CHAPTER 3

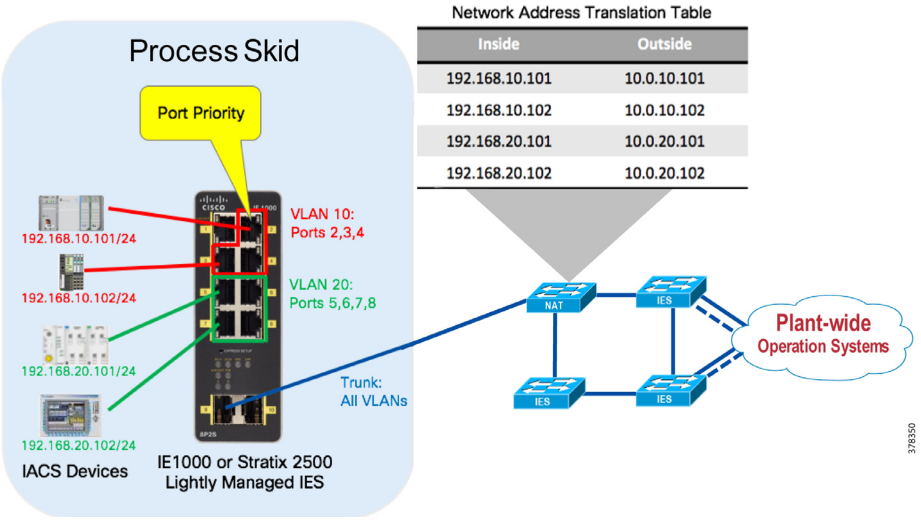
Integrating Lightly Managed IES into the CPwE Architecture

This chapter includes the following major topics:

- Connecting and Segmenting Access Ports to IACS Devices, page 3-2
- VLANs Trunked to Upstream Fully Managed IES, page 3-4
- Port Priority for Latency Sensitive IACS Device, page 3-4
- Layer 2 NAT on Managed IES, page 3-6

This chapter covers the basic configuration settings for the recommended deployment scenario for a lightly managed IES. In the examples that follow, which are applicable for the Cisco IE 1000 and Allen-Bradley Stratix 2500 lightly managed switches, the lightly managed IES is part of a process skid that contains several IACS devices. The lightly managed IES connects the IACS devices to an existing ring of managed IES switches.

Figure 3-1 Example Configuration Scenario for Lightly Managed IES



Network Address Translation Table

Inside	Outside
192.168.10.101	10.0.10.101
192.168.10.102	10.0.10.102
192.168.20.101	10.0.20.101
192.168.20.102	10.0.20.102

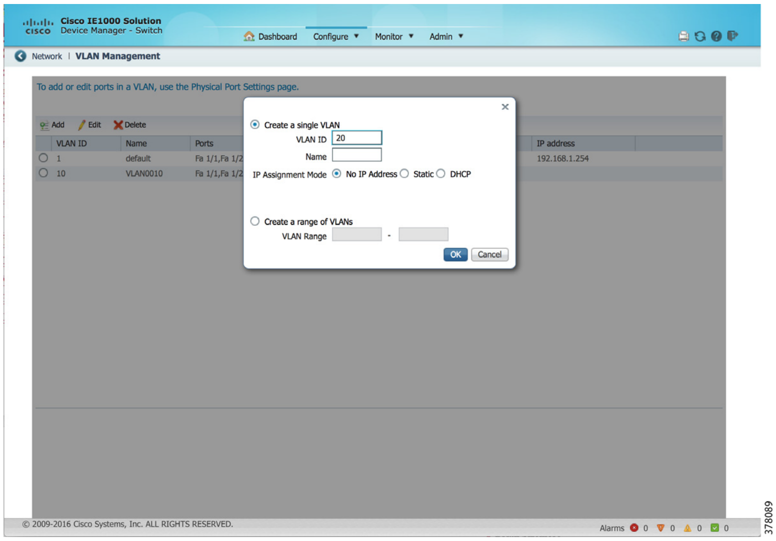
Connecting and Segmenting Access Ports to IACS Devices

The lightly managed IES support VLANs for segmenting the switch into multiple Layer 2 networks (smaller broadcast domains), as discussed in Chapter 2, "Lightly Managed IES in the Sub-Zone." This segmentation can help increase security and help reduce bandwidth utilization from unnecessary packet flooding (broadcast traffic).

