University of Southern Queensland

Faculty of Engineering and Built Environment

# Teleprotection Signalling over an IP/MPLS network

A dissertation submitted by

Nigel A.J. McDowell

in fulfilment of the requirements of

**Courses ENG4111 and 4112 Research Project**

towards the degree of

**Bachelor of Engineering (Electrical/Electronic)**

Submitted: October, 2014

# Abstract

Protection of electricity networks have developed to incorporate communications, referred to as protection signalling. Due to the evolution of the electricity supply system, there are many developments pending within the scope of protection signalling and protection engineering in general. This project investigates the use of current and emerging communications technologies (i.e. packetised networks) being applied and incorporated into current protection signalling schemes and technologies.

The purpose of the project is to provide a more cost-effective solution to protection schemes running obsolescent hardware. While the medium-term goal of the industry is to move entirely to IEC 61850 communications, legacy teleprotection relays using non-IP communications will still exist for many years to come. For companies to be ready for an IEC 61850 rollout a fully deployed IP/MPLS network will be necessary and it can be seen that various companies worldwide are readying themselves in this way. However, in the short-term for these companies, this means maintaining their existing TDM network (which runs current teleprotection schemes) and IP/MPLS network. This is a costly business outcome that can be minimised with the migration of services from and decommissioning of TDM networks.

Network channel testing was the primary testing focus of the project. The testing proved that teleprotection traffic with correct QoS markings assured the system met latency and stability requirements. Furthermore, MPLS resiliency features (secondary LSPs & Fast-reroute) were tested and proved automatic path failover was possible under fault conditions at sub-30ms speeds.

**University of Southern Queensland**
Faculty of Engineering and Surveying

# ENG411 & ENG4112 *Research Project*

## Limitations of Use

The Council of the University of Southern Queensland, its Faculty of Engineering and Surveying, and the staff of the University of Southern Queensland, do not accept any responsibility for the truth, accuracy or completeness of material contained within or associated with this dissertation.

Persons using all or any part of this material do so at their own risk, and not at the risk of the Council of the University of Southern Queensland, its Faculty of Engineering and Surveying or the staff of the University of Southern Queensland.

This dissertation reports an educational exercise and has no purpose or validity beyond this exercise. The sole purpose of the course pair entitled "Research Project" is to contribute to the overall education within the student's chosen degree program. This document, the associated hardware, software, drawings, and other material set out in the associated appendices should not be used for any other purpose: if they are so used, it is entirely at the risk of the user.

**Prof Lyn Karstadt**
Executive Dean
Faculty of Health, Engineering and Sciences

# Certification of Dissertation

I certify that the ideas, designs and experimental work, results and analyses and conclusions set out in this dissertation are entirely my own effort, except where otherwise indicated and acknowledged.

I further certify that the work is original and has not been previously submitted for assessment in any other course or institution, except where specifically stated.

**NIGEL MCDOWELL**
Student Number: 0050032943

_____
Signature

_____
Date

# Acknowledgements

I would like to acknowledge and thank my supervisor Dr Alexander Kist and my senior engineer Mr Andrew Howard for their technical expertise, guidance and support over the course of this project. I would also like to acknowledge Mr Michael McEvoy for his protection testing expertise during the system testing phase of the project.

Energex Limited is also acknowledged for the use of their IP/MPLS network for testing.

NIGEL MCDOWELL

# Contents

# List of Figures

# List of Tables

# List of Appendices

# List of abbreviations

| | |
|---|---|
| CB | Circuit Breaker |
| SEL | Schweiter Engineering Laboratories |
| MB | Mirrored Bits |
| VF | Voice Frequency |
| IEC | International Electrotechnical Commission |
| A/D | Analogue/Digital |
| Kbps | Kilobits per second |
| OPGW | Optical Ground Wire |
| TDM | Time Division Multiplexing |
| SCADA | Supervisory Control and Data Acquisition |
| WAN | Wide Area Network |
| SDH | Synchronous Digital Hierrachy |
| SONET | Synchronous Optical Networking |
| PDH | Plesiochronous Digital Hierachy |
| IED | Intelligent Electronic Device |
| PSN | Packet Switched Network |
| IP | Internet Protocol |
| MPLS | MultiProtocol Label Switching |
| OSI | Open Systems Interconnect |
| CIGRE | International Council on Large Electric Systems |
| LAN | Local Area Network |
| MPLS-TP | MultiProtocol Label Switching – Transport Protocol |
| OAM | Operation, Administration and Maintenance |
| QoS | Quality of Service |
| VPLS | Virtual Private LAN Service |
| VPN | Virtual Private Network |
| PW | Pseudowire |
| VLAN | Virtual LAN |
| FRR | Fast Re-Route |
| IOM | Input/Output Module |
| OTE | Operational Technology Environment |
| ATM | Asynchronous Transfer Mode |
| CIRCE | Research Centre for Energy Resources and Consumption |

# Chapter 1

# Introduction

## 1.1 Project Outline

Electricity supply systems are comprised of a number of unique and distinctly segregated sectors. Generally speaking, these sectors are defined as Generation, Transmission and Distribution/Sub-Transmission. The scope of this project does not extend to the generation sector, instead focussing on Transmission and Distribution networks where the learning and developments are applicable to these sectors. The two sectors of focus; Transmission and Distribution are inherently different. They are separated by their roles within the system, voltage levels, technology, philosophies and practises however, one aspect in particular is seen throughout; that is the need and philosophies of protection and protection signalling. Protection systems within all sectors of the electricity supply industry serve the same purpose in the detection and isolation of faults from the remaining healthy electricity network (Gers & Holmes, 2011). Protection of electricity networks have developed to incorporate communications, referred to as protection signalling. Due to the evolution of the electricity supply system, there are many developments pending within the scope of protection signalling and protection engineering in general. This report investigates the use of current and emerging communications technologies (i.e. packetised networks) being applied and incorporated into current protection signalling schemes and technologies.

## 1.2 Overview of the Dissertation

The dissertation is organised as follows:

**Chapter 2** describes protection signalling fundamentals including current teleprotection schemes, and also investigates the drivers behind the introduction of new technologies and protocols being implemented in this field.

**Chapter 3** discusses internetworking fundamentals including MPLS as a mature telecommunications technology. The chapter then investigates utilities use of packetised communications networks for 'mission critical' services and further investigates the concept of an IP/MPLS network being used in teleprotection signalling schemes.

**Chapter 4** completes a brief requirements analysis which establishes the deliverables for this project.

**Chapter 5** provides a basic description of a current TDM teleprotection system and designs the proposed system at a conceptual level.

**Chapter 6** describes all components to be used in the system. It also describes and evaluates both electrical and telecommunications test equipment required in the testing of an IP/MPLS protection signalling scheme.

**Chapter 7** describes the project methodology which includes configuration descriptions and testing methodologies.

**Chapter 8** presents the test results and analyses performance in-line with **Chapter 4** requirements.

**Chapter 9** concludes the dissertation, includes recommendations and further work in the IP/MPLS protection signalling field.

# Chapter 2

# Protection Signalling Fundamentals

## 2.1 HV Electricity Supply Network Protection

Various pieces of equipment are required to adequately protect the electricity network; generally, where protection is implemented sets of relays operate in conjunction to isolate faults from the healthy network through the operation of Circuit Breakers (CBs). This combination of CBs and relays is referred to as a protection scheme. In many cases a number of protection schemes are implemented to protect a single piece of plant or network (e.g. a feeder) forming what is known as a protection system. Protection schemes are implemented in electricity systems for a number of reasons, the most important of which are listed below:

- Maintenance of supply
- Public and personnel safety
- Equipment protection
- Power system integrity
- Power quality

The above are critically important in all sectors of the electricity supply network, and understandably philosophies and requirements for protection are generally carried through all

sectors of the network. When the design and implementation of protection schemes is considered the critical characteristics are generally considered as (Gers & Holmes, 2011):

- **Dependability** is the ability of a protection system to operate as and when it is designed to.
- **Security** is the ability of a protection system to operate only when it is required to.
- **Speed** is the minimum time it takes for a protection scheme to detect and subsequently isolating a fault.
- **Cost**: like all other investment in the network, the protection systems must be cost-effective.

The extent to which these characteristics govern the effectiveness of a protection scheme are the exact reason that many protection engineers and telecommunications engineers alike are hesitant to move away from current (and in some cases, legacy) technologies and practices.

## 2.2 Protection Signalling

The use of communications as part of the protection schemes or systems can provide unique functionality and enhance the primary performance characteristics of protection schemes or systems (being dependability, security and speed). Protection Signalling carried over various communication mediums has the ability to convey protection commands to additional relays (making the scheme more dependable, secure and faster) or facilitate the detection of faults through comparison of measured data depending on the type of scheme being implemented. It is hard to define which protection particular scheme or combination of schemes should be used in any given situation, given the number of valid alternatives, however generally the application governs the scheme to be implemented (Alstom, 2011) To ensure the power system is protected, relay signals need to be transferred between distance relays with minimal delay. This end-to-end delay includes the latency of the telecommunications network as well as the detection and activation time of the protection circuits. This latency requirement is often described by engineers with two different perspectives. Transmission and distribution (T&D) engineers typically focus on the fault clearing time, the maximum delay for a fault to be isolated. This requirement is often dependent upon the voltage class and can be stated as an absolute value or in terms of a number of cycles. Starting with the maximum fault clearing

time target latency, T&D engineers will subtract the fault detection time of the local relay, the processing time of the distance relay, the time to close the circuit breaker, etc., to identify the residual amount of latency which is the maximum for the telecom path. Telecom engineers tend to focus on the latency for the telecom path (Hunt, 2011). Protection signalling facilitates the enhanced performance and fundamental functionality of the following two common protection schemes:

- **Differential** protection schemes are comprised of a clearly defined 'zone of operation' with protection relays at the boundaries of the 'zone'. Differential protection involves the measurement of currents at each end of the zone, and the transmission of information between the equipment at zone boundaries. These measurements form the basis of the fault detection and isolation operation. Differential protection is used liberally in distribution networks in fact, the majority of 11kV tie feeders (feeders directly between substations), 33kV and 110kV feeders in the Energex network are protected by feeder differential protection (Kerven, 2011).

- **Distance** protection schemes are used to protect feeders predominantly. Distance protection operates on the measurements of line impedance (derived from voltage and current measurements). Generally speaking these relays are time graded to loosely define zones of protection however; commands can be sent to remote relays to enhance performance.

Protection schemes can generally be defined as 'unit' or 'non-unit' protection, based on the ability to clearly define the 'zone of operation' (e.g. Differential protection is an example of unit protection whilst Distance is a form of non-unit protection). Protection Signalling is utilized in different manners for unit and non-unit protection. Unit protection relies on protection signalling to convey measured data between relays to detect a fault within the zone of operation, while non-unit protection on the other hand, implements protection signalling to convey protection commands to remote relays in order to improve dependability, security and speed of the scheme. The protection commands that may be issued in communications-aided, non-unit protection schemes include (Ebrecht, 2013):

- **Direct Intertripping**: a 'TRIP' command is send directly to the master trip relay (remote) resulting in a CB operation. This form of Intertripping has the strictest dependability and security requirements as mal-operation can result in false tripping (and isolation of healthy network).

- **Permissive Intertripping**: a remote relay issues a permissive trip command when it detects a fault, if this command coincides with local fault detection, a CB operation is initiated. Due to this functionality (spurious CB operations are not possible) requirements on security are less than those placed on dependability and speed.

- **Blocking Intertripping** is used to prevent remote relays from tripping on faults outside of their 'zone of operation'. In operation a blocking signal is sent to the remote relay to over-ride the trip command generated locally upon fault detection. As such this application has the strictest latency (3-5msec) and dependability requirements.

## 2.3 Communications Facilitating Protection Signalling

In order to facilitate protection signalling between two (or more) relays, a fit-for-purpose communications link must be established. The manner in which this is achieved has changed dramatically over the years as both protection devices and communications equipment have developed; **Figure 2.1**, shows a number of methods and relevant interfaces for facilitating communications between two relays. These configurations include various transmission media, various implementations of communications

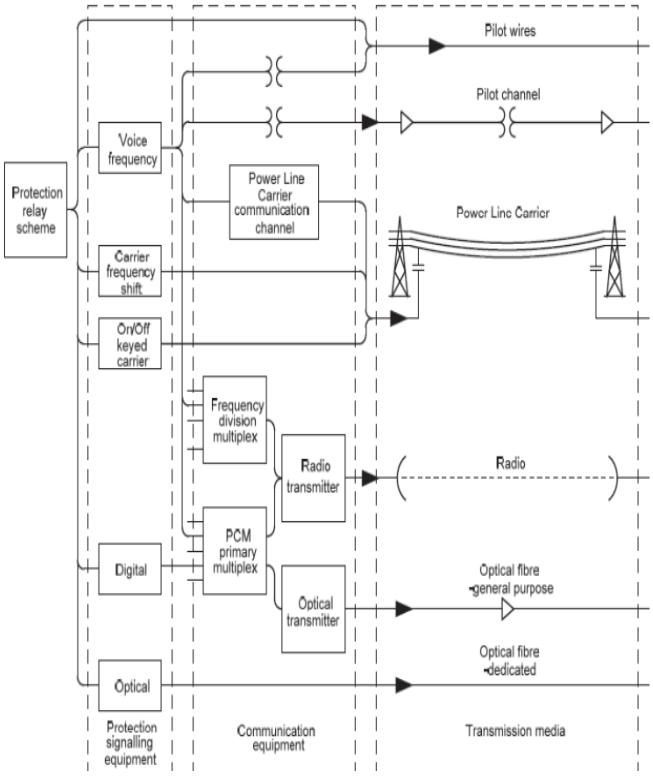



**Figure 2.1 – Protection Signalling and Communications Systems** (Alstom, 2011)

equipment (including bypassing communications equipment in the case of direct fibre), and various protection signalling equipment. In some cases, the protection signalling equipment is included within the protection relay, streamlining the process in transmitting the protection signal. The preference in transmission of protection signals is via direct fibre optics or direct copper connections. This allows the systems to avoid the use of multiplexers or other communications equipment and improving all aspects of the protection signalling system (dependability, security and speed).

The interface between protection device and protection signalling device is generally of a 'clean contact' nature. This signal however, is not suitable for dependable or secure transmission over the telecommunications infrastructure to the remote relay. Protection signalling devices are responsible for transforming this clean contact signal into a signal suitable for interfacing with communications devices or directly to communications medium in order to be transmitted dependably, securely and with minimal delays. In saying this, not all methods are suitable for transmission over every medium for various reasons. Examples of the forms of these protection signals include, but are not limited to (Alstom, 2011):

- **Voice Frequency (VF):** common multiplexing techniques often present standard communication channels of 2 to 4 kHz and are often referred to as VF channels. Protection signalling can present a dependable and secure signal through modulation within this bandwidth. VF signals are advantageous as they can make use of standardised communications interfaces.

- **DC Voltage Signalling:** a voltage step or reversal can be used to convey protection commands; however it is only suitable for transmission via utility owned pilot cabling.

- **SEL MBs (MIRRORED BITS)®:** a proprietary digital signal developed by SEL (Schweitzer Engineering Laboratories) that creates a virtual eight output to eight input connection in both directions (between two SEL MB compatible devices). By process both transmitted and received messages. MBs are transmitted repeatedly (3 times per 8 MBs) in a MB message and are subject to numerous error checks to ensure dependability, security and speed.

- **IEC 61850 (future):** IEC 61850 is a standard that defines mechanisms that ensure dependability; security and speed are met when protection signalling is implemented via Ethernet.

The signals presented by the protection signalling device described above are presented to the transmission medium or communications equipment. These interfaces are often capable of supporting both digital and digitized versions of analogue protection signals. In many cases these interfaces have developed around the use of protection signals and often can accommodate various methods of protection signalling including VF etc. most interfaces used to convey protection signalling are capable of supporting 64kbps signals (equivalent to one VF channel sampled at 8 kHz using an 8bit A/D (analogue/digital) converter. The following are examples of interfaces between protection signalling and communications equipment (IEEE – Guide for Power System Protection Relay Applications, 2013):

- **G.703** is a standard electrical initially developed in the 1970's. G.703 presents a 64kbps standard unit for transmission in the communications network. In co-directional operation, G.703 is presented over 4 wires, in either balanced (120Ω twisted pair) or unbalanced (dual 75Ω coaxial cabling).

