Extending the Substation LAN Beyond Substation Boundaries: Current Capabilities and Potential New Protection Applications of Wide-Area Ethernet

Veselin Skendzic
Schweitzer Engineering Laboratories, Inc.

Roger Moore
RuggedCom, Inc.

Presented at the
8th Annual Western Power Delivery Automation Conference
Spokane, Washington
April 11–13, 2006

Extending the Substation LAN Beyond Substation Boundaries: Current Capabilities and Potential New Protection Applications of Wide-Area Ethernet

Veselin Skendzic, *Schweitzer Engineering Laboratories, Inc.*, Roger Moore, *RuggedCom, Inc.*

***Abstract*—Ethernet-based Local Area Networks (LANs) have become an indispensable tool that promises to revolutionize power system communications. Recent advances in Ethernet-based technology have taken this industry from shared 10 Mbps LAN segments to switched 100 Mbps LANs followed by 1 Gbps backbones for Metropolitan Area Networks (MANs) and more recently 10 Gbps Ethernet technology for use in Wide-Area Networks (WANs).**

Up until now, intersubstation communications typically have been provided by a SONET/SDH communication infrastructure. Although well understood and widely deployed, this legacy approach is not optimized for data traffic and requires protocol mapping and/or translation at both ends of the interface. The more recent trend of migrating towards Voice Over IP services combined with the advent of low-cost gigabit Ethernet switches and low-cost long-haul fiber optics has made it possible to deploy native Ethernet networks in wide-area applications.

This paper looks at the new capabilities in substation automation, protection, and control made possible by native Intersubstation Ethernet. Analysis is made of the current capabilities of this technology and state of the art tools available for Ethernet network management. The paper also examines application examples such as: Ethernet-based POTT protection schemes and synchrophasor data collection infrastructure. It concludes with a short overview of future application trends, including Ethernet-based line differential example.

I. Introduction

The role and potential benefits of Ethernet-based substation LAN are well known and have been extensively documented in the literature. Somewhat less known are the methods and devices necessary for interconnecting individual substation LANs into a reliable and secure utility-wide network capable of satisfying different needs presented by SCADA, engineering/maintenance access and power system protection applications. This paper discusses design alternatives and gives practical information necessary to design such utility-wide networks.

The problem of connecting multiple substation LANs together is similar to the problem of connecting Ethernet LANs into Metropolitan Area Networks (MAN). MANs represent a relatively new class of networks filling the space between Local Area Networks (LANs) spanning several buildings and Wide-Area Networks (WANs) spanning thousands of miles.

MANs typically span anywhere from 3 to 30 miles, but can, if necessary, be extended to cover an entire state. They are often owned by a single corporate user and have a built-in hierarchy with clearly separated access, distribution, and core layers.

As the size of the network increases, so does the variety of traffic it is expected to carry. This variety may include time-critical messages between protective relays, live video surveillance streams, Voice Over IP (VOIP), SCADA, engineering access, business data, and other nonutility-related traffic. It is therefore necessary to provide strict separation between different classes of traffic and to ensure guaranteed levels of service needed by the most critical applications.

While corporate LANs are widespread on the business and engineering side of the Electric Utility, their extension into power system substations is sporadic at best. This situation is expected to change under constant pressure to increase power system network utilization and reliability. Pressure is mounting on both sides of the barrier—on the control center side there is an increasing need to obtain reliable, real-time data about power system operation, and on the substation side there is an increasing amount of data being collected by the modern protection and control devices.

Traditional challenges presented by incompatible communication protocols have recently been addressed with widely accepted LAN-based standards such as IEC 61850, DNP-IP (in the US), and IEC 60870-5-104 (in Europe). While some competition among these standards is expected, the fact that the number of contenders has been reduced to three (actually two in each US/EU market) is very encouraging. Furthermore, all three standards can peacefully coexist on the same Ethernet network, thus enabling gradual transition to the LAN-based environment.

With the amount of Ethernet-enabled equipment exponentially increasing, the cost of the substation LAN deployment decreasing, and the communications protocol standardization problem resolved, the biggest task remaining is to interconnect substation LANs together.

Two technologies have emerged as primary candidates for this task. They are Ethernet over SONET (Synchronous Optical Network) and native switch-based Ethernet. This paper compares the two technologies and presents an application example using native switch-based Ethernet.

II. Key Technologies

Before attempting to compare different methods for extending the LAN between the substations, it is good to take a look at key enabling technologies that are making it all possible. Those technologies are listed below:

- Long-range fiber-optic transceivers
- Affordable 100 Mbps and 1 Gbps Ethernet hardware
- Utility-grade Ethernet switches with priority tagging and VLAN support
- Utility-grade routers

Long-range fiber-optic transceivers take care of the physical data transmission and fiber link monitoring. Over time, these transceivers have evolved towards standardized, highly affordable solutions such as the Small Form-Factor Pluggable (SFP) transceiver module shown in Fig. 1.

