Understanding the differences between an office switch and a substation switch

N. C. Fernandes, V. D. Nicholas, S. L. Zimath, J. P. Oliveira, *and* C. Modelli.

Abstract -- **The standard IEC 61850 is pushing substations towards intensive use of high speed digital communication among their devices (IEDs). One of the key components of digital communication is the network switch device. There are many devices available on the market for office environments. However, protection engineers usually struggle to understand the characteristics of these "office" switches and decide if they are fit to meet the most restrict substation requirements. This article describes the similarities and differences between the office switches and the ones designed specifically to meet the requirements of the electricity sector, taking into account the standards and the specific needs of substations.**

Index terms -- **Switch for Substation, IEC61850, communication in substations, PTP, IEEE Std 1588-20.**

1. INTRODUCTION

Data communication between devices has evolved exponentially since the 1950s, when it was confined to research laboratories to interconnect mainframe computers. From the mid-'70s, with the advent of personal computers, communication gained a new momentum and was intensified when these machines began equipping corporate offices, specially towards the late 80s.

N. C. Fernandes and V. D. Nicholas are with Traceback Technologies, Rua Lauro Linhares 589, Florianópolis, SC 88.025-500 Brazil (e-mail: nestor@traceback.com.br, vladimir@traceback.com.br)
S. L. Zimath and J. P. Oliveira are with Reason Technology S. A., Rua Delinda Silveira, 855 Florianópolis, SC 88.025-500 Brazil (e-mail: sergio.zimath@reason.com.br, jurandir.oliveira@reason.com.br).
C. Modelli is with Endesa-CIEN, Garruchos, RS, Brazil (e-mail cmodelli@endesabr.com.br)

At that time, the communication infrastructure to link an office consisted of the use of a coaxial cable which formed an open bus that passed through all the computers, causing them to share the same physical environment.

The great amount of collisions during communication by disputing the same physical cable was a constant. However, as the need for traffic was little, the speed transfer of data was compatible with the processing capacity.

With the increasing efficiency of computers, alternatives such as increased speed of the physical environment and traffic segregation came about to reduce these losses. The increased throughput of the physical environment would decrease the chance of collision due to faster flow of data packets and thus shortening computer access time. This would be an acceptable solution if the computers and processes involved remained with the same traffic needs, which of course did not happen.

An additional problem associated with the network bus topology was the shutdown by impedance mismatch at any access node since it forms a shared waveguide. Simply increasing the throughput of the physical waveguide would leave this even more sensitive. In order to compensate for the increased sensitivity, the "hub" was created in order to implement a new connection bus, namely star connection. Hubs have an internal circuit that isolates the computers that have impedance mismatch without affecting the other networked devices.

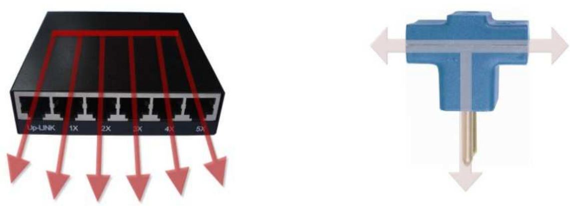

FIGURE 1 – Hub and T Connections

The other alternative would be to create a sort of temporary circuit between pairs of computers, since at any given time each computer can communicate with another computer by just using a single interface. To implement this alternative in open bus topology, it is necessary to have a new device that could manage these temporary connections. In terms of isolating failures, it should be like the "hub". However, it should have sufficient intelligence to route each data packet only to the target computer. This approach is known as "segregation of traffic," and the device that performs this feat was dubbed "switch".

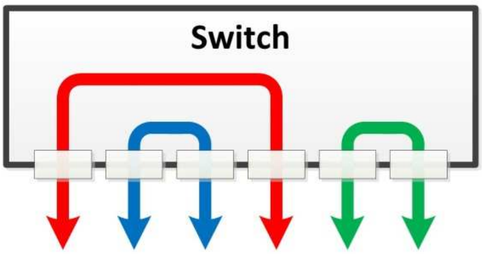

FIGURE 2 – Switch Connections

Today, the switches that make up the communication infrastructure in offices are "plug-n-play" devices, by simply connecting network cables to it without settings to operate. These switches do segregation of traffic very well, however, nothing else. The reliability of these devices are compatible with other points of failure in an office environment, such as operating systems, programs, computers, surge protectors, cables, etc., which can disrupt communication without major consequences.

