



Cisco Network Building Mediator Deployment Guide

Release 3.x.x

July, 2011

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-xxxxx-xx

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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Network Building Mediator Deployment Guide
© 2009–2011 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Mediator Deployment 1-1

Introduction	1-1
About this document	1-1
Related documentation	1-1
Deployment Architecture	1-1
Mediator Architecture Overview	1-2
Extends the Network as a Platform	1-2
Mediator Architecture for the Branch	1-3
Mediator Architecture for the Enterprise	1-4
Mediator Communication Ports	1-5
Illustrated Mediator Communication Ports	1-5
Detailed Mediator Communication Ports	1-6
Mediator Traffic and Bandwidth Usage	1-6
Network Security in Mediator Deployment	1-6
Installation Guidelines	1-8
Wiring and Mounting the Mediator	1-8
Wiring and Mounting the Mediator Manager	1-9
RS-485 Wiring Guidelines	1-10

CHAPTER 2

Mediator Configuration 2-1

Configuration	2-1
Mediator Configuration Model	2-1
Mediator Configuration Workflow and Best Practice	2-9
Mediator Manager Configuration Workflow and Best Practice	2-12
Commissioning	2-14
Mediator Checkout Procedure	2-14
Mediator Manager Checkout Procedure	2-16
3rd Party Device Controls Checkout Procedure	2-17
Backup and Restore	2-18
Backing up the Mediator	2-18
Steps to backup the Mediator manually using the System page:	2-18
Steps to backup the Mediator manually from the command line:	2-19
Steps to backup the Mediator automatically using cron:	2-19
Backing up the Mediator Manager	2-22

Steps to backup the Mediator Manager manually using the System page	2-22
Steps to backup the Mediator Manager manually from the command line	2-22
Steps to backup the Mediator Manager automatically using cron	2-23
Restoring the Mediator	2-25
Restoring the Mediator Manager	2-26



CHAPTER 1

Mediator Deployment

Introduction

- [About this document, page 1-1](#)
- [Related documentation, page 1-1](#)

About this document

This document is intended to help you understand how to efficiently and securely deploy the Cisco Network Building Mediator in different deployment scenarios. Included are topics that describe the architecture, network design, installation, configuration and maintenance of the Mediator.

The following people should use this document:

- Systems integrators and installers
- IT personnel
- Network Administrators

Related documentation

[Cisco Mediator Manager Hardware Installation Guide](#)

[Cisco Network Building Mediator Manager Quick Start Guide](#)

[Cisco Network Building Mediator Manager User Guide](#)

[Cisco Network Building Mediator 2500 and 5000 Hardware Installation Guide](#)

[Cisco Network Building Mediator Quick Start Guide](#)

[Cisco Network Building Mediator User Guide](#)

[Cisco Network Building Mediator Release 3.1.1 and Cisco Network Building Mediator Manager Release 1.1.1 XML-RPC API Guide](#)

Deployment Architecture

- [Mediator Architecture Overview, page 1-2](#)

- [Mediator Architecture for the Branch](#), page 1-3
- [Mediator Architecture for the Enterprise](#), page 1-4
- [Mediator Communication Ports](#), page 1-5
- [Mediator Traffic and Bandwidth Usage](#), page 1-6
- [Network Security in Mediator Deployment](#), page 1-6

Mediator Architecture Overview

This section describes about the Mediator architecture and includes the following sections:

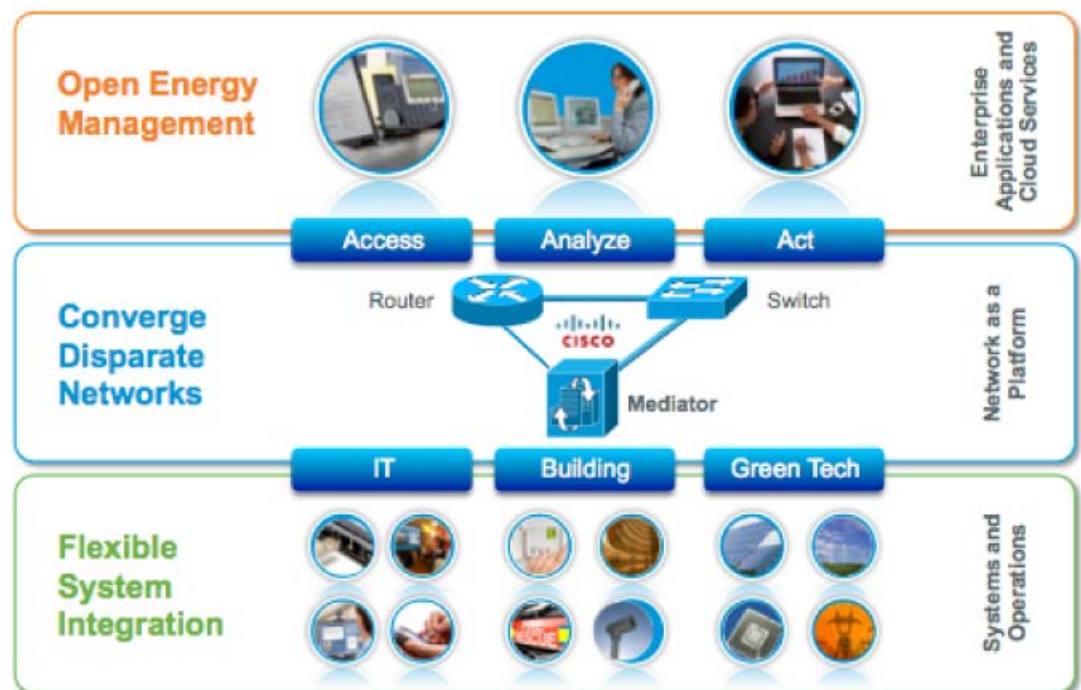
- [Extends the Network as a Platform](#), page 1-2
- [Illustrated Mediator Communication Ports](#), page 1-5
- [Detailed Mediator Communication Ports](#), page 1-6

Extends the Network as a Platform

The Mediator integrates disparate building systems onto an IP network leading to a truly converged, energy-efficient building. Building systems are deployed in a large variety of commercial facilities with diverse topologies such as universities, single and multi-tenant office buildings and branch/retail stores.

This architecture is meant to be the model to be used in all these types of environments, but clearly must be tailored based on the building class, building tenant and vertical market being served.

Figure 1-1 Open Energy Management



330106

Mediator Architecture for the Branch

At the building level the Mediator is used to integrate disparate building systems onto an IP network. These systems can include HVAC, Lighting, Electrical and Refrigeration. These systems use open standards such as BACnet or Modbus and proprietary protocols like Trane comm4 or Johnson N2. The physical connectivity also varies between systems with the most common being RS232, RS485 and IP. Both of these factors affect the number of devices that can be connected to the Mediator and need to be taken into account when designing the system.

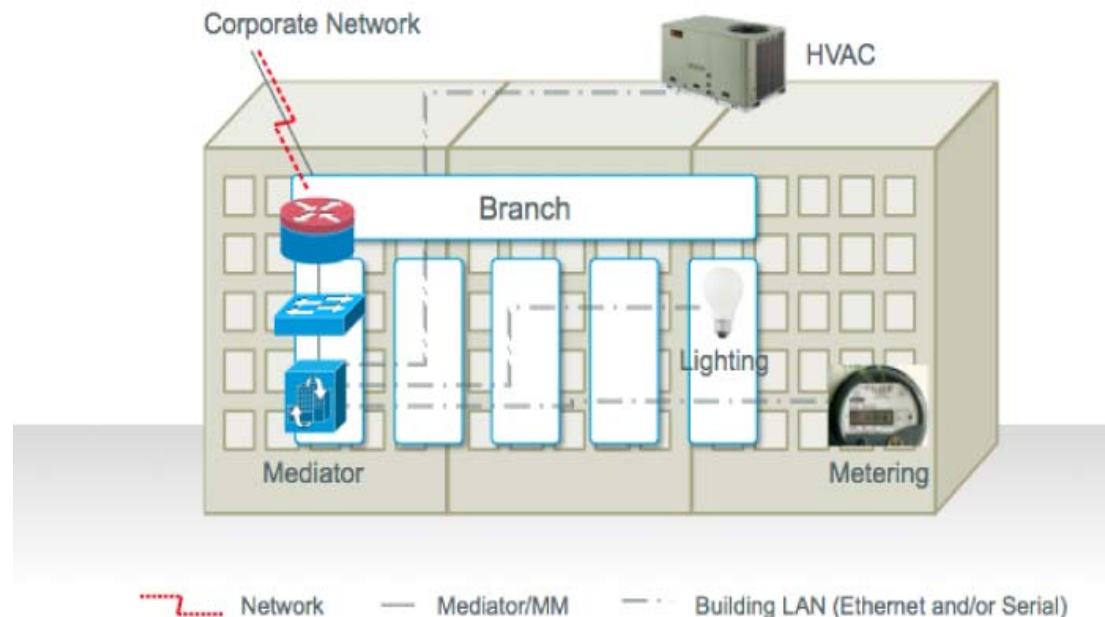
The Mediator is available in two configurations, the Mediator 2500 and 5000. The Mediator 2500 is designed for smaller branch and retail deployments and supports up to 1000 points. The Mediator 5000 is designed for larger commercial facilities and supports up to 5000 points.

The Mediator licensing mechanism allows the option to add additional points and protocols as needed. There are three types of licenses:

1. Point licenses: Each Mediator comes with a certain number of built in points. Additional licenses may be purchased to increase the number of points.
2. Protocol licenses: Each Mediator comes with certain set of built in protocols. Additional protocol licenses may be purchased as per the requirements of the project.
3. Global Management licenses: Each Mediator may be enabled with Global Management for use with the Cisco Network Building Mediator Manager.

Figure 1-2 shows an example of the Mediator Architecture.