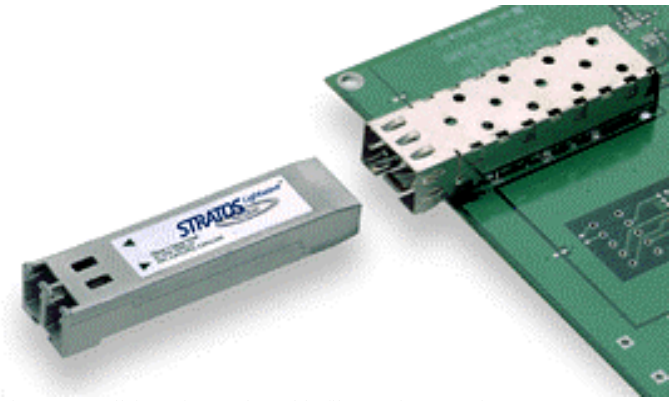

Fig. 1. Small form-factor pluggable fiber-optic transceiver

An SFP module enables very high port density and is equipped with a dual fiber-optic connector (LC shown) providing unambiguous termination for both transmit and receive fibers. The bottom side of the module is equipped with a special connector enabling it to be inserted into a mating "cage" (shown on the right-hand side of Fig. 1). An optional locking mechanism further ensures that the module can be securely fastened.

The modular, pluggable solution provides additional flexibility by making it possible to match the module cost and performance characteristics with the actual application requirements. Table I illustrates typical SFP module characteristics. Additional information about fiber-optic media and associated connector types can be found in [1].

Although Table I shows five different options for each speed grade, it is important to point out that they vary in popularity. Multimode fiber operating at 1310 nm is a clear winner for short-range applications (inside the substation), while the 1310 nm single-mode transceivers are most popular for connection between substations. Long wavelength (1550 nm) single-mode transceivers are used for very long links that cannot be established by any other means.

When required, Erbium Doped Fiber (EDF) amplifier repeaters can be used to extend maximum link distance. EDF amplifiers typically work at 1550 nm (C band), span 80 to 120 km per hop, have 17–30 dB of gain, and permit more than 20 hops in a row. The price tag associated with such amplifiers is significant, limiting their application to large network backbone deployments.

Table I
Ethernet SFP module Capabilities (typical values)

Speed	Fiber Type	Standard	Range	Wavelength
100 Mbps	Copper	100Base-TX	100 m	N/A
100 Mbps	Multi-Mode	100Base-SX	300 m	850 nm
100 Mbps	Multi-Mode	100Base-FX	2 km	1310 nm
100 Mbps	Single Mode	100Base-FX	10 km, 15 km, 50 km, 90 km	1310 nm
100 Mbps	Single Mode	100Base-LH	80, 120, 160 km	1550 nm
1 Gbps	Copper	1000Base-T	100 m	N/A
1 Gbps	Multi Mode	1000Base-SX	300 m	850 nm
1 Gbps	Multi Mode	1000Base-LX	500 m	1310 nm
1 Gbps	Single Mode	1000Base-LX	10, 30, 70 km	1310 nm
1 Gbps	Single Mode	1000Base-LH	50, 80 km	1550 nm

Another advantage brought forward by the module standardization is the fact that different long-haul network transports use the same fiber-optic modules. An example showing applicable Ethernet and SONET speeds is given in Table II.

Table II
Multi-Standard SFP Modules with Dual Ethernet/SONET Support

	Ethernet Speed	SONET Speed	SONET Channel
Module #1	100 Mbps	155 Mbps	OC3
Module #2	1 Gbps	2.45 Mbps	OC48
Module #3	10 Gbps	9.6 Gbps	OC192

Affordable Ethernet hardware and its ever-increasing speed have made the advancements in LAN technology possible. At the time of this writing, 100 Mbps represents the technology mainstream, with 1 Gbps being commonly available on more powerful servers and larger Ethernet switches. The 10 Gbps speeds are still reserved for core network backbones and are often aggregated together (on a single fiber) by using Waveform Division Multiplexing (WDM) technology.

Utility grade Ethernet Switches with RSTP, CoS, and VLAN support are a key factor behind substation Ethernet. Historically, Ethernet provided shared network access via CSMA/CD, which was a collision-based scheme inappropriate for critical substation communications and real-time control.

Modern Ethernet switching (also known as bridging) uses a store and forward mechanism to eliminate collisions and allow full duplex operation. Network redundancy with fast failover times is provided via the rapid spanning tree protocol (RSTP). Class of service (CoS) is provided via IEEE 802.1P to reduce latency for critical traffic. Network segregation and increased security are provided by IEEE 802.1Q VLANs. Access control to the LAN is provided by MAC-based port security and IEEE 802.1x. Numerous other features exist in Ethernet switches to improve network utilization, increase security, and reduce administration [2]. Ethernet-based switching technology is finding its place at the very core of the telecommunication network convergence (carrier routing systems) with data processing bandwidths scaling up to terabit rates [3].