To segment the switch's ports into different VLANs, first use the Device Manager to create the VLANs by navigating to **Configure > Network > VLAN Management** in Device Manager. Then click **Add** to create a single VLAN, or a range of multiple VLANs. In this example, two VLANs are created: VLAN 10 and VLAN 20. These VLANs are used to separate the IACS devices attached to each VLAN from communicating with each other at Layer 2. In order for the devices to communicate, the packets between them would need to pass a Layer 3 boundary using a router or a Layer 3 IES, which provides a central place to enforce security policies such as access control lists. In many cases, lightly managed IES will use a basic configuration with a single VLAN, however this example illustrates what is possible with the lightly managed IES.

After the VLANs are created, you can see that, by default, all VLANs are assigned to all ports.

Figure 3-2 Device Manager—VLAN Creation



To add or edit ports in a VLAN, use the Physical Port Settings page.

	VLAN ID	Name	Ports	IP address
○	1	default	Fa 1/1,Fa 1/2	192.168.1.254
○	10	VLAN0010	Fa 1/1,Fa 1/2	

● Create a single VLAN
VLAN ID 20
Name
IP Assignment Mode ● No IP Address ○ Static ○ DHCP

○ Create a range of VLANs
VLAN Range -

© 2009-2016 Cisco Systems, Inc. ALL RIGHTS RESERVED.

The next step is assign a single VLAN to each physical port that connects to one of the IACS devices. This is accomplished by navigating to **Configure > Network > Port Settings** in the Device Manager. From there, select a single port, click **Edit**, and change the **Administrative Mode** to **Access**, and the **Access VLAN** to either **VLAN 10** or **VLAN 20**. In this example (and as shown in Figure X), ports 2 through 4 are assigned to VLAN 10, and ports 5 through 8 are assigned to VLAN 20. Port 1 is left in VLAN 1 (the default) because, in this case, it is being used to connect to the management network in order to administer the switch.

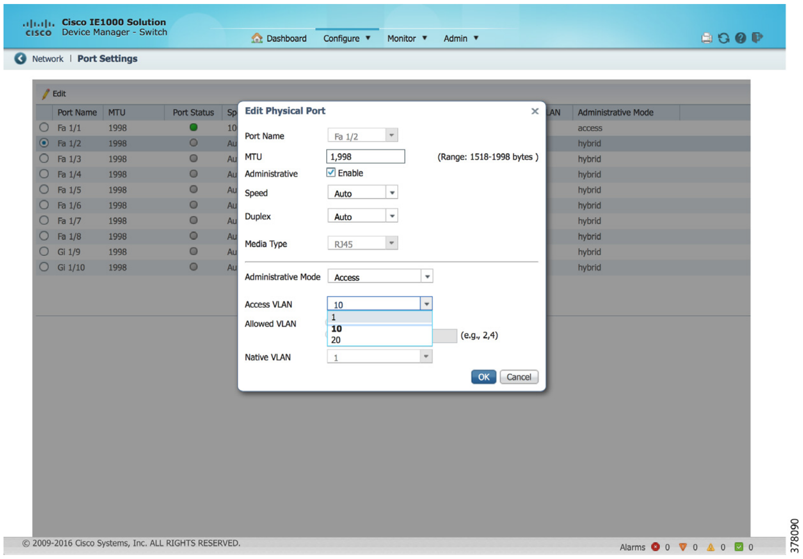
The available administrative modes are described below, including a hybrid mode, which may be new to people familiar with typical managed switch configuration.

- **Access**—The interface belongs to exactly one VLAN. The switch only accepts frames that are not tagged with a VLAN, and transmits frames that are not tagged.
- **Trunk**—This interface transmits and receives frames for all or some VLANs. The switch will examine the VLAN tag for incoming traffic, and include the appropriate VLAN tag for egress frames. Frames that are destined for the Native VLAN are sent out untagged.

- **Hybrid**—This is similar to a Trunk interface, but by default it is a member of all VLAN IDs. It will allow packets tagged with VLAN ID of 0 to be switched, which is useful for PROFINET traffic. Both tagged and untagged frames are accepted.

