Mediator your computer can access on the network.
	Add Favorite Mediator Configuration	Add a Mediator to your Favorites List.
	Remove Mediator Configuration	Remove a Mediator from the list of the Mediator hosts. The configTOOL performs a multicast to discover the Mediators on the network.
	Configure Basic System	Configure the network connection parameters of the Mediator.

Mediator Units Window Right-Click Menu

You can right-click the row describing a Mediator to view the right-click menu commands. Table 4-3 describes the right-click menu commands.

Table 4-3 Right-Click Menu Commands

Name	Allows you to...
Configure	Configure the network connection parameters of the Mediator.
Restart	Reboot the Framework and the Mediator Operating Environment (MOE).
Terminal	Open a secure terminal window and log on to your Mediator.
Upgrade	Configure the network connection parameters of the Mediator.

Send documentation comments to cbsbu-docfeedback@cisco.com

Using the Mediator Units Window to Restart the Mediator

To use the Mediator Units window to restart the Mediator, perform the following steps:

Note When you make changes to the configuration file of the active Mediator, you must restart the Mediator for the changes to take effect.

Step 1 Choose **File > Save As**.

The Save Mediator Configuration dialog box appears. The active Mediator host is selected.

Step 2 From the Restart Mediator drop-down list, choose **soft** or **hard**.

The soft option performs a soft reboot (a soft reboot restarts the panework only), and the hard option performs a hard reboot (a hard reboot restarts both the Mediator Framework and the MOE).

Specifying the Node Path

The following sections describe how to specify the path of a node. Some node entries use the value of another node in determining their own values. The data entry pane of these nodes displays the text box in which you to enter the path to that other node. The configTOOL provides two methods for specifying the node path. This section includes the following topics:

- Using the Node Selector, page 4-10
- Using the Copy Node Path Command, page 4-10

Using the Node Selector

To specify the node path using the Node Selector, perform the following steps:

Step 1 In the configTOOL window, click the **driver** node under the Interfaces/relay1 node.

The driver tab displays the data entry text boxes.

Step 2 In the lower area of the tab, click the arrow next to the Input Node text box.

Step 3 From the Node Selector dialog box, choose the **DI1** node under the interfaces node.

The node path /interfaces/DI1 is the value of Digital Input 01.

Step 4 Click **Select**.

The node path of the DI1 node appears in the Input Node text box.

Using the Copy Node Path Command

To use the Copy Node Path command, perform the following steps:

Step 1 In the configTOOL window, click the **DI1** node under the interfaces node.

Step 2 Right-click the **DI1** node, and choose **Copy Node Path**.

Step 3 Click the node to which you want to copy the path.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 Press **Ctrl-C**.

The file path of the selected node is copied to the data entry text box.

Using the Tooltips and Keyboard Shortcuts

The configTOOL displays a tooltip when you position the cursor over any of the areas in the configTOOL window.

Customizing the configTOOL Interface

You can set a user preference to control the view of the configTOOL interface that appears when you initially log in.

To set a view, in the configTOOL window, choose **View > Look and Feel**, and choose the appropriate view.

Accessing Mediators Using configTOOL

This section describes the procedure to connect to your Mediator and includes the following topics”

Connecting to a Local Mediator

To connect to the Mediator using the configTOOL, perform the following steps:

Step 1 Start the configTOOL and choose **File > Open Mediator > From Network**.

The Open Mediator Configuration dialog box appears.

Step 2 Select the row describing the Mediator host you want to configure and click **OK**.

The Login to Mediator dialog box appears.

Step 3 (Optional) If your Mediator is not listed in the Mediator Units list, click **Add Favorite Mediator**.

The Enter Host Name dialog box appears.

Step 4 (Optional) In the Mediator Host name text box, enter the IP address or hostname of your Mediator, and then click **OK** to continue with Step 3.

Step 5 In the Login to Mediator dialog box, enter the username and the password, and then click **OK**.

The configTOOL window displays the node tree of the selected Mediator.

You can also connect to a Mediator from options such as:

- From File—Opens a Mediator from an existing file.

Send documentation comments to cbsbu-docfeedback@cisco.com

- From Recently Opened—Opens a Mediator from the list of recently opened Mediator.
- From Favorite—Opens a Mediator from those stored under the favorite locations.

Connecting to a Remote Mediator

Note The Mediator menu SSH Terminal command allows you to log in to your local Mediator. The System menu SSH Terminal command allows you to log in to a remote Mediator.

To log in to a remote Mediator, perform the following steps:

Step 1 Start the configTOOL (see Starting configTOOL, page 4-3).

The configTOOL window appears.

Step 2 Choose **System > SSH Terminal**.

The Enter Host Name dialog box appears.

Step 3 In the Host name text box, enter the IP address of the remote Mediator.

Step 4 Click **OK**.

The SSH User Authentication dialog box appears.

Step 5 In the Username text box, enter the username.

Step 6 In the Password text box, enter the Password.

Step 7 Click **Login**.

The Secure Terminal window appears.

Restarting and Rebooting the Mediator

Restarting (also called a soft reboot) restarts only the framework. Rebooting (also called a hard reboot) restarts both the framework and the Mediator Operating Environment (MOE).

Note When you modify the configuration file on the active mediator and save the files, the Mediator restarts automatically to show the modified configuration. When you modify an offline configuration file, you have to restart the Mediator manually.

You can restart the Mediator when you need to save the changes to the existing configurations. You can reboot the Mediator, when you upgrade the MOE or power on the Mediator.

- To restart the Mediator (framework only), choose **Open the Mediator > Restart**.
- To reboot the Mediator (framework and MOE), choose **Open the Mediator > Reboot**.

The Online/Offline Indicator turns red (see Status Bar, page 4-7) and the Power LED stops flashing.

Send documentation comments to cbsbu-docfeedback@cisco.com

When the Mediator finishes restarting or rebooting, the Online/Offline Indicator turns green and the Power LED begins emitting three long flashes followed by a pause (Morse code O). This indicates that the panework functions are normal.

The Mediator Units window also has controls for restarting or rebooting the Mediator (See Mediator Units Window, page 4-8).

Configuring Virtual Nodes

This section describes a virtual node and includes the following topics:

About Virtual Node

The Mediator configTOOL supports ten virtual nodes. These are child nodes that can be configured under many types of interface and service parent nodes. Unlike the interface nodes, which represent a physical device or data point, virtual nodes represent a functionality. For example, mathematical calculation. A virtual node may introduce a new value into the system, change the value of its parent node, or use the value of its parent node to produce a different value.

The value of the virtual node is available to all other nodes including the parent node in the system. For example, the value of a Multiplier node that is configured as the child node of a Digital Input parent node may also be used by an unrelated counter node.

Adding a Virtual Node

To add a virtual node, perform the following steps:

Step 1 Start the configTOOL and connect to the Mediator.

For more information, see the following sections:

- Starting configTOOL, page 4-3.
- Accessing Mediators Using configTOOL, page 4-11.

Step 2 Click **interfaces** to display the available interfaces.

Step 3 To configure a virtual node under a parent node, click the parent node. For example, click **DI1** (Digital Input1).

Step 4 Right-click the **DI1** node, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears listing the different types of virtual nodes.

Step 5 In the Available Devices dialog box, choose **Calculated Virtual Point (calculator)**, and then click **OK**.

A new child node (calculator node) appears under the parent node DI1 in the node tree pane.

Send documentation comments to cbsbu-docfeedback@cisco.com

The calculator tab displays the default name, description, and the configurable parameters of the node. You can change the default name and description of the calculator node (or retain the defaults). The configurable parameters are located in the lower area of the data entry window. To modify the parameters, choose an appropriate value from the relevant drop-down list or enter a value in the text boxes provided.

Note All text boxes that are labelled in red indicate that the text box entry is mandatory.

Step 6 In the Statement text box, enter the expression that you want the node to calculate. For example, (a+b)/2 (the average of the values of the two temperature sensor nodes).

a = the value of the F (degrees Fahrenheit) child node of Control_Room_Temp_01.

b = the value of the F (degrees Fahrenheit) child node of Control_Room_Temp_02.

Step 7 Click **+** to define the variables.

Step 8 In the Variable text box, do the following:

- Enter the variable name in the Variable Name column. For example, a.
- Enter the node references path in the Node Reference column. For example, /interfaces/dallas1/Control_Room_Temp_01/F. The value that you enter in the Node Reference column will determine the value of the parent node.

Step 9 Repeat Step 8 to define the variable b.

Step 10 Save the configuration.

Calculated Virtual Point Node

This section describes the functionality and configuration of a calculated virtual point node, also known as the *calculator* node, and includes the following topics:

About Calculated Virtual Point

A calculated virtual point (calculator) node allows you to use the mathematical functionality built into the Mediator software, the values of other nodes, and the constants to configure an expression that determines the value of the node. That value becomes available to other nodes in the Mediator environment. The calculator node supports six, basic arithmetic operations as described in Table 4-4.

Table 4-4 Basic Arithmetic Operation

Operation	Symbol	Example
Exponentiation	**	5 ** 2 = = 25
Multiplication	*	2 * 3 = = 6
Division	/	14 / 3 = = 4

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 4-4 Basic Arithmetic Operation (continued)

Operation	Symbol	Example
Remainder	%	14 % 3 = = 2
Addition	+	1 + 2 = = 3
Subtraction	-	4 - 3 = = 1

The calculator follows the normal mathematical order of operations:

- Parentheses ()
- Exponents **
- Multiplication *, division \, and remainder %
- Addition + and subtraction -

The calculator supports the mathematical functions as described in Table 4-5.

Table 4-5 Mathematical Function

Function	Return
acos(x)	The arc cosine of x.
asin(x)	The arc sine of x.
atan(x)	The arc tangent of x.
atan2 (y,x)	atan(y / x).
ceil(x)	The ceiling of x as a float.
cos(x)	The cosine of x.
cosh(x)	The hyperbolic cosine of x.
exp(x)	e**x.
fabs(x)	The absolute value of the floating point number x.
floor(x)	The floor of x as a float.
fmod(x, y)	fmod(x, y).
frexp(x)	The mantissa and exponent of x as the pair (m, e). m is a float and e is an integer such that x == m * 2**e. If x is zero, returns (0.0, 0), otherwise 0.5 <= abs(m) < 1.
hypot(x,y)	The Euclidean distance, sqrt(x*x + y*y).
ldexp(x, i)	Return x * (2**i).
log(x)	The natural logarithm of x.
log10(x)	The base-10 logarithm of x.
modf(x)	The fractional and integer parts of x. Both results carry the sign of x. The integer part is returned as a float.
pow(x, y)	x**y.
sin(x)	The sine of x.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 4-5 Mathematical Function (continued)

Function	Return
sinh(x)	The hyperbolic sine of x.
sqrt(x)	The square root of x.
tan(x)	The tangent of x.
tanh(x)	The hyperbolic tangent of x.

The Calculator also supports the following two mathematical constants:

- pi—The mathematical constant *pi*.
- e—The mathematical constant *e*.

The Calculator supports the logical operators as described in Table 4-6.

Table 4-6 Logical Operators

Operator	Example	Description
or	x or y	Logical or (y is evaluated only if x is false).
and	x and y	Logical and (y is evaluated only if x is true).
not	not x	Logical negation.
<, <=, >, >=, ==, <>, !=	Not Applicable	Comparison operators.
is, is not	Not Applicable	Identity tests.
in, not in	Not Applicable	Sequence membership.
|	x | y	Bitwise or.
^	x ^ y	Bitwise exclusive or.
&	x & y	Bitwise and.
<<	x << y	Shift x left by y bits.
>>	x >> y	Shift x right by y bits.

Configuring the Calculator Node

The following procedure uses a simple example to explain how you can configure a calculator node. The value of the node is the average of the values of two temperature sensors, the F (degrees Fahrenheit) child node of Control_Room_Temp_01 and the F (degrees Fahrenheit) child node of Control_Room_Temp_02.

To configure the calculator node, perform the following steps:

Step 1 Perform Step 1 and Step 2 of the "Adding a Virtual Node" section on page 4-13.

Step 2 In the node tree pane, expand the node tree, click **interfaces**, and then click **Dallas1**.

Step 3 Right-click the **Dallas1** node, and then choose **Add** from the right-click menu.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Available Devices dialog box appears.

Step 4 In the Available devices dialog box, choose **Calculated Virtual Point (calculator)**, and then click **OK**.

A new child node (calculator node) appears under the parent node (Dallas1) node in the node tree pane.

The calculator tab displays the default name, description, and the configurable parameters of the calculator node.

Step 5 (Optional) To change the default name of the child node, in the Name text box, enter the new name for the modem, and then press **Enter**.

Step 6 (Optional) In the Description text box, enter a description to identify the purpose of the calculator child node.

Step 7 In the Statement text box, enter the expression that you want the node to calculate. For example, (a+b)/2 (the average of the values of the two temperature sensor nodes).

a = the value of the F (degrees Fahrenheit) child node of Control_Room_Temp_01.

b = the value of the F (degrees Fahrenheit) child node of Control_Room_Temp_02.

Step 8 Click **+** to define the variables.

Step 9 In the Variable text box, do the following:

- Enter the variable name in the Variable Name column. For example, a.
- Enter the node reference path /interfaces/dallas1/Control_Room_Temp_01/F in the Node Reference column. The value that you enter in the Node Reference column will determine the value of the parent node.

Step 10 Repeat Step 9 to define the variable b.

Step 11 Save the configuration.

Configuring the Time Node

This section describes the different time nodes, explains how to configure the time nodes in the Mediator and includes the following topics:

About Time Node

The time node implements the date and time service in the Mediator. The time node allows you to specify two types of date and time settings in the Mediator.

1. Set the date and time in the Mediator manually.
2. Update the date and time settings in the time server automatically.

The time node output is a value that expresses the time as the number of seconds since January 1, 1970 (the standard UNIX method of reporting time). The time node has several pre-configured child nodes. Similar to the time node, the outputs of the UTC (Coordinated Universal Time, also called Greenwich

Send documentation comments to cbsbu-docfeedback@cisco.com

Mean Time) node and the local node are also in number of seconds since January 1, 1970. The UTC and the local nodes both have eight pre-configured child nodes, that provides the output values for the current day, hour, and so on.

Note The value of the weekday node is a number in the range of 0 to 6, where 0 = Monday, 1 = Tuesday, 2 = Wednesday, and so on. The synch_continuous and synch_periodic nodes allow you to configure a time server.

Configuring Date and Time Manually

To configure the date and time manually, perform the following steps:

Step 1 Perform Step 1 and Step 2 of the "Adding a Virtual Node" section on page 4-13.

Step 2 In the node tree pane, expand the node tree, click **services**, and then click **time**.

The time tab for the time node displays the default name, description, and the configurable parameters.

Note You cannot change the default name.

Step 3 (Optional) To change the description of the time node, in the Description text box, enter a description to identify the purpose of this node.

Step 4 In the Date and Time text box, enter the current date and time in your location, in the following format: dd-mmm-yyyy hh:mm:ss. For example, 07-Jul-2011 08.33.16.

Step 5 From the Time Zone drop-down list, choose the time zone of your location. For example, PST.

Step 6 Click **Set Date/Time**.

The date/time was set dialog box appears.

Step 7 Click **OK**.

Note The UTC, local child nodes, and their inherent child nodes do not require any specific configuration.

Formatting the Date and Time Using a Calculated Virtual Point

To format the date and time, and to display a timestamp, perform the following steps:

Step 1 Perform Step 1 and Step 2 of the "Adding a Virtual Node" section on page 4-13.

Step 2 In the node tree pane, expand the node tree, and then choose **interfaces > virtuals**.

Step 3 Right-click the **virtuals** node, and choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 4 In the Available Devices dialog box, choose **Calculated Virtual Point (calculator)**, and then click **OK**.

Step 5 Click **+** to define the variables.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 6 In the Variable text box, do the following:

- Enter the variable name in the Variable Name column. For example, h.
- Enter the node reference path in the in the Node Reference column. For example, /services/time/local/hour.

Step 7 Repeat Step 5 and Step 6 to create two other variables with the variable names, m and s, with the node references path /services/time/local/minute and /services/time/local/hour respectively.

Step 8 In the Statement text box enter the expression string '%d:%d:%d' % (h, m, s).

The value of the node gets time formatted as hh:mm:ss.

Step 9 Save the configuration.

Configuring a Time Server

This section describes how to configure the time server and includes the following topics:

You can configure the date and time in the Mediator by using a time server. The time node has two child nodes that you can use to configure the Mediator to use a time server:

- The synch_continuous node allows you to configure a time server continuously.
- The synch_periodic node allows you to configure a time server at periodic intervals.

Configuring a Continuously Available Time Server

To configure the available time server, perform the following steps:

Step 1 In the node tree pane, expand the node tree, then choose **services > time > sync_continuous**.

The sync_continuous tab displays the default name, description and the configurable parameters of the sync_continuous node.

Note You cannot change the default name of the sync-continuous node.

Step 2 (Optional) In the Description text box, enter a description to identify the purpose of the synch_continuous child node or retain the default description.

Step 3 Select the **Enabled** check box to enable the node. By default, the node is enabled.

Step 4 In the connection drop-down list, retain the default value, which is LAN.

Step 5 Click **+** to specify one or more time servers.

Step 6 In the Time Servers:Server entry text box, enter the hostname or the IP address of the time server.

Note Ensure that an external NTP (Network Time Protocol) is available before entering the IP address and the connection is always LAN.

Send documentation comments to cbsbu-docfeedback@cisco.com

This step ensures that the time in all the Mediators is synchronized to allow scheduling (For example, equipment start and stop times), and logging operations to commence at predefined times and is recommended for all large enterprise deployements.

Step 7 Repeat Step 5 and Step 6 for each additional time server that you want to configure.

Configuring an Intermittently Available Time Server

To configure an intermittently available time server, perform the following steps:

Step 1 In the node tree pane, expand the node tree, then choose **services > periodic**.

The sync_periodic tab displays the default name, description, and the configurable parameters of the sync_periodic node.

Note You cannot change the default name of the sync-continuous node.

Step 2 (Optional) In the Description text box, enter a description to identify the purpose of the sync_periodic child node (or leave the defaults).

Step 3 Select the **Enabled** check box.

Step 4 In the Connection type drop-down list, retain the default value, which is LAN.

Note The Dial out option is not supported.

Step 5 You can specify the interval at which you want the Mediator to connect to the time server. The configurable parameters are located in the lower area of the data entry pane. To do so, enter a appropriate value in the text boxes provided.

- In the Minutes text box, enter the time interval in minutes to connect to the time server more than once in an hour.
- In the Hours text box, enter the time interval in minutes to connect to the time server less than once an hour but more than once a day.
- In the Days text box, enter the interval in minutes to connect to the time server less than once a day.

Step 6 Click **+** to specify one or more time server.

Step 7 In the Time Servers:Server entry text box, enter the hostname or the IP address of the time server.

Step 8 Repeat Step 6 and Step 7 for each additional time server that you want to configure.

Viewing Nodes

You can view the online values of the nodes configured on the Mediator. The Mediator web client allows you to navigate to a node and then view the node details.

To view the details associated with a node, perform the following steps:

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 1 In the Mediator web client homepage, click **Nodes**.

The Nodes pane appears.

Step 2 Click one of the children nodes. Navigate to the node you want to view.

Step 3 Click the node. The corresponding details are displayed in the pane.

Using Snippets

Snippets are a set of configuration files which can be reused because doing so allows you to minimize repetitive configuration. You can use the configTOOL to create snippets, save the configured files on your computer hard disk, and import these files when required.

This section describes how to create and import snippets and includes the following topics:

Creating a Snippet

To create a snippet, perform the following steps:

Step 1 In the configTOOL window, expand the aliases node to display the sub nodes.

Step 2 Right-click the **RTU1** node and choose **Output From Here**. The Output Mediator Configuration dialog box appears.

Step 3 In the Output Mediator Configuration dialog box, click **Save to File**.

Step 4 Save the file in any directory on your computer hard disk. The file should be saved as an Extensible Markup Language (XML extension) file. For example: rtu1snippet.xml

Importing a Snippet

To import a snippet, perform the following steps:

Step 1 In the configTOOL window, right-click the Aliases node, and choose **System>Import configuration fragment**.

Step 2 Browse through the computer directory and locate the XML file that you want to import in the configTOOL. For example: rtu1snippet.xml

Step 3 Click **OK** to import the selected snippet.

The imported snippet now appears as a node under the aliases node.

Send documentation comments to cbsbu-docfeedback@cisco.com

Configuring Logs and Exporters

Logs are used to periodically collect and store Mediator data in a file on the Mediator. You can analyze the efficiency, record the energy usage, and troubleshoot associated problems of the Heating, Ventilating, and Air Conditioning (HVAC) system with the help of the logs data.

The Log Wizard in the configTOOL enables you to configure the logs to define the interval at which the data can be stored. You can then export the logged data by configuring an exporter.

The process of configuring logs and exporters using the Log Wizard can be summarized as follows:

Step 1: Create a new log.	See Step 4 of the "Configuring Logs" section on page 4-22.
Step 2: Edit log columns.	See Step 7 of the "Configuring Logs" section on page 4-22.
Step 3: Define log exporters. (Optional)	See the "Defining Exporters" section on page 4-25.
Step 4: Define formatters.	See the "Defining Formatters" section on page 4-28.
Step 5: Define transporters	See the "Defining Transporters" section on page 4-33.
Step 6: Save the configuration.	–

This section describes how to configure logs and exporters and includes the following topics:

Configuring Logs

To configure logs, perform the following steps:

Step 1 In the node tree pane, expand the node tree, click the **service** node, and then click the **logger** node.

The logger tab appears.

Step 2 Click the **Plug-In** tab in the lower area of the logger tab.

A **Wizard is available** button appears on the Plug-In tab.

Step 3 Click **Wizard is available**. The Log Wizard screen appears.

Step 4 Click **Create New Log**. The Log Wizard opens in the Edit Log Details mode.

Step 5 In the Edit Log Details window, perform the following steps:

a. In the Log Name text box, enter a descriptive name for the new log.

Note Ensure that you specify a unique name for the log because you cannot configure a log with a name that already exists.

b. From the Log Type drop-down list, choose **Periodic log**. This log type samples and records Mediator values at specified intervals of time.

Send documentation comments to cbsbu-docfeedback@cisco.com

c. In the Minimum Size (Kb) text box, enter the minimum size of the log file.

d. In the Maximum Size (Kb) text box, enter the maximum size the log file is allowed to grow to.

When the log file reaches the maximum size, it is reduced to the minimum size that is specified.

e. From the Period drop-down list, choose the log period, which is the interval at which the Mediator collects and stores the data.

f. Ensure that the **Enabled** check box is selected. By default, this check box is selected.

g. (Optional) Click the Trigger Node drop-down list to open the Node Selector dialog box. In the Node Selector dialog box, choose the appropriate node to enable sampling of data. If the log file should always collect data at the specified interval of time, leave this field blank.

Note If you are defining triggered exporters, leave this field blank.

h. Ensure that the **Debug** check box is unselected.

Note You should enable debugging only if you have been instructed to do so by Cisco Technical Support (TAC).

Step 6 Click **Next**. The Edit Log Column pane appears.

Step 7 Click **Create New Column**. The Edit Column Details dialog box appears.

Step 8 In the Edit Column Details dialog box, perform the following steps:

a. In the Column Name text box, enter a name for the new column.

b. From the Column Type drop-down list, choose the appropriate column type from the following options:

- Periodic column—Records the current value of the sampled node.
- Periodic delta column—Records the delta between the current sample and the previous sampled value of the node.
- Periodic Column with Attributes of an FSG Channel—Records the current value of the sampled node along with attributes, such as Channel Name, Unit of Measure, Delta Values, Totalize Values, and Key.
- Periodic average column—Records the average of the current sample and the previous sampled value of the node.
- Periodic Delta Column with Attributes of an FSG Channel—Records the delta between the current sample and the previous sampled value of the node, along with attributes, such as Channel Name, Unit of Measure, Delta Values, Totalize Values, and Key.
- Periodic Delta Column with Attributes of an Enernoc Channel—Records the delta between the current sample and the previous sampled value of the node, along with attributes, such as Value Function, Arguments, Execution Context, and Column Position.
- Periodic Delta Column with Attributes of an Enernoc V2 Channel—Records the delta between the current sample and the previous sampled value of the node, along with attributes, such as Conversion, Value Function, Arguments, Execution Context, Column Position, and Client Source.
- Periodic Column with Attributes of an Enernoc Channel—Records the current value of the sampled node along with attributes, such as Value Function, Arguments, Execution Context, and Column Position.

Send documentation comments to cbsbu-docfeedback@cisco.com

- Periodic Column with Attributes of an Enernoc V2 Channel—Records the current value of the sampled node along with attributes, such as Conversion, Value Function, Arguments, Execution Context, Column Position, and Client Source.

Note When defining an Enernoc formatter, you can only choose one of the following column types—Periodic Delta Column with Attributes of an Enernoc Channel or Periodic Column with Attributes of an Enernoc Channel.

Note When defining an Enernoc V2 formatter, you can only choose one of the following column types—Periodic Delta Column with Attributes of an Enernoc V2 Channel or Periodic Column with Attributes of an Enernoc V2 Channel.

c. Column Source—Choose the appropriate node path from the Node Selector dialog box.

Step 9 Click **Finish** to finish the addition to the column.

Step 10 Continue with the "Defining Exporters" section on page 4-25.

Configuring Exporters

An exporter comprises two components—a transporter and a formatter. An exporter enables you to format the stored log data and send it to a third-party application or service for analysis or archiving. The Mediator currently supports four main types of transport mechanisms: Standard FTP, Secure FTP, HTTP Post, and SMTP.

This section includes the following topics:

Table 4-7 outlines compatible combinations of log column types, exporters, formatters, and transporters. Any deviation from these recommended combinations could result in incompatibility issues.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 4-7 Recommended Log Column and Exporter Combinations

Log Column Type	Exporter Type	Formatter Type	Transporter Type
• Periodic column • Periodic delta column • Periodic average column	Silicon Energy	Silicon Energy XML	Silicon Energy HTTP Post
	• Standard periodic data • Synchronized • Triggered	CSV	• HTTP Post • SMTP • Secure FTP • Standard FTP
		Delimited data	• HTTP Post • SMTP • Secure FTP • Standard FTP
		XML	• HTTP Post • SMTP • Secure FTP • Standard FTP
Periodic delta column with attributes of an FSG channel	• Standard periodic data • Synchronized • Triggered	FSG XML	• Secure FTP • Standard FTP
		MeterMail XML	• Secure FTP • Standard FTP
Periodic delta column with attributes of an Enernoc channel	• Standard periodic data • Synchronized • Triggered	Enernoc	• Secure FTP • Standard FTP
• Periodic delta column with attributes of an Enernoc channel • Periodic column with attributes of an Enernoc channel	• Standard periodic data • Synchronized • Triggered	Enernoc	• Secure FTP • Standard FTP
• Periodic delta column with attributes of an Enernoc V2 channel • Periodic column with attributes of an Enernoc V2 channel	• Standard periodic data • Synchronized • Triggered	Enernoc V2	• Secure FTP • Standard FTP

Defining Exporters

This section describes how to configure the different types of exporters and includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

- Defining Synchronized Exporters, page 4-27
- Defining Triggered Exporters, page 4-28

Defining Silicon Energy Exporters

The Silicon Energy exporter exports data at specified intervals of time. It automatically configures the appropriate formatter, and therefore does not enable you to edit the configuration.

To define a Silicon Energy exporter, perform the following steps:

Step 1 Configure logs as outlined in the "Configuring Logs" section on page 4-22.

Step 2 Click **Next** in the Log Wizard screen to open the wizard in the Define Log Exporters mode.

Step 3 Click **New**. The Define Exporter pane appears.

Step 4 In the Define Exporter pane, perform the following steps:

a. In the Exporter Name text box, enter a descriptive name for the exporter. Alternatively, you can retain the default value.

b. From the Exporter Type drop-down list, choose **Silicon Energy exporter**.

c. In the Connection Node text box, retain the default value, which is /services/network.

d. In the Connection Attempts text box, retain the default value, which is 1.

e. In the Timeout (in secs) text box, retain the default value, which is 60.

f. From the Minutes drop-down list, choose the time interval in minutes at which the Mediator should export the data.

g. From the Hours drop-down list, choose the time interval in hours at which the Mediator should export the data.

h. From the Days drop-down list, choose the time interval in days at which the Mediator should export the data.

i. Ensure that the **Enabled** check box is selected. By default, this check box is selected.

j. Ensure that the **Debug** check box is unselected.

Step 5 Click **Next**.

Step 6 Continue with the "Defining Formatters" section on page 4-28.

Defining Standard Periodic Data Exporters

The standard periodic data exporter exports data at specified intervals of time.

To define a standard periodic data exporter, perform the following steps:

Step 1 Configure logs as outlined in the "Configuring Logs" section on page 4-22.

Step 2 Click **Next** in the Log Wizard screen to open the wizard in the Define Log Exporters mode.

Step 3 Click **New**. The Define Exporter pane appears.

Step 4 In the Define Exporter pane, perform the following steps:

a. In the Exporter Name text box, enter a descriptive name for the exporter. Alternatively, you can retain the default value.

Send documentation comments to cbsbu-docfeedback@cisco.com

b. From the Exporter Type drop-down list, choose **Standard periodic data exporter**.

c. Ensure that the **Use GMT** check box is selected. By default, this check box is selected.

d. In the Connection Node text box, retain the default value, which is /services/network.

e. In the Connection Attempts text box, retain the default value, which is 1.

f. In the Timeout (in secs) text box, retain the default value, which is 60.

g. From the Minutes drop-down list, choose the time interval in minutes at which the Mediator should export the data.

h. From the Hours drop-down list, choose the time interval in hours at which the Mediator should export the data.

i. From the Days drop-down list, choose the time interval in days at which the Mediator should export the data.

j. Ensure that the **Enabled** check box is selected. By default, this check box is selected.

k. Select the **Always Export** check box if you want to always export logs irrespective of logged data.

l. In the Synchronization Time text box, specify the initial time of the day (00:00 - 23:59) that is used to calculate when to export.

m. Ensure that the **Debug** check box is unselected.

Step 5 Click **Next**.

Step 6 Continue with the "Defining Formatters" section on page 4-28.

Defining Synchronized Exporters

The synchronized exporter exports data when the specified number of log entries are added.

To define a synchronized exporter, perform the following steps:

Step 1 Configure logs as outlined in the "Configuring Logs" section on page 4-22.

Step 2 Click **Next** in the Log Wizard screen to open the wizard in the Define Log Exporters mode.

Step 3 Click **New**. The Define Exporter pane appears.

Step 4 In the Define Exporter pane, perform the following steps:

a. In the Exporter Name text box, enter a descriptive name for the exporter. Alternatively, you can retain the default value.

b. From the Exporter Type drop-down list, choose **Synchronized exporter**.

c. Ensure that the **Enabled** check box is selected. By default, this check box is selected.

d. Ensure that the **Use GMT** check box is selected. By default, this check box is selected.

e. In the Log Multiple text box, specify the number of log entries before attempting an export.

f. In the Connection Attempts text box, retain the default value, which is 1.

g. In the Connection Node text box, retain the default value, which is /services/network.

h. In the Timeout (in secs) text box, retain the default value, which is 60.

i. Ensure that the **Debug** check box is unselected.

Step 5 Click **Next**.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 6 Continue with the "Defining Formatters" section on page 4-28.

Defining Triggered Exporters

The triggered exporter exports data when the trigger node value is set to True.

To define a triggered exporter, perform the following steps:

Step 1 Configure logs as outlined in the "Configuring Logs" section on page 4-22.

Step 2 Click **Next** in the Log Wizard screen to open the wizard in the Define Log Exporters mode.

Step 3 Click **New**. The Define Exporter pane appears.

Step 4 In the Define Exporter pane, perform the following steps:

a. In the Exporter Name text box, enter a descriptive name for the exporter. Alternatively, you can retain the default value.

b. From the Exporter Type drop-down list, choose **Triggered exporter**.

c. Ensure that the **Enabled** check box is selected. By default, this check box is selected.

d. Ensure that the **Use GMT** check box is selected. By default, this check box is selected.

e. In the Connection Attempts text box, retain the default value, which is 1.

f. In the Connection Node text box, retain the default value, which is /services/network.

g. In the Timeout (in secs) text box, retain the default value, which is 60.

h. Click the Trigger Node drop-down list to open the Node Selector dialog box. In Node Selector dialog box, search and choose the point whose node value data needs to be exported.

i. Ensure that the **Debug** check box is unselected.

Step 5 Click **Next**.

Step 6 Continue with the "Defining Formatters" section on page 4-28.

Defining Formatters

This section describes how to configure the different types of formatters and includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Defining CSV Formatters

The comma separated values (CSV) formatter stores tabular data in plain text. The lines in the text file represent the rows of a table, and the commas in the line separate values or fields in the rows of a table.

To define a CSV formatter, perform the following steps:

Step 1 Define an exporter as outlined in the "Defining Exporters" section on page 4-25.

Step 2 In the Define Formatter pane, perform the following steps:

a. In the Formatter Name text box, enter a descriptive name for the formatter. Alternatively, you can retain the default value.

b. From the Formatter Type drop-down list, choose **CSV formatter**.

c. In the Timestamp format text box, enter the format in which you want the timestamp to appear. The default format is Year-Month-Day Hour-Minutes-Second.

Step 3 Click **Next**.

Step 4 Continue with the "Defining Transporters" section on page 4-33.

Defining Delimited Data Formatters

The delimited data formatter is similar to the CSV formatter. However, the delimited data formatter enables you to specify characters for the header and the data delimiter.

To define a delimited data formatter, perform the following steps:

Step 1 Define an exporter as outlined in the "Defining Exporters" section on page 4-25.

Step 2 In the Define Formatter pane, perform the following steps:

a. In the Formatter Name text box, enter a descriptive name for the formatter. Alternatively, you can retain the default value.

b. From the Formatter Type drop-down list, choose **Delimited data formatter**.

c. In the Timestamp format text box, enter the format in which you want the timestamp to appear. The default format is Year-Month-Day Hour-Minutes-Second.

d. In the Data Delimiter text box, enter a character or a sequence of characters, such as a comma, tab, or a colon that act as delimiters and separate the values.

e. In the Header Delimiter text box, enter a character or a sequence of characters, such as a comma, tab, or a colon that act as delimiters and separate the values.

Step 3 Click **Next**.

Step 4 Continue with the "Defining Transporters" section on page 4-33.

Defining Enernoc Formatters

The Enernoc formatter is a proprietary CSV format that includes additional attributes, which are added to the Periodic Delta Column with Attributes of an Enernoc Channel configuration.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note Before defining an Enernoc formatter, ensure that the Periodic Delta Column with Attributes of an Enernoc Channel or the Periodic Column with Attributes of an Enernoc Channel column type is chosen when configuring the log. The Enernoc formatter fails to export data if any other column type is chosen.

To define an Enernoc formatter, perform the following steps:

Step 1 Define an exporter as outlined in the "Defining Exporters" section on page 4-25.

Step 2 In the Define Formatter pane, perform the following steps:

a. In the Formatter Name text box, enter a descriptive name for the formatter. Alternatively, you can retain the default value.

b. From the Formatter Type drop-down list, choose **Enernoc formatter**.

Step 3 Click **Next**.

Step 4 Define a transporter as outlined in the "Defining Transporters" section on page 4-33.

Step 5 In the node tree pane, expand the node tree, then choose **services** > **logger** > ***Log Name*** > **columns** > ***Column Name***.

The *Column Name* tab displays the following configurable attributes of the periodic log:

- Data Stream Name—The name of the Enernoc channel (point).
- Commodity
- Measure
- Unit of Measurement
- Measurement Type—The type of physical quantity being measured.

Step 6 After configuring the desired attributes, click **Save** to save the configuration.

Defining Enernoc V2 Formatters

The Enernoc V2 formatter is a proprietary CSV format that includes additional attributes, which are added to the Periodic Delta Column with Attributes of an Enernoc V2 Channel configuration.

Note Before defining an Enernoc V2 formatter, ensure that the Periodic Delta Column with Attributes of an Enernoc V2 Channel or the Periodic Column with Attributes of an Enernoc V2 Channel column type is chosen when configuring the log. The Enernoc V2 formatter fails to export data if any other column type is chosen.

To define an Enernoc V2 formatter, perform the following steps:

Step 1 Define an exporter as outlined in the "Defining Exporters" section on page 4-25.

Step 2 In the Define Formatter pane, perform the following steps:

a. In the Formatter Name text box, enter a descriptive name for the formatter. Alternatively, you can retain the default value.

b. From the Formatter Type drop-down list, choose **Enernoc V2 formatter**.

Step 3 Define a transporter as outlined in the "Defining Transporters" section on page 4-33.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 In the node tree pane, expand the node tree, then choose **services** > **logger** > ***Log Name*** > **columns** > ***Column Name***.

The *Column Name* tab displays the following configurable attributes of the periodic log:

- Client Source—The hostname or IP address of the Mediator to which the configTOOL is connected.

Step 5 After configuring the desired attributes, click **Save** to save the configuration.

Defining FSG XML Formatters

The FSG XML formatter is a proprietary XML format that includes additional attributes as defined in the log column of type Periodic Column with Attributes of an FSG channel.

To define an FSG XML formatter, perform the following steps:

Step 1 Define an exporter as outlined in the "Defining Exporters" section on page 4-25.

Step 2 In the Define Formatter pane, perform the following steps:

a. In the Formatter Name text box, enter a descriptive name for the formatter. Alternatively, you can retain the default value.

b. From the Formatter Type drop-down list, choose **FSG XML Formatter**.

c. In the Timestamp format text box, enter the format in which you want the timestamp to appear. The default format is Year-Month-Day Hour-Minutes-Second.

d. In the Location Info text box, enter a description of the device (panel) location.

e. In the Location Key text box, enter a unique ID to identify the device (panel) location.

f. In the Panel Info text box, enter a description of the device (panel).

g. In the Panel Key text box, enter a unique ID to identify the device (panel).

Step 3 Click **Next**.

Step 4 Continue with the "Defining Transporters" section on page 4-33.

Defining MeterMail XML Formatters

The MeterMail XML formatter is a proprietary XML format that includes additional attributes as described in the following procedure.

To define a MeterMail XML formatter, perform the following steps:

Step 1 Define an exporter as outlined in the "Defining Exporters" section on page 4-25.

Step 2 In the Define Formatter pane, perform the following steps:

a. In the Formatter Name text box, enter a descriptive name for the formatter. Alternatively, you can retain the default value.

b. From the Formatter Type drop-down list, choose **MeterMail XML Formatter**.

c. Enter information in the following data entry text boxes in the lower area of the pane. The information that is entered appears in the exported XML file as the value of the corresponding tag name.

Send documentation comments to cbsbu-docfeedback@cisco.com

For example, if device1 is entered in the device_name text box, the following appears in the exported XML file:
<device_name> device1 </device_name>

- device_name
- data_recorder_id
- data_recorder_label
- data_recorder_handle
- device_signature
- device_configuration_template
- device_configuration_owner
- device_configuration_tag1
- device_configuration_tag2
- device_configuration_revision
- generated_by
- generated_by_namespace
- generated_by_type
- generated_by_signature
- device_namespace
- device_type

d. Unselect the **add_smtp_envelope** check box.

Step 3 Click **Next**.

Step 4 Continue with the "Defining Transporters" section on page 4-33.

Defining Silicon Energy XML Formatters

The Silicon Energy XML formatter is a proprietary XML format that includes additional attributes that are automatically configured when the Silicon Energy XML formatter is selected as the formatter type.

To define a Silicon Energy XML formatter, perform the following steps:

Step 1 Define an exporter as outlined in the "Defining Exporters" section on page 4-25.

Step 2 In the Define Formatter pane, perform the following steps:

a. In the Formatter Name text box, enter a descriptive name for the formatter. Alternatively, you can retain the default value.

b. From the Formatter Type drop-down list, choose **Silicon Energy XML formatter**.

Step 3 Click **Next**.

Step 4 Continue with the "Defining Transporters" section on page 4-33.

Send documentation comments to cbsbu-docfeedback@cisco.com

Defining XML Formatters

The XML formatter is a generic XML format that contains timestamp, column name, and value information.

To define an XML formatter, perform the following steps:

Step 1 Define an exporter as outlined in the "Defining Exporters" section on page 4-25.

Step 2 In the Define Formatter pane, perform the following steps:

a. In the Formatter Name text box, enter a descriptive name for the formatter. Alternatively, you can retain the default value.

b. From the Formatter Type drop-down list, choose **XML formatter**.

c. Select the **Pretty Format** check box to add formatting, such as tabs and carriage returns to the XML output. If the XML output will be viewed by a human, it is helpful to select this check box. However, if it will only be parsed by a machine, you do not need to select this check box.

d. In the Information text box, enter any information that should be included with the data. For example, metadata, such as building name, equipment name, and so on.

e. In the Timestamp Format text box, enter the format in which you want the timestamp to appear. The default format is Year-Month-Day Hour-Minutes-Second.

Step 3 Click **Next**.

Step 4 Continue with the "Defining Transporters" section on page 4-33.

Defining Transporters

This section describes how to configure the different types of transporters and includes the following topics:

Defining HTTP Post Transporters

The HTTP Post transporter uses the POST request method of the HTTP protocol to upload a file from the Mediator to another host on the network.

To define an HTTP Post transporter, perform the following steps:

Step 1 Define exporters and formatters as outlined in the "Defining Exporters" section on page 4-25 and the "Defining Formatters" section on page 4-28.

Step 2 In the Define Transporter pane, perform the following steps:

a. In the Transporter Name text box, enter a descriptive name for the transporter. Alternatively, you can retain the default value.

Send documentation comments to cbsbu-docfeedback@cisco.com

b. From the Transporter Type drop-down list, choose **HTTP Post transporter**.

c. In the Timeout text box, enter an upper limit for how long the export will be attempted.

d. In the Content-Type text box, retain the default value, which is text/html. This specifies the MIME-type of the data in the message body.

e. In the Post URL text box, enter the Post URL, which is required when sending data to the web server.

f. In the User text box, enter the username of the user on the destination server. You need to specify this credential because some servers require authentication using a username and password before they respond to a POST request.

g. In the Password text box, enter the password of the user on the destination server. You need to specify this credential because some servers require authentication using a username and password before they respond to a POST request.

h. Select the **Chunk Data** check box to break the message body into a series of chunks.

Step 3 Click **Finish** to complete the configuration of the transporter.

Step 4 Click **Finish** again to complete the configuration of the Logger and Exporter Wizard.

Step 5 Click **Save** to save the configuration.

Defining Secure FTP Transporters

The secure FTP transporter uses the Secure File Transfer Protocol (sFTP), also known as the SSH File Transfer Protocol to securely copy a file from the Mediator to another host on the network.

You can define a secure FTP transporter in much the same way as a standard FTP transporter. For more information, see the "Defining Standard FTP Transporters" section on page 4-35.

Note When defining a secure FTP transporter, we recommend that you retain the port number as 22 in the Port text box.

Defining Silicon Energy HTTP Post Transporters

You can define the Silicon Energy HTTP Post transporter in much the same way as the HTTP Post transporter, except for a few attributes that are predefined.

To define a Silicon Energy HTTP Post transporter, perform the following steps:

Step 1 Define exporters and formatters as outlined in the "Defining Exporters" section on page 4-25 and the "Defining Formatters" section on page 4-28.

Step 2 In the Define Transporter pane, perform the following steps:

a. In the Transporter Name text box, enter a descriptive name for the transporter. Alternatively, you can retain the default value.

b. From the Transporter Type drop-down list, choose **Silicon Energy HTTP Post transporter**.

c. Select the **Chunk Data** check box to break the message body into a series of chunks.

d. In the **post_url** text box, enter the Post URL, which is required when sending data to the web server.

Step 3 Click **Finish** to complete the configuration of the transporter.

Step 4 Click **Finish** again to complete the configuration of the Logger and Exporter Wizard.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 5 Click **Save** to save the configuration.

Defining SMTP Transporters

The SMTP transporter uses the internet standard for e-mail to transmit a file from the Mediator to another host on the network.

To define an SMTP transporter, perform the following steps:

Step 1 Define exporters and formatters as outlined in the "Defining Exporters" section on page 4-25 and the "Defining Formatters" section on page 4-28.

Step 2 In the Define Transporter pane, perform the following steps:

a. In the Transporter Name text box, enter a descriptive name for the transporter. Alternatively, you can retain the default value.

b. From the Transporter Type drop-down list, choose **SMTP transporter**.

c. In the Host text box, enter the hostname or IP address of the e-mail server.

d. In the Subject text box, enter a description. This is the message that will appear in the e-mail.

e. In the Timeout text box, enter an upper limit for how long an export will attempt to send an e-mail.

f. In the Port text box, retain the default value, which is 25; the default port for SMTP.

g. In the Sender text box, enter the e-mail address of the sender.

h. In the Recipients text box, enter e-mail addresses of the recipients. Separate multiple addresses with commas.

i. Select the **Authenticate** check box if the e-mail server requires authentication.

j. In the Username text box, enter the username for the e-mail account on the mail server.

k. In the Password text box, enter the password of the mail server.

l. In the Custom Domain text box, enter the e-mail message heading. You can leave this text box blank.

m. Select the **Send as an attachment** check box if the e-mail message must be sent as an attachment.

n. Select the **Debug** check box to enable debugging.

Step 3 Click **Finish** to complete the configuration of the transporter.

Step 4 Click **Finish** again to complete the configuration of the Logger and Exporter Wizard.

Step 5 Click **Save** to save the configuration.

Defining Standard FTP Transporters

The standard FTP transporter uses the File Transfer Protocol (FTP) standard to copy a file from the Mediator to another host on the network.

To define a standard FTP transporter, perform the following steps:

Step 1 Define exporters and formatters as outlined in the "Defining Exporters" section on page 4-25 and the "Defining Formatters" section on page 4-28.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 2 In the Define Transporter pane, perform the following steps:

a. In the Transporter Name text box, enter a descriptive name for the transporter. Alternatively, you can retain the default value.

b. From the Transporter Type drop-down list, choose **Standard FTP transporter**.

c. In the Host text box, enter the IP address of your machine.

d. In the Username text box, enter the username to log into your machine.

e. In the Password text box, enter the password to log into your machine.

f. In the Port text box, enter the port number that is specified in your FTP client.

g. In the Directory text box, specify a shared local folder where the file will be exported.

h. In the File Name Prefix text box, enter the file name for the exported file.

i. In the File Name Suffix text box, enter the file name extension. For example, enter .log.

j. From the File Naming Scheme drop-down list, choose **timestamp**.

k. Select the **Append** check box to append a local file to a file on the remote computer, or to create a new file each time the data is exported.

l. From the Passive Mode drop-down list, choose the **On** option to complete the FTP transport in passive mode. If you choose the **Off** option, active mode is used. This setting must correspond with the setting that is specified on the destination FTP server.

m. In the Timeout text box, enter an upper limit for how long the export will be attempted.

n. Select the **Enabled** check box if you want to start the transporter and export the data. This is useful when you want to temporarily suspend the export of data without removing the log.

o. Select the **Debug** check box to enable debugging.

Step 3 Click **Finish** to complete the configuration of the transporter.

Step 4 Click **Finish** again to complete the configuration of the Logger and Exporter Wizard.

Step 5 Click **Save** to save the configuration.

Managing Mediator Configuration Files

While you can create a new configuration file using the existing NodeDefs, you are not allowed to edit the existing NodeDefs.

When you open a Mediator, configTOOL downloads a version of the NodeDef only in the following situations:

- There is a change between the local copy of the NodeDef and the NodeDef of the Mediator.
- You do not have a local copy of the NodeDef.

When you create a new configuration file, all the NodeDef versions are displayed.

This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Opening Mediator Configuration Files

The configTOOL provides four ways to open an existing configuration file as follows:

- From a stored file accessible from your computer.
- From a Mediator accessible to your computer on the network.
- From a list of recently opened configuration files.
- From a list of user-specified favorites.

You select these options from the Open Mediator submenu (see Accessing the Open Mediator Submenu, page 4-37).

This section includes the following topics:

Accessing the Open Mediator Submenu

To access the Open Mediator submenu, perform the following steps:

Step 1 Start the configTOOL (see Starting configTOOL, page 4-3).

The configTOOL window appears.

Step 2 Choose **File > Open Mediator**.

The Open Mediator submenu appears.

Stored Configuration File

To open a stored configuration file, perform the following steps:

Step 1 Choose **File > Open Mediator > From File**.

The File Open dialog box appears.

Step 2 From the Look In drop-down list, choose the folder where the configuration file is saved.

Step 3 From the list of files and folders, choose the configuration file you want to open.

Step 4 Click **OK**.

Send documentation comments to cbsbu-docfeedback@cisco.com

The file downloads onto your computer hard disk. The file path appears as the root node in the node tree.

Configuration File from the Network

To open a configuration file from the network, perform the following steps:

Step 1 Choose **File > Open Mediator > From Network**.

The Mediator Units window appears. The configTOOL performs a multicast to discover the Mediator on the network, and displays a list of the Mediator hosts.

Step 2 In the Mediator Units window, click the row describing the Mediator host, and then click **OK**.

The Login to Mediator dialog box appears .

Step 3 In the User text box, enter the username.

Step 4 In the Password text box, enter the password.

Step 5 Click **OK**.

The configTOOL window with the populated node tree appears.

The IP address of the Mediator appears as the root node in the node tree. The green indicator in the right area of the status bar indicates that Mediator is online.

Configuration File from the Recently Opened Mediator List

The configTOOL maintains a list, on the hard disk of your computer, of Mediator that have been opened recently. It allows you to download the configuration file of any Mediator on that list.

To open the configuration file from the recently opened Mediator list, perform the following steps:

Step 1 Choose **File > Open Mediator > From Recently Opened**.

The Most Recent dialog box appears.

Step 2 From the Most Recent list, choose the Mediator whose configuration file you want to open.

Step 3 Click **OK**.

If the selected Mediator is on the network, the Login to Mediator dialog box appears.

Step 4 Enter a username in the Username text box.

Step 5 Enter a password in the Password text box.

Step 6 Click **OK**.

The configTOOL window reappears. The IP address of the Mediator appears as the root node in the node tree. The green indicator in the right area of the status bar indicates that the Mediator is online.

Send documentation comments to cbsbu-docfeedback@cisco.com

Downloading the Configuration File from the Favorites List

The configTOOL maintains a list of your favorite Mediators on your computer hard disk. It allows you to download the configuration file of any Mediator in that list.

To open a configuration file from the favorites list, perform the following steps:

Step 1 To open a configuration file from the Favorites list, access the Open Mediator submenu (see Accessing the Open Mediator Submenu, page 4-37).

Step 2 Choose **File > Open Mediator > From Favorites**.

The Favorites dialog box appears.

Step 3 From the Favorites Mediator list, choose the desired Mediator, and then click **OK**.

The configTOOL window reappears. The IP address of the Mediator appears as the root node in the node tree. The green indicator in the right area of the status bar indicates that you are online with the Mediator.

Working with the Configuration File XML Code

The configuration file is coded in Extensible Markup Language (XML).

The configTOOL allows you to display the XML code of the configuration file in a special window called the XML Display window. You can use the configTOOL to display the whole file, specify a segment of the file that you want to display, or save to another file. The segment includes a selected node and its child nodes.

You can import the segment to another node by saving the segment of the file. This allows you to configure a node once, save its XML code to a file, and duplicate it without having to repeat the entire configuration procedure for each duplicate node.

This section includes the following topics:

Displaying the Configuration File XML Code

To display the entire configuration file XML code, perform the following steps:

Step 1 In the configTOOL window, choose **View > Configuration XML**.

The XML Display window appears.

The upper area in the window displays the actual XML code, and the lower area displays a graphical representation that shows the nesting structure of the file.

Step 2 Click **Load** to load an XML file saved onto your computer.

Step 3 (Optional) Click **Refresh** to refresh the XML code after you use the configTOOL to edit the file.

Send documentation comments to cbsbu-docfeedback@cisco.com

Saving Partial Configuration File XML Code to a File

To save a partial configuration file XML code, perform the following steps:

Step 1 Perform Step 1 to Step 3 as described in Displaying the Configuration File XML Code, page 4-39.

Step 2 Click **Save**.

The Save File dialog box appears.

Step 3 From the Look In drop-down list, choose the folder where you want to save the configuration file.

Step 4 In the File Name text box, enter the filename.

Note To help identify the file, you can add the file extension .xml.

Step 5 Click **OK**.

Importing Partial Configuration File XML Code to a Node

To import a partial configuration file XML code to a node, perform the following steps:

Step 1 In the node tree pane of the configTOOL window, expand or collapse the node tree to list the interface nodes.

Step 2 Click the node to which you want to import a segment of the XML code.

Step 3 Choose **Edit > Import**.

Alternatively, you can right-click the node to which you want to import a segment of the XML code, and choose **Systems > Import Configuration Fragment**.

The file selection dialog box appears.

Step 4 From the Look In drop-down list, choose the folder where you want to save the configuration file XML segment.

Step 5 In the File Name text box, enter the filename.

Step 6 Click **OK**.

The nodes represented in the XML segment appear as child node under the parent node you selected in Step 2.

Displaying Node Values

You can display the current value of a configured node from the configTOOL window. You can display the value in numerical form or in a graph form that shows changes in the value over time.

To display the node values, perform the following steps:

Step 1 In the node tree pane of the configTOOL window, expand or collapse the node tree to list the interface nodes.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 2 Right-click the node of which you want to display the value, and choose **Get Value**.

The RNA Value message dialog box appears and displays the current value of the selected node.

Step 3 Click **OK**.

Step 4 Right-click the node of which you want to display the running graph, and choose **Graph Point**.

The Mediator View Graphing tool appears with a graph of the node value.

(Optional) You can select the time interval for refreshing the value and the log interval.

Refreshing the Current Configuration

Refreshing the current Mediator configuration reloads the configuration file in the state in which it is currently stored on the Mediator. To refresh the current configuration, perform the following steps:

Step 1 On the toolbar, click the **Refresh Configuration** tool.

A dialog box appears prompting you to confirm the operation.

Step 2 Click **Yes**.

The configuration file is reloaded.

Creating an Offline Configuration File

The configTOOL allows you to create and save a new configuration file while you are in an offline mode.

To create a configuration file when you are in an offline mode, perform the following steps:

Step 1 From the toolbar, click  to open a new Mediator configuration file.

The Select Version dialog box appears.

Step 2 From the Select Version window that appears, choose the Mediator host, and then click **OK**.

The Available Devices dialog box appears.

Step 3 From the Available Devices list, choose the Mediator, and then click **OK**.

The configTOOL window with the populated node tree appears.

Step 4 Click **Interfaces** to display the available interfaces.

Step 5 Click the desired com1 or com2 node to configure.

Step 6 You can change the configuration of the selected device to create a new configuration.

Step 7 Click **Save** to save the new configuration.

The Save Mediator Configuration dialog box appears.

Step 8 In the Save Mediator Configuration dialog box, select the Mediator that you want to store the newly created configuration, and then click **OK**.

The Login to Mediator dialog box appears.

Step 9 In the Username text box, enter the username.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 10 In the Password text box, enter the password, and then click **OK**.

The Save configuration progress dialog box appears that appears indicates the status of the new configuration file.

Saving Mediator Configuration Files

This section includes the following topics:

Saving an Existing Configuration File

The configTOOL allows you to save a new or edited configuration file. This configuration file is saved to the currently active Mediator or to an another Mediator on the network.

The configTOOL supports several methods to save a file. The method you choose depends on two aspects:

- Choosing to save a new file or an existing file.
- Choosing to save the file to a hard disk or to a Mediator.

Saving a New Configuration File

When you complete generating a new configuration file, you have two options for saving the file:

- You can save it to the hard disk of your computer, (or to a computer you can access over the network) for later downloading the file to a Mediator.
- You can save it to a Mediator on the same network as the computer running the configTOOL.

Validating a Configuration

You can validate the configuration in the configTOOL. The Validate option in the configTOOL is used to find inappropriate, or omitted required text box entries. To validate the configuration, choose **File > Validate Configuration**.

  - If the configTOOL does not detect any errors, it displays a message box stating that the message configuration is valid.
  - If the configTOOL does not detect any errors, the configTOOL window switches to the Errors View (see Accessing the Errors View, page 4-7).

Exiting the configTOOL

You can either log out or exit the configTOOL. To log out of the current Mediator session without exiting from the configTOOL, you have to choose Open Mediator > Logout.

To exit the configTOOL, perform the following steps:

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 1 Choose **File > Open > Exit**.

Step 2 Click **OK** to confirm the exit.

Uninstalling the configTOOL

To uninstall the configTOOL application on a Windows PC, perform the following steps:

Step 1 Close all running instances of configTOOL.

Step 2 Choose **Start > All Programs > Cisco Systems > Uninstall Mediator ConfigTOOL** to run the uninstall script.

Step 3 When you are prompted with the following message, press **Y**.

You are presented with the message:

Are you sure you want to Uninstall?

Press **Y** to uninstall, or **N** to exit.

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 5

perfectHOST

This chapter provides a description of the supervisory control capabilities of the Cisco Network Building Mediator (Mediator), and describes how to use the perfectHOST graphical programming software.

This chapter includes the following topics:

Note Before you install, operate, or service the system, read the *Regulatory Compliance and Safety Information for the Cisco Network Building Mediator* document for important safety information.

Overview

perfectHOST is graphical programming software used for creating complex and sophisticated building automation and control programs. Graphical programming is the creation of a schematic drawing of the desired control scheme, using a library of symbols called *Templates*. These templates are placed on the computer screen and interconnected by lines, which direct the flow of data. The control scheme is drawn from the inputs, through the control logic. The control logic directs inputs to the outputs.

Send documentation comments to cbsbu-docfeedback@cisco.com

When the drawing is completed, it is converted into a computer program, which is downloaded into the Mediator. perfectHOST programming gives the Mediator the ability to act as a powerful supervisory control platform incorporating any integrated system, device, or protocol into intelligent business applications.

The perfectHOST application that runs on the Mediator is also known as the Templates Inside Mediator (TIM) application.

perfectHOST Templates

This section includes the following topics:

Programming Graphics

In perfectHOST, the control logic and programs are created by placing logical elements within a drawing. These logical elements are called perfectHOST templates. You can connect the inputs and outputs of these templates to control the data flow through a program.

You can place the templates on your drawing workspace and interconnect them by lines, which direct the flow of the data. The control scheme is drawn from the inputs, through the control logic. The control logic directs inputs to the outputs.

When the drawing is completed, it is converted into a computer program, which is downloaded into the Mediator. The perfectHOST programming tool gives the Mediator its ability to act as a powerful supervisory control platform, incorporating any integrated system, device, or protocol into intelligent business applications.

Templates and Macros

A template is a self-contained logical element. It is externally comprised of a graphical symbol with input and output connection points.The graphical symbol should serve as a visual mnemonic of the function performed by the template. Input points receive data from other templates and output points send their values to other templates.

Each template is represented by a logical element and is associated to a system action and default variables attached to it. These system actions and default variables perform various basic functions. In this way, although you do not create variables for each template, you can control the logic and program within the system.

Macros are sets of instructions or drawings that perform specific operations on target devices. The perfectHOST macros contain an application drawing that contains other templates. It has inputs and outputs like a regular template and associates them with the inputs and outputs of templates contained in the drawing. Macro templates can contain other Macro templates. All macros have predefined functionalities.

Send documentation comments to cbsbu-docfeedback@cisco.com

Installing perfectHOST

The Mediator perfectHOST software should be installed on your computer.

This section includes the following topics:

Prerequisites

The prerequisites for perfectHOST programming for the Mediator are as follows:

- IP address of the Mediator
- PC with perfectHOST installed
- PC with a web browser

  For a PC running the perfectHOST software, we recommend that you use Windows-based platforms (95 or later) with 2 GB of RAM and 10 GB of free disk space.

Installation Instructions

To install this software, access Cisco.com at the following website:

http://www.cisco.com/en/US/products/ps10454/index.html

This software is available in the Support section at this website.

Note To download this software, you need to have a valid CCO username and password.

To download and install the software on your workstation, perform the following steps:

Step 1 Click **Download Software**.

Step 2 Choose **Smart Connected Building Software > Cisco Network Building Mediator**.

Step 3 Choose the appropriate hardware platform.

Step 4 Click **Network Building Mediator Programming Software** to download perfectHOST.

Step 5 Choose the appropriate release, click the release number, and click **Download Now**.

The Download Cart page appears.

Step 6 Click **Publish**.

The Cisco End-User Software License Agreement page appears.

Step 7 Click **Agree** to accept the software download rules specified in the Cisco End-User Software License Agreement page. Click **Disagree** to cancel the download process.

The download software page appears with two options to download perfectHOST.

- Download Manager Option
- Non-Java Download Option

Send documentation comments to cbsbu-docfeedback@cisco.com

Note The Download Manager Option requires a working Java version of 1.4.2.xx and later. If you choose this option to download the perfectHOST software, the file is saved on your PC and you are allowed to run this file to install this software.

Step 8 Click **Non-Java Download Option** to proceed with the download.

Step 9 Click **Download URL** to download perfectHOST.

The file download dialog box appears.

Step 10 Click **Run**.

You see the welcome message in the perfectHOST Installer window.

Step 11 Click **Next** and follow the instructions to install perfectHOST. Alternatively, click **Cancel** to cancel the download process.

Step 12 Once you install perfectHOST, you can start this application from **Start > All Programs > Cisco Systems > perfectHOST**.

Creating perfectHOST Applications

Note The following procedure assumes that you have installed perfectHOST on your PC.

To create a new perfectHOST application on your PC, perform the following steps:

Step 1 Choose **Start > All Programs > Cisco Systems > perfectHOST**.

The perfectHOST homepage appears.

Step 2 Click **Application Editor**.

The Select Application dialog box appears.

Step 3 Click **New**.

The Prompter dialog box appears.

Step 4 In the Enter Job Name text box, enter the new job name, and click **OK**.

The Please Confirm dialog box appears.

Step 5 Click **Yes** to create a new application.

Connecting to the Mediator with perfectHOST

To connect to the Mediator with perfectHOST, perform the following steps:

Step 1 Perform the tasks described in Creating perfectHOST Applications, page 5-4.

Step 2 Choose **System > Com Settings**.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Communication Settings dialog box appears. By default, the Direct radio button is selected.

Step 3 Select the **Mediator/M2** radio button.

Step 4 In the IP text box, enter the hostname or the IP address of your Mediator, and click **OK**.

Note All IP addresses are subject to change, based on the location where the Mediator is installed.

Step 5 Choose **File > Save Application**.

Step 6 Choose **System > Communications and Administration**.

The Perfect Host Communication dialog box appears.

Step 7 Click **Get Broadway.xml File**.

If prompted to accept, click **Yes**. You will see a flashing command prompt, while the file is downloaded. When the command prompt stops flashing, the download of the broadway.xml file is complete.

