

ECLYPSE User Guide

DISTECH
CONTROLS™

Innovative Solutions for Greener Buildings™

Document Revision History:

1. Version 0.1 – Beta Release - December 2014
2. Version 1.0 – Release to Market – January 2015
3. Version 1.1 – Updated Web Interface Information – February 2015
4. Version 1.2 – Added the ECY-VAV series controllers, BACnet MS/TP, Modbus RTU, and Modbus TCP network support – September 2015
5. Version 1.3 – Added Wi-Fi Mesh and Smart Room Control support – October 2015

ECLYPSE User Guide 1.3

05DI-UGIPNET-13

©, Distech Controls Inc., 2015. All rights reserved.

While all efforts have been made to verify the accuracy of information in this manual, Distech Controls is not responsible for damages or claims arising from the use of this manual. Persons using this manual are assumed to be trained HVAC professionals and are responsible for using the correct wiring procedures, correct override methods for equipment control and maintaining safe working conditions in fail-safe environments. Distech Controls reserves the right to change, delete or add to the information in this manual at any time without notice.

ENVYSION, ECLYPSE, Distech Controls, the Distech Controls logo, Open-to-Wireless, Allure and Innovative Solutions for Greener Buildings are trademarks of Distech Controls Inc.; LONWORKS is a registered trademark of Echelon Corporation. BACnet is a registered trademark of ASHRAE. Windows, Windows XP, Windows Vista, and Visual Basic.Net are registered trademarks of Microsoft Corporation. Niagara^{AX} is a registered trademark of Tridium, Inc.

TABLE OF CONTENTS

CHAPTER 1	9
Introduction	9
Introduction	10
About the ECY Series Controller	10
About the IP Protocol Suite	10
About BACnet®	10
About This User Guide	11
Purpose of the User Guide	11
ECLYPSE Introduction	11
Network Security	11
Intended Audience.....	11
Conventions Used in this Document	11
Related Documentation.....	12
Acronyms and Abbreviations Used in this Document	13
CHAPTER 2	15
Internet Protocol Suite Fundamentals	15
About the Internet Network.....	16
Internet Protocol Suite Overview	17
CHAPTER 3	18
IPv4 Communication Fundamentals	18
DHCP versus Manual Network Settings.....	19
Dynamic Host Configuration Protocol (DHCP).....	19
Why Should ECLYPSE IP Controllers use a Fixed IP Address or Hostname Management	19
Networking Basics	20
IP Addressing	20
About the Subnetwork Mask	20
CIDR Addressing.....	20
Private IPv4 Address Ranges	21
Reserved Host Addresses.....	21
Default Gateway.....	21
Domain Name System (DNS)	22
About Routers, Switches, and Hubs.....	23
Connecting a Router.....	23
Network Address Translation / Firewall.....	24
IP Network Segmentation.....	24
CHAPTER 4	26
ECLYPSE Controller IP Network Protocols and Port Numbers	26
About Port Numbers	27
ECLYPSE IP Network Port Numbers and Protocols	28
ECLYPSE Services that Require Internet Connectivity.....	30
CHAPTER 5	31
Connecting IP Devices to an IP Network	31
Connecting the IP Network.....	32
Wired Network Cable Requirements	32
About the Integrated Ethernet Switch.....	34
Fail-Safe Ethernet (ECY-VAV Model Only).....	34
Spanning Tree Protocol.....	35
Connecting the Network Cable to the ECLYPSE Controller	36
Wireless Network Connection	37

About the 2.4 GHz ISM band	37
Distance between ECLYPSE Wi-Fi Adapter and Sources of Interference	38
About Wi-Fi Network Channel Numbers	38
Radio Signal Range	38
Radio Signal Transmission Obstructions	39
Where to Locate Wireless Adapters.....	39
Transmission Obstructions and Interference	39
ECLYPSE Wi-Fi Adapter Mounting Tips.....	40
Planning a Wireless Network	42
ECLYPSE Wi-Fi Adapter Connection Modes	44
Wi-Fi Client Connection Mode	45
Wi-Fi Access Point	45
Wi-Fi Hotspot.....	46
Mesh Network	47
Wireless Network Commissioning Architectures.....	49
Client to Access Point Configuration.....	49
Client to Hotspot Configuration	50
Mesh Configuration	51
CHAPTER 6.....	52
First Time Connection to an ECLYPSE Controller	52
Connecting to the Controller.....	53
Controller Identification.....	53
Ethernet Network Connection	54
Network Connections for ECY-VAV and ECY-S1000 Model Controllers	54
Network Connections for ECY-VAV-PoE Model Controllers.....	55
Wi-Fi Network Connection.....	57
Configuring the Controller	58
Using the XpressNetwork Utility.....	58
Using the Controller's Factory-default Hostname in the Web Browser.....	58
Using the Controller's IP Address in the Web Browser.....	59
Connecting to the Controller's Configuration Web Interface	60
Next Steps.....	60
CHAPTER 7.....	61
Supported RADIUS Server Architectures.....	61
Overview.....	62
Authentication Fallback	62
RADIUS Server Architectures	63
Local Credential Authentication	63
ECLYPSE-Based Centralized Credential Authentication.....	64
EC-Net ^{AX} -Based Centralized Credential Authentication	65
Configuring the EC-Net ^{AX} Station's RestService.....	66
CHAPTER 8.....	67
ECLYPSE Web Interface.....	67
Overview.....	68
Login Credentials	69
Web Configuration Interface.....	70
Main Screen	70
Menu Button	70
Network Settings	72
IP Configuration.....	72
Wireless Configuration	73
Hotspot Configuration.....	75
Advanced	75
BACnet Settings	77

General	77
Routing	78
Network Port IP	79
BBMD Settings	80
Foreign Device Settings	81
Network Port MS/TP	82
Firmware Update	84
User Management	85
Authentication	85
Local RADIUS Server	86
Local User Management	86
Adding a User	87
Remote RADIUS Server	88
Device Information	90
System Settings	91
Saving a Certificate	92
Viewer Information	95
CHAPTER 9	96
Configuring the ECLYPSE Wi-Fi Adapter Wireless Networks	96
Setting up a Wi-Fi Client Wireless Network	97
Setting up a Wi-Fi Access Point Wireless Network	98
Setting up a Wi-Fi Hotspot Wireless Network	99
Setting up a Wi-Fi Mesh Wireless Network	101
Mesh Network Diagnostics	101
CHAPTER 10	103
Securing an ECLYPSE Controller	103
Introduction	104
Passwords	105
Change the Default Platform Credentials	105
Use Strong Passwords	105
Do Not Allow a Browser to Remember a User's Login Credentials	105
Account Management and Permissions	106
Use a Different Account for Each User	106
Use Unique Service Type Accounts for Each Project	106
Disable Known Accounts When Possible	106
Assign the Minimum Required Permissions	106
Use Minimum Possible Number of Admin Users	106
Additional Settings	107
Update the ECLYPSE Controller's Firmware to the Latest Release	107
External Factors	108
Install ECLYPSE Controllers in a Secure Location	108
Make Sure that ECLYPSE Controllers Are Behind a VPN	108
CHAPTER 11	109
BACnet MS/TP Communication Data Bus Fundamentals	109
BACnet MS/TP Data Transmission Essentials	110
Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate	112
Data Bus Segment MAC Address Range for BACnet MS/TP Devices	112
Device Loading	113
Data Bus Physical Specifications and Cable Requirements	115
Data Bus Topology and EOL Terminations	116
When to Use EOL Terminations	116
When to use EOL Terminations with BACnet MS/TP Thermostats	116
About Setting Built-in EOL Terminations	117
Only a Daisy-Chain Data Bus Topology is Acceptable	117

Data Bus Shield Grounding Requirements	119
ECB 24V-Powered Controller Data Bus Shield Grounding Requirements	119
ECB-PTU Line-Powered Data Bus Controller Shield Grounding Requirements	120
Data Bus Shield Grounding Requirements When Mixing Both ECB 24V-Powered Controllers and ECB-PTU Line-Powered Controllers.....	121
Using Repeaters to Extend the Data Bus	122
Device Addressing.....	125
Power Supply Requirements for 24VAC-Powered Controllers	130
CHAPTER 12.....	134
Subnetwork Installation Guidelines	134
About the Subnetwork Data Bus	135
Subnetwork Connection Method	135
Subnetwork Module Compatibility and Supported Quantity Charts	136
Subnetwork Module Connection	136
Subnetwork Data Bus Length	137
Cat 5e Cable Subnetwork Data Bus.....	139
Cat 5e Cable Subnetwork Data Bus Cable Requirements	139
Cat 5e Cable Subnetwork Bus Topology and End-of-Line Terminations	141
Setting the Subnet ID Addressing for Room Devices	143
Setting the Allure EC-Smart-Vue Sensor's Subnet ID Address	144
Setting the Allure EC-Smart-Air and EC-Smart-Comfort Communicating Sensor Series' Subnet ID Address.....	145
Setting the EC-Multi-Sensor Series' Subnet ID Address	146
Setting the ECx-Light and ECx-Blind Series' Subnet ID Address.....	147
Commissioning a Connected VAV Controller with an Allure EC-Smart-Vue Sensor.....	149
CHAPTER 13.....	150
Modbus TCP Configuration	150
Modbus TCP Device Connection	151
Device Addressing.....	152
CHAPTER 14.....	154
Modbus RTU Communication Data Bus Fundamentals	154
Modbus RTU Data Transmission Essentials.....	155
Maximum Number of Modbus RTU Devices on a Data Bus Segment and Baud Rate	156
Data Bus Segment Addressing Range for Modbus RTU Devices	156
Data Bus Physical Specifications and Cable Requirements	158
Data Bus Topology and EOL Terminations.....	159
When to Use EOL Terminations	159
About Setting Built-in EOL Terminations.....	159
Only a Daisy-Chain Data Bus Topology is Acceptable	160
Data Bus Shield Grounding Requirements	161
Modbus RTU Data Bus Shield Grounding Requirements.....	161
Device Addressing.....	162
CHAPTER 15.....	163
Resetting or Rebooting the Controller	163
Resetting or Rebooting the Controller	164
CHAPTER 16.....	166
ECY Controller Troubleshooting.....	166
CHAPTER 17.....	170
Allure EC-Smart-Vue Communicating Sensor Troubleshooting	170

CHAPTER 18	172
Wi-Fi Network Troubleshooting Guide	172
APPENDIX A	173
Metric Conversions for Wire Gauge	173
APPENDIX A	174
Referenced Documentation	174

CHAPTER 1

INTRODUCTION

This section provides an overview of the user guide.

In This Chapter

Topic	Page
Introduction	10
About This User Guide	11
Acronyms and Abbreviations Used in this Document	13

Introduction

This document describes best practices, specifications, wiring rules, and application information to implement robust and reliable communications networks.

About the ECY Series Controller

The ECY Series Controller is a modular and scalable platform that is used to control a wide range of HVAC applications. It uses IP protocol to communicate on wired Ethernet networks and Wi-Fi to communication on wireless networks.

This user guide also explains how to connect to the ECLYPSE controller's configuration interfaces.

About the IP Protocol Suite

Distech Controls' ECLYPSE Series controllers use a widely used IP protocol to communicate with each other and with other applications for control and supervision. What is commonly referred to as IP is actually a multi-layered protocol suite that reliably transmits data over the public internet and privately firewalled-off intranets. As integral part of our interconnected world, this protocol is used by applications such as the World Wide Web, email, File Transfer Protocol (FTP), datashares, and so on.

ECLYPSE Series controllers are able to work across geographic boundaries as a unified entity for control and administration purposes.

About BACnet®

The BACnet® ANSI/ASHRAE™ Standard 135-2008 specifies a number of Local Area Network (LAN) transport types. Distech Controls' controllers support both BACnet/IP and BACnet Master-Slave/Token-Passing (MS/TP) communications data bus (based on the EIA-485 medium) as a local network for internetworking of supervisory controllers and field controllers.

About This User Guide

Purpose of the User Guide



This user guide does not provide and does not intend to provide instructions for safe wiring practices. It is the user's responsibility to adhere to the safety codes, safe wiring guidelines, and safe working practices to conform to the rules and regulations in effect in the job site jurisdiction. This user guide does not intend to provide all the information and knowledge of an experienced HVAC technician or engineer.

This user guide shows you how to integrate ECLYPSE controllers into your IP network environment while enforcing standard network security practices.

ECLYPSE Introduction

The ECLYPSE series is a modular and scalable platform that is used to control a wide range of HVAC applications. It supports BACnet/IP communication and is a listed BACnet Building Controller (B-BC).

The ECY Series Controller consists of an automation and connectivity server, power supply, and I/O extension modules.

This programmable Connected System Controller provides advanced functionality such as customizable control logic, Web-based design and visualization interface (ENVYISION embedded), logging, alarming, and scheduling.

This user guide also explains how to configure the ECLYPSE controller's configuration interfaces.

Network Security

Maintaining the highest level of network security, especially when IP devices are connected to the Internet requires specially-trained personnel who are aware of the necessary techniques to ensure continued protection. This must include the implementation of a Virtual Private Network (VPN) to connect with IP controllers over the Internet. It is also important to coordinate with Information Technology (IT) department personnel the use of shared network resources.

The first connection to the ECY Series Controller uses a factory-default username and password. You will then be forced to change the password to a strong password to protect access to the controller.

Intended Audience

This user guide is intended for system designers, integrators, electricians, and field technicians who have experience with control systems, and who want to learn about how to make a successful IP network installation. It is recommended that anyone installing and configuring the devices specified in this user guide have prior training in the usage of these devices.

Conventions Used in this Document

Notes



This is an example of Note text. Wherever the note-paper icon appears, it means the associated text is giving a time-saving tip or a reference to associated information of interest.

Introduction

Cautions and Warnings



This is an example of Caution or Warning text. Wherever the exclamation icon appears, it means that there may be an important safety concern or that an action taken may have a drastic effect on the device, equipment, and/or network if it is improperly carried out.

Related Documentation

The follow documentation is referenced in this document. These documents are available on Distech Controls SmartSource website.

- Always refer to the [Hardware Installation Guide](#) for the devices you are installing.
- [EC-gfxProgram User Guide](#)
- [Open-to-Wireless™ Solution Guide](#)
- [Network Guide](#)

Acronyms and Abbreviations Used in this Document

Table 1-1: Acronyms and Abbreviations

Acronym	Definition
ASHRAE	American Society of Heating, Refrigeration, and Air-Conditioning Engineers
AP	Access Point
APDU	Application Protocol Data Units
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
BACnet[®]	Building Automation and Control Networking Protocol
BAS	Building Automation System
B-BC	BACnet Building Controller
BBMD	BACnet/IP Broadcast Management Device
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EOL	End Of Line
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilating, and Air Conditioning
ID	Identifier
IP	Internet Protocol
IPv4	Internet Protocol version 4
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MB	Megabyte
MHz	Megahertz
MS/TP	Master-Slave/Token-Passing
NAT	Network Address Translation
NTP	Network Time Protocol
PC	Personal Computer
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
RTU	Remote Terminal Unit (for Modbus)
SSID	Service Set IDentification

Introduction

Acronym	Definition
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
WWW	World Wide Web

CHAPTER 2

INTERNET PROTOCOL SUITE FUNDAMENTALS

This chapter describes the Internet protocol operating principles necessary to configure the IP parameters of an IP controller.

In This Chapter

Topic	Page
About the Internet Network	16
Internet Protocol Suite Overview	17

About the Internet Network

The internet is the world-wide interconnection of networks. At its root however, it is not one big network, but a group of networks that communicate between each other by using standard protocols and by using gateways between these networks called routers.

The structure of the internet is decentralized and non-hierarchical. On the internet, all communication uses the Internet Protocol (IP) to communicate and all connected devices are identified by their IP address. An Internet Registry allocates IP addresses to internet service providers to be used by their users.

Data is sent across the network in packets. Each packet has a header that identifies the sender's and intended receiver's IP addresses.

Internet Protocol Suite Overview

Internet Protocol (IP) is part of a multi-layered suite that together enables data communication. The following descriptions are an overview of the IP suite protocol layers as used by IP devices:

- Physical layer (bits): This is the physical and device-to-device electrical connection layer otherwise known as Ethernet. This layer defines:
 - The requirements for the physical connection between devices (the signal medium). For example, RJ-45 connectors (attached per TIA/EIA-568-A), using Cat 5e data cable. The maximum cable length between devices is 328 ft. (100 m) at 100 MB/s data rate.
 - The electrical signal requirements for data packet transport.
 - The data packet structure including data payload and the source and destination device's MAC addresses.

In the case of Wi-Fi connected devices, the link layer is the air interface defined by the Wi-Fi standard, such as radio frequencies, data rates, authentication, data channel encryption, and so on.

- Data Link layer: This layer implements the ability for two devices to exchange data with each other.
- Network layer: This layer implements the ability to connect multiple distinct networks with each other. It provides the internetworking methods that allow data packets to travel from the source device to a destination device across network boundaries, such as a router through the use of an IP address. See [About Routers, Switches, and Hubs](#).
- Transport Layer (segments): This layer provides end-to-end communication data stream connection between two or more devices through a variety of protocols. However it is the Transmission Control Protocol (TCP), the most commonly used internet transport protocol that is used by Distech Controls IP controllers to communicate with each other. TCP creates a connection-oriented channel between two applications; that is to say the data stream is error-checked, is sorted into the correct sequence (missing data packets are re-transmitted) and this data stream has a port number for addressing a specific application at the destination host computer.
- Session layer (data): This layer implements the protocol to open, close, and manage a session between applications such that a dialog can occur.
- Presentation layer: This layer implements the display of media such as images and graphics.
- Applications layer: This layer implements the process-to-process communications protocol that includes among other services the BACnet/IP protocol, programming, debugging, WWW, and so on.

All of the above IP suite protocol layers must be fully functional for any two devices or controllers to communicate with each other. For more detailed information about the IP suite protocol layers, see <http://www.wikipedia.org/>.

CHAPTER 3

IPv4 COMMUNICATION FUNDAMENTALS

This chapter describes IPv4 Communication operating principles.

In This Chapter

Topic	Page
DHCP versus Manual Network Settings	19
Networking Basics	20
About Routers, Switches, and Hubs	23

DHCP versus Manual Network Settings

The following methods can be used to set the network settings:

- Manually set network settings allow precise control over the network's configuration. This option may require an in-depth understanding of arcane networking details – much of which is covered in this guide. See [Networking Basics](#) on page 20.
- Use the router's DHCP setting to automatically connect devices to the network by negotiating the appropriate settings with the device. This option may not be applicable to all networks; for example, the network administrator does not want to use DHCP and has supplied information to manually configure the device's IP interface.

No matter which option is chosen, it will be necessary to coordinate with Information Technology (IT) department personnel the use of shared network resources.

Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is a router feature that dynamically allocates configuration parameters to connected devices such as IP, DNS, and default gateway addresses. Enabling DHCP on a router normally eliminates the need to manually configure network settings on connected devices. The implementation of DHCP on most routers allows a device to be assigned a fixed IP address by associating a specific IP address to a device's MAC address.



Devices that use ECLYPSE's internal router with the DHCP option (Hotspot/AP mode) cannot assign a fixed IP addresses according to the device's MAC address.

Enable Manual Assignment		
Enable Manual Assignment		<input checked="" type="radio"/> Yes <input type="radio"/> No
Manually Assigned IP around the DHCP list (Max Limit : 64)		
MAC address	IP Address	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="button" value="+"/> <input type="button" value="-"/>
98:4B:E1:CB:DA:D6	192.168.1.188	<input type="button" value="-"/>

Figure 3-1: Typical Router Configuration to Assign a Device's MAC Address to a Fixed IP Address

If your router supports DHCP and you have access to the router's configuration interface, this is the most straight-forward way to configure your network. Ensure that all devices that require a fixed IP address use a manually assigned IP address.

Why Should ECLYPSE IP Controllers use a Fixed IP Address or Hostname Management

To program or to access an IP controller, you must be able to connect to it. Like a postal address, a fixed IP address that is always assigned to the same device allows you to consistently connect to and work with the same device.

An alternative to using a fixed IP address is to use the controller's Hostname Management which allows a controller to be identified by a nickname such as **Office_205** instead of the controller's IP address. The hostname can be used in a Web browser's address bar or in the EC-*gfx*Program's **Connect to** screen.

Networking Basics

When manually configuring the TCP/IP interface on an ECLYPSE IP controller (the DHCP option is not used), an IP address, subnetwork mask, and a default gateway are required in the Network Settings.

IP Addressing

The most widely used internet addressing scheme is IPv4. It codes an IP address in 32 bits.

An IPv4 address is made up of two parts defined by a subnetwork mask; the network portion (which identifies a specific network or subnetwork) and the host portion (which identifies a specific device).

About the Subnetwork Mask

Devices on the same sub-network can address IP packets to each other directly without routing. The range of IP addresses available in a sub-network is defined by the subnetwork mask. This is also called the subnetwork mask's 'address space'. The subnetwork mask is coded in 32 bits as follows.

An IP packet addressed to a device on another network portion will have to be routed through the router's WAN port as such an address is not local. BACnet/IP broadcast discovery messages such as "Who-Is" do not pass through network routers that separate subnetworks. This means that BACnet/IP controllers on different subnetworks will not normally communicate with each other.

BBMD allows broadcast message to pass through a router: on each subnet, a single device has BBMD enabled. Each BBMD device ensures BACnet/IP connectivity between subnets by forwarding broadcast messages found on its subnetwork to each other, and then onto the local subnetwork as a broadcast message. See [BBMD Settings](#) on page 80.

CIDR	Subnetwork Mask	Block Size	Number of Subnetworks according to the Network Type			Number of Hosts according to the Network Type		
			Class A	Class B	Class C	Class A	Class B	Class C
/8	255.0.0.0	256	1			16777214		
/9	255.128.0.0	128	2			8388606		
/10	255.192.0.0	64	4			4194302		
/11	255.224.0.0	32	8			2097150		
/12	255.240.0.0	16	16			1048574		
/13	255.248.0.0	8	32			525286		
/14	255.252.0.0	4	64			262142		
/15	255.254.0.0	2	128			131070		
/16	255.255.0.0	256	256	1		65534	65534	
/17	255.255.128.0	128	512	2		32766	32766	
/18	255.255.192.0	64	1024	4		16382	16382	
/19	255.255.224.0	32	2048	8		8190	8190	
/20	255.255.240.0	16	4096	16		4094	4094	
/21	255.255.248.0	8	8192	32		2046	2046	
/22	255.255.252.0	4	16384	64		1022	1022	
/23	255.255.254.0	2	32768	128		510	510	
/24	255.255.255.0	256	65536	256	1	254	254	254
/25	255.255.255.128	128	131072	512	2	126	126	126
/26	255.255.255.192	64	262144	1024	4	62	62	62
/27	255.255.255.224	32	524288	2048	8	30	30	30
/28	255.255.255.240	16	1048576	4096	16	14	14	14
/29	255.255.255.248	8	2097152	8192	32	6	6	6
/30	255.255.255.252	4	4194304	16384	64	2	2	2

CIDR Addressing

Another way to express the subnetwork mask is through CIDR addressing (Classless Inter-Domain Routing) which is written as a slash and a number which represents the number of

true bits set in the subnetwork mask. For example, the subnetwork mask 255.128.0.0 is 11111111 10000000 00000000 00000000 in binary or /9.

An IP address can be expressed with its CIDR subnetwork mask in the form of 192.168.0.0/24 for example.

Private IPv4 Address Ranges

Each IP address class has a private address range. Private IPv4 addresses cannot be routed over the Internet.

Distech Controls IP controllers will normally be assigned to a private IP address and are connected to the LAN ports of a router, thereby keeping them behind a firewall from the internet while allowing them to freely communicate to each other and to other trusted devices.

The following IPv4 address ranges are reserved for private networks.

Network Class	IP Address Range	Number of Addresses	Largest CIDR Block (subnetwork mask)
A	10.0.0.0 - 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)
B	172.16.0.0 - 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)
C	192.168.0.0 - 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)

Reserved Host Addresses

The first and the last IP addresses are reserved for special use on all subnetwork IP address ranges:

The first IP Address is the Network ID. Networks with different network IDs are considered to be distinct. By default, no direct communication can take place between two networks that have different Network IDs. This prevents computers on one network from being accessed by computers on another network. When one department or organization is on one network, it is segregated from computers on other networks.

Last IP Address is the Broadcast Address: this is used for a specific type of network traffic that is destined to every host in the subnetwork range of IP addresses. For example, the device's DHCP client uses the broadcast address to find the network's DHCP server.

For Example, with a typical class C private network:

Subnetwork Mask = 255.255.255.0

Network ID = 192.168.1.0

Broadcast Address = 192.168.1.255

Usable IP Addresses = 192.168.1.1 - 192.168.1.254

Default Gateway

Two hosts on the same subnetwork can directly communicate with each other. When a host wants to communicate to an IP address that is not in the subnetwork address range, the host sends the packet to the default gateway. The default gateway is usually the router's IP address and is usually set in the routers administration interface. For more information about IP routing, see [About Routers, Switches, and Hubs](#) on page 23.

Certain ECLYPSE controller services use the default gateway. See [ECLYPSE Services that Require Internet Connectivity](#) on page 30.

Domain Name System (DNS)

When you want to connect to another computer or service on the Internet (to a Website for example), rarely would you want to use the IP address to make the connection as it would be a pain to remember the numeric IP address for each and every site you want to visit. The Domain Name System (DNS) was created to allow internet users to take advantage of a meaningful Uniform Resource Locator (URL) such as <http://www.distech-controls.com/> to connect to an IP address without having to know the server's or computer's numerical IP address. The DNS does this by looking up the URL and providing the numeric IP address to the requesting computer. Should the IP address of a computer/server be changed, the DNS server can be updated with its new IP address, thereby ensuring that other networked computers can still find this computer/server through its URL.

Set the DNS IP address of the Domain Name System (DNS) servers in routers and in IP controllers that have manually-configured IP parameters. Between one and three DNS IP address is usually provided by the Internet Service Provider (ISP). The second and third DNS addresses are for failover should the first DNS become unavailable.

If you do not know the address of your DNS server(s), try the following publicly-available DNS server addresses: primary = 8.8.8.8 and secondary = 4.4.4.4

Some ECLYPSE controller services use DNS to resolve Web addresses thereby allowing the service to operate. See [ECLYPSE Services that Require Internet Connectivity](#) on page 30.

About Routers, Switches, and Hubs

The differences between a hub, switch, and router are discussed in the table below.

Device Type	Description
Hub	Every incoming data packet is repeated on every other port on the device. Due to this, all traffic is made available on all ports which increase data packet collisions that affect the entire network, thus limiting its data carrying capacity.
Switch	A switch creates a one-to-one virtual circuit that directs IP packets directly to the port that the destination computer is connected to. A switch maintains a lookup table that contains the MAC addresses of all the devices that are connected to the switch ports. The switch always refers to its lookup table before it forwards data packets to the destination devices.
Router	Like a switch, a router learns the IP addresses of all devices connected to any of its RJ-45 ports to create a routing table. If a data packet arrives at the router's port with a destination IP address that is: <ul style="list-style-type: none"> Found in the router's routing table, the router forwards the data packet to the appropriate port for the device that has this IP address. For a network with a different network ID than the current network ID, the router forwards the data packet to the uplink port where the next router will again either recognize the network ID and route the data packet locally or again forwards the data packet to the uplink port. By being exposed to traffic, a router adds to its routing table the pathways necessary to resolve a data packet's pathway to its final destination, by passing through one or more routers if necessary.

Table 3-1: Difference between a Hub, Switch, and Router

Connecting a Router

The way a router is connected to other devices changes its function.

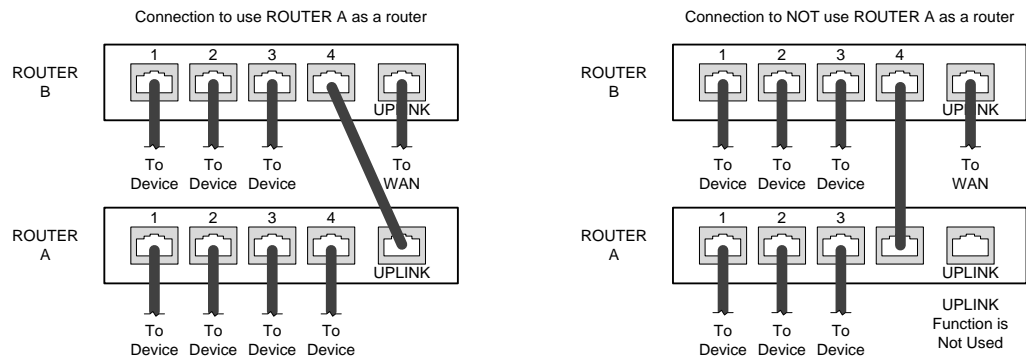


Figure 3-2: The Way a Router is Connected Changes its Function

On some routers, the uplink port is marked as WAN (Wide Area Network) and the numbered ports are to be connected to the LAN (Local Area Network) devices.

IPv4 Communication Fundamentals

Network Address Translation / Firewall

A router's uplink port provides Network Address Translation (NAT) and firewall functions.

NAT is a method to hide the private IP addresses of a range of devices (connected to LAN ports) behind a single IP address presented at the WAN uplink port. NAT uses a mechanism to track requests to WAN IP addresses and readdresses the outgoing IP packets on exit so they appear to originate from the router itself. In the reverse communications path, NAT again readdresses the IP packet's destination address back to the original source private IP address.

Due to this tracking mechanism, only requests originating from the LAN side can initiate communications. A request from the WAN to the router cannot be mapped into a private address as there is no outbound mapping for the router to use to properly readdress it to a private IP address. This is why a NAT acts as a firewall that blocks unsolicited access to the router's LAN side.

Most routers allow you to open a port in the firewall so that WAN traffic received at a specific port number is always forwarded to a specific LAN IP address. The standard port numbers used by ECLYPSE controllers is explained in [ECLYPSE Controller IP Network Protocols and Port Numbers](#) on page 26.

IP Network Segmentation

For efficient network planning, normally the IP controllers will be assigned to their own network segment of an IP network or subnetwork. This is done as shown in the figure below.

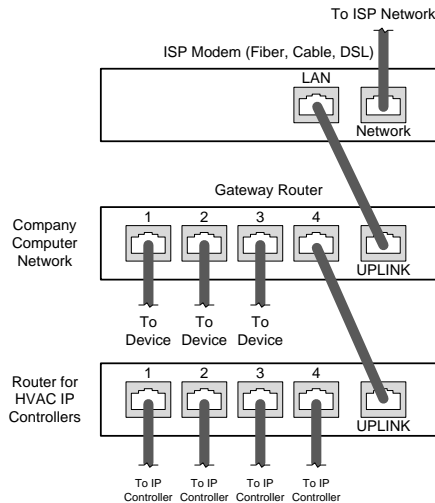


Figure 3-3: Network Segment for HVAC IP Controllers

IPv4 Communication Fundamentals

For certain wireless topologies, a wireless router can be used to connect ECLYPSE controller. In this scenario, a wireless operator interface (laptop or tablet) can be used for commissioning as shown in the figure below. If the laptop has Soft EC-BOS^{AX} installed, it can be used to program ECB series controllers connected to the RS-485 port of the Connected System Controller.

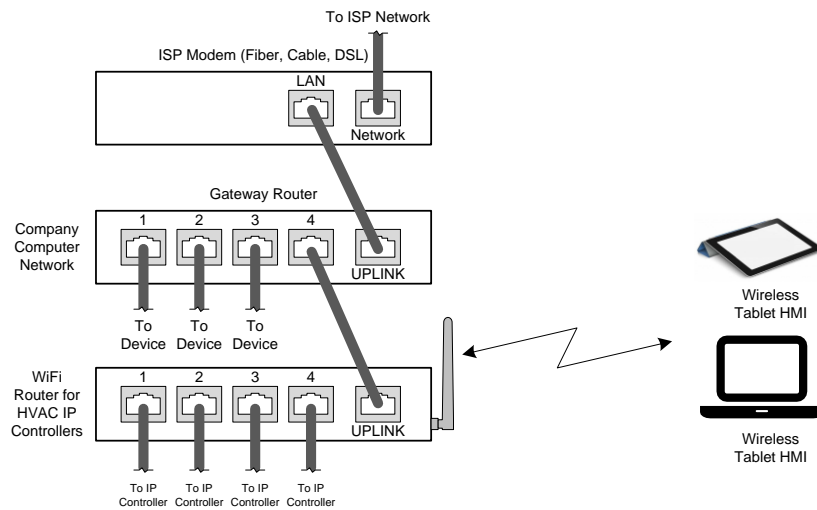


Figure 3-4: Network Segment for HVAC IP Controllers with a Wireless Access Point

If a wireless router is unavailable or is out-of-range, an ECLYPSE Wi-Fi adapter can be connected to an ECLYPSE controller's USB port to add wireless connectivity. See [Wireless Network Connection](#) on page 37.

CHAPTER 4

ECLYPSE CONTROLLER IP NETWORK PROTOCOLS AND PORT NUMBERS

This chapter describes the IP Network Protocols and Port Numbers used by the ECLYPSE controller.

In This Chapter

Topic	Page
About Port Numbers	27
ECLYPSE IP Network Port Numbers and Protocols	28
ECLYPSE Services that Require Internet Connectivity	30

About Port Numbers

In an IP packet, a port number is an extension of the packet's IP address and completes the destination address for a communications session. By convention, the packet's port number is associated with a protocol used between software applications and is used to uniquely identify a communications endpoint for a specific application or process running on a computer. This allows a multitude of applications to share a single physical connection to the Internet while allowing distinct communication channels between different applications.

For example, your web browser listens to port 80 on your computer to receive HTML web pages sent from a web server on port 80.

The standard port numbers used by ECLYPSE controllers is explained in [ECLYPSE IP Network Port Numbers and Protocols](#) on page 28.

Sometimes, two applications might use the same port number to communicate. To sort out this conflict, the following methods can be used.

- In the configuration of some applications, the port number can be changed from its default setting. Should you change it, you must also change it on the corresponding application also so that the port numbers will match.
- Routers have features such as port forwarding that can change an incoming packet's port number coming from the Wide Area Network (WAN) to another port number on the Local Area Network or vice versa.

ECLYPSE IP Network Port Numbers and Protocols

ECLYPSE uses the following IP Network Protocols to communicate over IPv4 networks. The corresponding default in-bound port number is also shown.

Service	Default Port Number (Protocol)	Description	Where can this port number be changed?
SMTP	25 (TCP)	Outgoing Email server port number. This parameter is normally provided by your ISP or network administrator.	See the EC-gfxProgram User Guide , Resources Configuration.
DNS	53 (TCP, UDP)	Domain Name Server URL lookup.	–
DHCP	67 (UDP)	The router's DHCP service that allows a device to auto-configure a devices' IP settings.	–
HTTP	80 (TCP)	<p>EC-gfxProgram Debugging Values (REST service): After the control logic or code has been sent to the controller, a live debugger allows programmers to execute code, view input/output values, and troubleshoot errors in real-time.</p> <p>ENVYSION: The ENVYSION server presents system status, trending visualization, real-time equipment visualization, schedule configuration, alarm monitoring, and dashboard functions to a Web browser operator interface.</p> <p>Web Configuration Interface: This is the network configuration interface for wired and wireless IP network interfaces.</p>	See System Settings on page 91. If this is used with EC-Net ^{AX} , this parameter can be changed in the RestService and WebService .
HTTPS	443 (TCP)	<p>Secure EC-gfxProgram Debugging Values (REST service): After the control logic or code has been sent to the controller, a live debugger allows programmers to execute code, view input/output values, and troubleshoot errors in real-time.</p> <p>Secure ENVYSION: The ENVYSION server presents system status, trending visualization, real-time equipment visualization, schedule configuration, alarm monitoring, and dashboard functions to a Web browser operator interface.</p> <p>Secure Web Configuration Interface: This is the network configuration interface for wired and wireless IP network interfaces.</p>	

ECLYPSE Controller IP Network Protocols and Port Numbers

Service	Default Port Number (Protocol)	Description	Where can this port number be changed?
Radius Server	1812 (UDP)	Authentication Port: This is the port on which authentication requests are made.	See User Management on page 85. If this is used with EC-Net ^{AX} , these parameters must be set in the RadiusService .
Radius Server	1813 (UDP)	Accounting Port: This is the port on which accounting request are made. This is only used to receive accounting requests from other RADIUS servers.	
Radius Server	1814 (UDP)	Proxy Port: This is an internal port used to proxy requests between a local server and a remote server.	
BACnet/IP	47808 (UDP)	The BACnet over IP protocol.	See BACnet Settings on page 77.

ECLYPSE Services that Require Internet Connectivity

In order to operate, the following out-bound services require:

- A working DNS. See [Domain Name System \(DNS\)](#) on page 22.
- The default gateway / router to be configured. See [Default Gateway](#) on page 21.
- Internet connectivity.

The corresponding default out-bound port number is also shown.

Service	Default Port Number (Protocol)	Description
SMTP	25 (TCP)	Outgoing Email server port number.
Network Time Protocol (NTP)	123 (UDP)	Used to set the controller's real time clock.
DNS server	53 (UDP, TCP)	Used to provide URL name resolution. The controller by default uses an internet DNS. If the local network has a DNS, set its IP address in Network Settings on page 72.

CHAPTER 5

CONNECTING IP DEVICES TO AN IP NETWORK

An IP network requires infrastructure such as Ethernet cable, routers, switches, or Wi-Fi hotspots in order to work. The following topics discuss the fundamentals of such a network.

In This Chapter

Topic	Page
Connecting the IP Network	32
Wireless Network Connection	37

Connecting the IP Network

There are two methods to connect a device to an IP Network:

- Wired (Ethernet connection with the PRI and SEC ports).
- Wireless (when the ECLYPSE Wi-Fi Adapter is connected to the controller).

Wired Network Cable Requirements

















Wired networks use commonly available Cat 5e structural cabling fitted with RJ-45 connectors. If you make your own patch cable, use Category 5e cable and crimp the RJ-45 connectors at both ends of the cable either as T568A or T568B.

Table 5-1: Wired Network Cable Physical Specifications and Requirements

Parameter	Details
Media	Cat 5e Cable; four (4) pairs of wires with RJ-45 Connectors (standard straight patch cable)
RJ-45 Pin Configuration	Straight-through wiring. Crimp connectors as per T568A or T568B (both cable ends must be crimped the same way).
Characteristic impedence	100-130 Ohms
Distributed capacitance	Less than 100 pF per meter (30 pF per foot)
Maximum Cat 5e Cable length between IP devices	328 ft. (100 m) maximum. See About the Integrated Ethernet Switch on page 34.
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections) ECLYPSE IP devices have two RJ-45 female RJ-45 connectors that provide IP packet switching to support follow-on devices.
Daisy-chain limit, Connected System Controllers	Up to 20 devices can be daisy-chained per network switch port.
Daisy-chain limit, Connected VAV Controllers	Up to 50 devices can be daisy-chained per network switch port.
EOL terminations	Not applicable
Shield grounding	Not applicable

Crimp both ends of the cable either as T568A or T568B as shown below.

Table 5-2: T568A and T568B Terminations for an RJ-45 Connector

Pin	T568A (at both cable ends)		T568B (at both cable ends)	
	Pair	Color	Pair	Color
1	3	 white/green stripe	2	 white/orange stripe
2	3	 green solid	2	 orange solid
3	2	 white/orange stripe	3	 white/green stripe
4	1	 blue solid	1	 blue solid
5	1	 white/blue stripe	1	 white/blue stripe
6	2	 orange solid	3	 green solid
7	4	 white/brown stripe	4	 white/brown stripe
8	4	 brown solid	4	 brown solid

The final result of a crimped RJ-45 connector is shown graphically below.

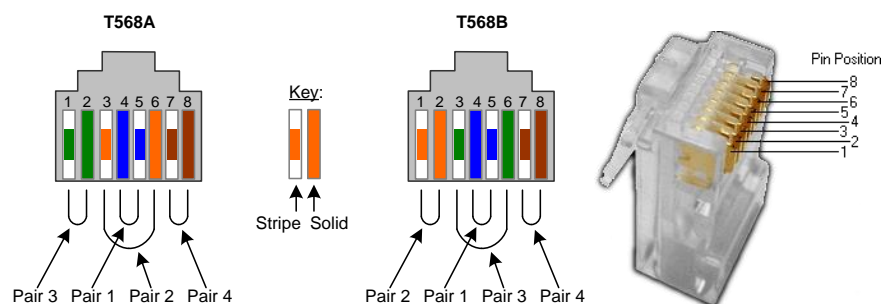


Figure 5-1: Pins on RJ-45 Jack Face

Distech Controls recommends the Cat 5e cables shown below. Cables fitted with connectors are crimped as T568B.

