University of Tennessee at Chattanooga

UTC Scholar

Honors Theses

Student Research, Creative Works, and Publications

12-2018

# An implementation of packet-switched communication for pilot protection at Tennessee Valley Authority

Ha Le Vo

*University of Tennessee at Chattanooga*, fvv257@mocs.utc.edu

# An Implementation of Packet-Switched Communication for Pilot Protection at Tennessee Valley Authority

**Ha Le Vo**

Departmental Honors Thesis
The University of Tennessee at Chattanooga
Department of Electrical Engineering

Examination Date: 11/16/2018

**Gary L. Kobet, M.S., P.E.**
Power System Specialist at TVA
Thesis Director

**Stephen D. Craven, Ph.D., P.E.**
Network Specialist at TVA
Thesis Director

**Ahmed H. Eltom, Ph.D., P.E.**
Department Head and Professor
Department Examiner

**Raga Ahmed, Ph.D.**
Assistant Professor
Department Examiner

# Table of Contents

## Table of Figures

# Table of Tables

# List of Abbreviations

| | |
|---|---|
| ADM | Add-Drop Multiplexer |
| BFD | Bi-directional Forwarding Detection |
| BPSR | Bi-directional Protection Switching Ring |
| CAPEX | Capital Expense |
| CC | Channel Coordination |
| CE | Carrier Ethernet |
| CSN | Circuit-Switched Network |
| CT | Current Transformer |
| DAN | Dually Attached Node |
| DCB | Directional Comparison Blocking |
| DCUB | Directional Comparison Un-Blocking |
| DPU | Digital Protection Unit |
| DTT | Direct Transfer Trip |
| ERPS | Ethernet Ring Protection Switching |
| FDM | Frequency Division Multiplexing |
| FEC | Forwarding Equivalent Class |
| FSK | Frequency Shift Keying |
| IEC | International Electro-Technical Commission |
| IEEE | Institutes of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| ITU | International Telecommunications Union |
| LCD | Line Current Differential |
| LDP | Label Distribution Protocol |
| LER | Label Edge Router |
| LIB | Label Information Base |
| LLC | Logical Link Control |
| LOS | Line-Of-Sight |
| LSP | Label Switch Path |
| LSR | Label Switch Router |
| MAC | Media Access Control |

| | |
|---|---|
| MMF | Multi-Mode Fiber |
| MPLS | Multi-Protocol Label Switching |
| MPLS-TP | Multi-Protocol Label Switching-Transport Profile |
| MW | Microwave |
| NERC | North American Electric Reliability Corporation |
| OPEX | Operating Expense |
| OPGW | Optical Ground Wire |
| OSI | Open Systems Interconnection |
| PLC | Power Line Carrier |
| POTT | Permissive Overreaching Transfer Trip |
| PPP | Point-to-Point Protocol |
| PRP | Parallel Redundancy Protocol |
| PSN | Packet-Switched Network |
| PUTT | Permissive Underreaching Transfer Trip |
| QoS | Quality of Service |
| RedBox | Redundancy Box |
| RSVP-TE | Resource Reservation Protocol-Traffic Engineering |
| SAN | Singly Attached Node |
| SMF | Single-Mode Fiber |
| SONET | Synchronous Optical Network |
| STS | Synchronous Transport Signal |
| TCP | Transmission Control Protocol |
| TDM | Time Division Multiplexing |
| TVA | Tennessee Valley Authority |
| UDP | User Datagram Protocol |
| UPSR | Unidirectional Protection Switching Ring |
| VT | Voltage Transformer |
| WDM | Wave Division Multiplexing |

# ABSTRACT

Teleprotection is a critical element for a reliable power system as it provides high-speed tripping for faults on the protected line and is applied in various pilot protection schemes. Protection schemes cannot perform at their best without a fast and reliable communication system. The long-used legacy technology Synchronous Optical Network (SONET) is becoming obsolete and ready to be replaced by Ethernet-based network communications. The transition from a circuit-switched technology like SONET to a packet-based technology like Multiprotocol Label Switching (MPLS) has caused reservations for protection engineers as they express their concerns for lacking guaranteed 100% availability and potential latency.

This paper will address this issue and the consistent test results from the TVA's lab have proven to satisfy the communication requirements in a teleprotection system. Teleprotection traffic make to its destination and never be dropped, the symmetrical delay is insignificant, and especially the recovery from a failure occurs under 50ms (3 cycles). Future work for Parallel Redundancy Protocol (PRP) implementation is also discussed in the paper in order to achieve a "seamless failover". The results reassure the protection engineers that the Ethernet migration is necessary yet provides a better performance compared to the legacy system.

# 1. INTRODUCTION

## 1.1 The General Network Communications

The utility network has long relied on Time Division Multiplexing (TDM) such as T1 and Synchronous Optical Network (SONET) as the main channel to transmit and receive data in a communication system. These circuit-switched techniques provide intrinsic bandwidth, Quality-of-Service (QoS), and latency guarantees, all requirements for teleprotection circuits. However, TDM technology is aging and its equipment becoming obsolete as vendors transition to Packet-Switched Networks (PSN) to make way for Ethernet-based network communications.

A variety of transport mechanisms available in PSN such as Multiprotocol Label Switching (MPLS), Carrier Ethernet (CE), Ethernet Ring Protection Switching (ERPS), etc. offer many SONET-like features to guarantee a smooth transition; these mechanisms also come with higher bandwidth capacity and better network efficiency compared to SONET.

The modern digital grid of the future or the Smart Grid is the driving key for this change as the demand for a higher capacity, more reliable, and more efficient transport mechanism. Also, requirements for lowering the operating cost, and network capacities of handling any traffic generated by the advanced grid applications are additional drivers for the change to switch over to PSN. A prime example of the needed change is the international standard communication protocol International Electro-Technical Commission (IEC) 61850, which has been globally implemented in substation automation, requires Ethernet capabilities equipment throughout the power system.

## 1.2 The Role of Communication Network in Teleprotection

Electrical faults due to equipment failures or outside disturbances due to weather conditions etc. can occur within the electrical network and could cause voltage collapse and power blackouts. This would affect not only public life but also may have adverse economic consequences. A key element for detecting and isolating the fault is the practice of relay protection.

Distance (or impedance) relaying is widely used to protect the transmission lines. Distance relays receive inputs from current transformers (CT), voltage transformers (VT), and require impedance characteristics of the protected transmission line. Due to errors in CT and VT measurements, as well as in the modeling of line impedance parameters, distance relays can only provide high-speed protection up to about 80% to 90% of the transmission line. The remaining 10% or more is protected with overreaching elements. These overreaching elements must be time-delayed and coordinated. If the resulting time-delayed faults clearing is unacceptable (e.g., to maintain system stability), communication-assisted schemes, also known as pilot relaying or teleprotection, is required. The Institute of Electrical and Electronics Engineers (IEEE) defines a pilot protection scheme is "a protection scheme involving relays at two or more substations that share data or logic status via a communication channel to improve tripping speed and/or coordination [8]."

Teleprotection provides high-speed tripping for faults on the protected line and is applied in various schemes, such as Permissive Overreaching Transfer Trip (POTT), Permissive Underreaching Transfer Trip (PUTT), Directional Comparison Blocking (DCB), and Directional Comparison Unblocking (DCUB). These schemes are used in a variety of ways depending on the communication medium that is available, reliable, and cost-effective.

The dependencies of protection schemes on communications have been proven in various technical papers [2], [3], and [13]. The underlying communication affects various protection schemes. Pilot protection schemes cannot perform at their best without a reliable communication system (Figure 1).

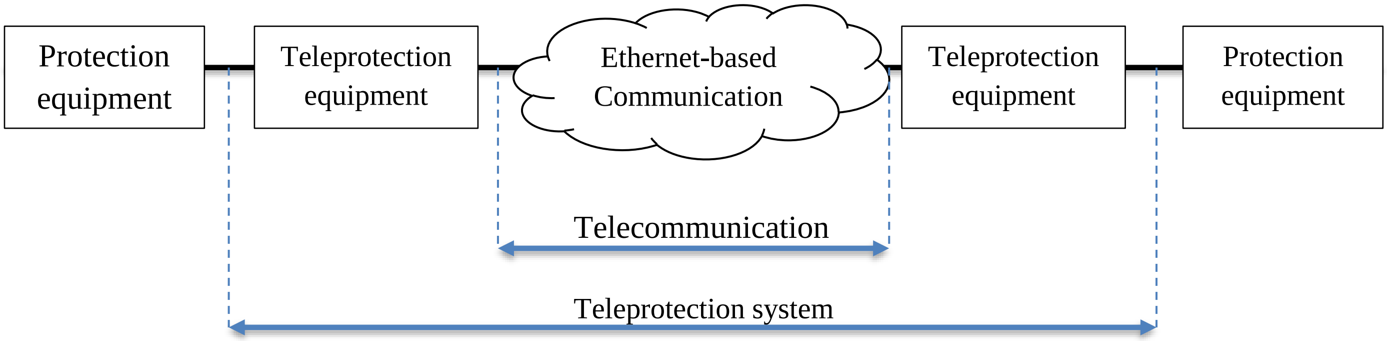


*Figure 1: Communication in Teleprotection*

## 2. TELEPROTECTION SYSTEM AT TVA

### 2.1. TVA Overview

The Tennessee Valley Authority (TVA) was created by Congress in 1933 and is the nation’s largest government-owned power provider. TVA delivers electricity to 154 local power companies, 54 industrial customers and federal facilities to serve 9 million people in parts of seven southeastern states. TVA’s power service territory covers 80,000 square miles, which covers most of Tennessee and parts of Alabama, Georgia, Kentucky, Mississippi, North Carolina, and Virginia.

### 2.2. Pilot Protection Schemes

The protective components (CT, VT…) must be installed properly so that the primary relay detects the first sign of trouble in its assigned protected zone. Should it fail, the backup system must be available to correspond immediately [6]. Additional redundancy is recommended, and even required at some high-voltage locations. As more systems are added for redundancy, the result may be an increase in the probability of incorrect operations, i.e., an increase in dependability results in a decrease in security. A protection system must maintain a balance between dependability, security, sensitivity, and selectivity to satisfy fault-clearing requirements. The IEEE defines dependability is “the facet of reliability that relates to the degree of certainty that a relay or relay system will operate correctly [7]”, security is “that facet of reliability that relates to the degree of certainty that a relay or relay system will not operate incorrectly [7]”. In other words, dependability is trip when expected to trip, and security is not trip when not expected to trip. A relay is said to have sensitivity when it can detect the smallest possible fault current, the smaller the fault current, the more sensitive it is. Selectivity is the ability of a protective relay to precisely locate the exact location of the fault and perform tripping by the closest available relay so that only the minimum portion necessary of the power system is isolated.

All these factors are interrelated. For instance, an increase in speed may reduce security and enhance dependability. Choosing one scheme over another such as DCB over POTT may improve dependability and sensitivity while decreasing speed and security [1]. Further discussion in Section 2 will cover the background and benefits of pilot protection, TVA’s general philosophy as well as schemes selection, and dual pilot protection required for critical substations.

### *2.2.1 Pilot Protection Background*

Pilot protection is protection that uses a communication channel to send information (Figure 1) at a high speed from a local relay terminal to a remote relay terminal [11] to improve fault clearance within various schemes such as underreaching/overreaching transfer trip. Directional comparison blocking schemes send a single bit of data across the communication system at a very high speed [1]. In POTT and PUTT schemes, this single bit tells the remote end if it has the permission to trip (permissive). In DCB and DCUB schemes, this single bit represents a signal to tell the remote end not to trip (block). In the scope of this work, this paper will mainly discuss DCB and POTT schemes.

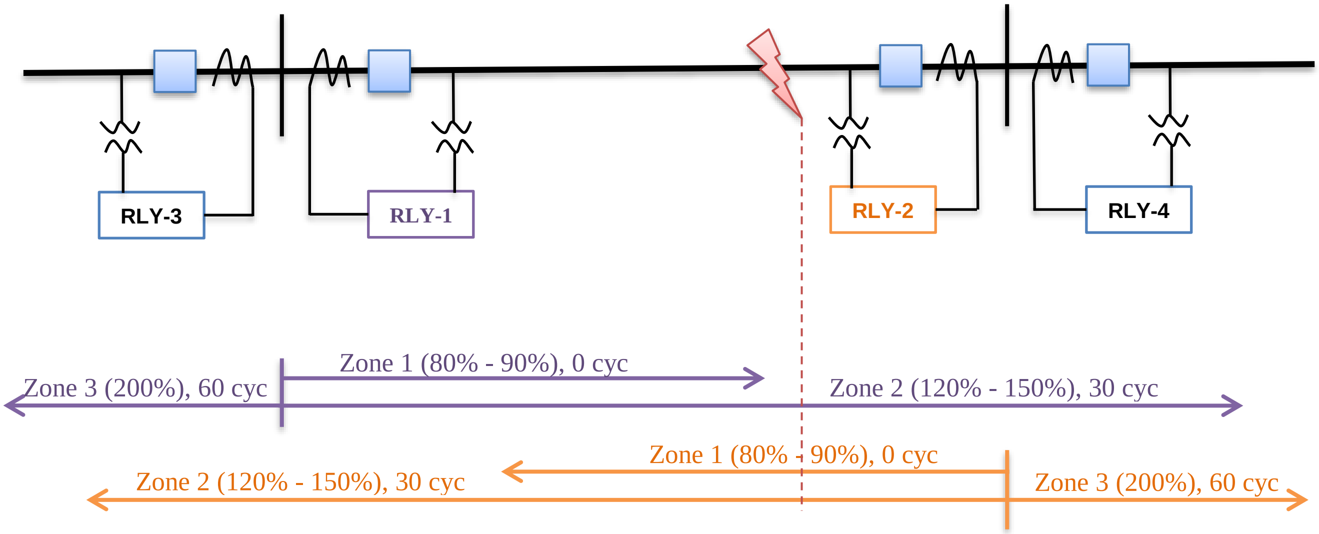

RLY-3
RLY-1
RLY-2
RLY-4
Zone 1 (80% - 90%), 0 cyc
Zone 3 (200%), 60 cyc
Zone 2 (120% - 150%), 30 cyc
Zone 1 (80% - 90%), 0 cyc
Zone 2 (120% - 150%), 30 cyc
Zone 3 (200%), 60 cyc

*Figure 2: Pilot Protection on a Single Line*

The boundary of the protection zone is defined by the location of the current transformer [6]. In a typical transmission line protection scheme (Figure 2), each relay terminal has a forward-underreaching element (Zone 1) that covers from 80-90% of the line, a forward-overreaching element (Zone 2) which covers from 120-150% of the line, and a reverse-looking element (Zone 3) that can cover up to 200% of the line. Zone 4 and 5 are optional and can be set either forward or reverse looking. Note that in both POTT and DCB schemes, Zone 1 provides instantaneous tripping independent of the pilot scheme logic.