Although extremely powerful, commercial LAN switching products often lack the robustness necessary to operate in the power system substation environment. Fortunately, Ethernet switches exist that are compliant with the IEEE 1613 and IEC 61850-3 standards for telecommunication equipment within a substation. Such Ethernet switches are as environmentally robust as substation IEDs and are capable of operating from the substation battery supply. Utility grade switches offer enhanced reliability, EMI immunity, and extended operating temperature range.

Utility-grade routers similar in robustness to utility-grade switches are specifically designed to offer reliable performance in the harsh substation environment. The two primary purposes of a router in a substation are to provide connectivity to other networks and to provide secure access to the LAN.

Routers are synonymous with the Internet protocol that forwards traffic to other networks based upon the destination IP address. Routers segregate traffic between LANs and stop broadcast traffic and unroutable traffic from crossing the boundary. The IP protocol was originally designed for redundant paths, and routing protocols such as RIP, OSPF, and BGP help attain that goal. Physical connectivity to other networks can be achieved via a variety of technologies including Ethernet, T1/E1, 56 k DDS, DSL, and POTS dial up using link protocols such as raw Ethernet, PPP, and Frame Relay. Though not a topic of this paper, physical layers and protocols other than Ethernet can also extend the substation LAN albeit with different and typically slower performance characteristics.

Routers are also used to provide an Electronic Security Perimeter for critical cyber assets within a substation as defined by NERC CIP-005-1. Controlled access to the substation LAN is provided by a firewall within the router that can limit access based on source or destination IP address and IP port number. Use of VPN technology within a router allows for secure access over untrusted networks whether that is the Internet, a telco-provided private network, or the utility corporate network. Routers can also provide intrusion detection system (IDS) capability and intrusion prevention system (IPS) capability to further enhance security.

Network security is a very complex problem. It is accomplished through coordinated deployment of the continuous oversight process and multiple protection mechanisms including event logging, user-based accounts, substation device password control, virtual LAN separation, unused port blocking, management traffic separation, and network security perimeter functions as described above. A complete discussion of the security requirements is well beyond the scope of this paper, and the reader is encouraged to review the information published by the National Energy Research Council (NERC) for Security Guidelines for the Electricity Sector.

III. MAN Network Technologies

In the past, telecommunications networks were optimized to carry voice-based communications. Typical examples include T1/E1 and other PDH (Plesiochronous Data Hierarchy) data channels commonly used for substation communications. As implied by the term Plesiochronous, various parts of the PDH network are almost (but not precisely) synchronized with each other, which leads to sporadic data dropouts. While voice traffic dropouts can easily be tolerated, the same cannot always be said about modern data traffic.

Synchronous Optical Networks (SONET) in the US and Canada and Synchronous Data Hierarchy (SDH) networks in the rest of the world were used to aggregate PDH networks together, to alleviate dropout concerns, and to increase overall network throughput. Table III shows the most popular SONET/SDH line rates.

TABLE III
SONET/SDH LINE RATES

SONET Designation	SDH Designation	Line Rate
OC1	–	51.84 Mbps
OC3	SDH-1	155.52 Mbps
OC12	SDH-4	622.08 Mbps
OC24	–	1244.16 Mbps
OC48	SDH-16	2448.32 Mbps
OC192	SDH-64	9953.28 Mbps
OC768	SDH-256	39813.12 Mbps

SONET networks provide a high level of service reliability and excellent path failure protection. Unfortunately, synchronous equipment at its core is still optimized for legacy voice-based communications. When faced with modern data traffic, SONET equipment incurs additional bandwidth penalties and can be significantly more expensive than its Ethernet network-based alternative.

Following is a short comparison of key factors distinguishing Ethernet and SONET-based MAN network options.

A. Strong Points

1) SONET

SDH/SONET is a mature, well-understood transport technology. It is widely deployed at the telecommunication network core and is regarded to be highly manageable. SONET supports built-in path protection switching strategy whose response time (50 ms) is considered to be very fast when compared with other competing options. Response time is

predictable and is specified by the standards. Additional vendor-specific enhancements (<3 ms) are available.

SONET network topology is very simple with the resilient ring being the most widely used option.

2) Ethernet

When compared to SONET, Ethernet offers more efficient use of bandwidth in point-to-point and mesh-based topologies. Ethernet network topology is virtually unlimited and includes resilient, SONET-like rings. Ethernet technology is highly scalable and offers seamless growth potential.

With native Ethernet transport, there is no need to perform conversion to and from synchronous wire formats.

Ethernet offers lower initial equipment cost with a more favorable engineering and maintenance cost structure.

When deployed in a mesh network configuration, switched-Ethernet offers exceptional bandwidth utilization.

B. Drawbacks

1) SONET

In contrast to Ethernet, SONET is not optimized for highly dynamic IP data traffic. It requires configuration of fixed point-to-point circuits. Total available bandwidth must be subdivided into fixed portions that are then allocated to individual circuits. Since each circuit is allocated a fixed amount of bandwidth, unused portions of any given circuit are simply wasted.

