SmartStruxure Lite Solution

MPM Series

Installation Instructions

Site and zone managers providing wired and wireless integrated control solutions for HVAC, lighting, and metering, as well as remote management via StruxureWare™ Building Expert.

MPM - UN Multipurpose Manager

MPM - VA VAV Manager

MPM - GW Wireless Manager

Get Control. Get Efficient. Get Value

Who Should Read this Guide

This guide is for integrators of SmartStruxure^{TM} Lite solutions. It provides important information for getting you started with the set-up and configuration of your building efficiency management system.

Ensure you follow the instructions to ensure a successful and trouble-free installation at the client's site.

Plan and Prepare

Read this entire guide
The information contained in this guide helps you work effectively and minimizes the likelihood of any critical issues occurring during installation. Keep this document handy when doing your installation.

Prepare your equipment before going to customer site
Commission and configure the equipment before you arrive at the customers site. Successful installation of your SmartStruxure Lite system requires proper preparation and planning. Planning in advance saves resources, prevents wasted effort, and saves time and money for you and your customer.

About this Guide

This guide provides instructions for the physical installation of the hardware components of your SmartStruxure Lite system. It also provides overviews of creating a network of Multi-purpose Manager (MPM) devices for the following:

- MPM-UN Multi-purpose Manager
- MPM-VA VAV Manager
- MPM-GW Wireless Manager

For more information visit our website at:

www.documentation.smartstruxurelite.com

Overview

Multi-Purpose Management Devices are flexible lines of site and zone Managers. They allow facility Managers and Contractors to install and manage integrated solutions for HVAC, lighting, and metering. They are also a quick and efficient link between multiple devices based on many standard protocols.

The Building Expert web building energy management system is embedded in the MPM Devices. The devices are also BACnet and oBIX compliant for integration into larger StruxureWare systems.

MPM-UN Multi-purpose Manager

The MPM-UN is an electronic device designed to monitor and control various end-devices for building automation applications. The Manager consists of a printed circuit board housed in a plastic shell casing.

External connectors are available for the following:

- 6 universal inputs
- 4 analog outputs
- 2 binary outputs (dry contact)
- LAN (Ethernet cable)
- RS-485 device (Modbus)
- CANbus
- Power supply

The Manager is compatible with BACnet (IP/Ethernet) and oBix. The device has optional wireless modules to enable bidirectional communication with EnOcean and ZigBee devices. As well, Managers may also communicate with each other wirelessly using their ZigBee modules.

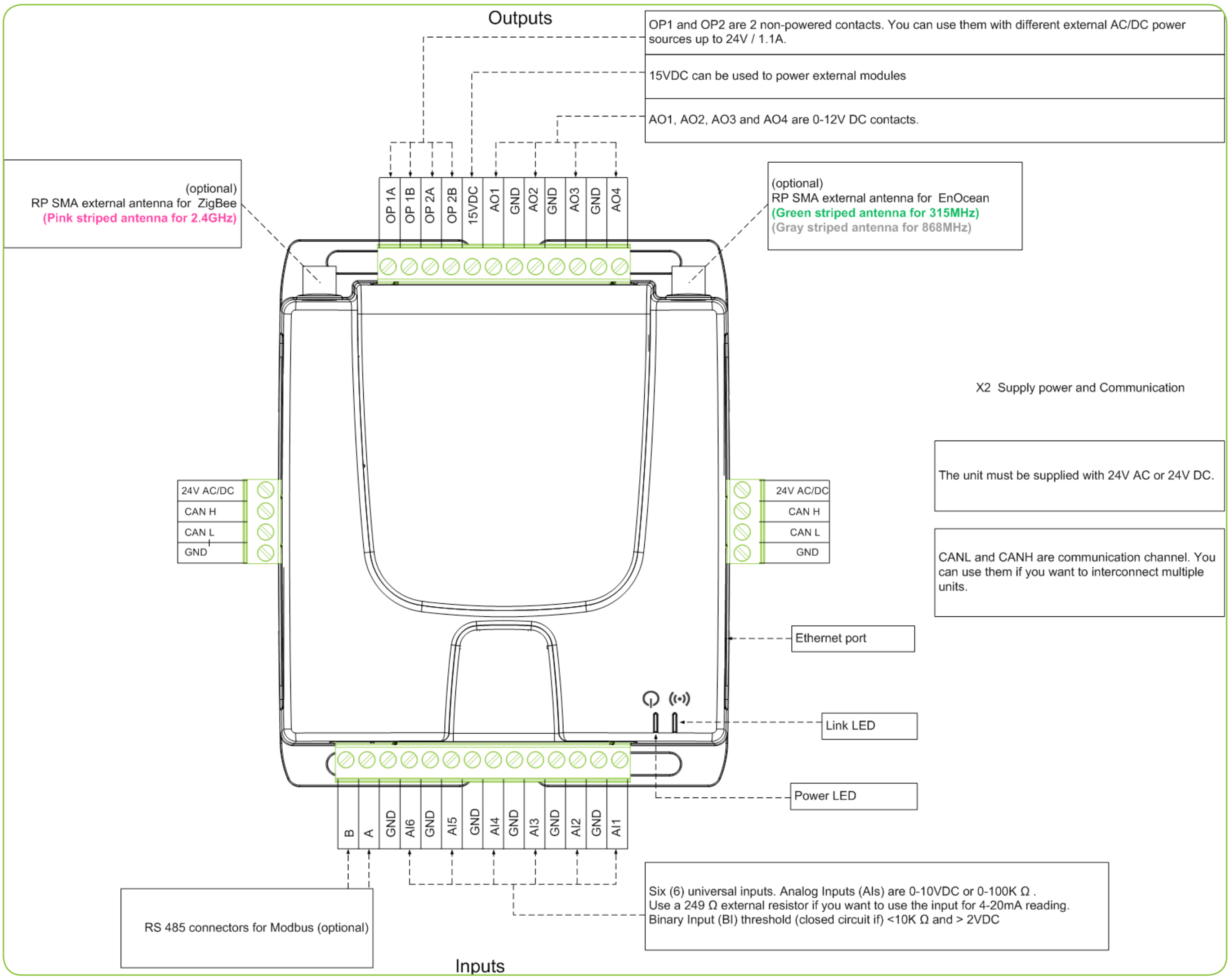
Uses

Multi-purpose Managers are fully programmable and are designed with wireless lighting and HVAC applications in mind. They can also be used to control a wide range of wired and wireless (EnOcean and ZigBee-compatible) end-devices, including light sensors, light switches, relays, thermostats, card readers, and magnetic door contacts. They are also targeted for commercial, industrial, and institutional buildings.

Pinout Diagram

The below figure shows the pinout information for the MPM - UN.

NOTE: You must remove the pink cap from the MPM before you install the pink-striped ZigBee antenna.


Outputs
OP1 and OP2 are 2 non-powered contacts. You can use them with different external AC/DC power sources up to 24V / 1.1A.
15VDC can be used to power external modules
AO1, AO2, AO3 and AO4 are 0-12V DC contacts.
(optional)
RP SMA external antenna for ZigBee
(Pink striped antenna for 2.4GHz)
OP 1A
OP 1B
OP 2A
OP 2B
15VDC
AO1
GND
AO2
GND
AO3
GND
AO4
(optional)
RP SMA external antenna for EnOcean
(Green striped antenna for 315MHz)
(Gray striped antenna for 868MHz)
X2 Supply power and Communication
The unit must be supplied with 24V AC or 24V DC.
CANL and CANH are communication channel. You can use them if you want to interconnect multiple units.
24V AC/DC
CAN H
CAN L
GND
24V AC/DC
CAN H
CAN L
GND
Ethernet port
Link LED
Power LED
B
A
GND
AI6
GND
AI5
GND
AI4
GND
AI3
GND
AI2
GND
AI1
RS 485 connectors for Modbus (optional)
Six (6) universal inputs. Analog Inputs (AIs) are 0-10VDC or 0-100K Ω .
Use a 249 Ω external resistor if you want to use the input for 4-20mA reading.
Binary Input (BI) threshold (closed circuit if) <10K Ω and > 2VDC
Inputs

MPM-VA VAV Manager

The MPM-VA VAV Manager is an electronic device designed to monitor and control various end-devices for building automation purposes, including VAV boxes. It can also control various end-devices for building automation applications.

The device consists of a printed circuit board housed in a plastic shell casing.

External connectors are available for the following:

- 6 universal inputs
- 4 analog outputs
- 2 binary outputs (dry contact)
- 1 damper actuator
- 1 pressure sensor
- LAN (Ethernet cable)
- RS-485 device (Modbus)
- CANbus
- Power supply

The device has a pressure sensor and is equipped with an optional damper actuator. The device also has optional embedded EnOcean and ZigBee wireless modules to enable bidirectional communication with EnOcean and ZigBee devices. The Managers can communicate with each other wirelessly using their ZigBee modules.

Uses

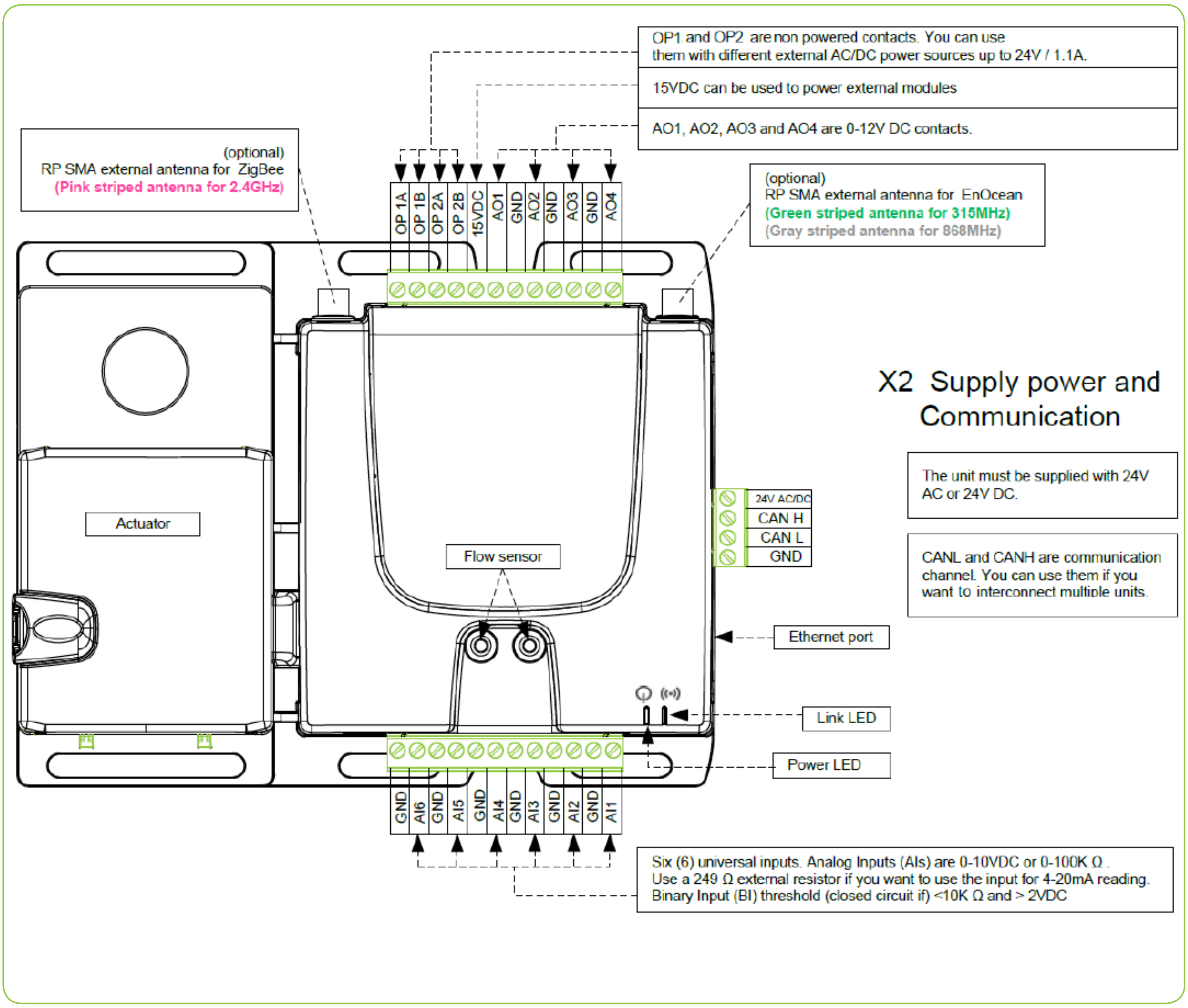
VAV Managers are fully programmable and are designed with VAV control in mind. In addition to all the features of the MPM, The VAV Manager has a pressure sensor and a damper actuator for direct control of VAV boxes.

