

Review of Digital Substation Communication Technologies

Galina S. Antonova, Shashi Sastry, Bharadwaj Vasudevan

Hitachi ABB Power Grids

Canada and USA

galina.s.antonova@hitachi-powergrids.com

Abstract

This paper contains a review of communication technologies commonly used for digital substations. It provides communications fundamentals, comparative analysis, standard references and recommendations, based on experiences from deployed digital substation projects. Fundamentals and protocols used for communication redundancy are included, as a topic of common confusion. Discussions based on field installations are used to illustrate the main points made.

1. Introduction

In place of conventional copper wire connections, digital substations rely on the exchange of electrical signals represented as values in data communication streams. The choice of communication technology, media, and architecture are crucial in achieving the required availability and reliability of the overall composite protection systems that include communication channels. The scale of engineering efforts, as well as its impact on the scheme's operation and maintenance are also important contributing factors.

Communications field is wide and varied. Due to the complexity of protection and control applications, making proper communications choices, in general, is a difficult task. Communications as well commonly fall beyond the area of expertise and even basic knowledge for most protection and control engineers. With growing number of digital substations deployed and digitalization clearly being a future of power and many other industries, a review of communication technologies standardized for use in digital substations today is very timely and much needed. Such review will help to educate and empower the audience and assist in making better and well-informed decisions.

The paper provides a clear and concise review of the standard communication technologies specified for use in digital substations. For ease of understanding, terms and analogies from protection, control and human communication worlds are used to explain technical communication concepts. Empowered by the newly received knowledge the audience will be able to make better communication choices, as well as revisit and revise communications-related decisions already made.

The paper is organized as follows. First, communications basics and fundamentals of Ethernet Layer 2 communications over a fiber optic media are covered, as the main method specified for digital communications by the IEC 61850 group of standards. Software Define Networking (SDN), as a technology at times applied for digital substations is reviewed next. Review of communication redundancy concepts and protocols follows. This is a critical part in maintaining high availability yet is known to cause confusions. A discussion on network architectures, and their reliability completes the analysis. Learnings from the deployed digital substation projects are used to illustrate the discussion. Finally, conclusions summarize the main points.

2. Communication Technologies used for Digital Substations

Communication data streams are used in digital substations to exchange binary signals (commands and status) and receive analog data (digital samples of voltages and currents). Layer 2 Ethernet has been specified by the IEC 61850 group of standards as the communication method for digital substations [1]. Its historic predecessor, Utility Communication Architecture (UCA) as well uses Ethernet communications (and bit pairs for increased reliability). Use of fiber optical communications media is defined and preferred over copper and air due to fiber's Electro-Magnetic Compatibility (EMC) characteristics and immunity to variety of disturbances commonly present in electrical power substations.

This section provides high level communications fundamentals and describes Ethernet technology, focusing on specific features that make performance of Ethernet networks sufficiently reliable and nearly deterministic, while keeping its configuration and setup needs minimal.

Next it describes the operating principles of Software Defined Networking (SDN) to explain its operation and shows how it essentially uses the same mechanisms as the standard Ethernet yet requires through configuration and per-stream engineering to achieve similar performance level in a non-standard way.

2.1 Communications Fundamentals

To explain communication technologies used for digital substations, at least a basic understanding of overall communications fundamentals is required. This subsection provides a concise summary sufficient for the concept discussed in this paper. For more information an interested reader can refer to a lecture/presentation format in [2]. Comprehensive information on this topic is also available in IEEE PSRC H9 Report [3].

As in human communications, data/signals communication include a data source (transmitter or sender) and a recipient or recipients (receivers or destinations). The source needs to put the data into an understandable by the receiver format. This could include data encoding and framing, for example. The receiver needs to receive and decode information, like human mind needs to understand the words it has just heard.

Digitalization process – the origin of 64Kbits/s channel

Digital communication (as opposed to analog signal exchange, e.g., in legacy telephone networks) uses digital data. Many channel banks commonly used in power utility communication systems today use 64Kbits/s channels to combine 24 such channels into a single T1 stream (at 1544Kbits/s). In Europe 32 64Kbits/s channels are combined into a single E1 link at 2048Kbits/s¹.

To illustrate the digitalization process of an analog signal, it is helpful to look at how 64Kbits/s channel was initially created. To digitize analog voice communication that occurs in 300-4000KHz frequency range, sampling at double the highest frequency, i.e., at 4KHz x 2 = 8KHz was performed, per Nyquist-Shannon criteria. Then the samples obtained were encoded as 8-bit value, resulting in 8KHz x 8 bits = 64Kbits/s data rate. This process is shown on Figure 1 below. As seen on the picture, digital values are pre-determined (are not continuous). While the closest digital value to the analog value is used, there is still commonly an error. The maximum size of such error is essentially the difference between closest digital values, called quantization step or a resolution. The error itself is referred to as quantization error. So, the better the resolution (the smaller quantization steps) the closer digital values are to the analog values, and the smaller the quantization error.

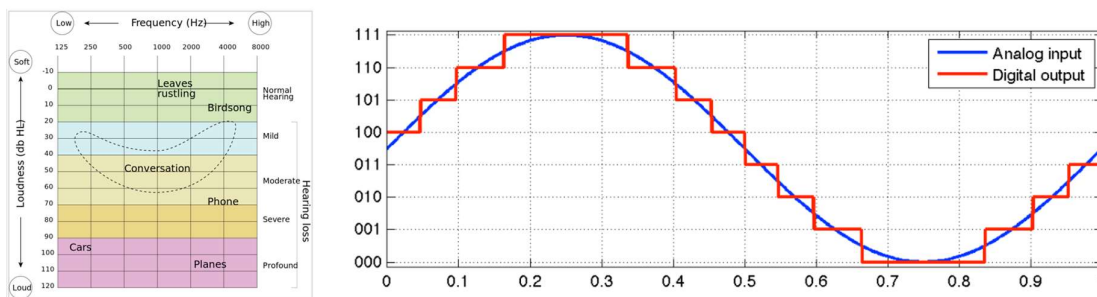


Figure 1 Digitalization of analog voice: formation of 64Kbits/s channel

Bits and Bytes

Communicated data represents electrical signals as a bit (a single one or zero), just like one copper binary input or output that can be set or reset, or bytes (a set of 8 bits). To grasp the scale of data exchange capacity, the smallest Ethernet frame is 64-bytes long in total, refer to Figure 10 in Ethernet section 2.2. Without the header (which mainly contains Source and Destination MAC Addresses), 46 bytes are available for the actual data. This means that the smallest Ethernet frame can contain $46 \times 8 = 368$ control and status bits (for bi-directional communication), thus can replace 368 conventional copper binary inputs and outputs. The largest Ethernet frame is 1518-bytes long or 1522-bytes long with VLAN tags (unless it is a jumbo frame with 9K bytes) and has 1500 data bytes that can replace $1500 \times 8 = 12000$ conventional copper binary inputs and outputs.

¹ It is interesting to note that one Kbit (kilobit) contains 1048 not 1000 bits.

Protocols

A common language understood by a transmitter and a receiver is called a “protocol”. The earliest and simplest protocol examples are a semaphore or Morse Code. Various communication protocols exist with various functions. Their functions are performed at one particular Layer (a shelf if one wishes), of an Open System Interconnect (OSI) model.

7-layer OSI model

Like protection engineers, communication engineers create and use abstract models. Protection world abstractions are, for example, positive, negative and zero sequence components. The most abstract concept in the communication world, is a 7-layer OSI model, that is nothing more than a division of complete communication functionality into 7 different steps/shelves or layers. Let us find analogies in human communications to explain these 7 Layers, refer to Figure 2.



Figure 2 Explaining 7-Layer OSI model using human communication analogy

In human communication, at the top Layer 7 (Application Layer) a thought could be formed in one’s mind. At Layer 6 (Presentation Layer), a sentence on how to express this thought gets formulated. At Layer 5 (Session Layer) a connection between data source and recipient is established. In human communication this could be making an eye contact, for instance. At Layer 4 (Transport Layer) the sentences are organized in the best order. Well-known protocols such as Transport Control Protocol (TCP) and User Datagram Protocol (UDP) reside on this Layer. At Layer 3 (Network Layer), data is delivered from sender to recipient. In our example a person may walk across a room to a person he or she wishes to talk to. Well-known Internet Protocol (IP) operates on this Layer using IP Addresses. IP protocol is described in Request for Comments (RFC) 791 [4]. At Layer 2 (Data Link Layer), the sentence gets “framed” with recipient’s name, an equivalent of a unique Media Access Control (MAC) Address. IEEE 802 and Ethernet protocols reside on this Layer. Both use MAC Addresses. Finally, at Layer 1 (Physical Layer), a person pronounces the words by engaging his or her vocal cords. Vocal cords act as a communication media in this case. Common communication medias in data communications are fiber, copper (including powerlines), and air (for wireless).

Error detection and correction

It is important to know that communication protocols typically include error correction mechanisms.

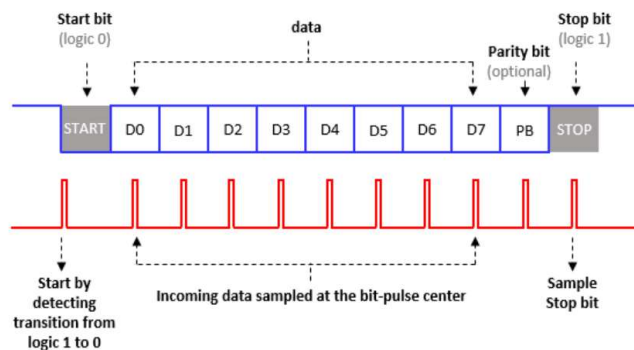


Figure 3 Simplest error detection mechanism

The simplest example could be configuring even or odd bit-parity for serial communication such as RS-232 or RS-485. This method requires a transmitter to set the last bit to 1 or 0 to make total number of 1s even or odd, so that a receiver can check and declare an error if even number of 1s is expected but odd number of 1s is received. This method is illustrated on Figure 3.

More complex error checking mechanisms include division of data by a known polynomial, and placing the remainder next to the data, into dedicated byte locations. Transmitter makes the calculation to determine and send the remainder along with the data. The receiver makes the division for the received data and compares its result with remainder received. If the two match it can declare that the data was received correctly. Such mechanism is called Cyclic Redundancy Check (CRC). Ethernet allocates 4 bytes (32 bits) for the remainder and uses CRC-32. The number (32 in this case) corresponds to the number of bits used in the calculation, and the size of the remainder. A 4-byte field called Frame Check is allocated at the end of Ethernet frame for this function. Note that not all errors are detectable by a CRC calculation. For more information, an interested reader could refer to the event analysis presented in [5]. It is interesting to note that some mechanisms don't only detect errors but are capable of correcting them.

Addresses

For data to arrive from a source to a destination, addresses and an addressing scheme are needed. One can think of unique Media Access Control (MAC) Addresses used at Layer 2, as unique people names. While IP Address used at Layer 3, could be thought of as mailing addresses that can and do change, when a person or a device relocate. Post office needs to know where each person lives so it maintains the correspondence between people's names and their mailing addresses to deliver their letters. In Internet communication Address Resolution Protocol (ARP) is used to establish correspondence between MAC and IP Addresses. This data is stored in co-called ARP Table. One can run an "arp -a" command in DOS Command Prompt on a laptop to view currently known by his/her machine IP and MAC Addresses. For detailed structure of MAC Address refer to Figures 11 and 12 in Ethernet section 2.2.