Note Hybrid mode is only recommended for PROFINET IACS traffic.

Figure 3-3 Device Manager—Port Settings



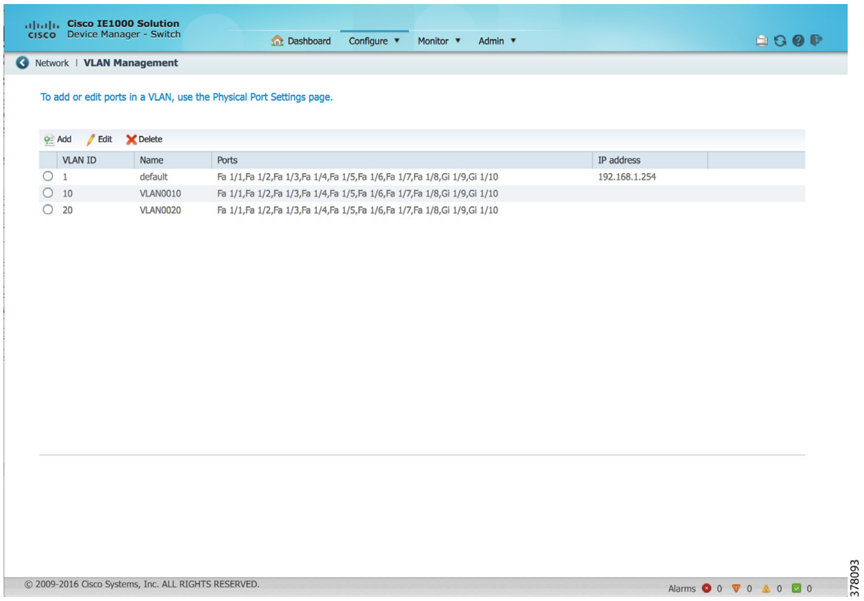
	Port Name	MTU	Port Status	Sp	LAN	Administrative Mode
○	Fa 1/1	1998	●	10		access
●	Fa 1/2	1998	○	Au		hybrid
○	Fa 1/3	1998	○	Au		hybrid
○	Fa 1/4	1998	○	Au		hybrid
○	Fa 1/5	1998	○	Au		hybrid
○	Fa 1/6	1998	○	Au		hybrid
○	Fa 1/7	1998	○	Au		hybrid
○	Fa 1/8	1998	○	Au		hybrid
○	Gi 1/9	1998	○	Au		hybrid
○	Gi 1/10	1998	○	Au		hybrid

Edit Physical Port

Port Name: Fa 1/2
MTU: 1,998 (Range: 1518-1998 bytes)
Administrative: ☑ Enable
Speed: Auto
Duplex: Auto
Media Type: RJ45
Administrative Mode: Access
Access VLAN: 10
1
10
20
Allowed VLAN: (e.g., 2,4)
Native VLAN: 1

In the next screen capture, going back to the VLAN Management page shows that each of the two new VLANs is assigned to the appropriate physical ports. Note that ports G1/9 and G1/10 are listed for all three VLANs—this is because these physical ports have not yet been configured and are still in the Hybrid mode (which is the default Administrative Mode).

Figure 3-4 Device Manager—VLAN List



To add or edit ports in a VLAN, use the Physical Port Settings page.

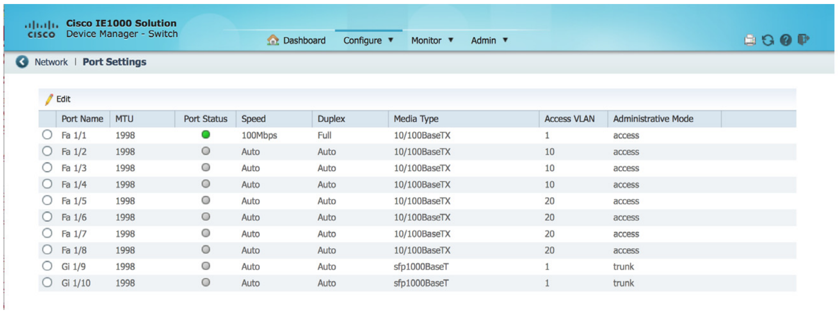
	VLAN ID	Name	Ports	IP address
○	1	default	Fa 1/1,Fa 1/2,Fa 1/3,Fa 1/4,Fa 1/5,Fa 1/6,Fa 1/7,Fa 1/8,Gi 1/9,Gi 1/10	192.168.1.254
○	10	VLAN0010	Fa 1/1,Fa 1/2,Fa 1/3,Fa 1/4,Fa 1/5,Fa 1/6,Fa 1/7,Fa 1/8,Gi 1/9,Gi 1/10	
○	20	VLAN0020	Fa 1/1,Fa 1/2,Fa 1/3,Fa 1/4,Fa 1/5,Fa 1/6,Fa 1/7,Fa 1/8,Gi 1/9,Gi 1/10	