VAV Managers can be used to control a wide range of wired and wireless (EnOcean and ZigBee-compatible) end-devices, including light sensors, light switches, relays, thermostats, card readers, and magnetic door contacts. The devices are targeted primarily for commercial, industrial, and institutional buildings.

Pinout Diagram

The below figure shows the pinout information for the MPM - VA VAV.

NOTE: You must remove the pink cap from the MPM before you install the pink-striped ZigBee antenna.



OP1 and OP2 are non powered contacts. You can use them with different external AC/DC power sources up to 24V / 1.1A.

15VDC can be used to power external modules

AO1, AO2, AO3 and AO4 are 0-12V DC contacts.

(optional)
RP SMA external antenna for ZigBee
(Pink striped antenna for 2.4GHz)

(optional)
RP SMA external antenna for EnOcean
(Green striped antenna for 315MHz)
(Gray striped antenna for 868MHz)

X2 Supply power and Communication

The unit must be supplied with 24V AC or 24V DC.

CANL and CANH are communication channel. You can use them if you want to interconnect multiple units.

Six (6) universal inputs. Analog Inputs (AIs) are 0-10VDC or 0-100K Ω .
Use a 249 Ω external resistor if you want to use the input for 4-20mA reading.
Binary Input (BI) threshold (closed circuit if) <10K Ω and > 2VDC

MPM-GW Wireless Manager

The MPM-GW wireless Manager is an electronic device designed to integrate wireless solutions to wired building automation systems. Small buildings system gateways can integrate wireless end-devices, based on EnOcean and ZigBee protocols and standards, into BACnet building automation systems. They are all interoperable with any BACnet compliant building management system.

The MPM-GW is a printed circuit board housed in a plastic shell casing. Unlike the MPN-UN and MPM-VA, there are no physical (wired) I/Os on this manager.

The following connectors are concealed in a casing, giving the device a neutral look for installation in institutional or commercial environments:

- LAN
- CANbus
- Power supply

The MPM-GWs have optional embedded EnOcean and ZigBee wireless modules to enable bidirectional communication with EnOcean and ZigBee devices. The Managers can also communicate with each other wirelessly using their ZigBee modules.

Uses

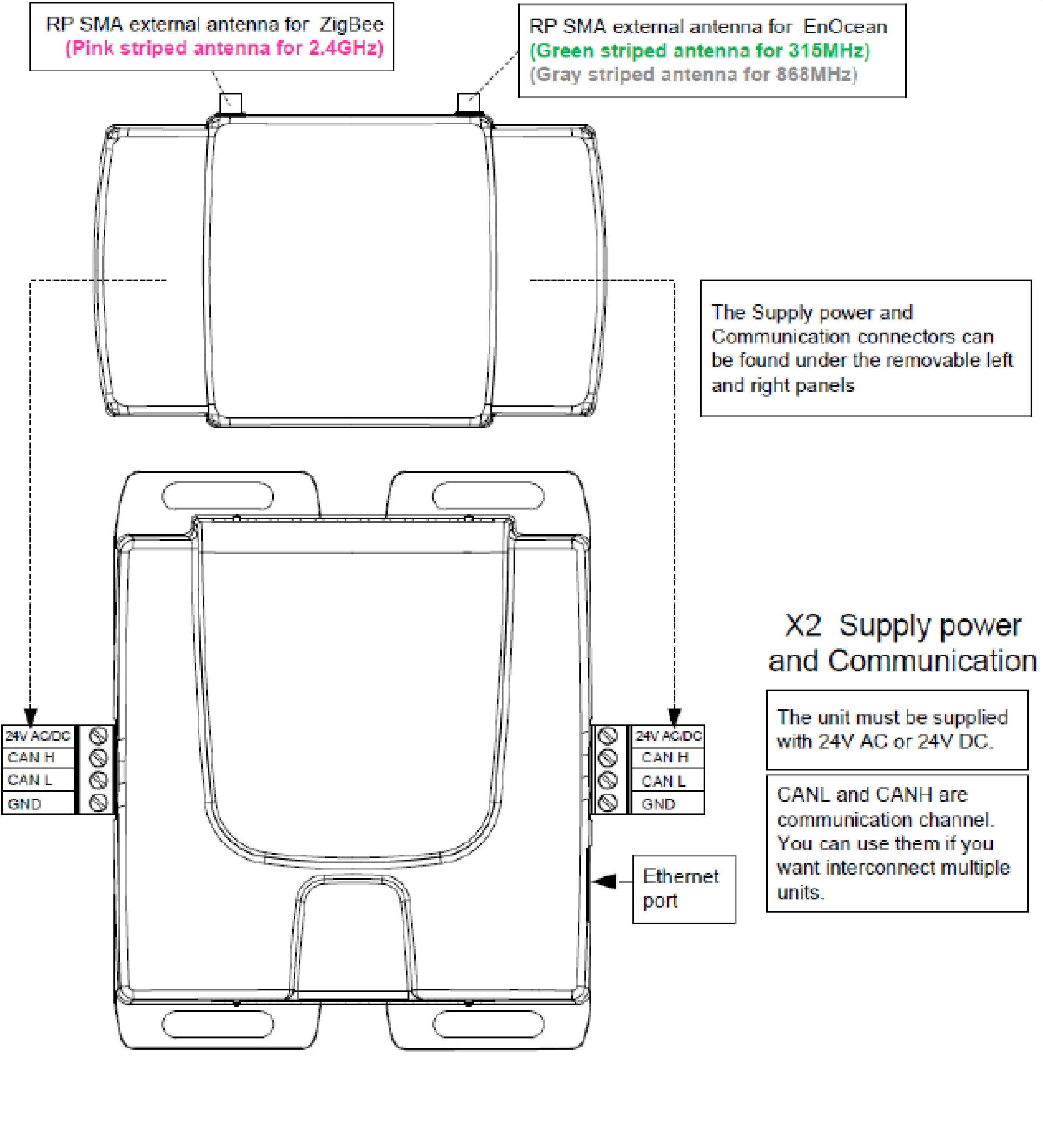
MPM-GWs are fully programmable and are designed with wireless lighting and HVAC applications in mind. They can also control wired end-devices and compatible wireless EnOcean and ZigBee end-devices. Wireless end-devices including light sensors, light switches, relays, thermostats, card readers, and magnetic door contacts.

MPM-GWs are targeted for installation in commercial, industrial, and institutional buildings.

Pinout Diagram

The below figure shows the pinout information for the MPM - GW.

NOTE: You must remove the pink cap from the MPM before you install the pink-striped ZigBee antenna.



RP SMA external antenna for ZigBee (Pink striped antenna for 2.4GHz)

RP SMA external antenna for EnOcean (Green striped antenna for 315MHz) (Gray striped antenna for 868MHz)

The Supply power and Communication connectors can be found under the removable left and right panels

X2 Supply power and Communication

The unit must be supplied with 24V AC or 24V DC.

CANL and CANH are communication channel. You can use them if you want interconnect multiple units.

Installation

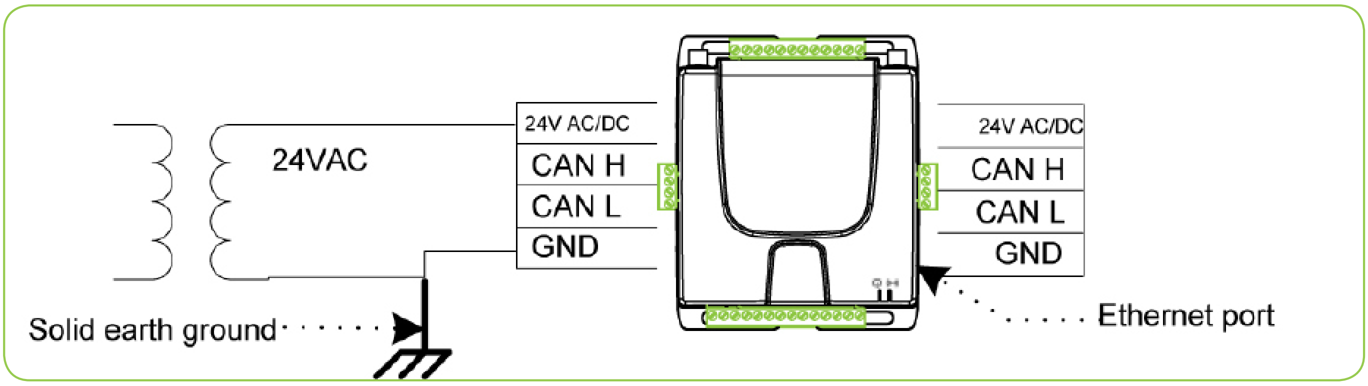
This sections explains how to install and power up your Manager(s).

Required Tools and Equipment

- One flat-blade screwdriver (3mm/1/8" wide or smaller)
- One straight-through Ethernet cable (RJ-45)
- Computer (PC, Mac, or Linux) with the Firefox browser (version 17 or later)
- Optional: Ethernet switch or hub if you want to connect your Manager to your local network.

Procedure - Powering Up Your Manager

The figure below shows the power connectors for your MPM-UN, MPM-VA, and MPM-GW managers.



1. Using flat-head screwdriver, connect positive wire to 24V AC/DC pin on Manager
2. Connect second wire to GND pin on Manager.
3. Plug power supply into outlet after fastening wires.
4. The green LED on the MPM-UN/MPM-VA or the RJ-45 connector's LED on the MPM-GW's go on, indicating the unit is powered.

Networking

You can connect your Manager(s) directly to your computer or to your local area network (LAN).

IMPORTANT: Multipurpose Managers (MPMs) should not be connected directly to the Internet or any public network. The SmartStruxure™ Lite Managers can make any lighting or HVAC site remotely accessible through the internet, but they do not offer any intrinsic security options such as authentication, encryption, packet inspection or filtering. However, many third-party devices and software can make these features available to a SmartStruxure™ Manager. These solutions provide a safe authentication mechanism and configurable encryption options to properly secure one or multiple remote sites. Regardless of the type of connection you intend to use for your network, you must connect your MPM directly to your computer for its initial set-up.

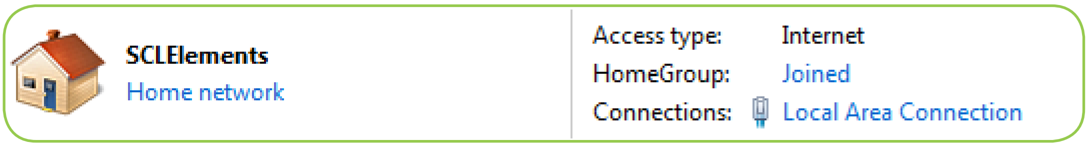
Refer to Appendix for more details.

