CHAPTER 5

Implementing and Configuring the Cell/Area Zone

Overview

This chapter outlines the configurations and configuration options to implement the recommendations and best practices described in Chapter 3, "CPwE Solution Design—Cell/Area Zone." The Cell/Area zone is where the Industrial Automation and Control System (IACS) end-devices connect into the Cell/Area IACS network. Careful planning is required to achieve the optimal design from both the Cell/Area IACS network and IACS device perspective. This chapter provides implementation and configuration guidance on both IACS devices, in particular EtherNet/IP-based devices, and the Cell/Area IACS network infrastructure.

This chapter covers the following:

- Implementation of the Cell/Area IACS network when deploying industrial Ethernet switches for the Cell/Area zone
- Implementing EtherNet/IP network modules when deploying the key IACS end-devices for the Cell/Area zone

Implementing the Cell/Area IACS Network

The following sections detail the network configurations for EtherNet/IP devices within the Cell/Area zone such as I/O and HMI. It is important that a thorough design process be completed. This chapter assumes implementation of the key recommendations from Chapter 3, "CPwE Solution Design—Cell/Area Zone." Where options are available, for example between network resiliency protocols, implementation guidance is provided for each supported option. The configuration details outlined below (e.g., VLAN numbers, hostnames, port numbers, etc.) are merely examples and should be adjusted accordingly to a particular plant IACS standards and environment.

This section provides the following:

- An overview of the Cell/Area IACS network implementation, including key tools and review of the recommendations from Chapter 3, "CPwE Solution Design—Cell/Area Zone."
- Implementation steps for deploying an industrial Ethernet switch.

- Troubleshooting recommendations.

Overview

There are different tools available for configuring the Stratix 8000 and IE 3000 switches. The choice of implementation tools used likely depends on the implementer's role within a manufacturing organization. Table 5-1 outlines the key network infrastructure implementation tools and the roles that typically use them.

Table 5-1 Configuration Tools for Stratix 8000 and IE 3000 Switches

Tool	IT	Hybrid	IACS
Express Setup		Yes	Yes
Device Manager		Yes	Yes
RSLogix 5000		Yes	Yes
Cisco Network Assistant	Yes	Yes	Yes
Command Line Interface	Yes	Yes	
SNMP Management Tool	Yes	Yes	

Note In Table 5-1 above and other subsequent tables in this chapter, Yes is used to indicate supported features.

Traditional IT network engineers will likely use the Cisco Command-line Interface (CLI) to configure and manage their Stratix 8000s or IE 3000s. While the CLI is very powerful and flexible, it requires significant knowledge and experience to configure and manage the switch. It is also common for IT staff to use a Simple Network Management Protocol (SNMP)-based network management solution such as CiscoWorks.

Traditional IACS Control Engineers will use the combination of the Stratix 8000 Express Setup, the Stratix 8000 Device Manager (web interface), and the RSLogix 5000 controller application editor to configure and manage their Stratix 8000s. These tools provide an easy to use graphical user-interface (GUI) for configuring the Stratix 8000. More importantly, they allow the IACS Control Engineer to integrate the Stratix 8000 into their IACS controller application via EtherNet/IP.

IT-hybrid engineers (IT with manufacturing focus) will use any of the available tools to manage their Stratix 8000s. Typically, these individuals will have a background in either IT or IACS. While they will start with the tools they are already familiar with, they will quickly begin to use the other tools as they become more familiar with them. For example, an IT-hybrid engineer that has a background as an IACS Control Engineer will likely begin with Express Setup, Device Manager, and RSLogix 5000. As their networking skill develop, they will begin to use the more advanced tools like Cisco Network Assistant and CLI to better support, troubleshoot, and maintain their Cell/Area IACS network.

Recommendation Summary

Table 5-2 to Table 5-7 summarize the design recommendations and network features that can be configured by the different tools available.

Table 5-2 Logical Segmentation and VLANs

Feature	Stratix 8000 Express Setup	IE 3000 Express Setup Plus Recommended System Setup	Device Manager	RSLogix 5000	Cisco Network Assistant	Command Line Interface
Virtual Trunking Protocol (VTP)—Transparent Mode	Yes				Yes	Yes
Create/Delete VLAN			Yes		Yes	Yes
Assign VLANs			Yes	Yes	Yes	Yes
Configure Access Interface			Yes[1]	Yes[1]	Yes	Yes
Configure Trunk Interface			Yes[1]	Yes[1]	Yes	Yes

1. Done via Smartport

Table 5-3 Network Resiliency

Feature	Stratix 8000 Express Setup	IE 3000 Express Setup Plus Recommended System Setup	Device Manager	RSLogix 5000	Cisco Network Assistant	Command Line Interface
Spanning Tree (MSTP)	Yes1[1,2]	Yes[1,2]				Yes
Spanning Tree (RPVST+)					Yes[3,4]	Yes[3]
Configure Root Bridge					Yes[4]	Yes
Flex Links						Yes
EtherChannel - LACP			Yes		Yes	Yes

1. Express Setup on the Stratix 8000 configures additional features.
2. MSTP is set as default by Express Setup for Stratix 8000 and IE 3000.
3. RPVST+ is supported by Stratix 8000 and IE 3000.
4. CNA 5.4 and earlier versions do not support MSTP.

Table 5-4 Multicast Management

Features	Stratix 8000 Express Setup	IE 3000 Express Setup Plus Recommended System Setup	Device Manager	RSLogix 5000	Cisco Network Assistant	Command Line Interface
IGMP Snooping	Yes[1]	Yes[1]	Yes[1]		Yes[1]	Yes[1]
IGMP Querier	Yes[1]	Yes[1]				Yes[1]

1. Enabled as default by Express Setup

Table 5-5 Quality of Service

Feature	Stratix 8000 Express Setup	IE 3000 Express Setup Plus Recommended System Setup	Device Manager	RSLogix 5000	Cisco Network Assistant	Command Line Interface
Quality of Service	Yes	Yes[1]			Yes	Yes

1. The QoS service policy is created but not applied to the interfaces.

Table 5-6 Management, Monitoring, and Security

Feature	Stratix 8000 Express Setup	IE 3000 Express Setup Plus Recommended System Setup	Device Manager	RSLogix 5000	Cisco Network Assistant	Command Line Interface
Enable Secret	Yes	Yes	Yes		Yes	Yes
Line Passwords	Yes	Yes[1]			Yes	Yes
CIP Security	Yes		Yes[2]			Yes
Local Passwords					Yes	Yes
AAA						Yes
Telnet	Yes	Yes[3]				Yes
SSH						Yes[4]
HTTP	Yes	Yes				Yes
HTTPS						Yes[4]
Common Industrial Protocol (CIP)	Yes	Yes[5]				Yes
Simple Network Management Protocol (SNMP)	Yes[6]		Yes[7]		Yes	Yes
SNMPv3						Yes[4]
Notification Banner						Yes
Logging	Yes					Yes
Alarm Profile	Yes[8]	Yes				Yes

1. Express Setup on the IE 3000 does not enable the password encryption service.
2. Device Manager on the IE 3000 cannot set the CIP Security password.
3. Telnet is a optional configuration in Express Setup.
4. IE 3000 only. Requires the LAN-base feature set.
5. The IE 3000 enables CIP but does not enable CIP Security.
6. Express Setup on the Stratix 8000 includes additional configuration options.
7. Device Manager can be used enable/disable SNMP an add SNMPv2 community strings.
8. Express Setup on the IE 3000 uses a simplified alarm profile.