In a POTT scheme, if both relay terminals (RLY-1 and RLY-2) see the fault in the forward direction, the fault is internal to the protected line. In Figure 2, Relay 2 trips instantaneously because the fault is in its Zone 1 of protection. The fault is in the forward direction hence Relay 2 sends a tripping permission to Relay 1. Not only Relay 1 sees the fault is internal (Zone 2 element) to the line but also receives a permissive signal from Relay 1, therefore Relay 1 trips with no delay. Figure 3 shows the tripping logic for POTT scheme. In order for a relay to send a tripping signal, it has to see the fault in its forward direction and receive the tripping permission from the remote terminal.

In DCB scheme, the relay does not send a blocking signal to the other terminal when a fault is in a forward direction. The zero signal (not receiving any blocking signal) will invert to one, AND'ing with one signal from seeing Zone 2 fault to produce a tripping output in Figure 4. The Channel Coordination (CC) delay box in Figure 4 allows time for the blocking signal to be received. If the signal is late or lost, a DCB scheme may over trip. The relay sends a tripping signal to the remote terminal when it sees a fault in a reverse direction, indicates that the fault is outside of the protected zone. The DCB logic receives one signal from the Zone 2 relay, and one signal from the remote terminal (the "blocking" signal) which is inverted. A Zone 2 signal with no remote blocking signal received will produce a tripping output.

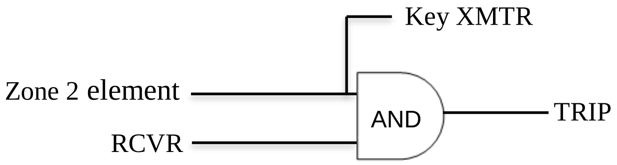


*Figure 3: POTT Logic*

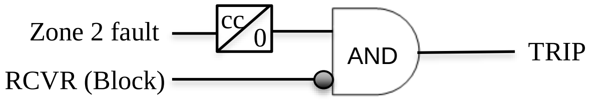


*Figure 4: DCB Logic*

When a fault occurs on the transmission line and the communication channel fails to operate, the relay in a DCB scheme will trip regardless. Thus, DCB scheme favors dependability. On the other hand, the relay in a POTT scheme has to receive a tripping permission, otherwise, the relay will fail to trip fast (30 cycles time delay or more). Hence, POTT scheme favors security.

Line Current Differential (LCD) is another pilot scheme. Despite not having zones of protection, it provides high-speed clearing of fault by covering 100% of the transmission lines. While distance relay uses the line impedance to detect faults, the LCD is only interested in the current level of the protected transmission line [19]. The currents on three phases of the transmission line are constantly monitored between two transmission line terminals, the current flowing into the line should be the same as the current flowing out of the same line unless there is a fault in the system. There are different methods can be used to measure: magnitude comparison, phase comparison, or phasor (both magnitude and angle) comparison. A current differential relay is simple to set compared to a distance relay [19], due to its simplicity, it is the preference on the TVA's transmission lines when tap stations are highly unlikely [11].

Although Direct Transfer Trip (DTT) is not a pilot scheme, it utilizes a pilot channel to exchange communication with other remote relays. The DTT scheme is used at some substations to provide remote primary protection for power equipment and mostly used for remote backup protection. DTT scheme is widely used at TVA as a breaker failure protection in conjunction with other protection schemes.

### *2.2.2. Benefits of Pilot Protection Schemes*

Pilot protection plays a crucial role in a power system as it provides tripping with no intentional delay, isolates the faulted area, and protects the power equipment. There are benefits to clearing faults at high-speed as it decreases the fault damage, improves the system stability, and decreases the effect of nearby generation and load [14]. In Figure 2, if there is only distance (line) relay used to protect the line, Relay 2- Zone1 trips its breaker immediately with no delay. However, the fault is out of Relay 1-Zone 1 protection but is seen in its Zone 2. Consequently, Relay 2 has to wait for 30 cycles to initial the tripping signal. Although 30 cycles is only 500ms (on a 60Hz system) and only half a second, this is relatively long for a power system and can result in severe damage to power apparatus or system instability. With a pilot scheme, the total tripping time for Relay 1 should be less than 3 cycles (50ms) for both relay time + breaker time, that is 27 cycles less than without pilot scheme.

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) – 014 states the importance in protecting transmission substations and its associated control centers "…rendered inoperable or damaged could result in widespread instability, uncontrolled separation… [10]." All pilot schemes provide some benefits to the system, but to maintain the balance of the four characteristics of a power system mentioned in Section 2, the two most commonly used are POTT and DCB schemes.

### *2.2.3. TVA's General Philosophy*

TVA's goal is to have pilot schemes installed on all transmission lines above 100kV as this has to be done in a cost-effective manner. For generic substations below 100kV, no pilot scheme is required, though protection engineers will use their best judgment and may add a pilot scheme to address special circumstances.  A single pilot scheme is installed for lines above 100kV while dual pilot schemes are deployed for 300kV and above [11].

From TVA's technical standard [11], some 161kV lines with a single pilot scheme can operate for a brief period of time without a pilot, 161kV lines with dual pilot schemes can operate indefinitely with only one pilot, and some critical 161kV lines are not to remain in service with no pilot scheme. All 500kV lines are considered critical, must have two pilot schemes. It is acceptable to operate 500kV lines indefinitely with only one pilot but is not to remain in service with no pilot scheme.

### *2.2.4. Pilot Schemes Selection*

Reliability of a power system is defined in terms of security and dependability. The ultimate goal for every system installation is a 100% security and 100% dependability. However, this is not obtainable since an enhancement in dependability causes a decrease in security. As explained how POTT and DCB schemes operate in Section 2.2.1 and how choosing one scheme over another may offer certain benefits, Table 1 lists different scenarios for POTT and DCB schemes.

*Table 1: Tripping Comparison Between POTT and DCB Scheme*

| Communication Path | Event | POTT Scheme | DCB Scheme |
|---|---|---|---|
| Active | In-zone fault | Trip | Trip |
| Active | Out-zone fault | No trip | No Trip |
| Inactive (loss) | In-zone fault | Fail-to-trip fast | Trip |
| Inactive (loss) | Out-zone fault | No trip | Misoperate |

Table 1 indicates POTT scheme leans more toward being secure (not trip when not expected to trip), while DCB scheme leans more toward being dependable (trip when expected to trip). The choice of a proper protection scheme depends on the existing scheme and the available communication equipment. The TVA Relay Misoperation team has preferred DCB scheme installed where high-speed clearing is required for technical reasons [11].

### 2.2.5. Single Pilot and Dual Pilot Protection

A single pilot scheme is commonly found on 161kV and below installations where the pilot scheme is typically installed on the first set of line relays while the second set of relays is non-pilot step distance. A single pilot scheme only requires one teleprotection terminal and a single communication circuit at each location (Figure 5) [12]. When a Zone 1 fault occurs on the transmission line, both relays at each terminal will independently and simultaneously send a trip signal to the breaker. The trip signal that gets to the breaker first will trip the breaker. When a Zone 2 fault occurs on the transmission line, the "A" set relay at each terminal will send a trip signal to trip the break instantaneously. The "B" set relay at each terminal will wait for 30 cycles before sending a trip signal, by that time the fault has been identified and cleared. There is no work needed for relay 'B' set.

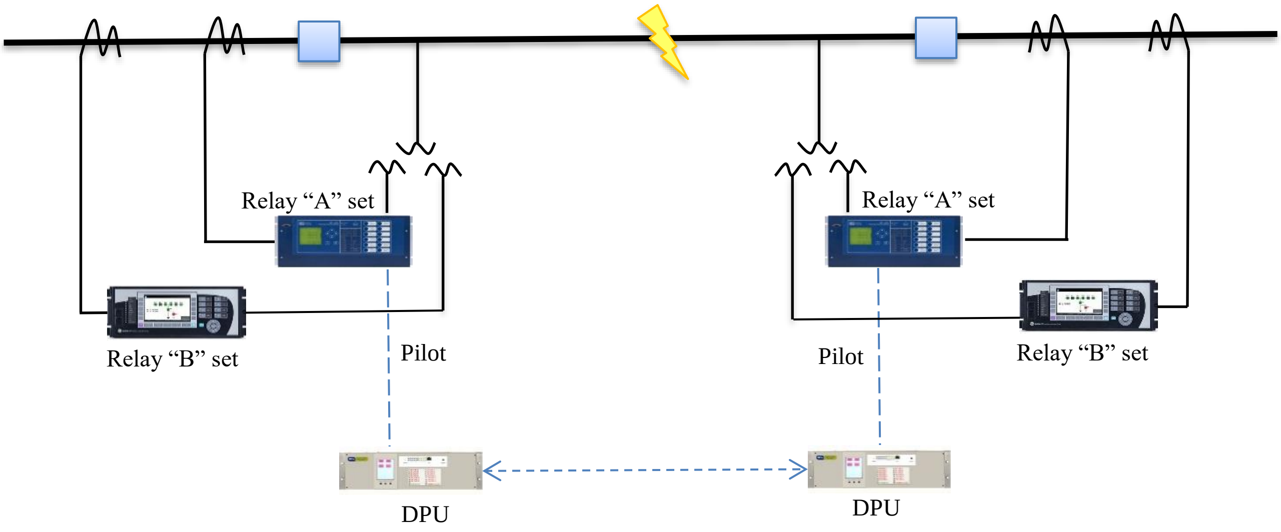


*Figure 5: Single Pilot Protection Scheme at TVA*

Dual pilot schemes are usually found on 230kV and above installations where reliable and redundant high-speed fault clearing are required. These installations require two separate teleprotection units and two communication circuits at each location, routed between the end locations (Figure 6) [12]. A teleprotection device called a Digital Protection Unit (DPU) is a user programmable interface that is used for teleprotection carrying communication. In addition, a DPU can support three teleprotection functions. At TVA, it is recommended to have a single protection relay installed on one DPU and two DPUs in dual protection schemes. The reason behind this is to avoid a single-node failure where a failed DPU will not terminate both relays.  For a Zone 1 and Zone 2 faults, both relays "A" and "B" set at each terminal will independently and with no intentional delay send the tripping signals to the remote breakers.

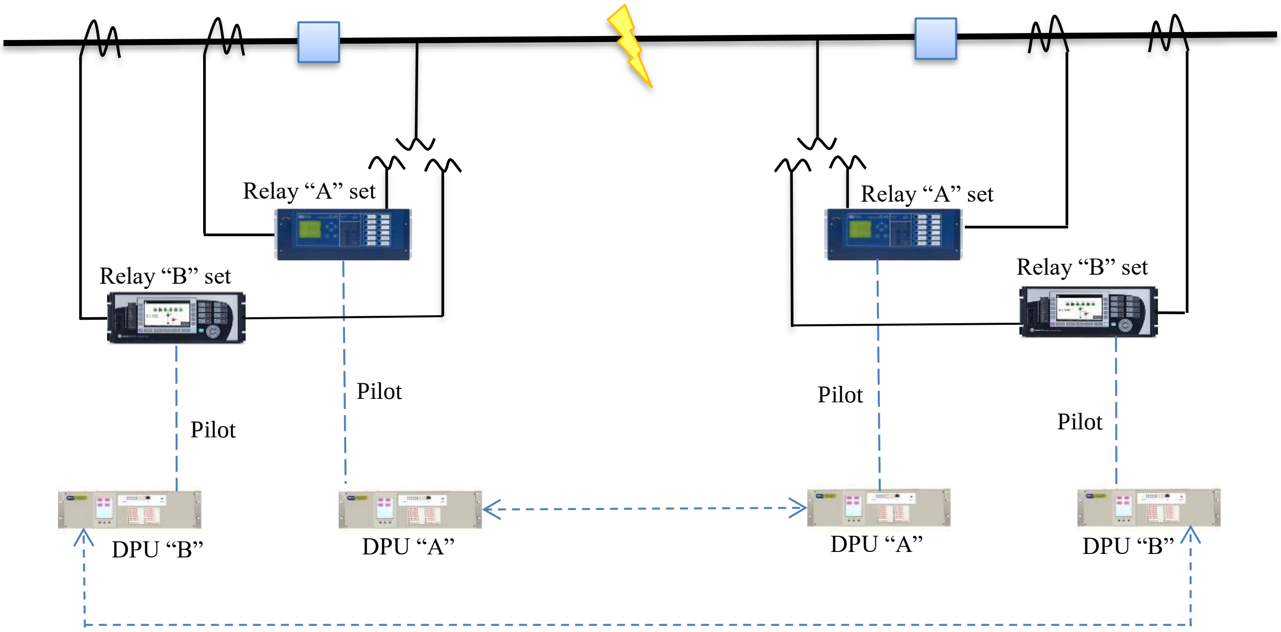


*Figure 6: Dual Pilot Protection Scheme at TVA*

In many cases, DTT is used for remote backup for breaker failure. In some cases, DTT is used in conjunction with either single or dual pilot schemes to provide extra protection. Though dual DCB scheme is preferred as discussed before, POTT/DCB is acceptable but should be avoided if possible since DCB carries the risk of tripping for an out-zone fault when a failure in a channel occurs (Table 1). Dual POTT scheme should be avoided since a channel failure would result in no tripping for both schemes. Figure 6 shows a dual protection at TVA, a separate CT is fed in each Relay “A” set and “B” set, and each relay has its own Digital Protection Unit (DPU). A relay is not able to communicate with other relays but through DPU. All DPUs in TVA’s system use T1s over SONET or Microwave to exchange communications.

