CHAPTER 2

Lightly Managed IES in the Sub-Zone

This chapter includes the following major topics:

- Highlights, page 2-1
- Network Considerations, page 2-2
- Comparison to Fully Managed Switches, page 2-4

The Cisco IE 1000 and Allen-Bradley Stratix 2500 series lightly managed industrial Ethernet switches (IES) provide machine level connectivity at the edge of the CPwE architecture. Designed from the ground up to operate in demanding industrial environments, these switches include capabilities for reliably, securely and easily connecting IACS equipment in a small, cost-effective package.

Highlights

- **Variety of Port Configurations**—These include FastEthernet and copper and between 5 and 10 ports per switch.
- **Easy Integration**—Zero-touch IP discovery or DHCP IP addressing and simple web GUI-based management.
- **Fast Startup Time**—Starts 30 seconds from cold boot.
- **Manageability**—Web GUI interface, Studio 5000 Logix Designer® for the Allen-Bradley Stratix 2500 only, and diagnostics and analysis options through Simple Network Management Protocol (SNMP) and syslog.
- **Security**—Secure access; port-security.
- **Minimize Data Load**—Internet Group Management Protocol (IGMP) and DHCP snooping to filter unwanted data.
- **Logical Segmentation in a Single Switch**—Virtual LAN (VLAN) support allows for logical segmentation in a single switch, which reduces total number of necessary switches.
- **Lightly Managed**—Rapid Spanning Tree Protocol (RSTP), Link Layer Discovery Protocol (LLDP), Cisco Discovery Protocol (CDP)-aware.
- **Gigabit Uplink**—Two SFP-based fiber optics; uplink for up to 50 miles (80 kilometers) links.
- **Industrial Power over Ethernet (PoE)**—Up to eight PoE (IEEE 802.af) and PoE+ (802.3at) supported on selected models.

- Redundant voltage feeds, alarm relays support and DIN rail mount.
- Industrial environmental compliance and certifications.

For detailed product specifications, refer to the following official documentation.

- *Cisco Industrial Ethernet 1000 Series Switches Data Sheet* at the following URL:
  - http://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-1000-series-switches/datasheet-c78-737277.html?cachemode=refresh
- *Allen-Bradley Stratix Ethernet Device Specifications* (Technical Data) at the following URL:
  - http://ab.rockwellautomation.com/Networks-and-Communications/Stratix-2500-Lightly-Managed

Network Considerations

This section describes some of the most important considerations for designing and implementing the Cell/Area Zone (and sub-zones), using features available on the lightly managed IES. For a more detailed discussion of these and other considerations, refer to *The OEM Guide to Networking* from Rockwell Automation at the following URL:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/rm/enet-rm001_-en-p.pdf

Network Segmentation (Zoning) and Addressing

IEC 62443 and the Purdue model illustrate the value and importance of a segmented industrial automation network. Network segmentation refers to logically (or physically) separating the network (and, more importantly, devices on the network) into multiple smaller networks based on IACS functionality zoning (scalable building blocks), for purposes that include traffic control, security (IEC 62443 zoning) or management efficiency.

Within a network, various types of traffic are typically broadcast to every host (for example, IACS device), which can quickly use up available bandwidth or expose sensitive data to unwanted recipients. By limiting the size of these Layer 2 networks (referred to as broadcast domains), traffic storms and reachability can be more tightly restricted. Segmenting the network based on physical location, function of the IACS end devices or similar factors is recommended. In Figure 1-1 on page 1-1, for example, the manufacturing plant is divided into three production lines, each with its own subnetwork.

Two basic methods exist for segmenting a Layer 2 network. Traditionally segmentation has often been accomplished with using one (or more) basic physical unmanaged switch per subnetwork. Segmentation can quickly become expensive because of the number of switches required to support different networks and the high potential for unused switch ports in areas with a small number of devices that need to be connected to a network.

In addition to segmentation with multiple switches, the second, preferred, method for segmenting the network is to logically separate the network using Virtual Local Area Networks (VLANs) within the IES. In this way a single IES can carry many different networks (or broadcast domains) on the IES, while allowing the network to still remain distinct and separate. Each physical port on the IES can be assigned to a specific VLAN, meaning that the device connected to that port can only communicate with other devices connected to different switch ports within the same VLAN. A single VLAN can potentially span across many different IES. When two IES need to connect to each other, they typically do so using ports configured as trunks that allow multiple VLANs to traverse the connection simultaneously, while staying separated by the use of a VLAN tag in the Ethernet frame header.

Each VLAN is assigned an IP subnetwork, which is a range of IP addresses that devices within the subnet use to communicate with each other. In order for devices to communicate with devices outside of their subnet/VLAN, they need to go through a Layer 3 IES. OEMs often want to use common IP addressing schemas for their IACS applications, where they often duplicate the build of machines, skids or equipment. In this case, the subnet would be contained within the IACS application-only used for communication between the IACS devices. Duplication of the OEM application, including the IP addressing schema, enables a common network configuration across the plant floor. Caution should be used when overlapping or identical IP addressing is used in multiple parts of the plant-wide IACS network. Network edge devices may communicate directly with common network applications that may not be capable of distinguishing between two devices with the same IP address. To resolve IP address duplication issues, NAT can be configured at the fully managed IES, functioning as the boundary of the VLAN and subnet. NAT, and more specifically Layer 2 NAT (L2NAT), works by maintaining a mapping of an IP address within the overlapping subnets and a unique address that is reachable by the rest of the network. The fully managed IES with NAT capability could then be used to aggregate the lightly managed IES.