Figure 1-2 Mediator Architecture



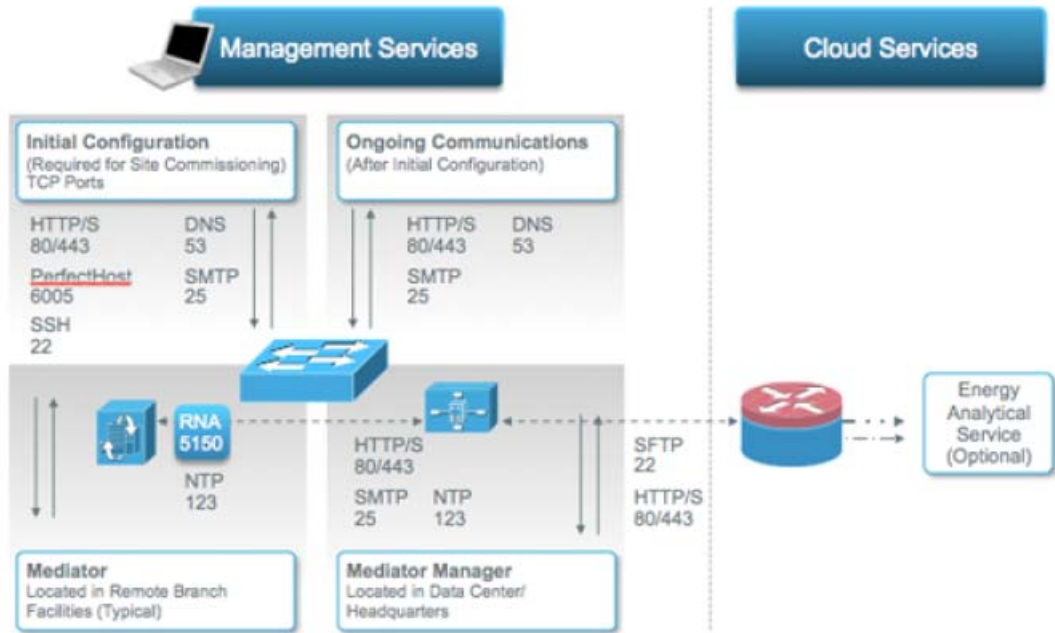
330108

Mediator Communication Ports

Illustrated Mediator Communication Ports

Throughout the life cycle of a Mediator deployment a number of different communication ports may need to be opened for configuration and management. Below is a comprehensive list of ports. This list should be tailored based on the required services for a particular deployment.

Figure 1-4 Communication Ports - Illustrated



330112

Detailed Mediator Communication Ports

Figure 1-5 Communication Ports - Detailed

Source	Destination	Protocol	Port	Direction
Cisco Development	Mediator/MManager	SSH	TCP/22	Ingress
Cisco Development	Mediator/MManager	HTTP	TCP/80	Ingress
Cisco Development	Mediator/Mmanager	HTTPS	TCP/443	Ingress
Cisco Development	Mediator/Mmanager	RNA	TCP/5150	Ingress
Cisco Development	Mediator/MManager	PerfectHOST	TCP/6005	Ingress
Mediator Manager	Mediators	SSH	TCP/22	In/Egress
Mediator Manager	Mediators	HTTP	TCP/80	In/Egress
Mediator Manager	Mediators	HTTPS	TCP/443	In/Egress
Mediator Manager	Mediators	RNA	TCP/5150	In/Egress
Mediator Manager	Mediators	PerfectHOST	TCP/6005	In/Egress
Mediator Manager	Mediators	ICMP	N/A	Egress
Mediators and Manager	Outside	NTP	UDP/123	Egress
Mediators and Manager	Outside	DNS	UDP/53,953	Egress

330113

Mediator Traffic and Bandwidth Usage

In most deployments the amount of bandwidth used by the Mediator is very low and is predictable and adjustable. Mediator traffic can be categorized into the following classes:

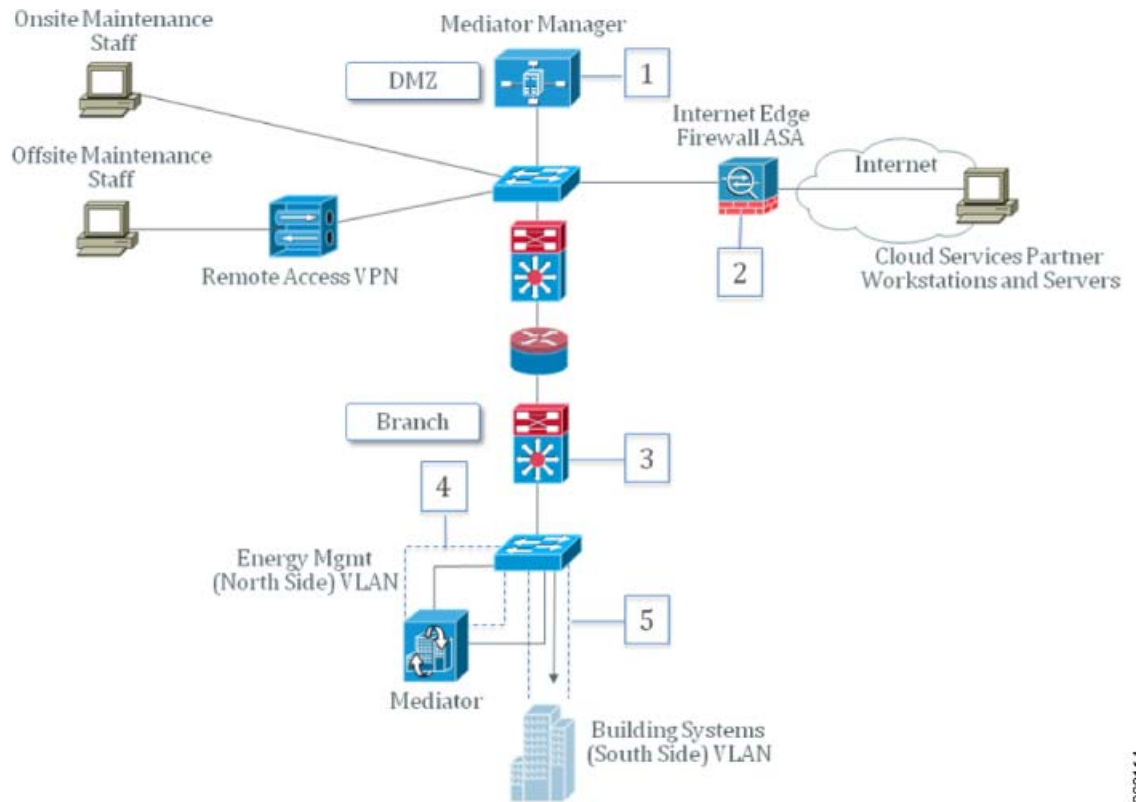
- Dashboard viewing–Webpage displaying metrics from one or more branches.
- Data aggregation–Mediator Manager to Mediator communications.
- Data exporting–Exporting logged data to a central repository at a predetermined time interval.
- Configuration update–Pushing configuration and programming changes such as schedule changes to remote locations via the Mediator Manager.
- Alarm aggregation and reporting–Events generated on Mediators are pushed to the Mediator Manager and reported on via e-mail.

Network Security in Mediator Deployment

When designing a converged IP network infrastructure to support both traditional IT services and energy management systems, you should be particularly aware of the security implications. These security requirements must be balanced against the business requirements of the energy management system itself.

Figure 1-6 shows a simplified example of a typical Mediator deployment.

Figure 1-6 Mediator Deployment



330114

The following describes the numbers shown in the above figure:

- Mediator Manager sitting on a DMZ segment within the corporate network.
- ASA 5500 Security Appliance deployed within the DMZ section provides address translation and stateful access control for incoming/outgoing connections to cloud-services partners.
- Layer-3 switch with ACLs or FWSM provides stateless/stateful firewall.
- Energy management VLAN is trunked to Layer-3 distribution switch along with data, voice, and other VLANs.
- Building systems VLAN is isolated by not trunking it from the Layer-2 access switch to the Layer-3 distribution switch stack.

Additional information on network design and security can be found in the Mediator Design Guide:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/Mediator_DG/mediator_DG.html.

**Note**

Mediator security guidelines will be covered in more detail in the Security section.

Installation Guidelines

This section describes about the installation guidelines of the Mediator and includes the following sections:

- [Wiring and Mounting the Mediator Manager, page 1-9](#)
- [Wiring and Mounting the Mediator Manager, page 1-9](#)
- [RS-485 Wiring Guidelines, page 1-10](#)

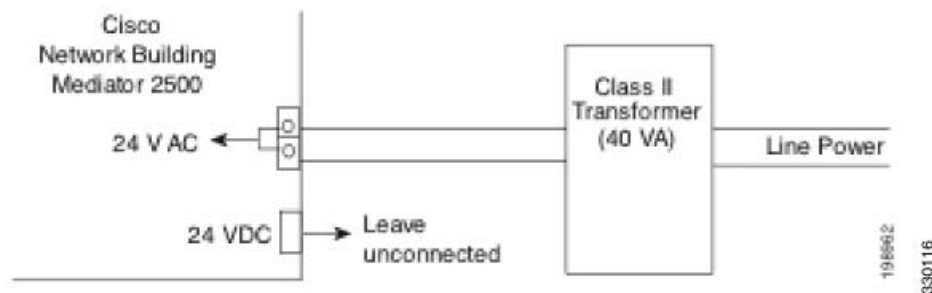
Wiring and Mounting the Mediator

The Mediator should be mounted in a control panel that meets the following general requirements:

- Mechanical design-Ensure that the control panel meets the regulations applicable to the location.
- Ambient conditions-The recommended ambient range for the Mediator is 23° to 131°F
- EMC Compliance-Ensure that the control panel complies with the following regulations:
- EN 55022, CISPR22, EN 300386, CFR47, EN61000-3-2, EN61000-3-3
- The Mediator both accepts AC and DC power supply and operates on 24 V AC or 24 V DC.

Connect the Mediator to AC power as shown below:

Figure 1-7 Mediator Connected to AC Power



Caution

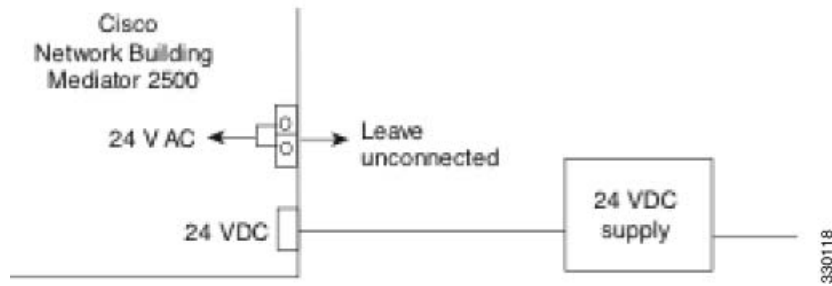
Do not power any other devices from the AC power transformer connected to the Mediator.