### 2.3. Pilot Channels for Teleprotection

A communication medium is a path between two relay terminals in which data can be exchanged between them over the medium. The path can be either fiber, microwave, Power Line Carrier (PLC), leased line or pilot wire. As the communication paths/equipment must be reliable and provide adequate on-demand availability with a special latency requirement, the choice of a communication network is critical as it must present a minimum delay.

Protection schemes, especially on a high-voltage transmission line would hardly perform at their best without the use of a communication channel. A communication channel is an integral part of a pilot protection system. It is used to protect the transmission line, to deliver information from one terminal to another in a timely manner so the fault location can be determined, and a decision can be made to execute the presence of an internal fault. Further discussion in this section will cover TVA’s communication medium such as telephone circuits, PLC, Analog/Digital Microwave, and Fiber Optics Network (Figure 7).

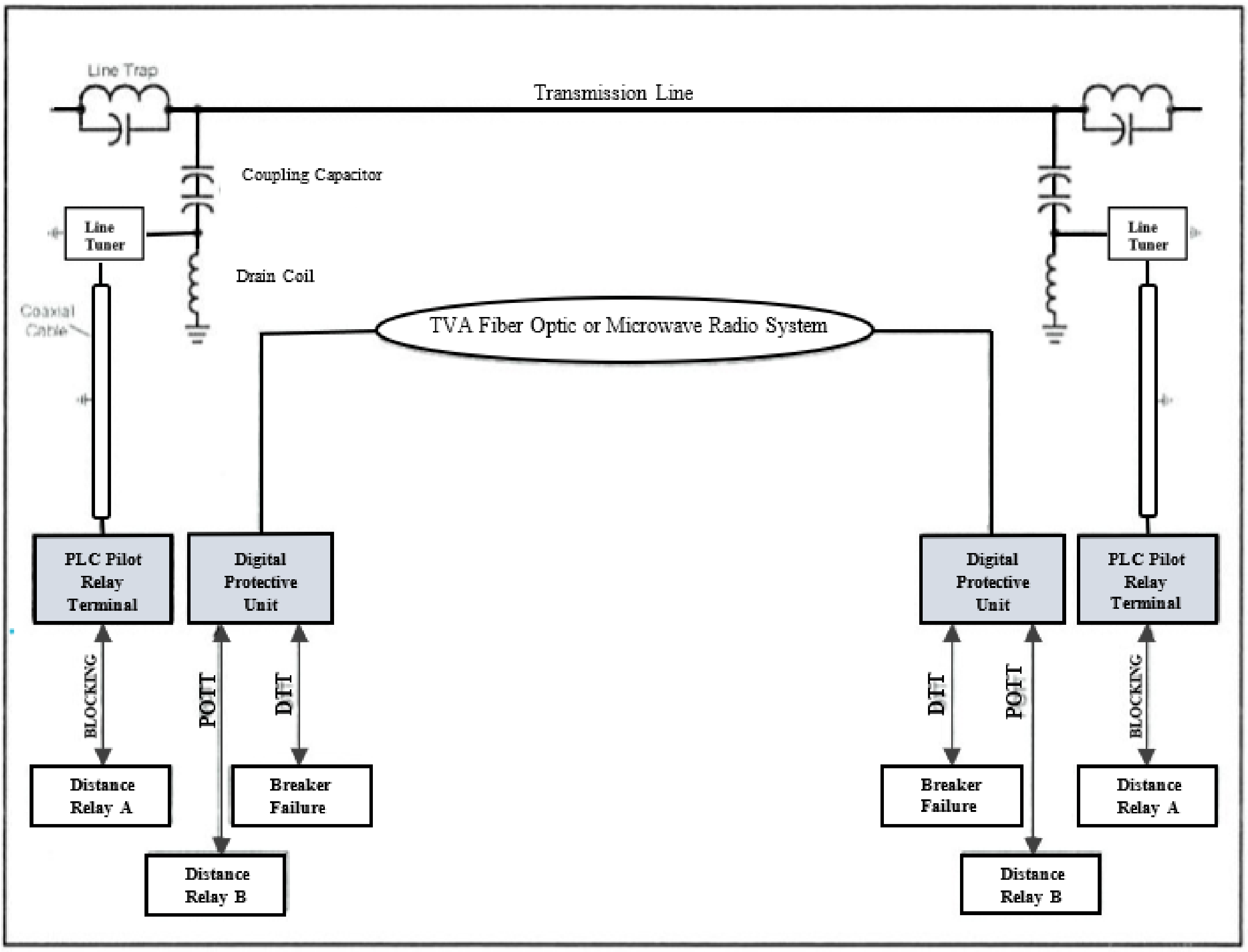


*Figure 7: Pilot Channels (PLC, MW, and Fiber) at TVA*

### 2.3.1 TVA's General Philosophy

The general philosophy at TVA is to own and maintain the communication path for pilot protection and for all TVA's teleprotection applications. The preferred transport mediums are TVA-owned fiber optics and digital microwave radio. Should these not be available for any reason, the next preferred is Power Line Carrier (PLC) and leased circuit is the last resort. Choosing a reliable communication is an important step, as a failure of these not only result in extensive equipment damage but often it is required to send misoperation reports to NERC and Southeast Electric Reliability Council (SERC) [11].

### *2.3.2. Dedicated Leased Telephone Circuits*

A telephone circuit is a dedicated path between two or more locations set up by a telecommunication carrier at a fixed monthly rate. A dedicated leased line means the bandwidth of the path is solely reserved for the subscriber. A leased line requires no capital investment and very little maintenance. However, it is considered among the least reliable communication path as it relies on the phone company for maintenance. Leased telephone circuits were used in the past but will not be used for any future installations at TVA [11].

### *2.3.3. Power Line Carrier*

PLC is the third choice of options and is reserved for use only when no digital path (TVA-owned fiber and microwave system) are not available [12]. PLC is not limited by distance, but the equipment and installation costs are appreciable. A PLC system (Figure 7) includes line traps, coupling capacitors, and line tuning units (tuners). A line trap (wave trap) is used to reduce corona losses, filters the unwanted signals, traps high-frequency communication signal sent over the power line path, and allows a 60Hz power frequency current to pass to the destination. The coupling capacitor permits the carrier frequency to pass through. The line tuner and coupling capacitor are usually located close in the switchyard to form a high-pass filter.

Noise is the biggest factor in determining the success of a PLC system. Noise is generated by corona, lightning, and other communication channels. The signal-to-noise ratio must be set above a certain level to ensure the distinction between signal and noise. An increase in the bandwidth of the receiver means the more susceptible it is to noise.

As Figure 7 shows, a single PLC can only support one pilot relay in a two-way direction. There are two modes of PLC used for teleprotection: ON-OFF frequency is used in DCB scheme, Frequency Shift Keying (FSK) is used in DCUB and DTT scheme [12]. The preference is to still use DCB over other pilot schemes. Although a POTT scheme can operate on a PLC system, it is highly risky and should be avoided. Moreover, PLC equipment usually installed on B phase on TVA's transmission line, if the B phase is in a faulted condition, the tripping permission for an internal fault sent from one terminal may not get to another remote terminal. As a result, the remote breaker will not operate.

Power Line Carrier was the main communication channel in the past for TVA substations. Nevertheless, the equipment, installation, and maintenance cost are expensive but not very effective, and it is less reliable compared to digital paths. Moving forward, TVA prefers to have the power line carrier converted to fiber or digital microwave at the first feasible opportunity [11].

### *2.3.4. Analog/Digital Microwave*

A digital microwave radio is a point-to-point transmission that uses a beam of radio wave to provide a wireless communication in the microwave frequency range to transmit data between two locations. An analog microwave radio is an older technology and has been rapidly being replaced by digital since digitizing signal improves network transmission and capacity. A digital microwave is flexible, and the communication distance can range from a few miles to very long distances (up to 50 miles).

A digital microwave is a line-of-sight (LOS) medium, usually built for transmitting digital signals such as voice and data and capable of transmitting for about 20-50 miles depending on the terrains. The LOS cannot travel along the earth's curvature; when the distance exceeds the limit, a repeater may be introduced [15]. Therefore, path calculation is the first step in the design process.

Physical elements like trees, mountains, or buildings can add losses by refracting the transmitted microwave signal.

A microwave system comprises four basic components: a transmitter, a receiver, transmission lines, and parabolic antennas. A transmitter transmits the signal from the end-user, a receiver receives and modulates the information received from the transmitter into a microwave frequency, a transmission line is a medium to confine the signal into a specific direction, and a parabolic antenna is to radiate the microwave energy.

All pilot schemes can be deployed using microwave radio; the preference still is DCB scheme for substation's teleprotection at TVA [11]. TVA's microwave system is an alternative transport medium where the deployment of fiber optics is not a cost-effective solution. Besides, TVA must apply licensed radios for frequencies, as licensed microwave frequencies are less prone to interference due to overloaded radio frequency bands [15].

A microwave system has many benefits compared to PLC system and fiber network. Since it is a LOS medium, it travels a little faster than fiber (the refractive index of glass is higher than air). Moreover, it is more affordable than fiber, has higher bandwidth and is more reliable than power line carrier. On the contrary, a microwave system can significantly be affected by adverse weather. For instance, wind can cause the antenna system to move out of alignment and rain or snow can add attenuation to the signal path.

### *2.3.5. Fiber Optics, Optical Ground Wire*

Shield wires or Optical Ground Wires (OPGW) are types of cables that are used in the overhead power lines for transmitting voice, high-speed data and teleprotection signals. Such cables serve dual functions: replace the traditional overhead ground wires with optical fibers that can also be used for telecommunications purposes [16]. An OPGW cable contains a tubular structure, the number of the optical fibers inside the cable can range from 12 to 144 fibers and is surrounded by layers of steel and aluminum wires.

Optical fibers are placed inside a central stainless-steel or aluminum tube. The tube is then armored by layers of aluminum strands to provide additional conductivity or layers of steel strands to provide tensile strength. A waterproof splice box is used for fibers to join between lengths, and repeater sites are installed when the distance between two locations is too great for optical loss to handle [18].

Single-Mode Fiber (SMF) has a small diameter core that allows only one light beam to propagate, thus the light reflections in the core are low creates the ability for the transmitting signal to travel a far distance. SMF is required for most applications at TVA [18].

Multi-Mode Fiber (MMF) has a large diameter that allows multiple light beams to propagate, thus the light reflection in the core is high which reduces the quality of the transmitting signal over a long distance. MMF is used for TVA's substation and switchyard applications where communication is only over short distances [18].

The Optical Ground Wire must be designed to withstand the mechanical stresses applied on the overhead line by the external factors such as wind, rain etc. and to handle electrical faults on the line by providing a path to the ground without damaging the sensitive and delicate optical fiber in the cable [16]. OPGW offers many advantages over the buried optical fiber cable. Including the installation cost for OPGW per mile is cheaper, an overhead fiber cable is unlikely to be damaged by groundworks such as road or pipelines reparations.

OPGW is the most reliable communication path and is the first choice when designing for teleprotection at TVA. As a result, fiber optics is considered using at greenfield sites if feasible and budget allowed. Fiber optics can work well with all pilot protection schemes, but the preferred approach is DCB as explained in Section 2.2.4 above. OPGW offers higher bandwidth than microwave and PLC system and demands little maintenance. It can travel up to 50 miles before needing support from a repeater. The downsides of this communication channel are the high cost in installation, requiring additional planning, and difficulties in repairing fiber damage.

In 2017, the TVA Board of Directors approved a $300 million strategic fiber that will expand TVA's fiber network to improve the reliability of the transmission system as well as accommodate the new energy resources. The fiber initiative will take five to 10 years to complete and will include 3,500 miles of fiber [9].

Below is the comparison of the four mediums at TVA ranging from the lowest to the highest preference (Table 2).

*Table 2: Communication Mediums Comparison*

| **Communication Medium** | **Reliability** | **Bandwidth** | **Equipment Costs** | **Installation Costs** | **Maintenance** |
|---|---|---|---|---|---|
| 4. Dedicated Telephone Lines | Low | Low | Low | Medium | Low |
| 3. Power Line Carrier | Medium | Low | High | High | Medium |
| 2. Microwave | Medium | Medium | High | Medium | Medium |
| 1. Fiber Optics | High | High | Low | High | Low |

# 3. TELECOMMUNICATIONS SYSTEM OVERVIEW

## 3.1. Migration Challenges

Protection engineers have expressed reservations due to the perceived lack of guaranteed 100% availability and potential latency. Some have been reluctant to the idea of migrating to IP networks without a proper SONET-like mechanism to ensure a level of reliability to secure mission-critical applications such as teleprotection.

The near future of smart grid implementations using packet-based technology demands high availability and reliable services to ensure low end-to-end delay. In addition, the demand for a high-speed and minimal delay for teleprotection translates to a very low symmetrical delay and jitter in the network - both of which are not inherent in packet technology's behavior. Nevertheless, the Ethernet technology nowadays has various mechanisms to overcome such impairments [20] and to ensure a smooth transition to the new technology with a performance the same or better than the legacy system.

The economic challenge from a utility perspective is to minimize the Capital Expense (CapEx) and Operating Expense (OpEx) cost when transitioning to a new technology especially when involving the co-existence of SONET and the new network generation.

## 3.2. Telecommunications System Overview

### *3.2.1. Communications Network Background*

Telecommunication is the exchange of information over a long distance. Teleprotection signals for protective relays are considered to be the most critical data across the utility network as they are used to assist protective relays in detecting and clearing faults on transmission lines. Hence, teleprotection traffic must be ensured immediate delivery (i.e., less than one power system cycle or 17ms) as soon as the problem is detected so that the fault can be isolated from the system.