- **C37.94**: defines both the physical and electrical interface for the connections between Teleprotection equipment and digital multiplexers using optical fibre exclusively. C37.94 defines nx64kbps channels supporting up to twelve concurrent channels within the interface running over multimode optical fibre, given the use of multimode optical fibre and operating power and sensitivity, C37.94 is somewhat limited in operating distances (capable of transmission up to approximately 2km) (IEEE Std. C37.94, 2013).

- **Serial Communications**: serial communications exist in a number of standards and formats specifying both physical and electrical interface requirements. In many cases identical interfaces are defined differently by different organizations. For example a common serial interface RS-232 is equivalent to the combination of V.24 and V28 and the standard X.21 interface (although this is seldom used in Energex) (Made-IT: Connectivity Knowledge Platform, 2014).

- **Ethernet (future):** is an IEEE standard that has existing since the 1980's, it hasn't however been used for protection signalling. With the developments made with IEC 61850, Ethernet will likely become the sole interface in protection signalling.

Carrying the protection signals between relays, the transmission medium varies quite dramatically depending of a number of factors including; timeframe of installation, geographic limitations and availability of existing communications infrastructure. Given the nature of a distribution network (shorter feeder lengths, closer substations etc.) protection signalling via direct communication (be it copper or preferably, fibre optics) is possible and preferred. The move towards fibre optic communications as a common standard owes to its ability to provide immunity from electrical interference and the fact that it is now readily available and available cheaply (Alstom, 2011). The most common communications media used within the protection domain are outlined below:

- **Fibre-optics** utilise light pulses to convey digital data. Fibre optic cables are often installed within. Overhead Earth Wires to transport data around the electricity network as Optical Ground Wire (OPGW).
- **Pilot wires** are continuous copper connections between signalling substations intermediate substations may be required to ensure distances are covered, and allow multiplexing of the signal to enhance channel use.
- **Power Line Carrier**: a communications link is established by injecting a high frequency signal over the existing 50Hz being carried by the overhead power cable. This presents a number of considerations including transmission of signals under fault conditions and signal filtering.
- **Microwave Radio**: point to point radio links can provide high-bandwidth communications links however, in practise it is seldom economic to provide radio equipment solely for protection signalling. Due to this, it is often multiplexed with other signals generated within the substation.

In instances of non-direct protection signalling (i.e. where multiplexing equipment is used to enhance utilization of communications channels) a transport technology is required to control the allocation of resources on the channel. In the case of electricity utilities this transport technology is more often than not TDM (Time Division Multiplexing).

TDM divides the shared medium or channel into a series of repeating timeslots which are permanently assigned to a service (e.g. Protection Signalling, SCADA (Supervisory Control and Data Acquisition), corporate WAN (Wide Area Network) etc.). The amount of bandwidth necessary to guarantee a certain level of performance dictates the number of time slots a service will require generally speaking, TDM channels are provided as 64kbps in order to accommodate digitized VF signals and equivalent signals. It is this functionality that allows TDM to be engineered to provide very deterministic latency and guaranteed bandwidth for all services operating on the channel (Schweitzer et al, 2012). TDM networks have typically been created using a number of technologies in the past with present instances of TDM networks being implemented using SDH/SONET (Synchronous Digital Hierarchy/Synchronous Optical Networking) rather than PDH (Plesiochronous Digital Hierarchy, which is typically being replaced by the former). As transport technologies continue to evolve the trend is to move towards packetised communications. Given the future of Ethernet based IEC 61850 protection signals; it is foreseeable that the majority of transport technologies will be packet-based; operating over primarily Ethernet based radio and dedicated fibre optics. Though dedicated fibre optics go a long way to ensuring dependability, security and speed of signalling, the actual signalling presented by IEC 61850 (and other future protocols) must be capable of meeting, and perhaps surpassing current standards presented by protocols such as SEL MIRRORED BITS and other protection signalling methods.

## 2.4 Drivers for the Introduction of New Technologies & Protocols

Protection relays have evolved over the years, from electromechanical devices to microprocessor based protection relays and more recently to the point they are more easily defined as Intelligent Electronic Devices (IEDs) as relays have evolved to the point where they are essentially a generic computing device. In many cases these IEDs have gained the capability to control, record, report, communicate and in some cases adapt to events on the power system; though their primary purpose has remained the same in facilitating protection functions (Sollecito, 2009). These developments have been driven by a number of factors including greater dependability, accuracy and a reduced cost.

As a greater number of protection and substation automation functions are moved into the digital realm, there is a substantial increase in the amount of data points and functionality available from a single IED (Mackiewicz, 2006). There is a variety of functions that a protection IED can theoretically carry out. Further to the protection data, an IED could also carry out automation, metering, diagnostics and communications functions. The amount of data that is now readily available (with the implementation of IEDs capable of more functions) has seen a push to implement features of the 'smart grid' roughout electricity distribution networks worldwide. Migrating to these 'smart' networks, is driven by three clear enterprise areas, including; financial performance of the organization, customer service and organizational effectiveness (Sollecito, 2009). In an attempt to manage the implementation of the growing number of IEDs in the substation environment and enable communication between various devices to fully realise these new possibilities, a new communication model was required. That model (though still under development) has evolved and has been standardized as IEC 61850 – Communication Networks and Systems in Substations (Sollecito, 2009).

The current vision of IEC-61850 is quite broad, whilst initially establishing a next-generation SCADA protocol; it has evolved to incorporate advanced applications in protection and control. Subsequently, the IEC 61850 concept became a standard for the next generation substation system with a higher degree of integration, reduced cost, greater flexibility, widely interoperable functionality and reduced construction and commissioning time (Kastenny et al, 2012). It is these foreseen advantages that make the implementation of IEC 61850 worthwhile for utilities in an attempt to improve financial performance, customer service, and organisational effectiveness.

The trend seen in electricity networks to move towards the 'smart' network also presents a number of problems concerning the communications infrastructure within the network. Generally utilities have used private TDM networks to ensure deterministic performance for critical operations and carrier grade performance. However, the increase in data presented by devices within the smart grid has promoted bandwidth usage of communications to a point that TDM communications can no longer cost-effectively support (CISCO, 2012). Utilities have relied upon TDM technologies for some time now; as is the case with protection once a standard is established engineers are often reluctant to move away from those technologies. This presents an issue when these technologies are no longer supported by manufacturers.

Many companies have recently faced this issue; however the way companies have responded has varied. Some companies have moved directly into the realm of packetised networks or PSNs (Packet Switched Networks), whilst others have opted to utilize current generation TDM networks (SDH/SONET) in an attempt to maximise the operational lifetime of their current communication networks.

In this vein, many transmission and distribution authorities have begun to adopt IP/MPLS (Internet Protocol/Multi-Protocol Label Switching) networks as their future primary communications network. Many are also initially leaving protection signalling on their legacy TDM based network in order to meet stringent performance requirements before a packetised telecoms solution has been heavily tested and proven. This project seeks to examine and test existing protection signalling schemes, currently running over a legacy TDM based network, over an IP/MPLS network.

Similarly to the drivers for the introduction of new standardised protocols, new technologies are also driven by the benefits they present to organizations implementing them. The drivers of financial benefits, quality of supply and organizational effectiveness still apply here.

Utilities are taking advantage of the network transformation required by the smart grid to create converged networks similar to those shown in **Figure 2.2**. A converged network provides the opportunity to reduce both capital and operational expenditure by supporting multiple types of utility communications over a common infrastructure.

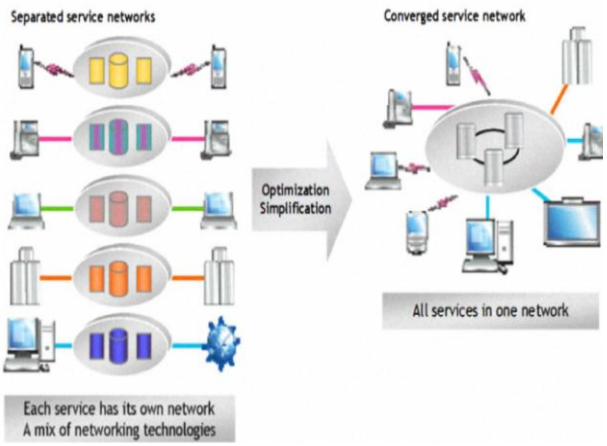



**Figure 2.2 – Example of a Converged Network**
(Hunt, 2011)

This can include both operational communications such as SCADA, video surveillance, protection signalling, advanced metering, as well as enterprise applications (voice over IP, email access, etc.) (Hunt, 2011). A survey conducted by RAD Communications in 2012 has exemplified the trend of utilities moving towards packetised networks. Results of the survey showing that 24% of respondents had already started the migration, a similar number stating they were planning to do so within the next 12-24 months, and 16% over the next 5 years,

showing a total of 64% of surveyed utilities within the industry moving to packet based communications within the next 5 years (RAD Communications, 2012).

Chapter 3

# Internetworking Fundamentals

## 3.1 The OSI Reference Model

The Open Systems Interconnection (OSI) reference model represents a logical way of organising how networks talk to each other so that all hardware and software vendors have an agreed-upon framework to developing networking technologies. The OSI model was created by the International Organisation for Standards (ISO) with the following goals:
Simplify complex procedures into an easy-to-understand structure:

- Allow vendors to interoperate.
- Provide the ability to isolate problems from one layer that may be passed to other areas.
- Allow a modular plug-and-play functionality.
- Provide an independent layer design (Dean, 2003).

The OSI model is represented by the seven layers shown in **Figure 3.1**. The layers can be grouped into two main areas, defined as the upper and lower layers. Although it is possible for a single device to execute all seven layers, generally speaking, this is not practical in real networks. Each layer has its own set of functions and interacts with the layers directly above

and below it. In todays' networks purpose-built devices are designed to handle a single or few layer functions. For example, a router is a purpose-built device for Layer 3 operations. (Hundley, 2009)

| | |
|---|---|
| (7) Application | Upper Layers |
| (6) Presentation | |
| (5) Session | |
| (4) Transport | Lower Layers |
| (3) Network | |
| (2) Data Link | |
| (1) Physical | |

**Figure 3.1 – OSI Reference Model**

The technology being investigated in this project uses the first three (3) layers of the model and a brief description of them is given below.

**Physical Layer –** Protocols at the Physical layer generate and detect voltage (or in the case of fibre optic transmission, pulses of light) so as to transmit and receive signals carrying data. They are responsible for applying raw binary data to the transmission medium. This layer does not include transmission media and connectors, but relies on them. The Physical layer sets the data transmission rate and monitors data error rates, though it does not provide error correction services. It defines both the protocol for flow control and also the establishment and termination of a connection of two directly connected nodes over the physical medium.

**Data Link Layer –** The second layer of the OSI model is the Data Link layer. It is used to control communications between the Network layer and the Physical layer. The primary function of this layer is to divide the received data from the Network layer into distinct frames that can then be transmitted by the Physical layer. A 'frame' is a structured package for moving data that includes not only the raw data, or 'payload', but also the sender's and receiver's network addresses; error checking and control information. While the addresses are used to identify where to deliver the frame, the error checking and control information ensures that the frame arrives without any problems. **Figure 3.2** below shows a simple data frame with essential components that are common to all frame types.

| Destination add. | Source add. | Control Info. | Payload | Error checking info. |
|---|---|---|---|---|

**Figure 3.2 – Simple Data Frame**

To better define shared access for multiple network nodes using the same communications channel the Data Link layer is divided into two sub layers:

- Logical Link Control (LLC) layer – responsible for control error checking and packet synchronization.
- Media Access Control (MAC) layer - responsible for appending the address of the destination computer onto the frame (Halsall, 2002).

These two sublayers will be further discussed in Section 3.2 –Ethernet.

**Network Layer –** The primary function of the Network layer is to translate network addresses into their physical counterparts and decide how to route data from the sender to the receiver. This translation will be described in further detail layer in the next section. Network layer addresses follow a hierarchical address scheme and can be assigned through the operating system software. There are hierarchical because they contain subsets of data that incrementally narrow down the location of a network node. Network layer addresses, therefore are more useful to internetworking devices, such as routers, because they make sorting data more logical (Chappel & Tittel, 2005). Network layer address formats differ depending on which protocols the network uses. Network layer addresses are also called Logical or Virtual addresses.

## 3.2 Ethernet

Ethernet is a standard that sits at the Data Link layer (Layer 2) and is defined in IEEE 802. It is an interconnectivity standard for data communications networks. The standard initially defined the Data-Link control format as well as hardware control format and additionally the data transport format. With the advent of the OSI model the data link and hardware interface formats became layer 2 for Ethernet. The data transport format was encapsulated in Layer 3, CSMA/CD. The standard Ethernet frame format consists of six (6) control fields and also allows a payload of between 46 and 1500 bytes.

An Ethernet MAC address (or Physical address/Data Link address) is a unique 12-digit hexadecimal number that identifies a network node at the Data Link layer. A node's MAC address is integrated into its NIC by the NIC's manufacturer. MAC addresses are divided into two parts. The part of the MAC address that is unique to a particular vendor is called the **Block ID**. Block IDs are 6-digits long and may also be known as Organisationally Unique Identifiers (OUIs) or the vendor codes. The remaining 6-digits of the MAC address form the **Device ID** (Dean, 2003).

## 3.3 Internet Protocol and static routing

Internet Protocol (IP) is a Network layer (Layer 3) protocol defined in RFC 791. IP provides a datagram (connectionless) transport service across a network. IP solves scalability issues encountered in Ethernet. IP has a hierarchical addressing structure….. In order to properly forward packets based on L3 addressing, routers need a way to build a forwarding table of these addresses. With routers this is accomplished through the use of a 'routing protocol' that allows a router to automatically build up entries in the forwarding table for L3 addressing. Routers consult this table when receiving an L3 packet to decide which physical interface to send this data out of. In addition to unique addressing and data forwarding, the network layer can get involved in marking the datagram specific to the application. This is to ensure differential treatment on the outbound packet by intermediate routers. This marking is what allows for different types of network traffic to be prioritised and forwarded differentially by intermediate routers and is a key component of quality of service (QoS) (Lammle, 2013). QoS is an essential function to be used in running teleprotection over a packet network and thus will be discussed in detail in Section 3.5 – QoS.

### 3.3.1 IP Addressing

An IPv4 (IP version 4) address is 32-bits long in binary format. It is normally expressed as four decimal numbers as a simpler representation for humans. This formal is commonly referred to as *dotted-decimal notation*. The dotted-decimal formal divides the 32-bit IP address into four octets of 8 bits each. These octets specify the value of each as a decimal

number. An example of a dotted-decimal IP address and its binary equivalent can be seen below.

Dotted-decimal IP address: 192.168.2.100
Binary equivalent: 11000000.10101000.00000010.01100100

These IP unicast addresses are logically divided into two parts: the network and the host. The first part is the network or network prefix, and identifies the network that a host resides in, The second part of the IP address is the host number, which uniquely identifies the host in the network. To support different network sizes, the unicast portion of the IP address space was originally divided into three classes: Class A, Class B and Class C, known as classful addressing. However this classful addressing is restrictive and largely irrelevant today. Todays' networks generally use classless addressing, where a subnet mask is exclusively used to indicate the size of the IP network. This subnet mask is a 32-bit long sequence of ones and zeros, where the zeros in the sequence correspond to the bits of the IP address that identify the host on that network. The mask is used by the router to derive the network address from a given IP address by using a logical **AND** between the address and the mask. This operation changes the host portion of the address to all zeroes and leaves the network portion intact (Warnock & Nathoo, 2011).

