SEL® Application Note AN2013-01

Applying VLANs With the SEL-2730M to Improve Network Manageability

Simon Loo

INTRODUCTION

A wide-area network (WAN) or local-area network (LAN) is designed to transport data among geographically distributed sites. Networks carry large amounts of data for a wide variety of applications and services. The electric power system, water treatment plants, large industrial facilities, petrochemical plants, gas pipelines, and transportation systems all rely on wide-area communication to run and manage complex processes and systems. The majority of the facilities in these operations are considered critical infrastructure facilities and are essential for the success and well-being of the economy. A utility substation contains a diverse range of equipment requiring communication between local equipment, other substations, and remote sites. A network is required to support applications that include voice, data, teleprotection, video, control and automation, and email and corporate LAN access.

PROBLEM

The nature of the WAN means that data have to leave the controlled local-area environment of an office, plant, or substation facility. Many WANs also interconnect with WANs operated by other organizations. These attributes introduce specific network security risks that in turn expose the processes and systems within the critical infrastructure facilities to threats from cyberattacks. The potential damage and disruption caused by a hacker gaining access to a power utility WAN is enormous, ranging from localized power outages to widespread blackouts, destruction of power equipment, and loss of life. It is therefore essential that the security risks of the network are understood and that appropriate steps are taken to safeguard the network against threats from cyberattackers.

SEL SOLUTION

The SEL-2730M Managed 24-Port Ethernet Switch has the ability to create virtual local-area networks (VLANs), which allow the partitioning of networks into individual pipes as a tool to segment workgroups or substation communication. VLANs are defined by the IEEE 802.1Q standard and allow a single physical Ethernet infrastructure to support multiple logically separate Ethernet networks.

In most network applications, VLAN tagging can be applied to data at the SEL-2730M Ethernet port while the end devices are completely unaware that a tag has been applied. An end device connects to an untagged port, and a managed switch assigns that port to a logical VLAN, which segments it from the other ports not in that particular VLAN. When the end device sends an untagged Ethernet frame, the SEL-2730M applies a VLAN tag to the Ethernet port traffic before forwarding it to an adjacent switch, which removes the tag before sending the untagged frame to the destination, as shown in Figure 1.

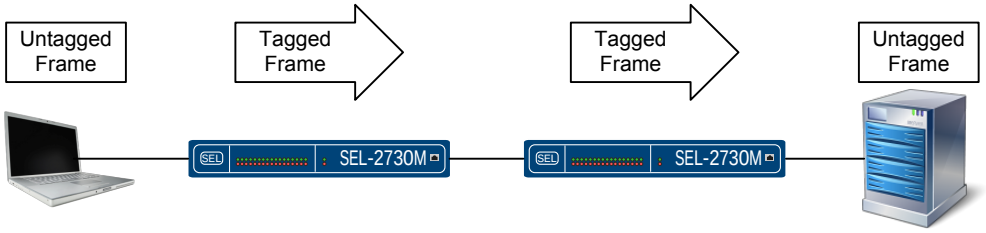

Figure 1 VLAN for Network Applications

The SEL-2730M ensures that the broadcast domains of each application are kept separate and that one application cannot interfere with another application. However, while VLANs improve network manageability, correct switch configuration and network architecture are more important for securing a system.

Generic Object-Oriented Substation Event (GOOSE) messaging transmits sets of data within a time period of 4 milliseconds. The SEL-2730M can use the same VLAN tags defined by intelligent electronic devices (IEDs) participating in a GOOSE messaging transmitted frame, and the destination IED receives the frame with the tagging still applied (see Figure 2). This creates an isolated pipe among groups of IEDs while it minimizes latency for mission-critical GOOSE applications.

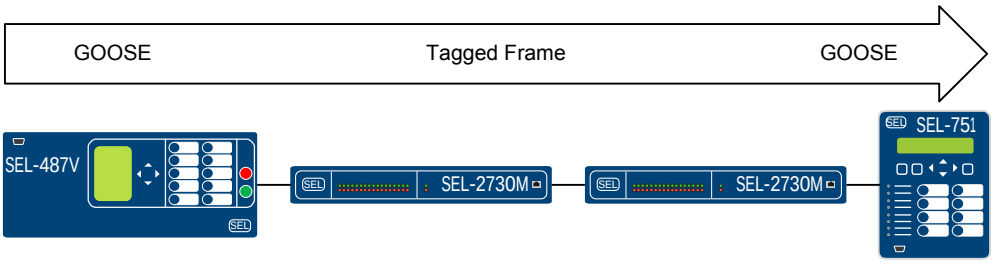

Figure 2 VLAN for GOOSE Application

Figure 3 shows an example of a port-based VLAN applied with SEL-2730M switches at Sites A, B, C, and D. The network is required to support the following applications: video over Internet Protocol (IP), Voice over IP (VoIP), corporate LAN access, and communication between IEDs. The video-over-IP network is on the port-based VLAN 33, the VoIP network is on the port-based VLAN 11, the corporate LAN access network is on the port-based VLAN 55, and the IED network is on the port-based VLAN 22. These applications are completely isolated, do not have awareness of other VLANs, and cannot interfere with the operation of other VLANs.

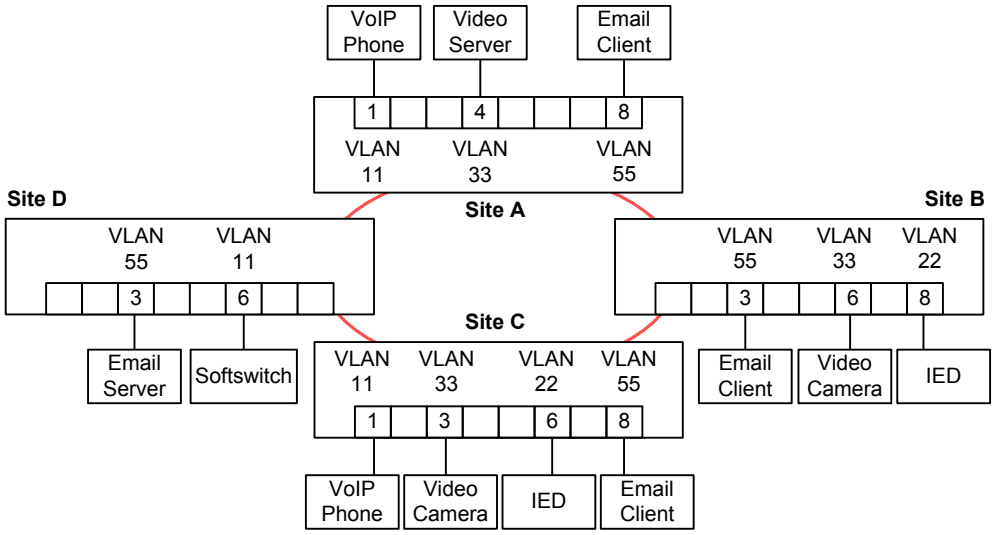

Figure 3 Example of Port-Based VLAN

CLOSING NOTE

As communications networks trend toward becoming more robust, cybersecurity is more important than ever. The possibility of a successful cyberattack against the power infrastructure cannot be ignored. Proper network architecture and switch configuration are required for improved security, while VLANs can help improve network manageability. Mitigating vulnerabilities is a manageable task and power industry professionals should all be aware of the methods to secure communications networks.

LAN2013-01

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com