VLANs Trunked to Upstream Fully Managed IES

In order for the lightly managed IES to forward traffic for all of its VLANs to upstream fully managed IES over a single physical port, a trunk is used. This trunk maintains separation of the VLANs by tagging each frame with an IEEE 802.1Q VLAN ID. When the fully managed IES receives a frame with the tagged VLAN ID, it is able to determine to which VLAN the frame should be forwarded.

Trunks are configured on the Port Settings page of Device Manager. In Figure 3-5, both interfaces Gi 1/9 and Gi 1/10 are configured as trunks; however, typically just a single interface would be connected to an upstream fully managed IES, unless EtherChannel was used.

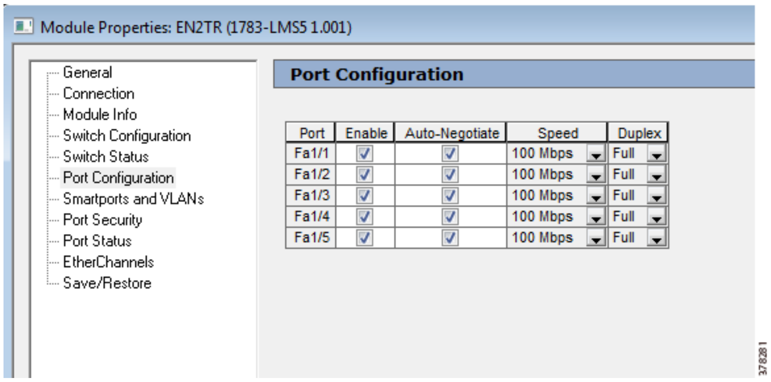
Figure 3-5 Device Manager—Port Settings



	Port Name	MTU	Port Status	Speed	Duplex	Media Type	Access VLAN	Administrative Mode
○	Fa 1/1	1998	●	100Mbps	Full	10/100BaseTX	1	access
○	Fa 1/2	1998	●	Auto	Auto	10/100BaseTX	10	access
○	Fa 1/3	1998	●	Auto	Auto	10/100BaseTX	10	access
○	Fa 1/4	1998	●	Auto	Auto	10/100BaseTX	10	access
○	Fa 1/5	1998	●	Auto	Auto	10/100BaseTX	20	access
○	Fa 1/6	1998	●	Auto	Auto	10/100BaseTX	20	access
○	Fa 1/7	1998	●	Auto	Auto	10/100BaseTX	20	access
○	Fa 1/8	1998	●	Auto	Auto	10/100BaseTX	20	access
○	Gi 1/9	1998	●	Auto	Auto	sfp1000BaseT	1	trunk
○	Gi 1/10	1998	●	Auto	Auto	sfp1000BaseT	1	trunk

Shown below in Figure 3-6, for illustrative purposes, the Allen-Bradley Stratix 2500 lightly managed IES can also be managed using Studio 5000 Logix Designer software.