An external power supply with the follow specification supplies DC power to the Mediator:

- Operates from 100 V AC to 240 V AC
- Supplies 24 V DC at 1.25 A

Connect the Mediator to DC power as shown below:

Figure 1-8 Mediator Connected to DC Power



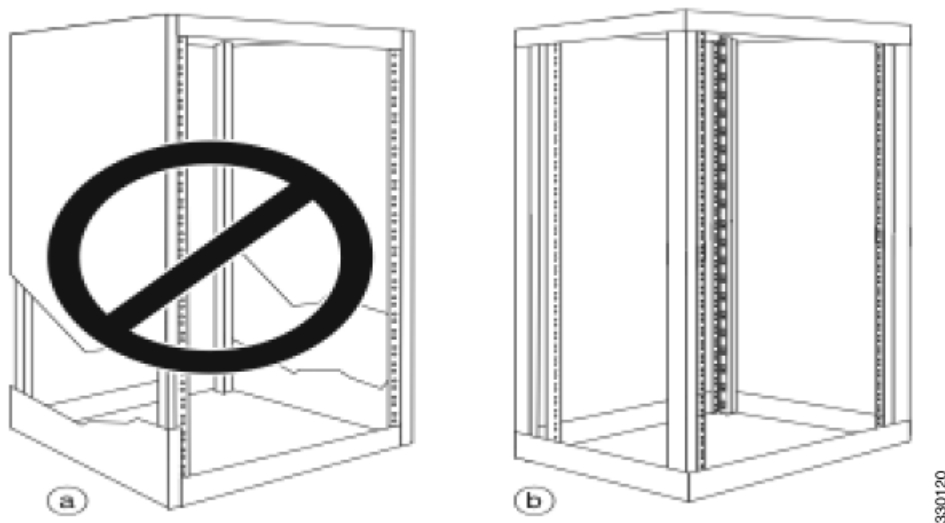
For additional information on Mediator hardware installation see:

http://www.cisco.com/en/US/docs/security/physical_security/cnbm/3.x/HW/Installation_Guide/hig.html

Wiring and Mounting the Mediator Manager

The Mediator Manager 6300 can be mounted in most 4-post (telco-type), 19-inch equipment racks that comply with the Electronics Industries Association (EIA) standard for equipment racks (EIA-310-D). The rack must have at least two posts with mounting flanges to mount the appliance. The distance between the center lines of the mounting holes on the two mounting posts must be 18.31 inches +/- 0.06 inch (46.50 cm +/- 0.15 cm). The rack-mounting hardware included with the appliance is suitable for most 19-inch equipment racks or telco-type frames. The Mediator Manager should *not* be installed in this type of enclosed rack.

Figure 1-9 Mounting the Mediator



Before installing your Mediator Manager 6300 in a rack, review the following guidelines:

- Two or more people are required to install the appliance in a rack.
- Ensure that the room air temperature is below 95°F (35°C).

- Do not block any air vents; usually, 6 inches (15 cm) of space provides proper airflow.
- Plan the appliance installation starting from the bottom of the rack.
- Do not extend more than one appliance out of the rack at the same time
- Connect the appliance to a properly grounded outlet.
- Do not overload the power outlet when installing multiple devices in the rack.
- Do not place any object weighing more than 110 lb (50 kg) on top of rack-mounted devices.

Configure the Mediator Manager 6300 with AC-input power only. The following precautions and recommendations must be followed:

- Install a power conditioner if necessary.
- Install proper grounding to your host equipment.
- The AC-input power supply operates on input voltage and frequency within the ranges of 100 to 240 VRMS and 50/60 Hz without the need for operator adjustments.

For additional information on Mediator hardware installation see:

http://www.cisco.com/en/US/docs/security/physical_security/cnbn_mgr/1.x/HW/Installation_Guide/hig.html

RS-485 Wiring Guidelines

The RS-485 is the most common asynchronous voltage standard in use today for multi-drop communication systems. It is very resistance to noise, can send data at high speeds (up to 10 Mbps), can run for long distances (5km at 1200 bps, 1200 m at 90kbps), and is easy and cheap to use.

A typical RS485 network can operate properly in the presence of reasonable ground differential voltages, withstand driver contentious situations, provide reliable communications in electrically noisy environments (good common mode rejection using twisted pair cable, shielding provides additional protection), and support thirty-two or more (many IC manufacturers have 1/2, 1/4, 1/8 unit load devices) drivers and receivers on the line.

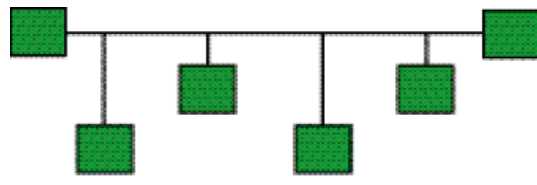
Twisted pair wire with a characteristic impedance of 120 ohms is recommended with 120 ohm termination at each end of the communications line. Care should be taken when selecting the cable because intermittent problems caused by marginal cable can be very difficult to troubleshoot.

Recommended Cable Part numbers:

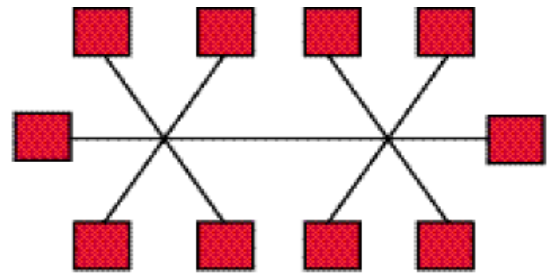
- Belden 3106A, 9842, 82842, 7201A
- Alpha Wire 6455, 6454
- Shielded CAT 5

The figure below shows several network topologies. Daisy chain is recommended.

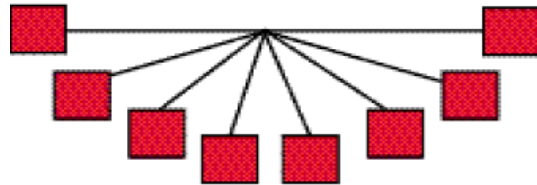
Figure 1-10 Network Topologies



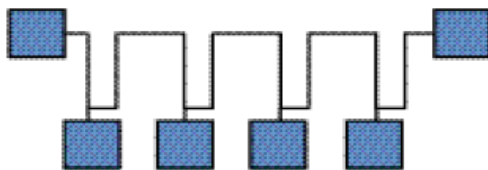
Backbone with stubs (workable)



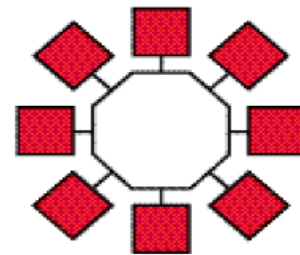
Backbone with stars or clusters (avoid)



Star network (avoid)



Daisy chain (best)



Ring (avoid)

330122



CHAPTER 2

Mediator Configuration

This section describes about the Mediator and Mediator Manager configuration and includes the following sections”

- [Configuration, page 2-1](#)
- [Commissioning, page 2-14](#)
- [Backup and Restore, page 2-18](#)

Configuration

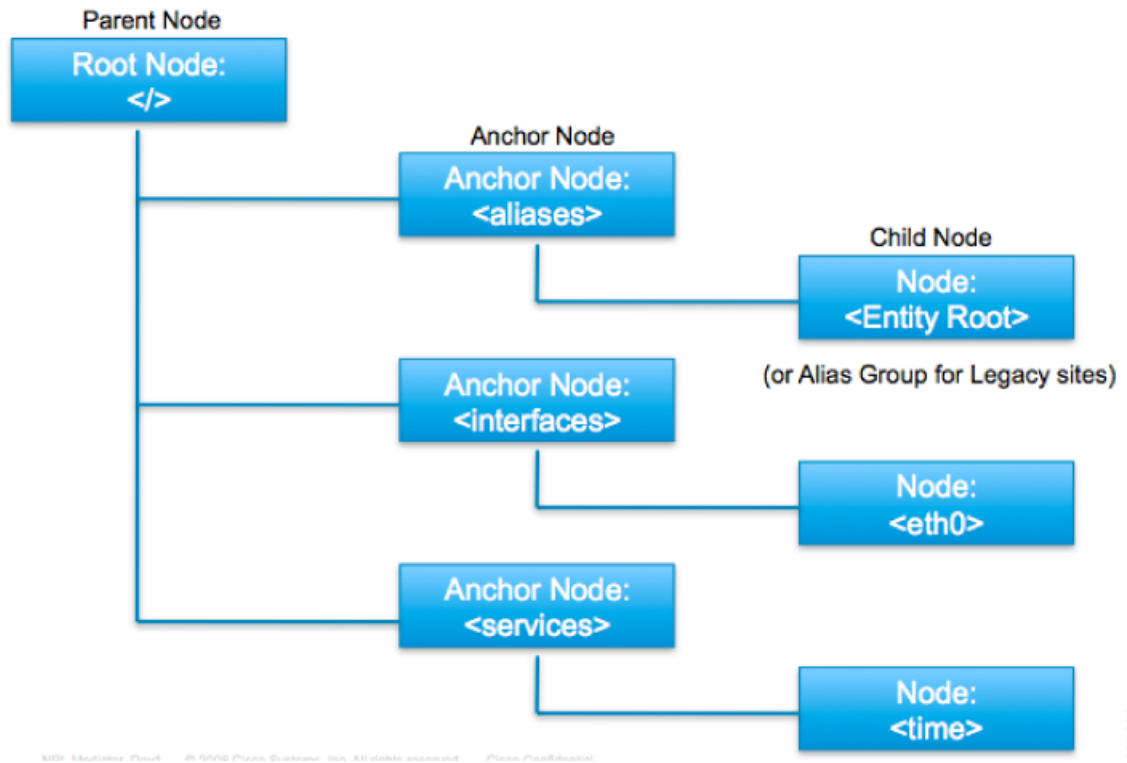
This section describes about how to configure the Mediator and Mediator Manager and includes the following sections:

- [Mediator Configuration Model, page 2-1](#)
- [Mediator Configuration Workflow and Best Practice, page 2-9](#)
- [Mediator Manager Configuration Workflow and Best Practice, page 2-12](#)

Mediator Configuration Model

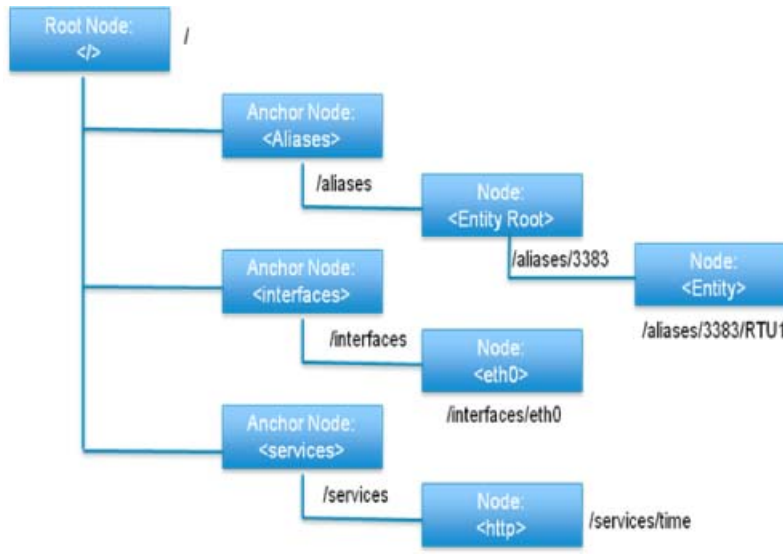
The Mediator Framework (FW) represents a site by assembling a hierarchical tree structure of objects called nodes. All Devices, Interfaces and Services are modeled as a collection of *nodes*.