Templates and Macro Groups

This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Default Templates and Macro Groups

The perfectHOST programming tool provides you with predefined templates and macros, which are grouped based on their functionalities. Table 5-1 describes the types of templates and macros that are grouped together.

Table 5-1 Templates and Macro Groups

Group	Sub Group	Available Template	Available Macro
control	central.plt	• boilrset • enthlpy.ecn • oachgovr • rampchill • reheat.rh • timepro1 • timepro1.adp • timepro1.at • timepro2.at • timepro3.at • timepro4.at	• Altrnatr • Altrnatr.rt • blsel3-2
	deadband	• db-cool • db-cool.stg • db-heat • db-heat.stg • db-hilo • dblimit • hyster • window • windowot	dbsubsub

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	electric	• edl-pri • edl-time • edl.bot • edl.top • sw.15 • sw.5 • swavg.15 • swprdct.15	NA
	lighting	NA	NA
	pids	• pid-cool • pid-cool.acc • pid-cool.ovi • pid-dir.acc • pid-heat • pid-heat.acc • pid-heat.ovi • pid-rev.acc • piddeh.ovi • pide2	NA

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	unitary	NA	• ahc2ecn • aheconfp • ahhwvf • ahuc1h1f • ahuc1h1f.ecn • ahuc1h1f.pat • ahuc1h1f.pdc • ahuc1h2f • ahuc1h2f.dmo • ahuc2h2f • ahuc2h2f.hum • ahuc2h2f.shd • ahuc2h2f.v2 • ahuc2hve • ahuc2hvf • ahucvh2f.eca • ahucvh2f.ecn • ahucvhvf • ahuprop.vav • econc2hv • econoclg • interlck • rtu(gas) • rtu(gas).shd • serv-rmp • vav-mtr.pos • vavmtr.clg • vavmtr.htg • vavrz100
	NA	• accum • counter • udcount	• accum.add • accum.mac

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
ios	analog.dig	• _ai_di • _aidi2do • _aidimux.ao • _aidimux_lax • _ao_1_do • _ao_2_do • _ao_3_do • _ao_4_do • _ao_5_do • _ao_di.spl • _ao_do24 • _dodi-sp.acc • _st-c3ao.4d0 • _st-s3ao.4do	NA

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	analog.io	• _1000ohm.aov • _aci2252 • _ad590 • _ai-ao_v • _ai-mam • _ai0-10v • _ai0-10v.ao • _ai0-5v.ao • _ai4-20 • _ai-20.ao • _ai-20.aov • _ai_c • _ai_hv_aov • _ai_lv.aov • _ai_v • _aihv.aov • _air100 • _air1000 • _ao • _ao_v • _aomux • _aopulse • _ba592.aov • _bc.10k • _bc10k.ao • _bc10k.hot • _belimo.b • _f-t10-f • _f-t30 • _he6000 • _im1000 • _mam205.b7 • _p593-3.h20	NA

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	NA	• _p593flw.5v • _p593flw.5vr • _p593flw.esc • _p593flw.low • _pcon • _pcon.aov • _platinm.375 • _pltnmht.375 • _pot104 • _rh • _rtd_1kp • _rtd_bc • _rtd_bc.ao • _rtd_ben.ao • _rzdp01 • _setpnt.10k • _setpnt.1k • _setpnt.s80 • _setpnt.spl • _st-c3 • _st-c3.ao • _st-c3.spl • _st-c3ht • _st-c3ht.ao • _st-s2 • _st-s2.ao • _st-s2.spl • _st-s3 • _st-s3.ao • _st-s3.spl • _st-s3ht • _stc3mrt.ao • _sts-3ht.ao • _sts3mrt.ao • _ta2keg	NA

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	NA	• _tcs1000.2a • _tcs1000.5 • _usr-116.ao • _vaisala	
	digital.inp	• _di • _di_nc • _di_off • _di_on • _dipulse • _ditimer	NA
	digital.out	• _do • _do_nc • _dodlync • _hoa • _hoa2 • _lcp • _lcp.dpb	_do_hoa
logic	latches	• edge.det • flipflop • freqdiv.2 • freqdiv.3 • freqdiv.4 • hiedge • latch • latch12 • latchmax • latchmin • lowpass • setreset • strstop	NA

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	selectors	• month.sel • moselect • sel • select • select.03 • select.04 • select.10 • select.24 • select.day • sp-clght.sel	NA
		• and • and3 • and4 • and5 • and7 • invert • nand • nand3 • nand4 • nand5 • nor • nor3 • nor4 • nor5 • not • or • oe12 • or14 • oe3 • or4 • or5 • or6 • xor	

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
math	averages	• average • avg • avg10 • avg10sel • avg15 • avg15sel • avg20 • avg20sel • avg3 • avg3sel • avg4 • avg4sel • avg5 • avg5sel • avg6 • avg7 • avg7sel • avg8 • avg8sel	NA

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	compare	• equal • equal.dat • equal.int • gtthat • hiselect.07 • hiselect.12 • hiselect.4 • hiselect.6 • hiselect.8 • loselect.10 • loselect.4 • ltthan • lttmplt • max • max3 • min • min3 • minmax	• gtthat • hiselect.3 • loselect.3 • max10 • max6 • min6
	covs	• cov • cov.01 • cov.1 • cov.25 • cov.5 • roundoff • roundpt1	• covlpss.tm • covlpss1.tm • mintrim

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	formula	• bitfield • cfm2lts • cfmto% • cfmtowc • ctof • dewpoint • enth2 • enthalpy • ftoc • hour_sec • intergar • ltrs2cfm • res • reset • sqrt • stom • timssmcv • truncate • wc2cfm.xfl	• bblcfm • in4out16
	NA	• abs • add • add10 • add12 • add15 • add3 • add6 • div • fraction • mul • remaindr • sub	NA
nodes	NA	• mpxget • mpxset	kmc

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
protocol	acm	• acm3300.3wd • acm3300.hz • acm3300.kwh • acm3300.pft • acm3300.std • wizon	NA
	act	• act_lcm • act_lcm.cid • act.lcm.dmx • act.lcm.mux • act_mac • act_mix • act_mpc	• scale.aea • scale.mix
	asi	• asivvd.sp2 • asivvd.spx	• asivvd.afs • asivvd.aht • asivvd.alm • asivvd.sps • asivvd.stx • asivvd.tb3 • asivvd.tb5
	bacnet	• bacnet • bacnet.ai • bacnet.ao • bacnet.bi • bacnet.bo	NA
	barbcole	• bcpem • bczone2.1 • bczone2.2	NA
	barring	microstr	NA
	bellcan	bc.chp	NA

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	carddread	• card.apb • card.cmp • card.rdr • card.tmr • card128.apb • card64.apb	NA
	carrier	• datalink.rd1 • datalink.wr1 • datalink.rd • datalink.wr • carrier.15 • carrier.dp	NA
	compu.air	ca2100	NA
	csi.	• ciscoucm • csi • csi1 • csi_10 • mr	• csi_vav1 • csiahu17
	dunham	dunhmbsh	NA
	func.dev	• fd_ai • fd_ao • fd_di • fd_do • fdcd9fdm	NA
	handheld	• hhmenu • hhpasswd • hhpoint	NA
	hsq	• hsq • hsq.ai • hsq.di • hsq.dv • hsq.sp	• hsq.af • hsq.av • hsq.dvm • hsq.zt
	hyrdolab	NA	• hydrolab • hydrolab.2

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	johnson	• n2 • n2.rd • n2.wr • n2master	NA
	mcquay	• mcquay.rd • mcquay.rd2 • mcquay.ts • mcquay_s.rd	NA
	mix	NA	• mixlc • mixlc.1 • mixcl.2 • mxprcn10.mac
	rz	• rzahu • rzahu.sv • rzahuscl • rzvav • rzvav.sc1 • rzvav.sc2 • rzvav1 • rzvav8.t2 • rzvav8.t3 • rzvvnvoe.t • rzvvnvoe.tav • rzvvnvos.t • rzvvnvos.tav • vav1indx • vav250n.t	• rzah2e • rzahu.bll • rzahus2 • rzvav.dat • rzvav.ss2 • rzvav8 • rzvavnvo • rzvavnvo • rzvvnvoe • rzvvnvoe.sav • rzvvnvos • rzvvnvos.sav • vav250.prn • vav250n • vavwrhtf.loc • vavwrhtf.wsa

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	staefa	• smart1.tst • smart1.vav • smart1dd.smt • smart1dd.svi • smart2 • smart2.bit • smart2.dds • smart2.do0 • smart2.do1 • smart2.do2 • smart2.do3 • smart2.do4 • smart2.do5 • smart2.htp • smart2.in • smart2.ins • smart2.max • smart2.min • smart2.po6 • smart2.po7 • smart2.rd • smart2.rst • smart2.tst • smart2.va1 • smart2.vav • smart2a.ddc • smart2b.vav • smart2mx.tst • smart2si.ddc • staefa.rw • staefa.rw4 • staefa.rw9 • staefa.wr	smart2di.rev

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	trane	• trane • tranecon.fgr • tranes1 • tranevav	NA
	triatek	• triatecn • triatek	NA
	york	• yorktalk • yorktalk.15 • yorktalk.16 • york.cmd • yorkalk.fsp	NA
python	NA	hello.py	NA
		pulse.mpx	NA

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
timings	delays	• delayoff • delayoff.rt • delayon • delayon.rt • dlystart • dutycycl • dutycycl.rt • hobbs • minoff • minoff.rt • minon • minon.rt • ramp.up • seconds • time • time.fmt	• hotlovr • maxon • minonoff • minonoff.rt • runtime • runtime.pgm
	sched	• optstart.c • optstart.h\optstart.hsp • optstrmd.8r • rampschd • rampsoak • date • date.dm • day • hours • minutes • schedule • timeclok	• optclgmd.8r • opthtgmd.8r • optstart.csp • optstart.h-c • predict.hst

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	triggers	• pulse.tmp • trg05m.60m • trg05s.60m • trg55m.60m • trig00.60 • trig1hr • trighr.tmp • trig24 • trig24.60 • trigday • trigger • trigger.01m • trigger.02h • trigger.02m • trigger.05m • trigger.05s • trigger.06m • trigger.12h • trigger.15m • trigger.15s • trigger.24h • trigger.30m • trigger.30s • trigger.60m • trigger.mth • trigger.wek • trig.wknd	NA

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
ui	alarms	• Talamac • alarm • alarm.1 • alarm.2 • alarm.3 • alarm.4 • alarm.5 • alarm.6 • alarm.7 • alarm.8 • alarm.m0 • alarm.m1 • alarm.m2 • alarm.m4 • alrmlmts	NA
	diagnose.sys	• peekbyte • peekdwrd • peekword • stimulate	• actual.run • ipfault • landiagm • landiag • status.lan
	graphics	NA	NA
	override	• ovdwntmr • ovdwntmr.sec • ref • trimbak • trimdwn • trimmer • trimup	• autonoff • autonoff.100 • autonoff.adj • hldtrim2 • holdtrim • liteovrd.mac • override.1-0 • override.1.-1 • override.15 • override.1 hr • override.1mn • trimana

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 5-1 Templates and Macro Groups (continued)

Group	Sub Group	Available Template	Available Macro
	trends	• degreday.c • degreday.h • trendlog.1 • trendlog.1c • trendlog.2 • trendlog.2c • trendlog.3 • trendlog.3c • trendlog.4 • trendlog.4c • trendlog.5 • trendlog.5c • trendlog.6 • trendlog.6c • trendlog.7 • trendlog.7c • trendlog.8 • trendlog.8c • trendlog.9 • trendlog.9c • trendn.4	• logavg.jee • loginter.sec • loginter.jee
user	NA	• integer.b • gttmplt • ao_do	runtime.fzd

Most Frequently Used Templates

This section describes the function of the most frequently used templates.

This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

absolute

This section includes the following topics:

Symbol

Figure 5-1 shows the absolute template.

Figure 5-1 absolute Template

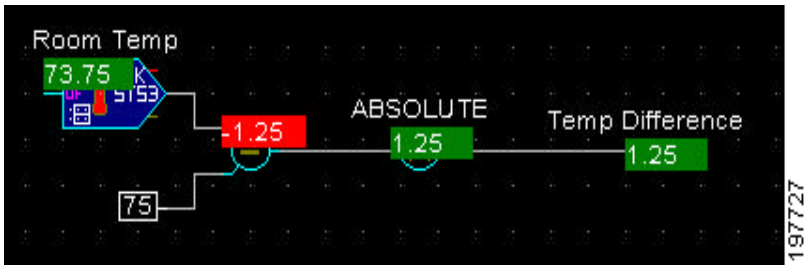
Function

This template accepts a negative or positive number as an input value and converts it to a positive value.

Example

In the following example, the negative value of 125 passes through the absolute template and shows a positive value 125 (see Figure 5-2).

Figure 5-2 Example - absolute Template



add

This section includes the following topics:

Symbol

Figure 5-3 shows the add template.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-3 add Template

Function

This template adds all the input values and displays the end output result.

Example

In the following example, the input numbers are added and the output values display the total sum of the input numbers (see Figure 5-4).

Figure 5-4 Example - add Template

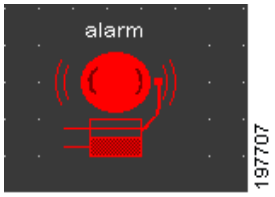
alarm

This section includes the following topics:

Symbol

Figure 5-5 shows the alarm template.

Figure 5-5 alarm Template



Function

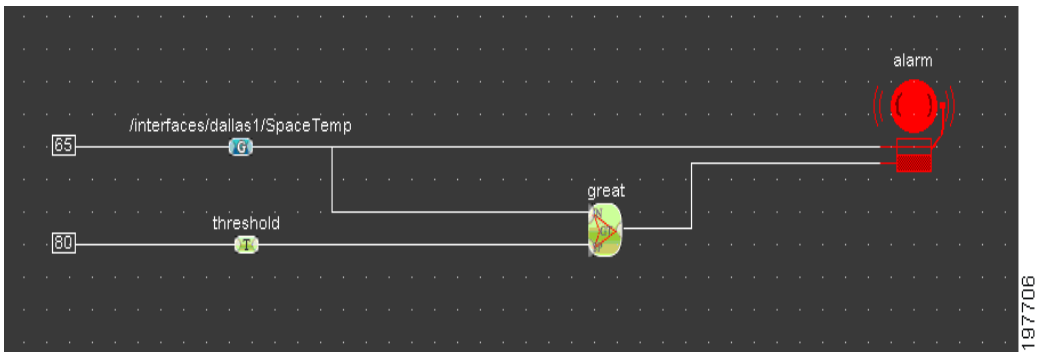
This template alerts you if there is a problem in your Mediator network. All the associated warnings are displayed on your PC, which monitors this system.

Send documentation comments to cbsbu-docfeedback@cisco.com

Example

The following example shows the template displaying an alarm, when it received an input value of one (see Figure 5-6).

Figure 5-6 Example - alarm Template



and

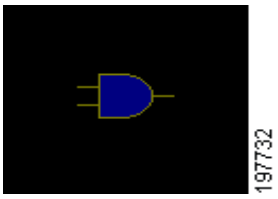
This section includes the following topics:

- Symbol, page 5-29
- Function, page 5-29
- Example, page 5-29

Symbol

Figure 5-7 shows the and template.

Figure 5-7 and Template



Function

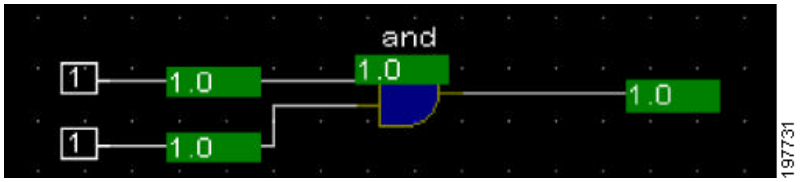
This template is one of the basic logic templates. The output value is one only if both the input values are one. If either of the input values is zero, the output value displays as zero.

Example

In the following example, the input values are one which results in the output value of one (see Figure 5-8).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-8 Example - and Template



_ao

This section includes the following topics:

Symbol

Figure 5-9 shows the _ao template.

Figure 5-9 _ao Template

Function

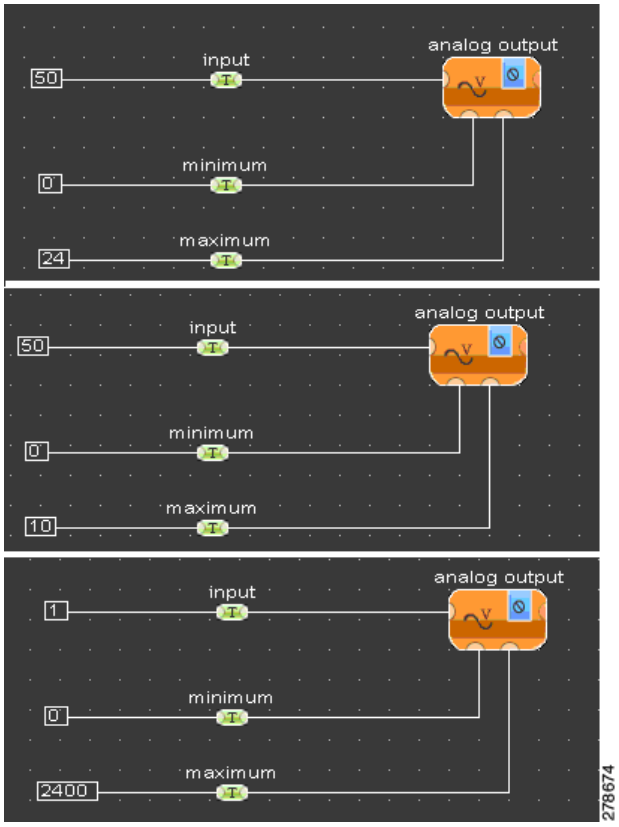
The _ao template generates scalable output. The input percentage is scaled between the minimum and maximum voltages, and converted to voltage produced at as analog output.

Example

In the following example, the input values are in a range of 0- 24 VDC, an input of 50% produces an output voltage of 12 V at the analogue output (see Figure 5-10).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-10 Example- _ao Template



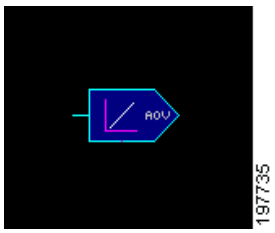
_ao_v

This section includes the following topics:

Symbol

Figure 5-11 shows the _ao_v template.

Figure 5-11 _ao_v Template



Send documentation comments to cbsbu-docfeedback@cisco.com

Function

This template converts an input value to an output voltage. This template can convert an input value to an output voltage of a maximum value of 24 VDC. If you connect a value of 100 to this template, it converts this value to an output voltage of 24 VDC.

Example

The following example shows how the template produces a voltage of 12 V at the analog output in which it is assigned (see Figure 5-12).

Figure 5-12 Example - _ao_v Template

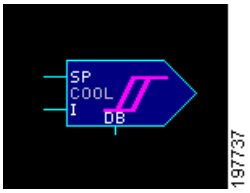
db-cool

This section includes the following topics:

Symbol

Figure 5-13 shows the db-cool template.

Figure 5-13 db-cool Template



Function

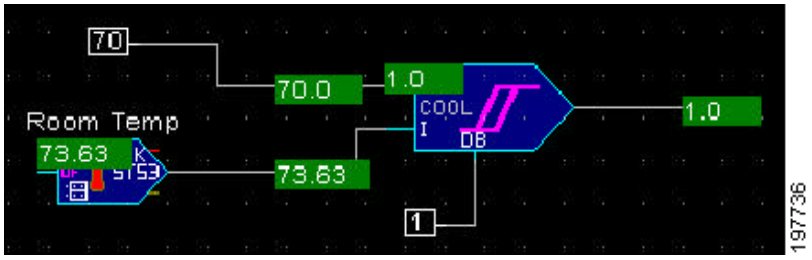
This template is used for the deadband control loop cooling. It produces an ON/OFF output in response to the input variable (normally the controlled space temperature) differing from the setpoint by more than the deadband range. The deadband is user-selectable.

Example

The following example shows a setpoint of 70 and a deadband of one, which in turn makes the deadband range from 69 to 71. The ouput value of the template does not go to zero until the input variable goes below 69, and does not go to one until the input variable goes above 71 (see Figure 5-14).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-14 Example - db-cool Template



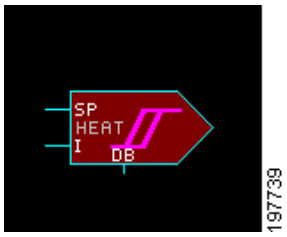
db-heat

This section includes the following topics:

Symbol

Figure 5-15 shows the db-heat template.

Figure 5-15 db-heat Template



Function

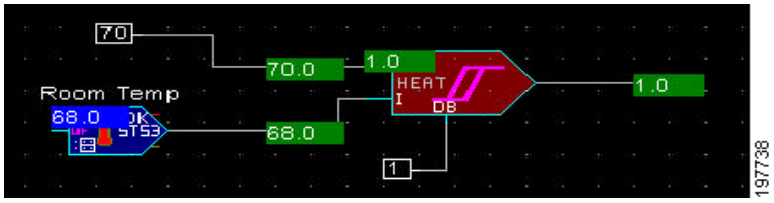
This template is used for deadband control loop heating. It produces an ON/OFF output in response to the input variable (normally the controlled space temperature) differing from the setpoint by more than the deadband range. The deadband is user-selectable.

Example

The following example shows a setpoint of 70 and a deadband of one, which in turn takes the deadband range from 69 to 71. The output of the template does not reach zero until the input variable goes above 71, and does not reach one until the variable reaches a value below 69 (see Figure 5-16).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-16 Example - db-heat Template



delayon

This section includes the following topics:

Symbol

Figure 5-17 shows the delayon template.

Figure 5-17 delayon Template

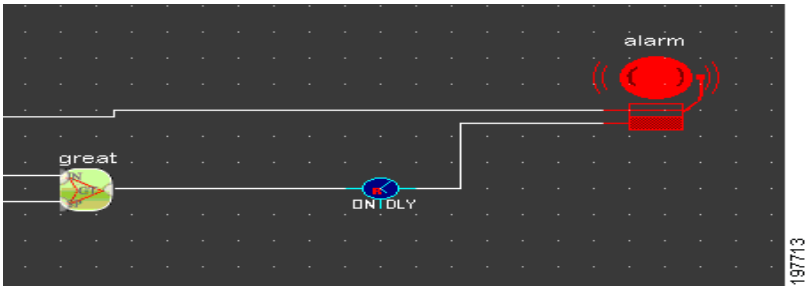
Function

The timing template changes an input value from zero to one. When the input value transitions from zero to one, the output value changes to one only after the delay time. When the input value transitions from one to zero, the output value changes to zero immediately.

Example

The following example shows how the delayon template retains the input value till the specified timeout (see Figure 5-18).

Figure 5-18 Example - delayon Template



Send documentation comments to cbsbu-docfeedback@cisco.com

delayoff

This section includes the following topics:

Symbol

Figure 5-19 shows the delayoff template.

Figure 5-19 delayoff Template

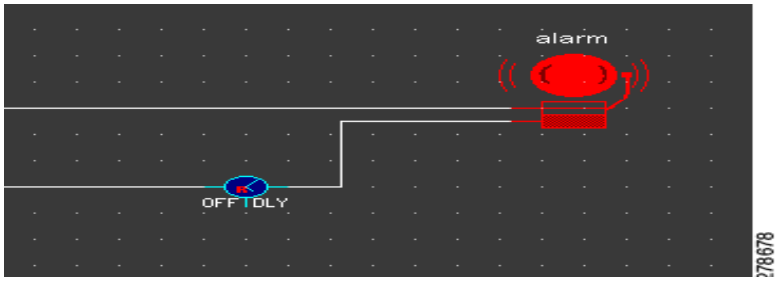
Function

The timing template changes an input value from one to zero. When the input value transitions from one to zero, the output value changes to zero only after the delay time. When the input value transitions to one, the output value changes to one immediately.

Example

The following example shows that the input value is overridden to a value of zero while the delayoff template displays a value of one until the specified delayoff period (see Figure 5-20).

Figure 5-20 Example - delayoff Template



_di_on

This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Symbol

Figure 5-21 shows the _di_on template.

Figure 5-21 _di_on Template

Function

A digital input (DI) senses whether a circuit is open or closed. A DI sources high voltages to one side of a set of contacts, and detects the presence of voltage on the other side of the contacts. Digital inputs are used to determine if equipment is working.

Example

The following example shows how a fan relay when connected to this template, displays an output value as zero when the relay contacts open (see Figure 5-22).

Figure 5-22 Example - _di_on Template

div

This section includes the following topics:

Symbol

Figure 5-23 shows the div template.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-23 div Template

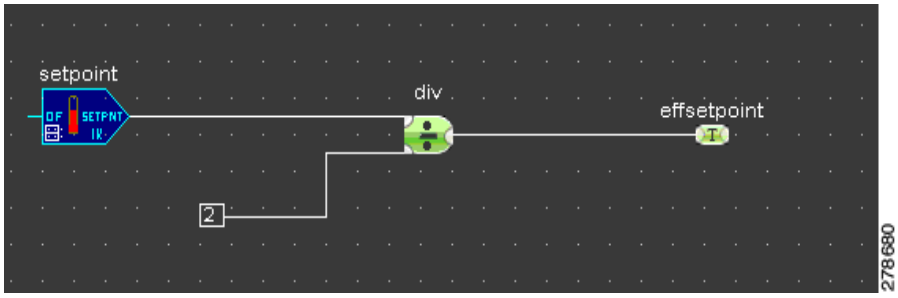
Function

This template divides the upper input by the lower input and shows the resulting output value. The output result displays a maximum value of two decimal places.

Example

The following example shows how the room setpoint when divided by two, displays an output value that is the dividend of the input value (see Figure 5-24).

Figure 5-24 Example - div Template



dlystart

This section includes the following topics:

Symbol

Figure 5-25 shows the dlystart template.

Figure 5-25 dlystart Template

Send documentation comments to cbsbu-docfeedback@cisco.com

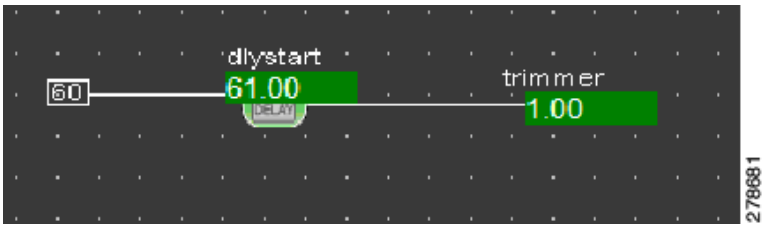
Function

This is a timing template. When an application is downloaded to a controller, or if the controller has just been powered on, this template does not show an output value of one, until the specified delay period is over.

Example

In the following example, the dlystart template is used to delay equipment, such as a fan, for a specified period. This template acts as a timer and times out at one second over the specified period and an output value of one second (see Figure 5-26).

Figure 5-26 Example - dlystart Template



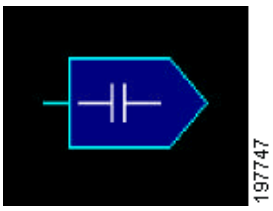
_do

This section includes the following topics:

Symbol

Figure 5-27 shows the _do template.

Figure 5-27 _do Template



Function

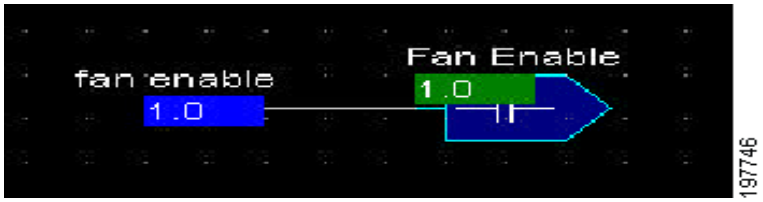
A digital output (DO) template closes an electrical circuit, typically with a set of contacts in a relay mounted on a controller. The closing of the circuit connects the power to a device, such as connecting power to a fan to start it.

Example

The following example shows how you can use this template to enable or disable equipment, such as a fan that is connected to a digital output template (see Figure 5-28).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-28 Example - _do Template



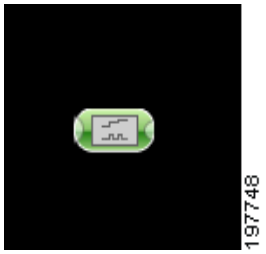
edgedet

This section includes the following topics:

Symbol

Figure 5-29 shows the edgedet template.

Figure 5-29 edgedet Template



Function

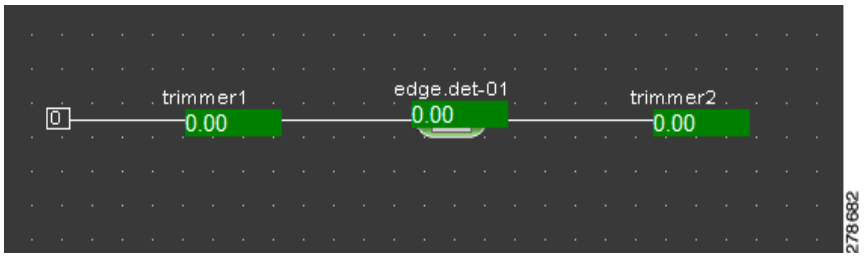
This template is sued to freeze a value within your application until some other condition arises.

Example

In the following example, the output value is true for one second when the input value changes from zero to one or from one to zero (see Figure 5-30).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-30 Example - edgedet Template



gtthan

This section includes the following topics:

Symbol

Figure 5-31 shows the gtthan template.

Figure 5-31 gtthan Template

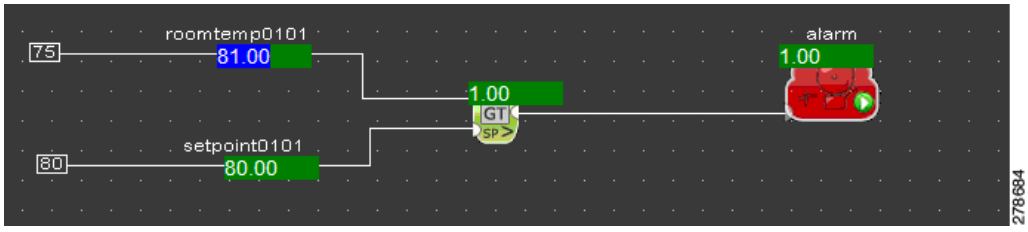
Function

This is a maths template that is an abbreviation for greater than. This displays an output value of one if the upper input value is greater than the value on the lower input. If both the input values are equal, or if the value of the lower input is greater, then the output is zero.

Example

In the following example, the gtthan template compares the room temperature to a setpoint and triggers an alarm when the room temperature is greater than the setpoint (see Figure 5-32)

Figure 5-32 Example - gtthan Template



Send documentation comments to cbsbu-docfeedback@cisco.com

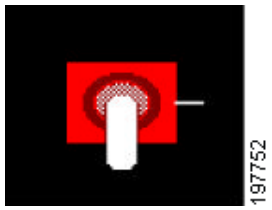
_hoa

This section includes the following topics:

Symbol

Figure 5-33 shows the _hoa template.

Figure 5-33 _hoa Template



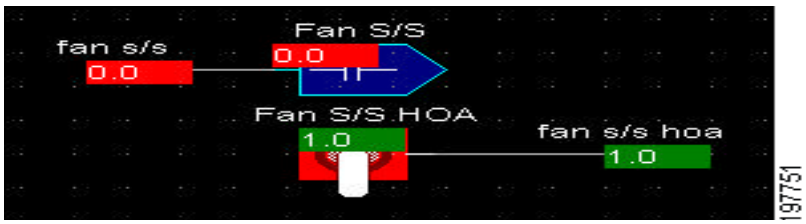
Function

This template displays an output number that corresponds to the position of the HOA switch. An HOA switch allows manual control over digital output. This three-position switch can manually override the relay on when in the hand position; manually override the relay off when in the off position; or it can allow the relay to be controlled by the application logic when it is in the auto position.

Example

In the following example, the _hoa template reports that the HOA switch on the board is in the auto position. The relay is not switched on because the logic does not call for it to be on (see Figure 5-34).

Figure 5-34 Example - _hoa Template



hours

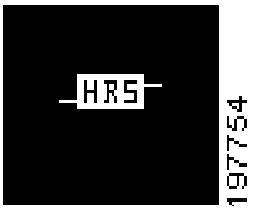
This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Symbol

Figure 5-35 shows the hours template.

Figure 5-35 hours Template



Function

This is a time conversion template. The seconds value is the standard value, thus the necessity for inputs values to be in seconds.

Example

In the following example, the template shows the conversion from two hours to 7200 seconds. If you prefer to use hours, you can use the hours template to convert hours to seconds (see Figure 5-36).

Figure 5-36 Example - hours Template

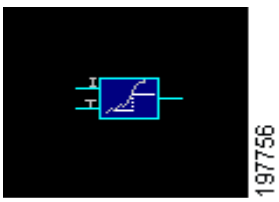
latch

This section includes the following topics:

Symbol

Figure 5-37 shows the latch template.

Figure 5-37 latch Template



Send documentation comments to cbsbu-docfeedback@cisco.com

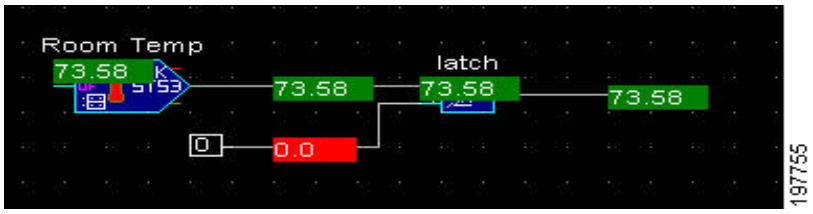
Function

This template latches the input values when the trigger goes from a low value to higher value.

Example

The following example shows the Room Temp value passing through the latch template. When the trigger value goes to a zero, the next value is not latched until the trigger turns true (see Figure 5-38).

Figure 5-38 Example - latch Template



latchmax

This section includes the following topics:

Symbol

Figure 5-39 shows the latchmax template.

Figure 5-39 latchmax Template

Function

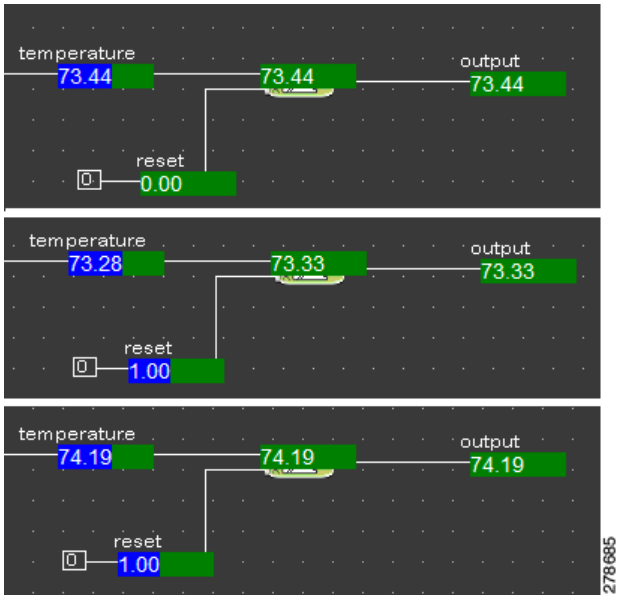
This template continuously stores the maximum value in a given period of time until you reset the value.

Example

In the following example, the room temperature of 73.44°C passes through the latchmax templates. When the reset value is set at two, this template passes through the minimum value that was latched at the stipulated time. In this case, although the room temperature drops to 72.38°C, the trimmer value is 73.33°C (see Figure 5-40).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-40 Example - latchmax Template



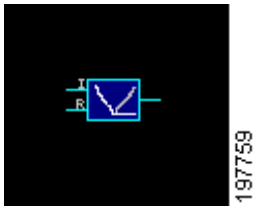
latchmin

This section includes the following topics:

Symbol

Figure 5-41 shows the latchmin template.

Figure 5-41 latchmin Template



Function

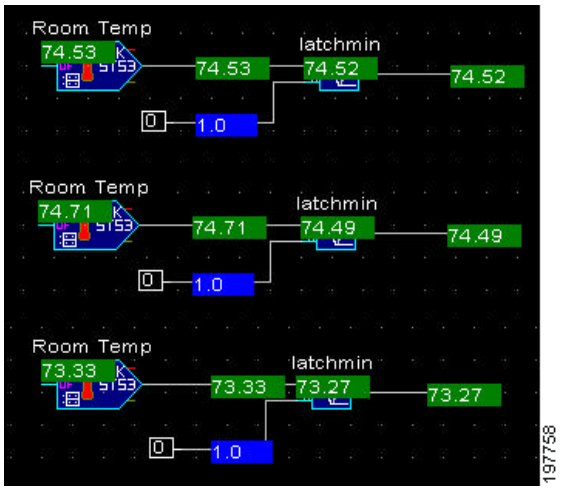
This template continuously stores the minimum value in a given period of time until you reset the value.

Example

The following example shows that the room temperate is at a minimum value. But when you reset the value, it sets the room temperature at the next minimum value (see Figure 5-42).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-42 Example - latchmin Template



ltthan

This section includes the following topics:

Symbol

Figure 5-43 shows the ltthan template.

Figure 5-43 ltthan Template

Function

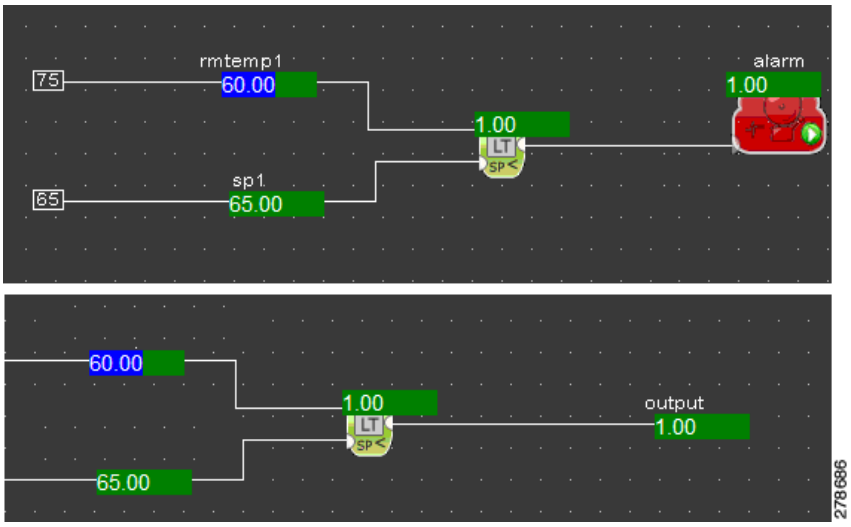
This template produces an output value of one when the upper input value is less than the lower input value. The output value is zero when the upper input value is greater. If both the inputs values are equal, then the output value is one.

Example

The following example shows how this template compares the room temperature to a setpoint and sends out an alarm when the room temperature is less than the defined setpoint (see Figure 5-44).

Figure 5-44 Example - ltthan Template

Send documentation comments to cbsbu-docfeedback@cisco.com



minon

This section includes the following topics:

Symbol

Figure 5-45 shows the minon template.

Figure 5-45 minon Template

Function

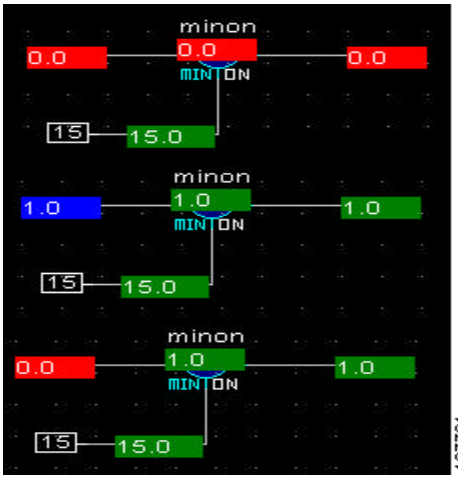
This is a minimum runtime template. When the input goes off, the output does not go off unless it has been on for the minimum specified time. This prevents the short-cycling of devices.

Example

In the following example, when the input value transitions from zero to one, the output value is one only if the output value has been one for the minimum specified period (see Figure 5-46).

Figure 5-46 Example - minon Template

Send documentation comments to cbsbu-docfeedback@cisco.com



minutes

This section includes the following topics:

Symbol

Figure 5-47 shows the minutes template.

Figure 5-47 minutes Template

Function

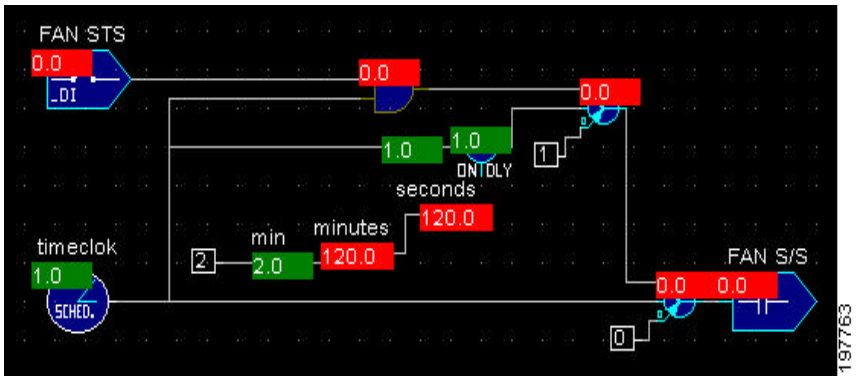
This is a time conversion template where the second is a standard value.

Example

In the following example, the seconds are converted to minutes using this template (see Figure 5-48).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-48 Example - minutes Template



multiply

This section includes the following topics:

Symbol

Figure 5-49 shows the multiply template.

Figure 5-49 multiply Template

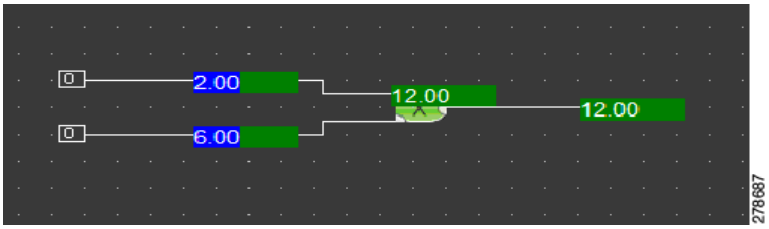
Function

This template produces an output value that is the result of its upper input value multiplied by its lower input value.

Example

The following example shows how two input values are multiplied to produce an output value of 12 (see Figure 5-50).

Figure 5-50 Example - multiply Template



Send documentation comments to cbsbu-docfeedback@cisco.com

not

This section includes the following topics:

Symbol

Figure 5-51 shows the not template.

Figure 5-51 not Template

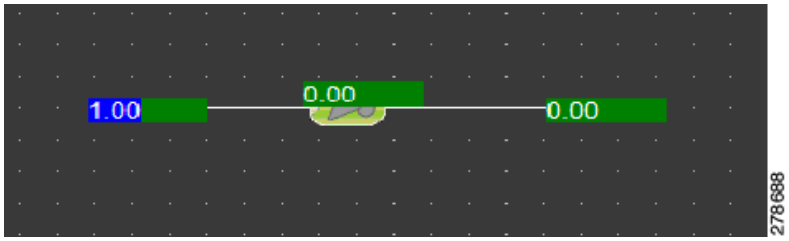
Function

This template produces the logical inverse of the input. If this template receives an input of value one, then it produces an output value of zero. If it receives an input of value zero, then it produces an output value of one.

Example

The following example shows the input value of one flows through the not template and produces an output value of zero (see Figure 5-52).

Figure 5-52 Example - not Template



or

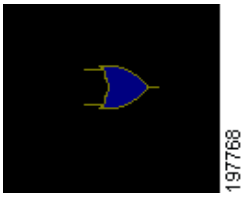
This section includes the following topics:

Symbol

Figure 5-53 shows the or template.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-53 or Template



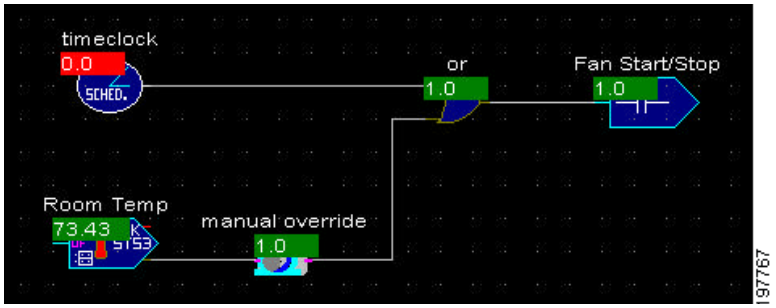
Function

The absolute template takes any negative or positive number as the input value and converts it to a positive value.

Example

The following example shows that the template makes a decision to switch the fan ON. This depends on whether the schedule is on or the override button has been pressed on the room temperature sensor (see Figure 5-54).

Figure 5-54 Example - or Template



override1hr

This section includes the following topics:

Symbol

Figure 5-55 shows the override1hr template.

Figure 5-55 override1hr Template

Send documentation comments to cbsbu-docfeedback@cisco.com

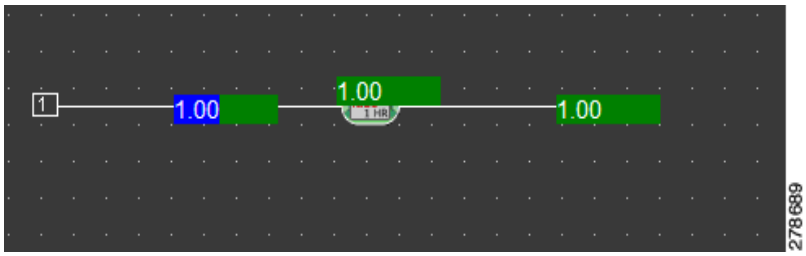
Function

When the input to the override1hr macro receives a value of one for two seconds, it produces an output of one for one hour. If the input receives a value of one for seven seconds, then it produces an output of zero.

Example

The following example shows how the input value of one is produced as an output value of one hour (see Figure 5-55).

Figure 5-56 Example - override1hr Template



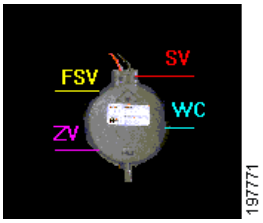
_p593-3h20

This section includes the following topics:

Symbol

Figure 5-57 shows the _p593-3h20 template.

Figure 5-57 _p593-3h20 Template



Function

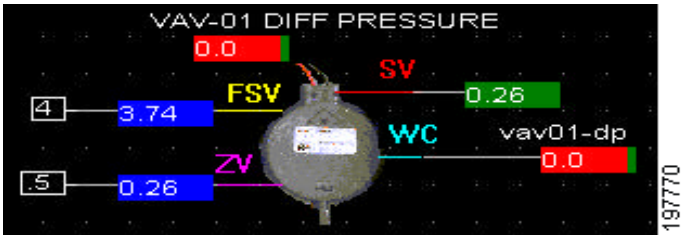
This template measures the differential pressure within the Mediator system.

Example

In the following example, the _p593-3h20 template sources a power of 5 VDC from an analog output to power the airflow sensor. The template then reads the voltage from the sensor with an analog input, and produces the output (see Figure 5-58).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-58 Example - _p593-3h20 Template



pid-cool

This section includes the following topics:

Symbol

Figure 5-59 shows the pid-cool template.

Figure 5-59 pid-cool Template

Function

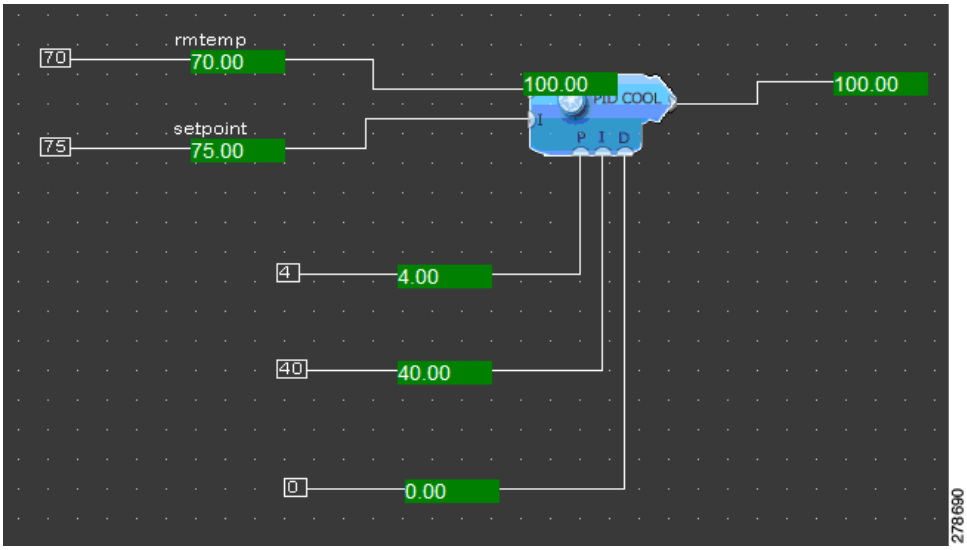
This template produces a numeric output from 0-100% based on the setpoint, input variable, and pid parameters. If a pid parameter is not used or set equal to zero, then it is not used in the computation.

Example

The following example shows the room sensor value and the room sensor setpoint attached to a pid-cool template produce an output value in percentage (see Figure 5-60).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-60 Example - pid-cool Template



pid-heat

This section includes the following topics:

Symbol

Figure 5-61 shows the pid-heat template.

Figure 5-61 pid-heat Template

Function

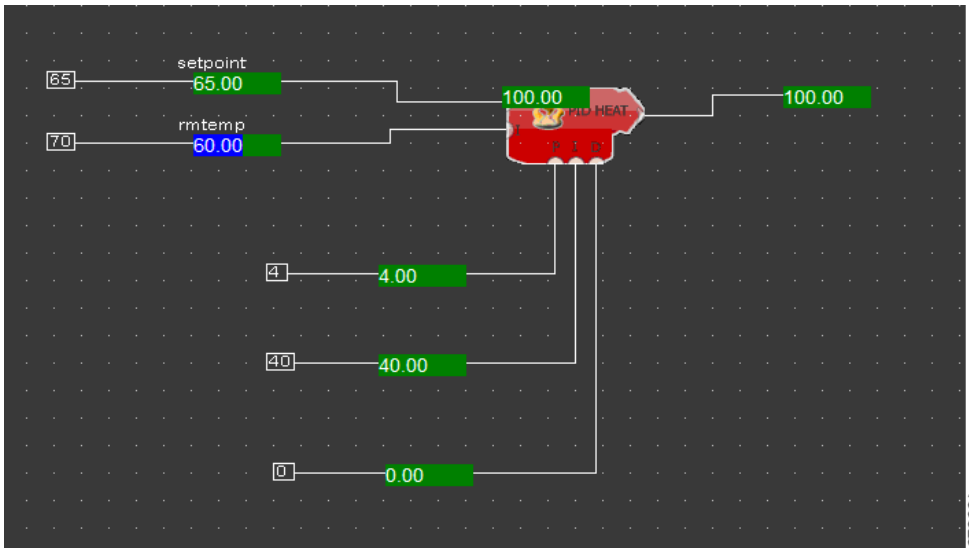
The percentage output value increases as the input value decreases below the setpoint. It produces a numerical output from 0-100% based on the setpoint, input variable, and pid parameters. If a pid parameter is not used or set equal to zero then it is not used in the computation.

Send documentation comments to cbsbu-docfeedback@cisco.com

Example

The following example shows the room sensor value and the room sensor setpoint attached to a pid-heat template produce an output value in percentage (see Figure 5-62).

Figure 5-62 Example - pid-heat Template



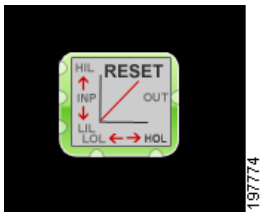
reset

This section includes the following topics:

Symbol

Figure 5-63 shows the reset template.

Figure 5-63 reset Template



Function

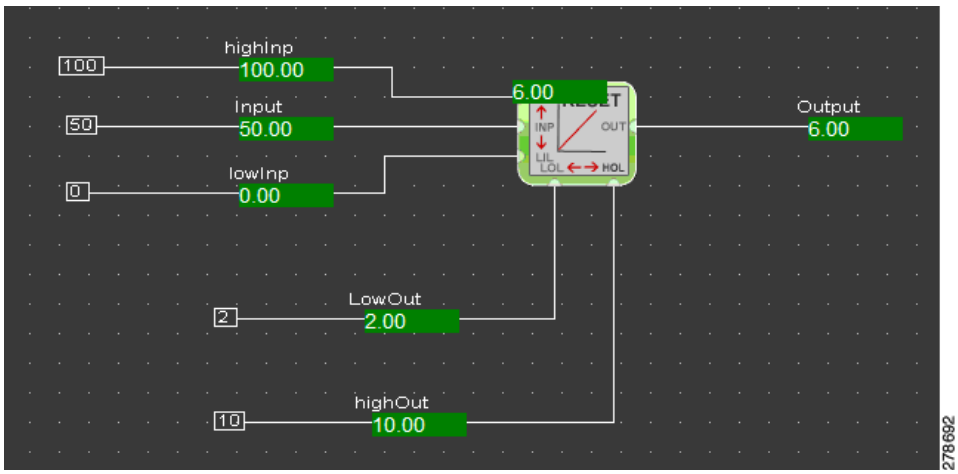
This template is used to rest existing input and output values.

Send documentation comments to cbsbu-docfeedback@cisco.com

Example

In the following example, the input value of 50 is between the zero and 100 input values. This means that the output value is six. If the input value is zero, then the output value is two (see Figure 5-64).

Figure 5-64 Example - reset Template



select

This section includes the following topics:

Symbol

Figure 5-65 shows the select template.

Figure 5-65 select Template

Function

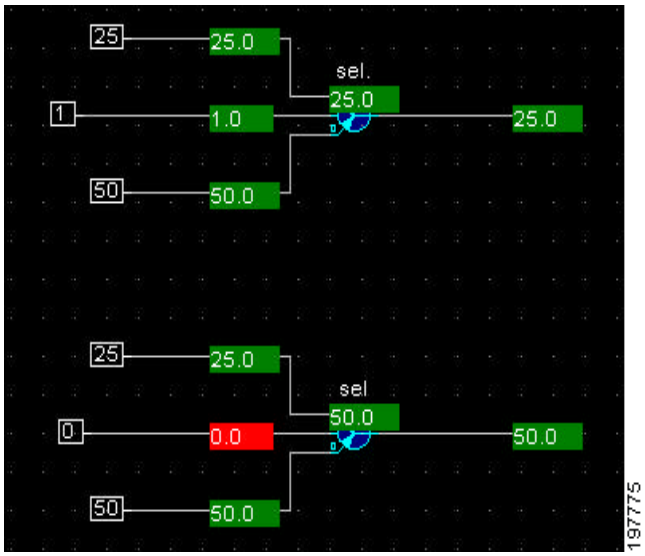
This template enables you to choose between two existing conditions.

Example

The following example shows how the input value chooses an appropriate condition (see Figure 5-66).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-66 Example - select Template



_setpnt10k

This section includes the following topics:

Symbol

Figure 5-67 shows the _setpnt10k template.

Figure 5-67 _setpnt10k Template

Function

This template converts the resistance in a 10-11 Kohm slidepot to a temperature between 55°F and 85°F.

Example

The following example shows how this template is applied to the application and assigned to a given universal analog point to control the setpoint of the temperature sensor, and to show the monitored value on the computer (see Figure 5-68).

Figure 5-68 Example - _setpnt10k Template

Send documentation comments to cbsbu-docfeedback@cisco.com

_st-s3

This section includes the following topics:

Symbol

Figure 5-69 shows the _st-s3 template.

Figure 5-69 _st-s3 Template

Function

This template controls a 10 Kohm type III thermistor temperature sensor.

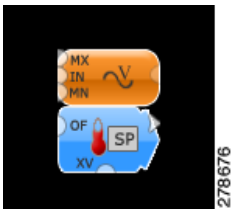
_setpntspl

This section includes the following topics:

Symbol

Figure 5-70 shows the _setpntspl template.

Figure 5-70 _setpntspl Template



Send documentation comments to cbsbu-docfeedback@cisco.com

Function

This template is a combination of an analog output template and a 10-11 Kohm slidepot analog input.

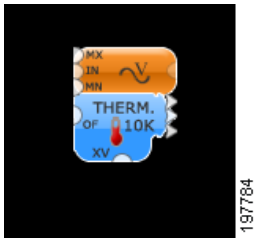
_st-s3ao

This section includes the following topics:

Symbol

Figure 5-71 shows the _st-s3ao template.

Figure 5-71 _st-s3ao Template



Function

This template uses one output to source all the temperature sensors on the same controller. This frees up the other outputs to drive other devices, such as damper actuators.

setresest

This section includes the following topics:

Symbol

Figure 5-72 shows the setreset template.

Figure 5-72 setreset Template

Send documentation comments to cbsbu-docfeedback@cisco.com

Function

This templates reset the input and output to a low value. The reset input values must be returned to low values to allow a set input of edge detect.

Example

The following example shows how the input and output values are reset to a low value (see Figure 5-73).

Figure 5-73 Example - setreset Template

sqrt

This section includes the following topics:

Symbol

Figure 5-74 shows the sqrt template.

Figure 5-74 sqrt Template

Function

This template takes the square root of the input values and produces an output value to a maximum of two decimal places.

Example

The following example shows that the sqrt template converts the input value of nine and produces an output value of three (see Figure 5-75).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-75 Example - sqrt Template

sub

This section includes the following topics:

Symbol

Figure 5-76 shows the sub template.

Figure 5-76 sub Template

Function

In this template, the upper input values are subtracted by the lower input values to produce output values. If the upper input value is greater than the lower input value, then the output value is a negative number.

Example

The following example shows that the upper input value is subtracted by the lower input value to display an output value on the right side of the template (see Figure 5-77).

Figure 5-77 Example - sub Template

timeclok

This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Symbol

Figure 5-78 shows the timeclok template.

Figure 5-78 timeclok Template

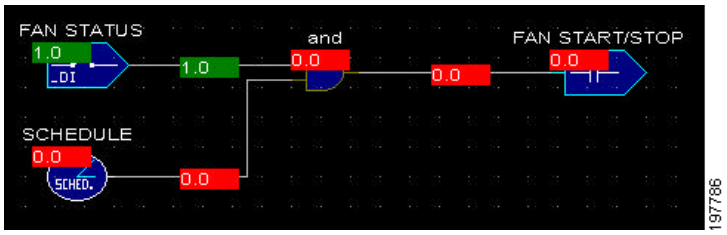
Function

This template enables you to perform all the scheduling for your programs.

Example

The following example shows how the template produces an output of one during the scheduled ON time and an output of zero during the scheduled OFF time (see Figure 5-79).

Figure 5-79 Example - timeclok Template



timepro2at

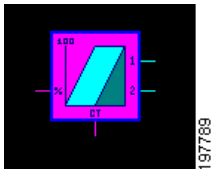
This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Symbol

Figure 5-80 shows the timepro2at template.

Figure 5-80 timepro2at Template



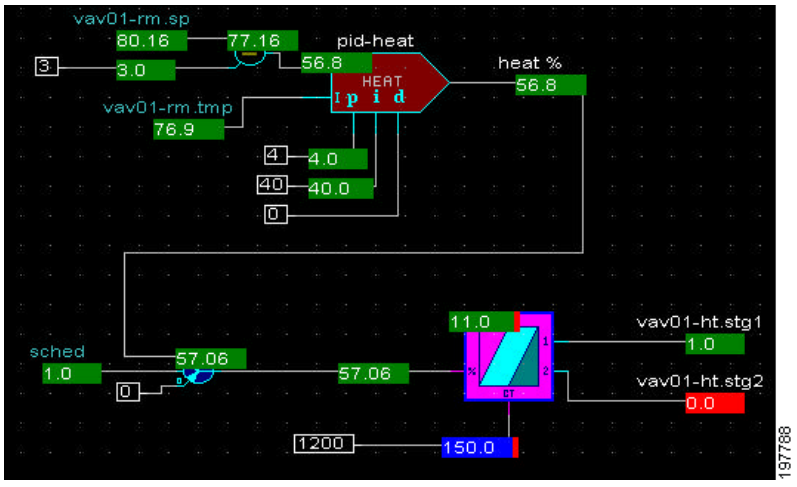
Function

A valve can be adjusted to 100 or more different positions. This provides smooth, precise control. A two-stage electric heater can be in one of only three positions (both stages off, one stage on, two stages on). Cycling the stages of the heater to provide smooth, precise control can be achieved with the timepro2.at template. This template might also be used for the two stages of a compressor.

Example

The following example shows the two separate stages of the timepro2at template being controlled by a pid-heat template. As the pid outputs a percentage according to the room temperature and setpoint values, it inputs a percentage into the timepro2at template, which in turn decides which stage should be controlled. In this example, the input value is 57.06%, which only turns on Stage 1 (see Figure 5-81).

Figure 5-81 Example - timepro2at Template



trigger

This section includes the following topics:

Symbol

Figure 5-82 shows the trigger template.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-82 trigger Template

Function

The trigger templates produce an output value of one and zero on an even time period. The basic trigger has a seconds input that customizes the time period of its output. This trigger is on for half the time, and then off for half the time.

trimmer

This section includes the following topics:

Symbol

Figure 5-83 shows the trimmer template.

Figure 5-83 trimmer Template

Function

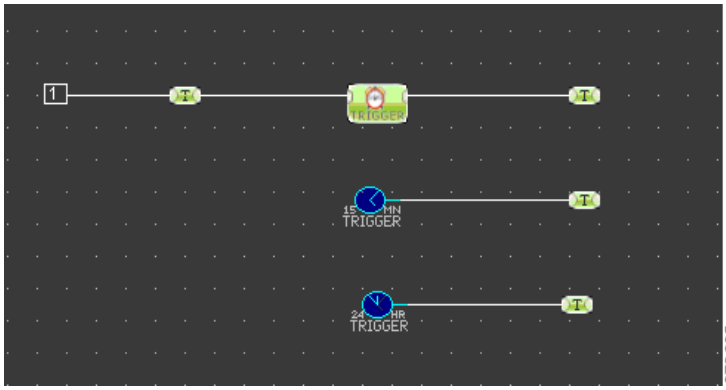
This template generates the input and output by itself. This enables you to override the points on your PC.

