

Areas for Redundancy in Ethernet Systems with focus on IEC 61850 Applications

Dominic Iadonisi, Industrial Market Manager, RuggedCom Inc.

René Midence, Utility Market Manager, RuggedCom Inc.

Introduction

Today Ethernet is the predominant networking technology used in office and home environments. Because Ethernet networks are inexpensive and fairly well understood, their use is quickly becoming popular for utility applications including substation automation networks.

Despite the fact that Ethernet networks were not developed specifically for operation in substations and other harsh environments, Ethernet is so popular in other applications that it is easiest and simpler to utilize and enhance Ethernet than to create something new. New Ethernet equipment has been designed to operate reliably under extreme harsh environment.

Utility networking experts are moving forward accepting the limitations of Ethernet networks and solving the problems associated with Ethernet networks. Advances in computing power and network technology allow us to take advantage of the popularity and availability of Ethernet networking equipment and solutions.

A variety of flexible network architectures offering different levels of performance, cost and redundancy are achievable using managed Ethernet switches.

This article looks at considerations when designing an Ethernet network for substation automation applications which may include IEC61850 Station or Process bus or a combination of both, with focus on redundancy. With Ethernet based networks and protocols, redundancy is needed to maintain maximum uptime and still be able to deal with minor outages and failures to the environment. This all gets rolled into the reliability of the entire system, from the very edge devices and IEDS, through the network core, to the plant backbone.

Understanding the relationships between the physical structure of a network and the protocols that run on the network to provide is key to creating a truly maintainable, adaptable and reliable network that deals with issues effectively.

The three main areas for Ethernet-based controls redundancy are physical, data link and network as show in Figure 1 below. We will be tackling each area individually showing the specific areas that can support redundancy. Security is a separate topic and will not be handled in this document

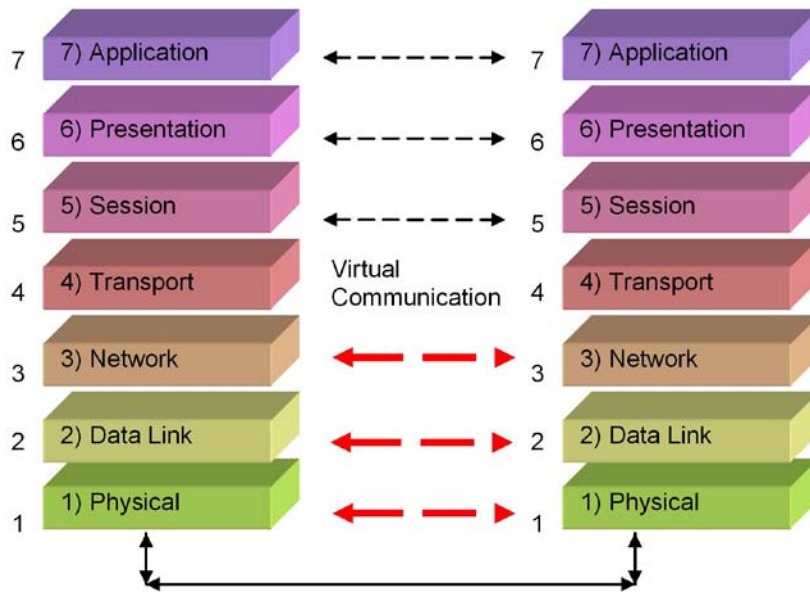
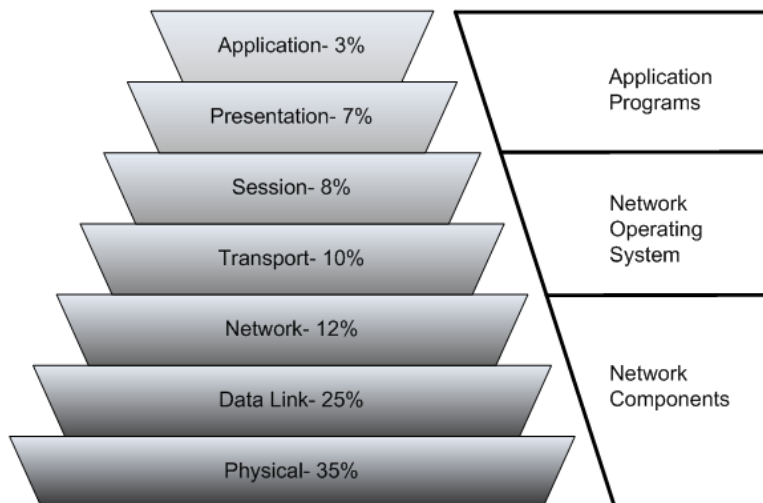


Figure 1 - Areas of redundancy focus in the OSI model

The lower you look at the OSI model, the greater the impact of failures that occur. For example, if you lose a cable connecting an end device to a switch port, there is no data movement of any kind and there is an impact for the entire process, depending on the importance of that end device. If there is an issue at layer 3 where a router may have experienced a loss of power and loses connection to the plant backbone, localized plant processes can still operate, but operation for distributed plant or business processes can be affected.

Figure 2 shows impact upon the network based upon percentages. Again, notice that the lower you go, the more impact failures have, with 72% of failures occurring on the first 3 layers. These include hardware failures, cabling failures, power losses, programming miss-configurations, etc.