Communication Media and Interfaces

As mentioned before, communication media varies from copper (including powerlines for Power Line Carrier (PLC) communication) to fiber and air (used by all wireless technologies).

Communication cables (for wired technologies), terminals (also called connectors) vary as well. Serial 2/4-wire cables, Ethernet shielded, and unshielded twisted pair (S/UTP) copper cables are used. Copper cables category has evolved over time from coaxial cables to TP category (CAT) 5 to CAT-6 and CAT-6e (enhanced). Copper Ethernet cables can be straight (transmit wires connect to transmit terminals on both ends) or cross over (transmit wires on transmit connect to receive terminals on receive). Cross over functionality for serial communication is implemented in null modem cables. Terminals-wise, RJ-11, RJ-45, DB-9, DB-25 are in common use at the by the end point devices. Fiber optic cables include multimode and single mode fibers. Terminals vary from ST, LC and SC type. Details on Ethernet fiber optic cables and terminals are provided in section 2.2.

For fiber communications, common cables are colored in orange (for multi-mode fibers used for short-range communication), and in yellow (for single mode fibers for medium and long-range communication). As data in fiber optic cable is transmitted using light, generally speaking, it is very sensitive to bending. Commonly an acceptable bend radius is specified by a manufacturer. A bend-resistant blue colored fiber cable was developed to address this challenge. Such cable is known to provide reliable data transmissions after being wrapped around a pencil about 10 times.

Communication types

Communication type can be one to one (called unicast), one to many (multicast) or one to all (broadcast). Special destination addresses are assigned to differentiate these communication types. For example, IP Destination Address consisting of all 1s (255.255.255.255) is assigned for broadcast communication. Protocols like ARP or Internet Control Message Protocol (ICMP) use this broadcast IP address to determine the correspondence between MAC and IP Addresses, and to verifying IP connectivity using a well-known "ping" command). Multicast Destination Addresses only have particular bit(s) set to 1. Multicast Destination MAC Addresses, for example, have single bit, called Group bit set to 1, it is the least significant bit (LSB) of the most significant byte (MSB) of the Destination MAC Address. Refer to Figure 12 in Ethernet section 2.2.

Communication modes

There are 3 communication modes:

- Simplex (communication in one direction only, e.g., transmit only)
- Half-duplex (communication in one direction at a time, e.g., transmit during one time interval and receive during another time interval)
- Full-duplex (the ability to transmit and receive data at the same time)

Links and Commutators

From functionality perspective, it is very important to understand that all communication devices can be divided into 2 large groups only: those which move data from point A to point B, let's call these communication links. And those which can connect\switch\forward\route data. Let's call these data commutators. Communication links just provide transport for the data and do not make any switching decisions. Data commutators have multiple ports and do decide what to do with the data, i.e., whether and where to send it for example. Commutators also need to know where data recipients reside and store this information in dedicated internal tables.

Channel types

Next very important concept to understand the communication channel types that exist. This is related to the concept of communication equipment functions, specifically if only data transport or a variant of data switching is provided. Broadly speaking, 3 main communication channel types exist:

- Dedicated channels
- Multiplexed channels
- Switched channels

Dedicated channels have high availability, and reliability, and don't provide any data switching/forwarding. These channels support data transport only and fully utilize communication all resources for a single data connection. While reliable, and available, this channel type clearly does not utilize communication resources efficiently.

Multiplexing principle is depicted on Figure 4. Multiplexed channel is essentially a set of dedicated channels, with resources dedicated to each individual channel. Multiplexing principles vary, these include

- Time Division Multiplexing (TDM), where time slot is assigned for a given channel, as for example in Synchronous Optical Network (SONET),
- Frequency Division Multiplexing (FDM), where frequency is assigned for a given channel, as in traditional Telegraph and Wi-Fi technologies,
- Wavelength Division Multiplexing (WDM), where wavelength is assigned for a given channel.

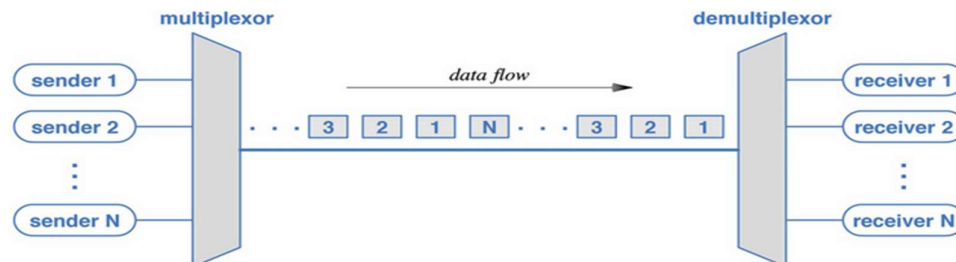


Figure 4 Multiplexing principle

More details on some of these technologies could be found in [6]. Multiplexed channel, being essentially a set of dedicated channels, inherits characteristics of dedicated channels such as high availability and reliability. It also provides a more efficient use of communication resources, as a single cable/media supports multiple channels separated by dedicated time slots, frequencies or wavelengths.

The third channel type called switched channel is fundamentally different from the first two, as its operation and performance does depend on availability of resources. Arriving data needs to be stored first (for store-and-forward type switches), a decision on where to forward the data to needs to be made, and outgoing channel(s) need to be available for communication to occur. These require sufficient and

well-organized internal data buffering, well-designed Address Resolution Tables for data forwarding decisions, and availability of incoming and outgoing channels (also called ingress and egress). Examples of switched channels are many and more and more communication technologies utilize this method, as it provides arguably better use of communication resources. These include old traditional Public Telephone Network (Called Public Branch eXchange, PBX) equipment stations, where channel availability was calculated using Markov chains (generally speaking only 80% of the connected numbers can in fact make connections in a given time), Asynchronous Transfer Mode (ATM) switches, IP routers, and of course Ethernet switches or bridges (per the proper term defined by IEEE). Term packet-switched networks² has been generally used for digital technologies with switched channels. Both IP routing and Layer 2 Ethernet switching belong to this category.

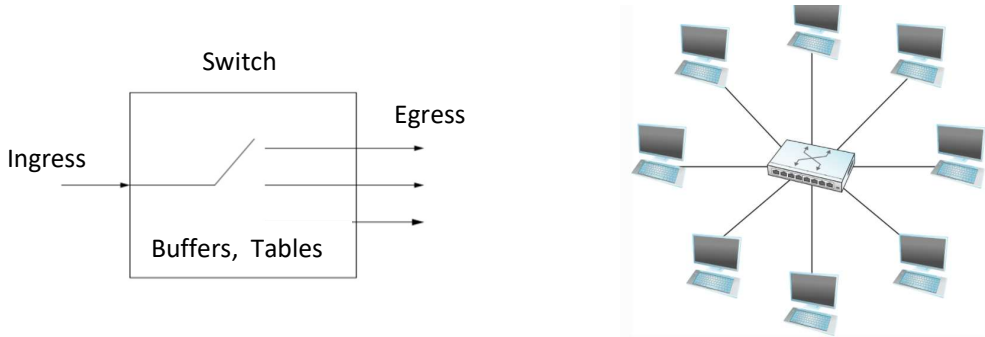


Figure 5 Principle of the switched communication channel

The next subsection specifically focuses on Layer 2 Ethernet functionality, and explains how it has evolved to the levels of reliability required for digital substation application use.

2.2 Layer 2 Ethernet

Ethernet communication provides switched communication channels, so its reliability depends on the availability of resources, such as internal buffers, incoming and outgoing channels, etc.

Ethernet is commonly used for short range Local Area Networks (LANs). It can also be mapped into Wide Area Network (WAN) communication technologies. An Ethernet variant specifically designed for WAN by Metro Ethernet Forum (MEF) is called Carrier Ethernet. While it uses the same principles, it is not covered in detail in this review. One can refer to [6] and [8] for more details on this technology.

Ethernet is a communication language (i.e., protocol) that operates on Data Link Layer 2 and is specified by IEEE 802 group of standards [9]. It is interesting to note that the number 802 is composed of a year (80) and a month (2) of when the standard was created: February 1980. There are small differences between Ethernet and IEEE 802 specification, that are not critical for our discussion.

Ethernet evolution

Ethernet communication evolved significantly from the time of its creation. It started as a half-duplex data exchange on a shared bus over a coaxial cable! One can imagine a single cable that every connected device can use to send and receive data. Data rates started from 5Mbits/s over thick 50Ohm coaxial cable³ for 10Base-5 and 2 Mbits/s over thin coaxial cable for 10Base-2 and finally raised to 10Mbits/s over twisted pair cable for 10Base-T.

² Per IEEE and IETF terminology, Ethernet data is uses Ethernet frames, while IP data is transmitted in IP packets. Despite of term difference, packet-switched networks can refer to network that use both IP-routed packets and Ethernet-forwarded frames.

³ It is interesting to note that while the use of coaxial cable for Ethernet has been deprecated by 2011, research in Ethernet transmission over coaxial cable continued, as both consumers and telecommunications operators strive to use existing 75 Ohm coaxial cable installations (from cable television or CATV), to carry broadband data into and through the home, and into multiple dwelling unit (MDU) installations. Most EoC technologies are being developed for in home or on premises networking and are expected to be operated within the domain of a single operator.

Modern Ethernet communication media include all: copper, fiber and air. This review is focused on Ethernet over fiber optic cables, as this media is standardized for the use in digital substations due to its electromagnetic compatibility (EMC) characteristics. For copper media, if used, most common interface today is RJ45, and most common cable types are TP CAT-6 or CAT-6e. Straight cables are mostly used, as cross over function of connecting transmit circuit to receive circuit is automatically performed by Ethernet switches and end devices, so the need in cross over cables has disabled.

For fiber communications, common cables are colored in orange (for multi-mode fibers used for short-range communication), and in yellow (for single mode fibers for medium and long-range communication). As data in fiber optic cable is transmitted using light, generally speaking, it is very sensitive to bending. Commonly an acceptable bend radius is specified by a manufacturer. A bend-resistant blue colored fiber cable was developed to address this challenge. Such cable is known to provide reliable data transmissions after being wrapped around a pencil about 10 times.

Connectors/terminals wise (properly referred to as communication Interfaces), for Ethernet communication ST fiber connectors are still in common use, and LC connectors are expected to be more common going forward. There is also the most flexible method called Small Form Factor Pluggable (SFP). It includes installation of an SFP cage for insertion of an SFP transceiver, with any connector type. In practice, however, mainly SFP transceivers with LC for fiber and RJ45 for copper Ethernet connections are used.

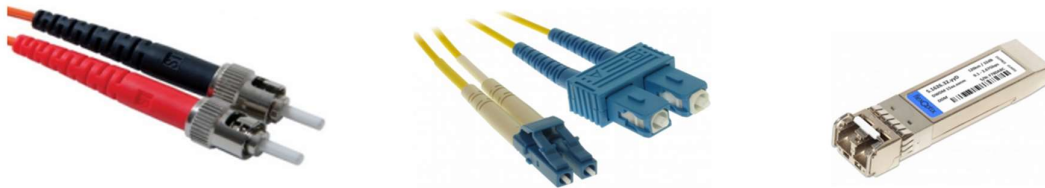


Figure 6 Common cables and connectors used for Ethernet

Initially, Ethernet networks were architecture as a single (communication) bus. Later star, ring and other more complex hieratical network architectures became possible.