Example

In the following example, the input value of the trimmer is passed on to the trimmer output value, thus the number 1999 is attached to the input of the trimmer, an output of 1999 is produced at the output of the trimmer, and sent as an input to trimmer 2 (see Figure 5-84).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 5-84 Example - trimmer Template



Adding Templates

This section describes how to add templates in perfectHOST and includes the folowing topics:

MPX_GET Template

To add MPX_GET as a template in perfectHOST, perform the following steps:

Step 1 Perform the tasks described in Creating perfectHOST Applications, page 5-4 and Connecting to the Mediator with perfectHOST, page 5-4.

Step 2 Choose **Add > Node > MPX_GET**.

Note MPX_GET(s) and MPX_SET(s) enable you to view and override nodes in the Mediator Framework with perfectHOST.

The Open Broadway Xml File dialog box appears.

Step 3 Click **OK**.

By default, perfectHOST will search the application directory for the broadway.xml file.

Step 4 In the Add Mediator Node Reference dialog box, double-click the parent node to view the options.

Choose the child node from the list.

Step 5 Select the Direction by selecting the appropriate radio button. You can select the **Get FROM Mediator Node** or **Set To Mediator Node** radio button.

Step 6 Click to select the desired child node, and then click **OK**.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Add Mediator Node Reference dialog box closes, and a template representing the node appears in the window.

The template is attached to the cursor.

Step 7 Move the template to the desired position, and click to place the template on the canvas.

The Add Mediator Node Reference dialog box appears again.

Step 8 Click **Cancel**.

MPX_SET Template

To add MPX_SET as a template in perfectHOST, perform the following steps:

Step 1 Perform the tasks described in Creating perfectHOST Applications, page 5-4 and Connecting to the Mediator with perfectHOST, page 5-4.

Step 2 Choose **Add > Node > MPX_SET**.

Step 3 In the Add Mediator Node Reference dialog box, double-click the parent node to view the options.

To select the child node from the list, drag the scroll bar.

Step 4 Click **relay1,** and click **OK**.

The Add Mediator Node Reference dialog box closes, and a template representing the node appears in the window.

The template is attached to the cursor.

Step 5 Move the template to the desired position, and click to place the template on the canvas.

The Add Mediator Node Reference dialog box appears again.

Step 6 Click **Cancel**.

Trimmer Template

To add Trimmer as a template in perfectHOST, perform the following steps:

Step 1 Perform the tasks described in Creating perfectHOST Applications, page 5-4 and Connecting to the Mediator with perfectHOST, page 5-4.

Step 2 Choose **Add > Template**.

The select template dialog box displays eight template folders.

Step 3 Choose a folder to view the list of available templates. To do so, double-click the desired folder. For example, 1_io >.

The list of templates available in the folder appears.

Note You can enter the first few letters of the desired template in the selection template, to view the list of templates.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 Click the desired template, and then click **OK**.

Note A description of the template functionality appears in the drop-down list at the bottom of the dialog box.

The select template dialog box closes, with the template attached to the cursor.

Step 5 Move the template to the desired position, and click the template to place it on the canvas.

The Prompter dialog box appears.

Step 6 In the template name text box, enter the name of the template, and click **OK**.

The select template dialog box appears, prompting you to add another template.

Step 7 To add a trimmer as your template, enter **trimmer** in the selection text box, and then click **OK**.

Note As you enter the word trimmer, the letters appear in the selection text box. Use the **Backspace** key to delete a letter. The list of options disappears when you enter the name of the template.

Step 8 Move the trimmer to the desired position by clicking the trimmer to place it on the canvas.

The prompter dialog box appears.

Step 9 In the Template Name text box, enter a name, and click **OK**.

The select template dialog box appears, prompting you to add another template.

Step 10 Click **Cancel**.

Number Template

To add Number as a template in perfectHOST, perform the following steps:

Step 1 Perform the tasks described in Creating perfectHOST Applications, page 5-4 and Connecting to the Mediator with perfectHOST, page 5-4.

Step 2 Choose **Add > Number**.

The Prompter dialog box appears.

Step 3 In the enter constant text box, enter the desired value, and then click **OK**.

For example, when you enter 65, a number template containing the number 65 appears in the text box.

Step 4 Move the number template to the desired position, and click the number template to place it on the canvas.

The prompter dialog box appears.

Step 5 In the Template Name text box, enter a name, and click **OK**.

The select template dialog box appears, prompting you to add another template.

Step 6 Click **Cancel**.

Send documentation comments to cbsbu-docfeedback@cisco.com

Alarm Template

To add Alarm as a template in perfectHOST, perform the following steps:

Step 1 Perform the steps described in Creating perfectHOST Applications, page 5-4 and Connecting to the Mediator with perfectHOST, page 5-4.

Step 2 Choose **Add > Template**.

Step 3 Create an Alarm using the alarm.1 template.

Step 4 Move the alarm template to the desired position, and click the alarm template to place it on the canvas.

The prompter dialog box appears.

Step 5 In the Template Name text box, enter a name, and click **OK**.

The select template dialog box appears, prompting you to add another template.

Click **Cancel**.

Schedule Template

To add schedules as a perfectHOST template, perform the following steps:

Step 1 Perform the steps described in Creating perfectHOST Applications, page 5-4 and Connecting to the Mediator with perfectHOST, page 5-4

Step 2 Choose **Add > Template**.

Step 3 Create a schedule using the timeclok template.

Step 4 Move the timeclok template to the desired position, and click the timeclok template to place it on the canvas.

The prompter dialog box appears.

Step 5 In the Template Name text box, enter a name, and click **OK**.

The select template dialog box appears, prompting you to add another template.

Step 6 Click **Cancel**.

Connecting Templates

This section describes how to connect templates and numbers in the perfectHOST application.

Use the following guidelines to draw connection lines in the perfectHOST application:

- You must draw lines in vertical and horizontal line segments.
- You must draw connection lines right to left, from inputs to outputs.
- Connection points are located on the left and right sides of templates, commonly at peaks or at radius.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note If you click within five pixels of a connection point, the line automatically finds the connection point and attaches to it.

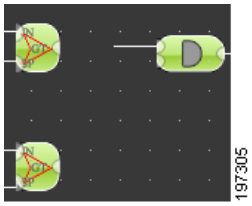
To connect templates in perfectHOST, perform the following steps:

Step 1 Choose **Add > Connect**.

You are now in Connect mode. You will see a checkmark by the Connect selection in the Add menu indicating this. You can now connect the created templates (see Adding Templates, page 5-64).

Step 2 Connect the templates by dragging the input nib of the first template to the output nib of the second template. (See Figure 5-85.)

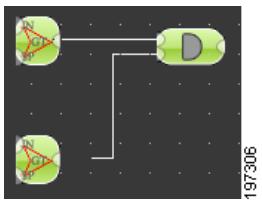
Figure 5-85 Dragging the Input Nib



Step 3 To change the line direction, drag the cursor in a new direction.

If the templates are successfully connected, this is indicated by a tone. (See Figure 5-86.)

Figure 5-86 Connected Templates



Saving and Compiling a perfectHOST Application

To save and compile a perfectHOST application, perform the following steps:

Step 1 Perform the tasks described in Creating perfectHOST Applications, page 5-4 and Connecting Templates, page 5-67.

Step 2 Choose **File > Save Application**.

The Prompter dialog box appears.

Step 3 In the save new drawing- enter name text box, enter the new drawing name, and click **OK**.

Step 4 Choose **System > Compile and Build Application**.

The Build Options dialog box appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 5 In the Mediator area, unselect all the check boxes to deactivate the options, and click **OK**.

If errors are found in the compile process, the COMPILE ERROR dialog box appears with error details.

Step 6 Click **OK**.

Step 7 To fix errors, click **Cancel** in the Build Options dialog box and repeat Step 4.

Creating HTML Monitor Drawings

HTML monitor drawings are graphical representations of the system configured on the Mediator. After you finish creating a monitor drawing, you can publish it to the Mediator in HTML format, so that you can access it using a web browser.

To create HTML monitor drawings in perfectHOST, perform the following steps:

Step 1 Perform the tasks described in the procedure in Creating perfectHOST Applications, page 5-4 through Saving and Compiling a perfectHOST Application, page 5-68.

Step 2 Choose **Drawing > Make Monitor Drawings**.

The Select Drawings dialog box appears.

Step 3 From the drawings list, choose the drawing you want to export, and click **OK**.

Step 4 Choose **Drawing > Export HTML Drawings for Mediator**.

The selected HTML drawings are exported to the Mediator.

Downloading the perfectHOST Application and HTML Drawing to the Mediator

To download the perfectHOST application and HTML drawing to the Mediator, perform the following steps:

Step 1 Perform the procedures described in Creating perfectHOST Applications, page 5-4 through Creating HTML Monitor Drawings, page 5-69.

Step 2 Choose **System > Communication and Administration**.

Step 3 To download the perfectHOST application, select the **Send Application to System** check box.

Step 4 Click **Perform Selected Commands**, and click **Done**.

The perfectHOST application downloads.

Step 5 To download the HTML drawing to the Mediator, select the **Send HTML to Mediator** check box.

Step 6 Click **Perform Selected Commands**, and click **Done**.

The choose images and pages to send to mediator dialog box appears.

Step 7 Click the desired images and .htm pages to send to the Mediator, and then click **OK**.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 8 When the Done button appears in the dialog box, click **Done**.

Viewing perfectHOST HTML Drawings on the Mediator

All perfectHOST HTML drawings sent to the Mediator are stored in a new directory with the same name as the application.

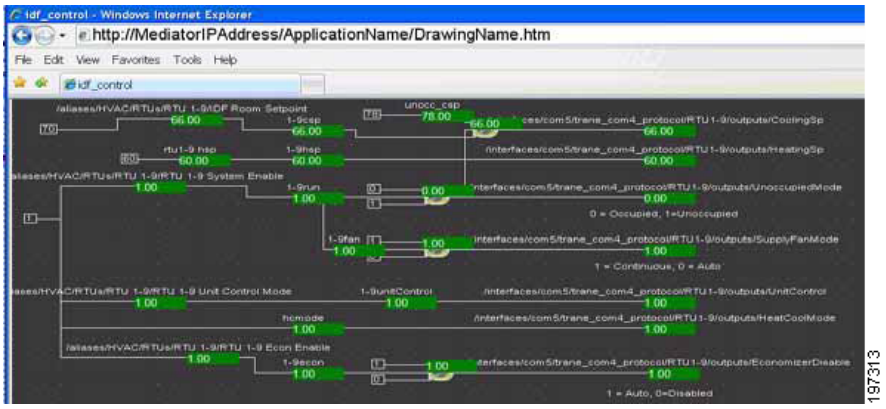
For example, /application name/drawing name.htm

To view the drawing, open a web browser and enter the following URL:

http://<MediatorIPAddress>/<ApplicationName>/<DrawingName>.htm

The drawing appears in the web browser as shown in Figure 5-87.

Figure 5-87 idf_control -Windows Internet Explorer



Uninstalling perfectHOST

To uninstall the Mediator perfectHOST application, perform the following steps:

Step 1 Close all running instances of perfectHOST.

Step 2 Choose **Start > All Programs > Cisco Systems > Uninstall perfectHOST** to run the uninstall script.

Step 3 When you are prompted with the following message, type **Y**.

You are presented with the following message:

Are you sure you want to Uninstall?

Press **Y** to uninstall, or **N** to exit.

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 6

Ports and Protocols

This chapter describes how to use the Cisco Network Building Mediator (Mediator) configTOOL to configure I/O port nodes and protocols on the Cisco Network Building Mediator and includes the following sections:

Note For more information on the configTOOL interface, see Chapter 4, "Mediator configTOOL."

Note A few protocols, which are documented in this chapter, have specific support and implementation requirements. These requirements are available in the *Ordering Guide* and *Protocol White List*. Please contact your *account representative* to obtain these documents.

About the I/O Ports

This section describes the I/O ports on the Mediator and includes the following topics:

Understanding I/O Ports

The Mediator provides the following I/O ports:

Send documentation comments to cbsbu-docfeedback@cisco.com

- Analog Inputs—Four analog inputs are available that have a minimum resolution of 24 bits and a maximum input voltage of 10 V. These inputs can be connected with a thermistor and used as a temperature sensor.
- Analog Outputs—Three analog outputs are available that have a 12-bit resolution digital-to-analog converter (DAC) and meet the 10-bit requirement. The outputs can be used to perform digital to analog conversions.
- Digital Inputs—Four digital inputs are available that serve as non-volatile counter inputs. The inputs are required to handle a maximum frequency of 1 KHz.
- Digital Outputs—Two optically isolated digital outputs are available.

You need to configure the I/O ports using the configTOOL.

The Analog Inputs (AI) and Analog Outputs (AO) ports that are found in 2500 and 5000. These ports are not in 2400 and 4800. For information on the wiring guidelines and different I/O ports , see the Wiring Guidelines section in the *Cisco Network Building Mediator 2500 and 5000 Hardware Installation Guide*.

Analog Inputs

Analog inputs can be configured. The analog input configuration determines the type of signal that is displayed. All values are measured relative to the ground terminals.

The defined range of values for the different signal types are as follows:

- Voltage Mode—From 0-10 V and is protected for a voltage of 32 V and above.
- Resistance Mode—From 0-100,000 ohms. It can display higher values, but accuracy is reduced.
- Current Mode—From 0-20 mA and is protected against higher values.

To configure analog inputs, perform the following steps:

Step 1 Launch the configTOOL main window.

For more information, see the following sections:

- Starting configTOOL, page 4-3
- Accessing Mediators Using configTOOL, page 4-11.

The configTOOL window appears. (See Figure 4-1).

Step 2 In the node tree pane, click the host node (represented by an IP address) of the Mediator to display the anchor nodes (aliases, interfaces, services).

Step 3 Click **interfaces** to display the available interfaces.

Step 4 Click the desired analog (AI1, AI2, AI3, or AI4) port to configure. For example, click **A1**.

The A1 tab displays the following information about the A1 analog port:

Note You cannot change the default name of the analog port.

Step 5 (Optional) In the Description text box, enter a description for the analog port to help you identify the purpose of the port.

Step 6 From the Signal Type drop-down list, choose the signal value to configure the analog port to that value.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note The available signal values are in volts, ohms, and ma. All the four analog inputs can be configured for these signal values. The default option is Volts.

Step 7 Click **Save Configuration** to save your configuration.

Analog Outputs

The analog outputs cannot be configured. It can display a voltage between 0 to 10 Volts. Floating point values in the range of 0.0 to 10 V are accepted, while the values that do not fall in the range are limited to 0-10 Volts.

Note The Analog Outputs can be set by a Periodic Driver or a TIM mpx_set template similarly to that of the digital output.

Digital Inputs

The digital inputs cannot be configured. They display a value of 1 for high input values and 0 for low input values in a contact closure that is wired between the input and ground terminals.

Digital Outputs

The digital outputs cannot be configured. They accept values, such as 1 or 0. Setting a value of 1 turns the digital output On (closes it contact), while setting a value of 0, turns the digital output Off.

Note The digital outputs can be set by the mpx_set template node reference within a TIM application.

Counter Points

The Mediator 2500 and Mediator 5000 have four counter inputs. These counter points are soft points that can be accessed under Nodes > Interfaces. The configTOOL represents these inputs as Nodes (counter1, counter2, counter3, and counter4). These inputs serve as both pulse counter inputs and digital inputs. In a typical pulse counter application, a pulse counter input is connected to a pulse meter that produces a series of dry contact closures that vary in frequency with the size of the electrical load. The number of times per second the circuit opens and closes is proportional to the amount of measured current in the meter.

Understanding Mediator Communications Ports

The Mediator has two RS-232 DB-9 serial communications ports and four RS-485 screw terminal ports.

Send documentation comments to cbsbu-docfeedback@cisco.com

You can configure the communications ports using the configTOOL. In the configTOOL, the RS-232 (com1 and com 2) and RS-485 (com3, com4, com5, and com6) communication ports of the Mediator are represented as nodes. An RS-232 com port node supports virtual nodes, devices, and multiple protocols. You can configure a com port node to add virtual nodes or devices connected to the Mediator.

About Protocols Over RS-232

This section describes how to configure the communication protocols over RS-232 (com1 and com2) communications ports on the Mediator and includes the following topics:

Before You Begin Configuring the Protocols

Before you begin configuring the desired protocols over the communication ports on the Mediator, perform the following steps:

Step 1 Launch the configTOOL main window.

For more information, see the following sections:

- Starting configTOOL, page 4-3
- Accessing Mediators Using configTOOL, page 4-11.

The configTOOL window appears.

In the node tree pane, click the host node (represented by an IP address) of the Mediator to display the anchor nodes (aliases, interfaces, services). The protocols can be configured either on any of the physical ports like com1, com2, com3, com4, eth0, and eth1, or under /services/network.

Step 2 Click the desired com1 or com2 node to configure. For example, click **com1**.

The com1 tab displays the following information about the com1 node:

- The default name and description of the node.

Note You cannot change the default name of the RS-232 com1 (or com2) node.

- The default communication parameters of the node.

Step 3 (Optional) In the Description text box, enter a description for the node that will help you identify the purpose of the node.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note In the node tree pane, when you position the cursor over the node, a tooltip appears. The tooltip displays the text provided in the Description text box.

Step 4 You can change the default values of the com1 node parameters. To do so, choose an appropriate value from the relevant drop-down list.

Step 5 You can add a device to a com1 node. The device will appear as a child node under the com1 node.

To add a device to a com1 node, in the node tree pane, right-click **com1**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears and displays the list of available communications protocols and devices supported by the Mediator.

Step 6 Click the protocol or device that you want to configure, and then click **OK**.

A new child node appears under the com1 (or com2) node in the node tree pane.

The tab displays the default name and description of the child node, and the configurable parameters for the child node. For each text box on the tab, enter or choose the appropriate parameter value to configure the child node.

Note All mandatory text boxes appear in red color.

For information on the default parameter values of the com nodes, see the "Configuring the Mediator" section on page 2-5

Configuring AirLink Redwing CDPD Modem Nodes

To configure AirLink Redwing CDPD modem nodes, perform the following steps:

Step 1 Perform Step 1 to Step 6 of the "Before You Begin Configuring the Protocols" section on page 6-4.

Step 2 In the Available Devices dialog box, click **AirLink Redwing CDPD modem (redwing_modem)**, and then click **OK**.

A new child node, redwing_modem, appears under the com1 node in the node tree pane. The configTOOL automatically adds the ppp0_ext child node to the redwing_modem node.

The com1 tab displays the following information about the com1 node:

The redwing_modem tab displays the following information about the redwing_modem child node:

- The default name and description of the modem node.
- The configurable parameters.

Step 3 (Optional) To change the default name of the child node, in the Name text box, enter the new name for the modem, and then press **Enter**.

The redwing_modem child node is renamed to the name that you provided, and appears in the node tree pane.

Step 4 (Optional) In the Description text box, enter a description to identify the purpose of the redwing-modem child node.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 5 (Optional) The redwing_modem node is enabled by default. If not, check the **Enabled** check box to enable the node.

Note You cannot change the default value of the Initialization String text box.

Step 6 In the node tree pane, click **ppp0_ext**.

The pp0_ext tab the default name, description and the configurable parameters of the pp0_ext node.

Step 7 (Optional) To change the default description of the ppp0_ext node, in the Description text box, enter a description to identify the purpose of the ppp0_ext node.

Step 8 In the node tree pane, expand the ppp0_ext node, and then click **outgoing**.

The outgoing tab displays the default name, description and the configurable parameters of the outgoing node.

Note You cannot change the default name of the outgoing node.

Step 9 (Optional) To change the description of the outgoing node, in the Description text box, enter a description to identify the purpose of this node.

Note In the node tree pane, when you position the cursor over the outgoing node, a tooltip appears. The tooltip displays the description text provided in the Description text box.

Step 10 Check the **Enabled** check box to enable the outgoing node.

Note The outgoing node is disabled by default.

Step 11 To connect to the modem, check the **Connect on-demand only** check box.

Note By default, connect on-demand is enabled.

By default, the modem is not connected until the Mediator framework needs to send a message, such as a log message. For the connection to be active at all times, uncheck the **Connect on-demand** check box.

Step 12 In the Phone number text box, enter the telephone number of your local Internet Service Provider (ISP).

Note Include any prefixes, such as 9, to dial out. Some telephone systems require the comma to add a delay before getting a dial tone.

Step 13 In the User ID text box, enter the user ID you use to log in to your ISP.

Step 14 In the Password text box, enter the password you use to log in to your ISP.

Step 15 In the Primary name server text box, enter the IP address of the primary server of your ISP.

Step 16 In the Secondary name server text box, enter the IP address of the secondary server of your ISP.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 17 You can define routes to remote hosts. To do so, in the Routes area, click **+** to add a route to a remote host. A row is added to the Routes area. Do the following:

a. In the Host/Net IP Address tab, enter the IP address of the remote host.

b. In the Netmask tab, enter the appropriate subnet mask value of the remote host. For example, 255.255.255.0.

Step 18 Repeat Step 17 to define additional routes for the modem.

Configuring Alpha Plus Meter Nodes

To configure Alpha Plus Meter nodes, perform the following steps:

Step 1 Perform Step 1 to Step 7 of the "Before You Begin Configuring the Protocols" section on page 6-4.

Step 2 In the Available Devices dialog box, click **Alpha Plus meter (meter)**, and then click **OK**.

A new child node, meter, appears under the com1 node in the node tree pane. The configTOOL automatically adds the inherent child nodes of the Alpha Plus meter node.

The meter tab displays the default name, description, and the configurable parameters of the meter node.

Step 3 (Optional) To change the default name and description of the meter node, do the following:

a. In the Name text box, enter the new name, and then press **Enter**.

The meter node is renamed to the name that you provided, and appears in the node tree pane.

b. In the Description text box, enter a description to identify the purpose of this node.

Note In the node tree pane, when you position the cursor over the meter node, a tooltip appears. The tooltip displays the description text provided in the Description text box.

Step 4 In the Device Number text box, enter a number from 0 to 255 as the address of the Alpha Plus Meter device.

Step 5 In the Password text box, enter **alphaplus**, the default password of the Alpha Plus Meter device.

Configuring Capstone Micro-Turbine Protocol Nodes

To configure Capstone Micro-Turbine Protocol nodes, perform the following steps:

Step 1 Perform Step 1 to Step 6 of the "Before You Begin Configuring the Protocols" section on page 6-4.

Step 2 In the Available Devices dialog box, click **Capstone Micro-turbine protocol (capstone protocol)**, and then click **OK**.

A new child node, capstone protocol, appears under the com1 node in the node tree pane.

The capstone protocol_1 tab displays the default name, description, and the configurable parameters of the capstone protocol node.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 3 (Optional) To change the default name of the capstone protocol node, in the Name text box, enter the new name, and then press **Enter**.

The capstone protocol node is renamed to the name that you provided, and appears in the node tree pane.

Step 4 (Optional) To change the description of the capstone protocol node, in the Description text box, enter a description to identify the purpose of this node.

Note In the node tree pane, when you position the cursor over the capstone protocol node, a tooltip appears. The tooltip displays the description text provided in the Description text box.

Step 5 In the Timeout text box, enter the time (in seconds) for the capstone protocol node to wait for a response to the request made to one of its data points. The default time out value is one second.

Step 6 In the node tree pane, right-click **capstone protocol**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears listing the available Capstone Micro-Turbine devices.

Step 7 Click **Capstone Micro-Turbine (capstone protocol)**, and then click **OK**.

A new child node, capstone_micro_turbine, appears under the capstone protocol node in the node tree pane. The configTOOL automatically adds the inherent ppp0_ext child node to the capstone_micro_turbine node.

The capstone_micro_turbine tab for the capstone_micro_turbine node displays the default name, description, and the configurable parameters.

Step 8 (Optional) To change the default name of the capstone_micro_turbine node, in the Name text box, enter the new name, and then press **Enter**.

The capstone_micro_turbine node is renamed to the name that you provided, and appears in the node tree pane.

Step 9 (Optional) To change the description of the capstone_micro_turbine node, in the Description text box, enter a description to identify the purpose of this node.

Note In the node tree pane, when you position the cursor over the capstone_micro_turbine node, a tooltip appears. The tooltip displays the description text provided in the Description text box.

Step 10 From the Turbine Address drop-down list, choose a value from 0 to 15 for the micro-controller that supervises the micro-turbine.

Step 11 (Optional) In the Password text box, enter the password of the micro-controller.

Configuring EDF Labview Device Nodes

To configure EDF Labview device nodes, perform the following steps:

Step 1 Perform Step 1 to Step 6 of the "Before You Begin Configuring the Protocols" section on page 6-4.

Step 2 In the Available Devices dialog box, click **EDF Labview device (labview)**, and then click **OK**.

A new child node, labview, appears under the com1 node in the node tree pane.

The labview_1 for the labview node displays the default name and description of the node.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note The labview node does not have any configurable parameters.

Step 3 (Optional) To change the default name of the labview node, in the Name text box, enter the new name, and then press **Enter**.

The labview node is renamed to the name that you provided, and appears in the node tree pane.

Step 4 (Optional) To change the description of the labview node, in the Description text box, enter a description to identify the purpose of this node.

Note In the node tree pane, when you position the cursor over the labview node, a tooltip appears. The tooltip displays the description text provided in the Description text box.

Configuring PPP Connection Nodes

You can configure a Point-to-Point Protocol (PPP) connection node when you connect a modem to one of the com ports of the Mediator. PPP is the standard for encapsulating and transmitting Internet Protocol (IP) datagrams over a point-to-point connection. PPP provides full-duplex, bi-directional connections that deliver data packets in order.

To configure PPP connection nodes, perform the following steps:

Step 1 Perform Step 1 to Step 6 of the "Before You Begin Configuring the Protocols" section on page 6-4.

Step 2 In the Available Devices dialog box, click **Internet access via a direct PPP connection (ppp)**, and then click **OK**.

A new child node, ppp, appears under the com1 node in the node tree pane. The configTOOL automatically adds the incoming child node to the ppp node.

The ppp_1 tab for the ppp node displays the default name, description, and the configurable parameters.

Step 3 (Optional) To change the default name of the ppp node, in the Name text box, enter the new name, and then press **Enter**.

The ppp node is renamed to the name that you provided, and appears in the node tree pane.

Step 4 (Optional) To change the description of the ppp node, in the Description text box, enter a description to identify the purpose of this node.

Note In the node tree pane, when you position the cursor over the ppp node, a tooltip appears. The tooltip displays the description text provided in the Description text box.

Step 5 To enable the ppp node, check the **Enabled** check box.

Step 6 In the node tree pane, click **incoming**.

Note If you do not see the incoming node in the node tree pane, then click **ppp** to expand the node.

Send documentation comments to cbsbu-docfeedback@cisco.com

The incoming tab for the incoming node displays the default name, description, and the configurable parameters of the node.

Note You cannot change the default name and user ID used in a PPP connection.

Step 7 (Optional) To change the description of the incoming node, in the Description text box, enter a description to identify the purpose of this node.

Note In the node tree pane, when you position the cursor over the incoming node, a tooltip appears. The tooltip displays the description text provided in the Description text box.

Step 8 To enable the incoming PPP node, check the **Enabled** check box.

Step 9 In the Password text box, enter the password required by the remote dial-up application, such as HyperTerminal.

Step 10 In the Local IP address text box, enter the IP address of the Mediator that establishes the PPP connection.

Note Do not enter an IP address that is in the IP address range assigned to the local network. For example, if the IP address of the Mediator is 192.168.2.12, and machines in the local network use the IP address range 192.168.2.*, then do not enter the IP address 192.168.2.12 for the Mediator in the Local IP address text box. Instead, use an alternate IP address (for example, 192.168.0.12) as the local IP address of the Mediator for the PPP connection to work correctly on the 192.168.2.* local network.

Step 11 In the Client IP address text box, enter the IP address of the Windows client machine (or any other client machine) that is used to dial in to a PPP connection.

Note Do not enter an IP address that is in the IP address range assigned to the local network. For example, if the IP address of the Windows client machine is 192.168.2.14, and machines in the local network use the IP address range 192.168.2.*, then do not enter the IP address 192.168.2.14 for the Windows client machine in the Client IP address text box. Instead, use an alternate IP address (for example, 192.168.0.14) as the client IP address of the Windows client machine for the PPP connection to work correctly on the 192.168.2.* local network.

Configuring RS-232 to RS-485 Converter Nodes

The Mediator allows you to convert one or both of its RS-232 ports to an RS-485 port.

To configure RS-232 to RS-485 converter nodes, perform the following steps:

Step 1 Perform Step 1 to Step 7 of the "Before You Begin Configuring the Protocols" section on page 6-4.

Step 2 In the Available Devices dialog box, click **RS-232 to RS-485 converter (rs485)**, and then click **OK**.

A new child node, rs485_1 tab, appears under the com_1 node in the node tree pane.

The rs485_1 tab for the rs485_1 node displays the default name and description of the node.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note The rs485 node does not have any configurable parameters.

Step 3 (Optional) To change the default name of the rs485_1 tab node, in the Name text box, enter the new name, and then press **Enter**.

The rs485_1 tab node is renamed to the name that you provided, and appears in the node tree pane.

Step 4 (Optional) To change the description of the rs485_1 tab node, in the Description text box, enter a description to identify the purpose of this node.

Note In the node tree pane, when you position the cursor over the rs485_1 tab node, a tooltip appears. The tooltip displays the description text provided in the Description text box.

Step 5 In the node tree pane, right-click **rs485_1** tab, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears listing the supported devices.

Note The RS-485 devices are also supported by the dedicated RS-485 ports of the Mediator.

Step 6 Configure the RS-485 node.

For information on configuring RS-485 protocol nodes, see the "About Communication Protocols Over RS-485 and IP" section on page 6-11

About Communication Protocols Over RS-485 and IP

This section explains how to configure the communication protocols over RS-485 communication ports and over IP port, and also describes how to configure specific devices that are connected to the Mediator, and includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

- Configuring the ETC-USAP Protocol, page 6-63
- Configuring the Omnimeter Protocol
- Configuring the Delphi Web Service Protocol

Overview

This section explains the overview of the supported protocols on the Mediator and includes the following topics:

BACnet

Building Automation and Control Networks (BACnet) is an open-communication protocol. BACnet protocol was developed by the American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE).

Initially, the BACnet protocol supported only HVAC systems. It now supports the objects for lighting, life safety, elevators, and other building systems. BACnet relies to a great extent on the use of common local area network (LAN) technologies, such as Ethernet and Attached Resource Computer Network (ARCNET). To achieve interoperability across a wide spectrum of equipment, the BACnet specification consists of three major parts. The first part describes a method for representing any type of building automation equipment in a standardized manner. The second part defines messages that can be sent across a computer network to monitor and control such equipment. The third part defines a set of acceptable LANs that can be used to convey BACnet communications.

Send documentation comments to cbsbu-docfeedback@cisco.com

BACnet Multi-port

BACnet Multi-port allows the Cisco Network Building Mediator to communicate with remote devices through one or more communications channel at a time without having to go through a BACnet router. A communications channel consists of a Master Slave Token Passing (MSTP) network connected to an RS-485 com port, a BACnet IP or BACnet Ethernet network.

BACnet Broadcast Management Device

If your Mediator or any other BACnet device has multiple routers that reside on different IP subnets, you must set up one router on each IP subnet as a BACnet/IP Broadcast Management Device (BBMD). Every subnet with a router must have a BBMD configured for broadcasts from controllers on that subnet to reach the other routers on the network.

BACnet COV

The BACnet Change-of-Value (COV) reporting is part of the BACnet Alarm and Event services. The COV reporting allows a COV-client to subscribe with a COV-server to get notifications of changes in the value of a specified property of a specified object. The BACnet COV implementation saves system load and network bandwidth by eliminating the need to periodically poll property values where possible. The COV reporting also eliminates the need to modify the polling interval to the expected rate of change in the values of properties.

Dallas

The Mediator includes physical Dallas wire ports. These ports are the physical interfaces on the Mediator and act as interfaces to the devices. Depending on the Mediator model, the number of ports vary.

The available wire ports are as follows:

- Mediator 2400 - Four Dallas wire ports
- Mediator 2500 - Two Dallas wire ports
- Mediator 4800 - Four Dallas wire ports
- Mediator 5000 - Two Dallas wire ports

The configTOOL represents these ports as nodes that communicate through Dallas ports.

These nodes are named as follows:

- Dallas1, Dallas2, Dallas3, and Dallas4 in Mediator 2400 and 4800
- Dallas1 and Dallas2 in Mediator 2500 and 5000

Note You cannot change the names of the Dallas1, Dallas2, Dallas3, and Dallas4 nodes.

The Mediator currently supports two dallas devices: 18B20 and 18S20 temperature sensors.

Send documentation comments to cbsbu-docfeedback@cisco.com

Modbus

The Modbus protocol was developed and published in the late 1970s by Modicon, Inc. It was designed as a communication protocol for Modicon programmable logic controllers. Modbus has now become one of the major communications standards, which has been widely adopted by vendors and users of industrial controls and building automation equipment and systems.

Modbus is a master/slave protocol with half-duplex transmission. The master device can initiate transactions (called queries). The other devices, called slaves, respond by supplying the requested data to the master, or by taking the action requested in the query. A slave can be any device that processes information and sends its output to the master using Modbus (for example, a Veris meter). A standard Modbus network can have one master and up to 247 slave devices. Some Modbus derivatives, such as JBus, support up to 255 slave devices.

The master initiates all Modbus transactions. The master initiates only one transaction at a time. In general, slave devices do not transmit data without a request from the master, nor do they communicate with other slaves. The master can address individual slaves, or it can initiate a broadcast message to all slaves. Slaves return a response to all queries addressed to them individually; however, they do not respond to broadcast queries.

Modbus does not specify physical network architecture. The Mediator supports RS-232 and RS-485 serial physical networks, including the multi-drop capability of Modbus over RS-485. The Mediator also supports Modbus TCP, an open standard for sending Modbus messages over Ethernet using TCP/IP packeting. The Modbus protocol specifies an address range from 1 to 247 (some versions support up to 255) for the RS 232 or RS 485 networks. The Mediator supports an unlimited address range. For example, while configuring Modbus TCP/IP network, the IP address of the device must be entered.

For RS-232 and RS-485 serial line bus networks, the Mediator supports Modbus RTU, which specifies the format for sending data in the binary format using the character-gap timing. Modbus RTU is suitable for one-on-one RS-232 or multi-drop RS-485 connections. The Mediator does not support Modbus ASCII. The Mediator also supports Modbus TCP, an open standard for sending Modbus messages over Ethernet using TCP/IP packeting.

The Modbus protocol describes a set of addressable registers that can store binary, numeric, or text data. These include two types of 16-bit data registers (Holding Registers and Input Registers,) and two types of 1-bit registers (Coils and Input Status Registers). The larger data elements must be configured as multiple register groups.

Because the user can assign registers to data points of a device, Modbus can be used as the communication protocol for many different types of devices. The Mediator implementation of Modbus supports generic (user-defined) device configuration, which allows the user to configure any type of device compliant with the Modbus protocol. In addition, it supports several pre-defined devices produced by specific Original Equipment Manufacturers (OEMs).

The Mediator allows the user to communicate with devices that are compliant with the Modbus protocol, and thereby incorporates Modbus devices into installations that include components that are not Modbus-compliant. Communication is two-way: the Mediator brings data in from Modbus devices, and also allows the user to send commands out to those devices. In addition, the Mediator makes information acquired from Modbus devices available to other devices on the network that are not Modbus-compliant. Therefore, information acquired from non-Modbus devices becomes available to Modbus devices through the Mediator.

Send documentation comments to cbsbu-docfeedback@cisco.com

SNMP

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can be queried (and sometimes set) by managing applications. SNMP is essentially a request-reply protocol running over User Defined Protocol (UDP) ports 161 and 162, though Transmission Control Protocol (TCP) operation is possible. SNMP itself does not define what information (variables) a managed system should offer. However, SNMP uses an extensible design, where the available information is defined by Management Information Bases (MIBs). A MIB is a database of the objects that can be managed on a device. The managed objects, or variables, can be set or read to provide information on the network devices and interfaces. MIBs use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

SNMP standards are defined in a series of documents called request for comments or RFCs, proposed by the Internet Engineering Task Force (IETF). There are three versions of SNMP available - SNMPv1, SNMPv2c, and SNMPv3, of which the Mediator currently supports SNMPv1 and SNMPv2c.

C-Bus

C-Bus (or Clipsal Bus) is a closed protocol. The C-Bus protocol was developed using the International Organization for Standardization (ISO) Layer 7 reference model. The C-Bus protocol supports a number of interfaces, such as RS-232 and TCP/IP.

The C-Bus system is available in both wired and wireless versions. A default gateway is available to allow messages to be sent between wired and wireless networks. The maximum number of C-Bus networks in a single installation cannot exceed 255. This limitation does not apply if a C-Bus Ethernet interface is used. The C-Bus system size is then limited only to the IP address of the Ethernet interface.

A disadvantage of the wired C-Bus protocol is that it does not work with standard mains wire installation. A completely new wiring system must be installed for a wired C-Bus system, which means it is normally used for new constructions. The C-Bus wireless (RF) system can, however, be provided using the existing mains wiring.

The C-Bus system can be used along with several standard protocols, such as TCP/IP, Crestron, AMX, LonWorks, ModBus, and Charmed Quark Controller protocols. The C-Bus system can be used to control lighting, electrical systems, and products through remote control. For example, C-Bus can be used to enable the interface on a home security system, AV products, or other electrical equipments.

Johnson N2

The N2 Communications Bus is a local network that links controllers and point interfaces to a Master device. The N2 Bus uses a master/slave protocol, in which the master device initiates all communication with the N2 Bus devices.

N2 is based on the Opto-22 protocol, which was designed for industrial applications, and is a proven communication network. The N2 Bus follows the electrical characteristics of Electronics Industry Alliance (EIA) Standard RS-485.

The N2 protocol uses an Auto discovery mode that creates N2 nodes only as they are requested, either from a Nodebrowser URL or as a request from a web express widget. To force a search for all N2 devices on a network, a call to the function **force_discovery** on the n2 node queries all 255 addresses for the presence of a device.

Send documentation comments to cbsbu-docfeedback@cisco.com

Barber-Colman

The Mediator can connect through one of its RS-485 ports to the Application Specific Device (ASD) bus of several Network 8000 Barber-Colman MicroZone II devices, MICROFLOW II devices, or Packaged Equipment Module (PEM) devices. If an MN3 (integrator) controller is present on the network, the Mediator will detect any device on its J-bus.

ALC WebCTRL SOAP Interface

The Mediator communicates with the ALC WebCTRL server through a Web Services interface that uses SOAP/XML technology.

Lennox SysBus

Lennox SysBus is a proprietary communications protocol used to manage Heating, Ventilating and Air Conditioning (HVAC), zoning, and building operations. The Mediator communicates directly with the Lennox IMC Controller using the native Lennox SysBus protocol.

Trane Com3

Trane Com3 is a proprietary communication protocol that typically links controllers and Trane BCUs. The Mediator supports communication directly with supported Trane Com3 devices.

Trane Com4

Trane Com4 is a proprietary communication protocol that typically links controllers and Trane BCUs. The Mediator supports communication directly with supported Trane Com4 devices.

TCS Basys

TCS Basys is a proprietary master/slave communication protocol. The TCS Basys communication network consists of a master device and multiple slave devices, such as SZ and SL controllers. A standard TCS Basys network has one master device and up to 255 slave devices. All the slave devices on the network have a unique address from 0-255.

The master device initiates communication to a specific slave device. It sends only one message at a time on the network. The slave devices are always in the received mode, and respond by supplying the requested data to the master, or by taking the action requested in the message.

Secure Remote Node Abstraction (SRNA) Protocol

The Remote Node Abstraction (RNA) is a Cisco proprietary protocol that enables application-specific communication between the Mediators as well as between a Mediator and a Mediator Manager over a TCP socket. The System Integrator (SI) uses the Secure Remote Node Abstraction protocol (SRNA) to secure the RNA communication through an un-encrypted authentication (Auth-only) mode or with Full Encrypted authentication (Full-Enc) mode.

Note The option of using no security for the RNA communications remains available.

Send documentation comments to cbsbu-docfeedback@cisco.com

There are three levels of security that can be configured on the Mediator and the Mediator Manager.

- NoSec—No authentication involved between the Mediators.
- Auth-only—Authentication happens through the packets that are transferred in plain text.
- Full-Enc—Authentication happens through the packets that are encrypted.

Securing the RNA communication requires execution of the SRNA installation scripts (one time installation activity) on the Cisco Network Building Mediator Manager (Manager). These scripts generate a private/public key-pairs for each of the Mediator and Mediator Manager, based on its IP address. Each Mediator and Mediator Manager uses its key-pairs as authentication credentials for establishing persistent SRNA connections with other Mediators and/or Mediator Managers. Currently, there is a restriction that the keys can be generated only for one single IP address (per physical interface) for a given Mediator.

Note This restriction does not affect un-secured RNA communications.

If the network uses NAT protocol, typically each Mediator interface to the gateway router will have at least two IP addresses: An internal IP (configured on the physical interface) and an external IP (Network Address Translated or NAT-ed IP configured at the gateway router).

ETC-USAP

The ETC (Electronic Theatre Controls) Unison Serial Access Protocol (USAP) controls the Unison lighting control system. The standard is applied for the point-to-point command exchange between Mediator devices and the Unison system.

Omnimeter

Omnimeter protocol is an RS-485 based communication protocol used to communicate with electricity meters, gas meters, water meters and heating meters.This protocol makes use of master-slave protocol in which the Mediator acts as a master and polls the Omnimeters connected to the interface to read data. The Omnimeter protocol is deployed in two ways:

1. RS-1- Deployed in offices and is used to read electricity meters.
2. RS-5- Deployed in homes and is used to read gas meter, water meters and heating meter readings.

Both RS-1 and RS-5 will have simple Request and Response packets. The protocol is a Request-Response model in which the Mediator sends a Request and Omnimeter responds with the data. The NBM sends a 'Read Data' Request to Omnimeter and the Omnimeter replies with a Response. The 'Request and Response' packet differs depending on whether the device is of RS-1 or RS-5 type. Omnimeter protocol is configured under any of the RS-485 interfaces in the Mediator. The address and type of the Omnimeter devices connected under each RS-485 bus needs to be preconfigured.

Delphi Web Service

The Delphi web server provides you with the Banquet Event Order (BEO) service and the Meeting Space Request service. The Delphi web servers are typically installed in a Hotel or in Conference Centers. The Delphi web service that runs on the Cisco Network Building Mediator supports only the Meeting Space Request service.

The Meeting Space Request service can be used for the following external systems:

Send documentation comments to cbsbu-docfeedback@cisco.com

- Energy and Climate Control Systems
- Digital Signage
- Labor Management

The Delphi Event Management System (EMS) interface enables a property, which can be used to read the detailed meeting, function, and booking information entered into the Delphi database. The interface application produces a file of event information that can be used to provide up-to-date information on digital sign boards (running on the Interface PC) or other systems.

Before You Begin Configuring the Protocols

To begin configuring the desired protocols that are supported on the Mediator, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator.

For more information, see the following sections:

- Starting configTOOL, page 4-3.
- Accessing Mediators Using configTOOL, page 4-11.

Step 2 Click **Interfaces** to view the list of services options.

Step 3 Right-click the **services > control** node to view the node tree right-click menu, and then choose **Add**.

The Available Devices dialog box appears and displays the list of supported available devices for a specific protocol that you want to configure.

Configuring the BACnet Protocol

This section explains how to configure the BACnet protocol on the Mediator to enable it to interact with various BACnet devices and includes the following topics:

- Prerequisites, page 6-18
- Configuring BACnet Over IP, page 6-19
- Configuring BACnet Over MSTP, page 6-20
- Configuring BACnet Over Ethernet, page 6-20
- Discovering BACnet Devices, page 6-21

Prerequisites

The prerequisites for the BACnet Protocol configuration are as follows:

- Device instance number of BACnet devices
- Network number of BACnet network
- BACnet communication medium for the network should be MSTP or IP or Ethernet.

Send documentation comments to cbsbu-docfeedback@cisco.com

Configuring BACnet Over IP

To configure the BACnet protocol over IP on the Mediator, perform the following steps:

Step 1 Perform Step 1 to Step 3 in the "Before You Begin Configuring the Protocols" section on page 6-18.

Step 2 In the node tree pane, expand the node tree, click **services**, and then click **network**.

Step 3 In the node tree pane, right-click **network**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears listing the protocols supported by the Mediator.

Step 4 Click **Bacnet protocol service (BACnet)**, and then click **OK**.

A new child node, BACnet, appears under the network node in the node tree pane. The BACnet tab for the BACnet node displays the default name and description.

Step 5 Choose **services > network > BACnet > internetwork**.

The internetwork node is an inherent child node under the BACnet node. The internetwork tab displays the default name and description along with the Write Priority text box.You can change the default value in the Write Priority text box. The default value is 11. You can choose any value between 0 to 16.

Note Write Priority value is the priority at which the Mediator writes to the properties of BACnet Devices using the WriteProperty service request. For example, if the value is 11, then the Mediator writes values to different properties of BACnet Devices at a priority of 11.

Step 6 To change the write priority value, enter the new value in the write priority check box.

Step 7 To configure BACnet over IP, choose **services > network > BACnet > internetwork Configuration > IP**.

Step 8 In the IP tab, check the **Enabled** check box to enable BACnet over IP.

Step 9 In the network text box, enter network number that is between 1 to 65,634. The default value is 1.

Step 10 To change the default value of the UDP port number, enter the new port number in the Port text box. The default value is 47808.

Step 11 In the node tree pane, right-click IP, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 12 Click **Ethernet or Com port assignment (eth_or_com_port_name)**, and then click **OK**.

A child node, eth_or_com_port_name, appears under the IP node in the node tree pane. The data entry pane for the eth_or_com_port_name node displays the default name and description.

Step 13 Click **eth_or_com_port_name node**.

A new tab, eth_or_com_port_name tab, appears with the default name, description, and the configurable parameter.

Step 14 In the Name text box, enter **eth0** to configure BACnet over IP on eth0 or enter **eth1** to configure BACnet/IP on eth1.

Step 15 To enable BACnet IP over the interface eth0 or eth1, check the **Enabled** check box.

Step 16 Save the configuration.

Send documentation comments to cbsbu-docfeedback@cisco.com

Configuring BACnet Over MSTP

To configure the BACnet protocol over MSTP, perform the following steps:

Step 1 Perform Step 1 to Step 5 in the "Configuring BACnet Over IP" section on page 6-19.

Step 2 In the node tree pane, expand the node tree, click **interfaces**, and then click **com4**.

The com4 tab for the com4 node displays the default name, description, and the configurable parameters of the node.

Note This example assumes you are configuring BACnet/MSTP on com4. Com 3-6 can be used for BACnet/MSTP, and Eth0 or Eth1 can be used for BACnet/IP or BACnet/Ethernet.

Step 3 (Optional) You can change the default values of the com4 node parameters located in the lower area of the data entry window. To do so, choose an appropriate value from the relevant drop-down list or enter a value in the text boxes provided.

Step 4 In the node tree pane, expand the internetwork node, click **Configuration**, and then click **MSTP**.

Step 5 In the lower area of the MSTP tab, check the **Enabled** check box to configure the network number and address.

Step 6 In the Network text box, enter the network number.

Step 7 In the Address text box, enter the IP address.

Note Every network must have a unique number, and every device instance on the combined network must be unique.

Step 8 In the node tree pane, right-click **MSTP**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 9 Click **Ethernet or Com port assignment (eth_or_com_port_name)**, and then click **OK**.

A child node, eth_or_com_port_name, appears under the MSTP node in the node tree pane. The data entry pane for the eth_or_com_port_name node displays the default name and description. i

Step 10 Click the **eth_or_com_port_name** node, and change the entry in the Name text box. You can choose to enter com4, com3, com5, or com6.

The name change is required based on whether you want to configure BACnet over MSTP to be enabled on the desired com port.

Step 11 Save the configuration.

Configuring BACnet Over Ethernet

To configure the BACnet protocol over Ethernet, perform the following steps:

Step 1 Perform Step 1 to Step 5 in the "Configuring BACnet Over IP" section on page 6-19.

Step 2 In the node tree pane, expand the internetwork node, click **Configuration**, and then click **Ethernet**.

Step 3 In the lower area of the Ethernet tab, check the **Enabled** check box, and configure the network number.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 In the Network text box, enter the network number.

Step 5 In the node tree pane, right-click **Ethernet**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 6 Click **Ethernet or Com port assignment (eth_or_com_port_name)**, and then click **OK**.

A child node, eth_or_com_port_name, appears under the Ethernet node in the node tree pane. The data entry pane for the eth_or_com_port_name node displays the default name and description.

Step 7 Click the **eth_or_com_port_name** node, and change the entry in the Name text box to eth0 or eth1, based on whether you want to enable BACnet/Ethernet on eth0 or eth1.

Step 8 Save the configuration.

Discovering BACnet Devices

To discover BACnet devices in the network and to get a complete list of discovered BACnet objects, perform the following steps:

Step 1 Launch an Internet browser (for example, Internet Explorer) and browse to the Mediator web client homepage. To do so, enter the IP address of the Mediator in the Address bar of the browser and log in when prompted.

The Mediator web client homepage appears in the Internet browser window.

Step 2 Click **NodeBrowser**.

The Mediator web client NodeBrowser homepage appears.

Step 3 Choose **services > network > BACnet > Internetwork > Devices**.

Step 4 In the Commands area, do the following:

a. To change the discovery mode to broad, click **directed**.

b. Click **send Who-Is**.

Wait until the previous page is loaded and refreshed.

Step 5 Click any of the discovered devices.

The discovered devices have their own device instance number. For example, 61.

Step 6 In the Commands area, click **CSV file of Objects Info**.

You will be prompted to save the output, which is in an excel format. The file extension is .csv. You can either choose to save or open it from the browser. The output excel sheet contains a complete list of discovered BACnet objects in the device.

Note If you do not see any objects under the discovered devices, click any of the devices object type. For example, **nodes > services > network > BACnet > internetwork > Devices > 2112236 > 6**, and then in the Commands area, click **Discovered object instances**.

Step 7 Save the result and use it to create aliases for all the required nodes by using the Mediator configTOOL.

The following is an example of the nodepath for a BACnet point:

/services/network/BACnet/internetwork/Devices/95001/0/1

Send documentation comments to cbsbu-docfeedback@cisco.com

95001 = Device Instance Number

0 = Object Type

1 = Object Instance

Configuring the BACnet Multiport and Proxy

This section describes how to configure BACnet Multiport and includes the following topics:

BACnet Multi-port Usage Configuration Guidelines and Restrictions

When configuring BACnet Multi-port, follow these configuration guidelines and restrictions:

- The Cisco Network Building Mediator does not act as a router between the various communication channels.
- All devices that are connected in the entire network should be assigned a unique ID.
- Each communication channel must have a unique network number.
- You must configure only one BACnet Server Device node with the unique network number for each channel.
- BACnet Server Device nodes with network numbers that do not match any physical channel are called Virtual Devices.
- All BACnet server device nodes are accessible through any communication channel.
- The BACnet client devices from all channels are accessible to the Mediator.
- The BACnet client devices on a channel are not accessible by the remote devices on a different channel. This is because the Mediator does not act as a router.

Configuring BACnet Multi-port

The Mediator supports BACnet/IP, BACnet/MSTP, and BACnet/Ethernet as communication media, and supports the Multi-Port capability that enables the Mediator to communicate with remote devices through one or more communication channels at the same time without having to go through a BACnet Router.

To configure BACnet Multi-port, based on the combination of BACnet over IP, BACnet over MSTP, or BACnet Over Ethernet, perform the tasks that are described in the "Configuring BACnet Over IP" section on page 6-19, or the "Configuring BACnet Over MSTP" section on page 6-20, or the "Configuring BACnet Over Ethernet" section on page 6-20, and save the configuration.

Send documentation comments to cbsbu-docfeedback@cisco.com

Adding BACnet Server and Proxy Objects

To add a BACnet server device and proxy objects, perform the following steps:

Step 1 In the node tree pane, expand the node tree, right-click **Devices**, and then click **Add**.

The Available Devices dialog box appears.

Step 2 Click **BACnet Server Device (device_instance_number_goes_here)** and then click **OK**.

A new child node and a device number appear under the device node in the node tree pane. The number tab for the device node displays the default name and description.

Step 3 In the Name text box, enter the BACnet Device ID of the BACNet server device. For example, enter 95001.

Note The Device ID of the BACnet server device must be unique in the network and should not be same as the other devices in the network.

Step 4 In the Network Number text box, enter the network number.

The network number must be the same value as:

- The proxied BACnet device (or)
- The network number of the Mediator network in which the Mediator acts as a server device.

Step 5 Right-click the new device node to view the node tree right-click menu, and then choose **Add**.

The Available Devices dialog box appears listing the available objects.

Step 6 Choose **Bacnet Analog Value Objects Type Group (2)**, and then click **OK**.

A new BACnet analog value object 2 under the new device node appears.

Step 7 Right-click the new object node to view the node tree right-click menu, and then choose **Add**.

The Available Devices dialog box appears.

Step 8 Click **Bacnet Analog Value Object Instance,** and then click **OK**.

Step 9 In the node tree pane, a new BACnet Analog Instance Number appears.

The data entry pane for the Bacnet Analog value Instance node displays the default Name, Description, and the Proxy Link.

Step 10 In the Name text box, enter the unique instance ID.

Step 11 In the Description text box, enter the description of the device property.

Step 12 Choose a proxy link from the Proxy Link drop-down list.

A Node Selector dialog box appears.

Step 13 Choose the desired node to link to the object, and then click **Select**.

Note You can select any node, interface, or protocols configured in the Mediator.

Step 14 Repeat Step 7 to Step 13 to add different objects.

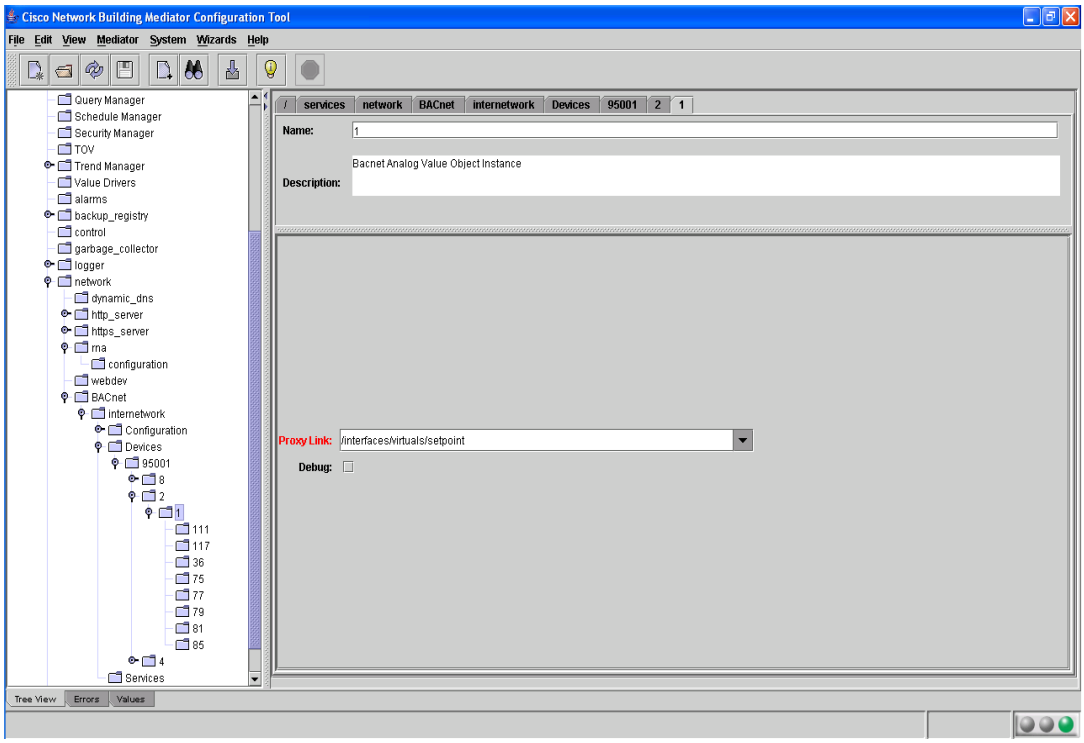
Send documentation comments to cbsbu-docfeedback@cisco.com

BACnet Proxy Server Usage Guidelines and Restrictions

- The BACnet analog value and binary value objects can be either Commandable or Writeable, depending on the presence of the following Optional Properties:
  - Relinquish Default (104)
  - Priority Array (87)

  For example, see Figure 6-1 for the analog value without Optional Properties.

Figure 6-1 configTOOL - Analog Value Object instance

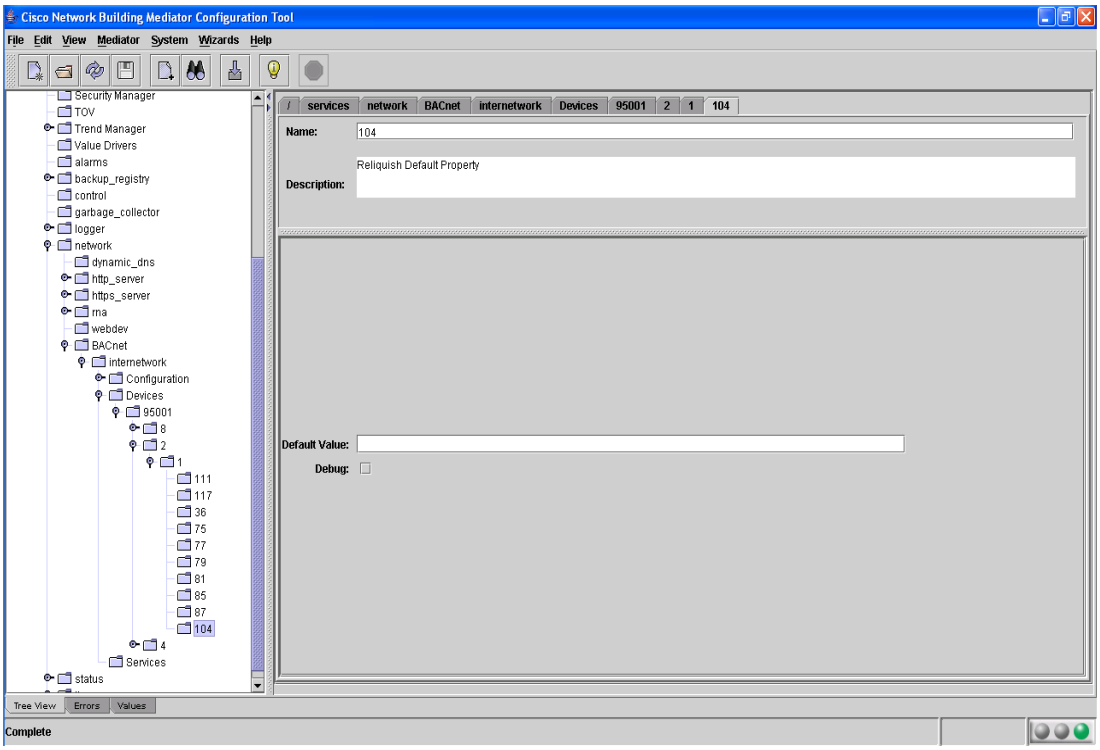


- If you provide the objects as Commandable, the Optional Properties need to be added as children of the Value Object.

  For example, see Figure 6-2 for adding Properties 87 and 104.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 6-2 configTOOL - Properties 87 and 104



Configuring BACnet Broadcast Management Device

This section describes how to configure BACnet Broadcast Management Device (BBMD) and static devices.

The BACnet Broadcast Management Device (BBMD) configuration enables communications under multiple subnets. The BBMD directly forwards a BACnet broadcast message initiated by a BACnet/IP device on its subnet to the other subnets with BACnet/IP devices. The message that arrives at a destination subnet broadcasts on that subnet. The BBMDs allow BACnet to operate through IP routers. Their primary purpose is to redistribute the essential broadcast messages that BACnet requires.

Caution Multiple BBMDs on an IP subnet disrupt BACnet communications. Therefore, define only one BBMD per subnet.

Caution Unless explicitly modified, the UDP Port for BACnet/IP is 47808. Do not change this parameter unless you have made a change in the router.

To configure the BACnet Broadcast Management Device, perform the following steps:

Step 1 Perform the steps described in the "Adding BACnet Server and Proxy Objects" section on page 6-23 to configure BBMD on a BACnet supported device.

Step 2 Perform the steps for all the other BBMD-supported BACnet devices that are on a different subnet.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note The BBMD address table should be identically configured for all BBMD-supported BACnet devices.

Note If you have configured the BACnet over an IP device that needs to communicate with the other BACnet text box devices in a different subnet, you need to configure BBMD.

Step 3 In the node tree pane, expand the node tree, click **IP,** and then **eth0**.

Step 4 Right-click **eth0** and choose **Add** from the right-click menu.

The Available Device dialog box appears.

Step 5 Click **Table of BBMD device IP addresses,** and then click **OK**.

A new child node BBMD appears under the eth0.

Step 6 In the Description text box, enter the description of the configured BBMD device.

In the lower area of the BBMD tab, in the BBMD Device Table area, click **+** to add the IP address, UDP port, and Broadcast mask of all the BBMD supported BACnet devices.

The default broadcast mask is 255.255.255.255.

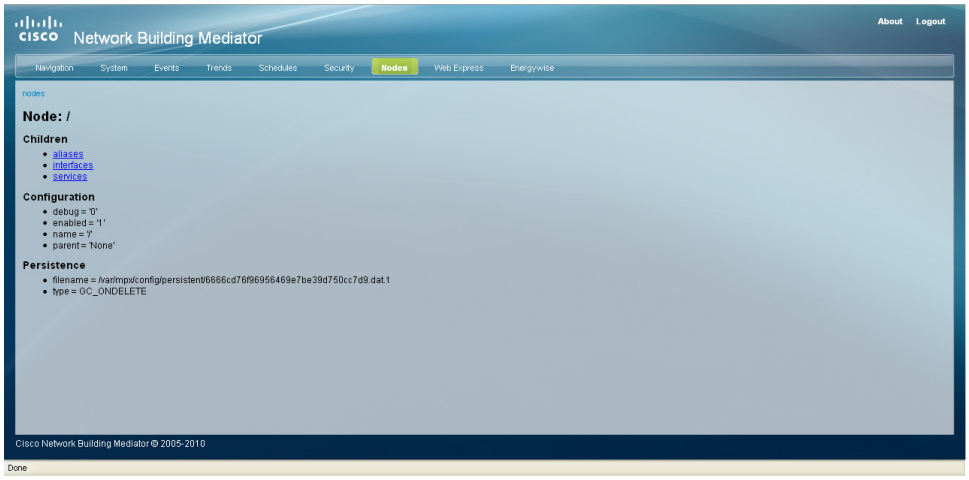
Step 7 Save the configuration.

Note All BBMD-supported BACnet devices should have an identical BBMD device table.

