Practical Applications of Ethernet in Substations and Industrial Facilities

Craig Wester
IEEE Member
GE Digital Energy Multilin
20 Technology Pkwy, Suite 300
Norcross, GA 30092
USA

Mark Adamiak
IEEE Fellow
GE Digital Energy Multilin
530 Swedesford Rd, 2nd Floor
Wayne, PA 19087
USA

***Abstract* - This paper is a tutorial in Ethernet communications and architectures. The defacto LAN standard throughout the world is Ethernet and the worldwide investment into this technology dwarfs that of investment into any other LAN standard. Speed, fiber support, multiple services and protocol support, and the emergence and usage of the IEC61850 protocol have resulted in an increase in the installation of Ethernet within substations and industrial facilities.**

There are many practical aspects associated with the application of Ethernet within the substation and industrial facility. This paper will address Ethernet fundamentals and will attempt to cover the most common elements of an Ethernet architecture from media selection, requirements for protective relaying systems, managed Ethernet Switch functions and terminology relevant to the protection relay engineer (such as VLAN, RSTP and QoS), network topology (ring, star, mesh, redundancy) and high speed recovery of redundant ring networks. Architectures for different applications will be reviewed, such as SCADA and GOOSE messaging. The intent of this paper is to educate the non-IT person, such as the protective relay engineer, on Ethernet fundamentals that are important to protective relaying applications.

I. Introduction

Modern utility and industrial sites have evolved into complex operations that perform many functions and require a wide variety of Intelligent Electronic Devices (IEDs) and controls to work properly and safely. To automate these environments, these IEDs need to work in close concert. Today, organizations are moving from coordinating these IEDs using low-speed serial connections, to implementing high-performance networks built from Optical, Wireless, and Ethernet technologies. These modern networks enable quick, reliable communications that allow critical IEDs to be managed, analyzed, or controlled from a single or multiple locations.

Taking the next step from automating a single site, organizations have begun to interconnect their various facilities to create larger, high-speed networks that allow control and monitoring from any location attached to the network. Many different technologies can be used to network together different sites. Over the past decade, Ethernet has become a popular networking technology because of its low cost, high bandwidth, and versatile support for multiple applications such as voice, video, and data.

Additional benefits of networking IEDs include the ability to securely access the IEDs from anywhere within or outside the facility. Engineers and maintenance technicians can have remote access to IED settings, informative and historic data to assist in post fault diagnostics from the networked IEDs.

Technological advancements in IED hardware design and the development of high-speed peer-to-peer communication protocols have resulted in a new generation of IEDs. These protective and control IEDs have the capability to accept multiple levels of current and voltage inputs and to analyze these values at significantly increased speeds. The main advantages of using these microprocessor-based IEDs are simplification of the device-to-device wiring, component cost reduction, increased system reliability and extensive data recording capabilities.

An efficient way to apply these microprocessor-based IEDs and obtain a reduction in device-to-device wiring is to use high-speed peer-to-peer IEC61850 Generic Object Oriented Substation Event (GOOSE) messaging between the protective IEDs. GOOSE is a user-defined set of data that is "Published" on detection of a change in any of the contained data items. With binary values, change detect is a False-to-True or True-to-False transition. With analog measurements, IEC61850 defines a "deadband" whereby if the analog value changes greater than the deadband value, the GOOSE with the changed analog value is sent.

IEC61850 uses an Ethernet connection as the physical medium of communication between the protective IEDs. Logical I/O via Ethernet communications is used in place of traditional hard wire to exchange the information between the protective IEDs. The information sent over the network might include connected device I/O, protective element statuses and programmable logic states. Modern IEC61850 implementations are able to send messages between protective relays at speeds of around 1 to 4 ms. Also, IEC61850 includes the capability of exchanging analog data between IEDs through IEC61850 GOOSE messaging, so actual values of currents and voltages are able to be sent over the high speed Ethernet network to other IEC61850 based IEDs.

In addition, use of an Ethernet network allows simultaneous use of multiple protocols and services on the same hardware, such as Modbus, DNP (Distributed Network Protocol), IEC61850 and Phasor Measurement Units (PMU).

II. TERMINOLOGY

As a basis for further discussion, we will first review some key terminology that will be useful to the non-IT specialist, such as a protective relay engineer. Some key terminologies are:

Backbone – The main cabling of a network that all of the segments connect to is called the Backbone. Typically, the backbone is capable of carrying more information than the individual segments. For example, each segment may have a transfer rate of 100 Mbps (megabits per second), while the backbone may operate at 1000 Mbps (or 1Gbps).

Bridge – Bridging is a forwarding technique used in packet-switched computer networks. Unlike routing, bridging makes no assumptions about where in a network a particular address is located. A bridge and an Ethernet switch are very much alike, where an Ethernet switch being a bridge with numerous ports.

Broadcast Domain – A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer. A broadcast domain can be within the same LAN segment or it can be bridged to other LAN segments. Any computer or IED connected to the same Ethernet switch is a member of the same broadcast domain. Routers and other higher-layer devices form boundaries between broadcast domains.

Client-Server – The client-server model distinguishes between applications as well as devices. Network clients make requests to a server by sending messages, and servers respond to their clients by acting on each request and returning results. One server generally supports numerous clients, and multiple servers can be networked together in a pool to handle the increased processing load as the number of clients grows. A client computer and a server computer are usually two separate devices, each customized for their designed purpose.

DHCP – The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by hosts (DHCP clients) to retrieve IP address assignments and other configuration information. DHCP uses a client-server architecture. The client sends a broadcast request for configuration information. The DHCP server receives the request and responds with configuration information from its configuration database. In the absence of DHCP, all hosts or IEDs on a network must be manually configured individually with IP, subnet and gateway addresses (This is the case for protective relay and metering IEDs on the utility and industrial company network – i.e. fixed IP, Subnet and Gateway addresses).

Ethernet Hub – A connectivity device that connects two or more nodes. It has multiple ports that carry cables in and out to various nodes or destinations. It takes what one device sends over the network and automatically distributes that information to all the other devices connected to that same Ethernet hub. Since every packet is being sent out through all other ports, packet collisions result, which greatly impedes the smooth flow of traffic.

Ethernet Switch – A "smart" hub. It divides the given LAN into different segments and streamlines the flow in and out of different ports. It allows signals from multiple ports and transfers it to another set of ports without interference or collisions. Ethernet switches are capable of inspecting data packets as they are received, determining the source and destination device of each packet, and forwarding them appropriately. By delivering messages only to the connected device intended, an Ethernet switch conserves network bandwidth and offers generally better performance than an Ethernet hub. The industry has moved to Ethernet Switches.

Firewall – A security device (either software or hardware) that establishes a barrier to contain designed network traffic within a specified area by allowing or denying access based upon a set of rules and other criteria.

Gateway – A gateway is a node (a router) on a TCP/IP Network that serves as an access point to another network. In enterprises, the gateway is the node that routes the traffic from a workstation to another network segment. It is an entry point and an exit point in a network.

Host – In networking, a network host is a computer connected to the Internet, or more generically to any type of data network. A network host can host information resources as well as application software for providing network services.

IP – The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.