Table 5-3: Distech Controls Recommended Cable Types to use for the Cat 5e Cable Subnetwork Bus

Bus and Cable Type	Non-Plenum Applications (Use in Conduit - FT4)		Plenum Applications (FT6)	
	Part Number	O.D. (Ø) ¹	Part Number	O.D. (Ø) ¹
300 m (1000 feet), Cat 5e Yellow Jacket Cable – Without Connectors	CB-W244P-1446YLB	4.6mm (0.18in.)	CB-W244P-2175YEL	4.6mm (0.18in.)
100 Crimp RJ-45 Connectors	CB-W5506E	N/A	CB-W5506E	N/A

1. Outer cable diameter – This does not take into account the RJ-45 connector.

Connecting IP Devices to an IP Network

About the Integrated Ethernet Switch

The 2-port wired interface uses a switch to forward packets addressed to downstream IP devices connected to it. This allows controllers to be daisy-chained together to extend the IP network's physical range and to reduce the amount of network cable required as each controller no longer has to make a home run to the network switch.

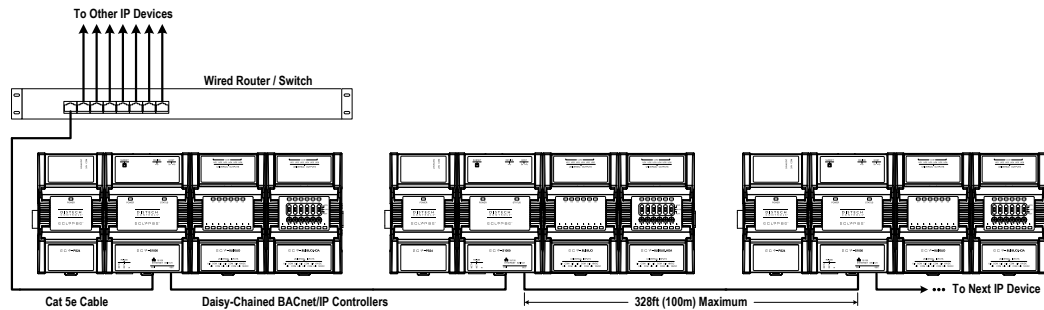


Figure 5-2: Wired Network Connection: Daisy-Chained ECLYPSE Controllers

Fail-Safe Ethernet (ECY-VAV Model Only)

To support fail-safe Ethernet, the onboard switch on the ECY-VAV model has a bypass capability that links inbound and outbound network segments together when there is an internal disruption (power is lost, for example). Under normal operating conditions, the onboard switch regenerates the electrical signal when it forwards the IP packet to the next device. For this reason, the maximum Cat 5e cable length between IP devices is 328 ft. (100 m).

When there is a failure and the switch is being bypassed, the network segments on both sides of the controller are directly connected together; however the same length limit applies. This means that the total maximum Cat 5e cable length between one functional switch and the next functional switch cannot exceed 328 ft. (100 m). Therefore, it is recommended that the cable length between controllers be no more than 50m so that if ever one device fails the total cable length between both working devices is less than 328 ft. (100 m) as shown in the following diagram:

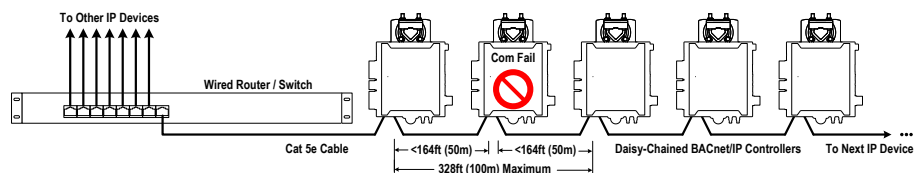


Figure 5-3: Wired Network Connection: Daisy-Chained ECY-VAV Controllers with Fail-Safe Ethernet Support

Spanning Tree Protocol

Switches and routers that support Spanning Tree Protocol (are IEEE 802.1D certified) are able to detect and eliminate a loop from being formed on the network by disabling any port on the router that is causing a loop. Such switches can be used to enhance network availability by allowing you to create a ring network of controllers that is resistant to a single point network failure (a cut wire for example).

In this scenario, non-PoE controllers are connected in a loop (or ring) such that the last controller is connected back to the switch / router. Under normal operation, the switch / router disables one of the ports to prevent a packet storm. This is shown below.

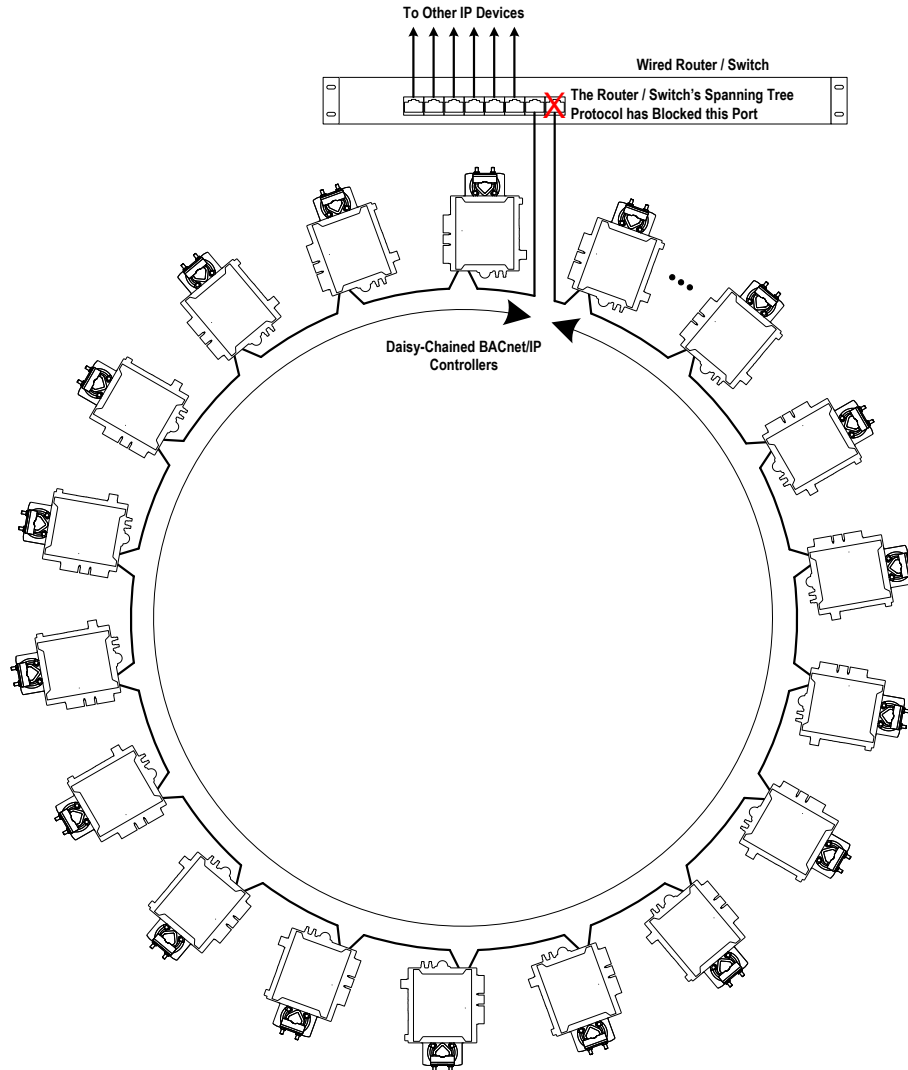


Figure 5-4: Wired Network Connection: Spanning Tree Protocol – Normal Operation

Connecting IP Devices to an IP Network

When a network wire is cut, the ring is split into two – the switch / router automatically enables the port to maintain service. This is shown below.

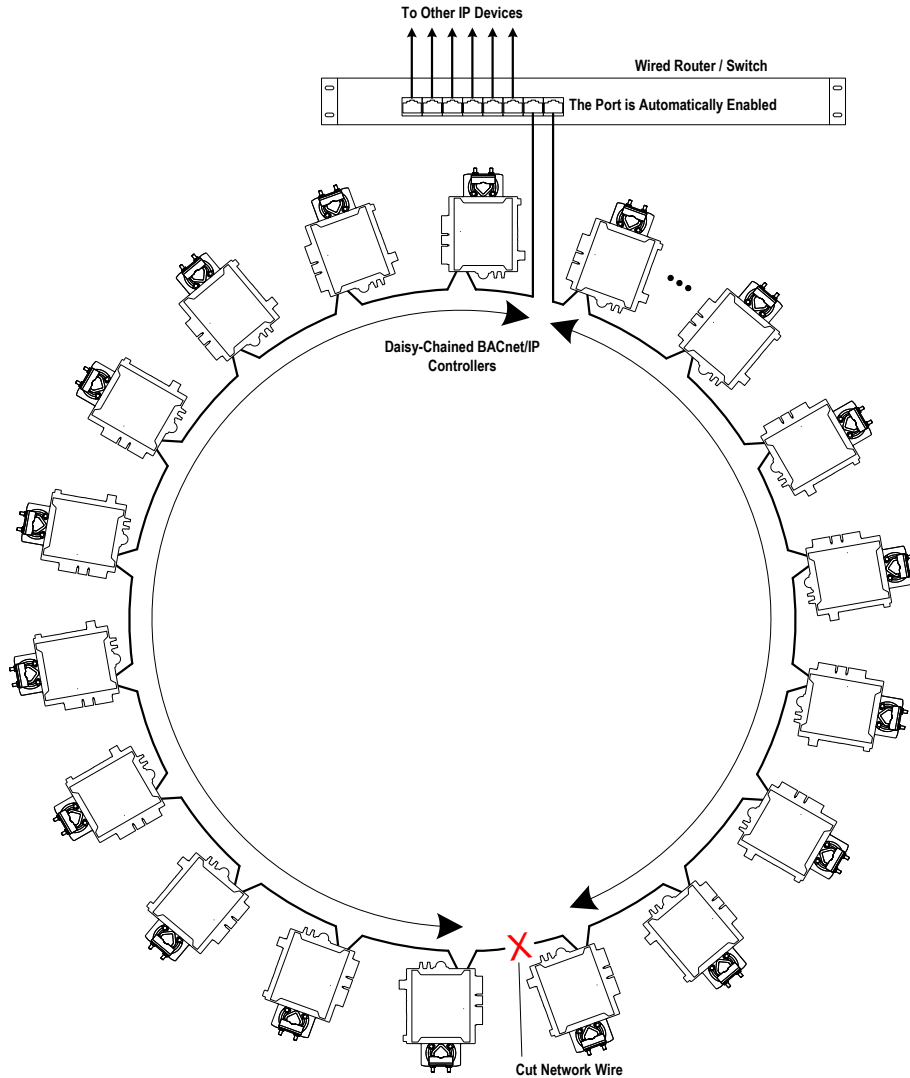


Figure 5-5: Wired Network Connection: Spanning Tree Protocol – Failover Operation

The switch / router can be configured to send an email message when port blocking is disabled thus signaling that a network wire has been cut.

Connecting the Network Cable to the ECLYPSE Controller

To connect controllers to an Ethernet network and then discover them, see [First Time Connection to an ECLYPSE Controller](#) on page 52.

Wireless Network Connection

The ECLYPSE Wi-Fi adapter connects to an ECLYPSE controller's USB port.



Figure 5-6: ECLYPSE Wi-Fi Adapter

It adds wireless IP connectivity to ECLYPSE controllers and it can be used in a number of wireless topologies and applications.

To wirelessly connect to a controller for the first time, see [First Time Connection to an ECLYPSE Controller](#) on page 52.

To configure an ECLYPSE Wi-Fi adapter, see [Network Settings](#) on page 72. See also [Configuring the ECLYPSE Wi-Fi Adapter Wireless Networks](#) on page 96.

Recommendations are provided regarding the radio signal obstructions and factors that should be avoided to obtain the best Wi-Fi radio signal transmission and reception. Walls attenuate radio wave propagation by an amount that varies with the construction materials used. See [Radio Signal Transmission Obstructions](#) on page 39 for more information on wall materials that can reduce range transmission.

About the 2.4 GHz ISM band

The 2.4 GHz ISM (Industrial, Scientific and Medical) band has been allocated worldwide for the use of radio frequency energy by industrial, scientific, and medical purposes as part of the device's method of internal operation and as such may have powerful emissions that cause interference to radio communications.

For example, microwave ovens operate in the 2.4 GHz ISM band with about 1000W emitted power and a fraction of a percent of that energy does leak from the oven. While this is not a health risk, Wi-Fi networks operate at even lower power levels to communicate and can be overwhelmed by this source of interference.

When setting up a 2.4 GHz band Wi-Fi network, you must take into consideration any equipment that operates in the 2.4 GHz ISM band such as medical and laboratory equipment. Other sources of interference are other telecommunications equipment such as cell phones, GSM/DECT, cordless phones, RFID reader, Bluetooth devices, walkie-talkies, baby monitors, and so on. Note that equipment that transmits in other frequency bands do emit spurious emissions at low levels over a wide spectrum so that a radio transmitter in close proximity to the ECLYPSE Wi-Fi adapter can cause interference, even if its operating frequency is 1.9 GHz for example.

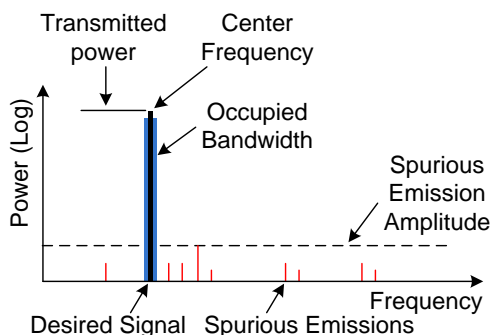


Figure 5-7: Typical Radio Transmitter Spurious Emissions

Distance between ECLYPSE Wi-Fi Adapter and Sources of Interference

Unrelated transmitters should be more than 6.5 feet (2 m) away from the ECLYPSE Wi-Fi Adapter to avoid possible interference.

About Wi-Fi Network Channel Numbers

Wi-Fi communications use a slice of radio spectrum or channel width for data transmission. In general terms, the amount of channel width required is proportional to the data transmission rate. Wi-Fi networks operate in a number of different frequency ranges or bands such as the 2.4 GHz band. Each band is divided into a number of industry-standard channels that represent a center frequency for data transmission. In practice, the center frequency is the mid-point between the upper and lower cutoff frequencies of the channel width.

When the channel width is larger than the channel spacing (the space between channels), overlap between the channels can occur, resulting in inter-channel interference that lowers overall network throughput. This is shown in the diagram below. For example, in the 2.4 GHz band using 802.11g, the channel width is 20 MHz while the channel spacing is 5 MHz. If one Wi-Fi network is using channel 1 that is in close proximity to another Wi-Fi network that is using channel 2, there will be significant inter-channel overlap and interference. Data throughput is reduced as a result.

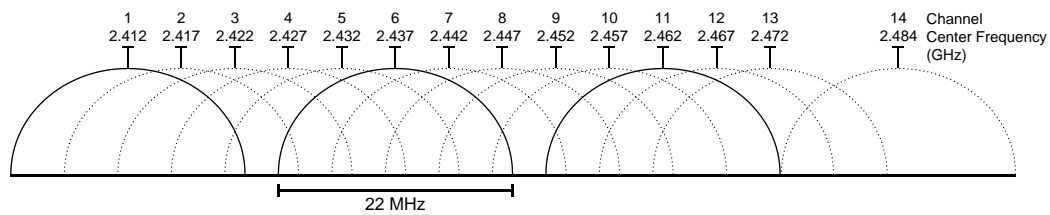


Figure 5-8: 2.4 GHz Band 802.11g Radio Spectrum Showing Inter-Channel Overlap

For a 20 MHz channel width in the 2.4 GHz band using 802.11g, the best channels to use to avoid inter-channel overlap are channels 1, 6, and 11. For a 40 MHz channel width in the 2.4 GHz band using 802.11g, the best channels to use to avoid inter-channel overlap are channels 3 and 11.

For a 20 MHz channel width in the 2.4 GHz band using 802.11n, the best channels to use to avoid inter-channel overlap are channels 1, 6, and 11. For a 40 MHz channel width in the 2.4 GHz band using 802.11g, the best channel to use to avoid inter-channel overlap is channel 3.

For industrial / commercial environments, it is recommended to avoid using a 40 MHz channel width in the 2.4 GHz band as it occupies a large part of the available radio spectrum. This means that it will be difficult to co-exist with other networks while avoiding interference, especially from devices that use mixed mode 802.11 b/g which significantly degrades 802.11n performance. One solution is to disable the 802.11 b/g mode on all hotspots to force all wireless clients to 802.11n mode, thereby forbidding the use of legacy devices.

Radio Signal Range

Range is dependent upon many environmental variables that are present in buildings. In normal conditions, a radio signal is transmitted at a maximum range between ECLYPSE Wi-Fi Adapters of 50 feet (15 m) at 2.4 GHz (IEEE 802.11b/g/n).

In certain cases where there are obstructions, the range could be less.

Because radio signals and transmission range can vary according to building and office setup, you can troubleshoot Wi-Fi network performance issues by running a Wi-Fi surveying

or Wi-Fi stumbling tool on a laptop computer. This software shows the currently operating Wi-Fi networks operating within range, their signal strength, and their channel number so as to make the best configuration choices.

Radio Signal Transmission Obstructions

Radio signals are electromagnetic waves; hence the further they travel, the weaker the signal becomes thereby limiting effective range of operation. Coverage is further decreased by specific materials found in the direction of the transmission. For example, while radio waves can penetrate a wall, they are dampened more than if the waves were on a direct line-of-sight (LoS) path.

The following table shows the different types of building materials and range reduction:

Wall Material	Range Reduction vs. LoS
Wood, drywall, glass (uncoated, without metal)	0 – 10%
Brick, particle board	5 – 35%
Metal, steel-reinforced concrete, mirrors See also Figure 5-9.	10 – 90%

Where to Locate Wireless Adapters

When installing the wireless adapter, it is important to ensure that distances and obstructions do not impede transmission. Metallic parts, such as steel reinforcement in walls, machinery, office furniture, etc. are major sources of field strength dampening. Furthermore, supply areas and elevator shafts should be considered as complete transmission screens ([Figure 5-9](#)).

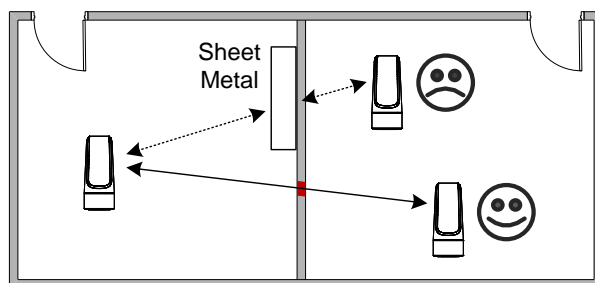


Figure 5-9: Screening of Radio Waves

Transmission Obstructions and Interference

One way to get around an obstruction, such as a duct, is to place the wireless adapter on the side of the obstruction that is nearer to the coordinating wireless device, even if the controller is on the opposite side of the obstruction. But always keep in mind that the wireless adapter performs best when it is away from metal objects or surfaces (more than 1" (2.5 cm)).

For more examples on how to position the wireless adapter, refer to section [ECLYPSE Wi-Fi Adapter Mounting](#) Tips on page 40.

In addition to obstructions, the angle with which the transmission travels through the obstruction has a major influence on the field strength. The steeper the angle through an obstruction, the radio wave has to travel through more material resulting in the field strength reduction ([Figure 5-10](#)). Therefore it is preferable that the transmission be arranged so that it travels straight and perpendicularly through the obstruction.

Connecting IP Devices to an IP Network

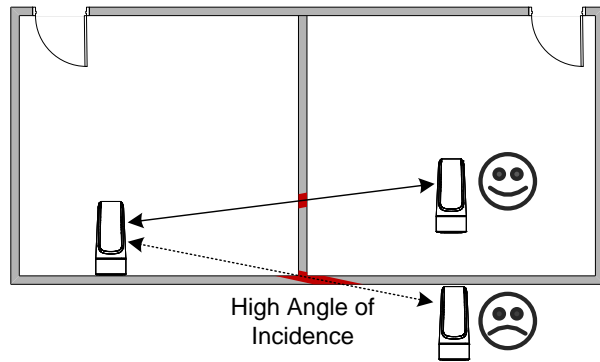


Figure 5-10: Angle of Radio Waves

A solution to avoid an obstruction is to add another wireless router located closer to the controller(s).

ECLYPSE Wi-Fi Adapter Mounting Tips

This section provides information and examples on how to properly position the ECLYPSE Wi-Fi Adapter to ensure reliable wireless communication. The most common guidelines to remember when installing the ECLYPSE Wi-Fi Adapter is to keep it at least 1" (2.5 cm) away from metal, and never install the ECLYPSE Wi-Fi Adapter inside a metal enclosure (relay panels, junction box, etc.).

Typical VAV Installation

The following image shows where to install an ECLYPSE Wi-Fi Adapter on a metal duct with a VAV controller installation to maximize wireless performance.

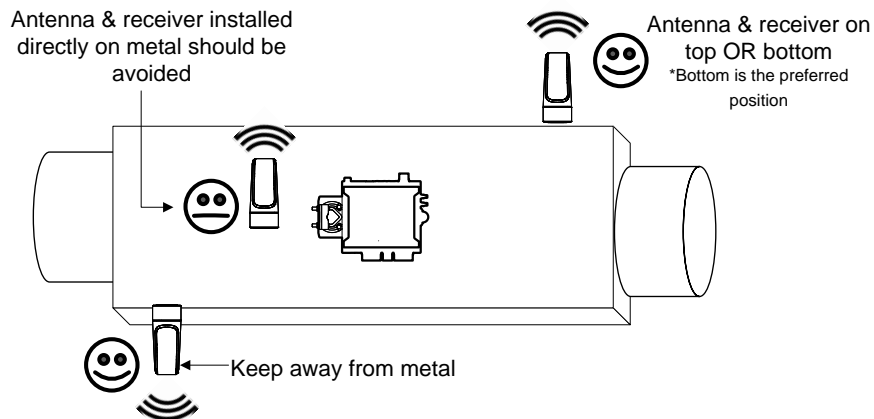


Figure 5-11: Typical VAV installation – One ECLYPSE Wi-Fi Adapter

Typical VAV Installation within a Metal Enclosure

The next example shows where to install an ECLYPSE Wi-Fi Adapter when a VAV controller is located inside a metal box. The ECLYPSE Wi-Fi Adapter should be installed on the outside of the metal box, on the top or bottom of the box.

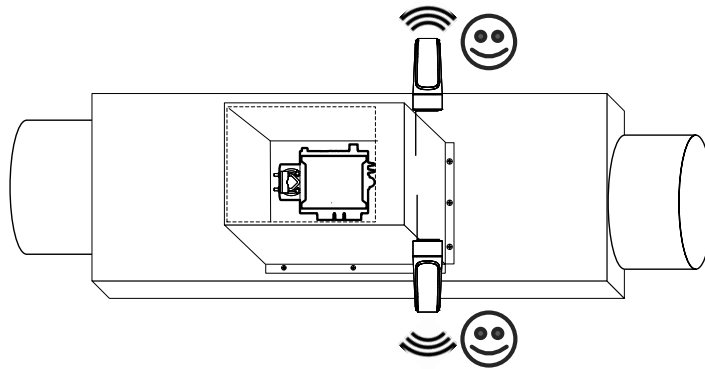


Figure 5-12: ECLYPSE Wi-Fi Adapter Position with VAV in Metal Enclosure

Typical Metal Relay Panel/Utility Box Installation

The following image shows where to install an ECLYPSE Wi-Fi Adapter on a metal relay panel or utility box with a controller inside the panel/box. To maximize wireless range, the ECLYPSE Wi-Fi Adapter must be installed on the top or side of the panel.

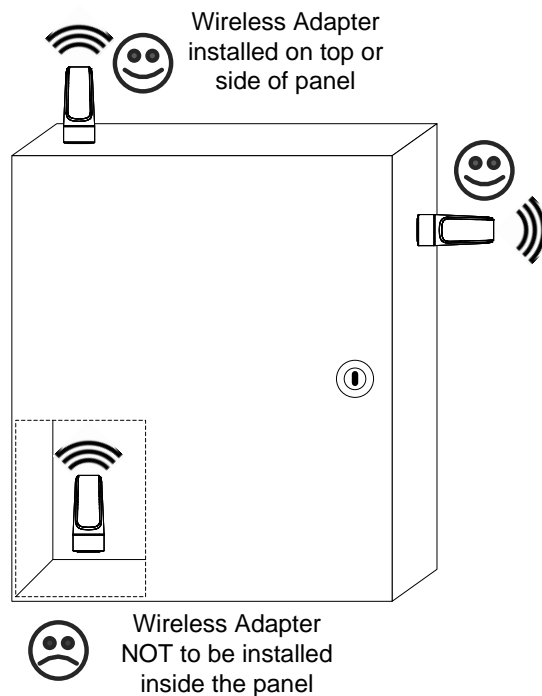


Figure 5-13: ECLYPSE Wi-Fi Adapter Position with Metal Relay Panel/Utility Box

Typical Fan Coil Unit Installation

The following example shows where to install an ECLYPSE Wi-Fi Adapter on a fan coil unit with a controller inside the unit. The ECLYPSE Wi-Fi Adapter must be installed on the top or side of the unit with the antenna straightened out and away from the metal. The ECLYPSE Wi-Fi Adapter and antenna should never be installed inside the metal enclosure.

Connecting IP Devices to an IP Network

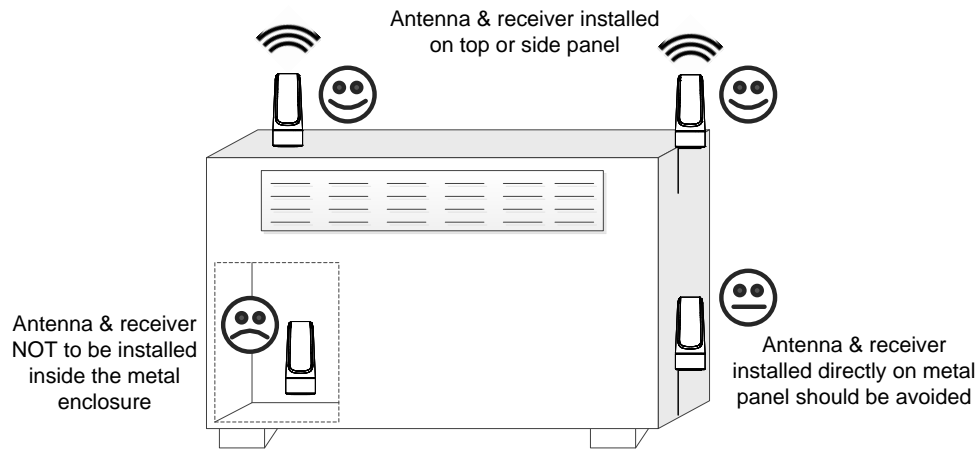


Figure 5-14: ECLYPSE Wi-Fi Adapter Position on Fan Coil Unit

Planning a Wireless Network

A wireless network can be installed in many different types of floor spaces, large or small: office space, commercial space, residential space, etc. The following provides an example on how to start planning a wireless network such as a large office space. This type of planning can also be used with smaller areas. To plan a mesh network, see [Mesh Network](#) on page 47.

1. Retrieve a copy of your floor plans and a compass.

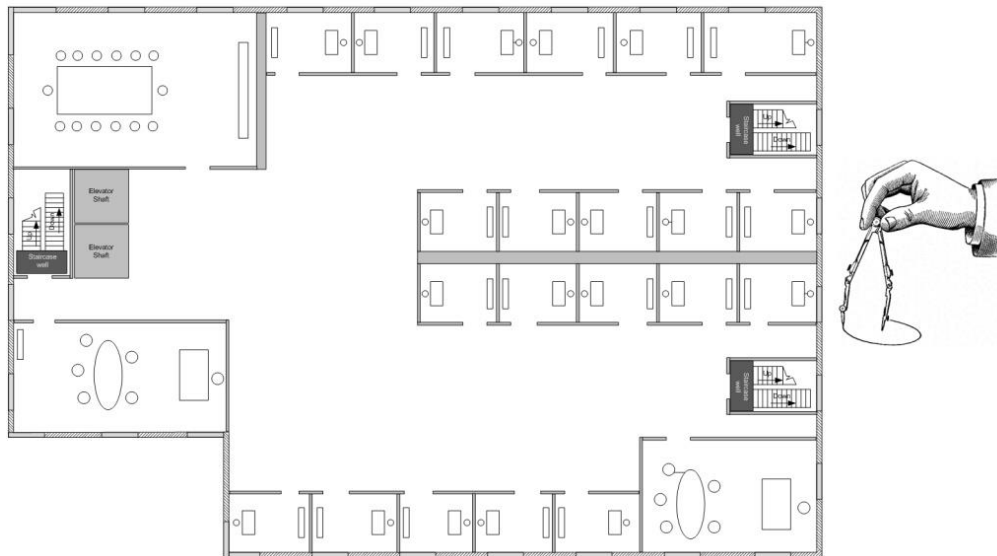


Figure 5-15: Copy of floor plan and a compass

2. Mark relevant radio shadings into floor plan such as: fire protection walls, lavatories, staircases, elevator shafts and supply areas.

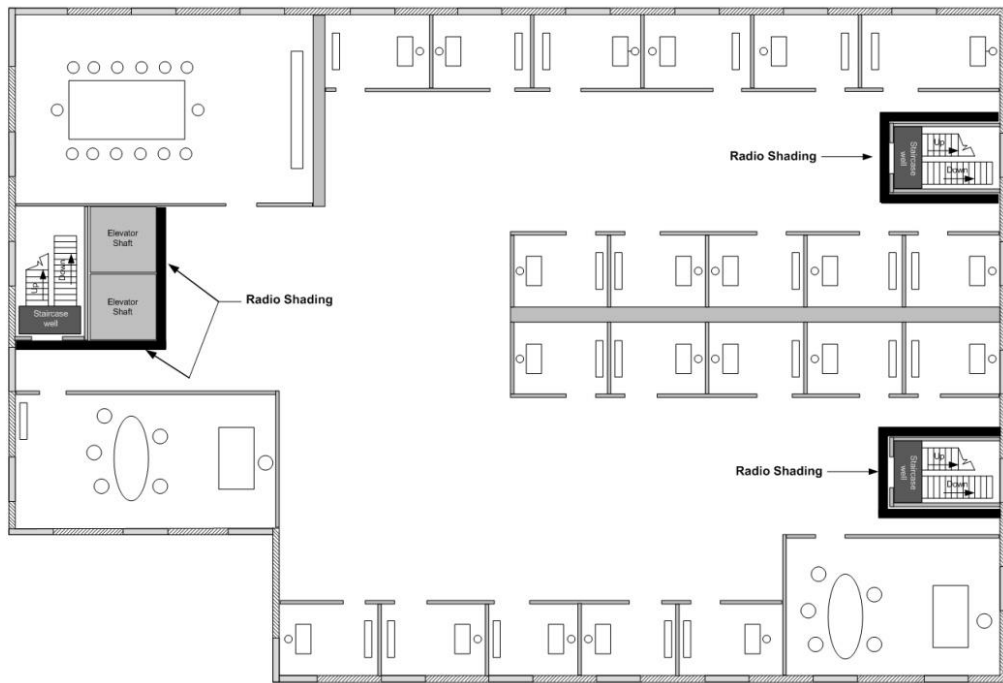


Figure 5-16: Mark relevant radio shadings

3. Draw circles to locate the ideal positions for your ECLYPSE Wi-Fi Adapter as shown below:

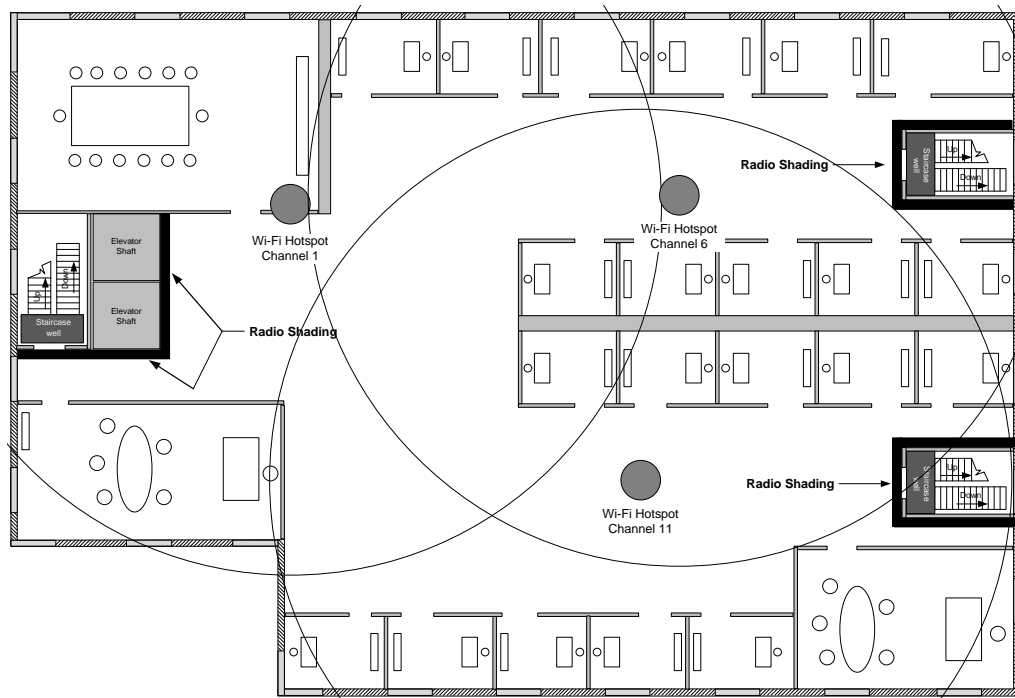


Figure 5-17: Radio ECLYPSE Wi-Fi Adapter Location



Make sure that the ECLYPSE Wi-Fi Adapter is positioned in a way such that no screens block the connection to any corner inside the fire safety section (potential sensor positions).

Connecting IP Devices to an IP Network



For reliable range planning, the unfavorable conditions should be detected at the beginning but often come from later changes to the environment (room filled with people, alteration of partition walls, furniture, room plants, etc.).



Even after careful planning, range and signal tests should be done during installation to verify proper reception at the ECLYPSE Wi-Fi Adapter positions. Unfavorable conditions can be improved by changing the antenna position or by adding a router closer to the controller(s).

ECLYPSE Wi-Fi Adapter Connection Modes

ECLYPSE Wi-Fi adapter supports a number of connection modes shown in the table below:

Connection Mode	Description	Maximum Number of Wireless Clients or Nodes
Client	This sets the mode of the ECLYPSE Wi-Fi adapter to connect the controller as a client of a Wi-Fi access point. This interface can auto-configure its IP parameters when the connected network that has a DHCP server. When an ECLYPSE controller is a Wi-Fi client, the Ethernet ports cannot be used to provide network connectivity to another ECLYPSE controller or to a laptop for example.	16
Access Point	This sets the mode of the ECLYPSE Wi-Fi adapter to be a Wi-Fi access point. This access point operates off of the same subnetwork and has the same IP connectivity that the controller has with its wired network connection. For example, if the controller's wired connection is to a network that has an active DHCP server, access point clients can also use this DHCP server to automatically configure their IP connection parameters.	16
Hotspot (default)	This sets the mode of the ECLYPSE Wi-Fi adapter to be a Wi-Fi hotspot with a router. This puts the hotspot into a separate subnetwork with a DHCP server to provide IP addresses to any connected device. Wide area network (WAN) connectivity is through the wired connection.	16
Mesh	This sets the mode of the ECLYPSE Wi-Fi adapter to be a member of a mesh network. This interface can auto-configure its IP parameters when the connected network has a DHCP server.	30 per mesh network

Typical application examples are shown below.

Wi-Fi Client Connection Mode

Cut installation costs by leveraging existing wireless infrastructure by eliminating the need for Ethernet cables. This architecture is characterized by the point-to-point connection between an access point and a client-controller.

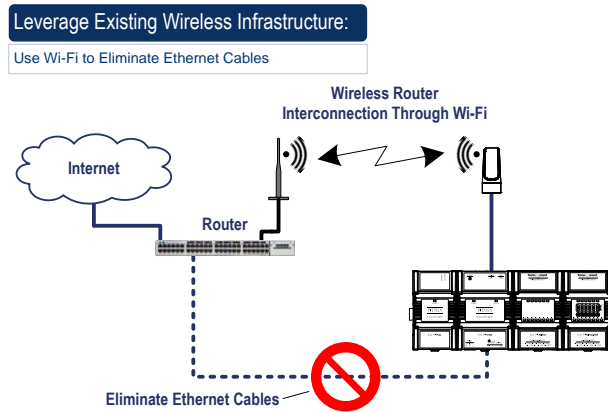


Figure 5-18: Leveraging Existing Wireless Infrastructure by Eliminating Ethernet Cables

To configure the Wi-Fi client connection mode, see [Setting up a Wi-Fi Client Wireless Network](#) on page 97.

Wi-Fi Access Point

Should there be no available access point; an ECLYPSE controller can be configured as a wired-to-wireless bridge to create an access point which can provide Wi-Fi access to other Wi-Fi enabled clients. This access point operates off of the same subnet and has the same IP connectivity that the controller has with its wired network connection. The ECLYPSE Wi-Fi adapter can also be temporarily added to an ECLYPSE controller for wireless commissioning purposes. A variety of software applications are available for system monitoring and override, commissioning, configuration and programming. To configure the Wi-Fi access point connection mode, see [Setting up a Wi-Fi Access Point Wireless Network](#) on page 98.

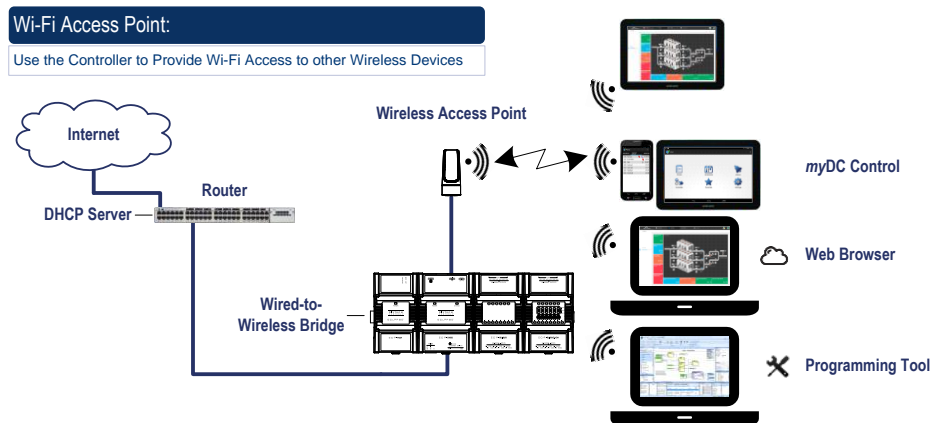


Figure 5-19: Using an ECLYPSE Controller Create an Access Point

Connecting IP Devices to an IP Network

A second ECLYPSE controller can be configured as a wireless client. This can be used as a solution to 'jump' architectural features that are not compatible with wires such as glass atriums and the like. To configure the Wi-Fi client connection mode, see [Setting up a Wi-Fi Client Wireless Network](#) on page 97.

An access point can provide Wi-Fi access to other Wi-Fi enabled clients and controllers.

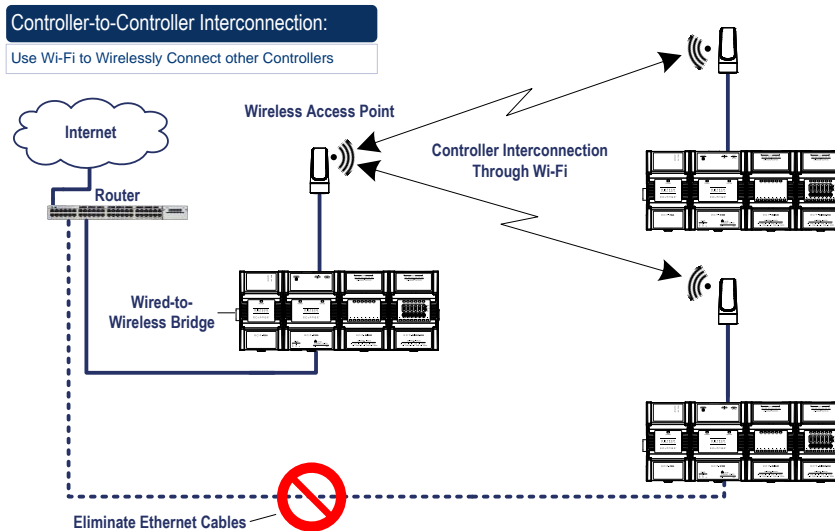



Figure 5-20: Using an ECLYPSE Controller as a Wireless Bridge

Wi-Fi Hotspot

Should the wired network not use a DHCP server (uses fixed IP addresses); an ECLYPSE controller can be configured to create a hotspot with a router that creates its own subnet and DHCP server which can provide Wi-Fi access to other Wi-Fi enabled clients. This is the default connection method when an ECLYPSE Wi-Fi adapter is connected to an ECLYPSE controller. The ECLYPSE Wi-Fi adapter can also be temporarily added to an ECLYPSE controller for wireless commissioning purposes. A variety of software applications are available for system monitoring and override, commissioning, configuration and programming. To configure the Wi-Fi hotspot connection mode, see [Setting up a Wi-Fi Hotspot Wireless Network](#) on page 99.