Step 8 To view the configured BACnet BBMD devices, launch an Internet browser (for example, Internet Explorer), and browse to the Mediator web client homepage. To do so, enter the IP address of the Mediator in the Address bar of the browser and log in when prompted.

The Mediator web client homepage appears in the Internet browser page.

Figure 6-3 configTOOL - Nodes



Step 9 Click **Nodes**.

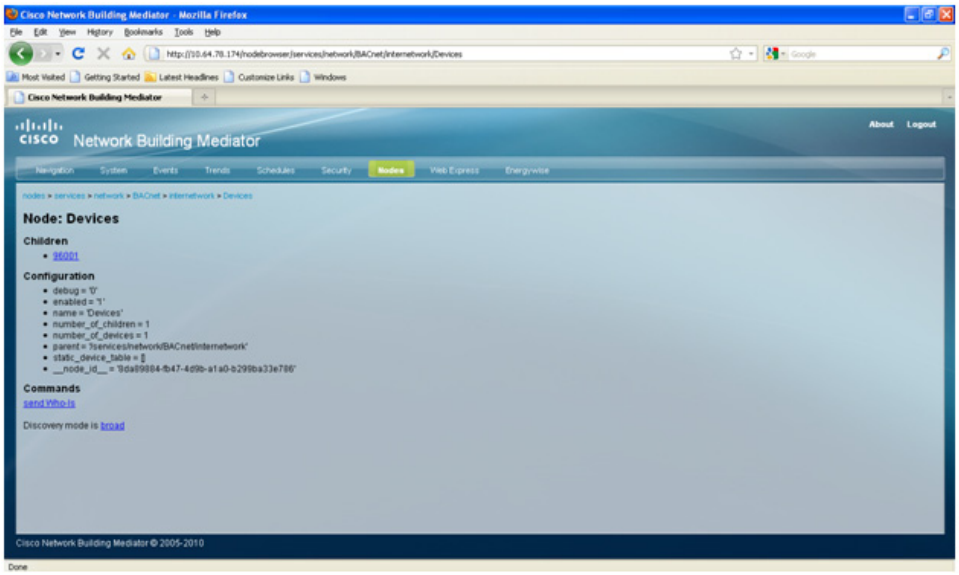
The Mediator web client NodeBrowser homepage appears. (See Figure 6-3.)

Step 10 Choose **services > network > BACnet > Internetwork > Devices**.

Send documentation comments to cbsbu-docfeedback@cisco.com

All the BBMD devices that are configured in the BBMD table are discovered. (See Figure 6-4.)

Figure 6-4 configTOOL - Discovered Devices



Configuring Static Devices

To configure static devices that are on a different IP subnet, where you cannot use a BBMD on multiple interfaces, perform the following steps:

Step 1 In the node tree pane, choose **BACnet > internetwork > Devices**.

Step 2 In the Device tab, enter the name and description of the static device.

Step 3 In the Remote Static Devices text box, click the **+** button to add the Device ID, IP Address, MAC address, Network Number, and the MAC Network.

Note If there is a router in between two networks, the IP address is the IP address of the Mediator, and the MAC address should be the IP address of the router.

BACnet COV

This section describes BACnet Change-of-Value (COV) functionality and includes the following topics:

- BACnet COV Deployment Model, page 6-28
- Enabling BACnet COV, page 6-28
- Usage Guidelines and Restrictions, page 6-28

Send documentation comments to cbsbu-docfeedback@cisco.com

BACnet COV Deployment Model

The Cisco Network Building Mediator supports client-side functionality of the COV service. The Mediator subscribes to COV notifications from field devices that are capable of generating COV notifications. The Mediator can function as a server for BACnet COV notifications when it acts as a proxy server for the BACnet objects.

The COV client-side functionality is not enabled by default on the Mediator. To enable COV client-side functionality on the Mediator, see the "Enabling BACnet COV" section on page 6-28. In deployments where the field devices do not support the COV server functionality, the behavior of the Mediator is set to the default behavior, which is active polling for the property values.

Note BACnet server device configuration is mandatory for enabling the BACnet COV functionality. To configure the BACnet server device, perform Step 1 and Step 2 of the "Adding BACnet Server and Proxy Objects" section on page 6-23.

Enabling BACnet COV

You need to enable the client-side functionality of the BACnet COV service on the Mediator.

To enable the BACnet COV functionality, perform the following steps:

Step 1 Depending on whether you are configuring BACnet over IP, BACnet over MSTP, or BACnet over Ethernet, follow the instructions outlined in the following sections:

- Configuring BACnet Over IP, page 6-19
- Configuring BACnet Over MSTP, page 6-20
- Configuring BACnet Over Ethernet, page 6-20

Step 2 In the node tree pane, choose **services > network > BACnet > internetwork**.

Step 3 On the **internetwork** tab, check the **Enable Change of Value (COV)** check box.

Step 4 Save the configuration.

Usage Guidelines and Restrictions

- The Mediator subscribes to SubscribeCOV service.
- SubscribeCOVProperty service is *not* supported in 3.1.1.
- Mediator subscribes to confirmed COV notifications. Subscription to unconfirmed COV notifications is *not* supported in the Mediator. The Mediator ignores the unconfirmed COV notifications.
- The Mediator supports the COV service for the following BACnet objects:
  - Binary Input
  - Binary Output
  - Binary Value
  - Analog Input
  - Analog Output

Send documentation comments to cbsbu-docfeedback@cisco.com

  - Analog Value
  - Multi-state Input
  - Multi-state Output
  - Multi-state Value
- The Mediator supports the COV service for the following BACnet properties:
  - Present Value
  - Status Flags
- When the field device that acts as the COV server has the COV service capability for the other objects or properties (standard or proprietary), the Mediator does not utilize the same.
- The COV service at the Mediator client addresses the following situations:
  - The COV subscription attempts can fail due to temporary resource constraints on the COV server and transient network conditions (in this case, the Mediator attempts to a re-subscription after 30 minutes).
  - The COV server device may reboot and lose the data on active subscriptions (to deal with this situation, a re-subscription is performed periodically every 45 minutes).
- The default life time of the subscription is set to one hour.

Configuring BACnet Schedules and BACnet Time Synchronization

To configure BACnet schedule and BACnet Time Synchronization, perform the following steps:

Step 1 Perform Step 1 to Step 5 in the "Configuring BACnet Over IP" section on page 6-19.

Step 2 In the node tree pane, expand the node tree, choose **services** > **time** > **local**.

Step 3 In the node tree pane, right-click **local**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 4 Click **BACnet Client Device Schedules holder (bacnet_device_time_schedules)**, and then click **OK**.

A new child node, BACnet Client Device Schedules holder, appears under the local node in the node tree pane.

The BACnet_device_time_schedules tab for the BACnet node displays the default name and description of the BACnet schedule. For example, MySite_SignageSchd for OutdoorLgtsSched

Step 5 In BACnet Device text box, enter the BACnet device path to the BACnet device where the schedules are added. For example, /services/network/BACnet/internetwork/Devices/<device instance>

Step 6 In the Auto Discover text box, choose **never** from the drop-down list.

The other options available in the drop-down list are: numberic, name, and name_and_numberic.

Step 7 In the node tree pane, you can add individual schedules to the schedules holder.

Step 8 To add an individual schedule, right-click the **Schedules** node.

Step 9 From the right-click menu, choose the schedule that you want to configure, and click **Add Schedule**.

Step 10 In the BACnet device schedule object text box, enter /services/network/BACnet/internetwork/Devices/<device instance>17/1

Send documentation comments to cbsbu-docfeedback@cisco.com

17= BACnet schedules type object

1= Schedule Object instance

Step 11 From the Default BACnet Data Type drop-down-list, choose the desired data type.

The options available for the schedule properties are: auto, integer, real, boolean, and enumerated. By default, the data type is auto.

Step 12 If the data type is not auto, check the **Force Default Data Type** checkbox.

Note For the *KMC BACnet device*, the data type should be set to enumerated and also select the Force Default Data Type check box.

Step 13 Repeat Step 1 to Step 7 for all the schedules that you want to add.

Step 14 If the BACnet server device on the Mediator is not defined, perform Step 1 to Step 15 as described in the "Adding BACnet Server and Proxy Objects" section on page 6-23.

Note It is recommended that you enable Time Synchronization to synchronize with the clocks on the Mediator and the BACnet Devices.

When a new BACnet server device with a unique device ID is added to the Mediator, an inherent child node is created under the server device node. The default inherent child node is 8.

Step 15 Right-click the inherent child node **8**, and then click **Add**.

The Available Devices dialog box appears.

Step 16 Click **Bacnet Device Object Instance**, and then click **OK**.

A new BACnet device object instance number appears in the node tree pane. The data entry pane for the new BACnet device instance node displays the default Name, Description, and the Proxy Link.

Step 17 In the Name text box, enter the value of the device instance ID of the new BACnet server device, which is added in Step 14.

The instance number of the device object must be the same as that of the BACnet server device. For example, if the BACnet server device has been assigned a Device ID as 95001, then the value in the Name text box for the newly added BACnet device object instance is 95001. The added BACnet device Object Instance node has all the mandatory properties of the Device object as that of the inherent child nodes.

Step 18 Right-click the Device Object Instance node, and then click **Add**. For example, 95001.

The Available Devices dialog box appears.

Step 19 Click **Generic BACnet Property**.

A new property node appears under the Device Object Instance node.

Step 20 In the Name Text Box, enter **116**.

116 is the property ID of BACnet Device Property-Time Synchronization recipients.

Step 21 To perform the Time Synchronization, click the default property **116**.

116 = Time synchronization recipient.

The 116 tab displays the default name and description.

Step 22 (Optional) You can change the name and description of the default property. To do so, in the Description text box, enter a description that will help you identify the property.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 23 In the default value text box, enter the device instances of the devices that should receive the Time Synchronization message.

The message is received in a comma separated format within square brackets. For example, [1,2,3,4,5,6].

Step 24 Save the configuration.

Note When Time Synchronization is enabled, the Mediator sends Time Synchronization service messages every hour to synchronize the clock between the Mediator and the BACnet Devices.

Step 25 Check the **include all** check box to ensure that all the devices in the network receive the Time Synchronization.

Step 26 Save configuration to the Mediator and restart.

Step 27 Open the NodeBrowser.

Step 28 Click the Schedules tab to view the added schedules utility in the Mediator.

The BACnet device schedules appear in the left hand pane.

Step 29 Select a schedule and then move the slide bars in the right pane to edit the schedule objects.

Configuring the Dallas Sensor Protocol

This section describes how to connect and configure a Dallas Sensor point, and includes the following topics:

Connecting a Dallas Sensor Point

The Dallas temperature sensor includes the following three legs:

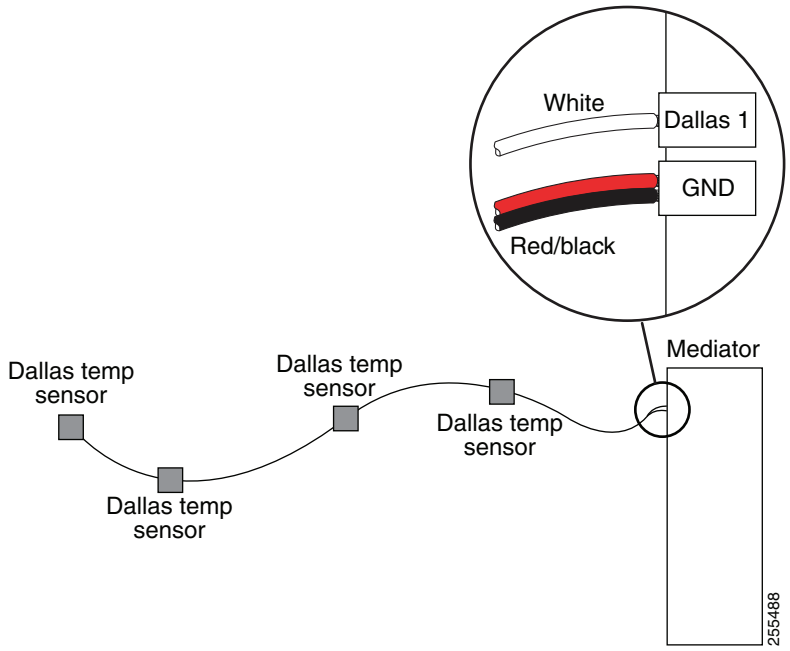
- Signal leg—wired to the Dallas1 input on the Mediator. Generally, a white wire is connected to this leg.
- Power leg—wired together with the ground leg into the ground (GND) input.
- Ground leg—wired together with the power leg into the ground input.

The GND input is located below the Dallas1 input. The red and black wires are connected to the power and ground legs on the Dallas Sensor.

Figure 6-5 describes the Dallas Sensor Point connection.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 6-5 Dallas Sensor Point Connection



Configuring the Dallas Sensor Point

To configure the dallas sensor point on the Mediator, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator.

For more information, see the following sections:

- Starting configTOOL, page 4-3
- Accessing Mediators Using configTOOL, page 4-11.

Step 2 In the node tree pane, expand the node tree, click **interfaces**, and then click **dallas1**.

The dallas tab displays the default name and description of the dallas node.

Step 3 (Optional) You can change the description of the node. To do so, in the Description text box, enter a description that will help you identify the purpose of the node.

Step 4 In the node tree pane, right-click **Dallas1**, and choose **28B20** from the drop-down list.

Note The Dallas sensor point includes two models: 18B20 and 18S20. Based on the model you choose, the node will appear as 18B20 or 18S20.

The 18B20 tab displays the default name, description, and the configurable parameters of the 18B20 node. You can change the description of the node.

Step 5 In the Address text box, enter the address of the Dallas sensor point. The address is printed on the dallas wire. For example, 289ccae0010000af.

Step 6 From the Model drop-down list, choose the appropriate model number.

Step 7 Save the configuration.

Step 8 In the node tree, expand the 18B20 node, and then click **C**.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 9 Right-click **C**, and choose **Get Value** from the drop-down list.

This displays the values in Celsius. Alternatively, you can click either F or K to see the temperature in Fahrenheit or Kelvin.

Step 10 Launch an Internet browser (example, Internet Explorer) and browse to the Mediator web client homepage. To do so, enter the IP address of the Mediator in the Address bar of the browser.

The Mediator web client homepage appears in the Internet browser window.

Step 11 Click **NodeBrowser**.

The Mediator web client NodeBrowser homepage appears.

Step 12 Choose **interfaces > dallas1 > 18B20**.

The dallas values appear in Celsius, Fahrenheit, and Kelvin.

Configuring Modbus Protocol

This section explains how to configure Modbus devices that are connected to the Mediator and includes the following topics:

Prerequisites

The prerequisites for configuring a Modbus device to the Mediator are as follows:

- Type of Modbus Protocol
- Physical network architecture of Modbus device
- Physical addresses of the Modbus RTU Device
- Register Map of the Modbus Device
- Communication Settings of the Modbus Device

Configuring a Modbus RTU over an RS-232 Bus Network Node

This section describes how to configure a Modbus RS-232 bus network for devices that are connected to the **com1** or **com2** ports of the Mediator.

To configure a Modbus RTU over an RS-232 Bus network node, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator.

Step 2 Open an existing Mediator configuration file or create a new one.

Step 3 Click **interfaces** to view the list of interfaces nodes.

Step 4 Click the **com1** node or **com 2** node.

When you click the com1 node, a tab appears in the right pane, and displays the default name, description, and the configurable parameters.

Send documentation comments to cbsbu-docfeedback@cisco.com

To change the default name and description of the node, enter a new name in the Name text box to identify the node, and press **Enter**. The new node name replaces the default in the node tree.

To change the description of the node, enter the new description in the Description text box.

Step 5 Right-click the node, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears displaying a list of child nodes that you can configure for this parent node.

For information on how to configure the devices, see the "Configuring a Modbus Device Node" section on page 6-35.

Configuring a Modbus RTU over an RS-485 Bus Network Node

This section describes how to configure a Modbus RS-485 bus network for devices that are connected to the com3 through com6 ports of the Mediator. To configure a Modbus RTU over an RS-485 network node, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator.

Step 2 Open an existing Mediator configuration file or start a new one.

Step 3 Click the **com3** node or **com 6** node.

When you click the com1 node, a tab appears in the right pane, and displays the default name, description, and the configurable parameters.

To change the default name and description of the node, enter a new name in the Name text box to identify the node, and press **Enter**. The new node name replaces the default in the node tree.

To change the description of the node, enter the new description in the Description text box.

Step 4 Right-click the node, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 5 From the Available Devices list, choose **modbus**, and then click **OK**.

For information on how to configure these devices, see the "Configuring a Modbus Device Node" section on page 6-35.

Configuring Modbus TCP/IP Devices

This section provides an overview of the Modbus TCP/IP client, and describes how to configure a Modbus TCP/IP network for devices that are connected to the Ethernet ports of the Mediator.

This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Configuring a Modbus TCP/IP Client

To configure a Modbus TCP/IP client, perform the following steps:

Step 1 Start Mediator configTOOL and connect to the Mediator.

Step 2 Open an existing Mediator configuration file or create a new one.

Step 3 Click to expand or collapse the node tree to list the interface nodes in the node tree pane.

Step 4 Right-click the **interfaces/eth0** or **interfaces/eth1** node, and then choose **Add** from the right-click menu.

Step 5 Click **Modbus TCP/IP client (Modbus Actual Devices)** and then click **OK**.

The Modbus Actual Devices appears under eth0 or eth1.

Step 6 Enter the IP address of the server to which the Mediator client will send commands and receive responses.

Step 7 Enter the number of the port the Mediator uses for Modbus communications in the Port text box.

The default port number is 502.

Step 8 To configure additional client nodes, repeat Step 4 to Step 7. You can configure multiple client nodes on the same Mediator, each with a different IP address

Step 9 Right-click **Modbus_device (Modbus Actual Device)**, and choose **Add** from the right-click menu.

Step 10 From the Available Devices list, choose **Modbus Device (modbus_devices)** and then click **OK**.

The Modbus Device appears under the Modbus Actual Devices.

Step 11 In the Address text box, enter the address of the Modbus Device.

For information on how to configure these devices, see the "Configuring a Modbus Device Node" section on page 6-35.

Configuring a Modbus Device Node

The Mediator implementation of Modbus supports the generic device configuration, which allows you to configure any type of device compliant with the Modbus protocol. In addition, it supports several pre-defined devices produced by specific OEMs.

This section describes how to configure a Modbus Device Node.

To configure a Modbus Device for any network, perform the following steps:

Step 1 Configure the network connection:

- If you are configuring devices for an RS-232 bus network, complete the procedure outlined in the "Configuring a Modbus RTU over an RS-232 Bus Network Node" section on page 6-33.

Send documentation comments to cbsbu-docfeedback@cisco.com

- If you are configuring devices for an RS-485 bus network, complete the procedure outlined in the "Configuring a Modbus RTU over an RS-485 Bus Network Node" section on page 6-34.
- If you are configuring devices for a TCP/IP network, complete the procedure outlined in the "Configuring Modbus TCP/IP Devices" section on page 6-34.

Step 2 Click **Modbus**.

Note To rename the node, type the new name in the Name text box, and then press **Enter**. The new node name replaces the default in the node tree. It also becomes the name of the node throughout the system. The communication parameter defaults appear in the drop-down list in the lower part of the tab.

Step 3 Right-click the **modbus device** node, and choose **Add** from the right-click menu.

Step 4 Click **Modbus**, and then click **OK**.

Note Text boxes for the required configuration parameters (labeled in red) and optional parameters appear in the lower area of the tab.

Step 5 In the Address text box, enter the device address (Device ID) of the Modbus device.

The device address is mentioned in the spec sheet or in the registry details sheet of the device from the manufacturer. It can also be obtained from the dip switches, which are available in the hardware.

Step 6 Click + in the Cache Exclude area to specify the cache.

Step 7 Click the **Register** tab to enter the register number of the first register that you want to include in the cache in the Register text box.

Note The upper boundary is determined by the start of the next cache (if any), the maximum message size, or the address of the last register in the group.

Step 8 Click the **TTL** tab to enter the length of time (in seconds) that the node retains the last value read before the system reads a new value from the device in the Time To Live (TTL) text box.

Step 9 Repeat Step 5 to Step 8 for any other caches that you want to configure.

Note The Cache Exclude capability is not explicitly supported in this release. To exclude a register from a cache, configure the cache that begins with the first register that you want to include, another cache that includes only the register that you want to exclude, and another cache that begins with the next register after the excluded one.

Step 10 Right-click the node, and choose **Add** from the right-click menu.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note The list contains register types that you can configure for a Modbus device. These include the four standard register types defined in the Modbus protocol as shown in Table 6-1.

Table 6-1 Standard Registers for Modbus Protocol

Name	Size	Access	Register Number Range
Holding Register	16 bit	Read | Write	40001 - 65535
Input Register	16 bit	Read Only	30001 - 39999
Coil	1 bit	Read | Write	1 - 9999
Input Status	1 bit	Read Only	10001 - 29999

For more information on configuring these registers, see the "Configuring the Modbus Holding Registers" section on page 6-37.

Configuring the Modbus Holding Registers

This section describes how to configure Modbus Holding Registers.

To configure Modbus Holding Registers, perform the following steps:

Step 1 Complete the procedure outlined in the "Configuring a Modbus Device Node" section on page 6-35.

Step 2 Right-click the node, and choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 3 From the Available Devices list, choose **modbus_holding_register**, and then click **OK**.

A new modbus_holding_register node appears in the node tree under its modbus_device_1 parent node.

Step 4 Enter a new name that more clearly identifies the node in the Name text box.

Step 5 In the Register Number text box, enter a value from 40001 to 65535.

Note The user documentation of the device that you are configuring should specify the mapping of register numbers to data points. Also, ensure to understand the offset in the device configurations that is set by the manufacturers when numbering the registers.

Step 6 Choose the length, in bits, required for the data type that you specify in Step 8 from the Register Length drop-down list.

Step 7 Choose the data type for the register (see Table 6-2) from the Data Type drop-down list.

Step 8 Check the **Read-Only** check box to specify the node as Read-Only.

Note The Modbus protocol supports two orders in which words, bytes, and bits can be stored in the register.

Send documentation comments to cbsbu-docfeedback@cisco.com

- Network Order (left to right, most significant to least significant)
- Reversed Order (right to left, least significant to most significant)

Step 9 Choose the order of the individual words stored in the register from the Word Order drop-down list.

Step 10 Choose the order of the individual words stored in the register from the Byte Order drop-down list.

Step 11 Choose the order of the individual words stored in the register from the Bit Order drop-down list.

Step 12 Enter the minimum limit to the value that can be written to the node in the Minimum text box. The default is None.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 13 Enter the maximum limit to the value that can be written to the node in the Maximum text box. The default is None.

Table 6-2 Holding Register Data Types

Type	Length	Description
int	1	16-bit signed integer
IEEE float	2, 4	32-bit and 64-it versions
hi byte	1	8-bit unsigned integer (high byte of register)
lobyte	1	8-bit unsigned integer (low byte of register)
loint	1	8-bit signed integer (low byte of register)
hiint	1	8-bit signed integer (high byte of register)
lochar	1	8-bit python char (low byte of register)
hichar	1	8-bit python char (high byte of register)
word	1,2	16 or 32-bit unsigned integer
dword	2	32-bit unsigned integer (same as word with length of 2)
string	–	Variable length
zstring	–	Same as string but terminated with a zero character
modulo	1,2,3,4	16, 32, 48, 64 bits. each 16 bits represents 0-9999
–	–	16-bit range -9999 to 9999
–	–	32-bit range -99,999,999 to 99,999,999
–	–	48-bit range -999,999,999,999 to 999,999,999,999
–	–	64-bit range -9,999,999,999,999,999 to 9,999,999,999,999,999
time	3,6	48 and 96-bit versions
–	–	48-bit version:
–	–	day = low byte first register
–	–	month = high byte first register
–	–	hour = low byte second register
–	–	year = high byte second register
–	–	second = low byte third register
–	–	minute = high byte third register

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 6-2 Holding Register Data Types (continued)

Type	Length	Description
–	–	96 bit version
–	–	second = first register as word
–	–	minute = second register as word
–	–	hour = third register as word
–	–	day = forth register as word

Configuring Modbus Input Registers

To configure Modbus Input Registers, perform the following steps:

Step 1 Complete the procedure outlined in the "Configuring a Modbus Device Node" section on page 6-35.

Step 2 Right-click the node, and choose **Add** from the right-click menu.

The Available Devices dialog box appears displaying a list of the child nodes that you can configure for this parent node.

Step 3 From the Available Devices list, choose **Modbus_Input_register**, and then click **OK**.

A new modbus_holding_register node appears in the node tree under its modbus_device parent node.

Step 4 Enter a new name and description that more clearly identifies the node in the Name and Description text boxes.

Step 5 Enter a number from 30001 (the default) to 39999 in the Register Number text box.

Note The user documentation of the device that you are configuring should specify the mapping of the register numbers to data points.

Step 6 Choose the register length, in bits, as required for the data type that you specify in Step 7 from the Register Length drop-down list. For example, 1 (The options available are 1,2,3,4,5, and 6.)

Step 7 Choose the data type that the register should contain (see Table 6-2) from the Data Type drop-down list.

Step 8 Check the **Read-Only** check box to specify the node as Read-Only.

Configuring the Modbus Coil Registers

To configure the Modbus Coil Registers, perform the following steps:

Step 1 Complete the procedure outlined in the "Configuring a Modbus Device Node" section on page 6-35.

Step 2 Right-click the node, and choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 3 From the Available Devices list, choose Modbus coil, and click **OK**.

Send documentation comments to cbsbu-docfeedback@cisco.com

A new modbus_coil node appears in the node tree under its modbus_device_1 parent node.

Step 4 Enter a new name and description that more clearly identifies the node in the Name and Description text boxes.

Step 5 Enter a number from 1 (the default) to 9999 in the Register Number text box.

Note The user documentation of the device that you are configuring should specify the mapping of register numbers to data points.

Step 6 Check the **Read-Only** check box to specify the node as Read-Only.

Configuring the Modbus Input Status Registers

To configure the Modbus Input Status Registers, perform the following steps:

Step 1 Complete the procedure outlined in the "Configuring a Modbus Device Node" section on page 6-35.

Step 2 Right-click the node, and choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 3 From the Available Devices list, choose Modbus_Input_Registers, and then click **OK**.

A new modbus_input_status_1 node appears in the node tree under its modbus_device_1 parent node.

Step 4 Enter a new name and a description that more clearly identifies the node in the Name and Description text boxes, or retain the default values.

Step 5 Enter a number from 10001 to 29999 in the Register Number text box.

The default is 10001.

Note The user documentation of the device that you are configuring should specify the mapping of register numbers to data points.

Step 6 Check the **Read-Only** check box to specify the node as Read-Only.

Configuring Modbus Groups

This section describes how to configure Modbus groups.

The Modbus implementation on the Mediator supports grouping and data caching of registers. Groups and caches are related, but they are not identical:

- Grouping of registers allows you to associate registers into groups that are read from (and possibly written to) the device together in a single message.
- Data caching allows you to specify groups of registers that can be read in a single message without accessing the device each time.

Send documentation comments to cbsbu-docfeedback@cisco.com

Modbus supports a maximum message size of 256 bytes, which sets a limit to the size of a register grouping that can be included in one message. If a register grouping exceeds that limit, the Mediator automatically breaks it up into smaller units.

Note All of the registers in a group must be contiguous registers of the same type.

To configure a group, specify the first register in the group as the Base Register Number, and then specify all of the child nodes of the group nodes with relative addresses. For example, if you specify 40100 as the Base Register Number, and a child node as 5, the Mediator adds the offset to the base to arrive at register 40105. A caching option allows you to cache the group.

To configure the Modbus groups, perform the following steps:

Step 1 Complete the procedure outlined in the "Configuring a Modbus Device Node" section on page 6-35.

Step 2 Right-click the node, and choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 3 From the Available Devices list, choose modbus_group_1.

A new modbus_group_1 node appears in the node tree under its modbus_group_1 parent node.

Step 4 Enter a new name and a description that more clearly identifies the node in the Name and Description text boxes, or retain the default values.

Step 5 Enter the register number of the first register in the group in the Base Register Number text box.

Step 6 Check or uncheck the **Enable separate cache** check box to enable or disable caching.

Note If you enable caching, the Base Register Number you specify in Step 6 becomes the cache boundary for the group.

Step 7 Right-click **modbus_group_1**, and choose **Add** from the right-click menu.

Step 8 Configure the registers in the group. For information on how to configure registers, see the sections covered in page 37 and page 41.

Note You must configure the child node for each register in the group individually. All of the registers in the group must be contiguous and of the same type.

In the Register Number text box, you can specify the address of each related nodes to the Base Register Number specified in Step 6. For example, if you are configuring a group of holding registers and specify 40100 as the Base Register Number, you specify the register address of the first child node as 1, the second as 2, and so on. The Mediator adds the offset to the base to arrive at register 40101, 40102, and so on.

Modbus supports a maximum message size of 256 bytes, which sets a limit to the size of a register grouping that can be included in one message. If a register grouping exceeds that limit, the Mediator automatically breaks it up into smaller units.

Send documentation comments to cbsbu-docfeedback@cisco.com

Configuring the Modbus Proxy

This section describes how to configure Modbus proxy. You can configure a Modbus proxy device by taking information from a BACnet thermostat and proxying it to Modbus. In some configurations, you can take the data from one system and proxy it to an another system that could not communicate. In other words, Modbus acts as a gateway.

To configure the Modbus proxy, perform the following steps:

Step 1 Right-click the appropriate com port in the node tree, and choose **Add** from the right-click menu. For example, com1.

The Available Devices dialog box appears.

Step 2 From the Available Devices list, choose Modbus Slave(s) over RS232 (modbus), and then click **OK**.

A new modbus node appears in the node tree under its com1 parent node.

Note Similarly, you can create Modbus Proxy over RS-485 ports and Modbus proxy over IP ports.

Step 3 Enter a new name and a description that more clearly identifies the node in the Name and Description text boxes, or retain the default values.

Step 4 Right-click modbus and choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 5 From the Available Devices list, choose **Modbus_proxy_device(modbus_proxy_device)** and click **OK**.

A new modbus_proxy_device node appears in the node tree under its modbus parent node.

Step 6 Enter a new name and a description that more clearly identifies the node in the Name and Description text boxes, or retain the default values.

Step 7 Enter an address desired for the Modbus Proxy device - 1 to 256. For example, enter 1.

Step 8 Right-click on Modbus Proxy device.

The Available Devices dialog box appears.

Step 9 From the Available Devices list, choose **modbus holding register (modbus_holding_register)**, and then click **OK**.

Step 10 Enter a new name and a description that more clearly identifies the node in the Name and Description text boxes, or retain the default values.

Note Any Entity can be linked in the link text box. For example, BACnet entity discovered and mapped under Entity: aliases/RTU1/.....”

Step 11 In the Link text box, enter /aliases/RTU1/Occupancy, and click the **Selector** icon.

Step 12 Enter modbus register number as 40001.

Step 13 Browse to the node /aliases/RTU1/Occupancy highlight it and click **Select**.

Save the configuration.

Send documentation comments to cbsbu-docfeedback@cisco.com

Configuring the SNMP Protocol

This section explains how to configure SNMP devices that are connected to the Mediator and includes the following topics:

Prerequisites

The prerequisites for configuring SNMP devices on the Mediator are as follows:

- MIBs for SNMP devices
- IP address and UDP port of the SNMP Devices
- Compiled MIBs for the SNMP device

Configuring SNMP devices on the Mediator

To configure SNMP devices on the Mediator, perform the following steps:

Step 1 Connect to the Mediator using WinSCP and move the compiled MIB of the SNMP device to the /usr/lib/broadway/mpx/lib/snmp/mibs directory on the Mediator.

Note If this is a newly supported SNMP device, you must perform Step 1. For unsupported SNMP devices, contact Cisco TAC to compile MIBs.

Step 2 Start configTOOL and connect to the Mediator.

Step 3 Click **services** to view the list of services options.

Step 4 Right-click the **/service/network** node, and choose **Add** from the right-click menu.

Step 5 Click **SNMP**.

By default, the Trap Engine and Remote Agents nodes are added.

Step 6 Right-click the **services/network/SNMP/Remote** agents node, and choose **Add** from the right-click menu.

Step 7 Click **SNMP Remote Agent (remote_agent)**, and then click **OK**.

The Managed Objects node is added automatically.

Note Text boxes for the required configuration parameters (labeled in red) and optional parameters appear in the lower area of the tab.

Step 8 Enter the IP address of the device in the IP Address text box.

Step 9 Enter the UDP Port number in use in the UDP port text box.

By default, the port number is 161 for SNMP.

Step 10 To add a new row, click **+** in the Built-In MIBs text box.

Step 11 Enter the name of the compiled MIB in the new row.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note Do not include the .py extension.

Step 12 Check the **Force discovery at start** check box.

Step 13 Right-click the **/services/network/SNMP/Remote Agents/remote_agent** node, and choose **Add** from the right-click menu.

The Available Devices dialog box appears listing the available SNMP versions.

Step 14 Enter version-specific security details for the device, and then click **OK**.

For example, you can choose SNMPv1, SNMPv2c, or SNMPv3 from the Available Devices dialog box, and then click **Add**.

Step 15 Save the configuration. After the configuration is saved, launch an Internet browser, and browse to the Mediator web client homepage.

Step 16 From the menu bar, choose **Nodes**, and go to the following URL:

nodebrowser/services/network/SNMP/Remote Agents/remote_agent

Step 17 Click **Invoke Discover() via nodebrowser**.

The SNMP nodes will be discovered.

Note The discovery process can take several minutes.

Step 18 Click **Invoke cached report () via nodebrowser**.

When you click **Invoke cached report () via nodebrowser**, Mediator generates a report that contains the names and node paths of the objects available from the SNMP device.

Step 19 Save the report as a .txt file.

Step 20 Using configTOOL and the SNMP discovery report, create aliases for the SNMP objects.

For example, the alias path will appear as the following:

/services/network/SNMP/RemoteAgents/UPS_1/Managed Objects/UPS_1/ManagedObjects/iso/org/dod/internet/private/enterprises/apc/products/hardware/ups/upsomm/upsCommStatus/0

Configuring C-Bus Protocol

This section describes the C-Bus protocol, explains how to configure C-Bus devices connected to the Mediator, and includes the following topics:

Prerequisites

Ensure the following:

- The PC-Interface Card connects the Mediator to the C-Bus Network over RS-232.

Send documentation comments to cbsbu-docfeedback@cisco.com

- The communication settings of the C-Bus device are configured.
- The C-Bus group address is mapped with the physical location of end devices.

Configuring C-Bus Devices

To configure C-Bus devices on the Mediator, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator.

For more information, see the following sections:

- Starting configTOOL, page 4-3
- Accessing Mediators Using configTOOL, page 4-11.

Step 2 Open an existing Mediator configuration file or create a new configuration file.

The configTOOL window appears.

Step 3 In the node tree pane, expand the node tree, then click **interfaces**, and then click **com1** or **com 2**. In this example, click **com1**.

The tab for the com1 node displays the default name, description, and the configurable parameters of the node.

Step 4 (Optional) You can change the description of the node. To do so, in the Description text box, enter a description that will help you identify the purpose of the node.

Step 5 (Optional) You can change the default values of the com1 node parameters located in the lower area. To do so, choose an appropriate value from the relevant drop-down list or enter a value in the text boxes provided.

Step 6 In the node tree pane, right-click **com1**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears listing the protocols supported by the Mediator.

Step 7 Choose **C-Bus via Clipsal PCI (cbus)**, and then click **OK**.

A child node, cbus, appears under the com1 node in the node tree pane.

The data entry pane for the cbus node displays the default name, description, and the configurable parameters.

Note Ensure that the Auto Discover check box and the Enable check box are checked.

Step 8 Save the configuration.

Step 9 Launch an Internet browser (for example, Internet Explorer) and browse to the Mediator web client homepage. To do so, enter the IP address of the Mediator in the Address bar of the browser.

The Mediator web client homepage appears in the Internet browser window.

Step 10 Click **NodeBrowser**.

The Mediator web client NodeBrowser homepage appears.

Step 11 Choose **interfaces** > **com1** > **cbus** > **local** to browse to the /interfaces/com1/cbus/local/ folder.

The Mediator web client NodeBrowser page displays a list of all C-Bus nodes discovered in the network.

Step 12 Click **a56**.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Mediator web client NodeBrowser page displays the group addresses of all available lighting modules.

Step 13 Map the group addresses with end devices and create aliases for all the required nodes using the configTOOL.

Note You can connect two types of devices to the C-Bus node: Relays and Dimmers.

Based on the device that you select, you must add the overridable property as follows:

- When you connect to Relays, add the property under the Binary Output (BO).
- When you connect to Dimmers, add the property under the Analog Output (AO).

Configuring the Johnson N2 Protocol

This section provides an overview of the Johnson N2 protocol, explains how to configure Johnson N2 devices that are connected to the Mediator, and includes the following topics:

- Prerequisites, page 6-47
- Configuration Instructions, page 6-47

Prerequisites

Data Definition Language (DDL) files are required for Johnson N2 devices for configuring Johnson N2 devices on the Mediator.

Configuration Instructions

To configure the Johnson N2 devices on the Mediator, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator.

Step 2 From the drop-down list of interfaces, choose **com4**, and then click **OK**.

Note This step assumes that com4 is connected to the N2 network. You can also use com3, com5, or com6.

Step 3 From the BPS drop-down list, choose **9600**.

Step 4 Set the default values in the other text boxes in the lower area of the tab.

Step 5 Right-click the **com4** node under **interfaces**, and choose **Add** from the right-click menu.

Step 6 Click **n2**.

Step 7 Configure the n2 node as follows:

a. Enable Auto Discovery Mode: all

b. Starting Address: 1

c. Ending Address: 255

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 8 Save the configuration.

Step 9 Perform a search for all N2 devices on a network by making a call to the function **force_discovery** on the n2 node. This will query all 255 addresses for the presence of a device.

This function is invoked from the Node browser with the following URL:

http://ipaddress/nodebrowser/interfaces/com4/n2?action=invoke&method=force_discovery

When you refresh the N2 page, it displays the devices on the network.

Step 10 Use the discovered device information and the object information contained in the DDLs to create aliases for the N2 devices.

The N2 driver nodes are organized as follows:

/ interfaces / com# / n2 / (*device number*) / (*region number*) / (*object number*) / [*attribute number*]

- [*device number*] is replaced by a number from 1 to 255. This is the N2 LAN address for a device.
- [*region number*] is replaced by a number from 1 to 7. N2 *regions* are defined as follows:
  - Analog Inputs
  - Binary Inputs
  - Analog Outputs
  - Binary Outputs
  - Float Internal Values (ADF)
  - Integer Internal Values (ADI)
  - Byte Internal Values
- [*object number*] is replaced by a number from 1 to 255. The range of numbers varies by device type.
- [*attribute number*] is an optional text box to allow access to various internal attributes of objects.

  Each object node directly returns the main value for each object instance; however, some applications may require access to other aspects on the state of the object.

  Details regarding Object Attributes can be found in the Open N2 protocol specification.

  For example, URLs for N2 objects on a device at address 10:

  AI 1 = /interfaces/com4/n2/10/1/1

  AI 2 = /interfaces/com4/n2/10/1/2

  ADF 123 = /interfaces/com4/n2/10/5/123

  ADI 22 = /interfaces/com4/n2/10/6/22

Configuring the Barber-Colman ASD Protocol

This section describes the Barber-Colman ASD protocol supported by the Mediator, explains how to configure Barber-Colman devices connected to the Mediator, and includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Prerequisites

Determine the communications (com) node that includes the Barber-Colman system.

Configuring Barber-Colman ASD Devices

To configure Barber-Colman ASD devices on the Mediator, perform the following steps:

Step 1 Start configTOOL to open the Mediator configuration (see the "Accessing Mediators Using configTOOL" section on page 4-11).

The configTOOL window appears.

Step 2 In the node tree pane, click **interfaces** to display the list of interface nodes.

Step 3 Click the com node to which the Barber-Colman system is connected. In this example, click com5 to display the Barber-Colman system that is connected to the com5 node.

Step 4 The data entry pane displays the default name, description, and the configurable parameters of the com5 node.

You can change the default values of the com5 node parameters located in the lower area of the com5 tab. The default values 9600- 8 -N-1-N.

Step 5 In the node tree pane, right-click **com5**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 6 Choose **Barber Colman ASD protocol (barber colman protocol)**, and then click **OK**.

A new child node, barber colman protocol, appears under the chosen com node in the node tree pane.

The barber colman protocol tab displays the default name, description, and the configurable parameters of the barber colman protocol child node.

Step 7 From the Discovery Mode drop-down list, choose **always**.

Step 8 In the Search Limit text box, enter 254.

Step 9 Save the configuration to the Mediator.

Note When the Mediator restarts, open the configuration that you had saved earlier.

Step 10 In the configTOOL window, choose **Mediator > Interrogate**.

When the device interrogation completes, a list of devices appear under the barber colman protocol snippet. Check the devices to ensure that they match the devices on your network.

Step 11 Save the barber colman protocol snippet.

Step 12 Re-open configTOOL. When prompted, do not save the interrogated configuration.

Step 13 Import the barber colman protocol snippet to the com5 node.

Step 14 Save the configuration to the Mediator.

Send documentation comments to cbsbu-docfeedback@cisco.com

Configuring the ALC WebCTRL SOAP Interface

This section describes the ALC WebCTRL SOAP interface supported by the Mediator, explains how to configure the ALC WebCTRL SOAP interface on the Mediator, and includes the following topics:

Prerequisites

Determine the following:

- WSDL for the ALC WebCTRL Server
- Username and password of the WebCTRL Server
- GQL Path of objects

Configuring an ALC WebCTRL SOAP Interface

To configure an ALC WebCTRL SOAP interface, perform the following steps:

Step 1 Connect to the Mediator using WinSCP, and move the WSDL to the following directory on the Mediator:

/var/mpx/config

Step 2 Start configTOOL and connect to the Mediator (see the "Accessing Mediators Using configTOOL" section on page 4-11).

The configTOOL window appears.

Step 3 In the node tree pane, click **interfaces** to display the list of available interfaces.

Step 4 Right-click **eth0**, and then choose **Add** from the right-click menu.

Note This step assumes that the eth0 interface is on the same network as the WebCTRL Server.

The Available Devices dialog box appears.

Step 5 Choose **ALC WebCtrl SOAP Interface (WebCtrl Server)**, and then click **OK**.

The WebCtrl Server_1 interface appears under the eth0 node in the node tree pane.

The WebCtrl Server_1 tab displays the default name, description, and the configurable parameters of the WebCtrl Server interface.

Step 6 In the Username text box, enter the username configured for the WebCtrl Server operator.

Step 7 In the Password text box, enter the password configured for the operator on the WebCtrl Server.

Step 8 In the WSDL text box, enter the WSDL name.

Note The WebCtrl Server operator must have Remote Data Access privilege to use the SOAP interface.

Step 9 In the node tree pane, right-click **WebCtrl Server_1**, and then choose **Add** from the right-click menu.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Available Devices dialog box appears listing the available WebCTRL interfaces.

Step 10 Choose **WebCtrl Point (Point)**, and then click **OK**.

The Point child node appears under the WebCtrl Server_1 node in the node tree pane.

The point tab displays the default name, description of the Point node, and the configurable parameters.

Step 11 In the Name text box, enter a new name that will identify the Point node.

Step 12 In the URL text box, enter the unique expression that identifies the WebCtrl Point.

You can determine the WebCTRL expression that uniquely identifies a WebCtrl Point. For more information, see the "Determining WebCTRL Expressions of WebCTRL Points" section on page 6-51.

Step 13 Repeat Step 9 to Step 12 to configure additional WebCtrl Points.

Step 14 Save the configuration.

Determining WebCTRL Expressions of WebCTRL Points

A WebCTRL expression uniquely identifies a WebCtrl point. You can determine the WebCTRL expression in two ways:

- Copying the Geographic Location, page 6-51
- Obtaining the GQL Path, page 6-51

Copying the Geographic Location

You can copy the geographic location path of the WebCtrl point. This path represents the URL of the WebCtrl Point.

To copy the geographic location, perform the following steps:

Step 1 Connect to the ALC WebCTRL server.

Step 2 Navigate to the Logic page, and click the appropriate WebCtrl Point.

Step 3 Click the **Details** page.

Step 4 Press **Alt**, and click **value**.

Step 5 Choose **Show Advanced**.

The Geographic Location text box displays the URL of the WebCtrl Point.

Step 6 Copy the value in the Geographic Location text box to the clipboard.

Obtaining the GQL Path

You can copy the GQL path of the WebCtrl Point. This path represents the URL of the WebCtrl Point.

To obtain the GQL path, perform the following steps:

Step 1 Connect to the ALC WebCTRL server.

Step 2 In the WebCtrl navigation tree, choose the appropriate equipment or group of equipment.

Step 3 Choose **Reports > Equipment > Points List**.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 Click the **Options** tab, and then check the **GQL Path** check box.

Step 5 Click **Run**.

Step 6 Click **Save**.

Save the report as a Microsoft Excel (.xls) document.

Open the Microsoft Excel document. In the GQL Path column, the value with a /present_value suffix is the URL of the WebCtrl point.
The following is an example of a URL for the WebCtrl point in a GQL Path column:

#b1_chiller/chws/present_value

For legacy CMNet GQL paths, replace *parameters* with *ospace*, and use the */output1.value* suffix instead of the */present_value* suffix as shown in the following example of a URL for a legacy WebCtrl point in a GQL Path column:

Original path: /#ahu1_1/legacy_fb/parameters/sat

Modified path: /#ahu1_1/legacy_fb/ospace/sat/output1.value

Note You can check or uncheck the check box for read-only documents.

Configuring the Lennox SysBus Protocol

This section describes the Lennox SysBus protocol supported by the Mediator, explains how to configure the Lennox SysBus devices on the Mediator, and includes the following topics:

- Prerequisites, page 6-52
- Configuring Lennox SysBus Devices, page 6-52

Note The Lennox SysBus driver has been tested with Lennox hardware version 1-7 and version 1-8, and firmware version 5.02 or greater.

Prerequisites

Determine the following:

- Addresses of the Lennox SysBus devices
- Com node that includes the Lennox Sysbus network

Configuring Lennox SysBus Devices

To configure Lennox SysBus devices that are connected to the Mediator, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator (see the "Accessing Mediators Using configTOOL" section on page 4-11).

The configTOOL window appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 2 In the node tree pane, expand the interfaces node, and then click **com4**. You can also use the com3, com5 or com6 port.

Note This step assumes that the com4 node is connected to the Lennox Sysbus network.

The com4 tab displays the default name, description, and the configurable parameters of the com4 node.

Step 3 From the BPS drop-down list, choose 9600.

Note Do not change the default values of the remaining parameters of the com4 node.

Step 4 In the node tree pane, right-click **com4**, and then choose **Add**.

The Available Devices dialog box appears listing the protocols supported by the Mediator.

Step 5 Choose **Lennox Sysbus protocol (lennox)**, and then click **OK**.

A new child node, lennox, appears under the com4 node in the node tree pane.

Step 6 In the node tree pane, right-click **lennox**, and then choose **Add**.

The Available Devices dialog box appears listing the available Lennox SysBus devices.

Step 7 Choose **Lennox device (device)**, and then click **OK**.

A new child node, device, appears under the lennox node in the node tree pane.

The device tab displays the default name, description, and the configurable parameters of the device node.

Step 8 (Optional) To change the name of the device node, in the Name text box, enter a new name for the device node.

The device node is renamed to the new name that you provided, and appears in the node tree pane.

Step 9 (Optional) To change the description of the device node, in the Description text box, enter a description to identify the purpose of this node.

Note In the node tree pane, when you position the cursor over the device node, a tooltip appears. The tooltip displays the description text provided in the Description text box.

Step 10 In the Address text box, enter the device address.

Step 11 Repeat Step 6 to Step 10 to configure additional Lennox SysBus devices.

Step 12 Save the configuration.

Configuring the Trane Com3 Protocol on the Mediator

This section provides an overview of the Trane Com3 protocol, explains how to configure Trane Com3 devices that are connected to the Mediator, and includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Note The devices currently supported in this release are Trane PCM, Trane RTA, Trane Scroll, and Trane TCM.

Prerequisites

Prerequisites for configuring the Trane Com3 protocol are as follows:

- Trane Com3 device addresses
- Trane Com3 Protocol Converter

Configuring the Trane Com3 Protocol

To configure the Trane Com3 protocol, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator.

Step 2 Choose **com2** from the drop-down list of interfaces, and then click **OK**.

Note This step assumes that com2 is connected to the Trane Com3 network. You can also use com1 if required.

Step 3 From the BPS drop-down list, choose **9600**.

Retain the default values in the other text boxes in the pane.

Step 4 Right-click the **interface/com2** node, and choose **Add** from the right-click menu.

Step 5 Choose **trane_com3_protocol** from the com2 drop-down list, and then click **OK**.

Configuring the Trane PCM Controller

To configure the Trane PCM controller, perform the following steps:

Step 1 Perform Step 1 to Step 4 as described in the "Configuring the Trane Com3 Protocol" section on page 6-54.

Step 2 Right-click the **interfaces/com2/trane_com3_protocol** node, and choose **Add** from the right-click menu.

Step 3 Click **pcm**.

Step 4 Enter a new name for the node in the Name text box.

Step 5 Enter the address of the device in the Address text box.

Step 6 Check the **Upload Setpoints** check box to set the default setting.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 7 Repeat Step 1 to Step 6 for each device.

Step 8 Save the configuration.

Configuring the Trane RTA Controller

To configure the Trane RTA controller, perform the following steps:

Step 1 Perform Step 1 to Step 5 as described in the "Configuring the Trane Com3 Protocol" section on page 6-54.

Step 2 Right-click the **trane_com3_protocol** node under **interfaces/com2**, and choose **Add** from the right-click menu.

Step 3 Click **RTA**.

Step 4 Enter a new name for the node in the Name text box.

Step 5 Enter the address of the device in the Address text box.

Step 6 Repeat Step 2 to Step 4 for each device.

Step 7 Save the configuration.

Configuring the Trane Scroll Controller

To configure the Trane Scroll controller, perform the following steps:

Step 1 Perform Step 1 to Step 5 as described in the "Configuring the Trane Com3 Protocol" section on page 6-54.

Step 2 Right-click the **interfaces/com2/trane_com3_protocol** node, and choose **Add** from the right-click menu.

Step 3 Click **Sroll**.

Step 4 Enter a new name for the node in the Name text box.

Step 5 Enter the address of the device in the Address text box.

Step 6 Check the **Upload Setpoints** check box to set the default setting.

Step 7 Repeat Step 1 to Step 5 for each device.

Step 8 Save the configuration.

Configuring the Trane TCM Controller

To configure the Trane TCM controller, perform the following steps:

Step 1 Perform Step 1 to Step 5 as described in the "Configuring the Trane Com3 Protocol" section on page 6-54.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 2 Right-click the **interfaces/com2/trane_com3_protocol** node, and choose **Add** from the right-click menu.

Step 3 Click **tcm**, and then click **OK**.

Step 4 Enter a new name for the node in the Name text box.

Step 5 Enter the address of the device in the Address text box.

Step 6 Check the **Upload Setpoints** check box to set the default setting.

Step 7 Repeat Step 2 to Step 5 for each device.

Step 8 Click **Save** to save the configuration.

Configuring the Trane VariTrane II \ III Controller

To configure the Trane VariTrane II \ III controller, perform the following steps:

Step 1 Perform Step 1 to Step 5 as described in the "Configuring the Trane Com3 Protocol" section on page 6-54.

Step 2 Right-click the **/interfaces/com2/trane_com3_protocol** node, and choose **Add** from the right-click menu.

Step 3 Click **VariTrane**, and then click **OK**.

Step 4 Enter a new name for the node in the Name text box.

Step 5 Enter the address of the device in the Address text box.

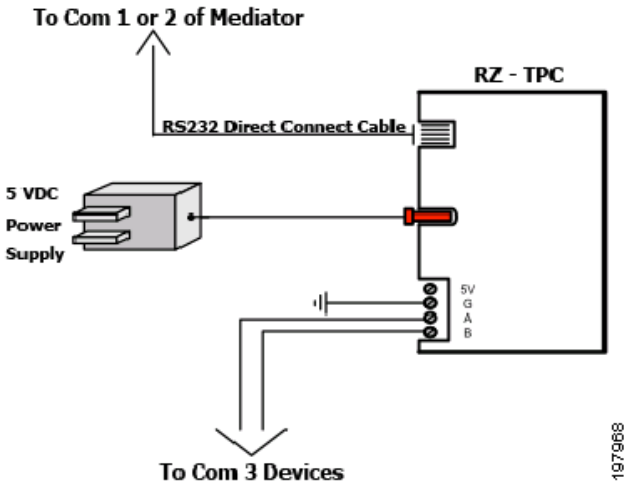
Step 6 Check the **Upload Setpoints** check box to set the default setting.

Step 7 Repeat Step 2 to Step 5 for each device.

Step 8 Click **Save** to save the configuration.

Figure 6-6 shows the wiring details of the RZ-Trane protocol convertor.

Figure 6-6 Wiring Detail of RZ-Trane Protocol Convertor



Send documentation comments to cbsbu-docfeedback@cisco.com

Configuring the Trane Com4 Protocol on the Mediator

This section provides an overview of the Trane Com4 protocol, explains how to configure Trane Com4 devices that are connected to the Mediator, and includes the following topics:

Note The devices that are currently supported are the Trane Intellipak, Trane Varitrane II\III, and Trane Voyager.

Prerequisites

Trane Com4 device addresses are required for configuring the Trane Com4 devices on the Mediator.

Configuring the Trane Com4 Protocol

To configure the Trane Com4 Protocol, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator.

Step 2 Choose **com4** from the drop-down list of interfaces, and then click **OK**.

Note This step assumes that com4 is connected to the Trane com4 network. You can also use com3, com5, or com6.

Step 3 From the BPS drop-down list, choose **9600**.

The other text boxes in the data entry pane have the default values.

Step 4 Right-click the **/interfaces/com4** node, and choose **Add** from the right-click menu.

Step 5 Click **trane_com4_protocol**.

Note The DIP switch address is set to 50. For more information on DIP switch settings, see table "TCI-3 board DIP switch address settings for Tracer 100 series panels and Tracer Summit" in the *Trane Communication Interface Installation Guide.*

Note The communication PIN set should be changed between COM4 and COM3 protocols.

Step 6 Save the configuration.

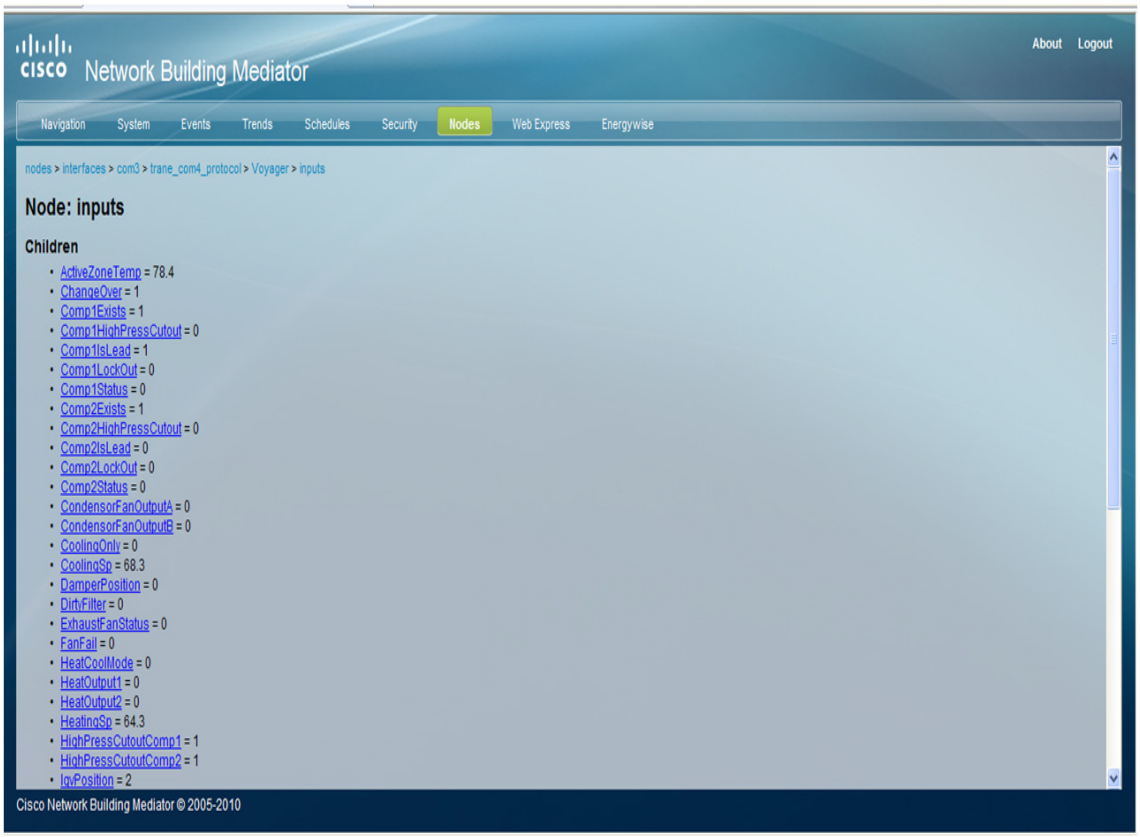
Send documentation comments to cbsbu-docfeedback@cisco.com

Step 7 To view the configuration, launch an Internet browser (for example, Internet Explorer), and browse to the Mediator web client homepage. To do so, enter the IP address of the Mediator in the Address bar of the browser and log in when prompted.

Step 8 Choose **nodes > interfaces > com3 > trane_com4_protocol > Voyager > inputs**

The Mediator web client NodeBrowser page displays the configured values. (See Figure 6-7.)

Figure 6-7 Trane Com4 Configuration



Configuring the Trane Intellipak Controller

To configure the Trane Intellipak controller, perform the following steps:

Step 1 Perform Step 1 to Step 5 as described in the "Configuring the Trane Com4 Protocol" section on page 6-57.

Step 2 Right-click the **interfaces/com4/trane_com4_protocol** node, and choose **Add** from the right-click menu.

Step 3 Click **Intellipak**.

Step 4 Enter a new name for the node in the Name text box.

Step 5 Enter the address of the device in the Address text box.

Step 6 Repeat Step 2 to Step 4 for each device.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 7 Save the configuration.

Configuring the Trane Voyager Controller

To configure the Trane Voyager controller, perform the following steps:

Step 1 Perform Step 1 to Step 5 as described in the "Configuring the Trane Com4 Protocol" section on page 6-57.

Step 2 Right-click **/interfaces/com4/trane_com4_protocol** node, and choose **Add** from the right-click menu.

Step 3 Click **Voyager**.

Step 4 Enter a new name for the node in the Name text box.

Step 5 Enter the address of the device in the Address text box.

Step 6 Check the **Upload Setpoints** check box to set the default setting.

Step 7 Repeat Step 2 to Step 5 for each device.

Step 8 Save the configuration.

Configuring the Trane 3 Non Isolated Controller

To configure the Trane Com3 Non Isolated Controller, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator.

Step 2 Choose **com4** from the drop-down list of interfaces, and then click **OK**.

Note This step assumes that com4 is connected to the Trane com4 network. You can also use com3, com5, or com6.

Step 3 From the BPS drop-down list, choose **9600**.

The other text boxes in the data entry pane have the default values.

Step 4 Right-click the **/interfaces/com3** node, and choose **Add** from the right-click menu.

Step 5 Click **trane_com3_noniso protocol**.

Configuring the Trane VariTrane II \ III Controller

To configure the Trane VariTrane II \ III controller, perform the following steps:

Step 1 Perform Step 1 to Step 5 as described in the "Configuring the Trane Com4 Protocol" section on page 6-57.

Step 2 Right-click the **/interfaces/com4/trane_com3noniso_protocol** node, and choose **Add** from the right-click menu.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 3 Click **VariTrane**, and then click **OK**.

Step 4 Enter a new name for the node in the Name text box.

Step 5 Enter the address of the device in the Address text box.

Step 6 Check the **Upload Setpoints** check box to set the default setting.

Step 7 Repeat Step 2 to Step 5 for each device.

Step 8 Save the configuration.

Configuring the TCS Basys Protocol

This section describes the TCS Basys protocol supported by the Mediator, explains how to configure TCS Basys devices connected to the Mediator, and includes the following topics:

Prerequisites

The Mediator connects to the TCS Basys network over RS-485. Therefore, determine the appropriate communications (com) node that includes the TCS Basys system.

Configuring TCS Basys Devices

To configure TCS Basys devices on the Mediator, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator (see the "Accessing Mediators Using configTOOL" section on page 4-11).

The configTOOL window appears.

Step 2 In the node tree pane, click **interfaces** to display the list of interface nodes.

Step 3 Click the com node to which the TCS Basys communication network is connected. In this example, click the **com6** node.

Step 4 From the BPS drop-down list, choose the appropriate baud rate.

Note This baud rate must match the baud rate that is configured on the TCS Basys device.

Step 5 From the Data Bits drop-down list, choose **8**.

Step 6 From the Parity drop-down list, choose **none**.

Step 7 From the Stop Bits drop-down list, choose **1**.

Step 8 Retain the default values in the remaining text boxes.

Step 9 In the node tree pane, right-click the **com6** node, and choose **Add** from the menu.

The Available Devices dialog box appears listing the protocols supported by the Mediator.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 10 In the Available Devices dialog box, choose **TCS Protocol Line Handler (tcs)** from the list, and then click **OK**.

A new child node, tcs, appears under the com6 node in the node tree pane.

The tcs tab displays the default name, description, and the configurable parameters of the tcs child node.

Step 11 From the Enable Auto Discovery Mode drop-down list, choose **all**. This enables auto discovery of all devices, both newly and previously configured devices.

Step 12 In the Starting Address text box, enter **0**.

Step 13 In the Ending Address text box, enter **255**.

Every TCS Basys device on the network has a unique address in the range of 0- 255. The Starting and Ending Address text boxes are used to specify the range of addresses to search within.

Step 14 Ensure that the **Debug** check box is unselected.

Step 15 Save the configuration to the Mediator.

Note When the Mediator restarts, open the configuration you had saved earlier.

Step 16 In the configTOOL window, choose **Mediator > Interrogate**.

When the device interrogation completes, a list of devices appear under the tcs node. Check the devices to make sure that they match the devices on your network.

Step 17 Save a snippet of the tcs node with the discovered devices by right-clicking the **tcs** node under the **com6** node, and choosing **Output From Here** from the menu. The Output Mediator Configuration dialog box appears.

Step 18 In the Output Mediator Configuration dialog box, click **Save to File**.

