Protection and the Communications Network: Can You Hear Me Now?

Ken Fodero and Adrian Silgardo, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—When protective relay traffic is run over a communications network, the security and dependability of the network are primary concerns. Security is defined as the immunity of critical traffic to threats. Dependability is defined as the on-time delivery of traffic. Power utility companies have used several different technologies to build their communications networks. This paper looks at SONET and Ethernet technologies and how they address security and dependability concerns.**

I. INTRODUCTION

Communications networks are a power utility's strategic asset and play an important role in the successful operation of an electric power grid. As a utility strives for greater power grid efficiency by using new applications, the demands on communications networks evolve.

Power utility communications networks are built with a wide range of technologies and media. Technologies used include power line carriers, T1 multiplexers, SONET (synchronous optical network) multiplexers, and Ethernet switches. Media used include leased lines, microwaves, and fiber-optic cables.

Traffic requirements in a utility communications network have evolved from low-bandwidth applications to a combination of low- and high-bandwidth applications. For example, early utility communications networks were designed to handle voice, low-speed SCADA, and teleprotection channels with point-to-point services. The utility communications network today is expected to handle not only low-bandwidth applications but also high-bandwidth applications such as video and corporate data, operating as either point-to-point circuits or point-to-multipoint circuits.

While traffic requirements and technologies have evolved for both communications and protective relays, the service demands on these areas continue to remain the same. The service must be dependable and secure, ensuring that the overall service is reliable.

In a utility communications network, dependability is defined in general terms as the on-time delivery of traffic and, in more specific relay terms, as being able to trip when required to trip. Security is defined in general terms as the ability to deliver critical traffic and, in specific relay terms, as being able to refrain from tripping when not required to trip. This security should not be confused with cybersecurity or network security.

In this paper, we will focus on SONET and Ethernet technologies. These are the two most popular technologies in use today in new system installations. Currently, these technologies coexist in the substation. In the time division multiplex (TDM) domain, teleprotection is easily applied, and overall system performance is understood. With the introduction of IEC 61850 and routable SCADA protocols, Ethernet is becoming a more popular technology. Ethernet applications have primarily grown from nonteleprotection services. Teleprotection applications over Ethernet are viable; however, performance differences exist in Ethernet versus TDM architectures. Ethernet segmentation and traffic prioritization are technologies that may provide the security and dependability required for teleprotection applications over Ethernet.

II. SONET NETWORKS

The telecommunications community developed SONET networks to improve efficiency and provide greater flexibility to telecommunications transmission networks.

A SONET network circuit enhances teleprotection security, as each circuit has its own dedicated bandwidth in the SONET payload, and traffic in one circuit cannot corrupt traffic in another circuit. A circuit is dependable, as the latency is deterministic. Dependability is further enhanced by deploying SONET networks in ring topologies. Dedicated communications paths for network management provide the user with the ability to manage circuits in the network. While a SONET network handles point-to-point circuits in an effective manner, difficulties arise in a SONET network when it comes to multicast traffic.

The SONET frame is defined as 9 rows by 90 columns, or 810 bytes. Each byte contains 8 bits, which are sampled 8000 times per second. The frame is transmitted in 125 µs.

$$\text{OC-1 or STS-1} = \frac{810 \text{ bytes} \bullet 8 \text{ bits}}{125\ \mu\text{s}} = 51.84\ \text{Mb/s}$$

The SONET frame consists of overhead and payload. The overhead carries information to manage the frame through the network, while the payload carries user data. Overhead is 27 bytes (9 rows by 3 columns), and the payload is 783 bytes (9 rows by 87 columns). The first column of the payload is the path overhead.