Figure 2-1 Nodes



The Framework creates a global namespace for each node on the Mediator in the form of a Uniform Resource Locator (URL). All attributes are accessible (either locally or remotely) via this unique identifier. The diagram below illustrates how nodepaths are constructed:

Figure 2-2 Nodepaths

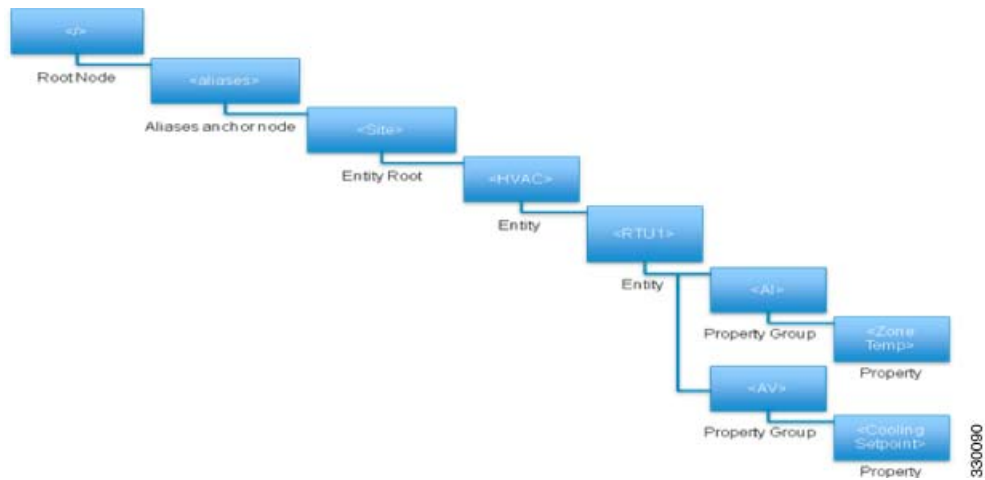


Entities provide a higher-order of abstraction. An Entity may consist of the properties of an "external" device coupled with its logical properties and associated logs, alarms and schedules. An entity may also be used to represent any physical object of interest. Some other important points related to entities are:

- Entities have a high degree of consistency with the BACnet object model.
- Entities support an extensible mechanism allowing for the addition of metadata like node type, purpose and engineering units.
- Entities allow for the association of an HTML display page.
- The relationship between Entities is established using a tree-like arrangement.
- Applications (Schedules, Setpoints, etc.) and external callers interact with Entities.

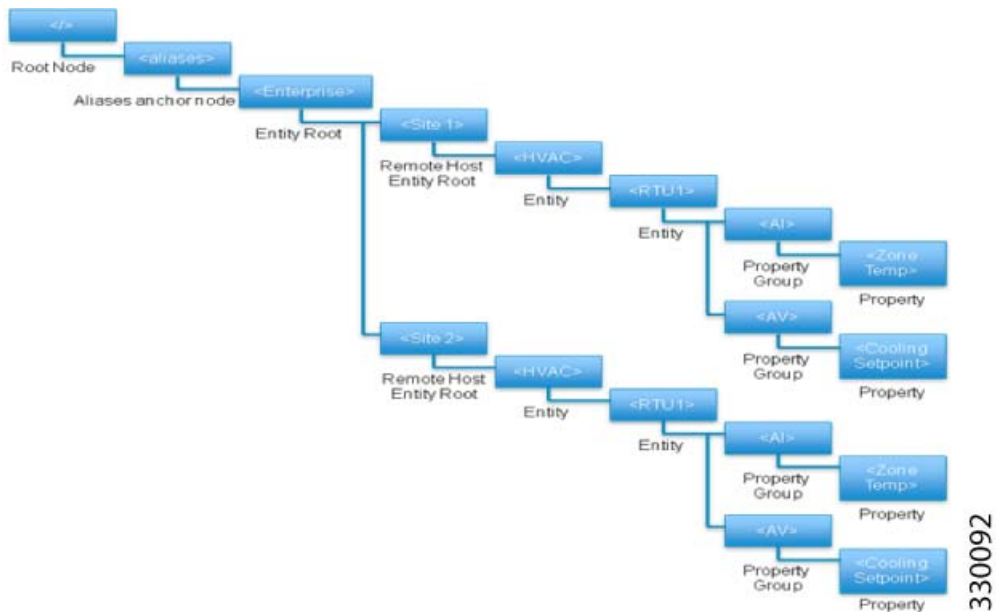
Example of an Entity configuration structure on a Mediator:

Figure 2-3 Entity Structure on the Mediator



Example of an Entity configuration structure on a Mediator Manager:

Figure 2-4 Entity Example

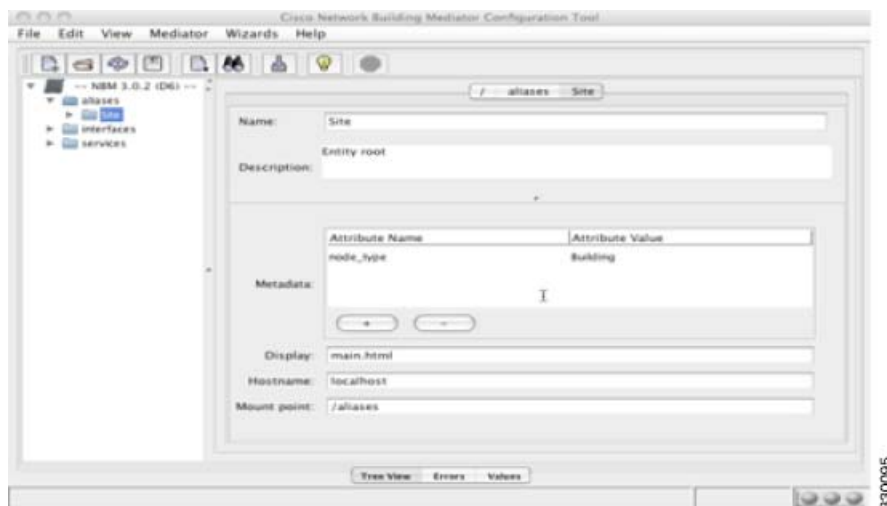


Each type of Entity has its own set of configuration options. These options are defined below:

Entity root

- Name—Name of the node. Used to create a global namespace for the node in the form of a URL. Also used as the node name in the navigation tree.
- Description—Describes the node type.
- Metadata—Used to add additional attributes such as node type.
- Display—HTML page that is displayed when this node is selected in the navigation tree.
- Hostname—Used by the Host Management Services to identify and connect to a device.
- Mount point—Used to identify where this root is configured on a remote host.

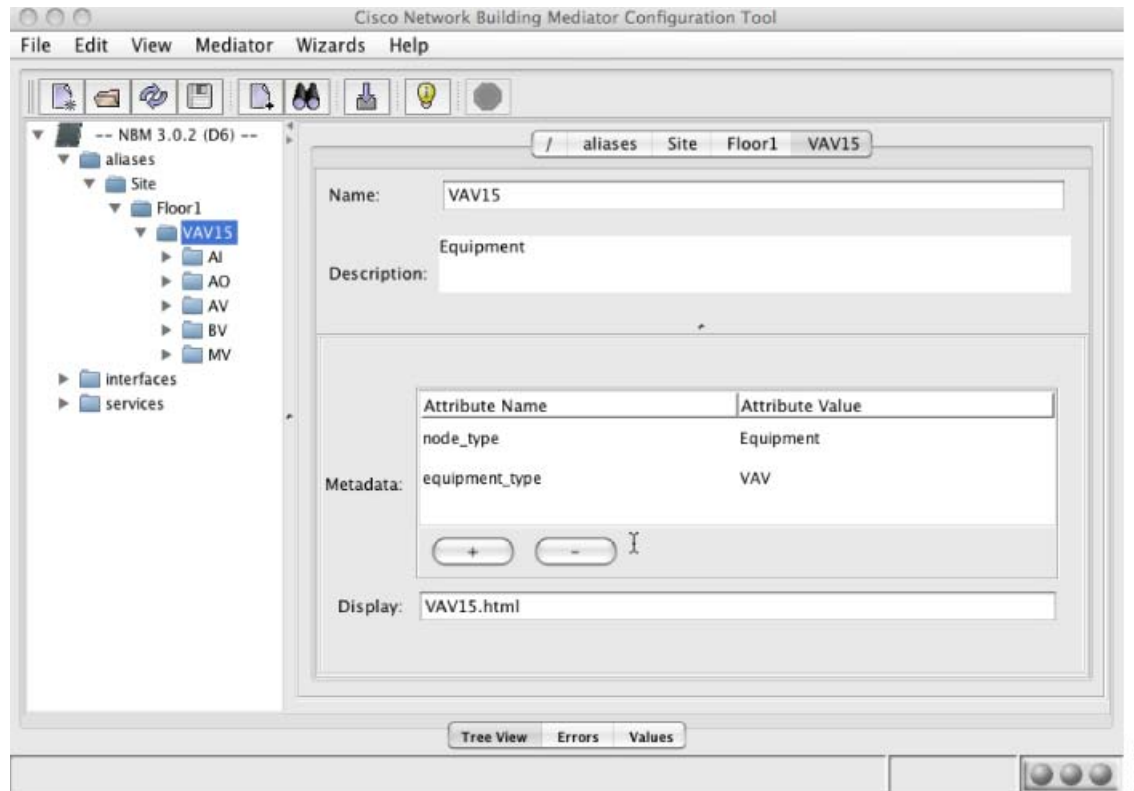
Figure 2-5 Entity Root



Entity

- Name—Name of the node. Used to create a global namespace for the node in the form of a URL. Also used as the node name in the navigation tree.
- Description—Describes the node type.
- Metadata —Used to add additional attributes such as equipment or node type.
- Display— HTML page that is displayed when this node is selected in the navigation tree.

Figure 2-6 Entity



Property Group

- Name—Name of the node. Used to create a global namespace for the node in the form of a URL.
- Description—Describes the node type.
- Type—Identifies property type.

Table 2-1 Property Group Types

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.(Overridable)
BV	A group of binary value properties.(Overridable)
I	A group of generic input properties.
Log	A group of log properties.

Property	Refers to
MI	A group of multistate input properties.
MO	A group of multistate output properties.(Overridable)
MV	A group of multistate value properties.(Overridable)
O	A group of generic output properties.(Overridable)
Sched	A group of schedule properties.

Property Configuration Options

- Name—Name of the node. Used to create a global namespace for the node in the form of a URL.
- Description—Describes the node type.
- Metadata—Used to add additional information about the node such as purpose or units.
- Refers to—The full path of the node this property refers to.
- Label—An optional label used by the UI when it displays this point.
- Description—An optional description for this point.

