Application of Ethernet Networking Devices Used for Protection and Control Applications in Electric Power Substations

Report of Working Group P6 of the Power System Communications and Cybersecurity Committee of the Power and Energy Society of IEEE

September 12, 2017

IEEE PES Power System Communications and Cybersecurity Committee (PSCCC) Working Group P6, *Configuring Ethernet Communications Equipment for Substation Protection and Control Applications*, has existed during the course of report development as Working Group H12 of the IEEE PES Power System Relaying Committee (PSRC). The WG designation changed as a result of a recent IEEE PES Technical Committee reorganization.

The membership of H12 and P6 at time of approval voting is as follows:

Eric A. Udren, Chair

Benton Vandiver, Vice Chair

Jay Anderson	**Galina Antonova**	**Alex Apostolov**
Philip Beaumont	**Robert Beresh**	**Christoph Brunner**
Fernando Calero	**Christopher Chelmecki**	**Thomas Dahlin**
Bill Dickerson	**Michael Dood**	**Herbert Falk**
Didier Giarratano	**Roman Graf**	**Christopher Huntley**
Anthony Johnson	**Marc LaCroix**	**Deepak Maragal**
Aaron Martin	**Roger E. Ray**	**Veselin Skendzic**
Charles Sufana	**John T. Tengdin**	

Application of Ethernet Networking Devices Used for Protection and Control Applications in Electric Power Substations

Table of Contents

Figures and Tables

Application of Ethernet Networking Devices Used for Protection and Control Applications in Electric Power Substations

1. Introduction

In electric utility and industrial substation applications, Ethernet local area networks (LANs) and wide area networks (WANs) are now widely used as data communications backbones for SCADA and informational (non-operational) data gathering. More recently, these networks also carry specialized messaging formats to replace wiring for high-speed protection and control (response in milliseconds). Protective relaying engineers must deal with the application of these networks.

Ethernet local area network (LAN) based protection and control schemes using IEC 61850 services, including GOOSE messaging for high speed status and control points, and SV (Sampled Values) service for streaming process values, all depend on the proper setting and operation of Ethernet switches and routers. Correct Ethernet configuration is required for correct operation of high-speed primary or backup relaying, breaker lockout after a backup trip, or other protective functions. The same is true for SCADA data and informational data gathering.

Relay engineers are now applying these data communications devices in new scheme designs. This report describes engineering considerations for protection and control:

- The basic purposes, functionality, and application guidelines for these Ethernet communications devices in substation LANs and utility WANs.
- Architecture and configuration of connections of the LAN for security, dependability, and maintainability.
- Settings or programmed configuration of switches and routers to control traffic flow to meet the required security and dependability – this has much in common with setting relays, and requires the same organizational control processes.

Ethernet switches and routers installed on relay panels in hostile substation environments are descended from equipment widely used in IT networks. Thus, the IT departments at some utilities participate in the selection, application, management, and setting of switches and routers. There may be a lack of mutual understanding between the protection/control designers and the IT experts about the role of these devices, performance and reliability requirements, maintenance procedures, how the Ethernet devices are to be managed, and by whom. The report aims to help both P&C and IT engineers gain a common understanding of how to design substation Ethernet networking infrastructure.

2. Ethernet for protection and control

The prime example of high speed relaying on Ethernet is the use of IEC 61850-8-1 [10] GOOSE messages in a substation Ethernet LAN environment to convey trip command status and supervising signals from one relay to another using status bit communications, without

conventional wiring dedicated to individual points. Analog measurement values can also be transmitted by GOOSE. More recently, IEC Technical Report 61850-90-1 [11] describes methods of tunneling or transferring GOOSE messages between substations for applications like transfer tripping, pilot or unit teleprotection of transmission lines, and wide-area special protection schemes. A new IEC Technical Report 61850-90-5 [14] specifies a transport method for multicast Layer 3 GOOSE (explained later) over wide area networks by utilizing services that are supported by commercially available Ethernet routers; and with encryption and authentication specifications for cyber security in a wide-area network environment.

The Ethernet networks in substations comprise wired connections or, more commonly, optical links connecting relays and other IEDs in a LAN using *Ethernet switches* whose nature is explored in the present report. The Ethernet switch is in fact an elaborate message-processing computer with a list of settings that impacts how messages are sent from one relay to another or from relays to other substation information hosting devices. As such, Ethernet switches and LANs become the new replacements for auxiliary relays in protection schemes. The network design and the configuration of these messaging computers impact the speed and reliability of relaying.

For the non-critical-application data exchanges with other substations, control centers, or the utility enterprise, these substation LANs are usually connected to the utility's control wide area network (WAN) or business enterprise WAN via Ethernet *routers.* Routers are sophisticated message formatting and forwarding computers operating on OSI Layer 3 as described in Sections 3.1 and 8. As inter-substation Ethernet messaging is increasingly used for control and protection, the routers and the WAN also become protective relaying auxiliary devices and channels.

For data exchanges with other substations supporting critical applications like relaying, as described in Sections 8 and 11, the typical choice today is a TDM technology such as SONET or SDH. However, there are practical installations in which SONET or SDH paths emulate Ethernet connections to extend the LAN as Section 11 describes. All-Ethernet wide-area packet communications using Layer 3 is, however, a recognized rising application supported by the direction of IT product development towards MPLS Ethernet as Section 8 describes..

Within the switches and routers are functions and services for managing and directing message traffic. The complexity of settings and application for these functions can equal that of the protective relays themselves. These devices also include communications services to support local or remote network management and monitoring. Sprinkled among the switches and routers may be cyber security functions that restrict access including firewalls, encryption functions, and virtual private network (VPN) secure interface access functions.

The major concern which has held back the use of Ethernet networks, particularly WANs, for time-critical applications is the inherent lack of determinism through these networks, Ethernet being a best-effort transport technology. The generally uncontrolled latency results from the bursting nature of the Ethernet packets, causing indeterminate queuing latencies (see Section 11.6 for examples). However, with proper engineering of the Ethernet network capacity itself, its worst-case traffic loading, and the prioritization scheme for packets carrying various critical

or non-critical traffic types, the latency and latency variation (jitter) can be contained within boundaries that are suitable for high-speed protective relaying and power system control applications. Each of these topics is addressed in this report.

3. Overview of Ethernet message frames

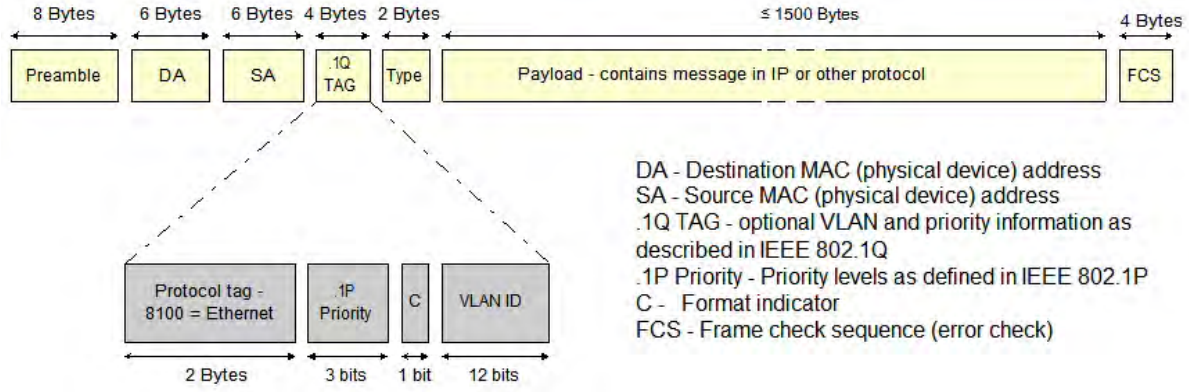

Figure 1- Ethernet Message Packet Structure

Figure 1 shows a typical Ethernet message packet passing around a LAN or WAN. The parts of the message are:

- Preamble – sequence showing the start of the message for framing the rest.
- DA - the destination address - a media access controller address (MAC address), a unique number specifically assigned to the physical electronic hardware device receiving the message. DA may also be a multicast or broadcast address.
- SA - the source or sending device address, also a MAC address or unique physical device identifier specifically assigned to the physical electronic hardware device sending the message.
- Type – identifier for the protocol used for the bytes following. See further below.
- Payload – the desired data to be transferred. This includes higher protocol layers of level 3 and above. If the packet carries the Internet Protocol (IP) network layer 3 there is an IP address also included in the payload that is used by routers to route the message. The switch deals mainly with layers 1 and 2, and does not pay attention to IP addresses for its message passing work. On the other hand some switches do allow the user to provide a mapping table to allow an IP messages' layer 3 6-bit "DiffServ" field to over-ride its layer-2 3-bit priority field.
- FCS – Frame check sequence - an error check calculated at the sending end from the frame bit sequence, and compared at the receiving end with a duplicate calculation there to detect if bits have been corrupted in transmission.

3.1 The OSI 7-Layer Model

Data transmitted in an Ethernet network is organized following the OSI (Open System Interconnection) 7-Layer Model. Table 1 describes the functions of the 7 layers:

Layer	Name	Function	Typical Usage (Device or Software)	Examples
7	Application	Meaning of the data (utility user specifics)	Application Programs	HTTP, FTP, NTP, PTP, SNMP, MMS
6	Presentation	Building blocks of data and encryption for security	O/S Ethernet Stack	JPEG, ASCII, HTML, Encryption
5	Session	Opening and closing specific communications paths	O/S Ethernet Stack	RPC, NETBIOS
4	Transport	Error checking	O/S Ethernet Stack	TCP, UDP
3	Network	Determining the data paths within the network	Router, L3 Switch	IP
2	Data Link	Data transmission, source & destination, checksum	Switch	Ethernet, ATM, PPP, Token Ring
1	Physical	Signal levels, connections, wires, fiber, wireless	Media Access Controller, Repeater	10Base-T, 100Base-FX

Table 3-1 – Implementation of OSI 7-Layer Communications Stack

More detailed layer descriptions appear in the Annex.

Building message packets using these standardized layers allows the use of the latest communications technology as it changes rapidly (physical and data link layers 1 and 2), while specialized applications (upper layers) built at great expense and integrated for specific uses can be retained and reused for a long time. Obsolete hardware can be replaced and performance can improve without discarding the most complex specialized portions of a communications system design. Communications component layers can be shared or adapted from system to system over time due to the standardized interfaces among the layers.

3.2 Example of how IEC 61850 services are mapped

The Figure 2 example shows how key services of the IEC 61850 protocol and modeling standard are interfaced over the different layers. This diagram is extracted from IEC 61850 specifications. The communications are divided into two categories. The first (left yellow down arrow) category shows the high-speed, real-time publisher-subscriber communications including GOOSE messaging service and the Sampled Values (SV) service. The GOOSE messages are used to exchange real time binary status including control commands, or to create fast automation. Because this service is directly mapped from the application layer to the Ethernet layer shown as

the payload in Figure 1, the high-speed application programs manage the repetition of the GOOSE packets (used to reduce risk of loss of information). The sampled value messages are used to transfer signal values and states from a switchyard merging unit to a relay. The use of fiber from the switchyard to the control house networking connections for protective relaying information avoids the loss of information during electrical transients. The use by GOOSE or SV services of direct mapping from the application into the Ethernet packet eliminates the time delays associated with the use of the standard implementations of the bypassed layers. These added layers are not generally suitable for real-time use in applications with speed demands like those of fault protection.

The second (right arrow) category shows the non-real-time client-server communications services, where we can find the IEC 61850 metering and status reports for SCADA and local HMI, operator control commands, logs, etc. These types of messages use TCP/IP and other OSI layers to improve the transmission of the information – they use the TCP/IP layer mechanism to resend automatically if receipt of the message is not acknowledged.

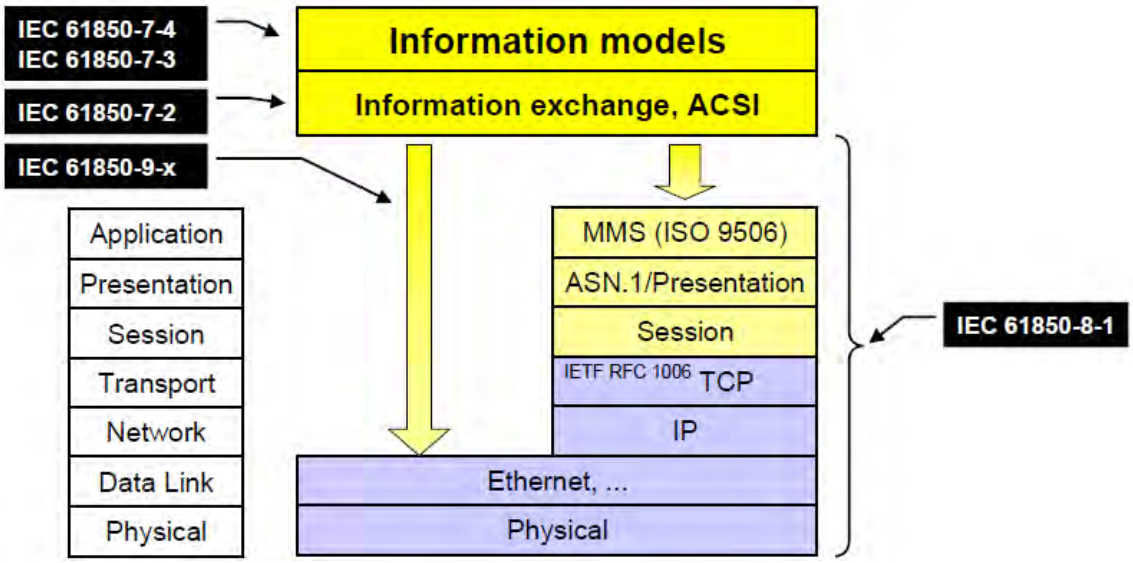

Figure 2 - OSI 7-layer model application for IEC 61850 services

3.3 TCP versus UDP

Transmission Control Protocol (TCP) is a core protocol for Layer 4 that complements the Internet Protocol (IP). TCP includes a mechanism by which the receiver can request retransmission of information that was corrupted or lost. User Datagram Protocol (UDP) is an alternative core protocol which simply uses best effort and does not inherently retransmit corrupted packets. The receiver can detect corrupted/lost packets but does not have the ability to ask for a resend via the protocol itself. The choice depends on whether the application requires that each unit of information sent is received, versus applications that stream constantly-changing information and are designed to survive a data loss and carry on when newer information is received later.

UDP may be used for measurement or status information to be sent using IP when latency is critical to performance.

Sometimes the user has a choice of using either TCP or UDP, a common example being for Terminal Servers (a common moniker for devices transporting RS232/422/485 asynchronous data over Ethernet communication paths). In synchrophasor transmission applications across a utility wide area Ethernet network (WAN), the user may choose UDP or TCP depending on whether the focus is control, or on error-free archiving of measurements.

UDP is the only choice for multicast traffic, but for point-to-point links either can be used. A user may at first think that the "guaranteed" (not really) nature of TCP makes it preferable, but the downside is that its accompanying acknowledgement and re-transmission of extra messages can result in a significant increase in traffic and degradation of the service (and collateral damage to other traffic) in a bandlimited network. In particular, Terminal Server users have often found that UDP provides better performance. Do not use TCP when the application handles the requests for repetition of missed data through a separate mechanism – the TCP then becomes redundant and may hurt performance.

4. Overview of Ethernet network configuration

An Ethernet local-area network (LAN) is a limited domain of connected devices that directly address and exchange message packets using the Ethernet frames' layer-2 (Media Access Control or MAC) addresses. There is no inherent limit to the physical range of these layer-2 LANs. For interfacing to a layer-3 wide-area network (WAN), Ethernet messages are processed with elaborate schemes for mapping the layer-2 addresses to the layer-3 (Internet Protocol or IP) addresses, and the readdressed messages can be forwarded in an arbitrarily large interconnection of communicating devices. This address recognition and translation capability is the basis of the Internet, as well as WANs used by business enterprises to interconnect all users while isolating specific information to subgroups of users that need access. LANs in utility substations may be connected directly to some part of the utility control WAN through the address translation computer called an *Ethernet router*, described in Section 8 below.

Figure 3 shows a typical Ethernet networking configuration in a substation, to support explanation of details and features in subsequent sections.

Figure 3 uses the device nomenclature of IEEE C37.2-2008 [2], *IEEE Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations*. This standard includes the familiar device numbers of protective relaying functions, previously referred to as ANSI device numbers, used in protection and control (P&C) system drawings and documentation. Ethernet communications devices have become critical relaying components appearing in system documentation for today's P&C schemes. The 2008 revision of C37.2 added Device Number 16, applied to data communications devices in substation protection and control (P&C) schemes, including serial or Ethernet communications network devices carrying protective relaying and control traffic. Standard C37.2-2008 includes a scheme of added letters that identify the particular type of data communications function that the box performs:

- C – Security processing function (VPN, encryption, etc.)
- E – Ethernet device
- F – Firewall or message filter function
- H – Hub (obsolescent)
- M – Network managed function (e.g., configured via SNMP)
- R – Router
- S – Switch (Examples: Port switch on a dial up connection is 16TS, and an Ethernet switch is 16ES)
- T – Telephone component (Example: Auto-answer modem)

Figure 3 shows an example of how a group of relays might be integrated with an Ethernet LAN. Additional benefit of using Ethernet is achieved when the network connection from the relays extends outside the substation to the utility enterprise shown as a wide-area network (WAN). Many utilities have a separate WAN for critical system control as opposed to enterprise business functions, and a firewall interface at a remote server location allows data to pass between the control WAN and the enterprise WAN.

This figure also shows that for better dependability, each of the protective relay and high-speed control connections in the substation could comprise a *pair* of surge and noise-immune optical fibers for conveying Ethernet message packets in each direction.

Using nomenclature taken from IEEE C37.2-2008, the Ethernet communications components in Figure 3 are:

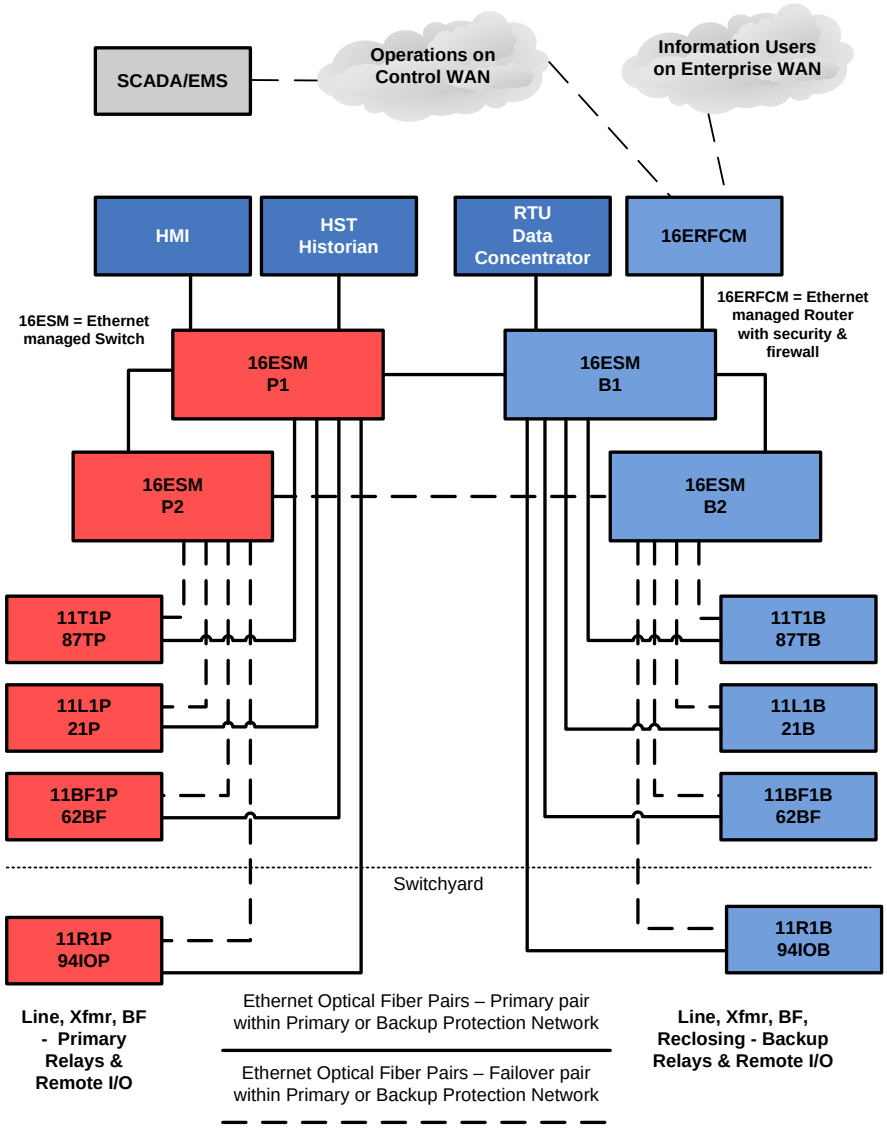

Figure 3 - Substation Ethernet LAN Connects to Utility WAN

16ESM – Ethernet Managed Switch. Each of the relay Ethernet network ports connects to a port on the Ethernet switch, described in more detail in Section 7 below. The term "managed" refers to the fact that the switch operation itself can be monitored and controlled over the same network, and this is typically done from a remote location using the Simple Network Management Protocol (SNMP) familiar to IT departments and software tools for network management. By contrast, an unmanaged switch has fixed operating parameters and modes, or is configurable only at the switch itself, and may not report performance or failure information to IT management systems tied to the network.

16ERFCM – Ethernet Router, managed, with firewall and VPN for cyber secured communications to the utility WAN. Routers are also described in Section 8 below.

RTU – the substation-level central information processor or data concentrator, performing the functions of a SCADA remote terminal unit. This processor polls all the relays and other IEDs via the Ethernet LAN for metered values, status, information records, and all other available data. It translates protocols as needed, and responds to control center polls and commands. It stores information in data bases that may be accessed later. Relay engineers, maintenance personnel, and managers can retrieve this data via the control WAN, tied via the enterprise WAN interface to their computers. For a secure and backed up archive, the utility can upload the data and save it on a protected and backed up server in a remote office location. A maintenance person on the road can dial into the utility remote secure server, rather than directly accessing the substation.