Protection relays require a communication channel to exchange communication between the local and remote relays. For a POTT scheme, communications channel delay simply delays the trip output and a loss of communication disables the scheme, requiring some forms of backup protection to affect the tripping [26]. Hence, a POTT scheme depends on the communications channel for tripping internal faults. Whereas a DCB scheme depends on the communications channel only to send blocking trips for external faults. The Coordinating time delay in Figure 4 must be set to be greater than the maximum expected channel communications delay [26] to prevent the scheme from tripping for external faults. If the communications channel is lost (Table 1), the DCB scheme may misoperate for faults outside of the protection zone. Therefore, the communications channel plays a crucial role in both protection schemes when evaluating a system in terms of speed, security, and dependability.

The traditional relay-to-relay communication has been via dedicated paths/equipment, packet switched communication implements some form of path sharing in an attempt to make optimal use of the path. At TVA, teleprotection is widely used over SONET, which is a standardized digital communication protocol that is used to transmit a large volume of data over a relatively long-distance using fiber as the main medium. SONET technology has been around for many decades and provides efficient services for telecommunication systems and therefore is widely adopted. A SONET network is comprised of mixed mediums including fiber and microwave. However, the technology is aging, its equipment is becoming obsolete and no new applications are being developed for SONET. The challenge in moving from a legacy deterministic SONET to non-deterministic packet-based networks is to guarantee the performance of well-established SONET network to a new Ethernet-based technology.

For a device to pass data to another in the network requires a path between the source and the destination. When there are many devices in the network, it is necessary to develop a mechanism for communication between each device. One alternative is a dedicated one-to-one connection and forms a mesh topology, but it soon becomes impractical and expensive especially in a big network where there are many devices (Figure 8). A better alternative is a one-to-many connection and forms a switched network where each device is a part of the connection between the source and the destination (Figure 9). The two common switching mechanisms are circuit-switching and packet-switching.

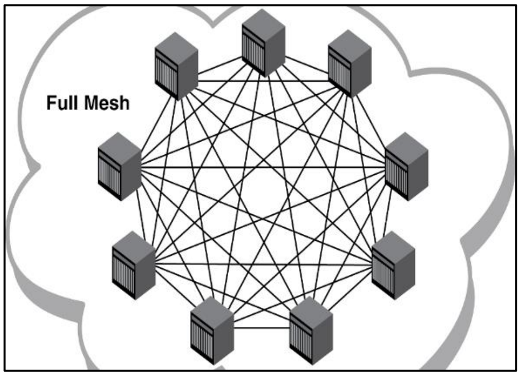


*Figure 8: A Mesh Topology*

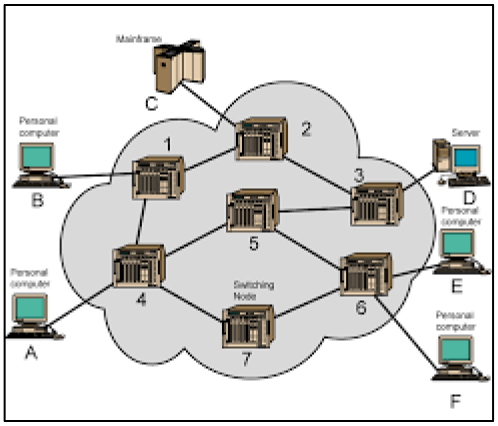
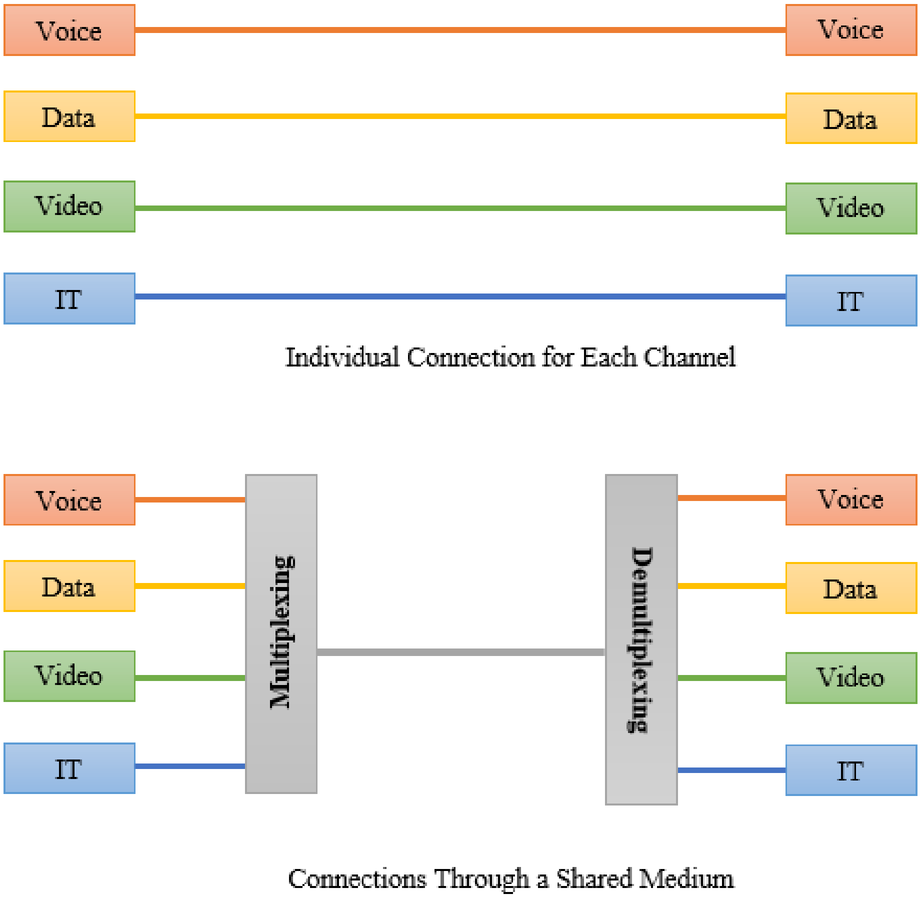


*Figure 9: A Switched Network*

### 3.2.3. Circuit-Switching Network

The capacity of the transmission system is determined by its bandwidth, which is measured in Hertz for an analog system and bits/second for a digital system [5]. In terms of the Open System Interconnection (OSI) model, multiplexing happens at the Physical Layer where the sharing of transmission systems through several connections take place. Multiplexing is desirable when each individual bandwidth of the input signals is smaller than the available bandwidth of the system. That is, a multiplexer can simultaneously carry multiple input signals over a single transmission line when the system has sufficient bandwidth to carry multiple connections (Figure 10). This approach maximizes the use of available bandwidth in the system as the number of users increases.



Individual Connection for Each Channel

Connections Through a Shared Medium

*Figure 10: Multiplexing Through a Shared Transmission Medium*

There are several multiplexing techniques in a circuit-switched network:

1. Frequency Division Multiplexing (FDM) is to transmit the signal by dividing the individual connection into frequency slots.

2. Time Division Multiplexing (TDM) is to transmit signals by dividing the time frame into slots — one slot for each message signal.

3. Wavelength Division Multiplexing (WDM) is used in fiber transmission system where it combines multiple light sources into one at the multiplexer and converts a single light into the original multiple light sources at the demultiplexer.

Circuit-switched networks (CSN) provide a dedicated communication path that enables the flow of information between the two locations [5]. The establishment of the path takes place before the actual transmitting occurs, a characteristic called connection-oriented. An example of a CSN is the telephone network. The data is sent in the network as a stream of bits. The CSN guarantees the Quality of Service (QoS) where the data is sent in a pre-determined path and is transmitted at a fixed rate. However, circuit-switching technology reserves bandwidth for the circuit even when there is no data to transmit to guarantee the deterministic behavior of the architecture.

### *3.2.4. Packet-Switching Network*

Packet-switch networks (PSN) transfer blocks of information that are divided into a sequence of packets. Each packet contains a header (with source and destination address) along with a packet number and is forwarded based on the address in the header. There are two fundamental approaches to transfer packets across the network: datagram and virtual-circuit.

Datagram packet-switching is where the packets are routed independently from node to node until it reaches the destination in the network without required setting up connection path. Each packet has a header that contains enough information to route the packet to its destination [5]. This approach is also called connectionless packet-switching.

Virtual-circuit packet-switching involves setting up a connection path (virtual circuit) across the network from a source to a destination prior to the transfer of packets. This approach is also called connection-oriented packet-switching. While the circuits in circuit-switching networks reside at the Physical layer (Layer 1) as data is sent in a stream of Bits, the circuits in packet-switching networks reside at the Network layer (Layer 3) as data is sent in a stream of Packets (Table 4).

There is no need to reserve bandwidth in packet-switching unlike in circuit-switching. If there are no messages to be transmitted, the resources are available to carry information from another source. This characteristic is known as statistical multiplexing. Below in Table 3 is the comparison between circuit-switching and packet-switching.

*Table 3: Comparison Between Each Switching Technique*

| Circuit-Switching | Datagram Packet Switching | Virtual-Circuit Packet Switching |
|---|---|---|
| Dedicated path | No dedicated path | No dedicated path |
| Connection-oriented (Layer 1) | Connectionless | Connection-oriented (Layer 3) |
| Connection setup delay | Transmission delay | Connection setup + transmission delay |
| Overload may block path setup | Overload increases packets delay | Overload block may block path setup and increases packet delay |
| Fixed bandwidth | Dynamic bandwidth | Dynamic bandwidth |
| No out-of-order packets | May have out-of-order packets | No out-of-order packets |
| No overhead bit after the path setup | Overhead bits in each packet | Overhead bits in each packet |

### 3.2.2. The OSI Model

The concept of telecommunication will be explained with the use of the Open Systems Interconnection (OSI) model. In 1984, the International Standards Organization (ISO) created OSI as a vendor-neutral networking model that would aid the competition between different vendors and reduce complexity. The goal of the OSI model is to design a common networking hierarchy to allow communication between all computers in the world and to guide vendors and developers so that the created digital products and software will interoperate [20]. The model has seven layers, which reference different hardware, software, and components of network communication. Each layer provides functions or services to the layer directly above and is in turn supported by the services provided by the layer directly below (Table 4).

*Table 4: The OSI Model*

| OSI Model | | | | |
|---|---|---|---|---|
| **Data Unit** | **Layer** | **Function** | **Protocols** | **Devices** |
| **Data** | 7. Application | End-user layer | HTTP, FTP, TELNET | Hosts, Firewalls |
| | 6. Presentation | Data encryption and decryption | JPEG, MPEG | |
| | 5. Session | Communications between hosts | Logical Ports | |
| **Segments** | 4. Transport | End-to-end connection | TCP, UDP | Hosts, Firewalls |
| **Packets** | 3. Network | Logical addressing IP | IP | Routers |
| **Frames** | 2. Data link | Physical addressing MAC | Ethernet 802.3 | Switch, Wireless Access Point, modem |
| **Bits** | 1. Physical | Physical medium, signal, and binary transmission | RJ-45, Ethernet 802.3 | Cables, hubs, optical fiber, SONET… |

Layer 7 (Application): The Application layer provides an interface from the application to the network and supports end-user processes such as file transfers, email, remote terminal access, etc.

Layer 6 (Presentation): The Presentation layer provides translation to/from the application layer, how data is presented. This layer negotiates the data formats to be sent across a network, this is where data encryption, decryption, compression and decompression of data takes place.

Layer 5 (Session): The Session layer is responsible for coordinating, establishing, and managing, and terminating connections between sessions between the applications. Also provides a method to group multiple bidirectional messages into a workflow for easier management.

Layer 4 (Transport): The primary focus of the Transport layer is to ensure the delivery of data between two hosts, that messages are delivered in sequence, error-free, and with no losses or duplicated. This layer reassembles data from the upper layer into segments and provides flow-control for data-loss prevention. The two common protocols operate on this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Layer 3 (Network): The Network layer provides logical addressing, switching and routing protocol used for routers, creating logical paths (virtual circuits), and transferring of data in the form of packets across the communication network.

Layer 2 (Data Link): The TCP/IP data link layer defines the protocol for the network for the transfer of frames (blocks of information) over a particular medium. The control and address information is inserted in the header and checks bits to enable transmission errors and flow control. This layer divided into sub-layers: Media Access Control (MAC) and Logical Link Control (LLC).

- MAC: controls how a computer on the network gains access to the data and permission to transmit it. Delivers frames using unique hardware addressing MAC.
- LLC: controls frame synchronization, flow control, and error detection and control.

Layer 1 (Physical): The Physical layer concerns with bit rates and data transfer mechanism. It defines a physical characteristic of the physical medium such as the layout of pins, voltages, cables, and establishes a connection from a terminal to a communication medium.

## 3.3. Synchronous Optical Network (SONET)

### *3.3.1. SONET Overview*

The Synchronous Optical Network is a standardized protocol developed in North America to provide high-level digital formats. The Synchronous Transport Signal level 1 (STS-1) is the basic SONET rate where it travels at 51.84 Mbps. A SONET multiplexer can combine transport input signals at lower levels into a higher STS-n level where the highest it can approach is STS-192 at nearly 10Gbps. SONET uses TDM to assign each circuit a fixed time slot, equivalent to a set percentage of the total bandwidth. The smallest, least-bandwidth time slot is sized to carry a single telephone conversation.

The SONET can be established in a ring topology where each terminal connected by an add-drop multiplexer (ADM) and can deployed in a self-healing manner, so they can recover from a failure. The self-healing rings can be formed to provide protection at the line layer as similar to Figure 15, 16 and 17. These types of protection schemes also referred to as liner APS and are required to recover from a fault within 50ms [5]. Other types of APS that provide protection at the path level are Unidirectional Path Switched Ring (UPSR) and Bidirectional Path Switched Ring (BPSR).

Figure 11 shows the UPSR protection. There are two fiber rings at each ADM: the working fiber carries traffic in the clockwise flow and the protection fiber carries traffic in the counterclockwise flow. In case of a failure, a UPSR can provide a fast-path protection. However, it is inefficient in terms of bandwidth consuming since two paths are used to carry every signal. Therefore, UPSR ring is used in the lower speed rings where traffic is gathered from various remote sites [5].