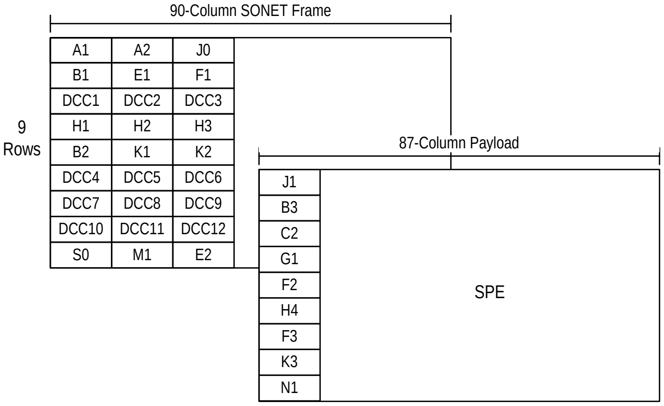

Fig. 1. SONET Frame

The SONET digital hierarchy comprises multiple instances of the basic frame by interleaving the bytes. The SONET digital hierarchy is shown in Table I.

Higher-order SONET signals are direct multiples of a lower-order signal. For example, an OC-3 signal is made up of three STS-1 signals, or an OC-12 signal is made up of 12 STS-1 signals.

TABLE I
SONET DIGITAL HIERARCHY

SONET				
STS Level	**OC Level**	**Line Rate Mb/s**	**Virtual Tributaries**	**DS0 Channels**
STS-1	OC-1	51.84	28	672
STS-3	OC-3	155.52	84	2016
STS-12	OC-12	622.08	336	8064
STS-48	OC-48	2488.32	1344	32256
STS-192	OC-192	9953.28	5376	129024

The synchronous transport signal (STS) is the electrical equivalent of an optical signal (OC). A virtual tributary (VT) is a synchronous signal with a line rate of 1.728 Mb/s and is transported within the SONET payload. A Virtual Tributary 1.5 can transport a DS-1 signal (1.544 Mb/s) or 24 DS0 channels (64 kb/s). Digital Signal Level 0 (DS0) is a 64 kb/s signal.

A. *Network Simplification*

Plesiochronous Digital Hierarchy (PDH) networks are widely used in utility networks. The PDH hierarchy is shown in Table II. PDH networks use bit stuffing to multiplex signals from one level to the next.

TABLE II
PDH HIERARCHY

Level	Line Rate (Mb/s)	DS0 Channels
DS-1	1.544	24
DS-2	6.312	96
DS-3	44.736	672
DS-4	139.24	2176

Fig. 2 shows a DS-3 PDH network with multiplexer equipment installed at Site A, Site B, and Site C. Site A and Site C house line-terminating equipment, while Site B houses drop and insert equipment. In this network, DS1 traffic is required between Sites A and B, and Sites A and C.

The DS1 signal between Sites A and C passes through Site B. At Site B, the 45 Mb/s line signal is demultiplexed to 6 Mb/s, and then the 6 Mb/s signal is demultiplexed to 1.544 Mb/s in order to pass through the DS1 signal to Site A or Site C.

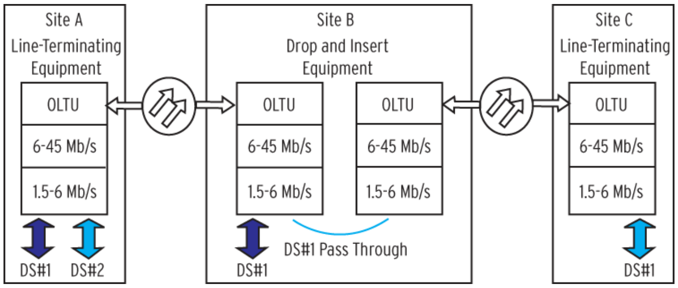

Fig. 2. PDH Network

Fig. 3 is a SONET network. In a SONET network, each network element is timed to a master clock. It is easy to identify the position of the channels in the SONET bit stream because the network is synchronous. In the SONET network, the 1.544 Mb/s signal can be dropped from the 155 Mb/s SONET line signal.