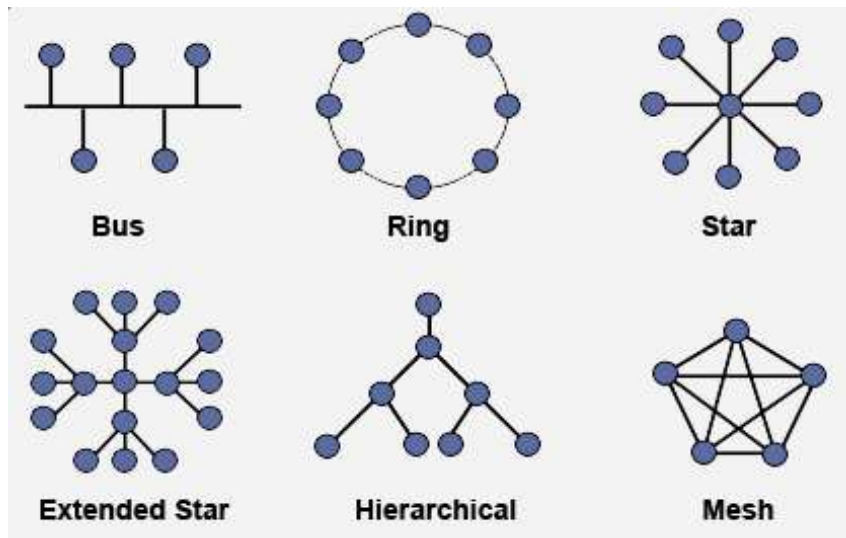


Figure 7 Ethernet network architectures

First Ethernet devices could not handle data transmission and reception at the same time. They operated in half-duplex mode. As there were no time slots assigned for data transmission and reception, data collisions occurred when more than one device were transmitting data at a time. The concept of data collisions handling, and their resolutions (by re-transmissions) are specified by the IEEE 803.2 standard as the Carrier Sense/Collisions Detection Multiple Access (CS/CDMA) mechanism [9]. In

essence, this mechanism required each transmitter, while sending its data to listen to the media for Carrier Sense (CS) signal, to determine if someone else was sending data at the same time. If CS signal was lost during transmission of the first 64 bytes of the data (i.e., some other device started data transmission during that time), the transmitter stops transmission, and waits for a random time interval to try to re-transmit the same data. Such event would be registered in data collisions counter. If CS signal was lost after transmitting the first 64 bytes, data transmission continues (with an expectation is that another transmitter that started transmission later will stop transmitting and re-send its data at another time). Such event is called late collision. Late and continuous collisions could lead to data losses so reduce reliability. They also obviously affect data delivery time. CSMA/CD mechanism is illustrated on Figure 8.

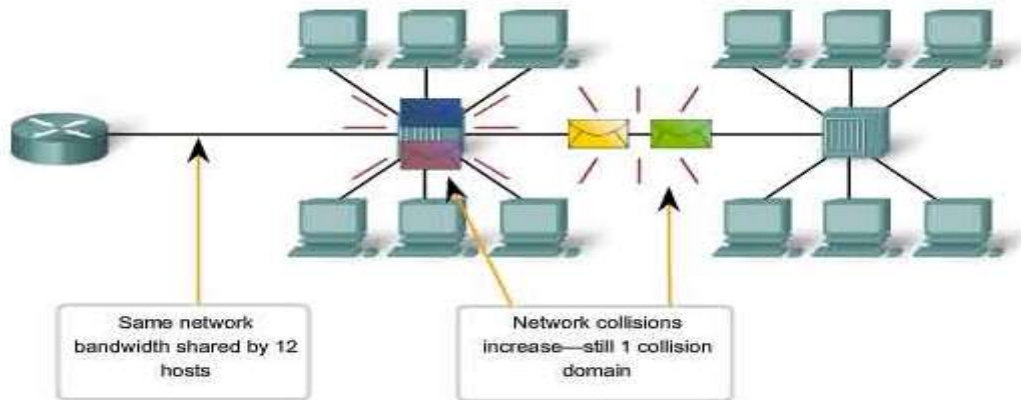


Figure 8 Collisions and Late Collisions in the original Ethernet

As data collisions and especially late collisions can result in data losses, the original Ethernet technology has been referred to as “best effort”, i.e., best efforts are made to deliver the data, yet data delivery could not be guaranteed⁴. Network devices used by the original Ethernet were called Repeaters, per IEEE term or Hubs, colloquially. Hubs essentially act as “wires” providing all-to-all connectivity with no switching capabilities, so are basically, communication links, not commutators.



Figure 9 Ethernet network architecture examples

Ethernet evolved with addition of full-duplex mode capability, i.e., the ability to transmit and receive data at the same time, resulting in no data collision possibilities. This certainly increased reliability of Ethernet communications. New device types called Ethernet Bridges (per IEEE term) or Ethernet switches (colloquially) were created. These devices operate in full-duplex mode and have data forwarding/bridging capabilities. Operation of Ethernet bridges is specified by IEEE 802.1 group of standards [10], [11].

The most common network architecture with Ethernet switches is a star, as shown on Figure 9. It should be noted that some newer repeaters (also known as “hubs”) also support full-duplex mode and are

⁴ Layer 3 Internet Protocol (IP) does not guarantee data delivery either. Higher layer protocols such as TCP do. Per RFC 793 [13], TCP establishes a connection between transmitter and receiver, acknowledges data receipt, and re-transmits the data, if it was not received. TCP communications uses more bandwidth than the connectionless UDP protocol, refer to RFC 768 [14].

sometimes called “unmanaged” or “dumb” switches. These are often quite helpful as growing complexity of managed Ethernet switches makes it difficult to use them for simple traffic monitoring, for example.

Ethernet Data format and Addressing Scheme

Data is packed into Ethernet frames. Basic Ethernet frame structure is shown on Figure 10. It includes Preamble (a set bit pattern), Destination and Source Addresses, Type (usually EtherType resides there), Data and Frame Check (CRC-32) fields.

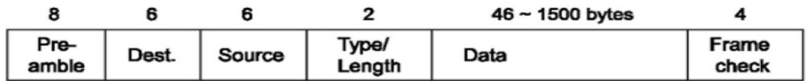


Figure 10 Basic Ethernet Frame structure

Unique Media Access Control Addresses (MAC) are used for identifying the devices and making forwarding decisions. The structure of MAC address includes identification of the 3-bytes manufacturing company called Organizationally Unique Identifier (OUI) assigned by IEEE Registration Authority and a unique number assigned by an Ethernet card manufacturer. This is shown on Figure 11.

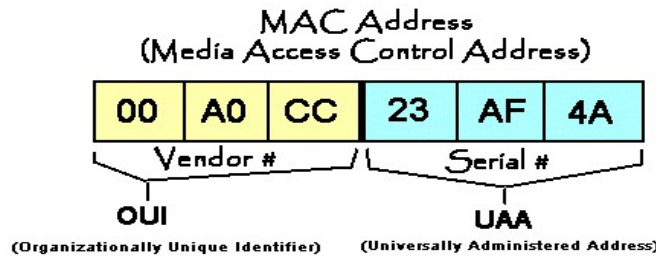


Figure 11 MAC Address structure

Specifically, designated bits as well identify communication type: broadcast and multicast. The least significant bit (b1) of the most significant byte (1st octet), as shown on Figure 12, is set to 1 for multicast communication.

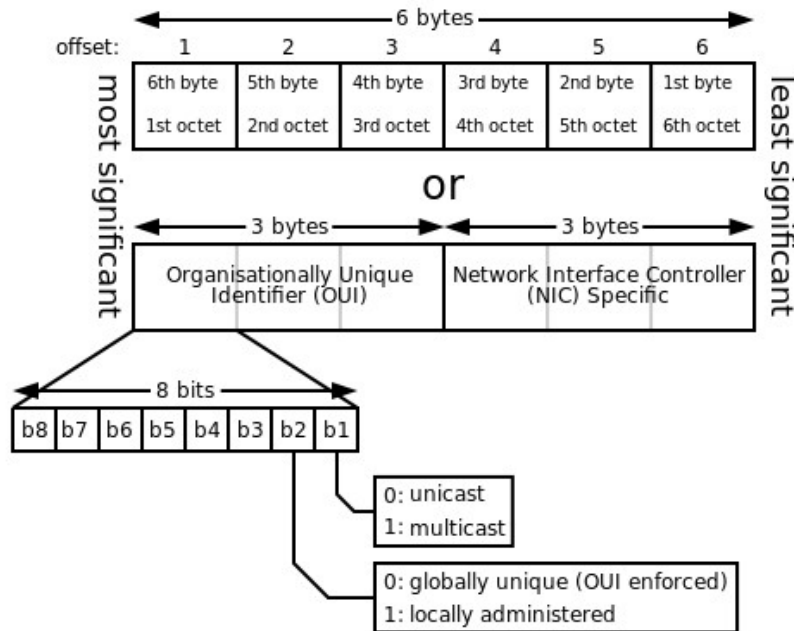


Figure 12 MAC address bit assignments for different communication types

Ethernet switch design considerations

To forward data, Ethernet switches need to

1. have enough internal memory to store the data before a forwarding decision is made (for store-and-forward switch architecture), and
2. maintain a correspondence of addresses (Media Access Addresses, MAC) and switch port numbers to make a data forwarding decision.

The first uses internal memory for frame buffering, the second is typically implemented in an internal MAC Address Table⁵.

Internal memory size and organization, and MAC Address Table implementation play critical role in achieving the most reliable data delivery. Well-designed Ethernet switches are very capable of delivering data reliably.

Ethernet switches can be designed for cut-through or store-and-forward data processing. The first, starts processing the frame to make a forwarding decision before receiving a complete frame, the second requires reception of the whole frame to start its processing. The second architecture is more commonly implemented. In this case data processing time is directly proportional to the size/length of the data frame. The type of data processing implemented affects data processing latency and is related to internal buffering capacity needs. Thus, internal switch architecture affects greatly reliability and data processing delay. For details on possible internal buffers organization interested readers can refer to H32 [15].

MAC Address Table

MAC Address Table is at the heart of Ethernet switch operation. In its simplest form it consists of 2 columns with (1) 6-byte MAC Address and (2) switch port to which a device with this MAC Address is connected to. The size of MAC Address Table basically defines maximum network size supported by a device, i.e., the maximum number of devices the switch can forward data to, without broadcasting it.