Table 5-7 Misc Features

Feature	Stratix 8000 Express Setup	IE 3000 Express Setup Plus Recommended System Setup	Device Manager	RSLogix 5000	Cisco Network Assistant	Command Line Interface
CIP Enable	Yes					Yes
Error Disable	Yes[1]	Yes				Yes
Precision Time Protocol (IEEE 1588 PTP)	Yes	Yes	Yes	Yes[2]		Yes
Unidirectional Link Detection (UDLD)	Yes	Yes				Yes
Assign Smartport			Yes	Yes		Yes

1. Express Setup on the Stratix 8000 includes additional configuration options.
2. RSLogix 5000 does not allow you to change the clock mode (transparent, boundary, or forward)

Configuration Tools

This section outlines the key configuration tools that can be used to configure and maintain the Stratix 8000 or IE 3000 industrial Ethernet switches.

Express Setup

Express Setup is used to load initial configuration, IP address, and passwords into a switch that is in an out-of-box state. Express Setup uses Device Manager, referenced below, to apply the switch management IP address and password.

For step-by-step instructions on running Express Setup, see the following links:

- *Stratix 8000 Ethernet Managed Switches Installation Instructions*

  http://literature.rockwellautomation.com/idc/groups/literature/documents/in/1783-in005_-en-p.pdf

- *Cisco IE 3000 Switch Getting Started Guide*
  http://cco.cisco.com/en/US/docs/switches/lan/cisco_ie3000/hardware/quick/guide/ie3000_gsg.html

The Stratix 8000 Express Setup enables the IACS Control Engineer to configure the switch for an EtherNet/IP IACS network without knowing or using the CLI. The IE 3000 Express Setup only provides a basic switch configuration and does not apply an EtherNet/IP IACS network-specific configuration. The IE 3000 includes a **Recommended System Setup** option in the Smartport configuration page. Checking this box applies many of the optimizations found on the Stratix 8000. In this chapter, any further references to Express Setup on an IE 3000 assume that the **Recommended System Setup** option has been applied.

Once Express Setup is complete, further configuration and management of the switch can be done using one of the following options, keeping in mind the feature details noted in the tables above:

- Device Manager Web-interface
- RSLogix 5000 controller application software, version 16 or later
- Cisco Network Assistant (CNA), version 5.4 or later
- Command-line interface (CLI)
- SNMP management applications such as CiscoWorks

Figure 5-1 Stratix 8000 and IE 3000 Device Managers

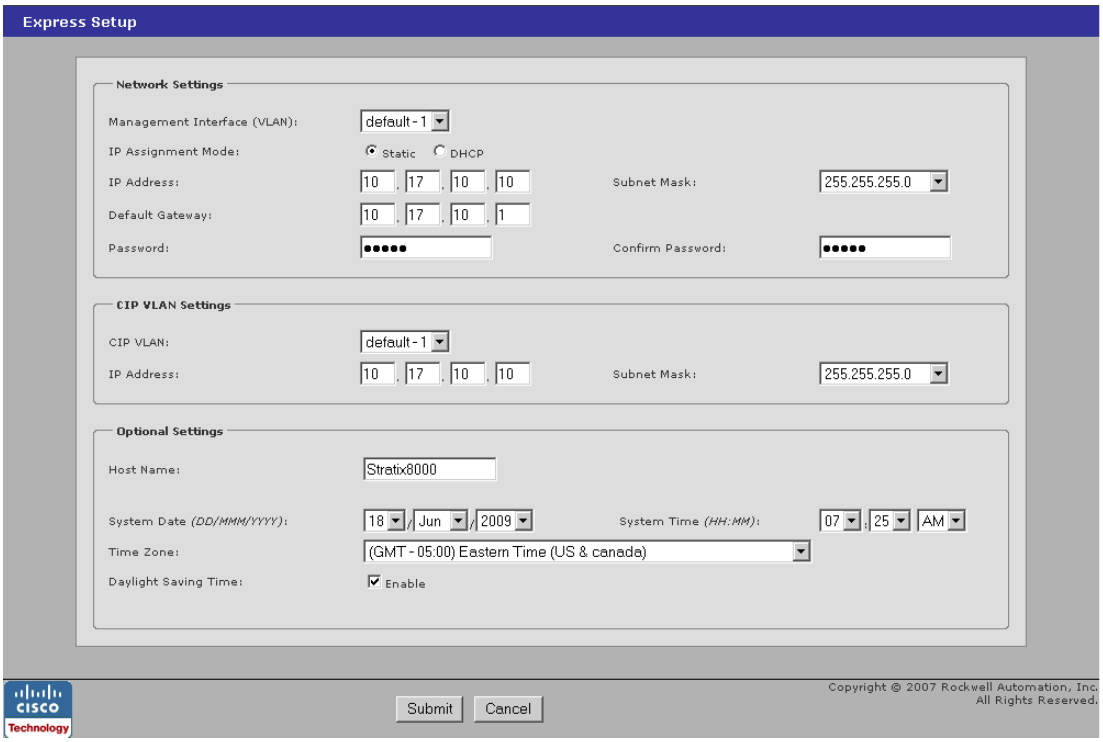
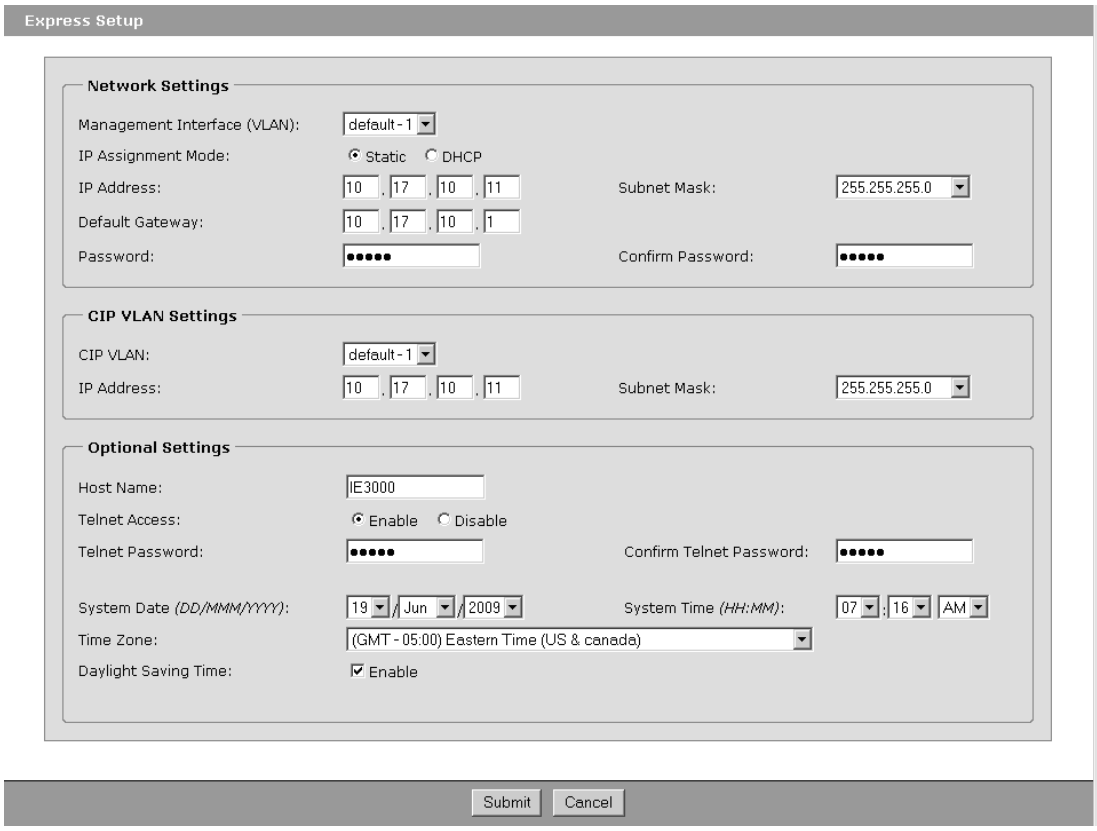