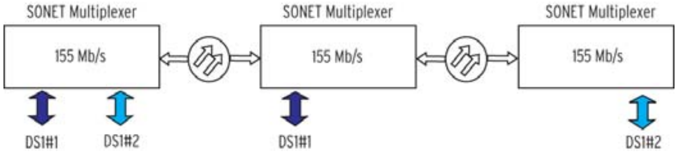

Fig. 3. SONET Network

The ability to drop and insert channels in an efficient manner in a SONET network means lower operating costs with less equipment, lower power consumption, and simpler maintenance.

B. *Network Management*

When developing the SONET standard, users were provided the ability to manage the SONET network from a remote location. Specific bytes in the overhead are defined for network management capability. The bytes assigned to carry network management information are DCC1 through DCC12 (refer to Fig. 1). User benefits include end-to-end circuit monitoring, event management, configuration management, and inventory management.

C. *Network Survivability*

SONET network elements can be deployed in a wide range of network architectures—from linear networks to protected linear networks, to ring networks and multiple ring networks. Selection of appropriate network architecture depends on a number of factors, e.g., the availability of fiber, fiber route diversity, and backup path requirements. The ring network architecture is popular because it provides communications path redundancy. Two types of ring architectures are proposed in the standard: the unidirectional path switched ring (UPSR) and the bidirectional line switched ring (BLSR).

Fig. 4 shows the operation of a UPSR. The application is a DS1 circuit between Sites A and B. In the transmit direction from Site A to Site B, the DS1 signal is mapped in a VT and is sent in opposite directions around the ring. Site B receives the DS1 signal from the clockwise and counterclockwise directions and selects one of the two signals. In our example, Site B has selected the clockwise direction; thus the primary path for our DS1 signal is Site A to Site B, while the alternate path is Site A to Site B through Sites D and C.

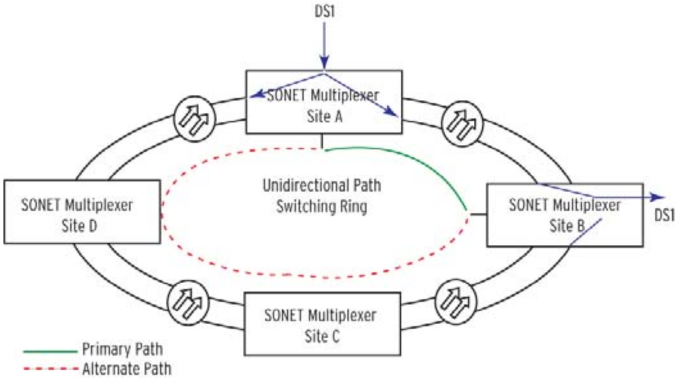

Fig. 4. Traffic From Site A to Site B

Fig. 5 shows an example of a failure on the primary path. For the DS1 signal path Site A to Site B, a switch occurs at the receiving end at Site B, and the VT path in the alternate direction around the ring is used. The SONET standard specifies a failure detection time of 10 ms and the switch time as 50 ms. Many vendors who manufacture equipment for utility protection applications provide switch times in the 5 to 50 ms range.