The benefits of network communication technology can be extended to many other environments beyond that of an office. Especially after the implementation of the standards IEC 61850, this is exactly what is now happening in the electric power substations scenario. The necessary technology is essentially the same, but the reliability and robustness requirements are much greater. If you lose one or two commands typed in an office environment it will not generate greater consequences. However, the same is not true regarding the loss of a message from an interlock protection relay that needs to arrive at its destination in four milliseconds so as not to compromise the entire system.

2. DIFFERENT ENVIRONMENTS, DIFFERENT REQUIREMENTS

An office environment consists of a group of people and computers that are interconnected by a communication infrastructure designed according to the dynamics of the group. People fail, programs fail, computers fail, therefore there is no infallible network since it is just another link in the chain. Every failure in this chain is accepted as being somewhat normal when it takes up to only a few minutes to recover, either by exchanging a cable, rebooting the computer OS, restoring a backup or even partially retyping the document occasionally damaged by the failure. In such scenario, a network failure per day is somewhat acceptable, thus the set of equipment in the network may have a low cost, because whenever a problem occurs it can resolved by simply turning the system off and on again.

On the other hand, in a substation environment (generation, transmission or distribution) there are devices communicating among each other, exchanging important data in order to maintain a consistent operation of the substation. When a protective relay detects any abnormality, the information sent is urgent and needs to reach the other devices within the shortest period of time possible.

2.1 Environment Requirements

The installation environment of the network infrastructure makes all the difference when selecting its components, including switches. Disturbances such as electromagnetic noise, vibration, and extreme temperatures can affect the normal operation with direct consequence on the reliability of the communication.

Table 1 – Environment Requirements

Requirement	Substation	Office
Electromagnetic Interference	Very strong	Negligible
Enclosure	Metal, for 19" rack or DIN rail	Plastic, desktop
Communication Interfaces	Optical and electrical	Electrical
Operating Temperature	-40 to +85 º C, per standard	0 to +40 º C with air conditioning
Power Supply	AC and/or DC, redundant and internal	AC, single and external
Operation	24 / 7	Working hours

2.1.1 Electromagnetic Noise Immunity

The network infrastructure of a substation that complies with IEC 61850 standard is implemented in the same environment as other IEDs and is subject to strong influence of electromagnetic phenomena that generate noise induced and conducted on all the equipment. The switches designed to operate in hostile environments, such as substations, must pass a battery of tests that certify their immunity to external electromagnetic interference. Any erratic behavior caused by such noise compromises the reliability of operation of the substation as a whole. Therefore, the requirements outlined in IEC 61850-3 are much more restricted, far beyond what a switch designed for an office environment could handle.

The enclosure of a substation switch is always made of metal to shield the internal circuitry, usually with metal tabs also placed into 19" racks and is always well grounded. The equivalent for an office usually has plastic casing and it is not subject to external electric fields in its location. Some switch models have tabs in order to be placed in a rack.

The communication interfaces available in office switches are almost all Ethernet twisted pair cable standard. Substations generally use optical interface because there are high voltages and differences in potential involved, since it provides high speed and full galvanic isolation. Because not all IEDs have optical interface, the switch must offer a mix of interfaces. The most common is to have electrical interfaces to IEDs that are in the same relay room and optical interfaces for connecting to other relay rooms.

Additionally, the standard IEEE Std 1613-2009 defines minimum requirements for networks in a substation environment, addressing climate testing and electromagnetic compatibility. Switches are considered as IEDs (communication) and thus are also subject to some tests required for protective relays as stated in IEEE Std C37.90-2005.

2.1.2. Operation in Extended Temperature Range

The temperature range of operation is another important requirement because the equipment operating in substations should use only natural convection cooling. Fans or other mechanical ventilation are not allowed due to their low reliability. Even when the air conditioning of a substation fails, the protection and control equipment must continue to operate normally. For this reason, switches designed to operate in the substation must operate at temperatures as low as -40 ºC and up to +85 ºC using only natural convection cooling. The office switches in turn operate in the same environment that humans and devices are fit for. Therefore, nearly all of the most sophisticated models have at least a small fan.