### 3.3.2 IP Forwarding

As a packet travels a network segment each host on the segment evaluates the packet and determines whether the destination MAC address listed in the packet matches its own or is a broadcast to all hosts. The host makes a copy of the packet and sends it along the network path. If the packet is for the local host's MAC address, a broadcast or a multicast for which is host is configured to receive, the packet is passed up the protocol stack.

MAC address checking happens at L2 of the OSI model. If the host decides the packet should be processed, the L2 header is removed and the packet is passed up the protocol stack to L3 (network layer). The destination IP address the packet contains is compared to the local host's. If the IP address listed in the packet matches the local host address the IP header will be removed and the packet passed up the protocol stack again. In the case of a router, the

destination IP address may not match. This is because the packet has been directed to this to be routed further. This concept will now be discussed.

When computers need to send packets to destinations not on their segment, they send the packets to the router (default gateway). The router connected to the segment on which the packet originated recognises the destination host is on a different subnet. The router must determine which subnet should receive the packet. The router will first remove the Data Link header which contains the router's MAC address, since it was addressed to the router. The router then analyses the IP header, more precisely, the destination IP address of the packet. The destination IP address in the IP address of the final destination of the packet and this will not change as the packet traverses the network. Only the MAC address changes. The router will now reference its routing table to determine which of its interfaces is connected to the destination network. Now the router rebuilds the IP header with the appropriate format for the destination network and sends the packet out through the correct interface (Hudson et al. 2003).

## 3.4 Dynamic Routing Protocols

IP routing can be divided into two main categories – static and dynamic. Dynamic routing can then be further divided into the two categories of Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). IGPs are intended for use in a network that is under the control of a single entity or administrative group. This single network entity is usually referred to as an Autonomous System (AS). EGPs are, in contrast, used to provide routes between Autonomous Systems, and as such have special features that allow them to handle later numbers of routes than IGPs (Hundley, 2009). This is project does not require the use of EGP's in its design and hence forth only IGP's will be discussed in further detail.

Additionally to this, there are two types of Dynamic Routing Protocols, that being, Distance Vector and Link-state Protocols. There are both IGP's and EGP's that come under these two headings. The IGP being used in the network design for this project is Open Shortest Path First (OSPF). OSPF is a Link-State Protocol and therefore Distance Vector protocols will not be discussed further.

### 3.4.1 Link-State Routing Protocols

In a link-state routing protocol, each router distributes information about its local topology, with this information including of the destination networks that are directly attached to the router and its links to other routers. When a router has received topology information from all other routers in the network, it has complete topology information about the network and can calculate the shortest path to every destination. This calculation is performed using the SPF (Shortest path first) algorithm, also known as the Dijkstra algorithm (Hundley, 2009).

### 3.4.2 Open Shortest Path First (OSPF)

OSPF is a link-state routing protocol developed in the late 1980s. It was specifically developed for IP routing and was the first routing protocol widely deployed in IP networks that provided a small convergence time of a few seconds with no loops in routing. For improved efficiency and increased scalability, OSPF can support a hierarchy by allowing the definition of different areas (Hundley, 2009).

There are two main versions of OSPF used today, OSPFv2 and OSPFv3. OSPFv3 was created to support IPv6 and is defined in RFC2740. This project however, will be implementing OSPFv2 so OSPFv3 will not be discussed further. The routers used in this project conform to the OSPFv2 specifications presented in RFC2328. The major aspects of OSPF operation are listed below.

1. An OSPF configured router sends Hello messages out every OSPF-enabled interface. Once a router OSPF interface receives a valid Hello, it will proceed to establish adjacencies with any OSPF routers on that network.
2. On a broadcast network, the Hello messages are used to establish a Designated Router (DR) and a Backup Designated Router (BDR).
3. Routers will then exchange Database Description packets, which are essentially an index of all link-state advertisements (LSAs) the router has in its topology database.
4. Based on these packets each router will request the appropriate LSAs it needs to bring its topology database up to date. This request is made via a link-state request (LSR) packet.

5. Upon request, the router will send link-state updates (LSUs) containing the LSAs requested by the neighbor and these LSUs are acknowledged with a link-state acknowledgement.
6. Once LSU exchange is finished the routers are considered to be fully adjacent. These routers will continue to exchange periodic Hello messages to maintain their adjacency.
7. When a topology change condition arises, the affected routers transmit an updated LSA to reflect the change. Every OSPF router updates its link-state database (LSDB), floods the new LSA to its neighbors, and runs SPF to calculate its forwarding database.
8. LSAs age over time in the LSDB and are considered obsolete after 3600 seconds. The originating router will re-flood an LSA after it reaches an age of ~1800 seconds (Warnock & Nathoo, 2011).

## 3.5 Quality of Service

Packetised traffic rarely has a steady rhythm; it can rapidly fluctuate from no traffic at all to high peaks of traffic. It can even peak to a magnitude that prevents the switching or routing node from processing the packets at the same speed with which they arrive. In that case, if no buffers are present, the excess traffic is lost. Therefore, nodes have buffers available, called FIFO: First In First Out. This buffer principle has the significant advantage of not losing as many packets, as without the buffer technology. Its disadvantage is that the packets incur delay while waiting in the buffer.

If only a single buffer or FIFO is present, all traffic will share the same buffer space and can be blocked by the packet in front. However, if the available buffer space is split, for example, into two FIFOs, some traffic can go into one buffer, while the rest of traffic can go into the other. That way, when one buffer experiences obstruction, the second can remain unaffected, and the traffic will experience no resistance of passage. This parallelisation of buffer space is the foundation of Quality of Service (ALU QoS Course Notes, 2012).

A router has two tools to make its purpose possible, its resource memory and processing power. These two tools are limited in their capacity and thus saturation of resources is

possible. This can be the result of an over-subscribed design, when, at a given moment in time and at a certain bottleneck in the network, more traffic is offered than the node can process. Furthermore, the total capacity of the network can also be reduced under network fault and outage conditions which can also produce unforeseen bottlenecks in the network. In a bottleneck situation, the traffic requests more resources than are available, and congestion results in the network. This congestion causes packets to be stored in available memory and, when no more memory is available, they are discarded. There are three possible negative effects of congestion: delay, jitter and packet loss.

Throughput (aka Bandwidth) is the amount of data delivered from one network device to another in a given period to time, and in this case it is generally measured in Kilobits per second. The maximum throughput on a link is referred to as the link's Capacity. Different applications have different bandwidth specifications that they need to function properly; some are bandwidth intensive, and some have variable bandwidth needs, while others require constant (fixed) bandwidth (ALU QoS Course Notes, 2012). Teleprotection signalling schemes transmit very small amounts of data compared to other applications but do require constant (fixed) bandwidth in a system that can provide consistent timing and minimal delay.

Delay is caused by latency in the network, which is the time that it takes for a packet to be stored then forwarded by an intermediate device. There are four main types of delay that, added together, give the total delay of a system. These different types of delay are:

- **Serialisation/transmission** delay is the time is takes to place the bits making up a packet on the wire for transmission out of the router.
- **Queueing** delay is the time that a packet spends at a queueing point before it is processed or forwarded.
- **Processing** delay is the amount of time taken by the router to perform forwarding table lookups, encapsulation and any other packet manipulation required, before sending the packet to the egress port.
- **Propagation** delay is the time it takes for a packet (signal) to travel across a link from one router to another.

Jitter is a measure of variable delay. Packets arrive at a router in fixed intervals and if the processing and queueing delay in the router is fixed, packets will exit the router at the same intervals, thus there will be no jitter. However, if the processing and queueing is variable, packets will exit the router at varying intervals; this variation is called jitter.

Appropriately configured Quality of Service settings will optimise the dispersion of the available limited network resources with a design that protects the traffic types as much as possible from the influences they are most vulnerable. A properly designed network will:

1. Avoid congestion as much as possible (Traffic Engineering)
2. Install a QoS model,
3. Define traffic types and traffic vulnerabilities during congested state,
4. Prioritise different traffic streams,
5. Parallelise the traffic streams into separate FIFOs,
6. Divide the buffer space resources, according to step 4, and
7. Divide the processing power resources, according to step 4.

There are two QoS architecture philosophies, that being, the Integrated Services model (IntServ) and the Differentiated Services model (DiffServ) which are defined in RFC 1633 and RFC 2475 respectively. Using the IntServ model QoS guarantees are provided by a protocol on a per flow basis. Each flow is treated individually and receives the exact treatment it need and is fully automatic. This results in the need for network nodes to maintain, manage and allocate resources for possibly thousands of individual flows, which adds heavy signalling, processing, load storing and complexity in implementation. An individual flow is referred to as a Microflow.

The DiffServ model groups one or more of these Microflows into bigger streams, called Macroflows. This allows different traffic streams to be treated similarly, resulting in a loss of granularity but also a decrease in the load on the network nodes. The model must be implemented at every router in the path. This is called Per Hop Behaviour (PHB) and is the model deployed by most vendors, including the Alcatel-Lucent SAR-7705 routers used in this project. Instead of using a protocol (like IntServ) this model groups packets into a small number of macroflows, or Forwarding Classes (FC). There are eight (8) FCs and **Figure 3.3** below defines each of these and for what they should be used for. Every packet must be

mapped or classified into one of these Forwarding Classes to receive the treatment specified for the FC. To assure consistent processing of traffic throughout the network a coherent QoS policy arrangement should be configured at every node in the network.

| Default Class Type | FC ID | FC Name | FC Designation | Definition |
|---|---|---|---|---|
| High Priority (Premium) | 7 | Network Control | NC | Intended for network control traffic. |
| | 6 | High-1 | H1 | Intended for network control traffic or delay/jitter sensitive traffic. |
| | 5 | Expedited | EF | Intended for delay/jitter sensitive traffic. |
| | 4 | High-2 | H2 | |
| Assured | 3 | Low-1 | L1 | Intended for assured traffic. Also the default priority for network management traffic. |
| | 2 | Assured | AF | Intended for assured traffic. |
| Best Effort | 1 | Low-2 | L2 | Intended for best effort traffic. |
| | 0 | Best Effort | BE | |

**Figure 3.3 – Forwarding Classes (for ALU SAR routers)**
(ALU QoS Course notes, 2013)

There are multiple QoS policies that must be configured at different locations within the router to ensure consistent handling of the traffic from ingress to egress of the traffic at a router. These different QoS policies are described below.

- **QoS Service Ingress Policy** – The QoS Service ingress policy defines how traffic arriving at a SAP is to be classified and queued before being forwarded to the fabric.
- **QoS Service Egress Policy** – The QoS Service egress policy defines how traffic is to be serviced as it exits a service, before it is forwarded to a SAP.
- **Network Policy** – The Network policy defines how traffic arriving is to be classified, based on its marking, and defines how traffic is to be marked before exiting.
- **Network Queue Policy** – The Network queue policy defines the queue and its associated parameters at network ports, and defines the mapping of traffic ingressing and egressing network ports to specific queues (ALU QoS Course Notes, 2012).
- **Slope policy** – The slope policy defines default buffer allocations and WRED slope definitions.
- **Scheduler policy** – The scheduler policy is used to configure hierarchical virtual schedulers (H-QoS).

The three policies to be used in the design of the circuit are the Service Ingress, Network and Network Queue policies.

## 3.6 Multiprotocol Label Switching

MPLS originated as IP switching or tag switching with the intent of simplifying the process of forwarding packets from the complex IP forwarding mechanism. However as technology progressed, hardware was developed that could perform IP forwarding at line rates. MPLS then evolved into a method for forwarding packets independently of their content. This made it ideal as a base for implementing VPN technology. MPLS is considered a tunnelling technology and the data being carried through the tunnel could be in any form: an IP datagram, an Ethernet frame, or TDM traffic, for example (Hundley, 2009)

MPLS enables the forwarding of traffic based on a simple label, which is embedded in the packet header. The term *multiprotocol* comes from its ability to transport any type of packet payload across any Layer 2 network protocol using a simple label switching approach. RFC 3031 describes the Multiprotocol Label Switching (MPLS) architecture. Creating tunnels across an IP network with MPLS resolves some limitations of IP routing while also providing a simple base for adding new services.

### 3.6.1 Forwarding Equivalence Class (FEC)

A Forwarding Equivalence Class (FEC) is a group of IP packets forwarded in the same manner, over the same path with the same forwarding treatment. In IP-only networks, FECs will generally correspond to an IP prefix in the route table. This means in conventional routing that a FEC lookup is done at each hop. However, in MPLS routing a FEC lookup is only done at the ingress router of the MPLS network. The FEC lookup performed will determine the next-hop and the label the source router pushes onto the packet. This now means that routers inside the MPLS network will now simply perform ‘swap’ operations based on the previously determined label values. In should also be noted that in MPLS, FECs can be both defined on destination IP prefixes (like in conventional routing) and other administrative criteria (ALU MPLS Course notes, 2012).

### 3.6.2 MPLS basics

The basics of MPLS operation can be seen below in **Figure 3.3**. A label header is a fixed length entity the router inserts into the packets as they enter the MPLS-enabled network. The initial label being attached to the packet is referred to as a 'Push' function. When the packet arrives at its next-hop, this router simply checks the incoming label against its Label Forwarding Database and changes the label and passes the packet onto its next-hop. This process is called a 'Swap'. When the packet reached the last MPLS-enabled router, this router strips the label and routes this packet according to its IGP preference. The path through which the packet traverses the MPLS network is called an LSP (Label Switch Path). An LSP is a logical entity that represents the MPLS connection through a MPLS network (Warnock & Nathoo, 2011). This is also commonly called a transport tunnel.

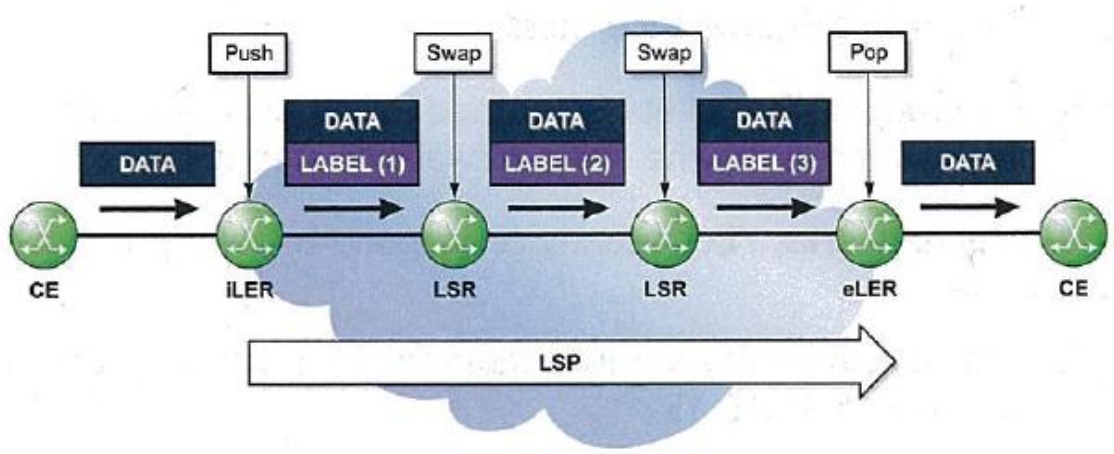



**Figure 3.4 – Simplified MPLS Operation**
(ALU MPLS Course notes, 2013)

MPLS headers are inserted between the Layer 2 of the network interface and the encapsulated MPLS payload. As such, MPLS is often known as a Layer 2.5 protocol because the label is inserted between the Layer 2 and Layer 3 headers. A MPLS label stack can be formed by encapsulating labels with other labels. Each layer provides a specific function on the network. A simple example of this is outlined above in **Figure 3.4**.