HST - A separate PC runs a substation historian program and other fault and disturbance recording programs. The historian continuously gathers states and values from the data concentrator and/or directly from relays and IEDs. New designs may include a phasor data concentrator (PDC) function that gathers synchrophasors from relays over the Ethernet network for disturbance recording, and to resample phasor streams at a lower rate to send to a phasor client system at the control center over the WAN. Historian records can be used for asset condition monitoring or post-mortem events analysis. The substation historian communicates over the same LAN to the control WAN, and on to a remote central enterprise historian, which gathers the records from all the substations and creates a single managed data base to serve utility asset managers and operational analysts.

WAN – The substation LAN connects to an array of control and separate enterprise wide area networks (WANs) and work locations. The communications connection could be via utility-owned T1 or SONET (optical fiber ring data network), utility owned microwave system, or via a common carrier data communications service. Two popular forms of the latter are Frame Relay protocol, and Ethernet Multi-Protocol Label Switching (MPLS) network, connected to the substation via an optical fiber or twisted metallic pair from a nearby service center of the communications provider. Note that despite the telecommunications world abandoning SONET/SDH for WANs (moving to Ethernet transport), most protective relaying users prefer widely-used and stable TDM (SONET or SDH) technologies for the protection applications requiring deterministic low-latency message transport. Another benefit of TDM communications paths is that they can be used to support Ethernet connections, using separate TDM channels for separate Ethernet applications isolates critical Ethernet traffic from unknown and untrusted Ethernet traffic.

Ethernet WANs based on MPLS or other technologies are being developed for implementation of predictable low latency and protected bandwidth that approaches that offered by SONET/SDH today. Movement of the IT world away from TDM and towards Ethernet WAN technologies will exert pressure on mission-critical low latency

applications to adapt, but performance of the WAN technologies must be demonstrated.

4.1 Redundant and failure resistant design of substation networks

Since GOOSE messages or other traffic are used for critical functions like tripping of circuit breakers or initiation of breaker failure timing, the installation may need to be designed so that no single hardware failure anywhere in the system can disable a critical protective function. To achieve this, the substation network may be configured with two separated LANs for use by System A and System B redundant relaying configurations. Having redundant systems also enables maintenance on protection systems for live substations without losing protection speed or taking primary equipment out of service.

4.2 Connection of System A and System B protection networks

In Figure 3 each of System A and System B relay groups for the substation has its own dedicated portion of the LAN, with its own pair of switches. The purpose of having multiple switches and relay connections within System A or within System B is explained in the next subsection.

For all critical protection, System A relays can exchange messages without any reliance on the System B side of the network. There is no single point of failure for any protection function, and any component in System A can be maintained while the corresponding System B function provides protection.

However, station level functions like the RTU/data concentrator, historian, and enterprise WAN connection need to access data from both System A and System B protection schemes. Therefore, Figure 3 shows a pair of connections between the switches of System A and those of System B. A station-level function can thus connect to either side of the network and access any device or data.

Optical fiber Ethernet connections between System A and System B through the switches are viewed as connections whose failure or malfunction cannot disable any protection function within System A or System B, and thus are not considered to violate the physical isolation of those systems. Assuming this entire substation network configuration exists within a cyber-secure physical boundary of a control house, the only possible concern is that some malfunctioning device on one side is filling the network with meaningless traffic that clogs the flow of important messages on both sides.

Unlikely as it is, this risk can be managed by configuration of the switches using principles and tools described below. Among the available tools are virtual separation of the networks using VLAN configuration in the switches, and limitation of the number of messages per second that can pass between System A and System B using limiting settings in the switches.

4.3 Primary and failover backup fiber connections of relays

Figure 3 shows two optical transceiver and two optical fiber pairs from each relay – solid (normal) and dotted (failover) paths. This provides additional redundancy within System A or

within System B – even if an optical transceiver, interface, fiber, or connected switch fails, the network continues to function normally within each redundant system. Thus, this network is robust against multiple failures of Ethernet components, even though these components are reliable.

The operation of the failover scheme is as follows:

Normally, each relay communicates through its primary fiber pair to its primary switch, such as 16ESM-P1 in Figure 3.

The backup fiber pair connects to a separate switch 16ESM-P2 as shown, which in turn ties back to 16ESM-P1. It has its own backup connection to System B, explained later.

If the relay detects a failure of its incoming data traffic flow or message carrier signal, it fails *all* of its Ethernet communications over to the backup fibers. The failure could have been at the relay port, in a fiber, or in the primary switch. All of these components have their function taken over by the failover components, including the second Ethernet switch. Note that there remains some message path from each of the relays to every station level device and to relays in the redundant protection network.

In order for a relay to detect a failure of its outgoing message transceiver or fiber path, it must either monitor the Remote Defect Indication (RDI) or Far End Fault Indication (FEFI) signal from the connected switch. Alternatively, it can be connected to a switch that has the ability to mute its output when it loses its received signal from the IED (if the particular switch has this capability included – check with the manufacturer); the switch shutdown of outgoing data on the port will be detected by the relay as an incoming data failure, and the relay will then switch all communications to the failover paths.

In this way, no single failure of a networking or communications component in System A by itself will impact communications within System A, except for a failover time of tens or hundreds of milliseconds.

The existence of this transparent failover mechanism must be considered whenever technicians are performing maintenance on the network or the relays and switches connected to it – if a complete shutdown is required, make sure it is really fully achieved and not circumvented by an automatic recovery mechanism like those described.

A more recent standard for using dual Ethernet ports on an IED to maintain functioning in the case of network or port failures are the IEC PRP and HSR protocols described in Section 4.6.

4.4 Switched mode port in IED

Some manufacturers have introduced a switched mode in which a small three port unmanaged switch is incorporated inside the IED or relay, connecting the communications of the device to the two physical external network connections as shown in Figure 4. The unmanaged switch is incorporated in the electronics of the device and can be made transparent to the user.

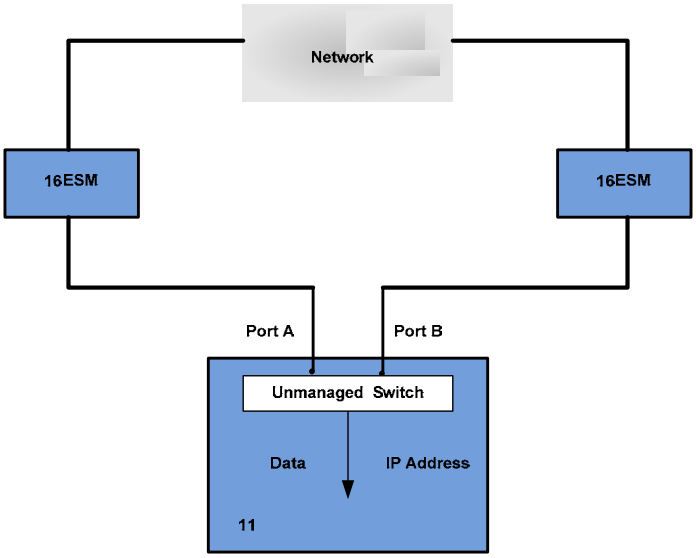

Figure 4 – IED with switched ports

In this scheme, both ports are connected to the network at all times. One is deactivated by the switch service called Rapid Spanning Tree Protocol (RSTP) explained below and is standing by, with occasional test messages as the only traffic on that extra path. However, if the main port or path fails, RSTP will cause communications to transfer to the working alternate path. RSTP requires some time to detect the failure and transfer (e.g. 50 ms) – ask the vendor what the failover time actually is, and consider its impact for relaying situations.

Note here that there are several ways of communicating through two ports on one relay or IED – this is just one of them. The example network of Figure 3 included dual redundant fibers, of which the second is a hot standby, and failure of the primary is detected by loss of the carrier light signal. Section 4.6 below gives a brief overview of the Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) network designs, each of which requires two ports on a relay or IED, and each of which requires a specialized electronic and communications implementation inside each IED on the network.

4.5 Rapid Spanning Tree Protocol (RSTP)

RSTP is a network service built into Ethernet switches, according to IEEE networking standard 802.1D-2004. Its purpose is to detect paths for loop flow of message packets in an operating network that has multiple redundant paths, to open those loops in a prescribed way, to monitor the operating integrity of the primary path in use, and to cause the network to fail over to a redundant path whose function was disabled. This is all done without ever creating a loop around which a message packet might circulate forever.

Consider the loop comprising the four Ethernet switches 16ESM-P1, P2, B1, and B2 in Figure 3. Without RSTP, the switch normally just forwards all input messages to all outputs. Thus, any message injected into any of these switches would exit in both directions on the loop and would circulate forever. The traffic in the loop would rapidly build to a saturation of repeated packets.

The RSTP service sends surveying messages out on the network and detects loops. It will open the loop by disabling some redundant path – for example, the dotted path between 16ESM-P2 and 16ESM-B2 in Figure 3. The designer can set or configure the switches so that they normally disable a chosen link like the one shown as dotted in Figure 3 when everything is working as it should. The only working connection between System A and System B is then the solid path from 16ESM-P1 to 16ESM-P2.

The RSTP service in the switches then periodically sends out test messages in the background, so that the switches always know what alternative paths are available in case of a failure, even if the network is modified by personnel on the fly.

If any path suddenly fails, the switch quickly detects the failure. It has maintained its background information on available alternate paths, and switches over to such an alternate path. Switches made for substation use can execute such a change of path in 5 to 50 ms. The switch produces an alarm for maintenance attention. Since System A and System B are not both impacted by any such failure, this is an acceptable and transparent event. Users should ask switch vendors to explain RSTP failover times for their products in applications where failover time is important. Users should also request switch vendor advice on network configurations and switch settings to optimize RSTP performance.

Interoperability tests conducted in 2011 by the UCA International Users' Group in support of IEC 61850 applications identified some compatibility issues among implementations of RSTP in certain Ethernet switch products for high-speed failover operation. Users should ask vendors about their experience in substation applications and, if vendors' products are mixed, about confirmation or testing of interoperability. Alternatively, configure a lab test with protection-like traffic to confirm that failover delay is compatible with protective relaying times in the worst combination of fault and network failure contingencies.

4.6 Multiport relays with bumpless network redundancy – PRP and HSR

RSTP provides, in case of link or bridge failure, recovery times that are acceptable for many applications at the station bus level, provided that the RTSP implementation (topology, configuration parameters) be done based on the calculation of the worst case recovery time. However, that recovery time is a 5 to 50 ms bump in network operation. Moreover, it does not handle link failures of devices connected on edge ports (without loop connection or failover capability). There may be circumstances where such a bump presents an operating problem. An example could be transmission of IEC 61850-9-2[26] sampled values (e.g. CT and VT measurements) in a system where isolated fully redundant System A and System B devices have not been provided. Network redundancy can be achieved by having devices attached to two separate physical networks using redundancy protocols based on the duplication of the LAN and/or the duplication of the transmitted information. Such protocols, like the Parallel Redundancy Protocol (PRP) and High availability Seamless Redundancy (HSR) ring are specified in IEC 62439-3 [16] and in IEC Technical Report 61850-90-4 [12]. They are briefly described in the following.

4.6.1 Parallel Redundancy Protocol (PRP)

Each PRP-compliant relay or IED has two separate Ethernet ports, each operating at all times and conveying the same information over two redundant networks as shown in Figure 5. The two ports use the same MAC (physical device) address and combine information at the link layer interface. The receiving devices process the first frame received and discards the duplicate. This is done through a link redundancy entity (LRE) or service which acts between the link layer and the Ethernet controllers. Aside from LRE drivers, PRP uses conventional Ethernet hardware.

Both ports of PRP devices operate with the same Internet Protocol (IP) addresses for traffic that uses IP (GOOSE messages do not use IP). Management protocols such as Address Resolution Protocol (ARP) operate correctly.

The two switched LANs in Figure 5 can have any topology, e.g. tree, ring or meshed. PRP more or less doubles the network infrastructure.

Single port devices can be either attached directly to one LAN only, or to both LANs through what is called in IEC 62439-3 a redundancy box (RedBox). Single port devices do not need to be aware of PRP.

The potential user can attach value to PRP based on savings of redundant IEDs or relays when those devices and their installation cost are high compared to the networking infrastructure. Where the cost of the redundant networking is significant, it may be equally effective to use redundant single relays or IEDs without PRP.

Be careful with applications sending large packets over PRP networks - for identifying the duplicate received packets, PRP adds a 4 octet RCT (Redundancy Control Trailer) to each packet, reducing the TCP's largest allowed MTU from 1500 to 1496 octets.

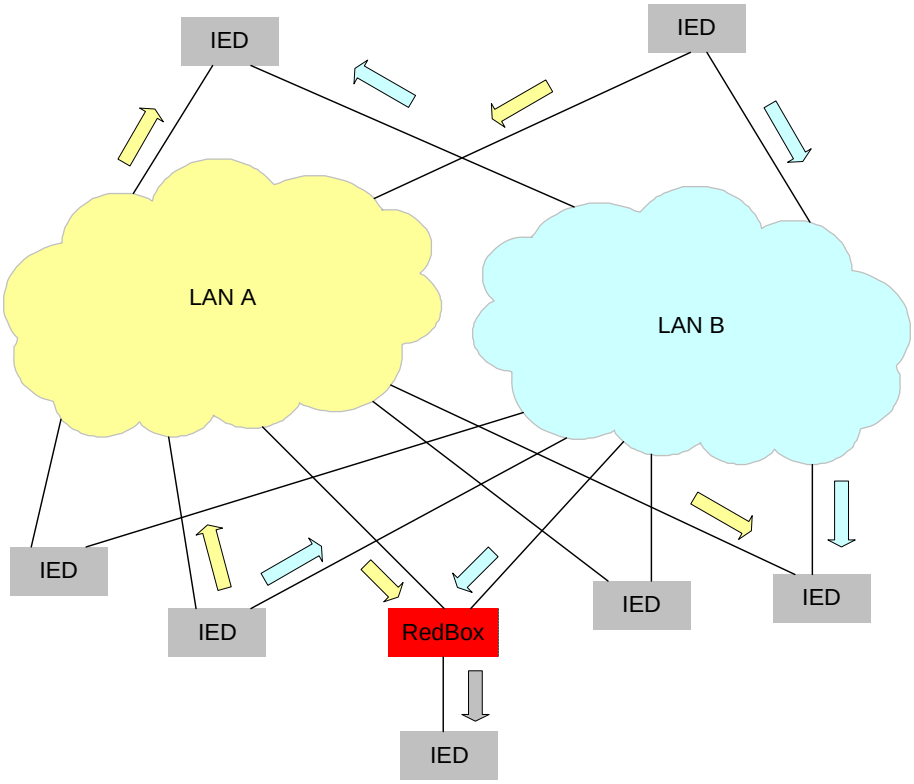

Figure 5 – Parallel Redundancy Protocol (PRP)

4.6.2 High-availability Seamless Redundancy (HSR)

With HSR, dual port devices are connected in a ring structure by full-duplex links as shown in Figure 6. The devices transmit frames out both ports, and also forward frames in both directions from one device port to the next device port, except for frames already forwarded – these frames must be identified and removed from the ring traffic to avoid infinite buildup of traffic. Forwarding or discarding frames requires HSR-specific hardware implementations.

The sending device sends a frame over each port after having inserted, in the Ethernet frame, a 6 octet HSR tag to uniquely identify copies of the same frame (the tag may correspondingly reduce the maximum packet payload size). The receiving device receives two identical frames from each port within a certain interval. Based on the source MAC address and the HSR tag, the receiving device passes the frame to the upper level receiving process and removes the duplicate. A specific addressed receiving device does not forward a frame for which it is the only destination. A sending device recognizes the frame it previously sent by recognizing its source address and the HSR tag, and removes that frame from the network.

Both ports of HSR devices share the same MAC address and operate with the same IP address(es) where relevant. Management protocols such as Address Resolution Protocol (ARP) operate correctly.

All devices within an HSR ring must be operating in accordance with HSR.

In return for the benefit of inherent messaging redundancy in a simple configuration, HSR tends to double the traffic on a given network link, halving the capacity of the network.

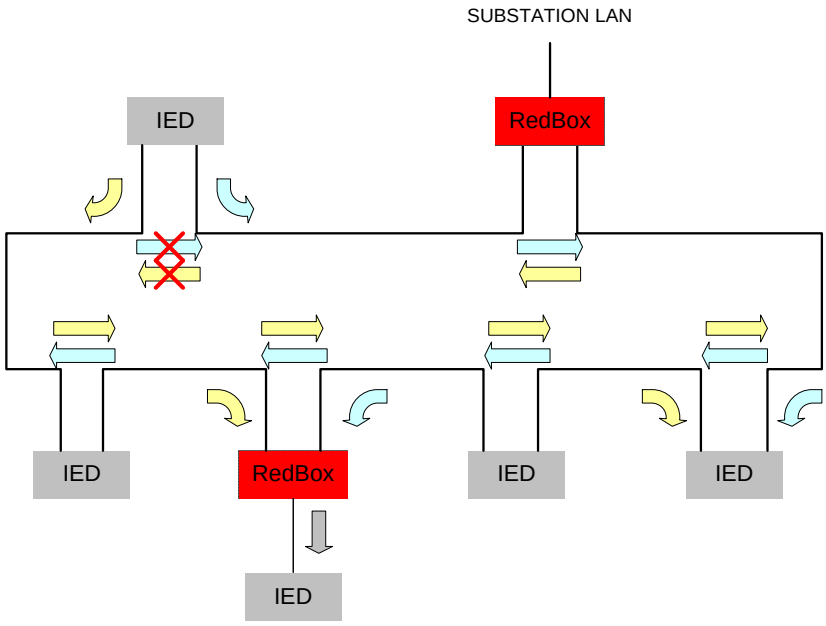

Figure 6 - High availability Seamless Redundancy (HSR)

4.7 Choosing among RSTP, HSR, and PRP

The introduction to Section 4.6 explained that PRP and HSR network designs may be helpful in certain application situations. At the time this report is written, there are limited numbers of compliant relay or RedBox products available; that situation may evolve by the time a reader sees this discussion. In any case, many users judge RSTP that is already widely available in switches, and single-port or failover-port relays without PRP or HSR compliant designs, to be satisfactory in substations with redundant LANs or where an RSTP bump does not cause unacceptable functional behavior.

Between PRP and HSR – PRP requires more network infrastructure but does not load the links with extra traffic, and is the high performance solution. HSR increases traffic but does not add network infrastructure, so it is the lower-cost solution.

Another new choice under evaluation by some utilities is Software Defined Network (SDN), which configures each switch for the primary and one or multiple backup paths for all the expected and allowed traffic, with continuous path monitoring for fast path switching in case of link failure.

4.8 Interconnecting RSTP with HSR or PRP - lessons learned

In many situations, instances of HSR or PRP will need to be interconnected to a RSTP network. This situation is likely to occur in existing substations that currently use RSTP for Ethernet redundancy but are adding HSR or PRP. In other situations, HSR/PRP could be chosen for critical high-speed redundancy and then interconnected to a network that does not have the high-

speed redundancy requirements (e.g. for connections from the substation/bay level to control center (e.g. what IEC 61850 refers to as Station Bus). The following advice results from the UCA International Users' Group Interoperability test of 2015.

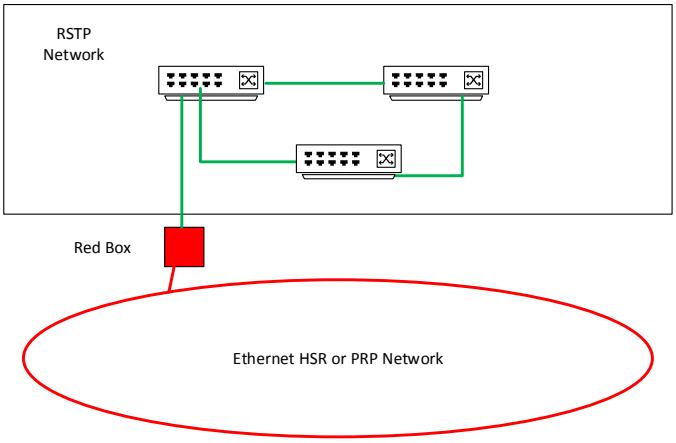

Figure 7 – Example of RSTP and HSR/PRP Interconnection

Figure 7 shows the typical interconnection between HSR/PRP networks and a RSTP network. The interconnection requires the use of what is known as a "Red Box". It is the purpose of the Red Box to take traffic from the RSTP network and add the appropriate information required to transmit it on the HSR/PRP network and to remove the same information when packets are transferred from HSR/PRP to RSTP.

In several situations, network designers consider the Red Box as a single point of failure and require a second Red Box be added (see Figure 8).

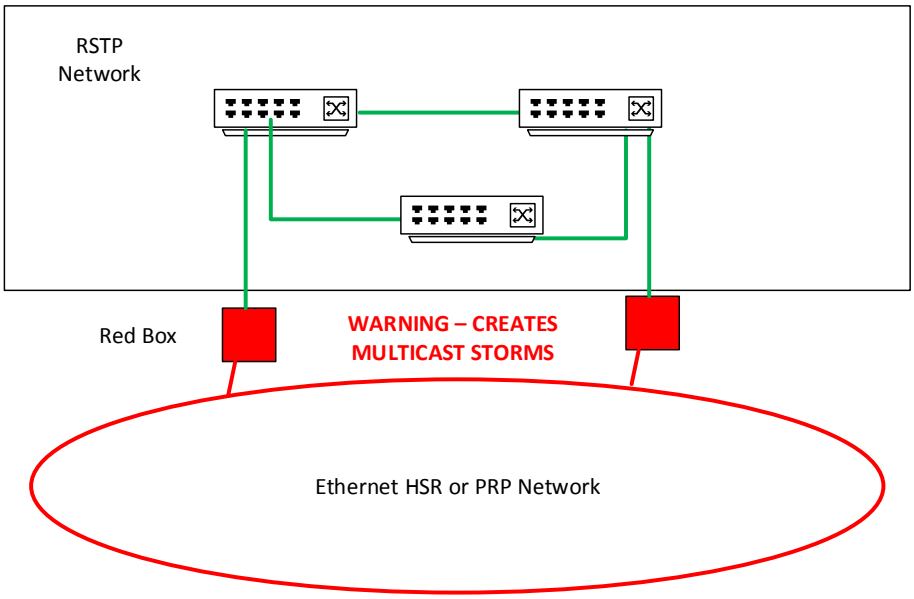

Figure 8 – Dual Connection of HSR/PRP with RSTP

The topology in Figure 8 causes multicast storms and packets to circulate both networks until network bandwidth capacities are reached. Therefore, this dual interconnection methodology SHOULD NOT BE USED unless the Red Boxes have a proprietary mechanism to prevent the problem. The problem is caused by two factors:

1. The RSTP Bridge Protocol Data Unit (BPDU) is not exchanged/known by the Red Boxes. There is therefore no ability of the Red Boxes to decide which is to transmit information from the HSR/PRP network to the RSTP network (e.g. to act as an extension of the RSTP network).
2. The information regarding the origination of the packet on the HSR/PRP network has been removed when the packet is transmitted onto the RSTP network.