Procedure - Configuring Your PC to Communicate Directly with Manager

You must configure the network card you connect to your Manager directly to your computer.

Note: The following example shows the procedure for Windows operating systems. For Mac or Linux, use the platform-specific commands or applications.

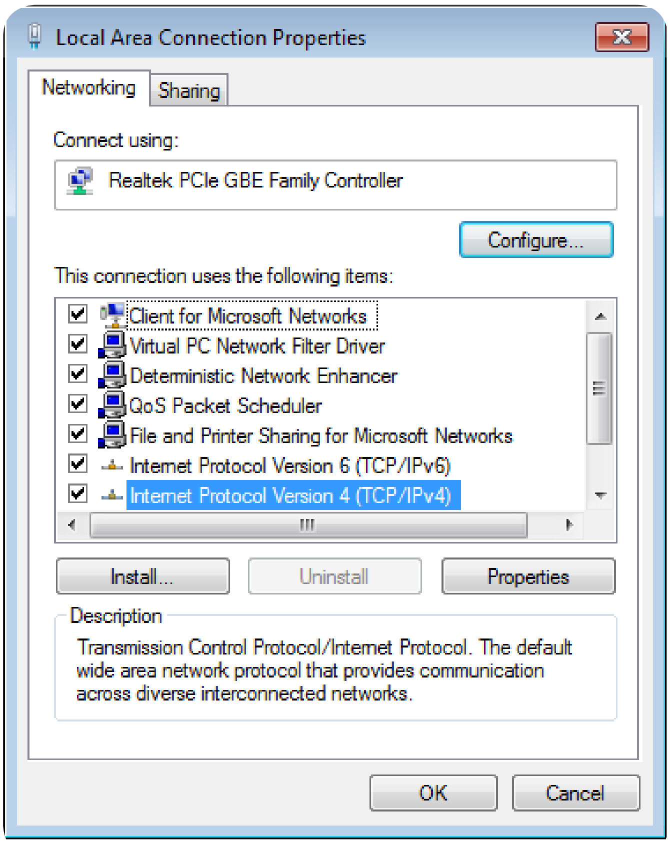
1. In **Control Panel**, open **Network Connections (Windows XP) or Network and Sharing Center (Windows 7)**.
2. Click **Local Area connection** and choose **Properties**.



SCLElements
Home network

Access type: Internet
HomeGroup: Joined
Connections: Local Area Connection

3. Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



Local Area Connection Properties

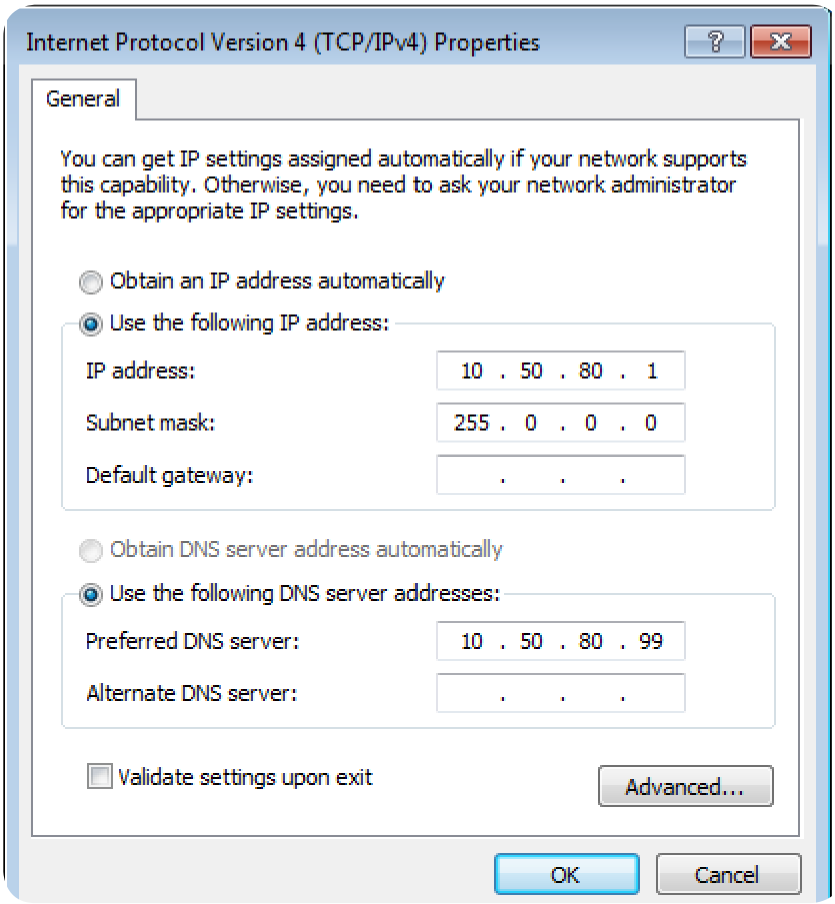
Connect using:
Realtek PCIe GBE Family Controller

This connection uses the following items:

☑ Client for Microsoft Networks
☑ Virtual PC Network Filter Driver
☑ Deterministic Network Enhancer
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

4. Enter properties as shown below.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 50 . 80 . 1

Subnet mask: 255 . 0 . 0 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 10 . 50 . 80 . 99

Alternate DNS server: . . .

□ Validate settings upon exit

Connecting to Your Local Area Network

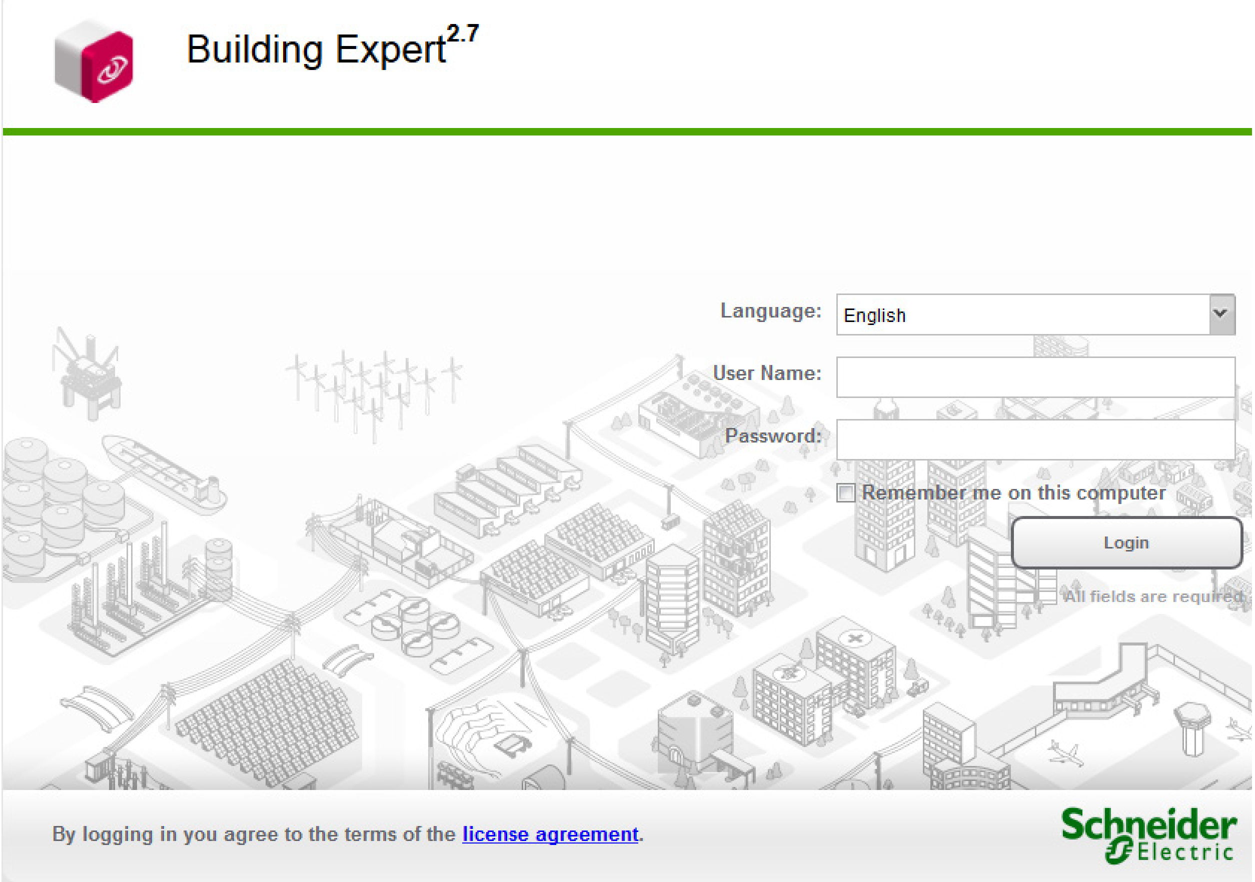
IMPORTANT! Check with your administrator to grant you access to network parameters if you want to connect the Manager to your local network.

By default, all Managers are configured with the same default IP address; 10.50.80.3 (10.50.80.4 for the MPM-VA). Since the same IP address cannot be used twice on a single subnet without creating a conflict, you must configure the Manager's Ethernet settings before you connect them together.

The IP addresses must be unique. Write down the IP addresses to avoid any confusion between managers.

Procedure - Login to Building Expert

To change the Ethernet configuration, open Firefox and navigate to Manager's IP address (http://10.50.80.3/ or http://10.50.80.4). The Building Expert web interface login screen shows.



Building Expert$^{2.7}$

Language: English

User Name:

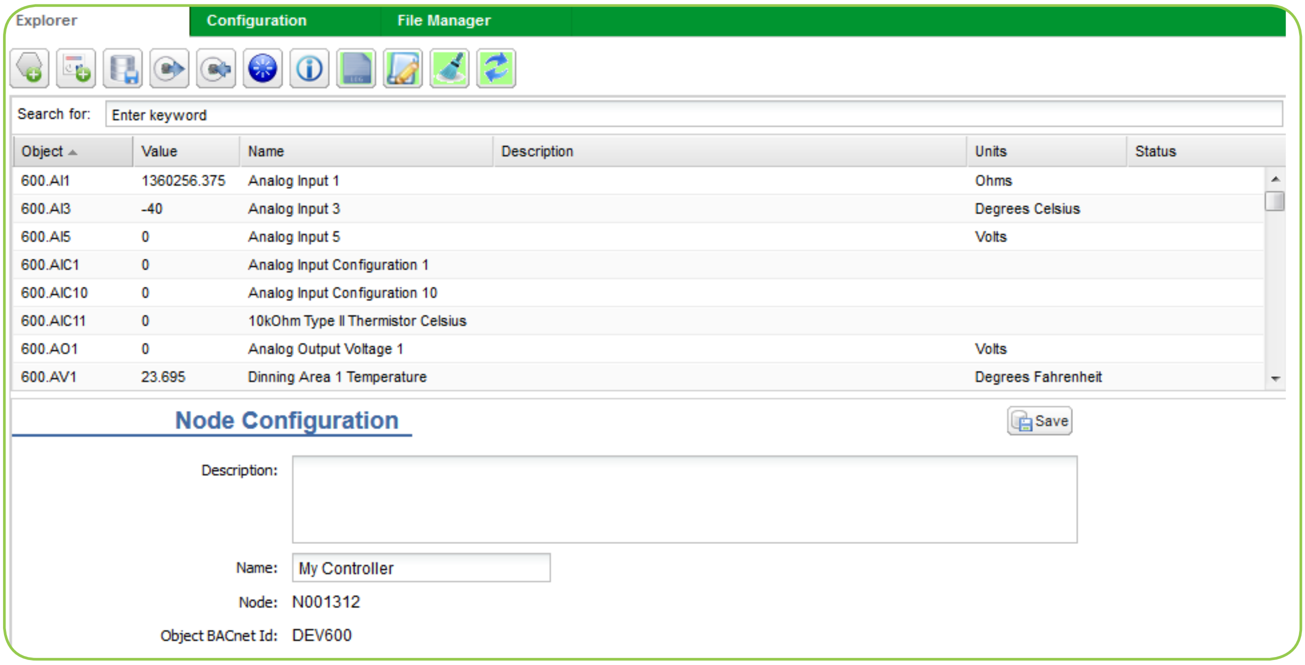
Password:

□ Remember me on this computer

All fields are required

By logging in you agree to the terms of the license agreement.