Step 19 Save the file to a directory on your local system. The file should be saved as an XML extension file. For example, tcssnippet.xml.

Step 20 On the toolbar, click the **Refresh Configuration** button to reload the Mediator configuration.

Step 21 In the node tree pane, choose **Interfaces > com6 > tcs**.

Step 22 Right-click the **tcs** node, and choose **Delete** from the menu.

Step 23 Click **Yes** in the Confirmation request message.

Step 24 Import the snippet of the tcs node that includes the discovered devices by right-clicking the **com6** node, and choosing **System > Import configuration fragment**.

Step 25 Browse and choose the snippet that was saved according to the instruction in Step 19.

Step 26 Click **OK**.

The tcs node, along with a list of devices under it, appears under the com6 node.

Step 27 From the Enable Auto Discovery Mode drop-down list, choose **never**.

Step 28 Save the configuration to the Mediator.

Step 29 To view the configured TCS Basys devices, launch an Internet browser (for example, Internet Explorer), and browse to the Mediator web client homepage. To do so, enter the IP address of the Mediator in the Address bar of the browser, and log in when prompted.

The Mediator web client homepage appears in the Internet browser window.

Step 30 Click **Nodes**.

The Mediator web client NodeBrowser page appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 31 Choose **interfaces** > **com6** > **tcs**.

The Mediator web client NodeBrowser page displays a list of all the TCS Basys devices.

Configuring Secure Remote Node Abstraction Protocol

This section explains how to configure Secure Remote Node Abstraction (SRNA) protocol.

Note All the other communication protocols described in this chapter are Building Management Systems (BMS) communication protocols. The SRNA protocol is based on IP for communicating with the Downstream Mediators.

To configure the SRNA protocol on the Mediator, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator (see the "Accessing Mediators Using configTOOL" section on page 4-11).

The configTOOL window appears.

Step 2 In the node tree pane, expand the node tree, then choose **services** > **network** > **rna**.

The rna tab displays the default name, description, and the configurable parameters of the rna node.

Step 3 Check the **Enabled** check box to enable the Mediator to act as an RNA server.

By default, this box is unchecked. In such cases, the Mediator will ignore incoming RNA messages.

Step 4 In the port text box, enter **5150**.

Step 5 From the interface drop-down list, choose the ethernet interface over which the Mediator communicates with the Mediator Manager using RNA.

By default, **eth0** is selected.

Step 6 In the Client-Side Connection Timeout text box, enter an upper limit (in seconds) for how long the client-side RNA allows the TCP/IP connection to be established.

The default timeout value is three seconds.

Step 7 In the Client-Side Transaction Timeout text box, enter an upper limit (in seconds) for how long the client-side RNA allows a TCP/IP send or receive transaction to be completed.

The default timeout value is 900 seconds.

Step 8 In the Security Level drop-down list, retain the security level to **NoSec**.

Note There are three security levels—NoSec, Auth-Only, and Full-Enc. These levels are described in detail in the *Cisco Network Building Mediator Manager User Guide*.

Step 9 Repeat Step 1 to Step 8 on all the Mediators that need to communicate with the Mediator Manager over SRNA.

Step 10 To enable communication between the Mediators using RNA, in the node tree pane, expand the root node, and click **Aliases**.

Step 11 Right-click the Aliases node, and then choose **Add** from the right-click menu.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Available Devices dialog box appears.

Step 12 In the Available Devices dialog box, choose **Alias** and click **OK**.

Step 13 In the alias tab, enter a new name and a description that more clearly identifies the node in the respective text boxes (or retain the default values).

Step 14 In the Alias For text box, enter the path of the point mpx://<ip address>:<port>/<point_url> for retrieving values from the remote Mediator. For example, mpx://<*ipaddress*>/services/time/local to retrieve the time from the remote Mediator.

Note The <ipaddress> is the *IP address* of the Mediator with which you want to communicate.

Step 15 If you have to change the default port on a remote Mediator, enter mpx://ipaddress:<*port*>/services/time/local.

Note There are two options mpxao and mpxfe. For more information, see the *Cisco Network Building Mediator Manager User Guide*.

Step 16 Save configuration.

Note Transport Layer Security protocol (TLS) 1.0 is enabled in SRNA communications that occur between Mediators as well as between a Mediator and a Mediator Manager. However, when a peer device is running an older software version that does not support TLS 1.0, the connection downgrades to SSL 3.0. For example, in SRNA communications between a Mediator 3.1.3 and Mediator Manager 1.1.3, TLS 1.0 is enabled. However, in SRNA communications between a Mediator 3.1.3 and Mediator Manager 1.1.2, the connection downgrades to SSL 3.0

Configuring the ETC-USAP Protocol

This section describes the prerequisites for configuring the ETC-USAP devices and how to configure the ETC-USAP devices on the Mediator. It includes the following topics:

Prerequisites

Ensure that the following requirements are met:

- The devices support ETC-USAP protocol.
- ETC-USAP licensing is enabled on the Mediator.

Configuring ETC-USAP Devices

The ETC-USAP devices are connected to the RS232 ports, com1 or com2, of the Mediator.

To configure ETC-USAP devices that are connected to the Mediator, perform the following steps:

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 1 Start configTOOL and connect to the Mediator (see the "Accessing Mediators Using configTOOL" section on page 4-11).

The configTOOL window appears.

Step 2 In the node tree pane, expand the interfaces node, and right-click **com1**.

The right-click menu appears.

Step 3 Choose **Add**.

The Available Devices dialog box appears listing the protocols supported by the Mediator.

Step 4 Choose **USAP Device (USAP Device)** and click **OK**.

The USAP Device tab appears and a new child node, USAP Device, appears under the com1 node in the node tree.

Step 5 In the USAP Device tab, do the following:

a. (Optional) In the Description text box, enter the description for the device.

b. Select the **enabled** check box to enable the USAP protocol.

c. Select the **unison_v1_9_0_prior** check box if the Unison operating code version on USAP controller is version 1.9.0 or earlier.

d. Select the **debug** check box to print the protocol related messages on the mslog_viewer.

Step 6 Right-click the **USAP Device** node and choose **Add**.

The Available Devices dialog box appears.

Step 7 Choose **USAP Room (Room)** and click **OK**.

The Room tab appears and a new child node, USAP Room, appears under the USAP Device node in the node tree.

Step 8 On the Room tab, do the following:

- (Optional) In the Description text box, enter the description for the room.

Step 9 Right-click the **USAP Room** node and choose **Add**.

The Available Devices dialog box appears listing the objects and sections.

Step 10 Choose **USAP Object (Object)** to add an object or **USAP Section (Section)** to add a section in the room.

The Object tab or the Section tab appears depending on your selection and a corresponding new child node, USAP Object or USAP Section, appears in the node tree.

Step 11 On the Object or the Section tab, do the following:

- (Optional) In the Description text box, enter the description for the room.

Note Ensure that the names of the objects, sections, and rooms correspond to the object, section, and room names that are configured in the device otherwise the configuration fails.

Step 12 Save the configuration.

Step 13 To view the configured USAP devices, launch the Internet browser and log in to the Mediator web client homepage.

The Mediator homepage appears.

Step 14 Click **Nodes**.

The Mediator web client NodeBrowser homepage appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 15 Choose **nodes > interfaces > com1 > USAP Device > Room > Section > Object**

All the rooms, sections and objects that are configured are listed in the page.

Note You can activate or deactivate the configurations by entering the **ACTI** or **DACT** commands in the Override text box.

Configuring the Omnimeter Protocol

To configure the Omnimeter protocol on the Mediator, perform the following steps:

Step 1 Start configTOOL to open the Mediator configuration (see the "Accessing Mediators Using configTOOL" section on page 4-11).

The configTOOL window appears.

Step 2 In the node tree pane, expand the interfaces node, and then click **com3**. You can also use any of the RS-485 ports. (For example, COM3, COM4, COM5, COM6)

Step 3 In the node tree pane, right-click **com3**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears listing the protocols supported by the Mediator.

Step 4 Choose **Omnimeter Protocol** and then click **OK**.

The Omnimeter tab appears.

Step 5 In the Omnimeter tab, do the following:

a. (Optional) In the Name text box, enter a descriptive name for the device.

b. (Optional) In the Description text box, enter the description for the device.

Note All mandatory text boxes appear in red color.

c. In the Number of Retries text box, enter the number of times the Mediator should try to read data from the device before reporting any error.

d. In the Reply Timeout text box, enter the time (in seconds) that the Mediator should wait for a reply from the device.

e. In the Cache life text box, enter the time (in seconds) that the current read value is cached by the Mediator.

Step 6 Right-click **Omnimeter Protocol**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 7 From the list of available devices, choose the appropriate Omnimeter device. For example, RS-1 or RS-5.

Step 8 Click **OK**.

Step 9 The Omnimeter_device tab displays the default name and description, and the configurable parameters. For each text box on the tab, enter or choose the appropriate parameter value to configure the device.

Step 10 In the Building Number text box, enter building number where the energy meter is deployed.

Step 11 In the Unit Number text box, enter unit number of the meter.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note Specify the unit number and the building number to identify the Omnimeter device in the network.

Step 12 In the Serial Number text box, enter the 12 digit serial number.

The manufacture serial number can be found at the bottom of the Omnimeter and is hardcoded. All devices have an unique serial number. For example, 096143016078.

Step 13 Save configuration.

Step 14 Repeat Step 9 to Step 11 for each device that you want to add.

Configuring the Delphi Web Service Protocol

This section describes how to configure the Delphi Protocol on the Mediator to enable it to interact with various Delphi devices and includes the following topics:

Prerequisites

The prerequisites for the Delphi web service protocol configuration are as follows:

- Access to the Interface PC with user credentials
- Location of the Event.NSS file on the Interface PC

Configuring the Delphi Web Service Protocol on the Mediator

To configure the Delphi protocol on the Mediator, perform the following steps:

Step 1 Perform Step 1 to Step 3 in the "Before You Begin Configuring the Protocols" section on page 6-18.

Step 2 In the node tree pane, expand the node tree, click **services**, and then click **network**.

Step 3 In the node tree pane, right-click **network**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears listing the protocols supported by the Mediator.

Step 4 Click **Delphi Web Service Client (Delphi Flatfile version)**, and then click **OK**.

A new child node, **Delphi Flatfile version_1**, appears under the network node in the node tree pane. The Delphi Flatfile version_1 tab for the delphi node displays the default name and the description.

Step 5 Select the **Enabled** check box to enable **Delphi Flatfile version_1** protocol.

Step 6 Select the **Debug** check box to print the debug messages from Delphi Flatfile version_1 protocol.

Step 7 In the node tree pane, right-click the Delphi Flatfile version_1 node, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 8 Click **Delphi Property Information (PropertyName)**, and then click **OK**.

A new child node, PropertyName_1, appears under the network node in the node tree pane. The PropertyName_1 tab for the Delphi node displays the default name and description.

Step 9 In the Interface PC Address text box, enter the communication address or the IP address of the Interface PC. For example, 198.162.1.1.

Step 10 From the Communications Interface drop-down list, choose the appropriate communication interface over IP.

The available communication interface options are: **http**, **https**, **ftp and sftp**.

Step 11 In the **User Name** text box, enter the username you use to access the Interface PC.

Step 12 In the **Password** text box, enter the password you use to access the Interface PC.

Step 13 In **Event File Location** text box, enter the location of **EVENT.NSS** file. For example, **/Delphi/Property/Harrah/EVENTS.NSS**.

Step 14 From the Polling Time drop-down list, choose the desired polling time. The **EVENT.NSS** file is retrieved from the Interface PC at every configured polling time.

The available polling time options, in minutes, are: **15**, **30**, **45** and **60**.

Step 15 From the Grace Time drop-down list, choose the desired grace time.

The available grace time options, in minutes, are: **0**, **10**, **15**, **20**, **25**, **30**, **35**, **40**, **45**, **50**, **55** and **60**.

Note All mandatory text boxes appear in red color.

DownloadStatus displays the recent download status of **EVENT.NSS** file with a time stamp. For example, Download Success at 2011-07-25 06:42:03.410809 or Download Failed at 2011-07-25 06:42:03.410809 on the node browser.

Note DownloadStatus node get included by default under the PropertyName node. You can configure only one download status node under a property.

Step 16 To add a Meeting Room, in the node tree pane, right-click the **PropertyName_1** node, and choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 17 Click **Room Name should match with the room name in EVENT.NSS**, and then click **OK**.

Note You can add multiple room names. Room Name should match with the room name present in **EVENT.NSS**. For example, **BURGUNDY**, **VERSAILLES 1/2**. Duplicate entries should not be made.

MeetingSpaces are just place holders.You can add multiple meeting spaces under each room.

Step 18 To add a MeetingSpace, in the node tree pane, right-click the **VERSAILES 1/2** node, and choose **Add** from the right-click menu.

The Available Devices dialog box appears.

Step 19 Click **Delphi Meeting Space Information (MeetingSpace)**, and then click **OK**.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note We recommended adding three meeting spaces under each room. The MeetingSpace name should not contain '/' character.

Each MeetingSpace contains the following nodes:

- AgreedAttendance
- EndDate Time
- EndEpochTime
- EventName
- StartDateTime
- StartEpochTime

Step 20 Save the configuration, and then click **Close**.

Property status is displayed against property name in node browser. The following enumerated messages are used to indicate the status of execution of a property:

- 0:'0: Init' - Property Initialization
- 1:'1: OK' - No error conditions
- 2:'2: OK with event file same as yesterday' - Event file is same as previous day
- 3:'3: Incomplete meeting information' - Incomplete meeting information in EVENTS.NSS (line length is not equal to 252)
- 4:'4: Communication Error, using backup event file' - Network connection error but uses previously downloaded file in the same day
- 5:'5: Communication Error' - Network connection error and no backup file
- 6:'6: File IO Error' - Error in file I/O operation

Viewing Delphi Nodes

To view the configured Delphi nodes, perform the following steps:

Step 1 Launch an Internet browser. For example, Internet Explorer.

Step 2 Enter the IP address of the Mediator in the address bar of the browser and log in when prompted.

The Mediator web client homepage appears in the Internet browser page.

Step 3 Click **Nodes**.

The Mediator web client NodeBrowser homepage appears.

Step 4 Choose **services > network > Delphi Flatfile Version_1**.

Step 5 Choose **PropertyName > MeetingRoom Name > MeetingSpace**.

The following four different status is displayed against each MeetingSpace (under MeetingRoom Name).

- **Unknown**: Indicates the status before parsing the events file.
- **Available**: Indicates the meeting space entry under a room is free and can be used to fill the received meeting information from the Interface PC.
- **Scheduled**: Indicates the meeting space entry under a room is filled with the scheduled meeting information received from the Interface PC.

Send documentation comments to cbsbu-docfeedback@cisco.com

- **In Progress**: Indicates the meeting space under a room is filled with a meeting which is currently in progress.

Step 6 View Delphi messages using mslog_viewer.

Connect to the mediator through console or ssh and enter the mslog_viewer command, a series of messages are displayed in the message log (msglog viewer). These messages are useful to verify whether the Delphi stack is running and how the downloads and updates from the Delphi network are configured on the stack.

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 7

KNX Deployment

This chapter provides an outline of the KNX topology, describes how to configure the KNX protocol on the Mediator, and includes useful troubleshooting tips and information for resolving issues that are encountered when configuring the KNX protocol on the Mediator. It includes the following sections:

Overview

KNX is a decentralized, distributed network protocol that is used to manage building controls, such as HVAC and lighting systems. The KNX protocol describes the means by which the devices can share information with each other by defining the communication mechanisms, standardized data types, and functional block objects.

KNX networks support two different configuration models—S-Mode (system) and E-Mode (easy). S-Mode is the primary mode. It describes the centralized free binding mode of operation that is provided by the PC-based tool ETS. E-mode relies on a structured binding principle, through simple manipulations, without the need for a PC-based tool. An E-Mode-based configuration is typically used for simple products (such as a light switch and actuator) that are tightly coupled, and are typically targeted towards home usage.

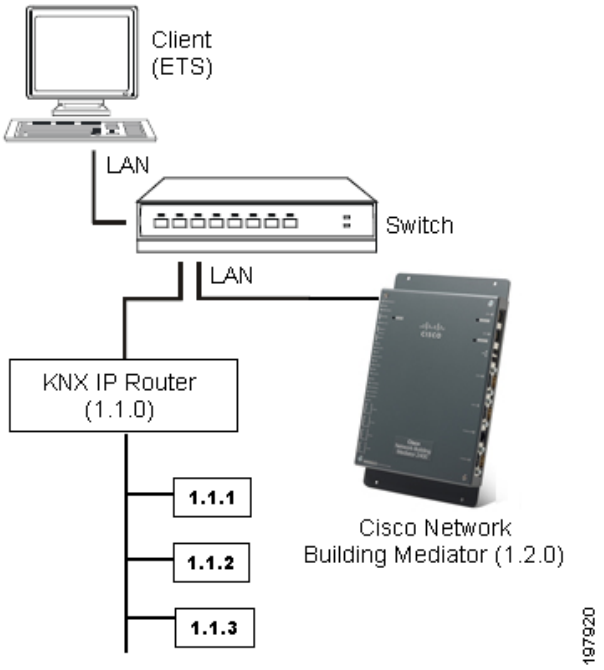
For more information on KNX, refer to the KNX documentation.

Topology

Figure 7-1 outlines the KNX architecture.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 7-1 KNX Architecture



The KNX architecture consists of the following components:

- Client (PC on which the ETS tool is installed)—The ETS tool is used to control the KNX devices on the KNX network. Using the ETS tool, you can configure the communication objects on the KNX network, and replicate and download this configuration on the Mediator. All the KNX communication objects (pattern) are replicated on the Mediator using the ETS Download program from the PC to the Mediator. Also, all attributes of these communication objects, such as type of data point and object function are the same as that configured for the KNX devices on the KNX network.
- Switch—The Mediator is connected to the PC on which the ETS tool is installed using a switch, preferably a passive switch. Connect the eth0 port of the Mediator to the PC. A switch is used to ensure that the KNX address configured on the Mediator is in the same network.
- KNX IP Router—The Mediator connects to the KNX network using the KNX IP router. The KNX IP router provides the IP interface to the KNX network, which is used to connect the Mediator via Ethernet since the Mediator does not have a KNX bus interface.
- KNX Network—A fully distributed network, which accommodates up to 65536 devices in a 16-bit address space. The logical topology (see Figure 7-1), accommodates sub-networks and allows 256 devices on one line. Lines may be grouped together with a main line into an area. Adding up to 15 areas together with a backbone line forms an entire domain. This topology is reflected in a numerical structure of the individual addresses, which uniquely identifies each node on the network. The address 1.1.16, for example, refers to the 16th node on the first line of area 1.
- Mediator—Interacts with the above components using a process referred to as binding. Binding takes place using the ETS tool, and is used to logically link the datapoints of different devices and applications across the network.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Mediator provides access to and visualizes the KNX network using configTOOL. The configTOOL creates a node tree to replicate the KNX communication objects that are present on the KNX network. This is done before downloading the KNX communication object database from ETS to the Mediator. The ETS Download program provides the real KNX communication object database to the Mediator on which the KNX stack is running.

Configuring the KNX Protocol

This section describes how to configure the KNX protocol on the Mediator and includes the following topics:

Prerequisites

The prerequisites for the KNX protocol configuration are as follows:

- When the Mediator is connected to the PC on which the ETS tool is installed using a switch, connect the eth0 port of the Mediator to the PC.
- When the Mediator is directly connected to the PC on which the ETS tool is installed (without using a switch), connect the eth1 port of the Mediator to the PC.
- Configure the same set of communication objects (using the ETS tool) for the Mediator as that configured for all other KNX devices on the KNX network. For example, Communication Object 1 in ETS for a given KNX device should be mapped to Communication Object 1 in ETS for the Mediator. All attributes of this communication object, such as type of data point and object function should be the same as that configured for the KNX devices in the KNX network.

Configuring KNX

To configure the KNX protocol on the Mediator, perform the following steps:

Step 1 Start Mediator configTOOL and connect to the Mediator.

Step 2 Open an existing Mediator configuration file or create a new configuration file. The Mediator configTOOL window appears.

Step 3 In the node tree pane, expand the node tree, then choose **services > network**. Right-click the network node, and choose **Add** from the drop-down list.

The Available Devices dialog box appears listing the protocols supported by the Mediator.

Step 4 In the Available Devices dialog box, choose **KNX Protocol (KnxProtocol)** from the list, and then click **OK**.

A new child node, KnxProtocol_1, appears under the network node in the node tree pane.

Step 5 In the node tree pane, right-click the KnxProtocol_1 node, and choose **Add** from the drop-down list to add a device.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Available Devices dialog box appears.

Step 6 In the Available Devices dialog box, choose **KNX Device (KnxDevice)**, and then click **OK**.

A new child node, KnxDevice, appears under the KnxProtocol_1 node in the node tree pane.

You are permitted to add only one device under a KNX protocol node. If you try to add another device, an exception error is displayed.

Step 7 On the KnxDevice tab, choose the interface from the interface drop-down list. You can select **eth0** for Ethernet-0 or **eth1** for the Ethernet-1 configuration.

Step 8 Select the **Programming Mode Enable** check box only if you want to put the Mediator in programming (self-learning) mode, so that you can change the KNX physical address of the Mediator as described in Configuring the KNX Physical Address of the Mediator, page 7-5.

Step 9 In the node tree pane, right-click the KnxDevice node, and choose **Add** from the drop-down list to add a communication object.

The Available Devices dialog box appears.

Step 10 In the Available Devices dialog box, choose **KNX Communication Object (KnxComObj)**, and then click **OK**.

A new child node, KnxComObj_1, appears under the KnxDevice node in the node tree pane.

Step 11 On the KnxComObj_1 tab, enter the communication object number and the communication object value.

Note When configuring the KNX communication objects, enter the communication object value as 0.

You can add up to 254 KNX communication objects under each device. To add the communication objects, you must be aware of the object number and it should be available in the KNX network.

Step 12 Save the configuration.

Managing KNX Communication Objects

You can view and override the values specified for the communication objects that are configured under each device.

To view and override KNX communication object values, perform the following steps:

Step 1 Launch an Internet browser (for example, Internet Explorer) and browse to the Mediator web client homepage. To do so, enter the IP address of the Mediator in the Address bar of the browser and log in when prompted.

The Mediator web client homepage appears in the Internet browser window.

Step 2 Click **Nodes**.

The Mediator web client Node page appears.

Step 3 Choose **services > network > KnxProtocol_1 > KnxDevice**.

The Mediator web client Node page displays the configured KNX communication objects and their corresponding values.

Send documentation comments to cbsbu-docfeedback@cisco.com

For example, if Communication Object 1 corresponds to a light switch, a value of 0 indicates that the switch is currently Off, and a value of 1 indicates it is On. While for a dimmer switch, a percentage value indicates its brightness.

Note The Mediator web client node browser displays a percentage as an analog value. For example, 40% is displayed as 40.

Step 4 To override the value specified for a given communication object, click the **Value** link against it.

The Mediator web client Node page displays the value for the given communication object in an editable text box.

Step 5 In the Action text box, enter the desired value. In the case of a communication point, such as a dimmer switch, enter an analog value.

For example, to specify the value as 40%, enter 40 in the Action text box.

Step 6 Click **Override** to save your setting.

Configuring the Mediator from the ETS Tool

This section describes how to configure the Mediator from the ETS tool and includes the following topics:

Note Ensure that you have installed the ETS tool and imported the .vd3 file using the **File > Import** option in the ETS tool. You need to import a .vd3 file or a higher file type for ETS 3 and higher versions.

Configuring the KNX Physical Address of the Mediator

By default, the Mediator has a physical address of 15.15.255 based on the KNX standard. You can change the physical address of the Mediator if you want to.

To configure the KNX physical address of the Mediator from the ETS tool, perform the following steps:

Step 1 Connect the **eth0** port of the Mediator to the switch. The PC on which the ETS tool is installed and the KNX IP router are also connected to the same switch. (See Figure 7-1.)

Step 2 Configure the KNX protocol on the Mediator as described in Configuring KNX, page 7-3, and verify that the **Programming Mode Enable** check box in the KnxDevice window is selected. See Step 8 in Configuring KNX, page 7-3.

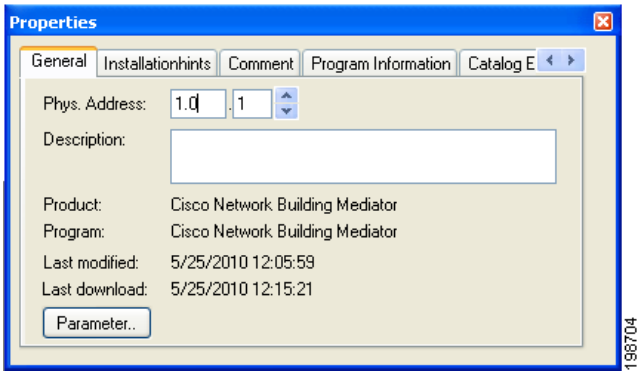
Step 3 Save the configuration.

Step 4 Open the ETS tool.

Step 5 In the Topology window, double-click the Mediator whose physical address you want to change. The Properties dialog box appears. (See Figure 7-2.)

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 7-2 Properties Dialog Box

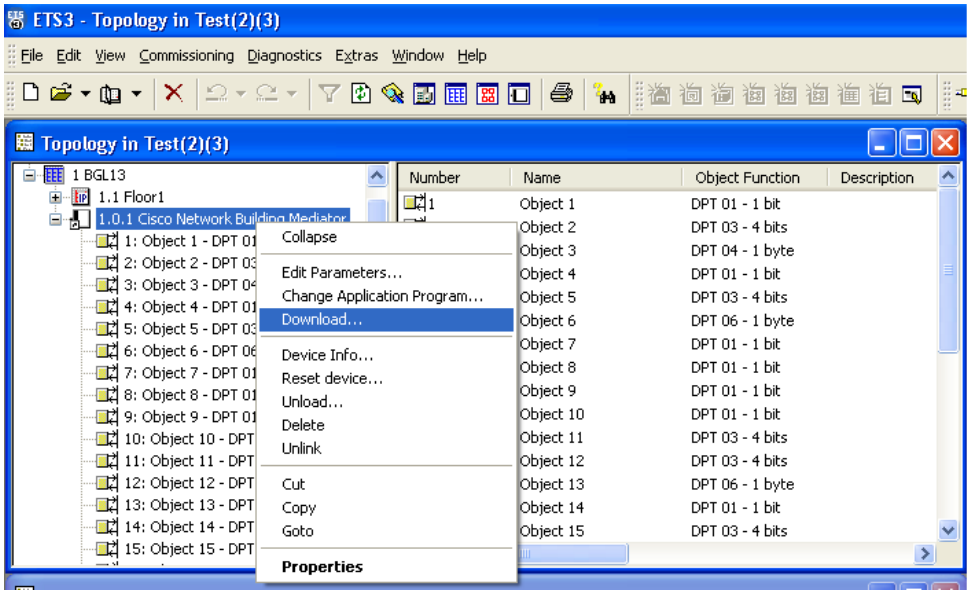


Step 6 In the Phys. Address text box, enter the new physical address of the Mediator.

Step 7 To save your changes and close the dialog box, click **Close**.

Step 8 In the Topology window, right-click the Mediator selected in Step 5, and choose **Download** as shown in Figure 7-3.

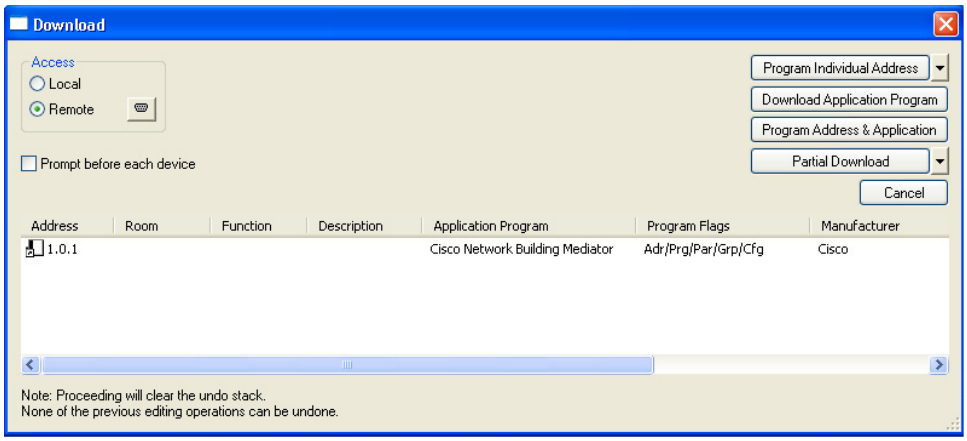
Figure 7-3 Download Option



The Download dialog box appears. (See Figure 7-4.)

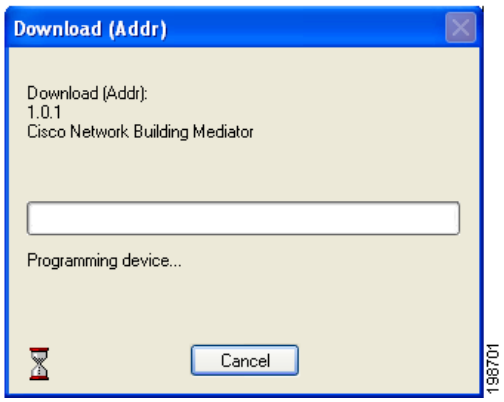
Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 7-4 Download Dialog Box



Step 9 From the list, choose the Mediator, and click **Program Individual Address**. The Download (Addr) dialog box appears displaying the progress of the operation. (See Figure 7-5.)

Figure 7-5 Download (Addr) Dialog Box



On completion of the operation, the physical address of the Mediator is changed.

Note After changing the physical address of the Mediator, ensure that you unselect the **Programming Mode Enable** check box (described in Step 8 of Configuring KNX, page 7-3), and save the configuration.

Step 10 Continue with Downloading KNX Communication Objects, page 7-7.

Downloading KNX Communication Objects

To download KNX communication objects from the ETS tool, perform the following steps:

Step 1 Connect the eth0 port of the Mediator to the switch. The PC on which the ETS tool is installed and the KNX IP router are also connected to the same switch. (See Figure 7-1.)

Step 2 Configure the KNX protocol on the Mediator as described in Configuring KNX, page 7-3, and verify that the KNX stack is ready.

Send documentation comments to cbsbu-docfeedback@cisco.com

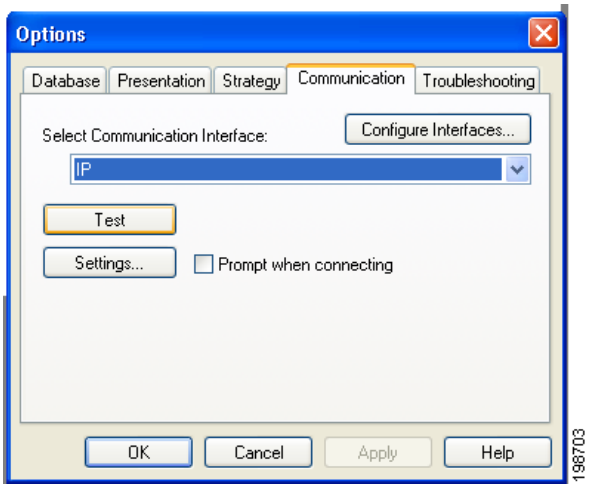
Step 3 Open the ETS tool, and open the project.

Step 4 Choose **Extras** > **Options**. The Options dialog box appears.

Step 5 Click the **Communication** tab. (See Figure 7-6.)

Use this tab to configure the communication interface.

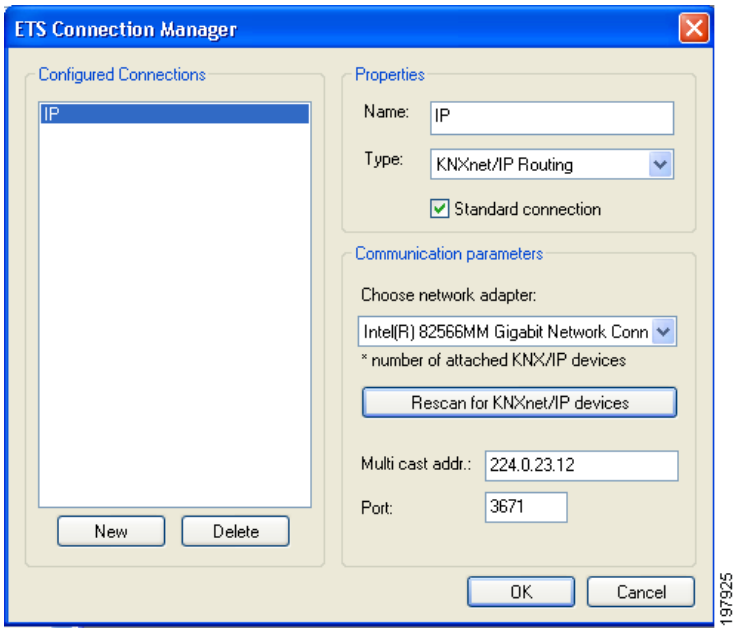
Figure 7-6 Options Dialog Box - Communication Tab



Step 6 Click **Configure Interfaces**.

The ETS Connection Manager dialog box appears. (See Figure 7-7.)

Figure 7-7 ETS Connection Manager Dialog Box



Step 7 In the Properties area, do the following:

a. In the Name text box, enter a name.

b. From the Type drop-down list, choose **KNXnet/IP Routing**. The Mediator only supports KNXnet/IP routing.

Send documentation comments to cbsbu-docfeedback@cisco.com

c. Select the **Standard connection** check box. This check box is selected by default.

Step 8 In the Communication parameters area, do the following:

a. From the Choose network adapter drop-down list, choose the adapter to which the eth1 port is connected.

b. Retain the default values specified in the Multi cast addr and Port text boxes.

Step 9 Click **OK**. The Options dialog box appears. (See Figure 7-6.)

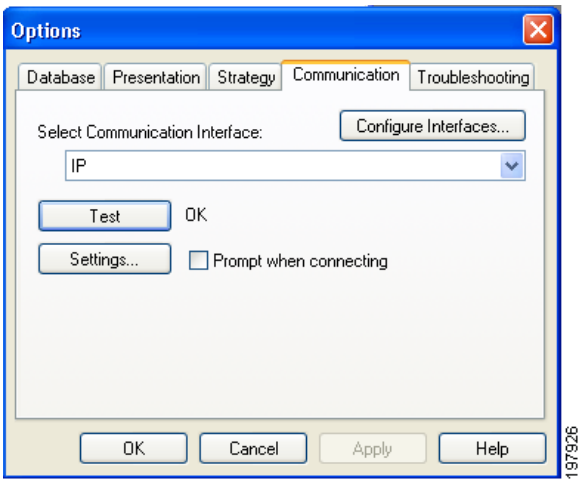
Step 10 From the Select Communication Interface drop-down list, choose an interface.

For example, choose **IP** as shown in Figure 7-6.

Step 11 Click **Test** to test the configuration.

If the configuration is correct, OK appears next to the Test button as shown in Figure 7-8.

Figure 7-8 Options Dialog Box - Communication Tab - Test



Step 12 Click **OK** to close the Options dialog box.

Step 13 In the Topology window, right-click the Mediator, and choose **Download** as shown in Figure 7-3.

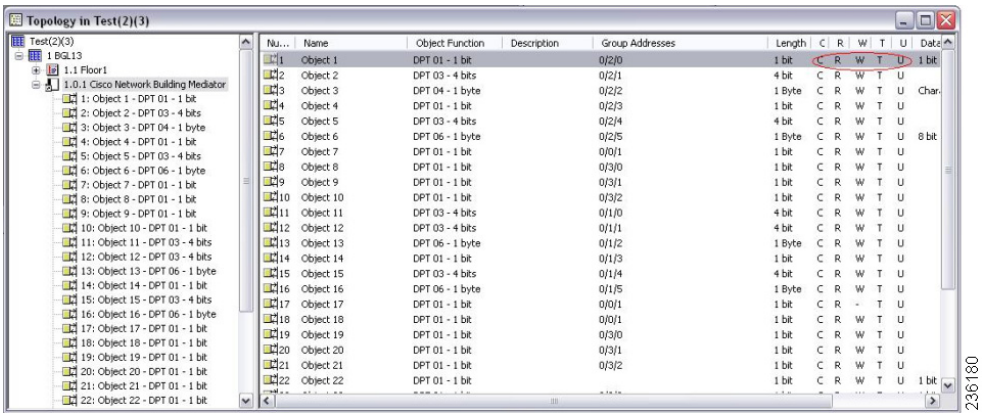
The Download dialog box appears. (See Figure 7-4.)

Step 14 From the list, choose the Mediator with the same physical address as selected in Figure 7-3.

Note Ensure that the U flag for all KNX communication objects are enabled (as shown in Figure 7-9), so that the real-time values of the communication objects are updated to the Mediator from the KNX network after startup of the Mediator.

Send documentation comments to cbsbu-docfeedback@cisco.com

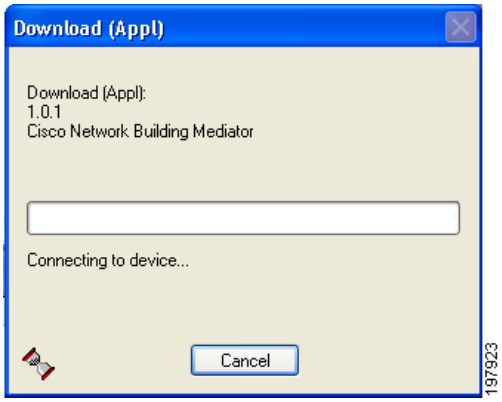
Figure 7-9 Settings for KNX Communication Objects



Step 15 In the Download dialog box (see Figure 7-4), click **Download Application Program**.

The Download (Appl) dialog box appears displaying the progress of the download operation. (See Figure 7-10.)

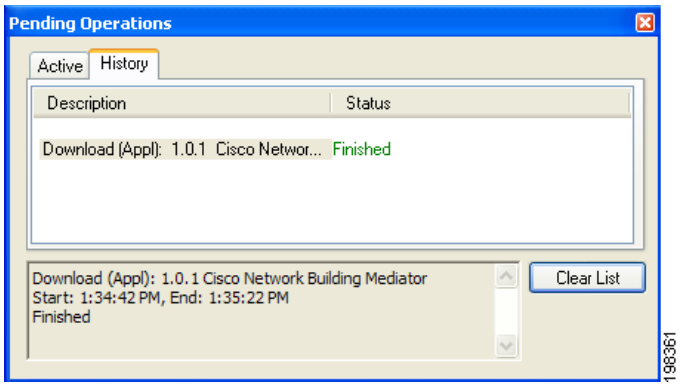
Figure 7-10 Download (Appl) Dialog Box



On completion of the operation, the Pending Operations dialog box appears and displays the status of the operation (see Figure 7-11). The KNX communication objects are downloaded on the Mediator.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 7-11 Pending Operations Dialog Box



Troubleshooting the KNX Configuration

When the Mediator starts up after the KNX protocol has been configured, a series of messages are displayed on the message log (msglog viewer). These messages are useful to verify whether the KNX stack is running, how the downloads and updates from the KNX network are configured on the stack, and whether the updated communication object values that are configured to the stack are correct. Apart from the message log, you can also verify the smooth running of the KNX process using certain commands on the Linux console of the Mediator or use the Mediator Web Client interface.

This section includes the following topics:

Verifying the KNX Stack on the Mediator

After the Mediator Framework has started and the KNX protocol is enabled on the Mediator, you can verify whether the KNX stack is running on the Mediator using the following command on the Linux console:

```
ps -ef | grep knx,……
```

The following output verifies that the KNX is stack is running:

```
[mpxadmin@mediator-05-02217 mpxadmin]$ ps -ef | grep knx
mpxadmin 29155 29118  0 Aug17 ?        00:00:05 [knxstackd]
mpxadmin 29405 29398  0 22:55 ttyp0    00:00:00 grep knx
[mpxadmin@mediator-05-02217 mpxadmin]$
```

Alternatively, on the Mediator web client Node page, navigate to **nodes > services > network**, and verify whether the KNX protocol is in an ON state.

Verifying the KNX Stack RunState

When the Mediator device is started up initially, the following message in the message log verifies the RunState of the KNX stack:

Send documentation comments to cbsbu-docfeedback@cisco.com

```
KNX RunState after initializing knx stack is 1
```

Explanation The RunState of 1 indicates that the KNX stack is active and running.

Recommended Action If you do not see this message in the message log, wait for a certain period of time till the stack becomes active. However, if the message does not appear for a long time, restart the Mediator Framework.

Verifying Persistent Data on the KNX Stack

The Mediator verifies whether persistent data exists on the KNX node tree database in the /var/mpx/config/persistent/knxconfig.bin directory.

Before KNX data has been downloaded from the ETS tool to the Mediator, no persistent data exists, hence the Mediator moves onto the next action.

After KNX data has been downloaded from the ETS tool to the Mediator, the Mediator programs the KNX stack with the available persistent data. The following message in the message log verifies this action:

```
KNX stack programmed with configuration data successfully 1
```

Explanation 1 indicates that the KNX stack configuration was successful.

Verifying KNX Communication Objects on the Mediator

When the KNX stack is ready to discover the KNX communication objects, the following message appears in the message log:

```
KNX stack is ready discovering all objects
```

When KNX communication objects are not downloaded on the Mediator, the Mediator waits for the download to occur.

When KNX communication objects are downloaded on the Mediator, the Mediator discovers all existing KNX communication objects from the available persistent data. The following message in the message log verifies this action:

```
KNX configured objects count: 30
```

Explanation 30 indicates the number of communication objects existing on the KNX network.

After the successful download of the KNX communication object database from the ETS tool to the Mediator, the following messages appear in the message log:

Send documentation comments to cbsbu-docfeedback@cisco.com

```
KNX processindication RESET_IND 4
```

Explanation This message notifies you that the Mediator has received a RESET indication from the ETS tool, and has received the downloaded KNX database.

```
KNX stack programmed successfully and saved in persistent data 1
```

Explanation This message notifies you that the downloaded database is successfully configured.

```
KNX configured objects count: 30
```

Explanation This message notifies you about the number of KNX communication objects that are available on the KNX network.

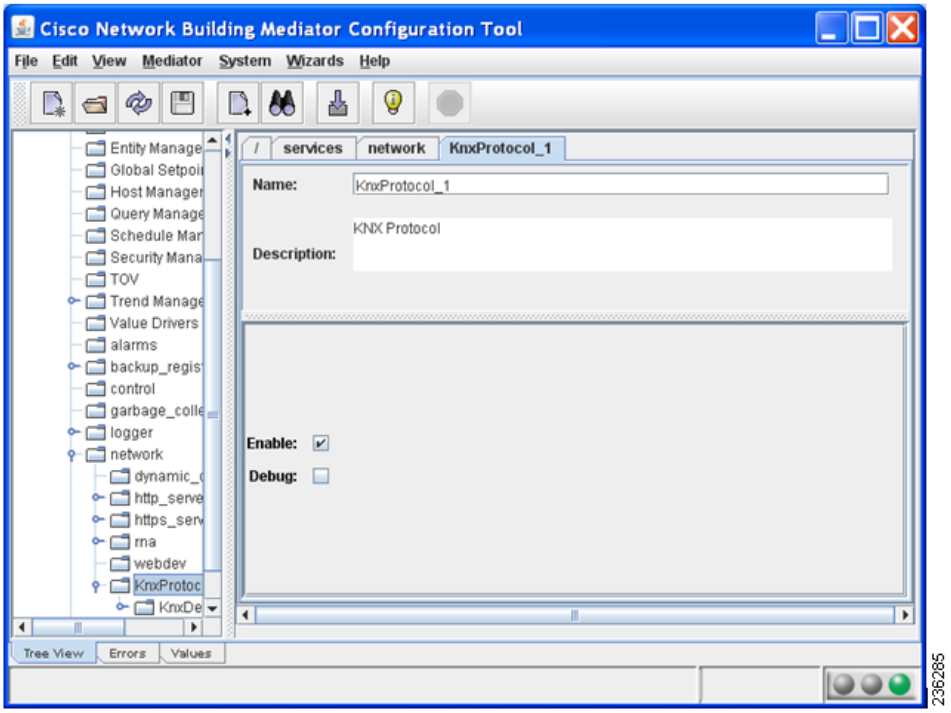
When changing or setting KNX communication objects from the ETS tool to the Mediator, the Mediator reflects this change to the KNX network by multicasting the telegrams.

Similarly, when a change occurs in the KNX network for a particular communication object, the following message appears in the message log:

```
broadway Object Number 1, changed to 1.
```

Note This message appears only if debugging is enabled. To enable debugging, in the configTOOL node tree pane, expand the node tree, and choose **services > network > KnxProtocol** as shown in Figure 7-12. Then, select the **Debug** check box.

Figure 7-12 configTOOL - KNX Protocol



Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 8

Getting Started with Mediator Web Client

The Mediator web client is a web-based GUI application that provides easy access to Mediator applications from a remote workstation. The web client displays real-time, onsite data and allows you to remotely monitor and manage the Mediator from a web browser.

You can view current conditions at a site, query and graph trend data points, export trend data, remotely edit system conditions and behavior by adjusting schedules, initiating overrides, changing set points, directly access error logs, alarms, events, and so on, from your work station.

The Mediator web client is a web application that allows you to manage a Mediator. You can connect to the Mediator web client from any PC on a local network, on a remote network, or over the Internet using a standard web browser.

This chapter includes the following sections:

System Requirements

Before you access the Mediator web client, you must verify that your system meets the following recommended prerequisites:

- Browser—Internet Explorer 7, 8 or Mozilla Firefox 3.5 and later
- Browser plug-in—Adobe Flash Player 9 or later

Launching Mediator Web Client

To start the Mediator web client, perform the following steps:

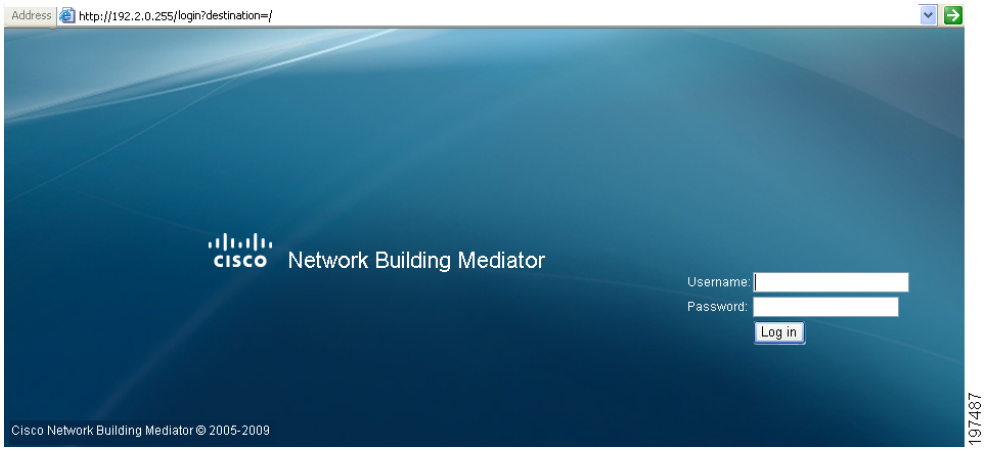
Step 1 Enter the hostname or the IP address of the Mediator in the Address text box of the browser.

Step 2 Press **Enter**.

The Mediator web client login appears as shown in Figure 8-1.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 8-1 Mediator Web Client Login Page



Step 3 Enter the username and password for the Mediator, and click **OK**.

The Mediator web client homepage appears in the Internet browser window.

Understanding Mediator Web Client

The Mediator web client is a software suite used to program and configure the Mediator and includes several web-based services that reside on the Mediator. All the software and instructions you need to set up your Mediator system are built into the web client.

Because the Mediator web client uses Dynamically Generated HTML (DGHTML) technology, you can reconfigure the Mediator without requiring a reboot after configuring or editing operations.

The Mediator web client homepage appears as shown in Figure 8-2.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 8-2 Mediator Web Client Homepage

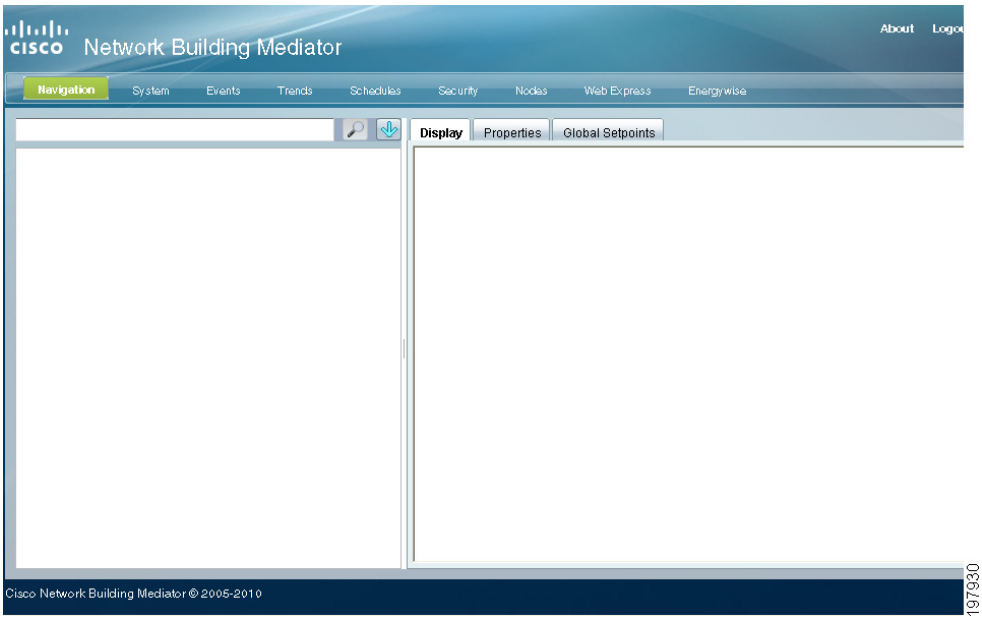


Table 8-1 describes the Mediator web client components.

Table 8-1 Mediator Web Client Components

Component	Description
Navigation	Displays the navigation tree and real-time data of the devices attached to the Mediator.
System	Displays information about the Mediator and allows you to customize the Mediator properties.
Events	Creates and manages alarms and exporters.
Trends	Configures and manages trends, displays them graphically, and embeds the graphics in web pages.
Schedules	Creates and manages schedules.
Security	Defines and manages users and roles in the Mediator.
Nodes	Inspects node values in the system.
Web Express	Creates and customizes HTML monitor pages.
Energywise	Measures and monitors power consumed by Energywise.

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 9

Managing Events

This chapter includes the following sections:

About Events

The Mediator web client integrates with the Mediator to enable alarm and event notification. The Mediator web client enables you to define alarm conditions that, when met, display alarm events in the web client and deliver e-mail alerts. You can also use open source RSS technology to be notified of the change in alarm states.

This section covers the following topics:

About Event Manager

The Event Manager enables you to view, filter, and sort all the events raised by an alarm on a Mediator.

The Event Manager tab appears as shown in Figure 9-1.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 9-1 Event Manager Tab

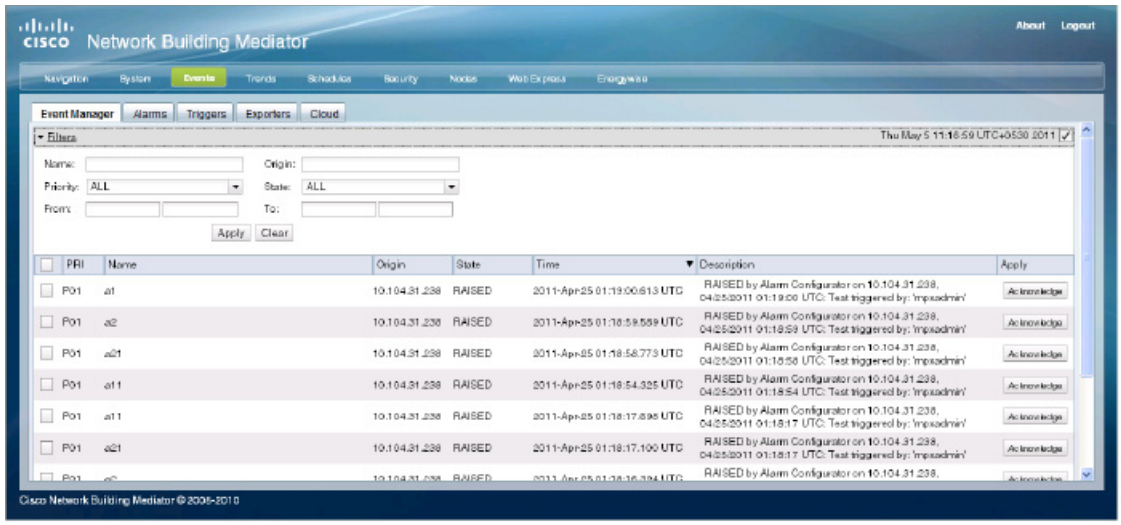


Table 9-1 lists the main text boxes that appear on the Event Manager tab. When you click **FILTERS**, you can use these text boxes to filter and sort events.

Table 9-1 Event Manager Text Boxes

Text Box	Description
Name	Displays the name of the event.
Origin	Displays the IP address/hostname of the Mediator that raised the event.
Priority	Displays the priority of the event.
State	Displays the event state.
Time	Displays the time according to the time zone of the browser where the event manager is being viewed.

A timestamp is displayed on the tab. This timestamp displays the date and time of the browser where the Event Manager is being viewed. Unselect the check box next to the timestamp to stop receiving event updates on the screen.

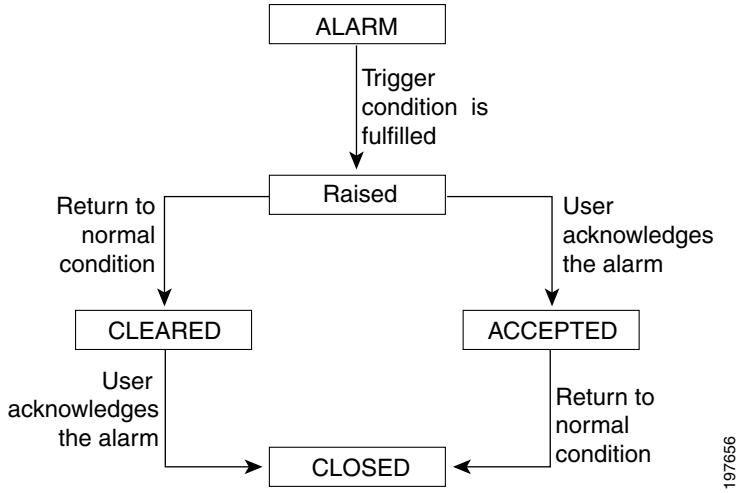
Each event passes through a series of states in its life cycle.The various states are as follows:

- Raised—An event is raised when the trigger condition for an alarm is fulfilled. A raised event can go to the accepted or cleared state. The raised state is the initial state of every event.
- Accepted—An event moves to the accepted state from the raised state if you acknowledge it.
- Cleared—An event moves from the raised state to the cleared state if the trigger condition becomes normal after acknowledging the event.
- Closed—An accepted event moves to the closed state if the trigger condition becomes normal. A cleared event can become closed if you acknowledge it. This is the final state of every event.

Figure 9-2 illustrates the various states in the event life cycle.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 9-2 Event State Life Cycle



The administrator should acknowledge each event after the appropriate action has been taken. You can acknowledge events individually by clicking the Acknowledge button in the Apply column for that event. To acknowledge multiple events, select the check box next to the event that you want to acknowledge, and click the Acknowledge button at the bottom of the page.

Note Only users who are assigned the System Administrator role or similar privileges (typically the mpxadmin user) can acknowledge alarm events.

To configure Event Manager, see Using Event Manager, page 9-8.

About Alarms

The Alarms tab enables you to manage various alarms across a Mediator. It enables you to view the list of alarms, to acknowledge each alarm, and to clear and delete alarms. The Alarms tab acts as the single interface from which all alarms can be managed.

The **Alarms** tab appears as shown in Figure 9-3.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 9-3 Alarms Tab

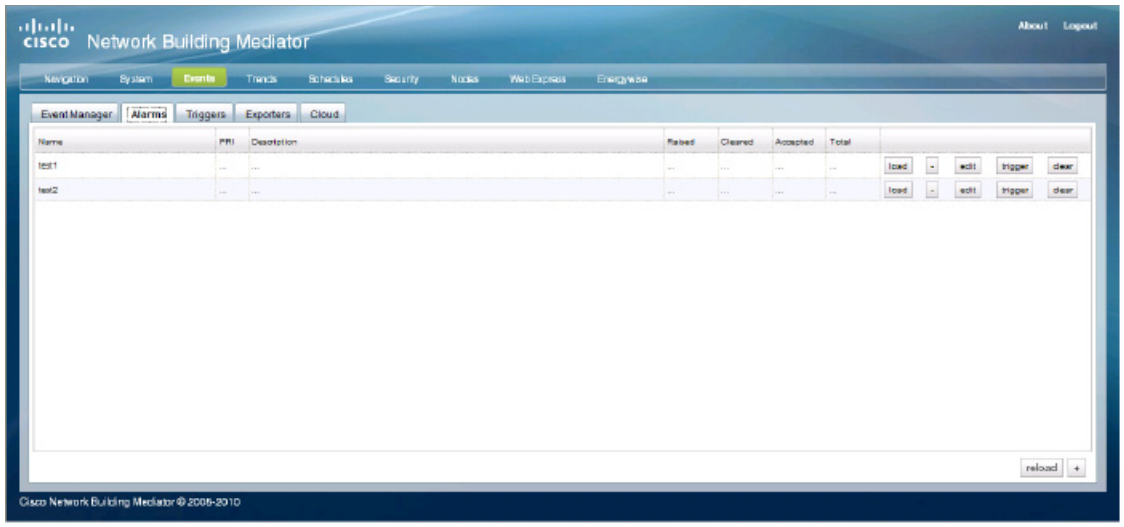


Table 9-2 describes the buttons shown in the **Alarms** tab.

Table 9-2 Alarms Tab - Description

Button	Description
load	Displays the alarm details.
+	Enables you to create new alarms.
-	Enables you to delete existing alarms.
edit	Enables you to edit existing alarms.
trigger	Enables you to trigger existing alarms.
clear	Enables you to clear raised alarms.

To learn more about alarms, see Managing Alarms, page 9-9.

About Triggers

Triggers are attached to an alarm and logical conditions are defined which, when met, send the alarm to the Mediator web client and trigger the exporter of the alarm.

The **Triggers** tab appears as shown in Figure 9-4.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 9-4 Triggers Page

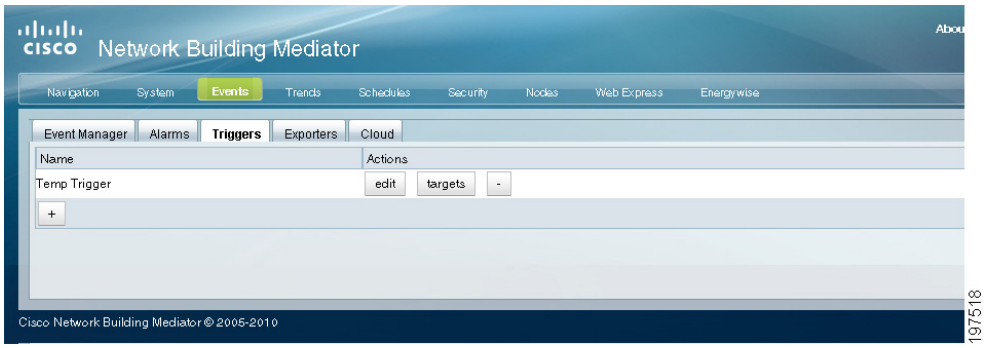


Table 9-3 describes the buttons shown in the **Triggers** tab.

Table 9-3 Triggers Tab - Description

Button	Description
+	Allows you to add triggers.
-	Allows you to delete triggers.
edit	Allows you to edit the trigger settings.
targets	Allows you to specify targets for triggers. To know more about targets, see About Targets, page 9-5.

This section includes the following topics:

About Targets

Targets are the alarms that a given trigger activates or clears depending on the input. In comparison triggers, the target alarms are triggered when the condition transitions to true, and cleared when the condition transitions to false. In bound triggers, the target alarms are triggered when the input alarm is triggered, and cleared when the input alarm is cleared.

If you do not configure targets for a trigger, the trigger will not have an impact on the alarms of the system.

Types of Alarm Triggers

There are two types of alarm triggers:

Comparison trigger—A comparison trigger uses the value of a point node as the input and compares the node value with a constant preset value. Depending on the configuration, if the point value is greater than or less than the constant value, the trigger activates the target alarms.

Bound trigger—A bound trigger forms a link between an input alarm and one or more output alarms. This trigger is a passive mechanism compared to the comparison trigger. The bound trigger activates the output alarms when the input alarm is triggered and clears the output alarms when the input alarm is cleared. The functionality of bound triggers allows you to name the alarm such that you can identify information such as location and events from the export content of the alarm.

Send documentation comments to cbsbu-docfeedback@cisco.com

To create and manage triggers, see Managing Triggers, page 9-12.

About Alarm Exporters

You can configure an exporter to be attached to an alarm and set up an exporter for e-mail alerts. Each alarm exporter is configured to send an e-mail notification when one or more alarms change their state.

The **Exporters** tab appears as shown in Figure 9-5.

Figure 9-5 Exporters Tab

Table 9-4 describes the buttons shown in the **Exporters** tab.

Table 9-4 Exporters Tab - Description

Button	Description
+	Allows you to add exporters.
-	Allows you to delete exporters.
edit	Allows you to edit the alarm exporter settings.
sources	Allows you to add alarm sources. For more information on sources, see About Sources, page 9-6.
formatter	Allows you to edit the exporter formatter settings. For more information on formatters, see About Formatters, page 9-7.
transporter	Allows you to add alarm transportes. For more information on transoporters, see About Transporters, page 9-7.

This section includes the following topics:

- About Sources, page 9-6
- About Formatters, page 9-7
- About Transporters, page 9-7

About Sources

An exporter source is a configured alarm that causes an alarm exporter to be exported. You can choose a specific alarm as a source or you can choose the Alarm Manager. If you select the Alarm Manager, an alarm export occurs whenever an alarm event occurs. If you choose specific alarms as an exporter source, you receive e-mail notifications only when the selected source alarms occurs.

Send documentation comments to cbsbu-docfeedback@cisco.com

You should also specify which state transitions should trigger the alarm exports. The exporter source can be configured to trigger an alarm for all or some of the four alarm states (raised, cleared, accepted, and closed). For example, you can configure the alarm exporter to send e-mail notifications only when an alarm is raised.