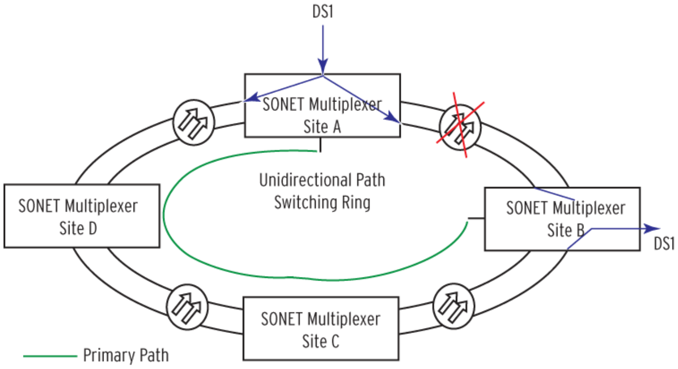

Fig. 5. Failure on Primary Path; Alternate Path Becomes Primary Path

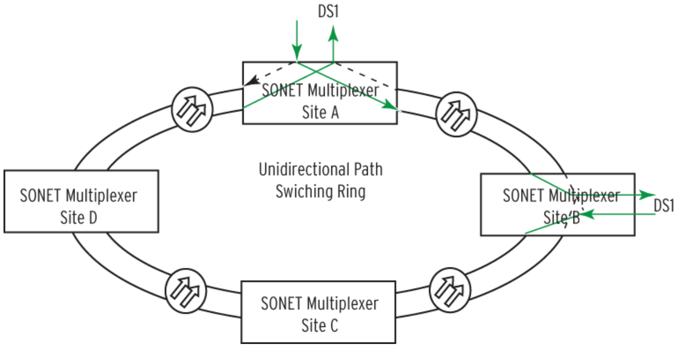

Fig. 6. Asymmetric Delays in a SONET Network

While SONET networks support fault-tolerant network architectures, protection engineers should be aware of the possibility of asymmetric delay—different delays on transmit and receive paths. For Fig. 6, consider the following: the traffic from Site A to Site B is clockwise, and the traffic from Site B to Site A is also clockwise. This could lead to different delays on the paths from Site A to Site B and from Site B to Site A. Analog current differential relays are not equipped to deal with asymmetric delays and are subject to misoperations under these conditions. Most modern, digital current differential relays are able to tolerate asymmetric channel delays. This is an example of an existing teleprotection scheme applied over a new communications technology with unexpected results.

D. *SONET Networks—Dependability and Security*

Latency is extremely important when assessing the dependability of a network. In a SONET network, latency is deterministic (0 to 125 µs) and typically caused by the 8 kHz fundamental sampling rate, latency (about 25 µs) passing through each repeater node, and latency of approximately 5 µs/km for internode fiber cables.

SONET is based on TDM technology, with each channel assigned its own time slot and each circuit isolated from the others.

III. ETHERNET NETWORKS

More power utilities are applying or evaluating Ethernet networks for substation instrumentation and control (I&C). Interest in Ethernet is driven in part by lower hardware costs and the use of IEDs with Ethernet ports.

In an Ethernet network, traffic can share the same transport pipe; however, traffic can be segmented to different domains using virtual local-area networks, or VLANs. While Ethernet networks are attractive for multicast traffic, they must be engineered properly in order to produce desired security and dependability. One security concern is mission-critical and untrusted Ethernet traffic coexisting in the same pipe. Using VLANs and filtering VLANs on untrusted ports can mitigate the security concern of mission-critical and untrusted source traffic sharing the same pipe. Packet queues add latency, which is a dependability concern. This can be mitigated by using high priorities for critical traffic and lowering the priorities of untrusted ports.

The Ethernet switch is the central network component in a substation Ethernet network. Ports on an Ethernet switch can be configured as either drop ports (connection to an IED) or trunk ports (connection to another network device's Ethernet switch or router). The primary function of an Ethernet switch is to establish a direct connection between a sender and a receiver, based on the media access control (MAC) address (Layer 2).

Ethernet switches support twisted-pair cable or dual-optical fiber connections to an Ethernet IED.

TABLE III
ETHERNET MEDIA DESIGNATIONS

Designator	Data Rate	Medium	Standard
10/100BASE-T	10 or 100 Mb/s	Twisted pairs of CAT 5 copper cable	IEEE 802.3u
100BASE-FX	100 Mb/s	Fiber-optic cable at 1300 nm wavelength	IEEE 802.3u
1000BASE-T	1 Gb/s	Twisted pairs of copper cable (CAT 5e or CAT 6)	IEEE 802.3ab
1000BASE-SX	1 Gb/s	Multimode fiber-optic cable at 850 nm wavelength	IEEE 802.3z
1000BASE-LX	1 Gb/s	Single-mode fiber-optic cable at 1270–1355 nm wavelength	IEEE 802.3z

A. *Ethernet Network Survivability*

A substation Ethernet network can consist of either unmanaged Ethernet switches dedicated for each application, as shown in Fig. 7, or of managed Ethernet switches in a network configuration, such as a ring or mesh network.