Fixed bandwidth allocation problems can best be illustrated by looking at an example in which packets need to be exchanged between all nodes (mesh network at the logical level). For example, in the case of five nodes as shown in Fig. 2, SONET ring bandwidth must be subdivided into 10 individual circuits (connecting each node with all other nodes). Fixed bandwidth allocation results with a very inefficient use of bandwidth.

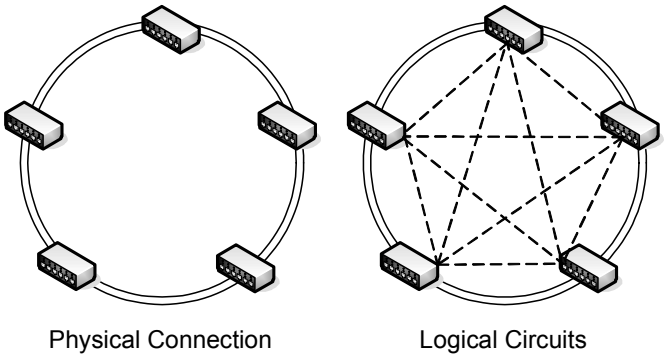

Fig. 2. SONET network bandwidth allocation example

SONET has limited topology support including point-to-point, linear, and ring. In addition, SONET is very inefficient for transferring multicast traffic. Since SONET ring consists of separate (pre-allocated) point-to-point circuits (one for each destination), each multicast message must be sent as multiple copies (one for each destination node).

In order to achieve path protection time specified by the standard, SONET rings are limited to a maximum of 16 nodes. The resulting maximum ring circumference is equal to 1200 km. Fast restoration time is accomplished by sacrificing 50 percent of the bandwidth (one fiber ring).

The cost of SONET technology has not managed to keep up with the steady decline in cost exhibited by Ethernet hardware.

The recent addition of the built-in Ethernet WAN/IP modules can alleviate some of the inherent SONET drawbacks.

2) Ethernet

In contrast to SONET, Ethernet was not optimized for ring network topologies commonly found while attempting to replace the legacy SONET/SDH infrastructure. Unless properly addressed, inadequate ring topology support can result in a slow response to fiber link failures (Spanning Tree algorithm speed issues). Rapid Spanning Tree (RSTP) and Enhanced Rapid Spanning Tree (eRSTP) algorithms were designed to address this drawback, with resulting ring reconfiguration times lowered from multiple seconds down to <5 ms per hop. Additional technologies such as Resilient Packet Ring (RPR) can be used to further reduce the required Ethernet ring restoration times.

Regardless of their individual drawbacks and advantages, it is important to note that both Ethernet and SONET technologies are continuing to evolve and are coming ever closer to meeting the same performance goals. Furthermore, a widely installed base of the SONET is very likely to ensure long and prosperous coexistence of both technologies. Native Ethernet links are most likely to be deployed in brand new installations without significant presence of legacy SONET equipment.

IV. VIRTUAL LAN AND COS PRIMER

Virtual Local Area Networking (VLAN) and Class of Service (CoS) are essential technologies for segregating and prioritizing Ethernet traffic as networks grow in size, complexity, and traffic diversity. This section will explain what VLANs and CoS are, how they work, and why they are so important.

A VLAN is a completely separate Ethernet network that shares cabling and equipment infrastructure with other VLANs. Each VLAN on a network has its own broadcast domain, meaning that Ethernet frames from one VLAN will not be transmitted onto another VLAN. This restricted broadcast domain provides a powerful security mechanism; users and IEDs on one VLAN cannot communicate with other VLANs unless a router is deployed to route between the VLANs. The router then becomes a central location for administering security policies for inter-VLAN communications.

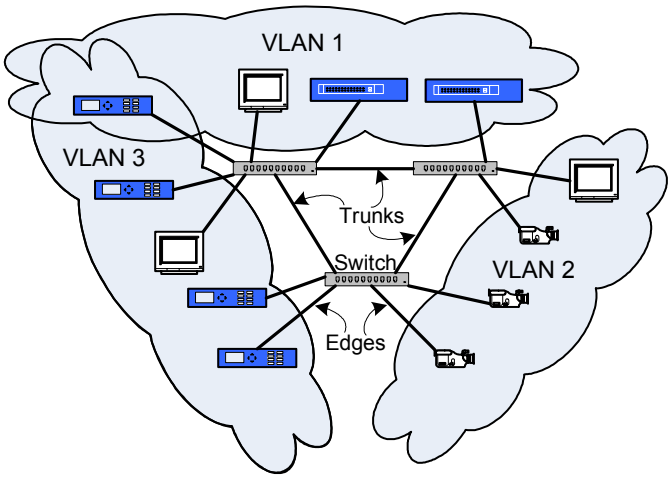

Fig. 3. VLAN segregated network

Managed Ethernet switches are required to implement a VLAN-enabled network; the managed switch ensures that traffic from one VLAN does not cross the boundary to another VLAN. User configuration of the managed switch is required to specify which VLANs exist, how they are assigned to the physical Ethernet ports, and whether the traffic is tagged or untagged.