Figure 2-7 Property Configuration Options

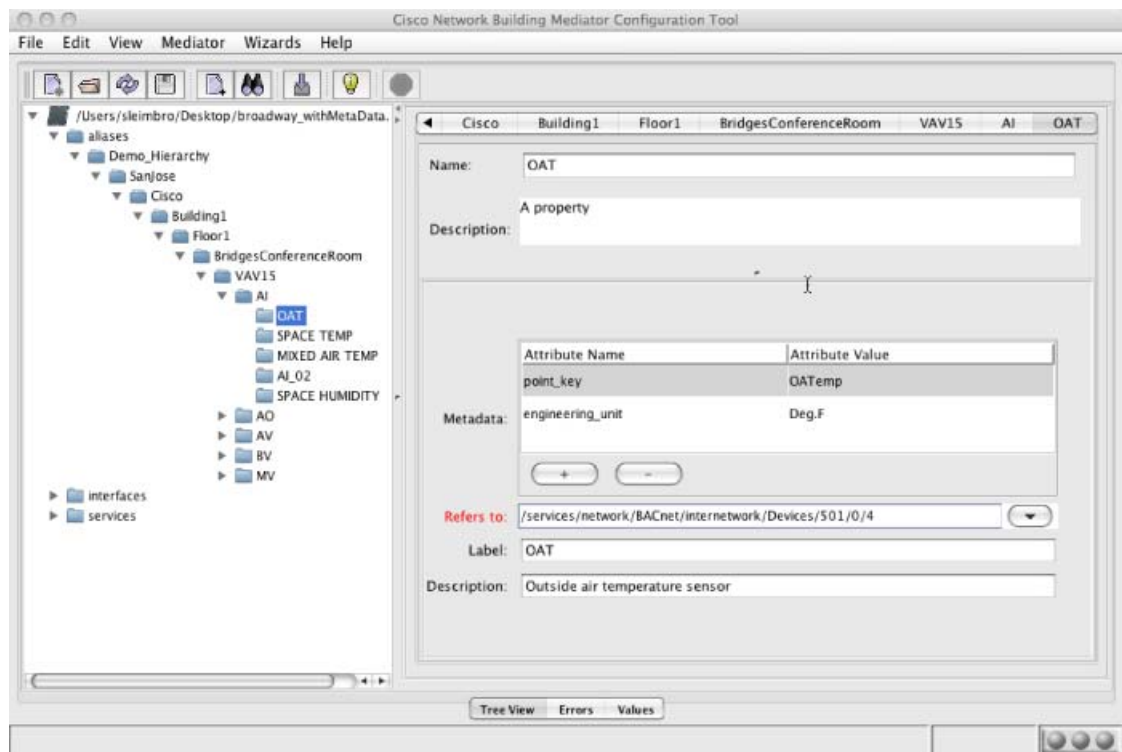


Table 2-2 Metadata Table

Attribute Name	Suggested Values
node_type	BaseHierarchy, Area, General, Building, Floor, Room, Equipment
equipment type	AHU, Boiler, BTU Meter, Chilled Water System, Chiller, Cisco Switch, Cooling Tower, Exhaust Fan, FCU, Gas Meter, Generator, Heat Pump, Heat Exchanger, Hot Water System, Lighting System, Oil Meter, Pump, Refrigeration System, RTU, Steam Flow Meter, UPS, UV, VAV, VFD, Water Meter, Weather Station

Table 2-2 Metadata Table (continued)

Attribute Name	Suggested Values
purpose	AuxHtg, Bo1CPmp, Bo1CPmpSts, Bo1En, Bo1HiFire, Bo1InTemp, Bo1LoFire, Bo1OutTemp, Bo1Sts, Bo2CPmp, Bo2CPmpSts, Bo2En, Bo2HiFire, Bo2InTemp, Bo2LoFire, Bo2OutTemp, Bo2Sts, CclVlcVtrl, CH1CntAlm, CH1Ctrl, CH1En, CH1sts, CH2CntAlm, CH2Ctrl, CH2En, CH2sts, ChgOvr, ChgOvrFb, CHWPmp1En, CHWPmp1Spd, CHWPmp1Sts, CHWPmp2En, CHWPmp2Spd, CHWPmp2Sts, CHWRTmp, CHWSTmp, ClgHtgVlv, ClgSPOffst, CWPmp1En, CWPmp1Spd, CWPmp1Sts, CWPmp2En, CWPmp2Spd, CWPmp2Sts, CWRTmp, CWSTmp, Comp1En, Comp1Fail, Comp2En, Comp2Fail, CoolEn, CoolingSP, CT1FanHi, CT1FanLo, CT1FanSpd, CT1HILWAlm, CT1LOLWAlm, CT2FanHi, CT2FanLo, CT2FanSpd, CT2HILWAlm, CT2LOLWAlm, DschPress, Dx1En, Dx2En, Dx3En, Dx4En, EaFanEn, EaFanSpd, EaFanSts, EconDmprCmnd, EconDmprPos, EconLowLimitSP, EffSP, EntCldTemp, EntHtTemp, FlowRate, FltAlm, HcVlvCtrl, HeatEn, HeatingSP, HtgSPOffst, HtgStg1, HtgStg2, HtgStg3, HtgStg4, HtRcvBypDmprCtl, HtRcvWhlCtrl, HtRcvWhlOut, HtRcvWhlSpd, HtRcvWhlSts, Humidity, HWDp, HWPmp1En, HWPmp1Sts, HWPmp2En, HWPmp2Sts, HWRTemp, HWSTemp, HXCap, Lightlvl, LightON_OFF, LightSts, Lux, LvgCldTemp, LvgHtTemp, MADmprCmnd, MADmprPos, MATemp, OATemp, OccClgSP, OccHtgSP, Occupancy, RACO2, RadStg1, RadStg2, RadVlvCtrl, RAFanEn, RAFanSpd, RAFanSts, RARH, RASmkAlm, RATemp, RmRH, RmTemp, RvrVlv, SAFanEn, SaFanSpdCtrl, SAFanSts, SAFlow, SARH, SASmkAlm, SASStaticPr, SATemp, SATempSP, StptOffst, SuctPress, UnOccClgSP, UnOccHtgSP, VavDmpr, VavDmprCmnd, WndDrct, WndSpd
engineering unit	Deg.F, Deg.C, Deg.K, GPM, PSI, Percent, RH, CFM, Amps, bar, BTU, Hg, H2O, FT, GAL, GPM, HZ, HP, in H2O, in HG, J, kV, kVA, kVAR, kWh, kW, LUM, MV, MHz, MOhm, MVA, MVAR, MW, MPH, mA, mV, mW, Ohm, PPM, Pa, PF, therm, ton, VA, VAR, V, Vac, Vdc, W-hr, W

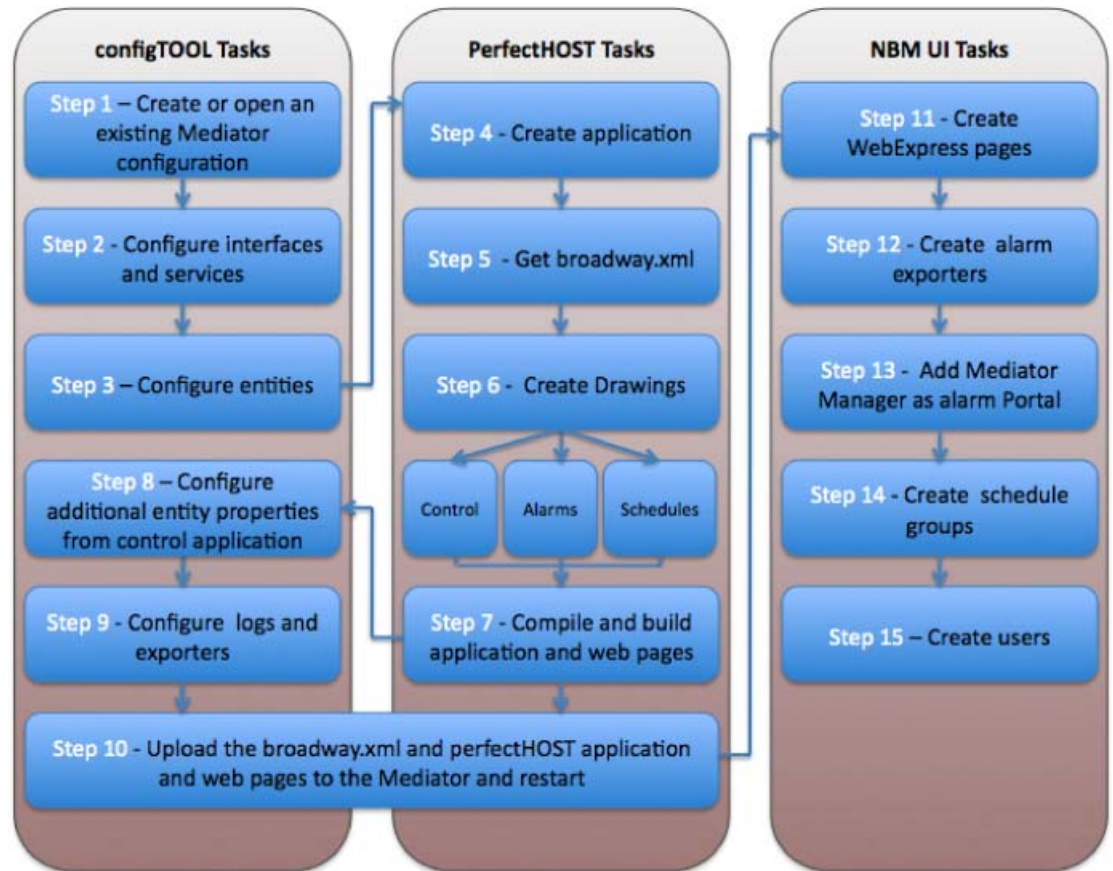
Mediator Configuration Workflow and Best Practice

Configuring the Mediator requires the use of three separate tools:

- configTOOL
- perfectHOST
- Mediator's web-based tools

The below workflow is recommended:

Figure 2-8 Mediator Configuration Workflow



330100

Mediator configuration workflow details are as below:

1. Create a new configuration or open an existing Mediator configuration
 - When working offline make sure to first 'load' the correct nodedefs by selecting **File > New Configuration > Select the correct Mediator software version > Select the correct Mediator platform**
2. Configure interfaces and services
 - Configure all interfaces (e.g., Modbus, Dallas) and protocol related services (e.g., BACnet, SNMP). Make sure appropriate services are enabled (e.g., RNA).
 - Discover auto-discovered protocols and save configuration as CSV for use when creating entities.

3. Configure entities

- Use generic names for the entity root and entities (e.g. Site, Building, RTU1, VAV1, etc.). This allows for the reuse of the configuration and associated control applications and web pages for similar sites.



Note

Only one entity root should be configured per Mediator.

- Create entities using appropriate property type mapping (e.g. Modbus input register maps to AI; BACnet points map one to one).
- Make sure overridable points are mapped to overridable property types (AO, AV, BO, BV, MO, MV and O).