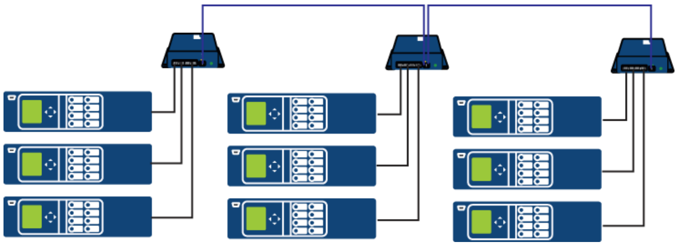

Fig. 7. Unmanaged Switches for Dedicated Intrasubstation GOOSE

Industry standards, like rapid spanning tree and spanning tree, with switch times of tens of milliseconds to many seconds were found to be too long for power utility protection applications. This prompted industrial Ethernet switch vendors to develop their own proprietary switching protocols with single-digit-millisecond switch times.

TABLE IV
ETHERNET SWITCHING PROTOCOLS

Ring Standard	Switching Time	Network Configuration
Spanning tree	Up to 2 min	Ring and mesh
Rapid spanning tree	50 ms to 5 s	Ring and mesh
Proprietary switching	5 to 10 ms per node or < 5 ms per circuit	Ring only

VLANs and priority tagging are Ethernet switch features that can play a role in enhancing security and dependability for these protection applications.

B. *VLANs*

A common definition of a VLAN is a logical group of network nodes that share similar resources and reside in a common broadcast domain without any router hops. The network nodes do not need to reside in the same physical location and can be spread out across the various facilities of the organization.

VLANs can be implemented in many ways. Common VLAN types include IEEE 802.1Q-based VLANs, which are formed using IEEE 802.1Q tags and port-based VLANs. The IEEE 802.1Q standard specifies a four-byte "tag" field that is added after the Ethernet frame source address. In this paper, VLANs with IEEE 802.1Q tags are referred to as QVLANs.

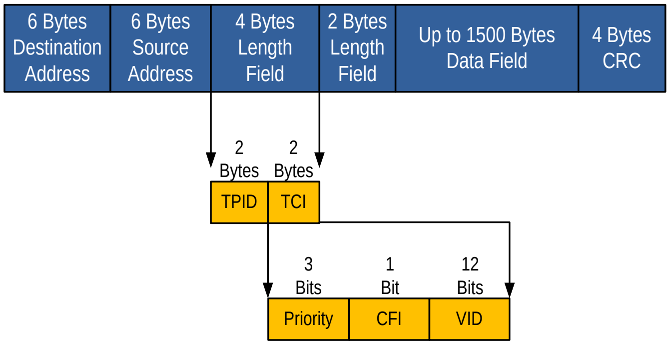

Fig. 8. IEEE 802.1Q VLAN Tag Field

The VLAN tag field consists of the tag protocol identifier (TPID) field (2 bytes) and the tag control information (TCI) field (2 bytes).

The TCI field consists of the VLAN ID (12 bits), user priority field (3 bits), and a CFI (canonical format indicator) bit (used for token ring networks).

Port-based VLANs are VLANs created by assigning a port to a particular VLAN number. One benefit of port-based VLANs is that they are easy to set up; however, a user is physically connected to one port, and moving to a different port will require reconfiguration. A common application of port-based VLANs involves segregating the different types of traffic by assigning each type a separate VLAN.