The IEEE 802.1Q standard defines a 4-byte extension to the Ethernet frame header that allows traffic from one VLAN to be distinguished from another VLAN as shown in Fig. 3. The VLAN Identifier (VID) is a 12-bit field that allows 4094 different VLANs to exist on a single LAN. Frames in a VLAN-enabled network will have both tagged and untagged traffic present. Trunk ports that interconnect switches have all frames tagged. Edge ports that connect IEDs and PCs to the network have untagged frames. The exceptions to the latter are Generic Object-Oriented Substation Event (GOOSE) and Sampled Measured Value (SMV) frames issued by IEC 61850 IEDs.

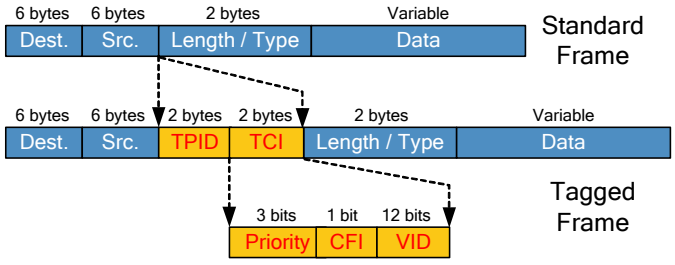

Fig. 4. Tagged Ethernet frame structure

The managed switch must be configured to classify untagged ingress traffic, assign it to the desired VLAN, and decide whether it has a tag added upon egress. Ingress traffic is that which is incoming to the switch whereas egress traffic is that which is outgoing from the switch. The most common scheme is referred to as Port-Based VLANs. Each port on the switch is configured to have a native PVID; any untagged ingress frames are assigned to the VID of the port. Thus the edge ports typically belong to only a single VLAN as defined by the PVID for the port. However, since GOOSE frames are already tagged, an IED may belong to more than one VLAN; the nonGOOSE or "normal" traffic can be assigned to a completely different VLAN from the GOOSE traffic. This is an important facility that will be exploited later in this paper in the application example.

The managed switch also can be configured to assign the 3-bit priority field to untagged ingress traffic. This yields eight different Classes of Service (CoS) with seven being the highest priority and zero being the lowest. The CoS priority causes ingress frames to be placed in different queues within the switch. The higher priority queues get emptied first, therefore reducing the travel time through the switch for more important traffic. When the network is lightly loaded, CoS has little impact; however, as the traffic load increases, the probability increases for frames to be queued. When frames are queued, the latency increases for that frame to reach its final destination. CoS serves to reduce latency which is crucial for time and jitter sensitive traffic like VOIP and GOOSE-based real-time control. It is important to note that CoS is a best effort service and cannot guarantee delivery times or bandwidth availability. However, by separating the real-time traffic into a high-priority VLAN queue, network loading becomes calculable. It can then be determined at design time.

The ability to classify frames based on other information such as the application protocol, particular commands, or subfields within a protocol would be very useful. For example, it would be sensible to classify the command to trip a breaker with a high priority and classify the oscillography packets with low priority. Unfortunately, Ethernet switches don't have the capability for such deep packet inspection; the IEDs themselves would be required to tag frames appropriately. In the world of substation automation, only one proprietary protocol solves this problem and IEC 61850 is the only standardized effort that has begun to address this issue.

One could argue that the use of VLANs and CoS are overkill within the substation LAN environment. The additional burden of learning and configuring managed switches may not be justified by the subtle improvements in network performance. However, as more advanced, intersubstation protection schemes that utilize the incredible flexibility and power of the Ethernet network begin to emerge, VLAN and CoS become essential to ensure that traffic arrives in a timely and secure manner. Additionally, those who would argue that it is overkill are thinking only of the predicted network traffic. The fact that the network is Ethernet, and that a plethora of tools (cameras and other devices) and applications can be added after installation means that the future traffic patterns are not predictable and care needs to be taken to reduce the risk of delay of critical messages.

V. Network Routing and Security

Ethernet on its own provides little security from malicious intruders from a larger corporate network. A cyber-security appliance with IP routing, firewall, VPN, and IDS is needed to create an "Electronic Security Perimeter" around the critical cyber assets of the substation as required by NERC CIP-005-1.

The NERC Cyber Security Goal is to:

> Ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems.

There are many aspects of security defined by NERC as shown in Table IV.

TABLE IV
NERC CYBER SECURITY STANDARDS

NERC Std #	Topic
CIP-002-1	Critical Cyber Assets
CIP-003-1	Security Management Controls
CIP-004-1	Personnel and Training
CIP-005-1	Electronic Security
CIP-006-1	Physical Security
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans

Critical Asset: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

Cyber Security Incident: Any malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the electronic or Physical Security Perimeter of a Critical Cyber Asset, or,
- Disrupts or was an attempt to disrupt the operation of a Critical Cyber Asset.