The result of these factors is that a packet transmitted onto the RSTP network by Red Box 1 will be re-transmitted on the HSR/PRP network by Red Box 2. Likewise, packets transmitted by Red Box 2 will be retransmitted onto the HSR/PRP network by Red Box 1.

During the IEC 61850 Interoperability test, the dually interconnected RSTP and HSR/PRP network was tested. The result was as expected, a multicast storm was created that consumed all of the available usable bandwidth of the 100 Mbps network HSR (see Figure 9).

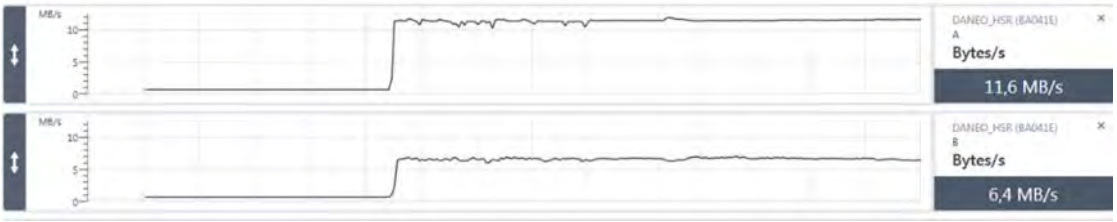

Figure 9 – Multicast Storm/Bandwidth Consumption caused by dual interconnection of HSR/PRP with RSTP.

Figure 9 clearly shows when the second Red Box was connected between the HSR/PRP networks. Additionally, traces of the HSR network activity were taken and GOOSE packets that were five (5) minutes old were still observed.
Upon close investigation, this behavior needs to be corrected through the IEEE 802 standard. IEC TC57 WG10 is attempting to forward this problem appropriately for standard resolution. Until such a resolution is reached, there are only two options:

1. Use a Red Box that has a proprietary mechanism to stop the problem. However, testing needs to be performed to make sure that such mechanisms actually work appropriately with the other network devices in use.
2. Only use a single Red Box between the HSR/PRP network and RSTP network.

5. Functional data flows

One of the most important features to grasp in considering a networked connection of devices as shown in Figure 3 is that the figure is only showing the *physical* connections of network paths – bidirectional optical fibers in our example – over which Ethernet message packets can flow. The physical configuration is influenced by need for reliability or redundancy of data flow paths as discussed in the previous section. The information can flow in circuitous paths among the devices depending on hierarchical processing functions within the devices. *This information flow does not follow directly from the physical connections*.

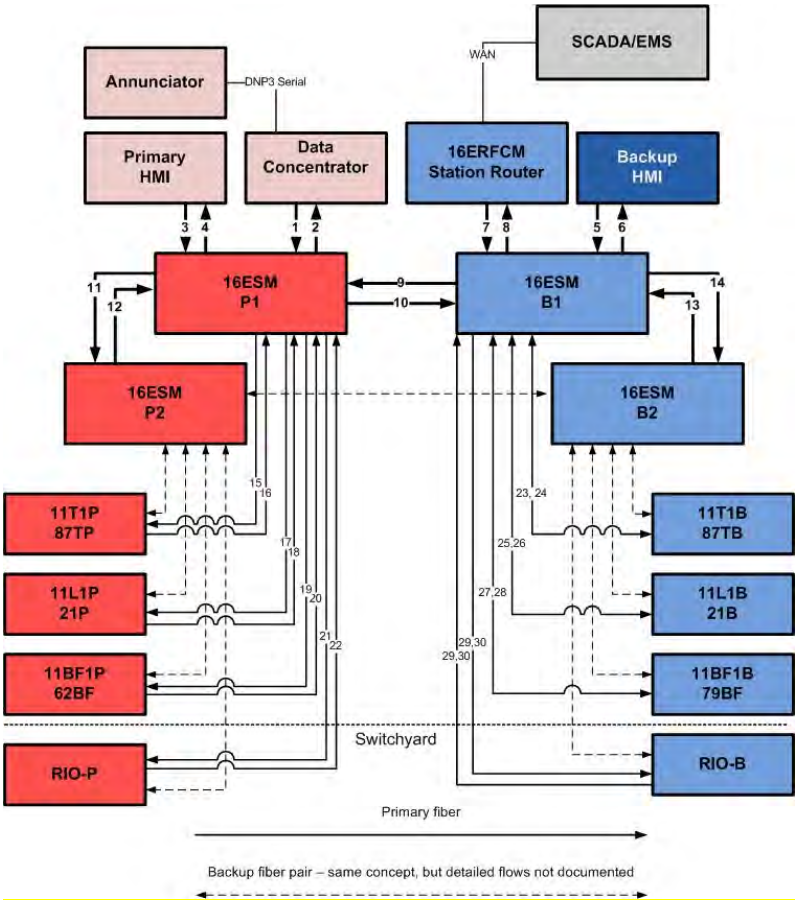

Figure 10 – Example of functional data flows

See Figure 10 for an example. The status of a particular circuit breaker may be monitored by switchyard I/O units RIO-P, RIO-B, and relays 21P and 21B. The data concentrator queries all field interface devices, polling via path 1 to primary switch 1, and across path 10 to backup switch 1. From these switches, the polls pass to relays and remote I/O units via paths 15, 17, 19, 21, 23, 25, 27, and 29. Responses pass back through the same switches via paths 16, 18, 20, 22 and 24, 26, 28, 30. The latter 4 sets pass from the backup switch 1 to primary switch 1 via path 9. All values pass through the primary switch 1 to the data concentrator that issued the polls via path 2.

The remote control center SCADA master polls the data concentrator through the station router 16ERFCM connected to the backup switch 1 by path 7. Its polls pass to the data concentrator by paths 9 and 2. The data concentrator responds with information it already gathered from the relays and organized in its data base, over paths 1, 10, 8, and the router through the remote path to the control center.

This scenario assumes all equipment is working normally. If any communications paths or switches fail, the messages pass over backup paths show as dotted lines in Figure 3, and through primary switch 2 and/or backup switch 2 – all different paths than shown above. An RSTP failover in the central loop will also alter the traffic paths.

On top of this, GOOSE messages published by relays are propagating over all the paths of the LAN. So it is clear that any physical path carries a variety of important monitoring, protection, and control traffic in both directions. This is not like the linear, sequential flow of information among devices with dedicated wired connections.

This example shows why design documentation for a project must include tabulation or charting of specific information elements exchanged among the relays and IEDs of the installation. The physical block diagram will not furnish adequate data for many troubleshooting or testing situations.

6. Interconnection options – fibers and wires

Cabling for an Ethernet network can be accomplished using either Category 5 (or better) copper twisted pair cables with RJ-45 connectors, or multi-mode & single-mode fiber optic cabling. Because of the EMI and RFI in substations, copper wire is judged by most users as suitable only for short physical runs among well-grounded devices close together; and/or for network connections that do not convey critical relaying signals. Optical cabling is not affected by EMI and RFI and is therefore the preferred method of connection inside a substation. There are two types of fiber optic cables - multi-mode and single-mode. Multi-mode is a larger fiber, 50 or 62.5 microns core diameter, compared to the 9 microns of a single-mode fiber. Multi-mode fiber has room for multiple paths or modes for the light to traverse as shown in Figure 11. Single-mode is smaller and only has room for a single path as shown in the figure.

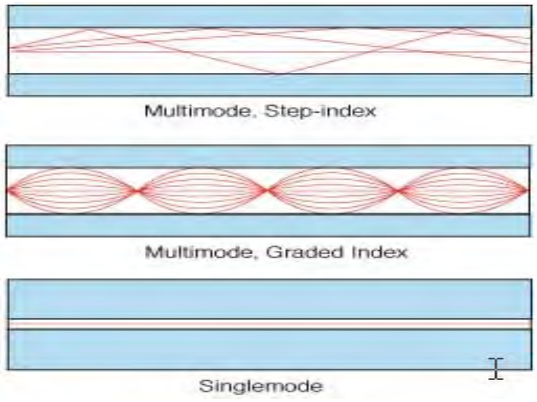

Figure 11 – Optical fiber types

Multi-mode fiber cannot support long distances or extremely high data rates -single-mode fiber is best for these requirements. On the other hand, multi-mode fiber can use LEDs or lasers as light sources - less expensive than the lasers needed with single-mode fibers. Connector interfacing is also less critical, so multi-mode fiber tends to be cheaper and easier than single mode for shorter distances. It is generally preferred for fiber runs within substation buildings.

Some users who are familiar with single mode fibers for long distance applications may choose to use those within substations as well. Common connector types are LC, ST, MTRJ, FC, and SC. ST has been popular for several years, but is being overtaken by LC for use with Ethernet over both fiber types at time of writing. Investigate manufacturer offerings, since technology and preferences are likely to change.

7. Ethernet switch description

The mainstay of the substation LAN is the Ethernet switch. To a protection engineer the switch is a message-processing computer with ports to connect all of the devices in a portion of the local area network, and is full of settings that affect protection messages sent among microprocessor relays and to substation level IEDs. Figure 12 shows the basic operation of a typical switch. To IT specialists, the switch is a device that operates at the data link Layer 2 of the OSI network model (see Section 3.1) and enables multiple physical LAN segments and nodes to be interconnected into a single larger network.

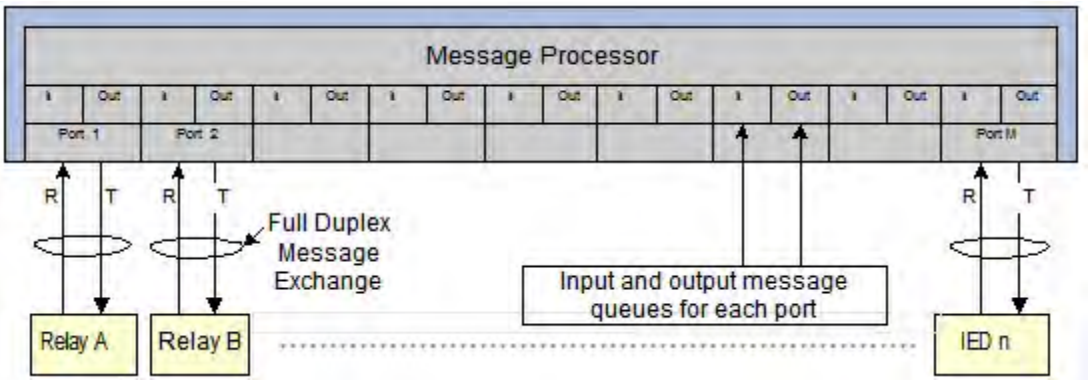

Figure 12 – Ethernet switch operation

Physically, a typical switch has 8 to 20 ports and is a 19-inch rack-mount unit that can be from 1 to 3 units high. There are smaller units that have 4 to 10 ports for installation on panels or DIN rails. Connected network paths employ either twisted-pair or fiber-optic cabling, both of which use separate conductors for sending and receiving data.

A protection scheme built on a substation LAN requires that protection engineers have some level of understanding of the functionality of the switch, along with support from IT specialists. Protection engineers must understand that in a fully switched network, relays and IEDs only communicate with the switch and never directly with each other. IT specialists on the project must understand that using an Ethernet switch in a protection scheme requires switches to be as environmentally robust as substation IEDs, which includes operating from the substation

battery supply. Utility grade switches offer enhanced reliability, EMI immunity, extended operating temperature range, high MTBF, and elimination of fan cooling. Ethernet switches used in substation automation applications should comply with IEC 61850-3 [27] and IEEE 1613 [16] standards for EMI immunity and environmental requirements to ensure reliable operation in substation environments.

The switch handles its many functional connections in parallel by inspecting each incoming Ethernet message frame. The switch checks each frame for errors and rebroadcasts the good frames through the correct ports to the desired target device(s). It typically performs this processing in a few microseconds per message, making it well suited to perform high speed protection tasks. It may forward to all other ports, or may use the physical addressing data included in the frame. It may associate only selected subsets of the ports for message forwarding, based on switch settings.

Unlike the specifically arranged and dedicated wiring of a non-Ethernet protection and control design, the switch is capable of interconnecting many intelligent devices thus allowing for many different control or measurement paths over a single physical path. Managed switches offer advanced Layer 2 and Layer 3 features that are useful for combining real-time protection and substation automation traffic with traditional operational and non-operational data sharing among LAN devices. These features increase performance by providing traffic prioritization, basic and advanced security capabilities, multicast traffic control, diagnostic capabilities, and a number of other features that are important for substation LANs. Some of these features are described in the following subsections.

7.1 SNMP (Simple Network Management Protocol)

The de facto standard for managing Ethernet switches is the Simple Network Management Protocol (SNMP) which allows their configuration, and the reporting of fault conditions such as loss of link, frame errors, and a variety of other statistical data about the network that can be used to monitor and detect switch or network problems remotely.

Similar to microprocessor relays, switches are managed by computers tied to them via the LAN or WAN, or sometimes via a serial port. See Section 7.9 for more details on settings and configuration of switches.

7.2 IGMP (Internet Group Management Protocol)

With IGMP enabled, the switch can receive commands or detect indications that certain groupings have been turned on or off, and can dynamically adjust its routing of multicast messages to certain VLANs or ports according to settings. IGMP has more significant applications in Ethernet routers, described below, where it manages the associations of specific routers in a large wide-area network (WAN).

7.3 IEEE 802.3x full-duplex operation on all ports

When Ethernet was created, a single (coaxial cable) was used to connect all devices, resulting in a half-duplex communication network; the introduction of switches ("bridges" in the IEEE language at the time of creation) eliminated message packet collisions, allowed full-duplex communications, and is now the dominant technology.

In addition, queuing and management of all transmitted messages on a link from one switch or IED port improves the probability that each packet is sent and received.

7.4 IEEE 802.1Q priority queuing

The quality of service (QoS) management provided by IEEE 802.1Q is an efficient tool for prioritization of traffic within a LAN, and is included in most managed switches offered for substation protection scheme use. Figure 1 shows where the priority tag is located in the Ethernet packet. Use of this tag is optional, but is to be utilized in IEC 61850 GOOSE message and sampled value packet specifications. By utilizing priority tags in a managed switch, critical data such as protection GOOSE messages can be prioritized over non-critical data such as the collection of historical records. This feature allows switches to recognize and shuffle frames tagged with different priority levels, as shown in Figure 13, to improve the probability that real-time critical traffic makes it through the network to its destination quickly and consistently even during high periods of congestion. Messages can be defined as having any of 8 priorities using the 3 bits of the priority tag. GOOSE messages that are used for high-speed tripping or control would generally be assigned a high priority (high value). A high priority is used for critical network management and configuration functions, without which the entire network cannot be kept in operation.

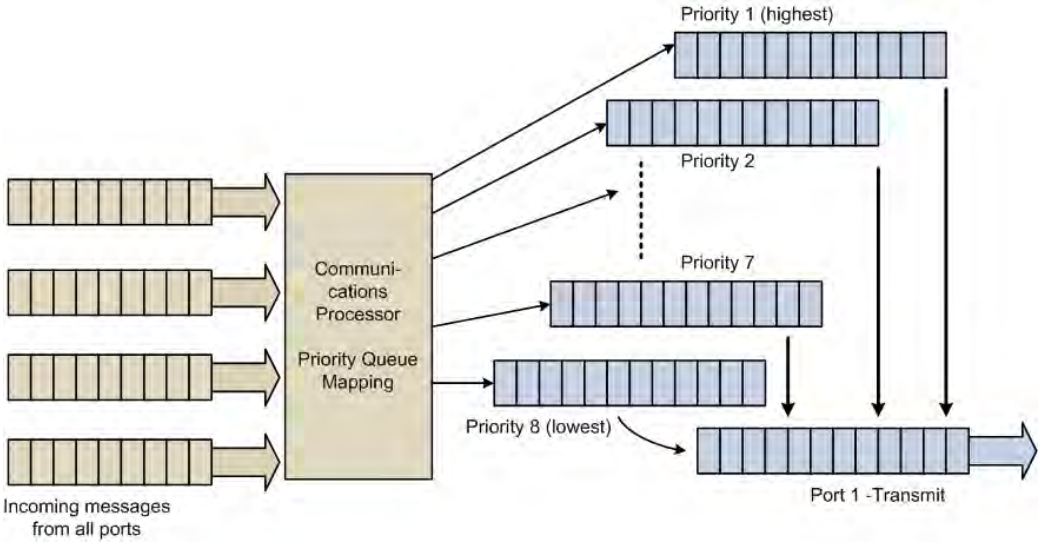

Figure 13 – Priority queuing in a switch

7.5 IEEE 802.1Q VLAN tagging

A VLAN is a logical grouping of IEDs or devices with a need to communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the

same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are located across multiple Ethernet network switches. Network reconfiguration can be done through software instead of physically relocating devices. In substation applications, assigning devices and functions to specific VLANs allows the switch to filter out irrelevant traffic that might clog a switch port or connected IED that doesn't need access to that traffic. There can be up to 4095 different VLANs in each LAN (value 4095 is not allowed).

This allows for the segregation and grouping of IEDs or switch ports into virtual LANs with isolation of message traffic in different VLANs. This can isolate real-time IEDs or mission critical GOOSE traffic from data collection or less critical traffic. The managed switch ensures that traffic from one VLAN does not cross the boundary to another VLAN. VLANs can be defined either by assigning specific ports to a desired VLAN, or the VLAN can be defined by a list of MAC addresses (physical addresses of devices on the LAN, described in the Ethernet packet discussion of Section 3). If a message packet has an embedded VLAN tag, located as shown in Figure 1 above, it is passed only to the ports or to the MAC addresses assigned to that VLAN. User configuration of the managed switch is required to specify which VLANs are allowed to ingress and egress each port (separate lists should be provided), and whether these are for the VLANs to be allowed or to be blocked; how they are assigned to the physical Ethernet ports; and whether the traffic is tagged or untagged.

An important, but under-appreciated, feature of VLANs is their use for security purposes; the fact that traffic cannot pass from one VLAN to another allows the protection of critical services from rogue attacks (assuming the associated Ethernet ports have been configured correctly).

IEEE 802.1Q tagging performs *explicit tagging* - the frame itself is tagged with VLAN information. The IEEE 802.1Q header contains a 4-byte tag header containing a 2-byte tag protocol identifier (TPID) and 2-byte tag control information (TCI). The TPID has a fixed value of 0x8100 that indicates that the frame carries the 802.1Q tag information. As shown in Figure 1, the TCI contains the following elements:

- Three-bit user priority
- One-bit canonical format indicator (CFI)
- Twelve-bit VLAN identifier (VID) - Uniquely identifies the VLAN to which the frame belongs – numbers from 0-4094 (4095 or hexadecimal FFF is not allowed)

A VLAN ID of 0 indicates that no VLAN assignment is intended for this packet – a tagged frame conveying only priority. However, not all switches handle VLAN ID of 0 in the same way. Check specifications or test the actual configuration if using VLANs and an ID of 0 (important if GOOSE messages are used). Also see VLAN section of PICS in Annex B of this report.

In the context of VLANs, the term "trunk" denotes a network link carrying multiple VLANs. Such trunks must run between "tagged ports" of VLAN-aware devices, so they are often switch-to-switch or switch-to-router links rather than links to end devices.

See Section 10.4 for more on isolating traffic with VLANs.

7.6 IEEE 802.1D GMRP

An alternate technology that constrains flooding of a network segment by multicast messages is the Generic Attribute Registration Protocol (GARP). GARP Multicast Registration Protocol (GMRP) is an implementation that allows for multicast data frames, such as IEC 61850 GOOSE frames, to be filtered and assigned only to those IEDs which request to listen to them. This feature reduces the load of traffic crossing the network and relieves many networked devices from processing and discarding frames they never needed. It is important to note that the above features are based on standards thereby ensuring interoperability among different vendors.

At time of writing, GMRP has not been required nor reported as used for applications with substation GOOSE messaging. Traffic has been managed with VLAN and priority tags, which are both explicitly supported in the IEC 61850 standard. The preference for VLANs derives from the static nature of substation IED traffic paths (compared to the dynamic nature of paths for applications such as video surveillance).

7.7 IEEE 802.1D Rapid Spanning Tree Protocol

The 802.1D Rapid Spanning Tree Protocol (RSTP) makes available the redundancy that protection networks require by automatically backing up paths of a fault tolerant ring network in the event an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. The use of RSTP was described in Section 4.5 above. "Rapid" indicates that the network reconfiguration by the 802.1D protocol occurs in tens or hundreds of milliseconds, as opposed to the 30-50 *seconds* for the old original Spanning Tree Protocol that is now obsolete in IEEE 802.1D-2004.

Vendor-specific path-protection algorithms for ring network architectures can be faster than the generic Rapid Spanning Tree algorithm – the generic algorithm is designed to handle mesh networks as well, and a substation installation may or may not have meshed path redundancies to handle. Users developing design standards for substations should check with switch suppliers regarding compatibilities of products, placement of RSTP functions within the network, and optimum configuration of switch settings to ensure the fastest failover performance. A laboratory development installation is recommended before finalizing a design standard or a field installation, to uncover interoperability issues of RSTP implementations.