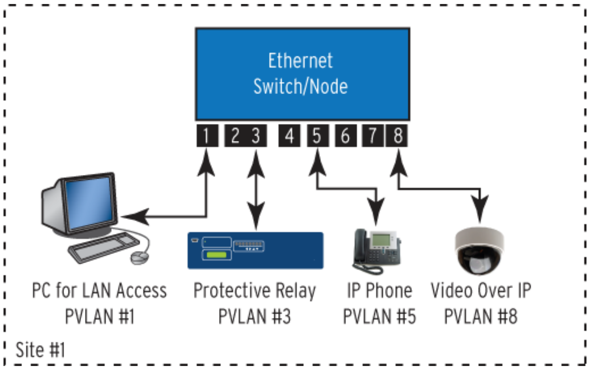

Fig. 9. Port-Based VLANs

As integration in the substation takes place and the number of devices is reduced, it would be useful if a device, such as a protective relay, could classify its services into different QVLANs. This proposed method of segregating device services is not available in today's protective relays. This application is being presented as a way to isolate unlike services in a network. In the TDM domain, this was accomplished by assigning different time slots to each service.

Fig. 10 shows three sites, with an Ethernet switch/node and a protective relay in each site. Four different services are supported on each relay, with each service assigned to a separate QVLAN.

TABLE V
QVLAN SERVICES SUPPORTED

Service	**QVLAN #**
Intersubstation GOOSE messages	4
Configuration	5
Intrasubstation GOOSE messages	6
Monitoring	7

The broadcast domain for each service is separate from the other services.

C. Quality of Service (QoS)

Ethernet applications in a power utility communications network are diverse and can range from time-sensitive applications, such as intersubstation GOOSE messages for teleprotection, to less time-sensitive applications, such as downloading engineering drawings from the engineering server. The QoS feature becomes important when network capacity is insufficient for the simultaneous transmission of real-time streaming data along with noncritical data. The intended application for QoS is Voice over IP (VOIP), IP-TV, and online games. These applications require fixed bit rates and are propagation-delay sensitive, much like the IEC 61850 GOOSE and teleprotection applications. The term *quality of service* can be misleading; QoS is a method of providing priorities to different applications and is not a measure of the achieved service quality. QoS allows the user to control the priority of different services across the network. Traffic classification is a function of the number of queues in the Ethernet switch/node and the flexibility provided to the user in directing traffic to the queues.

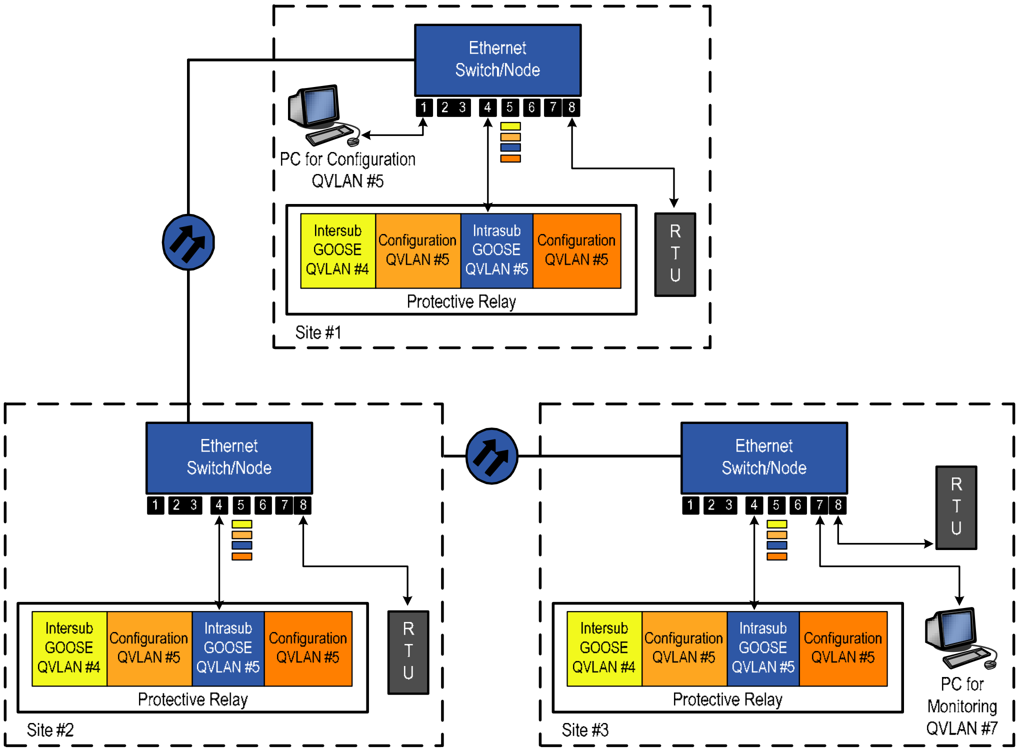

Fig. 10. Substation Implementation

As an example, consider the intersubstation traffic in Table VI.