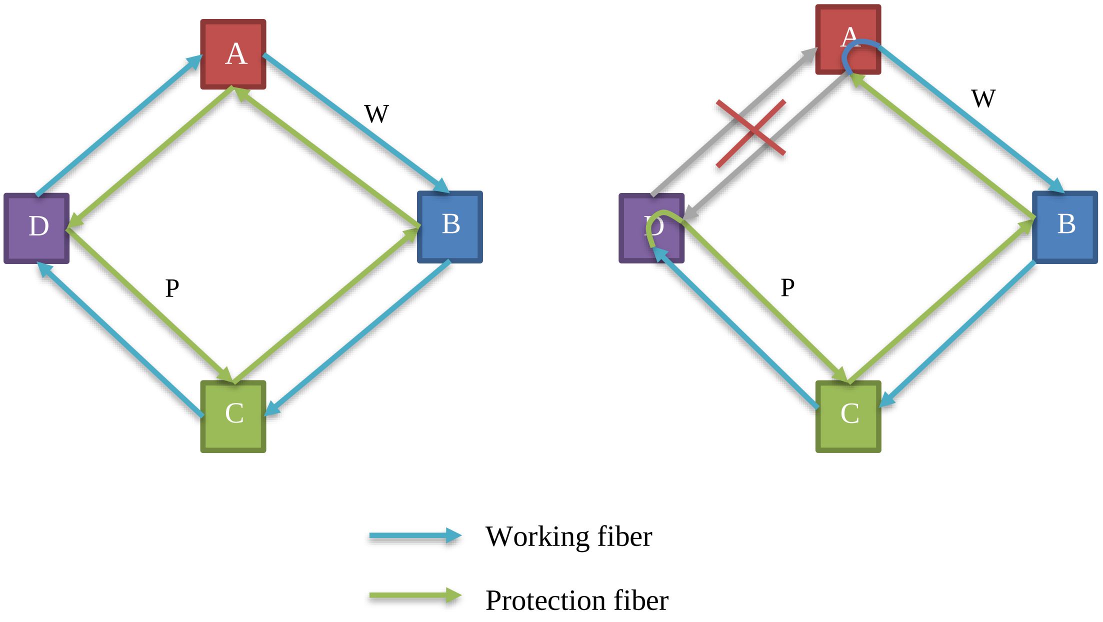


*Figure 11: Unidirectional Path Switched Ring (UPSR)*

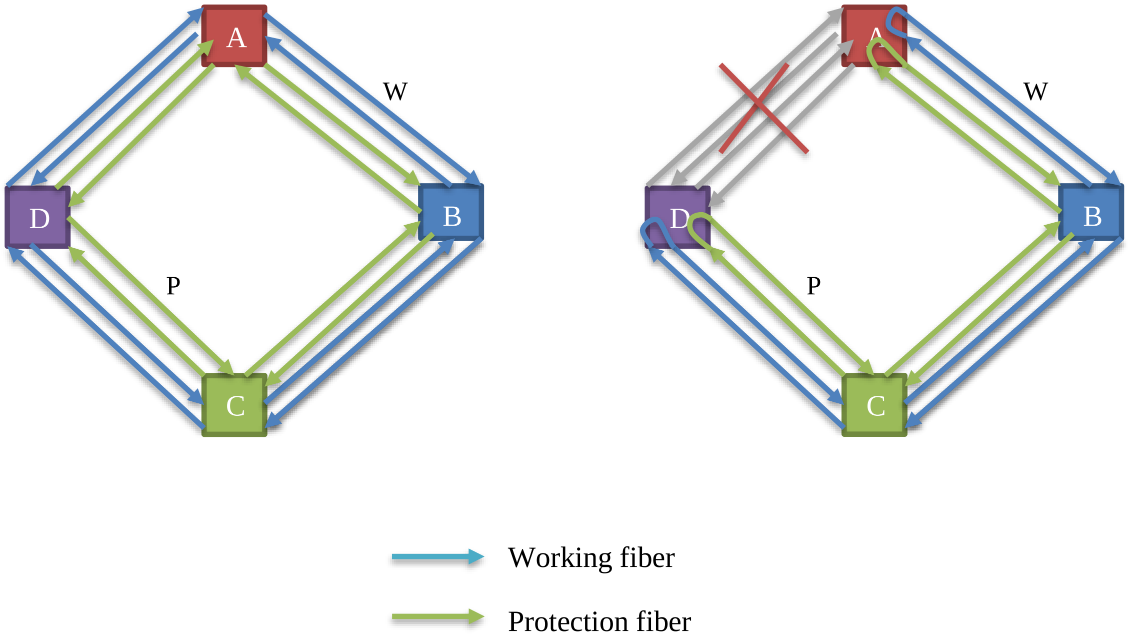


*Figure 12: Bidirectional Path Switching Ring (BPSR)*

Figure 12 shows the BPSR protection. There are two pairs of fiber at each ADM: a working pair and a protection pair in both directions. In comparison to the unidirectional ring, the bidirectional ring is more efficient as the traffic can be routed along the shortest path, so the bandwidth can be used to support more traffic [5]. When there is no fault in the ring, the protection path can be used to carry extra traffic in the system.

### *3.3.2. Advantages and Disadvantages of SONET*

Protection switching schemes previously discussed are connection-oriented. A pre-determined path is established before traffic starts flowing. SONET is a circuit-switching technology. While it provides very fast protection switching (failover) time and guarantees packets arrive and in order at the destination, it wastes bandwidth when there is no data to transmit. As briefly introduced in the beginning, SONET is becoming obsolete and there is limited support going forward.

### *3.3.3. A Solution for SONET*

One solution to the issues with SONET is a packet switched network. Packet Switched Network (PSN) offers high bandwidth data transmission, provides network efficiency and reliability, and many cost benefits. Thus, PSN offers a variety of benefits over SONET and is considered to be the replacement for SONET.

## 3.4. Multiprotocol Label Switching (MPLS)

### *3.4.1. MPLS Overview*

Multiprotocol Label Switching (MPLS) was defined by the Internet Engineering Task Force (IETF) in 1998 [24]. MPLS is a routing technique that provides a high-performance forwarding mechanism. Each router in the traditional IP network performs an IP lookup (routing) to determine the next hop and forwards the packet to that next hop repeatedly until it finds the final destination. This often causes congestion because of the time-consuming task and a significant delay in the forwarding process. In contrast, an MPLS router performs label switching. The first router performs a table lookup to find the destination router as well as a pre-determined path to reach the destination. Subsequent routers use that label to route the traffic without needing to perform additional IP lookup. MPLS will significantly reduce the time needed to perform IP routing lookups, lower the work on the core router, and provide a faster and better service.

The name “Multiprotocol” is used because the MPLS transport is independent of the underlying protocol; it could be Ethernet, SONET, or Point-to-Point Protocol (PPP). The MPLS resides at layer 2.5 with respect to the OSI model. MPLS maps onto any Lay 2 protocols and checks the IP packets that arrive at the network from Layer 3.

### 3.4.2. MPLS Operations

The Label Switch Router (LSR) is the combination of a switch and a router. It accepts the incoming packets, and forwards to the next correct LSR as soon as possible. The LSR that stays at the edge of the MPLS domain is called the Label Edge Router (LER). The LSRs have routing knowledge within the network and are insulated from the external network by LER (Figure 13).

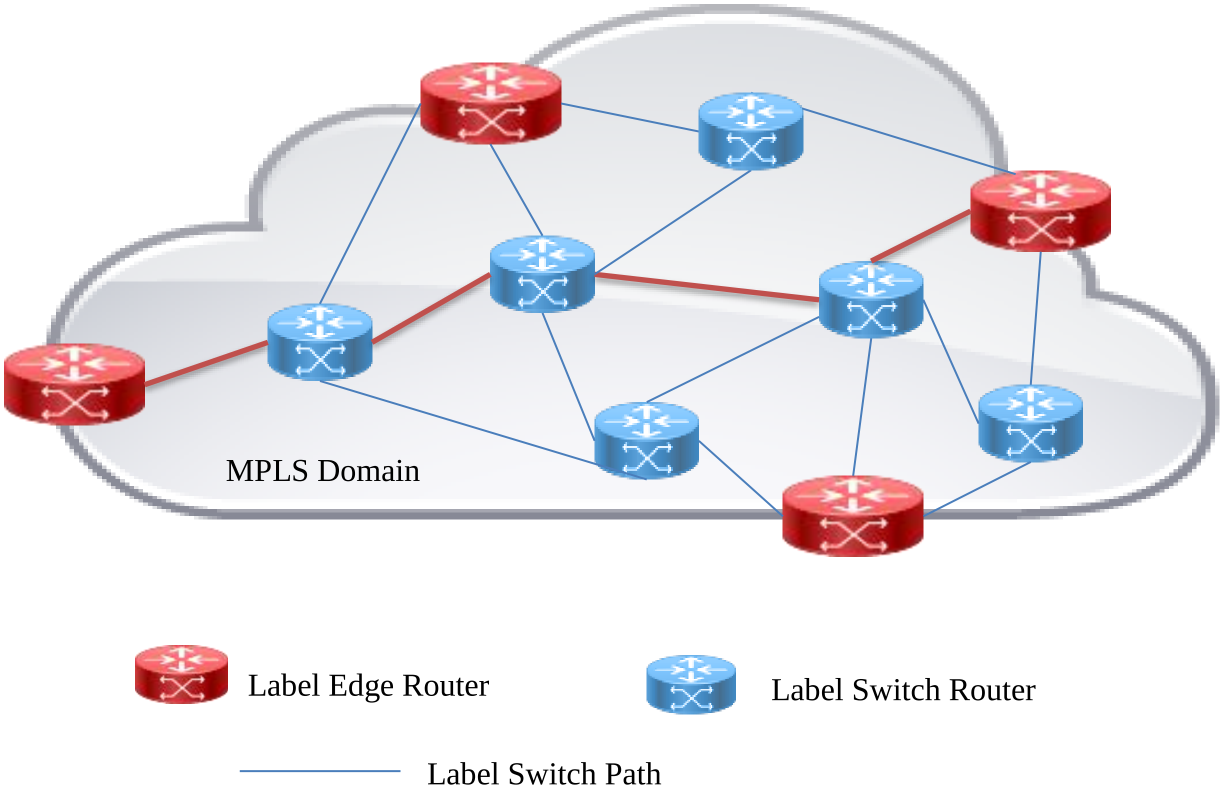
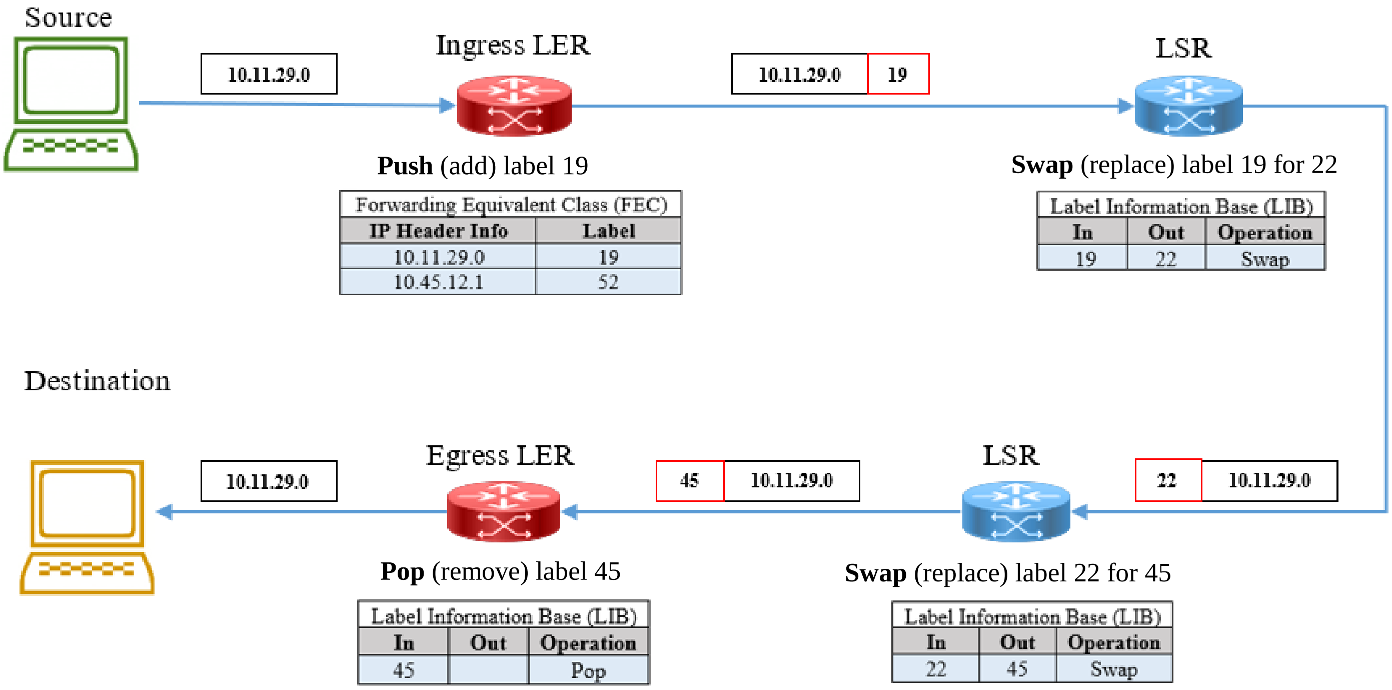


*Figure 13: MPLS Network*

A packet arrives at an Ingress LER from an IP domain. The LER checks the Layer 3 information on the packet, then checks the lookup table and finds the label matching the Forwarding Equivalent Class (FEC) for the route. An FEC is a set of similar packets sharing the same forwarding parameters and thus the same label. The label is pushed (added) onto the packet and forwarded into the MPLS domain. Inside the MPLS domain, the packet arrives at the LSR. The LSR checks the label in the Label Information Base (LIB), swaps (replaces) it for a new number and forwards it on to the next LSR or LER. Finally, the packet arrives at the edge of the MPLS domain, the Egress LER. The LER pops (removes) the label and forwards packet out to the network. The MPLS operations can be summarized in Figure 14.



| Forwarding Equivalent Class (FEC) | |
|---|---|
| **IP Header Info** | **Label** |
| 10.11.29.0 | 19 |
| 10.45.12.1 | 52 |

| Label Information Base (LIB) | | |
|---|---|---|
| **In** | **Out** | **Operation** |
| 19 | 22 | Swap |

| Label Information Base (LIB) | | |
|---|---|---|
| **In** | **Out** | **Operation** |
| 45 | | Pop |

| Label Information Base (LIB) | | |
|---|---|---|
| **In** | **Out** | **Operation** |
| 22 | 45 | Swap |

*Figure 14: MPLS Operations*

One of the advantages of the MPLS routing over IP routing is the path across the network, the Label Switch Path (LSP), is established even before the packet starts its journey. For each FEC there is a unique LSP established by Label Distribution Protocol (LDP) or Resource Reservation Protocol-Traffic Engineering (RSVP-TE). All LSPs are unidirectional paths and the return paths may take a different route.