7.8 A switch can have many settings

A managed substation LAN switch may require somewhere between several hundred to several thousand settings depending on the size and complexity of the network and the features required by the user. For example the type and settings for just one of 20 switch ports can be:

1. Name of device or link.
2. Enable/disable port.
3. Type of communications medium (wire or fiber).

4. Speed (10, 100, 1000 Mbps)
5. Duplex mode – half or full.
6. Enable/disable auto-negotiation with the connected device of speed and duplex mode
7. Enable/disable flow control – output port sends pause messages back to source ports that are sending too much data, to regulate flow of packets.
8. Enable/disable link failure indication (LFI) to the connected device (also known as Remote Defect Indication (RDI) or Far End Fault Indication (FEFI)).
9. Link alarms on/off.
10. Ingress rate limit – the maximum frame rate that will be accepted before excess incoming data is discarded. Excess message packets are discarded by the switch. (though unfortunately the measurement period is almost always never provided, or configurable)
11. Types of ingressing messages to limit and discard (all types including addressed messages, broadcast messages without destination address, multicast messages without destination address including IEC 61850 GOOSE relaying messages).
12. Egress rate limit – the maximum frame rate to be transmitted to the connected device. Excess message packets are discarded by the switch. (though unfortunately the measurement period is almost always never provided, or configurable)
13. Types of egressing messages to limit and discard (all types including addressed messages, broadcast messages without destination address, multicast messages without destination address including IEC 61850 GOOSE relaying messages).
14. Ingress VLAN filtering – a list of VLANs that will be blocked, or allowed to ingress the port.
15. Egress VLAN filtering – a list of VLANs that will be blocked, or allowed, to egress the port.
16. Settings to handle ingressing tagged messages with a VID- 0 (e.g. set a default VID)
17. Settings to handle ingressing untagged messages (e.g. set a default priority, and VID)
18. Settings to handle egressing messages which were tagged at ingress (keep or discard tag)
19. Populating a 64x8 table to map the DiffServ field of layer 3 IP frames to the desired priority queue (at egress).
20. Port mirroring enabling and selection – when enabled, the port carries the same output data as another chosen port, for diagnostic use. An application precaution: if separate ports for ingress and egress monitoring are not provided, the monitoring port may be overloaded.
21. Power-over-Ethernet settings – an additional list of settings for powering devices over wired link connections with set current limits, if enabled.

In addition to 20 lists for the 20 ports, there are overall settings for the operation of the switch, including operating parameters of the already-described switch services like RSTP. On top of this, the switch allows tables that configure VLANs and grouping parameters to use. Some of

these settings lists may grow as functions and features are enabled. The switch, like a modern relay, can have thousands of settings. As with a relay, a single incorrect switch setting can cause incorrect protective relaying behavior of the system. Using the switch manufacturer's default settings may lead to undesired behavior. Therefore, the list of settings for each switch must be developed and controlled as would be done for the settings of an important microprocessor transmission line relay. A settings management process also supports rapid and accurate recovery when a switch handling relaying traffic fails and is replaced in an emergency fields repair operation.

7.9 Configuring managed Ethernet switches

The network switches need to be configured. There are three primary ways to do this:

1. Serial port on the switch
2. Telnet
3. Web

Managed switches and routers usually have a serial port that can be used to communicate to the device for configuration. Switches can be completely configured from the serial port. For the routers, serial is for the configuring of the IP Address so that Telnet or the web can be used to configure the rest of the functions. In order to use Telnet or the web to configure the switch, an IP Address must be assigned for it to be reachable from a laptop or PC via an Ethernet cable. It must be in the same IP subnet as the computer used for the task and must be unique.

7.10 Ethernet switch port configuration

When configuring ports, the user is configuring the transport characteristics of the port. This includes the speed of the connection, the duplex and the connection orientation. A functionality called *auto-negotiation* is used by a switch to dynamically set the speed and duplex of the switch port by negotiating the maximum speed and duplex mode that the devices on both sides of the connection are capable of. The downside of this feature is that if only one end has this feature enabled, it is likely that this end will think it has a half-duplex connection even if the other end is set to a full-duplex connection.

Wired connections between negotiating devices can impact the ability to establish successful communications. The general rule of thumb for cabling between devices is to use crossover cables between "like" devices and straight-through cables between "unlike" devices. For example, to connect switch port to switch port, use a crossover Ethernet cable; for PC or RTU to switch, use a straight-through cable. An added feature for most Ethernet switches is the ability to auto-cross the port internally if the wrong type of cable is used to connect devices. In order for this to work, the port must be set for Auto MDI. Once the physical layer of the network is connected together, log onto the Ethernet switch to verify the speed and duplex of the connections to make sure that they are set and configured properly.

For substation protection and control applications with standardized Ethernet network designs, many users will prefer to disable automatic port configuration features and set fixed port parameters that are correct for this specific use. Fixing these settings can eliminate a potential source of tough-to-troubleshoot misbehaviors of switches.

7.11 Class of Service (CoS) and Quality of Service (QoS)

CoS - not to be confused with QoS - is a form of priority queuing that has been used in a number of communication and networking protocols. It is a way of classifying and prioritizing packets based on application type (voice, video, file transfers, transaction processing), the type of user (CEO, secretary), or other settings.

CoS is a queuing discipline while QoS covers a wider range of techniques to manage bandwidth and network resources. CoS classifies packets by examining packet parameters or CoS markings and places packets in queues of different priorities based on predefined criteria. QoS has to do with guaranteeing certain levels of network performance to meet service contracts or to support real-time traffic. With QoS, some method is used to reserve bandwidth across a network in advance of sending packets. In other words, QoS is the level of importance assigned to a type of traffic, CoS is the method employed to enforce it across the network.

The typical Ethernet switch supports 2 different types of Class of Service functions. The first, operating at layer 2 of the OSI model, is the three priority tag bits of the 802.1Q VLAN tag described in 7.4 above.

The second type of CoS is a layer three OSI function called Differentiated Service Control Point (DSCP). It uses the Type of Service (ToS) bits that are part of the Layer 3 portion of the Ethernet frame. Many managed Ethernet switches are able to look at the ToS bits and then assign the frame to a priority queue on the switch port.

7.12 LACP (Link Aggregation Control Protocol)

This protocol allows the user to configure multiple Ethernet ports between Ethernet switches into a Single virtual “Link” as shown in Figure 14. This allows load sharing of information between the links and is extremely fast in moving data between a failed port and an adjacent port if there is a link failure.

Link Aggregation Control Protocol (IEEE 802.1ad) provides redundancy without the use of Spanning Tree. It enables users to be able to bundle groups of ports between switches to form 1 virtual link with the bandwidth of the member links. LACP provides several functions:

- Higher bandwidth
- Enhanced Bandwidth Granularity
- Load sharing across the member links to balance bandwidth across the member links
- Fault tolerance provided by offloading data to working member links when a member link fails

LACP is a method of providing needed extra bandwidth between Ethernet switches that have extra non-utilized ports without buying a switch or switches with higher bandwidth ports. For example, moving from 100Mbps switching to Gigabit Ethernet switches.

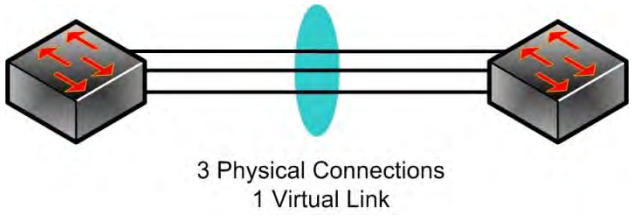

Figure 14 - Example of an LACP based Ethernet connection between switches

7.13 Product Implementation Conformance Statement (PICS)

For Ethernet switches to be used in networks transporting IEC 61850 traffic, and especially GOOSE messaging, the UCA International Users' Group (UCA) has developed a Product Implementation Conformance Statement (PICS) which is useful for evaluating the suitability of such switches. See **Annex B** for the draft Ethernet switch PICS, enhanced for this report. The PICS evolved considerably after UCA's 2011 interoperability testing of commercial Ethernet switches, whose behavior varied in unexpected ways during those tests. Along with checking conformance of a switch with this conformance statement, the user should perform live network tests with the actual switches to be used in a standard design, and with their configuration settings as intended for the final installation.

8. Ethernet router description

Ethernet routers are the traffic management computers between small local groups of devices on a LAN and a large or near-infinite WAN when layer 3 is used. A router is not needed for layer 2 networks of large physical extent with SONET connections among sections as described in Section 11). GOOSE messages are used only within LANs, or are conveyed in a router-configured tunnel between LANs separated by a WAN as described in IEC 61850-90-1. See Section 12.3 below for more on GOOSE tunneling. The following description describes more general communications of Internet Protocol (IP) traffic over arbitrary or widely variable paths, to support many enterprise applications beyond high-speed protection and control.

Ethernet networks are grouped in what are called subnets. A subnet is a logically visible, distinctly addressed part of a single Internet Protocol network. The process of defining component subnets (subnetting) is the division of a computer network into groups of IP devices that have a common, designated IP address routing prefix. Subnetting breaks a network into smaller realms that may use existing address space more efficiently, and, when physically separated, may prevent excessive rates of Ethernet packet collision in a larger network. The subnets may be arranged logically in a hierarchical architecture, partitioning the network address space into a tree-like routing structure.

It is currently almost impossible for an individual or company to be allocated IP address blocks. In most cases, they are allocated by either the Internet Service Provider (ISP) or the enterprise network administrator. The reason for this is the ever-growing size of the internet routing table. Just 10 years ago, there were less than 5000 network routes in the entire Internet. As of 2015, there are over 100,000. Using a mechanism called classless inter-domain routing (CIDR), the biggest ISPs are allocated large chunks of address space; the ISP's customers (often other, smaller ISPs) are then allocated networks from the big ISP's pool. That way, all the big ISP's customers (and their customers, and so on) are accessible via 1 network route on the Internet.

Routers are used to interchange traffic between sub networks and constitute logical or physical borders between the subnets. They manage traffic between subnets based on the routing prefix of the IP addresses.

A router can be defined as a device which provides a path from a node on one network or subnet to a node on another network. Routing is the process of determining the end-to-end path between the sender and the receiver of a packet. There are 2 types of routing:

1. Source routing - the source node determines the route and includes it in special fields in the data frame. Source route bridging in Token Ring uses source.
2. Hop-by-hop - The route between source and destination is determined along the way, hop-by-hop. Most routing protocols are hop-by-hop based.

Routers can provide data movement in 2 ways: Statically via routes that are mapped by hand (Static Routing) or dynamically via designated routing protocols (Dynamic Routing).

Static routing can be useful for small routing areas, but does not provide fast failover because it requires user interaction to program an alternate route manually. Dynamic routing is required where a hand off failover is required or the routing environment is large. Routing protocols are inherently slower on failover than layer 2 protocols.

The routing protocols most used are Routing Information Protocol (RIP), Routing Information Protocol Version 2 (RIPII) and Open Shortest Path First (OSPF) for standard protocols.

In a substation network, an Ethernet router serves as an interface between a local area network in a substation and the utility control or enterprise WAN. Since the WAN comprises far-flung segments accessed through long-distance data communications, which may be utility-owned or common carrier (purchased service from a communications company). To communicate with remote parts of the WAN, the router must handle message reformatting to utilize the available data communications path, which may or may not be an Ethernet link to other routers. It may also need to provide cyber security protection so that messages sent across unprotected networks cannot be monitored, disturbed, or corrupted by unknown persons.

Physically, the router is another microprocessor based communications device like a switch, typically in a 19 inch rack mount assembly of 1 to 3 rack units. It has fewer ports, since its role is to interface one or two LANs with one or a couple of external communications circuits. While

switches tested to IEEE 1613-2003/9 environmental standards [16, 17] have been available for years, IEEE 1613 routers have become available recently. This is explained in Section 14 below.

The router processor handles a larger array of functions and algorithms than what is required for a switch. It carries out sophisticated manipulation of layer 3 (network layer) routing information (such as IP address) in the message payload, which switches generally ignore. It may also manipulate the contents of the message packet as shown above and defined in layer 2. There are potentially thousands of user settings, configuring a database that describes how the WAN and the networked world outside the substation are accessed. With this, the router can direct messages through the WAN or even the Internet to remote locations requested by devices or users in the substation; and can recognize the origin of incoming messages from far away.

The functions in an example router include:

1. Ability to learn about remote servers on the WAN, including those that provide translation of domain names to numerical internet protocol addresses.
2. Manual entry of static WAN configuration.
3. Ability to translate addresses on the LAN to different addresses on the WAN or Internet for proper routing and for cyber security protection of LAN devices.
4. Firewall to protect substation LAN traffic and devices from unauthorized access.
5. Virtual Private Networking (VPN) using any of several standard protocols – establishing an isolated communications tunnel through an insecure public communications network to a secure remote utility server, with strong encryption of messages that protects against disruption or monitoring of message flow.
6. Processing all the messages on the LAN side and recognizing the packets intended for external communications to remote places; routing and prioritization of this external message traffic in both directions.
7. Routing of multicast messages to LANs or VLANs at remote sites - generic routing encapsulation, GRE. Recall that multicast messages have group destination addresses, and must be recognized by looking at what device sent them (if filtering is desired).
8. Ability to assign and manage IP addresses of devices on the LAN that request them - dynamic host control protocol, DHCP. In substations the IP addresses of relays and IEDs are usually fixed as settings in those units.
9. Recognition of external path failures and rerouting of traffic via alternate paths - virtual router redundancy protocol, VRRP.
10. Reformatting of messages for compatibility with a variety of external communications channel types, for example:
    a. T1/E1 (e.g. utility owned fiber ring or microwave)

b. T3/E3/DS3 (e.g. utility owned SONET)

c. Frame Relay (common carrier)

d. Multi-protocol layer switching (MPLS) (common carrier or utility)

e. Ethernet connection to WAN

f. DSL to common carrier

g. Serial RS-232 and RS-485 (e.g. to old SCADA master)

h. Modem over telephone circuit or voice channel

11. Monitoring, alarming, and logging of traffic behavior and diagnostics.
12. Network management protocol (SNMP) communications for router and network configuration management.
13. Secure shell (SSH) network web server communications with a remote management computer/server – another way of remotely managing the setting and configuration of the router.
14. Receiving and serving date/time information to the LAN - network time protocol, NTP; and simple NTP or SNTP.
15. Facilities for backing up and restoring the full configuration or setting data base.

On this last point – as discussed above for switches – the saved database should be handled and managed like settings of an important relay. Many of the settings and values impact the coordination of the router performance with remote routers and computers on the utility network, and network communications may fail if the data base restoration is not accurate and precise. It is critical to have a setting archive and a setting restoration work plan if the router fails and is replaced in the field, just as for a complex relay.

Routers support several types of protocols to communication like OSPF (Open Shortest Path First) and RIP (Routing Information Protocol) that have a communications redundancy built in as long as the physical network architecture remains in place.

For teleprotection or other applications with critical timing, most users choose not to let the router find its own available paths to the remote terminal. Specific fixed primary and failover paths are configured in the router so that latency and asymmetry can be tested and assured. A tertiary path may be defined; more than that are difficult to control and are generally considered unnecessary. Routers should not be allowed to fall back to choosing any available path unless the traffic is for an application known to have low sensitivity to latency or asymmetry.

The number of routing protocols, with new ones emerging on a regular basis, reflects their inability to provide the guaranteed deterministic reliability and dependability desired for many applications. They have been considered suitable for SCADA traffic, but had been considered unacceptable for most protection applications (which had been kept on layer-2 networks).

In recent years, Multi-protocol layer switching (MPLS) Ethernet routers are being applied for teleprotection channels and other high-speed, timing-critical applications over Ethernet WANs. MPLS uses a routing label on each Layer 2 packet, sometimes called Layer 2.5. Modern MPLS networks with preconfigured paths can have low latencies and asymmetries that may be suitable for teleprotection, including line current differential protection. However, in this early phase of application, extensive user performance testing is needed before commissioning to assure secure relay performance.

Layer 3 wide area protocols have been recently defined for control functions with slightly longer but critical time frames of 20 to 100 ms – see description of IEC 61850-90-5 in Section 12.

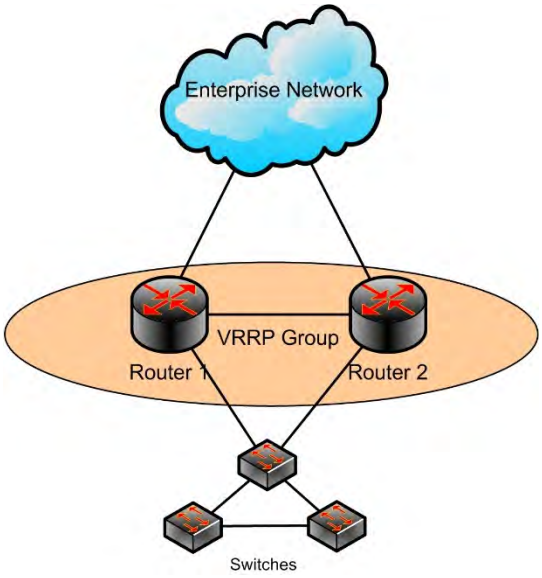

Figure 15 - VRRP Example

There is also a router physical redundancy protocol. If one router fails, its designated backup is placed into service seamlessly as if the original never left. This is called VRRP, Virtual Router Redundancy Protocol, shown in Figure 15. VRRP is the way for routers to perform physical redundancy to each other. If one router dies or is unable to function in the appropriate manner, its designated backup will take over the former routers function. They maintain this relationship through the use of HELLO packets and regular updates to make sure that both routers have all the same information.

The use of VRRP would be considered as a function to incorporate into an IEC 61850 substation networking design if there is a requirement to attach to a corporate network through a gateway and there is a requirement to maintain some sort of segregation between the substation IEC 61850 network and the corporate environment.

9. Network addressing with Internet Protocol (IP)

Local area networks (LANs) operate using only layer 2 (MAC addressing) of the 7-layer stack. However, most applications implement higher-level protocols, which are required anyway to

communicate over logically greater distances (wide area networks, WAN). Layer 3 defines so-called 'routable protocols,' using translation of fixed MAC addresses to (for example) IP addresses. While it is possible to build a physically-large layer-2 Ethernet network, in most cases messages transmitted outside the LAN are carried on another physical medium – telephone line (modem), SONET optical fiber, or radio link, for example. Routable protocols enable transparent interworking between the LAN and the outside world, making them the standard for the non-critical communications originating in Ethernet LANs. Ethernet routers described in Section 8 interface a LAN to the WAN.

9.1 IP Addressing and subnets

An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. An IP address serves two principal functions in networking: host or network interface identification and location addressing. The role of the IP address has also been characterized as follows: *"A name indicates what we seek. An address indicates where it is. A route indicates how to get there."*

The original designers of TCP/IP defined an IP address as a 32-bit (4-byte) number and this system, known as Internet Protocol Version 4 or *IPv4*, is still in use today. However, due to the enormous growth of the Internet and the resulting depletion of available addresses, a new addressing system (IPv6), using 128 bits (16 bytes) for the address, was developed in 1995 and last standardized by RFC 2460 in 1998. Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as 208.77.188.166 (for IPv4), and 2001:db8:0:1234:0:567:1:1 (for IPv6).

The Internet Protocol also has the task of routing data packets between networks, and IP addresses specify the locations of the source and destination nodes in the topology of the routing system. For this purpose, some of the bits in an IP address are used to designate a subnetwork. The number of these bits is indicated in CIDR notation, appended to the IP address, e.g., *208.77.188.166/24*.

Note that the commonly-used *legacy* means of designating subnets uses a subnet mask to delineate the assigned range of addresses. For example, a mask of 255.255.255.0 indicates a domain of 256 available addresses (xxx.yyy.zzz.0 – xxx.yyy.zzz.255); a mask of 255.255.254.0 a range of 512 addresses ((xxx.yyy.zzz.0 – xxx.yyy.zzz+1.255). This legacy notation appears elsewhere in this report. The CIDR notation for these two examples would be xxx.yyy.zzz.0/24 and xxx.yyy.zzz.0/23, respectively. At the time of this writing, an excellent discussion of CIDR notation can be found at: https://www.lifewire.com/cidr-classless-domain-routing-818375.

9.2 IPv4 (Internet Protocol Version 4) subnets

In the early stages of development of the Internet Protocol, network administrators interpreted an IP address in two parts, network number portion and host number portion. The highest order octet (most significant eight bits) in an address was designated the *network number* and the rest of the bits were called the *rest field* or *host identifier* and were used for host numbering within a

network. This method soon proved inadequate as additional networks developed that were independent from the existing networks already designated by a network number. In 1981, the Internet addressing specification was revised with the introduction of classful network architecture.

Classful network design allowed for a larger number of individual network assignments. The first three bits of the most significant octet of an IP address was defined as the *class* of the address. Three classes (*A*, *B*, and *C*) were defined for universal unicast addressing. Depending on the class derived, the network identification was based on octet boundary segments of the entire address. Each class used successively additional octets in the network identifier, thus reducing the possible number of hosts in the higher order classes (*B* and *C*). The following table gives an overview of this now obsolete system. This is how the IP Address classes were divided up:

Class	Range
A	**0**.0.0.0 to **127**.255.255.255
B	**128**.0.0.0 to **191**.255.255.255
C	**192**.0.0.0 to **223**.255.255.255
D	**224**.0.0.0 to **239**.255.255.255
E	**240**.0.0.0 to **255**.255.255.255

Table 7-1 – IP address classes

Today, remnants of classful network concepts function only in a limited scope as the default configuration parameters of some network software and hardware components (e.g. netmask), and in the technical jargon used in network administrators' discussions.

9.3 IPv4 private addresses

Early network design, when global end-to-end connectivity was envisioned for communications with all Internet hosts, intended that IP addresses be uniquely assigned to a particular computer or device. However, it was found that this was not always necessary as private networks developed and public address space needed to be conserved.