1. Select **Language** (default language is English).
2. Enter **User Name** (default user name is admin).
3. Enter **Password** (default password is admin).
4. Push **Login** button.
   The Building Expert page shows with Explorer tab selected (see next page).



Search for: Enter keyword

Object	Value	Name	Description	Units	Status
600.AI1	1360256.375	Analog Input 1		Ohms	
600.AI3	-40	Analog Input 3		Degrees Celsius	
600.AI5	0	Analog Input 5		Volts	
600.AIC1	0	Analog Input Configuration 1			
600.AIC10	0	Analog Input Configuration 10			
600.AIC11	0	10kOhm Type II Thermistor Celsius			
600.AO1	0	Analog Output Voltage 1		Volts	
600.AV1	23.695	Dinning Area 1 Temperature		Degrees Fahrenheit	

Node Configuration

Description:

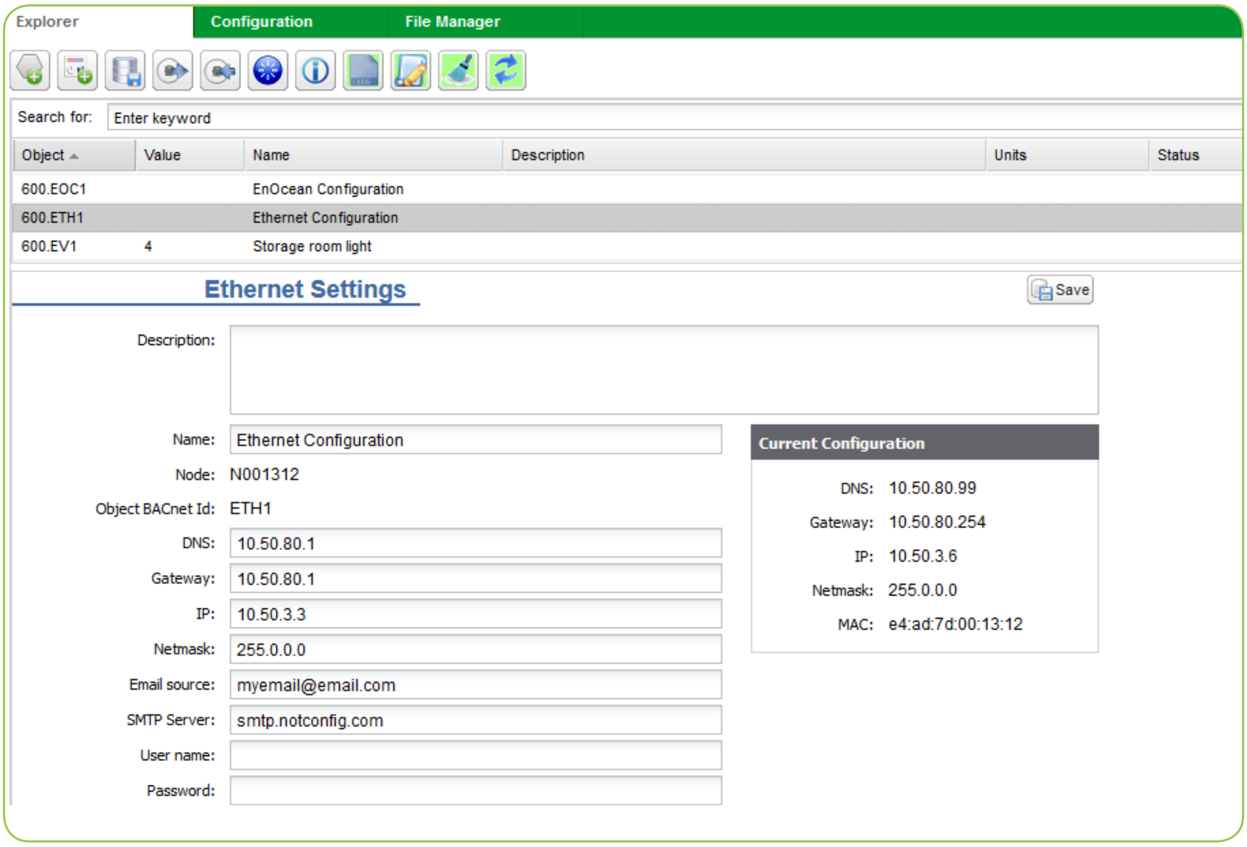
Name: My Controller

Node: N001312

Object BACnet Id: DEV600

Procedure - Configuring Building Expert

1. In **Explorer** tab, select **Ethernet Configuration (ETH1)**.
   Ethernet Settings parameters shows.



Search for: Enter keyword

Object	Value	Name	Description	Units	Status
600.EOC1		EnOcean Configuration			
600.ETH1		Ethernet Configuration			
600.EV1	4	Storage room light			

Ethernet Settings

Description:

Name: Ethernet Configuration

Node: N001312

Object BACnet Id: ETH1

DNS: 10.50.80.1

Gateway: 10.50.80.1

IP: 10.50.3.3

Netmask: 255.0.0.0

Email source: myemail@email.com

SMTP Server: smtp.notconfig.com

User name:

Password:

Current Configuration

DNS: 10.50.80.99

Gateway: 10.50.80.254

IP: 10.50.3.6

Netmask: 255.0.0.0

MAC: e4:ad:7d:00:13:12

2. Configure your settings as follows:

- **DNS:** domain name server is only required when accessing devices by hostname rather than by numerical IP addresses. Complete this optional field if, for example, you want to use the email feature or access SNTP servers using hostname.
- **Gateway:** local network default gateway is only required if another network, such as internet, must be connected to the device. This is typically your local router IP address. Complete this optional field if, for example, you want to use the email feature or access SNTP servers.
- **IP:** IP address of the Manager. It must be unique on the local network. If a gateway is specified, both should be part of the same subnet.
- **Netmask:** local network mask defining the subnet. When accessing IP addresses outside this mask, the requests are routed through the local gateway.
- **Email source:** e-mail account used to send e-mails using your Manager (optional).
- **SMTP server:** SMTP server used to send e-mails using your Manager (optional).

Once Ethernet settings have been modified, press the **Save** button. The IP address is modified and the connection with the Manager is lost. You must enter the new IP address in the Firefox address bar and press **Enter** to access the controller at its new address.

Once you have logged back on to your controller, save the database to ensure your changes stay after a controller reboot.

You can create a network of MPM devices using the following 3 inter-manager communication protocols:

- ZigBee
- CANbus
- UDP

What is ZigBee?

ZigBee is a high-level wireless communication protocol operating in the worldwide 2.4GHz radio band. Its digital radio uses the IEEE 802.15.4 standard for low-rate wireless Personal Area Networks (PANs).

The main advantage of ZigBee is its ability to provide mesh networking. ZigBee mesh networks are multipoint to multipoint and self-healing, which means the network still operates when one node breaks down, or if there is a poor connection. As a result, the network is very reliable because there is often more than one path between a source and a destination in the network.

What is CANbus?

Controller–area Network (CAN or CAN-bus) is a wired bus standard designed to allow microcontrollers and devices to communicate with each other within a vehicle without a host computer. Originally designed for the automotive industry, CANbus has now spread out to industrial and building automation and medical equipment.

CANbus provides the following advantages:

- Multi-master hierarchy to allow building intelligent and redundant systems. If one node is defective the network still operates.
- Broadcast communication where a sender of information transmits to all devices on the bus. All receiving devices read the message and decide if it is relevant to them. This guarantees data integrity as all devices in the system use the same information.
- Sophisticated error detecting mechanisms and re-transmission of faulty messages. This also guarantees data integrity.

SmartStruxure Lite Managers use CANbus as one of the multiple ways to communicate with each other. By using CANbus ports, SmartStruxure Lite Managers can be chained-linked together, effectively creating a network. CANbus can also be used to chain link two or more Managers using Shielded Twisted Pair (STP) cable.

What is UDP?

User Datagram Protocol (UDP) is a communications protocol used for communication between Managers on an IP/Ethernet network. You enable/disable and configure these protocols via the Manager's Network Configuration (C2G1) object on the Building Expert web interface.

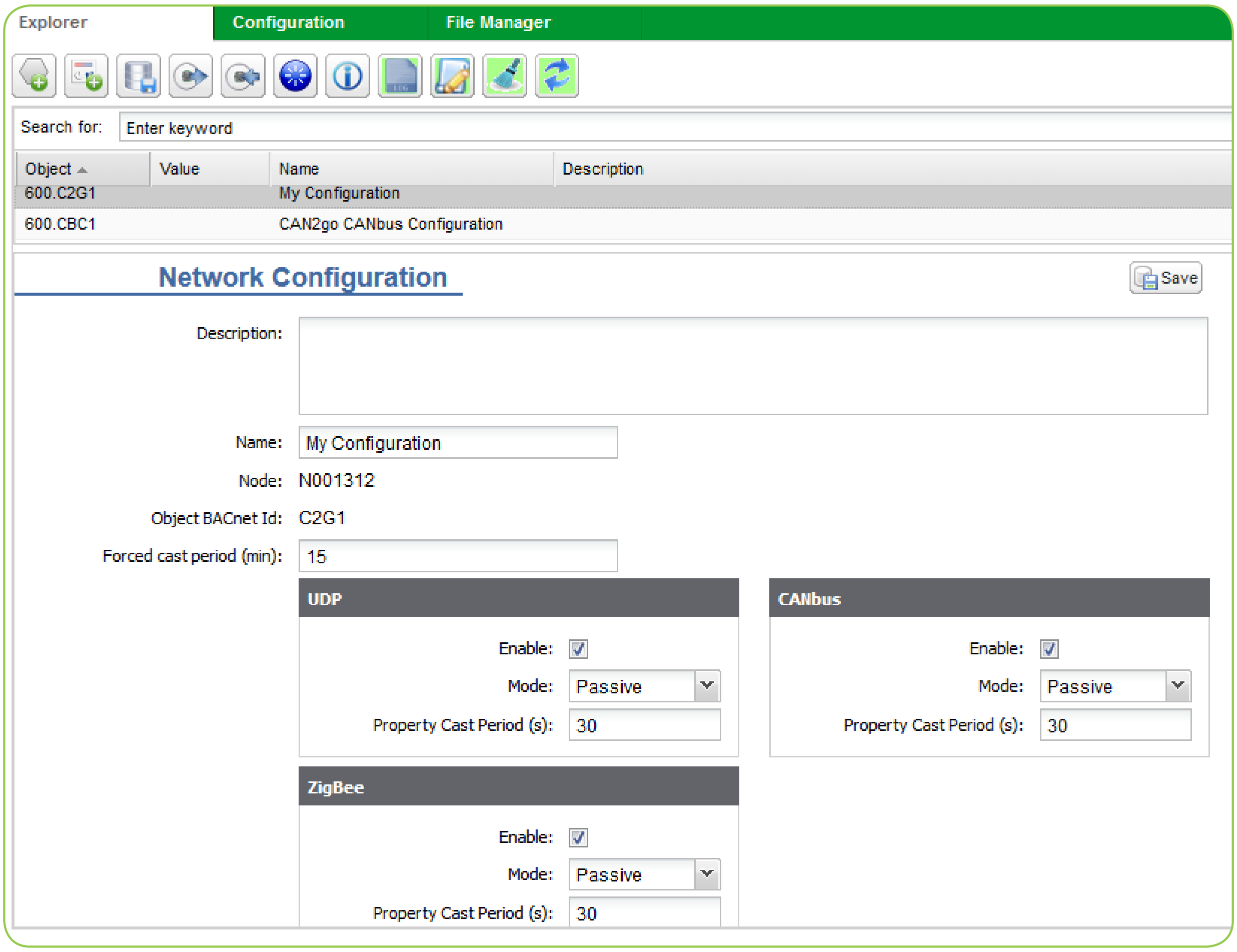
MPM Network Roles

Each Manager can be separately configured as a **Monitor** or a **Passive Node**.