 A hotspot creates a subnetwork. As a result, any connected BACnet device will not be able to discover BACnet devices on any other LAN subnetwork.

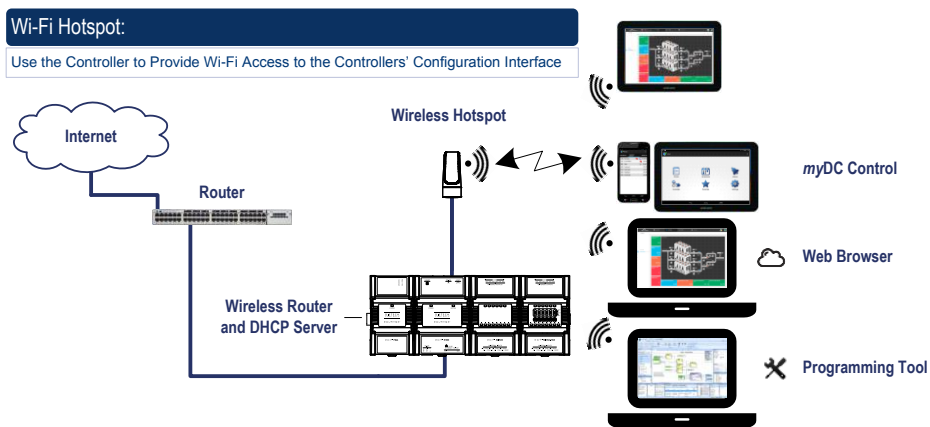


Figure 5-21: Using an ECLYPSE Controller Create a Hotspot

Mesh Network

A mesh network increases communication reliability and provides redundancy. When one node drops out, the remaining nodes can still communicate with each other, either directly or through one or more intermediate nodes, thus allowing the mesh network to self-heal, resulting in increasing network availability. To configure the Wi-Fi mesh connection mode, see [Setting up a Wi-Fi Mesh Wireless Network](#) on page 101.

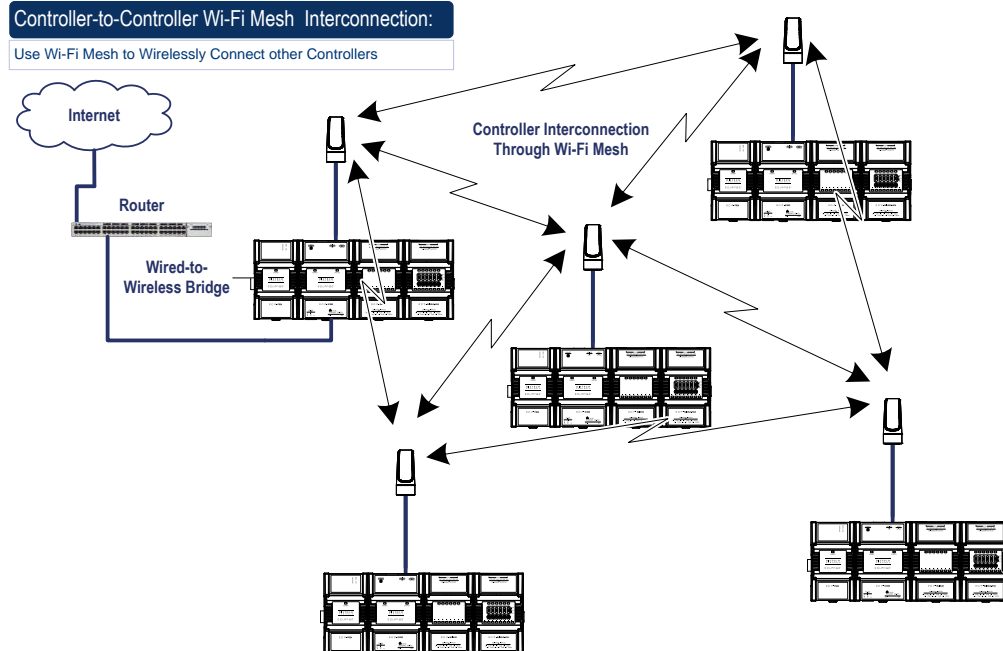


Figure 5-22: A Mesh Network Increases Wireless Communication Reliability

Avoid Network Broadcasts with a Mesh Network

When ECLYPSE controllers are connected in a Wi-Fi mesh network, it is best to prevent broadcast packets from being sent across a Wi-Fi mesh network. The following are the most common sources of network broadcast messages.

- PCs are continuously looking for services (printers, file servers, etc.) and each other on the network. The solution is to use a router to separate networks for ECLYPSE controllers that use a Wi-Fi mesh from PC networks: put the PCs on the WAN side of the router with the controllers on the LAN side of the router.
- BACnet controllers broadcast notification messages and network time updates. A broadcast from a BACnet MS/TP controller will be rebroadcasted on the BACnet/IP network by an ECLYPSE Connected System Controller. If the IP network has ECLYPSE controllers that use a Wi-Fi mesh, make use of BACnet Broadcast messages as infrequently as possible, whether the BACnet Broadcast message comes from a BACnet MS/TP or BACnet/IP controller.

Connecting IP Devices to an IP Network

Alternate the Mesh Network Channel Number

When there is a need for more than 30 mesh network clients, two or more mesh networks are used as shown below. To reduce interference between mesh networks and increase network throughput, it is important to alternate the mesh network's channel number between channel 1 and channel 3 for each mesh network that is next to another.

For example the following figure shows a 3-storey building that has a West wing and an East wing. It shows Wi-Fi mesh channel number alternating between channel 1 and channel 3 from wing to wing and floor to floor.

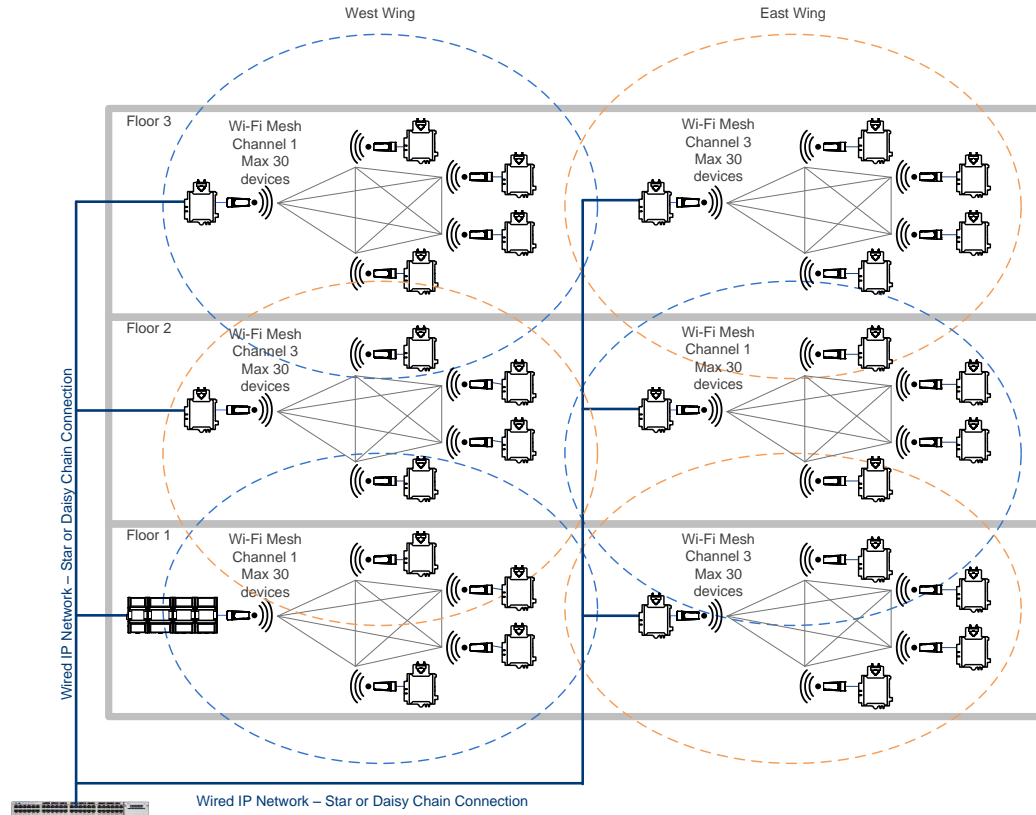


Figure 5-23: Alternate the Mesh Network Channel Number

Wireless Network Commissioning Architectures

Client to Access Point Configuration

A laptop is connected through Wi-Fi, as a Wi-Fi client, to any Connected VAV Controller that has its wireless settings configured as an Access Point. The other Connected VAV Controllers are configured as Wi-Fi Clients and are wirelessly connected to the same Access Point.

With this configuration, the laptop and all the ECLYPSE controllers are on the same subnet, so the laptop user has access to all networked ECLYPSE controllers.

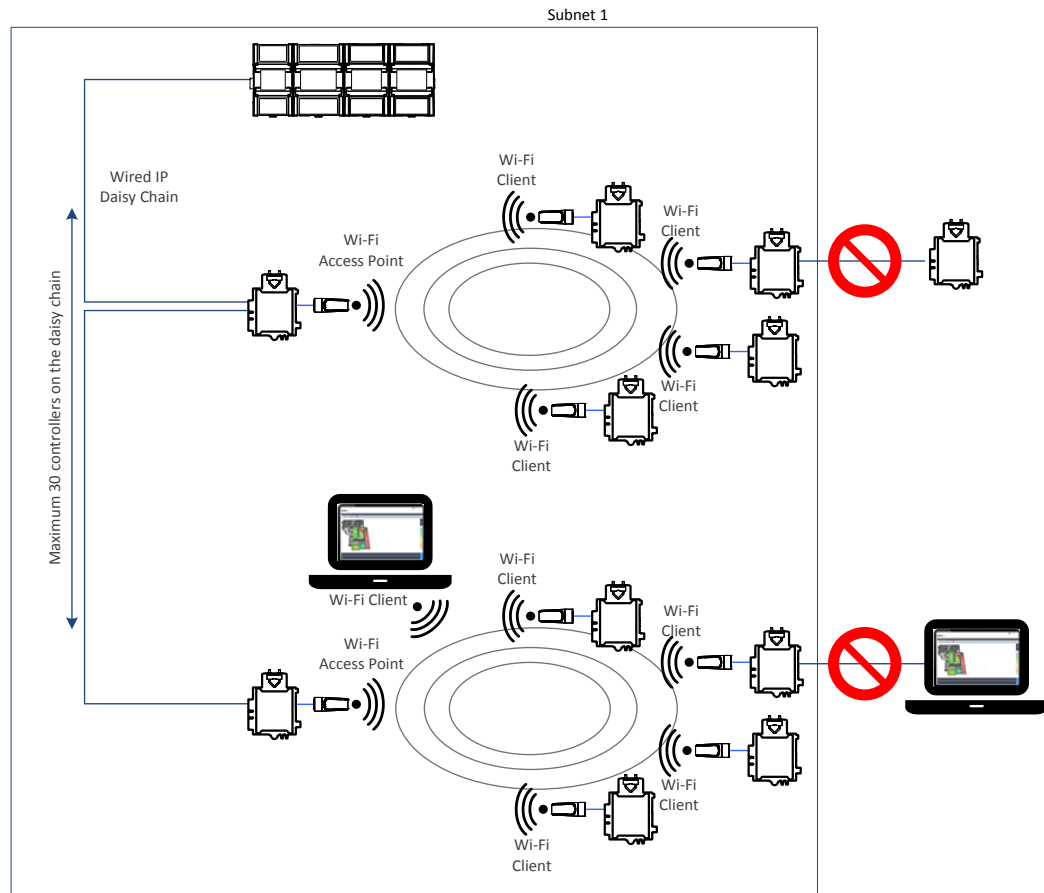


Figure 5-24: Client to Access Point Configuration

Connecting IP Devices to an IP Network

Client to Hotspot Configuration

A laptop is connected through Wi-Fi, as a Wi-Fi client, to a Connected System Controller that has its wireless settings configured as a Hotspot. The Connected VAV Controllers that are part of the wired network are configured, on their wireless side as a Wi-Fi Access Point.

The other Connected VAV Controllers are configured as a Wi-Fi Client and are wirelessly connected to an Access Point.

With this configuration, the laptop is on the same subnet as the Connected System Controller (Subnet 2 created by the Hotspot), but all the Connected VAV Controllers are on a different Subnet (Subnet 1), so the laptop user has access only to the Connected System Controller.

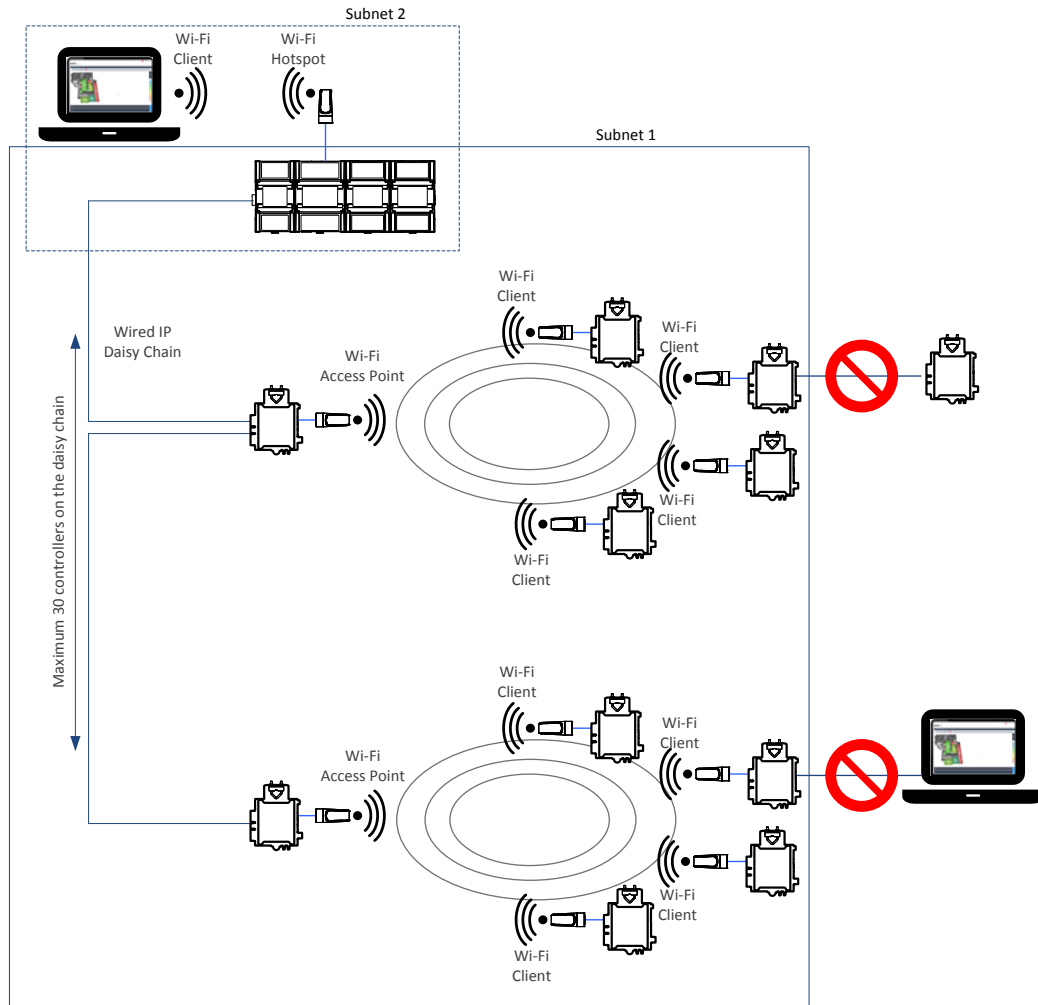


Figure 5-25: Client to Hotspot Configuration

Mesh Configuration

The laptop is part of the wired IP daisy chain. The Connected VAV Controllers that are part of the wired network are configured on their wireless side as Wi-Fi Mesh and they are enabled as the Mesh Gate (see [Wireless Configuration](#) on page 73). The other Connected VAV Controllers are configured as Wi-Fi Mesh.

With this configuration, the laptop and all the controllers are on the same subnet, so the laptop user has access to all the controllers.

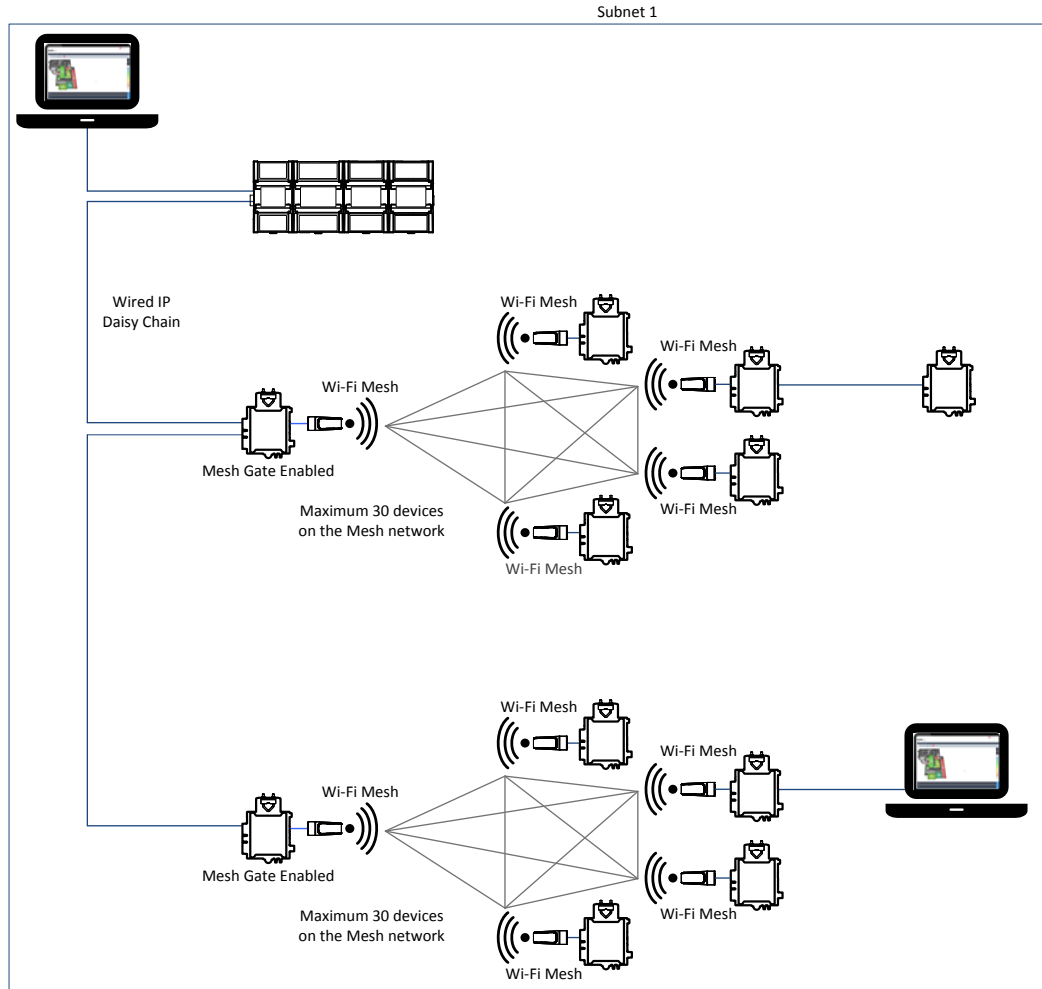


Figure 5-26: Mesh Configuration

CHAPTER 6

FIRST TIME CONNECTION TO AN ECLYPSE CONTROLLER

This chapter describes how to get started with an ECLYPSE controller. This includes discovering the controller on the network using the *XpressNetwork* Utility and gaining access to the controller's configuration interfaces.

In This Chapter

Topic	Page
Connecting to the Controller	53
Ethernet Network Connection	54
Wi-Fi Network Connection	57
Configuring the Controller	58
Connecting to the Controller's Configuration Web Interface	60

Connecting to the Controller

When connecting to the controller for the first time, the goal is to gain access to the controller so that you can configure it to work in its future network environment. To do so, you must connect the controller to form a network.

An ECLYPSE Network Configuration Tool is available that allows you to discover all ECY Series controllers connected to an IP network's subnetwork and to perform a range of operations on many controllers at once: you can set each controller's Hostname and IP address, launch *EC-gfxProgram* to program the controller, or you can access the controller's Web interface. It is a software application that runs on a PC that is connected to the same subnetwork as the controllers. See the [ECLYPSE Network Configuration Tool User Guide](#) for more information.

ECY Series Controller configuration can also be made through the controller's configuration Web interface that is accessed through the ECLYPSE Network Configuration Tool. This Web interface is used to set all the controller's configuration parameters including the controller's IP address according to your network planning. See [ECLYPSE Web Interface](#) on page 67.

There are two networking methods connect to a controller:

- Wired (Ethernet connection) with a PC. See Ethernet Network Connection on page 54.
- Wireless (when the ECLYPSE Wi-Fi Adapter is connected to the controller) with a PC. See [Wi-Fi Network Connection](#) on page 57.

Once you have connected the controller(s) to a network, configure the controller. See [Configuring the Controller](#) on page 58.

Controller Identification

Controllers are uniquely identified on the network by their MAC address. This identifier is printed on a label located on the side of the controller and another is on the controller's box. Get a printed copy of the building's floor plan. During controller installation, peel the MAC address sticker off of the controller's box and put it on the floor plan where the controller has been installed.

This MAC address is used as part of the controller's factory-default Wi-Fi access point name and its hostname.

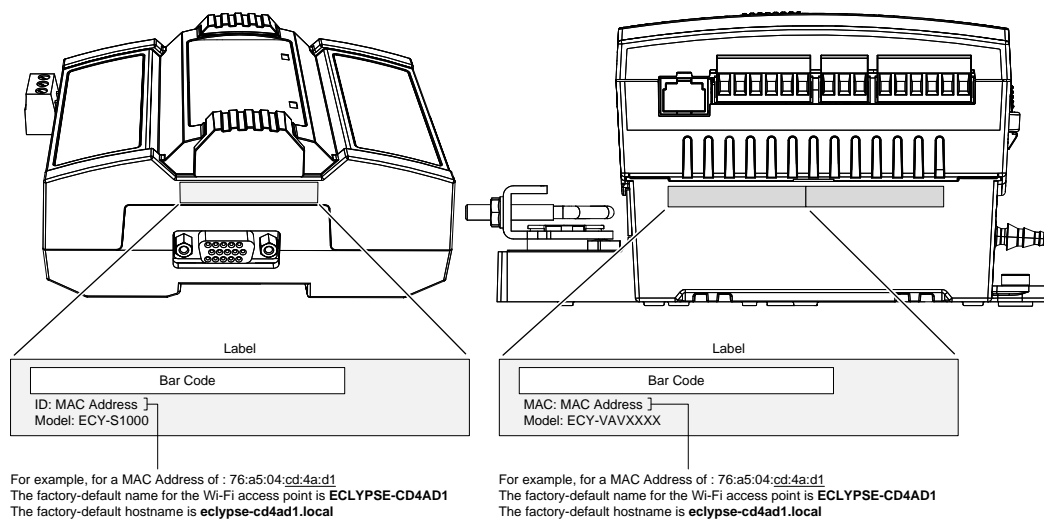


Figure 6-1: Finding the Controller's MAC Address

Ethernet Network Connection

Depending on the controller model, the way the controller is connected to the network will change according to whether the controller is a Power over Ethernet (PoE) model or not.

- For non-PoE controller models, see [Network Connections for ECY-VAV and ECY-S1000 Model Controllers](#) on page 54.
- For the ECY-VAV-PoE controller, see [Network Connections for ECY-VAV-PoE Model Controllers](#) on page 55.

See also [Connecting IP Devices to an IP Network](#) for network wiring considerations on page 31.

Network Connections for ECY-VAV and ECY-S1000 Model Controllers

Connect the controller to the network as follows:

1. Connect your PC's network card to the controller's **PRI** Ethernet port using a Category 5e Ethernet cable.

If you are commissioning more than one controller, connect the controllers and PC to a network switch. Two or more controllers can be connected to the network by daisy-chaining them together by using Cat 5e network Cables to connect the **Ethernet Switch Sec(ondary)** connector of one controller to the **Ethernet Switch Pri(mary)** connector of the next controller.

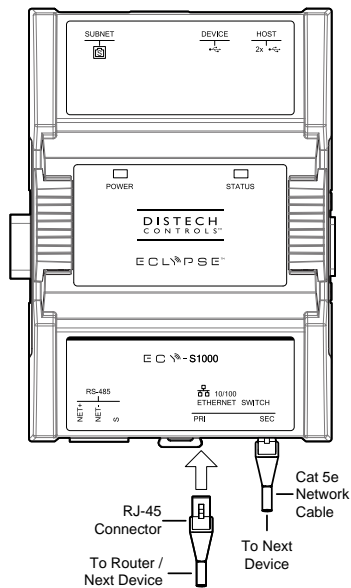


Figure 6-2: ECY-S1000 Wired Network Connection: Cat 5e Cables with RJ-45 Connectors are used

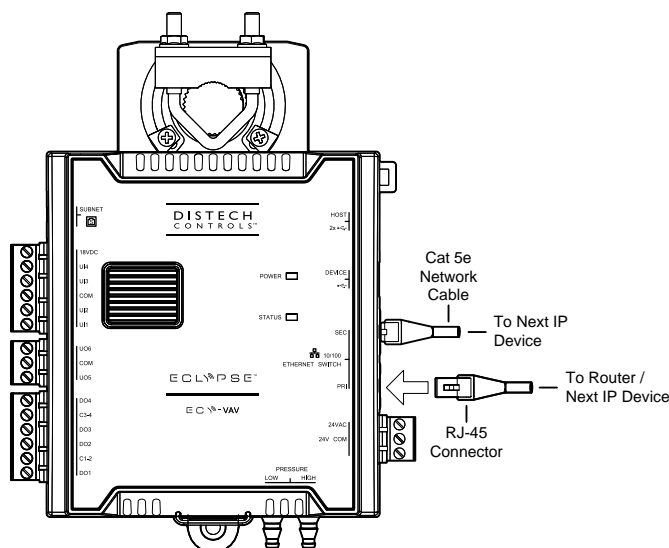


Figure 6-3: ECY-VAV Wired Network Connection: Cat 5e Cables with RJ-45 Connectors are used

2. Connect power to the controller(s). See the controller’s Hardware Installation Guide for how to do so.

Network Connections for ECY-VAV-PoE Model Controllers

The ECY-VAV-PoE controller is powered through the Ethernet network cable by using a technique called Power over Ethernet (PoE). A single network cable provides both data and power to the controller.

The ECY-VAV-PoE Controller must be used with an **IEEE 802.3at** type 2 certified network switch that can supply 25.5 W at the powered device. Each of the switch’s ports must be configured for static (hardware) power negotiation (that is, Data Link Layer Classification is not supported).

Connect your PC’s network card to the network PoE switch using a Category 5e Ethernet cable as shown in [Figure 6-4](#) and then connect the controller to the network PoE switch.

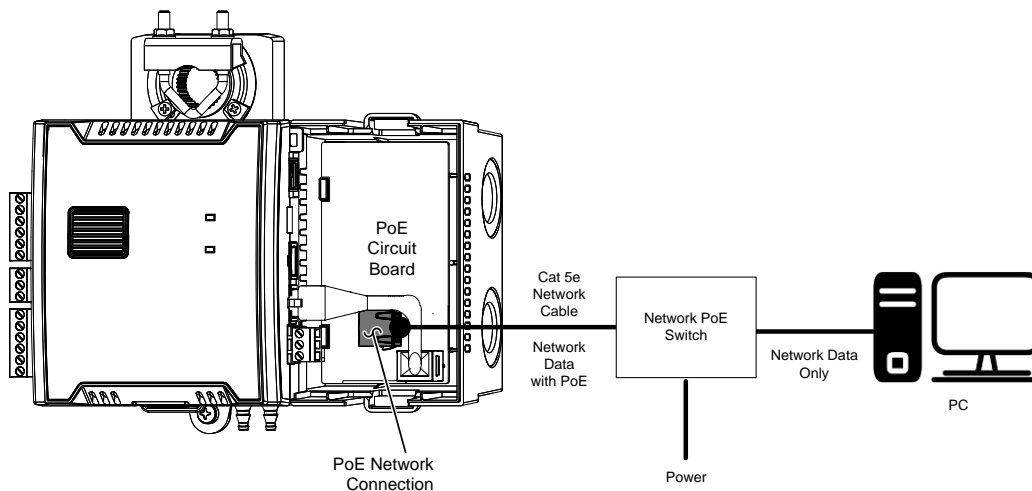


Figure 6-4: ECY-VAV-PoE Wired Network Connection: Cat 5e Cables with RJ-45 Connectors are used

The network connection to each PoE controller must go straight to the network PoE switch. Daisy-chaining controllers is not permitted.

First Time Connection to an ECLYPSE Controller

To remove power from an ECY-VAV-PoE controller, disconnect the “*PoE Network Connection*” shown in [Figure 6-4](#).

Wi-Fi Network Connection

Once the ECLYPSE Wi-Fi Adapter has been connected to a powered controller, a Wi-Fi hotspot becomes available that allows you to connect to the controller's configuration Web interface with your PC.

On your PC's wireless networks, look for an access point named **ECLYPSE-XXYYZZ** where **XXYYZZ** are the last 6 hexadecimal characters of the controller's MAC address. To find the controller's MAC address, see [Controller Identification](#) on page 53. The default password for the wireless network is: **eclipse1234**

Either of the controller's two USB HOST ports can be used to connect the wireless adapter.

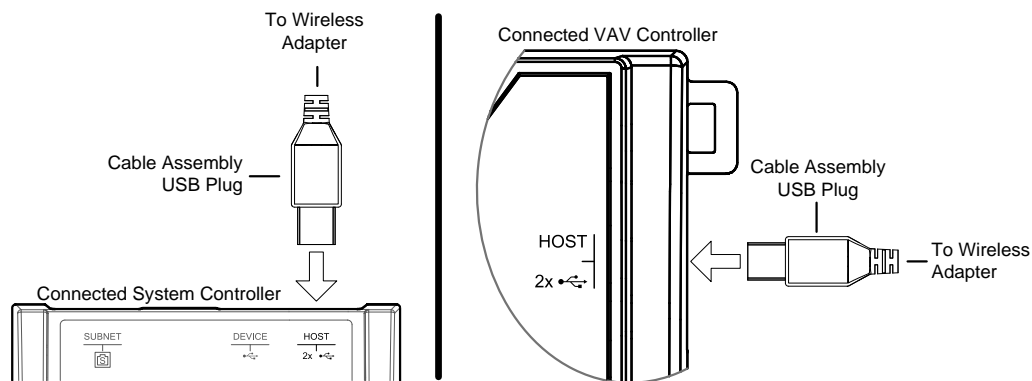


Figure 6-5: Connecting the Wireless Adapter to the Controller's USB HOST Port

Configuring the Controller

Any of the following methods can be used to connect to the controller's interface in order to configure it:

- Using the XpressNetwork Utility
- Using the controller's factory-default Hostname in the Web browser
- Using the controller's IP address in the Web browser

Using the XpressNetwork Utility

The XpressNetwork Utility is a software application that runs on a PC that allows you to discover all ECY Series controllers connected to an IP network's subnetwork or Wi-Fi network and to perform a range of operations on many controllers at once: you can set each controller's Hostname and IP address, launch EC-gfxProgram to program the controller, or you can access the controller's configuration Web interface. See the [XpressNetwork Utility User Guide](#) for more information.

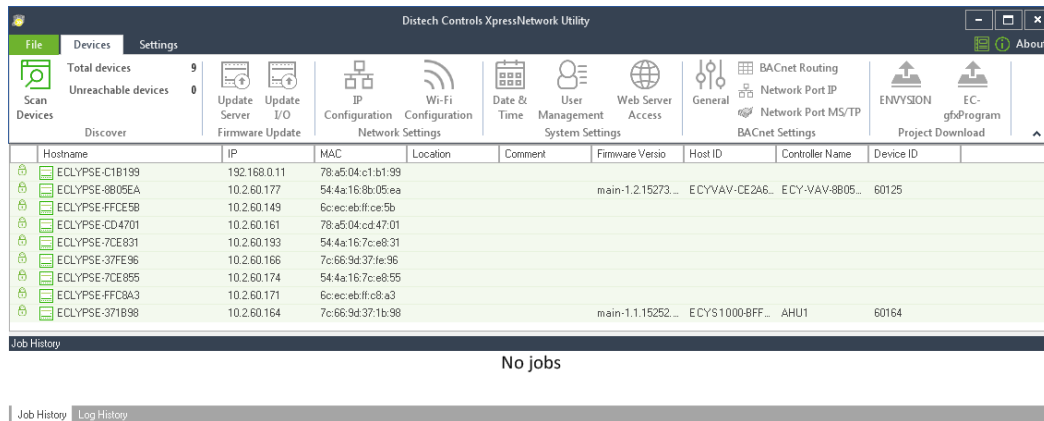


Figure 6-6: ECLYPSE Network Configuration Tool Discovers the Network-Connected Controllers

Using the Controller's Factory-default Hostname in the Web Browser

Controllers have a factory-default hostname that you can use instead of an IP address to connect to it¹. The hostname can be used in a Web browser's address bar or in the EC-gfxProgram's **Connect to** screen. When installing the latest version of EC-gfxProgram and your PC does not have the Bonjour service installed, a link to install the Bonjour service is provided. The Bonjour service must be installed on your PC to allow your PC to discover controllers by their hostname.

The controller's factory-default hostname is **eclipse-xxxxxx.local** where **xxxxxx** is the last 6 characters of the MAC address printed on a sticker located on the side of the controller. See Controller Identification on page 53.

For example, the sticker on the side of a controller shows that its MAC address is 76:a5:04:cd:4a:d1. Connect to the controller's Web interface as follows:

1. Open your Web browser.

¹ Not all smart phones / mobile devices have the Bonjour service installed and thus cannot use the hostname mechanism.

First Time Connection to an ECLYPSE Controller

2. In the Web browser's address bar, type **eclipse-cd4ad1.local** and click go.
3. Login to the controller. Then set the controller's configuration parameters in the controller's configuration Web interface. See Connecting to the Controller's Configuration Web Interface on page 60.

The Hostname can be changed in the System Settings on page 91.

Using the Controller's IP Address in the Web Browser

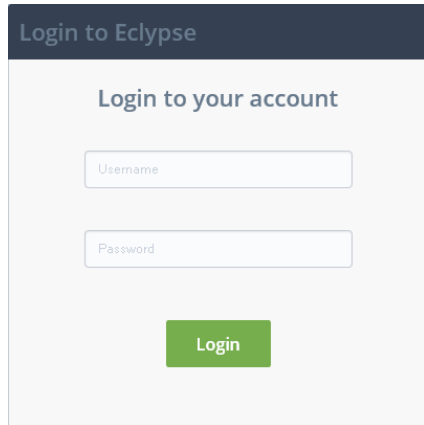
Connect to a controller through its IP address as follows:

- **For a Wi-Fi Network Connection:**
 1. Open your Web browser.
 2. In the Web browser's address bar, type **192.168.0.1** (the controller's factory-default wireless hotspot IP address) and click go.
 3. Login to the controller. Then set the controller's configuration parameters in the controller's configuration Web interface. See Connecting to the Controller's Configuration Web Interface on page 60.
- **For an Ethernet Network Connection:** You must know the controller's current IP address (from the DHCP server for example).
 1. Open your Web browser.
 2. In the Web browser's address bar, enter the controller's IP address and click go.
 3. Login to the controller. Then set the controller's configuration parameters in the controller's configuration Web interface. See Connecting to the Controller's Configuration Web Interface on page 60.

Connecting to the Controller's Configuration Web Interface

The ECLYPSE Series Controller configuration can be made through the controller's configuration Web interface to set all the controller's configuration parameters including the controller's IP address according to your network planning.

Once connected to the controller, you must login to the configuration Web interface.



The controller's configuration Web interface default Username is **admin** and password is **admin**. Click **Login**.

Next Steps

In Network Settings, configure the controller's network parameters so that they are compatible with your network. See [ECLYPSE Web Interface](#) on page 67.

It is important to create new user accounts with strong passwords to protect the controller from unauthorized access. Remove the factory default account admin / admin as this is a commonly known security breach. See [User Management](#) on page 85 and [Supported RADIUS Server Architectures](#) on page 61 .

CHAPTER 7

SUPPORTED RADIUS SERVER ARCHITECTURES

A RADIUS server is used to centralize user credentials (controller login username / password) across all devices. This chapter describes the supported RADIUS server architectures and how to configure a RADIUS server in EC-Net^{AX} or in an ECLYPSE controller.

In This Chapter

Topic	Page
Overview	62
RADIUS Server Architectures	63

Overview

When network connectivity allows, an EC-*gfx*Program user can connect directly to an ECLYPSE controller or a user can connect to the ECLYPSE controller through an EC-Net^{AX} station. No matter the connection method, a user has to authenticate themselves with their user credential (controller login username / password combination). Credentials can be held separately in each device (ECLYPSE controller / EC-Net^{AX} station), though this is not recommended as maintaining user credentials among multiple devices is more labor intensive.

Under such circumstances, the preferred method is to centralize user credentials in a RADIUS server on one device or server. When a user connects to an ECLYPSE controller, the ECLYPSE controller connects to the remote RADIUS server to authenticate the user's credential. A RADIUS server uses a challenge/response mechanism to authenticate a user's logon credentials. An unrecognized username or a valid username with an invalid password receive an 'access denied' response. A remote RADIUS server can be another ECLYPSE controller, or a suitably-configured EC-Net^{AX} / EC-BOS^{AX} station.

Authentication Fallback

Should the connection to the remote RADIUS server be temporarily lost, ECLYPSE controllers have a fall back authentication mode: users that have already authenticated themselves with the remote RADIUS server and then the connection to the RADIUS server is lost, these users will still be able to login to the controller as their successfully authenticated credentials are locally cached.



The user profile cache is updated when the user authenticates themselves while there is a working RADIUS server connection. For this reason, at a minimum, admin users should log in to each ECLYPSE controller at least once so their login can be cached on that controller. Otherwise, if there is a RADIUS server connectivity issue and a user who has never before connected to the ECLYPSE controller will be locked out from the controller. It is particularly important for admin user credentials to be cached on each controller as an admin user can change the controller's network connection parameters that may be at cause for the loss of connectivity to the RADIUS server.

RADIUS Server Architectures

Local Credential Authentication

Each device has its own credential database in the local credential authentication architecture. This approach is labor-intensive as multiple credential database instances must be maintained.

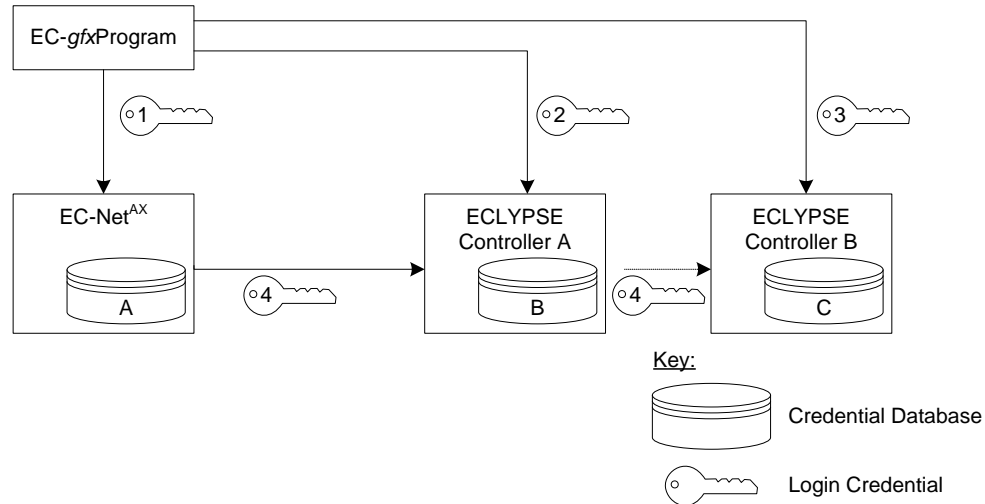


Figure 7-1: Local Credential Authentication

This authentication method has the following components.