IP Address – An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network that uses the Internet Protocol for communication between its nodes. An IP address serves two principal functions (host and network interface identification and location addressing). IP Addressing will be discussed in more detail later in the paper.

LAN – A local area network (LAN) is a computer network covering a small physical area, like a substation, building or facility.

Network – A group of computers and IEDs connected together in a way that allows information to be exchanged.

Node – Any device that is connected to or is part of the network. While a node is typically a computer, it can also be printer, storage device, switch, router, or IED.

Port – A signal interface to a device, which is either physical as on an Ethernet switch or logical as UDP/IP or TCP/IP ports on a processor.

QoS – In order to ensure high network performance for critical applications and data, Ethernet switches offer Quality of Service (QoS) in compliance to IEEE 802.1p standard [1]. By defining certain switch ports, or certain traffic types, with different priority levels, 802.1p prioritizes network flows, so that critical data is allowed to jump ahead of normal network traffic passing through the Ethernet switch at the same time. Network traffic priority classification can be made by Port, by Tag or by IP Type of Service (ToS). QoS will be discussed in more detail later in the paper.

Router – A router is a networking device whose software and hardware are customized to the tasks of routing and forwarding information.

RSTP – Rapid Spanning Tree Protocol (RSTP) is an evolution of Spanning Tree Protocol (STP). STP is obsolete. RSTP provides for faster spanning tree convergence after a topology change to ensure loop-free topology for a ring topology LAN. Recovery times for RSTP can be in the order of 5ms per hop or Ethernet Switch. RSTP will be discussed in more detail later in the paper.

Segment – Any portion of a network that is separated, by a switch, bridge or router, from other parts of the network.

SNTP – The Simple Network Time Protocol is a protocol for synchronizing the clocks of computer systems or IEDs over packet-switched, variable-latency data networks. SNTP uses UDP on port 123 as its transport layer. A less complex implementation of NTP (Network Time Protocol), using the same protocol but without requiring the storage of state over extended periods of time, is known as the Simple Network Time Protocol (SNTP). The timing accuracy of SNTP or NTP is approximately 1ms while direct connected IRIG-B signal is 1 μs accuracy. With SNTP, an IED can obtain clock time over an Ethernet network. The IED acts as an SNTP client to receive time values from an SNTP/NTP server, usually a dedicated product using a GPS receiver to provide an accurate time. Both unicast and broadcast SNTP are supported in most IEDs. To use SNTP in unicast mode, set to the SNTP/NTP server IP address in the IED. The IED attempts to obtain time values from the SNTP/NTP server. Since many time values are obtained and averaged, it generally takes three to four minutes until the IED's clock is closely synchronized with the SNTP/NTP server. It may take up to several minutes for the IED to signal an SNTP self-test error if the server is offline. SNTP is a very efficient method of setting all the IEDs on the network to the same time, which benefits for post event analysis. SNTP is not to be used with Synchrophasors applications (i.e. phasor measurement unit devices). If using a PMU, one must direct connect to a dc shift IRIG-B GPS time sync signal directly.

Subnet – A sub network, or subnet, is a logically visible, distinctly addressed part of a single Internet Protocol network. The process of sub netting is the division of a computer network into groups of computers that have a common, designated IP address routing prefix. Subnet Addressing will be discussed in more detail later in the paper.

TCP/IP – The acronym for the two primary protocols that operate the Internet, namely, Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite and the other being Internet Protocol, or (IP), so the entire suite is commonly referred to as TCP/IP.

Topology – The way that each node is physically connected to the network.

Transport Layer – The Transport Layer provides transparent transfer of data between end devices, providing reliable data transfer services to the upper layers. The Transport Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state and connection oriented. This means that the transport layer can keep track of the segments and retransmit those that fail. Typical examples of transport layer (Layer 4) are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

UDP – The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol (IP) Suite. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

VLAN - Virtual Local Area Networks (VLANs) can be configured and created to handle bandwidth more efficiently and provide additional network security. VLANs will be discussed in more detail later in the paper.

WAN – A wide area network (WAN) is a computer network that covers a broad area. A WAN can be any network whose communications links cross metropolitan, regional, or national boundaries, such as many substations or the entire utility or industrial company.

III. Networking Media

Today, the two most popular physical layer standards for Ethernet are twisted pair copper cable (Category 5 or Cat 5) and fiber optic cable. Twisted pair copper is easier to terminate, has lower installation costs, but is susceptible to electrical noise and a single run of twisted pair cable is distance limited to 100 meters (unshielded) to 150 meters (shielded) in length.

Fiber optic media brings two basic types of solutions, namely, Multi-mode fiber and Single-mode fiber. Both fibers typically have an overall diameter of 125μm. However, Multi-mode fibers have a typical core diameter of either 50 or 62.5μm whereas; Single-mode fiber has a typical core diameter between 8-10μm. Ethernet on Multi-mode fiber can be operated over much longer distances than copper cable (1.5-2km – typical), is immune to electrical noise, and, while being more difficult to terminate, is usually available as prefabricated cables. More details on fiber types is presented below.

Ethernet interfaces are identified by the speed (in Megabits per second), the modulation type (Base), and the physical interface (e.g. – T or TX is Twisted Pair, FL or FX is Fiber). Some common copper and fiber interfaces used in the protective relaying industry with the corresponding IEEE 802.3 definitions, distance and power budget are shown in Figure 1.

Port Type	Port Description	Typical Distance	Power Budget
10/100BaseT	10/100 Mbit RJ45 Copper - unshielded	100 m	N/A
10/100BaseT	10/100 Mbit RJ45 Copper - shielded	150 m	N/A
10BaseFL	10 Mbit Multimode ST Fiber Optic	2 km	17 dB
100BaseFX	100 Mbit Multimode ST Fiber Optic (full-duplex)	2 km	14 dB
100BaseFX	100 Mbit Multimode SC Fiber Optic (full-duplex)	2 km	14 dB
100BaseFX	100 Mbit Singlemode SC Fiber Optic	20 km	12.5 dB
100BaseFX	100 Mbit Singlemode SC Fiber Optic	40 km	12.5 dB
100BaseFX	100 Mbit Singlemode SC Fiber Optic	70 km	32.5 dB
100BaseFX	100 Mbit Multimode LC Fiber Optic	2 km	18 dB
100BaseFX	100 Mbit Singlemode LC Fiber Optic	15 km	23 dB
100BaseFX	100 Mbit Multimode MTRJ Fiber Optic	2 km	15.8 dB
1000BaseTX	1 Gbit RJ45 Copper - unshielded	100 m	N/A
1000BaseTX	1 Gbit RJ45 Copper - shielded	150 m	N/A
1000BaseFX	1 Gbit Multimode SC Fiber Optic	2 km	12.5 dB
1000BaseFX	1 Gbit Singlemode 1310nm SC Fiber Optic	10 km	10.5 dB
1000BaseFX	1 Gbit Singlemode 1310nm SC Fiber Optic	25 km	17.5 dB
1000BaseFX	1 Gbit Singlemode 1550nm SC Fiber Optic	40 km	17.5 dB
1000BaseFX	1 Gbit Singlemode 1550nm SC Fiber Optic	70 km	20.5 dB
1000BaseFX	1 Gbit Multimode LC Fiber Optic	550 m	10.5 dB
1000BaseFX	1 Gbit Multimode LC Fiber Optic	2 km	12 dB
1000BaseFX	1 Gbit Singlemode 1310nm LC Fiber Optic	10 km	11 dB
1000BaseFX	1 Gbit Singlemode 1310nm LC Fiber Optic	25 km	18 dB
1000BaseFX	1 Gbit Singlemode 1550nm LC Fiber Optic	40 km	17 dB
1000BaseFX	1 Gbit Singlemode 1550nm LC Fiber Optic	70 km	20 dB