### *3.4.3. MPLS-Transport Profile (MPLS-TP)*

The MPLS by itself does not provide the deterministic routing and failover times found in SONET. To address these deficiencies, the International Telecommunications Union (ITU) proposed an extension to MPLS called MPLS-Transport Profile (MPLS-TP). Note that MPLS-TP is not a subset of MPLS, it retains the basic principles of MPLS in which MPLS-TP is predictable, deterministic, and connection-oriented.

The drawback of MPLS is there is no guarantee that the returning path will follow the same route as the outgoing path. This characteristic is also known as non-deterministic congruent LSPs. Nonetheless, in MPLS-TP the pre-determined LSP is predictable, and the reversed path is the same as the forward path. This characteristic is also referred to as deterministic congruent LSP.

Bidirectional Forwarding Detection (BFD) is a protocol used to provide low overhead, fast detection of LSP failure (<50ms) between any two nodes. Messages are sent in a short interval from one end-point to another to check the continuity of the systems. If three or more expected incoming messages go missing, it can be assumed there is a line failure in the system which is reported within 10ms-30ms depending on equipment make up the network. An instruction is sent out to the switch selector to switch to the protection path in a guarantee of switch-over time less than 50ms. The path protection is a vital element in a transport network and is an indispensable element in a reliable MPLS-TP system. Figure 15, 16, and 17 show the three common backup protections the network.

Figure 15 provides a “one plus one” dedicated backup path protection where the transmit signal is sent in both working and protection path. A fault in a working path will cause a switching in the receiving end. The switching time is very fast (< 50ms). This scheme has a greater demand on network resources.

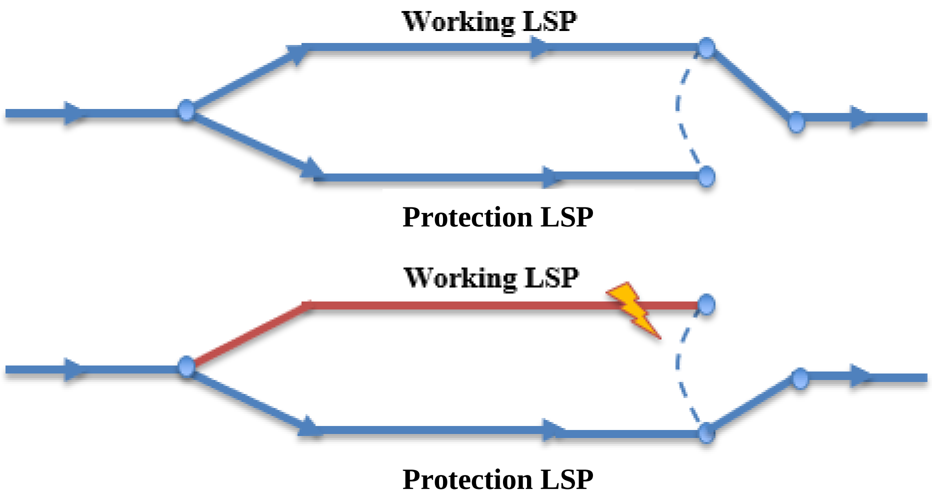


*Figure 15: 1+1 Path Protection*

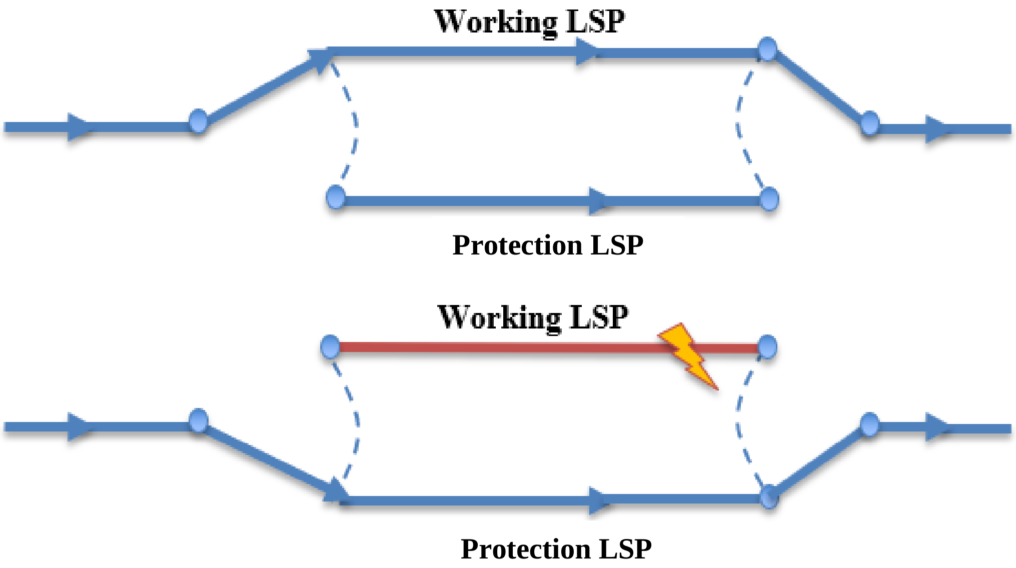


*Figure 16: 1:1 Path Protection*

Figure 16 shows a “one for one” protection scheme where the protection path only carries the transmit signal when there is a failure in the working path. When the working path carries the transmit signal, the protection path is available to carry lower priority traffics. This scheme has a lower demand on network resources.

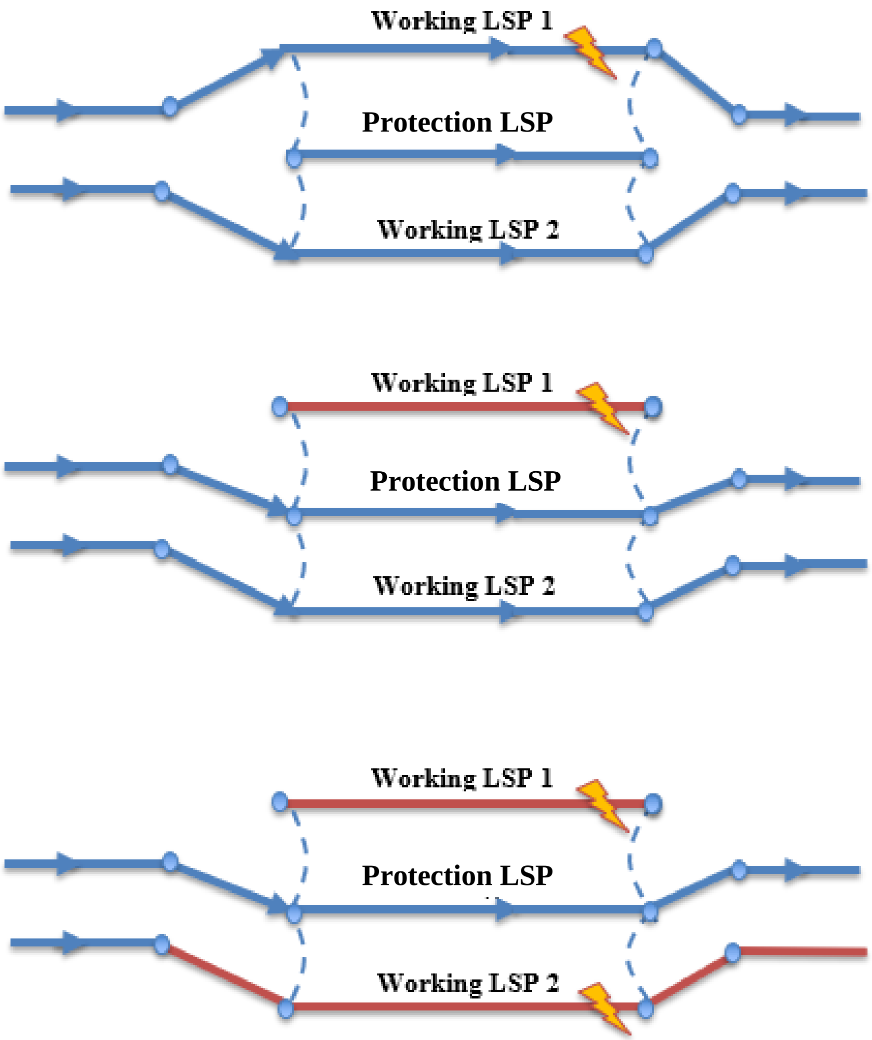


*Figure 17: 1: n Path Protection*

Figure 17 provides a “one for n” path protection where the scheme is designed to share a single protection path. Two or more working LSPs share one common protection path for use when one of the working paths fails. This is the most efficient use of resources, but clearly, it has the greatest risk since it cannot handle the failure of two working paths.

### 3.5. The Capital Expense and Operating Expense

The Capital Expenses (CAPEX) are funds that a company use to purchase, upgrade physical assets or fixed assets. The Operating Expenses (OPEX) are expenses required to maintain the daily operations of these assets. The transition to packet-based technology offers many benefits in both OPEX and CAPEX, Table 5 lists all the benefits in both expenses.

*Table 5: The CAPEX and OPEX*

| CAPEX | OPEX |
|---|---|
| Set up costs are low, as MPLS devices are cheap. | MPLS is designed to be inexpensive to maintain. |
| MPLS-TP deterministic nature of the path allows for increased efficiency and scalability in network design. | All the services were carried by traditional technologies are converted into a single MPLS based infrastructure. |
| | Maintenance knowledge and network management required for one type of transport network. |
| Devices are simple, require less training. | Better OAM, faster fault detection. |
| MPLS switches are low cost. | No more legacy equipment to maintain. |

# 4. TELEPROTECTION OVER PACKET TEST RESULTS

## 4.1. Communication Requirements for Teleprotection

Data is different from voice in which data is represented in a digital form, thus no need to convert to digital, however, voice is represented as an analog signal. Different characteristics in data and voice result in different requirements for an effective communication. Teleprotection traffic is more stringent compared to data, voice or video (Table 6) and it has the highest priority compared to others. Thus, teleprotection has to be transmitted first prior to other traffic.

Teleprotection communication is a mix of both data and voice in which the digital communication operates in real time similar like voice [22].

*Table 6: Communication Services Requirement*

| Service | Bandwidth | Latency | Criticality |
|---|---|---|---|
| Teleprotection | Low | Sub-cycle | Very high |
| SCADA (OT Data) | Low | N/A | High |
| Metering (OT Data) | Low | N/A | Low |
| IT Data | Low | High | Low |
| Voice (OT Data) | Low | < 150 ms | Low |
| Video (OT Data) | High | N/A | Low |
| Synchrophasors (OT Data) | Low-med | varies | varies |

There are several key requirements for teleprotection especially when migrating to the Ethernet-based communication:

1. The symmetrical delay or asymmetry is the difference in latency for each direction. The required latency from site A to site B has to be roughly the same as the delay from site B to site A. In other words, the asymmetry is calculated by = $|T_A - T_B|$ should be insignificant.

2. The teleprotection latency or channel delay is the time taken for a protection message from a local protection system to be transmitted to the remote protection system. The channel delay has to be as low as or even lower than the existing legacy system. Note that the channel latency directly adds the overall protection scheme fault clearing time.

3. The recovery time from a failure, or failover time, is the time taken for the network system to switch from the faulted working path to the unfaulted protection path. The time has to occur under 50ms. In teleprotection application, the MPLS failover time cannot match the SONET in most of the case. Hence, a future method will be proposed in Section 4.4 lab result.

4. Quality of Service (QoS): Packets will arrive in order and never be dropped.

## 4.2. Test Setup

To validate the testing results for the future migration from SONET TDM to MPLS packet-based within the TVA system, various laboratory testing performed at the TVA Chickamauga Test Lab. Figure 18 shows the network architecture built to perform the testing.

The MPLS network is constructed of four Ciena Ethernet switches that form a closed-loop ring (Figure 18). Ciena at Node 1 and Node 2 are either Ingress LER and Egress LER. Ciena at Node 3 and 4 are LSRs. The following equipment setup explanation is from the relay terminal (bottom) to the MPLS cloud (top).

Each location has one SEL-411L relay. The relay connects to an Ethernet switch RSG 2100, and in turn, the switch connects to a single Ciena switch. All Ciena switches are connected using fiber cable to form an MPLS ring topology in the network. Two test sets are used to measure the channel asymmetry. The Test Set 1 (TS1) monitors the longer path travels from Node 1 to 2, the Test Set 2 (TS2) also monitors the longer path but from Node 2 to 1. As a result, the asymmetry is the difference in TS1 and TS2.

In normal condition, the traffic from Station A travels on the shortest path (working path) to Station B while the longer path (protection path) is available to carry lower priority traffic. When a fault occurs on the working path, the switching takes place instantaneously and the protection path is now available to carry the transmitting signal. The concept of this "one for one" protection scheme for a communication path is explained in Section 3.4.3 and illustrated in Figure 16.

In a POTT scheme, a relay will not send a tripping signal if the internal fault occurs on the transmission line and the communication path fails. Unlike POTT, the DCB scheme will trip regardless. Thus, for the testing purposes, the pilot protection scheme used at both Station A and Station B is POTT to determine if the channel failure happens, will the tripping signal still make to its destination.