Figure 5-2 Stratix 8000 and IE 3000 Device Managers



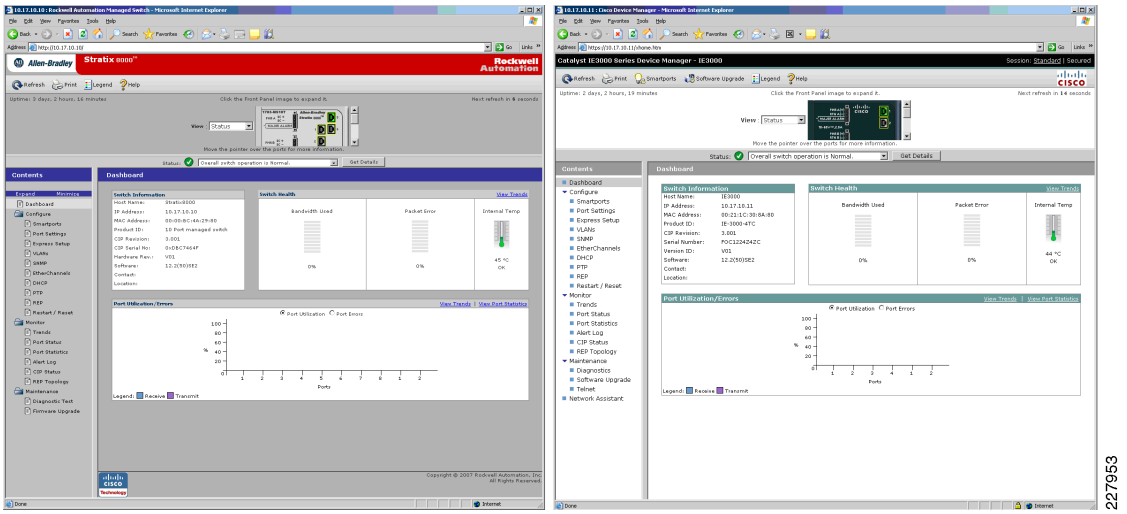
Device Manager

The Device Manager is the Web-based configuration interface for the Stratix 8000 and IE 3000. It allows the implementer to easily implement advanced configurations consistently across the Cell/Area IACS network.

Device Manager can be used to configure several advanced configuration options such as the following:

- Smartports, discussed in the "Smartports" section on page D-10
- Port Settings (Description, Enable, Speed, Duplex, Auto-MDIX, and MediaType)
- VLANs
- EtherChannels (IEEE Link Aggregation Control Protocol - LACP)
- Dynamic Host Configuration Protocol (DHCP) Server
- IEEE 1588 Precision Time Protocol (PTP)
- Resilient Ethernet Protocol (REP)
- Simple Network Management Protocol (SNMP)

Figure 5-3 Stratix 8000 and IE 3000 Device Managers



The Device Manager also provides the following basic monitoring and management capabilities:

- Utilization Trends
- Port Status
- Port Statistics
- Alert Log
- CIP Status
- REP Topology
- Diagnostic Test
- IOS Upgrade
- Reboot
- Restore to Factory Defaults

For information on how to configure the Stratix 8000 switch using Device Manager, see the *Stratix 8000 Ethernet Managed Switches Software User Manual* at the following URL:
http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um003_-en-e.pdf

For information on how to configure the IE 3000 switch using Device Manager, see the *IE 3000 Getting Started Guide* at the following URL:
http://www.cisco.com/en/US/docs/switches/lan/cisco_ie3000/hardware/quick/guide/ie3000_gsg.html

RSLogix 5000

The Stratix 8000 switch is a CIP-enabled EtherNet/IP device designed to integrate into the Rockwell Automation Integrated Architecture. The Stratix 8000 comes with an Add-on Profile (AOP) for RSLogix 5000. AOP allows the Stratix 8000 to be integrated into the Rockwell Automation Logix Programmable Automation Controller (PAC™) project. Once added to the project, the Stratix 8000 switch appears in the I/O tree like any other EtherNet/IP device.

The AOP enables controller tags to monitor the status of the switch ports and the health status of the switch itself. These tags can be incorporated into the RSLogix 5000 project to monitor the status of the Cell/Area IACS network.

The AOP also enables the ability to configure the Stratix 8000 directly from RSLogix 5000, such as assigning Smartport and port traffic thresholds. Any configuration changes made via RSLogix 5000 are automatically saved to the Compact Flash card. In addition, the Stratix 8000 configuration can be uploaded into an RSLogix 5000 project and be saved as a part of the native RSLogix 5000 project. The Stratix 8000 configuration can also be exported from RSLogix 5000 into a file format that can be imported into other RSLogix 5000 projects. This export/import feature provides for quick reuse of testing and proven Stratix 8000 configurations between RSLogix 5000 applications.