Computers not connected to the Internet, such as factory machines that communicate only with each other via TCP/IP, need not have globally unique IP addresses. Three ranges of IPv4 addresses for private networks were reserved in RFC 1918. These addresses are not routed on the Internet and thus their use need not be coordinated with an IP address registry.

Today, when needed, such private networks typically connect to the Internet through network address translation (NAT).

IANA-reserved private IPv4 network ranges

	Start	End	No. of addresses
24-bit block (/8 prefix, 1 × A)	10.0.0.0	10.255.255.255	16777216
20-bit block (/12 prefix, 16 × B)	172.16.0.0	172.31.255.255	1048576
16-bit block (/16 prefix, 256 × C)	192.168.0.0	192.168.255.255	65536

Any user may use any of the reserved blocks. Typically, a network administrator will divide a block into subnets; for example, many home routers automatically use a default address range of 192.168.0.0 through 192.168.0.255 (192.168.0.0/24). Utility LANs often use the 10.x.x.x range for more flexibility in choosing the IED addresses.

9.4 Example of DHCP server & static/dynamic IP addresses

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that allows a DHCP server to assign an IP address to a host that connects to a network and issues a DHCP discovery request. The DHCP server will issue an IP address for a limited period of time referred to as a lease. DHCP servers are commonly used in home or enterprise LANs. Without a DHCP server on a network the IP addresses will have to be manually entered; this is referred to as static IP addressing. It is common for all IP addresses on a substation LAN to be manually assigned, to ensure that they do not change.

9.5 Internet Protocol version 4 (IPv4) versus IPv6

The ability to acquire a public IPv4 address, particularly for Class A and B, is becoming more difficult due to the number of octets available for addressing (i.e. 4). This looming issue has been commonly referred to as address space exhaustion. The primary impetus for adoption for IPv6 is to increase the number of publically available addresses so that Internet growth, and other large scale networks, can be created. IPv6 supports 16 octets of addressing.

Besides resolving the address exhaustion issue, several countries have governmental regulations for IP applications provided to government agencies. These regulations basically state that any IP application, provided to governmental agencies, should be able to be migrated to the use of IPv6. In reality, this reflects an acknowledgment that governmental use represents, in its own right, a large intranet that may exceed the addressing capability of IPv4.

This is not to say that address exhaustion is the only issue/enhancement provided by IPv6. Some other functional enhancements, provided by IPv6, are regarding: security, quality of service; and packet prioritization. Any of these could be equally valid reasons for planning to utilize IPv6.

Although it would appear that IPv6 adoption should be straightforward and worthwhile, there are several questions that need to be asked prior to adopting IPv6 for an intranet or substation. These questions are:

- Does the utility intranet require the address space offered by IPv6?

- Does the intranet use public IPv4 addresses (e.g. not 192.168.xxx.yyy)?
- Are there regulations requiring IPv6 support?

If the answer to all of the above questions are NO, then migration to IPv6 may not be needed.

If the intranet/extranet plans migration to IPv6, here are some steps to consider:

- Do the current intranet/extranet routers have support for IPv6?
- Do the host systems support IPv6 in parallel to IPv4?
- Do the IEDs support IPv6? If not, address mapping will be needed.
- Is there a plan for mapping IPv4 addresses to/from IPv6 addresses?
- Has the user purchased training and network analysis tools that make diagnosing IPv6 issues easy?
- Who is going to manage/allocate the IPv6 addresses assigned to the enterprise?

In summary, there are many reasons that adoption of IPv6 will benefit an enterprise. However, careful analysis of the current network assets/IED's capabilities will be needed. It is a high probability that dual communication addressing (e.g. IPv4 and IPv6) will be needed to provide the capability for an easier migration path.

10. Ethernet network security

Security refers to the inability of untrusted devices (people or their machines) to monitor or control the network. There are many security vulnerabilities. Here is a sample of major issues:

1. Passwords- they aren't changed or are left at default. When employees leave, their passwords aren't changed or deleted
2. Device Authentication- no network based authentication is used to make sure that attached PCs and laptops are who they say they are
    a. As a side note, passive devices such as controllers, I/O, sensors, etc. cannot participate in network authentication as they are not interactive with the network. About 70-90% of an Industrial control network is comprised of passive devices.
3. Remote Access- just using dialup doesn't cut it. These access points need to be protected
4. Connections to existing corporate networks- establishing access rules and functions in these areas prevents unauthorized access from people that do not need to access these spaces
5. Connections between plant floor networks across a network that is not under control by you
6. Devices like laptops and PCs infected with viruses that come into a secure area and inadvertently (or even on purpose) infect the control system architecture
7. Outright hacking that is internal or external to the protected network

Security threats are mitigated using a combination of user-authentication, cybersecurity and circuit isolation technologies.

10.1 User authentication

In this context, user refers to a person with authority to monitor and/or change the settings of the network devices. This access must be controlled using technologies commensurate with the importance of the network's integrity; e.g. for networks carrying critical traffic a "two-factor" or better access technology should be used, probably with an RBAC (Role Based Access Control) feature.

10.2 Cybersecurity

If the network design allows messages from untrusted sources to reach critical IEDs, then the use of encryption and authentication technologies is needed to mitigate such threats.

Some issues include the management (creation, updates, and invalidation) of the keys used, the technical challenges encrypting low-latency messages (e.g. GOOSE, 1588) and the limited lifetime of acceptable algorithms (since math experts with hacking intent are constantly stepping up to the challenge of breaking security algorithms).

10.3 Circuit isolation

If the network design can prevent messages from untrusted sources reaching critical IEDs, then the need for cybersecurity technologies is avoided.

This can be achieved in VLAN-aware networks by assigning dedicated VLANs to the critical traffic (including management of the switches), and blocking these VLANs from ingressing and egressing untrusted ports, with firewalls being used to authenticate any untrusted-port traffic needing access to IEDs (e.g. from the IED's vendor).

To guard against an insider's attack, critical-traffic Ethernet ports should be monitored for loss-of-link events.

10.4 Using VLANs as an isolation tool for IEC 61850 applications

Virtual Local Area Networks, or VLANs, are logically separate Ethernet networks. Even though devices may share physical cabling or equipment, Ethernet packets cannot be shared between devices in different VLANs without a Layer 3 device, like a router for example. VLANs can serve as a powerful isolation tool when networking a group of devices because most network switches have the ability to be partitioned into multiple VLANs and each port on the switch can be configured to access specific VLANs defined by the user. For IEC 61850 applications, the use of VLANs as an isolation tool gives users the ability to move traffic from a group of Operational VLANs to Test VLANs so that IEDs can be isolated and tested without having to move any physical cables or reprogramming the IEDs. The key is that even though VLANs are set in the GOOSE message of the publishing IED it is the switch that interprets the VLAN information.

How switches are configured for VLANs varies widely between vendors, so it is important to understand the relevant nuances encountered. As an example, originally VLANs were only supported by the inter-switch ports called *trunk* ports, whereas it is now common for the *edge* ports (those connected to the IEDs) to also support multiple VLANS. This allows the IEDs to use different VLANs for different services - a useful tool for isolating specific services in each IED.

VLANs can be used to isolate IEEE 1588 Precision Time Protocol [28] traffic for protection of this critical service.

10.5 Fiber sniffing

Another concern could come from someone trying to tap into a fiber. The easiest and most undetectable method for optical hacking is bending since there is no interruption to the light signal. Using a commercially available clip-on coupler, a micro-bend is placed in the cable to allow a small amount of light to radiate through the polymer cladding. This light, and thus the data, is then captured with a photo detector and a transducer capable of translating an optical signal into an electrical signal. This is challenging to carry out on a well-protected, multi-fiber cable.

Splicing, another method, isn't practical; it often results in detection due to the momentary interruption of the light signal which would cause a switch in a SONET ring network or a path switch on an Ethernet over direct fiber network.

To protect against fiber hacking, a system capable of detecting slight changes in light, which may be too sensitive, or some type of data encryption would be required. However, it should be considered that tapping of the fiber optic cable between substations may carry a very low risk if the fiber network is built using Optical Ground Wire (OPGW). Since OPGW is placed above high voltage phase conductors and that to break into the OPGW one would have to first access the ground wire and second the outside metal part of the OPGW would have to be stripped away to gain access to the fiber optic cable.

Alternately the signal being transported could be encrypted (e.g. using AES-256), thereby preventing any attacker monitoring or injecting malicious data.

10.6 Network security ground rules

Network security is first and foremost defining, designing and implementing a series of practices and tools that allow you to protect the assets and data associated with your network. For the most part, the practices are simple and are common sense based. The number one requirement for all administrators is to know what is connected to the network and how the devices talk to one another. This mandates the use of protocol analyzers to see what the day to day traffic looks like, and up-to-date maps of the network that show how the devices are connected and how the network has grown over time. With this baseline, it is possible to find unknown or unauthorized attachments.

Securing a computer network is a multifunction task, normally based upon several physical aspects:

1. Is the network isolated or integrated? Isolated networks have no external access to the outside world; integrated networks do.
2. If it is an integrated network, do you own all of the network, or do you use the network of another provider, even if it is part of the same company?
3. Are you worried about data integrity, network access, or both? Data integrity is making sure that the data is what is actually generated and sent from producer to consumer.

Network access defines what and who should be allowed to access a network segment. This can be as small as a single IP Address to whole other networks that may be part of a corporate network environment.

10.7 Security plan

Security cannot be achieved without a security plan. The tools used to secure networks come from several sources. There are functions that reside within the network infrastructure devices that provide security related operations as well as external devices such as Firewalls and Virtual Private Network (VPN) systems. The simply stated rules are to keep in what's supposed to be in, keep out what's supposed to be out, and make sure that the data sent and received is protected and authentic.

In the control system arena, across all the various markets, the need for security that is focused upon the requirements of the control system operation is finally being brought to the fore and is becoming its own area of focus. Control system networks are not Enterprise networks. They do not have much in common aside from the fact that they both use Ethernet. Control system networks are normally a mixed bag of unique protocols, technologies (proprietary cables, connectors, etc.), and other connectivity technologies such as serial (RS232/422/485) and the need to support many legacy systems. The learning curve can be huge for people coming into this area.

Seeing that there is now a growing series of requirements that are focused strictly upon control systems and securing them, it is imperative that we identify the areas of security within and without the control system network. To identify these areas, we have to define a perimeter. Just like in the military, it serves much the same purpose. We assume that there are unknown harmful influences outside. The design and support of the perimeter will dictate how well the user can detect, identify, respond to and stop harmful intrusions.

10.8 Step 1- Defining the perimeter

Defining the network mandates validation of the original drawings, or generation of new ones. If it is a new network, define all the applications and determine what each device needs to talk to and who needs to access this new environment. Figure 16 shows how a network security perimeter can be defined. This can be very basic for small networks to very complex for large integrated networks.

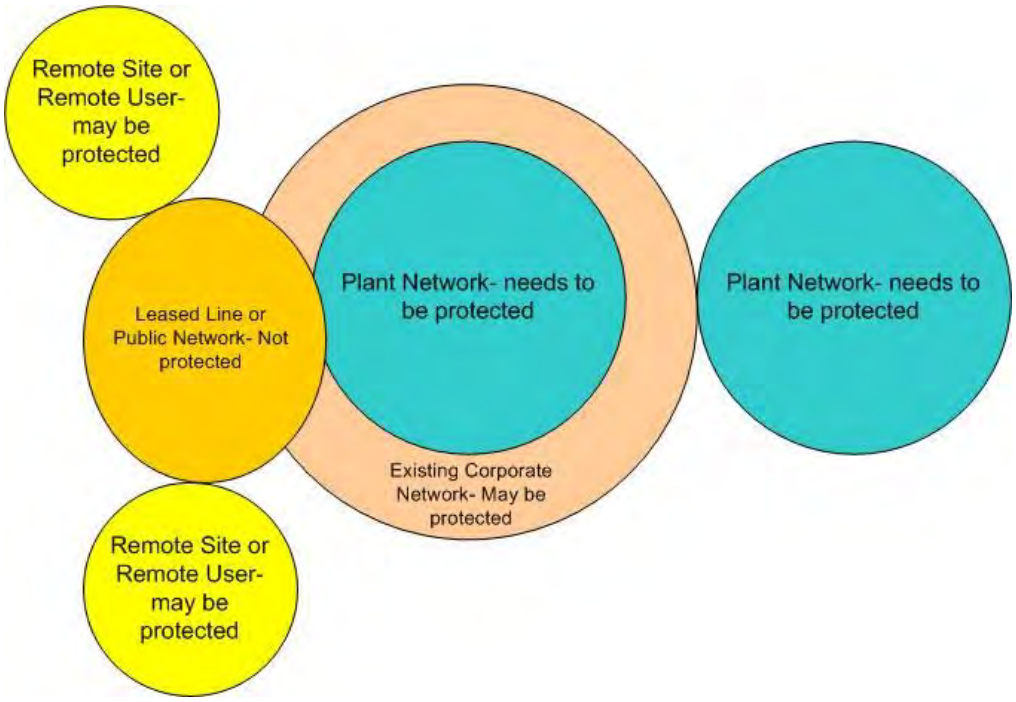

Figure 16 - Defining the network perimeter

One of the best ways to look at a network is to determine who needs access to whom in a logical way. Forget the physical design and look at the groups of devices and users and the way they are to interact. There are control system groups with all the associated HMIs, I/O, relays, control IEDs, RTUs, historians, etc. Administrative groups use monitoring video, voice services, physical security, fire response, and safety systems. The existing enterprise network may have to connect to provide business or operating information. Remote access may be needed by offsite engineers or technicians to monitor or diagnose systems and events.

10.9 Step 2- Add tools and plug holes

Review the list of where the security issues lie. The issue list corresponds to a set of functions and tools to fix these security holes. Some reside within the functions of the network infrastructure, while others are external devices put into the network to create secure access portals that allow or restrict access to the network. Additional tools protect the transmitted data by encrypting it across unprotected networks that you do not control, such as leased lines that connect remote sites to the central protected network. An example list follows:

1. Passwords-
    a. Change often, do not use the default passwords, and make the passwords complex and hard to crack.
    b. Apply also to the network infrastructure and control devices. These have password access that needs to be accessed as well. If not, a simple reconfiguration of a network element can create network outages.

2. Device Authentication-
    a. Radius authentication is a function found on managed Ethernet switches and Routers. It interrogates the attached PC or Laptop and asks for a key and Password.
    b. Note that passive devices such as most of today's relays, controllers, I/O, sensors, etc. cannot participate in network authentication as they are not interactive with the network.
3. Remote Access-
    a. These access points can be protected with a multilayer strategy, using a VPN (Virtual Private Network) to protect the data and a firewall to protect the access to the protected domain. To enhance the monitoring, Intrusion Detection Services (IDS) are useful for monitoring the data movement in and out of the protected network.
4. Connections to existing corporate networks-
    a. Very similar to protected remote site access accept you do not need the VPN support, but firewalls and IDS support serve to close the holes.
    b. Also, the judicious use of VLANs (Virtual Local Area Networks) and routers creates logical networks within the physical environment that can also control access through the use of IP Access Lists on the Routers that can be used to connect these two networks together, even if both networks can be considered "protected".
5. Connections between protection and control networks across a network that is not under utility control-
    a. Back to remote site access protection, but the decision to use a VPN connection depends on level of trust the connecting network. Latency and robustness for mission critical functions should be investigated, and are often addressed with an Ethernet-over- TDM connection until speed, reliability, and security of Ethernet are demonstrated for wide area networks.
6. Devices like USB memory drives and PCs that may be infected with viruses that come into a secure area and inadvertently (or even on purpose) infect the control system architecture-
    a. Deny access of non-company machines to the protected network.
    b. Utilize an up-to-date virus scan system which can scan memory drives and PCs externally before they are connected.
7. Outright hacking either internal or external to the protected network-

a. Use the remote access protection strategy, and optionally add an IPS (Intrusion Protection Service) which not only detects unexpected and dangerous data, but also can act to stop the interference.

b. Define a Demarcation Point. If there is an issue coming from outside that cannot be resolved or stopped, physically disconnect the demarcation point. This will allow you to then fix what may have been damaged during the attack.

8. Disaster recovery-

a. Have a disaster recovery plan in place addressing major natural and man-made events which may disrupt centralized network services and automated access control mechanisms normally in place.

Figure 17 shows the same perimeter picture, but with the added tools to secure the holes and make the network secure.

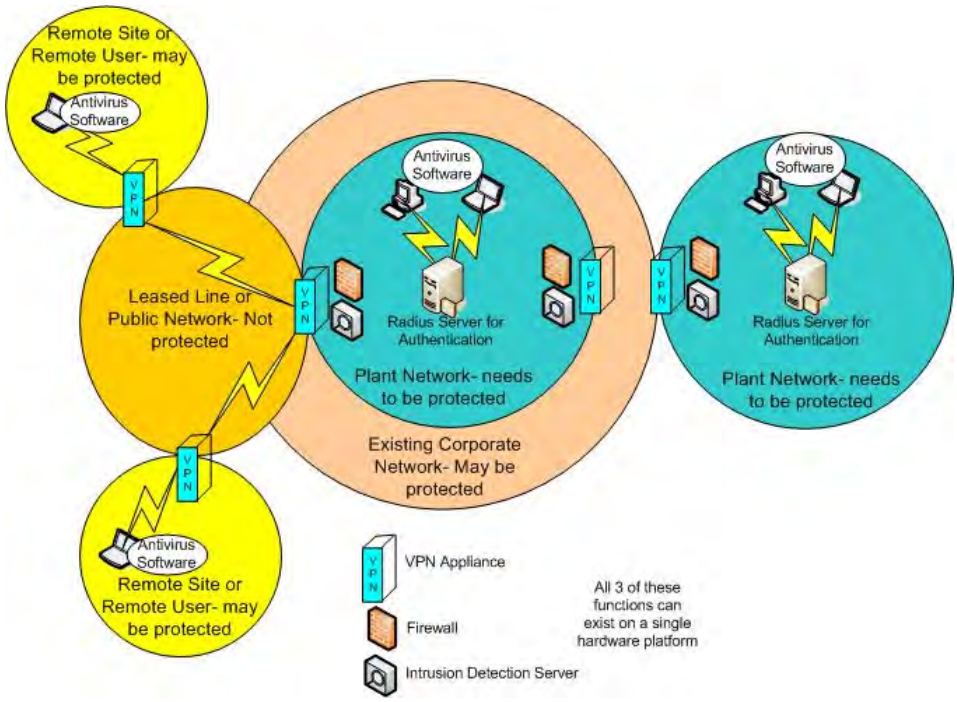

Figure 17 - The protected network perimeter

11. Ethernet network design for P&C communications

A substation LAN provides many benefits for protection and control (P&C) applications that will be discussed in this section. In the past, other high-speed LANs have been implemented in substations, but their benefit was not fully realized because a critical mass of equipment and usage was never attained. Prior to 2002, Modbus Plus was one high speed peer-to-peer LAN that was implemented by relay vendors, meter vendors, and PLC vendors and used by many

utilities. However, this LAN as well as other LANs had limitations that were ultimately surpassed by Ethernet.

11.1 Mix all types of messages and services.

With a LAN based upon Ethernet, it is possible to mix a wide variety of messages and services: data, management, time synchronization, remote access, and security. For the first time, one medium supports multiple protocols and multiple connections over the same physical interface.

Data collection and sharing uses protocols such as Modbus, DNP3, and IEC 61850. These protocols are used inside and outside the substation for SCADA data collection, where IEC 61850 also provides high-speed protection messages and other additional functionality not inherently supported by the other two protocols. See IEEE 1615 [18] for a more detailed comparison of these protocols. Other types of data connections may be supported by IEDs, such as data concentrators, such as OPC for data sharing.

In addition to these data protocols, Ethernet LANs also support other protocols that are used by substation IEDs in network management: SNMP is used for network management and monitoring and DHCP for IP address assignment.

Time synchronization is usually provided using IRIG-B signals; but for error tolerances of greater than 1 ms timing is also possible from Ethernet LANs using (Simple) Network Time Protocol (NTP/SNTP), which are time synchronization protocols that are supported by many IEDs (regardless of IEC 61850 implementation). The IEEE 1588-2008 Precision Time Protocol [28] with power profile per IEEE C37.238-2017 [24] is a recent standardized method that is expected to become widely used in the future as an alternate to both IRIG-B and NTP/SNTP; the first two both being able to provide the sub-microsecond accuracy needed for emerging synchrophasor applications. Note that whereas the separate cabling for IRIG-B makes it very secure, a transition to 1588 will need an assessment of its vulnerability to security threats; e.g. its transport on a dedicated VLAN can isolate all threats. In 2017 the original IEEE C37.238-2011 is being superseded by a split into an IEC-IEEE joint base profile IEC/IEEE 61850-9-3 [23] plus a revised IEEE C37.238-2017 [24] extended profile (for support of IEDs needing a real-time indication of the time quality (inaccuracy), and for support of 1588-to-IRIG protocol converters (needed for legacy IEDs requiring an IRIG source).

Remote access to IEDs is supported on Ethernet using a protocol such as Telnet, which is widely supported by IEDs. While Telnet provides a direct interactive terminal interface to the IED, vendor software configuration tools can give a similar experience through the use of configuration software that uses other protocols to communicate with the IED. Another form of remote access is the transfer of configuration or other files from the IED using FTP/SFTP. Another method of remote access is through a web server on the IED, where read only and sometimes read/write access is allowed from this interface in the IED.

Security services are also supported by a substation Ethernet LAN. Some of these security services are VPN, authentication, and encryption. Security services must be implemented on a

substation LAN in order to adequately limit the cyber vulnerabilities that lead to cyber-attack of the IEDs and network itself.

11.2 Listing operational and non-operational data traffic

The protocols and services listed above represent both operational and non-operational data. Operational data includes traditional SCADA protocols that transmit typical substation status, analogs, and accumulator data as well as provide remote control. This data is typically breaker/switch/transformer/capacitor status/control/loading as well as additional metering data such as accumulators. Typically, operational data represents less than 10% of the total data available from a substation.