Source: Datacom, Network Management Special

Figure 2 - Area of System Failure with Percentages

Functions of an Ethernet Switch

Ethernet is a packet based communications technology where an IED may start transmitting a data packet at any time. The function of a switch is to prevent collisions of these packets and to send the packet in the direction of the desired recipient. This is done using the descriptively named 'store and forward' process where received packets are buffered in memory on ingress, placed in a queue for the egress port, and then transmitted once the packet reaches the front of the queue. It is the queuing mechanism that eliminates collisions and allows full duplex operation.

Full duplex operation is a data communications term that refers to the ability to send and receive data at the same time. Legacy Ethernet is half-duplex, meaning information can move in only one direction at a time. In a totally switched network, nodes only communicate with the switch and never directly with each other. Switched networks also employ either twisted pair or fiber optic cabling, both of which use separate conductors for sending and receiving data. In the substation environment fiber is the preferred option.

In switched Ethernet the devices connected to the network can forgo the collision detection process and transmit at will, since they are the only potential devices that can access the medium. The end stations in this case can transmit to the switch at the same time that the switch transmits to them, achieving a collision-free environment.

This is in contrast to repeaters or hubs of the past that used CSMA/CD to detect that a collision occurred and then retransmitted a random amount of time later. Determination of the egress port is done via MAC address lookup and learning of addresses which makes this entire operation automatic. The basic functionality described above can be found in what is termed an *unmanaged switch*. A managed switch offers additional functionality for managing and optimizing the network. Some of these features include:

- User interface via RS232, Telnet, SNMP, HTTP, ...
- Status, statistics, and troubleshooting facilities
- Rapid Spanning Tree (IEEE 802.1D-2004) for fault tolerant topologies
- VLANs (802.1Q)
- Class of Service - CoS (802.1p)
- SNMPv2, RMON Groups 1, 2, 3, 9
- IGMP(Internet Group Messaging Protocol)
- GMRP(Generic Multicast Registration Protocol)
- GVRP(Generic VLAN Registration Protocol)
- Link aggregation (IEEE 802.3ad)
- Port Mirroring

The Ethernet switch certainly is an Intelligent Electronic Device with complexity that can rival protective relay IEDs. Current standardization efforts within IEEE C37.2 are even planning on giving the switch a power system device function number so that it may be incorporated into drawings in a more consistent manner. The proposed ANSI device number of '16S' for a network switch may one day become as common on one line diagrams as a '52' breaker.

IEC61850 Process - System design

One of the most important functions of the substation automation system is the protection function. The majority of large Utilities design their protection with two independent protection systems called Protection A and Protection B. With a conventional protection and control systems, this is normally achieved by means of two protection relays, usually from different manufacturers that are individually connected to the process equipment.

The same level of redundancy needs of course to be achieved when designing an Ethernet network that will be used for IEC 61850 applications. That requires the duplication not only of the IEDs in the process equipment but also the

communication system. This is considered in the architectural considerations for the use of IEC 61850 as process connection.

Substation automation consists commonly of three levels:

- Station Level which may include a Human Machine Interface (HMI) and possibly a gateway (GW)
- Bay Level consisting of protection and control IEDs
- Process Level near the switchyard which includes instrument transformers, breakers, etc.

At each level, IEC61850 capable devices are connected to a communications network. The basic assumption is that this network is based on Ethernet switches that facilitate the distribution of functions and information to more than one IED. At the process level there are some real time requirements in addition to the station level requirements typically needed for operations and supervision.

Basic Communication Architectures

The communications network may be one of the following:

- **Star Connection**, e.g. comprising of one central switch being connected to all IEDs by one link (star type, Figure 3 without dashed part).
- **Ring Connection** - Some inherent communication redundancy is provided e.g. by a ring of switches connected to IEDs with a single link (Refer to Figure 4 without dashed links).
- **Star or Ring Redundant** - The communication system may also consist of two independent star or ring subsystems where each IED has a separate port to each network, providing a higher level of availability as shown in Figure 3 and Figure 4 with dashed parts.
- **Multiple Redundancy** - Technical restrictions and performance requirements may imply a big system with many switches with a structure of several redundant networks. This last type will not be considered here.

The overall Substation Automation system redundancy depends not only on the redundancy of the communication system but also on the IEDs, especially on the number of parallel communication ports determining the number of possible links to the switches.

IEC61850 in Real Time

In a substation designed following IEC61850 standards, the information exchange between the process equipment and the substation automation is subject of high requirements regarding the real time behavior. The most critical information exchange is the one related to protection i.e. the transmission of the sampled values from the instrument transformers to the protection relay and the transmission of the trip command from the relay to the circuit breaker or transmission of interlocking commands between relays (per-to-peer communications). According to IEC 61850-5, the acceptable maximal communication delay is for the highest class as few as three milliseconds. This has to be achieved independent from the load of the communication network.

The communication stack for client-server communication specified in the mapping defined in IEC 61850-8-1 (Station Bus) and IEC 61850-9-2 (Process Bus) is MMS over TCP/IP and Ethernet. Ethernet as known from the office environment would not fulfill the requirements of a process connection. However, trends to use Ethernet as well in substation automation have lead to the development of Ethernet extensions that provide real time capabilities. IEC 61850 is using switched Ethernet to avoid collisions. The time-critical-messages are not routable and are directly mapped on the link layer. With the additional use of priority tagging and full duplex connections to the switch for the devices with time critical information, the real time requirements can be fulfilled.

Figures 3, 4 and 5 show typical network topologies used in Ethernet networks servicing IEC61850 Station Bus implementations. In these networks, the IEDs are connected to a Human Machine Interface (HMI) or Gate Way (GW) via new generation of Ethernet switches designed to meet the requirements of the standard.