Fig. 1. – Some Common Copper and Fiber Interfaces on Ethernet Switches Available to the Protective Relay Engineer

A. Ethernet – Unshielded Twisted Pair

10BaseT and 100BaseTX are the two most common twisted pair copper media standards. With respect to 10 or 100 BaseT, the 10 or 100 designation indicates a baud rate of either 10 or 100 megabits per second (Mbps). "Base" stands for baseband, while the T or TX stands for "twisted pair". Since Category 5 (Cat 5) and greater twisted pair cables can work at either baud rate, the designation 10/100BaseT has evolved to show this capability. The cable can be ether unshielded twisted pair (UTP) or shielded twisted pair (STP). The use of shielded twisted pair cabling within industrial or plant switchgear provides for reduced electrical noise immunity to Electromagnetic Interference (EMI).

Unshielded twisted pair cabling has several categories, such as Category 1, Category 2, Category 3, Category 4, Category 5, Category 5e, Category 6/6e and Category 7.

- Category 1: Used for telephone communications and not suitable for transmitting data.
- Category 2: Capable of transmitting data at speeds of up to 4 Mbps.
- Category 3: Widely used as a voice cabling format among computer network administrators in the 1990s. It is an unshielded twisted pair (UTP) that can carry up to 10 Mbps with a bandwidth performance of 16 MHz.
- Category 4: Used in Token Ring networks and can transmit data at speeds up to 16 Mbps and performance of up to 20 MHz. Cable consists of four unshielded twisted-pair (UTP) wires.
- Category 5: Twisted pair high signal integrity cable that has three twists per inch of each twisted pair of 24 gauge copper wires within the cables. Capable of transmitting data at speeds up to 100 Mbps.
- Category 5e: An enhanced version of Category 5 that prevents interference between one unshielded twisted pair to another twisted pair running in parallel within the same cable. Used in gigabit Ethernet networks running at speeds up to 1000 Mbps.
- Category 6 and 6e: A slightly advanced version of Category 5e, which can transmit data at speeds of up to 1000 Mbps (1 Gbps). A cable standard for Gigabit Ethernet.
- Category 7: It is the latest and a fully shielded cable used for technical applications, is also called Class F cable and can transmit data at speeds of up to 1000 Mbps (1 Gbps).

The cable itself consists of four pairs of wires terminated in RJ45 connectors. The maximum permitted cable length is 100 meters for unshielded twisted pair cable and 150 meters for shielded twisted pair cable. The cable pin connections can be one of two configurations. The first is called a "straight-through" cable and the second is called either a "crossover" or a "patch" cable. Whether the cable is straight through or crossover as per standard [The Electronic Industry Association (EIA) / Telecommunications Industry Association's (TIA) Standard 568B] each of the wires within the cable has the following color code:

- For the first twisted wire pair or wire pair #1, one wire is White with Blue bands while the other wire is Blue.
- For the second twisted wire pair or wire pair #2, one wire is White with Orange bands while the other wire is Orange.
- The third twisted pair (wire pair #3) consists of a White wire with Green bands and a second wire that is Green.
- The final wire pair (wire pair #4) consists of a White wire with Brown bands while the other wire is Brown.

Figure 2 shows the pin and cable color configuration for straight and crossover RJ45 Ethernet cables. Note that 10/100BaseT only uses two of the 4 pairs, namely, the Orange/Orange stripe and Green/Green Stripe pairs. The other pairs are either not used or sometimes used to supply 48V DC power to end devices (such as telephones). This is known as Power over Ethernet or POE. Note how the green pair of wires is split between pins 3 and 6.

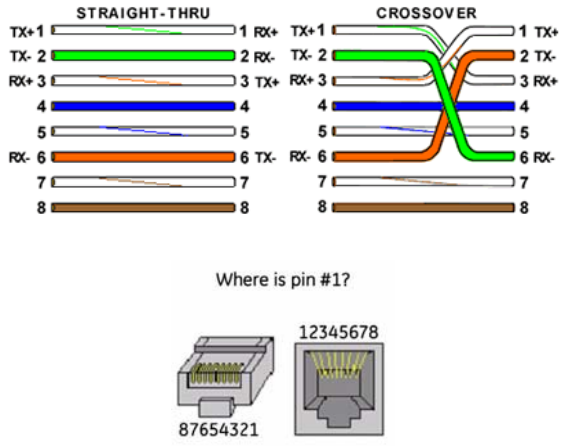

Fig. 2. - Pin Layout for a RJ45 Ethernet Straight and Crossover (Patch) Cables

B. Ethernet – Fiber Optic

Ethernet over fiber cable is rapidly becoming the medium of choice in applications where longer distances and/or immunity to Electromagnetic Interference (EMI) are of importance, such as power system applications. The cable cost differential between copper and fiber has almost disappeared; however, the Fiber Ethernet transceivers are more expensive. Fiber cable is slightly more difficult to terminate these days, but the cost benefit is now leaning towards fiber.

The primary wavelengths of light used in fiber optic communication are 820, 1300 and 1550 nanometers (nm) because it has been found that these wavelengths of light are attenuated the least as they travel through the fiber optic medium. Compatible ports between the IED and Ethernet Switch must operate at the same wavelength of light and be linked with appropriate fiber. There are two categories of fiber optic cable: "multi-mode" and "single-mode." Note that until recently, the cable used with 820nm wavelength light was offered only in multi-mode while 1300 and 1550nm wavelength light uses both single and multi-mode compatible fiber optic cable. If you purchase a multi-mode patch cable it will typically be orange and a single-mode patch cable will be yellow.

There are differences between multi-mode and single-mode cable. The principle of operation of light transmission in a fiber cable is that for a range of light injection angles, the index of refraction at the surface between the core and the cladding is such that there is total internal reflection of the light being transmitted down the core. Imagine that the clad is a tube whose interior surface is polished so smooth, it is like a mirror. Light shinning at one end of the tube will either travel straight down the tube or will travel down the tube by reflecting off of the inner mirrored surface. The primary difference between single-mode and multi-mode fiber is the diameter of the core of the fiber. Multimode has a larger core diameter and, as such, supports multiple injection angles resulting in a substantial amount of input pulse spreading. Single-mode fiber can be described as an elongated lens that is continuously focusing the light into the center of the fiber. Using these two analogies, it can be imagined that in the single-mode fiber more light travels through far less fiber medium resulting in far less attenuation per unit distance than it does in multi-mode fiber. As a result, for a given wavelength of light, single-mode fiber typically has less attenuation per unit distance than multi-mode fiber.