4. Create PerfectHOST control applications

- Use meaningful names when creating the applications.
- Make sure to select 'Yes' when prompted if this is a 'TIM application'.
- Improve organization and reusability of application by creating subsystems (**File > Open Subsystem > New**). Each subsystem can be the control for a piece of equipment (e.g. rtu1, rtu2, rtu3, lighting, etc.).

5. Download broadway.xml from the Mediator

- Make sure to set the Mediator's address, username and password (**System > Comm Settings**) and save the application (**File > Save > Application**) before attempting to download the broadway.xml.
- If the Mediator and PerfectHOST programming tool are not on the same network, SCP broadway.xml from the /var/mpx/config directory on the Mediator to your local machines directory: C:/PhApps/<Application Name>/<Subsystem Name>.

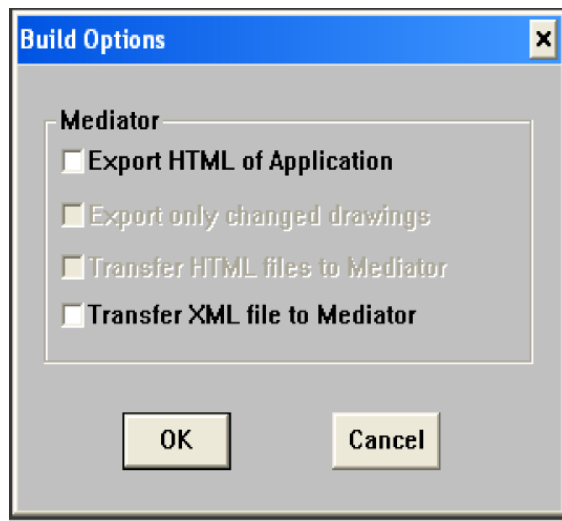
6. Create drawings

- Improve organization and reusability of subsystems by creating multiple drawings. (**Drawing > New Drawing**) Each drawing can be the control for a specific sequence (e.g. setpoint control, alarms, scheduling, etc.).

7. Compile and build application

- When you compile the application, make sure you get the below build options for the Mediator:Build Options

Figure 2-9 Build Options



- If you get different build options from the above, add a Mediator using the I/O Point editor (**File > I/O Point Editor**).
8. Configure additional entity properties from control applications
 - Create properties for any logic points that were added for equipment control (alarm thresholds, setpoint offsets, etc.).
 - Use description fields to identify these as being logical points.
 9. Configure logs and exporters
 - Make sure that any data that needs to be logged and exported is setup using configTOOL.
 - Trends created using the Mediator web tool should be considered transient and have no export option.
 10. Upload the `broadway.xml`, control service applications and web pages to the Mediator.

If configTOOL and the Mediator are not on the same network, SCP the `broadway.xml` file to the `/var/mpx/config` directory on the Mediator and restart - follow the steps below:

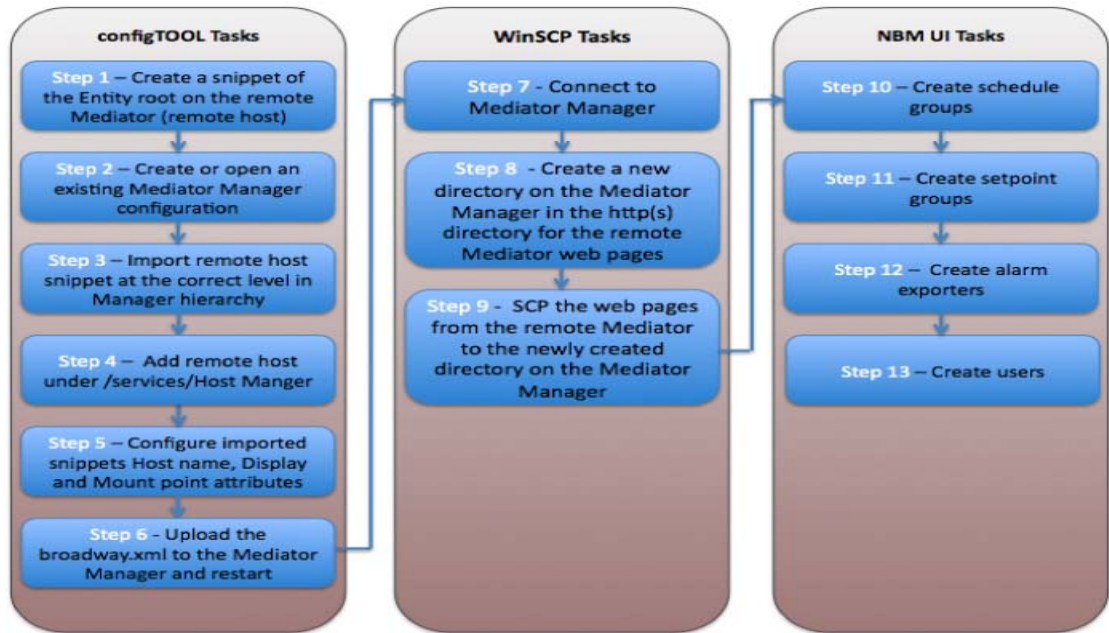
 - a. Connect to the Mediator with an SCP client and create new directories in `/var/mpx/www/http` for each subsystem (e.g. `/var/mpx/www/http/rtu1`).
 - b. Inside each of these new directories create a sub-directory named `images` (e.g., `/var/mpx/www/http/rtu1/images`).
 - c. SCP the control applications in `C:/PhApps/<Application Name>/<Subsystem Name>/<Subsystem Name.xml>` to the `/var/mpx/config/services/control` directory.
 - d. Repeat for each subsystem.
 - e. SCP the web pages in `C:/PhApps/<Application Name>/<Subsystem Name>/_HTML/*.htm` to the `/var/mpx/www/http/<Application Name>` directory on the Mediator - this is the directory you created in Step (1).
 - f. SCP the web page background images in `C:/PhApps/<Application Name>/<Subsystem Name>/_HTML/*.png` to the `/var/mpx/www/http/<Application Name>/images` directory on the Mediator - this is the directory you created in Step (2).
 11. Create equipment monitoring and dashboard web pages using WebExpress.

- Create web pages using generic names to increase reusability.
 - Use generic names for the web pages (e.g. rtu1.html, rtu2.html, etc.); this allows for reusing the web pages on similar sites.
12. Create alarm exporters
 - Optional if configured on Mediator Manager
 - Make sure to configure a DNS server if the SNMP server is being configured to use a hostname.
 - Create and test an alarm while running the Mediator's message log and watch for any errors. (To run the message log, SSH into the Mediator and type the command: msglog_viewer -f).
 13. Add Mediator Manager as alarm portal
 - Configure Mediator Manager as the portal in the Events tool under Cloud to propagate the Mediator alarms to the Mediator Manager.
 14. Create schedule groups
 - Group schedules at the Mediator level before adding them to the Mediator Manager to improve schedule organization.
 15. Create an account for any users that may need local access
 - This step is not necessary since access will typically be through the manager.

Mediator Manager Configuration Workflow and Best Practice

Configuring the Mediator Manager requires the use of three separate tools: configTOOL, WinSCP and the Mediator Manager's web-based tools. The below workflow is recommended:

Figure 2-10 Mediator Manager Configuration Workflow



Mediator manager configuration workflow details:

1. Create a snippet of the entity root on the remote Mediator

- Launch configTOOL and connect to the Mediator.
 - Under /aliases, right-click the node at the Entity root level.
 - Select 'Output from here'.
 - Select Save to File
 - Name the snippet with a .xml extension and save.
2. Create or open the Mediator Manager configuration in configTOOL
 - If working offline make sure to load the latest nodedefs by selecting File > New Configuration and selecting the appropriate software version and the Mediator Manager platform
 3. Import the snippet from the remote Mediator into the Mediator Manager configuration
 - Create a logical hierarchy by nesting entities to create additional areas (e.g., Cisco > United States > San Jose).
 - A logical, consistently named site organization allows users to make successful predictions about where to find things.
 - Import the snippet by selecting the desired level in the hierarchy then right-clicking and selecting **System > Import configuration fragment**.
 4. Add the remote Mediator as a Remote Host on the Mediator Manager
 - Under /services, right-click **Host Manager** and select **Add > Remote Host (Host)**.
 - In the Name field at the top, enter a meaningful name (e.g., building number) so the site is easily identifiable.
 - In the Host field enter the IP address or host name.
 - If a host name is used make sure a DNS server is configured.
 - Make sure the security level selected matches the security level defined on the Mediator Manager under /services/network/rna.
 5. Configure imported remote Mediator snippet
 - Modify the display page link by appending a unique identifier for the site (e.g., building number, store number, etc.). In step 8 you will create this directory on the Mediator Manager and transfer the web pages from the remote Mediator to the Mediator Manager.
 - Modify the Hostname from 'localhost' to match the name used for this Mediator under /services/Host Manager on the Mediator Manager. Make sure that the name is identical in spelling and case on the Mediator and the Mediator Manager.
 - Modify the Mount point to the location of the snippet on the remote Mediator (e.g., /aliases/Site).
 6. Upload the `broadway.xml` to the Mediator Manager and restart
 - Verify that the remote Mediator is communicating with the Mediator Manager by checking to see if values for the remote Mediator load on the Mediator Manager.
 - If no values are loading verify the Host name matches under aliases and the Host Management service, the Mount point is correct, the IP address is correct, RNA is enabled on both and the RNA security level matches.
 7. Connect to the Mediator Manager with WinSCP or other SCP client
 - Alternatively you can SSH into the Mediator Manager and perform steps 8 & 9 from the command line using the `cd`, `mkdir`, and `scp` commands.
 8. Create a new directory for remote Mediator web pages on the Mediator Manager

- This new directory is a sub-directory in /var/mpx/www/http(s)/
 - The name of the new directory must be the same name you appended to the display path in Step 5
9. SCP the user generated web page from the remote Mediator to the Mediator Manager.
 - This is a two-step process that requires you to copy the files from the Mediator to your local system then copy the files to the Mediator Manager.
 10. Create schedule groups
 - Create or edit an existing schedule group to include schedules inherited from the remote Mediator.
 11. Create setpoint groups
 - Create or edit an existing setpoint group to include setpoints from the remote Mediator.
 12. Configure alarm exporters
 - Optional if configured on Mediator
 - Make sure to configure a DNS server if the SNMP server is being configured to use a hostname.
 - Create and test an alarm while running the Mediator Manager's message log and watch for any errors. (To run the message log, SSH into the Mediator and type the command: msglog_viewer -f).
 13. Create users
 - If required, create accounts for new users.

Commissioning

This section presents procedures for use in the checkout of a Mediator system. These procedures verify that the system is installed and operating properly and performing as designed. These procedures may be used when commissioning new systems or after modifications to the existing system.

See ASHRAE Guideline 0-2005 for detailed commissioning guidelines.