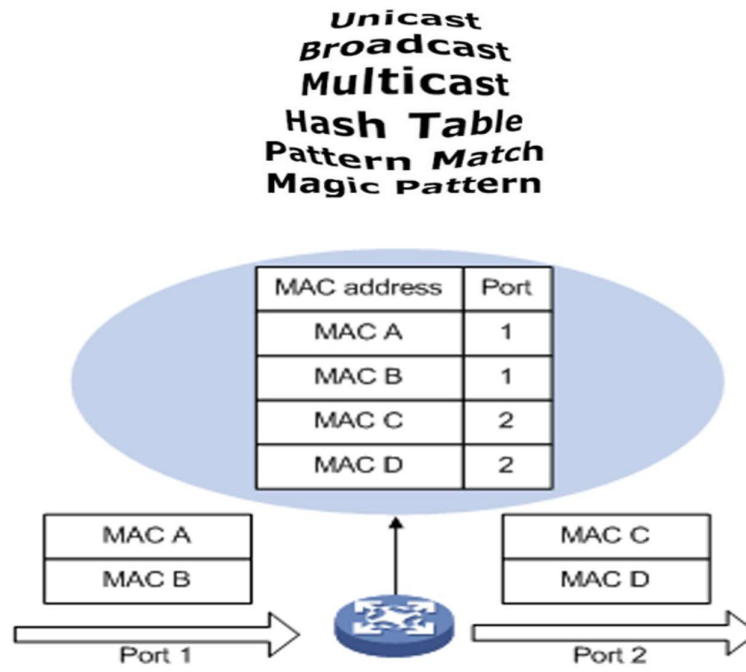


Figure 13 Simplified MAC Address Table organization

⁵ Data forwarding (a proper IEEE term) or switching (colloquially) is performed at Layer 2 for Ethernet communication. At Layer 3 data is typically routed using IP routing protocols, so IP routing is performed at Layer 3. Some devices refer to Layer 3 switching as a mechanism to switch using IP addresses only (without running classical IP routing protocols).

A MAC Address look up mechanism implemented (as switch needs to find out quickly, to which port a device with a particular MAC Address is connected to) defines efficiency and quality of data forwarding. A good look up mechanism as well provides protection from Denial of Service (DoS) attacks. Hashing using polynomial calculations, similar to CRC calculations, is often used by common off-the-shelf Ethernet switches. While it is cost effective, hashing introduces hash collisions, resulting in multiple MAC Addresses being placed into the same Table's row, sometimes referred to as "bin". This leads to continuous learning, and unnecessary data broadcasting that could create a DOS condition⁶. Switches with hashing used for MAC Address Tables are generally not acceptable for critical applications with high reliability requirements.

Other better look up methods exist that do not introduce collisions, such as binary search and Content Addressable Memory (CAM). Use of Ethernet switches with CAM chips is recommended for critical applications to achieve reliable data delivery. Interested reader can find more fascinating details about MAC Address Table designs, and their effect on reliability of data delivery in [16]. That paper explains that even performance tests specify unrealistic conditions (the use of sequential MAC Addresses in a network), that lead to misleading switch performance test results and levels claimed by in devices' documentation. Figure 13 illustrates MAC Address Table organizations and forwarding decisions.

IEEE 802.1Q Tags

Additional mechanisms were added to Ethernet technology to increase its reliability. Two concepts below in particular have been widely used:

1. Virtual Local Area Networks (VLANs)
2. Priorities

Both mechanisms use IEEE 802.1Q tag, comprising of 4 bytes: 2-byte Ether type and 4-bytes encoded information. This tag is added in the beginning of Ethernet frame, right after MAC Destination and MAC Source Addresses, as shown on Figure 14 below, refer to [12].

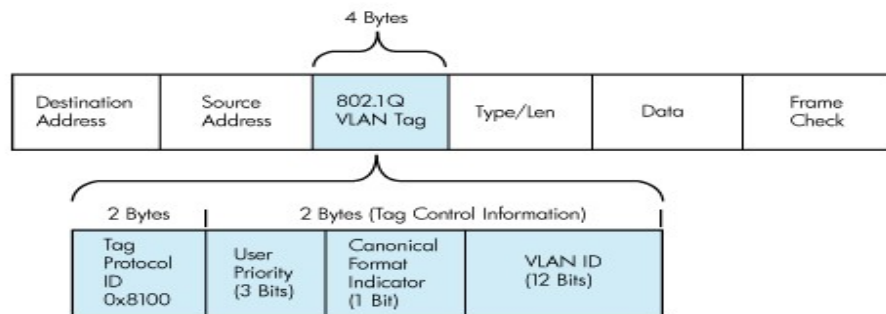


Figure 14 IEEE 802.1Q tag added to an Ethernet frame to support VLAN and Priority features

VLANs

VLANs are essentially a method to virtually isolate the traffic in the same physical network. The obvious benefit of the VLAN concept is isolation of data used for different applications, so that operational data and non-operational data can use the same physical network, while still being isolated. VLAN concept is shown on Figure 15.

Differentiate port-based VLANs, tag-based VLANs, MAC-Address based VLANs (rarely used). Most commonly, IEEE 802.1Q tag-based VLANs are used. VLAN Membership can also be established using Multiple VLAN Registration Protocol (MVRP) created specifically for this purpose.

VLAN Membership information is added to MAC Address Table for particular MAC Addresses or ports and is used for forwarding decisions. Data is only forwarded to/from Members of the same VLAN. To forward traffic between VLANs, a port defined as VLAN Trunk is used. This port carries traffic for multiple VLANs to connect remote locations, for example.

⁶ Note that if a switch does not know where to forward data, it generally forwards it to all its ports except the data source port, i.e., broadcasts it.

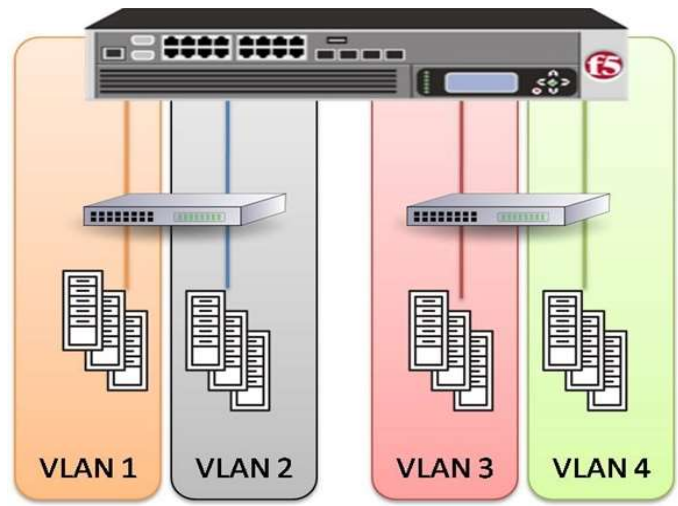


Figure 15 VLANs concept

VLAN identifier (ID) has 12 bits. 0 identifies that no VLAN is assigned (Priority only frames). VLAN ID = 1 is commonly used for Management VLAN, with all ports being its Members, by default. The rest of VLAN IDs up to 4095 are user configurable. Some switches may have a limitation for the number of VLANs supported (likely dictated by limited size of their MAC Address Tables, internal buffering, and processing power).

Priorities

Priorities, as the name imply, define criticality level for servicing the traffic. Priority concept is shown on Figure 16. 8 priority levels exist (a 3-bit field). Ethernet frames with the highest priority are serviced first, while Ethernet frames with the lowest priorities are serviced last. As a result, high priority frames will continue to be forwarded, while low priority frames can be dropped in high network traffic condition.

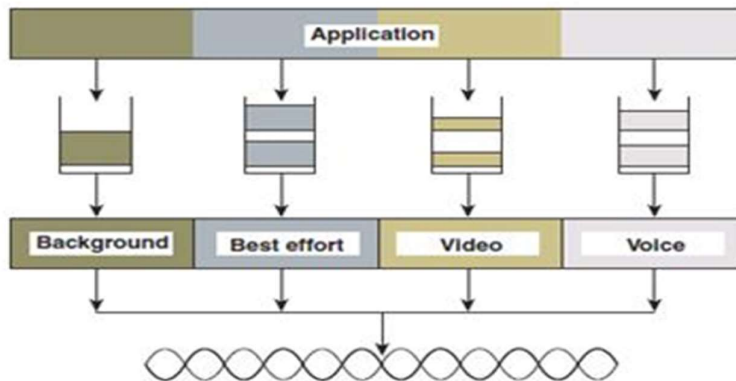


Figure 16 Priority concept

Other examples use of Pri = 7 for critical data, Pri = 6 for time synchronization, etc. It should be noted that some switches supporting Layer 2 and Layer 3 (IP) switching (or routing), can translate Layer 2 Pri field into a corresponding Layer 3 Quality of Service (QoS) value in the Layer 2 Differentiated Services Code Point (DSCP) field to provide the same prioritized processing at Layer 2 and Layer 3.

Ethernet technology application to Digital Substations

Communication data streams are used in digital substations to exchange binary signals (commands and status) and receive analog data (digital samples of voltages and currents). The first use Generic Object-Oriented Substation Event (GOOSE) messages, and the second - Sampled Values (SVs) data.

Fiber optic communication media at 100Mbps/s (or higher) rate is specified and used, due to fiber's EMC characteristics.

Both GOOSE and SV messages are defined by the IEC 61850-9-2 standard [17] to use Layer 2 Ethernet communication with a dedicated Ether Types, and multicast destination MAC addresses.

Multicasting is selected to increase the reliability of data delivery. IEC 61850 GOOSE messages in peer-to-peer communications are sent continuously at a configurable rate as a heartbeat by all devices publishing them. Upon a status change, new binary data is also multicasted in randomizes bursts (with various time randomization methods) to increase the probability of receiving it by the destinations reliably. IEC 61850 SV messages with analog data samples are sent continuously, most commonly at 80 or 256 samples per power cycle (16.66 ms for 60 Hz system) rate. Multiple recipients can subscribe to receive these multicasted data at the same time.

Table 8 in the IEC 61850-9-2 standard [17] specifies the following Ether Type values 88-B8 and 88-B9 for GOOSE messages and 88-BA for SV messages.

Table B.1 in the IEC 61850-9-2 standard [17] contains the recommended (multicast) address range assignments: 01-0C-CD-01-00-00 to 01-0C-CD-01-01-FF for GOOSE and 01-0C-CD-04-00-00 to 01-0C-CD-04-01-FF for multicast sampled values.

Both GOOSE and SV messages as well use IEEE 802.1Q tags. By default, Priority value of 4 is set to prioritize processing these data. (The value of 4 could have been selected because older Ethernet switches only had 2 or 4 priority queues). VLAIN ID value in the tag is set to 0 by default, identifying that no VLANs are configured, i.e., GOOSE and SV by default are priority only frames.

Complete frame structure for both messages is specified in Annex A [17]. Redundancy fields are also optionally included.

UCA IEC 61850-9-2LE implementation agreement as well uses the same frame structure and depicts it in Annex A [18].

IEC 61869 standard (for function -9 part and standalone merging units -13 part) specify dynamic merging unit behavior and other operation and communication profiles, including data filtering before samples transmission, that is a major new feature, refer to [41].

It is interesting to note that sometimes APPID field is set to the value of the last (unique) bytes of the multicast destination MAC address.

Per Ethernet fundamentals and specific features specified for digital substations communications, it is important for Ethernet switches used in digital substations to have:

1. A well-structured and sufficient internal data buffering
2. Large and well-designed MAC Address Table, preferably using a CAM chip
3. Robust queue management support with at least 4, preferably 8 IEEE 802.1Q priority levels
4. Support for proper forwarding of Priority only frames with IEEE 802.1Q tags' VLAN ID = 0.