Although RSLogix 5000 can assign individual ports to VLANs, other tools must be used to create and configure VLANs such as Device Manager. Device Manager is also used to configure Resilient Ethernet Protocol (REP), which is not included in this version of the solution. Multicast management and quality-of-service (QoS) are configured by default as part of the Stratix 8000 Express Setup.

The AOP can be used to configure the following features:

- CIP Connection to the Stratix 8000
- Port Settings (Enable, Speed, Duplex, Enable IEEE 1588 PTP)
- Smartports
- Native, Access, and Voice VLAN IDs
- Secure MAC Address (static port security)
- Storm Control Thresholds

In addition the following diagnostic information is available:

- Module Status
- Switch Status
- Port Status
- IEEE 1588 PTP Status
- Resiliency Protocol Status
- CIP Status

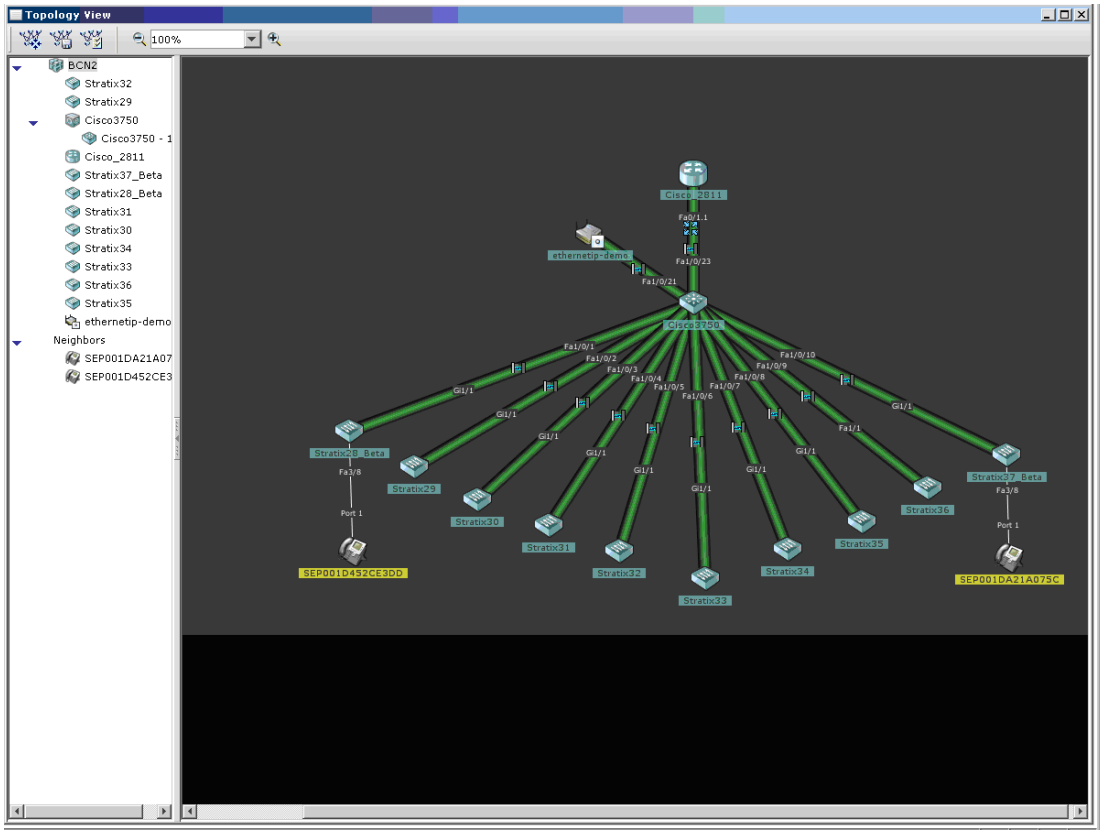
For information on how to configure the Stratix 8000 switch using the RSLogix 5000 AOP, see the *Stratix 8000 Ethernet Managed Switches Software User Manual* at the following URL:

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um003_-en-e.pdf

Cisco Network Assistant

Cisco Network Assistant (CNA) is a PC-based network management solution. It allows the configuration, management, and troubleshooting of small-to-medium sized Cisco networks including the Stratix 8000. See Figure 5-4.

Figure 5-4 CNA



CNA provides the following functions:

- Supports networks that include up to 40 Cisco routers and switches, including the Stratix 8000
- Allows for the customization of configurations using a GUI, not CLI
- Backup and restore configuration files for all routers and switches
- Inventory reports including hostname, IP address, model, and IOS version
- Event notification
- IOS upgrades
- Network utilization reports

CNA is a free download from the following URL: http://www.cisco.com/go/cna

Note At the time of the writing of this *Design and Implementation Guide (DIG)*, CNA version 5.4 does not support MSTP.

Command-Line Interface (CLI)

The CLI is the traditional IT method of configuring Cisco networking equipment. The CLI provides full access to all of the features and capabilities of the industrial Ethernet switches. The switches can be setup to allow CLI connections via the console port and Telnet sessions. The IE 3000 also provides the option to enable Secure Shell (SSH) for CLI access.

Some IT organizations may choose not to use Express Setup or the Smartports for the industrial Ethernet switches. It is important to understand the features recommended in this guide are enabled in the macros. If you choose not to use the macros, you need to incorporate many of these features into your existing template configurations. The contents of all of the Express Setup and Smartport macros can be viewed with the **show parser macro** commands.

Step-by-step instructions for configuring the industrial Ethernet switches via CLI can be found in the *Cisco IE 3000 Software Configuration Guide* at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/cisco_ie3000/software/release/12.2_50_se/configuration/guide/ie3000scg.html

A full list of CLI commands related to the industrial Ethernet switches can be found in *Cisco IE 3000 Switch Command Reference* at the following URL*:*
http://www.cisco.com/en/US/docs/switches/lan/cisco_ie3000/software/release/12.2_50_se/command/reference/ie3000cr.html.

Compact Flash Card

The industrial Ethernet switches come with a removable compact flash card. The switch stores the Internetworking Operating System (IOS) and the startup configuration on the compact flash card. In the event of a hardware failure, the compact flash card can be installed in the replacement switch. The replacement switch will boot using the IOS version and configuration stored on the card. No additional work is needed to restore the network.

Configuration changes made via the Device Manager or RSLogix 5000 are automatically saved to the compact flash card. Configuration changes made via the CLI or CNA must be manually saved to the compact flash card.

Smartports

Smartports are predefined configuration macros that were developed by Cisco and Rockwell Automation to simplify implementation of the switch for EtherNet/IP IACS networks. Smartports represent the joint design, testing, and implementation experience with IACS networks from both organizations. Smartports may be used by any of the available configuration tools to configure a port for a specific type of device. These configurations enable the easy implementation of many of the advanced features outlined in this *DIG*. Smartports and Express Setup enable consistent and simplified application of advanced, IACS optimized switch configurations across Cell/Area IACS networks.