Both multi-mode and single-mode fiber cables can support a wide range of light wavelengths but the most common wavelengths are 820, 1300, and 1550nm. Figure 3 is a fiber cross-section and physical specification of multi-mode and single-mode fiber cables. This figure is a scaled drawing of both a 62.5/125 µm multi mode fiber and 9/125 µm single mode fiber. The outer clad of both is 125 micrometers in diameter. The multi-mode core, at 62.5 micrometers, is a little bit thinner than the average human hair. The core of the 9/125 micrometer fiber is 9 microns in diameter (almost an eighth of that of the multi-mode fiber) surrounded by a second outer clad. Figure 4 further shows the difference between multi-mode and single-Mode fiber cables and attenuation.

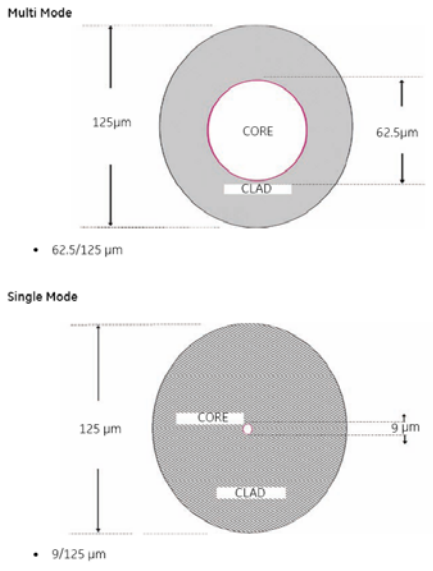

Fig. 3. – Fiber Cable Cross Sections and Physical Specifications

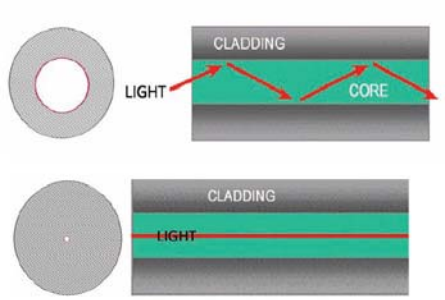

Fig. 4. – Differences between Multi-Mode and Single-Mode Fiber Cables

C. Optical Power Budget

Often the question arises regarding "What is the maximum practical communication distance when using a fiber optic cable?" The answer isn't straightforward, but can be calculated as described below.

First the "Optical Power Budget" is determined by subtracting the receiver's rated sensitivity from the transmitter's rated output power, both of which are defined in decibels (dB) of light intensity. For example if a particular transmitter is rated at minus 15 dB and the receiver's sensitivity is rated at minus 31 dB, the difference of 16 dB is the "Optical Power Budget."

The Optical Power Budget can be thought of as the maximum permitted attenuation of the light signal as it travels from the transmitter to the receiver, while still permitting reliable communication.

The next step is to calculate the worst case Optical Power Budget by subtracting from the Optical Power Budget 1 dB for LED aging and 1 dB for each pair of connectors (referred to as "insertion loss").

Optical Power Budget (OPB) =

Transmitter Output Power – Receiver Sensitivity

Worst Case OPB = OPB - 1dB (for LED aging) – 1dB (insertion loss for each pair of connectors) x number of pairs

The final step is to divide the calculated result by the rated cable loss per kilometer to determine the maximum distance. For costly installations, it is recommended to always measure the actual cable loss before and immediately after the installation to verify that the cable was installed correctly. To avoid damaging the receiver, ensure that the maximum optical input power of the receiver is not exceeded.

Worst case distance = [Worst case OPB, in dB] / [Cable Loss, in dB/Km]

Where the "typical cable loss" are:

- 62.5/125 µm and 50/125 µm is 2.8 dB/km
- 100/140 µm (Multi-mode, 850nm) is 3.3 dB/km
- 9/125 µm (Single-mode, 1310nm) is 0.5 dB/km (a worst case industry number)
- 9/125 µm (Single-mode, 1550nm) is 0.2 to 25 dB/km

These are typical cable losses. There will be deviations depending on the manufacturer. Always measure the loss before installation.

D. Fiber Optic Connectors

There are several styles of connectors used to terminate fiber optic cabling (ST, SC, and LC). ST and SC connectors are some of the more popular. MTRJ connections are becoming available on IEDs. It is important to make sure the Ethernet switch and connected IEDs have similar fiber connectors or fiber patch cables may have to be used from the IED to the Ethernet switch. The Fiber Optic ports on the IED and the Ethernet switch are not auto-negotiating and one must select proper hardware (connector and baud rate) on IEDs and Ethernet Switches to be compatible. Figure 5 shows ST, SC, LC and MTRJ connectors. ST fiber connectors are twist-lock type. SC, LC and MTRJ type connectors are snap-on type. ST, SC and LC based cables have separate cables for transmit and receive signals, whereas on MTRJ based cables, the two fibers are merged into a single connector.

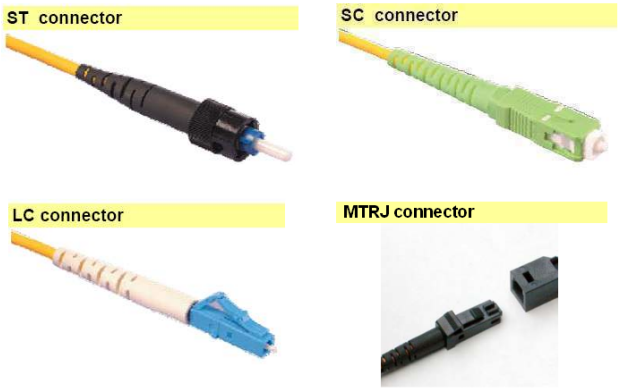

Fig. 5. – Common Fiber Optic Connectors

E. Fiber Optic – Full and Half Duplex

A half-duplex fiber optic system provides for communication in both directions, but only one direction at a time and not simultaneously. Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying. An example of a half-duplex system is a two-party system such as a "walkie-talkie" style two-way radio, wherein one must use "Over" or another previously-designated command to indicate the end of transmission, and ensure that only one party transmits at a time, because both parties transmit on the same frequency.

A full-duplex fiber optic system allows communication in both directions, and, unlike half-duplex, allows this to happen simultaneously. IEDs at each end of a full duplex link can send and receive data simultaneously over the link. Land-line telephone networks are full-duplex, since they allow both callers to speak and be heard at the same time. A good analogy for a full-duplex system would be a two-lane road with one lane for each direction. The full-duplex link can theoretically provide twice the bandwidth of normal (half-duplex) Ethernet link/connection. An IED at the end of a full-duplex Ethernet link does not have to listen for other transmissions or for collisions when sending data. 10BaseT, 10BaseFL, 100BaseTX, and 100BaseFX signaling systems can support full-duplex operation. It is recommended to use full-duplex whenever possible or available.

F. Ethernet – Copper Auto-Negotiation

Auto-Negotiation is the function of automatically detecting the maximum speed at which an nBaseT (copper) system can operate. Auto-negotiation is an Ethernet procedure by which two connected devices choose common transmission parameters, such as speed and duplex mode. In this process, the connected devices first share their capabilities for these capabilities and then choose the fastest transmission mode they both support.