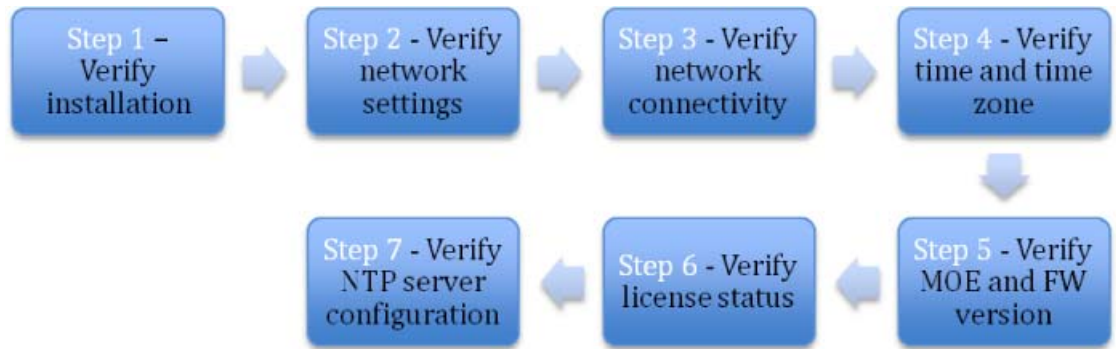
Before beginning work, a checkout form should be prepared for each component in the system. These checkout forms should be assembled and retained as proof of system checkout.

This section includes the following sections:

- [Mediator Checkout Procedure, page 2-14](#)
- [Mediator Manager Checkout Procedure, page 2-16](#)
- [3rd Party Device Controls Checkout Procedure, page 2-17](#)

Mediator Checkout Procedure

Checkout of the Mediator requires physical and network access. The below steps are recommended:

Figure 2-11 Mediator Checkout Procedure

330124

Verify installation

- Verify that the Mediator Manager is installed in accordance with the Hardware installation guide which can be found at the below link:

http://www.cisco.com/en/US/docs/security/physical_security/cnbm_mgr/1.x/HW/Installation_Guide/hig.html

Verify network settings

- Browse to the Mediator Manager System page and verify the network settings are correct.
- Make sure that a Name server is configured if any services (e.g., alarm exporters, log exporters) use a host name instead of an IP address.

Verify network connectivity

- Make sure all required inbound and outbound ports are open. Port details can be found in Chapter 1 Deployment Architecture.

Verify time and time zone

- From the command line, verify the time and time zone are correct by doing the following:
 1. Type date and verify the time, date and time zone are correct.
 2. If these need to be adjusted type 'mpxconfig' and select 'Set system date and time'.

Verify MOE and Framework version

1. Browse to the Mediator Manager System page and check the MOE and Framework version.
2. Verify it's the latest MOE and Framework version by browsing to the below link and selecting the appropriate platform and then selecting installation software:

<http://www.cisco.com/cisco/software/navigator.html?mdfid=282681537&i=rm>

3. If the Mediator Manager is not running the latest MOE or Framework it should be upgraded

http://www.cisco.com/en/US/docs/security/physical_security/cnbm_mgr/1.x/User/guide/Installation.html

Verify license status

- Browse to the Mediator System page and verify that the correct level of licensing is enabled (Base, Intermediate or Advanced).

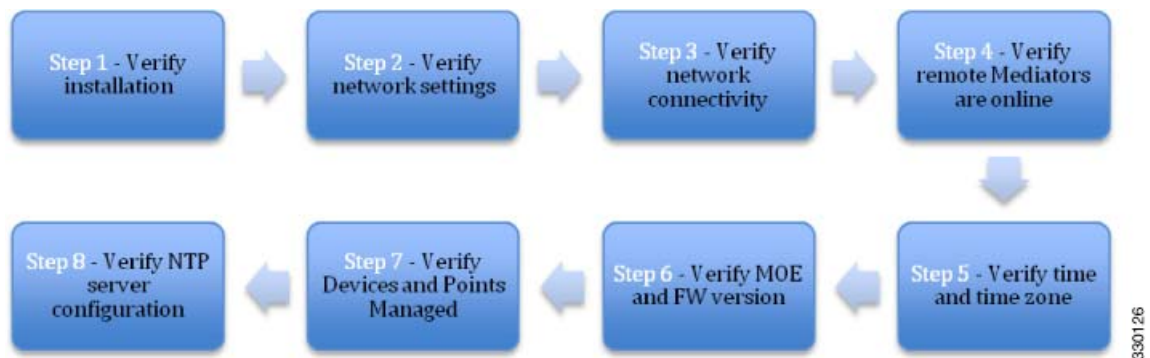
Verify NTP server configuration

- Connect to the Mediator Manager with configTOOL and verify that a timeserver is configured under /services/time/synch_continuous.

Mediator Manager Checkout Procedure

Checkout of the Mediator Manager requires physical and network access. The below steps are recommended:

Figure 2-12 Mediator Checkout Procedure



Verify installation

- Verify that the Mediator Manager is installed in accordance with the Hardware installation guide which can be found at the below link:

http://www.cisco.com/en/US/docs/security/physical_security/cnrm_mgr/1.x/HW/Installation_Guide/hi g.html

Verify network settings

- Browse to the Mediator Manager System page and verify the network settings are correct.
- Make sure that a Name server is configured if any services (e.g., alarm exporters, log exporters) use a host name instead of an IP address.

Verify network connectivity

- Make sure all required inbound and outbound ports are open. Port details can be found in Chapter 1 Deployment Architecture.

Verify remote Mediators are online

- Browse to the Mediator Manager and from the global navigation pane; verify the downstream mediators are indicated as 'online'.

Verify time and time zone

- From the command line, verify the time and time zone are correct by doing the following:
 1. Type date and verify the time, date and time zone are correct.
 2. If these need to be adjusted type 'mpxconfig' and select 'Set system date and time'.

Verify MOE and Framework version

- Browse to the Mediator Manager System page and check the MOE and Framework version.

- Verify it's the latest MOE and Framework version by browsing to the below link and selecting the appropriate platform and then selecting installation software:

<http://www.cisco.com/cisco/software/navigator.html?mdfid=282681537&i=rm>

- If the Mediator Manager is not running the latest MOE or Framework it should be upgraded using the instructions in the User Guide which can be found at the below link:

http://www.cisco.com/en/US/docs/security/physical_security/cnbn_mgr/1.x/User/guide/Installation.html

Verify Devices and Points managed are within limits

- Browse to the System page on the NBM manager and verify that the 150,000 point and 350 Mediator limit has not been reached.

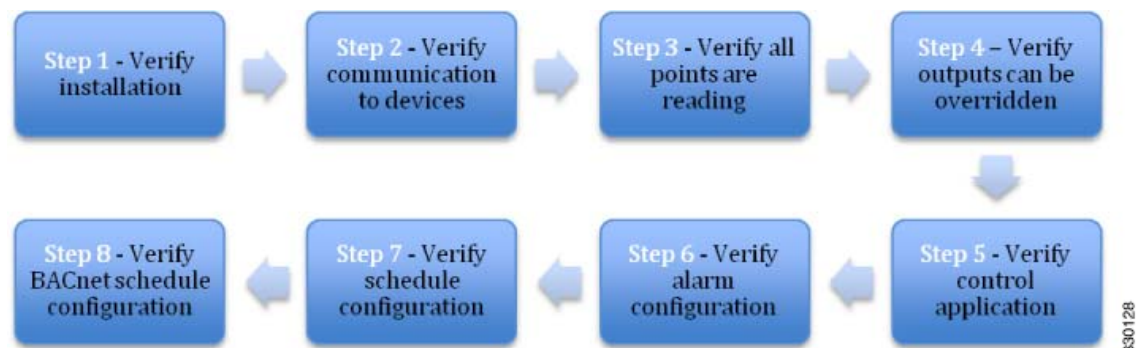
Verify NTP server configuration

- Connect to the Mediator Manager with configTOOL and verify that a timeserver is configured under /services/time/synch_continuous.

3rd Party Device Controls Checkout Procedure

Checkout of 3rd party devices connected to a Mediator varies depending on type of equipment controlled and manufacturer. The below is meant as a general overview of the procedure; please consult the device manufacturer for specific commissioning procedures.

Figure 2-13 3rd Party Device Controls Checkout Procedure



Steps below:

- Verify installation
 - Verify all devices are mounted and wired according to the manufacturer's recommendations.
- Verify communication from devices to the Mediator
 - Verify that the Mediator can communicate with all the devices on the network.
- Verify all points are reading
 - Verify that all the points for each device are being read on the Mediator.
- Verify outputs can be overridden
 - Verify that each output on the device can be overridden from the Mediator.
 - Verify the actual change in the output with a multimeter.

- Verify control application
 - Verify the control applications work per the sequence of operation by overriding points to simulate schedule changeover, alarm and failure conditions.
- Verify alarm configuration
 - Verify the alarm configuration by overriding points to simulate alarm conditions
 - Verify that the alarms show up in the Mediator Event queue and on the Mediator Manager if configured.
- Verify schedule configuration
 - Verify the schedule configuration by changing the schedule start/stop times and ensuring that the device changes the mode of operation.
- Verify BACnet schedule configuration
 - Verify that the device is added as a BACnet time sync client. See Configuring BACnet Schedules and BACnet Time Synchronization in the User Guide which can be found at the below link.

http://www.cisco.com/en/US/docs/security/physical_security/cnbm/3.x/User/Guide/PP.html#wp1076500

- Verify that the BACnet client schedules show up in the Mediator Schedule tool.

Backup and Restore

This section presents procedures for setting up automated and scheduled tasks. This chapter includes the following sections:

- [Backing up the Mediator, page 2-18](#)
- [Backing up the Mediator Manager, page 2-22](#)
- [Restoring the Mediator, page 2-25](#)
- [Restoring the Mediator Manager, page 2-26](#)

Backing up the Mediator

There are three options available for backing up the Mediator. The options are outlined below:

1. Backup manually using the Mediator System page
2. Backup manually from the command line
3. Backup automatically using cron



Note

The Mediator must be running at least framework version 3.1.3(x) to utilize cron.

Steps to backup the Mediator manually using the System page:

- Browse to the Mediator System page (<http://ipaddress/system.html>).
- Select the Backup/Restore tab.
- Select the Backup button next to 'Generate a new backup:'.



Note This may take a few minutes.