For example, the Stratix 8000 “Automation Device” Smartport enables the following settings and features:

- Sets the port to host mode
- Enables MAC flooding attack protection
- Sets the access VLAN number
- Enables the automation QoS policy
- Configures the interface's output queues

- Enables the alarm profile
- Disables Cisco Discovery Protocol (CDP)

For more details on the available Smartports, refer to Appendix D, "Configurations."

Implementation Steps

The implementation of the Cell/Area IACS network starts with the configuration of the Layer-2 access switches, specifically the Stratix 8000 and IE 3000. Default configuration and recommended configuration changes are reviewed to address the best practices to reduce Cell/Area IACS network latency and jitter, VLAN segmentation, IGMP multicast management, QoS prioritization, topology, and resiliency.

The following key steps are covered in this section:

- Use Express Setup and Device Manager to apply the Cisco and Rockwell Automation suggested basic configuration.
- Use of CLI to apply specific configuration recommendations.

This section first addresses the steps, with the assumption that a Stratix8000 is being used and identifies differences if using the IE 3000.

Express Setup and Device Manager

Step 1 Verify the IOS version.

Step 2 Run global industrial Ethernet configuration macros.

Step 3 Configure switch IP address.

Step 4 Set switch security.

Step 5 Configure VLAN.

Step 6 Configure port settings.

Step 7 If needed, configure EtherChannel links.

Features Configured Only via CLI

Some of the features and recommendations from Chapter 3, "CPwE Solution Design—Cell/Area Zone"are not configurable via Express Setup, Device Manager, or RSLogix 5000. The following features can only be configured through the CLI. This section outlines the CLI commands to implement these features and recommendations.

Logical Segmentation and VLANs

Virtual Trunking Protocol (VTP)

Express Setup on the IE 3000 does not configure VTP in transparent mode. The VTP configuration is a part of the global configuration. Enter the following command in global configuration mode.

```
vtp mode transparent
```

Express Setup on the Stratix 8000 configures VTP for transparent mode.

Availability and Network Resiliency

STP

- BPDU Guard

  Express Setup on the IE 3000 does not configure BPDU Guard globally. BPDU Guard should be enabled globally on the switch. When BPDU Guard is applied globally, it will be enabled on all interfaces that have the **spanning-tree portfast** command enabled. Enter the following command in global configuration mode:

  spanning-tree portfast bpduguard default

  The Stratix 8000 enables BPDU Guard globally.

- BPDU Filter

  Express Setup on the IE 3000 does not configure BPDU Filter globally.

  BPDU Filter should be enabled globally on the switch. When BPDU Filter is applied globally, it will be enabled on all interfaces that have the **spanning-tree portfast** command enabled. Enter the following command in global configuration mode:

  spanning-tree portfast bpdufilter default

  The Stratix 8000 enables BPDU Filter globally.

- RPVST+

  Where Cisco's RPVST+ implementation of the Spanning Tree Protocol (STP) is being used on the enterprise network switches, change the Spanning Tree configuration on the industrial Ethernet switches to RPVST+. The default for these switches is MSTP. The default for other Cisco IOS-based switches is RPVST+.

  For more information on choosing a resiliency protocol, see Chapter 3, "CPwE Solution Design—Cell/Area Zone." For information on configuring RPVST+ on the Stratix 8000 and IE 3000, see the *IE 3000 Software Configuration Guide* at the following URL:

  http://www.cisco.com/en/US/docs/switches/lan/cisco_ie3000/software/release/12.2_50_se/configuration/guide/ie3000scg.html

- Root Bridge

  The root bridge of the Spanning Tree network must be manually selected based on your topology. The distribution switches should be configured as the root bridges. To configure the primary root bridge, enter the following command in global configuration mode:

  spanning-tree mst 0 root primary

  To configure the secondary root bridge, enter the following command in global configuration mode:

  spanning-tree mst 0 root secondary

  These commands assume that you are using the default MSTP instance of 0.

  For information on configuring the root bridge on a RPVST+ network on the Stratix 8000 and IE 3000, refer to the *IE 3000 Software Configuration Guide* at the following URL:

  http://www.cisco.com/en/US/docs/switches/lan/cisco_ie3000/software/release/12.2_50_se/configuration/guide/ie3000scg.html

Flex Links

Flex Links are configured on the Stratix 8000 and the IE 3000 access switch. There are no configuration changes required to the distribution switches to use Flex Links. Flex Links requires that you designate an active and backup interface. Typically, **interface gi1/1** is the active and **interface gi1/2** is the backup. The following shows how to specify the configuration:

```
Straitx8000#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Stratix8000(config)#int gi1/1
Stratix8000(config-if)#switchport backup interface gi1/2 multicast fast-converge
Stratix8000(config-if)#
```

Security

Line Passwords

Express Setup on the IE 3000 does not enable the password encryption service. This means that the line passwords appear as clear text in the configuration. The password encryption service is enabled in the global configuration with the following command:

service password-encryption

Express Setup on the Stratix 8000 enables the password encryption service.

CIP Security

Express Setup on the IE 3000 does not enable CIP or configure a CIP security password. Enabling CIP without a CIP security password, any controller can connect to the switch and make changes to the configuration. The CIP security password can be configured with the following global configuration command:

cip security password *password*

Express Setup on the Stratix 8000 configures the CIP security password.

Notification Banner

A login banner should be configured to display at all logins. As part of a security policy, it is necessary to ensure that network resources are clearly identified as being off limit to the casual visitor. The contents of the banner should be discussed with your legal council. There are several methods of enabling the banner, including the **banner motd**, **banner login**, **banner incoming**, and **banner exec** commands. The **banner login** global configuration command should be used for the initial login banner.