The electronic components used in switches are also designed according to the temperature range of operation, which directly reflects on the casing material and final price. Processors, memories and other electronic components are classified into the following basic operating temperature ranges:

- Commercial, from 0 to +70 ºC
- Industrial, from -40 to +85 ºC
- Aviation and military, from -55 to +125 ºC

The environment conditions for electrical devices in substations are defined in the standard IEC 61850-3 (Communication networks and systems in substations - Part 3: General requirements), which refers to IEC 60870-2-2 (Telecontrol equipment and systems - Part 2: Operating conditions - Section 2: Environmental conditions (Climatic, mechanical and other non-electrical influences)). Such standard establishes four classes of sites according to the atmospheric environment:

- Class A: air-conditioned places (internal)
- Class B: indoors with heating / cooling
- Class C: sheltered places
- Class D: open air (external)

Most substations are class "C", which in turn is divided into four subclasses according to ambient temperature:

- Class C1, from -5 to 45 ° C
- Class C2, from -25 to 55 ° C
- Class C3, from -40 to 70 C
- Class Cx: Special

The standard IEC 60870-2-2 specifies that for IEDs in substations C2, C3 or Cx, the temperature range required is from -40 to 85 °C, consistent with the classification "industrial" in the electronic industry. It is interesting to note that Class C1 is enough to exclude the vast majority of office switches, either by exceeding the temperature specification (0 to +40 ºC) or by using fan cooling.

2.1.3. Redundant Power Supply

The power supply for switches is another important and very distinct requirement between substations and offices. Substations usually have two separate DC power supply circuits for each relay room, creating a redundancy to avoid single points of failure. The switches designed for use in substation have two separate AC/DC power supplies within the same casing with independent inputs. They also have double capacity so that in case one the power lines should fail, the other source can keep the equipment operating safely. On the other hand, office switches are often fitted with a single external AC power supply.

2.1.4 Operating Regime

The operating regimes of the network infrastructure are also different between substations and offices. In offices, most of the communication takes place during normal business hours, when there are people available to reset the switches in case of failure. On the contrary, substation operation is continuous and often unsupervised, which means operation 24 / 7 without any human intervention.

2.2 Management Requirements

The office switches are available in two variations: with and without management. The most common - and cheapest - is the model without management, which performs only the basic task of sending packets. The management model has access to internal performance counters via SNMP (Simple Network Management Protocol) and some access and configuration controls. Depending on the size of the switch, they have a feature called quality control of service or QoS (Quality of Service). Therefore, you can configure traffic restrictions to balance certain types of packets. The basic function of management in the office environment is the mapping of traffic for statistical effect of using the interface that connects to the Internet.

In a substation environment, the network infrastructure must operate without the human intervention and does not have any connection to the Internet for remote management. The operating parameters of the switches must be configured to ensure the flow of information even in situations of stress. Furthermore, the internal counters provide information for analysis of the network, showing the communication bottlenecks that need fine tuning. Therefore, management is actively used.

Table 2 – Comparison of Switches Management Requirements

Requirement	Substation	Office
Management	Indispensable	Dispensable
Access Control (security)	Indispensable	Dispensable
Configuration	Required and important	Dispensable

2.2.1 Access Control (Security) - Authentication and Authorization

The managed switches allow the user to configure their behavior in various situations of operation and consequently restricted to few people. Usually, only one password is used to control the access to the configuration settings. In some more sophisticated models, more than one password may be required, stratifying access and allowing better control over who can access what. At this point, the most sophisticated office switches and substations switches are similar.

Virtually all managed switches support remote authentication and authorization, using a single centralized server in order to verify passwords (authentication) and control level of access (authorization). This simplifies the management of switches by network administrator and improves the security of access.

The mostly used Authentication and Authorization protocols in managed switches are:

- TACACS (Terminal Access Controller Access-Control System), RFC-1492, July 1993
- TACACS + (Authentication Dial In User Service), RFC-2865, June 2000

2.2.2 - Access Control (Security) - Advantages and Constraints

Since switches make up the network infrastructure itself, their management can be performed from a centralized location. The authentication phase ensures that the switch is known by both the access control server and the end user. This is great feature for network administrators.