TABLE VI
INTERSUBSTATION TRAFFIC

Traffic Type	Traffic Priority
Intersubstation GOOSE messages	7 (Highest priority)
Synchrophasor traffic	6
Engineering server access	4
Email	2 (Lowest priority)

If the Ethernet switch/node only supports two queues, then the intersubstation GOOSE message and the synchrophasor traffic would be directed to the high-priority queue, while the engineering server access and email would be directed to the low-priority queue. If all frames are queued in the high-priority queue, the latency for the frame to reach its final destination increases.

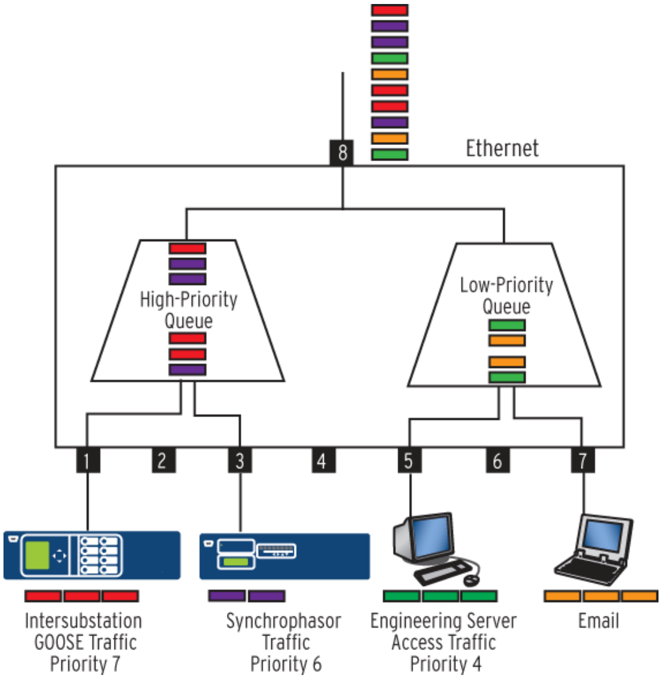

Fig. 11. Ethernet Switch With Two Queues

The greater the number of queues supported, the greater the flexibility provided in classifying the traffic.

IV. ETHERNET DETERMINISM

Ethernet communications have been labeled as a nondeterministic communications method. This is true when the Ethernet traffic is sent over the Internet. The Internet is a very large network, carrying large amounts of random data between unknown end points. Additionally, data traveling through the Internet can take many paths and will not take the same path consistently. This contributes to the nondeterministic nature of traffic sent over the Internet. This is also one reason the Internet is often represented as a cloud.

Private Ethernet networks should not be confused with the Internet. Private Ethernet networks can be designed to provide deterministic performance. The substation LAN shown in Fig. 12 is an example of an Ethernet network with predictable performance. There is no cloud associated with this network. The number of nodes and the data paths are known.