Logging

Express Setup on the IE 3000 does not configure the logging buffer size or the time stamping service.

```
logging buffered 16384
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

Express Setup on the Stratix 8000 configures the logging buffer and the time stamping service.

Additional logging features, such as logging to an external syslog server, are available. For more details on the IE switches, see *IE 3000 Software Configuration Guide* at the following URL:

http://cco.cisco.com/en/US/docs/switches/lan/cisco_ie3000/software/release/12.2_50_se/configuration/guide/ie3000scg.html

Authentication, Authorization, and Accounting (AAA)

AAA is the preferred method of securing access to the network switches. AAA relies on an external AAA server such as Cisco Secure ACS. Configuring AAA is beyond the scope of this guide. For more information, refer to the "Enforce AAA" section in "Chapter 2, Network Foundation Protection" of the *Cisco SAFE Reference Guide* at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap2.html

SSH

SSH should be enabled to encrypt management traffic to the IE 3000. SSH does not work with line passwords. It requires that either local usernames and passwords or AAA is configured. There are four parts to configuring SSH:

1. In order to use SSH, the switch must be using an IOS image capable of cryptography. The cryptography image for Cisco switches is available for download at http://www.cisco.com.

Note Some platforms may require the selection of the cryptography image at the time of purchase or pay a fee to upgrade the feature set to include the cryptography.

2. SSH requires the use of usernames and passwords for authentication. To accomplish this, the switch must be configured to use an AAA server like TACACS+ for authentication. If an AAA server is not available on the network, local usernames, and passwords can be used as an alternative.

   For more information, refer to the "Protect Local Passwords" section in "Chapter 2, Network Foundation Protection" of the *Cisco SAFE Reference Guide* at the following URL:

   http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap2.html

3. SSH must be configured in the global configuration. SSH requires that the switch is configured with a hostname and a domain name. The hostname is set with the **hostname** *hostname* global configuration command. The domain name is configured with the **ip domain-name** *domain-name* global configuration command. Once the hostname and domain names are set, a RSA key pair must be generated. The **crypto key generate rsa** global configuration command generates the RSA key pair and enables SSH on the switch.

4. The VTY lines must be configured to use SSH. By default, the VTYs accepts connections via both Telnet and SSH. The **transport input ssh** configuration command allows you to limit access to SSH. This command disables Telnet access to the switch. The **transport input all** command allows both SSH and Telnet access. The **transport input telnet** command allows only Telnet access.

HTTPS

HTTPS should be enabled to encrypt management traffic to the switch. At this time, the Stratix 8000 does not support HTTPS. In order to use HTTPS, the switch must use an IOS image capable of cryptography. The cryptography image for Cisco switches is available for download at the following URL: http://www.cisco.com.

Note Some platforms may require the selection of cryptography image at the time of purchase or pay a fee to upgrade the feature set to include the cryptography.

Once the proper IOS feature set is installed, the HTTPS server should be enabled with the **ip http secure-server** global configuration command. After the HTTPS server is enabled, the HTTP server should be disabled with the **no ip http server** global configuration command. In addition, HTTPS requires that Telnet is enabled on the VTY lines.

Miscellaneous Features

Error Disable

Express Setup on the IE 3000 does not fully configure the error-disable feature. The following error-disable settings are recommended for an Cell/Area IACS network. Error-disable is configured in the global configuration.