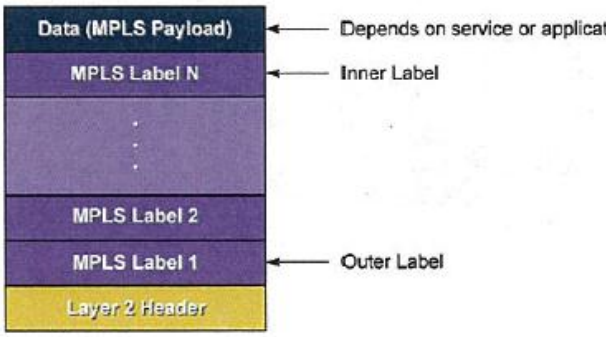



**Figure 3.5 – MPLS header stack**
(ALU MPLS Course notes, 2013)

The transport tunnel can multiplex and transport several service tunnels (See **Figure 3.5** below). Intermediate routers will only be aware of the transport tunnel, not the services running within it. This means these routers only look at the outmost label to make their forwarding decisions.

This improves both network performance and scalability. In the above diagram it can be seen that R2 will only be 'swapping' the transport label while when the packet reaches R3, both the transport and service labels are 'popped' (ALU MPLS Course notes, 2013).

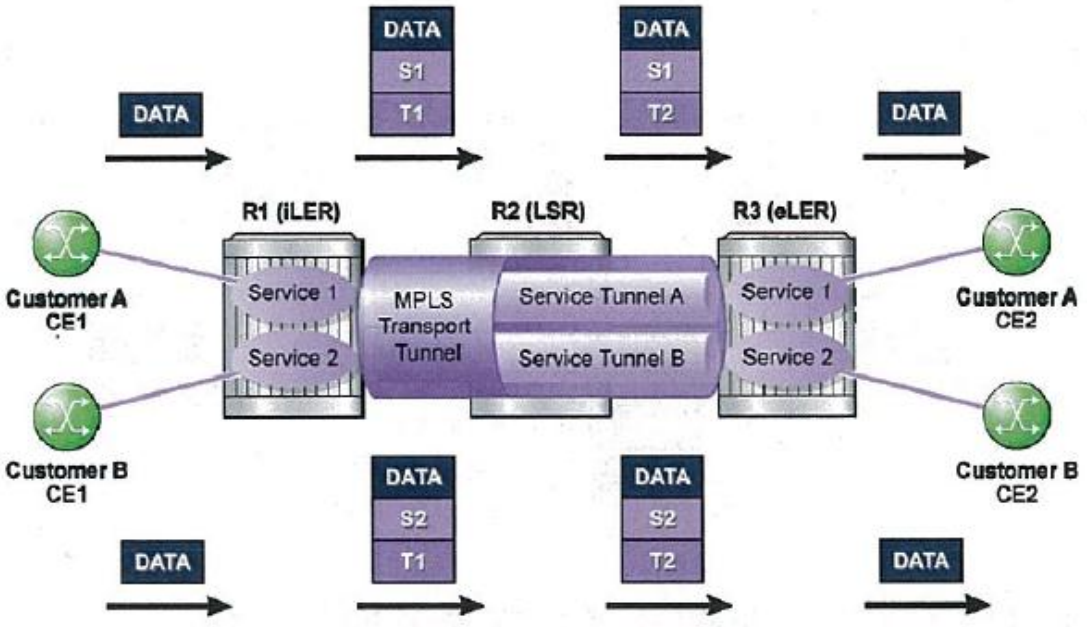



**Figure 3.6 – MPLS tunnelling**
(ALU MPLS Course notes, 2013)

### 3.6.3 Label Distribution Protocol

RFC 5036 defines LDP as an MPLS label distribution protocol. A router with LDP enabled will establish sessions with other LDP-enabled routers. This LDP session allows these routers to exchange label/FEC binding information. LDP was introduced to carry label binding information for FECs, regardless of the routing protocol used in the network. There are two types of LDP, that being;

- Link LDP; and,
- Targeted LDP.

Link LDP is used for establishing transport tunnels while Targeted LDP is used in establishing service tunnels for Layer 2 services, such as Virtual Leased Line (VLL) and Virtual Private LAN Service (VPLS) (Hundley, 2009). A VLL is a point-to-point Layer 2 service which will be used to transport the teleprotection traffic and will be covered in further detail in Section 3.7. LDP relies on the underlying IGP (OSPF, for the purpose of this project) to establish the sessions, obtain FEC information and maintain the tunnels.

### 3.6.4 Targeted-LDP

'RFC 4447 – Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)' describes how service labels are signalled using Targeted-LDP (T-LDP). T-LDP is the same protocol as Link LDP, used for signalling transport tunnels, discussed above (Section 3.6.3) with a few additional capabilities added. VLL and VPLS both use T-LDP to signal service labels.

Although MPLS tunnels are used to carry the data, the IGP is still required to help establish the transport tunnels and to allow T-LDP peer to communicate with each other. Once T-LDP has signalled service labels and a transport tunnel has been created between the endpoints RFC 4447 defines that a 'pseudowire' has been created. A pseudowire is an emulated, L2 circuit built across an MPLS network than can transport L2 data as if it were being transmitted on its native media. A Circuit Emulated Service (Cpipe) is an example of a pseudowire technology and is the technology used for the service in this project.

The main difference between link LDP and T-LDP is that T-LDP is used for exchanging service label information and the T-LDP peers do not need be directly connected. Because of this, a router must know the IP address of its T-LDP peer. It should be noted that LDP must first be enabled to configure a VLL or VPLS service so that T-LDP can signal the service labels, even if RSVP-TE is being used for signalling the transport labels (Warnock & Nathoo, 2011).

### 3.6.5 Resource Reservation Protocol – Traffic Engineering

Resource Reservation Protocol (RSVP), specified in RFC 2205, was originally developed as a network control protocol that a host would use to request specific qualities of service from

the network for particular application data streams or flows. Additionally to this, RSVP has been used by routers to deliver quality of service (QoS) requests to all nodes along the paths of the flows, and to establish and maintain a state that provides the requested service. IN RFC 3209, RSVP was enhanced to RSVP-TE (Resource Reservation Protocol – Traffic Engineering) for use with MPLS. When configured for this purpose, RSVP leverages this mechanism to set up traffic engineered LSPs (Warnock & Nathoo, 2011). This traffic engineering ability is essential in the use of MPLS with teleprotection schemes. This is due to the time-sensitive nature of these schemes and strict latency requirements.

RSVP is not a routing protocol as it operates with unicast and multicast routing protocols that determine where packets are forwarded. RSVP will in fact consult local routing tables to relay its messages. It requests resources and a label for a unidirectional flow; that is, it requests resources only in one direction.

RSVP-TE is a protocol used in signalling and establishing transport tunnels that can be used as an alternative to link LDP. RSVP-TE bring major benefits to MPLS which standard link LDP cannot provide including;

- The ability to administratively define LSPs,
- The ability to make advanced path calculations, that are not restricted to IGP cost values,
- The use of traffic protection features (secondary paths, Fast Reroute) and,
- The ability to make resource reservations.

RSVP-TE uses two message types to set up an LSP – the Path and Resv messages. The head end sends a Path message toward the tail end indicating the FEC for which a label binding is desired and any resource requirements. Each router along the path verifies that it can provide the resources requested and sends the Path message to the next downstream router.

The tail end router send label binding information in a Resv message in response to the received Path message. The Resv message is sent back along the same LSP path of the Path message. Now, each router makes the necessary resource reservations and provides a label binding to the upstream router. The LSP becomes operational when the head end receives the

label binding information for the FEC, via the Resv message. At this point, every router along the LSP path has received a label and made a bandwidth reservation for the FEC (Warnock & Nathoo, 2011).

## 3.7 Virtual Private Wired Services

Virtual private wired services (VPWS) define a virtual point-to-point service that emulates a private leased line connection. VPWS is also commonly referred to as a Virtual Lease Line (VLL) service. There are various types of VPWS that Alcatel-Lucent routers supports which include:

- Epipe – Emulates a point-to-point Ethernet service.
- Cpipe – Emulates a point-to-point TDM circuit.
- Apipe – Emulates a point-to-point Asynchronous Transfer Mode (ATM) Service.
- Fpipe – Emulates a point-to-point Frame Relay circuit.
- Ipipe – Provides IP networking capabilities between different L2 technologies (ALU Services Architecture Course Notes, 2013)

This project will make use of the Epipe and the Cpipe services and these two service types will be discussed further.

### 3.7.1 Service Access Point (SAP)

A service access point (SAP) is the point at which a service begins (ingress) or ends (egress) and represents the access point associated with a service. This is shown below in **Figure 3.4**. A SAP may be a physical port or a logical entity within a physical port. For example, a SAP may be a channel group within a DS1 or E1 frame, an ATM endpoint, an Ethernet port, or a VLAN that is identified by an Ethernet port and a VLAN tag. Each service connection on the 7705 SAR is configured to use only one SAP. A SAP identifies the interface point for a service on the router. Access to each of the aforementioned services is given via SAPs. For each service type, the SAP has slightly different parameters. SAPs are logical endpoints that are local to the router and are uniquely identified by:

- the physical Ethernet port, SONET/SDH port, or TDM channel group

- the encapsulation type for the service (for example, ATM)
- the encapsulation identifier (ID)

**SAP Encapsulation Types and Identifiers**

The SAP encapsulation type is an access property of the Ethernet port, SONET/SDH port, or TDM channel group used for the service. It identifies the protocol that is used to provide the service. The 7705 SAR supports three SAP encapsulation types: Ethernet, SONET/SDH, and TDM. Encapsulation types may have more than one option to choose from. For example, the options for TDM encapsulation type are “cem” (for circuit emulation service) and “atm” (for ATM service) (ALU 7705 SAR: Services Guide, 2013).

### 3.7.2 Service Distribution Point (SDP)

The transport tunnel for a service is represented by the SDP seen below in **Figure 3.4**.

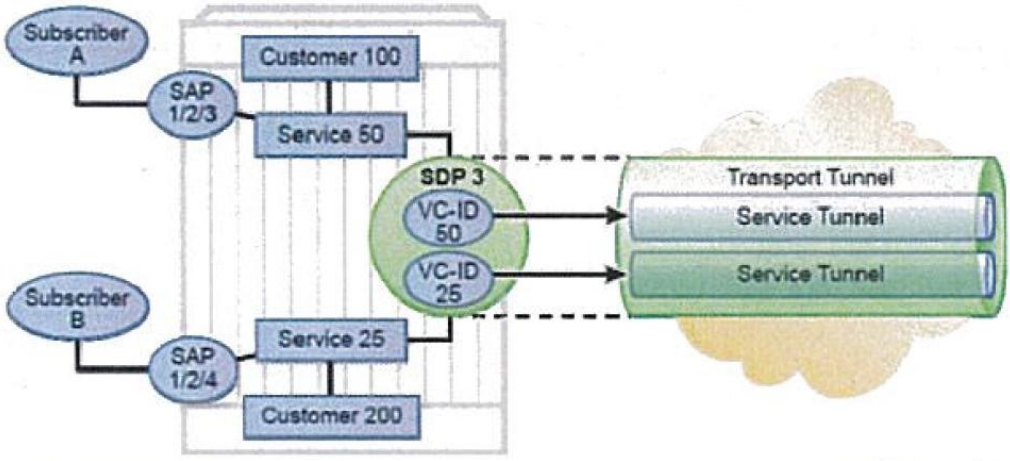



**Figure 3.7 – Service Configuration**
(ALU Services Architecture Course Notes, 2013)

Key characteristics of the SDP include:

- Multiple services of different service types can use the same SDP for transport.
- The SDP defines the encapsulation type to be used for the transport of the service data.
- The SDP ID is locally unique to the router. Other routers can use the same SDP ID.
- An SDP uses the system IP address to identify the far-end service router. A T-LDP session is established with the far-end router for Layer 2 services (Warnock & Nathoo, 2011)

### 3.7.3 Circuit Emulation VLL Service (Cpipe)

A Cpipe service is the Alcatel-Lucent implementation of TDM PW VLL as defined in the IETF PWE3 working group. The 7705 SAR used in this project can support TDM circuit applications that are able to transport delay sensitive TDM traffic over a packet network. There are two categories of Cpipes:

- **Structure agnostic** - SAToP (Structure Agnostic TDM over Packet) pseudowires are defined in RFC 4553 with their purpose being to transport unstructured T1 or E1 circuits.
- **Structure aware** – CESoPSN (Circuit Emulation Service over Packet Switched Network) pseudowires are defined in RFC 5086 and transport multiple DS0 channels from a T1 or E1 circuit (ALU 7705 SAR OS – Release 6.0.R4: Services Guide).

This project will be using the CESoPSN implementation of the Cpipe. Two important configurable parameters for Cpipe services include the jitter buffer and the payload size.

**Jitter Buffer**

The jitter buffer is required because a Cpipe runs over a PSN that may variable delay. However, the receiving TDM circuit is synchronous and must receive data at a constant rate. Packets received from the PSN are queued depending on the size of the buffer and then played out at a regular rate to the TDM circuit.

A properly configured jitter buffer will provide continuous play-out, thus it will, avoid discards due to both overruns and underruns. A larger jitter buffer and larger payload size provide the most efficient transfer and the least chance of losing data. However, this increased reliability comes at the cost of increased delay. For delay-sensitive services (such as teleprotection signalling) jitter buffer and payload size should be kept as small as possible to minimise delay while not affecting reliability of the service (Warnock & Nathoo, 2013).

The maximum receive jitter buffer size is configurable for each SAP configured for circuit emulation. The range of values is from 1 to 250 ms in increments of 1 ms.

Configuration/design Considerations

To determine the optimum configuration value for the jitter buffer some adjustments may be required to account for the specific network requirements, which can change PDV as nodes are added or removed.

For each circuit, the maximum receive jitter buffer is configurable. In order to give an operational PDV equal to half the maximum buffer size Play-out from this buffer must start when the buffer is 50% full. The buffer size must be set to at least 3 times the packetisation delay and no greater than 32 times the packetisation delay. Use a buffer size (in ms) that is equal to or greater than the peak-to-peak PDV expected in the network used by circuit emulation service. For example, for a PDV of ±5 ms, configure the jitter buffer to be at least 10 ms. (ALU 7705 SAR OS – Release 6.0.R4: Services Guide, 2013).

**Packet Payload Size**

The packet payload size defines the number of octets contained in the payload of a TDM PW packet when the packet is transmitted. Each DS0 (timeslot) in a DS1 or E1 frame contributes 1 octet to the payload, and the total number of octets contributed per frame depends on the number of timeslots in the channel group (for example, 10 timeslots contribute 10 octets per frame).

**Packetisation delay**

Packetisation delay can be described as the time needed to collect the payload for a CESoPSN packet. DS1 and E1 frames arrive at a rate of 8000 frames per second. Therefore, the received frame arrival period is 125 μs.

An example is given below:

Payload size = 16, ie. 16 frames were accumulated in the CESoPSN packet.

The packetization delay (D) can be calculated as follows:

D = 125 μs/frame × 16 frames

= 2.000 ms

The table exert below shows default and minimum payload size values.

| | Default Values | | | Minimum Values | | |
|---|---|---|---|---|---|---|
| **Number of Timeslots (N)** | **Frames per Packet (F)** | **Payload Size (Octets) (S)** | **Packetisation Delay (ms) (D)** | **Frames per Packet (F)** | **Payload Size (Octets) (S)** | **Packetisation Delay (ms) (D)** |
| 1 | 64 | 64 | 8.000 | 2 | 2 | 0.250 |
| 2 | 32 | 64 | 4.000 | 2 | 4 | 0.250 |
| 3 | 32 | 96 | 4.000 | 2 | 6 | 0.250 |
| 4 | 32 | 128 | 4.000 | 2 | 8 | 0.250 |
| 5 | 16 | 80 | 2.000 | 2 | 10 | 0.250 |
| …… | ……. | …… | …… | …… | …… | ….. |
| …… | …… | …… | …… | …… | …… | …… |
| 28 | 8 | 224 | 1 | 2 | 56 | 0.250 |
| 29 | 8 | 232 | 1 | 2 | 58 | 0.250 |
| 30 | 8 | 240 | 1 | 2 | 60 | 0.250 |
| 31 | 8 | 248 | 1 | 2 | 62 | 0.250 |

**Table 3.1 – Default and Minimum Payload Size for CESoPSN**
(ALU 7705 SAR: Services Guide, 2013)

### 3.7.4 Ethernet VLL service (Epipe)

An Ethernet pseudowire (PW) is used to carry Ethernet/802.3 protocol data units (PDUs) over an MPLS or IP network, allowing emulated Ethernet services over existing MPLS or IP networks. An MPLS Epipe service is the Alcatel-Lucent implementation of an Ethernet VLL based on the IETF RFC 4448, Encapsulation Methods for Transport of Ethernet over MPLS Networks. An Epipe service is a Layer 2 point-to-point service where the service data is encapsulated and transported across a MPLS or IP network. An Epipe service is completely transparent to the subscriber's data and protocols. Like other PW VLL services, Epipe service behaves like a non-learning Ethernet bridge.