The last bullet is critical and has commonly been a stumbling point. Most switches use VLAN ID = 1 as a Management VLAN, with all ports being its Members. Yet, IEEE 802.1Q tagged frames with VLAN ID = 0, can simply be discarded by default. An Ethernet switch settings change to enable forwarding of frames with VLAN ID = 0 can be required. This setting can be called VLAN ID = 0 Transparent Mode, or VLAN ID = 0 Promiscuous Mode. Stripping IEEE 802.1Q tags can also be enabled by default. If preserving the tags is necessary, the Ethernet switch needs to be set for required tags behavior.

As both IEC 61850-9-2 GOOSE messages for binary signal exchange and Sampled Values (SV) for sending analog data use IEEE 802.1Q tagged frames with VLAN ID = 0, and PRI = 4. So, proper switch configuration is required.

All other switch features need to be properly configured as well. And with these simple switch configuration steps, determined based on numerous field experiences and testing, networks with standard Ethernet switches fulling the above requirements are fully capable of meeting reliability and availability and redundancy requirements for critical digital substation applications.

While testing and debugging is not a subject of this paper, but the below notes are relevant to our discussion:

1. Wireshark tool, commonly used for network data sniffing and analysis, by default strip IEEE 802.1Q tags. To enable keeping these tags intact one needs to modify Windows registry. Specific depends on particular Network Interface Card (NIC) used, refer to [19].

2. With growing complexity of Ethernet switches, it is often simpler to use an unmanaged or “dumb” Ethernet switch that essentially acts as a full-duplex repeater just to sniff network data for testing⁷. (Note that ports mirroring feature designed for testing usually drops errored and other frames, and even if it is configured correctly is not very useful in practice).

Modern Ethernet switches use many more features, including time synchronization (not a subject of this paper), rate limiting (ingress and egress), multicast filtering (variously configured), redundancy features (discussed in Section 3).

All these standard Ethernet features, supported by the standard well designed Ethernet switches, wisely selected and properly configured, support Ethernet communication with data delivery reliability sufficient for digital substation applications. All the efforts have been made by standards developers and device manufactures to achieve these reliability levels and provide customers with inter-vendor interoperability.

For guidance on using Ethernet devices for protection and control applications, interested readers can refer to IEEE PSCCC P6/ PSRC H12 Report [20]. For guidance on how to test protection and control applications using IEC 61850 technology refer to IEEE PSRC H6 Report [21].

Technology discussed next essentially uses the same Ethernet features, yet adds an extra software control plane with complex per data flow settings, to reach performance already achievable by networks with standard well designed and simply set Ethernet switches. This extra complexity is not necessary and present more opportunities for human errors. Such solution is also not defined by any digital substation standards; thus, it prevents multi-vendor interoperability.

2.3 Software Defined Networking

Traditional communication networks consist of network devices, such as switches and routers, that are manually configured by administrators. The implementation of network and security policies is a manual process which makes traditional networking not flexible enough to interact with the dynamic environment of the Internet and new emerging applications. In the Software Defined Networking (SDN) paradigm, the network is divided into two distinct parts – the control plane and the data plane, as shown on Figure 17. SDN Layers, Architectures and Terminology are defined in [22]. For on-going SDN standardization work, the readers can refer to [23].

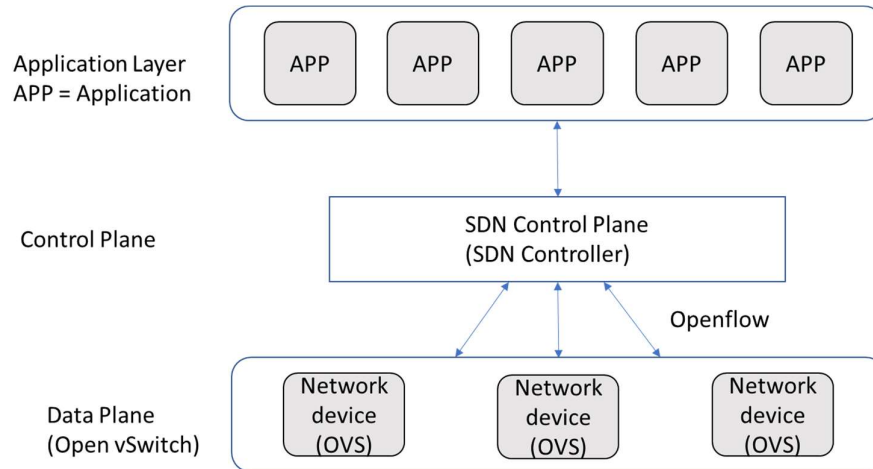


Figure 17 Software Defined Networking High Level Architecture with Open Virtual Switches (OVSs)

The main idea behind SDN is to create networks that are programmable such that network devices are able to respond faster in a more dynamic environment.

SDN’s central controller is an intelligence center of the network. Network policies and decisions are made from the central controller and distributed to the data plane which consists of the network devices, also known as the forwarding devices. Since the controller manages and monitors the network, it has the ability to maintain a global view of the state of the network and information regarding the network. As a result of the global view, for example for Data Center applications, Software Defined Networking

⁷ Note that port mirroring feature does not forward the errored frames to the mirror port, is not very useful for testing and traffic sniffing purposes.

could make forwarding and routing decisions at a faster rate and with more accuracy than a traditional network, however with a lot more complexity to setup, manage, and troubleshoot.

Just as in traditional networks, the data plane is responsible for applying the network policies and for making forwarding decisions on the data packets flowing through the network devices. The control plane manages the routing table (Routing Information Base or RIB) and any additional information that is required in the selection of the most optimal path for data packets flowing through the network. The data plane manages a forwarding table used for fast packet processing (Forwarding Information Base or FIB).

The control plane rules are applied to the data plane to form pathways or flows that carry data from source to destination. The interconnected network devices with the programmed flows forms the SDN fabric.

The separation of the control and data plane along with the distributed architecture provides for flexibility and agility in managing and operating networks. However, the SDN approach adds a whole lot of complexity and requires additional training and/or hiring of personnel with the expertise to deploy, configure, troubleshoot, and manage these networks.

Complexity of Managing Security Policies

With SDN, firewall functionality is provided by the SDN fabric. The firewall rules are defined and applied by using additional software inside the SDN fabric (examples include Cisco Application Centric Infrastructure (ACI) or VMware Network Virtualization and Security Platform (productized as NSX). Security policies in an SDN environment require a more granular approach as compared to monolithic security policies that are usually associated with traditional networking. The granularity allows for diverse security controls for traffic that flows both north-south and east-west. While the ability to add granular policies can seem attractive at first, there is a lot of complexity to monitor and manage. Identifying which assets are connected and identifying data flows is a pre-requisite. The next steps include planning and designing the granular security policies which can take a substantial amount of time and demands rigor. The final steps of deploying and managing the additional firewall software applications requires training and close supervision of the network to ensure that the correct policies have been applied in the SDN fabric. This leads into the topic of security policy management which comprises of enforcement and maintenance of these rules on an ongoing basis. Each time a new asset, application, or network device is introduced, or an existing one changed or removed, the security policies also need to change and have to be approved.

Segregation of the assets within the network requires identifying critical assets with the most sensitive data and separating these from others to control access and limit the exchange of information. Visibility into the flows is crucial here to identify which assets are talking to each other and how traffic is flowing throughout the network. This too requires constant monitoring and mapping all of the traffic flows within and through a SDN network. The ability to understand and work with the different tools in a complex networking environment is a requirement.

3. Communication Redundancy Technologies

Redundancy is a very familiar concept to protection engineers, commonly dealing with multiple sets of protective relay systems that provide multiple redundancy levels (Sets A and B, and Sets C and D), as documented for instance in [24]. The main goal of redundancy is well understood too: to eliminate single points of failures.

Communication redundancy serves the same purpose. Communication channel is a part of overall composite protection system for communication-assisted protection schemes, so redundancy requirements placed on the overall system apply to communication channels as well. Some most critical protection applications in addition to communication redundancy require redundant communication paths to be geographically diverse, per [8].

Figure 18 below shows the main communication redundancy concept that is no different from protection system redundancy concept.

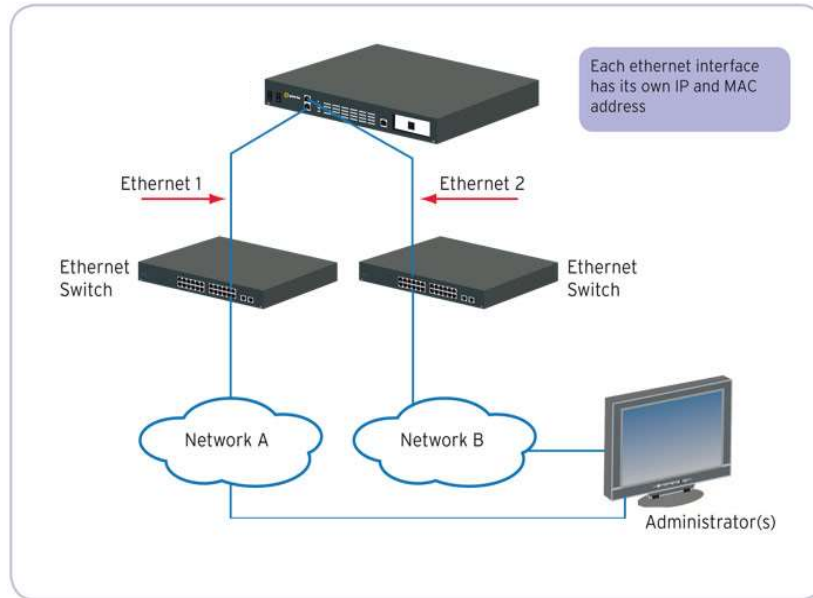


Figure 18 Communication redundancy concept

Various means of achieving different levels of communication redundancy exist. For the purpose of this review, methods and protocols used for digital substation communications are discussed in this section. As the number of deployed digital substations and on-going projects grows, more awareness and education in the area of communication redundancy is desired. Recent conference paper presentations revealed numerous confusions, so a review of communication redundancy concepts is timely.

First, let us note that some vendors choose to support a communication redundancy only for a link between relays and Ethernet switches, in a non-standard proprietary way. Such mechanisms commonly use Link Pulses that are always present in a healthy Ethernet communication to detect link failure and initiate switching. Communication link switching is not immediate and depends on implementation. These non-standard mechanisms are sometimes referred to as communication link failover.

Second, let's establish a common understanding that for the overall communication system redundancy, system-wide redundancy protocols and mechanisms are required. These are summarized in this section, starting from Ethernet Layer 2 concepts (in the order of their evolution), and continuing with concepts used by TDM-based communication such as Synchronous Optical Network (SONET), defined by [25], as these are still commonly used for data exchange between digital substations.

It should be noted that discussions below reference a summary paper on communications redundancy published at PEAC conference in 2010 [26]. That paper provides complete details on the operation of the main redundancy protocols, while discussions below broaden it per recent updates and field experiences.

3.1 Layer 2 Ethernet redundancy protocols with data losses during switching

Ethernet network architectures, shown on Figure 7, initially assumed that a single copy of data will reach a destination. With introduction of switched Ethernet, and fiber interfaces that allowed to expand Ethernet network size and distances, possibilities of connecting multiple switches, and looping data back occurred. To prevent multiple data copies and indefinite data loops, the original Ethernet was enhanced by a protocol called Spanning Tree. Spanning Tree is defined as a loop prevention protocol and was originally specified by IEEE 802.1D standard in 1998. A brief description of this protocol and its evolution is presented below. It should be emphasized that all various spanning tree protocols introduce data loss during switching, thus, are not suitable for critical protection and control applications. For more details on these protocols interested reader can refer to [26], the latest IEEE specification [12] or vendor specific product manuals.