```
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause arp-inspection
errdisable recovery cause loopback
errdisable recovery cause small-frame
errdisable recovery interval 30
```

Express Setup on the Stratix 8000 configures Error Disable.

Implementing the EtherNet/IP Network Modules

This section focuses on the configuration of the EtherNet/IP network devices. The following tools are required:

- RSLinx Classic (2.54.00.11 CPR 9 SR 1 or greater)
- RSLogix 5000 (v16 or greater)
- Stratix 8000 Add-on-Profile (AOP) (v3. 3.01.008 or greater)
- Stratix 8000 Express Setup (12.2(50)SE2 or greater)

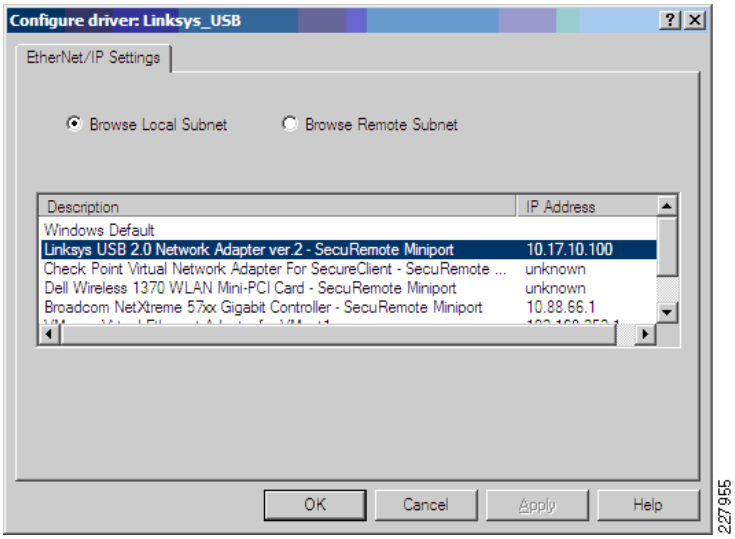
Overview

EIP Network Module Implementation Tools

RSLinx Classic

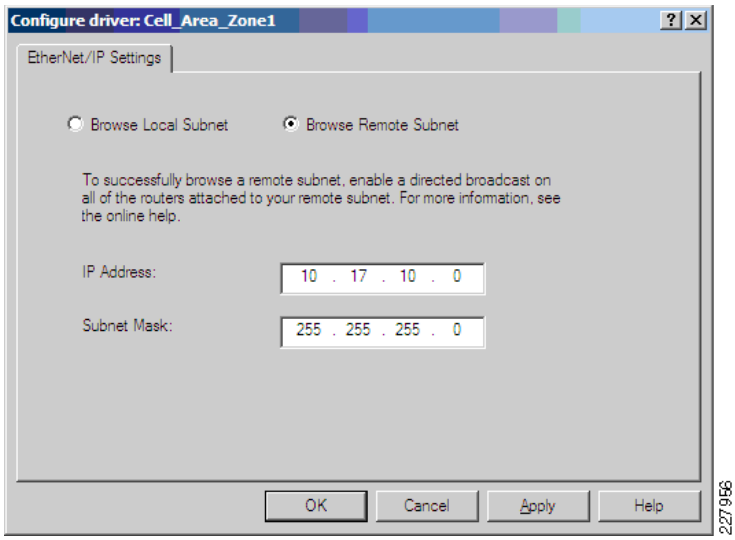
RSLinx Classic is a communication server that allows you to browse and communicate with EtherNet/IP devices on the Cell/Area IACS network. RSLinx Classic includes drivers to communicate with many different types of devices and several different network protocols. In most cases, RSLinx Classic should be configured to use the EtherNet/IP driver. The EtherNet/IP driver can be configured for local and remote browsing. Local browsing sends a discovery broadcast to devices on the local Ethernet network. This is useful when you need to discover devices on the local link. To configure local browsing, select the appropriate interface from the list. See Figure 5-5.

Figure 5-5 RSLinx Classic EtherNet/IP Driver Configuration Screen



Remote browsing sends a discovery broadcast directed at a specific IP subnet. This is useful when you need to browse devices in a specific Cell/Area zone from the Manufacturing zone. To configure the EtherNet/IP driver for remote browsing, enter the target subnet and mask. See Figure 5-6.

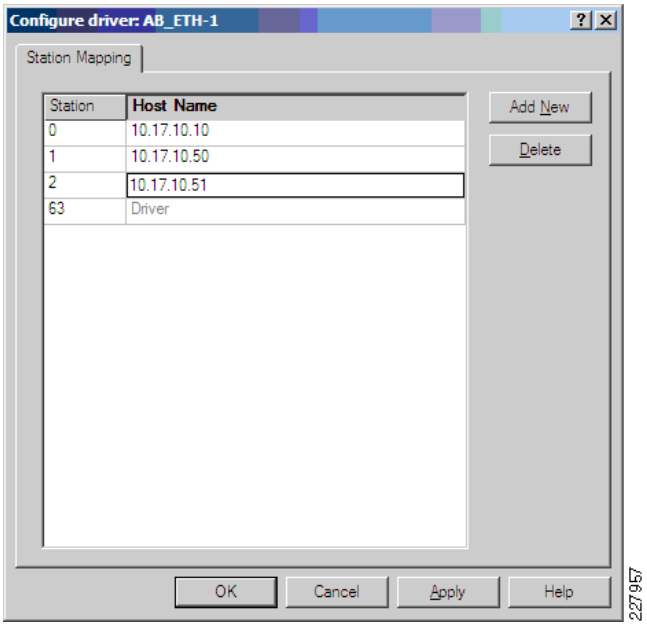
Figure 5-6 RSLinx Classic EtherNet/IP Driver Configuration Screen



The remote browse function uses a feature called IP-directed broadcast. Most Cisco Layer-3 switches and routers disable directed broadcasts by default. Directed broadcasts can be enabled with the **ip directed-broadcast** interface configuration command. This command needs to be applied to all routed interfaces for the subnets and Cell/Area zones you need to browse.

There is a second option for browsing EtherNet/IP devices with RSLinx Classic. The Ethernet devices driver supports manual entry of IP addresses to browse (see Figure 5-7). There is a second option for browsing EtherNet/IP devices with RSLinx Classic. The Ethernet devices driver supports manual entry of IP addresses to browse.

Figure 5-7 RSLinx Classic AB_Ethernet Driver Configuration Screen



EtherNet/IP Interface Configuration

- IP Configuration
- Link Speed and Duplex Mode

IP Configuration

EtherNet/IP uses the Internet Protocol (IP) to communicate between modules. The following are options for configuring the IP address of the module:

- Mechanical rotary switches
- DHCP/BOOTP
- CIP messaging

Table 5-8 provides the configuration parameters for the EtherNet/IP modules.

Table 5-8 Configuration Parameters for EtherNet/IP Modules

Parameter	Description	Required	Recommended	Optional
IP Address	The IP address of the EtherNet/IP module	Yes		
Network Mask	The network mask of the EtherNet/IP module	Yes		
Gateway Address	The default gateway address of the EtherNet/IP module		Yes	
Primary Name Server	The IP address of the primary DNS server			Yes
Secondary Name Server	The IP address of the secondary DNS server			Yes
Domain Name	The DNS domain name of the EtherNet/IP module			Yes
Host Name	The host name of the EtheNet/IP module			Yes

All EtherNet/IP modules must have a unique IP address on the network. The network mask is used to determine which subnet the EtherNet/IP module is on. The gateway address is used when the EtherNet/IP module needs to communicate with an TCP/IP device that is located on another subnet. The network mask is used to determine if the destination host is on the local or a remote subnet. If the destination is on the local subnet, the EtherNet/IP module sends the packet directly to the destination. If the destination is on a remote subnet, the EtherNet/IP module forwards the packet to the gateway. The gateway then forwards the packet to the appropriate subnet.

Most EtherNet/IP network implementations require that the gateway address is statically configured on the module. Some implementations may choose to use DNS name resolution. If your EtherNet/IP network implementation requires the use of DNS, the primary name server, secondary name server, domain name, and hostname field should be completed. This *DIG* does not cover the use of DNS in the EtherNet/IP network.

In most applications, the IP addresses of EtherNet/IP I/O devices are statically entered into the application. Because of this, it is important that the module's address always matches the address entered in the application.

Mechanical Rotary Switches

Many Rockwell Automation EtherNet/IP devices have three rotary switches for configuring the IP address. These switches are used to set the last octet of the IP address. The advantage of using the rotary switches is that maintenance staff can replace the module without needing a computer or knowledge of IP addressing. This greatly reduces mean-time-to-repair (MTTR). See Table 5-9.