During the laboratory this project will use an Epipe service in conjunction with an Ethernet tester to simulate real traffic over the MPLS network while testing the Cpipe (teleprotection) service.

## 3.8 IP/MPLS and the Requirements of Protection Signalling

The IEC standard 60834 defines the criteria for measuring teleprotection performance, and as outlined in Section 2.1 (for protection systems); these include transmission speed (latency), dependability (the ability to ensure communications) and security (prevention of false trips). Regardless of whether the packetised network is used to convey conventional protection signalling or next-generation signalling (such as messages defined in IEC 61850) it must perform to a level that meets these requirements. CIGRE defines QoS (Quality of Service) as "the ability to guarantee a certain level of performance to a user data flow and hance meeting the network user's requirements". In the terms of protection signalling, the user is the protection engineering group, and QoS is the networks ability to ensure latency, dependability and security (Alcatel-Lucent – Deploying IP/MPLS Comms, 2012).

In addition to the transmission delay associated with both TDM and Packetised networks (generally 2-3 μs/km for fibre optics) there are a number of delays introduced through the use of packetised networks. One of the major issues faced when implementing PSNs in the utility environment is the variance in delays i.e. unlike TDM networks where latency is deterministic, the latency in traditional PSNs is difficult to calculate. Typical causes for latencies in PSNs include a packetisation delay (for non-Ethernet traffic), network delay based on number of hops, switch delay, distance and link speeds, traffic congestion and configuration of the jitter buffer. The total end-to-end delay is comprised of the network latency and the Teleprotection equipment activation time (the time a device takes to react to the presentation of a protection signal) (CIGRE – Line and System Protection using digital Circuit and Packet Communications, 2012). It goes without saying that the use of Ethernet packets natively in the communications system reduces latency; this is where the use of emerging standards like IEC 61850 gains an advantage over conventional systems where typical interfaces such as G.703 and C37.94 must be packetised.

IP/MPLS networks utilize virtualization extensively in normal operation to ensure performance requirements are met for each service on the shared infrastructure (fibre optic cable or Ethernet). IP/MPLS utilizes VPLS (Virtual Private LAN services) and VPNs (Virtual Private Networks extensively) to create virtualised point-to-point connections at

either layer 2 (VPLS) or layer 3 (VPN). The use of VPLS allows remote IEDs to be virtualized into the same LAN segment, whereas VPNs allows remote IEDs to be virtualized into the same network. These virtualization services within IP/MPLS networks can be used to realise messaging defined throughout IEC 61850 over multipoint Ethernet connections giving the communications network a great deal of longevity (Alcatel-Lucent – Deploying IP/MPLS Comms, 2012).

In addition to establishing virtual LAN segments over the network, VLANs can be priority tagged to enhance QoS. These priority tags allow 8 levels of priority, each joining a different queue to be processed with discrimination, with higher priority traffic processed prior to lower priority traffic. In the case of protection signalling, traffic would be the only service given the highest priority in an effort to ensure minimal latencies (CIGRE – Line and System Protection using digital Circuit and Packet Communications, 2012). Colenso van Wyk (2011) states Teleprotection should be set at queue 7 (h1).

In addition to end-to-end Latencies, asymmetric delays or the discrepancy between latencies present on transmit and receive paths (described by the term ‘asymmetric path jitter’) is a major factor when differential or other comparative schemes are considered. Due to the nature of these schemes, where real-time values are compared, latencies must be symmetrical between transmit and receive paths. Protection relays in service today are capable of operating despite a range of latency discrepancies, although typical values are approximately 200μs (Levrau, 2011). PSNs are inherently prone to variance between latencies; as such MPLS networks utilize a number of mechanisms to reduce jitter including the jitter buffer (a buffer that controls transmission times), QoS and MPLS path definitions. As dependability is a key performance criterion, the ability to maintain communications given a failure of the communications network is paramount. IP/MPLS networks use the Fast Re-Route (FRR) mechanism to create a back-up path between network devices. In this instance, re-routing can be achieved in less than 50ms in line with requirements currently in place in TDM communications networks (CIGRE – Line and System Protection using digital Circuit and Packet Communications, 2012).

Overall, MPLS has various built-in mechanisms that allow it to be implemented in protection systems. Despite the theoretical capabilities, and proven test results utilities are still hesitant to implement protection signalling over packetised networks. This project will further

investigate and examine some of the complexities surrounding the use of an IP/MPLS network in protection signalling including asymmetric path latency and robustness under network fault conditions.

## 3.9 Packetised Communications Networks For Utility Communications

As previously stated, in a survey conducted by RAD Communications, close to 50% of respondents had either already started the migration to packetised communications or were going to within the next 24 months. Companies in this position must be fully aware of the functional difference between PSNs and legacy networks and their relevant performance limitations. The key difference between conventional TDM based communications networks and packet based networks is the use of the OSI (Open Systems Interconnection) model which appears as the 7 layer stack discussed in earlier in Section 3.1. The stack allows a logical transfer of data from the application (i.e. the protection device functional logic) to the physical medium being Ethernet (over copper or fibre in the packetised environment). As data packets (a formatted unit of data) are generated and moved down the stack, a number of headers may be added at each layer to facilitate various functions ranging from connection between remote and local functions, dependability enhancements (through transport protocols) to routing between devices (seen in the network layer e.g. IP or Internet Protocol). These headers aren't present in every instance of communications within a PSN, depending on the format and technologies used to implement them. The varying approaches taken in implementing Packetised networks present vastly different results regarding performance and capability to support time-critical applications. CIGRE (the International Council on Large Electric Systems) present various implementations of packetised networks including (CIGRE – Line and System Protection using digital Circuit and Packet Communications, 2012):

- **L2 Networks (switched Ethernet and direct Ethernet)**: Low level Ethernet (or Layer 2) networks can be implemented between devices called switches (in switched networks) or directly between Ethernet interfaces. Switched networks can use hardware addresses to direct traffic, whereas direct. Ethernet is a direct Ethernet connection between two devices (e.g. direct fibre protection signalling). In either case, L2 networks are used to create LANs (Local Area Networks), and typically would not

be used for communications between sites as large, widespread LANs are a performance and management impracticality.

- **Ethernet over TDM**: the transmission of Ethernet packets of a time domain multiplexed channel is possible, and many utilities are in fact taking this approach to migration to packetised networks. The nature of TDM channels are that there is a dedicated amount of bandwidth, giving the application a dedicated communications channel with high predictability (as seen in dedicated fibre etc.) but also providing the benefits of shared resources (as it is multiplexed). This approach presents a number of shortcomings in comparison to native Ethernet networks, in terms of scalability and decline of mainstream support which may lead to obsolescence, as seen in the case of PDH (CIGRE – Line and System Protection using digital Circuit and Packet Communications, 2012).

- **IP/MPLS**: Is a set of tools and mechanisms allowing a packetised network (connectionless, end-to-end network) to be transformed into a point-to-point, connection orientated network wherein packets are a directed based on a label header rather than network addresses. The use of the 20bit label rather than a network address allows MPLS to operate between layers 2 and 3 allowing it to operate directly on Ethernet traffic and over routers in the packet based network supporting traffic in both LANs and WANs. MPLS includes a set of tools that allow traffic shaping and engineering (ensuring quality of service is maintained) and guaranteed bandwidth for services through reservation protocols (Alcatel-Lucent – Deploying IP/MPLS Comms, 2012). CIGRE have noted that several investigated have demonstrated that an MPLS based network utilizing the above characteristic can be engineering in such a way as to meet the stringent requirements imposed in protection systems.

- **MPLS-TP**: MPLS-TP (Transfer Protocol) is an expansion of the ‘traditional’ MPLS standards that intend on more closely resembling the performance characteristics presented by existing TDM transport technologies such as SDH and PDH. Whilst MPLS-TP is a relatively new technology with standard specifications still underway, there are a number of differences from tradition MPLS that make MPLSTP a very promising PSN technology that will be compatible with already established MPLS

networks including; not relying on IP addressing, TDM-like OAM (Operation, Administration and Maintenance) and Bi-directional Path Switching as opposed to standard MPLS which supports the Fast Re-Route protocol. MPLS-TP also has the added advantage of being compatible with existing implementations of IP/MPLS networks, allowing the lifetime of packetised networks to be expanded.

One of the benefits of a well-engineered Packet network is the support it can grant to existing legacy applications. For example, in **Figure 1.1**, the transmission medium can be supporting any packetised technology and still support the protection signal in a wide range of traditional formats. A major advantage in using an Ethernet/IP/MPLS based PSN is the ability to transport legacy signals such as E1, T1 (TDM services) or fractional nx64kbps signals. These TDM services are transmitted through the Ethernet/IP network through the use of 'pseudowires' or virtual tunnels between two network elements (teleprotection over packet). It is worth noting that whilst the use of packetised communications networks in the utility environment has had a profound impact on the communications field, the critical nature of protection systems within the utility environment has meant that the majority of development has been in the use of packetised networks meeting the existing TDM performance levels making them suitable to replace legacy communications technologies.

Further to this, the movement towards the use of packetised networks will allow utilities to adopt next generation automation standards (e.g. IEC 61850) with greater fluency through increased bandwidth and native support for Ethernet packet based communications.

Chapter 4

# Requirements analysis

## 4.1 System Purpose

The purpose of the system is to provide a more cost-effective solution to protection schemes running obsolescent hardware. While the medium-term goal of the industry is to move to entirely IEC 61850 communications, legacy relays will still exist for many years to come. For companies to be ready for an IEC 61850 rollout a fully deployed IP/MPLS network will be necessary and it can be seen that various companies worldwide are readying themselves in this way. However, in the short-term for these companies, this means maintaining their existing TDM network (which runs current teleprotection schemes) and IP/MPLS network. This could be seen as a costly business outcome which can be minimised by the migration of and decommissioning of TDM networks.

The system being designed in this project seeks to migrate existing teleprotection schemes running over a TDM network onto a meshed IP/MPLS network. The system will need to operate within the same tolerances as the current TDM technology does and perform at a similar or better standard.

## 4.2 System Scope

A system scope has been prepared to provide focus on what the delivered testing results mean to the industry. This scope encompasses and defines all hardware and testing process that are used in the system scope into an In-scope and Out-of-scope layout.

### 4.2.1 In-Scope

The project investigates only a narrow scope of scenarios within the entire range of protection hardware and standards across the industry. However, in depth testing and analysis will be performed on the in-scope system outlined below.

**System**

| **Hardware** | **Communication Standard** | **Protection scheme type** | **Timing Alignment of current vectors** |
|---|---|---|---|
| • Areva P541 protection relays<br>• Alcatel-Lucent 7705 SAR-8<br>• Alcatel-Lucent Teleprotection card | IEEE C37.94 | Current Differential | Without GPS input |

**Testing**

- Jitter and latency characteristic testing using various IP/MPLS network configurations
- Customisation of circuit QoS settings
- Traffic engineering impact characterisation
- ALU 7705 SAR-8 failure cases

### 4.2.2 Out-of-Scope

The narrow scope of the project means there is a large cross-section of system hardware and differential system parameters that are out-of-scope for the project. The out-of-scope items include, but are not limited to:

**System**

| **Hardware** | **Communication Standard** | **Protection scheme type** | **Timing Alignment of current vectors** |
|---|---|---|---|
| • Relays offerings from different vendors<br>• Network equipment offerings from different vendors<br>• Other Areva protection relays | • SEL Mirror Bit<br>• Native G.703 | • Overcurrent and earth fault<br>• Distance | With GPS input |

**Testing**

- Accurate measurement and analysis and one-way delay

## 4.3 Project objectives and success criteria

The primary objective of the project is to provide proof of concept for a teleprotection-over-MPLS circuit. Upon this being achieved the project seeks to conduct in-depth testing and analysis on the above in-scope testing items.

The success of the project, in broad terms, will be highly dependent on the systems' ability to work within the requirements outlined below.

## 4.4 General System Requirements

### 4.4.1 Major System Capabilities

The proposed teleprotection circuit to be designed and configured will operate in parallel to an existing energised current differential circuit running over a TDM network. This existing circuit operates using PDH architecture and, once the proposed circuit is tested, results

between the two (2) circuits will be compared. The requirements of the results comparison state that the IP/MPLS teleprotection system must;

- Meet or reduce latency times of current TDM circuit,
- Meet or reduce circuit jitter parameters of the current TDM circuit,
- Meet or exceed circuit stability results of the current TDM circuit, and
- Meet or reduce relay operation time under in-zone protection testing scenarios.

Furthermore, the proposed system must also meet standard performance criteria which would include:

- Relays do not perform mal-operations during fault conditions on the communications network,
- Circuit must maintain stability under various load and fault event conditions, and
- Circuit responds to fault events correctly

## 4.5 Rules and Standards Requirements

### 4.5.1 Rules requirements

The '**National Electricity Rules (NER) – Version 64: S5.1a.8 Fault clearance times**' references the following table which outlines requirements for clearing faults at different points of the electricity network and at different voltages. This is shown below in **Table 4.1**.

It should be noted that the NER allows for an 8 hour reduction in network security where these requirements are not meet. This is to cover emergency or planned outages of protection and communications equipment.

| | Time (milliseconds) | | |
|---|---|---|---|
| Nominal Voltage at fault location (kV) | Primary protection within a substation, connected to plant or on the first half of a power line | Primary protection within the remote half of the power line | Backup or circuit breaker fail protection |
| 400kV and above | 80 | 100 | 175 |
| At least 250kV but less than 400kV | 100 | 120 | 250 |
| more than 100kV but less than 250kV | 120 | 220 | 430 |
| Less than or equal 100kV | As necessary to prevent *plant* damage and meet stability requirements | | |

**Table 4.1 – NER Fault clearance times**
(National Electricity Rules, p.501)

### 4.5.2 Standards Requirements

'IEC-60834-2 **Performance and testing of teleprotection equipment of power systems – Part 2: Analogue comparison schemes**' outlines basic system requirements for the 'In-scope' current differential scheme to be tested. **Figure 4.1** from the IEC 60834 standard shows typical operating times for analog comparison protection systems.

The two (2) primary timing requirements that are applicable to this project are the $T_A$ and $T_B$ figures.