Auto-negotiation can be used by devices that are capable of different transmission rates (such as 10 Mbps and 100 Mbps) and different duplex modes (half-duplex and full-duplex). Every device declares its technology abilities, that is, its possible modes of operation via “Link Pulses” sent from the Transmit port of each connected device. The two devices then choose the best possible mode of operation that are shared by the two devices, where higher speed (100 Mbps) is preferred over lower speed (10 Mbps), and full-duplex is preferred over half-duplex at the same speed.

Auto-negotiation is not available on fiber optic Ethernet ports of IEDs or Ethernet switches as the Ethernet speed is related to the light wavelength. 10MB fiber uses 820nm as the transmission wavelength whereas 100MB fiber uses 1300nm. One must select proper hardware (connector and data rate) on IEDs and Ethernet Switches to be compatible when using fiber optic communications.

IV. Network Topologies

With either copper or fiber optic media, supported topologies include: star, mesh and ring architectures. The port that connects one Ethernet switch to another is often called the uplink port. With many Ethernet switches, the uplink port can operate at much higher baud rates than the standard ports. The link formed by the connection of several Ethernet switches’ higher speed uplink ports is often referred to as a “Backbone”. Figures 6, 7 and 8 respectively show the Star, Full Mesh and Ring network topologies.

For the Star architecture, a single point of failure causes a loss of communication.

A mesh network is a LAN that employs one of two connection arrangements - either full mesh topology or partial mesh topology. In the full mesh topology, each node is connected directly to each of the others. In the partial mesh topology, some nodes are connected to all the others, but some of the nodes are connected only to those other nodes with which they exchange the most data. For a mesh architecture or topology, multiple points of failure are required before a loss of communications and additional cabling is required.

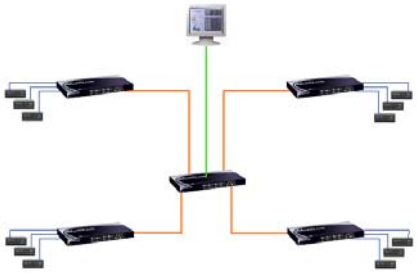

Fig. 6. – Star Network Architecture

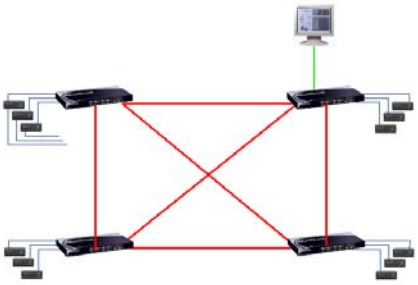

Fig. 7. – Full Mesh Network Architecture

Fig. 8. – Ring Network Architecture

A Ring architecture, by its design, provides network redundancy and using proprietary techniques, has a failure recovery time of 5 milliseconds per Ethernet switch or hop, and is the most cost effective solution. We will discuss configuration of a ring architecture or topology using Ring Mode and RSTP later in the paper.

A. Integrated Ethernet Switch in IED

Another efficient way of networking IEDs is to use IEDs that have an integrated Ethernet switch. Traditional architectures using discrete Ethernet Switches require one Ethernet switch for approximately 12 IEDs when using redundant fiber optic communications and require point-to-point Ethernet cabling and physical space to mount the external Ethernet switches.

When the Ethernet switch in integrated into the IED, there is a reduction in network connections and hardware. The IED is internally connected to the Ethernet switch through internal hardware. In addition, the last IED can be connected to the first IED to create a redundant ring network. All IED Ethernet communications goes through the switch module. Figure 9 shows a traditional architecture using external / discrete Ethernet Switches and a more efficient ring architecture using IED's integrated Ethernet Switches.

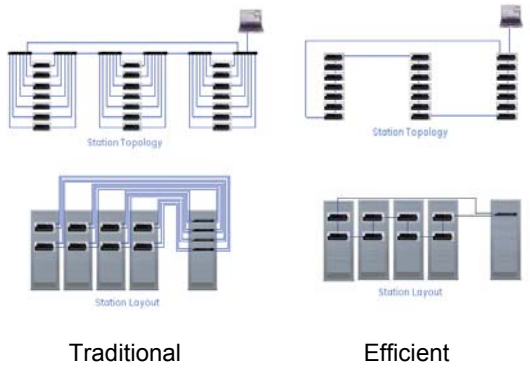

Fig. 9. – Traditional Architecture using External Ethernet Switches and Efficient Architecture using Internal IED Ethernet Switches

B. Connecting Serial Devices to Network

A port serial sever converts serial RS-485 or RS-232 signals into TCP/IP over Ethernet, such as Modbus, DNP (Distributed Network Protocol) protocols or any other serial protocol. Serial port servers are able to communicate with many devices using multiple serial ports (for example – 128 serial devices). Each serial port can have a different serial baud rate of up to 115kbps. Individual "TCP port" settings are used for each serial port with a single IP address in the port serial server. Some port serial servers include an integrated managed multi-port Ethernet switch with copper and/ or fiber Ethernet connectors. Figure 10 shows a typical architecture.

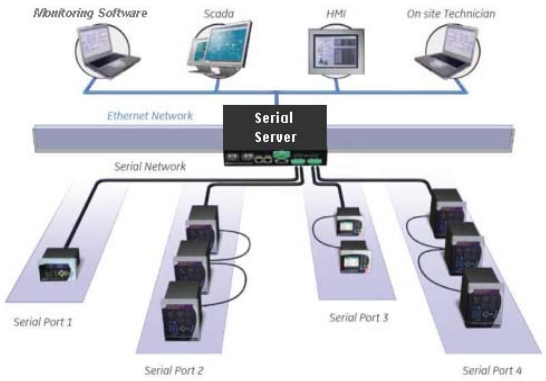

Fig. 10. – Typical Architecture using a Serial Port Server

C. Rapid Spanning Tree Protocol (RSTP)

When a number of switches are connected in a redundant configuration, and when one of the components fails, there is a need to detect the failure and to re-configure the communication paths. The IEEE standard that performs this function is known as the Rapid Spanning Tree Protocol or RSTP. This protocol sends out messages to the various nodes in the network to detect the broken paths and to then perform the re-configuration. RSTP works in Star, Ring, and Mesh configuration, but can take "seconds" to operate.

A unique requirements for the protection and control industry is to be able to "quickly" recover from network problems. There are several proprietary network recovery implementations that require the switches/devices to be configured in a Ring with no Mesh components. These proprietary implementations can operate in the 3 to 5 ms per Ethernet switch time frame. Figure 11 shows a ring mode only architecture.

Note that the proprietary recovery modes (i.e. ring only mode) has been tested and validated in rings of up to 106 Ethernet switches.