On other hand, in complex environments and potentially vulnerable ones, you can configure the switch to restrict access, even for people authenticated by the central system. In this situation, a switch in a substation differs from its counterpart in an office by offering the following additional possibilities:

- Definition of a given physical interface for point to point configuration
- Definition of the MAC address of the computer (PC or notebook) that can configure the switch

These constraints demand the physical presence of the operator in the substation environment to reconfigure the switch, even when using the same authentication and authorization server for password validation.

2.2.3 – Delivery Assurance

A switch is a device that receives messages from other devices that are connected to it and then relays such messages to their recipients. When multiple devices send messages to the same recipient a queue is usually formed on the output interface. In exceptional cases, when the queue reaches a certain size, a low cost switch may simply discard the last messages due to limited storage capacity. It is an extreme case, but possible in an office environment. If the office server does not receive a particular data packet, it will surely be repeated by the computer that is making the request in a transparent manner, that is, it all takes place without users´ awareness.

In the substation environment, the requirements are much more restricted, especially when a protective relay sends an emergency message. This message must be delivered in the shortest time possible. Having to enter a queue is undesirable by itself and having the messages silently discarded is totally unacceptable. To manage this situation, when an IED detects any problem, it starts repeating the same message every few milliseconds, flooding the network in hopes that at least one of them reaches its proper destination. This avalanche of data in turn contributes to the formation of the queue. Therefore, switches designed to work in substations need to provide delivery mechanisms that minimize the delay of some message types. These mechanisms can be longer queue capacity and dynamic change of priority of data packets in transit. One of the most efficient mechanisms is the creation of VLANs, which are virtual circuits that share the same physical environment without interfering with one another, coupled with quality control service.

2.2.4 - Bandwidth Reserve on VLAN

The VLAN (Virtual Local Area Network) standard is IEEE Std 802.1Q, which considers the grouping of IEDs, up to 4095 or distinct virtual circuits. Each group can see only the stations in their group, as if the network were exclusive to them. This simplifies management and allows the establishment of rules for the use of physical means, such as bandwidth reservation and priority delivery.

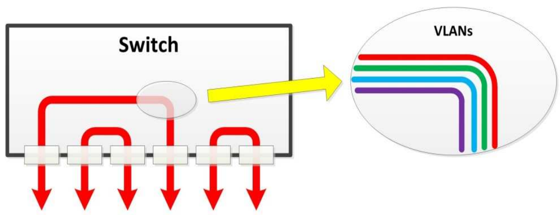

FIGURE 3 – VLAN Virtual circuits

The bandwidth allocation is based on the ranking of priorities of VLANs and follows the standard IEEE Std 802.1p (now incorporated in IEEE Std 802.1D-2004). The higher the priority of a particular VLAN, the shorter the delay in delivery of the packet and the greater the allocated bandwidth. Thus various types of communication can occur simultaneously, each confined to its own VLAN and the switch is in charge of dynamically distributing the available bandwidth. All substation switches must support these mechanisms, but only the most sophisticated (and most expensive) office switches provide this feature.

2.3 - Priority for GOOSE Messages

The IEC 61850 standard describes how the IEDs communicate among themselves using the network infrastructure, formatting and interpreting several ypes of messages such as GOOSE (Generic Object-Oriented Substation Events), Sampled Values, Reports and Synchronization.

GOOSE messages are generated to disclose events of the IEDs that have high priority traffic in the network, therefore, they must be confined on VLANs and sorted so that the delivery delay is minimized, even in comparison with other types of messages defined in the standard. This requires careful planning of the network and, of course, the switch must support this type of setup and operation.

A small detail of the IEC 61850 standard allows GOOSE messages to be sent without the IEDs having been configured to use VLAN. In this particular case, an ordinary office switch has no means of prioritizing traffic because it was not designed for use with this protocol in particular. The switches for the substation, on the other hand, need to detect this scenario and treat it as a priority.

2.4 – Synchronization of IEDs

Synchronization of IEDs with a precision time reference is a growing need as new technologies are been applied at substations. The reference which is accepted worldwide for synchronization is based on the GPS satellites system, and it ensures accuracy and monotonicity of the time readings. The reception of satellite signals and conversion into electrical signals within the substation is performed through special equipment (GPS-based clocks) by using IRIG-B standard interfaces.