About Formatters

The formatter function allows you to rename the formatter node.

About Transporters

You can configure the SMTP settings for the alarm exporter and send e-mail notifications using the exporter transporter function.

To create and manage alarm exporters, see Managing Alarm Exporters, page 9-14.

About Global Alarms

Alarms that are raised on a Mediator can be monitored using the Alarms tab in Event Manager. However, when there are multiple Mediators in a single geographical location, the Global Alarms functionality enables you to create *cloud formations* of multiple *cloud peers* (Mediators), so that you can easily view and act on alarms that are raised from any of the cloud peers in the cloud formation.

When there are multiple cloud peers that are located in different geographical locations, the Global Alarms functionality enables you to configure a *cloud portal* (Mediator Manager) to participate in a cloud formation. The cloud portal facilitates the centralized management of alarms across the cloud peers in a cloud formation.

Essentially, a cloud formation refers to a set of cloud peers (Mediators) and a cloud portal (Mediator Manager) that participate in a cloud.

The Cloud Manager is a service that runs on a Mediator and Mediator Manager, and facilitates in creating global alarms. The purpose of the Cloud Manager is to support efficient and flexible propagation of events throughout a finite set of cloud peers in a cloud.

A request handler, the Cloud Handler, handles the receipt of incoming events and dispatches them to the local Cloud Manager. Each Cloud Manager is responsible for notifying the target cloud peers within the cloud. This is done for all the events regardless of whether the event being propagated is local to the Cloud Manager, or one received from another cloud peer within the cloud.

The peers that form a cloud enable you to view the details of all the peers in that cloud from any peer in the cloud. You can open any Mediator in the cloud and monitor the details of all the other peers in that cloud.

A cloud formation can be modified by making changes to any cloud peer within the cloud. The peers communicate and synchronize among themselves to reflect the updated cloud structure.

To remove a cloud peer (for example, A) from a cloud that contains more than one peer, you need to log in to any of the other peers in the cloud (for example, B) and delete A from the cloud formation. The peer, B, in turn communicates this change to the other peers in the cloud. Therefore, the simple deletion of peer A from peer B results in peer A ceasing to be a part of the cloud. Peer A could now also be considered as a cloud in which it is the only participating peer.

Given a cloud with cloud peers A, B, and C, adding a fourth cloud peer, D, results in all four cloud peers having a cloud of all four cloud peers. It is not possible for cloud peers to have formations that differ from the formation of other cloud peers within the same cloud.

Send documentation comments to cbsbu-docfeedback@cisco.com

Each cloud can have only one cloud portal configured for it. However, multiple clouds can share a single cloud portal. If a cloud portal is overridden from any one cloud peer, it also gets overridden from all the other peers that are participating in that cloud.

For more information on cloud formation scenarios, see Cloud Formation Scenarios, page 9-22.

The **Cloud** tab appears as shown in Figure 9-6.

Figure 9-6 Cloud Tab

About RSS Feeds

RSS (Really Simple Syndication) is an open communication protocol that allows you to subscribe to an XML-based data feed from a source such as a news or weather feed. The Mediator supports RSS data feeds and uses RSS to send events to the Events pane in a Mediator. An RSS user is also called a feed reader.

To learn more about RSS feeds, see Checking RSS Feeds, page 9-31.

Using Event Manager

This section describes the Event Manager and includes the following topics:

Filtering Events

To filter events in Events, perform the following steps:

Step 1 In the web client homepage, click **Events**.

Step 2 Click the **Event Manager** tab.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Event Manager tab appears as shown in Figure 9-1.

Step 3 Click **FILTERS**.

Step 4 Filtering can be performed based on the values you enter in the various text boxes (see Table 9-1):

- Name—Type the name of the event that you want to see.
- Origin—Type the IP address/hostname from where the event has been raised.
- Priority—Choose the priority of the event.
- State—Choose the state of the event.
- From—Type the date you want to filter the event.

  In the next text box, type the time you want to filter the event. If you execute the filter without specifying the time, this text boxis auto-populated with the minimum time of that day (12:00:00 AM).
- To—Type the date you want to filter the event.

  In the next text box, type the time you want to filter the event. If you execute the filter without specifying the time, this text box is auto-populated with the maximum time of that day (11:59:59 PM).

Step 5 Click **Apply** to execute the filter.

The text boxes work in an AND function. A list of events that satisfies all the criteria will be displayed.

The events are sorted by time and displayed as shown in Figure 9-1.

Step 6 (Optional) Click **Clear** to clear the filtering. This displays the original events list sorted by time.

The Download Log button at the bottom of the tab allows you to download an event audit log. This log contains entries for each event, showing its state transitions.

Sorting Events

To sort events in Events, perform the following steps:

Step 1 In the web client homepage, click **Events**.

Step 2 Click the **Event Manager** tab.

The Event Manager tab appears as shown in Figure 9-1.

Step 3 Events can be sorted alphabetically in ascending or descending order. Click the desired column heading to sort the list of events. For example, if you wish to sort the events by Time, click the Time column heading.
Clicking the column heading again will reverse the sorting order. If you click the column heading a third time, the sorting is cleared and the initial time-sorted list is displayed.

Managing Alarms

This section describes how to create alarms on a Mediator and includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Creating Alarms

To create an alarm, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Alarms** tab.

The Alarms tab appears as shown in Figure 9-3.

Step 3 Click the plus symbol (+) to create an alarm.

The Create New Alarm dialog box appears. In the Create New Alarm dialog box, do the following:

a. In the Name text box, enter a name for the alarm.

b. From the Priority drop-down list, choose the priority of the alarm.

c. Enter the values in the Max raised, Max cleared, and Max accepted text boxes.

d. In the Description text box, enter a description for the alarm.

e. Click **Commit**.

The Alarms tab reappears. The new alarm is added to the bottom of the list.

Editing Alarms

To edit an existing alarm, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Alarms** tab.

The Alarms tab appears with all the created alarms as shown in Figure 9-3.

Step 3 Click **edit** next to the alarm that you want to edit.

The Edit Alarm dialog box appears.

Step 4 Change the values in the text boxes and click **Commit**.

The Alarm tab reappears with the changed values.

Send documentation comments to cbsbu-docfeedback@cisco.com

Triggering Alarms

An alarm gets triggered when the trigger condition for that alarm is fulfilled, that is, the trigger condition that is set becomes True.

To trigger an existing alarm, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Alarms** tab.

The Alarms tab appears with all the created alarms as shown in Figure 9-3.

Step 3 Click **trigger** next to the alarm that you want to trigger.

An event has been raised by the alarm, the system administrator needs to take appropriate action.

For more information about event states, see Using Event Manager, page 9-8.

Clearing Alarms

After an alarm is triggered, when the trigger condition becomes False, the alarm is cleared.

To clear a raised alarm, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Alarms** tab.

The Alarms tab appears with all the created alarms as shown in Figure 9-3.

Step 3 Click **clear** next to the raised alarm that you want to clear.

For more information about event states, see Using Event Manager, page 9-8.

Deleting Alarms

To delete an existing alarm, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Alarms** tab.

The Alarms tab appears with all the created alarms as shown in Figure 9-3.

Step 3 Click the minus symbol (-) to delete an existing alarm.

A confirmation message appears asking you to confirm the deletion of the alarm.

Step 4 Click **Yes**.

The Alarm tab reappears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Managing Triggers

This section describes how to manage triggers and includes the following topics:

Creating Triggers

To create a trigger, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Triggers** tab.

Step 3 Click the plus symbol (**+**) button to create a trigger.

The Create new Trigger dialog box appears.

Step 4 In the Create new Trigger dialog box, perform the following steps:

a. From the Type drop-down list, choose the type of trigger.

b. In the Name text box, enter a name for the trigger.

c. Click **Commit**.

The Triggers tab reappears. The new trigger is added to the bottom of the list.

Editing Triggers

Based on the type of trigger that you configured in Step 4 of Creating Triggers, page 9-12, you can choose one of the following procedures to edit the triggers:

Editing Comparison Triggers

To edit a comparison trigger, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Triggers** tab.

Step 3 Click **edit** next to the comparison trigger that you want to edit.

The Edit Trigger dialog box appears.

Step 4 In the Edit Trigger dialog box, perform the following steps:

a. In the Name text box, rename the trigger.

Send documentation comments to cbsbu-docfeedback@cisco.com

b. From the Alarm when drop-down list, choose a trigger level.

c. Next to the Input node text box, click the ellipsis (...) button.

The Node Selector dialog box appears.

In the Node Selector dialog box, perform the following steps:

1. Select a node from the drop-down list. The file path appears in the Node location text box.
2. Click **SAVE**.

The Node Selector dialog box closes.

d. In the Constant value text box, enter a threshold value for the trigger.

e. In the Poll period text box, enter a time period (in seconds) of the polling interval.

Note The poll period refers to the frequency that the Mediator evaluates the trigger condition. Because evaluating the trigger conditions consumes Mediator resources, you should set the poll period to a minimum of two seconds and to a higher value if there are many triggers defined.

f. In the Hysteresis text box, specify the amount of time the trigger should wait before clearing the alarm.

g. In the Alarm delay text box, specify the amount of time the trigger should wait before raising the alarm.

Step 5 Click **Commit**.

The Triggers tab reappears. The edited trigger is available in the list.

Editing Bound Triggers

To edit a bound trigger, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Triggers** tab.

Step 3 Click **edit** next to the bound trigger that you want to edit.

The Edit Trigger dialog box appears.

Step 4 In the Edit Trigger dialog box, perform the following steps:

a. In the Name text box, rename the trigger.

b. In the Source text box, click the ellipsis (...) button.

The Node Selector dialog box appears.

In the Node Selector box, perform the following steps:

1. Select a source under the /services/Alarm Manager path.

   The file path appears in the Node location text box

2. Click **SAVE**.

The Node Selector dialog box closes.

Step 5 Click **Commit**.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Triggers tab reappears. The edited trigger is available in the list.

Configuring Targets

To configure a target, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Triggers** tab.

Step 3 Click **targets** next to the desired trigger.

The Trigger Targets dialog box appears.

Step 4 In the Trigger Targets dialog box, perform the following steps:

a. Select the check box to select the desired alarm.

b. Click **Commit**.

The Triggers tab reappears.

Deleting Triggers

To delete a trigger, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Triggers** tab.

Step 3 Click the minus symbol (-) button next to the trigger that you want to delete.

The Delete Trigger dialog box appears prompting you to confirm the operation.

Step 4 Click **commit**.

The Triggers tab reappears. The trigger is removed from the list.

Managing Alarm Exporters

This section describes how to manage alarm exporters and covers the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Creating Alarm Exporters

To create an alarm exporter, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Exporters** tab.

The Exporters tab appears.

Step 3 Click the plus symbol (+) button to create an exporter.

The Create new Exporter dialog box appears.

Step 4 In the Create new Exporter dialog box, perform the following steps:

a. In the Name text box, enter the name for the exporter.

b. From the Format drop-down list, choose the message format from the following options:

- Standard message
- Named value
- XML alarm schema

c. From the Transport drop-down list, choose the transport mechanism from the following options:

- SMTP email
- FTP
- SFTP

d. Click **Commit**.

The Exporters tab reappears. The new exporter appears at the bottom of the list.

Editing Alarm Exporters

To edit the alarm export, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Exporters** tab.

Step 3 Click **edit** next to the exporter that you want to edit.

The Edit Alarm Logger dialog box appears.

Step 4 In the Edit Alarm Logger dialog box, perform the following steps:

a. In the Name text box, rename the exporter.

b. Click **Commit**.

The Exporters tab reappears. The edited exporter is available in the list.

Send documentation comments to cbsbu-docfeedback@cisco.com

Adding Exporter Sources

To add the exporter source, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Exporters** tab.

Step 3 Click **sources** next to the exporter that you want to edit.

The Export Triggers dialog box appears.

Step 4 In the Export Triggers dialog box, perform the following steps:

a. From the Source drop-down list, choose the alarm source. Alarm Manager is the default.

b. Select the check boxes for the alarm states that you want the exporter to trigger.

c. Click **commit**.

The Success dialog box, confirming the operation is successful, appears.

d. Click **OK**.

Editing Exporter Formatter

To edit the exporter formatter, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Exporters** tab.

Step 3 Click **formatter** next to the exporter that you want to edit.

The Edit Alarm Logger dialog box appears.

Step 4 In the Name text box, rename the formatter. The default name is Log Formatter.

Note We recommend that you do not change the default name.

Step 5 Click **Commit**.

Adding Exporter Transporter

Depending on the transport mechanism you select when creating an alarm exporter, you can add the following exporter transporters:

- SMTP Exporter Transporter
- FTP Exporter Transporter
- SFTP Exporter Transporter

Send documentation comments to cbsbu-docfeedback@cisco.com

SMTP Exporter Transporter

To add an SMTP exporter transporter, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Exporters** tab.

Step 3 Click **transporter** next to the exporter that you want to edit.

The Edit Transporter dialog box appears.

Step 4 In the Edit Transporter dialog box, perform the following steps:

a. In the Name text box, leave the default name.

b. Select the **Authenticate** check box if the e-mail server requires authentication.

c. In the User name text box, enter the username for the e-mail account on the mail server.

d. In the Password text box, enter the password of the mail server.

e. In the Custom domain text box, enter the e-mail message heading. You can leave this text box blank.

f. In the Recipients text box, enter e-mail addresses of the recipients and separate multiple addresses with commas.

g. Select the **As attachment** check box if the e-mail message must be sent as an attachment.

h. In the Subtype text box, enter html.

i. In the Host text box, enter the hostname or IP address of the e-mail server.

j. In the Subject text box, enter a description. This is the message that will appear in the e-mail.

k. In the Timeout (secs) text box, enter an upper limit for how long an export will attempt to send an e-mail.

l. In the Port text box, leave the port number as 25, which is the default port for SMTP.

m. In the Sender text box, enter an e-mail address. You can enter any properly formed e-mail address in this text box.

Step 5 Click **Commit**.

FTP Exporter Transporter

To add an FTP exporter transporter, perform the following steps:

Note Before performing the steps outlined in the procedure below, ensure that a destination FTP server is set up.

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Exporters** tab.

Step 3 Click **transporter** next to the exporter that you want to edit.

The Edit Transporter dialog box appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 In the Edit Transporter dialog box, perform the following steps:

a. In the Name text box, leave the default name.

b. In the Host text box, enter the IP address of your FTP client.

c. In the Port text box, enter the port number that is specified in your FTP client.

d. In the Directory text box, specify a shared local folder where the XML file with the alarm information will be exported.

e. In the User name text box, enter the username to log into your machine.

f. In the Password text box, enter the password to log into your machine.

g. In the Timeout (secs) text box, enter an upper limit for how long the export will be attempted.

h. In the File prefix text box, enter the file name for the XML file.

i. In the File suffix text box, enter the file name extension.

j. In the Name scheme text box, enter timestamp, so that the XML file records the actual time the alarm is generated.

k. Select the **Passive Mode** check box if you want to complete the FTP transport in passive mode. If you unselect this check box, active mode is used. This setting must correspond with the setting that is specified on the destination FTP server.

l. Select the **File append** check box to append a local file to a file on the remote computer, or to create a new file each time the data is exported.

Step 5 Click **Commit**.

SFTP Exporter Transporter

You can add an SFTP exporter transporter in much the same way as an FTP exporter transporter. For more information, see FTP Exporter Transporter, page 9-17.

Deleting Exporter Transporter

To delete the exporter transporter, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Exporters** tab.

Step 3 Click the minus symbol (-) button next to the exporter that you want to delete.

The Delete Alarm Logger dialog box appears prompting you to confirm the operation.

Step 4 Click **commit**.

The Exporters tab reappears. The exporter is deleted from the list.

Configuring XML-FTP Alarm Exporters

This section includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Creating XML-FTP Alarm Exporters

To create an XML-FTP alarm exporter, perform the following steps:

Step 1 In the Mediator web client, click **Events**.

Step 2 Click the **Exporters** tab.

The Exporters tab appears.

Step 3 Click the plus symbol (+) button to create a new exporter.

The Create new Exporter dialog box appears.

Step 4 In the Create new Exporter dialog box, perform the following steps:

a. In the Name text box, enter the name for the exporter.

b. From the Format drop-down list, choose **XML alarm schema**.

c. From the Transport drop-down list, choose **FTP**.

d. Click **Commit**.

The Exporters tab reappears. The new XML-FTP alarm exporter appears at the bottom of the list.

Note After creating an alarm exporter, you can only modify its name as outlined in Editing Alarm Exporters, page 9-15. You cannot modify its format and transport mechanism.

Step 5 Continue with Adding XML-FTP Exporter Sources, page 9-19.

Adding XML-FTP Exporter Sources

To add an XML-FTP alarm exporter source, perform the following steps:

Step 1 Create the XML-FTP alarm exporter as outlined in Editing Alarm Exporters, page 9-15.

Step 2 Add the exporter source as outlined in Adding Exporter Sources, page 9-16.

Step 3 Continue with Adding XML-FTP Exporter Transporters, page 9-19.

Adding XML-FTP Exporter Transporters

To add an XML-FTP exporter transporter, perform the following steps:

Note The configuration outlined in this section can only be performed using the Mediator web client. You cannot use the configTOOL to do so.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 1 Create the XML-FTP alarm exporter as outlined in Editing Alarm Exporters, page 9-15.

Step 2 Create the FTP exporter transporter as outlined in FTP Exporter Transporter, page 9-17.

When the alarm is generated, the XML file containing the alarm information is exported to the shared local folder on your machine.

Managing Global Alarms

This section includes the following topics:

Creating a Cloud Formation

This section includes the following topics:

Adding a Peer

To add a peer, perform the following steps:

Step 1 In the web client homepage, click **Events**.

Step 2 Click the **Cloud** tab.

The **Cloud** tab appears as shown in Figure 9-6.

The tab displays Portal (if configured) on top, followed by the IP address of the Mediator that you are currently logged into, and any existing peers in the cloud.

Step 3 Click the plus (**+**) symbol to add a peer.

The Create new Peer/Portal dialog box appears.

Step 4 From the Type drop-down list, choose **Peer**.

Step 5 In the Name text box, enter the IP address of the Mediator that you want to add as a peer.

Step 6 Click **Commit**. The added peer appears in the list on the Cloud tab.

Adding a Portal

To add a portal, perform the following steps:

Step 1 In the web client homepage, click **Events**.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 2 Click the **Cloud** tab.

The **Cloud** tab appears as shown in Figure 9-6.

The tab displays Portal (if configured) on top, followed by the IP address of the Mediator that you are currently logged into, and any existing peers in the cloud.

Step 3 Click the plus (+) symbol to add a portal.

The Create new Peer/Portal dialog box appears.

Step 4 From the Type drop-down list, choose **Portal**.

Step 5 In the Name text box, enter the IP address of the Mediator Manager that you want to add as a portal.

Step 6 Click **Commit**. The added portal appears at the top of the list on the Cloud tab.

Note There is currently no capability in a portal to determine the clouds or the peers in a cloud that are associated to it. This limitation will be addressed in subsequent releases.

Deleting a Cloud Formation

This section includes the following topics:

Deleting a Peer

To delete a peer from a cloud formation, perform the following steps:

Step 1 Click the minus (-) symbol next to the Mediator that you want to remove from the cloud. A confirmation message appears to confirm the deletion.

Step 2 Click **Commit**. The peer is removed from the list on the Cloud tab.

Deleting a Portal

To delete a portal from a cloud formation, perform the following steps:

Step 1 Click the minus (-) symbol next to the Mediator Manager that you want to remove from the cloud. A confirmation message appears to confirm the deletion.

Step 2 Click **Commit**. The portal is removed from the list on the Cloud tab.

Send documentation comments to cbsbu-docfeedback@cisco.com

Cloud Formation Scenarios

The Cisco Network Building Mediator (Mediator) supports cloud formation to group a set of Mediators into a logical entity known as a *cloud*. Each entity in a cloud is known as a *peer*. For example, a cloud is formed when Mediator X is added to Mediator Y as its peer. When this happens, Mediator X and Mediator Y become a part of a single cloud. There can be several clouds in the network, each consisting of one or more Mediators. However, at a given point in time, a Mediator can only participate in one cloud.

Peers in a cloud continuously synchronize with each other by exchanging information. Typically, they exchange information about alarm events and their corresponding states. For example, when a cloud is formed by adding Mediator X to Mediator Y as its peer, all alarm events from Mediator X are visible in Mediator Y and vice versa. For more information on cloud formation, see About Global Alarms, page 9-7.

This section describes the following scenarios in cloud formation and includes the following topics:

Cloud Formations Between Standalone Mediators

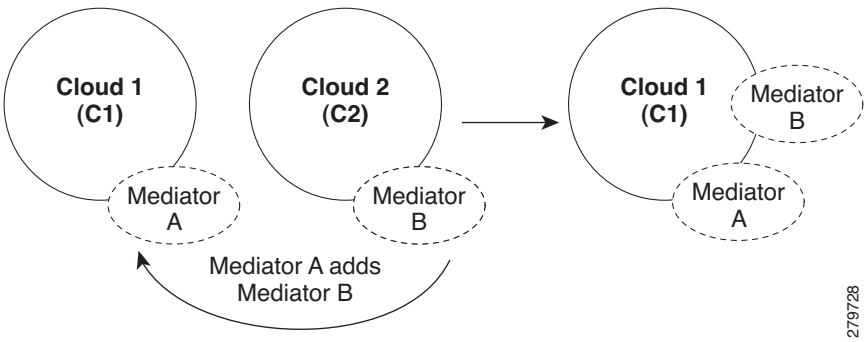
This section describes the following cloud formation scenarios between standalone Mediators and includes the following topics:

Scenario A

Figure 9-7 outlines a scenario in which:

1. Cloud 1 contains a single peer—Mediator A, and Cloud 2 contains a single peer—Mediator B.
2. Mediator B is added to Mediator A as a peer.
3. Mediator B moves to Cloud 1.
4. Cloud 1 now contains two peers—Mediator A and Mediator B; therefore, Cloud 2 ceases to exist.

Figure 9-7 Scenario A - Standalone Cloud Formations



To create the cloud formation outlined in Figure 9-7, perform the following steps:

Send documentation comments to cbsbu-docfeedback@cisco.com

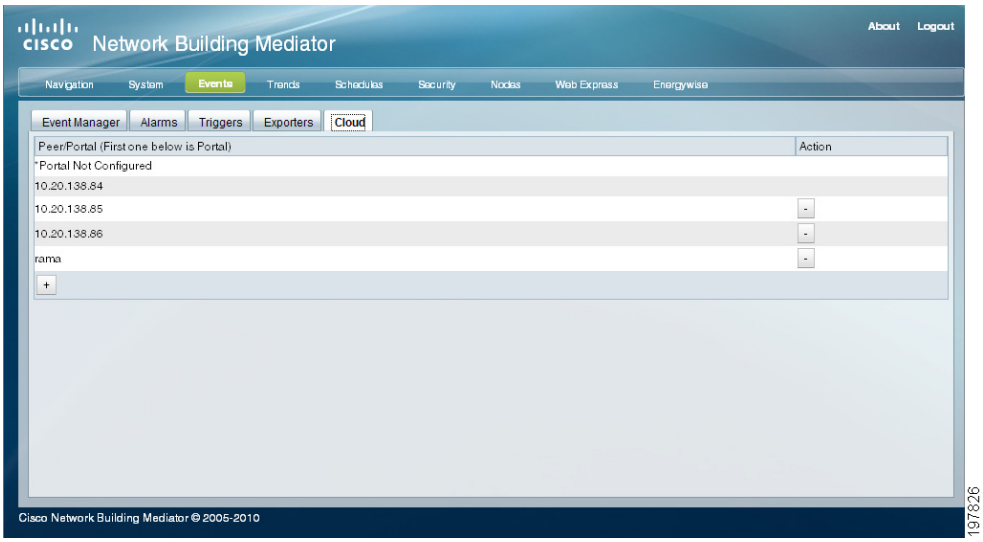
Step 1 Launch the Mediator A web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 2 In the web client homepage, click **Events**.

Step 3 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

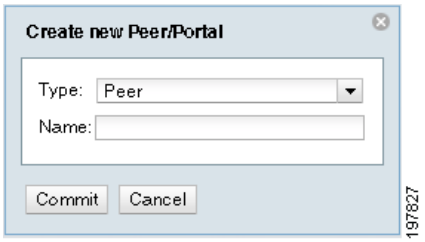
Figure 9-8 Cloud Tab



Step 4 Click the plus (+) symbol to add a new peer.

The Create new Peer/Portal dialog box appears as shown in Figure 9-9.

Figure 9-9 Create new Peer/Portal Dialog Box



Step 5 From the Type drop-down list, choose **Peer**.

Step 6 Enter the IP address of Mediator B in the Name text box, and click **Commit**.

Mediator B is added to Mediator A as a peer, and moves to Cloud 1.

Scenario B

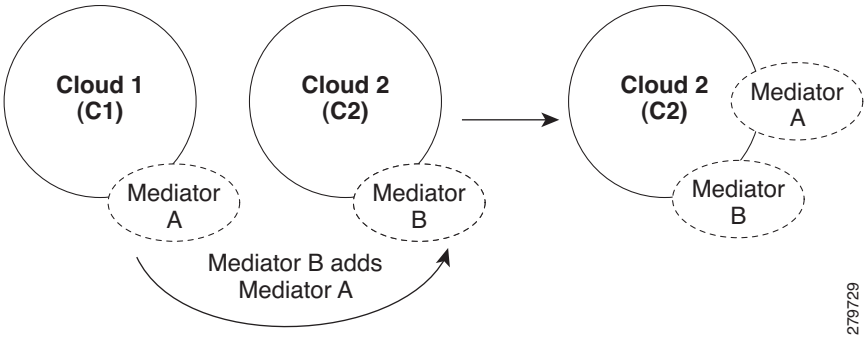
Figure 9-10 outlines a scenario in which:

1. Cloud 1 contains a single peer—Mediator A, and Cloud 2 contains a single peer—Mediator B.
2. Mediator A is added to Mediator B as a peer.

Send documentation comments to cbsbu-docfeedback@cisco.com

3. Mediator A moves to Cloud 2.
4. Cloud 2 now contains two peers—Mediator A and Mediator B; therefore, Cloud 1 ceases to exist.

Figure 9-10 Scenario B - Standalone Cloud Formations



To create the cloud formation outlined in Figure 9-10, perform the following steps:

Step 1 Launch the Mediator B web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 2 In the web client homepage, click **Events**.

Step 3 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 4 Click the plus (+) symbol to add a new peer.

The Create new Peer/Portal dialog box appears as shown in Figure 9-9.

Step 5 From the Type drop-down list, choose **Peer**.

Step 6 Enter the IP address of Mediator A in the Name text box, and click **Commit**.

Mediator A is added to Mediator B as a peer, and moves to Cloud 2.

Cloud Formations Between Single and Multi-Peer Clouds

This section describes the following cloud formation scenarios between single and multi-peer clouds and includes the following topics:

Scenario A

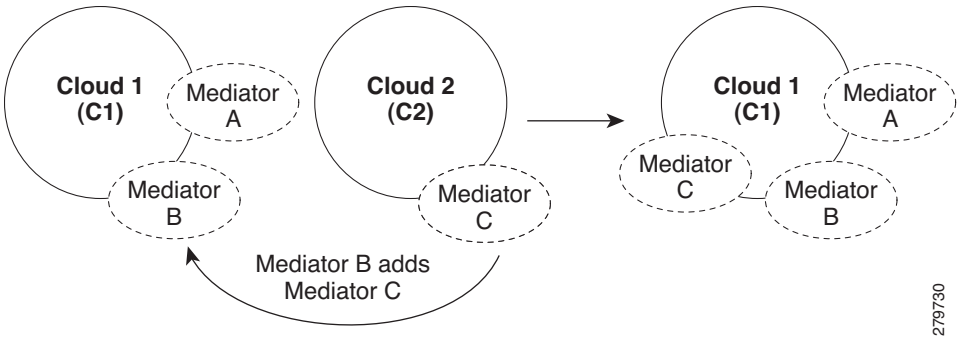
Figure 9-11 outlines a scenario in which:

1. Cloud 1 contains two peers—Mediator A and Mediator B.
2. Cloud 2 contains a single peer—Mediator C.
3. Mediator C is added to Mediator B as a peer.

Send documentation comments to cbsbu-docfeedback@cisco.com

4. Mediator C moves to Cloud 1.
5. Cloud 1 now contains three peers—Mediators A, B, and C; therefore, Cloud 2 ceases to exist.

Figure 9-11 Scenario A - Single and Multi-Peer Cloud Formations



Note Cloud formation is unidirectional in nature.

To create the cloud formation outlined in Figure 9-11, perform the following steps:

Step 1 Launch the Mediator B web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 2 In the web client homepage, click **Events**.

Step 3 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 4 Click the plus (+) symbol to add a new peer.

The Create new Peer/Portal dialog box appears as shown in Figure 9-9.

Step 5 From the Type drop-down list, choose **Peer**.

Step 6 Enter the IP address of Mediator C in the Name text box, and click **Commit**.

Mediator C is added to Mediator B as a peer, and moves to Cloud 1.

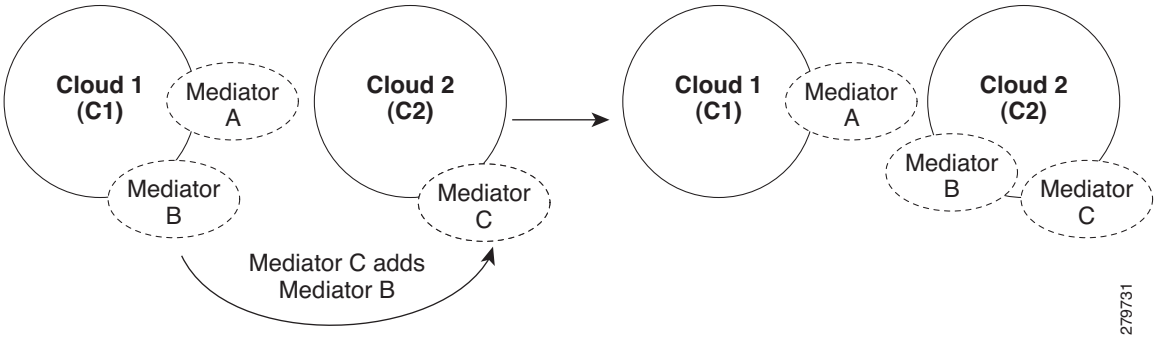
Scenario B

Figure 9-12 outlines a scenario in which:

1. Cloud 1 contains two peers—Mediator A and Mediator B.
2. Cloud 2 contains a single peer—Mediator C.
3. Mediator B is added to Mediator C as a peer.
4. Mediator B moves to Cloud 2.
5. Cloud 1 now contains a single peer—Mediator A, and Cloud 2 contains two peers—Mediator B and Mediator C.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 9-12 Scenario B - Single and Multi-Peer Cloud Formations



Note Cloud formation is unidirectional in nature.

To create the cloud formation outlined in Figure 9-12, perform the following steps:

Step 1 Launch the Mediator A web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 2 In the web client homepage, click **Events**.

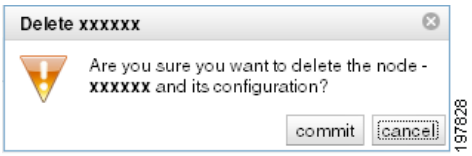
Step 3 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 4 Click the minus (-) symbol next to Mediator B to remove it from the cloud.

A dialog box appears as shown in Figure 9-13 to confirm the deletion.

Figure 9-13 Delete a Peer/Portal Dialog Box



Step 5 Click **commit** to delete Mediator B from the cloud.

Mediator B is removed from Cloud 1.

Note It is important that you remove Mediator B from Cloud 1 before proceeding further. Failure to do so can lead to ambiguous results.

Step 6 Launch the Mediator C web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 7 In the web client homepage, click **Events**.

Step 8 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 9 Click the plus (+) symbol to add a new peer.

The Create new Peer/Portal dialog box appears as shown in Figure 9-9.

Step 10 From the Type drop-down list, choose **Peer**.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 11 Enter the IP address of Mediator B in the Name text box, and click **Commit**.

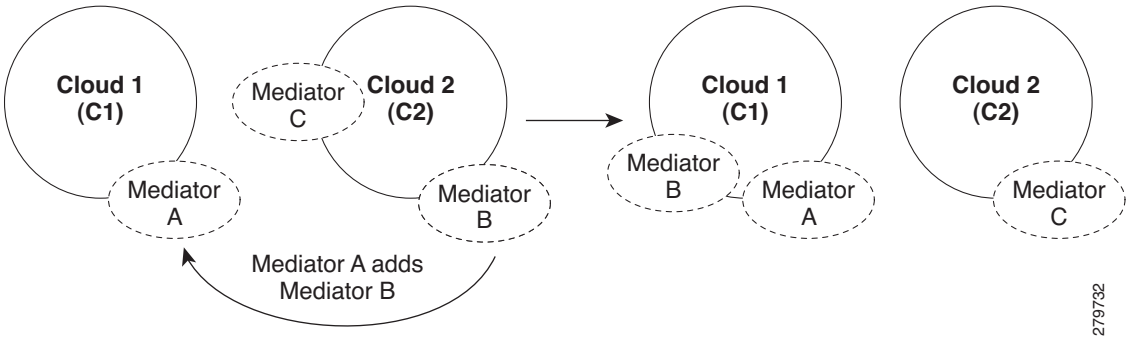
Mediator B is added to Mediator C as a peer, and moves to Cloud 2.

Scenario C

Figure 9-14 outlines a scenario in which:

1. Cloud 1 contains a single peer—Mediator A.
2. Cloud 2 contains two peers—Mediator B and Mediator C.
3. Mediator B is added to Mediator A as a peer.
4. Mediator B moves to Cloud 1.
5. Cloud 1 now contains two peers—Mediator A and Mediator B, and Cloud 2 contains a single peer—Mediator C.

Figure 9-14 Scenario C - Single and Multi-Peer Cloud Formations



Note Cloud formation is unidirectional in nature.

To create the cloud formation outlined in Figure 9-14, perform the following steps:

Step 1 Launch the Mediator C web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 2 In the web client homepage, click **Events**.

Step 3 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 4 Click the minus (-) symbol next to Mediator B to remove it from the cloud.

A dialog box appears as shown in Figure 9-13 to confirm the deletion.

Step 5 Click **commit** to delete Mediator B from the cloud.

Mediator B is removed from Cloud 2.

Note It is important that you remove Mediator B from Cloud 2 before proceeding further. Failure to do so can lead to ambiguous results.

Step 6 Launch the Mediator A web client. For more information, see Launching Mediator Web Client, page 8-1.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 7 In the web client homepage, click **Events**.

Step 8 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 9 Click the plus (+) symbol to add a new peer.

The Create new Peer/Portal dialog box appears as shown in Figure 9-9.

Step 10 From the Type drop-down list, choose **Peer**.

Step 11 Enter the IP address of Mediator B in the Name text box, and click **Commit**.

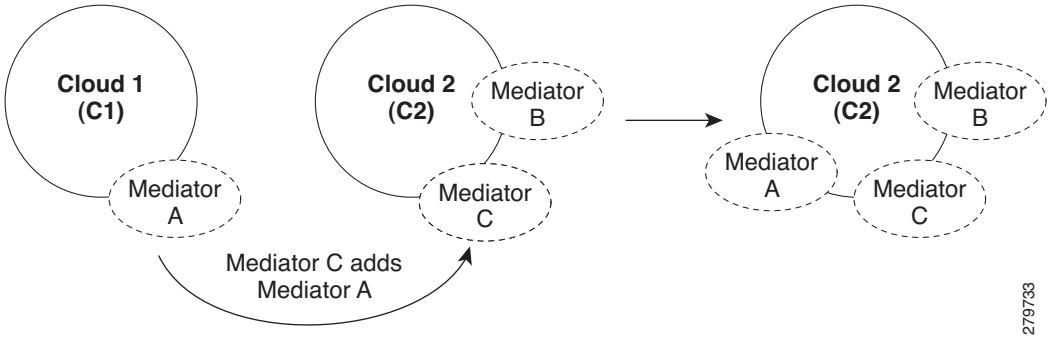
Mediator B is added to Mediator A as a peer, and moves to Cloud 1.

Scenario D

Figure 9-15 outlines a scenario in which:

1. Cloud 1 contains a single peer—Mediator A.
2. Cloud 2 contains two peers—Mediator B and Mediator C.
3. Mediator A is added to Mediator C as a peer.
4. Mediator A moves to Cloud 2.
5. Cloud 2 now contains three peers—Mediators A, B, and C; therefore, Cloud 1 ceases to exist.

Figure 9-15 Scenario D - Single and Multi-Peer Cloud Formations



Note Cloud formation is unidirectional in nature.

To create the cloud formation outlined in Figure 9-15, perform the following steps:

Step 1 Launch the Mediator C web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 2 In the web client homepage, click **Events**.

Step 3 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 4 Click the plus (+) symbol to add a new peer.

The Create new Peer/Portal dialog box appears as shown in Figure 9-9.

Step 5 Choose **Peer** from the Type drop-down list.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 6 Enter the IP address of Mediator A in the Name text box, and click **Commit**.

Mediator A is added to Mediator C as a peer, and moves to Cloud 2.

Cloud Formations Between Multi-Peer Clouds

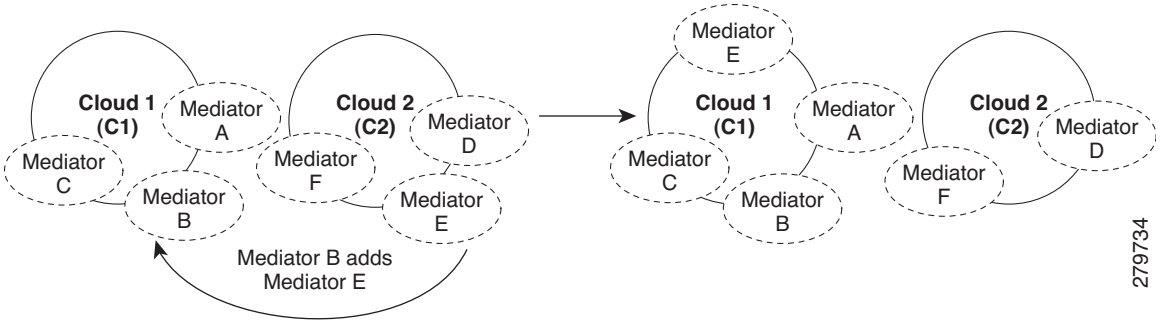
This section describes the following cloud formation scenarios between multi-peer clouds and includes the following topics:

Scenario A

Figure 9-16 outlines a scenario in which:

1. Cloud 1 contains three peers—Mediators A, B, and C.
2. Cloud 2 contains three peers—Mediators D, E, and F.
3. Mediator E is added to Mediator B as a peer.
4. Mediator E moves to Cloud 1.
5. Cloud 1 now contains four peers—Mediators A, B, C, and E.
6. Cloud 2 now contains two peers—Mediator D and Mediator F.

Figure 9-16 Scenario A - Multi-Peer Cloud Formations



Note Cloud formation is unidirectional in nature.

To create the cloud formation outlined in Figure 9-16, perform the following steps:

Step 1 Launch the Mediator D web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 2 In the web client homepage, click **Events**.

Step 3 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 4 Click the minus (-) symbol next to Mediator E to remove it from the cloud.

A dialog box appears as shown in Figure 9-13 to confirm the deletion.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 5 Click **commit** to delete Mediator E from the cloud.

Mediator E is removed from Cloud 2.

Alternatively, launch the Mediator F web client, and follow Step 2 through Step 5 to remove Mediator E from the cloud.

Note It is important that you remove Mediator E from Cloud 2 before proceeding further. Failure to do so can lead to ambiguous results.

Step 6 Launch the Mediator B web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 7 In the web client homepage, click **Events**.

Step 8 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 9 Click the plus (+) symbol to add a new peer.

The Create new Peer/Portal dialog box appears as shown in Figure 9-9.

Step 10 From the Type drop-down list, choose **Peer**.

Step 11 Enter the IP address of Mediator E in the Name text box, and click **Commit**.

Mediator E is added to Mediator B as a peer, and moves to Cloud 1.

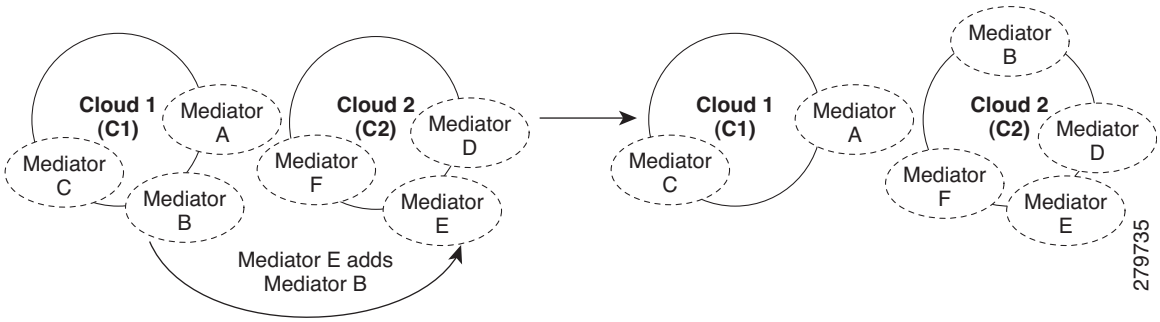
Alternatively, launch either the Mediator A or Mediator C web client, and follow Step 7 through Step 11 to add Mediator E to Cloud 1.

Scenario B

Figure 9-17 outlines a scenario in which:

1. Cloud 1 contains three peers—Mediators A, B, and C.
2. Cloud 2 contains three peers—Mediators D, E, and F.
3. Mediator B is added to Mediator E as a peer.
4. Mediator B moves to Cloud 2.
5. Cloud 1 now contains two peers—Mediator A and Mediator C.
6. Cloud 2 now contains four peers—Mediators B, D, E, and F.

Figure 9-17 Scenario B - Multi-Peer Cloud Formations



Send documentation comments to cbsbu-docfeedback@cisco.com

Note Cloud formation is unidirectional in nature.

To create the cloud formation outlined in Figure 9-17, perform the following steps:

Step 1 Launch the Mediator A web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 2 In the web client homepage, click **Events**.

Step 3 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 4 Click the minus (-) symbol next to Mediator B to remove it from the cloud.

A dialog box appears as shown in Figure 9-13 to confirm the deletion.

Step 5 Click **commit** to delete Mediator B from the cloud.

Mediator B is removed from Cloud 1.

Alternatively, launch the Mediator C web client, and follow Step 2 through Step 5 to remove Mediator B from the cloud.

Note It is important that you remove Mediator B from Cloud 1 before proceeding further. Failure to do so can lead to ambiguous results.

Step 6 Launch the Mediator E web client. For more information, see Launching Mediator Web Client, page 8-1.

Step 7 In the web client homepage, click **Events**.

Step 8 Click the **Cloud** tab.

The Cloud tab appears as shown in Figure 9-8.

Step 9 Click the plus (+) symbol to add a new peer.

The Create new Peer/Portal dialog box appears as shown in Figure 9-9.

Step 10 From the Type drop-down list, choose **Peer**.

Step 11 Enter the IP address of Mediator B in the Name text box, and click **Commit**.

Mediator B is added to Mediator E as a peer, and moves to Cloud 2.

Alternatively, launch either the Mediator D or Mediator F web client, and follow Step 7 through Step 11 to add Mediator B to Cloud 2.

Checking RSS Feeds

To create an RSS feed in the Events pane, perform the following steps:

Step 1 Open the browser and navigate to the syndication folder on a Mediator.

For example, http://192.2.0.255/syndication

Step 2 The Cisco-distributed alarm management portal web page appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

The portal web page displays the same set of events you would see in the Events pane.

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 10

Managing Security

The Mediator web client supports access by multiple users over the Internet, but access to resources is defined and managed using the Role-Based Access Control (RBAC) function.

RBAC refers to the method of regulating access to network resources based on the roles of individual users within an enterprise. Using RBAC, you can assign logins and restrict control using security levels. You can authorize and control the ability of users to view information, modify settings, add, modify, and delete files.

The security levels are easy to configure and allow maximum flexibility while maintaining complete control over access to resources on the Mediator. Access is controlled based on the roles that individual users are assigned.

This chapter includes the following sections:

About Security Elements

The elements of RBAC are defined as follows:

User—A user is an agent who interacts with the system. Users are identified by their usernames and passwords.

Note Agents who have not provided verifiable username and password information are treated as a special user (Anonymous). By default, the Anonymous user does not have access to any resources.

Role—A role refers to responsibilities and the authority conferred on the user assigned to a role. Every user is assigned one or more roles. Policies associate roles with resource access permissions.

Policy—A policy is a named set of access rules.

Policy context—The context identifies the resource to which the policy controls access. Users having roles also have the resource access permissions in the context of the policy.

Permission—A permission is a right to perform a certain action or set of actions on a resource. Access rules are specified by granting permissions to roles.

Send documentation comments to cbsbu-docfeedback@cisco.com

You need to define users, roles, and policies, and specify the relationship between these elements to configure security access levels. Users can be assigned multiple roles, and roles can be affected by multiple policies. This functionality allows you to achieve the control you want over resources with complete precision.

This section includes the following topics:

About Roles

Roles comprise operations and actions that are permitted for the user the role is assigned to. Each user can have multiple roles and each role can be defined by multiple policies. For example, if role_1 allows access to viewing operations and role_2 allows access to configuring operations, then users who belong to role_1 and role_2 can configure and view.

The following default roles are provided:

- Unknown
- Operator
- Manager
- System Administrator

Note You cannot edit or delete the default roles.

You can assign the following types of permissions to roles:

- View—Allows a user to only view data. The user cannot create or edit or delete nodes, and perform user management tasks, such as add or edit or delete users, roles, and policies.
- Configure—Allows a user to create, edit, and delete nodes. For example, create an alarm, delete an alarm, and so on.
- Override—Allows a user to override the value of an existing node. For example, override the value of a relay node.
- Manage Users—Allows a user to perform user management tasks, such as add or edit or delete users, roles, and policies.

Table 10-1 outlines the default permissions that are assigned to the default roles.

Table 10-1 Default Roles and Associated Permissions

	Permissions			
Default Roles	**View**	**Configure**	**Override**	**Manage Users**
Unknown	–	–	–	–
Operator	✓	–	–	–
Manager	✓	✓	✓	–
System Administrator	✓	✓	✓	✓

Send documentation comments to cbsbu-docfeedback@cisco.com

Note The System Administrator role is also required to log into the configTOOL and perfectHOST applications; access the System page in the Mediator web client to configure the Mediator settings, and back up and restore the Mediator.

The Roles tab appears as shown in Figure 10-1.

Figure 10-1 Roles Tab

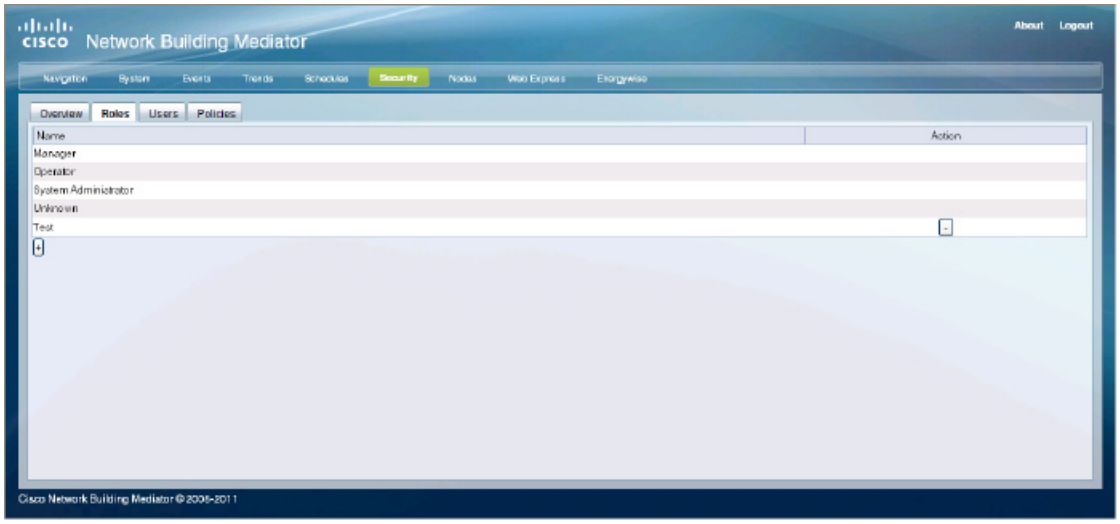


Table 10-2 describes the buttons that are shown on the Roles tab.

Table 10-2 Roles Tab - Description

Button	Description
+	Allows you to add roles.
-	Allows you to delete roles.

To know more about managing roles, see the "Managing Roles" section on page 10-5.

About Users

When you add a user, you assign a username and a password. You may configure a default homepage for the user, such as a personalized web page. You can also assign one or more roles to the user. The roles you assign are used by policies to specify the resources the user can access.

The following default users are assigned:

- mpxadmin
- Anonymous

The mpxadmin user has full access to the system resources.

The Users tab appears as shown in Figure 10-2.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 10-2 Users Tab

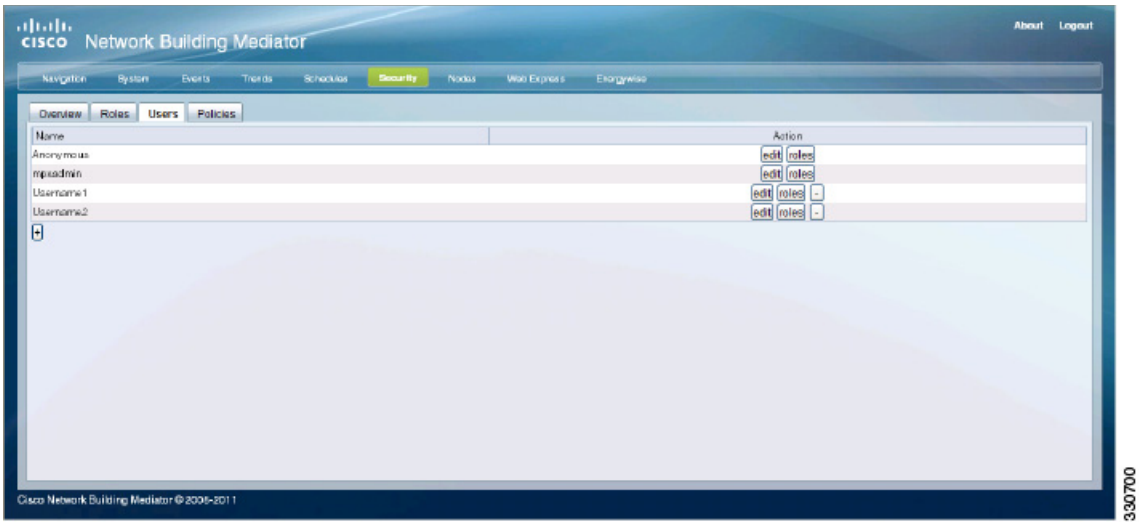


Table 10-3 describes the buttons shown on the Users tab.

Table 10-3 Users Tab - Description

Button	Description
+	Allows you to add users.
-	Allows you to delete users.
edit	Allows you to edit the user settings. Note: You cannot edit the names of users.

To know more about managing users, see the "Managing Users" section on page 10-6.

About Policies

You can define policies to limit the resources that the user can access. A policy comprises policy context and permissions. The policy context refers to the path where you want the policy to be implemented, for example, /alias/location/building1. The permissions refer to the controls and actions that the user can perform in that particular context, for example, configuring and viewing configurations.

To add a policy on the Mediator, you specify a resource that you want to control (for example, access to HTTP Files). You then grant access permissions to the role for the specified resource.

The following system-defined policies are provided:

- Default

Note Use the Default policy against each role that is created, so that users can view the navigation tree, schedules, events, trends, and so on.

- HTTP Files
- HTTPS Files

Send documentation comments to cbsbu-docfeedback@cisco.com

Note You cannot edit or delete the system-defined policies.

The Policies tab appears as shown in Figure 10-3.

Figure 10-3 Policies Tab

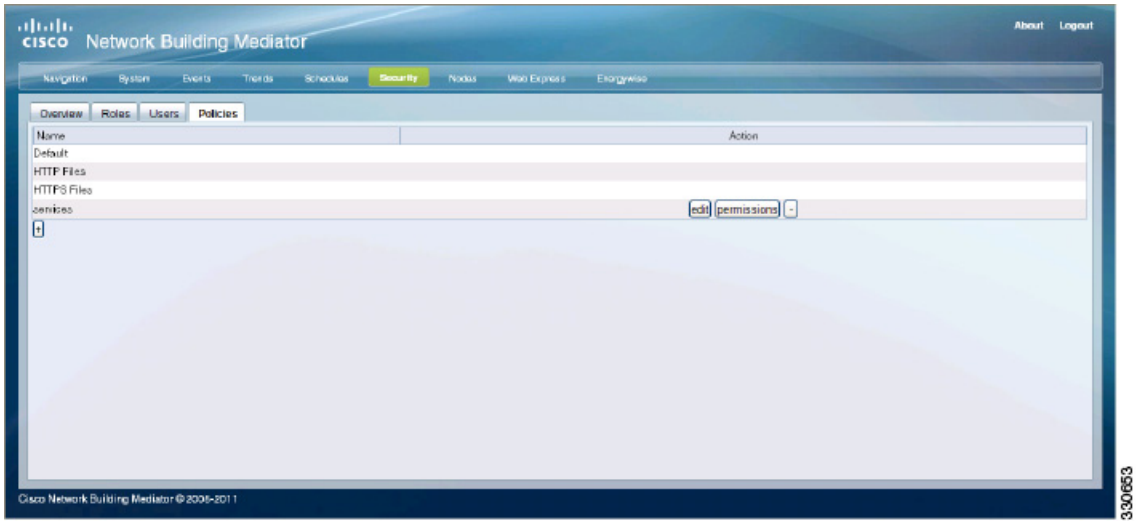


Table 10-4 describes the buttons shown on the Policies tab.

Table 10-4 Policies Tab - Description

Button	Description
+	Allows you to add policies.
-	Allows you to delete policies.
edit	Allows you to edit the policy settings. Note: You cannot edit the names of policies.
permissions	Allows you to set permissions for user-defined roles.

To know more about managing polices, see the "Managing Policies" section on page 10-10.

Managing Roles

This section includes the following topics:

Note You must be assigned the System Administrator role or a role that is granted the Manage Users privilege to perform the actions outlined in this section.

Send documentation comments to cbsbu-docfeedback@cisco.com

Adding Roles

To add a role, perform the following steps:

Step 1 In the Mediator web client, click **Security**.

Step 2 Click the **Roles** tab.

The Roles tab appears listing the configured roles.

Step 3 Click the plus symbol (+) button to add a role.

The Add Role dialog box appears.

Step 4 In the Add Role dialog box, perform the following steps:

a. In the Name text box, enter a name for the role.

You should choose a descriptive name that identifies a job function or position requiring authorization to access resources on the Mediator at a defined level.

Note You cannot include spaces in the name of a role.

b. Click **commit** to save the new role.

The new role is added to the list on the Roles tab.

Deleting Roles

To delete a role, perform the following steps:

Note You cannot delete the default roles—Unknown, Operator, Manager, and System Administrator.

Step 1 Click the **Roles** tab.

The Roles tab appears listing the configured roles.

Step 2 Click the minus symbol (-) button next to the name of the role that you want to delete.

The Remove Roles dialog box appears asking you to confirm the operation.

Step 3 Click **commit**.

The role is removed from the list on the Roles tab.

Managing Users

This section describes how to create, edit, and delete users; change password restrictions and edit user roles. It includes the following topics:

Send documentation comments to cbsbu-docfeedback@cisco.com

Creating Users

To create a user, perform the following steps:

Step 1 In the Mediator web client, click **Security**.

Step 2 Click the **Users** tab.

The Users tab appears listing the configured users.

Step 3 Click the plus symbol (+) button to add a user.

The Add User dialog box appears.

Step 4 In the Add User dialog box, perform the following steps:

a. In the Username text box, enter a name for the user.

You should choose a descriptive name that identifies an individual user.

b. In the Password text box, enter the password.

c. In the Confirm Password text box, re-enter the password that you entered in the Password text box.

d. In the Homepage text box, click **Select**.

The File Selector dialog box appears.

e. In the File Selector dialog box, perform the following steps:

1. Navigate to and select the homepage. The file path appears in the File name text box.
2. Click **SAVE**.

The File Selector dialog box closes. The homepage refers to the page that appears the next time the user logs into the Mediator web client.

f. To assign the System Administrator role to this user, select the **System Administrator** check box.

g. Click **commit** to save the new user.

The new user is added to the list on the Users tab.

Note If you do not assign the System Administrator role to the new user, the Unknown role is assigned by default. To assign a different role to the user, see the "Editing User Roles" section on page 10-9.

Changing Password Restrictions

The Mediator uses a strong password policy to enforce the use of complex passwords for secure access. However, you can modify the password restrictions using the configTOOL.

Send documentation comments to cbsbu-docfeedback@cisco.com

To edit the password policy, perform the following steps:

Step 1 Connect to the Mediator using the configTOOL.

Step 2 Navigate to and select /services/Security Manager.

The Security Manager tab appears in the data entry pane.

Step 3 On the Security Manager tab, perform the following steps:

a. In the Password min length text box, enter the minimum number of characters that the password must contain.

b. In the Admin password min length text box, enter the minimum number of characters that the password for the admin user must contain.

c. In the Password max length text box, enter the maximum number of characters that are permitted in the password.

d. Select the **Require complex password** check box to enforce the use of complex passwords for secure access.

e. Select the **Forbid repeated characters in password** check box to prevent the use of recurring characters in the password.

f. Select the **Forbid password equal username** check box to to prevent the use of the username as the password.

g. Select the **Forbid password equal to 'cisco'** check box to prevent the use of the term 'cisco' as the password.

h. Select the **Forbid password equal to 'mpxadmin'** check box to prevent the use of the term 'mpxadmin' as the password.

Step 4 Click **Save** to save the configuration.

Editing Users

To edit a user, perform the following steps:

Step 1 In the Mediator web client, click **Security**.

Step 2 Click the **Users** tab.

The Users tab appears listing the configured users.

Step 3 Click **edit** next to the name of the user that you want to edit.

The Edit Users dialog box appears with the Username text box disabled because you cannot edit the names of users.

Step 4 In the Edit Users dialog box, perform the following steps:

a. In the Old Password text box, enter the current password.

b. In the New Password text box, enter the new password.

c. In the Confirm Password text box, re-enter the new password.

d. In the User Homepage text box, click **Select**.

The File Selector dialog box appears displaying a list of preconfigured homepages.

Send documentation comments to cbsbu-docfeedback@cisco.com

e. In the File Selector dialog box, perform the following steps:

   1. Navigate to and select the user homepage. The file path appears in the File name text box.
   2. Click **SAVE**.

   The File Selector dialog box closes. The user homepage refers to the page that appears the next time the user logs into the Mediator web client.

f. Click **commit** to save the changes.

Editing User Roles

To edit a user role, perform the following steps:

Step 1 In the Mediator web client, click **Security**.

Step 2 Click the **Users** tab.

The Users tab appears listing the configured users.

Step 3 Click **roles** next to the user whose role you want to edit.

The Roles dialog box displaying a list of roles appears.

Note If the user was assigned the System Administrator role at the time of creation, you cannot edit the role. If the user was assigned any other role, you can assign a different role to the user. However, you will not be able to assign the System Administrator role.

Step 4 In the Roles dialog box, perform the following steps:

a. To assign a different role to the user, select the check box next to the role name.

b. Click **commit** to save the role assignments.

Deleting Users

To delete a user, perform the following steps:

Note You cannot delete the default users—mpxadmin and Anonymous.

Step 1 In the Mediator web client, click **Security**.

Step 2 Click the **Users** tab.

The Users tab appears listing the configured users.

Step 3 Click the minus symbol (-) button next to the user that you want to delete.

The Remove Users dialog box appears asking you to confirm the operation.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note When you attempt to delete a user that has active sessions, the Remove Users dialog box that appears notifies you that the user you are deleting is an active user.

Step 4 Click **commit**.

The user is removed from the list on the Users tab.

Managing Policies

This section describes how to add, edit, and delete policies and change policy permissions. It includes the following topics:

Note You must be assigned the System Administrator role or a role that is granted the Manage Users privilege to perform the actions outlined in this section.

Adding Policies

To create a policy, perform the following steps:

Step 1 In the Mediator web client, click **Security**.

Step 2 Click the **Policies** tab.

The Policies tab appears listing the configured policies.

Step 3 Click the plus symbol (+) button to add a policy.

The Add Policy dialog box appears.

Step 4 In the Add Policy dialog box, perform the following steps:

a. In the Name text box, enter a name for the policy.

You should choose a descriptive name to identify the resource on the Mediator controlled by the policy.

b. In the Policy Context text box, click **Select**. The Node Selector dialog box appears.

Note You cannot create more than one policy with the same context.

c. In the Node Selector dialog box, perform the following steps:

1. Navigate to and select the node that is the location of the resource controlled by the policy.
2. Click **SAVE**.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Node Selector dialog box closes.

Note If the Policy Context points to a service, then no authorizations are required.

d. Click **commit** to save the policy.

Note Policies that are created on the Mediator Manager do not get applied on downstream Mediators.

Editing Policies

To edit the policy, perform the following steps:

Step 1 In the Mediator web client, click **Security**.

Step 2 Click the **Policies** tab.

The Policies tab appears listing the configured policies.

Step 3 Click **edit** next to the name of the policy that you want to edit.

The Edit Policies dialog box appears with the Policy Name text box disabled because you cannot edit the names of policies.

Step 4 In the Edit Policies dialog box, perform the following steps:

a. In the Policy Context text box, click **Select**. The Node Selector dialog box appears.

Note You cannot create more than one policy with the same context.

b. In the Node Selector dialog box, perform the following steps:

1. Navigate to and select the node that is the location of the resource controlled by the policy.
2. Click **SAVE**.

   The Node Selector dialog box closes.

c. Click **commit** to save the changes to the policy.

Changing Policy Permissions

To change the permissions of the policy, perform the following steps:

Step 1 In the Mediator web client, click **Security**.

Step 2 Click the **Policies** tab.

The Policies tab appears listing the configured policies.

Step 3 Click **permissions** next to the name of the policy that you want to edit.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Permissions dialog box appears listing the roles for which you want to configure permissions. Each role appears as a button, which when clicked displays a collapsible pane with four check boxes—View, Override, Configure, and Manage Users.

Step 4 In the Permissions dialog box, perform the following steps:

a. Click the role for which you want to configure permissions.

b. Select one or more check boxes for the role. To deny all permissions to a role, leave the check boxes unselected.

c. Repeat Step 4a through Step 4b for each role whose permissions you want to configure.

d. Click **commit** to save the policy permissions.