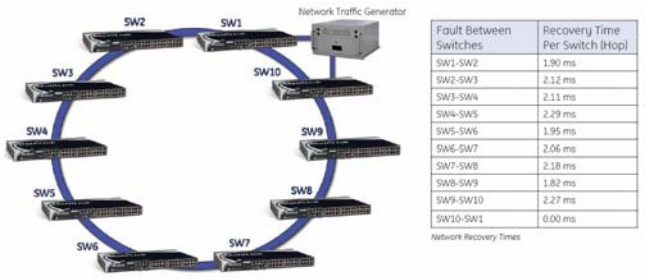

Fig. 11. – Example of Network Fault recovery testing using SMART RSTP in a Ring Network Architecture

D. Link Detection/Link Loss Alert Technology

The transmit ports of an Ethernet device, when idle; always send out "Link Pulses". These pulses are used to detect basic connectivity as well as device communication capability as described earlier with regard to Auto-Negotiation. When a receiver loses link, this implies that there is a problem and the system needs to switch to any alternate communication paths.

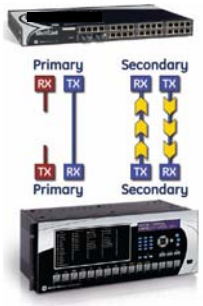

Fig. 12. – Link Loss Alert allows Recovery from a Broken Fiber Connection

In addition, the link loss alert function of an Ethernet Switch allows for protective relays or IEDs to recover from situations where only one of the two fiber cables connected to the IED is damaged. The Link loss alert function can be implemented with both 10Mbps and 100Mbps fiber ports and allows for seamless switching to the IED's secondary port under all network fault conditions. Upon detection of the broken transmit fiber, the Ethernet switch will cease sending a link pulse to the IED's receive fiber cable, thereby allowing the IED to switch to its secondary port. Figure 12 shows how link loss alert function allows recovery from a broken fiber connection.

E. Ethernet over Wireless

Use of 900 MHz radios is a cost effective way to transport secure information from remote locations that cannot be connected with direct fiber due to budget restraints or terrain. Distances of approximately 25-30 miles with a maximum data rate of 1Mbps can be achieved with 900 MHz radios. Field applications exist today where industrial and utility companies are using 900Mhz radios interfaced with Ethernet based IEDs for data and control. Both Modbus TCP/IP and DNP TCP/IP applications are in service today throughout the world.

F. Ethernet over SONET Considerations

Many utility and industrial locations have implemented SONET networks (Synchronous Optical NETworks) that multiplex many forms of information such as video, voice, serial data, Ethernet data (10, 100, and 1000 Mb speeds) and I/O (teleprotection). It is important to note that if your company has a SONET network that you have a high bandwidth backbone that can support high speed Ethernet networks. Figure 13 lists the potential Ethernet "backbone" that one would have at different SONET levels. For example at OC-3, one would have a 155Mbps – capable of hosting multiple 10Mb and one 100Mb Ethernet networks.

	LINE RATES (Mbps)	# OF 64 kbps CHANNELS
T-1	1.544	24
OC-1	51.84	672
OC-3	155.52	2016
OC-12	622.08	8064
OC-48	2488.32	32256

Fig. 13. – SONET Backbone Network Speeds

G. Virtual Local Area Networks (VLANs)

VLAN is short for "Virtual Local Area Network." A VLAN creates separate "virtual" network segments that can span multiple Ethernet switches. A VLAN is a group of ports designated by the Ethernet switch as belonging to the same broadcast domain. One can think of a VLAN as a piece of Ethernet coaxial cable and all the devices connected to that cable. VLANs provide the capability of having multiple networks co-existing on the same Ethernet switch. Two advantages of VLANs are the separation of traffic and

security. VLANs can be port based or tag based. Port based VLANs assign a specific port or group of ports to belong to a VLAN. When using tag based VLANs, a tag called a VLAN identifier is sent as part of the message. Note that the addition of this tag in an Ethernet message also includes the addition of a Priority flag – discussed later. This tag allows the message to move across multiple Ethernet switches whose ports are part of the same tagged VLAN. Tagged VLANs and priority (QoS) are used within IEC61850 GOOSE messaging.

The IEEE 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames. VLANs provide the capability of having two (or more) Ethernet segments co-exist on common hardware. The reason for creating multiple segments in Ethernet is to isolate broadcast domains. VLANs can isolate groups of users, or divide up traffic for security, bandwidth management, etc. VLANs need not be in one physical location. They can be spread across geography or topology. VLAN membership information can be propagated across multiple Ethernet switches. Figure 14 illustrates a VLAN as three separate broadcast domains. Depending on the switch, up to 32 VLANs can be defined per Ethernet switch.

A group of network users (ports) assigned to a VLAN form a broadcast domain. Packets are forwarded only between ports that are designated for the same VLAN. Cross-domain broadcast traffic in the Ethernet switch is eliminated and bandwidth is saved by not allowing packets to flood all ports. For many reasons, a port may be configured to belong to multiple VLANs.

Figure 15 shows an example of VLAN traffic (VLAN #5) from one relay (R1) sending IEC61850 GOOSE messages to other subscribing IEC61850 relays (R3, R4, R6, R7) on the network.

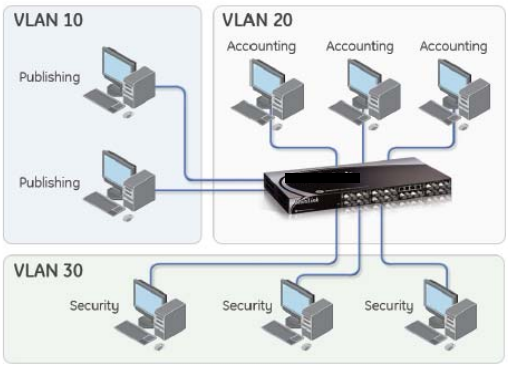

Fig. 14. – VLAN as Three Separate Broadcast Domains

H. Priority using Quality of Service (QoS) for IEC61850 GOOSE Messages

Quality of Service (QoS) provides the ability to prioritize traffic on the Ethernet network. Prioritizing traffic into different classes is important to ensure critical data is processed first (i.e. protection traffic, data, voice or video). Not all traffic in the network has the same priority. Being able to differentiate different types of traffic and allowing this traffic to accelerate through the network improves the overall performance of the network and provides the necessary quality of service demanded by different users and devices. The primary goal of QoS is to provide priority processing of a packet inside of the Ethernet switch.

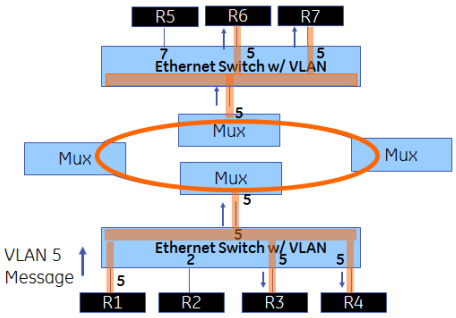

Fig. 15. – Example of VLAN Traffic from One Relay sending a IEC61850 GOOSE Message to Other Relays on the Network.

IEC61850 GOOSE messaging provides a priority setting with eight levels of priority. When processed in an Ethernet switch, the message with the "highest" priority is moved to the front of the queue as shown in Figure 16.