Electronic Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected, and for which access is controlled.

Connecting the utility corporate network to the substation has its obvious business advantages: access to real-time data; ability to troubleshoot and remedy problems remotely; integration of physical security measures like access control and video surveillance. However, these benefits come at the cost of potentially exposing critical cyber assets to the corporate users at large.

Fifty-eight percent (58%) of companies surveyed by Data-Monitor PLC reported authorized users and employees as the source of a security breach. Now add the threat from a large network and its potential for loopholes, hidden modems, and backdoor entry points from the public Internet and you have a serious issue. A few of the dangers the substation could be exposed to include spoofing, Denial of Service (DoS), replay attacks, viruses, and worms. The corporate network must be treated as an untrusted network.

Segregating a large, intersubstation, Ethernet network into multiple IP subnets is one approach to meeting the goal of a secure network. The substation boundary is an obvious demarcation point for different IP subnets and may be the only practical choice in many instances because of the reliance on existing utility network infrastructures. Each substation boundary then aligns cleanly with the electronic security perimeter boundary.

However, a large flat Ethernet network spanning substations is not altogether unthinkable. If the intersubstation communication network is private and completely secure, it is an interesting alternative to a more traditional IP segregated network. Through the use of VLANs, such a large flat network could still be made secure from corporate network access with a single demarcation point. The electronic security perimeter would then span all substations. For smaller networks this approach would save capital, commissioning, and long-term maintenance costs. This approach also has the added benefit of supporting GOOSE-based traffic with ease. The application example in Section VI presents a hybrid approach.

Protection against the threats from the untrusted corporate network can be handled with a cyber-security router appliance containing a firewall, VPN access, and IDS. Fortunately, like switches, substation grade routers meeting IEC 61850-3 and IEEE 1613 exist on the market today.

Firewall, VPN, and VLANs, when used in conjunction, provide a means to provide secure access to different cyber assets within the substation from different groups within the utility. For example, VLANs can be used on the substation LAN to separate protection and control IEDs from RTUs and video surveillance equipment. The firewall and or VPN can then restrict access to those VLANs to individuals from the engineering, SCADA, and operations group, respectively.

VI. PUTTING IT ALL TOGETHER: APPLICATION EXAMPLE

Let us look at an IEC 61850-based substation with multiple protective relays that use GOOSE messages for peer-to-peer communications. The substation also has one or more synchrophasor data sources (IEEE PC 37.118), Ethernet-based video cameras, and a substation controller providing SCADA interface functionality (DNP-IP). In addition, let us assume that one of the relays needs to exchange transfer trip information with a distant peer in a remote substation (using GOOSE [4]) and that the synchrophasor message latencies need to be minimized. Security is to be provided by deploying local firewall/router functionality.

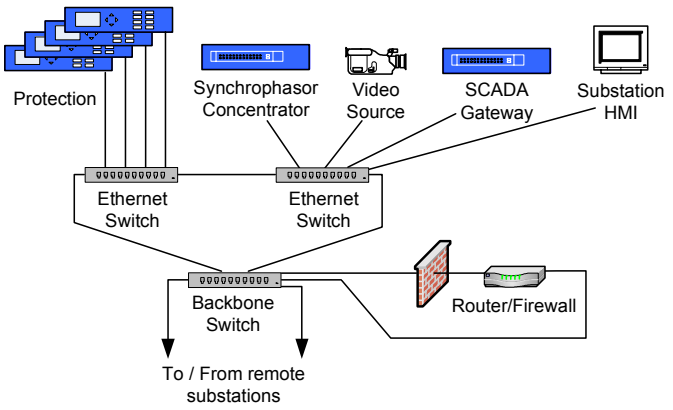

Fig. 5. Substation LAN example

For simplicity, Fig. 5 is shown without communication network redundancy, which will most often be required. Additional information about available redundancy solutions and their reliability characteristics can be found in references [5] and [6].

A. Network Configuration

The substation network configuration phase starts by determining the required number of Virtual LANs and VLAN groups. These application requirements can be summarized as follows:

TABLE V
VLAN NAMES AND NUMBER ASSIGNMENTS

Substation VLANs	
Name	**Number**
Substation LAN Management	10
SCADA/Engineering Access	11
Substation GOOSE Messages	12
External Backbone VLANs	
Name	**Number**
Backbone LAN Management	20
SCADA/Engineering Access	21
Common (Wide Area) VLANs	
Name	**Number**
Intersubstation GOOSE	30
Synchrophasors	31
Video Surveillance	32

The number of VLANs is based on the application requirements. In an ideal world, we would form a clean barrier between the substation and the external world (Ethernet backbone). Connection between the two domains would be established exclusively through a locally installed firewall and a router.

Unfortunately, for this particular example, we have decided to add the following three sources with special communication requirements.