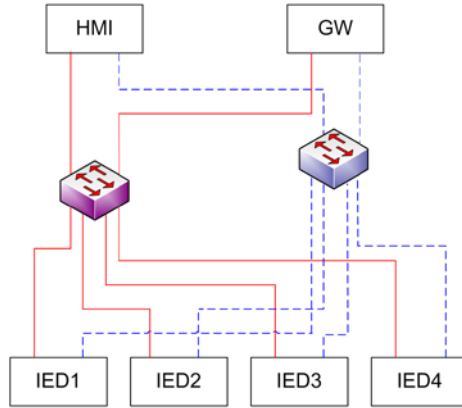


Figure 3 - Non-redundant Star Communication System

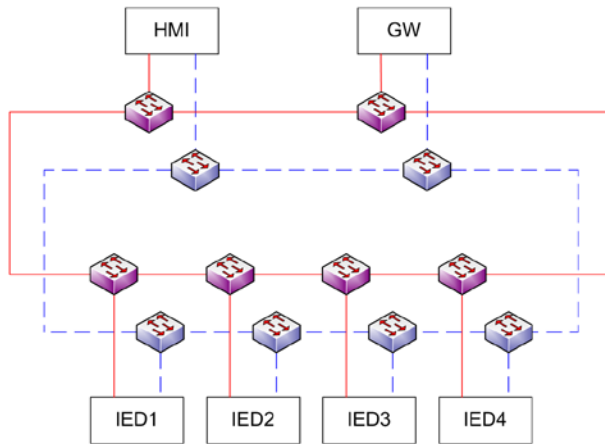


Figure 4 Doubled Parallel Redundant Network

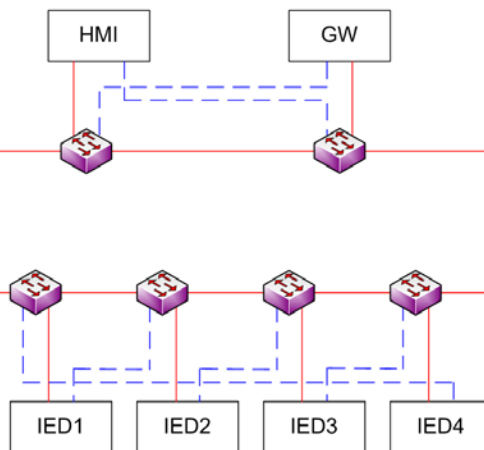


Figure 5 - Communications System with Ring Redundancy

Process busses and functional redundancy

Possible process bus architectures are determined by the fact that the protection could be redundant (Protection A, Protection B) at least at the transmission level of the power system. Any solution has to preserve this possible redundancy. That may not be the case of the Control System which up to now is not normally implemented redundantly.

An architecture fulfilling this requirement is shown in Figure 6, described as follows:

- Both bay protection units (IED1, IED3) own independently from each other a process communication system with a switch
- Non-redundant bay control unit (IED2) may be connected to both switches for operation in conjunction with IED1 or IED3 by means of possibly GOOSE messages
- Merging units (MU1, MU2) as source of current and/or voltage according to IEC 61850
- Breaker IED (IED4, IED5) representing the breaker controlling device, also the source of commands (trip or close)
- The station bus connectivity may be single or doubled (dashed in Figure 6).

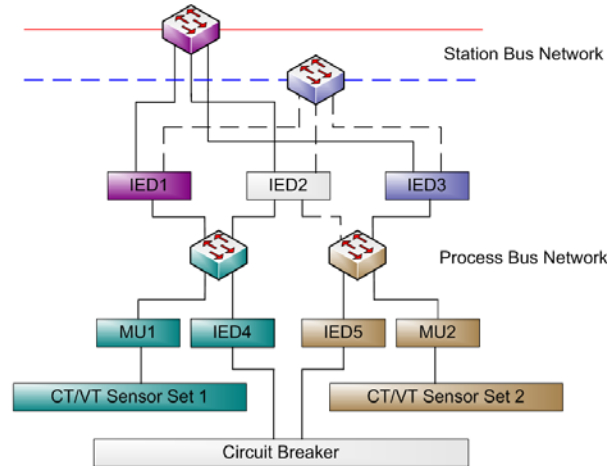


Figure 6 – Station and Process Bus Networks - Redundant Protection

Simplifying the Communication Architecture

According to Figure 6 with the dashed part the redundant station bus and redundant process bus together require 4 switches per bay. By combination of the process bus and the station bus switches, their total number is reduced to 2 per bay (Figure 7). The communication traffic on the process bus like the stream of current and voltage samples will not pollute the complete system since they may be confined locally to one switch using a virtual local network (VLAN) as standard means of the Ethernet technology.

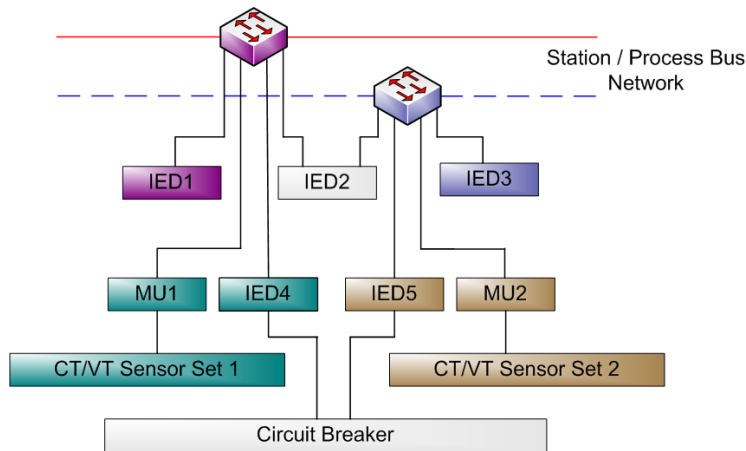


Figure 7 - Redundancy of Process and Station Bus

The combination of both Process Bus and Station Bus networks is conceivable and acceptable due to the further economic benefits it provides. However, the architecture of the network must be chosen such that it renders the highest availability possible.