Component	Description
Login Credential 1	This is the login credential used by an EC-gfxProgram user to connect to the EC-Net ^{AX} station. This credential is managed in the EC-Net ^{AX} User Service.
Login Credential 2	This is the login credential used by an EC-gfxProgram user to connect to ECLYPSE controller A. This credential is managed in controller's A User Management credential database.
Login Credential 3	This is the login credential used by an EC-gfxProgram user to connect to ECLYPSE controller B. This credential is managed in controller's B User Management credential database.
Login Credential 4	This is the login credential used by the EC-Net ^{AX} station's RestService to connect to ECLYPSE controller A and B. To program an ECLYPSE controller with EC-gfxProgram through EC-Net ^{AX} , the RestService must be configured on the EC-Net ^{AX} station with a login credential to all ECLYPSE controllers. This credential is managed in this controller's A and B User Management credential databases.
Credential Database A	This is the EC-Net ^{AX} station UserService credential database.

Supported RADIUS Server Architectures

Component	Description
Credential Database B and C	This is the ECLYPSE controller A's credential database and ECLYPSE controller B's credential database. If EC- <i>gfx</i> Program users are to connect to either of these controllers through the EC-Net ^{AX} station, the controller's credential database must have the credentials for EC-Net ^{AX} station's RestService. Each credential database must also have the credentials for each user that will login to ECLYPSE controller A (for example, administrators, direct connection EC- <i>gfx</i> Program users, ENVYISION users, etc.). See User Management on page 85.

ECLYPSE-Based Centralized Credential Authentication

The credential database is centralized in an ECLYPSE controller that is configured as a RADIUS server, to authenticate login requests made directly to it, and by other subscribed ECLYPSE controllers. This architecture is ideal when you are not using EC-Net^{AX} on your network.

⚠ EC-Net^{AX} cannot subscribe to a remote RADIUS server. Due to this, you will have to add user credentials to both the ECLYPSE RADIUS server and to the EC-Net^{AX} station. For this reason, if you are using EC-Net^{AX} on your network, it is best to centralize credential authentication by using this EC-Net^{AX} station as a RADIUS server. See [EC-NetAX-Based Centralized Credential Authentication](#) on page 65.

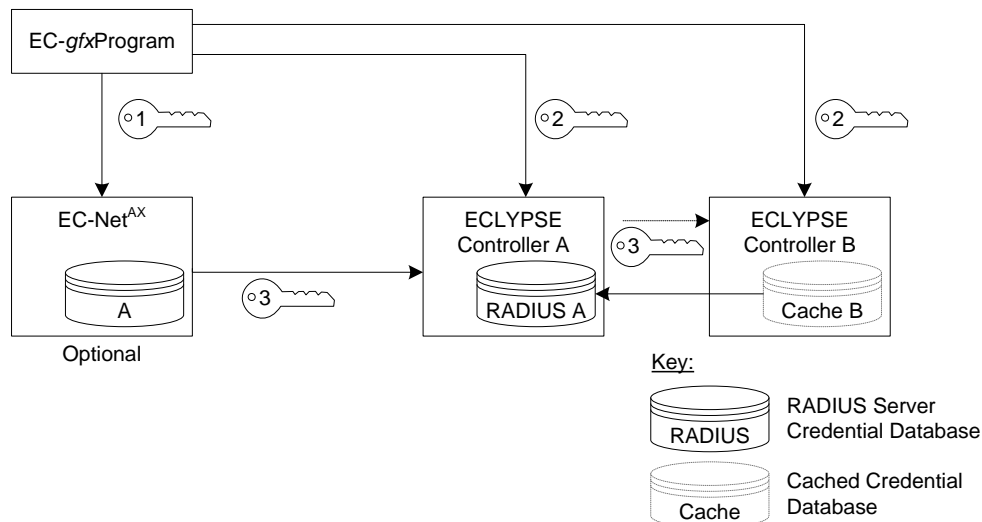


Figure 7-2: ECLYPSE-Based Centralized Credential Authentication

This authentication method has the following components.

Component	Description
Login Credential 1	This is the login credential used by an EC- <i>gfx</i> Program user to connect to the EC-Net ^{AX} station. This credential is managed in the EC-Net ^{AX} User Service.
Login Credential 2	This is the login credential used by an EC- <i>gfx</i> Program user to connect to any ECLYPSE controller. This credential is managed in this ECLYPSE controller A's User Management RADIUS server credential database.

Component	Description
Login Credential 3	This is the login credential used by the EC-Net ^{AX} station's RestService to connect to any ECLYPSE controller. To program an ECLYPSE controller with EC-gfxProgram through EC-Net ^{AX} , the RestService must be configured on the EC-Net ^{AX} station with a login credential to all ECLYPSE controllers. This credential is managed in this ECLYPSE controller A's User Management RADIUS server credential database.
Credential Database A	This is the EC-Net ^{AX} station UserService credential database. This credential database is independent of all other credential databases.
RADIUS Server A Credential Database	This is the ECLYPSE controller A's RADIUS Server credential database. If EC-gfxProgram users are to connect to this controller through the EC-Net ^{AX} station, this credential database must have the credentials for EC-Net ^{AX} station's RestService. This credential database must also have the credentials for each user that will login to any ECLYPSE controller (for example, administrators, direct connection EC-gfxProgram users, ENVYSION users, etc.). See User Management on page 85.
Credential Database Cache B	This is the ECLYPSE controller B's cached credential database. If the connection to ECLYPSE controller A's RADIUS Server is lost, users that have previously authenticated themselves with the ECLYPSE controller A's RADIUS Server credential database on a given controller will still be able to login to those controllers as their credentials are locally cached.

EC-Net^{AX}-Based Centralized Credential Authentication

The credential database is centralized in an EC-Net^{AX} station to authenticate login requests made by all other subscribed ECLYPSE controllers.

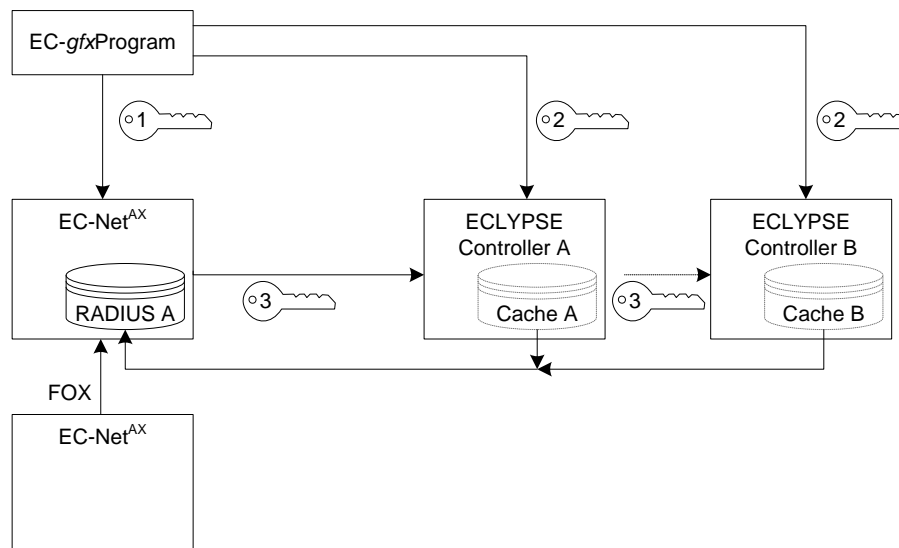


Figure 7-3: EC-Net^{AX}-Based Centralized Credential Authentication

This authentication method has the following components.

Component	Description
Login Credential 1	This is the login credential used by an EC-gfxProgram user to connect to the EC-Net ^{AX} station. This credential is managed in the EC-Net ^{AX} User Service.

Supported RADIUS Server Architectures

Component	Description
Login Credential 2	This is the login credential used by an EC- <i>gfx</i> Program user to connect to any ECLYPSE controller. This credential is managed in the EC-Net ^{AX} User Service.
Login Credential 3	This is the login credential used by the EC-Net ^{AX} station's RestService to connect to any ECLYPSE controller. To program an ECLYPSE controller with EC- <i>gfx</i> Program through EC-Net ^{AX} , the RestService must be configured on the EC-Net ^{AX} station with a login credential to all ECLYPSE controllers. This credential is managed in the EC-Net ^{AX} User Service.
RADIUS Server A Credential Database	This is EC-Net ^{AX} station UserService credential database that is also a RADIUS Server credential database. If EC- <i>gfx</i> Program users are to connect to this controller through the EC-Net ^{AX} station, this credential database must have the credentials for EC-Net ^{AX} station's RestService. This credential database must also have the credentials for each user that will login to ECLYPSE controller A or B (for example, administrators, direct connection EC- <i>gfx</i> Program users, ENVYSION users, etc.). Note that other EC-Net ^{AX} stations can use FOX protocol to authenticate users on those stations.
Credential Cache A and B Databases	These are ECLYPSE controllers' cached credential databases. If the connection to the EC-Net ^{AX} station's RADIUS Server is lost, users that have previously authenticated themselves with EC-Net ^{AX} station's RADIUS Server credential database on a given controller will still be able to login to those controllers as their credentials are locally cached.

Configuring the EC-Net^{AX} Station's RestService

To configure the REST service in EC-Net^{AX}, refer to the [EC-*gfx*Program User Guide: Getting Started on EC-Net^{AX} for ECB & ECY Series Controllers](#). Any ECLYPSE controller being connected to by the RestService must be able to authenticate the User name and password configured in the RestService configuration.

The screenshot shows the configuration page for the RestService. The title is "RestService (Rest Service)". The settings are as follows:

- Status: {ok}
- Fault Cause: (empty)
- Enabled: true
- Servlet Name: api
- Version: 1.0
- User Name: Rest67service
- Password: (masked with dots)
- Http Port: 80
- Https Port: 443
- Https Enabled: true
- Socket Timeout: 20000 ms [0 - max]
- Connection Timeout: 2000 ms [0 - max]
- Nb Rest Devices: 1
- Nb Rest Devices Poll Ok: 1
- Polling Devices: true

Figure 7-4: Typical RestService Configuration

CHAPTER 8

ECLYPSE WEB INTERFACE

This chapter describes the ECLYPSE controller's Web interface.

In This Chapter

Topic	Page
Overview	68
Web Configuration Interface	70
Network Settings	72
BACnet Settings	77
Firmware Update	84
User Management	85
Device Information	90
System Settings	91
Viewer Information	95

Overview

The ECLYPSE controller has a web-based interface that allows you to view system status, configure the controller, and update the controller’s firmware. Your current login username is shown in the top-right corner.



Figure 8-1: ECLYPSE Controller’s Web Interface Welcome Home Page

Option	Description	See
ENVYSION	Embedded graphic design and visualization interface. Host system-based graphics such as Air Handling Units, Boiler Room, and more, directly from the controller.	ENVYSION User Guide
Web Configuration Interface	View and set the controller’s configuration settings including its IP address, Wi-Fi settings, and to update the controller’s firmware.	Web Configuration Interface on page 70.

Login Credentials

The default user and password are:

- user: admin
- password: admin

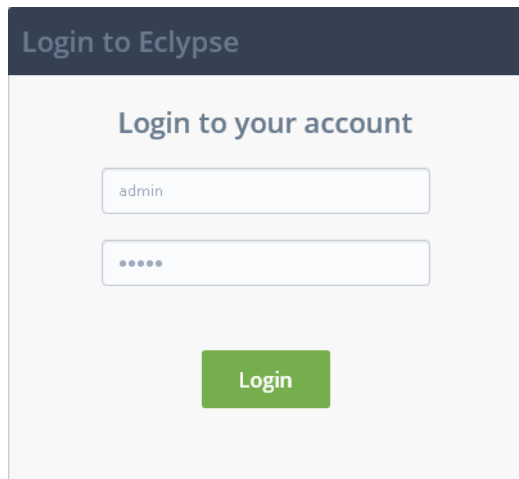


Figure 8-2: ECLYPSE Web Configuration Interface Login

It is important to create new user accounts with strong passwords to protect the controller from unauthorized access. Remove the factory default account admin / admin as this is a commonly known security breach. See [User Management](#) on page 85 and [Supported RADIUS Server Architectures](#) on page 61.

Web Configuration Interface

This allows you to view and set the controller’s configuration settings including its IP address, Wi-Fi settings, and to update the controller’s firmware. These configuration parameters are password protected.

Main Screen

The ECLYPSE controller’s network interface and wireless configuration parameters are configured through this web interface.

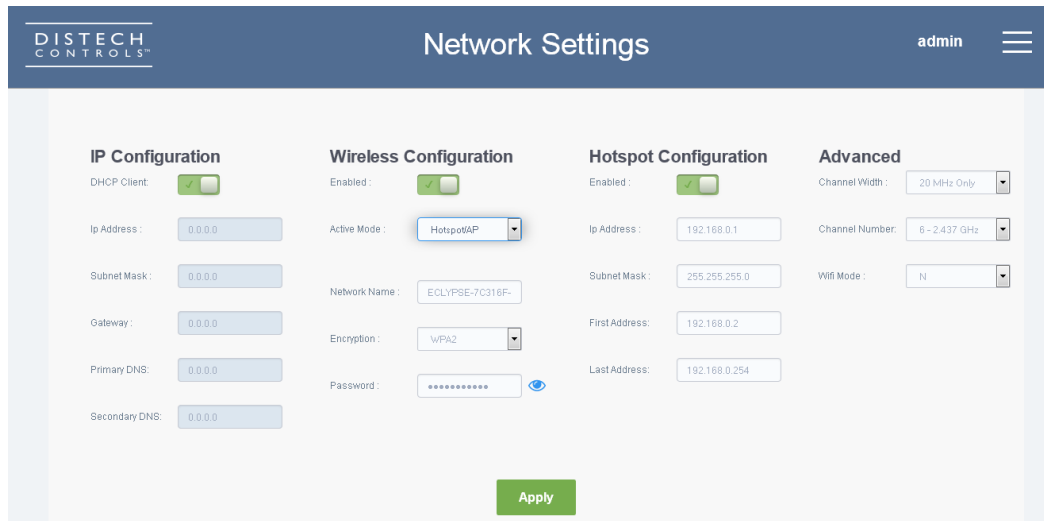


Figure 8-3: Network Settings

Certain settings are enabled and disabled as follows.

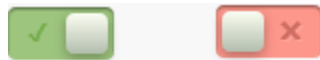


Figure 8-4: Setting Enabled on Left and Disabled on Right

Menu Button

In the upper right corner is the menu button.



Figure 8-5: The Menu Button

The menu button displays the following menus:

Item	Description	See
Network Settings	This is where wired and wireless network configuration parameters are set.	Network Settings on page 72
BACnet Settings	This is where the BACnet interface parameters are set.	BACnet Settings on page 77
Firmware Update	This allows you to update the controller’s or IO Module’s firmware by uploading a ZIP or DFF file to the controller.	Firmware Update on page 84

Item	Description	See
User Management	This is where the user access rights are set.	User Management on page 85
Device Information	This provides information about the device and its network connection.	Device Information on page 90
System Settings	This is where you set the controller's interface port numbers and the security certificate for the controller's secure interface.	System Settings on page 91
Viewer Information	When a user logs in, the landing page shown to each individual user can be set.	Viewer Information on page 95
Home	This takes you to the ECLYPSE controller's configuration interface welcome page.	Overview on page 68
Logout	This logs you out of your session. It takes you to the login screen.	Login Credentials on page 69

Network Settings

This is where wired and wireless network configuration parameters are set.

The screenshot shows a web interface with four main configuration sections:

- IP Configuration:** Includes fields for DHCP Client (checked), IP Address (0.0.0.0), Subnet Mask (0.0.0.0), Gateway (0.0.0.0), Primary DNS (0.0.0.0), and Secondary DNS (0.0.0.0).
- Wireless Configuration:** Includes Enabled (checked), Active Mode (HotspotAP), Network Name (ECLYPSE-7C316F-), Encryption (WPA2), and Password (masked).
- Hotspot Configuration:** Includes Enabled (checked), IP Address (192.168.0.1), Subnet Mask (255.255.255.0), First Address (192.168.0.2), and Last Address (192.168.0.254).
- Advanced:** Includes Channel Width (20 MHz Only), Channel Number (6 - 2.437 GHz), and Wifi Mode (N).

Figure 8-6: Network Settings

The following configuration options are available.

Item	See
IP Configuration	IP Configuration on page 72
Wireless Configuration	Wireless on page 73
Hotspot Configuration	Hotspot Configuration on page 75
Advanced	Advanced on page 75

IP Configuration

This configuration interface is for any wired IP connections that are made through either one of the controller's **Ethernet Switch Pri**(mary) connector or **Ethernet Switch Sec**(ondary) connector. See [Figure 6-2](#) and [Figure 6-3](#). The Wired IP parameters can be auto-configured when the connected network has a working DHCP server. The alternative is to manually configure the controller's IP parameters.

Option	DHCP Client: Enabled	DHCP Client: Disabled
DHCP Client	If the controller is connected to a network that has an active DHCP server, enabling this option will automatically configure the Wired IP connection parameters. The Wired IP parameters shown below are read only (presented for information purposes only).	If you want to manually configure the controller's network settings (to have a fixed IP address for example) or in the case where the network does not have a DHCP server, disable this option. In this case, you must set the Wired IP connection parameters shown below to establish network connectivity. See also DHCP versus Manual Network Settings on page 19.
IP Address	This is the IP Address provided by the network's DHCP server.	Set the IP address for this network device. See IPv4 Communication Fundamentals on page 18. Ensure that this address is unique from all other device on the LAN including any used for a hot spot's IP addressing.
Subnet Mask	This is the subnet mask provided by the network's DHCP server.	Set the connected network's subnetwork mask. See About the Subnetwork Mask on page 20.

Option	DHCP Client: Enabled	DHCP Client: Disabled
Gateway	This is the gateway IP Address provided by the network's DHCP server.	The IP address of the default gateway to other networks. This is usually the IP address of the connected network router. See Default Gateway on page 21.
Primary DNS Secondary DNS	This is the primary and secondary DNS IP Address provided by the network's DHCP server.	The connected network's primary and secondary IP address of the DNS servers. See Domain Name System (DNS) on page 22.

Wireless Configuration

- This configuration interface is for any ECLYPSE Wi-Fi Adapter connected to the **HOST** connector.





A hotspot creates a subnetwork. As a result, any connected BACnet device will not be able to discover BACnet devices on any other LAN subnetwork.

The Wireless connection parameters can be set as follows.

Item	Description
Enabled	This enables/disables the controller's wireless features.
Active Mode	<p>This sets the Wi-Fi network operating mode.</p> <ul style="list-style-type: none"> When Active Mode is set to Client, this connects the controller as a client of a Wi-Fi access point. See Setting up a Wi-Fi Client Wireless Network on page 97 for how to configure this mode. When Active Mode is set to Hotspot/AP and Hotspot Configuration is set to Enabled, this creates a Wi-Fi hotspot with a router. See Setting up a Wi-Fi Hotspot Wireless Network on page 99 for how to configure this mode. When Active Mode is set to Hotspot/AP and Hotspot Configuration is set to Disabled, this creates a Wi-Fi access point. See Setting up a Wi-Fi Access Point Wireless Network on page 98 for how to configure this mode. When Active Mode is set to Mesh, this connects the controller to a mesh network. See Setting up a Wi-Fi Mesh Wireless Network on page 101 for how to configure this mode. This feature is only available to Beta clients. <p>See also ECLYPSE Wi-Fi Adapter Connection Modes on page 44.</p>
Mesh Gate (available when Active Mode is set to Mesh only)	Set this option when this controller has direct access to another non-mesh network segment through a wired Ethernet connection that acts as a primary network interconnect. This increases the data rate between mesh network nodes and other network segments. When this option is enabled, this mesh node will broadcast to the other mesh nodes at regular intervals that this mesh node has the shortest path to other networks. Only one or two mesh network nodes should have this option set as these broadcasts use wireless network bandwidth.

ECLYPSE Web Interface

Item	Description
Network Name	<p>The network name is the Service Set IDentification (SSID) for a Wi-Fi hotspot. When this controller's active mode is configured as a:</p> <ul style="list-style-type: none"> • Hotspot: set a descriptive network name that other wireless clients will use to find this hotspot. • Client: select an available hotspot from the lists of access point connections that are within range. • Mesh network: set a network name for the mesh network. All mesh network nodes use the same network name to become a member of that mesh network. <p>This parameter is case sensitive.</p>
	<p>When the Active Mode is set to Client, click this icon to select an available Wi-Fi network from the list of access points that are within range.</p>
Encryption	<p>Set the encryption method to be used by the Wi-Fi network:</p> <ul style="list-style-type: none"> • None: this option should be avoided as it does not provide any wireless security which allows any wireless client to access the LAN. • AuthSAE: choose the Simultaneous Authentication of Equals (SAE) option to secure a mesh network with a password. • WPA2: select the Wi-Fi Protected Access II option to secure the Wi-Fi network with a password. • WPA2 Enterprise: Use this option if you are connecting to an enterprise network that has a working RADIUS authentication server. This RADIUS server provides user authentication.
Password	<p>When encryption is used, set the password to access the Wi-Fi network as a client or the password other clients will use to access this hotspot. Passwords should be a long series of random alphanumeric characters and symbols that are hard to guess. This parameter is case sensitive.</p>
	<p>Click to show or hide the password.</p>

Hotspot Configuration

When a wireless network type (**Active Mode**) is configured as a **Hotspot/AP**, this configuration interface sets the wireless network's mode (hotspot mode or access point mode) and corresponding network parameters.



Item	Description
Enabled	<p>This sets the wireless network's mode.</p> <ul style="list-style-type: none"> When Active Mode is set to Hotspot/AP and Hotspot Configuration is set to Enabled, this creates a Wi-Fi hotspot with a router. This creates a separate subnet that has its own IP address range. Any connected BACnet device will not be able to discover BACnet devices on any other LAN subnetwork. The parameters shown below will have to be configured. When Active Mode is set to Hotspot/AP and Hotspot Configuration is set to Disabled, this creates a Wi-Fi access point. This is an extension of the wired IP network. The parameters shown below do not have to be configured. <p>See ECLYPSE Wi-Fi Adapter Connection Modes on page 44.</p>
IP Address	<p>This is the IP address for this hotspot (or gateway address that wireless clients will connect to). Ensure that this address is:</p> <ul style="list-style-type: none"> Not in the range of IP address set by First Address and Last Address. Not the same as the IP address set under IP Configuration for the wired network.
Subnet Mask	<p>The hotspot's subnetwork mask. See About the Subnetwork Mask on page 20.</p>
First Address Last Address	<p>This defines the range of IP addresses to be made available for hotspot clients to use. The narrower the range, the fewer hotspot clients will be able to connect due to the lack of available IP addresses. For example, a range where First Address = 192.168.0.22 and Last Address = 192.168.0.26 will allow a maximum of 5 clients to connect to the hotspot on a first-to-connect basis.</p>

Advanced

When a Wi-Fi hotspot or access point is configured, this sets the channel width and number the hotspot is to use. The wireless mode can also be set.

Item	Description
Channel Width	<p>This sets the amount of radio spectrum bandwidth to use for data transmission. 20 MHz Only option allows for a throughput of up to 150 MB/s. 40 MHz Only option allows for a throughput of up to 300 MB/s. Beware that the 40 MHz Only option leaves little spectrum for other Wi-Fi networks even if they are operating on another channel number and should be avoided if other Wi-Fi networks are nearby to avoid interference and network drop-outs. See also About the 2.4 GHz ISM band on page 37.</p>

ECLYPSE Web Interface

Item	Description
Channel Number	<p data-bbox="565 184 1373 300">This sets the center frequency of the transmission. If there are other Wi-Fi networks are nearby, configure each Wi-Fi network to use different channel numbers to reduce interference and network drop-outs.</p> <p data-bbox="565 310 1373 373"> The range of available channels may vary from country to country.</p>
Wi-Fi Mode	<p data-bbox="565 384 1373 478">This sets the wireless mode (wireless G or wireless N). Wireless N mode is backwards compatible with wireless G and B. Wireless G mode is backwards compatible with wireless B.</p> <p data-bbox="565 489 1373 510">A mesh network uses the wireless N mode.</p>
Diagnostics	<p data-bbox="565 520 1373 615">This shows the currently connected neighboring mesh network controllers and the corresponding connection receive signal strength and data rate.</p> <p data-bbox="565 625 1373 720">This information is used to troubleshoot a mesh network. It is best that a controller has at least two mesh network neighbors with a receive signal strength stronger than -70 dBm.</p> <p data-bbox="565 730 1373 867"> Signal strength is measured in negative units where the stronger the signal, the closer it is to zero. A weaker signal strength will have a more negative number. For example, a receive signal strength of -35 dBm is much stronger than a receive signal strength of -70 dBm.</p>

BACnet Settings

This is where the BACnet interface parameters are set.

General

This sets the controller's BACnet network parameters.

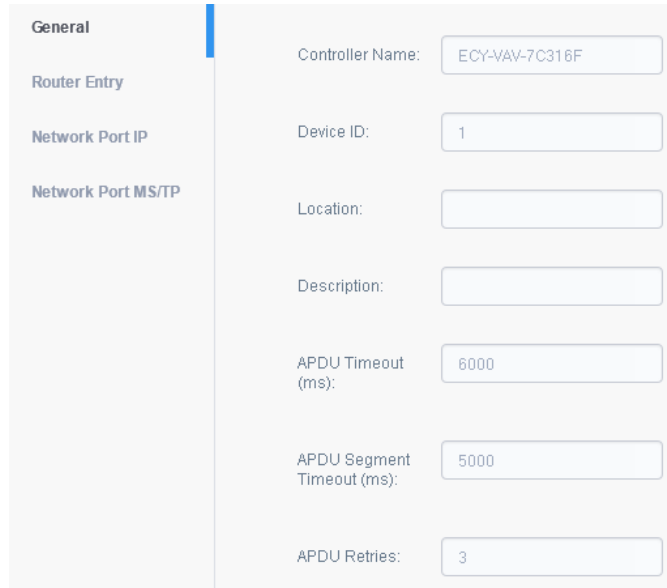


Figure 8-7: General BACnet Settings

Item	Description
Controller Name	Set a descriptive name by which this controller will be known to other BACnet objects.
Device ID	Each controller on a BACnet intra-network (the entire BACnet BAS network) must have a unique Device ID. Refer to the Network Guide for more information.
Location	The current controller's physical location. This is exposed on the BACnet network as a device object property.
Description	A description of the controllers function. This is exposed on the BACnet network as a device object property.
APDU Timeout	The maximum amount of time the controller will wait for an acknowledgement response following a confirmed request sent to a BACnet device before re-sending the request again or moving onto the next request. This property is exposed on the BACnet network as a device object property.
APDU Segment Timeout	The maximum amount of time the controller will wait for an acknowledgement response following a confirmed segmented request sent to a BACnet device before re-sending the segmented request again or moving onto the next request. This property is exposed on the BACnet network as a device object property.
APDU Retries	This sets the number of times to retry a confirmed request when no acknowledgement response has been received. This property is exposed on the BACnet network as a device object property.

ECLYPSE Web Interface

Routing

This enables the routing of BACnet packets between BACnet MS/TP controllers connected to the ECLYPSE Connected System Controller's RS-485 port and BACnet/IP controllers connected to the ECLYPSE Connected System Controller's Ethernet Switch ports. For example, routing must be enabled for EC-Net^{AX} to discover the BACnet MS/TP controllers connected to the ECLYPSE Connected System Controller's RS-485 port.

Enable Routing:

Routing Table

Network Number	Mac Address
1	172.16.254.1:47808

Apply

Figure 8-8: BACnet Routing Configuration

Network Port IP

This sets the IP network configuration parameters including BACnet Broadcast Management Device (BBMD) and Foreign Device for intranetwork connectivity.

Enable :

Network Number :

BACnet IP UDP Port :

Enable BBMD:

BACnet/IP Broadcast Management Device (BBMD)

Enable Foreign Devices:

Foreign Device

Figure 8-9: BACnet IP Configuration

Item	Description
Enabled	This enables/disables the routing of BACnet packets between BACnet MS/TP controllers connected to the ECLYPSE Connected System Controller's RS-485 port and BACnet/IP controllers connected to the ECLYPSE Connected System Controller's Ethernet Switch ports.
Network Number	A network number identifies a LAN for routing purposes. All controllers with the same network number are members of the same logical BACnet network. See Device Addressing on page 125.
BACnet IP UDP Port	This is the standard BACnet/IP port number (UDP 47808) used by BACnet devices to communicate.
Enable BBMD	BBMD allows broadcast message to pass through a router. See BBMD Settings on page 80. To enable this feature, set Enable BBMD on only one device on each subnet.

ECLYPSE Web Interface

Item	Description
Enable Foreign Devices	Foreign Device Registration allows a BACnet/IP device to send broadcast messages to a device with BBMD enabled. See Foreign Device Settings on page 81. To enable this feature, set Enable Foreign Devices on only one device on each subnet.

BBMD Settings

BACnet/IP devices send broadcast discovery messages such as “Who-Is” as a means to discover other BACnet devices on the network. However, when there are two or more BACnet/IP subnetworks, broadcast messages do not pass through network routers that separate these subnetworks.

BBMD allows broadcast message to pass through a router: on each subnet, a single device has BBMD enabled. Each BBMD device ensures BACnet/IP connectivity between subnets by forwarding broadcast messages found on its subnetwork to each other, and then onto the local subnetwork as a broadcast message.

In the BBMD table, add the BBMDs-enabled controllers of all other subnetworks.

BACnet/IP Broadcast Management Device (BBMD)

IP	Port	Mask
192.168.1.99	47808	255.255.255.255

ADD EDIT REMOVE

Figure 8-10: BBMD Settings

Item	Description
Add	Add another subnetwork’s BBMD to this controller’s a Broadcast Distribution Table.
Edit	Edit a BBMD’s information.
Remove	Remove a BBMD from this controller’s Broadcast Distribution Table.

Figure 8-11: Adding a BBMD

Item	Description
IP	The IP address of the BBMD located on the other subnetwork.
MASK	The subnetwork mask for the other subnetwork.
PORT	The port number for the BACnet service of the BBMD located on the other subnetwork.

Foreign Device Settings

Some BACnet/IP devices also support a feature called Foreign Device Registration (FDR). FDR allows a BACnet/IP device to send broadcast messages to a device with BBMD enabled. The BBMD-enabled device will then forward these broadcast messages to all other BBMDs and onto all other FDR devices. If a subnet has only FDR supported devices then it does not need a local BBMD. These devices can register directly with a BBMD on another subnetwork.

In the Foreign Device table, add the IP addresses for the controllers located on other subnetworks.

Figure 8-12: Foreign Device Settings

Item	Description
Add	Add the IP addresses for the controllers (foreign devices) located on other subnetworks.
Edit	Edit a foreign device's information.

ECLYPSE Web Interface

Remove	Remove a foreign device from this controller's Broadcast Distribution Table.
--------	--

Figure 8-13: Adding a Foreign Device

Item	Description
IP	The IP address of a controller (foreign device) located on another subnetwork.
PORT	The port number for the BACnet service of the controller located on the other subnetwork.
TTL	This is the delay after which the foreign device is forgotten.

Network Port MS/TP

This sets the MS/TP network configuration parameters.

Figure 8-14: BACnet MS/TP Configuration

Item	Description
Enabled	This enables/disables the controller's BACnet MS/TP connection. If the controller has been configured to use Modbus RTU, this option cannot be enabled. First disable Modbus RTU in EC-gfxProgram.

Item	Description
Network Number	A network number identifies a LAN for routing purposes. All controllers with the same network number are members of the same logical BACnet network. See Device Addressing on page 125.
Baud Rate	The recommended baud rate setting is 38 400. See Baud Rate on page 113.
Mac Address	The ECY series controller's MAC Address on the BACnet MS/TP Data Bus.
Max Master	When commissioning a BACnet MS/TP Data Bus, it is useful to start with the Max Master set to 127 so as to be able to discover all devices connected to the data bus. Then, once all devices have been discovered and the MAC Addressing is finalized by eliminating any gaps in the address range, set the Max Master (the highest MAC Address) to the highest Master device's MAC Address number to optimize the efficiency of the data bus. See Setting the Max Master and Max Info Frames on page 127.
Max Info Frames	For the ECY series controller, this should be set to 20. See Setting the Max Master and Max Info Frames on page 127.

Firmware Update

The controller's firmware can be updated through the Web Update file upload interface. The firmware can be uploaded for:

- The ECLYPSE series controller under the "Automation & Connectivity Server" icon.
- The ECY Series Controller's I/O modules under the "I/O Extension Modules" icon.

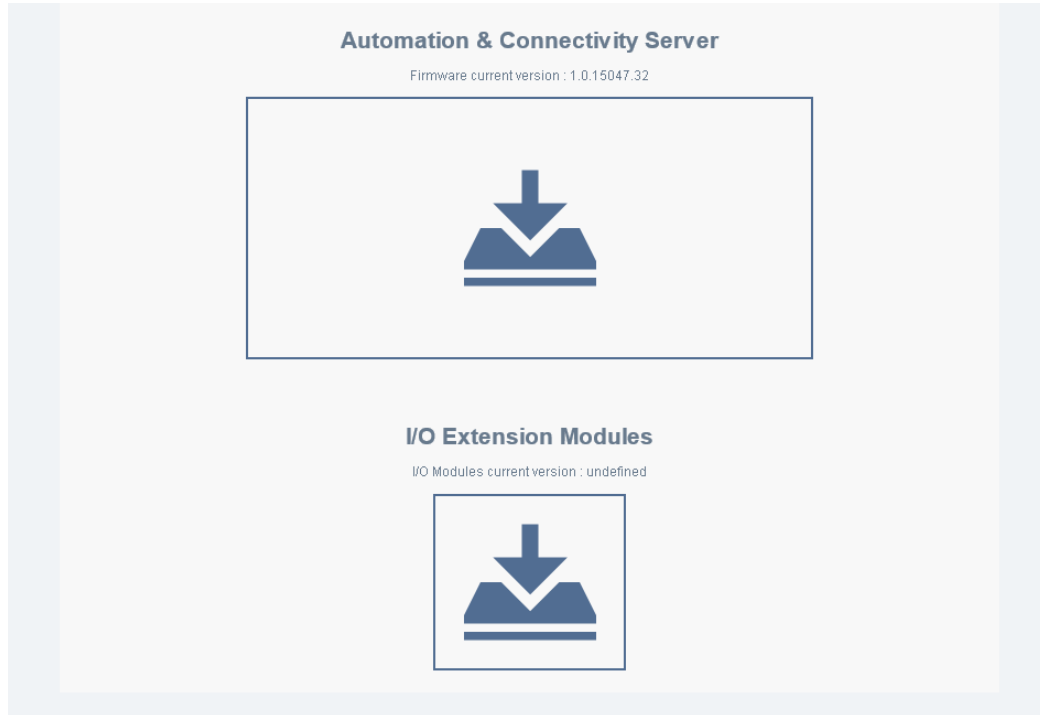


Figure 8-15: The Web Update File Upload Interface

The following firmware upload options are available.

Item	Description
Automation & Connectivity Server	Use this option to update the ECY series' firmware.
I/O Extension Modules	Use this option to update the Connected System Controller's I/O modules' firmware.

Two file upload methods are supported:

- Click the box to open the **File Upload** window. Find the firmware file on your PC and click **Open**.
- In Windows Explorer, find the firmware file on your PC and drag and drop it onto the firmware update icon.

The file upload starts and the firmware upgrade then starts. Once the upgrade is complete, the controller will reboot.



Do not remove power from the controller or interrupt the network connection to the controller during the firmware upgrade process. Failing to do so may render the controller unusable.

User Management

User management is the control of who can access the controller by enforcing the authentication credentials users need to access the controller. User management can either be locally managed or remotely managed. If there is more than one ECLYPSE controller on the network, it is best to centralize access management – see [Supported RADIUS Server Architectures](#) on page 61.

The screenshot displays the configuration page for a Local Radius Server. At the top, there is a dropdown menu for 'Authentication' set to 'Local'. Below this, the 'Local Radius Server' section includes input fields for 'Authentication Port' (1812) and 'Accounting Port' (1813). A 'Shared Key' field contains the text '5*@!sK<Ah4Ho%7.' with a 'Generate' button and a copy icon to its right. The 'Local User Management' section features a table with two columns: 'Username' and 'Roles'. The table lists three users: 'admin' with roles 'Admin,Rest', 'gfx' with role 'Rest', and 'admin1' with roles 'Admin,Operator,Viewer,Rest'. Below the table are three buttons: 'ADD', 'EDIT', and 'REMOVE'. At the bottom center of the form is a green 'Apply' button.

Authentication

The following user management schemes are available.

This is a close-up of the 'Authentication' dropdown menu. The text 'Authentication :' is followed by a box containing the word 'Local' and a downward-pointing arrow.

Figure 8-16: Authentication


Item	Description
Local	When Authentication is set to Local , credentials are added to and are managed by this controller. In this mode, this controller is also a RADIUS server that other controllers can use to authenticate user access to those controllers. See Local RADIUS Server on page 86.
Proxy	When Authentication is set to Proxy , credentials are managed by a remote RADIUS server on the network. See Remote RADIUS Server on page 88.

Local RADIUS Server

When **Authentication** is set to **Local**, the following configuration parameters are available.

This controller can be used as a RADIUS server by other controllers on the network. In this scenario, the other controllers must be configured to use the **Remote RADIUS server** mode with this controller's IP address. This centralizes access management on this controller thereby saving time by eliminating the need to add users to each controller individually. Set the port numbers and shared key that other controllers will use to connect to this controller. See [Supported RADIUS Server Architectures](#) on page 61.

The port values of 1812 for authentication and 1813 for accounting are RADIUS standard port numbers. However, other port numbers may be used. No matter which port numbers are used, make sure that the port numbers are unused by other services on this controller and that both the RADIUS server and the RADIUS clients use the same port number values. See also [ECLYPSE IP Network Port Numbers and Protocols](#) on page 28.

Item	Description
Authentication Port	The RADIUS server authentication port number.
Accounting Port	The RADIUS server accounting port number.
Shared Key	This is an encryption key that devices use to encrypt and decrypt user authentication credentials that are sent between devices. The shared key should be a long string of up to 32 alphanumeric characters and symbols that would be difficult to guess. For example, he^sg3iq6pg2*gqw@89hsm,wz[This same key must be copied to the remote RADIUS client.
Generate	Click to generate a random 32 character shared key.
	Click to copy the shared key to the clipboard.

Local User Management

User access to this controller and to other controllers that are using this controller as their RADIUS server are managed by adding them to the **Local User Management** shown below.



Figure 8-17: Local User Management

Item	Description
Add	Add a new user to user management. These users will have login access to the controller.
Remove	Remove a user from user management.
Edit	Edit a user's information.

Adding a User

Adding a user creates a user profile that allows a person to login to the controller with a username / password combination and to have access to certain controller software interfaces. When this controller is used as a RADIUS server by other controllers, users connecting to those controllers will have to those controllers as defined by their user profile.

User Details
✕

All form fields are required.
Password must contain :

- Between 8 and 16 characters
- A minimum of one lower case letter [a-z]
- A minimum of one upper case letter [A-Z]
- A minimum of 1 numeric character [0-9]

●●●●●●●●

Admin :

Operator :

Viewer :

Rest :

Ok
Cancel

Figure 8-18: Adding a User

Item	Description
Username	The user's login.
Password	The user's password credential.
	View/conceal the user's password credential.

ECLYPSE Web Interface

Item	Description
User access attributes:	<p>The access levels the user will be able to use. Set one or more options according to the user's role.</p> <p>Admin: Allows user access to the ENVYSION studio and viewer. The user can also view and modify all configuration interface parameters and program the controller with EC-<i>gfx</i>Program.</p> <p>Operator: Allows user access to the ENVYSION interface in viewing mode as well as gives partial access to the ECLYPSE Web Configuration Interface. Certain configuration interface screens are unavailable such as User Management, Viewer Information, etc.</p> <p>Viewer: Allows user access to the ENVYSION interface in Viewing mode. The user is not allowed to access the ECLYPSE Web Configuration Interface.</p> <p>Rest: Allows a user to program the controller with EC-<i>gfx</i>Program. This user does not have access to the ECLYPSE Web Configuration Interface or ENVYSION.</p>

Remote RADIUS Server

When **Authentication** is set to **Proxy**, the following configuration parameters are available. This centralizes access management on a remote RADIUS server thereby saving time by eliminating the need to add users to each controller individually. A remote RADIUS server can be another ECY series controller or a suitably-configured EC-Net^{AX} / EC-BOS^{AX} station. See [Supported RADIUS Server Architectures](#) on page 61.

Should the connection to the remote RADIUS server be temporarily lost, ECLYPSE controllers have a fall back authentication mode: Users that have already authenticated themselves with the remote RADIUS server and then the connection to the RADIUS server is lost, these users will still be able to login to the controller as their successfully authenticated credentials are locally cached.