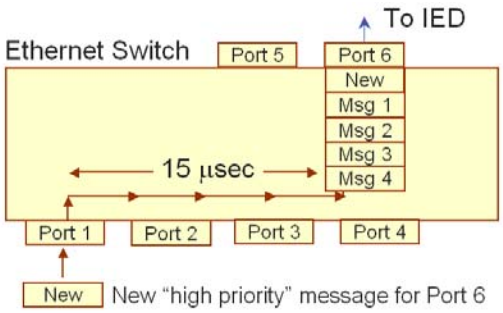

Fig. 16. – Example of Priority for IEC61850 GOOSE Messages

I. Applicable Ethernet Switch Standards and Considerations Relevant to the Protection Engineer and Environment

When using Ethernet switches in harsh environments, such as chemical plants, paper mills, oil refineries, water & waste water facilities and power plants, one should consider using hardware that is conformal coated. This ensures product function and viability in corrosive or other environments that can damage typical electronic equipment. Reliability is greatly improved when using the conformal-coated hardware.

An important consideration when selecting an Ethernet switch for your protection and control application is to make sure that the Ethernet switch complies with all required certifications and with all major International Standards for networking communications including: UL Listed/CE Agency Approved, IEC61850-3, IEEE 1613, NEBS Level 3, ETSI Certified, NEMA TS2, MIL-STD-167.

Redundant power supplies are offered on Ethernet switches and provide options for full power redundancy with

support for two power supplies. These power supplies can be of the same type, or of mixed voltage types to ensure even greater reliability through diverse power sources.

J. Redundant Networks or Redundant IED Ports Considerations

It is common in most facilities to have a single point connection from the IED to the network. As IEC61850 GOOSE messaging is becoming more widely used in both industrial and utility applications, reliability of these critical messages could be improved by using redundant Ethernet networks, redundant power supplies on the Ethernet switches and redundant fiber optic Ethernet ports on the IEDs. When IEC61850 GOOSE messaging is used for protective functions, reliability and redundancy of the communication network should bear the same considerations as the reliability and redundancy of the protective IEDs.

Per IEEE Power System Relaying Committee Working Group WG119 report [2], the following recommendations are made when using IEC61850 for critical applications:

"*1. Connect multiple switches in a ring, so that there are at least two paths from any switch port used by a relay to any other such switch port. Ethernet switches include the failover service called rapid spanning tree protocol (RTSP) by which the switches discover and use a normal or default message path without circulating messages forever in a loop – one link in the loop is blocked to achieve this. If the ring suffers a break or if one switch fails, the switches can detect the path loss and immediately set up new routing of messages by unblocking the spare path to maintain communications.*

2. Many GOOSE-capable relays have primary and failover communications ports. Provide two switches or switch groups within the redundant Set A, and also in Set B. Connect the relay's primary port to one switch or switch group, and connect the relay's failover port to the other switch group."

K. Utility and Industrial Network Architecture Considerations

As shown previously in Figure 1, it is possible to direct connect Ethernet switches from each location using single-mode fiber up to 70km between sites. For example, small or medium sized electric utilities could interconnect their substations using single-mode fiber cabling and the necessary Ethernet switches to create a DNP Supervisory Control and Data Acquisition (SCADA) network without the use of Remote Terminal Units (RTUs). Today's protective relay IED have the capability to restrict the data sent (analog inputs and binary inputs) for a DNP class 0 integrity poll by the SCADA master. In addition, other TCP protocols such as Modbus and Synchrophasors (IEEE C37.118) can be used simultaneously on the same network with the added benefit of the capability to remotely make setting changes and access critical operation data (events and waveforms).

Ethernet networks in industrial facilities are very common and connecting today's IEDs to the network is a very efficient way to transport metering data and perform IED control from a Distributed Control System (DCS) and other systems in the facilities. Many industrial facilities are also installing monitoring systems for their electrical system that can automatically retrieve real-time event data waveform data.

V. Testing

There are several tools that are recommended when testing or monitoring the messages on an Ethernet network.

The PING command (type PING at the DOS command prompt). For example, type ping 192.168.0.133 and press Enter and you can verify connection to an IED by pinging the IED's IP address (see Figure 17). Follow the command by a "-t" to continuously ping the IED every 1 second so you can check the connection to the IED or Ethernet Switch.

```
D:\>ping 192.168.0.133

Pinging 192.168.0.133 with 32 bytes of data:

Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\>ping 192.168.0.133 -t

Pinging 192.168.0.133 with 32 bytes of data:

Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255
Reply from 192.168.0.133: bytes=32 time<1ms TTL=255

D:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.192
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DHCP Class ID . . . . . . . . . . : efe
```

Fig. 17. – Use of PING and IPCONFIG Commands

If a message of "Request timed out" or "Hardware error" is returned, Ethernet connectivity to the device is not present. In this case, the connection between computer, Ethernet switch and devices/IEDs should be checked (especially to see that they are powered), that the Ethernet connectors are properly seated, and that link (Link Light ON) has been established. For fiber cable, this may be simply just switching the transmit and receive fibers. For a copper Ethernet cable, you may have to change the cable or put new RJ45 connectors on the cable.

Also check that the correct IED IP address is in place. The IPCONFIG command may also be used to make sure computer IP address is properly set as shown in Figure 17.

Other useful tools for capturing and analyzing network traffic and IEC61850 GOOSE messages are called Ethereal and WireShark. They are available for no-charge from the SISCO web site:

http://www.sisconet.com/downloads/mms_ethereal_install_v120.exe

http://www.sisconet.com/downloads/mmswireshark200.exe

Figure 18 shows how an IEC61850 GOOSE message can be analyzed with Ethereal.

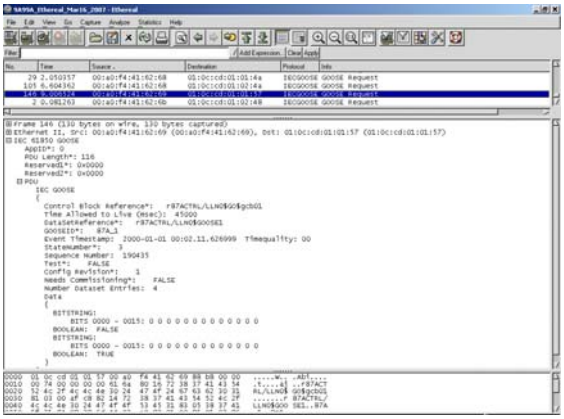

Fig. 18. – Use of Ethereal to Analyze IEC61850 GOOSE Messages

VI. IP AND SUBNET MASK ADDRESSING

A. IP Addressing

IP address is short for Internet Protocol address. The IP address is the address of a computer or IED that is connected to a network. It is in many ways similar to a combination of your house address and your zip code. Senders of mail must have knowledge of your address. This knowledge is obtained either through a service called a Domain Name System (DNS) or from your local address book. When the Internet was invented it was never envisioned that there would be hundreds of millions of computers connected, so the address system is limited.

The present protocol (IP ver. 4) uses a 32-bit number that is divided into four octets or bytes (8-bit sections), each octet being in the range 0 to 255. Each octet is separated by a decimal point and this type of format is commonly called 'dotted decimal notation' (e.g. 3.179.249.17, pronounced three dot one seventy nine dot two forty nine dot seventeen). So the lowest number is 0.0.0.0 and the highest is 255.255.255.255. Note that a new version of the IP protocol is now available and is known as IP ver. 6. The new version of the IP protocol has and address range of 128 bits – or about 3.4 x 10^{38} addresses.