Non-operational data includes items such as fault records, event records, COMTRADE files, configuration files, event reports, and other IED files and reports; plus data available from the substation IEDs such as targets, breaker wear, fault location, power quality, substation equipment monitors (breakers and transformers).

See IEEE C37.1 for different system architectures for obtaining operational and non-operational data. Typically, operational data goes back to the SCADA master and non-operational data goes back to the Enterprise because SCADA masters operate over limited bandwidth that do not handle well the many types of non-operational data.

IEEE 1615 [18] includes a table that shows how substation data (operational, non-operational, and control) are used by different utility departments.

11.3 Matrix of the types of traffic & characteristics

Operational data should be delivered reliably and continuously so that the power network can be properly managed during normal and emergency conditions. Control (here included as operational data) requires secure, reliable, and timely delivery and feedback. Typically this is in the order of seconds outside the substation to milliseconds inside the substation for high-speed protection messages using IEC 61850.

Non-operational data may have similar requirements as operational data, but can usually be delayed or interrupted while operational data is being transmitted over the network. Update times can range from minutes to hours to days depending upon the application.

11.3.1 SCADA and data gathering messaging

Data collection typically occurs using a SCADA protocol. See IEEE C37.1 for different ways data collection can occur. Traditional data collection occurs via master/slave; typically a slave may only respond when polled by the master or the protocol may allow for a slave to send a message to the master without being polled. Data collection has advanced to a client/server or subscriber/publisher models. Peer to peer networks are also possible.

As the number of data points being transmitted increases, more bandwidth is required. As the collection interval decreases (or polling gets faster), more bandwidth is required. Serial networks are typically limited to speeds below 1 Mbps, and most are implemented at or under

19,200 bps. This limits the amount of data and the frequency that data is updated. Serial network loading due to data and polling cycles is such a concern that IEEE C37.1 includes an annex showing how to perform bandwidth calculations.

With Ethernet, bandwidth is less of a concern because it is normally 10 Mbps or higher and is full duplex, allowing simultaneous transmit and receive. The design limitation typically turns from bandwidth limiting the number of points and polling frequency to the processing power of the master to handle thousands of points coming back from each IED.

Substation Ethernet networks have significantly different requirements than typical enterprise networks. An enterprise network is used for email, printer services, file transfer and other applications that are not Real Time. In contrast, a substation network has critical data that is often Real Time. Data for SCADA systems is typically delay sensitive and GOOSE messages are also delay sensitive. What does this mean to the actual substation network? This means that the data flowing through a substation network is more critical than data in an enterprise network. Networks that run critical data must have a requirement for high availability and no single point of failure. For protective relaying of critical bulk electric system components, NERC may eventually require at least dual redundant designs with no single point of failure that could disable both the primary and backup protection functions shown in Figure 3.

To do this we must design a network with redundancy at many levels. Power supplies, power sources, equipment redundancy and diverse paths for cabling are all important considerations for a high availability network. Network equipment with redundant power supplies that can be connected to separate power sources are an important step to building a fault tolerant redundant network. A single point of failure analysis is a good way to analyze a network design. For example if you have a switch with dual ac power supplies and you plug them into outlets that feed back to the same breaker that breaker becomes a single point of failure that can bring down a network that requires high availability.

Ring topology provides two paths across the network, clockwise and counter clockwise. If a cable is cut then there is an alternate path available in the opposite direction. Rapid Spanning Tree Protocol (RSTP) explained in Section 4 allows the use of ring network topology while preventing packet traffic that circulates in the ring forever. Section 4.6 also describes new PRP and HSR methods to control circulating traffic while avoiding a bump in traffic flow during detection and failover, although the RSTP bump time can be in tens of milliseconds and not a real concern when redundant systems are in service during the bump time. Another important step is path diversity. Path diversity requires that cabling between switches is not run in the same conduit or cable raceway. When all of these considerations are taken into account the result is a resilient network that has been optimized for high availability.

11.4 Model the worst case

The design of a substation network that will be used to transport protection and control information must consider the following critical points for the highest possible network

availability with minimum impact on response time. Depending on the degree of importance, the designer must consider various levels of redundancy as follows:

- Equipment power supplies – Network equipment with dual power supplies able to connect to AC and DC sources simultaneously
- Power sources – Considerations must be given to have both AC and DC power distribution
- Equipment redundancy – Dual networks
- Network topology – Ring topology with path-failure protection (e.g. using RSTP)
- Cable routing – Communication cables running in separate cable raceways
- Network response time – Necessary to estimate additional latency introduced by the network

One of the most difficult decisions to be made during the network design is the level of redundancy, particularly in cases where the P&C system includes Protection A and Protection B as shown in Figure 3 of Section 4. The designer must consider then:

- Network equipment with dual power supplies fed from two separate dc (or uninterruptable ac) distribution systems.
- Two communications networks one for each Protection System
- Each network including ring topology with path-failure protection

The level of network complexity is dictated by the type of information that will flow, which could be a combination of the following data, listed from the most to the least critical:

- Peer-to-peer communications - IEC 61850 GOOSE messages used for:
    - Protection interlocking
    - Transfer commands
- Remote control commands for:
    - Equipment operation
    - Protection blocking / enabling
- System status – equipment status, alarms
- Real time metering
- Oscillography and SER retrieval

The simplest network will be the one used to transport non critical information such as real time metering, and oscillography and SER retrieval. Once the network is used to transport system status, commands and peer-to-peer communications, the engineer must consider a high level of

redundancy as indicated above and possibly the use of VLANs for an efficient and secure network.

Once the network components and network topology have been selected, one must then analyze how it will affect the performance of protection and control system under several scenarios, deciding what will be the course of actions that will take place under each condition and calculating, if possible, the potential additional response time imposed by the new network.

A total network failure should also be considered since critical signals will probably be lost under extreme system failure including a possible total shut down produced by auxiliary digital outputs at Ethernet switches and / or Routers. The outputs are used in a hardwired emergency shutdown sequence.

A protection and control engineer should not be surprised by the complexity and the number of possible scenarios that should be analyzed. If engineers spend time and money doing real time simulation studies for important and complex protection systems, they should also allocate resources to perform network failure analysis to determine the implications that the network will have in the performance of the protection and control system. The following is a possible list of network simulations that must be performed:

- Response under heavy traffic
- Path-recovery response time (e.g. RSTP) under link failures - this may involve several scenarios depending on the network topology
- GOOSE message response time under link failures – this may involve several scenarios depending on the network topology
- Protection and Control system response under a partial network failure
- Protection and Control system response under a total network failure

The last two points should be done taking into consideration P&C functional logic and possibly relay settings and functional schematics. The number of scenarios is directly related to the complexity of the P&C System as well as the traffic of GOOSE messages in the network.

With the network and considering the P&C functionality, one can then point out possible scenarios to be analyzed in order to ensure a reliable P&C system based on a highly available network

11.5 Latency control

Latency is the time it takes data to get from the source to the destination. Every switch introduces latency and the latency is cumulative for every switch that must be traversed. Latency can be broken down to switching latency, frame, and queuing latency. Switching latency is the latency that a switch adds in processing the frame and frame latency is the time to read the frame. There are two types of switching - cut through switching and store and forward switching. Cut through switching starts to switch the frame as soon as the 6th octet containing

the destination address arrives and it introduces a frame delay of 4.8 µs for a 100 Mbps link. Store and forward (the more common choice) receives the entire frame before it switches and verifies the Frame Check Sequence (FCS), if the FCS is corrupt the frame is discarded. Because it receives the entire frame before switching and frame sizes can vary from 64 to 1516 bytes on a 100 Mbps link the frame delay can vary between 5 µs and 120 µs. Queuing latency is the time for which the frames are stored in a device's egress port queue (how long it takes to egress the existing queue's frames).

The requirements for message latency are application dependent, the most critical being typically less than 5 to 8 ms for teleprotection circuits. The latency impacts tripping time, and the maximum acceptable value depends on the criticality of tripping speed in a particular application. In addition, 87L also requires that the asymmetry of latency between the two directions always be less than 3 ms (unless external time synchronization of compared current values is used). Note that 3 ms asymmetry may be the worst tolerable value in an 87L application with no other error sources; allowance for CT and other measurement errors suggests a lower asymmetry limit of 1 ms or less [25].

Bandwidth is a choice that must be made when designing the network. Common Ethernet bandwidths are 10 Mbps for the 10 base (TX/FL) standard, 100 Mbps for the 100 Base (TX/FX) or 1000 Mbps for the 1000 Base (TX/LX). The best way to determine the required bandwidth is to understand all of the traffic types on the network and add up the bandwidth that is required and add extra for future requirements. Then match the bandwidth required with the available choices. A typical design limit is 80% duty cycle maximum on a link. However, aiming for a much lower value like 10% to 20% in a LAN environment allows for future function additions that come rapidly in networking technology.

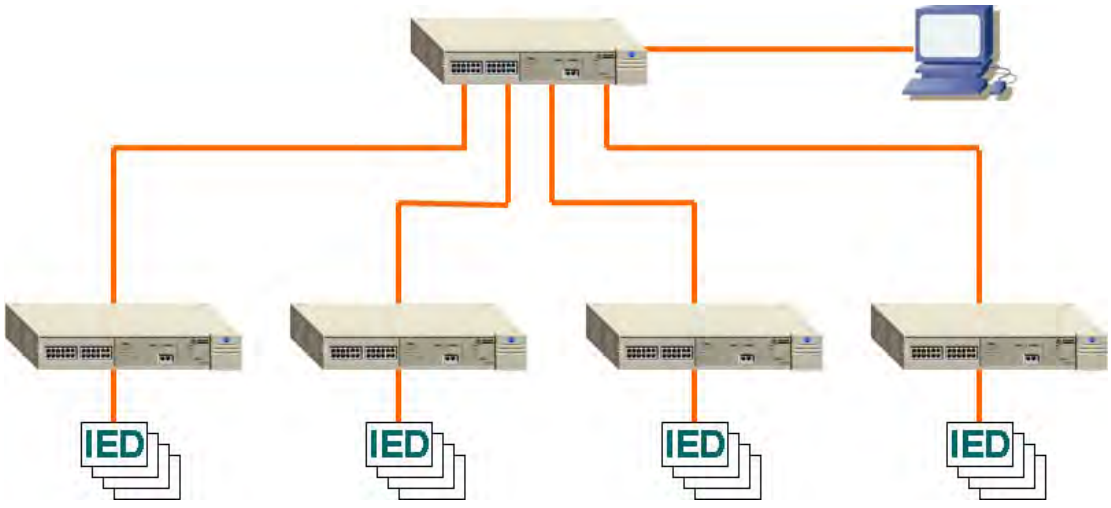

Figure 18 - Calculating latency for a star topology

The minimum latency for GOOSE messages between IEDs for a store and forward switch. Processing latency + frame latency = total latency. For maximum, add the queuing latencies.

5 *µs* x 3 (switches) + 120 *µs* x 3 (switches) = 375 *µs* best case from any IED to any IED.

11.6 Examples of packet delays

At each egress switch port, a high-priority packet may have to wait for a maximum-length lower-priority packet to egress; a 1518 byte packet takes 122 µs at 100 Mbps and 12 µs at 1 Gbps.

A potential 2 ms extra delay could therefore be incurred for a network path comprising 16 hops if at 100 Mbps or for 160 hops if at 1 Gbps.

At each egress switch port, a high-priority packet may also have to wait for many other high-priority packets to egress; a 600 byte packet (typical for GOOSE) requires 48 µs at 100 Mbps, 4.8 µs at 1 Gbps.

A potential 2 ms extra delay could therefore be incurred for an event-triggered burst of 40 GOOSE packets if at 100 Mbps, 400 packets if at 1 Gbps.

11.7 Features for verification of performance & troubleshooting

Once the network has been installed connectivity to every device must be verified. For layer-3 devices the ping utility is useful in testing connectivity. Initiate a ping to every device within the VLAN under test. Any device that does not respond needs to be investigated. First verify the cabling of any device that does not respond. Next verify that link light is on at both devices at the either end of the cable. After the link light has been checked verify that the correct IP address, subnet mask and gateway are configured in the suspect device. Next initiate a ping from the suspect device to the next directly connected device. If the ping fails verify the configuration on the switch, check for proper VLAN configuration and speed and duplex configuration. If the ping is successful initiate a ping to the next device connected and repeat the above steps to isolate and repair the problem.

11.8 Calculating capacity on parts of the network

Managed Ethernet switches collect information about the traffic flowing through them. There will be Ethernet statistics that are available on a per port basis. These statistics will be able to provide link utilization performance data. The installation should include a network management function that gathers performance statistics to ensure that:

- All network segments are operating well within capacity at all times.
- No part has failed, degraded, or been adversely impacted by the appearance of new types of message traffic.
- Failures are reported and alarmed for quick maintenance attention.

11.9 Expansion, reconfiguration, migration impacts

Expansions and changes occur in any network over time. While the network is being reconfigured the goal is to minimize downtime. Additions where there are available switching capacity (unused switch ports) are extremely easy, just install and configure the device and connect the cable to the switch. If the port was disabled it will need to be enabled and

configured for the appropriate VLAN if VLANs are used. If there are no spare switch ports available a new switch will be required to meet the new requirements. The switch should be preconfigured to minimize downtime during the installation. Physically install the switch and power up the device. Then disconnect the cables on the existing switch where the new switch will be connected and insert the switch into the network. Now any new devices can be connected and downtime has been limited to the time necessary to connect the switch.

11.10 Auto-Negotiation settings on ports

While managed Ethernet switches have the ability to auto-negotiate speed and duplex it is a good practice to manually configure those setting on a per port basis to eliminate any chance of an incorrect auto-negotiation.

As already mentioned in Section 7.10, if only one end has this feature enabled, it is likely that this end will think it has a half-duplex connection even if the other end is set to a full-duplex connection.

11.11 Use of VLANs

A Virtual Local Area Network (VLAN) is a logical grouping of two or more devices. See Section 7.5 above. When VLANs are introduced, all traffic in the network must belong to one or another VLAN. Traffic on one VLAN cannot pass to another, except through an intra-network router or layer 3 switch. In a substation environment VLANs can be used to segregate traffic types. For instance the user can assign all of the relays on a VLAN and have a separate VLAN for substation CCTV cameras. This will keep the multicast traffic from the traffic being received by the relays. It can also guarantee that rogue messages from a malicious hacker cannot interfere with critical traffic.

Switches can operate in two different modes VLAN aware and VLAN unaware. VLAN aware mode is the standard 802.1Q VLAN and the VLAN IDs can take on values of 1-4094. VLAN unaware mode is a result of some IED vendors that used the 802.1p priority field to prioritize the GOOSE messages. Some of these set the VLAN ID to 0 which violates the IEEE Ethernet 802.1Q standard. So if the VLAN ID cannot be changed to a standard value, VLANs cannot be used. VLAN unaware mode allows the VLAN tag to pass through the network unchanged so the 802.1p portion of the tag can still be used to provide Class of Service to the GOOSE messages.

11.12 Use of priority

There are several ways to prioritize traffic in a managed switch. See Section 7.4 above. Traffic can be prioritized based on the ingress port, by the priority field in the 802.1Q tag, by the source or destination MAC address, and by the TOS field in the IP header. Managed switches have multiple output queues that are each assigned a different priority such as high, medium and low. The queues are emptied in order high first then medium and then low. The queues can be filled based on the 4 different methods above. An intelligent IED can have the ability to set the priority field in the 802.1Q tag or TOS field in the IP header. In this case the switch will read the field and en-queue it to the appropriate queue. For IEDs that don't have the ability to set the

priority field they can be prioritized by either using their MAC address or configuring the switch to prioritize all traffic coming in on a specific port to be set to a specific queue. For example the traffic arriving on switch port 1 is en-queued to the high priority queue and the traffic arriving on port 2 to the medium priority queue. This mechanism allows the important time sensitive traffic to have priority throughout the network. Since not all switches support all of the 8 priority settings provided by 802.1Q tags, the user should ensure that the switches chosen provide the quantity desired.

12. Intersubstation P&C applications

While SONET or SDH communications multiplexers provide the majority of intersubstation P&C data communications today, there is increasing standardization work and experimentation with the use of Ethernet networking approaches.

Applications for this transport include pilot or unit protection of transmission lines, transfer tripping, and remedial action schemes (RASs) or System Integrity Protection Schemes (SIPS). More recently, utilities seek to stream synchrophasor values at a rate of 30 to 120 sets per second over wide-area networks for mission critical power system control applications. Latest-generation IEDs have recently demonstrated real-time wide-area streaming of instantaneous measurements at a rate of 1 million 6-channel sets per second.

Tripping signals or GOOSE messages are being transmitted today over physically large LANs as described in Section 12.1.

IEC Technical Report 61850-90-1 [11], *Use of IEC 61850 for the communication between substations*, explains how to map whatever communications are available – Ethernet or legacy – into IEC 61850 based P&C systems in substations at the two ends of a transmission line or associated communications path. It includes tunneling of Ethernet LANs through router configuration, as well as modeling of other communications such as power line carrier with a few binary I/O states communicated for protection.

With synchrophasor measurements, analog values from around the system are time-correlated to within less than a microsecond using GPS or Ethernet network coordination of timing across the region. Along with synchrophasor definitions and measurement techniques, IEEE C37.118-2005 describes a streaming communications protocol for synchrophasor values based on manual configuration and serial or Ethernet data paths.

More recently, IEEE has split the C37.118-2005 synchrophasor standard into a new measurement-only part C37.118.1-2011 and a communications-only part C37.118.2-2011. In parallel, the IEC 61850 development working group has created a new transport protocol described in IEC Technical Report 61850-90-5[14] that is compatible with IEC 61850 systems and configuration methods. The measurements can be synchrophasors or any other streamed data types. The transport mechanism is a new pair of services – wide-area Ethernet network routable GOOSE (R-GOOSE) and routable Sampled Values (R-SV) services. Whereas 61850-90-1 uses special router configuration and optional encryption to transfer GOOSE over SONET/SDH

WAN links, IEC 61850-90-5 provides a service that naturally and easily transports such information across the WAN in an IEC 61850 format using standard router services. Among the features of IEC-61850-90-5 transport are:

- Layer 3 UDP/IP multicast passes readily through routers and across WANs.
- Using the IT-standard router service Internet Group Management Protocol (IGMP) Version 3, subscribing IEDs and their routers can automatically locate the publishers they seek even when separated by an arbitrary WAN having multiple hops.
- A standard encryption technique is defined.
- R-GOOSE and R-SV message packets are enhanced with a key-based high security (Secure Hash Algorithm or SHA-256, also called SHA-2) authentication signature to foil spoofing or substitution disruptions.
- Management of the ongoing distribution of security keys to approved publishers for use in creating authentication signatures employs the IT-standard Group Domain of Interpretation (GDOI) key distribution center process.

With convenient auto-configure routing using standard IT equipment, leading-edge security features, and compatibility with the IEC 61850-6 configuration process, IEC Technical Report 61850-90-5 is an excellent solution for phasor streaming and wide-area GOOSE control. However, the technical report was published in 2012, and corresponding normative or standard requirements for R-GOOSE and R-SV are just now being added in Amendment 1 of IEC 61850-8-1, resulting in Edition 2.1. These requirements will have to be implemented in products. Furthermore, IED manufacturers are just introducing new communications processing platforms that can handle the complex authentication hash code calculations at high speed. Trial products are emerging, and fully compliant products will become available over time. Thus, TDM solutions cannot yet be widely replaced with those using IEC 61850-90-5 Ethernet WAN transport. One temporary workaround in use for now is to use the methods of 61850-90-5 with the authentication fields populated with dummy data (and without the security benefits of authentication).

12.1 LANs of large physical extent

Communications between substations are sometimes provided using only LAN facilities. Links in a LAN may be implemented over long distances with channels in wide area communications equipment such as T1 on SONET or microwave. These can function just like a LAN within a building – the wide area connections simply transport the packets over long distances. These do have limited data rates and add some latency (typically 5us/km) compared to local fibers.

12.1.1 Ethernet over SONET

Traditionally SONET has been used in inter-substation WAN configurations while Ethernet is being used in intra-substation or LAN configurations. The desire to link Ethernet LANS together over the SONET WAN is commonly referred to as Ethernet over SONET (EoS). The object of EoS

is to provide an efficient bandwidth pipe that is transparent for Ethernet traffic. There are several technologies used in EoS to encapsulate the packetized data and efficiently transport it over SONET. These technologies include Virtual Concatenation, Link Capacity Adjustment Scheme and Generic Framing Procedure.

12.1.2 Virtual Concatenation (VCAT)

The first issue to address is that Ethernet rates differ from traditional SONET input rates. VCAT allows for non-standard SONET/SDH multiplexing in order to address the bandwidth mismatch problem. Using virtual concatenation, the SONET/SDH transport pipes may be right-sized for Ethernet transport. VCAT is a technique that allows SONET channels to be multiplexed together in arbitrary arrangements. This permits custom-sized SONET pipes to be created that are any multiple of the basic rates. Virtual concatenation is valid for STS-1 rates as well as for Virtual Tributary (VT) rates. The SONET pipe size may be any multiple of approximately 50 Mbps for high-order virtual concatenation (STS-1) or 1.6 M b/s (VT1.5) for low-order virtual concatenation. The table below compares the typical Ethernet rates versus the SONET rates using virtual concatenation.

Ethernet Bit Rate	SONET Rate	SONET Effective Payload Rate	Bandwidth Efficiency
10 Mbps	7 VT1.5s	11.2 Mbps	89%
100 Mbps	2 STS-1s	96.77 Mbps	100%
1 Gbps	21 STS-1s	1.02 Gbps	98%

Table 11-1 – Ethernet on SONET

The plurality of Ethernet pipes within a SONET payload allows the assignment of separate pipes for the different classes of inter-substation traffic applications, allowing not only the optimum pipe bandwidths, but more importantly the complete isolation of critical traffic (e.g. protection) from the typically-unknown traffic of the other applications. This assured determinism for mission-critical applications explains why the SONET/SDH transport technology has a healthy survival despite the major inroads of Ethernet (typically using MPLS transport) for telecommunications industry transport.