- **Monitor:** stores information from all Managers active on its network. Ideally, only one Manager should be monitored over a given network type since each monitor uses a lot of bandwidth. The monitor node should be the Manager connected to your LAN via its Ethernet port to give you access to all information.
- **Passive Node:** casts its changed values to its monitor once every **Property Cast Period**. See "Property Cast Period" on page 17. In UDP, the passive Manager does not require a LAN connection.

Procedure - Specify Network Roles

You configure network roles for your MPM devices using the Network Configuration (C2G1) object.



Search for: Enter keyword

Object	Value	Name	Description
600.C2G1		My Configuration	
600.CBC1		CAN2go CANbus Configuration	

Network Configuration

Description:

Name: My Configuration

Node: N001312

Object BACnet Id: C2G1

Forced cast period (min): 15

UDP

Enable: ☑

Mode: Passive

Property Cast Period (s): 30

CANbus

Enable: ☑

Mode: Passive

Property Cast Period (s): 30

ZigBee

Enable: ☑

Mode: Passive

Property Cast Period (s): 30

1. In **Devices** tab, click on your Manager.
2. In **Object** tab, click **C2G1.**

The C2G1 object specifies the way the Manager communicates with its peers whenever using the inter-manager communication protocols (UDP, CANbus, and ZigBee).

For each of the 3 protocols, you can enable or disable functionality, and specify its operating mode and property cast period.

Note: All 3 protocols are enabled by default. Disable or enable the protocols as required for your network.

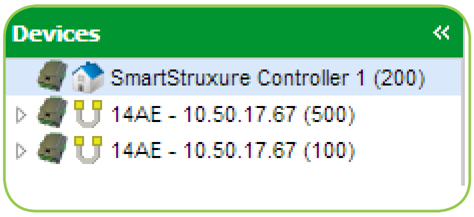
Property Cast Period

The Property Cast Period defines the interval (or frequency) with which a passive node casts information to a monitor. The cast comprises all changed values detected by the passive node since the last request from the monitor.

Notes: By default, a passive node casts its values to a monitor once every minute. You should not set this interval to a value of less than 30 seconds.

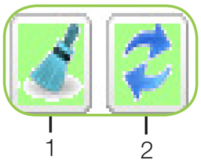
Creating a Network on the Monitor

Once all the Managers have been configured and properly connected, you must create the image of the network on the monitor. When looking at a MPM network through the monitor, you are looking at an image being refreshed periodically by the casting of changed values from the passive devices to the monitor.



The monitor is presented on the network tree next to the “house” icon.

The passive devices on the network are presented next to an icon representing the protocol used for communication. Clicking on any Manager calls up the list of objects in Building Expert.



Clicking the **Clean** button (1) erases the local copy of the network information and reboots the monitor Manager. This does not affect the information residing on passive managers.

To initiate discovery of all information from all passive managers on the network, click on the **Scan for new nodes added to the network** (2). During discovery, the icon activates and assumes this shape before returning to its original state when discovery is complete.

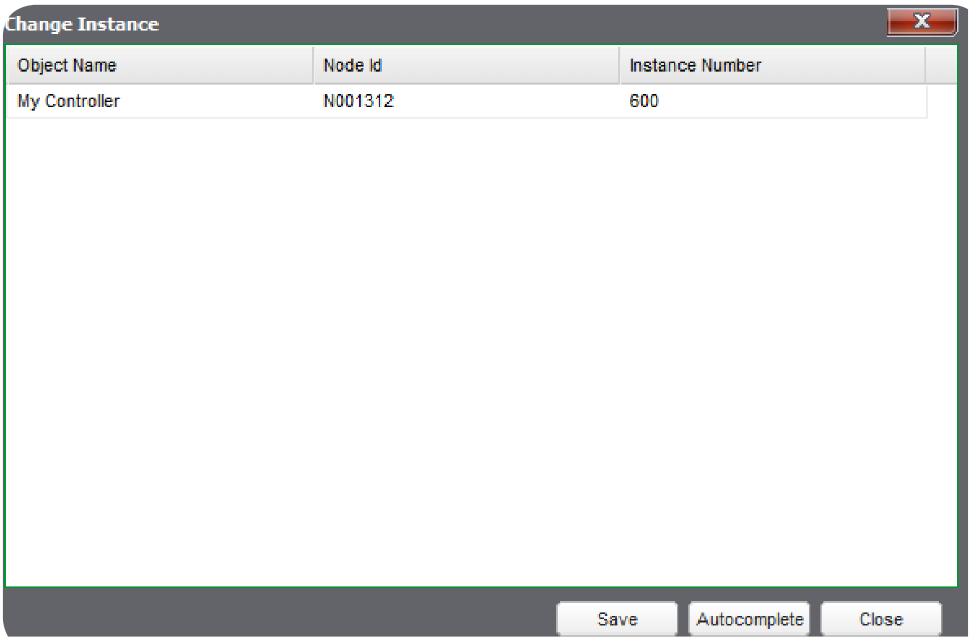
Identifying Devices on the Network

Managers on the network are identified by 2 distinct numbers:

- **Node number:** fixed (uneditable) and unique number assigned to each Manager by the SmartStruxure Lite internal protocol.
- **Device number:** editable identifier that must be unique within the context of the extended network. The device number is used for integration with BACnet and SmartStruxure. See “Changing a Device Number” on page 18.

Procedure - Changing a Device Number

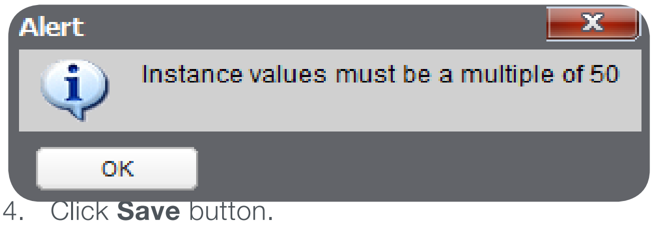
IMPORTANT: To change the device number of a Manager, you must be connected directly to the Manager. You cannot change a device number over the network.



Object Name	Node Id	Instance Number
My Controller	N001312	600

1. In **Devices** tab, click on your Manager.
2. From toolbar, select **Change any node instance number** icon.
   The **Change Instance** dialog shows.
3. Click in **Instance Number** field and type in a new instance number for Manager.
   The new instance number must conform to the following rules:

- It must be greater than or equal to 50.
- It must be less than or equal to 3999950.
- It must be a multiple of 50 (50, 100, 150, etc), otherwise the following error shows:



Instance values must be a multiple of 50

4. Click **Save** button.

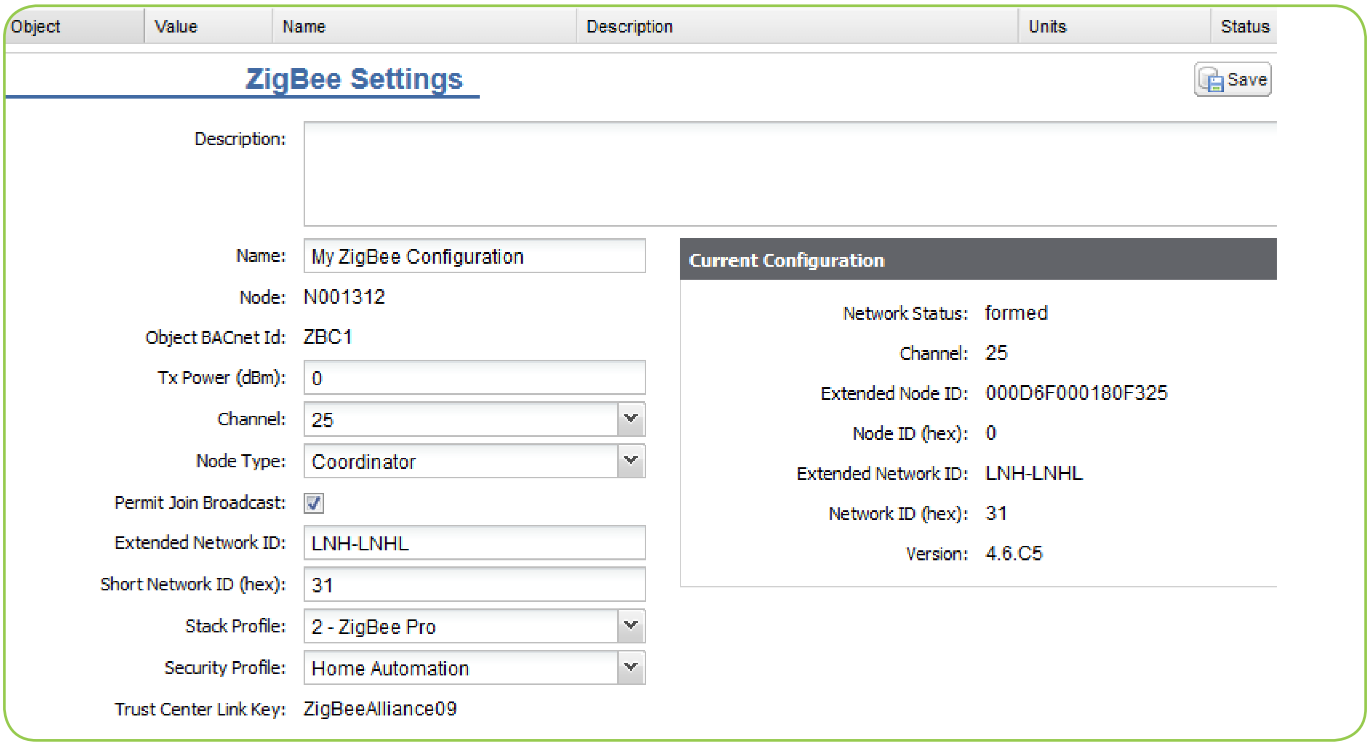
NOTE: The new instance number(s) may take time to propagate across the network. You may have to restart Building Expert to see your changes.

Setting up Managers in a ZigBee Network

Each MPM can be configured independently through ZigBee Settings (ZBC1) configuration object.

All settings should be configured when you are connected directly to the Manager.