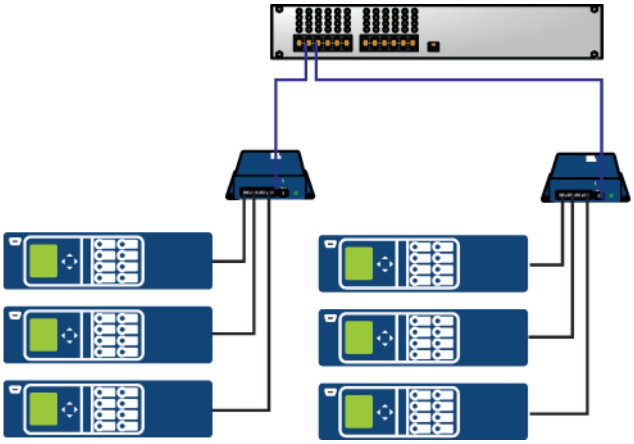

Fig. 12. Substation LAN

In an Ethernet network, the latency of an Ethernet frame is comprised of the propagation delay through the medium (in the case of fiber-optic cables, 5 µs/km) and the delay in the queue buffer at each network egress port.

The queue will always be at least one frame, as the switch/node needs to receive a complete frame before it can be forwarded and stored. The time to egress a maximum-length frame of 1518 bytes is 120 µs at 100 Mb/s and 12 µs at 1 Gb/s. If the network is busy, the queue can get as deep as eight frames. This will increase the delay through each switch/node by less than 1 ms at 100 Mb/s.

V. CONCLUSION

SONET networks provide point-to-point paths with dedicated bandwidth for each circuit/application. Dedicating bandwidth to a function is a method of enhancing the dependability of that function.

Using Ethernet products that support VLANs and QoS can also enhance dependability of an application over Ethernet. These features allow the switch or end device to filter out other data on the network (reducing the noise).

SONET or other TDM communications networks are inherently deterministic; however, asymmetric channel delays are possible.

Ethernet networks can provide deterministic communications. The network needs to be designed with this as a performance criterion.

VI. FURTHER READING

[1] IEC 60870-4: Telecontrol Equipment and Systems, Part 4: Performance Requirements.

[2] IEC 61850-3: Communication Networks and Systems in Substations, Part 3: General Requirements, Section 5: Environmental Conditions, First Edition, 2002-01.

[3] S. Ward, W. Higinbotham, and E. Duvelson, “Inside the Cloud – Network Communications Basics for the Relay Engineer,” proceedings of the 34th Annual Western Protective Relay Conference, Spokane, WA, October 2007.

[4] G. W. Scheer, “Comparison of Fiber-Optic Star and Ring Topologies for Electric Power Substation Communications,” proceedings of the 1st Annual Western Power Delivery and Automation Conference, Spokane, WA, April 1999. Available: http://www.selinc.com/techpprs.htm.

[5] V. Skendzic and R. Moore, “Extending the Substation LAN Beyond Substation Boundaries: Current Capabilities and Potential New Protection Applications of Wide-Area Ethernet,” proceedings of the 8th Annual Western Power Delivery and Automation Conference, Spokane, WA, March 2006. Available: http://www.selinc.com/techpprs.htm.

[6] G. Leischner and C. Tews, “Security Through VLAN Segmentation: Isolating and Securing Critical Assets Without Loss of Usability,” proceedings of the 9th Annual Western Power Delivery and Automation Conference, Spokane, WA, April 2007.
Available: http://www.selinc.com/techpprs.htm.

[7] “Virtual LAN Security Best Practices,” VLAN Security White Paper. Available: http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml.

[8] R. Breyer and S. Riley, *Switched, Fast, and Gigabit Ethernet: Understanding, Building, and Managing High-Performance Ethernet Networks*, 3rd ed., Sams, 1998.

VII. BIOGRAPHIES

Ken Fodero is currently an R&D manager for the time and communications product lines at Schweitzer Engineering Laboratories, Inc. (SEL). Before coming to work at SEL, he was a product manager at Pulsar Technology for four years in Coral Springs, Florida. Prior to Pulsar, Ken worked at RFL Electronics for 15 years; his last position there was director of product planning.

Adrian Silgardo is a senior product engineer with Schweitzer Engineering Laboratories, Inc. (SEL) in Canada. Adrian has over 13 years experience in the design and implementation of utility communications networks in North American and international markets. Prior to joining SEL, Adrian worked with GE Multilin Canada and Nortel Networks Canada building SONET networks for utilities.

20080922 • TP6325-01