It is important to remember that dotted decimal notation described above only exists to aid human beings to understand IP Addresses, computers just use a long series of 1's and 0's.

IP address are classified into four class's (groups) depending on the decimal equivalent of the 1st octet in the address as below.

0-255.xxx.xxx.xxx = all address's

Class A - Intended for a small number of networks that had a large number of computers (hosts) attached. Class A IP Addresses have a value in the range of 1 through 126 as the first octet. The values 0 and 127 are not available because they have special uses. Class A addresses use the first octet to identify the network which means that 126 addresses are usable, each of which can support 16,777,216 computers (hosts).

Class B - Intended for some networks that had an intermediate number of computers (hosts) attached. Class B IP Addresses have a value in the range 128 through 191 as the first octet. Class B addresses use the first two octets to identify the network which means that 16,320 addresses are usable, each of which can support 65,536 computers (hosts).

Class C - Intended for a large number of networks that would have a small (relatively) number of computers (hosts) attached. Class C IP Addresses have a value in the range 192 through 223 as the first octet. Class C addresses use the first three octets to identify the network, which means that 2,080,800 addresses (networks) are possible, each of which can support 254 computers (hosts).

Class D – is a range of addresses known as "Multicast" addresses. These addresses are used when information needs to reach a group of receivers and is typically used for streaming data. An example of a use for a Multicast address is Synchrophasors where a set of Synchrophasors is desired at multiple locations. The range of IP Multicast addresses is 224.xxx.yyy.zzz to 239.xxx.yyy.zzz

B. Subnet Mask Addressing

A subnet is the concept of taking a large number of Host addresses in the IP Host address range and breaking the address down into a sub-network (subnet) and a number of host computers that are part of the respective sub-networks. This mechanism minimized the amount of work that a router must perform when routing a message to a host address. In order to facilitate this task, a mask (or number) is used to determine the number of bits used for the subnet and host portions of the address. The subnet mask is a 32-bit value that uses one-bits for the network and subnet portions and a combination of ones and zeros to identify a specific subnet in which a host is located.

The subnet mask plays a crucial role in defining the size of a subnet. Whenever you're dealing with subnets, it will come in handy to remember eight special numbers that reoccur when dealing with subnet masks. They are 255, 254, 252, 248, 240, 224, 192, and 128. You'll see these numbers over and over again in IP networking, and memorizing them will make your life much easier.

C. Recommendations for IP Addressing in a Utility Substation or Industrial Facility

The following IP address ranges are allocated as private, non-routable (externally) addresses:

Class A:	10.0.0.0 to 10.255.255.255
Class B	172.16.0.0 to 172.31.255.255
Class C	192.168.0.0 to 192.168.255.255

The above Class A address range would allow 16,777,216 addresses (256 x 256 x 256), 1,048,576 (16 x 256 x 256) addresses for Class B and 65,536 (256 x 256) for Class C.

The Natural subnet mask addresses (that is, allowing any subnet to pass) for the above three classes are:

Class A:	255.0.0.0
Class B:	255.255.0.0
Class C:	255.255.255.0

Note that IEC61850 GOOSE messages do not use the IP, subnet mask, nor gateway addresses. They use the Ethernet Media Access Control (MAC) address and GOOSE ID (or GO ID). A subnet address of 0.0.0.0 will not allow the IEDs/devices to communicate on the network even if the IP address is set correctly. If you have the IP address set correctly, you could set the subnet mask address to 255.255.255.255 for testing purposes, which allows the IED to communicate on any subnet.

For utility substation or industrial facility applications spread over a large private network, we recommended considering setting the IP addresses as follows. Let us use the Class A private address range that starts with 10.0.0.0 and use Octet 2 as the "district or territory" identifier, which will allow 256 districts or territories. Then configure Octet 3 to the "substation number" identifier, which will allow 256 substations per district or territory. Finally, use Octet 4 to assign the IEDs in the substation or site, which allows for 256 IEDs per substation or site. Figure 19 details this IP setting recommendation.

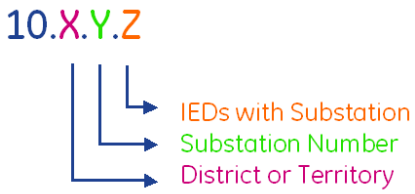

Fig. 19. – Recommended IP Address Configuration for Private Substation Networks

VII. Conclusions

Over the past decade, Ethernet has become a popular networking technology because of its low cost, high bandwidth, and versatile support of multiple protocols and services. There are numerous network topologies that can be implemented and the best topology is a ring. Redundant ring networks, redundant fiber optic ports on IEDs and redundant power supplies can be used for critical protection applications in the substation and industrial facility. Ethernet switch functions such as Rapid Spanning Tree Protocol (RSTP), Virtual Local Area Networks (VLANs), Quality of Service (Qos) and Link Loss Alert allow utility and industrial protective engineers to create networks with high reliability and availability. Finally, it was recommended to use Class A private, non-routable (externally) address of 10.x.y.z for utility substation or industrial facility applications spread over a large private network, which allows 16,777,216 addresses.

VIII. Biographies

Craig Wester is the southeast US Regional Sales Manager for GE Digital Energy Multilin in Norcross, Georgia. He was born in Belgium, Wisconsin, and received a B.S. in Electrical Engineering with a strong emphasis on power systems from the University of Wisconsin-Madison in 1989. Craig joined General Electric in 1989 as a utility transmission & distribution application engineer. He is a member of the IEEE.

Mark Adamiak is the Director of Advanced Technologies for GE Digital Energy Multilin and is responsible for identifying and developing new technology for GE's protection and control business. Mark received his Bachelor of Science and Master of Engineering degrees from Cornell University in Electrical Engineering and an MS-EE degree from the Polytechnic Institute of New York. Mark started his career with American Electric Power (AEP) in the System Protection and Control section where his assignments included R&D in Digital Protection and Control, relay and fault analysis, and system responsibility for Power Line Carrier and Fault Recorders. In 1990, Mark joined General Electric where his activities have ranged from advanced development, product planning, application engineering, and system integration. Mr. Adamiak has been involved in the development of both the UCA and IEC61850 communication protocols, the latter of which has been selected as a NIST Smart Grid protocol. Mark is a Fellow of the IEEE, a member of HKN, past Chairman of the IEEE Relay Communication Sub Committee, a member of the US team on IEC TC57 - Working Group 10 on Utility Communication, the US Regular Member for the CIGRE Protection & Control study committee, a registered Professional Engineer in the State of Ohio and a GE Edison award winner for 2008.

IX. References

[1] IEEE Std 802.3™-2008, IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks, Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

[2] Paper – Redundancy Considerations for Protective Relaying Systems (IEEE PSRC WG 119), presented at 2010 Texas A&M Protective Relaying Conference, April 2010.

[3] MultiLink - Ethernet Communications Switch - Quick Start Guide (GEK-113393B)

[4] MultiLink ML2400 - Ethernet Communications Switch - Instruction Manual (GEK-113042M)