- Select the Save button, select the location for the backup and select the Save button. Optionally you can rename the backup file with the date or other unique identifier if multiple backups are being retained

Steps to backup the Mediator manually from the command line:

- Connect to the Mediator with an SSH client such as PuTTY.
- Create a compressed backup using the below command:

```
[mpxadmin@nbm] $ tar czPf mediator_backup.tgz /var/mpx/www/http /var/mpx/www/https /var/mpx/config
```

- Optional - Exclude files by listing these in a text file using the below commands:

```
[mpxadmin@nbm] $ vi exclude.txt
```

Type 'i' to insert text and type the full directory path for the files to be excluded.

```
/var/mpx/config/broadway.xml.*
```

```
/var/mpx/www/http/customImages
```

Hit the Escape key to terminate insert-text mode and type 'ZZ' to save and exit.

```
[mpxadmin@nbm] $ tar czPf mediator_backup.tgz -X exclude.txt /var/mpx/www/http /var/mpx/www/https /var/mpx/config
```

- Optional - Transfer the file to a remote server. An example of transferring files to a server from the Mediator is below:

```
[mpxadmin@nbm] $ scp mediator_backup.tgz user@server:/backups/
```

Steps to backup the Mediator automatically using cron:

Cron is a utility that allows tasks to automatically run in the background at specified intervals.

- Connect to the Mediator with an SSH client such as PuTTY.
- Create a file which contains the commands you want executed using the below commands:

```
[mpxadmin@nbm] $ vi backup
```

Type 'i' to insert text and type the following.

```
tar czPf /home/mpxadmin/mediator_backup.tgz -X /home/mpxadmin/exclude.txt /var/mpx/www/http /var/mpx/www/https /var/mpx/config
```

Hit the Escape key to terminate insert-text mode and type 'ZZ' to save and exit.

```
[mpxadmin@nbm] $ chmod a+x backup
```

- Create a cron job file which describes the program that you want executed and the times that cron should execute them using the below commands

```
[mpxadmin@nbm] $ vi backup.cron
```

Type 'i' to insert text and type the following.

```
0 0 * * 0 /home/mpxadmin/backup
```

Hit the Escape key to terminate insert-text mode and type 'ZZ' to save and exit.

This schedules the backup to occur weekly on Sunday at midnight. Crontab syntax is below:

Figure 2-14 Crontab Syntax



Use crontab to load the cron jobs into cron using the following command

```
[mpxadmin@nbm ~] $ crontab backup.cron
```

- Check to see if it was loaded by typing `crontab -l`. It should display:

```
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (backup.cron installed on Tue May 3 11:09:58 2011)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
0 0 * * 0 /home/mpxadmin/backup
```

Optional - Automatically transfer the file to a remote server using Cron, SFTP and a Python script.

- Create a Python script to SFTP the backup to a remote server by using the following commands:

```
[mpxadmin@nbm ~] $ vi backup.py
```

Type 'i' to insert text and type or copy and paste the following.

```
#!/usr/bin/env python-mpx
```

```
# version 1
```

```
import paramiko

# set the server parameters.

# replace serverIP, sftpUser, sftpPass and serverDir with the server address, backup directory,
  username and password

host = "serverIP"

port = 22

transport = paramiko.Transport((host, port))

password = "sftpUser"

username = "sftpPass"

directory = "serverDir"

try:

    transport.connect(username = username, password = password)

    sftp = paramiko.SFTPClient.from_transport(transport)

    filepath = '/home/mpxadmin/mediator_backup.tgz'

    localpath = '/' + directory + '/mediator_backup.tgz'

    sftp.put(filepath, localpath)

    print 'Copying mediator backup to ' + host + '.'

    sftp.close()

    transport.close()

except:

    print 'Could not connect. Make sure you can ping ' + host + '.'

    sftp.close()

    transport.close()
```

Hit the Escape key to terminate insert-text mode and type 'ZZ' to save and exit.

```
[mpxadmin@nbm ~] $chmod a+x backup.py
```

- Modify the backup cron job file to include the transfer script using the below commands:

```
[mpxadmin@nbm] $ vi backup.cron
```

Type 'i' to insert text and type the following.

```
0 0 * * 0 /home/mpxadmin/backup
```

```
30 0 * * 0 /home/mpxadmin/backup.py
```

Hit the Escape key to terminate insert-text mode and type 'ZZ' to save and exit.

- Use crontab to load the cron jobs into cron using the following command:

```
[mpxadmin@nbm ~] $ crontab backup.cron
```

- Check to see if it was loaded by typing crontab -l. It should display:

```
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (backup.cron installed on Tue May 3 11:09:58 2011)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
0 0 * * 0 /home/mpxadmin/backup
30 0 * * 0 /home/mpxadmin/backup.py
```

Backing up the Mediator Manager

There are three options available for backing up the Mediator Manager. The options are outlined below:

- Backup manually using the Mediator Manager System page
- Backup manually from the command line
- Backup automatically using cron

Steps to backup the Mediator Manager manually using the System page

- Browse to the Mediator Manager System page (<http://ipaddress/system.html>).
- Select the Backup/Restore tab.
- Select the Backup button next to 'Generate a new backup:'.



Note This may take a few minutes.

- Select the Save button, select the location for the backup and select the Save button. Optionally you can rename the backup file with the date or other unique identifier if multiple backups are being retained.

Steps to backup the Mediator Manager manually from the command line

- Connect to the Mediator Manager with an SSH client such as PuTTY.
- Create a compressed backup using the below command:

```
[mpxadmin@nbm] $ tar czPf mediator_manager_backup.tgz /var/mpx/www/http
/var/mpx/www/https /var/mpx/config
```

- Optional - Exclude files by listing these in a text file using the below commands:

```
[mpxadmin@nbm] $ vi exclude.txt
```

Type 'i' to insert text and type the full directory path for the files to be excluded.

```
/var/mpx/config/broadway.xml.*
```

```
/var/mpx/www/http/customImages
```

Hit the Escape key to terminate insert-text mode and type 'ZZ' to save and exit.

```
[mpxadmin@nbm] $ tar czPf mediator_manager_backup.tgz -X exclude.txt
/var/mpx/www/http /var/mpx/www/https /var/mpx/config
```

- Optional - Transfer the file to a remote server. An example of transferring files to a server from the Mediator Manager is below:

```
[mpxadmin@nbm] $ scp mediator_manager_backup.tgz user@server:/backups/
```

Steps to backup the Mediator Manager automatically using cron

Cron is a utility that allows tasks to automatically run in the background at specified intervals.

- Connect to the Mediator Manager with an SSH client such as PuTTY.
- Create a file which contains the commands you want executed using the below commands:

```
[mpxadmin@nbm] $ vi backup
```

Type 'i' to insert text and type the following.

```
tar czPf /home/mpxadmin/mediator_manager_backup.tgz -X /home/mpxadmin/exclude.txt
/var/mpx/www/http /var/mpx/www/https /var/mpx/config
```

Hit the Escape key to terminate insert-text mode and type 'ZZ' to save and exit.

```
[mpxadmin@nbm] $ chmod a+x backup
```

- Create a cron job file which describes the program that you want executed and the times that cron should execute them using the below commands:

```
[mpxadmin@nbm] $ vi backup.cron
```

Type 'i' to insert text and type the following.

```
0 0 * * 0 /home/mpxadmin/backup
```

Hit the Escape key to terminate insert-text mode and type 'ZZ' to save and exit.

This schedules the backup to occur weekly on Sunday at midnight. Crontab syntax is below:

Figure 2-15 Crontab Syntax



380131

- Use crontab to load the cron jobs into cron using the following command:

```
mpxadmin@nbm ~] $ crontab backup.cron
```

- Check to see if it was loaded by typing crontab -l. It should display:

```
0 0 * * 0 /home/mpxadmin/backup
```

- Optional - Automatically transfer the file to a remote server using Cron, SFTP and a Python script.
- Create a Python script to SFTP the backup to a remote server by using the following commands.

```
xadmin@nbm ~] $vi backup.py
```

Type 'i' to insert text and type or copy and paste the following.

```
#!/usr/bin/env python-mpx
```

```
# version 1
```

```
imp# set the server parameters.
```

```
# replace serverIP, sftpUser, sftpPass and serverDir with the server address, backup directory,
  username and password
```

```
host = "serverIP"
```

```
port = 22
```

```
transport = paramiko.Transport((host, port))
```

```
password = "sftpUser"
```

```
username = "sftpPass"
```

```
direct# set the server parameters.
```

```
# replace serverIP, sftpUser, sftpPass and serverDir with the server address, backup directory,
  username and password
```

```
host = "serverIP"
```

```
port = 22
```

```
transport = paramiko.Transport((host, port))
```

```
password = "sftpUser"
```

```
username = "sftpPass"
```

```
directory = "serverDir")
```

Hit the Escape key to terminate insert-text mode and type 'ZZ' to save and exit.

```
[mpxadmin@nbm ~] $chmod a+x backup.py
```

- Modify the backup cron job file to include the transfer script using the below comments:

```
[mpxadmin@nbm] $ vi backup.cron
```

Type 'i' to insert text and type the following.

```
0 0 * * 0 /home/mpxadmin/backup
```

```
30 0 * * 0 /home/mpxadmin/backup.py
```

Hit the Escape key to terminate insert-text mode and type 'ZZ' to save and exit.

- Use crontab to load the cron jobs into cron using the following command

```
[mpxadmin@nbm ~] $ crontab backup.cron
```

- Check to see if it was loaded by typing crontab -l. It should display:

```
0 0 * * 0 /home/mpxadmin/backup
```

```
30 0 * * 0 /home/mpxadmin/backup.py
```

Restoring the Mediator

The Mediator can be restored from a backup file created using any of the methods listed above by following the below steps:

1. If the Mediator is being replaced, ensure that it's installed according to the Installation Guidelines and it's running the correct framework version.
2. Connect to the Mediator with a web browser.
3. After logging into the Mediator select the Systems tab.
4. Select the Backup/Restore tab on the Systems page.
5. Click on the Browse... button, locate and select the backup file on your local system.
6. Click on the Restore button.
7. Wait for the following confirmation message: Backup restored successfully
 - If the backup file was not located or it is not a valid backup file you'll receive the following error: ERROR: Invalid backup file "". Make sure that the correct file was selected and that it was generated using one of the methods described above.
8. Select the Status tab to return to the System Status page.

9. Click on the Reboot button to restart the Mediator. The Mediator will restart running the restored configuration.

Restoring the Mediator Manager

The Mediator Manager can be restored from a backup file created using any of the methods listed above by following the below steps:

1. If the Mediator Manager is being replaced, ensure that it's installed according to the Installation Guidelines and it's running the correct framework version.
2. Connect to the Mediator Manager with a web browser.
3. After logging into the Mediator Manager select the Systems tab.
4. Select the Backup/Restore tab on the Systems page.
5. Click **Browse**, locate and select the backup file on your local system.
6. Click **Restore** button.
7. Wait for the following confirmation message: **Backup restored successfully**
 - If the backup file was not located or it is not a valid backup file you'll receive the following "error: ERROR: Invalid backup file". Make sure that the correct file was selected and that it was generated using one of the methods described above.
8. Select the Status tab to return to the System Status page.
9. Click **Reboot** to restart the Mediator Manager.

The Mediator Manager will restart running the restored configuration.