Protection operating time ($T_B$): 2.0 – 60ms
Teleprotection operating time ($T_A$): 1.0ms – 10ms

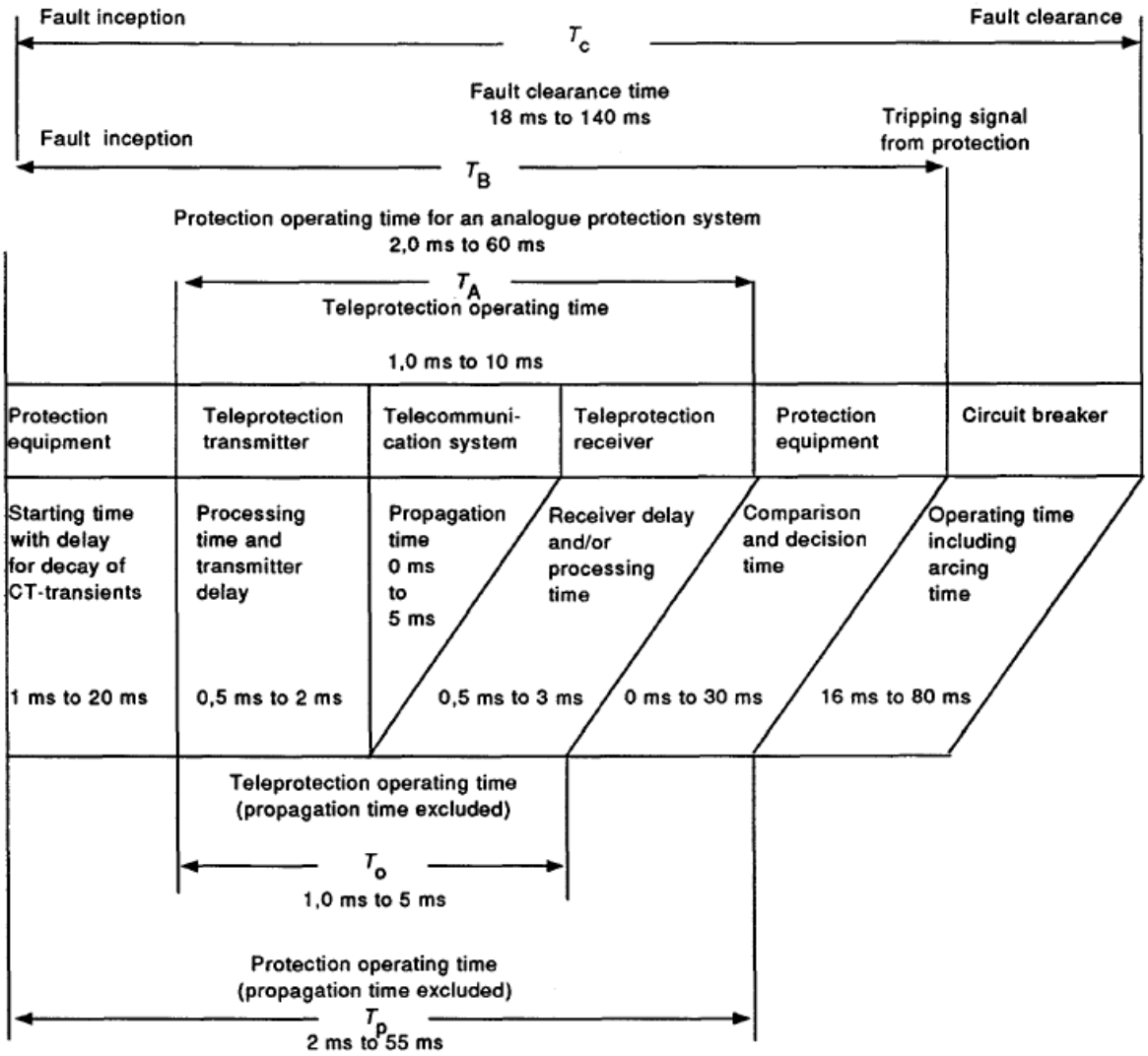



**Figure 4.1 – Typical operating times for analogue comparison protection systems**
(IEC-60834-2, p.55)

Chapter 5

# Conceptual Design

## 5.1 Design Overview

The proposed system seeks to deliver C37.94 protection traffic, which currently runs through a TDM network, using IP/MPLS as the telecommunications infrastructure. The protection relay will transmit its C37.94 traffic to a C37.94 teleprotection interface on the Alcatel-Lucent Voice & Teleprotection Card. This is card installed directly into the 7705 SAR-8 router chassis and from this point the traffic will traverse the IP/MPLS network to the remote end router. It can be seen from **Figure 5.2** below that primary and secondary LSP paths will be designated. These traffic engineering paths will be made possible by the use of RSVP-TE for transport tunnels and the T-LDP protocol for service tunnels.

## 5.2 Current System

The current teleprotection scheme that this project examines, communicates over a TDM network running PDH architecture. The C37.94 traffic is initially transmitted from the protection relay to the C37.94 optical data interface card. This interface card connects directly to the 2Mbit/s internal bus of the DM2 Primary Multiplexing chassis. The DF2-8 line interface card is also connected to the DM2 and is used for transmission of the signal across

the TDM network inside an E1 frame. The corresponding DF2-8 card at the remote end of the signalling scheme receives this traffic. As seen in **Figure 5.1** below, the remote end is an identical setup to the local end and the traffic is transmitted through the equipment to the protection relay. Alternatively, a DB2 branching card can replace the DF2-8 line interface card if required.

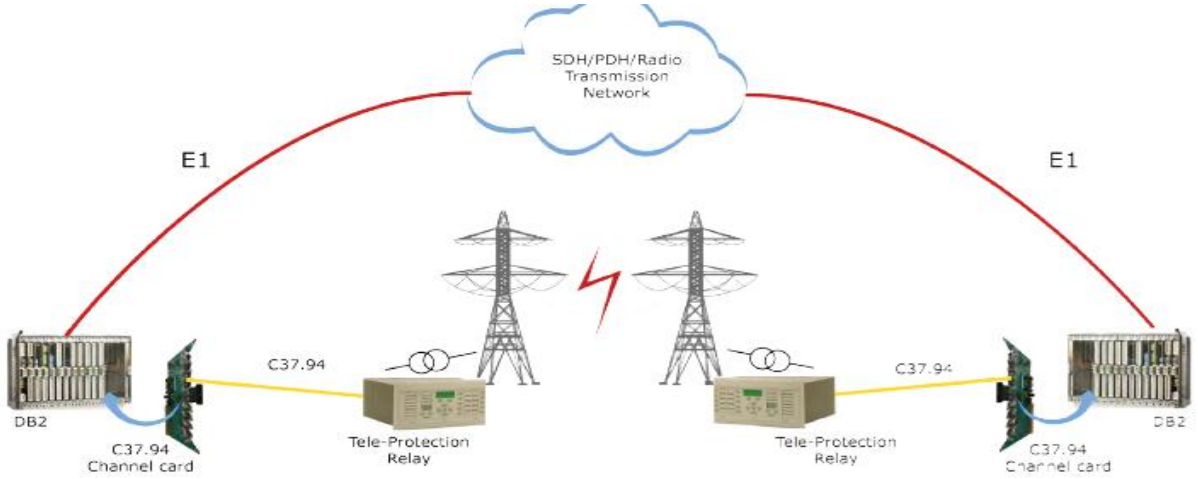



**Figure 5.1 – Teleprotection-over-TDM network system**
(Avara C37.94 Optical Data Interface Unit, 2010)

## 5.3 Proposed System

### 5.3.1 Concept Design

The concept of the system is shown simply below in **Figure 5.2**. The Areva P541 relay transmits traffic to the a8-vt (C37.94-capable teleprotection card) in the ALU 7705 SAR-8 chassis. The figure shows the IP/MPLS enabled cloud with two (2) LSP paths running through it.

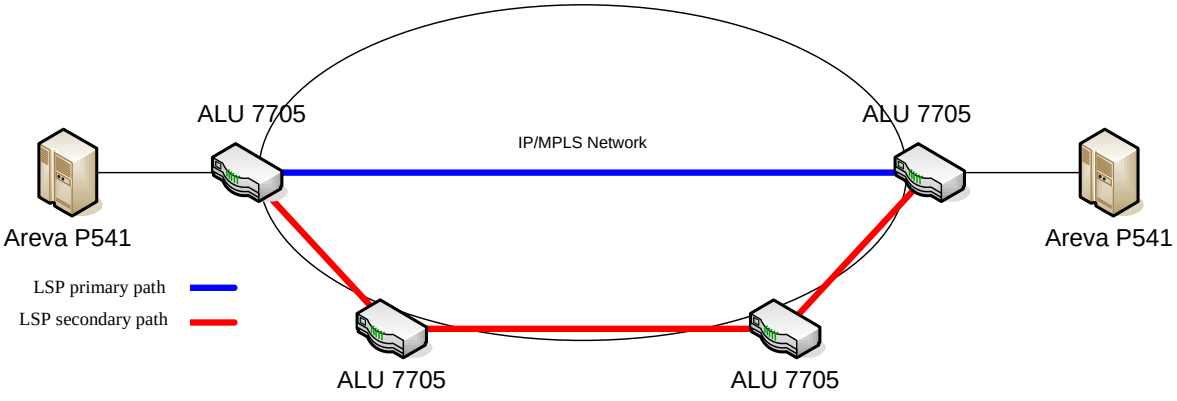



**Figure 5.2 – Proposed IP/MPLS Design**

### 5.3.2 Detailed design

There are a number of configuration steps involved to make the system operational. These steps are outlined below.

#### **5.3.2.1** OSPFv2 configuration

The four (4) routers are first configured with system interfaces (and addresses) and Network-Network Interface (NNI) addresses. Next, OSPF is enabled and both the ‘system’ and NNIs are added into OSPF. It should be noted that only one OSPF area will be used, that being Area 0. If the routers are in separate OSPF areas, area-stitching will need to be performed. Area-stitching is considered out-of-scope for the project.

#### **5.3.2.2** Transport tunnel configuration

System transport tunnels will be created using RSVP-TE. Initially RSVP and LDP will be turned on and appropriate interfaces will be added. To configure a transport tunnel MPLS needs to be enabled with also with appropriate interfaces added. Once this is completed path definitions will be defined and a LSP will be created. The project will test various LSP configurations which include, un/signalled secondary paths and fast re-route. All these options are configured in the LSP directly. **Figure 5.3** shows that transport tunnels are unidirectional and thus, must be configured at both ends of the tunnel.

#### **5.3.2.3** Service tunnel configuration

As can be seen below in **Figure 5.3** multiple service tunnels can lie inside one transport tunnel, i.e. Multiple services can be transported using the same LSP. The signalling and establishment of the service tunnels tunnel will be completed with the used of T-LDP. This will be achieved by configuring a ‘targeted-session’ for each appropriate peer in the LDP context. In should be noted that these ‘targeted-session’s only need to be configured at each end of the service, and not at intervening routers. This is because the service traffic is passed transparently through intervening routers. A SDP that references a LSP will be configured at each end of the service. The transport tunnel LSP will be re-used in this way.

#### **5.3.2.4** Cpipe service configuration

A Cpipe service is now created and will have the configured SDP bound to it. A SAP will also be created in the service configuration. It should be noted that adjustment of the jitter-buffer and payload size settings will be performed within the SAP context. **Figure 5.3** shows **Subscriber A** attached to this SAP. For the purposes of this project **Subscriber A** refers to the Areva P541 protection relay.

#### **5.3.2.5** QoS Configuration

Appropriate QoS policies are now created and configured. These configured policies are then set at various points within the system. There are three (3) QoS policies to be configure, which are, *network, network-queue* and a *SAP-ingress* policy. The *network-queue* policy will be configured at the MDA and port, while the *network* policy is configured at the NNI. The *SAP-ingress* policy is simply configured at the SAP.

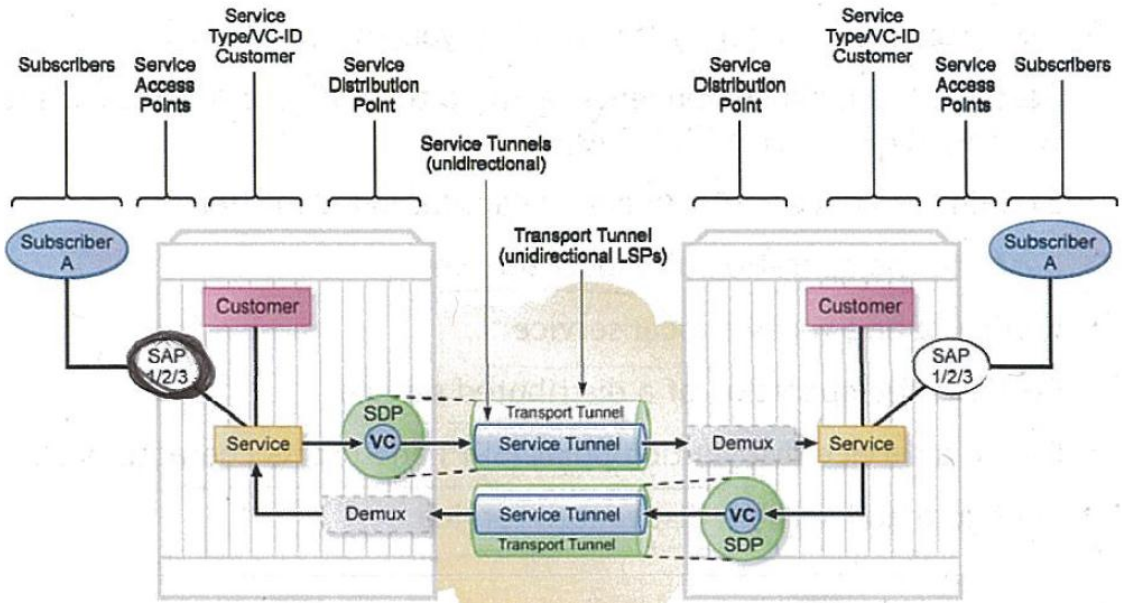



**Figure 5.3 – Detailed network design**
(ALU Service Architecture Course Notes, 2013)

# Chapter 6

# System Components and Testing Instruments

## 6.1 Introduction

This project will use a variety of equipment in the construction of the system. Furthermore, various items of test equipment will be required to verify the operation and performance of the constructed system. The following sections present, in detail, the hardware and software used for the system and its' testing.

## 6.2 IP/MPLS routing equipment

The vast majority of equipment within an IP/MPLS network are switches and routers; interconnected devices capable of receiving a packet and transmitting it to the next destination (operating on layers 2 (Data Link) and 3 (Network) respectively). Switches operating on the Data Link layer handle Ethernet traffic and as such are used in developing the LAN environment whereas routers operate on the network layer and are used to define the WAN allowing the interconnection of LANs. As outlined in the requirements analysis, IP/MPLS equipment manufactured by Alcatel Lucent will be the focus. Alcatel-Lucent's series of routers support the use of various interfaces through the use of modular interface devices referred to as IOMs (Input/output Modules). Whilst supporting Ethernet and IP traffic, they can also natively (where packetisation delay is limited to within the router)

support serial communications, VF signals and protection signalling interfaces such as analogue four wire circuits and G.703 traffic (Alcatel-Lucent – Deploying IP/MPLS Comms, 2012).

### 6.2.1 Alcatel-Lucent 7705 SAR-8 (Service Aggregation router)

The 7705 SAR-8 is a Layer 3 routing device and is at the core of the proposed system. The main components of the 7705 SAR-8 are the chassis, Control and Switching Module (CSM), Fan module, and adapter cards. **Figure 6.1** shows the front view of the 7705 SAR-8. There are eight horizontal slots for the CSMs and adapter cards, and one vertical slot for the Fan module. The connectors for the DC power feeds are located to the right of the Fan module.

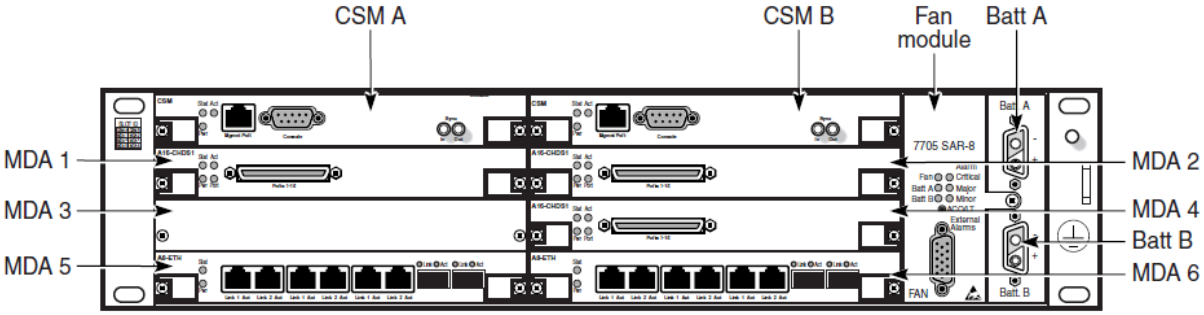



**Figure 6.1 – 7705 SAR-8 Front View**
(ALU 7705 SAR-8 Chassis Installation Guide, 2013)

The main features shown in the above figure are the slots used for the CSMs, adapter cards (MDA), and Fan module. In redundant systems, the CSMs are installed in slots CSM A and CSM B. The adapter cards are installed in slots MDA 1 through MDA 6. The 7705 SAR-8 chassis supports six 1 Gb/s-capable adapter cards.