Figure 3-6 Management via Studio 5000 Logix Designer



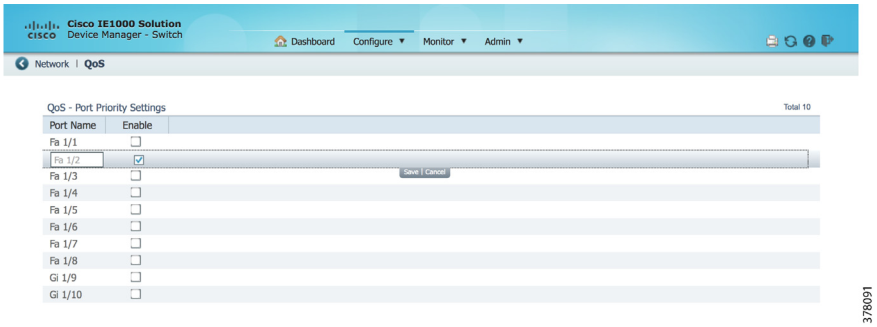
Port	Enable	Auto-Negotiate	Speed	Duplex
Fa1/1	☑	☑	100 Mbps	Full
Fa1/2	☑	☑	100 Mbps	Full
Fa1/3	☑	☑	100 Mbps	Full
Fa1/4	☑	☑	100 Mbps	Full
Fa1/5	☑	☑	100 Mbps	Full

Port Priority for Latency Sensitive IACS Device

Depending on a variety of factors (including type and number of IACS devices and other endpoints), the industrial network can experience congestion at times. Congestion can lead to high latency and jitter, or even packet loss. When congestion does occur, the network needs to intelligently validate that the most critical traffic is not impacted.

Lightly managed IES support basic QoS for prioritizing important traffic that is not tolerant of latency, jitter or packet loss. QoS is implemented on the switches in the form of a port priority feature that is accessed by navigating to **Configure > QoS**. The port priority is simply configured by selecting one (or more) interfaces and then checking the **Enable** check box. In this example, an IACS device that is not tolerant of packet loss or latency is connected to port Fa 1/2.

Figure 3-7 Device Manager - QoS



QoS - Port Priority Settings Total 10

Port Name	Enable
Fa 1/1	□
Fa 1/2	☑
Fa 1/3	□
Fa 1/4	□
Fa 1/5	□
Fa 1/6	□
Fa 1/7	□
Fa 1/8	□
Gi 1/9	□
Gi 1/10	□

By default, the lightly managed IES will trust DSCP and COS markings on ingress frames, and will not re-write the markings on egress, unless the egress interface has port priority enabled. With port priority enabled, the lightly managed IES re-marks ingress frames with DSCP = 24 and COS = 3, no matter the original marking.

The lightly managed IES has eight egress queues using strict priority scheduling algorithm, meaning a fixed mapping exists between the DSCP/COS markings and the egress queue.

Table 3-1 COS to Egress Queue Mapping

COS Value	Egress Queue (7 is highest priority)
1	0
0	1
2	2
3	3
4	4
5	5
6	6
7	7

Table 3-2 DSCP to Egress Queue Mapping

DSCP Value Range	DSCP Name	Egress Queue (7 is highest priority)
8-15	CS1	0
0-7	CS0	1
10-14	AF11 - AF13	
16-23	CS2	2
18-22	AF21 - AF23	
24-31	CS3	3
26-30	AF31 - AF33	
32-39	CS4	4
34-38	AF41 - AF43	
40-45, 47	CS5	5

Table 3-2 DSCP to Egress Queue Mapping (continued)

DSCP Value Range	DSCP Name	Egress Queue (7 is highest priority)
48-55	CS6	6
46, 56-63	EF CS7	7

The Port Priority feature should only be enabled on one, or possibly two, of the ports of the switch—those connected to critical devices that are not tolerant of latency, jitter or loss. If the feature is enabled on all ports, all ports will have the same priority, thus negating the intended benefit.

Layer 2 NAT on Managed IES

As shown in Figure 1-5, the lightly managed IES is connected to an upstream fully managed IES with NAT capability. In this example, the process skid containing the lightly managed IES and attached IACS devices is one of many such sub-zones. To simplify the network design and configuration, duplicate IP addressing is used in all of the sub-zones—192.168.10.x/24 and 192.168.20.x exist in multiple locations in the plant. In order for IACS devices in multiple sub-zones to coexist with overlapping IP addresses, network address translation (with multiple instances of NAT, on a per-VLAN basis) is configured on the upstream fully managed IES. This allows the overlapping addresses to be statically mapped to unique "outside" IP addresses reachable throughout the plant.

More information on “Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture” can be found at the following URLs:

- Rockwell Automation site:
  - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf
- Cisco site:
  - https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html