The following sections will focus on considerations of redundancy in the Ethernet network architecture design, with the objective of ensuring maximum network availability when the same will be used with IEC61850 in mind.

Physical redundancy: More than just the cabling.

Physical redundancy covers the physical Ethernet network connections (and control system equipment) AND the physical hardware the connections go between (the Ethernet Network). Network redundancy focuses upon the multiple routes that can be used between edge devices. The more available routes edge to edge, the more failures the network can sustain and still keep the process alive and functioning. Physical redundancy normally follows two scenarios:

1. Diverse routing of cabling- installing cabling in diverse conduits to prevent the total loss of connectivity if the conduit is damaged
2. Redundant hardware- having multiple connections on a controller or other hardware allows the controller reliable connectivity in cases where a connection or port has suffered a failure. This also involves having redundant network hardware in case of failures, including multiple power supplies, multiple CPU cards on controllers, etc.

When looking at redundancy for the Ethernet network, one need to first look at the application and the area of coverage, including the number of devices that are attaching to the Ethernet network. Answer to the following questions is required”

- Are they grouped according to location and function?
- Application performed?
- Device type?
- Will there be a requirement to connect to the existing Substation Backbone network?

Based on this knowledge you can begin to put together a picture of how the Ethernet network will look like and what the number of ports will be on the Ethernet switches that will be put in those areas. This is needed to determine number of cables, physical routing of the cables, and location of network nodes to connect the cables, and so on.

A popular way to look at system connectivity needs is the Zone/Cell view where you have a Zone of control divided up into functional Cells. Refer to Figure 8:

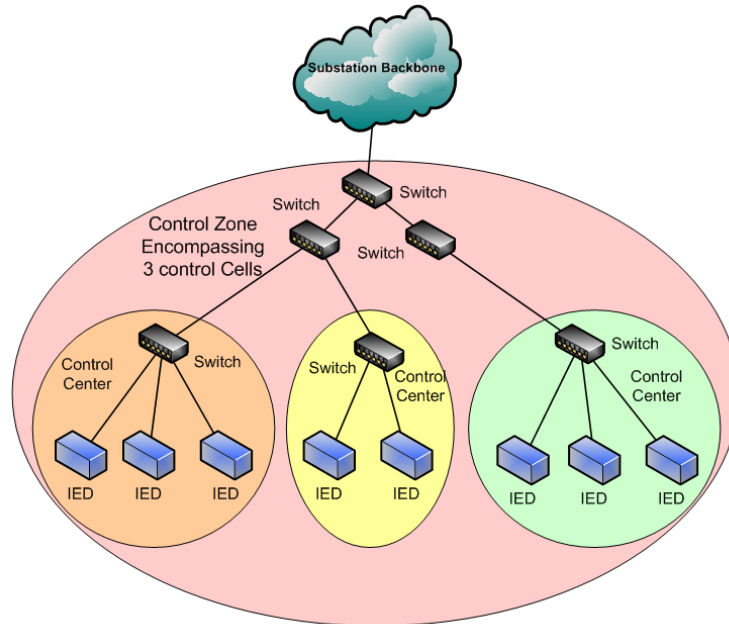


Figure 8 - Control Zone/Cell Reference Diagram

Looking at Figure 8, assuming that each line is a single cable connection, it would be very easy to isolate sections of the process with the loss of just 1 or 2 cables. At the physical layer, it is important to plan out redundant connections to devices that can support multiple connections. Many devices only have one data interface, but the Ethernet switches they connect to have multiple ports to support connections to other switches, forming redundant paths and being able to work around port and cabling failures. In the next sections we will discuss what network protocols are available to make the best use of these redundant paths between network nodes.

Once the connection of devices to the network has been decided, the next decision is the level of redundancy required to achieve maximum system uptime. This implies evaluating the cabling and Ethernet network hardware needs. Then, more questions need to be answered:

- Do we need redundant cabling between devices?
- Is it going to be redundant cable installation?
- Does it require physical segregation of the cabling?
- Is there more than one Ethernet interface on the device to be used (many controllers have multiple Ethernet interfaces in case of Ethernet port or module failure)?

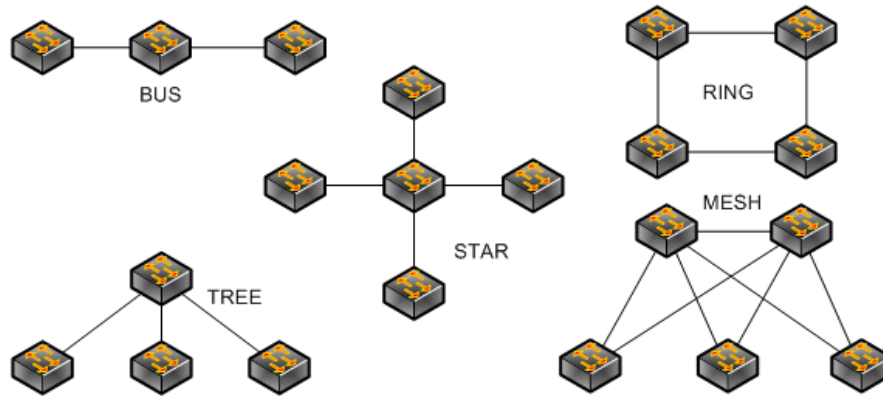


Figure 9 - Ethernet Network Physical Topologies

Data Link Layer Redundancy

Ethernet switches in the network can be used to provide protocol redundancy and maintaining Ethernet network health. Layer 2 Redundancy protocols do two things: Identify all the possible paths amongst the networking devices and place the redundant extra paths in a blocking state to remove network loops. Loops in an Ethernet network cause data duplication and will bring a network to its knees in a short period of time. In the event network segment fails, the protocol activates the appropriate ports that are in a blocking state to reestablish connectivity. The object being to fix the issue before the process even knows there is a problem.