The user profile cache is updated when the user authenticates themselves while there is a working RADIUS server connection. For this reason, at a minimum, admin users should log in to each ECLYPSE controller at least once so their login can be cached on that controller. Otherwise, if there is a RADIUS server connectivity issue, and a user who has never connected to the ECLYPSE controller before will be locked out from the controller. It is particularly important for admin user credentials to be cached on each controller as an admin user can change the controller's network connection parameters that may be at cause for the loss of connectivity to the RADIUS server.

Authentication : Remote

Remote Radius Server

Ip Address : 127.0.0.1

Authentication Port : 1812

Accounting Port : 1813

Proxy Port : 1814



Shared Key : 5^@!sK<Ah4Ho%7_ 

Figure 8-19: Using the Network's RADIUS Server for User Authentication Management

The port values of 1812 for authentication and 1813 for accounting are RADIUS standard port numbers. However, other port numbers may be used. No matter which port numbers are used, make sure that the port numbers are unused by other services on this controller and that both the RADIUS server and the RADIUS clients use the same port number values. See also [ECLYPSE IP Network Port Numbers and Protocols](#) on page 28.

Item	Description
IP Address	The IP address of the remote RADIUS server. This can be the IP address of an ECY series controller that has Authentication set to Local , or a suitably-configured RADIUS server on an EC-Net ^{AX} / EC-BOS ^{AX} station.
Authentication Port	This is the port on which authentication requests are made.
Accounting Port	This is the port on which accounting request are made. This is only used to receive accounting requests from other RADIUS servers.
Proxy Port	This is an internal port used to proxy requests between a local server and a remote server.
Shared Key	This is an encryption key that devices use to encrypt and decrypt user authentication credentials that are sent between devices. The shared key should be a long string of up 32 alphanumeric characters and symbols that would be difficult to guess. For example, he^sg3iq6pg2*gqw@89hsm,wz[If EC-Net ^{AX} is the remote RADIUS server, the same value must be copied to the Shared Secret parameter in the RadiusService .
	Click to copy the shared key to the clipboard.

Device Information

This shows detailed information about the controller such as the software version, MAC address for each network interface, extension modules versions, and Wi-Fi information.

Device

- Controller Name: ECV-MW7C316F
- Device Instance: 254001
- Model Name: ECV-MW Rev 0
- Firmware Version: main-1.1.15203.420
- Vendor Name: Ditech Controls, Inc.

Wired IP

- IP Address: 172.16.254.1
- Subnet Mask: 255.255.255.0
- Gateway: 172.16.254.1
- Mac Address (eth0): 54-4A-16-7C-31-6F

Extensions

Name	Hardware ID	Version
VW 4U-4DO-2U0	53FF7006889525313301567	1.0.15195.1

Wifi Keys

Wi-Fi Primary

- IP Address: 192.168.0.1
- Subnet Mask: 255.255.255.0
- Mac Address: E8 DE 27 0F E1 89

Wi-Fi Auxiliary

- IP Address: N/A
- Subnet Mask: N/A
- Mac Address: N/A

Reboot

Figure 8-20: Device Information

Item	Description
	Click to refresh the information in the list.
Reboot	Click to reboot the controller. Rebooting the controller will interrupt the operation of any connected equipment and the controller will be offline from the network for the duration of the reboot.

The Mac Address is the same for both Primary (PRI) Wired Ethernet connection (ETH0) and the Secondary (SEC) Wired Ethernet connection.

System Settings

This is where you configure the controller's Web interface, port numbers, and secure web interface. A secure web interface requires a SSL certificate.

Figure 8-21: System Settings

Item	Description
Date	Set the controller's date
Time and Time Zone	Set the controller clock's time and the time zone the controller is located in.
Get Current Date Time	Click to get the current time a date from an internet time clock server. Internet connectivity is required for this feature to work.
Use HTTPS	Set this to enable the secure Webserver on this controller. Connections to this sever are encrypted which helps to prevent eavesdropping thereby keeping passwords secure.
Use HTTP	Set this to enable the standard Webserver on this controller.
Port Number	Set the port numbers the secure and standard Webservers are to use.
Hostname	<p>Give this controller a label or nickname to identify it on the network. The hostname can be used in place of an IP address to identify this controller on the network. This hostname can be used in a Web browser's address bar or in the EC-gfxProgram's Connect to screen for example.</p> <p>A hostname may contain only the ASCII letters 'a' through 'z' (case-insensitive), the digits '0' through '9', and the hyphen ('-'). A hostname cannot start with a hyphen, and must not end with a hyphen. No other symbols, punctuation characters, or white space are permitted.</p>
Common name	For HTTPS connections, a certificate must have the controller's current URL or IP address encoded into it to show to the connecting device that the connection corresponds to the certificate. Set the controller's current IP address, hostname, or DNS name.
Export Authority Key Certificate	For HTTPS connections, click to export the public key from the local authority that generates the internal certificate to a file on your PC. You must import this certificate into all PCs that are going to connect to this controller as a trusted certificate. See Saving a Certificate on page 92.

ECLYPSE Web Interface

Item	Description
Import certificate	Set this to import a pre-existing certificate saved as a file on your PC.
Import Certificate	To import the custom certificate.
Status	Not present: No certificate has been imported. Present: A certificate has been imported.
Password	The password for the certificate to be imported.
Host ID	This is a unique un-alterable identifier for this controller. Use this identifier when making a license request.
Import From Server	Imports a license file directly from a Web server. Internet connectivity is required.
Import From PC	Imports a license file from your PC.
Export To PC	Saves the controller's license file to your PC.

Saving a Certificate

When the HTTPS Certification has been configured, you can save the certificate on your PC. This certificate must be distributed to all PCs that will connect to this controller. It is this certificate that allows a trusted connection to be made between the two devices.

1. Enable **Use internal certificate**, and set this controller's IP address or DNS name in **Common name**. Click **Export Authority Key Certificate** to save the certificate on your PC.

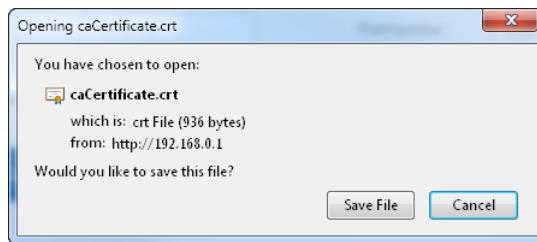


Figure 8-22: Saving the Certificate

2. Save the file on your PC.
3. Distribute this file to all PCs that will connect to this controller.
4. Install the certificate on the PC by double-clicking it in Microsoft Windows Explorer. Click **Open**.

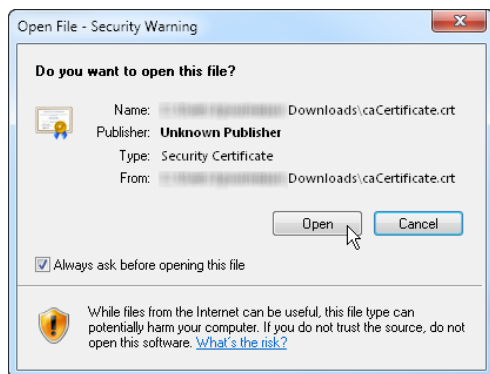


Figure 8-23: Installing the Certificate on the PC

5. Install the certificate in the Trusted Root Certification Authorities store. Click **Install Certificate**.

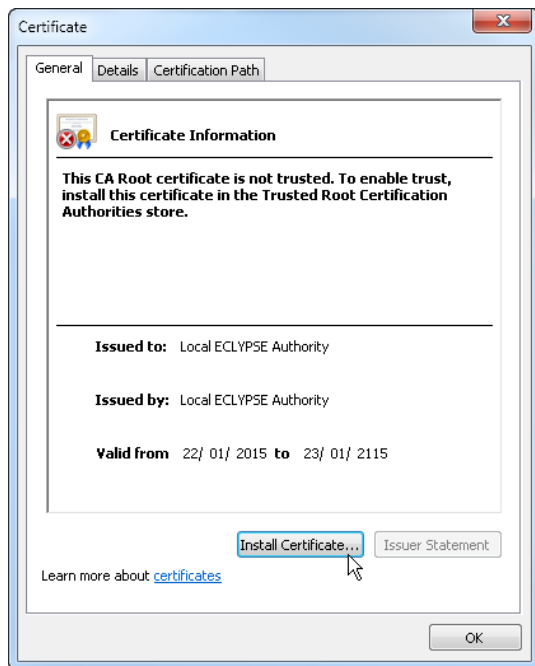


Figure 8-24: Installing the Certificate on the PC

6. Select Place all certificates in the following store. Click Browse.

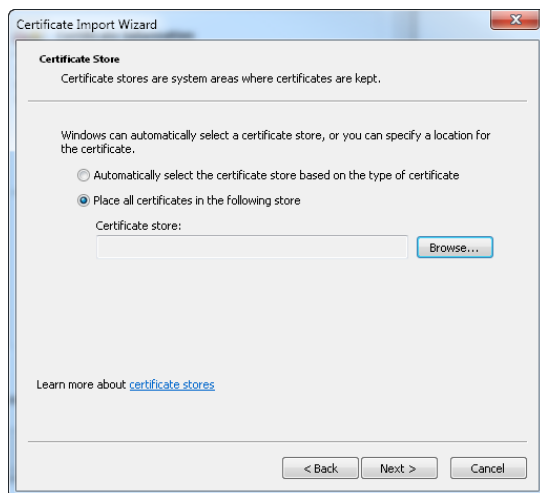


Figure 8-25: Selecting the Store

7. Select Trusted Root Certificate Authorities and click OK.

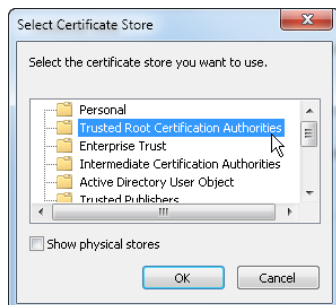


Figure 8-26: Selecting the Store

8. Click Next. Click Finish.

ECLYPSE Web Interface

9. Accept the warning. Click **Yes**.

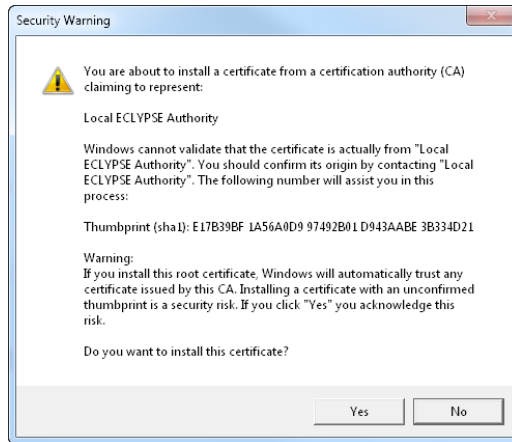


Figure 8-27: Accept the Warning

Viewer Information


When a user logs into the controller, the first page they will see can be set so they do not have to navigate to that page every time they connect to the controller. This allows a user to be immediately situated in a task according to their role.

Add user default page

User Access Management

Name	URL	
admin	//192.168.0.1/config /viewer.html	<input type="button" value="Delete"/>

Figure 8-28: Viewer Information Settings

Item	Description
Add User	Set the user's username they use when logging into the controller. Click <input type="button" value="▼"/> to view and select a user from a list of currently configured users.
Add URL	<p>This sets the landing page that will be displayed to individual users when they logging in to the controller. The URL for any page the controller can serve according to the user's access rights can be used (see User Management on page 85).</p> <p>Click  in the lower right corner to resize the window.</p> <p>The username of the account that will be redirected to a specific web page or URL.</p> <ul style="list-style-type: none"> In the top field, enter the user name. In the bottom field, enter the full URL of the web page. This should be copied from your Web browser's address bar including HTTP:\ or HTTPS:\ when you have navigated to the target page. For example, if the connection to the controller is encrypted (only the HTTPS protocol has been enabled in System Settings) and you do not specify HTTPS:\ in the URL, the controller will default the address to HTTP protocol, which will direct the user's browser to a URL that will fail to load.
Delete	Click to delete the corresponding table entry.

CHAPTER 9

CONFIGURING THE ECLYPSE Wi-Fi ADAPTER WIRELESS NETWORKS

ECLYPSE Wi-Fi Adapter supports a number of wireless network connection modes. This chapter describes how to configure a controller's wireless network. See also [ECLYPSE Wi-Fi Adapter Connection Modes](#) on page 44.

In This Chapter

Topic	Page
Setting up a Wi-Fi Client Wireless Network	97
Setting up a Wi-Fi Access Point Wireless Network	98
Setting up a Wi-Fi Hotspot Wireless Network	99
Setting up a Wi-Fi Mesh Wireless Network	101

Setting up a Wi-Fi Client Wireless Network

This connects the controller as a client of a Wi-Fi access point. See [Wi-Fi Client Connection Mode](#) on page 45 for more information.

Wireless Configuration

Enabled :

Active Mode : Client

Network Name : ECLYPSE-CD4C93 (🔍)

Encryption : WPA2

Password : gFRfsa-dfjtb285,rt (🔍)

Figure 9-1: Client Wireless Network Settings

Configure the controller's ECLYPSE Wi-Fi adapter mode as a Wi-Fi client as follows.

1. Set **Enabled**.
2. Set the **Active mode** to **Client**.
3. Click (🔍) for the controller to search for available access points that are within range. The access points are listed on the right.

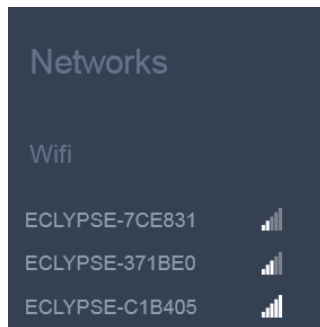


Figure 9-2: List of Available Access Points to Pair With

4. Select an access point to pair with from the access point list. The **Encryption** mode is provided by the access point.
5. Set the access point's authentication password in **Password**. This password is set in the access point's (or wireless router's) configuration.
6. Click **Apply**.

Setting up a Wi-Fi Access Point Wireless Network

This turns the controller into a Wi-Fi access point that other wireless clients can use to have network access. This access point operates off of the same subnetwork and has the same IP connectivity that the controller has with its wired network connection. For example, if the controller's wired connection is to a network that has an active DHCP server, access point clients can also use this DHCP server to automatically configure their IP connection parameters. See [Wi-Fi Access Point](#) on page 45 for more information.

Wireless Configuration	Hotspot Configuration	Advanced
Enabled : <input checked="" type="checkbox"/>	Enabled : <input type="checkbox"/>	Channel Width : 20 MHz Only
Active Mode : Hotspot/AP	Ip Address : 192.168.0.1	Channel Number: 6 - 2.437 GHz
Network Name : ECLYPSE-7C316F-	Subnet Mask : 255.255.255.0	Wifi Mode : N
Encryption : WPA2	First Address : 192.168.0.2	
Password : eclypse1234	Last Address : 192.168.0.254	

Figure 9-3: Access Point Wireless Network Settings

Configure the controller's ECLYPSE Wi-Fi adapter mode as a Wi-Fi access point as follows.

1. Under **Wireless Configuration**, set **Enabled**.
2. Set the **Active mode** to **Hotspot/AP**.
3. Set the name for this access point by which wireless clients will identify it in **Network Name**.
4. Set the encryption mode to be used by this access point in **Encryption**:
 - **None: this option should be avoided** as it does not provide any wireless security which allows any wireless client to access the LAN.
 - **WPA2**: select the Wi-Fi Protected Access II option to secure the Wi-Fi network with a password.
 - **WPA2 Enterprise**: Use this option if you are connecting to an enterprise network that has a working RADIUS authentication server. This RADIUS server provides user authentication.
5. Set the access point's authentication password in **Password**. This is the password wireless clients will need to know in order to connect to this access point.
6. Under **Hotspot Configuration**, disable **Enabled**.
7. Under **Advanced**, set the **Channel Width**, **Channel Number**, and **Wi-Fi Mode**. See [Advanced](#) on page 75 for an explanation of these parameters.
8. Click **Apply**.

Setting up a Wi-Fi Hotspot Wireless Network

This turns the controller into a Wi-Fi hotspot with a router. This puts the hotspot into a separate subnetwork with a DHCP server to provide IP addresses to any connected device. See [Wi-Fi Hotspot](#) on page 46 for more information.

Wide area network (WAN) connectivity is through the wired connection. See [Network Address Translation / Firewall](#) on page 24. Though BACnet/IP uses IP protocol to communicate, this hotspot acts as an IP router; it does not forward broadcast messages which are important in BACnet to identify services that are available within the BACnet internetwork. See [BACnet/IP Broadcast Management Device Service](#) on page 129.

Wireless Configuration	Hotspot Configuration	Advanced
Enabled : <input checked="" type="checkbox"/>	Enabled : <input checked="" type="checkbox"/>	Channel Width : 20 MHz Only
Active Mode : Hotspot/AP	Ip Address : 192.168.0.1	Channel Number : 6 - 2.437 GHz
Network Name : ECLYPSE-7C316F-	Subnet Mask : 255.255.255.0	Wifi Mode : N
Encryption : WPA2	First Address : 192.168.0.2	
Password :	Last Address : 192.168.0.254	

Figure 9-4: Hotspot Wireless Network Settings

Configure the controller's ECLYPSE Wi-Fi adapter mode as a Wi-Fi hotspot as follows.

- Under **Wireless Configuration**, set **Enabled**.
- Set the **Active mode** to **Hotspot/AP**.
- Set the name for this access point by which wireless clients will identify it in **Network Name**.
- Set the encryption mode to be used by this hotspot in **Encryption**:
 - None: this option should be avoided** as it does not provide any wireless security which allows any wireless client to access the LAN.
 - WPA2**: select the Wi-Fi Protected Access II option to secure the Wi-Fi network with a password.
 - WPA2 Enterprise**: Use this option if you are connecting to an enterprise network that has a working RADIUS authentication server. This RADIUS server provides user authentication.
- Set the hotspot's authentication password in **Password**. This is the password wireless clients will need to know in order to connect to this hotspot.
- Under **Hotspot Configuration**, set **Enabled**.
- Set the hotspot's IP address that wireless clients will connect to in **Ip Address**. Ensure that this address is:
 - Not in the range of IP address set by **First Address** and **Last Address**.
 - Not the same as the **IP address** set under IP Configuration for the wired network.
- Set the hotspot's subnet mask in **Subnet Mask**. See [About the Subnetwork Mask](#) on page 20.
- Set the hotspot's addressing range in **First Address** and **Last Address**. This defines the range of IP addresses to be made available for hotspot clients to use. The narrower the range, the fewer hotspot clients will be able to connect due to the lack of available IP addresses. For example, a range where First Address = 192.168.0.22 and Last Address

Configuring the ECLYPSE Wi-Fi Adapter Wireless Networks

- = 192.168.0.26 will allow a maximum of 5 clients to connect to the hotspot on a first-to-connect basis.
10. Under **Advanced**, set the **Channel Width**, **Channel Number**, and **Wi-Fi Mode**. See [Advanced](#) on page 75 for an explanation of these parameters.
 11. Click **Apply**.

Setting up a Wi-Fi Mesh Wireless Network

This feature is only available to Beta clients. This makes the controller a member of a mesh network. This interface can auto-configure its IP parameters when the connected network has a DHCP server. See [Mesh Network](#) on page 47 for more information.

The screenshot displays the configuration interface for a Wi-Fi Mesh network, divided into two main sections: **Wireless Configuration** and **Advanced**.

Wireless Configuration:

- Primary/Auxiliary:** Tabs for switching between Primary and Auxiliary configurations.
- Enabled:** A green toggle switch is turned on.
- Active Mode:** A dropdown menu is set to "Mesh".
- Mesh Gate:** An unchecked checkbox.
- Network Name:** A text input field containing "ECLYPSEMesh".
- Encryption:** A dropdown menu set to "SAE".
- Password:** A password input field with masked characters and a visibility toggle icon.

Advanced:

- Channel Width:** A dropdown menu set to "40 MHz Only".
- Channel Number:** A dropdown menu set to "6 - 2.437 GHz".
- Diagnostics:** A link to view network diagnostics.

Figure 9-5: Mesh Wireless Network Settings

Configure the controller's ECLYPSE Wi-Fi adapter mode as a Wi-Fi mesh as follows.

1. Under **Wireless Configuration**, set **Enabled**.
2. Set the **Active mode** to **Mesh**.
3. Set the **Mesh Gate** option when this controller has direct access to another non-mesh network segment through a wired Ethernet connection that acts as a primary network interconnect. This increases the data rate between mesh network nodes and other network segments. When this option is enabled, this mesh node will broadcast to the other mesh nodes at regular intervals that this mesh node has the shortest path to other networks. Only one or two mesh network nodes should have this option set as these broadcasts use wireless network bandwidth.
4. Set a network name for the mesh network in **Network Name**. All mesh network nodes must use the same network name to become a member of that mesh network.
5. Set the encryption mode to SAE in **Encryption**. All mesh network nodes must use the same encryption mode to become a member of that mesh network.
6. Set the mesh network's authentication password in **Password**. All mesh network nodes use the same authentication password.
7. Under **Advanced**, set the **Channel Width**, **Channel Number**, and **Wi-Fi Mode**. See [Advanced](#) on page 75 for an explanation of these parameters. See also [Alternate the Mesh Network Channel Number](#) on page 48.
8. Click **Apply**.

Mesh Network Diagnostics

Click Diagnostics to see the currently connected neighboring mesh network controllers and the corresponding connection receive signal strength and data rate.

This information is used to troubleshoot a mesh network. It is best that each controller has at least two mesh network neighbors with a receive signal strength stronger than -70 dBm.

Configuring the ECLYPSE Wi-Fi Adapter Wireless Networks



Signal strength is measured in negative units where the stronger the signal, the closer it is to zero. A weaker signal strength will have a more negative number. For example, a receive signal strength of -35 dBm is much stronger than a receive signal strength of -70 dBm.

CHAPTER 10

SECURING AN ECLYPSE CONTROLLER

This chapter describes how to harden an ECLYPSE controller from unauthorized access and use.

In This Chapter

Topic	Page
Introduction	104
Passwords	105
Account Management and Permissions	106
Additional Settings	107
External Factors	108

Introduction

This chapter describes how to implement best security practices for ECLYPSE controllers. Security is built up layer upon layer to make the system more resistant to attacks. This involves taking simple but effective steps to implement built-in security features.

Passwords

A username / password combination (or credentials) authenticates a user's access rights to a controller. If an attacker gains access to a user's password, the attacker has access to carry out any action on the controller that is allowed by that user's permissions.

Change the Default Platform Credentials

When a controller is shipped, the following default credentials provide 'administrator' access rights. It is essentially important to change these credentials when first logging into the controller.

```
Username: admin
```

```
Password: admin
```

It is important to create new user accounts with strong passwords to protect the controller from unauthorized access. Remove the factory default account admin / admin as this is a commonly known security breach. The username / password can be changed in [User Management](#) on page 85 and see also [Supported RADIUS Server Architectures](#) on page 61.

Use Strong Passwords

Passwords should be hard to guess. Avoid birthdates and common keyboard key sequences. A password should be composed of a random combination of 8 or more uppercase and lowercase letters, numbers, and special characters.

Do Not Allow a Browser to Remember a User's Login Credentials

When logging into an ECLYPSE controller with certain browsers, the browser asks to remember a user's login credentials. When this option is set, the next time the user logs in, the credentials will automatically be filled in. While this is convenient, anyone with access to the computer can login using those credentials. Do not set this option for administrator accounts or when accessing an account from an unsecure computer.

Account Management and Permissions

User accounts must be properly managed to make it harder for an attacker to compromise security, and to make it easier to detect that an attack has occurred. To set user account parameters, see [User Management](#) on page 85.

Use a Different Account for Each User

Each user account should represent an individual user. Multiple users or user groups should not share an account.

Suspending an account shuts-off a single user's access to the controller – it does not disrupt many users.

Permissions can be tailored to the needs of each user. A shared account may have more permissions than all users should have.

A shared account has a shared password which is more likely to be leaked.

It is harder to implement password expiration requirements.

Use Unique Service Type Accounts for Each Project

System integrators should use different credentials for each job they do. Should an attacker gain access to one system, they cannot readily access all systems installed by the same system integrator.

Disable Known Accounts When Possible

Create a new user admin account with new credentials then delete the default admin account. It is easier to attack the default admin account when an attacker only has to guess the password.

Assign the Minimum Required Permissions

When creating a new user account, give that account only the minimum rights to access or modify the system needed for that user.

Use Minimum Possible Number of Admin Users

A compromised admin account can be disastrous as it allows complete access to everything. Only give a user admin privileges only when absolutely necessary.

Additional Settings

Update the ECLYPSE Controller's Firmware to the Latest Release

Always keep the ECLYPSE controller's firmware up-to-date. The most recent firmware has the latest bug fixes and stability enhancements.

External Factors

Install ECLYPSE Controllers in a Secure Location

Ensure that the ECLYPSE Controller is installed in a physically secure location, under lock and key. Through physical access, an attacker can take over the controller to do with it what they please. For example, the reset button can be used to reset the controller to its factory default settings.

Make Sure that ECLYPSE Controllers Are Behind a VPN

For offsite connections, ensure that users access the controllers through a Virtual Private Network (VPN). This helps to prevent an attack through eavesdropping on the communications channel to steal user credentials.

CHAPTER 11

BACNET MS/TP COMMUNICATION DATA BUS FUNDAMENTALS

This chapter describes the BACnet MS/TP Communications Data Bus operating principles.

In This Chapter

Topic	Page
BACnet MS/TP Data Transmission Essentials	110
Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate	112
Data Bus Physical Specifications and Cable Requirements	115
Data Bus Topology and EOL Terminations	116
Data Bus Shield Grounding Requirements	119
Using Repeaters to Extend the Data Bus	122
Device Addressing	125
Power Supply Requirements for 24VAC-Powered Controllers	130

BACnet MS/TP Data Transmission Essentials

Certain models of the ECY Series Controller support BACnet MS/TP to BACnet/IP routing according to the controller model purchased. See the Controller's datasheet for more information. To enable BACnet MS/TP to BACnet/IP routing, see [Routing](#) on page 78.

The ECY Series Controller can support either BACnet MS/TP or Modbus RTU network on its RS-485 port. This option is selected in the controller's web interface. When the ECY Series Controller is configured for BACnet MS/TP, values from the connected BACnet MS/TP controllers can be used in ENVYSION graphics hosted on the ECY Series Controller. Furthermore, the ECY Series Controller acts as a BACnet/IP to BACnet MS/TP bridge that allows BACnet objects to be shared among BACnet intra-networks through BBMD.

The BACnet MS/TP data bus protocol is part of the BACnet[®] ANSI/ASHRAE[™] Standard 135-2008 that uses the EIA-485 (RS-485) physical layer standard for data transmission (herein called the data bus). Multiple data buses can be logically tied together as each BACnet MS/TP data bus is assigned a unique Network Instance that distinguishes it from other data buses in the BACnet MS/TP Local Area Network (LAN). An example of an interconnected BACnet MS/TP data bus is shown in [Figure 11-16](#) on page 128).

EIA-485 is a standard that defines the electrical characteristics of the receivers and drivers to be used to transmit data in a differential (balanced) multipoint data bus that provides high noise immunity with relatively long cable lengths which makes it ideal for use in industrial environments. The transmission medium is inexpensive and readily-available twisted pair shielded cable.

While there are many possible LAN topologies for an EIA-485 data bus, only devices that are daisy-chained together are allowed with BACnet MS/TP (see [Figure 11-4](#)). A spur is only permitted when it is connected to the data bus through a repeater (see [Using Repeaters to Extend the Data Bus](#) on page 122).

End-of-line (EOL) terminations are critical to error-free EIA-485 data bus operation. The impedance of the cable used for the data bus should be equal to the value of the EOL termination resistors (typically 120 ohms). Cable impedance is usually specified by the cable manufacturer.

BACnet MS/TP Data Bus is Polarity Sensitive

The polarity of all devices that are connected to the two-wire BACnet MS/TP data bus must be respected. The markings to identify the polarity can vary by manufacturer. The following table summarizes the most common identification labels for BACnet MS/TP data bus polarity.

Table 11-1: Common Identification Labels for BACnet MS/TP Data Bus Polarity for Distech Controls' Products


Distech Controls Product	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
ECB Series Controllers	NET –	NET +	24V COM
ECB-PTU Series Line-Powered Controllers	NET –	NET +	COM
ECY Series Controllers	NET –	NET +	S
Thermostat	–	+	Ref
Repeater	Data– Data1–	Data+ Data1+	N/A
BACnet/IP to MS/TP Adapter	RT–	RT+	COM
BACnet/IP to MS/TP Router	–	+	SC

BACnet MS/TP Communication Data Bus Fundamentals

 Except for an ECB-PTU Line-Powered Controllers and ECY Series Controllers, never connect the shield of the BACnet MS/TP data bus to the Reference terminal. See [Data Bus Shield Grounding Requirements](#) on page 119 for more information.

Table 11-2: Common Identification Labels for BACnet MS/TP Data Bus Polarity for other Manufacturers

Device Manufacturer	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
Common identification labels for BACnet MS/TP data bus polarity by other Manufacturers	B	A	SC
	-	+	G
	TxD-/RxD-	TxD+/RxD+	GND
	U-	U+	COM
	RT-	RT+	REF
	Sig-	Sig+	S
	Data-	Data+	

 When interfacing with BACnet MS/TP devices from other manufacturers, refer to the documentation provided with the device to correctly wire the device.

Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate

The following technical parameters limit the number of devices on a BACnet MS/TP Data Bus Segment.

- The BACnet MS/TP Data Bus Segment has a hard limit on the number of devices that can communicate due to the device addressing scheme (the MAC Address Range for BACnet MS/TP Devices). See [Data Bus Segment MAC Address Range for BACnet MS/TP Devices](#) on page 112.
- Each device presents an electrical load on the BACnet MS/TP Data Bus Segment. This is called *device loading*. The number of devices that can be connected to a BACnet MS/TP Data Bus Segment is limited by the loading of each device. See [Device Loading](#) on page 113.
- Choosing a low baud rate can cause BACnet MS/TP Data Bus congestion that can limit the amount of data that can be efficiently exchanged between devices connected to the BACnet MS/TP Data Bus. For example, at 9600 baud, the maximum number of devices is reduced to 25 due to the increased time it takes for token passing between devices. The recommended baud rate is 38 400. See [Baud Rate](#) on page 113.
- Distech Controls recommends that you connect no more than 50 of our $\frac{1}{8}$ or $\frac{1}{2}$ -load devices on a single BACnet MS/TP Data Bus Segment when a baud rate of 19 200 or higher is used (preferably 38 400 baud). This is to ensure that the BACnet MS/TP Data Bus has enough bandwidth to efficiently communicate network variables between controllers.

These parameters are described in greater detail below.

Data Bus Segment MAC Address Range for BACnet MS/TP Devices

The BACnet MS/TP data bus supports up 255 devices:

- Up to 128 devices (with device MAC addresses in the range of 0 to 127) that are BACnet MS/TP Masters (that can initiate communication).
- Up to 128 devices (with device MAC addresses in the range of 128 to 255) that are BACnet MS/TP Slaves (cannot initiate communication).

However, it is recommended that any given data bus segment have no more than 50 devices, when a baud rate of 19 200 or higher is used for the BACnet MS/TP Data Bus. A repeater counts as a device on each data bus segment to which it is connected.

All Distech Controls' devices are categorized as BACnet MS/TP Masters, that is, their device MAC address can be set in the range of 0 to 127 only.

Device Loading

Each device presents an electrical load on the BACnet MS/TP Data Bus Segment. This is called *device loading*. The use of full load devices limits the number of devices connected to a BACnet MS/TP Data Bus Segment to 32 devices. Distech Controls' BACnet MS/TP devices are $\frac{1}{8}$ -load devices and $\frac{1}{2}$ -load devices, which allows more devices to be connected to the BACnet MS/TP Data Bus Segment, as compared to full load devices.

Table 11-3: Device Loading

Manufacturer	Device load on the attached BACnet MS/TP Data Bus
Distech Controls' ECB and ECY Series controllers Distech Controls' ECB-PTU Series Line-Powered Controllers	$\frac{1}{8}$ -load devices
Distech Controls' BACnet MS/TP Thermostats	$\frac{1}{2}$ -load devices
Other manufacturers	Refer to their documentation

However, if a data bus segment is interoperating with devices that are full-load, $\frac{1}{2}$ -load, $\frac{1}{4}$ -load, or $\frac{1}{8}$ -load, then the device that supports the fewest devices on the same data bus is the one that sets the limit for the maximum total number of devices for that data bus segment. For example, you plan to put on one data bus the following devices:

Table 11-4: Device Loading Example

Manufacturer	Quantity of devices (example)	Equivalent full-load devices	Maximum devices supported by the manufacturer
Distech Controls' devices ($\frac{1}{8}$ -load devices)	8	1	128 ¹ Maximum 50 recommended
Distech Controls' BACnet MS/TP Thermostats ($\frac{1}{2}$ -load devices)	14	7	64 Maximum 50 recommended
Manufacturer Y (full load devices)	26	26	32
Total Full-Load Devices		34	There are too many devices on the data bus. It is limited to a maximum of 32 devices by Manufacturer's Y devices.

1. This is limited by the maximum number of master devices allowed on a BACnet MS/TP Data Bus.

The solution for the above example is to create two data bus segments connected together by a repeater and then split up the devices between the data bus segments, ensuring again that the maximum number of devices on each separate data bus is not exceeded. See [Using Repeaters to Extend the Data Bus](#) on page 122.

Baud Rate

Most devices will have a range of baud rate settings and possibly an AUTO setting that detects the baud rate of other devices transmitting on the data bus and adjusts the baud rate of the device accordingly. Typical baud rates are 9600, 19 200, 38 400, and 76 800. The baud rate setting determines the rate at which data is sent on the BACnet MS/TP data bus.

BACnet MS/TP Communication Data Bus Fundamentals



At 9600 baud, the maximum number of devices is reduced to 25 due to the increased time it takes for token passing between devices.

All devices on the data bus must be set to the same baud rate. Therefore, the chosen baud rate must be supported by all devices connected to the data bus.

The recommended baud rate for Distech Controls' devices is 38 400.

We recommend that you:

- Set the baud rate of two controllers on a BACnet MS/TP Data Bus Segment to the same baud rate to provide failover protection.

For example, set the baud rate of the ECY Series Controller (if equipped) and one other controller to 38 400 baud. If the ECY Series Controller becomes unavailable and there is a power cycle, the ECB controller will set the baud rate for the BACnet MS/TP Data Bus.

- Set all other devices to automatically detect the baud rate, if this option is available.

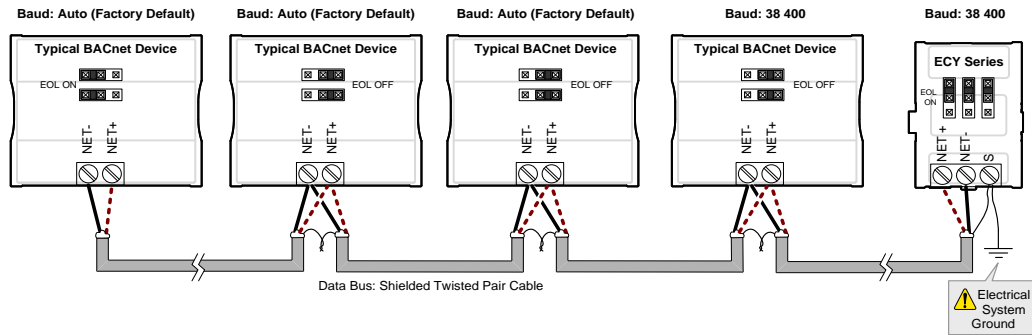


Figure 11-1: Setting the Baud rate on two Controllers on a BACnet MS/TP Data Bus Segment for Failover Protection

To set the baud rate for:

- ECY Series Controllers, see [Web Configuration Interface](#) on page 70.
- ECB Series controllers, see the controller's hardware installation guide or the [Network Guide](#).

Data Bus Physical Specifications and Cable Requirements

Cables composed of stranded conductors are preferred over solid conductors as stranded conductor cable better resist breakage during pulling operations. Distech Controls strongly recommends that the following data bus segment cable specifications be respected.

Table 11-5: BACnet MS/TP Data Bus Segment Physical Specifications and Cable Requirements

Parameter	Details
Media	Twisted pair, 24 AWG (see also Metric Conversions for Wire Gauge on page 173)
Shielding	Foil or braided shield
Shield grounding	The shield on each segment is connected to the electrical system ground at one point only; see Data Bus Shield Grounding Requirements on page 119.
Characteristic impedance	100-130 Ohms. The ideal is 100-120 Ohms.
Distributed capacitance between conductors	Less than 100 pF per meter (30 pF per foot). The ideal is less than 60 pF per meter (18 pF per foot).
Distributed capacitance between conductors and shield	Less than 200 pF per meter (60 pF per foot).
Maximum length per segment	1220 meters (4000 feet)
Data Rate	9600, 19 200, 38 400, and 76 800 baud
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections)
EOL terminations	120 ohms at each end of each segment
Data bus bias resistors	510 ohms per wire (max. of two sets per segment)

Shielded cable offers better overall electrical noise immunity than non-shielded cable. Unshielded cable or cable of a different gauge may provide acceptable performance for shorter data bus segments in environments with low ambient noise.

Table 11-6: Distech Controls Recommended Cable Types for BACnet MS/TP Data Buses

Cable Type	Part Number	O.D. (Ø)
300 meters (1000 feet), 24 AWG Stranded, Twisted Pair Shielded Cable – FT6, Rated for Plenum Applications	CB-BACN6BL1000	3.75mm (0.148 in.)

Distech Controls BACnet cable offers the best performance over the full range of baud rates, cable lengths, and number of connected devices. This is primarily due to lower conductor-to-conductor capacitance of this cable.

Data Bus Topology and EOL Terminations

Function of EOL Terminations

The first and last device on the data bus must have End-of-Line (EOL) termination resistors connected across the two data lines/wires of the twisted pair. These resistors serve the following purposes:

- EOL terminations dampen reflections on the data bus that result from fast-switching (high-speed rising and falling data edges) that otherwise would cause multiple data edges to be seen on the data bus with the ensuing data corruption that may result. The higher the baud rate a data bus is operating at, the more important that EOL terminations be properly implemented. Electrically, EOL terminations dampen reflections by matching the impedance to that of a typical twisted pair cable.
- EIA-485 data bus transmitters are tri-state devices. That is they can electrically transmit 1, 0, and an idle state. When the transmitter is in the idle state, it is effectively offline or disconnected from the data bus. EOL terminations serve to bias (pull-down and pull-up) each data line/wire when the lines are not being driven by any device. When an un-driven data bus is properly biased by the EOL terminations to known voltages, this provides increased noise immunity on the data bus by reducing the likelihood that induced electrical noise on the data bus is interpreted as actual data.

When to Use EOL Terminations

EOL terminations should only be enabled / installed on the two devices located at either end of the data bus. All other devices must not have the EOL terminations enabled/installed.

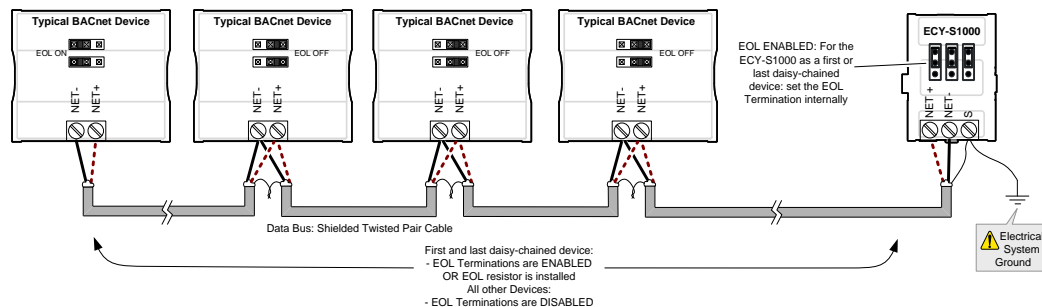



Figure 11-2: EOL Terminations Must be Enabled at Both the First and Last Device on the Data Bus

Devices with built-in EOL terminations are factory-set with the EOL termination disabled by default.

 The *BACnet/IP to MS/TP Adapter* does not have EOL Termination (and BACnet MS/TP Data Bus biasing) capabilities to be used at the end of a BACnet MS/TP data bus. Instead, use the *BACnet/IP to MS/TP Router* for this application.

When to use EOL Terminations with BACnet MS/TP Thermostats

BACnet MS/TP thermostats support external EOL termination resistors only. When a BACnet MS/TP thermostat is the first or last daisy-chained device, add a 120 Ohm resistor across the – and + BACnet MS/TP data bus connections.

The BACnet MS/TP data bus must be biased. This bias can only be provided by built-in EOL termination resistors (ones set with jumpers or DIP switches – refer to the controller's Hardware Installation Guide for how to identify and set a controller's built-in EOL terminations). If a BACnet MS/TP data bus has a BACnet MS/TP thermostat at one end of

BACnet MS/TP Communication Data Bus Fundamentals

the BACnet MS/TP data bus and an ECY Series Controller at the other end, you must set the built-in EOL termination in the ECY Series Controller so that proper biasing is provided to the BACnet MS/TP data bus.