Chapter 3, “Integrating Lightly Managed IES into the CPwE Architecture” contains additional information on network segmentation.

Note The lightly managed IES does not support NAT.

Data Prioritization

Within an industrial environment, applications that have very strict network requirements exist to help ensure that their application messages get through the network reliably and quickly. Latency and jitter must be minimized as much as possible, especially at the edge of the network where critical IACS devices are communicating directly with each other to operate physical equipment and processes.

When a network experiences high levels of load, it will be forced to start queuing packets and potentially dropping/discarding some of them if the network cannot physically accommodate all of the traffic. In scenarios like this, critical application data such as IACS protocols must be given priority over less important types of traffic. Quality of Service (QoS) generically refers to a set of features that help facilitate that specific types of traffic are given preference over others. Giving priority to IACS protocols such as CIP or PROFINET helps to make sure that they do not have wait in a queue behind less critical data, or get dropped during times of congestion.

Note The lightly managed IES does not support CIP QoS policies for time critical IACS applications such as motion control.

Resiliency

Network resiliency is critical when the operation of the manufacturing plant machinery depends on it. Resiliency should be built into every level and layer of the network to help confirm that (whenever possible), no single point of failure in the network can cause an outage. Within the Cell/Area Zone, the IES should be connected redundantly to give traffic an alternate path in the event of a device or link failure. As discussed in the first chapter, deploying switches in ring or redundant star topologies is highly recommended, along with implementing redundancy protocols such as REP.

Note The lightly managed IES only supports RSTP for ring topologies and EtherChannel for redundant star topologies.

For an OEM application, using STP (or its improved variants like Multiple STP or Rapid STP) allows the lightly managed IES to protect itself from loops when using multiple redundant uplinks, while helping it to re-converge over an alternative path if a primary, active link goes down.

Using Link Aggregation Control Protocol (LACP)-based EtherChannels allow IES, even for OEM applications, to connect to the aggregation switch using two uplinks (both active) and automatically load balance traffic across them. In that one of the uplinks fails, the switches can dynamically shift all traffic to the remaining interface in the EtherChannel.

Security

CPwE is designed to address security using a holistic *defense in depth* approach, using multiple technologies, across all levels of a plant-wide architecture. This approach helps to prevent issues before they happen, identify anything that is able to penetrate defenses and help remediate future incidents.

Within the Cell/Area Zone, one of the simplest means of enforcing security is preventing new, unwanted devices from connecting to the network and potentially accessing sensitive resources. A simple unmanaged switch will generally allow anything that plugs into it full access to all available resources. The port-security feature in the lightly managed IES helps combat this issue by monitoring the devices (by their MAC address) that are connected to each switch port. The IES can be configured to permit a certain number of learned devices to communicate using a specific port. If additional devices (identified by a new MAC address) are detected on the same port, the IES can react in several different ways either to continue forwarding traffic from known devices and alert the administrator of new devices or to completely shut down the interface.

Multicast

Multicast traffic within the Cell/Area Zone should be considered carefully when designing and implementing the IACS network. Various industrial protocols rely on multicast transmissions in which a single source needs to simultaneously talk to multiple hosts. A host can use IGMP to signal to the network that it wants to receive multicast packets sent to a specific group or IP address. Without IGMP enabled in the Cell/Area Zone, multicast packets will behave like broadcast packets that are forwarded out every port in the Layer 2 network (VLAN). This can mean that potentially a lot of data that is not desired traverses the network, which leads to congestion or security concerns if the multicast packets contain sensitive information that not all hosts should see. The lightly managed IES can monitor the network for IGMP control messages using a feature called IGMP Snooping. Using this feature, the switch can learn which of its ports are connected to hosts that have joined a specific multicast group. The multicast traffic for this group will only be forwarded out these ports. As more and more devices are connected to the network, the control of multicast/broadcast packets with IGMP snooping and other methods becomes much more important.

Comparison to Fully Managed Switches

The lightly managed IES are ideal for deployment as OEM skid, machine and Equipment IES and in the Cell/Area Zone (and especially sub-zones). Cisco and Rockwell Automation offer other industrial switches that are considered *fully managed*. Depending on customer requirements, these switches may be a better fit for certain scenarios. They offer additional options for port types and configurations and support for more

advanced network features such as Layer 3 routing, additional resiliency protocols such as REP and DLR and Flex Links and additional security features such as IEEE 802.1x. The full list of differences is available in the official documentation and is outside the scope of this CRD. Visit the following links to find information about the full line-ups of Cisco and Allen-Bradley IES:

- Cisco Industrial Ethernet Switches at the following URL:
  - http://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html
- Rockwell Automation/Allen-Bradley EtherNet/IP Network at the following URL:
  - http://ab.rockwellautomation.com/Networks-and-Communications/Ethernet-IP-Network