Ethernet networks have redundancy protocols that are supported by identified Ethernet standards. These are supported in Layer 2 and Layer 3 of the OSI model. First we will look at Layer 2:

Standard Layer 2 Network Redundancy Protocols-

1. **Spanning Tree** - There are several flavors of Spanning Tree.
 - a. STP (Spanning Tree Protocol) - Standardized in 1996 as IEEE 802.1D, it is the first and slowest of the Spanning Tree protocols. Average failover time for STP started at 30 seconds and went up. Way too slow for any industrial Process. Next came...
 - b. RSTP (Rapid Spanning Tree Protocol) – Currently standardized as IEEE802.1D 2004, it is an evolutionary leap for STP. It is more rapid, with failover times from about 250msec to up to 12 seconds, so it was better than STP. Still an issue with the speed of failover for Industrial processes.
 - c. MSTP (Multiple Spanning Tree Protocol) - Originally standardized as IEEE 802.1s and then incorporated into IEEE 802.1Q 2003, it allows multiple instances of Spanning Tree Protocol per Virtual LAN. This means that in a single physical network, there can be multiple virtual network groupings, each with their own instance of Spanning Tree Protocol.
 - d. There are proprietary implementations of Spanning Tree that are optimized for use in Industrial Networks. They are based upon standard RSTP, but are not designated as a standard STP protocol.
2. **LACP (Link Aggregation Control Protocol)** - This protocol allows the user to configure multiple Ethernet ports between Ethernet switches into a Single virtual “Link”. This allows load sharing of information between the links and is extremely fast in moving data between a failed port and an adjacent port if there is a link failure.

The amount in interconnections amongst the network elements dictates the amount of failures the network can take and still maintain the process. Refer to Figures 10 and 13 which show examples of these protocols.

Spanning Tree is a redundant topology in that it provides network redundancy instead of just path redundancy while preventing loops in a network. For Ethernet to function properly, only one active path can exist between devices. To provide redundancy, Spanning Tree relies on having multiple paths or connections to different switches and configures some of these paths into standby (Blocked) state. If a network segment becomes unreachable, spanning tree reconfigures and reestablishes link by activating the "Blocked" links.

All switches in the LAN gather information about each other through an exchange of data messages called BPDU's or Bridge Protocol Data Units. The exchange of messages causes the following:

- The election of a "Root" switch for stability.
- The election of a designated switch.
- The removal of loops by placing redundant switch ports in a backup state.

The "Root" switch is considered to be the "logical" center of the Spanning tree network. All paths that are not needed to reach the "Root" switch from anywhere in the network are placed in backup mode. BPDU's contain information about the transmitting switch it came from and its ports including:

- Unique switch Identifier or MAC address.
- Switch priority
- Port priority
- Port cost.

Spanning Tree uses this information to elect the "Root" switch and "Root" port for the switched network.

The switches send configuration BPDU's to configure the spanning tree topology. All switches connected to the LAN receive the transmitted BPDU. The BPDU's are not forwarded by the switch, but the information contained in the BPDU can be used by the receiving switch to transmit a new BPDU.

The resulting action of this communication is:

- One switch is identified as the Root.
- The shortest distance to the root is determined for each switch.
- A designated switch or switch closest to the Root is selected.
- An active port from each switch is selected and the others are blocking.

If all the switches are enabled with default settings, the switch with the lowest MAC address becomes the root by default. However, due to traffic patterns, number of forwarding ports or just simply physical location, this may not be the best way to select the root switch. By increasing the priority (lowering the actual numerical value of the priority number) of the ideal switch so that it becomes the root, you are forcing spanning tree to recalculate and form a new topology. The same can be said for which port is active and which port stays in standby. By increasing the priority (lowering the actual numerical value of the priority number) of the ideal port so that it becomes active, you are forcing spanning tree to recalculate and form a new topology.