Deleting Policies

To delete an existing policy, perform the following steps:

Note You cannot delete the system-defined policies—Default, HTTP Files, and HTTPS Files.

Step 1 In the Mediator web client, click **Security**.

Step 2 Click the **Policies** tab.

The Policies tab appears listing the configured policies.

Step 3 Click the minus symbol (-) button next to the name of the policy that you want to delete.

The Remove Policies dialog box appears asking you to confirm the operation.

Step 4 Click **commit** to delete the policy.

The policy is removed from the list on the Policies tab.

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 11

Managing Trends

Trends provides historical data of a node in the network over a period of time. When the value of a node in the specified trend changes, the changes are recorded in the trend logs and displayed in real-time, animated graphs.

This section includes the following topics:

About Trends

The Mediator web client provides an interface to configure and manage trends. You can use the Mediator web client to modify the appearance of the trend graphs, view the trends, and also export the trend data in MS Excel format.

For example, if you want to view and compare the room temperatures of two roof top units (RTU), you can use the web client to view the real-time data and also historical data over a period of time.

The Trends page appears as shown in Figure 11-1.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 11-1 Trends Page

Table 11-1 describes the buttons as shown in the Trends page.

Table 11-1 Trends Page- Description

Button	Description
+	Allows you to add trends.
-	Allows you to delete trends.
view trend	Allows you to view trends. This button will remain disabled until the points are configured.
configure points	Allows you to configure points for a trend.
trend preferences	Allows you to set preferences for your trend.

Creating Trends

To create a new trend, perform the following steps:

Step 1 In the Mediator web client, click **Trends**.

The Trends pane appears displaying a list of currently configured trends.

Note Periodic log nodes that are configured using the configTOOL also appear in the Trends pane. However, the **configure points** button remains disabled and you cannot edit the point.

Step 2 Click the plus symbol (**+**) button located below the last trend in the table.

A new trend is added to the table in the Trends pane. The default name is the next trend in numerical order. The view trend button is disabled for the newly created trend.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note The Mediator uses the default name to identify the trend internally. If you examine the node tree (for example, with nodes), you will find the node listed by number, not by name. However, you can change the default name. When specifying a trend name, we recommend avoiding the use of special characters in trend names.

Step 3 Click **configure points**.

The Configure Points dialog box appears.

Step 4 In the Configure Points dialog box, do the following:

a. In the Point Name text box, enter a name for the point.

The name should identify the function of the point.

b. Click the ellipsis (…) button in the first row of the table.

In the Node Selector dialog box, perform the following steps:

1. Navigate to and select the node you want to include in the trend.
2. Click **SAVE**.

Note If you select the cache check box, the Mediator saves the location of the selected node, and automatically returns to it the next time you open the Node Selector dialog box. This feature is useful when you are configuring multiple nodes for a trend.

The node path appears in the Node location text box in the Configure Points dialog box.

c. Repeat Step 4b for each file you want to include in the trend. Alternatively, you can enter the pathname in the Node Path text box instead of using the Node Selector option.

Note Do not leave blank rows between rows containing file configurations.

d. In the Period text box of the Configure Points dialog box, enter the interval in seconds at which the Mediator logs the values of the nodes you selected. The default value is 60 seconds.

e. Click **commit** to save the configuration.

The Configure Points dialog box closes and the Trends pane reappears. The view trend button is now enabled.

Note Trends that are not associated with any points are not saved after restarting the Mediator.

Viewing Trends

To view an existing trend, perform the following steps:

Step 1 In the Mediator web client, click **Trends**.

The Trends pane appears displaying a list of currently configured trends.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 2 Click **view trend** next to the trend you want to view.

A window appears displaying a MacroMedia Flash graph of the trend. The graph scrolls and shows the trend node logging the selected nodes in real time.

Note Periodic log nodes that are configured using the configTOOL also appear in the Trends pane. However, if more than nine points are associated with the trend, you cannot view the graph of the trend. This limitation will be addressed in future releases.

Step 3 To stop the scrolling of the graph, right-click anywhere in the graph, and choose **Stop Auto-Scroll** from the menu. To restart scrolling, right-click the graph, and choose **Start Auto-Scroll** from the menu.

Step 4 Click the **Legend** link.

The Legend lists the assigned point names and indicates the colors of their trend lines.

Step 5 Use the slider at the bottom of the graph to select different time periods in the graph.

The plus (+) and minus (-) buttons to the right of the slider allows you to zoom in and out in the graph. The X and Y axis scales are automatically adjusted.

Step 6 To reload the graph, right-click anywhere in the graph, and choose **Reload** from the menu.

The graph in the window is refreshed.

Step 7 To navigate back to the Trends pane, right-click anywhere in the graph, and choose **Trend Manager** from the menu.

A new window appears displaying the Trends pane.

Note After creating and viewing a trend in the Mediator web client, if both the time and time zone of the Mediator are changed using an SSH client, such as PuTTY, the trend in the Mediator web client does not reflect this change in the time. However, if only the time is changed, the trend in the Mediator web client is updated with the changed time. This occurs because a change in the time zone of the Mediator constitutes a change in the system configuration, and for this change to be reflected, you need to restart the Mediator Framework.

Editing Trends

You can control the appearance of the trend graphs by editing and specifying trend parameters.

To edit an existing trend, perform the following steps:

Step 1 In the Mediator web client, click **Trends**.

The Trends pane appears displaying a list of currently configured trends.

Step 2 Click **trend preferences** next to the trend you are configuring.

Note Periodic log nodes that are configured using the configTOOL also appear in the Trends pane. However, if more than nine points are associated with the trend, you cannot edit the trend. This limitation will be addressed in future releases.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Trend Preferences dialog box appears containing the General Preferences, Point Preferences and Axis Preferences areas.

Use the three areas in the Trend Preferences dialog box to define your settings:

- General Preferences: Specify the name of the trend and configure the dimensions, colors, type font, and initial time span of the trend.
- Point Preferences: Specify the display color of the nodes in the trend, and the XY axes on which they are plotted.
- Axis Preferences: Configure the parameters of the XY axes. The Axis Preferences area contains a table with entries for the parameters that define the two Y axes. The Y axes are numbered as 1 and 2.

Step 3 In the Trend Preferences dialog box, perform the following steps:

a. In the Display Name text box, enter a name that identifies the trend.

Note This name identifies the trend for system users. You should select a descriptive name that identifies the function of the trend. The Mediator identifies the trend node internally by the default number, not by this name.

b. In the Width and Height text boxes, enter the dimensions of the trend graph in pixels.

c. In the Background Color text box, click the color block next to the text box.

The Select Color dialog box appears.

d. Click the color you want for the background of the trend graph.

The Select Color dialog box closes.

e. In the Text Color text box, click the color block next to the text box.

The Select Color dialog box appears.

f. Click the color you want for the text that appears in the trend graph.

Note Choose a color that is readable against the background color you selected in Step 3d. For example, black shows up well on white or light grey, whereas red on black does not appear clear.

The Select Color dialog box closes.

g. In the Text Size text box, enter the size for the text that appears in the trend graph.

h. In the Font text box, enter the font for the text that appears in the trend graph.

Note Arial, Verdana, and Times New Roman fonts work well. Accept the defaults if you do not have experience specifying fonts.

i. In the Initial Timespan text boxes, set the initial time period of the X (horizontal) axis when the trend is first started. Choose the unit of the time period (samples taken, hours, minutes, or seconds) from the drop-down list.

In the Point Preferences area, perform the following steps:

j. Choose the time stamp from the Time Reference drop-down list.

k. In the Color text box, click the color block next to the text box.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Select Color dialog box appears.

l. Click the color you want for the background of the trend graph.

The Select Color dialog box closes.

You should select colors that will contrast against the background color that you selected in Step 3d.

In the Axis Preferences area, perform the following steps:

m. Choose the **Y** (vertical) axis from the Axis Status drop-down list. The Y axis is used for reading the plot of each node in the trend graph.

You can have two Y axes: Y axis 1, with its scale on the left side of the graph, and Y axis 2, with its scale on the right side of the graph. Choose 1 for the left Y axis or 2 for right Y axis from the drop-down list in the first row.

Repeat this activity for each of the other nodes in the trend.

n. In the first row of the Axis Status column, Y axis 1 is set to enabled and cannot be changed.

o. In the second row of the Axis Status column, Y axis 2 defaults to disabled. Choose **enabled** from the drop-down list if you want your trend graph to have two Y axes.

p. In the Range area, specify the range of the Y axis scales by entering the minimum value in the From text box and the maximum value in the To text box.

The default for both the values is auto, which allows Trends to automatically set the scales from the minimum to the maximum values output by the nodes, with an appropriate increment.

q. From the Type drop-down list, choose **numeric** for nodes with numeric values or **binary** for nodes with binary values (1 or 0, On or Off, and so on).

Note You cannot set the axis type as binary for both the axes.

r. Click **commit** to save the configurations.

Downloading Trends

To download a trend, perform the following steps:

Step 1 In the Mediator web client, click **Trends**.

The Trends pane appears displaying a list of currently configured trends.

Step 2 Display a trend graph. To learn more about displaying graphs, see Viewing Trends, page 11-3.

Step 3 To save the complete trend log, right-click anywhere in the graph, and choose **Save All** from the menu.

Alternatively, to save only the part of the log that is currently visible in the graph, right-click anywhere in the graph, and choose **Save Visible** from the menu.

The Download File dialog box appears.

Step 4 Click **Download** to choose a location on your local system, and save the trend log as a .csv (Comma Separated Value) file.

Step 5 Open the saved file.

Send documentation comments to cbsbu-docfeedback@cisco.com

The file contains a line for each event recorded in the log.

Deleting Trends

To delete an existing trend, perform the following steps:

Step 1 In the Mediator web client, click **Trends**.

The Trends pane appears displaying a list of currently configured trends.

Step 2 Click the minus symbol (-) button on the trend you want to delete.

A dialog box appears prompting you to confirm the operation.

Step 3 Click **OK** to remove the trend.

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 12

Managing Schedules

This chapter describes how to manage schedules using the Cisco Network Building Mediator graphical user interface (GUI), and includes the following topics:.

About Schedules

Schedules allow the devices to power on and off as necessary to maintain the programmed setpoints for that state. You can view the scheduled operating hour of each device that can be scheduled on either a weekly or a monthly calendar-based graphical schedule. This lets you select and adjust each schedule and time period, and to simultaneously schedule other related devices.

Prerequisites for using schedules:

- PC with Internet Explorer. The Mediator is supported on Mozilla Firefox 3.5 and later, and Internet Explorer version 7.0 or 8.0.
- Mediator Manager, Downstream Mediators, and PC on the same network.

It is understood that you have installed the Mediator and are ready to configure it. (For more information on installing the Mediator, see Getting Started, page 2-1.)

Note Before you install, operate, or service the system, read the *Regulatory Compliance and Safety Information for the Cisco Network Building Mediator* document for important safety information.

The following schedules-related terms are used in this section:

- Schedule group—A conceptual grouping of devices or other schedule groups that may contain schedule data or calendar entries.
- Schedule data—The weekly schedule that is in effect for the schedule groups and devices in the group.
- Calendar entry—Calendar date that defines exceptions to weekly schedules. They apply to the group and its devices and subgroups.

Send documentation comments to cbsbu-docfeedback@cisco.com

- Scheduling hierarchy—The schedule groups and devices tree that are defined at a Mediator portal or EBMS server.

Creating Schedules

You can create new schedules and customize them per your requirements. This section describes how you can create and customize a new schedule.

This section includes the following topics:

Creating New Schedules

To create a new schedule, it is important that an entity root is created under the Aliases node. To create an entity root, see Adding an Entity Root, page 15-2.

Note The Mediator does not support multi-level schedules, since multi-level schedules cannot be imported to the Mediator Manager. Hence, you must create only one-level schedules on the Mediator. Multi-level schedules are created when you use special characters such as a semi-colon.

To create a new schedule, perform the following steps:

Step 1 In the Mediator web client homepage, click **Schedules**.

Step 2 In the name pane, expand the Schedules node to list the nodes.

Step 3 Select the schedule that you want to configure, and click **Add Schedule**.

Step 4 In the dialog box that appears, enter a new schedule name in the Name text box, and click **OK**.

Note We recommend that you do not use special characters (such as [; # ? %]) while naming the schedules. But you can use specific special characters such as [_ - @]).

The new schedule appears in the Name pane, under the selected schedule.

Step 5 Click **Save** to save the new schedule.

Step 6 (Optional) Click **Change Name** to change the schedule name.

Defining Properties

You can edit schedule values for an existing property, remove an existing property, or add a new property.

Send documentation comments to cbsbu-docfeedback@cisco.com

To define the properties for a new schedule or edit the properties of an existing schedule, perform the following steps:

Step 1 Click the **Properties** tab.

Step 2 To define a new property, click **Add Property**. The Property Selection Panel dialog box appears.

Step 3 Select the check box for the appropriate entity, and click **OK**. The newly added entity appears on the Properties tab, in the Property Name column.

Step 4 (Optional) Click **Remove Property** to remove the defined property.

Step 5 Click **Edit Custom Values** to customize the existing values for the defined entity/property. The Update Values dialog box appears.

Step 6 In the Update Values dialog box, enter the appropriate values for required state in the Custom Value column. Click **OK** to save the values.

The defined state of the entity displays the new value.

Step 7 In the Mediator web client homepage, click **Save** to save the defined properties.

Defining Options

The Schedules feature allows you to create new actions for a schedule. Once you create an action, you can create a new time entry, edit, or delete the existing time entries for that action within a schedule.

To create a new action, edit, or delete a time entry for an action, perform the following steps:

Step 1 Click the **Options** tab.

Step 2 To add a new action and the corresponding value to it, click **Add**. A new event appears.

Step 3 On the Options tab, enter the following information:

- Name—Enter the name of the new event. For example: ON
- Color—Select the color that represents the new event. For example: Green
- Value—Select the appropriate BO value. For example: 1 or 0

Step 4 (Optional) Click **Delete** to delete an existing event.

Step 5 (Optional) Click **Move Up** or **Move Down** to move an event in an ascending or descending order.

Step 6 In the Mediator web client homepage, click **Save** to save the new values.

Note Any event that appears at the beginning of the list, will not display the corresponding color. By default, this event is the OFF state. You must not move a newly created event to the beginning of this list.

Creating Weekly Schedules

You can create a schedule for either an entire week or for specific days.

Send documentation comments to cbsbu-docfeedback@cisco.com

To create weekly schedules, perform the following steps:

Step 1 Click the **Weekly Schedule** tab.

Step 2 To create a time entry for a particular day, click **Add**.

Step 3 In the Add New Entry dialog box that appears, enter the following information:

- Entry—Enter the hour and minutes in the provided text box or select by using the up and down arrows.
- Day—Choose the day from the drop-down list.

Step 4 Click **Add Entry**. The new entry appears on the Weekly Schedule tab.

Note You must manually enter the time entries for each day and action for a weekly schedule.

Step 5 In the Mediator web client homepage, and click **Save** to save the weekly schedule.

Creating Exceptions

Exceptions are one or more days (such as holidays) during which the normal schedule changes. You are allowed to create exceptions to the normal schedule.

To create an exception schedule, perform the following steps:

Step 1 Click the **Exceptions** tab.

Step 2 Click **Add** to enable all the text boxes on the Exceptions tab.

To set the exception specifications, enter the following information:

- Name—Enter a descriptive name for the new exception schedule.
- Single Day—Click the **Single Day** radio button for an exception for a single day.
- Multiple Days—Click the **Multiple Days** radio button for an exception for multiple days.
- Start Date—Click the **Start Date** to select the start date for the exception schedule.

Step 3 To set the time entries for the new exception, click the + icon. This enables the time entry text box

Step 4 Enter the hour and minutes in the provided text boxes, or select by using the up and down arrows.

Step 5 In the Mediator web client homepage, click **Save** to save the exception schedule.

Grouping Schedules

To create a schedule group, you need to group together all the local schedules that need to be part of that schedule group.

To create a schedule group, perform the following steps:

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 1 In the Mediator web client, click **Schedules**.

The left pane displays the local schedules.

Step 2 Click **Add Schedule**. A new dialog box appears.

Step 3 In the New Schedule dialog box, enter a new schedule group name in the Name text box, and click **OK**

The new schedule group appears in the Name pane.

Step 4 Drag and drop the local schedule that you want to add to the schedule group. The local schedule now appears as a child of the schedule group.

All schedules grouped under a particular group inherit the schedule of that particular group.

Overriding and Releasing Schedules

The Override feature allows you to give preferences to the local schedules over the global schedules. You can override the local schedules by clicking Override for that schedule. If you do not select the override option, the global schedules will get preference over the local schedules.

You are also allowed to control the level at which the local schedule can override all the points that it controls. To control these levels, you have to set the override priority values in the configTOOL.

The Schedule Manager node is an inherent child node under the Services node in the configTOOL. The Schedule Manager tab displays the default name and description along with the Override Priority text box. You can change the default value in the Override Priority text box. While the default value is set to 10, you can choose any value between 1 to 16.

Note Override Priority value is the priority at which the local schedule overrides all the points that it controls. This option is applicable to all schedules that are created and operating on a specific Mediator.

The Release feature allows you to reverse the override options.

Click **Release** to activate the global schedule for that Mediator. In such cases, the global schedules take precedence over the local schedule until you change the preference

Deleting Schedules

To delete a schedule, select the schedule, and click **Remove Schedule**. The schedule is deleted.

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 13

Customizing HTML Pages Using Web Express

The Mediator Web Express feature is a web-page authoring tool that allows you to create HTML monitor drawings using customizable widgets and graphics. Web Express incorporates live data points, from the Mediator, in the drawings.

This chapter includes the following sections:

Creating New Files

You can enhance and customize the web pages stored in the Mediator by adding widgets using Web Express.

To create a new web page, perform the following steps:

Step 1 In the Mediator web client, click **Web Express**.

The Web Express pane appears as shown in Figure 13-1.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 13-1 Web Express Pane

Step 2 Choose the web page you want to modify from the drop-down list.

Note The hierarchy of the HTML pages appearing in the drop-down list is logically tied to the Enterprise Navigation feature. The pages are displayed in the same sequence as they are specified during the entity root configuration in the configTOOL. For more information, see Understanding Enterprise Navigation, page 15-1.

Step 3 Click **Create New File**.

A blank Web Express drawing pane appears as shown in Figure 13-2.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 13-2 Create New File Pane

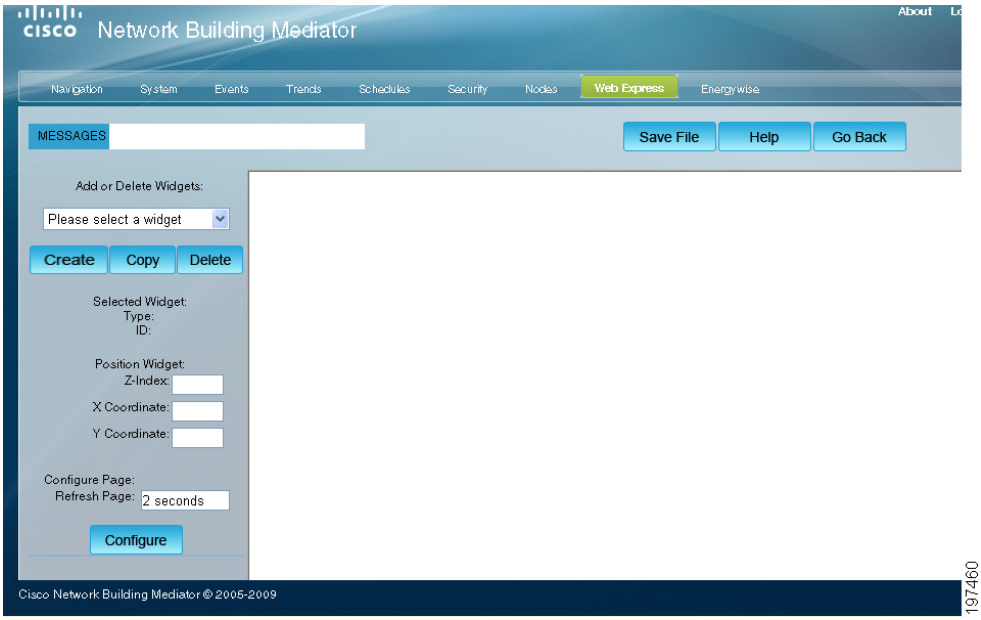


Table 13-1 describes the Web Express drawing pane and the associated elements.

Table 13-1 Web Express Drawing Pane Elements

Element	Description
MESSAGES text box	This text box displays the messages that occur when you preform operations like saving, viewing and editing.
Save File button	Click this button to save the latest changes in the drawing pane.
Help button	Click this button to view the online Web Express Help file.
Go Back button	Click this button to return to the Web Express pane. You can return to the main window irrespective of the number of pages that have been created and edited. (This button is different from the browser back button which only takes you to previously viewed page).
Create button	Click this button to create a widget.
Copy button	Click this button to copy a widget.
Delete button	Click this button to delete a widget.
Configure button	Click this button to control whether the web page refreshes automatically and how often to automatically refresh the web page.

Creating Widgets

Using Web Express, you can create widgets by specifying parameters like graph settings, font, color, axes and configure them to appear in any web page of the Mediator. You can create new widgets, edit existing widgets, copy widgets to other web pages, and delete widgets.

This section includes the following commonly used widgets and the list of additional widgets:

- Adding an Embedded Graph Widget, page 13-4

Send documentation comments to cbsbu-docfeedback@cisco.com

Adding an Embedded Graph Widget

The embedded graph widget allows you to create graphs of preconfigured trends in your web page. The graph allows you to view data over a period of time and also export the information to MS Excel.

For example, if you want to view the temperature changes occurring in an RTU, apply the Trends function to create a trend and measure the temperature variations. Use the embedded graph widget to create a graph for the temperature trend and to view the temperature variations over time.

To learn more about creating a trend, see Creating Trends, page 11-2.

To add an embedded graph widget, perform the following steps:

Step 1 In the Web Express pane, click **Create New File**.

A new HTML drawing pane appears.

Step 2 Choose **EmbeddedGraph** from the Add or Delete Widgets drop-down list.

Step 3 Click **Create**.

The EmbeddedGraph widget pane appears.

Step 4 Click the widget.

The border of the widget turns red and the Configure Widget dialog box appears.

Table 13-2 describes the values you can enter in the Configure Widget dialog box.

Table 13-2 Configure Widget Description for EmbeddedGraph Widget

Text Box	Description
name	Provides the name of the widget.
z index	Enter the z index of the frame. The default is 1000.
graph width	Enter the desired width of the graph. The default is 400px.
graph height	Enter the desired height of the graph. The default is 200px.
log node	Browse to select a preconfigured trend. **Note** You should navigate to the /services/logger folder and choose the trend whose graph you want to embed in your web page.
graph title	Enter the title for the graph.
text fontname	Enter the font type of the text in the graph. The default is Verdana.
text fontsize	Enter the font size of the text in the graph.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 13-2 Configure Widget Description for EmbeddedGraph Widget (continued)

Text Box	Description
text color	Click the color block and choose the color for the text. The default is gray.
background color	Click the color block and choose the background color. The default is black.
y-axis from	Enter the starting point of the y-axis. The default is auto.
y-axis to	Enter the ending point of the y-axis. The default is auto.
y-axis type	Choose the y-axis type as numeric or binary from the drop-down list.
Initial timespan	Enter the time period (width) of the graph.
time reference	Choose the time stamp from the drop-down list.
enable secondary axis	Select the enable secondary axis check box to set the secondary axis parameters.
secondary yaxis points	Enter the starting point of the secondary y-axis. The default is auto
secondary yaxis from	Enter the ending point of the secondary y-axis. The default is auto.
secondary yaxis type	Choose the secondary y-axis type from the drop-down list.
point color	Click the color block and select the color of the point.

Step 5 Enter the configuration values in the appropriate text boxes.

Step 6 Click **Save**.

The Configure Widget dialog box closes.

Step 7 Click **Save File**.

The File Selector dialog box appears.

Step 8 In the File name text box, enter a name for the widget.

Step 9 Select the **Open File after Save** check box.

Step 10 Click **SAVE**.

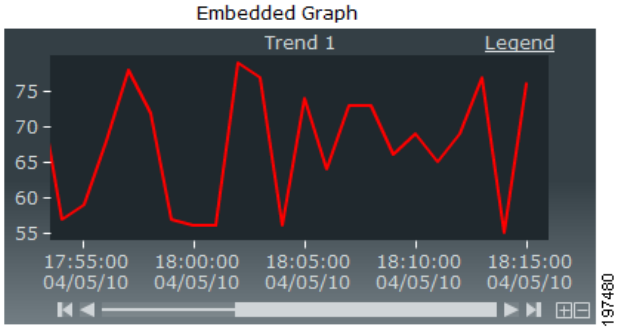
A dialog box appears prompting you to save or cancel.

Step 11 Click **OK**.

An HTML page with the newly created graph appears as shown in Figure 13-3.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 13-3 EmbeddedGraph in an HTML Page



Note You can use the controls at the bottom of the graph to adjust the view.

Adding a Generic Color Status Overlay Widget

The generic color status overlay widget is similar to the generic color status box widget and is the most commonly used overlay tool in Web Express. You can use the generic color status overlay widget to signify changes in the control points being monitored by setting color status boxes to the control points. Changes in the control points would result in the change in color of the status boxes.

For example, you can use the generic color status overlay widget to monitor the temperature of a building. You can create an overlay to see whether the points in the building stays within a predefined range. When the temperature exceeds or drops beyond the specified limits, the color of the overlay changes color and warnings and alarms are generated.

The generic color status overlay widget allows you to add five warning color status boxes in contrast to the generic color status box widget, which allows you to add one warning color status box.

To add a generic color status overlay widget, perform the following steps:

Step 1 In the Web Express pane, click **Create New File**.

A new HTML drawing pane appears.

Step 2 Choose **GenericColorStatusOverlay** from the Add or Delete Widgets drop-down list.

Step 3 Click **Create**.

The GenericColorStatusOverlay widget pane appears.

Step 4 Click the widget.

The border of the widget turns red and the Configure Widget dialog box appears.

Table 13-3 describes the values you can enter in the Configure Widget dialog box.

Table 13-3 Configure Widget Description for GenericColorStatusOverlay Widget

Text Box	Description
name	Provides the name of the widget.
z index	Enter the z index of the frame. The default is 1000.
node	Browse to and select a set point to be monitored.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 13-3 Configure Widget Description for GenericColorStatusOverlay Widget (continued)

Text Box	Description
status box width	Enter the width of the status box. The default is 20px.
status box height	Enter the height of the status box. The default is 20px.
level trigger	Choose the level on which alarm should be triggered.
color opacity	Enter the opacity of the color. The default percentage is 50.
normal color	Click and choose the normal color.
warning	Choose to enable or disable warnings.
warning threshold	Enter the threshold value for warning to be raised. You can enter up to five warning threshold values
warning color	Click and choose the warning color. You can choose up to five warning colors.
alarm	Choose to enable or disable alarms.
alarm threshold	Enter the threshold value for alarm to be raised.
alarm color	Click and choose the alarm color.

Step 5 Enter the configuration values in the appropriate text boxes.

Step 6 Click **Save**.

The Configure Widget dialog box closes.

Step 7 Click **Save File**.

The File Selector dialog box appears.

Step 8 In the File name text box, enter a name for the widget.

Step 9 Select the **Open File after Save** check box.

Step 10 Click **SAVE**.

A dialog box appears prompting you to save or cancel.

Step 11 Click **OK**.

An HTML page with the newly created color status overlay appears.

Adding a Generic Label Widget

A generic label allows you attach information to the elements in the web pages. For example, if you have many images in your web page, you can use the generic label widget to create labels and place specific labels to the images to identify them.

To add a generic label widget, perform the following steps:

Step 1 In the Web Express pane, click **Create New File**.

A new HTML drawing pane appears.

Step 2 Choose **GenericLabel** from the Add or Delete Widgets drop-down list.

Step 3 Click **Create**.

Send documentation comments to cbsbu-docfeedback@cisco.com

The GenericLabel widget pane appears.

Step 4 Click the widget.

The border of the widget turns red and the Configure Widget dialog box appears.

Table 13-4 describes the values you can enter in the Configure Widget dialog box.

Table 13-4 Configure Widget Description for GenricLabel Widget

Text Box	Description
name	Provides the name of the widget.
z index	Enter the z index of the frame. The default is 1000.
text	Enter the label name.
text color	Click the color block and choose the color for the text. The default is black.
text font family	Enter the font type of the label name.
text font size	Enter the font size of the label name. The default is 12px.
text font weight	Enter the thickness of the label text to be displayed. The default is normal.

Step 5 Enter the configuration values in the appropriate text boxes.

Step 6 Click **Save**.

The Configure Widget dialog box closes.

Step 7 Click **Save File**.

The File Selector dialog box appears.

In the File name text box, enter a name for the widget.

Step 8 Select the **Open File after Save** check box.

Step 9 Click **SAVE**.

A dialog box appears prompting you to save or cancel.

Step 10 Click **OK**.

An HTML page with the newly created label appears.

Adding a Generic Image Widget

You can populate your web pages with different types of images using the generic image widget.

To add a generic image widget, perform the following steps:

Step 1 In the Web Express pane, click **Create New File**.

A new HTML drawing pane appears.

Step 2 Choose **GenericImage** from the Add or Delete Widgets drop-down list.

Step 3 Click **Create**.

The GenericImage widget pane appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 Click the widget.

The border of the widget turns red and the Configure Widget dialog box appears.

Table 13-5 describes the values you can enter in the Configure Widget dialog box.

Table 13-5 Configure Widget Description for GenericImage Widget

Text Box	Description
name	Provides the name of the widget.
z index	Enter the z index of the frame. The default is 1000.
Image Source	Browse to select a image to be uploaded.
tooltip	Enter the text that should be displayed in the image when you move the mouse over it.

Step 5 Enter the configuration values in the appropriate text boxes.

Step 6 Click **Save**.

The Configure Widget dialog box closes.

Step 7 Click **Save File**.

The File Selector dialog box appears.

Step 8 In the File name text box, enter a name for the widget.

Step 9 Select the **Open File after Save** check box.

Step 10 Click **SAVE**.

A dialog box appears prompting you to save or cancel.

Step 11 Click **OK**.

An HTML page with the newly created image appears.

Adding a PHAnimation Widget

The PHAnimation widget allows you to include animated graphics, for example, fans, lights, damper position, and so on in your web pages.

You can create static or dynamic animations using this widget. A dynamic animation is activated by a data point and the application cycles through a stack of images with intervals between animations. For a static animation, the application calls images out of a stack depending on the number of images.

For example, you can use the PHAnimation widget to view a damper position and upload 100 animation frames of the damper going from 0 to 100. For example, when the damper returns a value of 42, the application would upload the 42nd image.

To add a PHAnimation widget, perform the following steps:

Step 1 In the Web Express pane, click **Create New File**.

A new HTML drawing pane appears.

Step 2 Choose **PHAnimation** from the Add or Delete Widgets drop-down list.

Step 3 Click **Create**.

Send documentation comments to cbsbu-docfeedback@cisco.com

The PHAnimation widget pane appears.

Step 4 Click the widget.

The border of the widget turns red and the Configure Widget dialog box appears.

Table 13-6 describes the values you can enter in the Configure Widget dialog box.

Table 13-6 Configure Widget Description for PHAnimation Widget

Text Box	Description
name	Provides the name of the widget.
z index	Enter the z index of the frame. The default is 1000.
node	Browse to and select the data.
animation type	Choose the type of animation from the drop-down list.
animation scale	Enter the size (in percentage) to which the image should be displayed.
animation images	Browse to and select the images to be uploaded.
animation width	Enter the width of the animation.
animation height	Enter the height of the animation.
animation interval	Enter the time interval between animations.

Note You must enter the animation scale manually. If you are loading a static and a dynamic image for the same data point, it is important that you ensure that the width and the height of the images are the same prior to loading them to maintain uniformity.

Step 5 Enter the configuration values in the appropriate text boxes.

Step 6 Click **Save**.

The Configure Widget dialog box closes.

Step 7 Click **Save File**.

The File Selector dialog box appears.

Step 8 In the File name text box, enter a name for the widget.

Step 9 Select the **Open File after Save** check box.

Step 10 Click **SAVE**.

A dialog box appears prompting you to save or cancel.

Step 11 Click **OK**.

An HTML page with the newly created animation appears as shown in Figure 13-4.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 13-4 PHAnimation Widget in an HTML Page

Adding a PHVirtualPoint Widget

The PHVirtualPoint widget is commonly used to show a configured data point. You can display a data point as a numerical value, for example, 50 or as a string, for example, off and on. You can also use the widget to signify changes in the data point and the changes in the values can be displayed as changes in colors.

For example, you can configure a node that changes values from 50 to 80 units. You can use the PH virtual widget to show changes in the value of the node. When the node reaches a value of 80, you can set up the node to display red and when it reaches the warning threshold value, you can set the color to change to yellow.

To add a PHVirtualPoint widget, perform the following steps:

Step 1 In the Web Express pane, click **Create New File**.

A new HTML drawing pane appears.

Step 2 Choose **PHVirtualPoint** from the Add or Delete Widgets drop-down list.

Step 3 Click **Create**.

The PHVirtualPoint widget pane appears.

Step 4 Click the widget.

The border of the widget turns red and the Configure Widget dialog box appears.

Table 13-7 describes the values you can enter in the Configure Widget dialog box.

Table 13-7 Configure Widget Description for PHVirtualPoint Widget

Text Box	Description
name	Provides the name of the widget.
z index	Enter the z index of the frame. The default is 1000.
node	Browse to and select the data point.
units	Enter the measurement units. **Note** The units are added as a character to the end of the node, for example,% or F. If you leave it blank, nothing is added to the end of the node.
precision	Enter the number of decimal places till which the value of the node should be displayed.
display character length	Enter the number of characters of the text.
text color	Click the color block and select the color of the text.
text font family	Enter the type of the text font.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 13-7 Configure Widget Description for PHVirtualPoint Widget (continued)

Text Box	Description
text font size	Enter the size of the text font.
text font style	Enter the style of the text font.
text font weight	Enter the thickness of the text font.
upper alarm threshold	Enter the maximum value of the data point beyond which the alarm color should be displayed.
upper warning threshold	Enter the maximum value of the data point beyond which the warning color should be displayed.
lower alarm threshold	Enter the minimum value of the data point below which the alarm color should be displayed.
lower warning threshold	Enter the minimum value of the data point below which the warning color should be displayed.
offline color	Click the color block and select the color to be displayed when the data point is offline. This color is specific to the node background.
normal color	Click the color block and select the color to be displayed when the value of the data point is within the normal range. This color is specific to the node background.
warning color	Click the color block and select the color to be displayed when the value of the data point reaches the warning levels. This color is specific to the node background.
alarm color	Click the color block and select the color to be displayed when the value of the data point reaches the alarm levels. This color is specific to the node background.
override color	Click the color block and select the color to be displayed when the node value has been overridden. This color is specific to the text font. The default color is blue.
pulse length	Enter the length of the pulse.
override enabled	Choose from the override enabled drop-down list.
tooltip	Enter the text that should be displayed in the image when you move the mouse over it.

Step 5 Enter the configuration values in the appropriate text boxes.

Step 6 Click **Save**.

The Configure Widget dialog box closes.

Step 7 Click **Save File**.

The File Selector dialog box appears.

Step 8 In the File name text box, enter a name for the widget.

Step 9 Select the **Open File after Save** check box.

Step 10 Click **SAVE**.

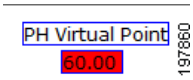
A dialog box appears prompting you to save or cancel.

Step 11 Click **OK**.

Send documentation comments to cbsbu-docfeedback@cisco.com

An HTML page with the newly created PHVirtualPoint appears as shown in Figure 13-5.

Figure 13-5 PHVirtualPoint in an HTML Page



You can change the values that you assigned to the node using the Override option.

To override the value of the node, perform the following steps:

Step 1 Double-click the node.

A value appears in the Override text box.

Step 2 Enter a new value.

Step 3 Click **Override**.

The value changes in the web page.

Adding a Checkbox Widget

A checkbox is a specific type of two-states button that can be either selected or unselected. The checkbox widget creates checkboxes in HTML pages that can be used to select or unselect specific actions.

To add a checkbox widget, perform the following steps:

Step 1 In the Web Express pane, click **Create New File**.

A new HTML drawing pane appears.

Step 2 Choose **Checkbox** from the Add or Delete Widgets drop-down list.

Step 3 Click **Create**.

The Checkbox widget pane appears.

Step 4 Click the widget.

The border of the widget turns red and the Configure Widget dialog box appears.

Table 13-8 describes the values you can enter in the Configure Widget dialog box.

Table 13-8 Configure Widget Description for Checkbox Widget

Text Box	Description
name	Provides the name of the widget.
z index	Enter the z index of the frame. The default is 1000.
node	Browse to and select a node.
selected value	Enter the value to signify the off or the on condition. It can be either 1 or 0.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 13-8 Configure Widget Description for Checkbox Widget

Text Box	Description
selected value label	Enter a label description for the selected condition.
unselected value	Enter the value to signify the off or the on condition. It can be either 1 or 0.
unselected value label	Enter a label description for the unselected condition.
tooltip	Enter the text that should be displayed in the image when you move the mouse over it.
text color	Enter the color with percent specified in the style attribute.
text font family	Enter the type of the font.
text font size	Enter the size of the font. The default is 12px.

Step 5 Enter the configuration values in the appropriate text boxes.

Step 6 Click **Save**.

The Configure Widget dialog box closes.

Step 7 Click **Save File**.

The File Selector dialog box appears.

Step 8 In the File name text box, enter a name for the widget.

Step 9 Select the **Open File after Save** check box.

Step 10 Click **SAVE**.

A dialog box appears prompting you to save or cancel.

Step 11 Click **OK**.

An HTML page with the newly created URL appears.

Adding a Generic Switch Widget

You can use widgets to create switches in your web pages. The switches can be made to change states depending on the changes in the values being monitored.

For example, if the generic switch widget is tied to the air conditioning unit, you can switch the unit on or off by using the toggle functionality of the widget.

The generic switch is similar to checkbox except the image of the button can be changed in the switch widget.

To add a generic switch widget, perform the following steps:

Step 1 In the Web Express pane, click **Create New File**.

A new HTML drawing pane appears.

Step 2 Choose **GenericSwitch** from the Add or Delete Widgets drop-down list.

Step 3 Click **Create**.

The Generic Switch widget pane appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 Click the widget.

The border of the widget turns red and the Configure Widget dialog box appears.

Table 13-5 describes the values you can enter in the Configure Widget dialog box.

Table 13-9 Configure Widget Description for GenericSwitch Widget

Text Box	Description
name	Provides the name of the widget.
z index	Enter the z index of the frame. The default is 1000.
node	Browse to and select a node.
display type	Choose the type of value to be displayed from the drop-down list.
display character length	Enter the number of characters of the text.
text color	Click the color block and choose the color for the text. The default is black.
text font family	Enter the font of the text.
text font size	Enter the size of the text. The default is 12px.
text background color	Click the color block and choose the color for the background. The default is gray.
text align	Choose the alignment of the text from the drop-down list.
text padding bottom	Enter the spacing in pixels between the bottom of the text and the border of the element. The default is 5px.
text padding left	Enter the spacing in pixels between the bottom of the text and the border of the element. The default is 5px.
text padding right	Enter the spacing in pixels between the bottom of the text and the border of the element. The deafult is 5px.
text padding top	Enter the spacing in pixels between the bottom of the text and the border of the element. The default is 5px.
button scale	Enter the size (in percentage) to which the toggle button should be displayed.
toggle button source	Enter the pathname to the directory where the toggle button image is available.
toggle button width	Enter the width of the toggle button image. The default is 50px.
toggle button height	Enter the height of the toggle button image. The default is 20px.

Step 5 Enter the configuration values in the appropriate text boxes.

Step 6 Click **Save**.

The Configure Widget dialog box closes.

Step 7 Click **Save File**.

The File Selector dialog box appears.

Step 8 In the File name text box, enter a name for the widget.

Step 9 Select the **Open File after Save** check box.

Step 10 Click **SAVE**.

Send documentation comments to cbsbu-docfeedback@cisco.com

A dialog box appears prompting you to save or cancel.

Step 11 Click **OK**.

An HTML page with the newly created image appears.

Adding a Generic Alarm Widget

You can use widgets to create visual or audio alarms in your HTML pages.

For example, if you are monitoring the temperature in a room and the temperature exceeds the predefined limits, the alarm widgets can be used to produce visual alarms (where color changes are displayed) or audio alarms (where a sound file is played).

To add a generic alarm widget, perform the following steps:

Step 1 In the Web Express pane, click **Create New File**.

A new HTML drawing pane appears.

Step 2 Choose **GenericAlarm** from the Add or Delete Widgets drop-down list.

Step 3 Click **Create**.

The GenericAlarm widget pane appears.

Step 4 Click the widget.

The border of the widget turns red and the Configure Widget dialog box appears.

Table 13-10 describes the values you can enter in the Configure Widget dialog box.

Table 13-10 Configure Widget Description for GenericAlarm Widget

Text Box	Description
name	Provides the name of the widget.
z index	Enter the z index of the frame. The default is 1000.
node	Browse to select a image to be uploaded.
level trigger	Choose the alarm trigger level from the drop-down list.
alarm threshold	Enter the value at which the alarm should be displayed.
sound file	Enter the pathname to the directory where the sound file is available.
sound duration	Choose the number of times the alarm is notified from the drop-down list.
animation type	Choose the type of animation from the drop-down list.
animation scale	Choose the size (in percentage) to which the animation image should be displayed.
animation directory	Enter the pathname to the directory where the animation file is available.
animation images	Enter the alarm image names separated by commas.
animation width	Enter the width of the animation image. The default is 100px.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 13-10 Configure Widget Description for GenericAlarm Widget

Text Box	Description
animation height	Enter the height of the animation image. The default is 50px.
animation interval	Enter the time interval between two animation images. The default is 250.

Step 5 Enter the configuration values in the appropriate text boxes.

Step 6 Click **Save**.

The Configure Widget dialog box closes.

Step 7 Click **Save File**.

The File Selector dialog box appears.

Step 8 In the File name text box, enter a name for the widget.

Step 9 Select the **Open File after Save** check box.

Step 10 Click **SAVE**.

A dialog box appears prompting you to save or cancel.

Step 11 Click **OK**.

An HTML page with the newly created image appears.

Additional Widgets

Table 13-11 describes the additional widgets and their functionality.

Table 13-11 Additional Widgets

Widget	Allows you to
EmbeddedMiniGraph	Insert graphs in web pages. This widget is similar to the embedded graph widget, except that it has smaller dimensions.
GenericColorStatusBox	Create status boxes that change colors depending on the changes in the control points being monitored. The status boxes can generate warnings and alarms and signify when alarms are offline or online.
GenericLabelBox	Create labels in your web pages. This widget is similar to the generic label widget, except that it creates labels that have more spacing between the text and the border.
GenericNode	Insert nodes in your web pages.
GenericNodeBox	Insert nodes in your web pages. This widget is same as the generic node, except that it creates nodes that have more spacing between the text and the border.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 13-11 Additional Widgets

Widget	Allows you to
GenericOverride	Create overridable nodes in your web pages.
OverridablePoint	View changes in values of a configured data point. This widget is same as the PH virtual point widget, except that it allows you to specify a timed override in periods of seconds, minutes, hours, or indefinite.

Configuring the Refresh Rate of Web Pages

Configuring the refresh rate of web pages ensures the latest data is available on the browser. You can choose to control whether the page refreshes automatically and how often the page gets refreshed automatically. The refresh settings that you specify in the drawing pane affects the refresh mode of the web pages.

To configure the refresh rate of a web page, perform the following steps:

Step 1 In the Mediator web client, click **Web Express**.

The Web Express pane appears.

Step 2 Choose the web page you want to modify from the drop-down list.

Step 3 Click **Create New File**.

A blank Web Express drawing pane appears.

Step 4 Click Configure.

The Configure Page dialog box.

Step 5 In the Configure Page dialog box, perform the following steps:

a. From the refresh rate drop-down list, choose the web page refresh rate. The default is 2 seconds.

b. In the user name text box, enter the username.

c. In the user password text box, enter the password.

d. In the html title text box, enter the name of the HTML page you want to refresh.

e. Click the color box next to the html body background color text box.

The Select Color dialog box appears.

f. Double-click a color to choose it.

The Select Color dialog box closes and returns you to the Configure Page dialog box. You will see that the color box depicts the color you chose and the html body background color text box contains the corresponding hexadecimal value.

g. Click **Save** to save the changes.

Send documentation comments to cbsbu-docfeedback@cisco.com

Viewing Web Pages

The web pages created in each of the Mediators in the network are loaded into the directory of the Mediator. These HTML pages can be viewed in the Mediator using the Web Express pane.

To view a web page, perform the following steps:

Step 1 In the Mediator web client, click **Web Express**.

The Web Express pane appears.

Step 2 Choose the web page you want to view from the drop-down list.

Step 3 Click **View Selected File**.

The selected web page is displayed.

Editing Web Pages

To edit an existing drawing, perform the following steps:

Step 1 In the Mediator web client, click **Web Express**.

The Web Express pane appears.

Step 2 Choose the web page you want to modify from the drop-down list.

Step 3 Click **Edit Selected File**.

The web page to be edited appears as the drawing pane.

Deleting Web Pages

You can use Web Express to delete the web pages stored in the Mediator default directory.

To delete a web page, perform the following steps:

Step 1 In the Mediator web client, click **Web Express**.

The Web Express pane appears.

Step 2 Choose the web page you want to delete from the drop-down list.

Step 3 Click **Delete Selected File**.

A dialog box appears prompting you to confirm the operation.

Step 4 Click **OK**.

The web page is deleted and a dialog box appears confirming that the operation was successful.

Send documentation comments to cbsbu-docfeedback@cisco.com

Copying Multiple Web Pages

You can use Web Express to make multiple copies of a web page. The copies will be stored in the Mediator directory.

The Copy Multiple feature is used to make copies of VAV monitor drawings.

To copy multiple web pages, perform the following steps:

Step 1 In the Mediator web client, click **Web Express**.

The Web Express pane appears.

Step 2 Choose the web page you want to copy from the drop-down list.

Step 3 Click **Copy Multiple Files.**

The Web Express Copy Multiple files pane appears.

Step 4 Choose the template file from the drop-down list.

The template file name appears in the File Base Name text box. The file name appears with a tilde (~) in the name.

Step 5 In the Number of Copies text box, enter the desired of the copy files.

Step 6 Click **Copy Multiple**.

A message appears indicating that the operation is completed successfully.

Step 7 Click **Web Express**.

The Web Express pane reappears. The web pages are available in the drop-down list.

Deleting Multiple Files

To delete multiple web pages, perform the following steps:

Step 1 In the Mediator web client, click **Web Express**.

The Web Express pane appears.

Step 2 Click **Delete Multiple Files.**

The Web Express Delete Multiple Files pane appears.

Step 3 Choose the files that you want to delete from the drop-down list.

Press **Shift+Click** to select a contiguous range or press **Ctrl+Click** to select multiple items.

Step 4 Click **Delete**.

The Confirm Delete dialog box appears.

Step 5 Click **Yes to All**.

The list of web pages is updated and the web pages that were not deleted remain in the list.

Send documentation comments to cbsbu-docfeedback@cisco.com

Uploading Files

You can upload files, for example, custom artwork, PDF files of cut sheets or Operations and Maintenance manuals, text files, and spreadsheets from your PC to the Mediator. The files can then be incorporated into web page drawings that you create with Web Express.

The graphics files (gif, png, or jpg) are uploaded to the /images folder of the Mediator and the HTML files are uploaded to the root folder. Any other files that you upload (pdf, zip, doc, and so on) are routed to the /webexpressuploads folder.

To upload a file, perform the following steps:

Step 1 In the Mediator web client, click **Web Express**.

The Web Express pane appears.

Step 2 Click **Upload A File.**

The Web Express Upload pane appears.

Step 3 Click **Browse**.

Step 4 Navigate to and choose an image file to upload.

Step 5 Click **Upload File**.

A message appears indicating that the file has been uploaded successfully.

Step 6 Click **Continue**.

The Web Express homepage appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 14

Energywise Manager

This chapter describes how to configure and view the Energywise service and energy consumption using configTOOL and the Mediator.

This chapter includes the following topics:

About Energywise Manager

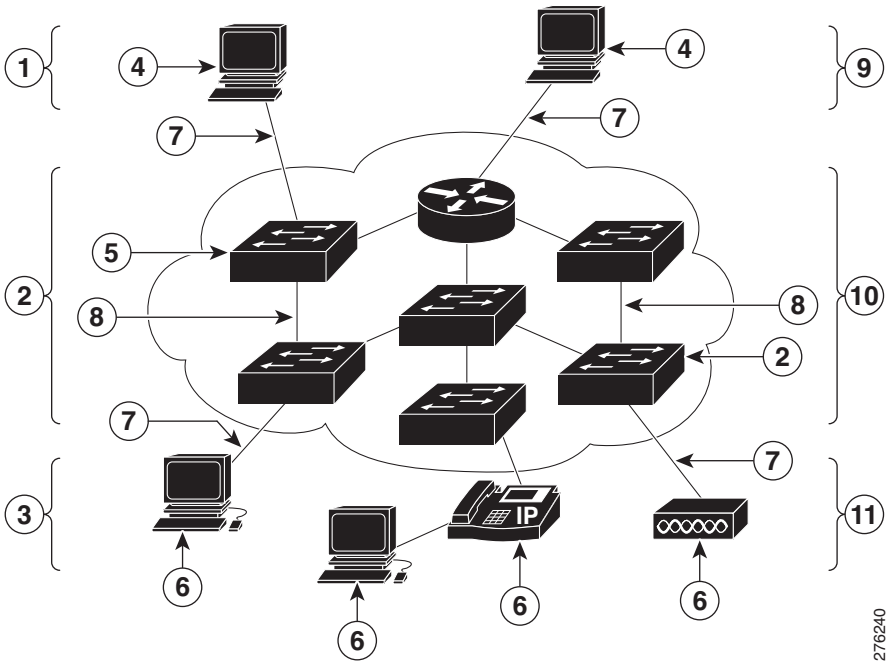
Cisco Energywise is a Cisco IOS-based software application that enables Cisco networks to control and perform energy management. The Energywise software enables customers to monitor, control, and report on the energy use of building equipment and IT devices using an Energywise-enabled network. More importantly, Energywise enables customers to set dynamic power policies that enable them to save money and reduce greenhouse gas emissions when equipment is not in use. Energywise is part of Cisco IOS within Cisco Catalyst switches, ISR routers, and other equipment. A software toolkit is available for customers to communicate with a Cisco network to monitor and control Energywise information.

Energywise gives customers the ability to monitor and control AC-powered devices like smart power distribution units, building systems, and PCs. It also enables customers to control the power consumption of networking equipment including routers, LAN switches, and connected Power over Ethernet (PoE) devices, such as phones, access points, IP security cameras, and door access equipment. Energywise can orchestrate power control across a series of devices in the network.

In an Energywise network, Energywise monitors and manages the power usage of powered devices, Cisco devices in a *domain* and the *end points* connected to them. An end point can be a device connected to the network, such as an IP phone, access point, or PC. An *entity* refers to a *domain member* or an end point. You can configure policies, referred to as recurring events, to manage the power usage (See Figure 14-1).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 14-1 Energywise Network



1	Network management stations	7	TCP
2	Domain members	8	UDP
3	End points	9	Runs queries
4	Management station	10	Runs, forwards, and responds to queries
5	Domain member	11	Responds to queries
6	End point		

- Management stations—Control applications and devices that use Energywise to monitor and manage the power usage of domain members and end points. Management stations also send queries.
- Domain members—Cisco switches, routers, and network devices that use power. They forward messages across the network to form an Energywise domain with other Cisco devices and end points. They also forward and reply to queries from the management station and from other domain members and aggregate power-usage information from the end points.

  A domain is treated as one unit of power management and is similar to a network-management community.
- End points—Devices that use power. They only respond to queries.

  Domain members and end points can receive power from an AC power source, a DC power source, or a power supply. Power over Ethernet (PoE) domain members and end points can also receive power from PoE switches or Cisco EtherSwitch service modules. For example, IP phones and access points connected to a PoE switch receive power from the switch.

Send documentation comments to cbsbu-docfeedback@cisco.com

Requirements for Energywise Manager

By default, Energywise is disabled on Cisco network devices. All domain members must run either:

- Energywise Phase 1
- Energywise Phase 2 or later

Note Energywise Phase 2 is not backward-compatible with Energywise Phase 1.

Phase 2 implementation of Energywise on the Mediator supports two modes of communication:

- Using SNMP
- Using Energywise Query/Native method

Note For Energywise Query/Native method, you need Energywise Phase2 or above running on the switches. You do not need SNMP enabled on the Mediator. You can get data for the complete Energywise domain by configuring one switch on the Mediator.

We recommend that before you begin configuring the Energywise service on the Mediator, you perform the following tasks:

- Enable Energywise
- Create an Energywise domain on the switch
- Add switches to the domain
- Configure POE / non-POE devices connected to the switches
- Verify the Energywise domain information on the switch

For more information on Energywise Phase 1, go to http://www.cisco.com/en/US/docs/switches/lan/energywise/phase1/ios/configuration/guide/ew_v1.html

For more information on Energywise Phase 2, go to https://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/configuration/guide/ew_v2.html

For more documentation on Energywise, go to http://energywise.cisco.com.

Configuring Energywise Manager

Note

- If you are configuring the Energywise service on the Mediator to run on the Native mode, you do not need SNMP enabled on the Mediator.

Note

- If you are configuring the Energywise service on the Mediator, to run on the SNMP mode, ensure that you have enabled SNMP on the switch.
  To configure SNMP, in the node tree pane of the configTOOL window, right-click the network node, and choose **Add** from the drop-down list. The Available Devices dialog box appears. Choose **SNMP (SNMP)** from the list, and then click **OK**.

Send documentation comments to cbsbu-docfeedback@cisco.com

When you configure SNMP on an Energywise switch, the Energywise MIB elements are discovered and created at the following location: /services/network/SNMP/Remote Agents/EW Switch. These MIB elements provide the flexibility to control individual Energywise entities.

To add the Energywise Manager using configTOOL, perform the following steps:

Step 1 Start the configTOOL and connect to a Mediator (see Accessing Mediators Using configTOOL, page 4-11 for further information).

The configTOOL window appears.

Step 2 In the node tree pane of the configTOOL window, right-click the services node, and choose **Add** from the drop-down list.

The Available Devices dialog box appears.

Step 3 In the Available Devices dialog box, choose **Energywise Manager (Energywise Manager)** from the list, and then click **OK**.

A new child node, Energywise Manager_1, appears under the Services node in the node tree pane.

Step 4 In the node tree pane, right-click the Energywise Manager_1 node, and choose **Add** from the drop-down list to add a domain.

The Available Devices dialog box appears.

Step 5 In the Available Devices dialog box, click the **Build EW Domain hierarchy (EW Domain)**, and then click **OK**.

A new child node, EW Domain, appears under the Energywise Manager_1 node in the node tree pane.

Step 6 In the Name text box, enter the same Energywise domain as specified on the switch.

For example, if the Energywise domain configured on the switch is *A.B.C*, configure the Energywise domain hierarchy on the Mediator as follows:

a. In the Name text box, enter A.

b. In the node tree pane, right-click the A node, and choose **Add** from the drop-down list. The Available Devices dialog box appears.

c. In the Available Devices dialog box, click **Build EW Domain hierarchy (EW Domain)**, and then click **OK**.

A new child node, EW Domain, appears under the A node in the node tree pane.

d. In the Name text box, enter B.

e. In the node tree pane, right-click the B node, and choose **Add** from the drop-down list. The Available Devices dialog box appears.

f. In the Available Devices dialog box, click **Build EW Domain hierarchy (EW Domain)**, and then click **OK**.

A new child node, EW Domain, appears under the B node in the node tree pane.

g. In the Name text box, enter C.

Therefore, an Energywise domain A.B.C on the switch translates to a hierarchical domain structure on the Mediator.

Step 7 In the node tree pane, right-click the C node, and choose **Add** from the drop-down list to add a switch.

Note Before adding a switch, ensure that at least one domain is configured under Energywise Manager because a switch cannot be directly added to Energywise Manager.

Send documentation comments to cbsbu-docfeedback@cisco.com

The Available Devices dialog box appears.

Step 8 In the Available Devices dialog box, click **Energywise Switch (EW Switch)**, and then click **OK**.

A new child node, EW Switch, appears under the EW Domain node in the node tree pane.

Step 9 Enter the switch details in the following text boxes:

- Name: Enter a name for the switch. This name does not have to match the hostname on the switch.
- Description: Enter a description of the switch.
- IP Address: Enter the IP address of the switch. This is a mandatory text box.
- Shared Secret: Enter the Energywise switch shared secret. This is a mandatory text box for all the switches.
- Management Port: Enter the management port value in this text box. This value should match the management port value configured on the switch. The default value is 43440. This text box is not used for SNMP enabled switch.
- Primary: Select this check box if you want to configure this switch as the primary switch. A primary switch is used as the primary point of contact for collection of information from the domain and is valid for Native switch configuration only.
- Protocol: Choose Native or SNMP from the Protocol drop-down list. This option changes the mode of communication to SNMP or Native method.

Note You cannot combine both Native and SNMP enabled switches under a single domain configuration.

- SNMP Version: Choose v1 or v2c from the SNMP version drop-down list. The default value is v2c. All switches in a domain should be either v1 or v2c switches, a combination of both types is not allowed.

The following text boxes contain default values. You should change the values in these text boxes to reflect the configuration on the switches, if required.

- Community Name
- Security Name
- User Name
- Authentication Protocol
- Authentication Key
- Privacy Protocol
- Privacy Key
- Debug

Step 10 Click the **Save** icon to save the configuration.

Step 11 (Optional) To delete the Energywise Manager, right-click the Energywise Manager node, and choose **Delete** from the drop-down list.

Send documentation comments to cbsbu-docfeedback@cisco.com

Viewing Energy Consumption

This section explains how the Mediator web client can be used to query and get accumulated energy consumption value for a domain or group of domains.

In the case of desktop switches, the switch reports a constant energy consumption value. In future implementations, this limitation is likely to be addressed. However, in the case of 4500 and 6000 series switches, actual energy consumption values are reported.

This section includes the following topics:

Viewing Reports

To view reports using the Mediator web client, perform the following steps:

Step 1 Launch an Internet browser (for example, Internet Explorer) and browse to the Cisco Network Building Mediator homepage. To do so, enter the IP address of the Mediator in the Address bar of the browser and log in when prompted.

The web client homepage appears in the Internet browser window.

Step 2 Click **Energywise**. The Energywise pane appears.

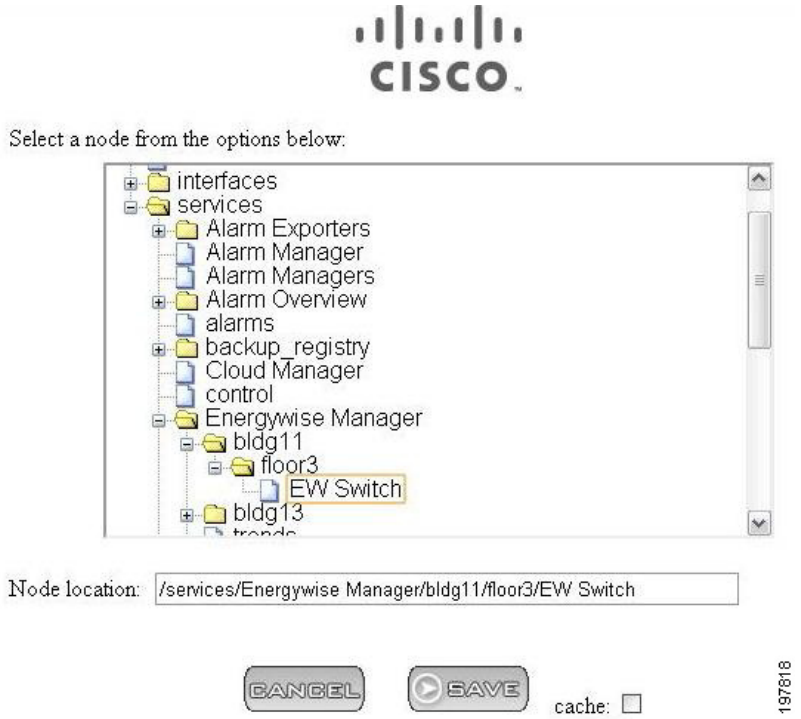
Step 3 Click the **Configure** tab. The tab displays Frequency for a domain and the configured Energywise Domain. The frequency signifies the time period after which the domain energy consumption value will be refreshed.

The user can add more domains. To add a new domain, perform the following steps:

- Click the plus (+) symbol. A new row appears.
- Click Browse in the Energywise Domain column, and click the domain as shown in Figure 14-2.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 14-2 Energywise Domain Browser



– Click **SAVE**. A new domain has now been added and is displayed on the Configure tab.

Step 4 (Optional) To delete the Energywise domain, click the minus (-) symbol in the Energywise Domain column. This removes the Energywise domain from the Trend Manager also.

The configured domains can be viewed using the following methods:

- Using the Report tab
- Using the Trends tab

For viewing the configured domains using the Report tab, go to Step 5.

For viewing the configured domains using the Trends tab, see Viewing Trends, page 11-3

Note For domains configured using Energywise > Configure tab, you can only view them using the Trends tab. You cannot edit or delete these domains using the Trends tab.

Step 5 Click the **Report** tab. The Report tab appears.

This tab displays the configured domains as in the Configure tab.