3.1.1 Spanning Tree Protocol (STP)

As the name implies, to prevent data loops formation Spanning Tree Protocol (STP) establishes a hierarchical structure in an Ethernet network with multiple switches, refer to Figure 19. One switch is selected to be a Root Bridge, using an exchange of protocol-specific multicast messages, called Bridge

Protocol Data Units (BPDUs). The same messages are used to determine which ports on each switch shall be active (i.e., placed into Forwarding state to forward data) and which shall be disabled (i.e., placed into Blocked state and not forward any data). BPDUs are sent periodically (once a second per default) to keep active network configuration current, and support prompt (in the 1999 Ethernet world terms) network reconfigurations.

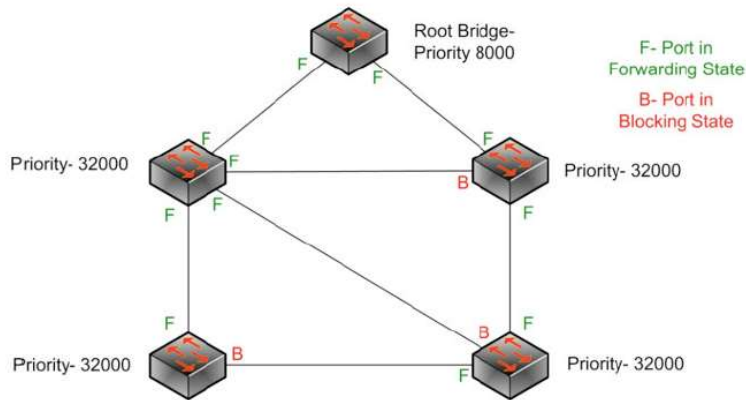


Figure 19 Active network architecture per Spanning Tree Protocol

If a single (bi-directional) Ethernet communication link fails and another path exists, after network switching time, a new data communication path will be used. This original Spanning Tree Protocol specifies 30 seconds (an eternity in protection world) to switch from one communication path to another or reconfigure network architecture. During this long switching time all data in the whole network will be lost.

3.1.2 Rapid Spanning Tree (RSTP)

As switching time of 30 seconds (during which data losses occur) was not acceptable, a faster version of Spanning Tree Protocol, called Rapid Spanning Tree Protocol (RSTP) was developed, as specified in [11] RSTP is essentially the same as STP, with faster BPDU transmission rate and faster reconfiguration time. Still, it reconfigures in 5 seconds per network hop. Thus, with 6 network hops (a network with 5 Ethernet switches) it again reaches 30 seconds network reconfiguration time, during which data loss occurs. This again is not acceptable for critical applications.

3.1.3 Multiple Spanning Trees (MSTP), Per VLAN Spanning Trees

With introduction of Ethernet network segmentation, e.g., using VLANs, Multiple Spanning Trees and per VLAN Spanning Tree protocol versions appeared. Some use non-standard proprietary vendor specific implementations so are not interoperable with devices from other vendors. The same general Spanning Tree concept is used for these protocols, except that each network segment has its own Spanning Tree established.

3.1.4 Proprietary enhanced Spanning Tree Protocol (eRSTP)

The fastest Spanning Tree Protocol version was developed by some switch manufactures, in a proprietary non-interoperable way only. While using the same standard mechanisms, it increased BPDU transmission rate 1000 times (thus, significantly increased network traffic), and specifies network reconfiguration in 5ms per network hop. While these times are getting closer to those required in protection and control world, there are still data losses, for example for 30ms in a network of 5 Ethernet switches.

For more information on Spanning Tree functionalities and interoperation of various Spanning Tree Protocols, one can refer to [27].

3.2 SONET channel redundancy

As the TDM-based SONET technology is still in common use for communication between digital substations, a discussion on SONET redundancy is included into this review.

SONET technology has an embedded redundancy feature, as it is commonly deployed as redundant rings, referred to for example East and West, Primary and Secondary or Working (active) and Protection

(redundant) rings. Even linear SONET configurations are commonly deployed as flat rings, because of the nature of this technology itself.

Data between data sources and destinations can travel in East to West or West to East directions.

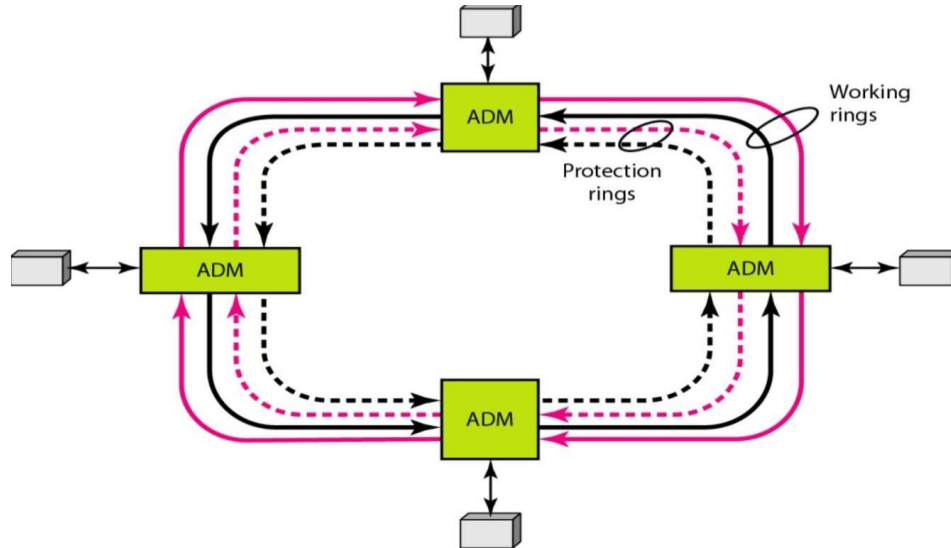


Figure 20 SONET and its embedded redundancy concept

One data direction is used at a time. If a single fiber failure occurs, another data direction gets activated. Commonly reported SONET switching/network reconfiguration times are in order of 50ms for the whole system, during which data loss occurs.

Both Ethernet and SONET use dedicated fiber strands for transmit and receive directions (unless different wavelengths in the same fiber are used). Transmit and receive fibers can be bundled together (making it difficult to cut one fiber without cutting another one) or be completely separated.

While single fiber cut really only affects data in one direction only, well-designed SONET systems actually switch both data direction to a new communication path at the same time. Realistically, it is probably more likely for both fibers to fail in the same cable, while single fiber cuts are still possible.

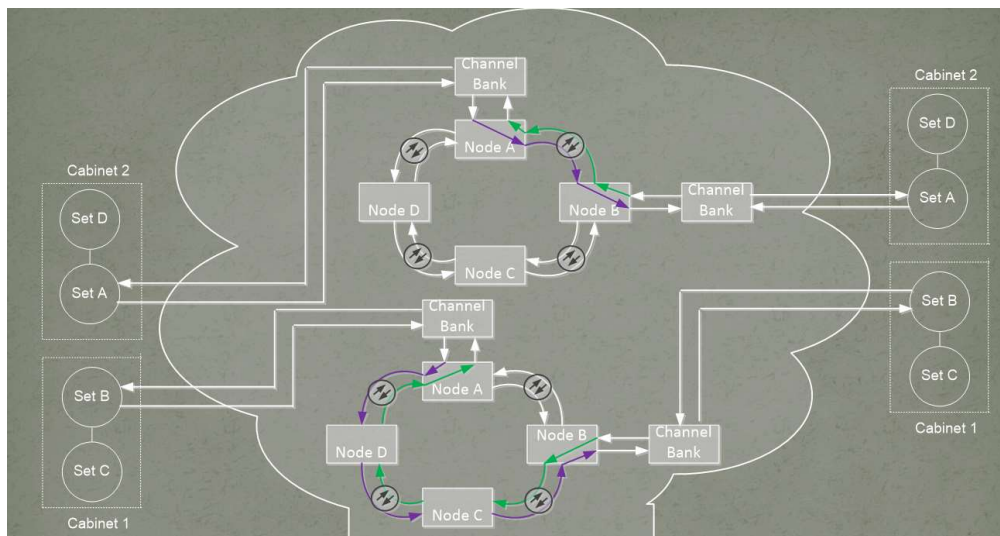


Figure 21 SONET Network Diagram example from [24]

Switching data path for both directions even if fiber failed only for one direction is a very important. If it is not implemented, transmit and receive communication paths will have different latency. As delay symmetry (in transmit and receive directions) is commonly assumed and required by line protection applications, this could and have led to serious consequences, such as 500kV line protection mis

operations. Delay symmetry is also required if communication channel is used for distributing time between line terminals.

Some utilities recognized SONET redundancy with predictable and reliable switching of both communication paths as a very useful feature and have been successfully using it in their power systems.

As some SONET equipment vendors do not support switching both data directions on a failure of a single fiber, other utilities (based on their hard way learnings), decided not to use the SONET redundancy feature. Disabling SONET redundant switching is referred to by some vendors as Locked Bandwidth. Interested readers can find more details in [24]. Network diagram discussed in that paper is shown on Figure 21.

3.3 Layer 2 Ethernet protocols without data losses during switching

All communication redundancy methods discussed so far support single or double (one bi-directional) communication link failures, but loose data during switching/reconfiguration time. The fastest recovery times discussed are 5ms per network hop (for a proprietary method, capable of switching a network of 5 Ethernet switches in 30ms), and typical SONET system switching in 50ms.

Protocols described in the next section support the same network failures with zero switching time and no data losses. These are standard non-proprietary protocols defined by [28]. These protocols are specified for digital substation applications.

3.3.1 Parallel Redundancy Protocol (PRP)

Parallel Redundancy Protocol (PRP) is specified by [28]. Its concept is straight forward: two separate networks are used to transmit same data all the time. It doubles network resources yet is well positioned to meeting the main requirement for critical high voltage applications – redundant communication channels shall use geographically diverse paths.

Conceptual diagram of a PRP network is depicted on Figure 22. As illustrated, the same data is sent over both Network A and Network B. The destination receives data twice. It keeps the data that arrives first and discards its duplicate.

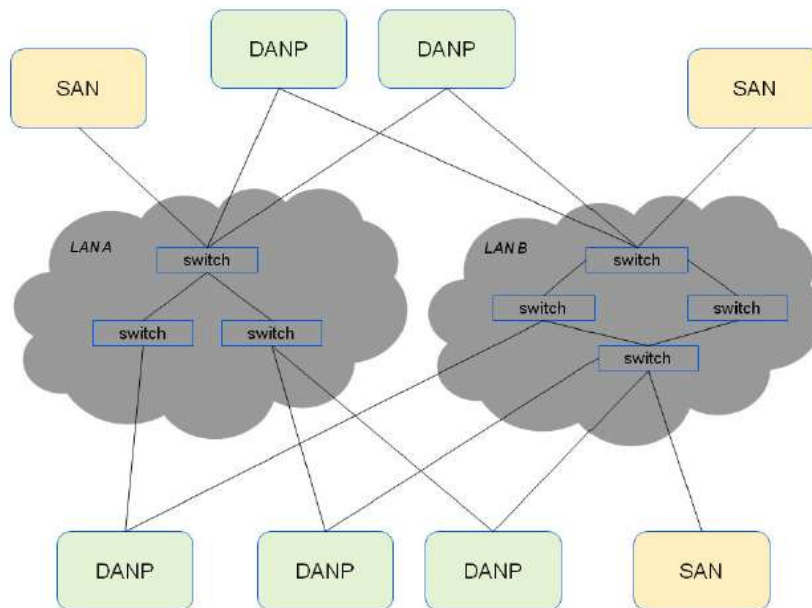


Figure 22 Conceptual diagram of a PRP network from [26]

The association between data with its duplicate is done via information stored in PRP Trailers bytes, see Figure 23 below. PRP Trailer is added to Layer 2 Ethernet frames by PRP transmitters and is removed by PRP receivers.