**Control and Switching Module (CSM)**

The Control and Switching Module (CSM) has three main functions:

- it provides the management and console interfaces to the 7705 SAR-8;
- it provides system synchronization interfaces for external synchronization input and output signals; and
- it controls the routing, switching, and services functions for the entire system.

**Media Dependant Adapters (MDA)**

Adapter cards on the 7705 SAR-8 provide a wide variety of interfaces of different speed and type which include:

- T1/E1 interfaces (channelized and unchannelised)
- Ethernet interfaces (10/100/1000/10 000 Base-T and optical)
- SONET/SDH (OC3/STM1) interfaces (channelised and unchannelised)
- DS3/E3 interfaces
- V.35, RS-232 (also known as EIA/TIA-232), and X.21 serial data interfaces
- Foreign Exchange Office (FXO) interfaces
- Foreign Exchange Subscriber (FXS) interfaces
- G.703 codirectional interfaces
- IEEE C37.94 teleprotection interfaces (TPIF)

The two MDA types to be implemented for this project are:

| **Adapter Card and type** | **Description** |
|---|---|
| 8-port Gigabit Ethernet Adapter card version 2 (a8-1gb-v2-sfp) | • A maximum of six cards can be installed in MDA slots 1 to 6<br>• Has eight GigE SFP ports for 10/100/Gigabit Ethernet SFPs (optical or electrical)<br>• All GigE SFP ports can be configured in either access or network mode<br>• All GigE SFP ports are 10/100/1000 Mb/s-capable ports that support autosense and autonegotiation<br>• Supports synchronous Ethernet as a timing source (the electrical SFP does not support synchronous Ethernet) |
| 8-port Voice & Teleprotection card (a8-vt) | • A maximum of six cards can be installed in MDA slots 1 to 6 (however, because the 8-port Voice & Teleprotection card supports access mode only, for network applications, at least one of the installed cards must be a network-capable adapter card).<br>• A multi-functional adapter card with two FXS ports, two FXO ports, two G.703 64-kb/s codirectional ports, and two IEEE C37.94 teleprotection interfaces (TPIF) |

| | |
|---|---|
| | • Provides legacy voice, data, teleprotection, and networking applications and a migration path to MPLS with the optical interfaces |

(ALU 7705 SAR-8 Chassis Installation Guide, 2013)

The 8-port Gigabit Ethernet adapter card will be used in the simulating of IP traffic across the network while the teleprotection circuit is running and being tested. The 8-port Voice and Teleprotection card is the adapter that is going to facilitate the transporting of C37.94 protection data across the IP/MPLS network.

### 6.2.2 Alcatel-Lucent 7705 SAR-8 Voice and Teleprotection (VT) card

The 7705 SAR-8 MPLS switch Voice and Teleprotection (VT) card is a purpose designed protection device interface module providing two ports of G.703 (64kbps), two ports of IEEE C37.94 optical and two sets of two wire VF interfaces.

A G.703 codirectional interface provides a 64-kb/s channel over a G.703 framed link. A G.703 bipolar signal transmits data and timing over twisted pairs (one transmit, one receive). The two G.703 64-kb/s co-directional ports are accessed through two RJ-45 connectors on the faceplate.

As discussed earlier, C37.94 is an IEEE standard for N x 64-kb/s transmission between teleprotection and multiplex equipment. The 8-port Voice & Teleprotection card has two IEEE C37.94 teleprotection interfaces. The G.703 64-kb/s codirectional data ports and IEEE C37.94 teleprotection interfaces can be configured for T1/E1 or MPLS network access services (ALU 7705 SAR-8 8-port Voice & Teleprotection Card Installation Guide, 2012).

The optical interfaces can be connected to end equipment using glass multimode optical fibre with an active core diameter of 50 or 62.5 µm with BFOC/2.5 type (ST) connectors (ALU 7705 SAR-8 Chassis Installation Guide, 2013).

## 6.3 Protection relay and software

### 6.3.1 MiCOM Alstom P541 – Current Differential Protection Relay

The Alstom P541 relay is a high-speed current differential designed for both overhead line and cable applications. The relay operates using the proven characteristic of comparing differential current with through current. The phase differential elements of this type offer consistent detection of solid and resistive faults, with faulted phase selection, tripping and indication. There is also a full range of backup protection available integrated into the relay. Hot-standby elements (such as overcurrent) can be brought into service whenever a signalling channel outage may occur. The P541 relay interfaces to a variety of end-to-end communications channels including:

- Direct fibre optic communication (up to 130km)
- IEEE C37.94 standard multiplexed link
- G.703, V.35 and X.21 multiplexed links (MiCOM Alstom P541 & P542 product brochure, 2013)

### 6.3.2 MiCOM S1 software

The MiCOM S1 software package enables connectivity to the P541 relay. It is used for various purposes including initial relay configuration and extraction of data from the relay. Data extraction will be performed and data analysed in-line with the test requirements.

## 6.4 Protection scheme testing equipment

### 6.4.1 Doble F6150sv – Power System Simulator

The Doble F6150sv is an all-in-one power system simulator used for testing protection relays and schemes. The F6150sv is capable of performing the most simple through to the most complex of protection tests. The F6150sv is capable of testing both individual components or test an entire scheme. It will test and assess protection system performance for analog testing of 1A and 5A protection devices.

The F6150sv has a maximum of 12 high level analog sources are available at any time. There are 6 AC/DC Amplifier sources: 3x150 VA Voltages & 3x175/262.5 VA currents. These sources can be configured in a variety of configurations to achieve what is required (Doble F6150sv – Technical Specification, 2013).

### 6.4.2 Doble Protection Suite 2.2 software

The Protection Suite 2.2 software is an application made for use with the F6150sv. This software enables the user to run anything from simple ramp and step functions (voltage, current and frequency) through to programming and running complex test plans on the F6150sv. The state simulation application is used for testing of protection schemes. By using the correct test plan on the scheme, the software can verify that the scheme is running correctly by confirming trip and close functions are output under the proper circumstances (Doble Protection Suite 2.2 – Product Brochure, 2013).

## 6.5 Network channel testing equipment and software

### 6.5.1 JDSU – HST3000c

The HST-3000 is a portable test tool for Ethernet testing. It can perform layer 2 and layer 3 testing at 10Mbps, 100Mbps and 1Gbs. The HST3000c will be used to simulate IP traffic over the IP/MPLS network while testing the teleprotection service (JDSU HST3000c – Product Brochure, 2012).

### 6.5.2 Sunrise Telecom MTT (Modular Test Toolkit) w/ SSMTT-45 IEEE C37.94 Module

The SSMTT-45 is a piece of modular test equipment that plugs into the Sunrise Telecom MTT test unit. It makes available the following primary testing functions:

- Bit Error Rate Test (BERT) measurements
- Network propagation delay measurements
- Optical power level measurements (Sunrise Telecom IEEE C37.94 Module – Data Sheet, 2007).

Chapter 7

# Project Methodology

## 7.1 Introduction

In order to achieve each of the objectives of this project, several separate tasks were defined from the list of objectives. In this chapter, the objectives outlined in **Appendix A** – Project Specification are mapped to this document. Further explanation on objectives is given where necessary.

| **Item** | **Objective Description** | **Mapping** |
|---|---|---|
| 1 | Research information on current protection signalling schemes, their interface to current communications equipment and on IP/MPLS as a mature industry telecommunication technology. | Chapter 2 & 3 |
| 2 | Complete a basic requirements analysis to establish the deliverable for this project. | Chapter 4 |
| 3 | Undertake a comprehensive literature review covering all aspects of this project including IP/MPLS networking in High Voltage substations and other similar environments. | Chapter 2 & 3 |
| 4 | Design the system at a conceptual level. | Chapter 5 |

| | | |
|---|---|---|
| 5 | Evaluate the design and appropriate electrical and telecommunications test equipment required for the testing of an IP/MPLS protection signalling scheme. | Chapter 6 |
| 6 | Build a testbed to test IP/MPLS teleprotection signalling as a service. This includes complete router configurations. | Chapter 7 |
| 7 | Fully configure, test and evaluate a C37.94 protection signalling scheme. | Chapter 8 |

## 7.2 IP/MPLS network configuration

From the research conducted the basic router configurations have been designed and explained below. While the full router configurations can be seen in **Appendix B** this section outlines the configuration required for each step of the network configuration including MPLS service and transport tunnel creation. It should be noted that the following router commands are performed from the 'configure' context.

- Design Network Address Plan including system, out-of-band management and NNI (Network-Network Interface) addresses. This address plan follows.

| **Node** | **System address (/32)** | **Out-of-band mgmt (/31)** |
|---|---|---|
| Athena-mg00 | 172.16.6.2 | 172.16.7.2 |
| Apollo-md00 | 172.16.6.3 | 172.16.7.3 |
| Osiris-mg00 | 172.16.6.6 | 172.16.7.6 |
| Apollo-mg00 | 172.16.6.8 | 172.16.7.8 |

**Table 7.1 – Network System & Out-of-band mgmt Addressing**

| **NNI addresses (/31)** | | | |
|---|---|---|---|
| **Node** | **Address** | **Node** | **Address** |
| athena-md00 | 172.16.0.10 | apollo-mb00 | 172.16.0.11 |
| athena-md00 | 172.16.0.16 | osiris-mg00 | 172.16.0.17 |
| apollo-mb00 | 172.16.0.20 | apollo-mg00 | 172.16.0.21 |
| osiris-mg00 | 172.16.0.24 | apollo-mg00 | 172.16.0.25 |

**Table 7.2 – Network-to-Network Interface Addressing**

```
router
        interface "apollo-mg00-ieg1-1-1"
            address 172.16.0.25/31
            description "to osiris-mg00"
            port 1/1/1
        exit
        interface "apollo-mg00-ieg1-2-1"
```

```
            address 172.16.0.21/31
            description "to apollo-mb00"
            port 1/2/1
        exit
        interface "system"
            address 172.16.6.8/32
        exit
        autonomous-system 65400
```

- Configure TDM teleprotection port with encapsulation-type and timeslot

```
port 1/3/1
        tdm
            tpif
                channel-group 1
                    encap-type cem
                    no shutdown
                exit
                no shutdown
            exit
        exit
        no shutdown
    exit
```

- Configure OSPFv2 including Traffic Engineering

```
        ospf
            traffic-engineering
            area 0.0.0.0
                interface "system"
                exit
                interface "apollo-mg00-ieg1-1-1"
                    interface-type point-to-point
                    hello-interval 4
                    dead-interval 17
                    bfd-enable
                exit
                interface "apollo-mg00-ieg1-2-1"
                    interface-type point-to-point
                    hello-interval 4
                    dead-interval 17
                    bfd-enable
                exit
            exit
        exit
```

- Turn on LDP and MPLS

```
    mpls
            interface "system"
            exit
            interface "apollo-mg00-ieg1-1-1"
            exit
            interface "apollo-mg00-ieg1-2-1"
            exit
        exit

    ldp
            peer-parameters
                peer 172.16.6.6
                exit
            exit
            interface-parameters
                interface "apollo-mg00-ieg1-1-1"
                exit
                interface "apollo-mg00-ieg1-2-1"
                exit
            exit
            exit
```

```
        exit
    exit
```

- Turn on RSVP on interfaces to signal and establish traffic engineered-capable transport tunnels

```
    rsvp
            interface "system"
            exit
            interface "apollo-mg00-ieg1-1-1"
            exit
            interface "apollo-mg00-ieg1-2-1"
            exit
            no shutdown
        exit
```

- Configure paths and LSP's for traffic engineering

```
        mpls
            path "to-osiris-mg00-1"
                hop 1 172.16.6.6 strict
                no shutdown
            exit
            path "to-osiris-mg00-2"
                hop 1 172.16.6.3 strict
                hop 2 172.16.6.2 strict
                hop 3 172.16.6.6 strict
                no shutdown
            exit
            lsp "to-osiris-mg00-lsp"
                to 172.16.6.6
                cspf
                fast-reroute facility
                    no node-protect
                exit
                primary "to-osiris-mg00-1"
                exit
                secondary "to-osiris-mg00-2"
                    standby
                exit
                no shutdown
            exit
            lsp "to-osiris-mg00-traffic-lsp"
                to 172.16.6.6
                primary "to-osiris-mg00-1"
                exit
                no shutdown
            exit
            no shutdown
        exit
```

- Configure SDP that use the LSP's created for their service path

```
service
    sdp 5 create
            far-end 172.16.6.6
            lsp "to-osiris-mg00-lsp"
            keep-alive
                shutdown
            exit
            no shutdown
```

- Establish T-LDP peering between nodes to establish service tunnels

```
    ldp
            targeted-session
                peer 172.16.6.3
                exit
```

```
                peer 172.16.6.6
                exit
            exit
        exit
    exit
```

- Configure a CPipe service and customer that references the configured SDP

```
    cpipe 20 customer 10 vc-type cesopsn create
            sap 1/3/1.1 create
                exit
                ingress
                    qos 4000
                exit
            exit
            spoke-sdp 5:20 create
            exit
            no shutdown
        exit
```

- Configure QoS policies

```
qos
        network-queue "4001" create
            queue 1 create
                high-prio-only 10
            exit
            queue 7 create
                rate 10 cir 10
                high-prio-only 10
            exit
            queue 8 create
                rate 10 cir 10
                high-prio-only 10
            exit
            queue 9 multipoint create
                high-prio-only 10
            exit
            fc h1 create
                multicast-queue 9
                queue 7
            exit
            fc nc create
                multicast-queue 9
                queue 8
            exit
        exit
        sap-ingress 4000 create
            queue 1 create
            exit
            queue 7 create
                rate 256 cir 256
                mbs 8
                cbs 2
                high-prio-only 10
            exit
            fc "h1" create
                queue 7
            exit
            default-fc "h1"
            default-priority high
        exit
        mc-mlppp
        exit
        network 4002 create
            ingress
                dscp nc2 fc nc profile in
                lsp-exp 6 fc h1 profile in
            exit
```

```
            egress
                fc nc
                    dscp-in-profile nc1
                exit
            exit
        exit
    exit
```

- Configure QoS on router MDA, port, interfaces and SAP

```
card 1
        mda 1
            network
                ingress
                    queue-policy "4001"
                exit
            exit

port 1/1/1
        description "to osiris-mg00"
        ethernet
            network
                queue-policy "4001"
            exit
        exit
        no shutdown
    exit

router interface "apollo-mg00-ieg1-1-1"
    qos 4002
    exit

service cpipe 20
            sap 1/3/1.1
                ingress
                    qos 4000
                exit
            exit
```

## 7.3 Protection Relay configuration

The current differential protection scheme being simulated and tested is a 33kV feeder running from Energex Newmarket Substation (SSNMK) to Energex Ashgrove Substation (SSAGE).

The relay settings for each end of this site are as follows:

| SSAGE relay | SSNMK relay |
|---|---|
| CT ratio – 1200/5A<br>Communications setup<br><br>• Scheme Setup 2 Terminal<br>• Address 11-A<br>• Comm Delay Tol 500.0us<br>• Comm Fail Timer 5.000 s<br>• Char Mod Time 500.0ms<br>• Inrush Restraint Disabled | CT ratio – 800/5A<br>Communications setup<br><br>• Scheme Setup 2 Terminal<br>• Address 11-B<br>• Comm Delay Tol 500.0us<br>• Comm Fail Timer 5.000 s<br>• Char Mod Time 500.0ms<br>• Inrush Restraint Disabled |

| | |
|---|---|
| • Vectorial Comp Yy0 (0 deg)<br>• Ph CT Corr'tion 1.500<br>• Comms Mode IEEE C37.94<br>• Ch1 N*64kbits/s 1 | • Vectorial Comp Yy0 (0 deg)<br>• Ph CT Corr'tion 1.000<br>• Comms Mode IEEE C37.94<br>• Ch1 N*64kbits/s 1 |

## 7.4 System Testing

There will be two primary stages of testing performed on the IP/MPLS developed teleprotection scheme. Firstly, testing will be performed in a laboratory environment. The laboratory environment to be configured is reflected in **Figure 7.1** below.