IMPORTANT: Do not change **ZBC1** parameters on a remote Manager as you will lose communication with the Manager. Ensure **Coordinator** is selected for **Node Type.**



ZigBee Settings

Description:	
Name:	My ZigBee Configuration
Node:	N001312
Object BACnet Id:	ZBC1
Tx Power (dBm):	0
Channel:	25
Node Type:	Coordinator
Permit Join Broadcast:	☑
Extended Network ID:	LNH-LNHL
Short Network ID (hex):	31
Stack Profile:	2 - ZigBee Pro
Security Profile:	Home Automation
Trust Center Link Key:	ZigBeeAlliance09

Current Configuration

Network Status:	formed
Channel:	25
Extended Node ID:	000D6F000180F325
Node ID (hex):	0
Extended Network ID:	LNH-LNHL
Network ID (hex):	31
Version:	4.6.C5

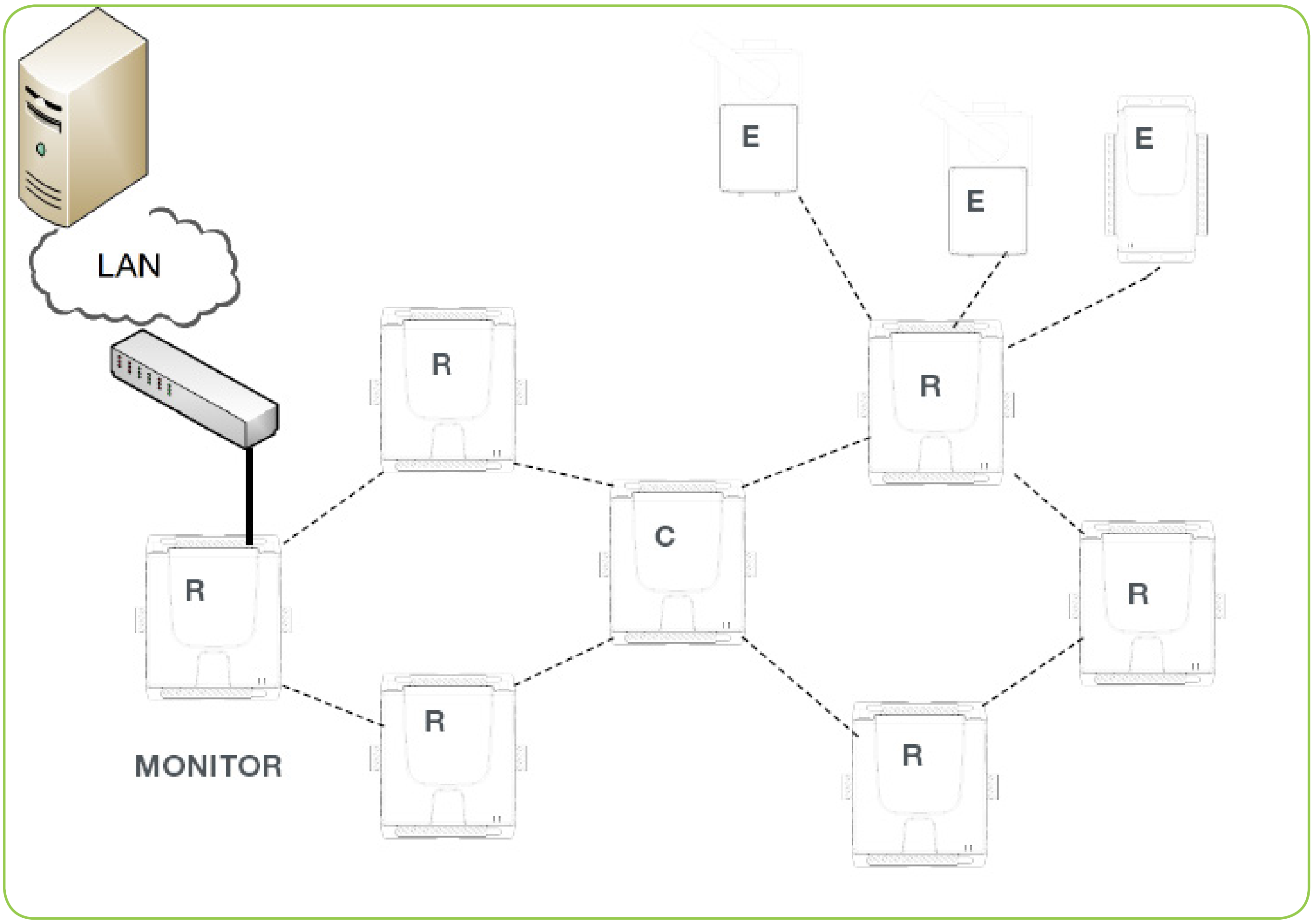
ZigBee Roles

In a ZigBee network, three types of devices are available:

1. **ZigBee Coordinator:** heart of the network. There can be only one coordinator per network. Its role is to act as a trust center to allow and approve all routers and end devices attempting to join its network.
2. **ZigBee Router:** link in the network. This route packets between other nodes, providing extended network range through a maximum of 30 hops. A router device is always set to 'On' to provide routes for other devices. It also acts as a parent for end devices.
3. **ZigBee End Device:** only has the functionality to achieve a specific task and communicate with a parent node, either the coordinator or a router. Examples of end devices are SEC-TE smart terminal controller and a SED-0 smart wireless actuator.

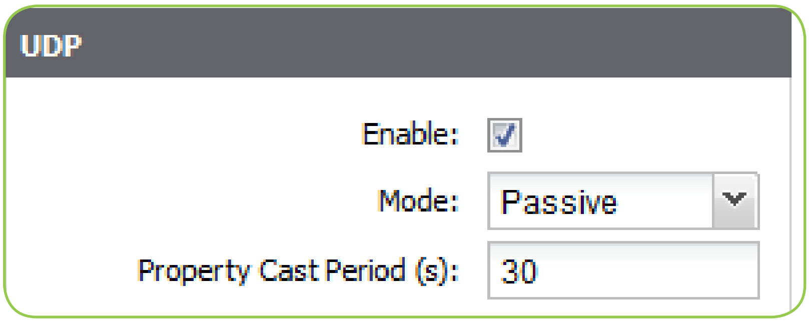
The figure and table below show an example of network architecture for MPMs communicating over ZigBee.

LEGEND
C = Coordinator
R = Router
E = End device



Procedure - UDP Settings

1. In **Devices** tab, select your Manager.
2. From **Object** panel, select **C2G1** object.
3. In **UDP** box, ensure **Enable** is selected.



UDP

Enable: ☑

Mode: Passive

Property Cast Period (s): 30

4. Click **Save** button.
5. From **Object** panel, select **Ethernet Communication (ETH1)** object.
6. In **IP** field, enter IP address for your Manager.
7. Click **Save** button.
8. Repeat steps 1 - 7 for all Managers on your UDP network. Ensure they are part of the same subnet and are assigned unique IP addresses.

Network Guidelines

The table below provides the theoretical range between two controllers with a Zigbee radio.

ENVIRONMENT	RANGE
Open air/Line of sight	Up to 300m (1000 feet)
In Building/Line of sight	Up to 100m (300 feet)
In Building/Non line of sight (gypsum wall)	Up to 50m (150 feet

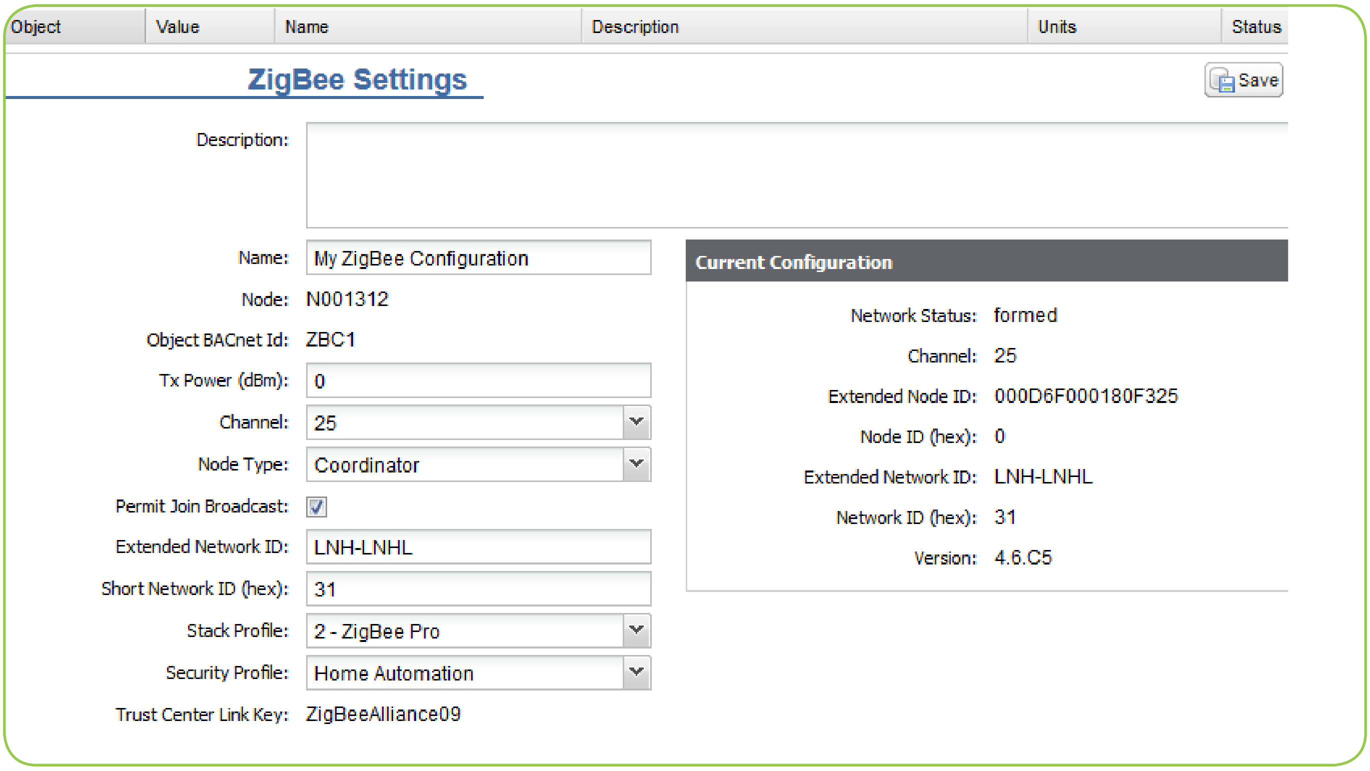
As a rule of thumb, you can estimate a dedicated ZigBee Manager can monitor up to 15 passive Managers performing typical control tasks (Air Handler/Fan Coil/VAV controls, Lighting controls, etc.).

Depending on your specific application, the monitor-to-router ratio may vary. Refer to https://documentation.smartstruxurelite.com for detailed deployment guidelines, or contact Small Business Systems customer support for a review of your application.