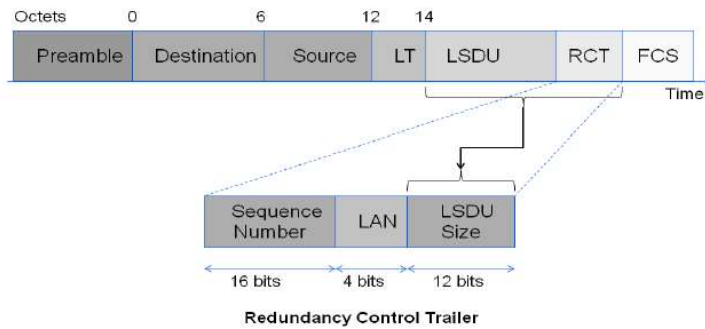


Figure 23 PRP Trailer from [26]

If a device does not support PRP, it would be called a Singularly Attached Node (SAN). It can still be connected to a PRP network using a Redundancy Box (RedBox).

As data arrives to the destination over both networks continuously, when one network path fails, data received over another network is used right away. Thus, there is no switching time and no data losses at all.

3.3.2 High-availability Seamless Ring Redundancy protocol (HSR)

High-availability Seamless Redundancy (HSR) protocol is specified by [28]. It uses the same concepts as PRP but does not require two separate networks. HSR's operating principle is illustrated on Figure 24.

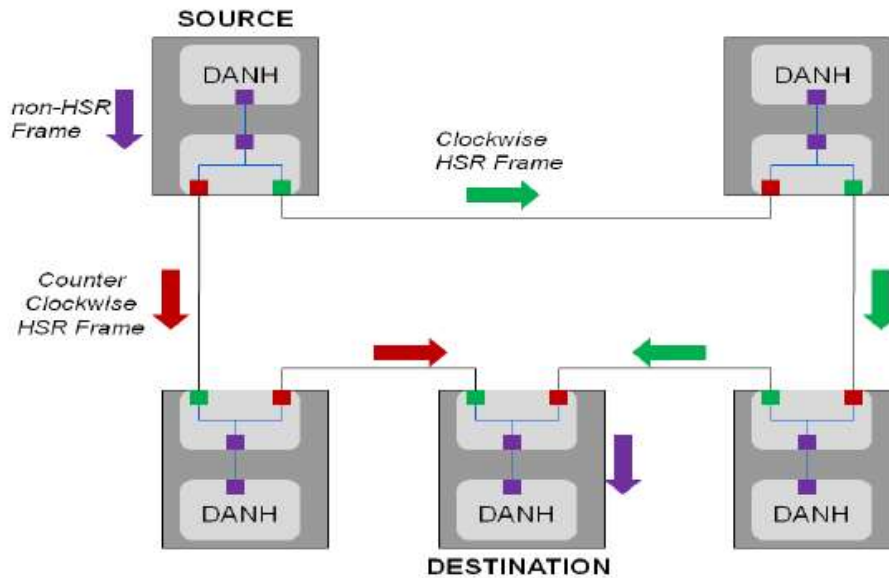


Figure 24 HSR operating principle from [26]

In an HSR ring, data is forwarded in both directions continuously. So, destinations accept first data and discard its duplicate. The association of data with its duplicate is made based on information provided in the HSR Tag, refer to Figure 25 below.

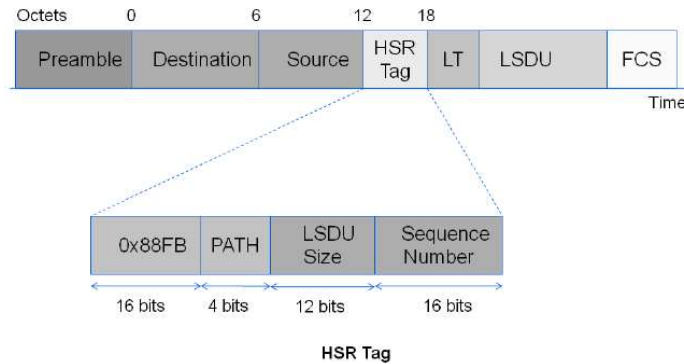


Figure 25 HSR Tag without IEEE 802.1Q Tag from [26]

If a connection in one ring direction fails, only one data sent in another ring direction arrive to a destination. That data will be accepted, and no data will be discarded. If connections in both ring directions fail, no data communication will occur between a source and a destination. For this scenario, another layer of communication redundancy can be considered. It as well can use zero loss redundancy protocol.

While these are bidirectional communication links, theoretically and practically single fiber affecting one data direction only can fail, thus, a possibility of using different path for transmit and receive data directions exists.

Based on the above discussions, the obvious question is why one would use redundancy methods that introduce data losses, while standard protocols with no data losses are specified and supported by devices available on the market today.

For multiple levels of redundancy, multiple levels of these standard protocols can be used as well. There is no need to use any flavors of Spanning Trees to provide communications redundancy for critical applications.

It should also be noted that these protocols, or their variants can support Wide-Area substation to substation communication, where they bring the much-desired no data loss reconfiguration feature.

4. Communication Architecture considerations

Various Ethernet network architectures are possible, and many have been discussed in literature, reports and industry standard, such as [29] and [30]. Comments on the recent industry discussions and recommendations on the most reliable and commonly used architectures are included into this review.

Recent conference paper discussions evolved around mainly two topics:

- (1) combining binary data and analog data exchange at IEC 61850 station bus level with analog data streaming over IEC 61850-9-2 process bus
- (2) using direct or switched connection for analog data streaming – IEC 61850 sampled values.

Using separate networks for IEC 61850 station bus and IEC 61850 process bus traffic may have various drivers, including utility's requirement to use physically separate networks due to devices involved or bandwidth considerations. While separate networks can certainly be used, combining station and process bus into a single redundant network has various benefits. These are discussed in this section, supported by reliability analysis and recommendations provided in [31].

For analog data streaming over IEC 61850 process bus Sampled Values (SVs), a direct connection between a Merging Unit (MU) and a relay can be used (this is referred to by one vendor as 'relay centered'). Switched connection is possible as well (referred to by the same vendor as 'switch centered'). Either will work with well-designed and correctly configured Ethernet switches. Direct connection, obviously, provides a dedicated channel, which prevents sharing data with other devices (for redundancy and monitoring purpose). Switched connection uses communication resources more

efficiently and supports redundant data transmissions plus extended monitoring that can assist with reducing or even eliminating maintenance testing per NERC PRC-005 [32].

Detailed analysis of various Ethernet communication network architectures best suitable for digital substations, including Maximum Time Between Errors (MTBF) assessment using Markov Chains was done in [31]. Overall, the paper discussed various architectures and noted that reducing the number of switches obviously, increases reliability. While redundancy is required, less devices translates to less single points of failures. An optimal network architecture proposed in that paper is still a valid suggestion.

Specifically, after considering multiple network architectures, and covering their redundancy requirements, that paper settled on recommending a ring-based architecture with combined protection and control functionality in IEDs and shared redundant network for both station bus and process bus.

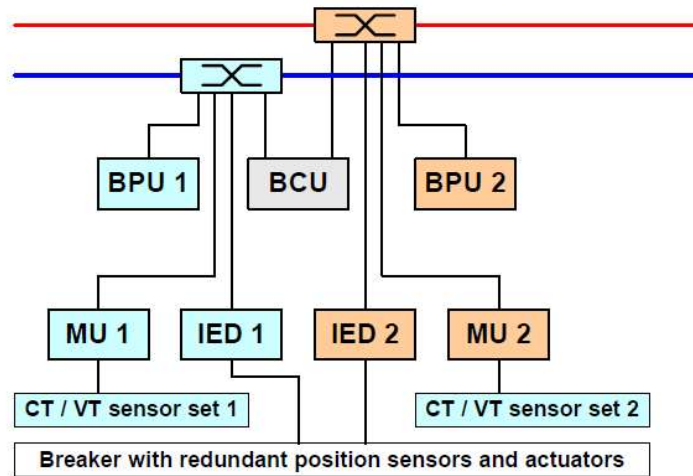


Figure 26 Network/system architecture from [31]

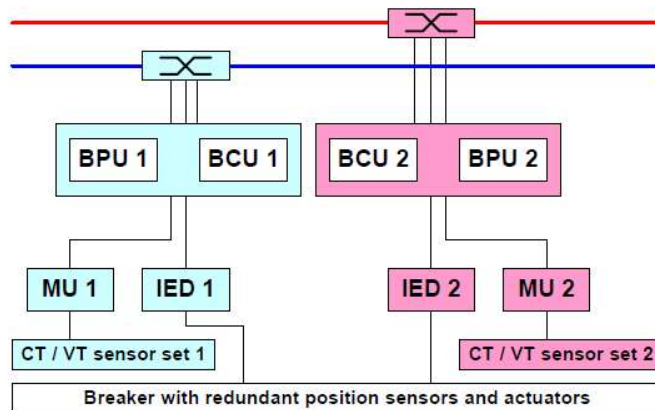


Figure 27 Simplified and consolidated functionality and networks from [31]

While redundancy considerations are very important, having separate dedicated redundant devices for protection and control devices, and dedicated redundant networks for both station and process bus increases the number of devices in the system and, consequently, reduces systems' MTBF.

A balanced simplified redundant ring network topology and protection and control functions consolidation in IEDs were proposed to provide more reliable, yet redundant and simplified architecture.

It should be noted that at the time of writing that paper there were not much MTBF data available for Ethernet switches yet, and now, with more data, a better and higher reliability numbers could be provided.

Another important concept is time synchronization, that is done over Ethernet communication as well for digital substations. Precision Time Protocol (PTP) is used (for the latest version refer to [33]), with specific profiles. For the latest profiles refer [35] and [35]. Note that both are currently under revision: the IEC/IEEE 61850-9-3:2016 is being updated to use the latest PTP standard and combine the features of two power system profiles into a single profile for the industry. For details on time synchronization networks design, implementation, and maintenance one can refer to IEEE 2030.101 [34]. Those interested in what can happen when synchronization is not setup or used correctly, and how to mitigate the risks can refer to [37].

In overall, functions and networks consolidation reduce the number of devices while providing required functionality and redundancy. It is a valid future-proof approach for the digital substation configurations of today and the future.

Each utility typically has specific preferences for digital substation architectures and implementation choices driven by local standards, design or other considerations. The review continues with a summary of main considerations and lessons learnt from digital substation projects recently deployed in North America.