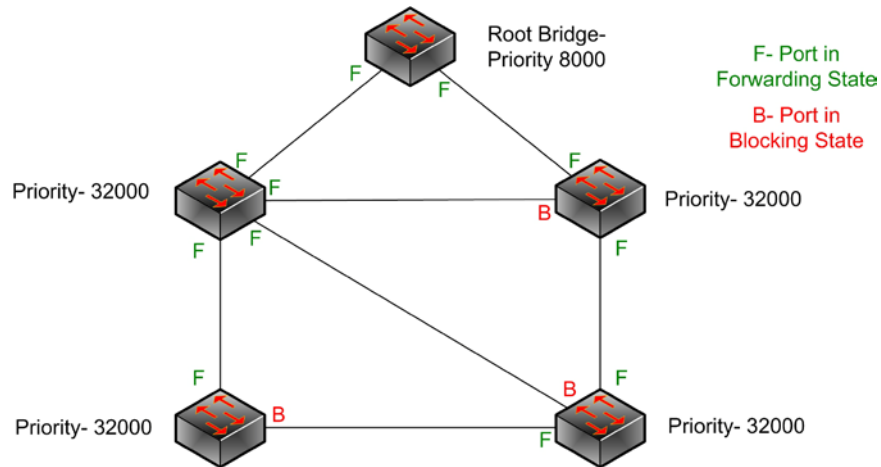


Figure 10 - Example of a Spanning Tree Ethernet Network

Spanning Tree networks can support either ring or mesh topologies. A ring topology is basically a ring of Ethernet Switches connected together in a ring fashion. A mesh topology requires the use of a couple of Ethernet switches at the top with switches below that have connection to both the upper switches. Mesh networks use more fiber than ring networks, but can typically survive more network hits intact. Figure 11 shows a typical Mesh network while Figure 12 shows a Ring network example.

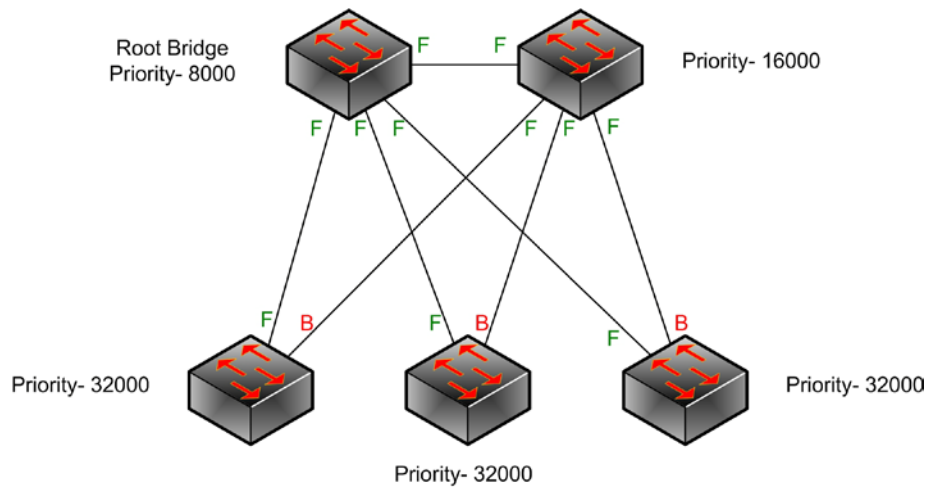


Figure 11 - Spanning Tree in a Mesh Network

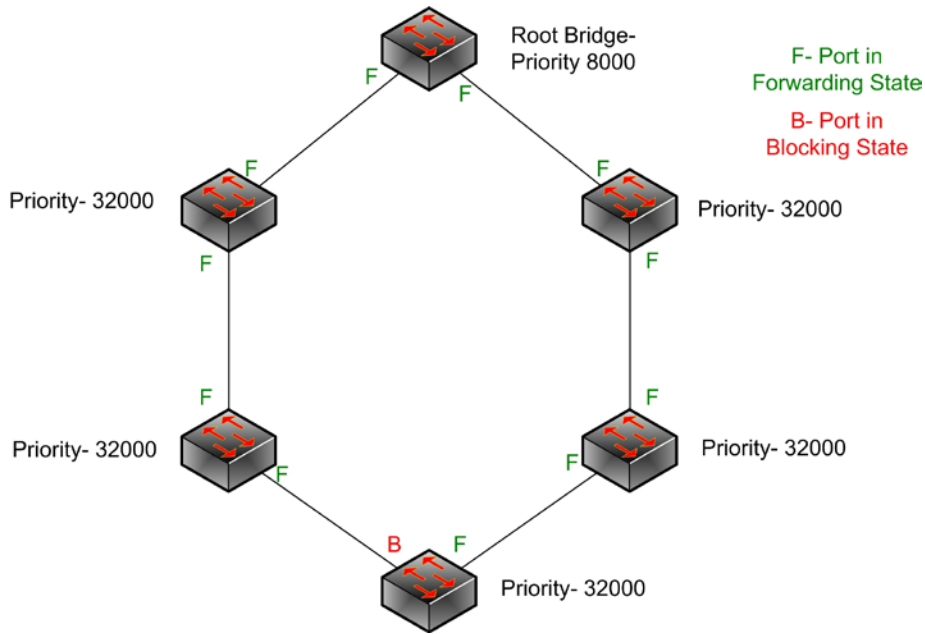


Figure 12 - Spanning Tree in a Ring

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

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

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

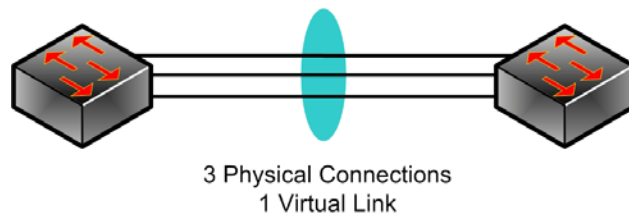


Figure 13 - Example of an LACP based Ethernet connection between switches

Network Layer Redundancy Protocols - How Routers talk to each other and fix breaks.

It is growing more and more apparent that as IEC61850 networks expand, the use of a single IP subnet is not enough. In order to facilitate communication between IP Subnets, you need to use a Layer 3 network device, namely, a router. Routers can provide data movement in 2 ways: Statically via routes that are mapped by hand (Static Routing) or dynamically via designated routing protocols (Dynamic Routing).