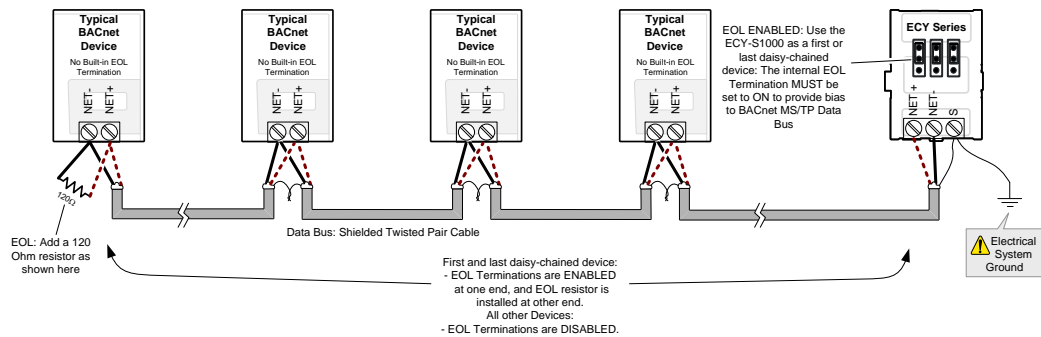


Figure 11-3: Typical EOL Terminations with BACnet MS/TP Thermostats with Biasing Provided by the ECY Series Controller's Built-in EOL Termination set to ON

About Setting Built-in EOL Terminations

ECY Series Controllers have built-in EOL terminations. These Controllers use jumpers to enable the EOL resistors and biasing circuitry.

ECB-PTU Series Line-Powered Controllers use DIP switches (found alongside those DIP switches used to set the MAC address) to enable the built-in EOL resistors and biasing circuitry.

ECB Series 24V-Powered Controllers have built-in EOL terminations. These Controllers use jumpers to enable the EOL resistors and biasing circuitry.

Refer to the controller's Hardware Installation Guide for how to identify and set a controller's built-in EOL terminations.

Only a Daisy-Chained Data Bus Topology is Acceptable

Use a daisy-chained BACnet MS/TP data bus topology only. No other data bus topology is allowed.

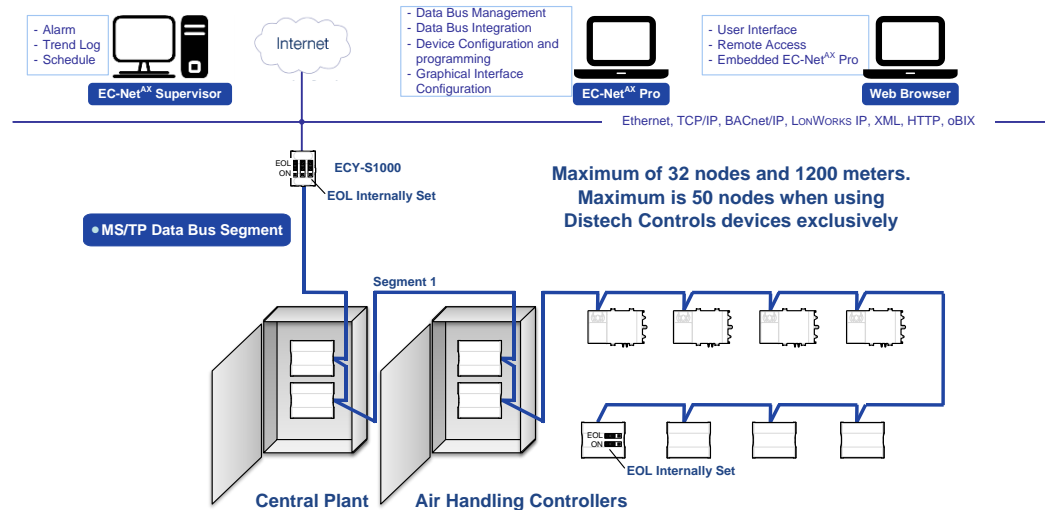


Figure 11-4: Typical BACnet MS/TP LAN Topology Showing How Devices are Daisy-Chained Together to Form One Data Bus Segment

BACnet MS/TP Communication Data Bus Fundamentals



Only linear, daisy-chained devices provide predictable data bus impedances required for reliable data bus operation. Only a daisy-chained data bus topology should be specified during the planning stages of a project and implemented in the installation phase of the project. A spur is only permitted when it is connected to the data bus through a repeater (see [Using Repeaters to Extend the Data Bus](#) on page 122).

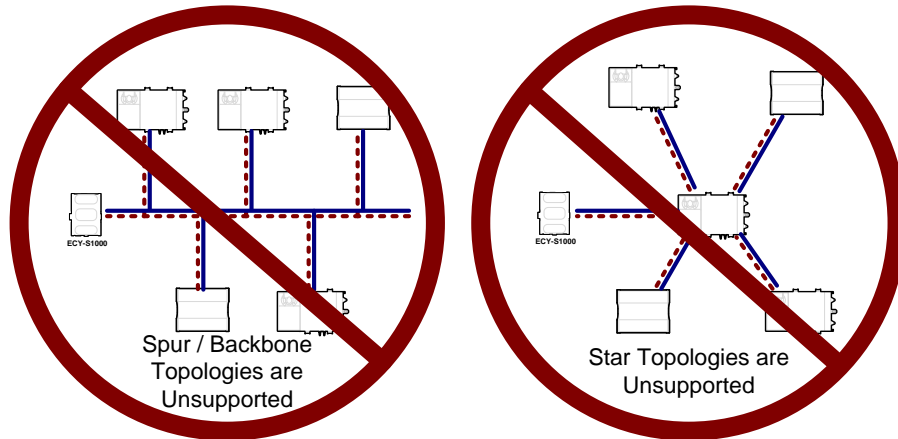


Figure 11-5: Unsupported BACnet MS/TP LAN Topologies

Data Bus Shield Grounding Requirements

The EIA-485 data bus standard requires that the data bus must be shielded against interference. A BACnet MS/TP data bus must also be properly grounded.

For ECB Series 24V-Powered Controllers: The data bus' cable shields must be twisted together and isolated with electrical tape at each device. Note that for ECB 24V-Powered Controllers, the power supply transformer's secondary that is connected to the 24V COM terminal is grounded. This provides the ground reference for the data bus (see [BACnet MS/TP is a Three-Wire Data Bus](#) on page 130). If the controller is at the end of the BACnet MS/TP data bus, simply isolate the data bus shield with electrical tape.

For ECB-PTU Series Line-Powered Controllers: The data bus' cable shields must be twisted together and connected to the **COM** terminal at each ECB-PTU Line-Powered Controller. Keep the cable shield connections short and take steps at each device to isolate the cable shield from touching any metal surface by wrapping them with electrical tape, for example. Note that for ECB-PTU Line-Powered Controllers, the data bus' cable shield provides the ground reference for the data bus (see [BACnet MS/TP is a Three-Wire Data Bus](#) on page 130). If the controller is at the end of the BACnet MS/TP data bus, simply connect the data bus shield to the **COM** terminal.

ECY Series Controller: The data bus' cable shields must be twisted together and connected to the **S** terminal at each ECY Series Controller. Keep the cable shield connections short and take steps at each device to isolate the cable shield from touching any metal surface by wrapping them with electrical tape, for example. Note that for ECY Series Controller, the data bus' cable shield provides the ground reference for the data bus (see [BACnet MS/TP is a Three-Wire Data Bus](#) on page 130). If the controller is at the end of the BACnet MS/TP data bus, simply connect the data bus shield to the **S** terminal.



Grounding the shield of a data bus segment in more than one place will more than likely reduce shielding effectiveness.

ECB 24V-Powered Controller Data Bus Shield Grounding Requirements

The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the ECY Series Controller, as shown below in [Figure 11-6](#) and [Figure 11-7](#).

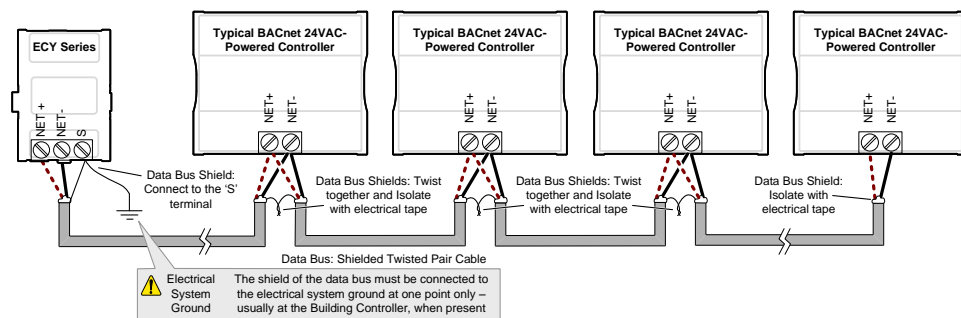


Figure 11-6: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located at the End of the Data Bus

BACnet MS/TP Communication Data Bus Fundamentals

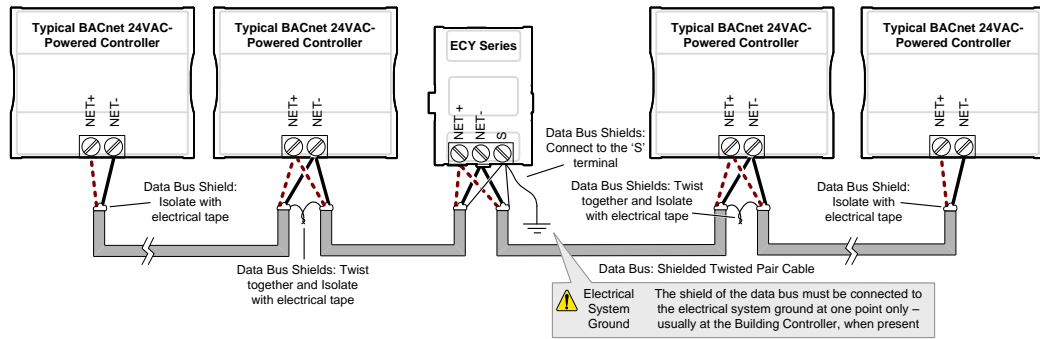


Figure 11-7: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located in the Middle of the Data Bus

ECB-PTU Line-Powered Data Bus Controller Shield Grounding Requirements

The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the ECY Series Controller, as shown below in [Figure 11-8](#) and [Figure 11-9](#).

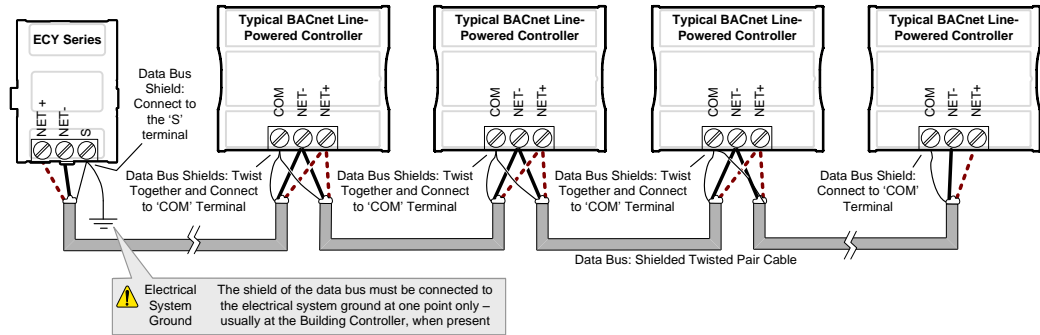


Figure 11-8: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located in the End of the Data Bus

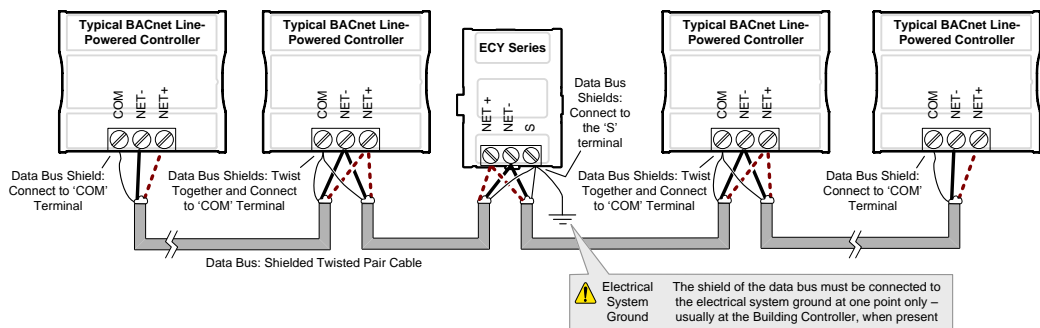


Figure 11-9: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located in the Middle of the Data Bus

Data Bus Shield Grounding Requirements When Mixing Both ECB 24V-Powered Controllers and ECB-PTU Line-Powered Controllers

The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the ECY Series System Controller, as shown below in [Figure 11-10](#) and [Figure 11-11](#).

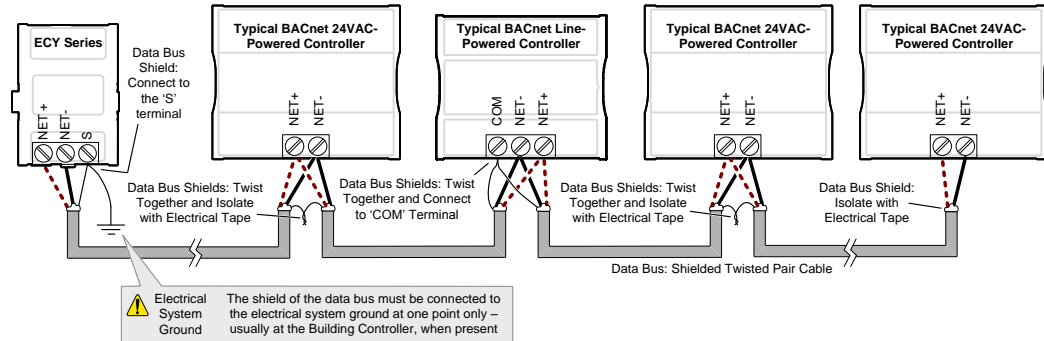


Figure 11-10: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located in the End of the Data Bus

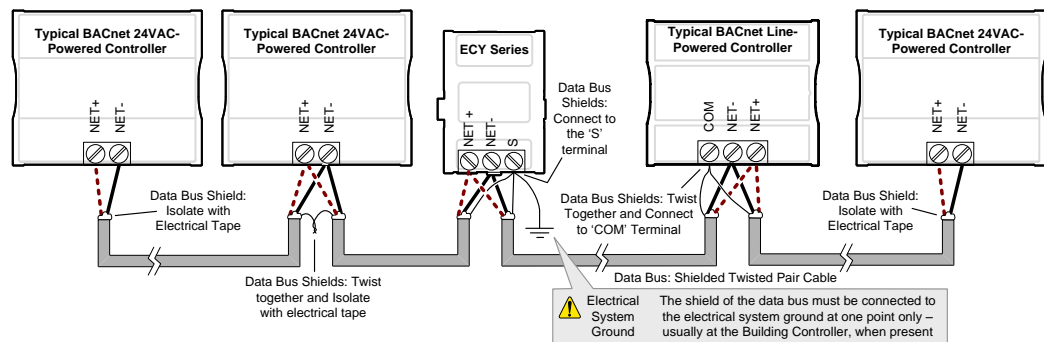


Figure 11-11: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECY Series Controller located in the Middle of the Data Bus

Using Repeaters to Extend the Data Bus

A BACnet MS/TP data bus segment can be up to 1220 meters (4000 feet) long with up to a maximum of 50 devices. When a greater length is required, a solution is to use a repeater. A repeater increases the maximum length of the data bus.

Using a Repeater to Extend the Length of the BACnet MS/TP Data Bus

Repeaters can be used to extend a BACnet MS/TP data bus up to 3660 meters maximum total length. Do not use more than two repeaters on a BACnet MS/TP LAN.

A BACnet MS/TP repeater is a bi-directional device that regenerates and strengthens the electrical signals that pass through it. It creates two electrically-isolated BACnet MS/TP data bus segments that transparently enable devices on one side of the repeater to communicate with any device on the other side. The two BACnet MS/TP data bus segments have the same requirements of an ordinary BACnet MS/TP data bus segment; that is, each BACnet MS/TP data bus segment:

- Can be up to 1220 meters (4000 feet) long.
- The first and last device on the data bus must have End-of-Line (EOL) termination resistors connected across the two data lines/wires of the twisted pair.
- Must respect the maximum limit for [Device Loading](#) on page 113.
- Will have the same network number as they remain part of the same network or LAN.

Distech Controls recommends that you connect no more than 50 of our 1/8 or 1/2-load devices on all BACnet MS/TP Data Bus repeater segments when a baud rate of 19 200 or higher is used (preferably 38 400 baud). This is to ensure that the BACnet MS/TP Data Bus has enough bandwidth to efficiently communicate network variables between controllers.



Do not use more than two repeaters on a BACnet MS/TP data bus. A repeater can only connect two BACnet MS/TP data bus segments even if it has ports to support more than two BACnet MS/TP data bus segments.

A repeater can be added anywhere to a data bus segment including the end of the segment as shown below.

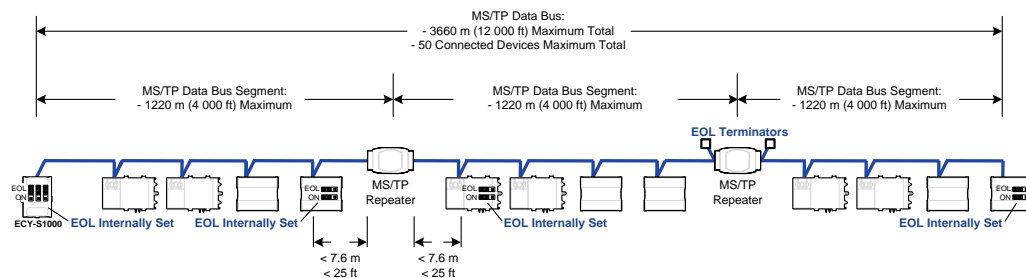


Figure 11-12: Using a Repeater to Extend the Range of the LAN

BACnet MS/TP Communication Data Bus Fundamentals

A repeater can be used to create a spur as shown below.

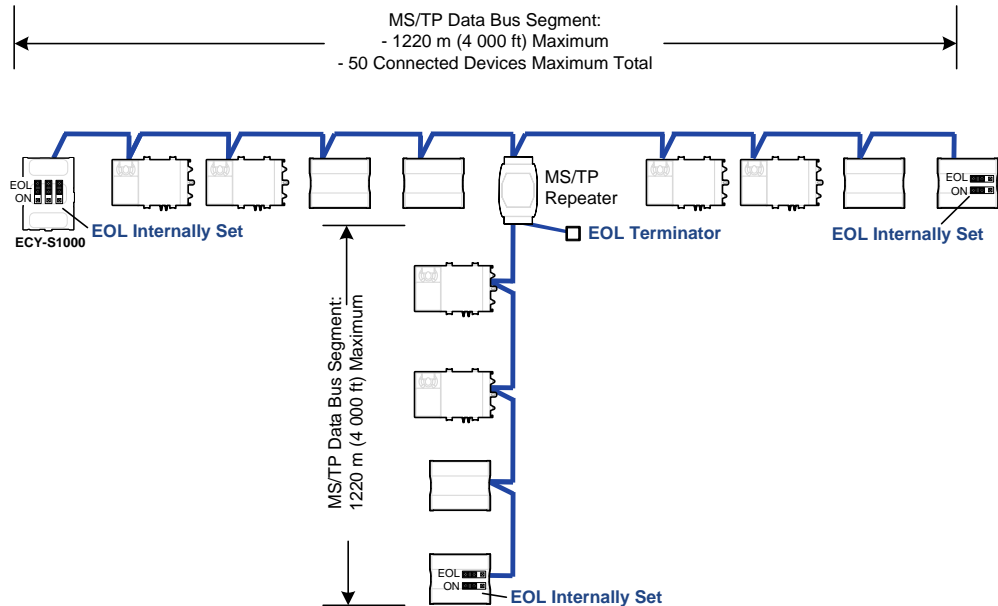


Figure 11-13: Adding a Spur by Using a Repeater

A repeater is counted as a device on each data bus to which it is connected.

When third party devices are connected to a data bus segment, the number of devices that can be connected to that data bus segment may be reduced. See [Device Loading](#) on page 113.

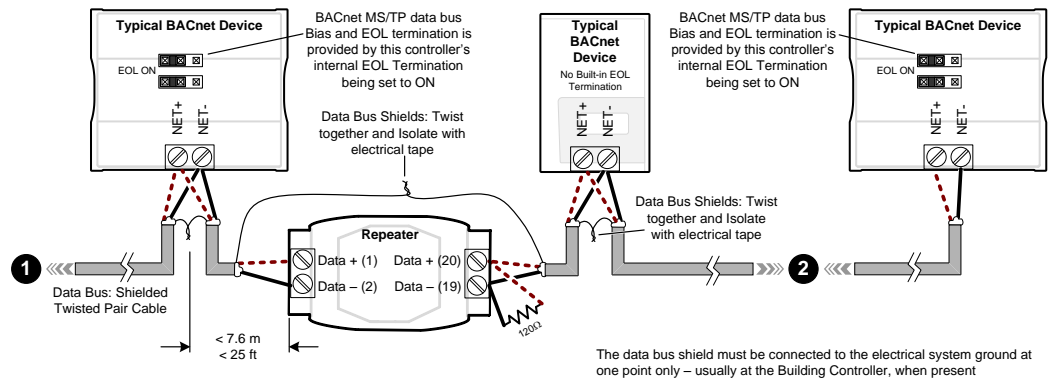


Figure 11-14: Repeater Connections when it is the First or Last Device on its Respective Data Bus Segment

The BACnet MS/TP Data Bus must be biased. This bias can only be provided by built-in EOL termination resistors (ones set with a jumper or DIP switch). When a repeater is the first or last device on its respective data bus segment, use the following methods to provide MS/TP Data Bus biasing and EOL termination as applicable to your situation:

1. On the BACnet MS/TP data bus segment ❶ shown in [Figure 11-14](#), bias and EOL termination is provided by a controller's built-in EOL termination being set to ON. In this case the connection to the repeater cannot be more than 7.6 meters (25 feet) from this controller.
2. On the BACnet MS/TP data bus segment ❷ shown in [Figure 11-14](#), a 120Ω EOL Termination resistor is added to the repeater's terminals. Biasing for this BACnet MS/TP data bus segment is provided by the built-in EOL termination being set to ON at the last controller at the other end of this data bus.

BACnet MS/TP Communication Data Bus Fundamentals

See [When to Use EOL Terminations](#) on page 116 for more information. The shield of one data bus must be grounded at one point as specified in [Data Bus Shield Grounding Requirements](#) on page 119. The shields of the two data buses must be connected together and isolated with electrical tape as shown in [Figure 11-14](#). Refer to the controller's Hardware Installation Guide for how to identify and set a controller's built-in EOL terminations.

Device Addressing

Device addressing allows the coordinated transfer of messages between the intended devices on the BACnet MS/TP data bus and with devices connected to the internetwork. For this, each device connected to the BACnet MS/TP data bus is identified by a MAC address, a Device Instance number, and a Network Number:

- The MAC Address uniquely identifies a device on a Network (identified by a Network Number). Devices on another Network can have the same MAC Address as messages are not passed at the internetwork level using the MAC Address. The MAC Address also defines the devices on the data bus that are Masters and Slaves, among other categories (see [Table 11-7](#)). The MAC Address is also used to share data bus bandwidth between devices through token passing between Master devices.
- The Device Instance uniquely identifies a device across the BACnet internetwork. The Device Instance is any number between 0 and 4 194 303. It is with the Device Instance that messages are exchanged between BACnet devices. The Device Instance is also used by routers to forward messages to devices located elsewhere in the internetwork. Unlike a MAC Address, a Device Instance cannot be reused elsewhere in the BACnet internetwork (it must be unique for the entire network).
- The Network Number is any number between 1 and 65 534. A network number identifies a LAN for routing purposes.

Both the MAC Address and the Device Instance must be set for each device and are essential for proper BACnet LAN operation.

For an example of how MAC address, Device Instance number, and Network Number apply to a typical BACnet network, see [Figure 11-16](#).

About the MAC Address

The MAC Address is a number from 0 to 255; however we recommend reserving some MAC Addresses for common commissioning and maintenance tasks. For example, when a portable adaptor is set to use one of these reserved MAC Addresses, it can be temporarily connected with certainty to any BACnet MS/TP data bus of any site without conflicting with other devices already connected to the BACnet MS/TP data bus. We strongly recommend that the MAC address of ECY Series Controller’s MS/TP port be always set to 0.

MAC Addresses should be used as shown in the following table.

Table 11-7: Recommended BACnet MS/TP Bus MAC Address Values / Ranges for BACnet MS/TP Data Bus Devices

MAC Address Value / Range	Usage	Devices
0	Data Bus Master (ECY Series Controller)	This address is invalid for Distech Controls’ ECB series devices
1	Temporary commissioning connection	Portable adaptor MAC Address for a temporary commissioning and maintenance connection
2	Reserved	Other
3-127	Master Range	Master devices: All Distech Controls’ devices are master devices and should be in this MAC Address range
128-254	Slave Range	Slave devices and network sensors
255	Broadcast	Do not apply address 255 to any device

BACnet MS/TP Communication Data Bus Fundamentals

BACnet MS/TP Data Bus Token-Passing Overview

The BACnet MS/TP data bus protocol is a peer-to-peer, multiple-master protocol that shares data bus bandwidth by passing a token between Master devices on the data bus that authorizes the device that is holding the token to initiate communications on the data bus. Once the device has completed its request(s), it closes the communications channel, passes the token to the next Master device (making it the current Master), and liberates the data bus.

The token is passed through a short message from device to device on the BACnet MS/TP data bus in consecutive order starting from the lowest MAC address (MAC Address = 0) to the next MAC Address.

Gaps or pockets of unassigned device MAC Addresses should be avoided as this reduces data bus performance. Once a master has finished making its requests, it must poll for the next master that may exist on the Data Bus. It is the timeout for each unassigned MAC Address that slows down the data bus.

The way MAC Addresses are assigned is not a physical requirement: Devices can be daisy-chained on the data bus in any physical order regardless of their MAC Address sequence. The goal is to avoid gaps in the device MAC Address range.

Slave devices cannot accept the token, and therefore can never initiate communications. A Slave can only communicate on the data bus to respond to a data request addressed to it from a Master device. Gaps in slave device MAC Addressing have no impact on BACnet MS/TP data bus performance.

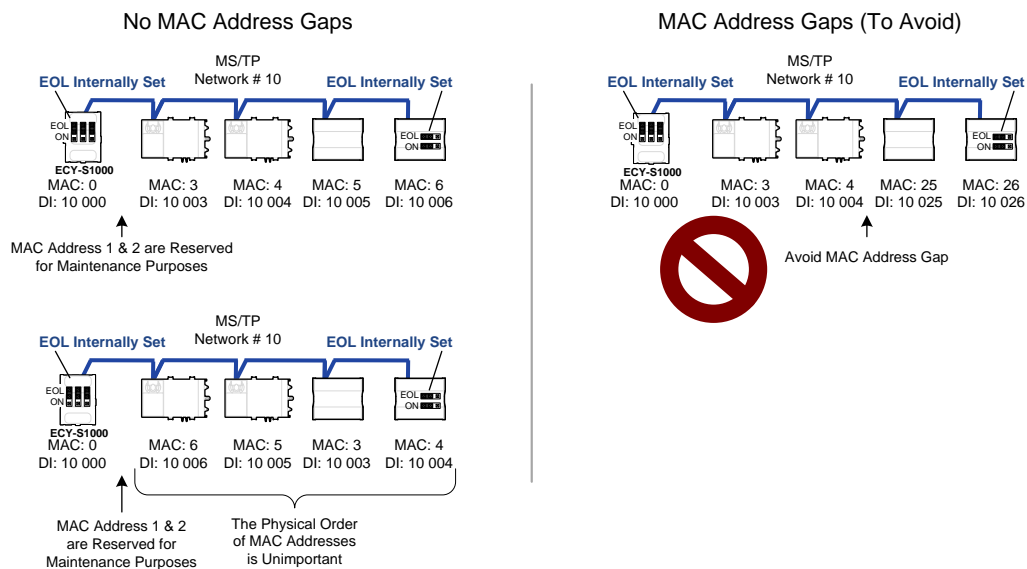


Figure 11-15: Setting the Max Master on the ECY Series Controller to the Highest MAC Address Used on the BACnet MS/TP Data Bus

About Tuning the Max Info Frames Parameter

Once a device has the token, it can make a number of information requests to other devices on the BACnet intranetwork. The maximum number of requests is limited by the **Max Info Frames** parameter. Once the device has made the maximum number of requests it is permitted to make according to the **Max Info Frames** parameter, the device passes the token to the following device with the next higher MAC address. This makes the BACnet MS/TP Data Bus more reactive for all devices by preventing a device from hanging on to the token for too long. Ordinary BACnet MS/TP devices should have the **Max Info Frames** parameter set to between 2 and 4. The Data Bus Master (ECY Series Controller) should have the **Max Info Frames** parameter set to 20.

About Tuning the Max Master Parameter

To prevent the passing of the token to unused MAC Addresses situated after the final Master device, the Max Master parameter must be set. By default, the Max Master for an ECY Series Controller or a [Soft EC-BOS^{AX}](#) is set to 127 which allows for the theoretical maximum of 127 devices besides the [Data Bus Master](#) to be connected to the data bus.

In practice, the actual number of devices connected to a data bus is far less, resulting in a gap between the highest MAC Address of any device connected to the data bus and the value set for Max Master. This gap unnecessarily slows-down the data bus with Poll for Master requests.

When commissioning a BACnet MS/TP Data Bus, it is useful to start with the Max Master set to 127 so as to be able to discover all devices connected to the data bus. Then, once all devices have been discovered and the MAC Addressing is finalized by eliminating any gaps in the address range, set the **Max Master** (maximum MAC Address) in the ECY Series Controller and in the [Soft EC-BOS^{AX}](#) to the highest Master device's MAC Address number to optimize the efficiency of the data bus.

Setting the Max Master and Max Info Frames

The **Max Master** and **Max Info Frames** are parameters used to optimize a BACnet MS/TP Data Bus. This is set in the ECY Series Controller and separately with the [Soft EC-BOS^{AX}](#) for each connected BACnet MS/TP device.

For the ECY Series Controller, set the **Max Info Frames** to 20 in the screen shown in **BACnet Settings** of the [Network Port MS/TP](#) on page 82 as this is a device that will make more requests for service from other devices on the network. In general, according to the way a device is programmed, the **Max Info Frames** may have to be set to a higher value than for other devices. For example, when Roof Top Unit Controllers are used with VAV controllers that use *gfxApplications* code, they should also have their **Max Info Frames** set to a higher value such as 5, as Roof Top Unit Controllers will poll many VAV controllers for information.

To set the **Max Master** and **Max Info Frames** for BACnet MS/TP devices (for example, an ECB series controller), use a [Soft EC-BOS^{AX}](#) to do so. See the [Network User Guide](#) for more information.

Default Device Instance Number Numbering System for Distech Controls' controllers

By default, controllers from Distech Controls automatically self-assign a Device Instance number generated from the unique MAC Address assigned to the controller during installation. The Device Instance number is calculated as follows:

Device Instance number = 364 X 1000 + MAC Address

Where 364 is Distech Controls unique BACnet Manufacturer ID.

This Numbering system is sufficient for a BACnet network that has only one ECY Series Controller. For larger BACnet networks that have more than one ECY Series Controller (to form a BACnet intranetwork), set the MAC Addresses, Device Instance Numbers and Network Numbers according to the numbering scheme below.

Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers

Good network planning requires a well thought-out numbering scheme for device MAC Addresses, Device Instance Numbers (DI), and Network Numbers. We recommend the following scheme, as it reuses the MAC Address and Network Number in the Device Instance number to make it easier for a network administrator to know where a device is located in the network. This is shown below.

BACnet MS/TP Communication Data Bus Fundamentals

Table 11-8: Recommended Numbering Scheme for MAC Addresses, Instance Numbers, and Network Numbers

Description	Range	Example
BACnet/IP Network Number	0 to 65 534	1
ECY Series Controller BACnet/IP Device Instance Numbers: Multiples of 10 000	10 000 to 4 190 000	10 000 20 000
BACnet MS/TP Network Number: ECY Series Controller BACnet/IP Device Instance Number/1000 + 0,1,2,3,4 (for each LAN)	10 to 4190	10 20 30
BACnet MS/TP Device Instance Number = ECY Series Controller BACnet MS/TP Network Number * 1000 + MAC Address	10 000 to 4 190 256	10 006 where MAC = 6

An example of this numbering system is shown below.

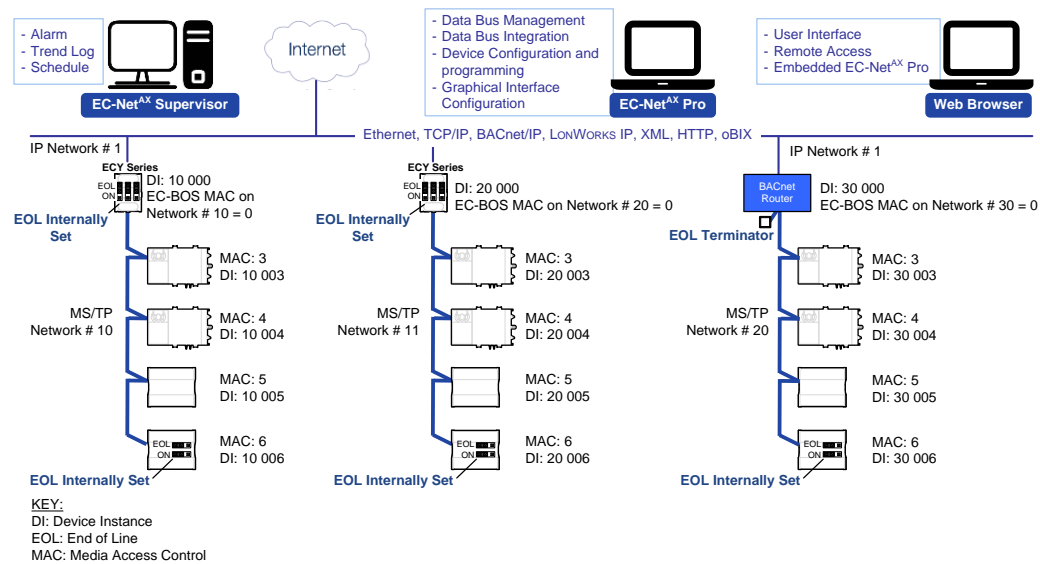


Figure 11-16: BACnet MS/TP Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers

⚠ When discovering devices with EC-Net^{AX} which has the routing option configured, it will discover all BACnet devices connected to all ECY Series Controllers when routing is enabled (see Routing on page 78). Make sure to add only the devices connected to the MS/TP port of the specific ECY Series Controller being configured. Using this numbering system will greatly help to identify those devices that should be added to a given ECY Series Controller.

Setting the ECY Series Controller's MAC Address

The ECY Series Controller's MAC address can be set in **BACnet Settings** of the [ECLYPSE Web Interface](#) on page 67.

BACnet MS/TP Communication Data Bus Fundamentals

Inter-Building BACnet Connection

BACnet network connections between buildings must be made using BACnet/IP as shown below.

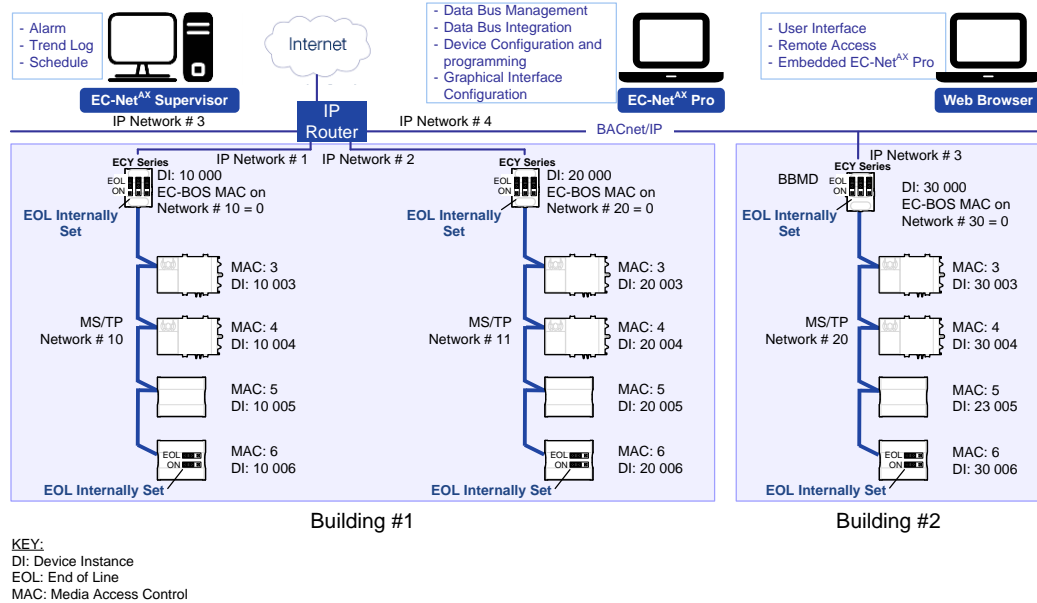


Figure 11-17: Typical Inter-Building Connection Using BACnet/IP or FOX

BACnet/IP Broadcast Management Device Service

Though BACnet/IP uses IP protocol to communicate, a standard IP router does not forward broadcast messages which are important in BACnet to identify services that are available within the BACnet internetwork.

When two ECY Series Controllers communicate to each other over a standard IP connection that is separated by an IP router, both ECY Series Controllers need the BACnet/IP Broadcast Management Device (BBMD) service to be configured and operational.

The BBMD service identifies BACnet messages on the BACnet MS/TP network that are intended for a device located on another BACnet network. The BBMD service encapsulates these messages into an IP message to the appropriate BBMD service of the other BACnet MS/TP network(s). The BBMD service on these networks strips out the encapsulation and sends the BACnet message on to the appropriate devices.

When sending BACnet messages across a standard IP connection that has an IP router, there must be one BBMD service running on each BACnet MS/TP network.

Power Supply Requirements for 24VAC-Powered Controllers

BACnet MS/TP is a Three-Wire Data Bus

Even though data is transmitted over a 2-wire twisted pair, all EIA-485 transceivers interpret the voltage levels of the transmitted differential signals with respect to a third voltage reference common to all devices connected to the data bus (signal reference). In practice, this common signal reference is provided by the building's electrical system grounding wires that are required by electrical safety codes worldwide. Without this signal reference, transceivers may interpret the voltage levels of the differential data signals incorrectly, and this may result in data transmission errors.



ECY-PS100-240 Power Supply is a double-insulated device and therefore is not grounded. The reference for the BACnet MS/TP data bus is made by connecting the shield of the BACnet MS/TP data bus to the ECY Series Controller's **S** terminal to provide a signal reference. This shield is grounded at one point only – see [Data Bus Shield Grounding Requirements](#) on page 119.

Avoid Ground Lift

24V Power wiring runs should not be too long, nor have too many devices connected to it. Wiring used to supply power to devices has a resistance that is proportional to the length of the wiring run (see [Table 11-9](#)).

Table 11-9: Resistance of Common Copper Wire Sizes

AWG	Diameter (Ø)		Area		Copper wire resistance	
	(inch)	(mm)	(kcmil)	(mm ²)	(Ω/km)	(Ω/1000 ft.)
14	0.0641	1.628	4.11	2.08	8.286	2.525
16	0.0508	1.291	2.58	1.31	13.17	4.016
18	0.0403	1.024	1.62	0.823	20.95	6.385

If the power run from the power supply is relatively long and it supplies power to many devices, a voltage will develop over the length of wire. For example, a 1000 ft. of 18 AWG copper wire has a resistance of 6.4 Ohms. If this wire is supplying 1 Ampere of current to connected devices (as shown in [Figure 11-18](#)), the voltage developed across it will be 6.4 volts. This effect is called ground lift.