- Intersubstation GOOSE, which cannot tolerate delays, has tag-based VLAN capability, requires high priority, and exists only at Layer 2 (cannot be routed).
- Synchrophasor traffic, which cannot tolerate delays and should be separated from the rest of the network in order to enhance security.
- Ethernet-based video surveillance, which generates large amounts of streaming traffic and could overload the router.

Since these sources cannot be routed, an additional router bypass mechanism is needed. This mechanism must be secure and must be capable of protecting both the devices within the substation and the specialized real-time traffic.

A VLAN mechanism provides an excellent tool for this job. It can easily contain the normal traffic within the substation and can prevent multicast traffic created inside the substation from flooding the rest of the network (GOOSE). It allows us to assign separate priorities to separate types of traffic and permits fine grain configuration of protected traffic data flow outside of the substation. Fig. 6 illustrates the concept of separation between the GOOSE messages within the substation on VLAN 12 and the intersubstation GOOSE assigned to VLAN 30. Similar situations occur for the remaining VLANs that are omitted in order to simplify the drawing.

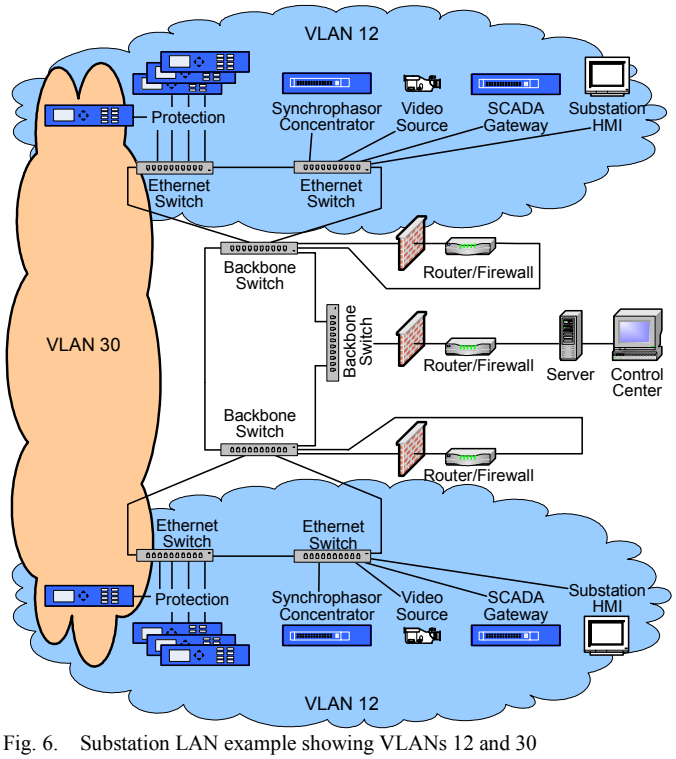

Fig. 6. Substation LAN example showing VLANs 12 and 30

As explained in Section VI, VLAN configuration is simple; but in our case, will require a few additional parameters. Individual parameters that can be assigned for each of the switch ports are listed below:

- VLAN port type (Edge or Trunk)
- Native VLAN number (1–1000)
- Native VLAN format (Untagged, Tagged)

IEC 61850-capable relays will, in general, be transmitting both tagged (GOOSE) and untagged frames (everything else). It will therefore be necessary to configure all switch ports connected to these relays to Trunk mode, with the Native VLAN format set to Tagged. The Native VLAN number makes it possible to take the untagged messages (everything other than GOOSE) and assign them to a particular VLAN group.

In our example, the native VLAN mechanism is used to safely transmit the SCADA/engineering access traffic to the firewall/router. It is important to note that the GOOSE message VLAN and priority assignments are set by the relays (as configured through the IEC 61850 configuration software). In our example, this means that the distance relays on the left side of the picture need to produce at least two distinctly different GOOSE messages. One message is used for the POTT scheme communication with remote substation (shown on VLAN 30), and the other message is used for communication within the substation (both shown on VLAN 12).

It is easy to see how this simple POTT scheme could, in the future, be extended to a fully functional line differential scheme. The only ingredients still lacking at this time are actual relay hardware and necessary confidence in the communication network reliability.

- Once the Ethernet switch ports have been segregated into different virtual LANs, it is necessary to configure those VLANs by assigning appropriate message priorities (quality of service). VLAN priority options are VLAN priority (0–7).

While there are eight possible priorities, it is important to determine the actual number of priority queues being supported by a particular Ethernet switch. This number is normally between two and four. Actual priority mapping for four queues would be as shown in Table VI.

TABLE VI
PRIORITY QUEUE MAPPING EXAMPLE (4 QUEUES)

Queue	VLAN Priority
Highest	6, 7
Medium High	4, 5
Medium Low	2, 3
Lowest	0, 1

The Ethernet switch configuration parameters proposed for our example substation are listed in Table VII.