Procedure - Configuring ZigBee Settings

Form a ZigBee network among multiple Managers:

1. Enable ZigBee driver for each Manager on the network
2. In **Device** tab, click on your Manager.



ZigBee Settings

Description:

Name: My ZigBee Configuration
Node: N001312
Object BACnet Id: ZBC1
Tx Power (dBm): 0
Channel: 25
Node Type: Coordinator
Permit Join Broadcast: ☑
Extended Network ID: LNH-LNHL
Short Network ID (hex): 31
Stack Profile: 2 - ZigBee Pro
Security Profile: Home Automation
Trust Center Link Key: ZigBeeAlliance09

Current Configuration

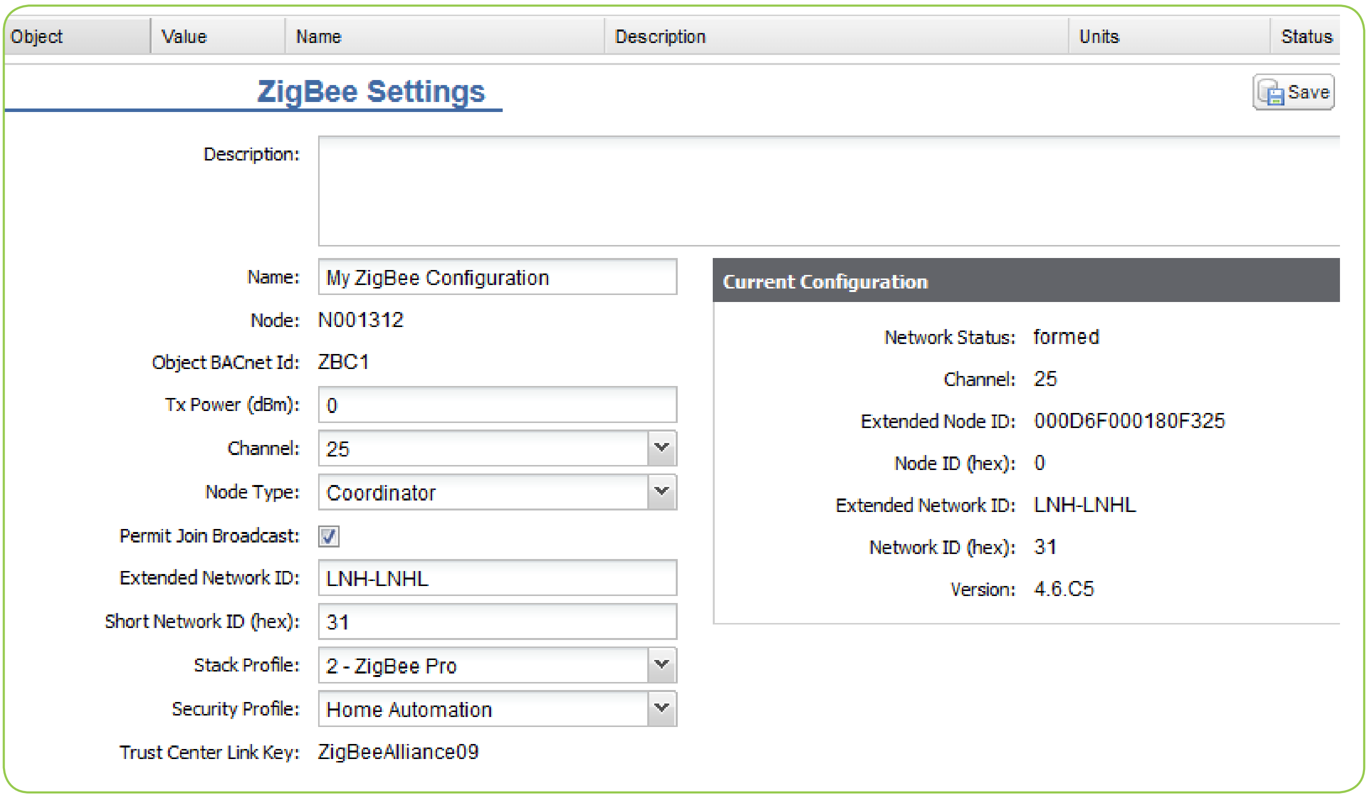
Network Status: formed
Channel: 25
Extended Node ID: 000D6F000180F325
Node ID (hex): 0
Extended Network ID: LNH-LNHL
Network ID (hex): 31
Version: 4.6.C5

3. From **Object** panel, select **Communication Configuration (C2G1)**.
4. Ensure ZigBee **Enable** check box is selected.
5. Configure **Mode** parameters as follows:

- For Manager connected to your LAN, set **Mode** to Monitor
- For all other Managers, set **Mode** to *Passive*.

Set ZigBee Configuration parameters to common values for each Manager on the network.

1. In **Devices** tab, click on your Manager.
2. In **Object** panel, select **ZigBee Configuration (ZBC1)**.
   ZigBee Settings shows.



ZigBee Settings

Description:	
Name:	My ZigBee Configuration
Node:	N001312
Object BACnet Id:	ZBC1
Tx Power (dBm):	0
Channel:	25
Node Type:	Coordinator
Permit Join Broadcast:	☑
Extended Network ID:	LNH-LNHL
Short Network ID (hex):	31
Stack Profile:	2 - ZigBee Pro
Security Profile:	Home Automation
Trust Center Link Key:	ZigBeeAlliance09

Current Configuration

Network Status:	formed
Channel:	25
Extended Node ID:	000D6F000180F325
Node ID (hex):	0
Extended Network ID:	LNH-LNHL
Network ID (hex):	31
Version:	4.6.C5

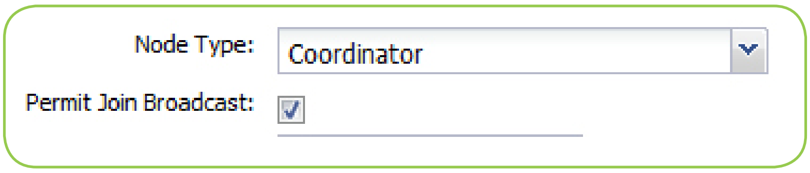
1. In **ZigBee Settings** window, configure parameters according to the table below.

PARAMETER	VALUE
Channel	Recommended values: • North America: 25, 26 • Europe : 15, 16, 21, 22 • Asia: 25, 26
Extended Network ID	8-character string. Default value is ZBC-CBAC
Short Network ID	4-digit Hexadecimal value. Default value is CBAC. **Note:** In firmware version 2.6.x and subsequent, you can enter Short network ID in decimal or Hexadecimal and conversion gets applied automatically.
Stack Profile	Select **Custom** or **ZigBee Pro**. See *Security Profile*.
Security Profile	Select **None** or **Home Automation.** **ZigBee Pro** Stack Profile must be selected to use Home Automation Security Profile. **Custom** Stack Profile is used when no Security Profile is selected.

2. Set **Node Type** of only one Manager to be a network coordinator. For ease of operation, it is recommended to use the network monitor as coordinator.
3. During commissioning of your Manager, leave **Permit Join** check box selected. “Permit Join” on page 24.

Permit Join

The Permit Join feature allows control of the Managers or Devices to join any ZigBee network.



Node Type: Coordinator

Permit Join Broadcast: ☑

The Permit Join feature is set only on the ZigBee Coordinator. As a result, the **Permit Join Broadcast** check box appears only if the **Node Type** selected is Coordinator.

When **Permit Join Broadcast** is activated (checked), a broadcast is sent periodically to all routers on the network letting them know it is possible to join the network.

Conversely, if **Permit Join Broadcast** is deactivated (unchecked), a broadcast gets sent periodically to prevent routers to let any device join the network.

This feature is useful for joining End Devices to a specific network when more than one ZigBee network is formed in a specific environment.

In normal operation, **Permit Join Broadcast** should be left unchecked on all coordinators, and checked only during commissioning or when adding a new Manager, Gateway, or End Device to the network.

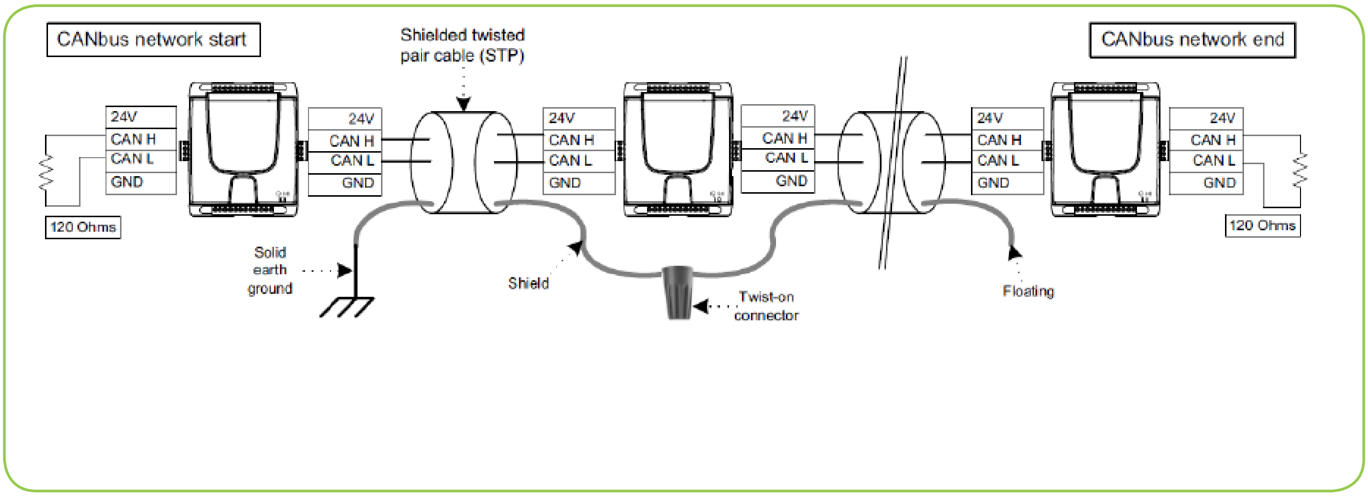
Setting up Managers in a CANbus Network

CANbus Roles

All Managers in a CANbus network have the same status.

Network Guidelines

The below figure describes how to chain-link three managers.



IMPORTANT: You must use shielded twisted pair cables as well as three-wire shielded cable. Always solid earth ground each Manager in the CANbus network!

Use the STP cabling to connect the + and – pins of the CANbus port of the Managers, and ground the shield of the STP cabling of the first Manager to the solid earth ground. Only the first Manager should have the shield grounded. The shield must be left floating at the other end. Never ground the shield of a network in more than one place along the network. If the shield is connected to two different ground potentials, the resulting current will induce noise into the CANbus network.

IMPORTANT: Star networks are not acceptable. CANbus networks must be linear.

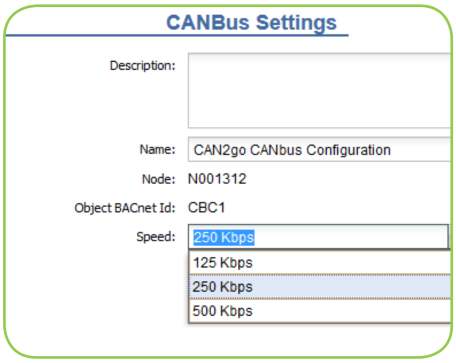
The CANbus ports of Managers operate by default at 250kbps and may be configured at 125 and 500kbps.

CANbus transfer rate is proportional to total chain-link length:

- 125Kbps: Up to 500m (1500 feet)
- 250kbps: Up to 250m (750 feet)
- 500kbps: Up to 100m (300 feet)

Changing the CANbus speed is not applied immediately. When changing the CANbus bitrate, save the Manager DB and then reset the Manager.

As a rule of thumb, you can estimate that a dedicated CANbus Manager can monitor up to 15 passive Managers performing typical control tasks such as Air Handler/Fan Coil/ VAV controls and Lighting controls.