Table 5-9 Mechanical Rotary Switches

Switch Setting	IP Address
001 – 254	192.168.1.xyz Where xyz is the values of switches x, y, and z Subnet Mask: 255.255.255.0 Gateway Address: 0.0.0.0
888	Resets module to initial out of box settings. Do not use for normal operation
Any Other Value	IP address configuration is controlled via software: BootP DHCP User Entered

While the rotary switches work well in a small isolated network such as a machine or line, they are not effective in larger plantwide EtherNet/IP networks. The EtherNet/IP modules do not allow the configuration of a default gateway when using the rotary switches. This prevents the module from communicating with any devices outside of the local 192.168.1.0/24 subnet.

Setting the rotary switches to a value other than 001 to 254 or 888 sets the module to have its IP address configured via software. This is the default configuration.

DHCP/BOOTP

The Dynamic Host Configuration Protocol (DHCP) or the Bootstrap Protocol (BootP) can be used to assign the IP address from a server or workstation. This is the default setting for modules that do not have rotary switches. If the module has rotary switches any number other than 001 to 254, 888 will configure the device to use DHCP/BootP.

On boot up, the module sends a request for an IP address. A BootP server assigns an address to the module based on its MAC address. Since the address is assigned by the MAC address, BootP guarantees that the device will always get the same IP address. However, if the device fails and is replaced the BootP table must be updated with the new MAC address. The replacement device will not get its assigned address until the BootP table is updated.

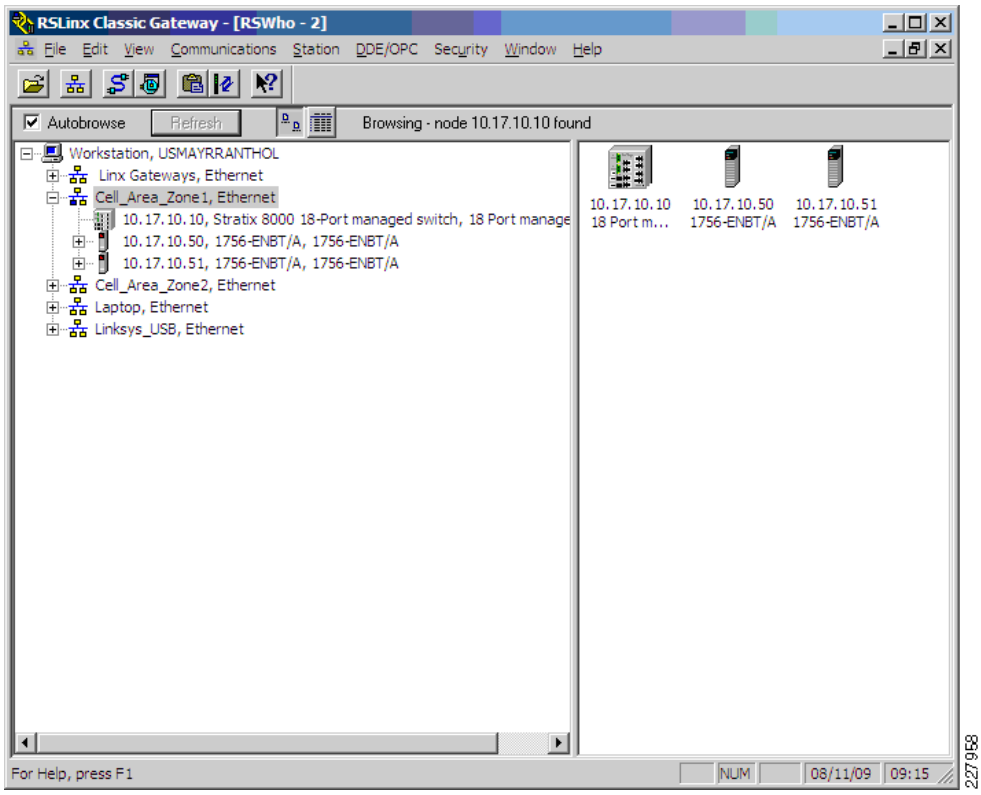
A DHCP server has the ability to assign the IP address based on a pool of available addresses. This is convenient in the Enterprise zone where the IP address of the client is not critical. DCHP also has the ability to assign IP addresses based on a Client-ID. The default Client-ID is the MAC address of the host. This means that the DCHP server can be setup to statically map an IP address to a MAC address like BootP.

Again, it is important that IP addresses of the EtherNet/IP modules in the controller application are consistent within the Cell/Area zone. Because of this, it is recommended that the IP address is manually entered into the EtherNet/IP module. DHCP is commonly used to assign an initial address to that the module can be statically configured via CIP messaging.

CIP Messaging

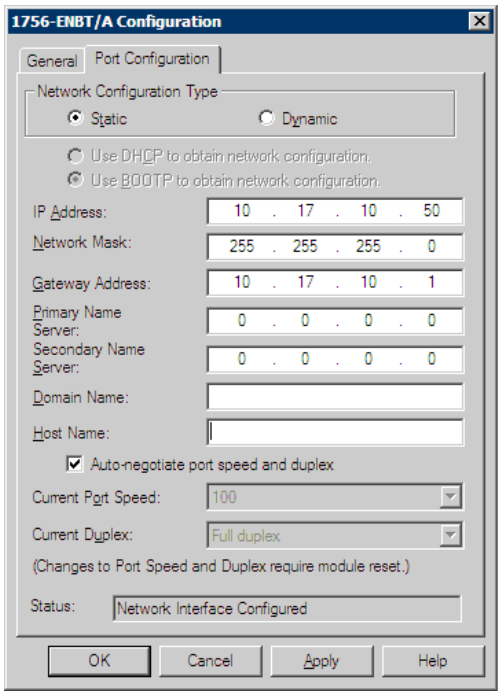
The IP address of an EtherNet/IP module can be set using CIP messages. The two most common ways to set CIP messages are through RSLinx Classic or the RSLogix 5000 AOP for the EtherNet/IP module. The EtherNet/IP module must be reachable on the CIP network to set the IP address via CIP messaging. This can be done via EtherNet/IP, DeviceNet, ControlNet, RS232, or USB. See Figure 5-8.

Figure 5-8 RSLinx Classic RSWho



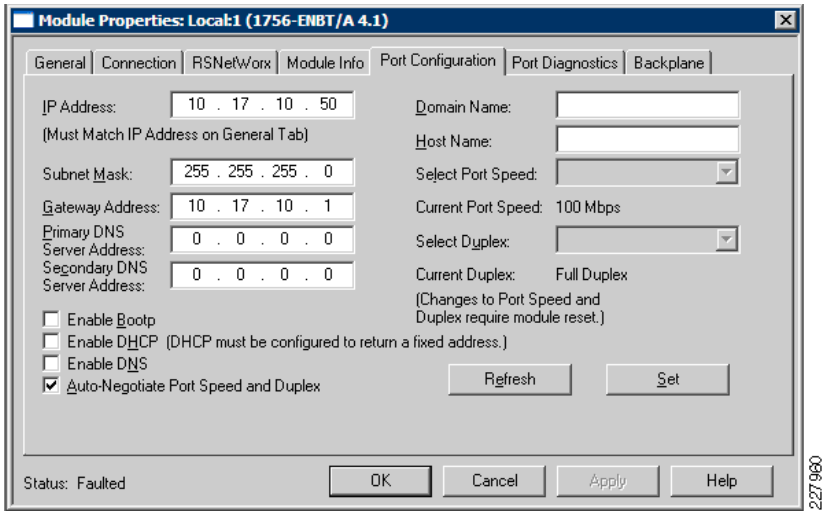
The RSWho window allows you to browse the CIP devices on the CIP network. The IP address of an EtherNet/IP module can be set by right-clicking on the module and selecting **Module Configuration**. The *Port Configuration* tab allows you to configure the module to use DHCP/BootP or a static IP address. If you select a static address, you can enter the IP address, subnet mask, and default gateway for the module. Optionally, you can configure DNS-related information such as DNS servers and hostname. See Figure 5-9.

Figure 5-9 RSLinx Classic EtherNet/IP Module Configuration Screen



RSLogix 5000 with an online connection has the same capability. Double-clicking on the module in the I/O tree brings up the module properties window. The *Port Configuration* tab allows you to configure the IP address information. See Figure 5-10.

Figure 5-10 RSLogix 5000 AOP EtherNet/IP Module Configuration Screen



It is important to check the product manuals for the EtherNet/IP modules for any additional requirements. For example, some modules may require that all active I/O sessions are stopped before the IP address can be changed. Other modules may require a power cycle to load the new IP address.

For more information, refer to the *EtherNet/IP Modules in Logix5000 Control Systems User Manual* at the following URL:

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/enet-um001_-en-p.pdf

Link Speed and Duplex

In Chapter 3, "CPwE Solution Design—Cell/Area Zone," the pros/cons of using auto-negotiate or setting the speed/duplex are discussed. If you choose not to use auto-negotiate or if the hardware does not support it, it is important to ensure that both sides of the link are using the same speed and duplex settings.

A good example of this is the Allen-Bradley 1756-EN2F ControlLogix EtherNet/IP Fiber Module. The 1756-EN2F does not support auto-negotiate and only operates at 100Mbps full-duplex. In order to use this module, the interface on the Stratix 8000 must be manually set to 100Mbps full-duplex to match the module.