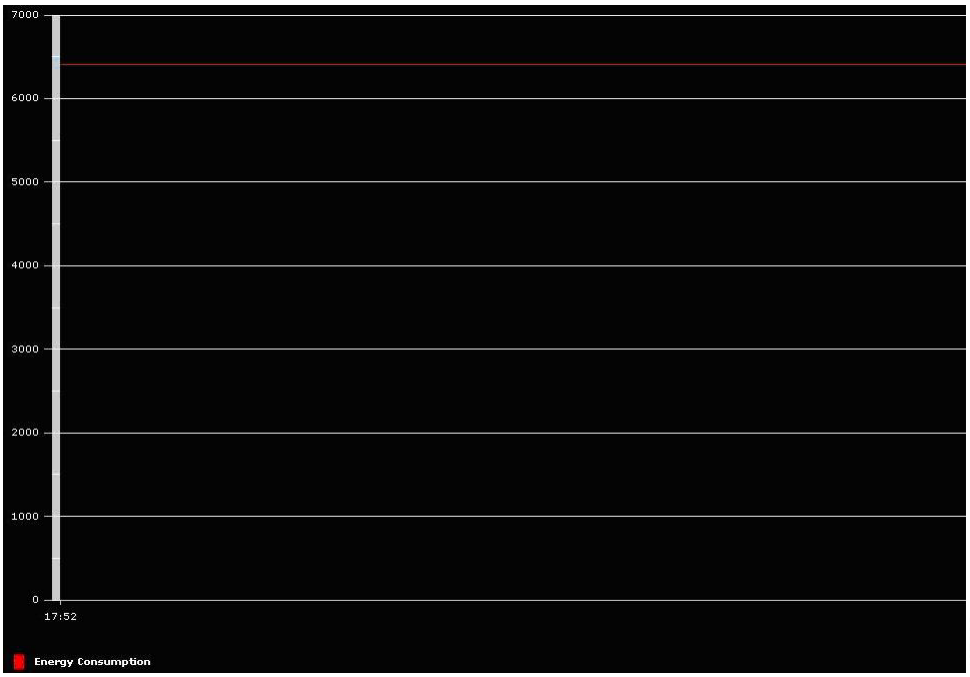
Step 6 Click the ellipsis (...) button next to the Energywise Domain. Browse in the Energywise Domain column and click the domain for which you want to generate the graph.

Note You can create only one trend for each point in a domain.

Step 7 Click **GenerateGraph** to generate a graph for a particular domain. A graph appears as shown in Figure 14-3.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 14-3 Energywise Graph



Note Trends that are created on the Report tab can also be viewed using the Trends tab. However, you cannot use the Report tab to view trends that are created on the Trends tab.

Viewing a List of Entities

To view a list of entities using the Mediator web client, perform the following steps:

Step 1 Launch an Internet browser (for example, Internet Explorer) and browse to the Cisco Network Building Mediator homepage. To do so, enter the IP address of the Mediator in the Address bar of the browser and log in when prompted.

The web client homepage appears in the Internet browser window.

Step 2 Click **Nodes**. The node tree pane appears.

Step 3 In the node tree pane, expand **services > Energywise Manager**.

The values for the network status and the framework status are displayed.

Step 4 Browse to the switch level to view the switch details.

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 15

Enterprise Navigation

This chapter describes the overview of the enterprise navigation feature, how to configure and set up the navigation tree in the Cisco Network Building Mediator (Mediator) and includes the following sections:

About Enterprise Navigation

This section describes the enterprise navigation feature and includes the following topics:

Overview

The enterprise navigation feature enables you to browse all the systems connected to the Mediator and navigate to different levels. Using the navigation tree, you can monitor and control systems attached to the Mediator in real time.

Understanding Enterprise Navigation

The navigation tree is used by the System Integrator (SI) to navigate all the systems that are connected to the Mediator. It provides a hierarchical tree structure, Search text box, a Display tab, a Properties tab and a Global Setpoints tab. It is possible to view the system graphics and real-time value of all the points in the Mediator. The value of editable points may be set directly from the Enterprise Navigation portal.

The hierarchical tree enables you to search through entities by traversing the navigation tree and expanding the entities. The search text box enables you to find and display the desired entities from the navigation tree, instead of traversing the entire tree and expanding the entities. The Display tab is used

Send documentation comments to cbsbu-docfeedback@cisco.com

to present a graphical view that summarizes key system data. The Properties tab lists all points and its attributes associated with a particular device. The Global Set points tab enables you to set point control for changing system set points across entities.

Enterprise Navigation Terms

- Downstream Mediator—The Mediator to which different subsystems and devices are connected physically through the interfaces like RS-485 ports, RS-232 ports, Ethernet ports, and so on.
- Navigation Tree—Provides the hierarchical tree structure of the system from where you can select the level and view the Navigation pane.
- Navigation Pane—Consists of a Display tab and a Properties tab. The Display tab is used to present a graphical view that summarizes key system data. The Properties tab lists all points and its attributes that are associated with a particular device.
- Entity Root—The container for all entities that are attached to a Mediator.

Note A navigation tree may have multiple roots and in turn the root may have sub-roots, depending upon how you want to define the hierarchy during deployment.

- Entity—A child of the Entity root that represents a group of devices or a particular device that controls or monitor a piece of equipment.
- Device—The hardware that controls a piece of equipment based on sensor inputs and the control program in memory of the module.
- Points—Generic term used to describe a single item of information in a building control system. For example, the temperature of a room, the duct pressure of an Air Handling Unit (AHU), and the chiller water flow rate are some examples of points.
- User—Refers to an end user (you) who operates the system (Mediator). The user is identified by a name and a password.

Creating a Navigation Tree in Mediator Using configTOOL

This section describes how to create a navigation tree in the Mediator and includes the following topics:

Adding an Entity Root

To create an entity root in the navigation tree using configTOOL, perform the following steps:

Step 1 Launch the Mediator configTOOL main window.

For more information, see:

- Starting configTOOL, page 4-3

Send documentation comments to cbsbu-docfeedback@cisco.com

- Accessing Mediators Using configTOOL, page 4-11.

The Mediator configTOOL window appears.

Step 2 In the node tree pane, click the host node of the Mediator (represented by an IP address) to display the anchor nodes (aliases, interfaces, and services).

Step 3 To expand the aliases node tree, click **aliases**.

The node tree pane displays the available aliases in the navigation tree and on the aliases tab.

The aliases tab appears in the right part of the Mediator Configuration Tool window. The default name and description of the connected device appear in the upper area of the tab.

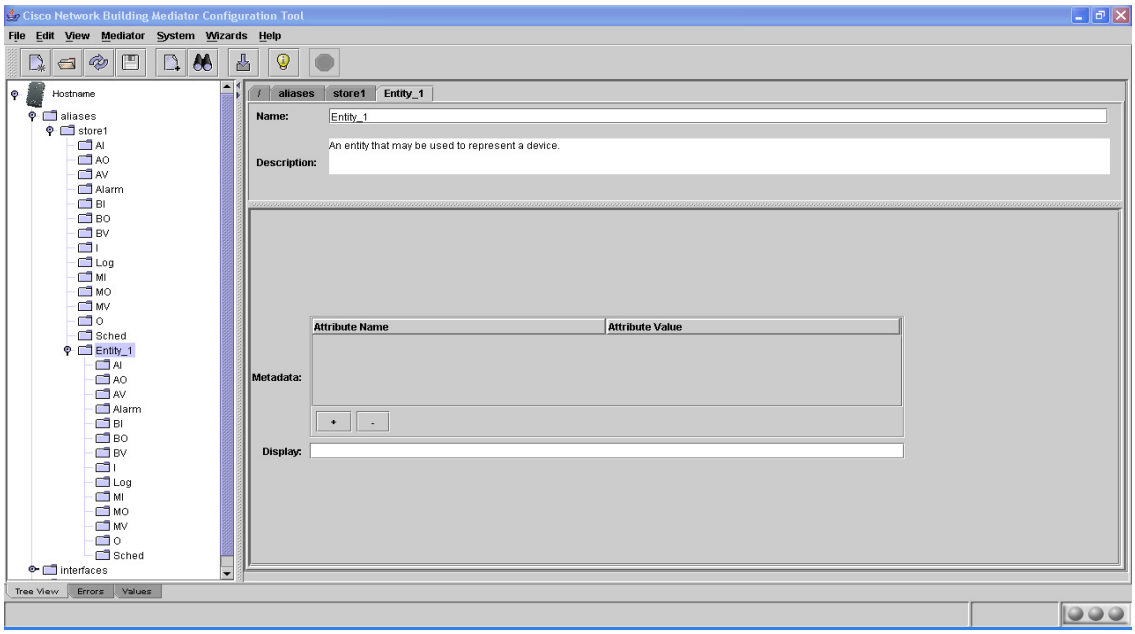
Step 4 To add an entity root to the aliases node, right-click **aliases**, and then choose **Add** from the right-click menu.

The Available Devices dialog box appears. This dialog box displays the list of available devices that can be added to the aliases node.

Step 5 Choose **Entity root**, and then click **OK**.

A new entity root appears under the aliases node in the node tree pane along with the properties. (See Figure 15-1.)

Figure 15-1 Entity root Node



The tab displays the default name (Entity Attach Point) and description of the node in the upper area, and the configured parameters in the lower area.

Step 6 (Optional) To change the default name and description of the entity root node, do the following:

a. In the Name text box, enter the new name (for example,Store1) and then press **Enter**.

The entity root node is renamed and appears in the node tree pane.

Note See Table 15-1 for the description of Entity properties.

b. In the Description text box, enter a description to identify the purpose of this node.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note In the Display text box, enter the URL of a web page that represents this element. For example, /store_dash.html.

Note The web page can be added in the Mediator and stored in /var/mpx/www/http, before the page is added in the Display text box.

Step 7 In the Hostname text box, enter the hostname of the Mediator.

The default is localhost.

Step 8 (Optional) In the Mount point text box, retain the default value.

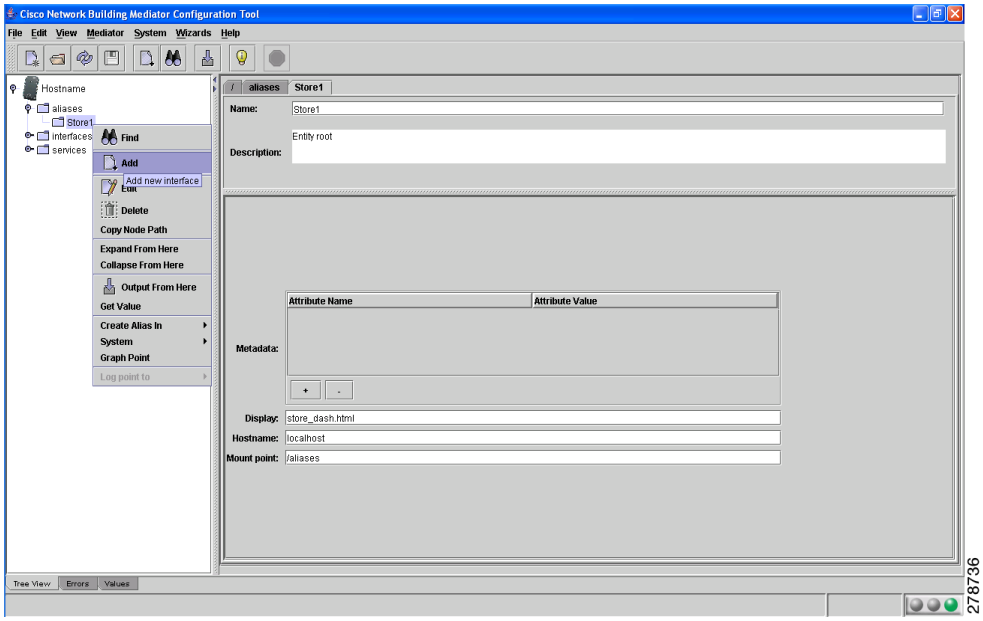
The default is /aliases.

Adding an Entity

To add an entity to the entity root node in the navigation tree, perform the following steps:

Step 1 Right-click the entity root and then choose **Add** from the right-click menu. See Figure 15-2.

Figure 15-2 Adding an Entity



Step 2 The Available Devices dialog box appears and displays the list of available devices that can be added to the entity root node.

Step 3 Choose **Entity** and then click **OK**.

Send documentation comments to cbsbu-docfeedback@cisco.com

A new child node and a list of entity property groups appear under the entity root in the node tree pane. The new child nodes created will be Entity_1,Entity_2, and so on.

Table 15-1 describes the entity property groups and their description.

Table 15-1 Entity Properties

Property	Refers to
AI	A group of analog input properties.
AO	A group of analog output properties.
AV	A group of analog value properties.
Alarm	A group of alarm properties.
BI	A group of binary input properties.
BO	A group of binary output properties.
BV	A group of binary value properties.
I	A group of generic input properties.
Log	A group of log properties.
MI	A group of multistate input properties.
MO	A group of multistate output properties.
MV	A group of multistate value properties.
O	A group of generic output properties.
Sched	A group of schedule properties.

The Entity_1 tab displays the default name (Entity_1) and description of the Entity_1 node in the upper area, and the configured parameters in the lower area.

Step 4 (Optional) To change the default name (for example, RTU01) and description of the entity node, perform the following steps:

a. In the Name text box, enter the new name, and then press **Enter**.

The entity is renamed and appears in the node tree pane.

b. In the Description text box, enter a description to identify the purpose of this node.

In the Display text box, enter the URL of a web page that represents this element.

Note The web page should be built before it can be added in the Display text box.

Step 5 To add the entity property under the entity property group, right-click **Property Group** and choose **Add**.

Step 6 In the Available devices dialog box, choose **Property** and click **OK**.

The Property tab displays the default name (Property) and description of the Property node in the upper area, and the configured parameters in the lower area.

Step 7 (Optional) To change the default name (for example, Occupancy) and description of the property node, perform the following steps:

a. In the Name text box, enter the new name (Occupancy), and then press **Enter**.

The property is renamed and appears in the node tree pane.

Send documentation comments to cbsbu-docfeedback@cisco.com

b. In the Description text box, enter a description to identify the purpose of this node.

Step 8 In the Refers to text box, enter the node path of the Property. For example, /services/network/BACnet/internetwork/Devices/76004/19/11.

Step 9 In the Label text box, enter the label for the Property.

Step 10 In the Description text box, enter a description to the Property.

Note The metadata attribute named 'purpose' is needed for global set point feature, while the value is a user defined string. The Global Setpoint will discover and give the user all purposes that have been defined, as 'point type'. For more information, see Discovery, page 16-12.

Saving the Configuration

To save the Mediator configuration file, perform the following steps:

Step 1 Choose **File > Save Configuration**.

A Confirmation request dialog box appears.

Step 2 Click **Yes** to save the confirmation.

A Save configuration progress dialog box appears.

The configuration file is saved and the Mediator reboots.

Step 3 Click **Connect** to connect to the Mediator.

Verifying the Point Association

To verify the Mediator configuration and check if you can get the values for a particular point, perform the following steps:

Note See Mediator configTOOL, page 4-1 for adding property under entities and how to associate the node path.

Step 1 Right-click a point in the node tree pane, and then choose **Get Value** from the shortcut menu.

A Get Value dialog box appears.

Step 2 The Node path text box displays the value of the node and the node path.

Step 3 Click **OK**.

Send documentation comments to cbsbu-docfeedback@cisco.com

Verifying the Link to the Web Pages

To verify the link to the web pages, verify that the proper URL appears in the Display text box for the entity root (see Figure 15-1) and for the entity as shown in Figure 15-2.)

Viewing the Navigation Tree Using a Web Browser

To view the navigation tree in the Mediator, perform the following steps:

Step 1 Open a web browser and enter the Mediator IP address.

Step 2 Enter the username and password.

The Mediator homepage appears, see Customizing HTML Pages Using Web Express, page 13-1.

Step 3 In the Mediator homepage, click the **Navigation** tab.

The left pane displays the navigation tree and the right pane displays the Display and Properties tabs. You can click and navigate to various nodes in the Navigation pane to monitor the real-time status of all devices and entities in the tree.

Step 4 Click the **Display** tab.

The Display tab displays the corresponding web page defined the configTOOL. This web page is typically used to display summary status information for an entity. (See Figure 15-3.)

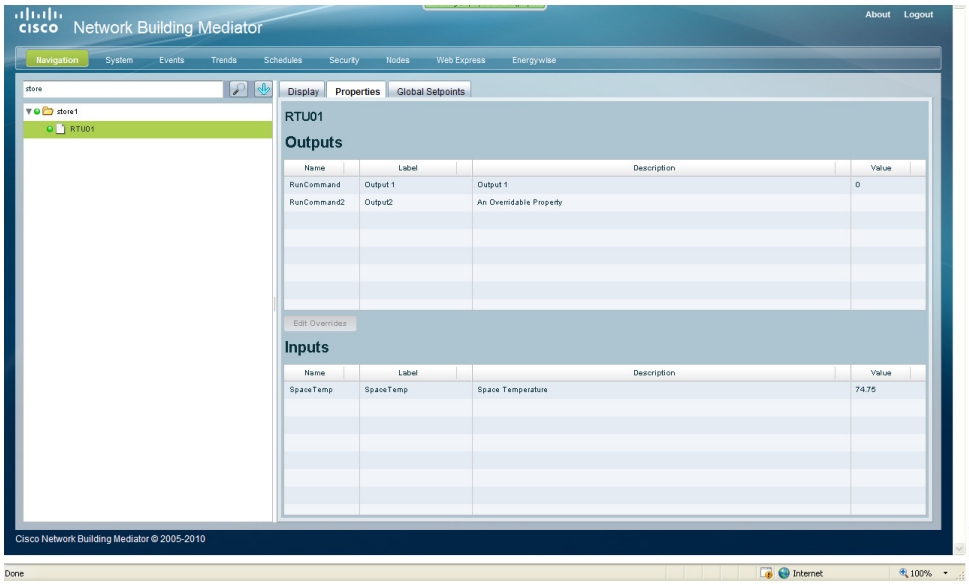
Figure 15-3 Navigation - Display Tab

Step 5 Click the **Properties** tab.

The Properties tab displays the output and input properties defined in configTOOL. (See Figure 15-4.)

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 15-4 Navigation - Properties Tab



Searching Entities in the Navigation Tree

To search entities in the navigation tree in the Mediator, perform the following steps:

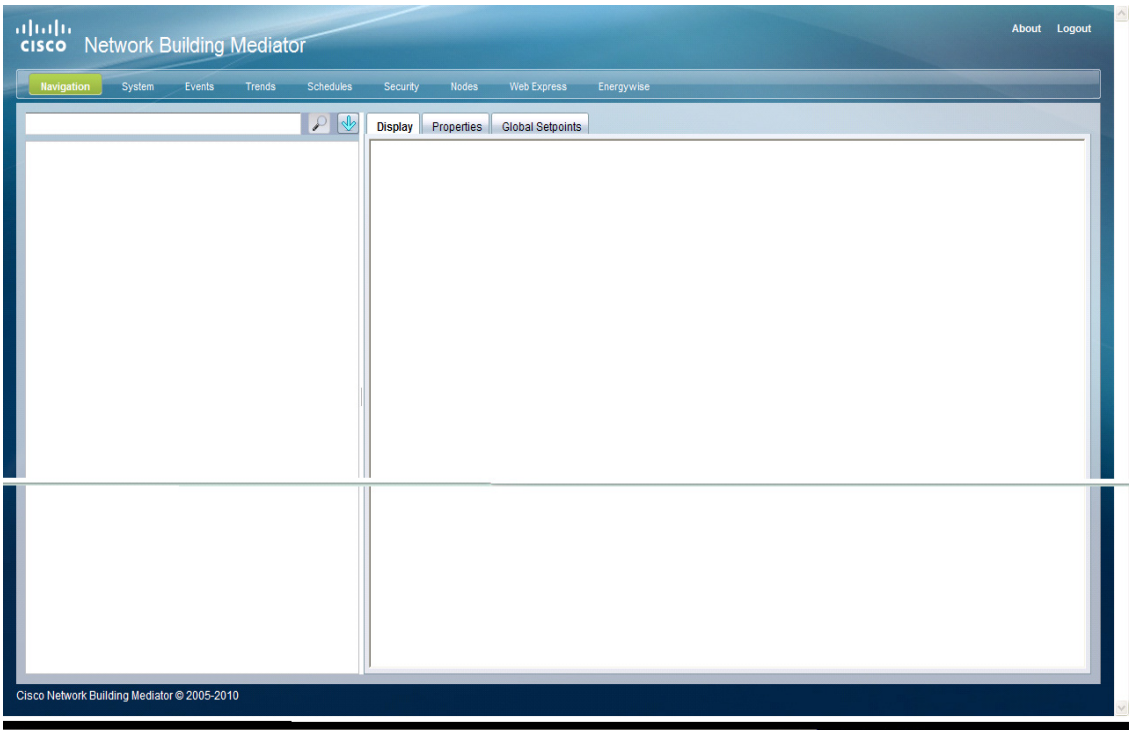
Step 1 Open a web browser and enter the Mediator IP address.

Step 2 Enter the username and password.

The Mediator homepage appears, see Customizing HTML Pages Using Web Express, page 13-1.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 15-5 Cisco Network Building Mediator - Navigation



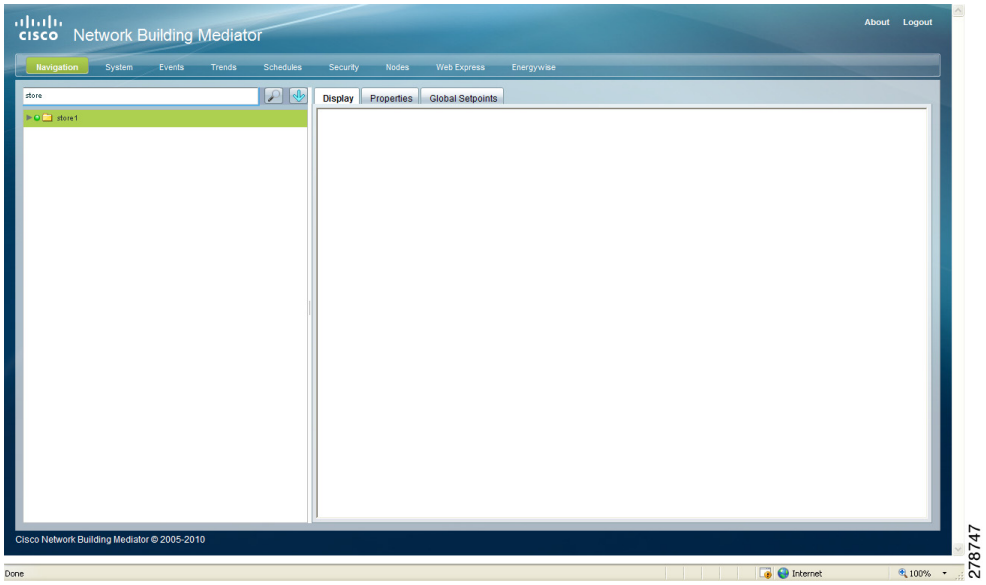
Step 3 In the Mediator homepage, click **Navigation**.

The left pane displays the search text box and the navigation tree. The right pane displays the Display, Properties and Global Setpoints tabs. You can search for the desired navigation tree entities using the search text box instead of traversing through the entire tree and expanding the entities. (See Figure 15-6.)

Step 4 Enter the desired entity name in the search text box, and click the **Search** icon.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 15-6 Cisco Network Building Mediator - Search



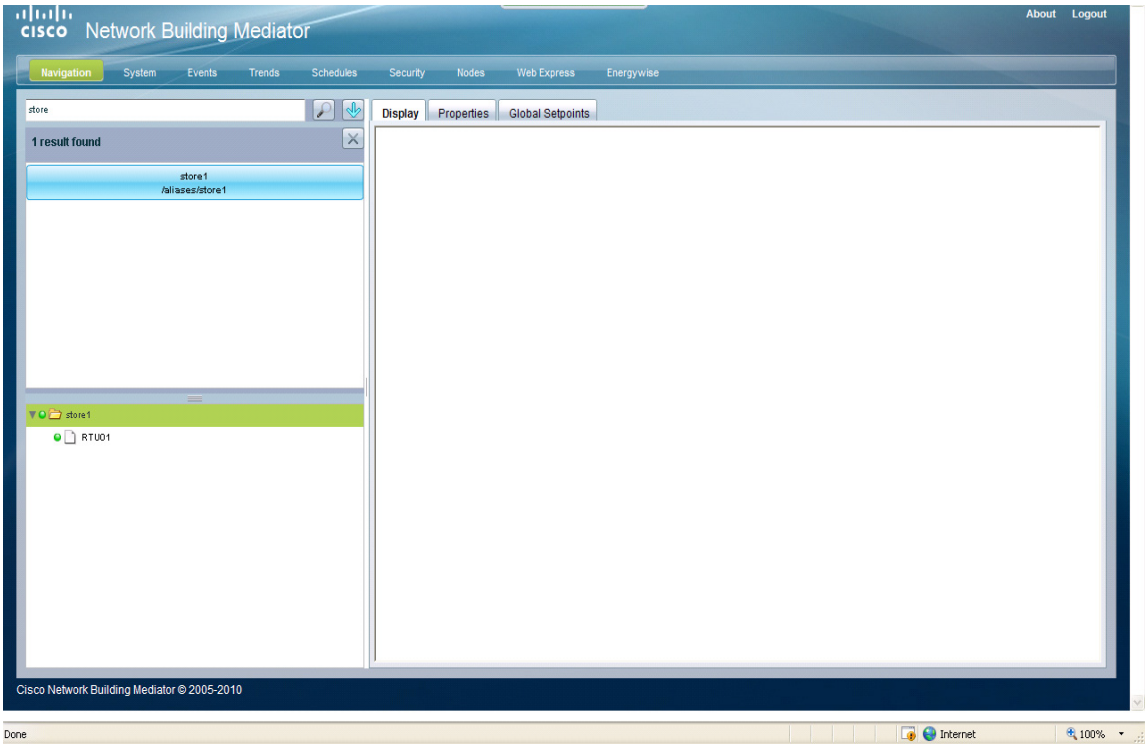
The results are displayed in the search text box. The navigator continues to appear in the left pane under the search text box. Each result shows the name of the entity and the path to the entity. (See Figure 15-7.)

Note The search supports the wild characters like * and ? where * represents more than one character and ? represents one character. Any search string that does not provide a wild character is actually converted into *<str>* by prefixing and suffixing *.

Note You can search for exact names by enclosing the query in single quote (‘) or double quotes (“). For example, “ahu-1” will find only those entities with the exact name of ahu-1. These searches are not case sensitive.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 15-7 Cisco Network Building Mediator - Results



Step 5 Click a search result to select the corresponding entity in the navigation tree.

Step 6 If you want to restrict the search to only the children of a certain entity, perform the following steps:

a. Click the **down arrow** icon, next to the Search icon.

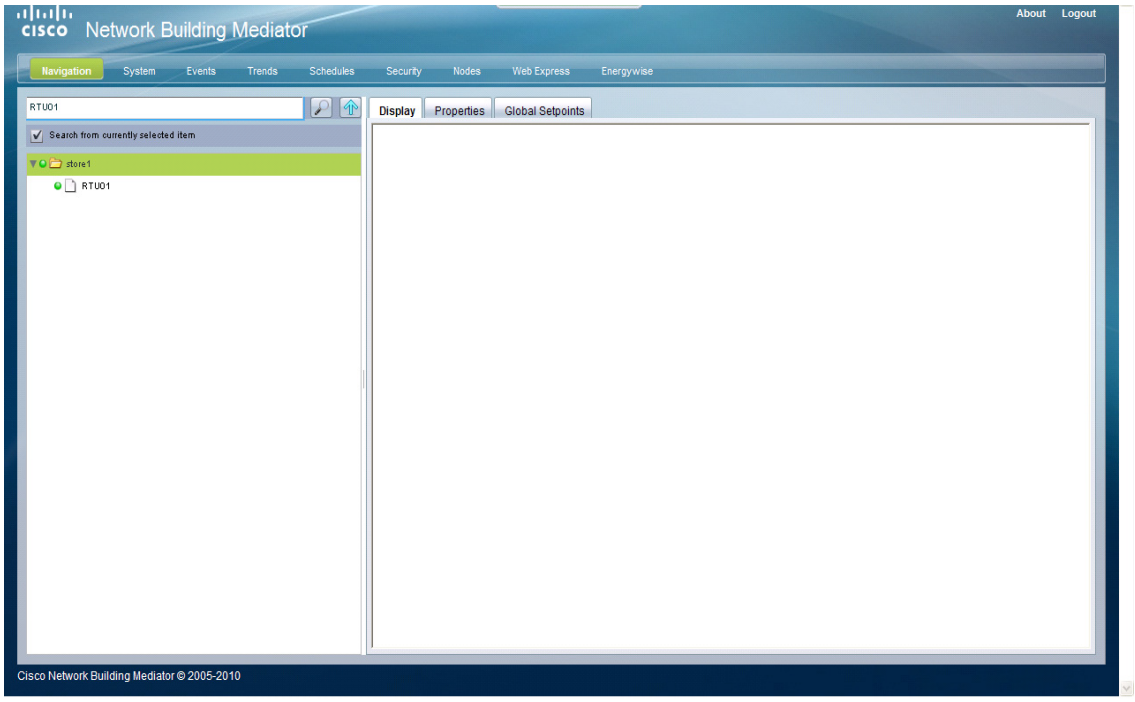
b. Select the **Search from currently selected item** check box.

c. In the navigation tree, select the entity you want the search to begin with and enter the search term in the search text box.

d. Click the **Search** icon or press **Enter**. (See Figure 15-8.)

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 15-8 Cisco Network Building Mediator - Specific Search



The results are displayed in the search text box. The navigator continues to appear in the left pane under the search text box. Each result shows the name of the entity and the path to the entity.

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 16

Global Setpoints

This chapter describes how to configure and manage Global Setpoints and includes the following topics:

About Global Setpoints

Global Setpoints lets you control various devices. The global setpoint group is a list of setpoints and a list of devices controlled by those setpoints. The global setpoint group lets you to monitor and modify the setpoints across different devices and systems connected to the Mediator.

While you can define and manage the different setpoint groups, you can also exclude a device from the list of devices that are being controlled by a setpoint group.

This section includes the following topics:

Global Setpoint Terminology

The following terms are used in this section:

- Setpoint—A target value that an automatic control system aims to reach.
- Global setpoint group—A list of setpoints and a list of devices controlled by these setpoints.
- Entity—Any device that is connected to the Mediator network.

Global Setpoints Tab

The Global Setpoints tab lets you to modify the global setpoint and the defined values for these setpoints.

The Global Setpoints tab displays the following:

- The current values for the global setpoints.
- The priorities you have set for each global setpoint.

Send documentation comments to cbsbu-docfeedback@cisco.com

- The list of devices controlled by the global setpoints.
- The list of devices with values that do not match the available global setpoints.

Managing Global Setpoint Groups

This section includes the following topics:

Viewing Global Setpoint Groups

To view the list of setpoints in the global setpoint group, perform the following steps:

Step 1 Log in to the Mediator web client homepage.

Step 2 In the Navigation pane, click the **Global Setpoints** tab.

The Global Setpoints tab displays a list of setpoints that are defined for the nodes that you select.

The controls on the Global Setpoints tab are enabled or disabled based on the node that you select, such as the following:

- If you select a valid entity, then the global setpoints associated for that entity are displayed in the list and the View button is enabled.
- If the selected entity does not have defined setpoints, then all of the controls are disabled.
- If the selected entity displays incorrect setpoints, then an error message is displayed.

Adding Global Setpoint Groups

There are no default global setpoint groups; you create global setpoint groups as needed.

To add a new global setpoint group, perform the following steps:

Step 1 Log in to the Mediator web client hompage, and click the **Global Setpoints** tab.

Step 2 Click **Add**.

Step 3 In the New Global Setpoint Group dialog box that appears, enter an appropriate, unique name in the Name text box, and click **Add**.

Note If you enter an existing name, the Add button is disabled and an error message appears. If the new name is appropriate, a progress bar appears that indicates the creation of a new setpoint appears.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 Click **Cancel** to cancel the addition of a new global setpoint group.

Deleting Global Setpoint Groups

To remove an existing global setpoint group, perform the following steps:

Step 1 Log in to the Mediator web client, and click the **Global Setpoints** tab.

Step 2 Choose the global setpoint group that you want to delete, and click **Remove**.

Step 3 In the Remove Global Setpoint Group confirmation dialog box that appears, click **OK**.

Step 4 Click **Cancel** to cancel this procedure.

Configuring Global Setpoints Within a Group

This section includes the following topics:

Viewing Global Setpoints- View Mode

This view allows you to view the entity values based on the setpoint you specifiy.

To view the Global Setpoints tab in a view mode, perform the following steps:

Step 1 Log in to the Mediator web client, and click the **Global Setpoints** tab.

Step 2 Choose the global setpoint group that you want to view, and click **View**.

Step 3 (Optional) Double-click the global setpoint group to view it in the view mode.

The Global Setpoints tab appears in the view mode (see Figure 16-1).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 16-1 Global Setpoints Tab - View Mode

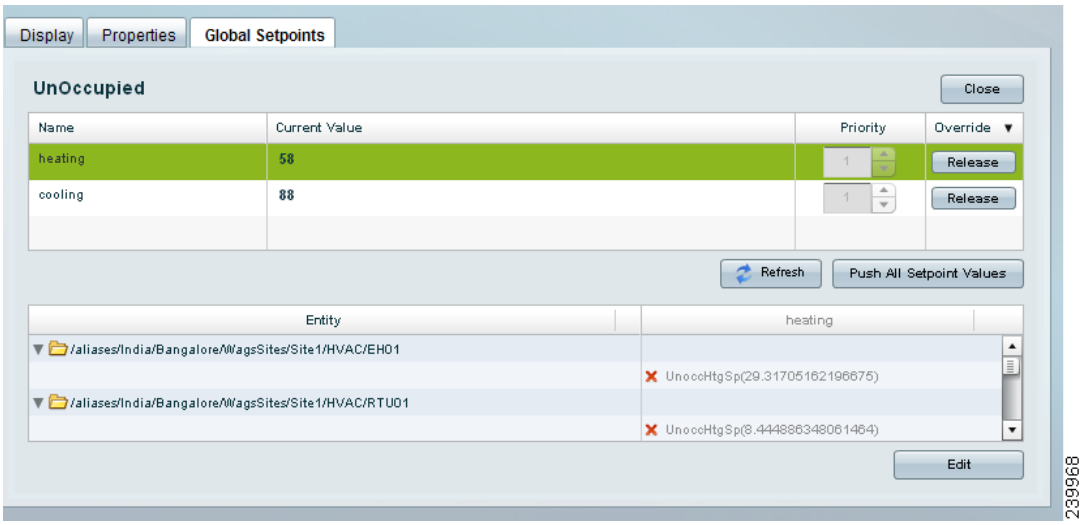


Table 16-1 describes the different elements in the view mode of the Global Setpoints tab.

Table 16-1 Global Setpoints - View Mode

Element	Description
Name	Displays the setpoint name.
Current Value	Displays the current value that has been set for the setpoint.
Priority	Displays the current priority that has been set for the setpoint. You cannot change the priority values in this mode.
Override	Click the Release button to release the set priority of the selected setpoint.
Refresh	Click this button to refresh the setpoint values.
Push All Setpoint Values	Click this button to push the all the setpoint values to the Mediator network. For more information, see Pushing Global Setpoint Values, page 16-13.
Entity	Displays all the devices that are managed by the selected setpoint.
Heating(or the column next to the entity column)	This column display the name of the property and the current values that are set for the property. This column display colored icons that provide the status of the current setpoint values, such as the following: • The red icon implies that the property value does not match the setpoint value. • The green icon implies that the value of the property matches the setpoint value.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 16-1 Global Setpoints - View Mode (continued)

Element	Description
Edit	Click this button to navigate to the edit mode of the Global Setpoints tab. For more information, see Editing Global Setpoint Groups, page 16-5.
Close	Click this button to close the Global Setpoints View page.

Editing Global Setpoint Groups

You can edit a newly created global setpoint group or an existing group. The Global Setpoints tab enables you to edit the setpoint names, current values defined for a setpoints, reset the priority of the setpoint, and push the values to the server.

Note Changes to the Global Setpoints tab are not effective until you save the changes. If you click the Cancel button, you will lose all the changes done.

This section includes the following topics:

Viewing Global Setpoints - Edit Mode

To view the Global Setpoints tab in an edit mode, perform the following steps:

Step 1 Log in to the Mediator web client and click the **Global Setpoints** tab.

Step 2 Select the Global Setpoint Group that you want to view, and click **View**.

Step 3 Optional) Double-click the global setpoint group to view it in the view mode.

The Global Setpoints tab appears in the edit mode.

Step 4 Select the Setpoint that you want to edit and click **Edit**.

The Global Setpoints tab appears in the edit mode (see Figure 16-2).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 16-2 Global Setpoints Tab - Edit Mode

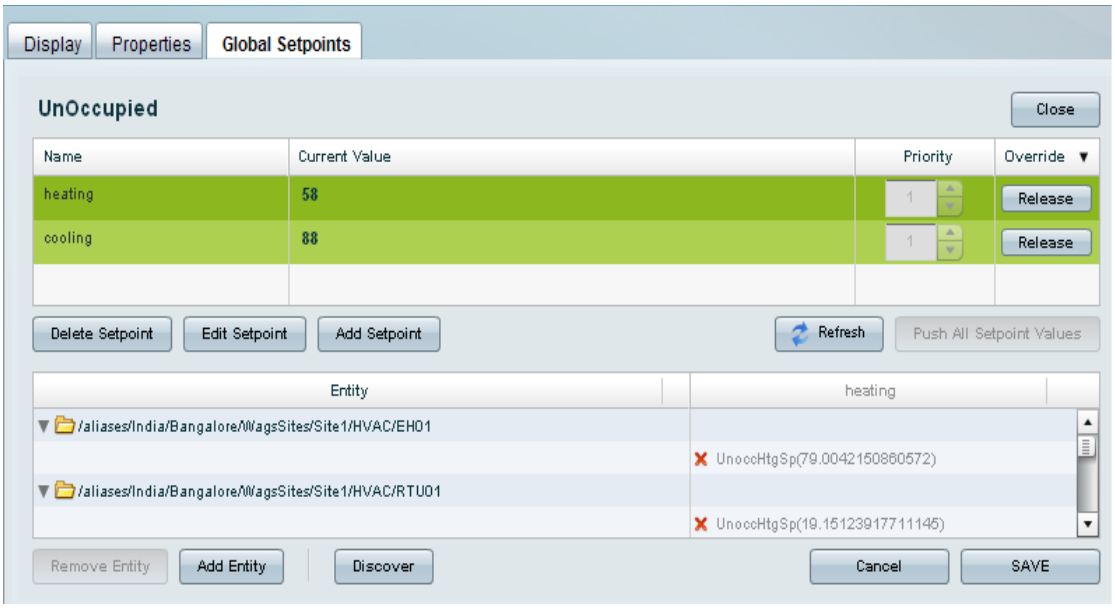


Table 16-2 describes the different elements in the edit mode of the Global Setpoints tab.

Table 16-2 Global Setpoints Tab - Edit Mode

Element	Description
Name	Displays the setpoint name.
Current Value	Displays the current value that has been set for the setpoint. Double-click to reset the values.
Priority	Displays the current priority that has been set for the setpoint. Double-click the existing priority value to reset these values. You are allowed to reset the values between 1-16.
Override	Click the Release button to release the set priority of the selected setpoint.
Delete Setpoint	Click this button to delete the selected setpoint within a group. For more information, see Deleting Global Setpoints, page 16-12.
Edit Setpoint	Click this button to edit an existing setpoint within a group. For more information, see Editing Global Setpoints, page 16-10.
Add Setpoint	Click this button to add a new setpoint to the group. For more information, see Adding Global Setpoints, page 16-7.
Refresh	Click this button to refresh the setpoint values.
Push All Setpoint Values	Click this button to push the values to the Mediator network. This button is disabled by default. It is enabled when you save any changes that you make. For more information, see Pushing Global Setpoint Values, page 16-13.

Send documentation comments to cbsbu-docfeedback@cisco.com

Table 16-2 Global Setpoints Tab - Edit Mode (continued)

Element	Description
Entity	Displays all the devices that are managed by the setpoints.
Remove Entity	Click this button to remove an existing entity within a setpoint. For more information, see Deleting Entities, page 16-13.
Heating (or the columns next to the entity column)	This column display the name of the property and the current values that are set for the property. This column display colored icons that provide the status of the current setpoint values, such as the following: • The red icon implies that the property value does not match the setpoint value. • The green icon implies that the value of the property matches the setpoint value.
Add Entity	Click this button to add a new entity to an existing setpoint. For more information, see Adding Entities, page 16-12.
Discover	You can add an entity by discovering the existing entities. Click this button to discover existing entities. For more information, see Discovery, page 16-12.
Cancel	Click this button to cancel the changes made to the Global Setpoints tab.
Save	Click this button to save the changes made to the Global Setpoints tab.
Close	Click this button to close the Global Setpoints tab.

Adding Global Setpoints

Every setpoint requires specific data type and the Global Setpoints tab enables you to add set points based on different types of data types.

The following data types are currently available:

- Text—Enables you to enter a free-form text value.
- Numeric—Enables you to enter numeric values such as integers, decimal points, and negative or positive numbers. You can configure maximum and minimum values allowed in the input text box.
- Enumerated—Enables you to choose a value from a list of displayed values.

Note If you try to add a Global Setpoint when you do not have the necessary permissions, you are allowed to add the Global Setpoint, and the Global Setpoint appears on the Global Setpoints tab window. When you click the Save button to save this Global Setpoint, you get an error message that indicates that you are

Send documentation comments to cbsbu-docfeedback@cisco.com

not authorized to add the Global Setpoint and the addition fails. However, the Global Setpoint continues to appear on the Global Setpoints tab window. To view the actual list of all the Global Setpoints, you should either clear the browser cache, refresh the window, or logout and login again.

This section describes how you can add global setpoints based on the data types that you select and includes the following topics:

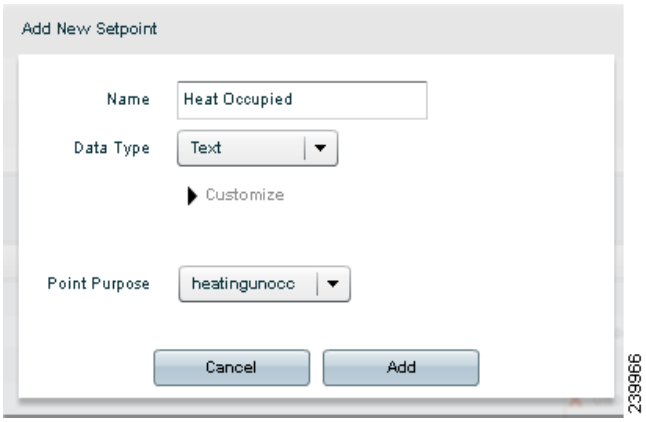
Text Data Type

To add a global setpoint with a text data type value, perform the following steps:

Step 1 Navigate to the Global Setpoints tab in the edit mode and click **Add Setpoint**.

The Add New Setpoint dialog box appears (see Figure).

Figure 16-3 Add New Setpoint Dialog Box - Text



Step 2 Enter the following information:

- Name—Enter an appropriate name for the new global setpoint.
- Data Type—Choose **Text** from the Data Type drop-down list.
- Point Purpose—Choose the appropriate Point Purpose from the drop-down list.

Step 3 Click **Add**. This button is disabled if a name is not defined for the new setpoint.

Step 4 Click **Cancel** to cancel the operation.

Numeric Data Type

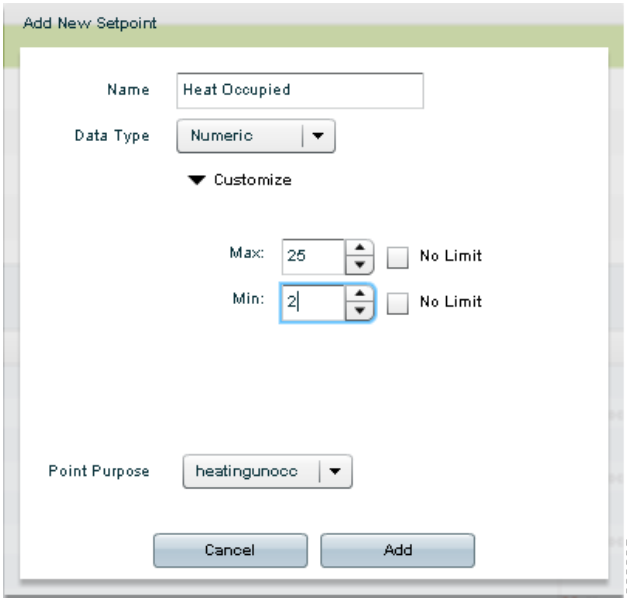
To add a global setpoint with a numeric data type value, perform the following steps:

Step 1 Navigate to the global setpoints tab in the edit mode and click **Add Setpoint**.

The Add New Setpoint dialog box appears (see Figure 16-4).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 16-4 Add New Setpoint Dialog Box - Numeric



Step 2 In the Name text box, enter an appropriate name for the new setpoint.

Step 3 From the Data Type drop-down list, choose **Numeric**. The Customize option is enabled.

Step 4 (Optional) Enter the following information:

- Max—Enter the maximum allowed value.
- Min—Enter the minimum allowed value.
- No Limit—Select the check boxes if you do not want to set any limits.

Note If you specify the minimum and maximum values, you see a numeric slider in the edit mode of the Global Setpoints tab. If you do not specify a limit, then all types of values are accepted. In this case, the numeric slider in the Global Setpoints edit mode is not displayed.

Step 5 From the Point Purpose drop-down list, choose the valid value.

Step 6 Click **Add**.

Note The Add button is disabled if a name is not defined for the new setpoint.

Step 7 Click **Cancel** to cancel this procedure.

Enumerated Data Type

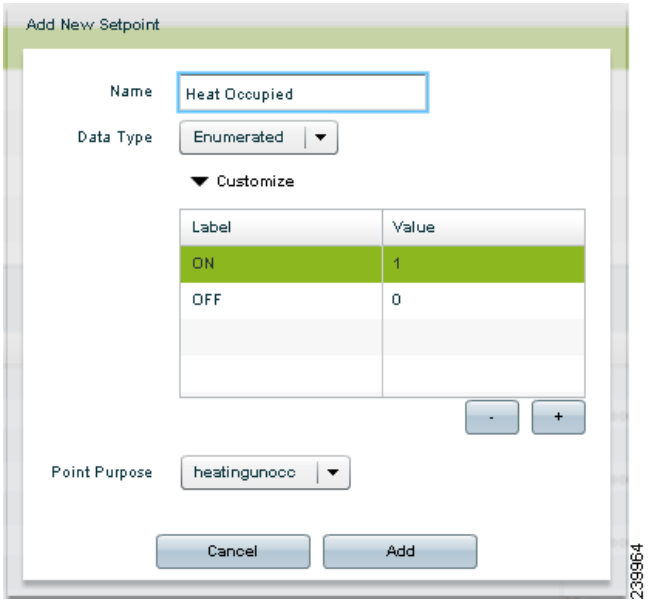
To add a global setpoint with an enumerated data type value, perform the following steps:

Step 1 Navigate to the Global Setpoints tab in the edit mode and click **Add Setpoint**.

The Add New Setpoint dialog box appears (see Figure 16-5).

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 16-5 Add New Setpoint Dialog Box - Enumerated



Step 2 In the Name text box, enter an appropriate name for the new setpoint.

Step 3 From the Data Type drop-down list, choose **Enumerated**. The Customize option is enabled.

Step 4 (Optional) Click **Customize** to view additional configurational options. A table that displays labels and the corresponding values appears.

Step 5 Click the "+" button to enter a new label and a corresponding value.

Step 6 Click the "-" button to delete an existing label and its corresponding value.

Step 7 From the Point Purpose drop-down list, choose the valid value.

Step 8 Click **Add**.

Note This button is disabled if a name is not defined for the new setpoint.

Step 9 Click **Cancel** to cancel this operation.

Editing Global Setpoints

You are allowed to edit global setpoints based on the data types, but you cannot change the defined data type of any global setpoint.

This section describes how you can edit the global setpoints and includes the following topics:

- Text Data Type, page 16-10
- Numeric Data Type, page 16-11
- Enumerated Data Type, page 16-11

Text Data Type

To edit a global setpoint with a text data type value, perform the following steps:

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 1 Navigate to the Global Setpoints tab in the edit mode and click **Edit Setpoint**.

The Edit Setpoint dialog box appears.

Step 2 To modify the global setpoint, change the following information:

- Name—Change the name of the global setpoint.
- Point Purpose—Choose the appropriate Point Purpose from the drop-down list.

Step 3 Click **Update** to update the modified values.

Step 4 Click **Cancel** to cancel this procedure.

Numeric Data Type

To edit an existing global setpoint with a numeric data type value, perform the following steps:

Step 1 Navigate to the Global Setpoints tab in the edit mode and click **Edit Setpoint**.

The Edit Setpoint dialog box appears.

Step 2 To modify the global setpoint, change the following information:

- Name—Change the name of the global setpoint.
- Max—Choose the maximum allowed value.
- Min—Choose the minimum allowed value.
- No Limit—Select the check boxes if you do not want to set any limits.
- Point Purpose—Choose the appropriate Point Purpose from the drop-down list.

Step 3 Click **Update** to update the modified values.

Step 4 Click **Cancel** to cancel this operation.

Enumerated Data Type

To edit an existing global setpoint with an enumerated data type value, perform the following steps:

Step 1 Navigate to the Global Setpoints tab in the edit mode and click **Edit Setpoint**.

The Edit Setpoint dialog box appears.

Step 2 To modify the global setpoint, change the following information:

a. In the Name text box, enter a new name for the global setpoint.

b. Click the “+” button to enter a new label and a corresponding value.

c. Click the “-” button to delete an existing label and its corresponding value.

d. Choose the appropriate Point Purpose from the drop-down list.

Step 3 Click **Update** to update the modified values.

Step 4 Click **Cancel** to cancel the operation.

Send documentation comments to cbsbu-docfeedback@cisco.com

Deleting Global Setpoints

To delete a global setpoint within a group, perform the following steps:

Step 1 Navigate to the edit mode of the Global Setpoints tab.

Step 2 Select the global setpoint that you want to delete, and click **Delete Setpoint**.

Step 3 In the Remove Setpoint dialog box that appears, click **OK**.

Step 4 On the Global Setpoints tab, click **Save** to save the changes.

Adding Entities

Entities are devices that are added to the Mediator. These can be added to existing global setpoint groups using the following two methods:

- Manually, page 16-12
- Discovery, page 16-12

Manually

To manually add entities to the global setpoints group, perform the following steps:

Step 1 Navigate to the Global Setpoints tab, and click **Add Entity**. The Add Entity dialog box appears.

The nodes that you select in the navigation tree appear in the Add Entity dialog box. The left column displays check boxes; the entities that are used in another global setpoint group are disabled and cannot be selected. All entities appear in an alphabetical order.

Step 2 Select the check box next to the desired entity, and click **OK**. The selected entities are added to the entity group.

Discovery

You can discover entities that match one or more of the entity type setpoints defined in a group.

Note We recommend that you configure the list of point types using Mediator configTOOL before you create the setpoints. Doing so helps you to discover the listed points during the discovery methods.

You can discover entities using the following two methods:

- Device Purpose, page 16-12
- Name, page 16-13

Device Purpose

You can discover the entities by the device type only if you specified the devices while creating the entities.

To discover an entity by the device purpose, perform the following steps:

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 1 Navigate to the Global Setpoints tab, and click **Discover**.

Step 2 In the Auto Discovery dialog box that appears, select the **Discover device by purpose** radio button.

Step 3 Click **Next**. The Auto Discovery dialog box appears.

The nodes that you selected in the Navigation tree appear in the Auto Discovery dialog box. The left column displays check boxes; the entities that are used in another global setpoint group are disabled and cannot be selected.

Step 4 Select the check box next to the desired entity, and click **Finish**.

The selected entities are added to the entity group.

Step 5 On the Global Setpoints tab, click **Save** to save the changes.

Name

To discover an entity by the device name, perform the following steps:

Step 1 Navigate to the Global Setpoints tab, and click **Discover**.

Step 2 In the Auto Discovery dialog box, select the **Discover device by name** radio button.

Step 3 Click **Next**. The Auto Discovery dialog box appears.

The nodes that you selected in the Navigation tree appear in the Auto Discovery dialog box. The left column displays check boxes; the entities that are used in another global setpoint group are disabled and cannot be selected.

Step 4 Enter **text** in the Name text box, and click **Find**. A list of entities that match the search criteria appear.

Step 5 Select the check box next to the desired entity, and click **Finish**.

The selected entities are added to the entity group.

Step 6 On the Global Setpoints tab, click **Save** to save the changes.

Deleting Entities

To delete an entity, select the entity that you want to delete, and click **Remove Entity**. You can select one or more entities to delete.

Pushing Global Setpoint Values

You can push the setpoint values to the properties of the entities that are managed by the setpoint group. These values, when pushed appear on all points on the downstream Mediators. Pushing the setpoint values pushes all the setpoint values and is not based on the selection of any setpoint.

To push the values for a select global setpoint group, click **Push All Setpoint Values**. The Pushing Values progress bar appears.

The Pushing Values progress bar closes once the values are pushed to the network successfully.

Send documentation comments to cbsbu-docfeedback@cisco.com

Note Clicking **Push All Setpoint Values**, pushes all the setpoint values and is not based on the setpoint selection.

Send documentation comments to cbsbu-docfeedback@cisco.com

CHAPTER 17

OpenADR Client Service

This chapter provides an overview of the OpenADR client service and the DRAS architecture, and describes how to configure the OpenADR client service on the Mediator. It includes the following sections:

About Open Automated Demand Response

A *Demand Response* (DR) program involves the dynamic management of energy usage through cooperation between power consumers, their electric utility, and the electric system operator (or the independent system operator - ISO). It is an element of the *Smart Grid* that is used to optimize electric supply and demand. When the electric grid is nearing capacity, for example, when a large number of air conditioners are operating on a warm day, the ISO notifies the electric utility and power consumers of the situation, which may require electric load reduction or shifting by the power consumers.

The *Open Automated Demand Response* (OpenADR) standard is used to define the communication methods that enable ISOs and electric utilities to continuously send signals to power consumers using open network protocols. These utility-generated DR signals indicate the presence or scheduling of a DR event, which can be *automatically* translated into load sheds or shifts.

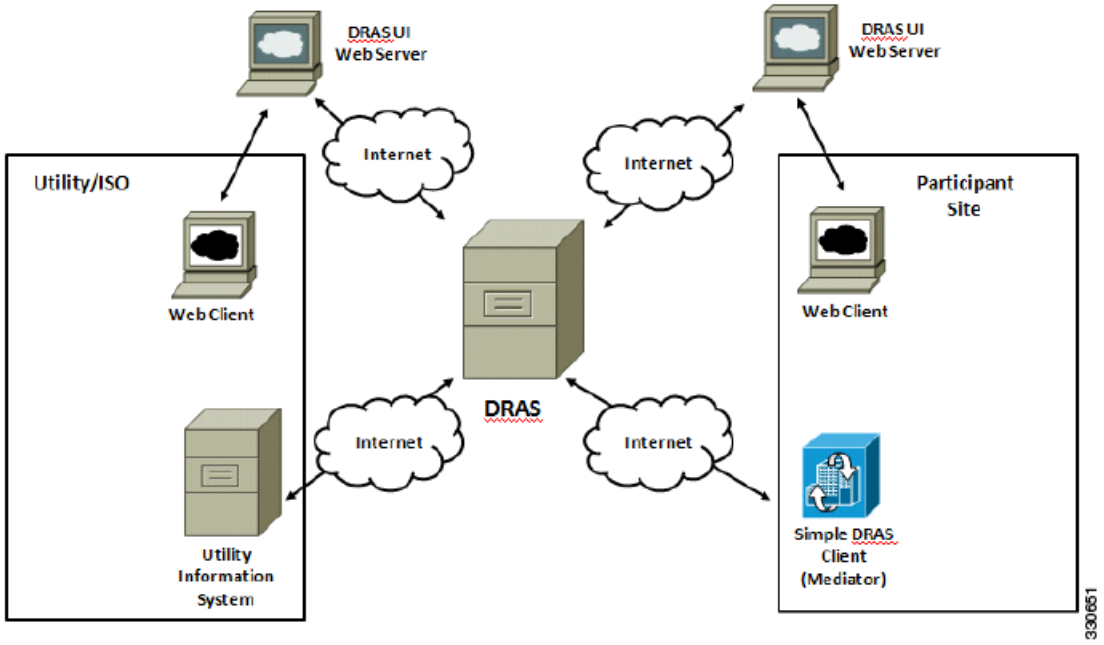
For more information on OpenADR, refer to the Open Automated Demand Response Communications documentation.

DRAS Architecture

Figure 17-1 outlines a generic Demand Response Automation Server (DRAS) architecture.

Send documentation comments to cbsbu-docfeedback@cisco.com

Figure 17-1 DRAS Architecture



A generic DRAS architecture consists of the following components:

- DRAS—Facilitates communication between the entities that produce and distribute electricity (utilities and ISOs) and the entities that manage the consumption of electricity (facilities). The Akuacom DRAS is used as the primary DRAS, which presents a web service to DRAS clients.
- Simple DRAS client—Interfaces between the DRAS on the utility/ISO side and other systems on the participant side. The DRAS client typically exists on the participant side. When the OpenADR service is configured as a network service on the Cisco Network Building Mediator (Mediator), it acts as a simple DRAS client that communicates with the DRAS using the PULL mode of interaction. In the PULL mode, the DRAS client periodically polls the DRAS for DR event information at configurable intervals of time.
- Utility/ISO interface—This is the interface that utilities and ISOs use to set up, manage, and monitor a DR program.
- Participant interface—This is the interface that participants of the DR program use to convey electricity demand requests to the DRAS.

  For more information on the DRAS architecture, refer to the Open Automated Demand Response Communications documentation.

About DR Event Information

The simple DRAS client periodically polls the DRAS for DR event information. This information is returned from the DRAS in the form of an XML document. In this XML document, the *EventState* entity is of significance because it is a representation of the state that the DRAS client is in with respect to a particular DR event. The *EventState* entity contains the following variables that describe a specific DR event to the DRAS client:

- EventStatus—Depicts the current temporal state of a DR event and can take on the following values:
  - NONE (1)—There is no event pending.

Send documentation comments to cbsbu-docfeedback@cisco.com

  - FAR (2)—An event is pending far into the future.
  - NEAR (3)—An event is pending soon.
  - ACTIVE (4)—An event is currently in progress.

    In general, the EventStatus variable transitions from NONE to FAR to NEAR to ACTIVE.

- OperationModeValue—Depicts the operational state of the facility and can take on the following values:
  - NORMAL operation (1)
  - MODERATE shed or shift (2)
  - HIGH shed or shift (3)

    The OperationMode variable takes on values according to a schedule during the event that is defined by the participant or the utility or ISO.
- CurrentTime—Signifies the time till the ACTIVE state of the event is reached.
- OperationModeSchedule(ResponseSchedule)—Defines how a participant responds to DR events. It is an ordered list of rules that are valid within a specific time slot of the ACTIVE period of the DR event. These rules determine how the OperationMode variable transitions during the time slot. For more information on how the Mediator handles response schedules, see the "Handling Response Schedules" section on page 17-5.

Configuring the OpenADR Client Service

This section describes how to configure the OpenADR client service on the Mediator and includes the following topics:

Prerequisites

Before configuring the OpenADR client service on the Mediator, ensure that the Mediator network has access to the public DRAS network, so that it can obtain the necessary DR event information from the DRAS. If the Mediator network is protected by a firewall, ensure that access to the DRAS network is open using the default HTTPS port number 8443.

Configuring the OpenADR Client

To configure the OpenADR client service on the Mediator, perform the following steps:

Step 1 Start configTOOL and connect to the Mediator (see the "Accessing Mediators Using configTOOL" section on page 4-11).

The configTOOL window appears.

Step 2 In the node tree pane, expand the node tree, then choose **services** > **network**.

Step 3 Right-click the **network** node, and choose **Add** from the drop-down list.

The Available Devices dialog box appears listing the protocols supported by the Mediator.

Send documentation comments to cbsbu-docfeedback@cisco.com

Step 4 In the Available Devices dialog box, choose **Open ADR Protocol Service (OpenADR)** from the list, and then click **OK**.

A new child node, OpenADR, appears under the network node in the node tree pane.

Step 5 In the node tree pane, right-click the **OpenADR** node, and choose **Add** from the drop-down list.

The Available Devices dialog box appears.

Step 6 In the Available Devices dialog box, choose **OpenADR Simple Client (OpenADR_Client)** from the list, and then click **OK**.

A new child node, OpenADR_Client, appears under the OpenADR node in the node tree pane.

The OpenADR_Client tab displays the default name, description, and the configurable parameters of the OpenADR_Client child node.

Step 7 In the Serverip text box, enter the IP address of the DRAS.

Step 8 In the User Name text box, enter the user name of the participant account. The electric utility creates the participant account and provides this information.

Step 9 In the Password text box, enter the password of the participant account. The electric utility creates the participant account and provides this information.

Step 10 In the Port Number text box, retain the port number as 8443, which is the default port for HTTPS.

Step 11 In the File Path text box, retain the default path, which is the location of the EventState file in the DRAS.

Step 12 In the Poll Period text box, enter the polling frequency, in seconds, with which the simple DRAS client polls the DRAS.

Step 13 Save the configuration.

Viewing DR Event Information

You can view the DR event information that the simple DRAS client polls from the DRAS.

To view the DR event information, perform the following steps:

Step 1 Launch an Internet browser (for example, Internet Explorer) and browse to the Mediator web client home page. To do so, enter the IP address of the Mediator in the Address bar of the browser and log in when prompted.

The Mediator web client home page appears in the Internet browser window.

Step 2 Click **Nodes**.

The Mediator web client Node page appears.

Step 3 Choose **services > network > OpenADR > OpenADR_Client**.

The Mediator web client Node page displays the variables of the EventState entity and their corresponding values. For more information on the variables and the significance of their values, see the "Viewing DR Event Information" section on page 17-4.

This information can now be used to create control logic that can reduce the energy usage of a facility.

Send documentation comments to cbsbu-docfeedback@cisco.com

Handling Response Schedules

The following scenario outlines how the Mediator (acting as a simple DRAS client) handles the response schedule:

1. A DR event notification is issued by the DRAS 300 seconds (5 minutes) before the ACTIVE state of the DR event.
2. The Mediator polls the DRAS sometime between the FAR and NEAR state of the DR event.
3. In the Node Browser, the services > network > OpenADR > OpenADR_Client > OperationModeSchedule > ModeSlot node provides the Mediator with information on how the OperationMode variable changes during the ACTIVE period of the DR event.
4. If the ModeSlot values are 0 and 300, and the OperationMode values are MODERATE and HIGH, the Mediator schedules a procedure to update the OperationMode at the relevant time.

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

INDEX

A

C

Send documentation comments to cbsbu-docfeedback@cisco.com

Send documentation comments to cbsbu-docfeedback@cisco.com

D

Send documentation comments to cbsbu-docfeedback@cisco.com

E

Send documentation comments to cbsbu-docfeedback@cisco.com

F

G

H

I

K

Send documentation comments to cbsbu-docfeedback@cisco.com

L

M

N

O

Send documentation comments to cbsbu-docfeedback@cisco.com

P

R

Send documentation comments to cbsbu-docfeedback@cisco.com

S

T

U

Send documentation comments to cbsbu-docfeedback@cisco.com

V

W

Send documentation comments to cbsbu-docfeedback@cisco.com