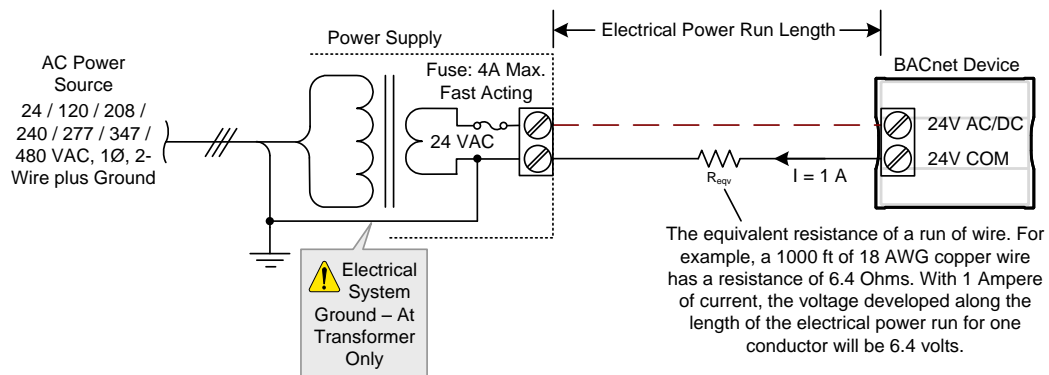


Figure 11-18: Ground Lift from a Long Power Run with a 24VAC Device

Because the 24V COM terminal on ECB series controllers is the signal reference point for the data bus, ground lift offsets the data bus voltage reference that is used to interpret valid data levels sent on the data bus. If the ground lift is more than 7 volts peak, there is a risk of data corruption and offline events due to the device being incapable of correctly reading data

signals from the data bus. **Thus it is important to keep the power supply (transformer) as close to the controller as possible.**

Techniques to Reduce Ground Lift

Reduce the impact of ground lift as follows:

- Use a heavier gauge wire.
- Add more wire runs. Connect these wire runs to the power supply in a star pattern.
- For controllers that accept DC power (that is, models without triac outputs): Specify a 24VDC power supply. The continuous and even voltage of a DC power supply makes more efficient use of the power handling capabilities of a power run. A 24VDC power supply eliminates the 2.5 multiplication factor associated with the peak AC current being 2.5 times the average RMS AC current. See below.

About External Loads

When calculating a controller's power consumption to size the 24VAC transformer, you must also add the external loads the controller is going to supply, including the power consumption of any connected subnet module (for example, for Allure series communicating sensors). Refer to the respective module's datasheet for related power consumption information.

A controller can support a maximum of two Allure series sensor models equipped with a CO₂ sensor. See [Subnetwork Module Compatibility and Supported Quantity Charts](#) on page 136 for how many Allure series communicating sensors are supported by a given controller model. The remaining connected Allure series sensor models must be without a CO₂ sensor.

Transformer Selection and Determining the Maximum Power Run Length

For the ECY Series, see the calculator spreadsheet available for download from our website to determine the power requirements and supported quantities of connected subnet modules: **ECLYPSE Selection Tool.xlsm**



Distech Controls' 24V-powered devices are Class 2 Products. To conform to Class 2 installation requirements, only use transformers of 100VA or less to power the device(s).

It is recommended to wire only one controller per 24VAC transformer.

For VAV devices, if only one 24VAC transformer is available, determine the maximum number of daisy-chained VAVs that can be supplied on a single power cable supplied by a 100 VA transformer, according to the controller's expected power consumption including external loads, the cable's wire gauge, and the total cable length from the following table. Any installation condition that is outside of the parameters of [Table 11-10](#) should be avoided.

Daisy-chaining controllers is not permitted when a VAV controller's expected power consumption including external loads is over 15VA. In this case the controller must be connected to the 24VAC transformer in a star topology. The transformer must be installed in close proximity to the controller.

Table 11-10: Maximum Number of 24VAC VAV Devices on a Power Run with a 100 VA Transformer (Daisy-Chained)

AWG ¹	Power Run Total Cable Length	Maximum Number of Devices @ 7 VA per device ²	Maximum Number of Devices @ 10 VA per device ³	Maximum Number of Devices @ 15 VA per device ⁴
14 ⁵	75 m (250 ft.)	4	2	1
14	60 m (200 ft.)	5	3	2
14	45 m (150 ft.)	5	4	3
14	30 m (100 ft.)	5	5	4

BACnet MS/TP Communication Data Bus Fundamentals

AWG ¹	Power Run Total Cable Length	Maximum Number of Devices @ 7 VA per device ²	Maximum Number of Devices @ 10 VA per device ³	Maximum Number of Devices @ 15 VA per device ⁴
16	60 m (200 ft.)	3	2	1
16	45 m (150 ft.)	5	3	2
16	30 m (100 ft.)	5	4	3
18	45 m (150 ft.)	3	2	1
18	30 m (100 ft.)	5	3	2

1. See also [Metric Conversions for Wire Gauge](#) on page 173.
2. Typical VAV with 1 Allure series sensor (non-CO₂ sensor model) and actuator activated. No external loads.
3. Typical VAV with 1 Allure series sensor (non-CO₂ sensor model), 2 triac loads (1.6 VA each), 1 analog output (20 mA), and actuator activated.
4. Typical VAV with 1 Allure series sensor (non-CO₂ sensor model), 4 triac loads (1.6 VA each), 2 analog outputs (20 mA each), and actuator activated.
OR
Typical VAV with 1 Allure series sensor with CO₂ sensor, 2 triac loads (1.6 VA each), 1 analog output (20 mA), and actuator activated.
5. Device terminals are not capable of accepting two 14 AWG wires (when daisy-chaining devices). Use a wire nut with a pig tail to make such a connection.

For non-VAV devices, determine the appropriate size transformer for the job as follows:

1. Add up the power requirements of all devices plus all external loads (see [About External Loads](#) on page 131). Multiply the total power needed by a multiplier of 1.3, as a security margin. For example, to power five devices (15 VA each), the total load is 75 VA multiplied by 1.3 is 98 VA. Choose a size of transformer just over this amount: For example, a 100 VA model.
2. When the total load of a number of devices requires a transformer with a rating greater than 100 VA, use two or more transformers. Ensure that the load to be connected to each transformer follows the guideline of Step 1 above.

Recommended 24V Power Cable

The table below lists Distech Controls' recommended power cable.

Table 11-11: Distech Controls Recommended 24V Power Cable

Cable Type AWG – Number of Conductors	Non-Plenum Applications (FT4)		Plenum Applications (FT6)	
	Part Number	O.D. (Ø)	Part Number	O.D. (Ø)
18-2	CB-W181P-1002	5.0mm / 0.20in.	CB-W181P-2051	5.0mm / 0.20in.
16-2	CB-W161P-1031	4.8mm / 0.19in.	CB-W161P-2062	4.8mm / 0.19in.
14-2	CB-W141P-1081	7.2mm / 0.29in.	CB-W141P-2013	7.2mm / 0.29in.

24VAC Power Supply Connection

Use an external fuse on the 24VAC side (secondary side) of the transformer, as shown in [Figure 11-19](#), to protect all controllers against power line spikes.

The Connected System Controller uses the **S** terminal as the signal reference point for the data bus (see [Table 11-1](#) for common device terminal labels).

BACnet MS/TP Communication Data Bus Fundamentals

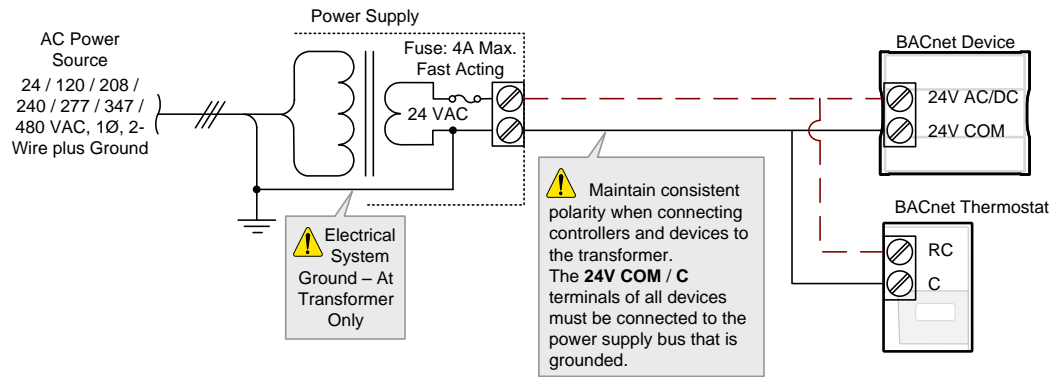


Figure 11-19: The 24V COM / C Terminal of all Devices must be Connected to the Grounded Power Supply Bus

CHAPTER 12

SUBNETWORK INSTALLATION GUIDELINES

This chapter describes the subnetwork installation guidelines. This subnetwork supports a range of expansion / extension modules.

In This Chapter

Topic	Page
About the Subnetwork Data Bus	135
Cat 5e Cable Subnetwork Data Bus	139
Setting the Allure EC-Smart-View Sensor's Subnet ID Address	144
Commissioning a Connected VAV Controller with an Allure EC-Smart-View Sensor	149

About the Subnetwork Data Bus

ECY Series Distech Controls' controllers use the subnetwork data bus to support various optional modules that add extra inputs, outputs, sensor inputs (temperature, humidity, CO₂, motion, receive wireless commands from a remote control), and interactive screen menus for user control. The subnetwork data bus uses the EIA-485 (Electronic Industries Alliance) standard for data transmission.

Subnetwork Connection Method

Connection to the subnetwork data bus is made through the RJ-45 **SUBNET** port to quickly connect expansion modules and sensors in a daisy-chained fashion to the subnetwork using a Cat 5e cable (standard straight Ethernet patch cable). Any device that connects to a controller's **SUBNET** port is collectively referred to as *room devices*.

This is summarized in the table below.

Subnetwork Room Device or Extension Module	Type	Connection Method
Allure EC-Smart-View series	Room Device: Sensors	Cat 5e cable with RJ-45 connectors – See Cat 5e Cable Subnetwork on page 139.
Allure EC-Smart-Comfort series		
Allure EC-Smart-Air series		
EC-Multi-Sensor series		
ECx-Light-4 / ECx-Light-4D / ECx-Light-4DALI	Room Device: Application specific expansion modules	
ECx-Blind-4 / ECx-Blind-4LV		

Table 12-1: Subnetwork Connection Method

Subnetwork Module Compatibility and Supported Quantity Charts

Not all subnetwork modules work with all controller models: The subnetwork module compatibility for an individual controller is shown in the table below along with the maximum supported quantity of room devices and extension modules. The Subnet ID address of all subnet devices must be set to be within the shown addressing range.

Controller Model	Subnetwork Data Bus Device	Permitted Subnet ID Addressing Range	Maximum Quantity Allowed
ECY-VAV	Allure EC-Smart-Vue series	1 to 4	See below ^{1, 3, 4}
	Allure EC-Smart-Comfort series		
	Allure EC-Smart-Air series		
	EC-Multi-Sensor series	1 to 4	
	ECx-Light-4 / ECx-Light-4D / ECx-Light-4DALI	1 to 4 ²	
	ECx-Blind-4 / ECx-Blind-4LV		
ECY-S1000	Allure EC-Smart-Vue series	1 to 12	12 ³
	Allure EC-Smart-Comfort series		
	Allure EC-Smart-Air series		
	EC-Multi-Sensor series	1 to 4	Not Supported
	ECx-Light-4 / ECx-Light-4D / ECx-Light-4DALI	1 to 4 ²	Not Supported
	ECx-Blind-4 / ECx-Blind-4LV		Not Supported

Table 12-2: Subnetwork Module Compatibility and Maximum Supported Quantity Chart

1. See the room device calculator spreadsheet available for download from our website to know the permitted quantities for these controller models: **VAV-Smart Room Control Device Calculator.xlsm**
2. Light and blind/shade expansion modules share the same Subnet ID addressing range. For example, you cannot set both an ECx-Light-4 and an ECx-Blind-4 to have a Subnet ID as 1.
3. A controller can support a maximum of two (2) Allure series sensor models equipped with a CO₂ sensor. Any remaining connected Allure series sensor models must be without a CO₂ sensor.
4. These models support a recommended maximum of 4 sensors (Allure series sensors and EC-Multi-Sensor series) combined in total. Each Allure series sensor model equipped with a CO₂ sensor counts as 2 sensors (for example, you cannot connect any other sensors if you connect two Allure series sensor models equipped with a CO₂ sensor or you can connect up to two other non-CO₂ sensors if you connect one Allure series sensor models equipped with a CO₂ sensor). When a longer system response time is acceptable, up to 4 Allure series sensors (no more than 2 of which are equipped with a CO₂ sensor) and up to 4 EC-Multi-Sensor series can be connected in total.

Subnetwork Module Connection

The following sections will provide further information needed to connect and configure the subnetwork devices such as cable type, cable length, wiring, data bus termination, device addressing, and more.

Subnetwork Installation Guidelines

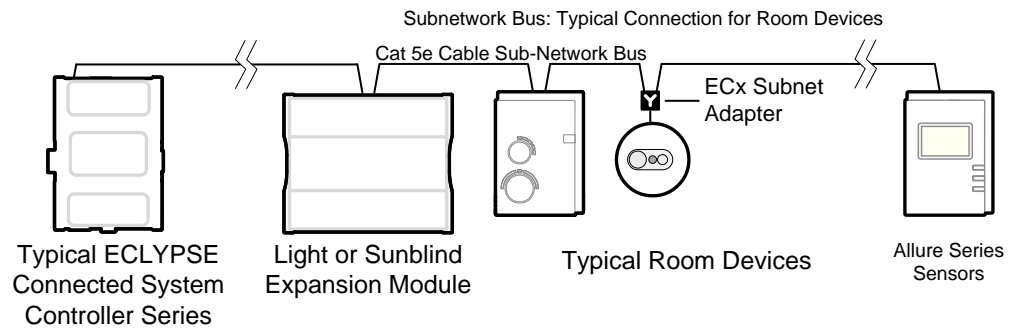


Figure 12-1: Subnetwork Module Connection to the ECY Series Controller Example

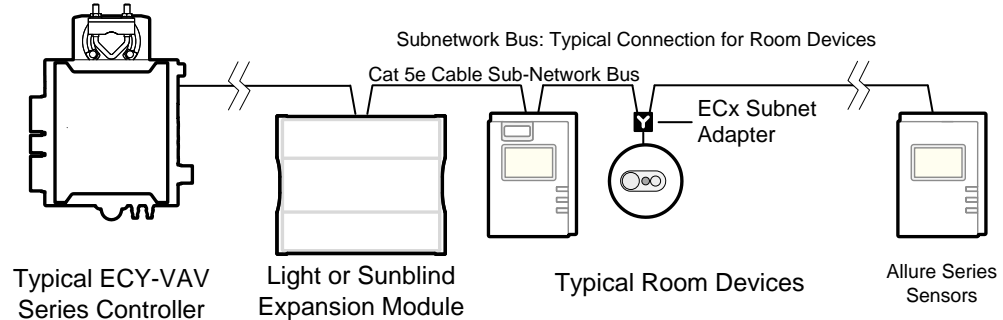


Figure 12-2: Subnetwork Module Connection to the ECLYPSE Connected VAV Controller Example

Subnetwork Data Bus Length

The length of the subnetwork data bus varies according to the type of controller and the types of connected subnetwork modules as follows:

The maximum length of the Cat 5e cable subnetwork data bus is 600 ft. (180 m). See [Figure 12-3](#).

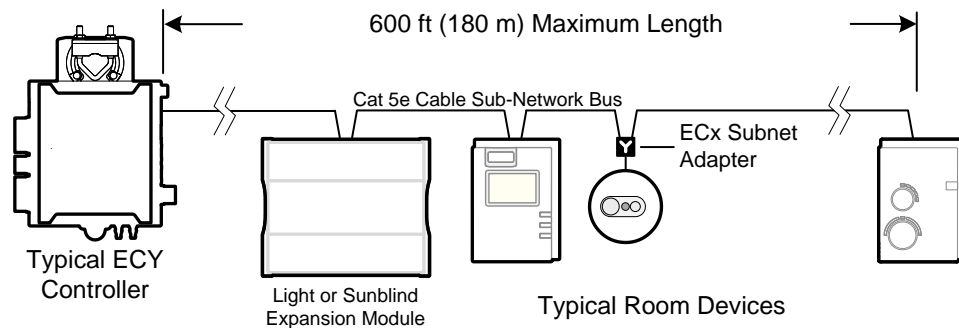


Figure 12-3: Maximum Length of the Cat 5e Cable Subnetwork Data Bus, ECLYPSE Connected VAV Controller

A controller can support a maximum of two (2) Allure series sensor models equipped with a CO₂ sensor; the remaining connected models must be without a CO₂ sensor. See [Subnetwork Module Compatibility and Supported Quantity Charts](#) on page 136 for the quantity of room devices supported by each controller model.


For instance, if the subnetwork for the controller model supports a subnetwork with 12 Allure series communicating sensors in total, then 10 Allure series sensor models must be without a CO₂ sensor and the remaining two (2) Allure series sensor models can be equipped with a

Subnetwork Installation Guidelines

CO₂ sensor. To ensure proper operation, it is recommended to distribute the sensors throughout the length of the subnetwork.

Cat 5e Cable Subnetwork Data Bus

The Cat 5e Cable subnetwork data bus is used to connect compatible room devices ([Table 12-1](#)) to any Distech Controls ECLYPSE series controller. See [Subnetwork Module Compatibility and Supported Quantity Charts](#) on page 136 for a list of compatible extension / expansion modules.

 Never connect an IP (Ethernet) network to the SUBNET PORT connector of a controller or RJ-45 connector of a room device. Equipment damage may result.

Cat 5e Cable Subnetwork Data Bus Cable Requirements

The Cat 5e Cable subnetwork data bus uses commonly available Cat 5e structural cabling fitted with RJ-45 connectors. If you make your own patch cable, use Category 5e cable and crimp the RJ-45 connectors at both ends of the cable either as T568A or T568B.

















Table 12-3: Cat 5e Cable Subnetwork Data Bus Physical Specifications and Cable Requirements

Parameter	Details
Maximum number of room devices	See Subnetwork Module Compatibility and Supported Quantity Charts on page 136. See also the Controller's Datasheet.
Subnet ID Addressing Configuration	See Setting the Subnet ID Addressing for Room Devices on page 143.
Media	Cat 5e Patch Cable with RJ-45 Connectors (standard straight patch cable)
RJ-45 Pin Configuration	Four (4) pairs required. Straight-through wiring. Crimp connectors as per T568A or T568B (both cable ends must be crimped the same way). See Table 12-4 and Figure 12-4 .
Characteristic impedance	100-130 Ohms
Distributed capacitance	Less than 100 pF per meter (30 pF per foot)
Maximum total length of the Cat 5e Cable subnetwork data bus plus the 2-Wire subnetwork data bus	300 m (1 000 ft.) Maximum – See Subnetwork Data Bus Length on page 137
Maximum length of the Cat 5e Cable subnetwork data bus	180 m (600 ft.) Maximum – See Subnetwork Data Bus Length on page 137
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections) Most room devices have two RJ-45 female pass-through connectors to facilitate the daisy-chain connection of room devices. For the EC-Multi-Sensor: An optional ECx Subnet Adapter (Y-splitter) is available to facilitate the daisy-chain connection of room devices. The ECx Subnet Adapter must be connected directly to the EC-Multi-Sensor and its length cannot be extended.
EOL terminations	Must be set / enabled on the last room device only
Shield grounding	Not applicable

Subnetwork Installation Guidelines

Crimp both ends of the cable either as T568A or T568B as shown below.

Table 12-4: T568A and T568B Terminations for an RJ-45 Connector

Pin	T568A (at both cable ends)		T568B (at both cable ends)	
	Pair	Color	Pair	Color
1	3	 white/green stripe	2	 white/orange stripe
2	3	 green solid	2	 orange solid
3	2	 white/orange stripe	3	 white/green stripe
4	1	 blue solid	1	 blue solid
5	1	 white/blue stripe	1	 white/blue stripe
6	2	 orange solid	3	 green solid
7	4	 white/brown stripe	4	 white/brown stripe
8	4	 brown solid	4	 brown solid

The final result of a crimped RJ-45 connector is shown graphically below.

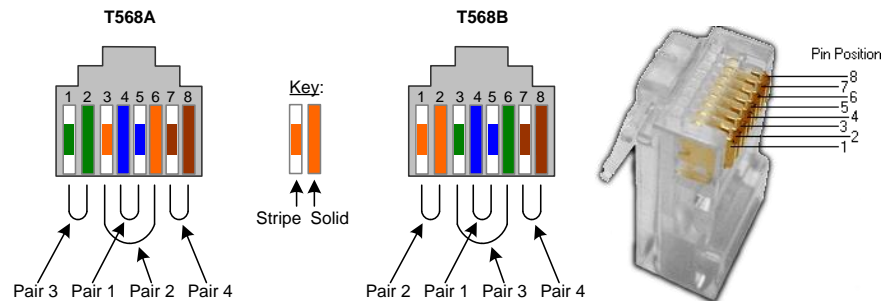


Figure 12-4: Pins on RJ-45 Jack Face

Distech Controls recommends the Cat 5e cables shown below. Cables fitted with connectors are crimped as T568B.

Table 12-5: Distech Controls Recommended Cable Types to use for the Cat 5e Cable Subnetwork Data Bus

Cable Type	Non-Plenum Applications (Use in Conduit - FT4)		Plenum Applications (FT6)	
	Part Number	O.D. (Ø) ¹	Part Number	O.D. (Ø) ¹
0.3m (1 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0001	4.6mm (0.18in.)	CB-CAT5PC6WH0001	4.6mm (0.18in.)
4.6m (15 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0015	4.6mm (0.18in.)	CB-CAT5PC6WH0015	4.6mm (0.18in.)
9m (30 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0030	4.6mm (0.18in.)	CB-CAT5PC6WH0030	4.6mm (0.18in.)
15m (50 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0050	4.6mm (0.18in.)	CB-CAT5PC6WH0050	4.6mm (0.18in.)
22m (75 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0075	4.6mm (0.18in.)	CB-CAT5PC6WH0075	4.6mm (0.18in.)
30m (100 ft.), Cat 5e Cable fitted with RJ-45 Connectors	CB-CAT5PC4WH0100	4.6mm (0.18in.)	CB-CAT5PC6WH0100	4.6mm (0.18in.)

Cable Type	Non-Plenum Applications (Use in Conduit - FT4)		Plenum Applications (FT6)	
	Part Number	O.D. (Ø) ¹	Part Number	O.D. (Ø) ¹
300 m (1000 feet), Cat 5e Cable – Without Connectors	CB-W244P-1446WHTB	4.6mm (0.18in.)	CB-W244P-2176WHTB	4.6mm (0.18in.)
100 Crimp RJ-45 Connectors	CB-W5506E	N/A	CB-W5506E	N/A

1. Outer cable diameter – This does not take into account the RJ-45 connector.

Cat 5e Cable Subnetwork Bus Topology and End-of-Line Terminations

The EOL termination settings for the Cat 5e Cable subnetwork data bus will vary depending on the type of controller the room device or extension module is connected to. By default, all room devices and ECx-4XX Series I/O Extension Module EOL terminations are factory set to OFF (except for the EC-Multi-Sensor).



For the Cat 5e Cable subnetwork data bus, only a daisy-chain topology is acceptable and T-connections are not allowed. For the EC-Multi-Sensor, an optional ECx Subnet Adapter (Y-splitter) is available to facilitate the daisy-chain connection of room devices. The male-end of the ECx Subnet Adapter must be connected directly to the EC-Multi-Sensor and its length cannot be extended.



Figure 12-5: An ECx Subnet Adapter (Y-Splitter)

EOL Terminations for the ECLYPSE Connected VAV Controller and ECY Series Controller Series Controllers

When one or more room devices are connected to the **Subnet Port** of an ECY-VAV series controllers, only the EOL terminations of the last room device is set to ON. All other room devices on the subnetwork data bus must have their EOL terminations set to OFF. The controller must be the first device on the Cat 5e Cable Subnetwork data bus as its internal EOL termination is permanently enabled.

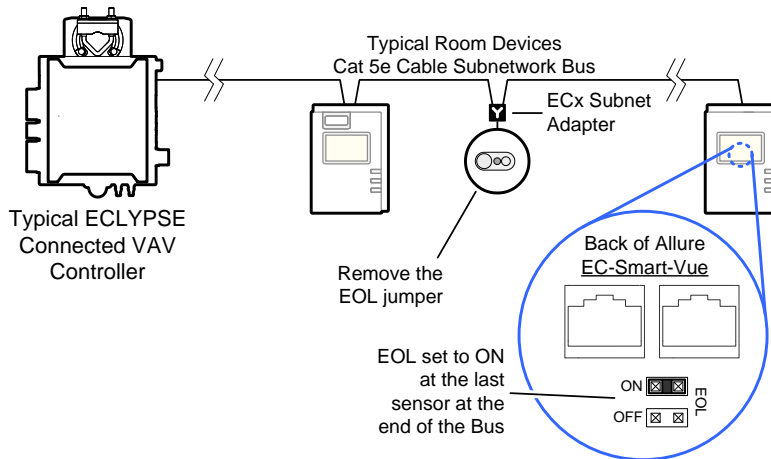


Figure 12-6: Setting the EOL Terminations on the Cat 5e Cable Subnetwork Data Bus ECLYPSE Connected VAV Controllers

Subnetwork Installation Guidelines

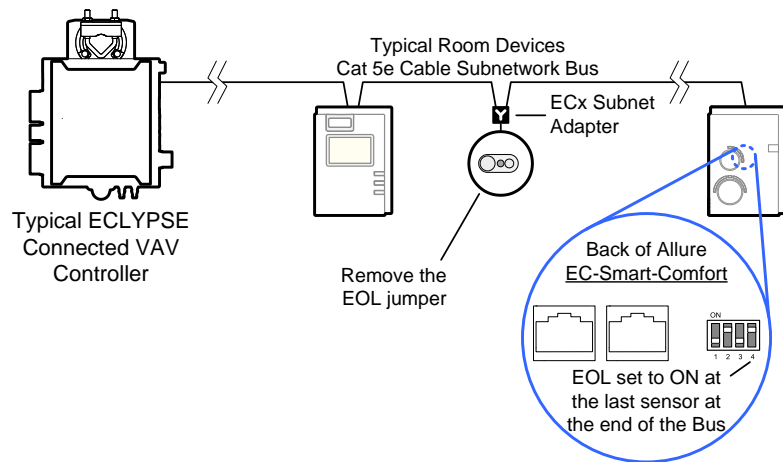


Figure 12-7: Setting the EOL Terminations on the Cat 5e Cable Subnetwork Data Bus ECLYPSE Connected VAV Controllers

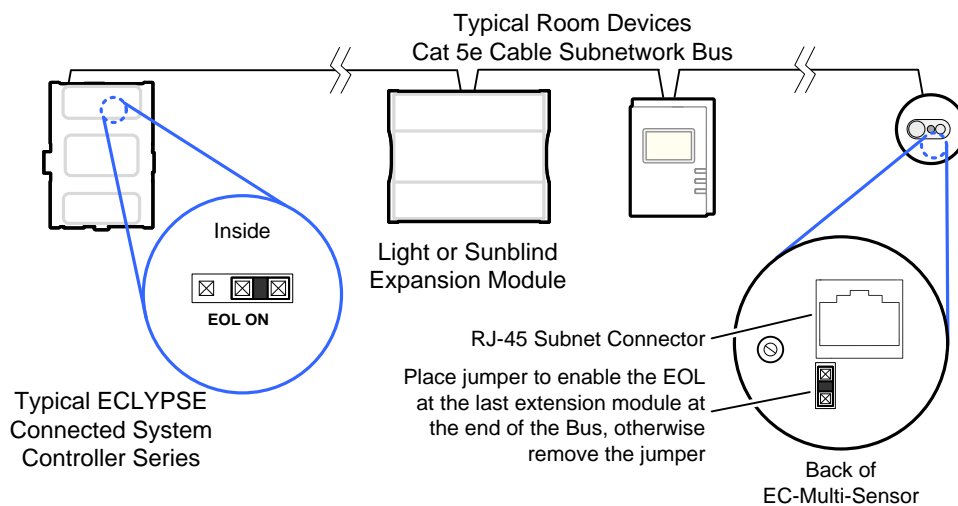


Figure 12-8: Setting the EOL Terminations on the Cat 5e Cable Subnetwork Data Bus for the ECY Series Controller Series Controllers

- Depending on the type of expansion module, the subnetwork data bus EOL may be set by configuring jumpers or DIP switches. Refer to the expansion module's hardware installation guide for how to identify and set a room devices' built-in EOL terminations.

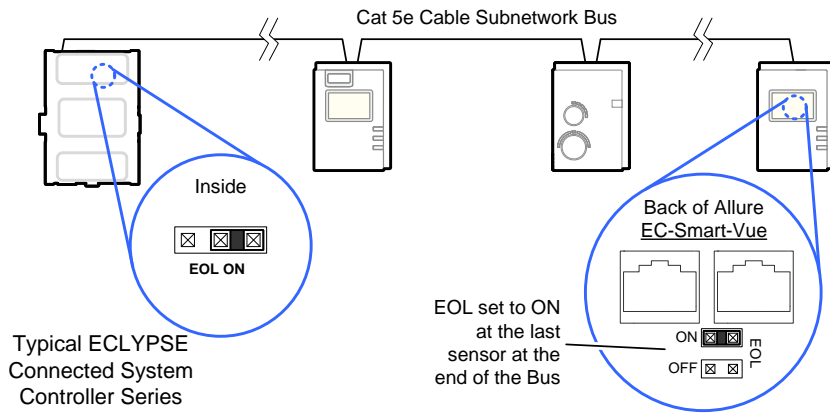


Figure 12-9: Setting the EOL Terminations on the Cat 5e Cable Subnetwork Data Bus for the ECY Series Controller Series Controllers

Setting the Subnet ID Addressing for Room Devices

Each type of room device connected to a controller's **Subnet Port** must be set to a unique subnet ID address. The permitted subnet ID addressing range according to controller model is shown in [Error! Reference source not found.](#). The method to use to set a room device's subnet ID address is shown in the table below.


Room Device Type	Configuration Method	See
Allure EC-Smart-Vue series	Configured in an on-screen menu.	Setting the Allure EC-Smart-Vue Sensor's Subnet ID Address on page 144.
Allure EC-Smart-Comfort sensors	Dip Switch located next to the RJ-45 subnet connectors	Setting the Allure EC-Smart-Air and EC-Smart-Comfort Communicating Sensor Series' Subnet ID Address on page 145
Allure EC-Smart-Air series		
EC-Multi-Sensor series	Rotary selector located next to the RJ-45 subnet connector	Setting the EC-Multi-Sensor Series' Subnet ID Address on page 146
ECx-Light-4 / ECx-Light-4D / ECx-Light-4DALI ECx-Blind-4 / ECx-Blind-4LV	DIP switch located next to Subnet Port connectors	Setting the ECx-Light and ECx-Blind Series' Subnet on page 147

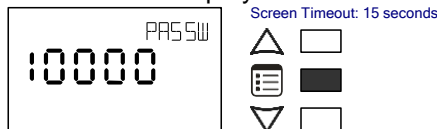
Table 12-6: Subnetwork Module Compatibility and Maximum Supported Quantity Chart


Setting the Allure EC-Smart-Vue Sensor's Subnet ID Address

An Allure EC-Smart-Vue sensor's Subnet ID corresponds to the ComSensor block instance programmed in the controller with EC-gfxProgram. The Allure EC-Smart-Vue sensor's Subnet ID can be set in the procedure below.


ECLYPSE Connected VAV Controllers can be commissioned with an Allure EC-Smart-Vue sensor. The default Subnet ID for an Allure EC-Smart-Vue sensor is 1. To commission an ECLYPSE Connected VAV Controller, the Allure EC-Smart-Vue sensor's Subnet ID must be set to 1. If the Allure EC-Smart-Vue sensor's Subnet ID has been set to another value (for example, the display flashes error code 1 with the Bell icon when the Allure EC-Smart-Vue sensor is connected to a controller for commissioning), change the Subnet ID to 1 as follows:

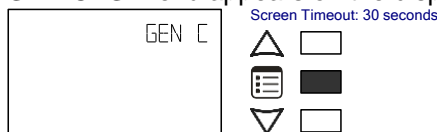
1. Connect an Allure EC-Smart-Vue sensor to the controller with a Cat 5e patch cable. Wait for the Bell icon and the number 1 to flash on the display.
2. Press and hold the **Menu** button  for 5 seconds to enter the password menu. 10000 is shown on the display.





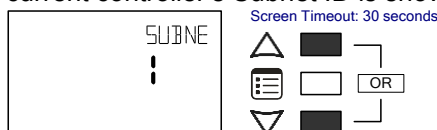
3. Use the down button  to set the number to 9995 (this is the default password).









4. Press the **Menu** button  to submit the password. Upon submitting the password, the **GEN CFG** menu appears on the display.



5. Press the down button  once to enter the **GEN CFG** submenu.
6. Press the **Menu** button  several times until **SUBNET ID** appears on the display. The current controller's Subnet ID is shown.



7. For commissioning purposes, use the up and down buttons   to set the controller's Subnet ID to 1. Tip: Hold down either the up or down button to fast-advance the display value. Otherwise use the up and down buttons   to set the controller's Subnet ID to the ComSensor block instance value programmed in the controller with EC-gfxProgram.
8. Press the **Menu** button  once to apply the value.
9. Press and hold the **Menu** button  for 5 seconds to exit the configuration menu.

The Allure EC-Smart-Vue sensor can now be used to go from one ECLYPSE Connected VAV Controller to the next for commissioning purposes.

When the controller has been programmed, each connected Allure EC-Smart-Vue's Sensor must be assigned a unique Subnet ID.

Setting the Allure EC-Smart-Air and EC-Smart-Comfort Communicating Sensor Series' Subnet ID Address

Each Allure EC-Smart-Air or EC-Smart-Comfort communicating sensor connected to a controller's **Subnet Port** must be set to a unique subnet ID address. This address should correspond to the block number of the associated Subnet Extension block in EC-*gfx*Program. The address is set through a DIP switch located inside the sensor near the RJ-45 connectors.

- ⚠ Allure EC-Smart-Comfort and EC-Smart-Air communicating sensor series share the same Subnet ID range: the same address cannot be assigned concurrently to an Allure EC-Smart-Comfort communicating sensor series and to an Allure EC-Smart-Air communicating sensor series.

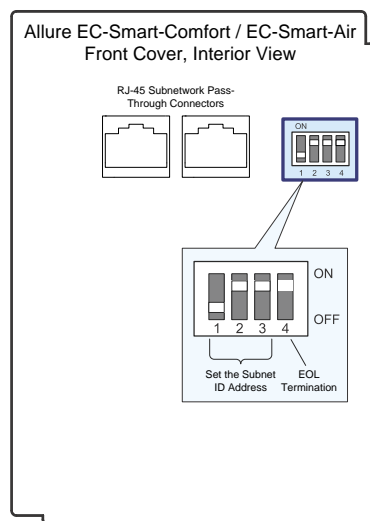


Figure 12-10: Setting the Allure EC-Smart-Air or EC-Smart-Comfort communicating sensor's Subnet ID Address

Switch Position				Allure EC Smart-Air or EC-Smart-Comfort communicating sensor's Subnet ID Address
1	2	3	4	
OFF	OFF	OFF	OFF: EOL disabled ON: EOL enabled	1
ON	OFF	OFF		1
OFF	ON	OFF		2
ON	ON	OFF		3
OFF	OFF	ON		4
ON	OFF	ON		5
OFF	ON	ON		6

Table 12-7: Allure EC-Smart-Air or EC-Smart-Comfort communicating sensor's Subnet ID Address DIP Switch Settings

Figure 12-10 shows an example of how to set the Allure EC-Smart-Air or EC-Smart-Comfort communicating sensor's Subnet ID address DIP switch to 6 and how to set the EOL termination to ON.

Setting the EC-Multi-Sensor Series' Subnet ID Address

Each EC-Multi-Sensor connected to a controller's **Subnet Port** must be set to a unique subnet ID address. This address should correspond to the block number of the associated Multi Sensor block in EC-gfxProgram. The address is set through the rotary selector located next to the **Subnet Port** connector.

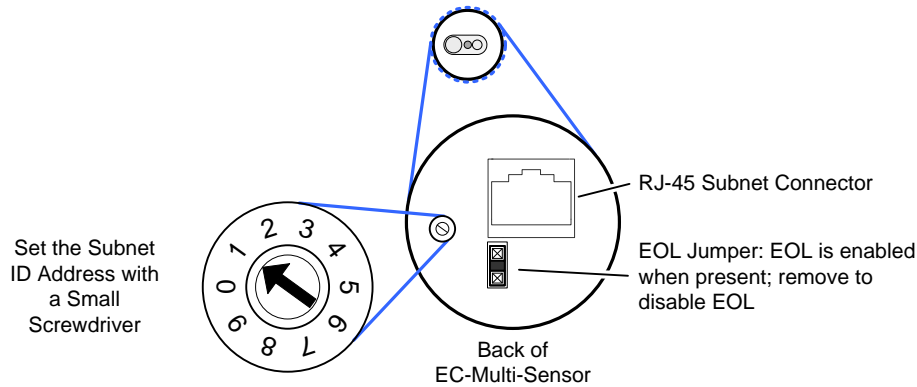


Figure 12-11: Setting the EC-Multi-Sensor Series' Subnet ID Address

Use a small screwdriver (for example, a precision or jeweler's screwdriver) to set the selector. Figure 12-11 shows an example of how to set the EC-Multi-Sensor Series' Subnet ID address DIP switch to 1 and the EOL termination is ON.



Once an EC-Multi-Sensor is installed, the following tip can be used during system commissioning to verify if the EC-Multi-Sensor is set to the correct subnet ID address for the zone in which it is physically located.

Run EC-gfxProgram in debug mode for the controller with 4 *Multi Sensor* block instances, 1 to 4. Set a remote control to zone ID 0, then aim it at the EC-Multi-Sensor and press a command (fan speed button for example). In EC-gfxProgram, see which block instance shows an output (*RemoteFanSpeed*). Usually it is easier to reassign *Multi Sensor* block numbers in EC-gfxProgram code than it is to change the Subnet ID Address of an installed EC-Multi-Sensor.

Setting the ECx-Light and ECx-Blind Series' Subnet ID Address

Each ECx-Light and ECx-Blind Series' connected to a controller's **Subnet Port** must be set to a unique subnet ID address. The address is set through the DIP switch located next to the **Subnet Port** connectors.

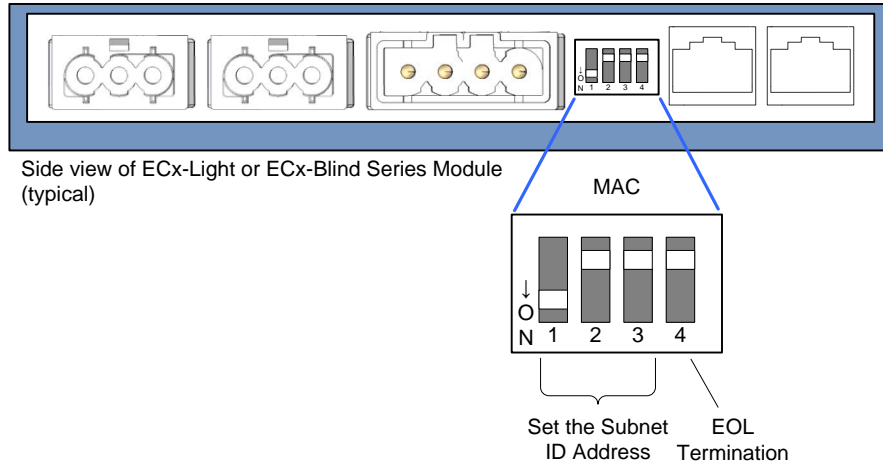


Figure 12-12: Setting the ECx-Light and ECx-Blind Series' Subnet ID Address (Typical)

Switch Position				Expansion Module's Subnet ID (MAC) Address
1	2	3	4	
OFF	OFF	OFF	OFF	See Table 12-9
ON	OFF	OFF	OFF	1
OFF	ON	OFF	OFF	2
ON	ON	OFF	OFF	3
OFF	OFF	ON	OFF	4

Table 12-8: ECx-Light and ECx-Blind Series' Subnet ID Address DIP Switch Settings

Figure 12-12 shows an example of how to set the ECx-Light and ECx-Blind series' Subnet ID address DIP switch to 1 and how to set the EOL termination to OFF.

Auto-assigned Subnet ID Address for Light and Blind Expansion Modules

Often only one type of expansion module is connected to the controller; for example, one ECx-Light-4 and one ECx-Blind-4 model. By leaving the Subnet ID address DIP switch at 0 (factory default position) for these two expansion modules, the ECx-Light and ECx-Blind room device sets its own Subnet ID Address according to its model type so no configuration is necessary.