CANBus Settings

Description:

Name: CAN2go CANbus Configuration

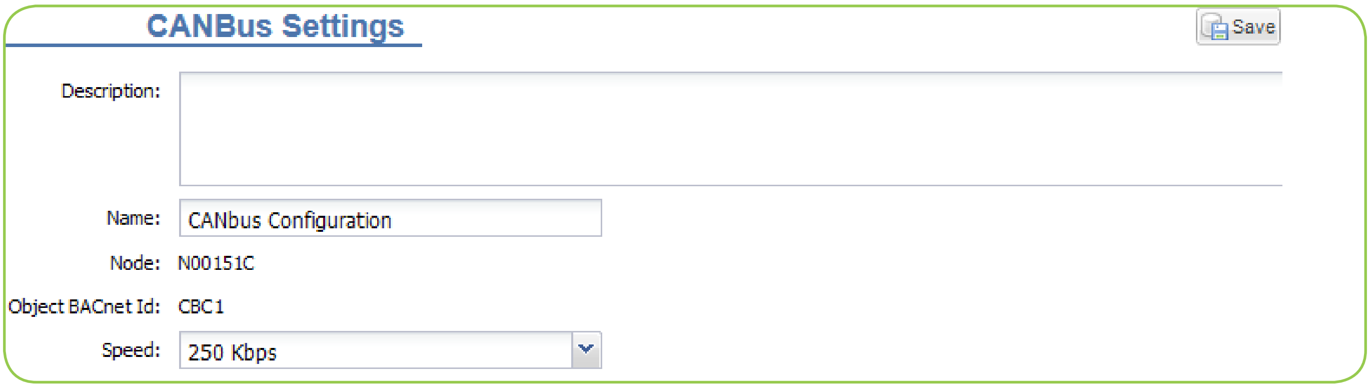
Node: N001312

Object BACnet Id: CBC1

Speed: 250 Kbps

CANbus Settings

CANbus settings are accessible via CANbus Configuration (CBC1) object.



CANBus Settings

Description:

Name: CANbus Configuration

Node: N00151C

Object BACnet Id: CBC1

Speed: 250 Kbps

NOTE: The CANbus speed of all Managers on a network must be the same to enable network communication.

Setting up Managers in a UDP Network

UDP Roles

There are no roles specific to a UDP network.

Network Guidelines

In a UDP network, all Managers must be connected to the same LAN, and their individual IP addresses must share the same subnet.

As a rule of thumb, you can estimate a dedicated UDP Manager can monitor up to 15 passive Managers performing typical control tasks such as Air Handler/Fan Coil/VAV controls and Lighting controls.

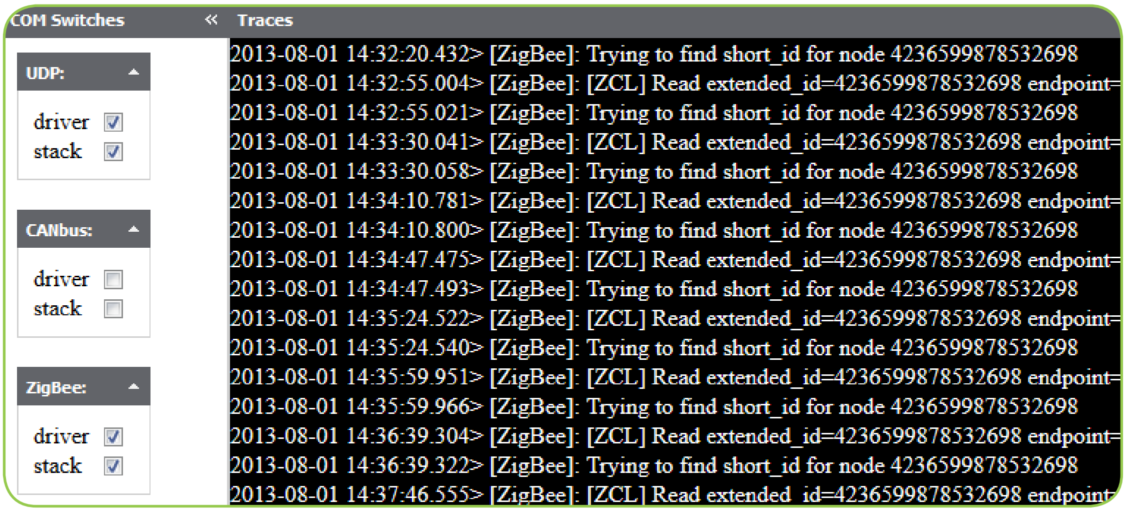
Refer to “UDP Settings” on page 21 to set-up your UDP Settings.

Visualizing Inter-manager Network Communication

From the monitor of a network, you can visualize the communication on a network. This is used to confirm a passive node is communicating properly, or verify a new passive node joined the network.

Procedure - Verify Network Communication

1. In **Devices** tab, right-click your Manager and choose **Show Com Log**.
2. Check **drive** and **stack** boxes for protocol of your network.
   The figure below shows.



UDP:
driver ☑
stack ☑

CANbus:
driver □
stack □

ZigBee:
driver ☑
stack ☑

```
2013-08-01 14:32:20.432> [ZigBee]: Trying to find short_id for node 4236599878532698
2013-08-01 14:32:55.004> [ZigBee]: [ZCL] Read extended_id=4236599878532698 endpoint=
2013-08-01 14:32:55.021> [ZigBee]: Trying to find short_id for node 4236599878532698
2013-08-01 14:33:30.041> [ZigBee]: [ZCL] Read extended_id=4236599878532698 endpoint=
2013-08-01 14:33:30.058> [ZigBee]: Trying to find short_id for node 4236599878532698
2013-08-01 14:34:10.781> [ZigBee]: [ZCL] Read extended_id=4236599878532698 endpoint=
2013-08-01 14:34:10.800> [ZigBee]: Trying to find short_id for node 4236599878532698
2013-08-01 14:34:47.475> [ZigBee]: [ZCL] Read extended_id=4236599878532698 endpoint=
2013-08-01 14:34:47.493> [ZigBee]: Trying to find short_id for node 4236599878532698
2013-08-01 14:35:24.522> [ZigBee]: [ZCL] Read extended_id=4236599878532698 endpoint=
2013-08-01 14:35:24.540> [ZigBee]: Trying to find short_id for node 4236599878532698
2013-08-01 14:35:59.951> [ZigBee]: [ZCL] Read extended_id=4236599878532698 endpoint=
2013-08-01 14:35:59.966> [ZigBee]: Trying to find short_id for node 4236599878532698
2013-08-01 14:36:39.304> [ZigBee]: [ZCL] Read extended_id=4236599878532698 endpoint=
2013-08-01 14:36:39.322> [ZigBee]: Trying to find short_id for node 4236599878532698
2013-08-01 14:37:46.555> [ZigBee]: [ZCL] Read extended_id=4236599878532698 endpoint
```

3. Press **Scan for new nodes added to the network** to initiate communication if you do not see communication on network.
4. After visualization is completed, uncheck **drive** and **stack** boxes.

Adding Languages to Building Expert

Building Expert can operate in several languages. To change the GUI langauge, you must import a language.json file and a baswi.po file to your Manager.

The following describes a language definition:

```
{  “ISO 639-1 language code”: {
        “label”:”displayed string in the language selector box”
        “translations”:”/root/data/<language.po file>” }
}
```

You must be logged in to your Manager before you can load any language.

.JSON File

The “language.json” file specifies additional languages to be loaded to the Manager. The language.json file is an open standard format using human-readable text to transmit data objects consisting of key:value pairs. The language.json file can be created in a text editor, however, you must use the following syntax to load any language:

```
{
   “your language”: {
      “label”: “your language”,
      “translations”: “/root/data/baswi-your language.po”
   }
}
```

.PO File

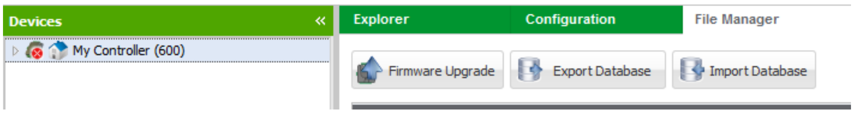
The .po file is a text-based object file referenced by other software programs as a properties file. The file must be saved in the Manager in a human-readable format that can be viewed in Building Expert. You must save the .po file as baswi-yourlanguage.po

Procedure - Add Language

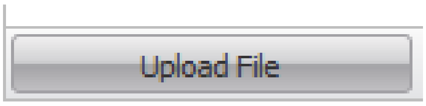
1. In text editor, open languages.json file.
2. Edit languages according to the following:

```
  {
"your language": {
   "label": "your language",
   "translations": "/root/data/baswi-your language.po"
      }
  }
```

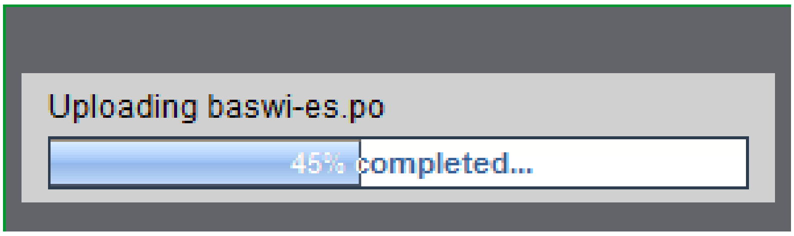
3. Save and close languages.json file.
4. Login to your Manager
5. In **Building Expert**, click on **File Manager** tab.



6. On bottom of **File Manager** tab, click **Upload** button. A new window opens.
7. Navigate to correct languages.json file and select it. **Building Expert** automatically uploads the languages.json file.
8. On bottom of **File Manager** tab, click **Upload** button. A new window opens.



9. Navigate to correct baswi-yourlanguage.po file and select it.
10. Click **Upload** button. Initialization window shows.



Uploading baswi-es.po

45% completed...

11. Reboot **Building Expert.** The uploaded language shows as an option in **Language** menu.
12. Login to **Building Expert**.

Procedure - Switch Language

1. Logout of existing **Building Expert** session.
2. In **Language** menu of **Building Expert** login page, select language you want.
3. Login to **Building Expert.**

Appendix

Securing remote sites

Overview

Building Expert firmware 2.14, and upcoming versions, include Digest Authentication. This provides the Multipurpose Managers (MPM) a higher level of security. However, in spite of the Digest Authentication implementation, the MPM must NOT be connected directly to the Internet or any public network unless it is properly secured on one or multiple remote sites. Refer to application note Securing Remote Sites for more details as this applies to Firmware earlier than 2.14.0.

Note: MPMs should not be connected directly to the Internet or any public network. Also, simply opening a port in a typical home router configuration is not a secure configuration.

Option 1 - Commercial Grade SSL and VPN Routers

Most router manufacturers (Linksys/Cisco, D-Link, Netgear, etc.) provide SSL/TLS solutions or even VPN-enabled secure routers that can be easily installed on any internet connection (DSL, cable, dedicated, etc.) to secure them. The following is a quick list of such devices:

- Cisco RVL200 wired-only (4-port 10/100Mbps) VPN router
- Cisco RVL4000 wired-only (4-port Gigabit) VPN router
- Cisco WRV210 wireless G (4-port 10/100Mbps) VPN router
- Cisco WRV4010 wireless N (4-port Gigabit) VPN router
- D-Link DIR-130 wired-only (8-port 10/100Mbps) VPN router
- D-Link DIR-330 wireless G (4-port 10/100Mbps) VPN router
- Option Technologies Globesurfer III (3G enabled wireless VPN router)

Option 2 - Proxies and Remote Access Software

If a server is already installed on the site, whether it runs Linux, Mac, Unix, Windows or any other operating system, there is always some software available to make it a secure content provider. The below a table listing a few available options.

Software and Libraries	Operating Systems
Apache (mod_ssl, mod_auth, mod_rewrite, **mod_proxy**)	**Any** (Windows, MAC, Linux, Unix, BSD, etc.)
Microsoft Routing & **Remote Access** (**VPN** Server)	Microsoft **Windows** (2000 and up)
Open Source VPN Solutions (Open VPN)	**Any** (Windows, MAC, Linux, Unix, BSD, etc.)