12.1.3 Link Capacity Adjustment Scheme (LCAS)

Ethernet traffic may be created in bursts, and therefore the amount of bandwidth required can vary. The principle behind LCAS is the ability to dynamically change the amount of bandwidth used for a virtual concatenated channel. Using Link Capacity Adjustment Scheme (LCAS), signaling messages are exchanged within the SONET overhead in order to change the number of tributaries being used by a Virtually Concatenated Group (VCG). The number of tributaries may be either reduced or increased, and the resulting bandwidth change may be applied without loss of data in the absence of network errors. This feature is unlikely to be used for the static paths of substation traffic.

12.1.4 Generic Framing Procedure (GFP)

GFP is the protocol for mapping packet data into an octet-synchronous transport such as SONET. GFP uses a cell delineation protocol to encapsulate variable length packets. A fixed amount of overhead is required by the GFP encapsulation that is independent of the contents of the packets which allows deterministic matching of bandwidth between the Ethernet stream and the virtually concatenated SONET stream. Within GFP, there are two different mapping modes, one uses frame based (GFP-F) mapping and the other uses transparent (GFP-T) mapping. Each mode has different characteristics

GFP-F supports variable-sized packet lengths of framed data, where one frame maps directly into one GFP-F frame. In order to support the frame delineation mode utilized within GFP, the frame length must be known and pre-pended to the head of the packet. In many protocols, this forces a store-and-forward encapsulation architecture in order to buffer the entire frame and determine its length. GFP-F incurs higher latency through the system, because complete frames must be buffered before transmission.

GFP-T supports fixed-sized packet lengths and transports block-coded constant rate bit streams. This generates a GFP frame that encapsulates block coded data, which contains the client protocol 8B/10B data and control (symbols) that are mapped to 64B/65B block codes. The transparent-mapped protocol does not require that application buffers complete frames before transmission. Instead, both data and control symbols are accumulated. Eight 8B/10B symbols (plus a flag bit) are combined to create a 64B/65B block code. This block code will include both data words and control characters.

The selection of GFP-F versus GFP-T depends on the application and system requirements. GFP-F provides bandwidth efficiency by ensuring that only actual data is transmitted, whereas GFP-T transmits all information including data, framing codes, preamble, and idles.

GFP-F incurs higher latency through the system, because complete frames must be buffered before transmission. GFP-T does not require complete frame transmission, and therefore can achieve lower system latencies.

12.2 Ethernet over direct fiber ring or mesh

It has been traditional to use fiber to interconnect devices on a LAN where it is desired to provide a network that is very secure and not prone to lost packets due to high surge noise in a substation. In a LAN environment, communication between devices on the LAN is usually done at a layer two level. Since packets at the layer two level do not have an IP address (layer three) attached to them they are not routable outside the LAN. Thus, because these packets don't pass through a router they are never seen by anyone connected to the LAN via a router. The communication between devices can therefore be very secure.

There is no reason why this same concept cannot be applied to a multi-station LAN. If one is interested in connecting two or more substation LANs together using fiber optics it can be done in a secure manner. This would be advantageous for a network that is used for protection and

control information. In this manner protection and control devices can communicate with each other via the extended LAN at the Layer 2 level.

If it is desired to make data from devices on the multi-station LAN available to some corporate offices then a multi-station LAN could also have a single point of entry into the LAN. Any one of the substations on the multi-station LAN can be used to place a secure router/firewall to be connected either to the corporate network or to an ISP for internet access. This would provide access without compromising the security of communications between devices communicating on a layer two level.

12.3 IEC 61850 GOOSE tunneling

IEC 61850 GOOSE uses Layer 2 multicast frames to distribute its messages and hence is incapable of operating outside of a switched Ethernet Network. GOOSE tunneling provides a capability to transfer GOOSE frames over a wide-area network (WAN) in a pipeline isolated from other traffic.

A key feature of a tunnel is that it does not interact with configuration of IEC 61850 GOOSE associations – it pipelines the GOOSE message from one physical LAN to another such that the LANs are functionally connected for the tunneled GOOSE.

GOOSE tunnels pipeline the selected GOOSE traffic over the WAN via an encapsulating or tunneling protocol which may be based on standards or may be proprietary. At the GOOSE publishing LAN or VLAN, the router inspects the Media Access Control (MAC) destination address of frames received from Ethernet to determine which GOOSE group they are in. The GOOSE messages to be tunneled can also be identified from their VLAN. The frames to be tunneled are encapsulated in WAN headers and forwarded (with MAC source and destination addresses intact) to the remote physical LANs, where routers remove the WAN headers and forward the unmodified GOOSE messages.

One GOOSE traffic source can be mapped to multiple remote router Ethernet tunnel interfaces. When Virtual Router Redundancy Protocol (VRRP) is employed, GOOSE transport is improved by sending redundant GOOSE packets from each VRRP gateway.

IEC 61850 recommends that the MAC destination address should be in the range 01:0c:cd:01:00:00 to 01:0c:cd:01:01:ff (but this is not a requirement).

GOOSE Packets received from the WAN, after being stripped of their network headers, are forwarded to Ethernet ports configured for the same multicast address. The forwarded frames contain the MAC source address of the originating device, and not that of the transmitting interface. The VLAN used will be that programmed locally for the interface and may differ from the original VLAN.

By contrast with a GOOSE tunnel, a device on the LAN which recognizes or interprets the GOOSE message on the LAN where it is published and *reproduces* it in a format to be transmitted over the WAN is a *gateway*. Gateways interact with GOOSE configuration, and need to be reconfigured if the GOOSE configuration is changed.

13. Standards for communications performance

13.1 IEC 60834-1 requirements for security and dependability of protection

For the various protection schemes, the CIGRÉ brochure TB192 “Protection using Telecommunications” (2001) addresses the requirements from protection on the teleprotection interfaces and the communication channels.

The term “teleprotection” refers to the equipment needed to interface the protection equipment to the telecommunication equipment; for IEC 61850 systems this would comprise the equipment generating and processing the Ethernet packets for the protection functions (e.g. GOOSE).

(Non-protection IEC 61850 functions are far less critical, e.g. delivery times of an order of 1 second for SCADA functions may be tolerable.)

13.2 Security requirements of protection schemes, from CIGRÉ and IEC

The security requirements from protection on telecommunications, per Tables 6-1-1 and 6-1-2 in the CIGRÉ TB192 vary from “medium” to “high”, with a reference to IEC 60834-1.

The IEC 60834-1 Figure 21 shows that the probability of an unwanted command (from an error burst) should be less than 10^{-4} (for blocking pilot schemes) through 10^{-8} (for intertripping or transfer tripping schemes). An “unwanted command” is a message that would result in an undesirable event, such as a false trip.

Therefore the telecommunication network is required to have an unwanted-message probability of lower than 10^{-8} (for intertripping protection schemes).

For security against corrupted frames, the CRC-32 frame-integrity check appended to each Ethernet frame meets the 10^{-8} requirement for bit errors.

For security against rogue frames emulating protection messages, the network must be engineered for this purpose (e.g. by using VLANs reserved for protection messages). See Section 10 on Ethernet network security.

13.3 Dependability requirements of protection schemes, from CIGRÉ and IEC

The dependability requirements from protection on telecommunications, per Tables 6-1-1 and 6-1-2 in the CIGRÉ TB192 vary from “medium” to “high”, with a reference to IEC 60834-1.

The IEC 60834-1 Figure 21 shows that the probability of a “missed command” (from a 10^{-6} continuous BER) should be less than 10^{-2} (for permissive-underreach schemes) through 10^{-4} (for intertripping schemes).

The IEC 60834-1 Figure 21 also shows that the “maximum actual transmission time” (called transfer time in IEC61850) should be less than 10 ms for all the protection schemes.

Therefore the telecommunication network is required to have a greater than 10 ms message latency probability of lower than 10^{-4} (for intertripping protection schemes).

For dependability against fiber failures causing an excessive delay of protection messages, the network must be engineered for this requirement (e.g. by using a failure-recovery technology with less than 10 ms interruption, or by using a dual-path topology).

For dependability against network traffic causing an excessive delay of protection messages, the network must be engineered for this requirement (e.g. by assuring that the highest-priority queues are reserved for protection messages); more quantitative description of these delays are given in subsections of Section 11.

14. Installation and environment for substation networks

14.1 IEEE 1613 environmental requirements

There is a view in some quarters that, except for temperatures, that the environment in a substation control house is the same as in a commercial office. Nothing can be further from the truth. Even though there may not be direct exposure to the electrostatic and electromagnetic fields from high voltage busses (no close proximity) in a control house, there are environmental conditions that must be considered in selecting communications networking equipment. These are described in IEEE 1613 Standard Environmental and Testing Requirements for Communication Networking Devices in Electric Power Substations [16]. They include the transient voltages on the CT or VT wiring from switching operations in the high voltage yard, transient voltages on relay panel wiring due to operation of dc control devices on the panels, and electrostatic discharges from human interaction with non-conducting flooring material. IEEE 1613 defines the required tests for all these transients, and describes two classes of possible compliance.

Class 1: This performance class is for communications devices used for general-purpose substation communications where temporary loss of communications and/or communications errors can be tolerated during the occurrence of the defined transients. IEEE 1613 states that all devices shall meet Class 1 requirements unless Class 2 is specified by the user or manufacturer.

Class 2: This performance class is for communications devices used in substation communications where it is desired to have error-free, uninterrupted communications during the occurrence of the defined transients. The practical effect of requiring Class 2 is that all communications traffic must be carried on fiber optic cable, as no practical shielding of copper cables is effective against the defined transients.

In addition, because substation control houses may not be heated or cooled (or that equipment may fail) the minimum operational temperature range of devices that meet IEEE

1613 is – 20 degrees C to + 55 degrees C. Other more severe temperature ranges may also be specified. Operational temperature is defined as "the temperature of still air (i.e. no fans or forced-air movement) measured 30 cm from the surface of the unit (communications networking device) enclosure while in operation". For a specified temperature range (for example, -20˚ C to +55˚ C), a unit shall be able to start up and continue its operation at the specified minimum temperature (i.e. –20 ˚C) within five minutes after having been de-energized for a sufficient time such that its internal components have cooled to that temperature without condensation. A unit shall also be able to start up and continue its operation within five minutes at the specified maximum temperature (i.e. +55 ˚C) after having been deenergized for a sufficient time such that its internal components have heated to that temperature.

14.2 IEC 61850-3 Edition 2 general requirements of communication network and systems in substations

This standard [27] specifies general requirements for communications networks in a substation automation system with emphasis on maintaining high quality of service during adverse environmental and power supply conditions. The following requirements apply:

1. *Reliability*: The substation needs to operate according to "graceful degradation" principle if any of SAS communication component fails. The standard requires users to take into account the redundancy factors in communications and power supplies in order to prevent single point of failure in communications. While redundancy is not mandatory for all substation applications, importance of the substation and the specific application has to be considered while deciding on redundancy. For example, communications system in extra high voltage transmission substations would be considered more critical requiring higher degree of reliability than medium voltage distribution substations. Similarly, communications systems for substation protection applications would require a more fail-safe architecture than monitoring applications. The standard requires users and manufacturer to agree upon reliability class severity (R1, R2, or R3) as described in IEC 60870-4. These reliability classes are based on MTBF of the equipment application reliability needs.
2. *System availability*: Availability is measured by the ratio of uptime to the total time wherein substation automation system is able to perform its critical functions. The standard requires users and manufacturer to agree upon availability class severity (A1, A2, or A3) as described in IEC 60870-4. The function availability depends on the architecture of Substation Automation System. For example, if the system designed to be completely redundant and one of the components fail in the main system, the system function will still be available 100% in the backup system.
3. *Maintainability*: The standard requires user and manufacturer to agree upon maintenance class severity (M1, M2, M3, or M4) as described in IEC 60870-4.
4. *Security*: Requirements stated in IEC 60870-4 need to be followed.

5. *Data Integrity*: Data Integrity has to be ensured in a congested network and noisy substation environment. The standard requires users and manufacturer to agree upon integrity classes (I1, I2, or I3) as described in IEC 60870-4 which is based on MTBF of the equipment.
6. *General network requirements*: The communication network should have enough bandwidth to serve typical substation configurations, and it should be able to expand up to 2 km in order to cover the entire substation area.

For environmental requirements, the standard refers to IEC 60721-3-3, IEC 60721-3-4 and IEC 60870-2 and lists number of performance classes and severity levels of environmental climate conditions:

Weather protected locations:

- Class A: Air-conditioned locations
- Class B: Heated and/or cooled enclosed locations
- Class C: Sheltered locations

Non-weather protected locations

- Class D: outdoor locations

The manufacturer is required to specify the equipment conformance to the performance class and severity levels as specified in IEC 60870-2-2:

1. *Temperature*: Performance classes for air temperatures range from -50°C to 70°C. Separate performance classes are specified while transporting and storing the equipment. These air temperatures range from -65°C to 85°C and depend on whether ventilated enclosure is provided.
2. *Humidity*: Performance classes for relative humidity levels range from 5% to 100%.
3. *Barometric Pressure*: Performance classes for air pressure ranging from 70kPa to 106kPa. Requirements specified in IEC 60694 need to be followed when the communication equipment forms an integral part of high voltage switchgear and control gear.
4. *Mechanical and Seismic*: Due to diverse mechanical and seismic conditions, national and international standards according to the needs of the location/application have to be followed. When applicable, performance class as specified in IEC 608702-2 can be followed. These list the severity levels for stationary & sinusoidal vibration, shock and free fall conditions. IEC 60255-21-3 is referred for performance classes in seismic activity.
5. *Pollution and Corrosion*: This standard refers to guidelines in IEC 60654-4 for pollution, corrosion, and erosion influences on communications equipment.
6. *Electromagnetic Compatibility*: Communication equipment in a substation are exposed to various types of electromagnetic inference from electrostatic discharges from personnel to equipment, magnetic interference due to nearby current carrying conductors, radio frequency inference from hand-held devices and inference from

lightning & switching surges. The standard requires tests to be performed on a communication equipment as per IEC 61000 standard subparts - voltage levels of electrostatic discharge, fast transient/burst signals, surges, common mode immunity, ripple, oscillatory wave amplitude and ac/dc power supply variations/interruptions, and electromagnetic radio frequency fields of steady state and damped oscillatory signals.

7. *Dielectric Strength*: Power supply voltages in a substation environment vary during operation due to motor start-up, switching, and disturbance conditions. Since the communications equipment has to withstand over or undervoltages from its auxiliary supply, the standard requires that communications equipment be tested for a range of voltages and tolerances as described in IEC 60870-2-1.

15. IT engineering and management needs for P&C experts

As the communication networks are integrated into the electric system operations, protection and control, it is critical to build a basis of communication between multiple disciplines within the engineering community. To aid in the development of this understanding IEEE developed Standard 2030-2011, the IEEE Guide for Smart Grid Interoperability of Energy technology and Information Technology Operation with the Electric Power System (EPS), End-Use Application, and Loads. More recently, an IEEE PES working group has developed the application-specific guidance document 2030.100, *IEEE Recommended Practice for Implementing IEC 61850 Based Substation Communications, Protection, Monitoring and Control Systems.* IEEE 2030.101, *IEEE Recommended Practice for the Design and Implementation of Time Synchronization Distribution Systems for Substation Automation*, is under development in early 2017.

It is the intent of this guide to provide a common communication structure that allows the individual engineering disciplines to define the requirements according to their own terms and tie those elements to the other disciplines to develop a comprehensive definition of how the overall system should operate.

This guide breaks the overall system into three separate areas: Power Systems, Communication Technology, and Information Technology.

15.1 Power systems (interfaces)

The first section of this guide defines the power system performance metrics at each interface. An example of this would be that for a line current differential relay on the bulk electric system, the expected operating time would be two cycles or 32 milliseconds. The Protection and Control expert should not be defining the communication technology that is require for the application, but the functional requirements on how the final system should perform and what testing will be performed to prove that performance. This would then be passed on to the next discipline.

15.2 Communications technology

The communications technology expert would then take the functional requirements and define the communications specific requirements. It would be the responsibility of the communications

expert to examine the different communications technologies and identify the one that meets the functional requirements. The communications expert would then document the functional and system specification and testing required to support the defined system. This information would then be passed to the Information Technology expert.

15.2.1 High level overview of network management

The OSI model for network management refers to the activities, methods, procedures, and tools that pertain to faults, configuration, accounting, performance and security (FCAPS) of networked systems. A common network management technique is to implement a Simple Network Management Protocol (SNMP) based network management system to collect data about network devices. SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. Network management systems collect information about the network in two ways. Internet Protocol (IP) attached devices are monitored by responses or lack of responses to polls from the network management application as well as SNMP messages called traps (unsolicited SNMP messages) generated and sent to the management station. The management station will usually have a graphical network diagram and will flash an indicator such as a node blinking red to indicate a fault.

15.3 Information technology

The information technology (application) expert would then examine the overall system requirement and recommended communication technology for any application specifics. The IT expert would then define the remaining system specifications and identify tests required to adequately test these remaining specifications. Upon completion of this process a complete set of system specification and tests should be available for the application.

15.4 Developing concerns

Many utilities have successfully developed an informal process that mirrors much of the IEEE 2030 guide. With the rapidly changing environment of the utility industry, both in new technologies and the aging of the workforce, these informal processes that depend on interpersonal relations may need to be replaced with formal processes.

15.4.1 Settings file management

As the new technology is deployed, the wiring of conventional systems is replaced by the mass of configuration settings in a modern P&C scheme based on complex microprocessor relays and IEDs, and configured Ethernet switches, routers, and appliances described in earlier sections – for example, see Section 7.8. Without clear, reliably backed up configuration files and information, it is impossible to troubleshoot a network installation, or even to quickly replace and configure a failed unit of equipment. Since a single incorrect setting can disrupt critical functions, the user should have a

strictly managed process for developing and tracking setting or configuration files, as well as associated hardware and firmware versions. Maintenance personnel must have access to a reliable, protected, and controlled archive of the latest configuration and setting files for rapid updating or recovery of the P&C system.

Within regulatory authority of NERC, the retention and recovery of these files have been codified in the NERC Critical Infrastructure Protection (CIP) regulations. While it is understood that these requirements are not international, they do provide good guidance in the development of disaster recovery documentation.

References

1. *IEEE (ANSI) Device Number 16 – Ethernet Switches and Routers*, Eric A. Udren, KEMA Consulting, Pittsburgh, PA (Georgia Tech Protective Relay Conference, Atlanta, GA, May 2008; Texas A&M Conference for Protective Relay Engineers, April 2008).
2. IEEE Standard C37.2-2008, *IEEE Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations*.
3. *Extending the Substation LAN Beyond Substation Boundaries: Current Capabilities and Potential New Protection Applications of Wide-Area Ethernet,* Veselin Skendzic, Schweitzer Engineering Laboratories, Inc. and Roger Moore, RuggedCom, Inc.; 8th Annual Western Power Delivery Automation Conference, Spokane, WA, April 11–13, 2006.
4. *Selecting, Designing, and Installing Modern Data Networks in Electrical Substations*, Gary W. Scheer and David J. Dolezilek, Schweitzer Engineering Laboratories, Inc.; 9th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2007
5. Cisco Internetworking Technology Handbook - *Chapter 4 - Bridging and Switching Basics,* Cisco Press, www.cisco.com.
6. IEEE PSRC H6 Special Report, *Application Considerations of IEC 61850/UCA 2 for Substation Ethernet Local Area Network Communication for Protection and Control,* http://www.pes-psrc.org/Reports/H6Paper-App%20Consider%20of%20IEC61850&UCA_072205_083105.pdf.
7. *Industrial Ethernet: A Control Engineer's Guide*, Cisco White Paper, http://www.cisco.com/c/dam/en/us/products/collateral/switches/catalyst-2950-series-switches/prod_white_paper0900aecd8013313e.pdf.
8. *Ethernet in the Substation,* M. P. Pozzuoli and Roger Moore, RuggedCom, Inc.; IEEE Power Engineering Society General Meeting, 2006; IEEE Xplore.
9. *LAN Congestion Scenario and Performance Evaluation* by Mark S. Simon, Charles R. Sufana, and John T. Tengdin; IEEE Winter Power Meeting, Volume 2, 99CB36233, page 919, IEEE Xplore.
10. IEC 61850-8-1:2011, *Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, IEC* Webstore, https://webstore.iec.ch/publication/6021.
11. IEC TR 61850-90-1:2010, *Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations*, https://webstore.iec.ch/publication/6024.

12. IEC TR 61850-90-4:2013, *Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines*, https://webstore.iec.ch/publication/6025.
13. IEC TR 61850-90-12:2015, *Communication networks and systems for power utility automation - Part 90-12: Wide area network engineering guidelines*, https://webstore.iec.ch/publication/22942.
14. IEC TR 61850-90-5:2012, *Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118*, https://webstore.iec.ch/publication/6026.
15. IEC 62439-3 Ed 3.0: 2016, *Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*, https://webstore.iec.ch/publication/24438.
16. IEEE 1613-2009, *IEEE standard environmental and testing requirements for communications networking devices installed in electric power substations,* IEEE Xplore.
17. IEEE 1613.1-2013, *IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Transmission and Distribution Facilities* (extension of IEEE 1613-2009), IEEE Xplore.
18. IEEE STD 1615-2007, *IEEE Recommended Practice for Network Communication in Electric Power Substation*s, IEEE Xplore.
19. PSRC WG C3 Report, *Processes, Issues, Trends and Quality Control of Relay Settings*, http://www.pes-psrc.org/Reports/Processes_Issues_Trends_and_Quality_Control_of_Relay_Settings.pdf.
20. IEEE P2030.100, *IEEE Draft Recommended Practice for Implementing IEC 61850 Based Substation Communications, Protection, Monitoring and Control Systems.*
21. North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP) standards series, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
22. IEEE C37.1-2007, *IEEE Standard for SCADA & Automation Systems*.
23. IEC/IEEE 61850-9-3 *Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation.* (The base profile).
24. IEEE C37.238-2017 *Standard Profile for use of IEEE 1588 Precision Time Protocol in Power System Applications.* (This extends the base profile).
25. IEEE PSRC H32 Special Report, *Performance Requirements for Ethernet Circuits Applied to Teleprotection* (Expected publication in 2017).