5. Communications Considerations from the Deployed Digital Substation Projects

Many papers were recently published on digital substation projects and lessons learned, such as those described in [38], [39] and [40].

The first wave of digital substation implementations in the utilities stopped at the station bus level and included Ethernet-based communication for Human Machine Interface (HMI) controls, alarm collection and primary equipment monitoring. With no main-stream protection or bay level controls included, utilities still considered requirements for these stations with minimal or less stringent redundancy technologies. Most utilities relied on RSTP-based communication redundancy during this period. Utilities which were extending their station bus all the way to the switchyard very close to the primary equipment relied on HSR-based communication redundancy.

As the technology matured, the processing power of numerical IEDs increased dramatically, this gave the ability for utilities to use end device-based redundancy techniques, such as PRP. PRP became the norm for any station bus communication redundancy.

In the last five years, with many utilities starting to implement process bus technologies, communication redundancy has taken a forefront in the design. With mission critical protection and control schemes getting deployed using the process bus, the need for a seamless redundancy has become a key factor in the selection of redundancy methods and communication architectures. The need for multi-level communication redundancy at the device level is becoming a common requirement in these new digital substation designs.

Table 1 compares various communication redundancy methods for digital substations with process bus implementations.

Table 1 Comparison of communication redundancy methods

Device Level HSR	Switch Level HSR	Device Level PRP
Bandwidth is limited to device port capability. 100Mbps/s is common in these designs.	Bandwidth can be increased to the switches' capability. Most customer use the 1Gbits/s mode in the switches.	Maximum bandwidth option. Utilizes the full capability of the switches.
Simplest design with minimal need for extra network switches for external interfaces into the ring.	The availability is reduced by the addition of more switches in the design and the single node connection of the end devices to the switches.	Maximum availability as this design runs two parallel fully redundant networks.
Cheapest option available	Implementation cost is higher than the device-based HSR.	Overall cost to implement is slightly higher than the switch-based HSR option.
	Configuration complexity also increases.	Configuration is very minimal.

The common witnessed user experiences when deploying digital substations are captured below:

1. By choosing industry standards, common communication redundancy methods, users have been able to successfully reuse their designs for many substations.
2. Vendor dependencies have greatly reduced for standard-based designs.
3. Performance requirements are well established in these standard-based designs and there are very minimal differences experienced by the users when choosing multi-vendor implementation.
4. Users are seeing an increase in maintenance requirements for these networks especially when they become a part of Bulk Electric System (BES). Operation community is always striving to reduce this impact by focusing on minimalistic designs with less network devices.
5. From a configuration perspective, most designs are very standardized leading to a very repeatable common architecture.
6. Users see the value of traffic engineering which helps balance the complexity of the network configuration against the need to use more network devices. This results in very customized engineering efforts that are very much project dependent. Even for these projects the use of standard techniques like VLANs and MAC Address filtering simplify the designs.
7. Precision Time Protocol (PTP) is becoming an important requirement in all digital substation designs with process bus. It plays a significant role in the network design. Time distribution in such networks is an important design criterion. The following choices are usually made in such designs:
 - a. Some vendor products have the capability to support boundary clock (BC) functionality in bay level products. In such cases, end users tend to set the IEDs as boundary clocks and use a PTP grandmaster clock (GM) from the station bus level. Carefully chosen IEDs can transfer time from station bus to process bus level. There is no need for special provisions to tie various bays in the network for such systems.
 - b. Frequently PTP GM clock is connected directly to the process bus. In case of PRP-based systems, it's relatively simple to restrict traffic to port(s) on this clock to reduce network traffic and avoid overloading it. For HSR-based designs, there is a need to either interconnect various HSR rings in the station or connected have multiple clock ports individually to each HSR ring.
 - c. Equally common are designs where clocks do not support any communication redundancy protocols. In this case REDundancy (RED) box device is added to connect such clock to PRP or HSR network.

The above considerations lead into the discussion on future designs. If there is a need to interconnect multiple redundant networks, e.g., by connecting all PRP switches in LAN A and LAN B, or by tying multiple HSR rings together, a need for QUAD box arises. In the early implementations with multiple redundancy levels, the users were relying on RSTP for connecting PRP LAN A and LAN B switches. With growing importance of seamless zero loss redundancy, the users are requiring a QUAD box functionality to provide seamless zero loss redundancy at multiple levels. The theory behind QUAD box operation and the various functions it can serve have been well defined over the recent years. It is expected that QUAD box devices will be common in the future digital substation designs.

6. Conclusions

Digital substations do rely on communications, and choosing best methods and technologies is critical in achieving reliability levels of protection and control applications. Layer 2 Ethernet communication is the specified digital substations' communication technology. Use of multicast messaging and prioritized data processing is defined to achieve required reliability levels. Zero loss redundancy protocols (HSR and PRP) as specified to achieve communications redundancy.

Design and configuration of Ethernet switches does affect communications performance. Use of Ethernet switches with well-organized buffering and forwarding tables increases reliability of communications and protection and control schemes overall.

Network configurations vary, and the future proof trend shows that functions and networks consolidation lead to simpler designs and higher reliability.

References:

- [1] IEC 61850 “Communication networks and systems in substations”, 2002-2021 (www.iec.ch)
- [2] G. S. Antonova “Basics of Communications for Protection Engineers”, Fundamentals Track Lecture given at WPRC 2020.
- [3] IEEE PSRC Working Group H9 Report “Understanding communications technologies applied to relaying”.
- [4] RFC 791 Internet Protocol, DARPA/ARPA Program Protocol Specification, September 1981, available at <https://datatracker.ietf.org/doc/html/rfc791>
- [5] A. Martin, R. Cooke, G.S. Antonova “Effect of communication channel and time synchronization quality on protection”, WPRC 2016, Spokane, WA, USA.
- [6] G.S. Antonova, J. Chang, R. Forrester, J. Shore and P. Stroemich “Line Current Differential: Communication Channel Considerations”, WPRC 2013, Spokane, WA, USA.
- [7] R.M. Cooke “Carrier Ethernet Technology in an Electric Utility’s Communications Network” CIGRE Canada Conference 2016, Vancouver BC Canada.
- [8] WECC Guideline “Communication Systems Performance Guide for Electric Protection Systems”, July 25, 2013
- [9] IEEE 802 LAN/MAN Standards available at <https://standards.ieee.org/featured/802/index.html>
- [10] IEEE Std 802.3-2018 “IEEE Standard for Information technology— Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications”
- [11] IEEE Std 802.1D-2004/2018 “IEEE Standard for Local and metropolitan area networks Media Access Control (MAC) Bridges” (merged in 2018 with IEEE 802.1Q)
- [12] IEEE Std 802.1Q-2018/2020 “IEEE Standard for Local and metropolitan area networks Virtual Bridged Local Area Networks”
- [13] RFC 793 Transmission Control Protocol, DARPA/ARPA Program Protocol Specification, September 1981, available at <https://datatracker.ietf.org/doc/html/rfc793>
- [14] RFC 768 User Datagram Protocol , available at <https://datatracker.ietf.org/doc/html/rfc768>
- [15] IEEE PSRC H32 Report / PES TR-76 “Channel Performance Considerations for Ethernet Circuits Applied to Teleprotection”, June 2020.
- [16] C. Huntley, G. Antonova, P. Guinand “Effect of Hash Collisions on the Performance of LAN Switching Devices and Networks”, Proceedings of the 31st IEEE Conference on Local Computer Networks LCN’06, Tampa, Florida, U.S.A. November 14-16, 2006, pp. 280-284.
- [17] IEC 61850-9-2:2011+AMD1:2020 CSV Ed. 2.0 Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3
- [18] UCA International Users Group “Implementation Guideline for Digital Interface to Instrument Transformers using IEC 61850-9-2” available at http://iec61850.ucaiug.org/implementation%20guidelines/digif_spec_9-2le_r2-1_040707-cb.pdf
- [19] WireShark Capture Setup/VLAN available at <https://wiki.wireshark.org/CaptureSetup/VLAN>
- [20] IEEE PSRC/PSCC Report by WG H12/P6 “Application of Ethernet Networking Devices Used for Protection and Control Applications in Electric Power Substations”, 2017.
- [21] IEEE PSRC WG H6 Report PES TR-84 “Application Testing of IEC 61850 Based Systems”, November 2020.
- [22] IETF RFC 7426 Software-Defined Networking (SDN): Layers and Architecture Terminology, available at <https://datatracker.ietf.org/doc/html/rfc7426>
- [23] SDN standardization efforts, available at <https://sdn.ieee.org/standardization>

- [24] D. P. Erwin, T. Kruckewitt, G.S. Antonova “Interrelationship of Protection and Communication to Improve Power System Reliability”, WPRC 2014, Spokane, WA, USA.
- [25] Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria (A Module of TSGR, FR-440; FR-SONET-17; and FD-29). Telcordia Technologies Generic Requirements GR-253-CORE, Issue 4, December 2005.
- [26] G.S. Antonova, L. Frisk, J-C Tournier «Communication Redundancy for Substation Automation”, Texas A&M Conference 2011, College Station TX, USA
- [27] G. Antonova “Spanning Tree Protocol Interoperability with Other Loop Prevention Algorithms”, 20th Canadian Conference on Electrical and Computer Engineering CCECE 2007, Vancouver, Canada.
- [28] IEC 62439-3:2016 Ed 3.0. “Industrial communication networks - High availability automation networks -Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).”
- [29] IEC TR 61850-90-4:2020 Communication networks and systems in power utility automation Part 90-4: Network Engineering Guidelines.
- [30] IEEE Std 2030.100™-2017 IEEE Recommended Practice for Implementing an IEC 61850-Based Substation Communications, Protection, Monitoring, and Control System.
- [31] L. Andersson, K-P Brand, Ch. Brunner, W. Wimmer “Reliability investigations for SA communication architectures based on IEC 61850”, Presented in Poster Session at PowerTech, June 27-30, 2005 St.-Petersburg, Russia
- [32] NERC PRC-005 Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance, 2020
- [33] IEEE 1588-2019 - IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
- [34] IEEE 2030.101-2018 - IEEE Guide for Designing a Time Synchronization System for Power Substations
- [35] IEC/IEEE 61850-9-3:2016 Ed. 1.0 Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation.
- [36] IEEE C37.238-2017 IEEE Standard Profile for Use of IEEE 1588™ Precision Time Protocol in Power System Applications
- [37] G. S. Antonova, M. Weiss, D.P. Erwin “Protection and Control Dependencies on Time: Applications, Challenges and Solutions”, WPRC 2018, Spokane WA, USA.
- [38] C. Cheng, R. Kimura, J. Chang « Lessons Learned Engineering a Digital Substation”, Power Energy and Automation Conference, PEAC, 2019, Spokane WA, USA.
- [39] T. Roseburg, W. Rees, G.S. Antonova “Benefits of using IEC 61850 messages for testing conventional protection schemes”, WPRC 2020.
- [40] G. Gresko, S. A. Kunsman, S. Morbin, M. Kockott, Smart substation: design, installation, testing, and training experience, presented at the 44th Western Protective Relaying Conference, WPRC, Spokane, WA, USA, October 2017.
- [41] IEC 61869-9:2016 Ed. 1.0 Instrument transformers - Part 9: Digital interface for instrument transformers