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

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

There is also a router physical redundancy protocol. If one router fails, its designated backup is placed into service seamlessly as if the original never left. This is called VRRP, Virtual Router Redundancy Protocol.

Distance Vector vs. Link State Routing protocols

Distance vector

- Sends routing table info only to neighbors, so change communication may need one min/router
- Also called “routing by rumor”
- Easy to configure, but slow
- Does not scale well

Link state

- Floods routing information about itself to all nodes, so changes are known immediately
- Efficient, but complex to configure
- Scales very well in large networks

OSPF and RIP - Standard Router Communications Protocols:

OSPF and RIP protocols are used as ways that routers communication with each other and tell each other what IP Subnets they have attached. By sending these Routing table update to each other the routers build a map of how the network is constructed at Layer 3. This also identifies the redundant ways that these routers can maintain connection to each other if a router loses connection on a port. If a router knows of another way to get to an IP Subnet it needs to send data to, it will use these alternate paths. Figures 14 and 15 show some examples of routing protocols.

OSPF is referred to as a Link-State Routing protocol. The best routes from router to router are based upon the A class of routing algorithms in which each router broadcasts connection information to all other routers on an internetwork. This saves the routers from checking for available routes but adds the memory requirement of storing all the routing information.

This algorithm relies upon the cost of the links between routers, not the number of hops. The cheaper the cost on a connection indicates a higher bandwidth capability. OSPF keeps in memory ALL of the possible routes, not just the active routes.

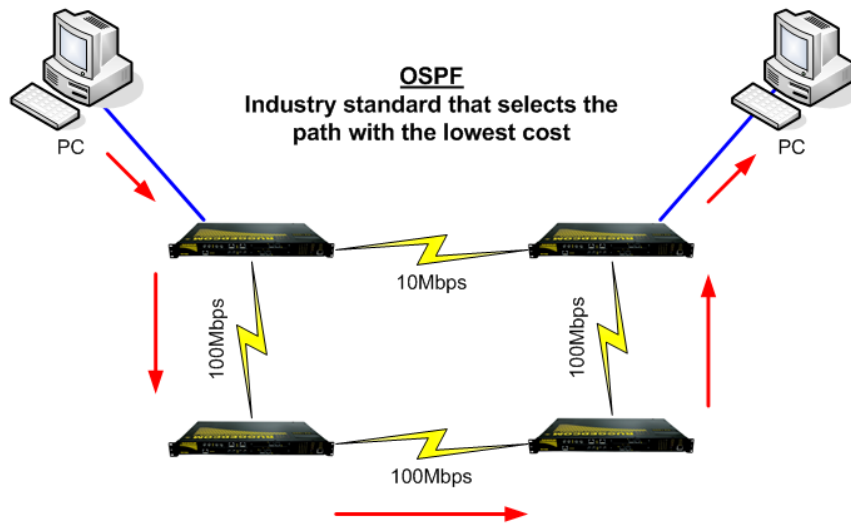


Figure 14 - OSPF Routing Protocol example

RIP and RIP II are types of Distance Vector protocols. Distance vector algorithms compute distances from a node by finding paths to all adjacent nodes and by using the information these nodes have about continuing on the paths adjacent to them, router hop by router hop. Distance vector algorithms can be computationally intensive, a problem that is alleviated somewhat by defining different routing levels. They rely upon the number of hops in a particular direction between the source router and destination router. They do not take into consideration the speed of the physical media, so it is possible to move traffic across a suboptimal link

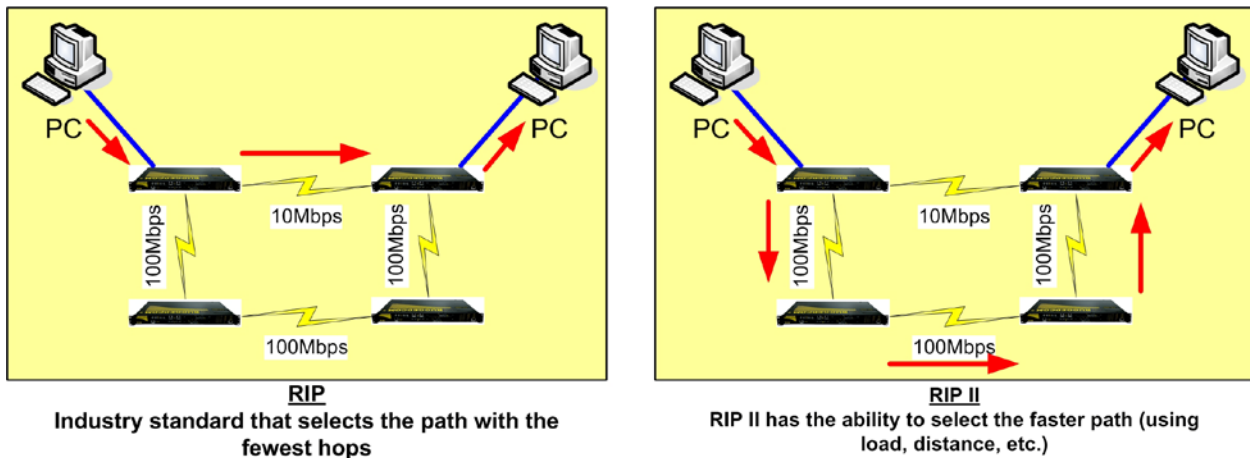


Figure 15 - RIP and RIP 2 routing protocol examples

Router Redundancy

VRRP is the way for routers to perform physical redundancy to each other. If one router dies or is unable to function in the appropriate manner, its designated backup will take over the former routers function. They maintain this relationship through the use of HELLO packets and regular updates to make sure that both routers have all the same

information. The use of VRRP would be a function to incorporate into an IEC61850 design if there is a requirement to attach to a corporate network and there is a requirement to maintain some sort of segregation between the substation IEC61850 network and the corporate environment. Figure 16 shows an example of VRRP.