26. IEC 61850-9-2 Edition 2, 2011, *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled Values over ISO/IEC 8802-3.*

27. IEC 61850-3 Edition 2, 2013: *Communication networks and systems for power utility automation – Part 3: General requirements.*

28. IEEE 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, http://ieeexplore.ieee.org/document/4579760/ .

Annex A - Ethernet Data Transmission and OSI Layers

An application program sending or receiving data over Ethernet, in a computer or substation IED, generally uses the services of its operating system (O/S) Ethernet stack. This is a collection of software modules and memory structures which formats and decodes data sent via the Ethernet, according to the requirements of the 7-layer model and the applications programs. Data is physically sent and received using a device called a Media Access Controller (MAC), which interfaces to the communications medium (e.g. copper wire or optical fiber). The MAC device may include the actual connection to the medium, or this may be provided using a separate device called a physical-layer interface, often referred to as a 'PHY.'

Data sent using Ethernet and the 7-layer model is formatted in frames. The lower layers (2-4) of the OSI model each add a 'header' to the frame. Using the information in the headers, the frame may be properly routed to, and decoded at, its destination. This is true for devices connected directly to the same local area network (LAN); and using routable (IP) protocols, even when the destination is far away. Most familiar applications use Internet protocols (IP), which operate at layers 3 and 4 of the 7-layer stack; but applications may also communicate directly at layer 2. These protocols are limited to LAN scope; without a routable (IP or equivalent) header, they cannot be sent over layer-3 wide-area networks.

At the **physical layer (layer 1)**, the header consists of synchronization and framing-control bits or symbols, used by the receiving device to locate the beginning and end of each data frame. These bits or symbols are not normally visible to the higher levels of the model (i.e., software), but they may be examined using a protocol analyzer.

At the **data link layer (layer 2)**, as defined by IEEE Standard 802.3, this 14-octet header includes the source and destination Media Access Controller (MAC) addresses (SA and DA), and a length/type field. Data and a Frame Check Sequence (FCS) follow; for Ethernet, the FCS is a 32-bit (4-octet) Cyclic Redundancy Check (CRC). The CRC is calculated on the entire message, including the SA, DA, length/type and data. This frame is sometimes called a 'MAC frame' or 'MAC data frame' (Table A-1).

Each line in the following tables describes 32 bits (4 octets or 8 hex digits) in the frame.

Octet 1	Octet 2	Octet 3	Octet 4
DA First Octet	**Destination MAC Address (DA)**		
DA	**DA Last Octet**	**SA First Octet**	**SA**
Source MAC Address (SA)			**SA Last Octet**
Length/Type		Data	
Data			
Ethernet FCS – CRC			

Table A-1 - Ethernet (IEEE 802.3) header – MAC Frame

The source and destination MAC addresses (SA and DA) are 48-bit (6-octet or 12 hex digit) numbers. They are unique for each MAC, which is normally a physical device (integrated circuit) or in some cases a part of one (a system-on-chip microcontroller, for instance). The manufacturer gives MAC addresses to a computer or IED when the device is made. The IEEE Registration Authority assigns the high-order 3 octets (6 hex digits) to each manufacturer; the manufacturer assigns the lower 3 octets. The high-order octets are sometimes known as the Organizationally Unique Identifier (OUI).

The DA address may also be modified, by setting the lowest bit of the first octet in the OUI to create a multicast address. Several addresses are reserved for special purposes, such as broadcast messages. Tables of these assignments, and of OUIs, are updated frequently and may be found elsewhere; for example at the website www.iana.org (IANA, the Internet Assigned Number Authority).

The two-octet length/type field has two possible meanings. Values of 1500 decimal (0x05DC) or less denote message length, used with layer-2 protocols. Values greater than 1536 (0x0600) are ‘Ethertypes’ which identify the protocol used for the bytes following, e.g. an 802.1Q tag or a higher-level (layer 3) protocol such as IPv4 (Ethertype 0x0800).

An extension of the layer 2 header, a 4 octet ‘VLAN header,’ may be inserted between the DA and length/type field (Table A-2). With VLAN, or ‘Virtual LAN,’ individual physical connections may be grouped together logically as members of independent ‘virtual local area networks.’ Using VLANs, a switch may control which ports can ‘see’ each other and communicate, and also may prioritize traffic between them.

Octet 1	**Octet 2**	**Octet 3**	**Octet 4**
DA First Octet	Destination MAC Address (DA)		
DA	DA Last Octet	SA First Octet	SA
Source MAC Address (SA)			SA Last Octet
VLAN Ethertype = 0x8100		**Priority**	**VLAN ID** (12 bits)
Length/Type		Data	
Data			
Ethernet FCS – CRC			

Table A-2 - Ethernet (IEEE 802.3) header with VLAN (IEEE 802.1Q)

At the **network layer (layer 3)**, the Internet Protocol (IP) header consists of 20 octets (Table A.-3). This header includes network-layer management data, including protocol ID and information to re-construct messages broken into fragments. Important for our purposes, it also identifies the layer-4 protocol (e.g., TCP: protocol 6 and UDP: protocol 17 or 0x11) and the source and destination IP addresses.

Octet 1		**Octet 2**	**Octet 3**	**Octet 4**
Version	Length	Type of Service	Total Length	
Unique Frame ID			Flags and Fragment Offset	
Time to Live		Layer 4 Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options and Padding				
Data				

Table A-3 - IP Header

IP addresses are not the same as physical MAC addresses. They are only 32 bits (4 octets) long, and are assigned under the control of the network. Assignments may be *manual* (fixed, requested by the client device); '*automatic*,' assigned once and thereafter unchanged; or *dynamic*, assigned as requested. DHCP (Dynamic Host Control Protocol) manages IP address assignments.

Dynamic addresses are assigned for a period of time (called a 'lease'), and must be renewed. Dynamic address allocation simplifies network management, for example in ISP or enterprise networking applications. Manual or automatic (fixed) address assignment can enhance security in a network with a known topology, reducing opportunities for adversaries to access a network.

Note that some IP addresses are fixed by IANA, and some blocks are available for assignment (see IANA).

To know where to physically send a frame, a router must be able to match IP addresses with MAC addresses. For IPv4, this is done using Address Resolution Protocol (ARP); for IPv6 the corresponding protocol is NDP (Neighbor Discovery Protocol). Switches operate at layer 2, based on MAC addresses, which they 'learn' by monitoring the SA in each received frame. Switches, particularly managed switches, may also prioritize and/or route traffic based on the contents of the L3 or L4 headers.

At the **transport layer (layer 4)**, the header format is defined by the protocol (TCP or UDP, or one of many other protocols, identified in the IP header). The UDP header (Table A-4) is simpler (than TCP), since UDP is a connection-less protocol, and does not provide assured message delivery. It includes source and destination Port Numbers, message length and checksum. The TCP header (Table A.5) also includes fields for re-assembly of data segments, acknowledgement, and other information needed to maintain a connection, verify valid data, and request re-transmission of corrupted frames.

Octet 1	**Octet 2**	**Octet 3**	**Octet 4**
Source Port		**Destination Port**	
Length		Checksum	
Data			

Table A-4 - UDP Header

Octet 1	**Octet 2**	**Octet 3**	**Octet 4**
Source Port		**Destination Port**	
Sequence Number			
Acknowledgement Number			
Data Offset, ECN, Control Bits		Window	
Checksum		Urgent Pointer	
Options and Padding			
Data			

Table A-5 - TCP Header

IP port numbers (Table A-6) identify the higher-level protocol used by the frame. The O/S Ethernet stack uses the port number to send each frame to the correct application. Message priority may be set using port numbers.

Port Number	Application
0	Maintenance
20	FTP, File Transfer Protocol, Data
21	FTP Control
22	SSH, Secure Shell
23	Telnet
25	SMTP, Simple Mail Transfer Protocol
37	TIME Protocol
42	Internet Name Server
45	Internet Message Protocol
53	DNS, Domain Name System
57	MTP, Mail Transfer Protocol
80	HTTP, HyperText Transfer Protocol
115	SFTP, Simple File Transfer Protocol
123	NTP, Network Time Protocol (also SNTP)
161	SNMP, Simple Network Management Protocol
319	PTP (IEEE-1588 Precision Time Protocol), Event Port
320	PTP (IEEE-1588 Precision Time Protocol), General Port
366	SMTP (ref. Port 25) on-demand mail relay (ODMR) extension
500	IKE, Internet Key Exchange
502	Modbus
546	DHCPv6 Client
547	DHCPv6 Server
580	SNTP Heartbeat
4712-13	PMU

Table A-6 - Useful IP Port Numbers (Partial list)

Higher-level layers are specific to each application and/or protocol. Layer 7, the application layer, includes familiar services such as HTTP, NTP, SNMP, and MMS used by IEC 61850 client-server services. Layer 6 describes methods for encoding data, including encryption and compression. Layer 5 handles sessions, which means that it deals with frames going to and from different applications, much like a ‘traffic cop’ deciding who can proceed and who must wait. These layers do not add headers, as the lower-level layers handle this.

To configure substation Ethernet hardware (switches, routers, IEDs), the most useful data fields are generally (but not always) found in the layer 2-4 headers. Based on the contents of these headers, the user can set priorities, reserve port bandwidth, control access, enable or disable multicast and broadcast traffic, and set other configuration parameters to optimize your network for reliable, timely transmission of critical messages; while allowing other traffic to co-exist on the same network.

Example of Overall Ethernet Message Format

This example shows the format of an NTP message, sent using UDP-IP v4. This example uses the IEEE 802.1Q VLAN tag. The example shows how each higher-level header and the data message are 'encapsulated' into the lower-level message, building the complete data frame which will be sent to the MAC for transmission across the Ethernet physical layer.

Octet 1	Octet 2	Octet 3	Octet 4
DA First Octet	Destination MAC Address (DA)		
DA	DA Last Octet	SA First Octet	SA
Source MAC Address (SA)			SA Last Octet
VLAN Ethertype = 0x8100		Priority	VLAN ID
IP Ethertype = 0x0800			
Version=4 / Length=5	Type of Service	Total Length	
Unique Frame ID		Flags and Fragment Offset	
Time to Live	Layer 4 Protocol=17 (0x11) – UDP	Header Checksum	
Source IP Address			
Destination IP Address			
Source Port=123 (NTP)		Destination Port=123	
Length		Checksum	
NTP Data Message …			
Ethernet FCS – CRC			

Table A-7 - NTP Message Header Example

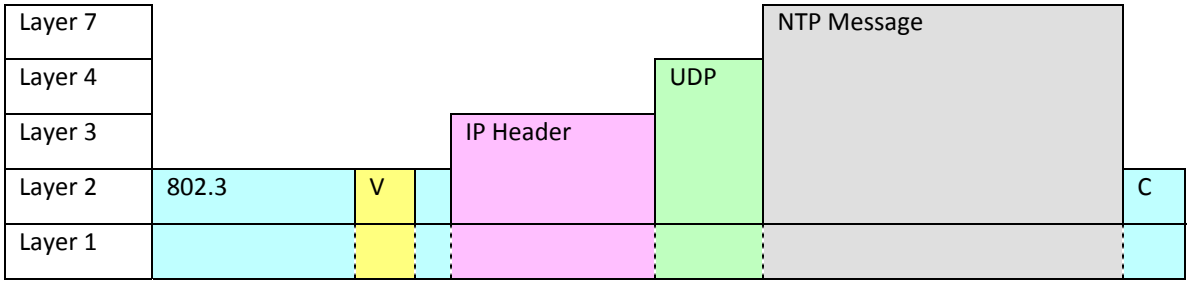

Table A-8 - Encapsulation Overview (V=VLAN tag; C=CRC)

Annex B - Ethernet Switch Protocol Implementation Conformance Statement (PICS)

In order to assist in the selection of Ethernet switches, the following table proposes a Product Implementation Conformance Statement (PICS) in a format like that used by IEC TC 57 WG 10 (developers of IEC 61850). Its purpose is not to tell the user exactly what to specify, but rather to prompt user interaction with switch vendors in determining how a particular Ethernet switch product fits the application requirements. The IEEE Power System Relaying Committee working group that compiled this report has updated and added to the original UCA IUG table PICS draft.

The table below originated with work done by leaders in the UCA International Users' Group (UCA IUG). They observed, after the 2011 interoperability testing event (IOP), that questions arose regarding how to verify Ethernet switch data sheets. The IOP demonstrated how misconceptions on the datasheets can impact system configuration.

As an example, there are 8 priority levels (0-7) in IEEE 802.1P (See Sections 3 and 7.4 above). However, many switches do not have queues for each priority. In some cases, there are only three priorities supported. Thus if a substation protection and control designer inadvertently chooses two priorities that map into the same queue, the priority differentiation of those messages will be lost.

Some entries in the right *Value/Comments* column give expansion of acronyms appearing to the left.

Basic Ethernet switch conformance statement

The following attributes apply to a switch used in any environment.

Table B-1 – Basic Conformance Statement

			Value/ Comments
▪ Non-blocking, store and forward			Number of ports
S1	Port speed 100 Mbps	Y/N	
S2	Port speed 1 Gbps	Y/N	
S3	Port speed 10 Gbps	Y/N	
S4	Typical Latency		Specify in microseconds
S5	Auto negotiating	Y/N	

▪ Supported physical interfaces			
	Type	Number of connections	**For each – state speed, wavelength, distance**
I1	RJ45 UTP/STP	#	Copper wiring interface

I2	ST (Note 1)	#	Optical fiber connection type
I3	SC (Note 1)	#	Optical fiber connection type
I4	LC (Note 1)	#	Optical fiber connection type
I5	MTRJ (Note 1)	#	Optical fiber connection type
I6	SFP (Note 1)	#	Optical fiber connection type
I7	Critical alarm relay	Y/N	Contacts; fail-safe dropout?
I8	Modular port configuration	Y/N	
I9	Local management port	Y/N	
I10	Accessible memory	Y/N	
Note 1	Light level incompatibility or overload is a known issue with all optical interface types. In particular, there are known interoperability issues between different vendors SFP transceivers.		Test or validate interoperation of switches with these interfaces.

▪ Management			
M1	IEC 61850	Y/N	For what standard parts and services is conformance claimed?
	Supports IEC 61850-7-4 Logical Nodes	Y/N	Which logical nodes?
M2	SNMP	Y/N	Versions supported? (Simple Network Management Protocol, IT standard)
M3	Is remote access supported?	Y/N	If (Y), specify the method(s) of remote access: HTTP, HTTPS, telnet, SSH, other (specify).
M4	Is there a mechanism to disable remote access?	Y/N	
M4	Proprietary configuration tool	Y/N	
M5	RMON support	Y/N	IT standard remote monitoring. How much/many/which fields are supported?
M6	Syslog support	Y/N	
M7	Configuration backup and restore	Y/N	How long does it take?
M8	Firmware backup and restore	Y/N	If (Y), specify which methods are used: HTTP, HTTPS, TFTP, FTP, Other (specify). How long does it take? Does it wipe out settings?
M9	Does the upgrade process failsafe (e.g. the upgrade fails but no changes are applied)	Y/N	
M10	Does the device support 802.1AR	Y/N	Standard for Local and Metropolitan Area Networks: Secure Device Identity

Substation Ethernet switch conformance statement

For the use of the Ethernet switch in a substation environment the following aspects need to be considered.

Table B-2 – Substation Ethernet Switch Conformance Statement

			Value/ Comments
▪ Redundancy protocols			
RR1	(R)STP	Y/N	State convergence time in ms ((rapid) spanning tree protocol, explained in report)
RR2	PRP	Y/N	(Parallel high-speed Redundancy Protocol; see Section 4.6.1)
RR3	HSR	Y/N	(High-availability Seamless Redundancy; see Section 4.6.2)
RR4	What is the largest MTU supported?		Specify in number of bytes. (Maximum Transmission Unit is the size (in bytes or octets) of the largest protocol data unit that the switch can pass onwards.)
RR5	Type of port mirroring supported		None, SPAN, RSPAN, ERSPAN, Ethernet frame over UDP, Ethernet frame over GRE

▪ Virtual LAN (VLAN)			
V1	Is the full range of IEEE 802.1Q VLAN IDs (VIDs) supported?	Y/N	How many? See Sections 7.5 and 11.11.
V2	Specify the range of VLAN IDs that can be supported by the switch simultaneously:		
	a) All (0-4095)	Y/N	
	b) A range of values	Y/N	Specify how the range is constrained.
	c) A specific number	Y/N	How many?
V3	Specify the maximum number of VLAN IDs supported per port:		Number of VIDs?
	a) A range of values	Y/N	Specify how the range is constrained.
	b) A specific number	Y/N	How many?
V4	Support for priority levels	Y/N	How many levels?
V5	How many priority levels per queue		Amount
V6	Specify which priorities map into the same queue		Specify priorities vs queue mapping.

V7	Do the trunk port(s) discard packets with VLAN ID = 0	Y/N	IEC 61850 & IEEE 1588 both specify use of VLAN = 0, but some switches do not pass these packets.
V8	Do the egress trunk port(s) remove VLAN ID = 0?	Y/N	
V9	Do ingress trunk port(s) remove VLAN ID = 0?	Y/N	
V10	Can ingress port(s) add VLANs?	Y/N	
V10	VLANs per trunk port		Number
	a) A range of values	Y/N	Specify how the range is constrained.
	b) A specific number	Y/N	How many?
V11	VLANs per edge port		Number
	a) A range of values	Y/N	Specify how the range is constrained.
	b) A specific number	Y/N	How many?
V12	Methods available for VLAN registration		VTP, legacy GVRP, 802.1AK, MVRP, manual?

▪ RSTP			
R1	Root bridge?	Y/N	
R2	User configurable priority?	Y/N	
R3	Version of (R)STP		802.1? Mixing versions is risky for speed or other issues.
R4	MAC filters per port		amount
R5	Matching algorithm (Exact or hash)		Exact/hash
R6	Worst case fault recovery time per hop		< 5ms
R7	Bridge Diameter		160 switches

▪ Time synchronization			
T1	SNTP	Y/N	(Simple Network Time Protocol)
T2	IEEE 1588 with hardware time-stamping	Y/N	(Precision Time Protocol)
T3	What profile of 1588 is supported		Specify versions/profiles if any Note IEC/IEEE 61850-9-3 and/or IEEE C37.238 version.
T4	Transparent Clock 1 Step	Y/N	Accuracy
T5	Transparent Clock 2 Step	Y/N	Accuracy
T6	Grandmaster Clock	Y/N	Accuracy / Time Source
T7	Boundary Clock	Y/N	Accuracy
T8	Ordinary Clock	Y/N	
T9	Synchronization Source		GPS/IRIG-B/1588
T10	Timing Output	Y/N	IRIG-B TTL/AM/PPS

▪ Management Security			
S1	RADIUS support for login authentication	Y/N	(Remote Authentication Dial-In User Service, IT standard)
S2	Authentication mechanisms are supported		
	RADIUS	Y/N	
	TACACS	Y/N	(Terminal Access Controller Access-Control System; IT standard)
	LDAP		Active directory (Lightweight Directory Access Protocol)
	Other		List other mechanisms
S3	Roles supported	Y/N	Specify number of roles
	Specify the different authorization/roles (limited, operator, manager, and other).		Limited, Operator, Manager, other (specify).
S4	Passwords supported	Y/N	
S5	Minimum allowed length of passwords		Enter length
S6	Maximum allowed length of passwords		Enter length
S7	Password expiration supported	Y/N	Enter default expiration period.
S8	Validation that firmware is genuine version from manufacturer	Y/N	Vendor methods vary – requires vendor description

▪ Switch Properties			
SP1	Port enable/disable	Y/N	
SP2	Port based IEEE 803.AR authentication	Y/N	
SP3	Port MAC authentication	Y/N	Specify number of roles
SP4	Port rate limiting	Y/N	State ingress and egress values, which may be different.
SP5	Switching Bandwidth		Specify Gbps
SP6	MAC Addresses filtering supported	Y/N	
	If (Yes), how many MAC addresses can be supported prior to forwarding all MACs		Specify number of MACs or MAC table size support
	What technology is used for learning - hash or CAM?		Content addressable memory
SP7	802.1p Class of Service	Y/N	
SP8	GMRP Multicast Filtering	Y/N	See Section 7.6
SP9	Type of port mirroring supported		None, SPAN, RSPAN, ERSPAN, Ethernet frame over UDP, Ethernet frame over GRE
SP10	Is SDN supported	Y/N	Software Defined Network
	If Yes, what technology is supported?		One choice is OpenFlow - Communications protocol that gives access to the forwarding plane of a network switch or router over the network.

▪ EMI and Environmental			
E1	Complies with IEC 61850-3?	Y/N	Which edition of 61850-3? What class of conformance?
E2	Meets IEEE 1613 and 1613.1 Class 2 (electric utility substations)	Y/N	Class 2 – functions during the disturbance; not just survival.
E3	Specify operational ambient temperature range		Degrees Celsius
E4	Quantity and monitoring of cooling fans		IEEE 1613 specifies no fans, but monitored redundant fans may be required for some practical high-performance switches and routers
E5	Cold startup at lowest rated temperature?	Y/N	
E6	Boot time to full operation of all functions to specifications from cold start	Seconds	

▪ Prioritization			
P1	Number of classes of service support		Specify number
P2	Prioritize by ingress port	Y/N	
P3	Prioritize by 802.1Q priority field	Y/N	
P4	Prioritize by source or destination MAC address	Y/N	
P5	Prioritize by TOS DSCP in IP header	Y/N	Used in IEC TR 61850-90-5. (Type Of Service – Differentiated Service Control Point)
P6	Prioritize by VLAN	Y/N	

▪ Power Supplies			
PS1	Dual redundant, load sharing power supplies	Y/N	Do they have separated and isolated feeds?
PS2	24 Vdc	Y/N	
PS3	48 Vdc	Y/N	
PS4	88-300 Vdc	Y/N	
PS5	85-264 Vac	Y/N	
PS6	Is Power-Over-Ethernet (PoE) supported?	Y/N	
	If Yes, what is the maximum aggregate load?		Specify capacity in watts and/or amperes at defined voltage