With the deployment of network infrastructure on the standards set by IEC 61850, the point-to-point synchronization becomes meaningless, since the same effect can be obtained through the network. Today, NTP (Network Time Protocol) servers are used to distribute the time reference obtained from the satellites, and virtually all modern equipment offer this method of synchronization. The problem is that this protocol was not designed for precise synchronization but rather only to allow computers distributed around the world to synchronize their internal clocks with accuracy of a few tens of milliseconds. Even when putting the NTP server within the substation, this accuracy is not enough to meet the one-millisecond precision required by most electrical power systems.

With the proliferation of PMUs (Phasor Measurement Unit) the current need for accuracy is around a few microseconds, making it necessary to use some mechanism better than the NTP to synchronize the IEDs. Thus, the PTP (Precision Time Protocol) was created. The PTP is defined by IEEE Std 1588-2008, also known as IEEE 1588 v.2. With this protocol it is possible to synchronize dozens of IEDs with accuracy below one microsecond.

The PTP is a simple protocol for use only in local networks, as opposed to NTP, which was designed to be used on the Internet. The implementation of PTP, however, requires careful planning and a special hardware within the switches to ensure microsecond precision. No office switch supports PTP for at least two basic reasons:

- Cost, as additional hardware is required for each interface
- The precision offered by PTP is not necessary in the office environment

These requirements alone are enough to invalidate the use of office switches in substation environments because any uncompensated internal delay will cause significant reduction of the PTP signal accuracy.

Version 2 of IEC 61850 was adopted as the PTP synchronization pattern, thereby meeting the requirements of new applications in the electricity sector that require precision of 1 millisecond. A new synchronization profile for substations, which will facilitate the configuration of IEDs using PTP, is expected to be published in 2011 in the standard IEEE C37.238.

2.5 – Protocols

To ensure the operation of the network infrastructure at substations, switches must support a set of standardized protocols, such as:

- IEEE Std 1588-2008 or PTP (Precision Time Protocol), used for synchronization of IEDs
- IEEE Std 802.1D-2004 (Media Access Control Bridges), defines the basic operation of switches

and includes standard and replaces the Following:

- IEEE Std 802.1w (Rapid Spanning Tree Protocol), Which defines the control dial ring
- IEEE Std 802.1p Quality of Service (at MAC level), Which Classifies and controls traffic

- IEEE Std 802.1Q-2005 (Virtual Local Area Network Bridges), defines the creation of virtual subnets within the physical network
- IEEE Std 802.1ak (Multiple Registration Protocol), sets automatic configuration of VLANs
- 802.1AX IEEE Std-2008 (Link Aggregation), defines the channel bandwidth aggregation for Increased Between Two switches and replaces the IEEE Std 802.1ad
- IEEE Std 802.1X-2010 (Port Based Network Access Control) defines security access to the configuration of switches
- IEEE Std 802.3i (Ethernet) defines the transmission at 10 Mbps electrical interface
- IEEE Std 802.3u (Fast Ethernet) defines the transmission of 100 Mbps in electrical and optical interfaces
- IEEE Std 802.3z (Gigabit Ethernet) defines the transmission of 1 Gbps in electrical and optical interfaces
- IETF STD0062 (Simple Network Management Protocol version 3 - SNMP v3), used to manage communications equipment, set the number of documents RFC 3411 to RFC 3418
- RFC 2021 (Remote Network Monitoring version 2 - RMON v2), defines the management information and control communications equipment must withstand
- RFC 3376 (Internet Group Management Protocol version 3 - IGMP v3) defines the interaction between switches and routers within the same local network for processing of messages in multicast
- RFC 5905 (Network Time Protocol version 4 - NTP v4), used for synchronization of IEDs
- RFC 2865 (Remote Authentication Dial In User Service - RADIUS), defines the interaction of equipment with the server authentication and authorization
- IEC 61850-8-1:2004-05 (Communication networks and systems in substations Part 8-1: Specific Communication Service Mapping) defines the basic encoding of messages GOOSE and Sampled Values GSE Management

2.6 – Network Redundancy

The first version of the standard IEC 61850 has not addressed the issue of network redundancy. This feature is an important requirement to ensure that the communications between all IEDs will continue without interruption in case of a single failure at some point in the network, such as a broken optic fiber cable.