TABLE VII
EXAMPLE NETWORK CONFIGURATION SETTINGS

Priority	VLAN Name	VLAN #	Comment
7	Substation LAN Management	10	Port based VLAN
1	SCADA/Engineering Access (substation side)	11	Device dependent
7	Substation GOOSE messages	12	Assigned by the relay
7	Backbone LAN Management	20	Port based VLAN
1	SCADA / Engineering Access (backbone side of the router)	21	Port based VLAN
7	Intersubstation GOOSE	30	Assigned by the relay
5	Synchrophasors	31	Port based VLAN
3	Video surveillance	32	Port based VLAN

As will be noticed by many readers, proposed priorities are biased in favor of protection and synchrophasor data delivery. Actually priorities may have to be modified to match specific project/system requirements.

The total number of configurable switch parameters is relatively large, offering a significant amount of flexibility. Although it may appear complicated at first, Ethernet network planning and configuration are well-understood tasks, performed daily by the Information Technology (IT) specialists. The overall process is very similar to that used by power system engineers to configure protective relay systems. It should come as no surprise that once it is to be used for protection related traffic, the Ethernet network needs to be designed and configured as an integral part of the power system engineering design process.

VII. Conclusion

Network-based communication technologies are slowly extending their reach into power system substations, bringing with them new opportunities and new challenges for people designing, operating, and maintaining the power system.

The number of substation devices capable of supporting Ethernet-based communication technologies (IEC 61850, DNP-IP, IEC 60870-5-104, PC 37.118) is rapidly increasing, creating a wide gap between current practice and modern device capabilities. This gap becomes especially visible when Ethernet networks are intended to enhance mission-critical systems, such as power system protection, or to deploy new technologies such as synchrophasor-based power system monitoring and control.

This paper looks at LAN technologies necessary to deploy a viable substation LAN and the technologies for connecting multiple substations into a larger, utility-owned communication network. It provides a short comparison between the two major intersubstation network contenders: switch-based Ethernet and SONET.

The paper explains some of the key technologies behind substation Ethernet and gives a short application example demonstrating the use of Ethernet switch-based technology, IEC 61850 GOOSE messages, Virtual LAN planning, and message priority management.

The primary goal of this paper, however, is to help establish a dialogue between power system engineers and the Information Technology group. While it may not be necessary for power engineers to get involved in every step of the communications network design process, a clear understanding of the principles and the ability to communicate power system requirements to the IT and communication system professionals is becoming essential for success of the new Ethernet network-based technology.

VIII. References

[1] RuggedCom, Inc, "Fiber optic networks revealed," 2003, [Online], Available at: http://www.ruggedcom.com/pdfs/fiber_guide/RuggedCom Fiber Guide 1.0.pdf.

[2] K. Clark, K. Hamilton, "Cisco LAN Switching," Cisco Systems, 2004. www.ciscopress.com.

[3] Cisco Systems, "Understanding Carrier Grade Ethernet," 2003, [Online], Available at: http://www.cisco.com/warp/public/cc/techno/lnty/etty/ggetty/prodlit/intgn_wp.pdf.

[4] V. Skendzic, A. Guzman, "Enhancing power system automation through the use of Real-Time Ethernet," Presented at DistribuTECH, San Diego, February, 2005, [Online], Available at: http://www.selinc.com/techpprs/6188_EnhancingPower_20041114.pdf.

[5] M. Galea, M. Pozuoli, "Redundancy in substation LANs with the rapid spanning tree protocol," RuggedCom Inc, [Online], Available at: http://www.ruggedcom.com/pdfs/white papers/Rapid_Spanning_Tree_in_the_Substation.pdf.

[6] G.W. Scheer, D. Dolezilek, "Comparing the reliability of Ethernet network topologies in substation control and monitoring networks," Presented at Western Power Delivery Automation Conference, Spokane, Washington, April, 2000, [Online], Available at: http://www.selinc.com/techpprs/6103.pdf.

IX. Biographies

Veselin Skendzic is a Principal Research Engineer at Schweitzer Engineering Laboratories in Pullman, Washington. Veselin earned his BSEE from FESB, University of Split, Croatia; his M.Sc. from ETF, Zagreb, Croatia; and his Ph.D. from Texas A&M University. Veselin has over 20 years of experience in electronic circuit design, has lectured at FESB, and spent over 16 years working on power system protection related problems. Veselin is a senior member of IEEE, has authored multiple technical papers, has six patents, and has contributed to four IEEE standards. Veselin is an active member of the IEEE Power System Relaying Committee.

Roger Moore is a co-founder and Engineering Vice President of RuggedCom, Inc., a leading manufacturer of industrially hardened communications technology for mission-critical applications in harsh environments. Prior to founding RuggedCom, Roger was a project manager for General Electric's Power Management division where he developed advanced protective relaying systems and substation automation technology. Roger graduated from the University of Toronto in 1990 with a Bachelor of Applied Science degree majoring in computer science and physics. He holds patents related to advances in communications and protective relaying technology. He is also an active member of the IEEE and is involved in developing the new IEEE 1588 standard for precision time synchronization of devices via a communications network.