A channel failure happens where there is a fault on the communication path of the MPLS network. To create a fault on the fiber path, a connection at either terminal on the working path was removed between Node 1 and 2. The fiber connection is tested on 1Gbps and 10Gbps rate, the results are presented in Section 4.3.

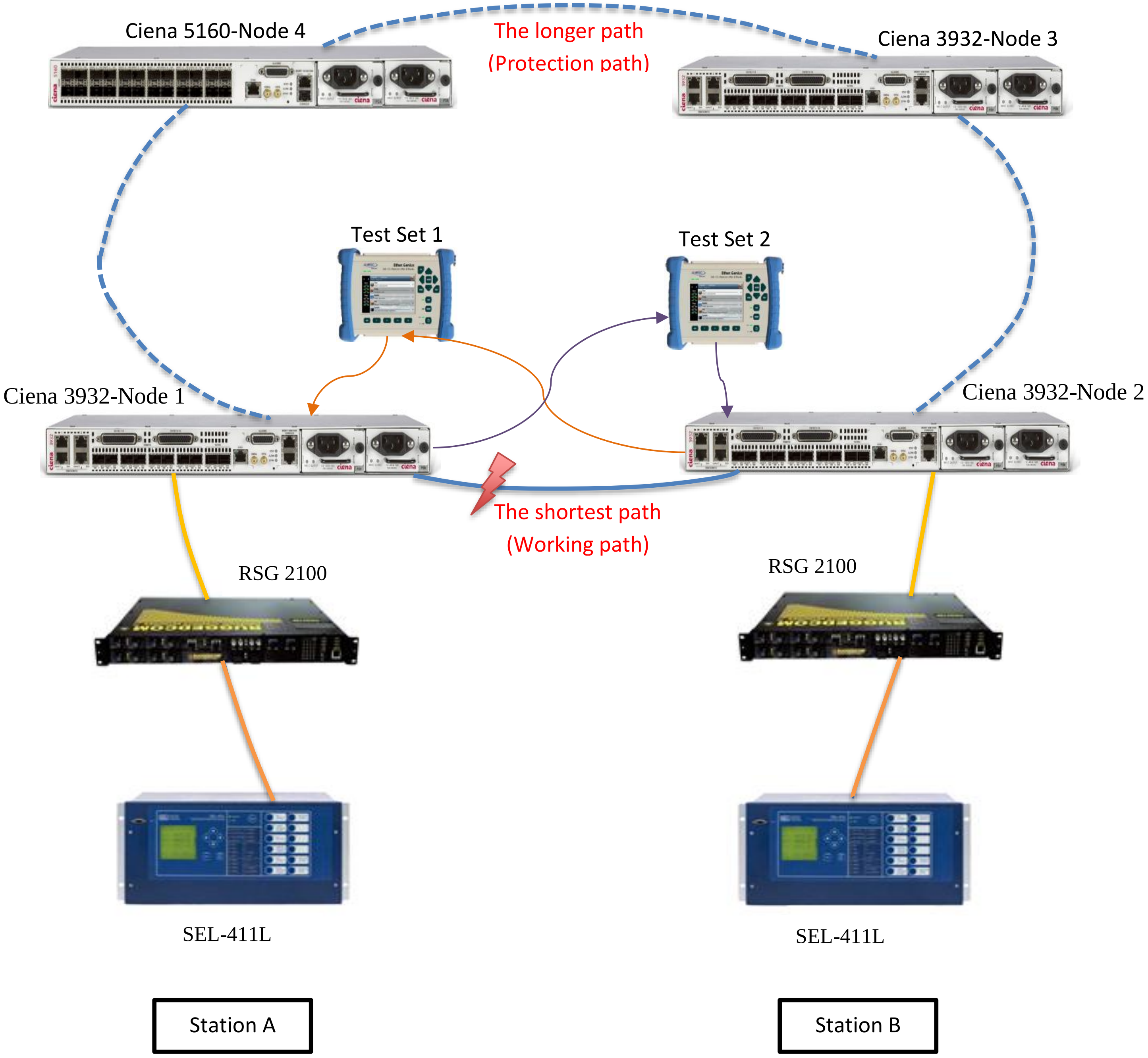


*Figure 18: Test Setup Network Connection*

## 4.3. Lab Results

Table 7 and 8 show results in five testing trials, “before” means when the system is in the normal condition, “after” means when the fault occurs in the network system. The latency in the system is very small (measured in microseconds) and there is no measurable asymmetry. The jitter in the network is the variation in latency measured in one direction across the network [23]. A network with constant latency barely has any jitter. The jitter is found to be 1µs in both tests. The average failover time in the 1G fiber connection is 28ms while in 10G connection is 30ms. Both are well under the 50ms requirement for teleprotection failover time. The teleprotection traffic was later flooded with other lower priority traffics and none of the teleprotection packets were dropped or lost. This guarantees the QoS of the system. In conclusion, lab testing has proven to satisfy all the communication requirements for teleprotection (Table 9).

Additionally, a large spool of fiber cable, called Fiber Lab, is connected between Node 1 and 4 to extend the fiber distance up to 20km (12.4 miles) long on a 10Gbps fiber connection. The test results for this are not in the tables below. However, the fiber spool only affects the latency of the network system, the latency when a fault occurs in the network is 113µs. The fiber distance does not affect the failover time.

*Table 7: 1G Fiber Connection Communication Path Failure*

| Communication Requirements | 1st | | 2nd | | 3rd | | 4th | | 5th | | Average | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Before | After | Before | After | Before | After | Before | After | Before | After | Before | After |
| **Latency** | 16µs | 29µs | 16µs | 29µs | 16µs | 29µs | 16µs | 29µs | 16µs | 29µs | **16µs** | **29µs** |
| **Asymmetry** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| **Jitter** | 1µs | 1µs | 1µs | 1µs | 1µs | 1µs | 1µs | 1µs | 1µs | 1µs | **1µs** | **1µs** |
| **Failover** | n/a | 30ms | n/s | 28ms | n/a | 28ms | n/a | 33ms | n/a | 22ms | n/a | **28ms** |

*Table 8: 10G Fiber Connection Communication Path Failure*

| Communication Requirements | 1st | | 2nd | | 3rd | | 4th | | 5th | | Average | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Before | After | Before | After | Before | After | Before | After | Before | After | Before | After |
| **Latency** | 11µs | 15µs | 11µs | 15µs | 11µs | 15µs | 11µs | 15µs | 11µs | 15µs | **11µs** | **15µs** |
| **Asymmetry** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| **Jitter** | 1µs | 1µs | 1µs | 1µs | 1µs | 1µs | 1µs | 1µs | 1µs | 1µs | **1µs** | **1µs** |
| **Failover** | n/a | 28ms | n/a | 28ms | n/a | 35ms | n/a | 29ms | n/a | 31ms | n/a | **30ms** |

*Table 9: Summary of Lab Test Results*

| **Communication Requirements** | **1G** | **10G** | **Result** |
|---|---|---|---|
| **Latency** | 29µs | 15µs | Pass |
| **Asymmetry** | 0 | 0 | Pass |
| **Failover** | 28ms | 30ms | Pass |

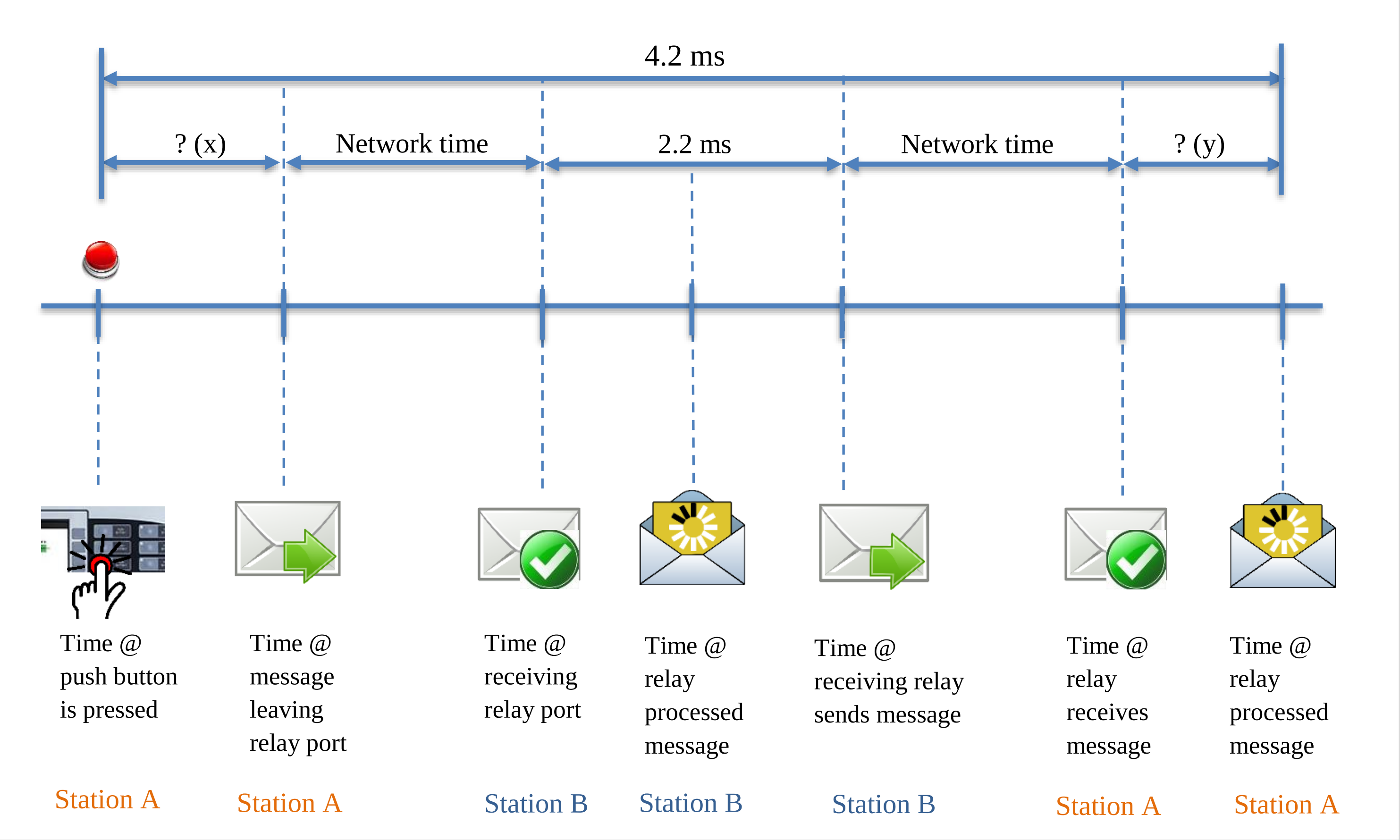

4.2 ms
? (x)
Network time
2.2 ms
Network time
? (y)
Time @ push button is pressed
Station A
Time @ message leaving relay port
Station A
Time @ receiving relay port
Station B
Time @ relay processed message
Station B
Time @ receiving relay sends message
Station B
Time @ relay receives message
Station A
Time @ relay processed message
Station A

*Figure 19: Timing Chart*

A test on how fast a teleprotection packet travels when an actual fault occurs on the transmission line from a local protection relay at Station A to remote protection relay at Station B. The setup is same as in Figure 18. In the real world, the relay will automatically send a signal to the other relay when it detects the fault. In the lab environment, a person will press the relay's button to send the signal. Figure 19 shows the time is taken (in both directions) from the pushbutton is pressed at Station A until it receives an acknowledge message back from Station B is only 4.2ms. In other words, it takes up to 1.0ms for the remote relay to receive the signal from the local relay traveling on the shortest path in the communication system.

From Figure 19, the network time is calculated by the following formula:

$$x + \text{network time} + 2.2\ \text{ms} + \text{network time} + y = 4.2\ \text{ms}$$

$$x + y + 2(\text{network time}) = 2.0\ \text{ms}$$

$$\text{Network time} = \frac{2.0\ \text{ms} - (x+y)}{2}$$

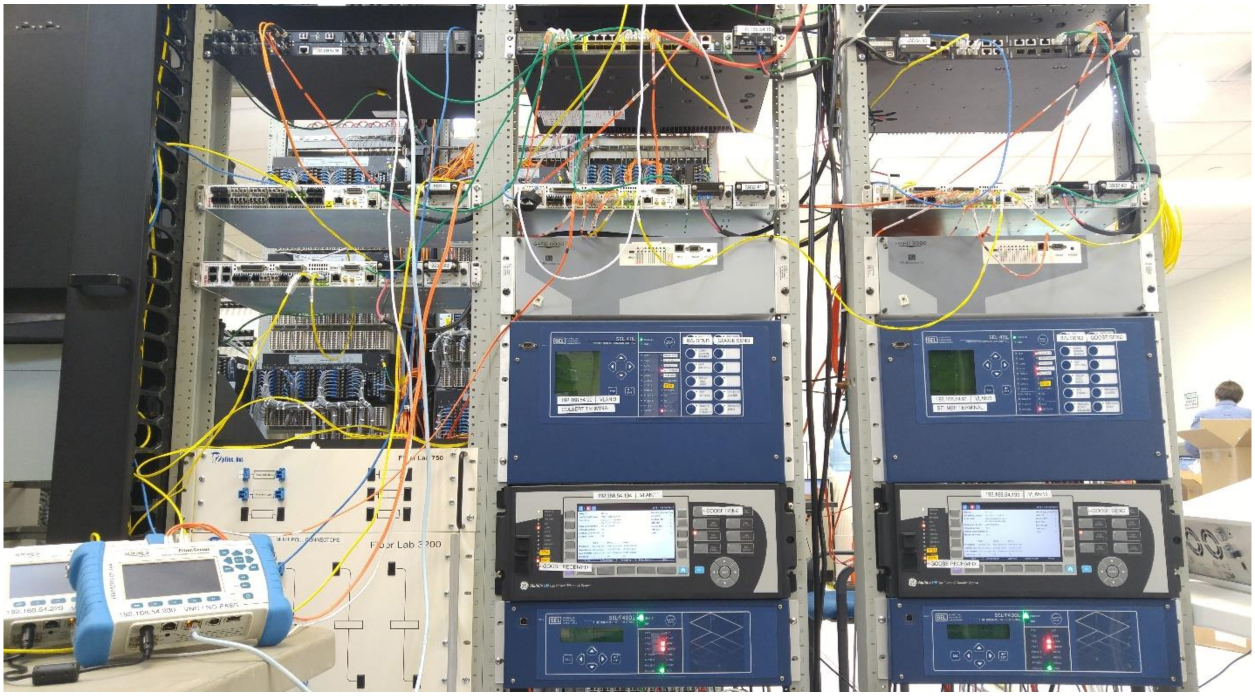


*Figure 20: The Actual Image in the Lab*

## 4.4. Future Work

Although the method shown in Figure 18 satisfies all communication requirements, it does not approach the speed of SONET in terms of fault recovery in most of the teleprotection applications. To provide SONET-like recovery times, the Parallel Redundancy Protocol (PRP) is used in the system to duplicate all Ethernet traffics along diverse paths and provides a seamless network failover with a guarantee of no loss of traffic [25]. Some relays have the PRP functionality, thus, for the future work, the relay could use PRP to communicate with the Ciena through dual physical connections to achieve “zero loss”, “zero recovery” network redundancy with each connection routed through a different path in the network to the far station.