The basic redundancy in communication involving multiple switches is done through a ring connection between them, thus creating a second delivery path between any stop switches. Paradoxically, this topology introduces a problem that could lead to a situation of a data packet circulating continuously until the ring saturates, making the switches inoperative. The protocol that avoids this is called RSTP (Rapid Spanning Tree Protocol), and is described in IEEE Std 802.1D-2004. The weakness in this protocol is the time it takes to discover that something has gone wrong with the ring and then reconfigure the switches involved in order to use the alternate route, usually in the order of several tens of milliseconds.

Version 2 of the IEC61850 standard provides two ingenious redundancy solutions that reduce recovery time of a crash of communication by a single point of failure to zero. However they require that their IEDs support additional hardware. Both solutions add information into data packets and require the IEDs to have dual network interface. Moreover they address the inevitable duplication of information as part of their routine communications.

The standard HSR (High-availability Seamless Protocol), described in IEC62439-3.5 standard proposes the addition of the switch function within each IED so that the IEDs themselves make up the communication ring. Thus the use of traditional switches becomes optional.

The standard PRP (Parallel Redundancy Protocol) is described in the IEC62439-3.4 standard and supports the creation of two identical and parallel networks without any connection between them. All the IEDs will be simultaneously connected to both networks and, therefore, redundancy is total and, of course, recovery time is zero.

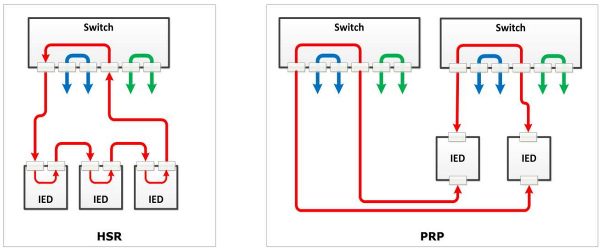

FIGURE 4 – Architecture of HSR and PRP.

3. CONCLUSIONS

There are several factors that qualify a switch to operate within a substation as part of the network infrastructure. Even in an ideal world, where all the substations would have the same conditions as those in offices, such as: temperature controls, no electromagnetic interferences, use of only electrical interfaces and without the need to prioritize GOOSE messages or precisely synchronize IEDs, the choice for an office switch would still arise questions regarding reliability. As its name implies, operating at a substation depends on the network infrastructure, which cannot be considered as a weak link or compromise the whole electrical system and the safety of the substation. Definitely it is not a good idea to cut down on costs in the network infrastructure since repairing the damage from such “economy” may eventually be much more costly.

4. REFERENCES

- 1588-2008 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
- IEC 61850-3 Communication networks and systems in substations - Part 3: General requirements
- 1613-2009 IEEE Standard Environmental and testing requirements for communications networking devices installed in electric power substations

5. AUTHORS

Nestor Charles Fernandes, B.S. in Physics (1982) and M.S. in Electrical Engineering - Control Systems (1984) from Federal University of Santa Catarina. He has developed major projects in hardware and software since 1985 and currently serves as CEO and CTO for Traceback Technologies Precision Link.

Vladimir Duk Nicholas, B.S. in Electrical Engineering (2000) from Federal University of Santa Catarina. Working for Traceback since 2008 as the principal hardware engineer.

Sergio Luiz Zimath, B.S. Control Engineering and Automation (1997) from Federal University of Santa Catarina. Working for Reason Technology since 1995. Involved in the development various products, including RT1000 and RT2000 GPS clocks and fault digital recorder RPIV. He is currently the director of innovation and responsible for the development of new products and research projects.

Jurandir Paz de Oliveira received his Ms.C. (1997) and Electrical Engineering (1988) degrees from Federal University of Santa Catarina (UFSC), Brazil. He has been related with Reason Tecnologia since 1995, as partner and technical director.

Cleberson Modelli received his B.S. in Electrical Engineering (2002) from Engineering Federal University of Itajuba (UNIFEI - Brazil), with emphasis in Electrotechnics. He has been working at ENDESA – CIEN since 2007. He is Protection and Control senior specialist.