Expansion Module Model Type	Auto-assigned Subnet ID Address when the expansion modules' MAC DIP Switch is set to 0 (factory default position)			
	1	2	3	4
ECx-Light-4 (4 lights 230V)	■			
ECx-Light-4DALI (4 DALI buses)	■			

Subnetwork Installation Guidelines

Expansion Module Model Type	Auto-assigned Subnet ID Address when the expansion modules' MAC DIP Switch is set to 0 (factory default position)			
	1	2	3	4
ECx-Light-4D (4 dimming lights)		■		
ECx-Blind-4 (4 blinds/shades 230V)			■	
ECx-Blind-4LV (4 blinds/shades 24V)				■

Table 12-9: ECx-Light and ECx-Blind Series' Automatic Subnet ID Address when the DIP Switch is set to 0

If you connect a second expansion module of the same type to the controller's subnetwork data bus, you must set at least one of the two expansion modules' MAC DIP switch to a unique (that is, unused) subnet ID (MAC) address and then set the same value in **Default address** in EC-gfxProgram. See "Manage Light and Sunblind Module Instances" in the EC-gfxProgram User Guide.

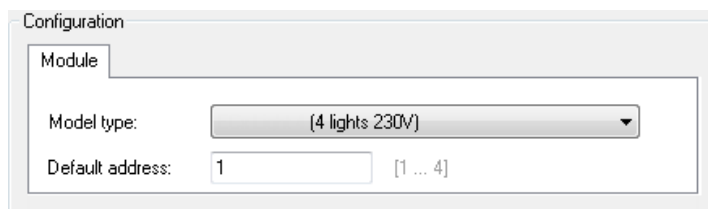


Figure 12-13: In EC-gfxProgram: Default Address: Setting an Expansion Modules' Subnet ID (MAC) Address for this Expansion Module Instance

Auto Learn Light and Blind/Shade Expansion Modules in EC-gfxProgram

In EC-gfxProgram, when the connection status for the controller is **Connected**, this scans the controller's subnetwork data bus for connected expansion modules, when each expansion module has a unique subnet ID (MAC) address on the controller's subnetwork data bus. Using this feature will delete any previously configured expansion modules. See "Manage Light and Sunblind Module Instances" in the EC-gfxProgram User Guide.

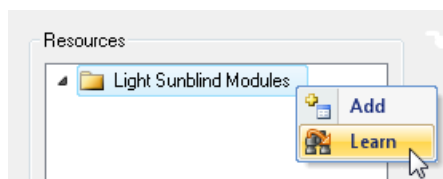


Figure 12-14: Light and Blind/Shade Modules Tree Options



Learn is only available after 2 minutes of the controller having been powered up. This information is no longer available after 30 minutes. Reboot the controller if **Learn** is unable to find the connected modules (in Project Synchronization, select **Download to device** and **Reboot controller** only).

Commissioning a Connected VAV Controller with an Allure EC-Smart-View Sensor

Commissioning a Connected VAV Controller with an Allure EC-Smart-View sensor involves the following tasks:

- Set the Allure EC-Smart-View sensor's Subnet ID. See [Setting the Allure EC-Smart-View Sensor's Subnet ID Address](#) on page 144.
- For controllers that support preloaded applications: Select the controller's preloaded application to use. See the ECY-VAV [Preloaded Application User Guide](#) for more Information.

CHAPTER 13

MODBUS TCP CONFIGURATION

This chapter describes the Modbus TCP Configuration.

In This Chapter

Topic	Page
Modbus TCP Device Connection	151
Device Addressing	152

Modbus TCP Device Connection

Modbus TCP devices are connected to the same subnet that the controller is connected to:

- Connect the Modbus TCP device to the same network switch/router that the controller is connected to.
- Connect the Modbus TCP device to either one of the controller's Ethernet ports.

Device Addressing

Device addressing allows the coordinated transfer of messages between the master (the ECY Series Controller) and the slave Modbus TCP device. For this, each Modbus TCP device is identified by its address.

About the Device Address

Each slave device must have its own unique address number in the range from 1 to 254.

Refer to the device's hardware installation guide for information about how to set its address number.

Set the Modbus device parameters with EC-gfxProgram in the Resources Configuration window, Modbus Device block.

General

Name: Modbus Device 1
Description:

Modbus

Network: TCP/IP
IP address: 164.0.12.22
IP port: 502 [1 ... 65,535]
Address: 1 [1 ... 254]

Encoding

Int16 byte ordering: Byte Swap
Int32 byte ordering: Byte Swap Word Swap
Int64 byte ordering: Byte Swap Word Swap Double Word Swap
Float byte ordering: Byte Swap Word Swap
Double byte ordering: Byte Swap Word Swap Double Word Swap

Options

Supports write multiple coils:
Supports write multiple registers:
Maximum read coils: 2,000 [1 ... 2,000]
Maximum write coils: 1,968 [1 ... 1,968]
Maximum read registers: 125 [1 ... 125]
Maximum write registers: 123 [1 ... 123]
Request timeout: 1 s
Request throttle: 0 s

Figure 13-1: Setting the Modbus Device Parameters in EC-gfxProgram's Resources Configuration Window

See the [EC-gfxProgram User Guide](#) for more information.

CHAPTER 14

MODBUS RTU COMMUNICATION DATA BUS FUNDAMENTALS

This chapter describes the Modbus RTU Communications Data Bus operating principles.

In This Chapter

Topic	Page
Modbus RTU Data Transmission Essentials	155
Maximum Number of Modbus RTU Devices on a Data Bus Segment and Baud Rate	156
Data Bus Physical Specifications and Cable Requirements	158
Data Bus Topology and EOL Terminations	159
Data Bus Shield Grounding Requirements	161
Device Addressing	162

Modbus RTU Data Transmission Essentials

The ECY Series Controller can support either BACnet MS/TP or Modbus RTU network on its RS-485 port. This option is selected in the controller’s web interface. When the ECY Series Controller is configured for Modbus RTU, it acts as the Modbus master that initiates requests to any slave device connected to this data bus. All slave devices must support Modbus RTU communications protocol. The ECY Series Controller does not work with Modbus ASCII devices.

The Modbus network communication parameters and the Modbus device parameters are configured with EC-gfxProgram in the Resources Configuration window, Modbus Device block.

The Modbus RTU data bus protocol uses the EIA-485 (RS-485) 3-wire physical layer standard for data transmission. EIA-485 is a standard that defines the electrical characteristics of the ECLYPSE Wi-Fi Adapters and drivers to be used to transmit data in a differential (balanced) multipoint data bus that provides high noise immunity with relatively long cable lengths which makes it ideal for use in industrial environments. The transmission medium is inexpensive and readily-available twisted pair shielded cable.

While there are many possible LAN topologies for an EIA-485 data bus, only devices that are daisy-chained together are allowed with Modbus RTU (see [Figure 14-5](#)).

End-of-line (EOL) terminations are critical to error-free EIA-485 data bus operation. The impedance of the cable used for the data bus should be equal to the value of the EOL termination resistors (typically 120 ohms). Cable impedance is usually specified by the cable manufacturer.

Modbus RTU Data Bus is Polarity Sensitive

The polarity of all devices that are connected to the Modbus RTU data bus must be respected. The markings to identify the polarity can vary by manufacturer. The following table summarizes the most common identification labels for Modbus RTU data bus polarity.

Table 14-1: Common Identification Labels for Modbus RTU Data Bus Polarity for Distech Controls’ Products

Distech Controls Product	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
ECY Series Controller	NET –	NET +	S

Table 14-2: Common Identification Labels for Modbus RTU Data Bus Polarity for other Manufacturers

Device Manufacturer	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
Common identification labels for Modbus RTU data bus polarity by other Manufacturers	D0	D1	SC, C, or C’
	A or A’	B or B’	Common
	Data –	Data +	Data 0V



When interfacing with Modbus RTU devices from other manufacturers, refer to the documentation provided with the device to correctly wire the device.

Maximum Number of Modbus RTU Devices on a Data Bus Segment and Baud Rate

The number of Modbus devices supported by an ECY Series Controller is software limited according to the controller model purchased. See the controller's datasheet for more information. For ECY Series Controller models that are not software limited, the controller can support a combined maximum of 32 Modbus RTU and Modbus TCP devices.

Data Bus Segment Addressing Range for Modbus RTU Devices

The Modbus RTU device address range is 1 to 254. Address 0 is used to broadcast messages to all slave devices and write only. When address 0 is used to broadcast a message, there is no confirmation that the message was properly received by any slave device.

However, it is recommended that any given data bus segment have no more than 50 devices, when a baud rate of 19 200 or higher is used for the Modbus RTU Data Bus. A repeater counts as a device on each data bus segment to which it is connected.

Baud Rate

Most devices will have a range of baud rate settings and possibly an AUTO setting that detects the baud rate of other devices transmitting on the data bus and adjusts the baud rate of the device accordingly. Typical baud rates are 9600, 19 200, 38 400, and 76 800. The baud rate setting determines the rate at which data is sent on the Modbus RTU data bus.

All devices on the data bus must be set to the same baud rate. Therefore, the chosen baud rate must be supported by all devices connected to the data bus.

The recommended baud rate is 38 400.

We recommend that you:

- Set the baud rate of two controllers on a Modbus RTU Data Bus Segment to the same baud rate to provide failover protection.

For example, set the baud rate of the ECY Series Controller (if equipped) and one other controller to 38 400 baud. If the ECY Series Controller becomes unavailable and there is a power cycle, the controller will set the baud rate for the Modbus RTU Data Bus.

- Set all other devices to automatically detect the baud rate, if this option is available.

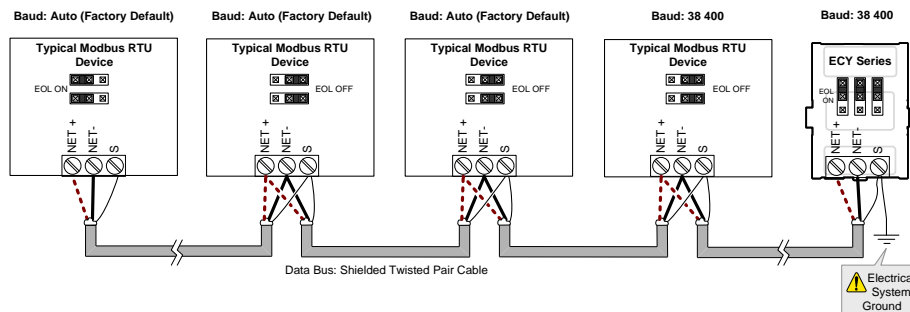


Figure 14-1: Setting the Baud rate on two Controllers on a Modbus RTU Data Bus Segment for Failover Protection

Set the Modbus network communication parameters with EC-gfxProgram in the Resources Configuration window, Modbus Device block.

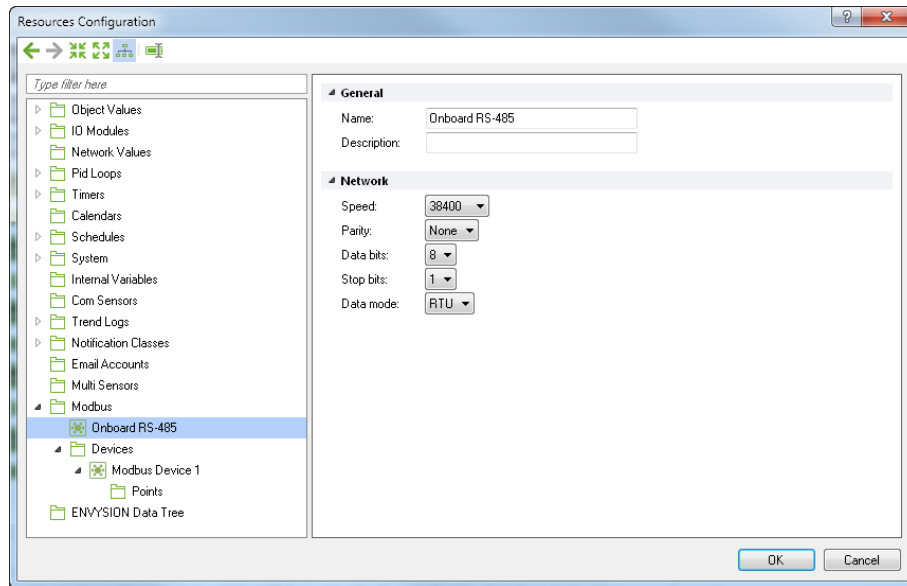


Figure 14-2: Setting the Modbus Network Communication Parameters in EC-gfxProgram's Resources Configuration Window

See the [EC-gfxProgram User Guide](#) for more information.

Data Bus Physical Specifications and Cable Requirements

Cables composed of stranded conductors are preferred over solid conductors as stranded conductor cable better resist breakage during pulling operations. Distech Controls strongly recommends that the following data bus segment cable specifications be respected.

Table 14-3: Modbus RTU Data Bus Segment Physical Specifications and Cable Requirements

Parameter	Details
Media	Twisted pair, 24 AWG (see also Metric Conversions for Wire Gauge on page 173)
Shielding	Foil or braided shield
Shield grounding	The shield on each segment is connected to the electrical system ground at one point only; see Data Bus Shield Grounding Requirements on page 161.
Characteristic impedance	100-130 Ohms. The ideal is 100-120 Ohms.
Distributed capacitance between conductors	Less than 100 pF per meter (30 pF per foot). The ideal is less than 60 pF per meter (18pF per foot).
Distributed capacitance between conductors and shield	Less than 200 pF per meter (60 pF per foot).
Maximum length per segment	1220 meters (4000 feet)
Data Rate	9600, 19 200, 38 400, and 76 800 baud
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections)
EOL terminations	120 ohms at each end of each segment
Data bus bias resistors	510 ohms per wire (max. of two sets per segment)

Shielded cable offers better overall electrical noise immunity than non-shielded cable. Unshielded cable or cable of a different gauge may provide acceptable performance for shorter data bus segments in environments with low ambient noise.

Table 14-4: Distech Controls Recommended Cable Types for Modbus RTU Data Buses

Cable Type	Part Number	O.D. (Ø)
300 meters (1000 feet), 24 AWG Stranded, Twisted Pair Shielded Cable – FT6, Rated for Plenum Applications	CB-BACN6BL1000	3.75mm (0.148 in.)

Distech Controls Modbus RTU cable offers the best performance over the full range of baud rates, cable lengths, and number of connected devices. This is primarily due to lower conductor-to-conductor capacitance of this cable.

Data Bus Topology and EOL Terminations

Function of EOL Terminations

The first and last device on the data bus must have End-of-Line (EOL) termination resistors connected across the two data lines/wires of the twisted pair. These resistors serve the following purposes:

- EOL terminations dampen reflections on the data bus that result from fast-switching (high-speed rising and falling data edges) that otherwise would cause multiple data edges to be seen on the data bus with the ensuing data corruption that may result. The higher the baud rate a data bus is operating at, the more important that EOL terminations be properly implemented. Electrically, EOL terminations dampen reflections by matching the impedance to that of a typical twisted pair cable.
- EIA-485 data bus transmitters are tri-state devices. That is they can electrically transmit 1, 0, and an idle state. When the transmitter is in the idle state, it is effectively offline or disconnected from the data bus. EOL terminations serve to bias (pull-down and pull-up) each data line/wire when the lines are not being driven by any device. When an un-driven data bus is properly biased by the EOL terminations to known voltages, this provides increased noise immunity on the data bus by reducing the likelihood that induced electrical noise on the data bus is interpreted as actual data.

When to Use EOL Terminations

EOL terminations should only be enabled / installed on the two devices located at either end of the data bus. All other devices must not have the EOL terminations enabled/installed.

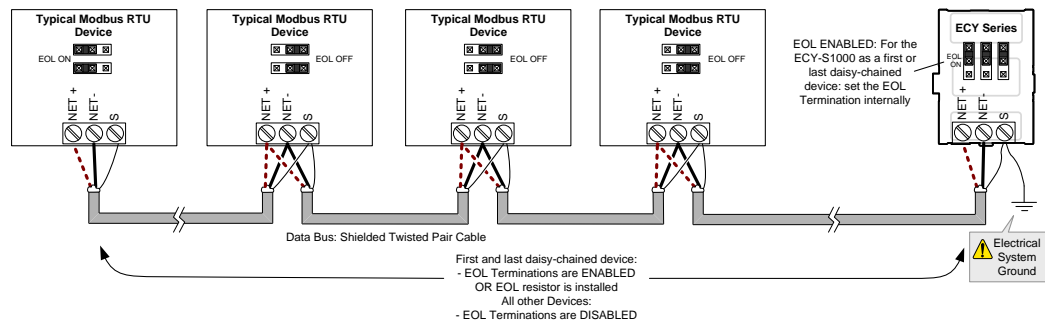


Figure 14-3: EOL Terminations Must be Enabled at Both the First and Last Device on the Data Bus

Devices with built-in EOL terminations are factory-set with the EOL termination disabled by default.

The *BACnet/IP to MS/TP Adapter* does not have EOL Termination (and Modbus RTU Data Bus biasing) capabilities to be used at the end of a Modbus RTU data bus. Instead, use the *BACnet/IP to MS/TP Router* for this application.

About Setting Built-in EOL Terminations

ECY Series Controllers have built-in EOL terminations. These Controllers use jumpers to enable the EOL resistors and biasing circuitry. Refer to the [ECLYPSE Connected System Controller Hardware Installation Guide](#) or to the [ECLYPSE Connected VAV Controller Hardware Installation Guide](#) for more information.

Refer to the Modbus RTU device's Hardware Installation Guide for how to identify and set a device's built-in EOL terminations.

Only a Daisy-Chained Data Bus Topology is Acceptable

Use a daisy-chained Modbus RTU data bus topology only. No other data bus topology is allowed.



Only linear, daisy-chained devices provide predictable data bus impedances required for reliable data bus operation. Only a daisy-chained data bus topology should be specified during the planning stages of a project and implemented in the installation phase of the project.

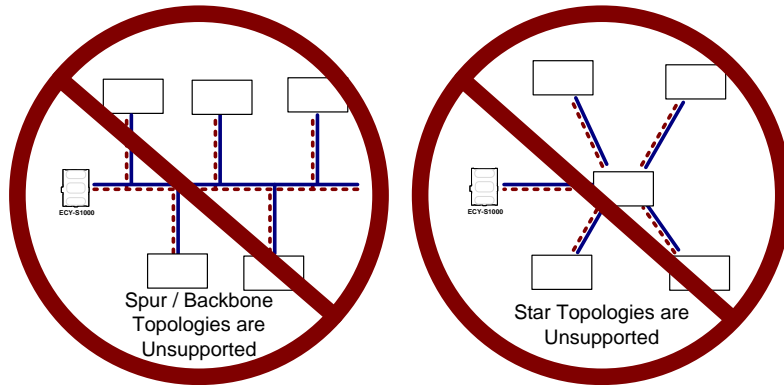



Figure 14-4: Unsupported Modbus RTU Data Bus Topologies

Data Bus Shield Grounding Requirements

The EIA-485 data bus standard requires that the data bus must be shielded against interference. A Modbus RTU data bus must also be properly grounded.

The data bus' cable shields must be twisted together and connected to the **S** or shield terminal at each ECY Series Controller. Keep the cable shield connections short and take steps at each device to isolate the cable shield from touching any metal surface by wrapping them with electrical tape, for example. Note that for ECY Series Controllers, the data bus' cable shield provides the ground reference for the data bus. If the controller is at the end of the BACnet MS/TP data bus, simply connect the data bus shield to the **S** terminal.

 Grounding the shield of a data bus segment in more than one place will more than likely reduce shielding effectiveness.

Modbus RTU Data Bus Shield Grounding Requirements

The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the ECY Series Controller, as shown below in [Figure 14-5](#) and [Figure 14-6](#).

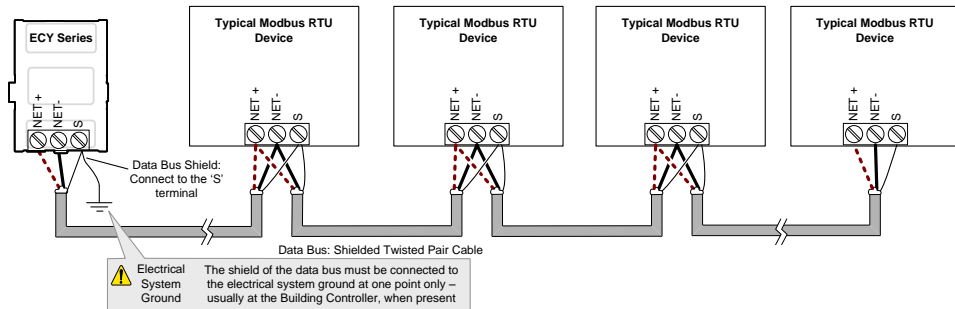


Figure 14-5: Typical Cable-Shield Grounding Requirements for a Modbus RTU Data Bus Segment with an ECY Series Controller located at the End of the Data Bus

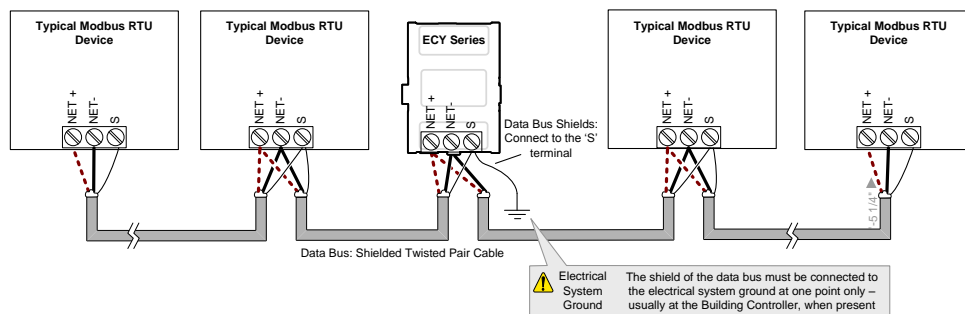


Figure 14-6: Typical Cable-Shield Grounding Requirements for a Modbus RTU Data Bus Segment with an ECY Series Controller located in the Middle of the Data Bus

Device Addressing

Device addressing allows the coordinated transfer of messages between the master (the ECY Series Controller) and the slave Modbus RTU device. For this, each device connected to the Modbus RTU data bus is identified by its address.

About the Device Address

Each slave device must have its own unique address number in the range from 1 to 247.

Refer to the device's hardware installation guide for information about how to set its address number.

Set the Modbus device parameters with EC-gfxProgram in the Resources Configuration window, Modbus Device block.

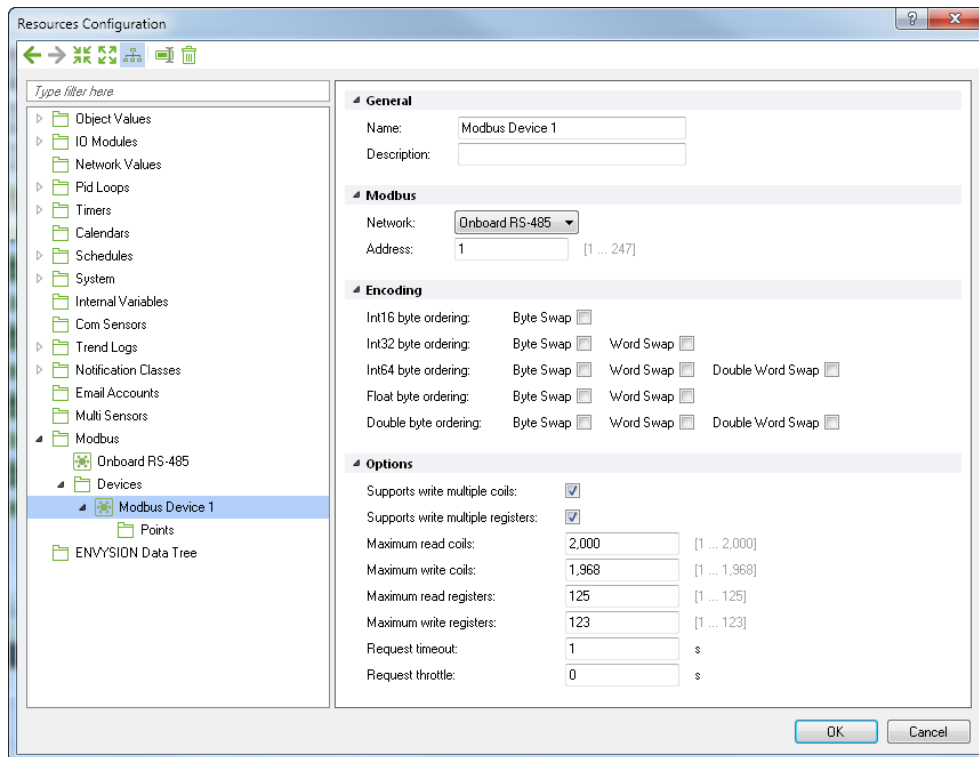


Figure 14-7: Setting the Modbus Device Parameters in EC-gfxProgram's Resources Configuration Window

See the [EC-gfxProgram User Guide](#) for more information.

CHAPTER 15

RESETTING OR REBOOTING THE CONTROLLER

This chapter describes how to recover control over the controller by resetting it to the factory default settings.

In This Chapter

Topic	Page
Resetting or Rebooting the Controller	164

Resetting or Rebooting the Controller

The reset button is located between the RS-458 and Ethernet connectors on connected system controllers and underneath the cover on connected VAV controllers. Depending on the amount of time the reset button is held down, different actions are taken by the controller.

Hold Reset for	To
5 seconds	Restart / reboot the controller.
10 seconds	Reset both Ethernet and Wi-Fi IP addresses back to factory default settings.
20 seconds	Reset the controller to its factory default settings. User accounts (user names and passwords) will also be reset to the factory default settings and the controller license will be cleared.



Always backup the controller's license through the controller's Web interface before you hold the reset button for 20 seconds. Once the controller reboots, you will have to install the license through the controller's Web interface. To backup and install the license, see [System Settings](#) on page 91. Click **Export To PC** to backup the controller's license to your PC. Click **Import From PC** to restore the controller's license file from your PC.

CHAPTER 16

ECY CONTROLLER TROUBLESHOOTING

Table 16-1: Troubleshooting ECY Controller Symptoms

Symptom	Possible Cause	Solution
Controller is powered but does not turn on	Fuse has blown (for 24V controllers)	Disconnect the power. Check the fuse integrity. Reconnect the power.
	Power supply polarity	Verify that consistent polarity is maintained between all controllers and the transformer. Ensure that the COM terminal of each controller is connected to the same terminal on the secondary side of the transformer. See DHCP versus Manual Network Settings on page 19.
	The device does not have power / poor-quality power (for 24V controllers)	Verify that the transformer used is powerful enough to supply all controllers. See Transformer Selection and Determining the Maximum Power Run Length on page 131.
Device does not communicate on the BACnet MS/TP network	Absent or incorrect supply voltage (for 24V controllers)	1. Check power supply voltage between 24VAC/DC and 24V COM pins and ensure that it is within acceptable limits ($\pm 15\%$ for 24V controllers). 2. Check for tripped fuse or circuit breaker.
	Overloaded power transformer (for 24V controllers)	Verify that the transformer used is powerful enough to supply all controllers. See Transformer Selection and Determining the Maximum Power Run Length on page 131.
	Network not wired properly	Double check that the wire connections are correct.
	Absent or incorrect network termination	Check the network termination(s).
	Max Master parameter	Configure the Max Master to the highest MAC Address of any device on the MS/TP data bus. See Setting the Max Master and Max Info Frames on page 127.
	There is another controller with the same MAC Address on the BACnet MS/TP data bus	Each controller on a BACnet MS/TP data bus must have a unique MAC Address. Look at the MAC Address DIP switch on the faceplate of each controller. If it is set to 0 (all off), use an Allure EC-Smart-Vue sensor to check the MAC Address.
	There is another controller with the same Device ID on the BACnet intranetwork	Each controller on a BACnet intranetwork (the entire BACnet BAS network) must have a unique Device ID. Use an Allure series communicating sensor to check the Device ID of each controller. See Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers on page 127.
	BACnet data bus polarity is reversed.	Ensure the polarity of the BACnet data bus is always the same on all devices. See BACnet MS/TP Data Bus is Polarity Sensitive on page 110.

Symptom	Possible Cause	Solution
	Cut or broken wire.	Isolate the location of the break and pull a new cable.
	The BACnet data bus has one or more devices with the same MAC Address.	See Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers on page 127.
	The baud rate for all devices are set to AUTO	At least one device must be set to a baud rate, usually the data bus master. See Baud Rate on page 113.
	The device is set to a MAC Address in the range of 128 to 255.	See if the STATUS LED on the device is showing a fault condition. See Table 16-2 for a list of fault codes. This range is for slave devices that cannot initiate communication. All Distech Controls' devices are master devices and must their MAC Address set accordingly. See Device Addressing on page 125.
	The maximum number of devices on a data bus segment has been exceeded.	Use a repeater to extend the BACnet data bus. See Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate on page 112.
The STATUS LED is blinking	The device has auto-diagnosed a fault condition	See Table 16-2 for a list of fault codes.
Controller communicates well over a short network BACnet MS/TP network, but does not communicate on large network	Network length	Check that the total wire length does not exceed the specifications of the Network Guide: Data Bus Physical Specifications and Cable Requirements on page 115.
	Wire type	Check that the wire type agrees with the specification of the Network Guide: Data Bus Physical Specifications and Cable Requirements on page 115.
	Network wiring problem	Double check that the wire connections are correct.
	Absent or incorrect network termination	Check the network termination(s). Incorrect or broken termination(s) will make the communication integrity dependent upon a controller's position on the network.
	Number of controllers on network segment exceeded	The number of controllers on a channel should never exceed 50. Use a router or a repeater: See Data Bus Segment MAC Address Range for BACnet MS/TP Devices on page 112.
	Max Master parameter	Configure the maximum number of master device on the MS/TP network in all devices to the controller's highest MAC address used on the MS/TP trunk. See BACnet MS/TP Data Bus Token-Passing Overview on page 126.
Hardware input is not reading the correct value	Input wiring problem	Check that the wiring is correct according to the module's hardware installation manual and according to the peripheral device's manufacturer recommendations.

Symptom	Possible Cause	Solution
	Open circuit or short circuit	Using a voltmeter, check the voltage on the input terminal. For example, for a digital input, a short circuit shows approximately 0V and an open circuit shows approximately 5V. Correct wiring if at fault.
	Configuration problem	Using the controller configuration wizard, check the configuration of the input. Refer to the controller's user guide for more information.
	Over-voltage or over-current at an input	An over-voltage or over-current at one input can affect the reading of other inputs. Respect the allowed voltage / current range limits of all inputs. Consult the appropriate datasheet for controller input range limits.
Hardware output is not operating correctly	Fuse has blown (Auto reset fuse, for 24V controllers)	Disconnect the power and outputs terminals. Then wait a few seconds to allow the auto-reset fuse to cool down. Check the power supply and the output wiring. Reconnect the power.
	Output wiring problem	Check that the wiring is correct according to the module's hardware installation manual and according to the peripheral device's manufacturer.
	Configuration problem	With EC-gfxProgram, check the configuration of the output; for example, is it enabled? Refer to the EC-gfxProgram User Guide for more information.
	0-10V output, 24VAC powered actuator is not moving	Check the polarity of the 24VAC power supply connected to the actuator while connected to the controller. Reverse the 24VAC wire if necessary.

Refer to the controller's Hardware Installation Guide for how to identify and set a controller's configuration jumpers and switches.

Table 16-2: LED Fault Condition Interpretation for ECB Devices

ECB Device LED Interpretation	Description	Solution
RX LED not blinking	Data is not being received from the BACnet MS/TP data bus.	If there is no communication, see Table 16-1 .
TX LED not blinking	Data is not being transmitted onto the BACnet MS/TP data bus.	
POWER constant on	Power is available at the device. However this does not mean that the quality of supplied power is good. See Power Supply Requirements for 24VAC-Powered Controllers on page 19.	If not lit, see Power Supply Requirements for 24VAC-Powered Controllers on page 130 for the power requirements.
STATUS blinking	See below.	–

Table 16-3: STATUS LED Interpretation for Normal Operation with ECB Devices

Device STATUS LED blink patterns	Status	Description
One fast blink ●	Initialization	The device is starting up.
The STATUS LED is always OFF (Not applicable to ECB-PTU Series)	No anomaly	Normal operation.

Table 16-4: Verify that the Following Recommendations have been Carried Out Before Calling Technical Support

Recommendation	Description
Properly terminate the BACnet MS/TP data bus	EOL terminations must be enabled / installed at either end of the data bus only. See Figure 11-2 .
Avoid duplicate MAC Addresses	Verify that no device has a duplicate MAC Address by checking the MAC Address DIP switch settings on all devices on the data bus, including segments connected by a repeater. If necessary, isolate devices from the data bus to narrow-down the number of devices that may be at fault.
All devices must be set to the same baud rate	When all devices are set to AUTO baud rate, at least one device must be set to a baud rate, usually the data bus master. See Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate on page 112.
The data bus is polarity sensitive	Ensure that the polarity of all data bus wiring is consistent throughout the network. See BACnet MS/TP Data Bus is Polarity Sensitive on page 110.
Do not overload the data bus with Change of Value (COV) reporting	COV reports create the most traffic on the BACnet MS/TP data bus. Set the COV report rate to the largest value that provides acceptable performance. Only map COV reports for values that are necessary. For mapped analog points that are continuously changing, try increasing the COV increment on these points or set the COV minimum send time flag to true to send the value at a regular frequency.
Do not leave address holes in the device's MAC Address range	Assign MAC Address to device starting at 3, up to 127. Do not skip addresses. Set the maximum MAC Address in the ECY Series Controller to the final MAC Address number actually installed. NOTE: The physical sequence of the MAC Address of the devices on the data bus is unimportant: For example, the MAC Address of devices on the data bus can be 5, 7, 3, 4, 6, and 8.
Only daisy-chained devices are acceptable	Eliminate T-taps and star configurations. Use a router to connect a data bus spur.
Connect no more than five devices to a power supply transformer (for 24V controllers)	BACnet MS/TP devices require good power quality. See Power Supply Requirements for 24VAC-Powered Controllers on page 130.

CHAPTER 17

ALLURE EC-SMART-VUE COMMUNICATING SENSOR TROUBLESHOOTING

Table 17-1: Allure EC-Smart-Vue Sensor Normal Operation

Symptom	Status	Description
When the Allure EC-Smart-Vue sensor is connected to a Controller, the LCD display on the Allure EC-Smart-Vue sensor is blank with the backlight ON for about 30 to 45 seconds	Firmware upgrade in progress	Wait for the upgrade to complete. Do not disconnect the Allure EC-Smart-Vue sensor from the controller as the upgrade will only restart once it is reconnected.

Table 17-2: Troubleshooting Allure EC-Smart-Vue Sensor Symptoms

Symptom	Possible Cause	Solution
Allure EC-Smart-Vue sensor screen is blank & back light is off	Is the Allure EC-Smart-Vue sensor connected to the controller?	Verify that the Allure EC-Smart-Vue sensor is connected to the controller and that the patch cables are plugged-in to the connectors. See Cat 5e Cable Subnetwork on page 139 for more information.
	Is power being supplied to the controller?	There may be no power being supplied from the controller. Check if the controller has power or if the controller's internal fuses have blown or tripped.
	Is the cable connected to the controller and Allure EC-Smart-Vue sensor?	Verify wiring.
	Was the patch cable made onsite?	Verify that the RJ-45 crimp connectors were installed on the cable correctly. See Cat 5e Cable Subnetwork on page 139 for more information.
Device is not communicating with controller	Is the address correctly set to a unique address?	Each Allure EC-Smart-Vue sensor must be set to a unique address for each controller. See Commissioning a Connected VAV Controller with an Allure EC-Smart-Vue Sensor on page 149.
	Is the device too far from controller?	Verify the distance between the device and the controller. See Subnetwork Data Bus Length on 137.
	Is there a configuration problem?	With EC-gfxProgram, check the configuration of the sensor, for example, is it enabled? Refer to the EC-gfxProgram User Guide for more information.
	Have the subnetwork EOL settings been correctly set?	Only the last module on the subnetwork data bus must have its EOL termination set to ON. See Figure 12-6 , Figure 12-8 , and Figure 12-9 .

Symptom	Possible Cause	Solution
Allure EC-Smart-View sensor motion detector window indicator is always ON	Does the connected controller have Allure EC-Smart-View sensor firmware that supports the motion and CO ₂ sensor?	When the Allure EC-Smart-View sensor is connected to a controller, its firmware is loaded from the controller. In this case, the controller has an earlier version of Allure EC-Smart-View sensor firmware that does not support the motion or CO ₂ sensor. To upgrade to the latest Allure EC-Smart-View sensor firmware, download the firmware from SmartInstaller and refer to the firmware upgrade procedure in the EC-gfxProgram User Guide .
The Motion or CO ₂ output of the associated ComSensor block always reads NULL in EC-gfxProgram		
The CO ₂ sensor readings are too high, too low, or inconsistent between sensors	Immediately after installing the Allure EC-Smart-View sensor with CO ₂ sensors, are the CO ₂ sensor readings incoherent?	<p>If the CO₂ sensor readings seem unusual or show inconsistencies between sensors in the same building right after installation, the following reasons should be taken into consideration:</p> <ul style="list-style-type: none"> • Concentration levels in each space may be different • The installer may have unintentionally blown into the sensor while installing it. • The sensor may have been dropped or mishandled during shipment causing a minor shift in the original factory calibration. <p>Allow up to 14 days of operation (without power interruptions) for the sensor to calibrate itself according to its new environment.</p>

Table 17-3: Error code Interpretation for Allure EC-Smart-View Sensor Symptoms

Symptom	Possible Cause	Corrective action
Clock icon flashing for 15 seconds	Cannot communicate with controller.	Wait for the communication link to the controller to be established. Verify wiring. Verify that all Allure EC-Smart-View sensor's Subnet IDs are unique for this controller. See Setting the Allure EC-Smart-View Sensor's Subnet ID Address on page 144.
After 15 seconds: Error code 1 with Bell icon		
Error code 2 with Bell icon	Invalid configuration.	In EC-gfxProgram, resynchronize the code with the controller. Contact Distech Controls Customer Support.
Error code 3 with Bell icon	Allure EC-Smart-View sensor is not properly configured in the controller	With EC-gfxProgram, check the configuration of the sensor, for example, is the ComSensor block enabled? Refer to the EC-gfxProgram User Guide for more information.

CHAPTER 18

WI-FI NETWORK TROUBLESHOOTING GUIDE

Any wireless system consists of two or more Wi-Fi transceivers and a radio propagation path (Radio Path). Problems encountered can be any of the following.

Symptoms	Probable Causes	Corrective actions
Wi-Fi communications are inexistent or intermittent	Presence of a low power jammer	If the low power jammer is close to the transceiver antenna, move low power jammer (PC, telephone, etc.) at least 6.5 feet (2 m) away from transceiver antenna.
		Change the Wi-Fi channel on the router. Use a Wi-Fi surveying or Wi-Fi stumbling tool on a laptop computer to identify unused Wi-Fi channels that may provide a better interference-free radio path.
		Move the ECLYPSE Wi-Fi Adapter's position where it has a clear line of sight to the router.
		Move the wireless router's position. Try moving the router to the center of the room where it has a clear line of site to each wireless device.
	Presence of a high power jammer	Remove high power jammer if possible. If not, you will have to accept strong range reduction or add another wireless router closer to the controller(s).
		Use a wired Ethernet connection to the controller.
Defective ECLYPSE Wi-Fi Adapter	Exchange the wireless dongle with another ECLYPSE Wi-Fi Adapter. If the dongle is found to be defective, replace the dongle.	
The maximum wireless operating range has been exceeded	Add another wireless router closer to the controller(s).	
The controller has a known technical issue	Upgrade the controller's firmware. See Firmware Update on page 84.	
The ECLYPSE Wi-Fi Adapter has been tested functional and there is no jammer in the field to interfere with the signal.	Radio signal path might be obstructed	If a new screening or metal separation wall has been installed since the network was set up, try moving the receiver to see if the issue is corrected.
	Router may have a known technical issue	Upgrade the router's firmware. See the manufacturer's Website.

Table 18-1: Troubleshooting the ECLYPSE Wi-Fi Adapter

Appendix A

METRIC CONVERSIONS FOR WIRE GAUGE

The following table provides information about metric wire equivalents for wire gauge.

AWG	Diameter (Ø)		Area		Approximate stranded metric equivalents
	inch	mm	kcmil	mm ²	
10	0.1019	2.588	10.4	5.26	
12	0.0808	2.053	6.53	3.31	
14	0.0641	1.628	4.11	2.08	
16	0.0508	1.291	2.58	1.31	
18	0.0403	1.024	1.62	0.823	24/0.2
20	0.0320	0.812	1.02	0.518	16/0.2
22	0.0253	0.644	0.642	0.326	7/0.25
24	0.0201	0.511	0.404	0.205	1/0.5, 7/0.2, 30/0.1

Appendix A

REFERENCED DOCUMENTATION

The following documentation is referenced in this document.

Controller Hardware Installation Guides:

These documents are available on Distech Controls SmartSource website

[XpressNetwork Utility User Guide:](#)

This document is available on Distech Controls SmartSource website

[EC-gfxProgram User Guide:](#)

This document is available on Distech Controls SmartSource website