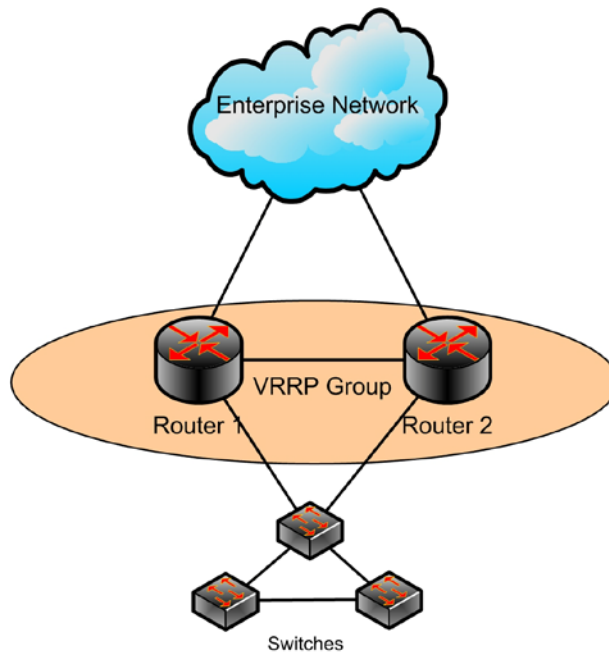


Figure 16 - VRRP Example

Determining the cost of Redundancy: How much is too much?

Designing redundancy into a system is always a balancing act. You must think about how much to incorporate into the various areas, physical, network and application. The first thing that has to be determined is the scope of the system being installed. Here is a list of questions to be answered when designing an IEC61850 design-

1. Is this a new install or and upgrade to a previous installation?
2. Is there any existing cable that can be reused?
3. Is there any existing equipment that can be reused?
4. Has the area of the Installation been determined?
5. Copper or Fiber Optics? This is dependent upon distance and the environment for the installation.
6. Who is the IED system vendor?
7. Will there be a point of connection to the existing network?
8. What sort of data is intended to be passed to this network from the substation IEDs?
9. Will the connection be Layer 2 or Layer 3 based?
10. To what extent has redundancy been considered? Is the network a ring or mesh based network?
11. If Ethernet Network redundancy is not being considered, is it economically feasible to do without it? How many outages are you prepared to pay for in lost revenue? Balance this against the cost of managed vs. unmanaged switches or more advanced Ethernet networking devices like routers.
12. How experienced are the substation support people in supporting Ethernet networking and will the IT staff being involved in the support?
13. What is the projected budget for the control system, including the network cabling and equipment?

Redundancy levels are dependent upon the operation expectation of the IEC61850 system being installed. Substation Automation systems usually incorporate most of the redundancy into the Ethernet network, requiring Ethernet

network devices that are smarter and more expensive but able to heal around network breaks. Based upon years of observations regarding Ethernet networks and the types of devices purchased to make them (namely buying Unmanaged switches instead of Managed), it is very typical to actually see the cost differential between managed and unmanaged Ethernet switches exceeded by the lost revenue of an extended downtime event caused by a network outage. The ability to be able to monitor a network and see the application in action can help predict events that can cause outages. An unmanaged switch is in effect a “blind” switch. It is not possible to see how the network is performing and perform predictive maintenance based upon what you cannot “see”. Also, the ability to use port mirroring on a managed switch can assist with troubleshooting Application level issues as you can use a protocol analyzer to see the IEC61850 application in operation.

Interestingly enough, you can go overboard on redundancy as well. Using too many connections between Ethernet switches can cause slow downs in reconvergence of a network if there is a loss link or switch. Ring topologies typically use 2 interswitch links per switch, mesh topologies can use 3 or more. I normally don't recommend more than 3 for edge switches in a mesh network environment. Too many links between switches can cause the reconvergence around a network outage to take much longer to calculate.

Summary

Understanding the relationships between the physical structure of a network and the protocols that run on the network to provide is key to creating a truly maintainable and adaptable network that deals with issues effectively. It is best to consult with the Ethernet switch vendor that is the basis of the network being installed. Use their experience to help determine how much is needed to make your IEC61850 based control system a success in operation over its lifetime.

Considering the basic communication architectures discussed above, for switches with reasonably high availability the ring is an acceptable and economical, i.e. a suitable solution. The reconfiguration time is a critical issue for safety suggesting that the Ethernet switches shall be chosen with fastest rapid spanning tree protocol also known as eRSTP which it is proven to offer recovery times as low as 5 ms per hop. This is a critical factor when the network will be the carrier of mission critical information such as GOOSE messages between IEDs. A GOOSE message that does not reach the destination on time could imply a blocking signal that did not reach the destination in a timely manner, hence possibly a complete station shot down.

If higher availability is needed, doubled communication networks are recommended, which however need special handling at protocol level to run them in parallel. Having a zero reconfiguration time this solution provides higher safety also, for interlocking as well as for protection related distributed functions.

In HV substations, all bays are protected by redundant protection (Protection A, Protection B). Therefore, the related process bus has to be doubled by definition to avoid a single point of failure. Sharing the process bus switches with station bus connectivity reduces the number of switches and communication ports. As already stated above, for higher availability and safety of the control function, the single controller can be connected to both communication networks.