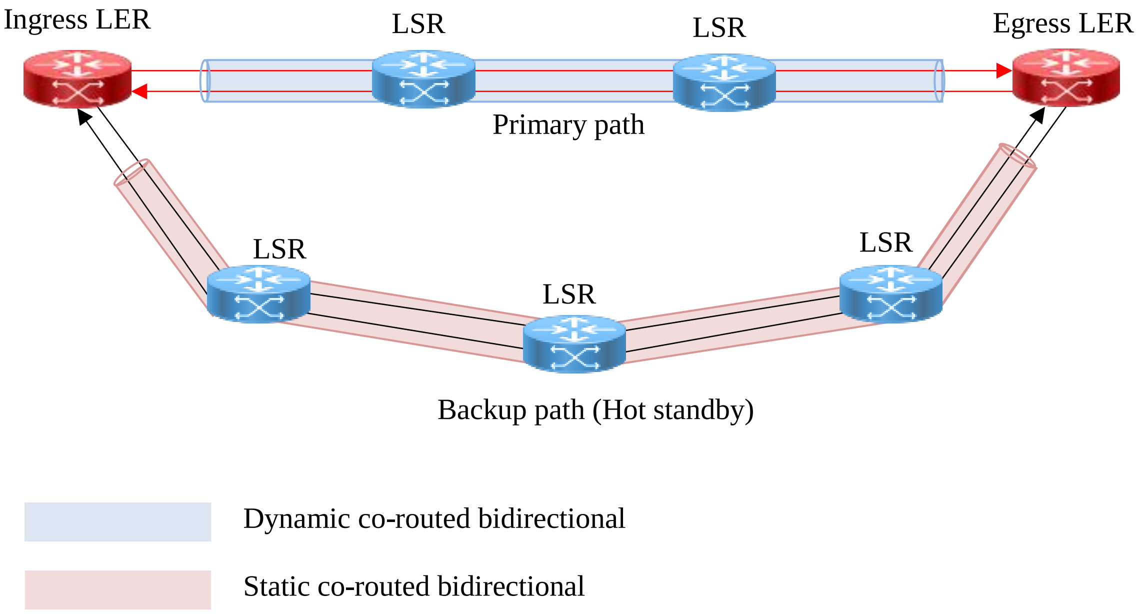

Ingress LER
LSR
LSR
Egress LER
Primary path
LSR
LSR
LSR
Backup path (Hot standby)
Dynamic co-routed bidirectional
Static co-routed bidirectional

*Figure 21: PRP Path for Teleprotection*

In Figure 21, the teleprotection packets travel independently on two paths (primary and backup) of the network. Should a fault occur on the primary path, the teleprotection packets travel on the backup path will not be affected. No switching needed since the two paths are independent. The primary path for teleprotection will be dynamic co-routed bidirectional that means a single path composed of two LSPs for both forward and reverse direction and is setup automatically. The backup path for teleprotection will be static co-routed bidirectional, same characteristics as the primary path but is manually configured in the system.

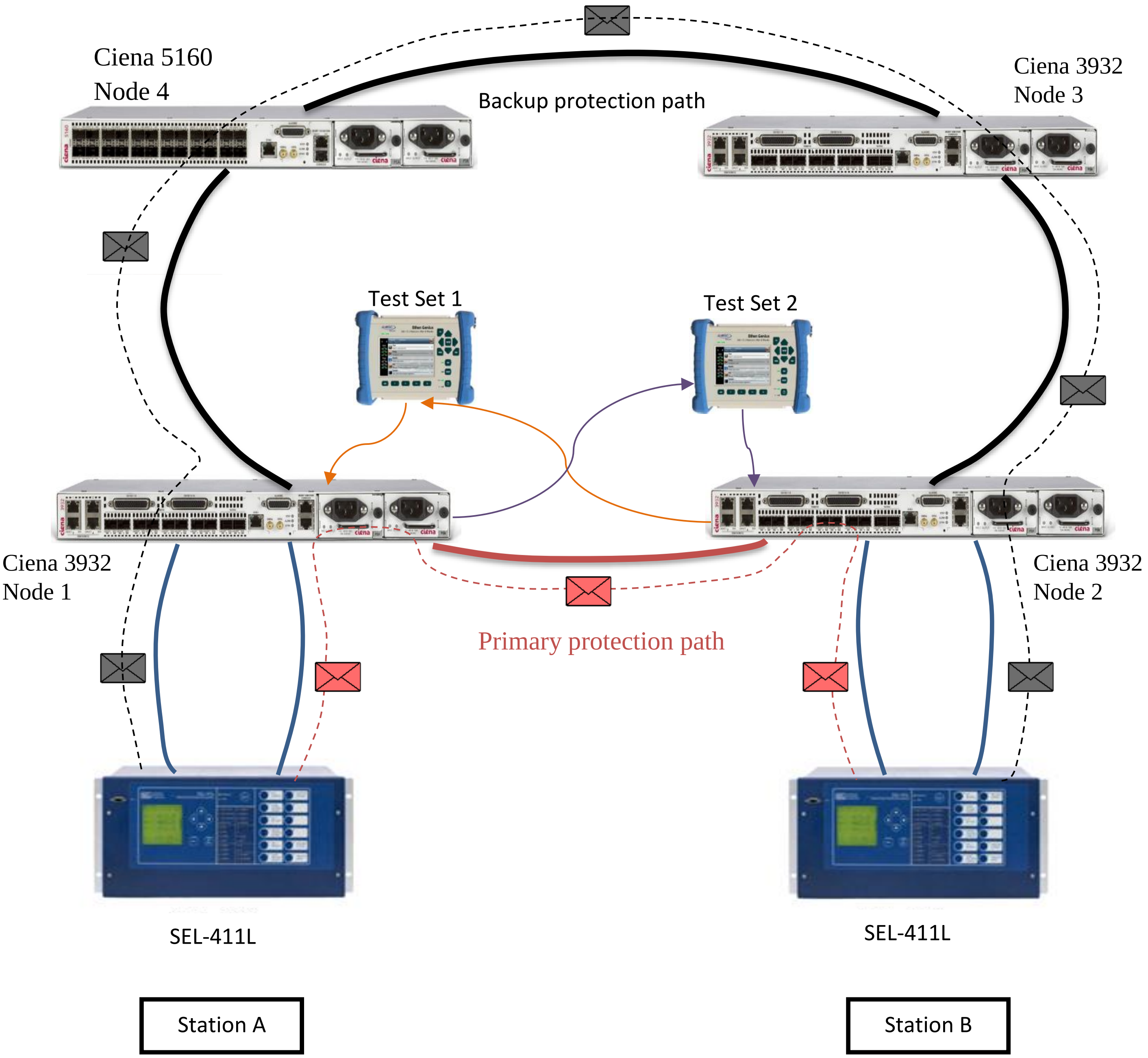


*Figure 22: PRP Lab Setup for Future Work*

The SEL-411L relays in Figure 22 use PRP to communicate with the Ciena switches. Moreover, the PRP relays in the figure can be referred to as Dually Attached Node (DAN). When the DAN relay sends out two identical Ethernet packets travel on separate paths to the Ciena switch, the Ciena switch will not discard but forward both packets to their destination along the two protection paths. For relay that does not have PRP functionality and can be referred to as Singly Attached Node (SAN), a Redundancy Box (RedBox) is used to mirror the traffics in both networks. No switching needed if a fault occurs on the path, and no packets will be dropped on any single failure (other than failure in relay or Ciena switch).

## 5. CONCLUSION

The future smart grid is the key driver for an increased demand for higher capacity, reliable, and more efficient communication. The long-used legacy technology SONET is becoming obsolete and ready to be replaced by Ethernet-based network communications.

The SONET system reserves bandwidth and transmits blank patterns when there is no traffic to send in order to maintain its deterministic behavior. This does not make efficient use of bandwidth. On the other hand, there is no need to reserve bandwidth in the packet-switched technology so that bandwidth may be freely shared among competing applications.

A reliable power system needs to have pilot protection schemes to provide high-speed clearing of faults (DCB, POTT, etc.). In order to transmit these signals requires durable communication channels (fiber optics, microwave, etc.). The local relay has to communicate and cooperate with the remote relay to clear fault on a system, thus demands a stable network communication path, such as provided by MPLS-TP. The test results from TVA’s lab have proven to satisfy all the requirements for teleprotection communication, assuring the migration to a packet-based system will be, if not same, better than the legacy system. Besides, the PRP function will be used in the future work, this approach will provide the system with “zero loss” and “zero recovery” network redundancy.

Packet delay variations in the past have raised concerns for the protection engineers when migration to a new network communication. Moreover, high latency in network communications can slow down the tripping, thus leaving serious consequences in the power system. However, testing assures that MPLS-TP offers many SONET-like features to guarantee a smooth transition; these mechanisms also come with higher bandwidth capacity and better network efficiency compared to SONET.

Moreover, the CAPEX and OPEX are in favors of new technology as the new devices are simple, setting up costs are low, and the MPLS is designed to be inexpensive to maintain.

## 6. REFERENCES

[1] “Transmission Line Protection-Review of Communications-Assisted Tripping schemes”, Schweitzer Engineering Laboratory 2012.

[2] G. Antonova, E. Colmenares, and I. Jankovic, "Analysis of Protection Scheme Dependencies on Communications," in Texas A&M Relay Conference, College Stations, TX, 2013.

[3] “Digital Communications for Relay Protection,” Working Group H9 of the IEEE Power System Relaying Committee, 1998.

[4] S. Ward, W. HiginBotham, and E. Duvelson, “Inside the Cloud-Network Communications Basics for Relay Engineer,” in 34th Annual Western Protective Relay Conference, Spokane, WA, 2007.

[5] A. Garcia, and I. Widjaja, “Communication Networks: Fundamental Concepts and Key Architectures”, 2nd ed., McGraw-Hill, 2004.

[6] J. Blackburn, and T. Domin, “Protective Relaying: Principles and Application”, 3rd ed., CRC Press Inc, 2007.

[7] IEEE Guide for “Standard Definitions for Power Switchgear,” in IEEE Std C37.100-1992, 1992.

[8] The Authoritative Dictionary of IEEE Standards Terms, 7th, in IEEE Std 100-2000, 2000.

[9] Flessner, Dave. “TVA to Spend $300 Million to Upgrade Fiber Optic Connections across Valley.” Timesfreepress.com, 11 May 2017.

[10] NERC Guide for “Physical Security” in NERC CIP-014-1, 2014.

[11] J. Roberts, TRANS-TP-09.10, “Guidelines for Pilot Protection on Transmission Line”, Tennessee Valley Authority, 2017.

[12] F. Jerry, TCS-ES-DES-09.206.4.1, “Teleprotection Installations”, Tennessee Valley Authority, 2013.

[13] S. Ward, T. Dahlin, and B. Ince, "Pilot Protection Communication Channel Requirements," 57th Annual Conference for Protective Relay Engineers, 2004, College Station, TX, USA, 2004.

[14] W. Elmore, “Pilot Protective Relaying”, ABB Automation, Inc., 2000.

[15] P. Haymaker, TCS-TPS-DES-09.204.2.1, “Microwave Point to Point Radio System”, Tennessee Valley Authority, 2017.

[16] “OPGW”, AFL - Upstate, SC, 10 Nov. 2018, www.aflglobal.com/Products/Fiber-Optic-Cable/Aerial/OPGW.aspx.

[17] C. Bertani, TRANS-MAINT-TP-06.003, “Fiber Testing Procedure”, Tennessee Valley Authority, 2017.

[18] P. Haymaker, TCS-TPS-DES-09.204.1.1, “Fiber Optic Systems”, Tennessee Valley Authority, 2017.

[19] S. Ward and T. Erwin, “Current Differential Line Protection Setting Considerations”, 2005.

[20] “Network Migration for Utilities: Teleprotection Over Packet”, RAD Solution Paper, 2011.

[21] R. Freeman, “Telecommunication System Engineering”, 4th ed, John Wiley & Sons, 2004.

[22] T. Rahman, S. Ward, and M. Bryan, “Teleprotection with MPLS Ethernet Communications-Development and Testing of Practical Installations”, Georgia Tech Protective Relay Conference, 2018.

[23] IEEE/PSRC Working Group H32, “Performance Requirements for Ethernet Circuits Applied to Teleprotection”, IEEE Power System Relay Committee, 2017.

[24] IETF-RFC 3031, “Multiprotocol Label Switching Architecture”, Network Working Group, 2001.

[25] IEC Guide for “Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR),” in IEC Std 62439-3: 2016, 2016.

[26] IEEE Guide for "Power System Protective Relay Applications Over Digital Communication Channels," in IEEE Std C37.236-2013, 2013.