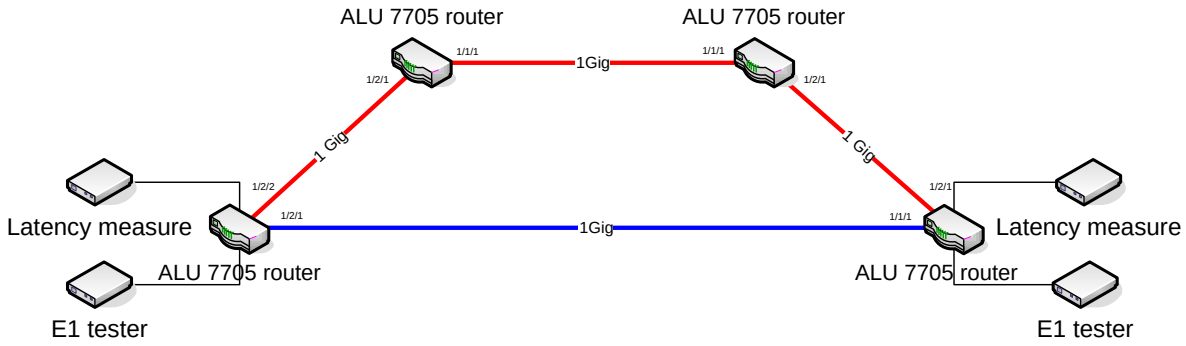



**Figure 7.1 – Laboratory Testing Configuration**

The second phase of testing will be performed in the field. This means configuring a MPLS teleprotection in parallel to a current working circuit running over a TDM network running PDH infrastructure. Once the testing is complete the results can be compared with testing results from the TDM circuit.

### 7.4.1 Network configuration verification tests

This set of tests will confirm that the base configuration of the network and Cpipe service are configured correctly. The Network Verification tests will not however, test and confirm the QoS configuration setup. This is be tested and examined in Section **7.4.2**.

#### **7.4.1.1** Confirm router connections through NNI links

This is a simple test to confirm a physical connection between the NNI links. Run the following command to confirm the interfaces are both administratively and operationally Up.

- Show router interface

#### **7.4.1.2** Verifying OSPF Operation

Verify the OSPF protocol has established sessions with Neighbors. Confirm Traffic-Engineering (TE) is turned on. This is made possible using the following router commands:

- Show router ospf neighbor
- Show router ospf status

#### **7.4.1.3** Confirm Link LDP sessions established

Prove Link LDP sessions have been successfully established to confirm transport tunnels have been established. This is proven by the use of the following command:

- Show router ldp session

Confirm under the ‘adjacency type’ sessions are ‘link’.

#### **7.4.1.4** Confirm MPLS interfaces are Operationally Up

The following command will confirm the correct configuration of the MPLS instances running on the interfaces.

- Show router mpls interface

#### **7.4.1.5** Confirm Path definitions are Administratively Up

Show that created MPLS paths are administratively up. This is achieved by the following command.

- Show router mpls path

#### **7.4.1.6** Confirm LSPs are established using lsp-ping & lsp-trace

Using the lsp oam tools, confirm LSPs are pingable and traceable. The use of the oam tools is shown below.

- Show router mpls lsp
- oam lsp-ping ‘*lsp-name’*
- oam lsp-trace *‘lsp-trace’*

#### 7.4.1.7 Confirm RSVP sessions are running

Confirm that RSVP sessions are running and in an ‘Up’ state using the below command.

- Show router rsvp session

#### 7.4.1.8 Confirm T-LDP sessions have been established for service tunnels

Prove T-LDP sessions have been successfully established to confirm service tunnels can be established. This is acheived by the use of the following command:

- Show router ldp session

Confirm under the ‘adjacency type’ sessions are ‘both’.

#### 7.4.1.9 Confirm SDPs are established and using T-LDP for service tunnels

Confirmation that SDPs have been established and are using T-LDP signalling is achieved using the following commands.

- Show service sdp
- Show service sdp-using

#### 7.4.1.10 Confirm SAP and Cpipe service are established

SAP and Cpipe establishment confirmation is achieved using the following command.

- Show service cpipe ‘*cpipe-no.’* detail

#### 7.4.1.11 Sunrise SSMTT-45 IEEE C37.94 Module Test

The SSMTT-45 IEEE C37.94 Module tests the C37.94 circuit in-line with ITU-T Recommendation G.821. This recommendation covers Error performance of a digital connection, operating at a bit rate below the primary rate and forming part of an Integrated Services Digital Network. The tester measures and logs Error performance events and parameters which are defined in the ITU-T recommendation as:

- **Events** – Error performance parameters are derived from the following events:

- **Errored second (ES):** It is a one-second period in which one or more bits are in error or during which Loss of Signal (LOS) or Alarm Indication Signal (AIS) is detected.
- **Severely errored second (SES):** It is a one-second period which has a bit error ratio ≥ 1.10–3 or during which Loss of Signal (LOS) or Alarm Indication Signal (AIS) is detected.
- **Parameters** -> It should be noted that total observation time (Stotal) is split into two parts, namely, time for which the connection is deemed to be available (Savail) and that time when it is unavailable (Sunavail). Error performance should only be evaluated whilst the connection is in the available state.
- **Errored second ratio (ESR):** The ratio of ES to total seconds in available time during afixed measurement interval.
- **Severely errored second ratio (SESR):** The ratio of SES to total seconds in available time during a fixed measurement interval (ITU-T Recommendation G.821).

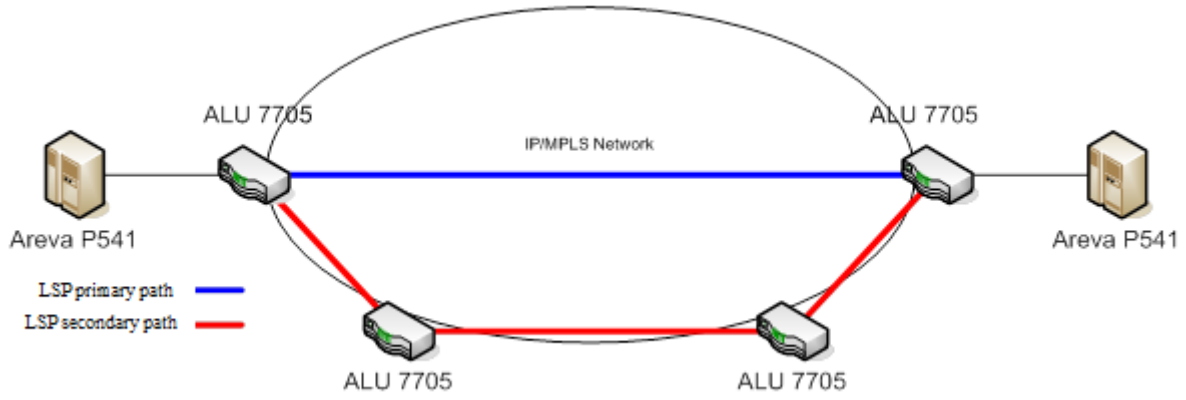
### 7.4.2 Network functionality testing and analysis

The main purpose of these tests is to gain an understanding of the system responds under different network conditions. As covered earlier, asymmetrical path delay is a characteristic associated with packet networks and needs to be minimised for use with teleprotection schemes.

This project attempts to investigate and minimise this using various methods. These methods include investigating ‘tuning’ of the service circuit by using a jitter buffer and adjusting the payload size. QoS testing will also be conducted to gain an understanding of how the system responds to various network conditions with, and without, QoS configured.

This section also covers testing of various traffic engineering configuration and finally, failure cases.

**Laboratory Test-Bed Configuration**




**7.4.2.1** Latency and Jitter Characterisation – RSVP-TE

This test scenario firstly validates the latency performance of Cpipe services across the MPLS network using RSVP-TE LSP's.

As described in **Section 3.7**, in the service configuration used, payload size can be adjusted from between 2 to 64 octets and the Cpipe jitter buffer can be adjusted from 2 to 32 milliseconds. This test scenario will also attempt to tune the Cpipe circuit for maximum stability within protection signalling latency tolerances.

**Test setup both 7.4.2.1 & 7.4.2.2 tests**

| **Setup 1** | **Setup 2** |
|---|---|
| Create Cpipe between adjacent nodes. | Create Cpipe between nodes with two (2) of intervening nodes. |
| Cpipe will use an RSVP-TE tunnel with primary path only, no FRR. | Cpipe will use an RSVP-TE tunnel with primary path only, no FRR. |
| Cpipe will be configured to use minimum data transport settings. | Cpipe will be configured to use minimum data transport settings. |

**Procedure**

| Step | Activity |
|---|---|
| 1 | Initial Configuration<br>Record initial latency values from the circuit using the default jitter buffer and payload size, ie. JB – 32ms, PS – 64 octets. |
| 2 | Test change in latency and PDV<br><br>Step the Payload size from 2 octets through to 12 octets at 2 octet steps. Record 100 samples of delay for each step.<br><br>Plot this data and attempt to characterise using some form of Probability Density Function.<br><br>*Note: While it is clear that 100 samples is a relatively small figure for such an experiment, the available test equipment does not allow for automation of such and must be sampled manually 100 times.*<br><br>Record the results using configuration described in **6.5.2.1** Step 4 & 5. |
| 3 | As described in Section 3.7, calculate an appropriate jitter buffer. Ie. PDV +/- 5ms, JB = 10ms. |
| 4 | Analyse the PDV and latency figures. |
| 5 | Attempt to find payload figure that combines best latency with minimum jitter. |

**7.4.2.2** Quality of Service Impact Characterisation

For each of the two test setups outlined above, run the following QoS configuration tests in the below table.

**Configuration**

| QoS Configuration | QoS Markings | 1 Gbs injected traffic |
|---|---|---|
| **Config 1** | No | Nil |
| **Config 2** | No | Full line speed |
| **Config 3** | No | Burst traffic 80% duty cycle |

| | | |
|---|---|---|
| **Config 4** | Yes | Nil |
| **Config 5** | Yes | Full line speed |
| **Config 6** | Yes | Burst traffic 80% duty cycle |

**Procedure**

| **Step** | |
|---|---|
| 1 | Initial Configuration<br>Enable/disable QoS settings and inject traffic as per the configuration settings. |
| 2 | Confirm latency tolerance<br>Sample the latency of the link and record results. |
| 3 | Confirm link stability<br>Confirm the change in PDV from previous tests. |
| 4 | Confirm QoS functionality<br>Confirm traffic is being marked and passed at correct QoS levels. |

### **7.4.2.3** Traffic Engineering Impact Characterisation

*Note: All testing from this point onwards assumes correctly configured QoS markings.*
This test scenario will test the behaviour of the Cpipe service under various traffic engineering configurations and state changes.

**Test setup for 7.4.2.3 tests**

In all cases the secondary path will be a longer path, with no overlap with the primary path.

| **Setup 1** |
|---|
| Create Cpipe between adjacent nodes using RSVP-TE |
| Cpipe will use tunnel with:<br>• primary path, strict hops<br>• secondary path, unsignalled, strict hops |
| Cpipe will be configured to use minimum data transport settings. |

| **Setup 2** |
|---|
| Create Cpipe between adjacent nodes using RSVP-TE |

| |
|---|
| Cpipe will use tunnel with:<br>• primary path, strict hops<br>• secondary path, pre-signalled, strict hops |
| Cpipe will be configured to use minimum data transport settings. |

| **Setup 3** |
|---|
| Create Cpipe between adjacent nodes using RSVP-TE |
| Cpipe will use tunnel with:<br>• primary path only, strict hops<br>• FRR, using link protection. |
| Cpipe will be configured to use minimum data transport settings. |

| **Setup 4** |
|---|
| Create Cpipe between adjacent nodes using RSVP-TE |
| Cpipe will use tunnel with:<br>• primary path, strict hops<br>• secondary path, pre-signalled, strict hops<br>• FRR, using link protection |

For each of the test setups above perform the following procedure. Multiple cycles may be required.

| **Step** | **Activity** |
|---|---|
| 1 | Failover<br>Generate test traffic across circuit at maximum line rate.<br>Drop the primary path through link failure.<br>Record failover times, based on lost bytes, between failure event and traffic restoration. |
| 2 | Failback<br>Generate test traffic across circuit at maximum line rate.<br>Restore the primary path.<br>Record failover times, based on lost bytes, between restore event and traffic restoration to primary path. |

#### **7.4.2.4** Failure Modes

This test scenario will test the behaviour of the Cpipe circuit under failure conditions of various elements in the traffic path. These test cases use the most reliable RSVP-TE configuration to test the service behaviour.

**Test setup for 7.4.2.4 tests**

In all cases the secondary path will have no overlap with the primary path. Service delivery nodes will have two paths configured.

| **Setup 1** |
|---|
| Create Cpipe between adjacent nodes using RSVP-TE |
| Cpipe will use tunnel with:<br>• primary path, strict hops<br>• FRR using link protection<br>• secondary path, pre-signalled, strict hops using end node only. |
| Cpipe will be configured to use minimum data transport settings. |

| **Setup 2** |
|---|
| Create Cpipe across two (2) intervening nodes using RSVP-TE |
| Cpipe will use tunnel with:<br>• primary path, strict hops<br>• FRR using link protection<br>• secondary path, pre-signalled, strict hops using end node only. |
| Cpipe will be configured to use minimum data transport settings. |

**Test procedure**

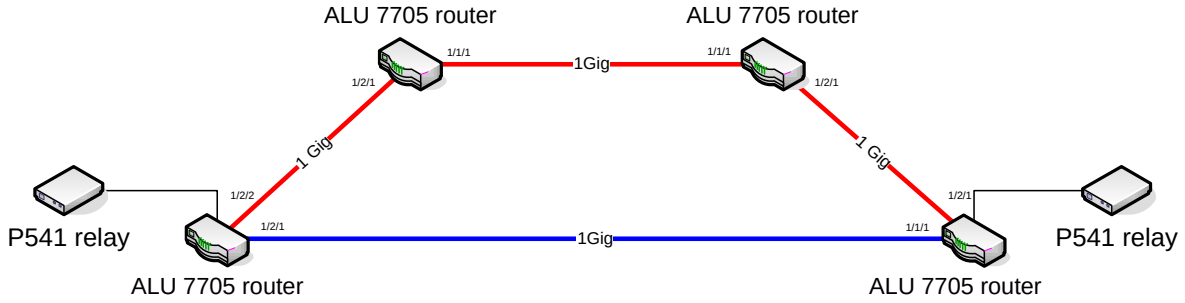
| **Step** | **Activity** |
|---|---|
| 1 | Line Card Failure<br>• Generate test traffic across circuit at maximum line rate.<br>• Pull an NNI line card from the originating node.<br>• Record lost traffic time based on lost bytes. |

| | |
|---|---|
| 2 | <u>CSM failure</u><br>• Generate test traffic across circuit at maximum line rate.<br>• Pull a CSM card from the originating node.<br>• Record lost traffic time based on lost bytes. |
| 3 | <u>CSM manual switch</u><br>• Generate test traffic across circuit at maximum line rate.<br>• Manually switch CSM/CPM card from the originating node.<br>• Record lost traffic time based on lost bytes. |
| 4 | <u>Full Node Failure</u><br>• Generate test traffic across circuit at maximum line rate.<br>• Pull the power on an intervening node.<br>• Record lost traffic time based on lost packets.<br>• Restore node power, and monitor until fully rebooted. |

### 7.4.3 Protection Relay functionality tests

This stage of testing will validate the operation of the selected P541 protection relay across the MPLS network. Before starting this stage a decision will be required on the SAP configuration parameters. This decision will be based on the data collected from the tests performed in *Section 7.4.2 – Network Functionality testing and analysis – Lab Environment*.

**System Testing Configuration**

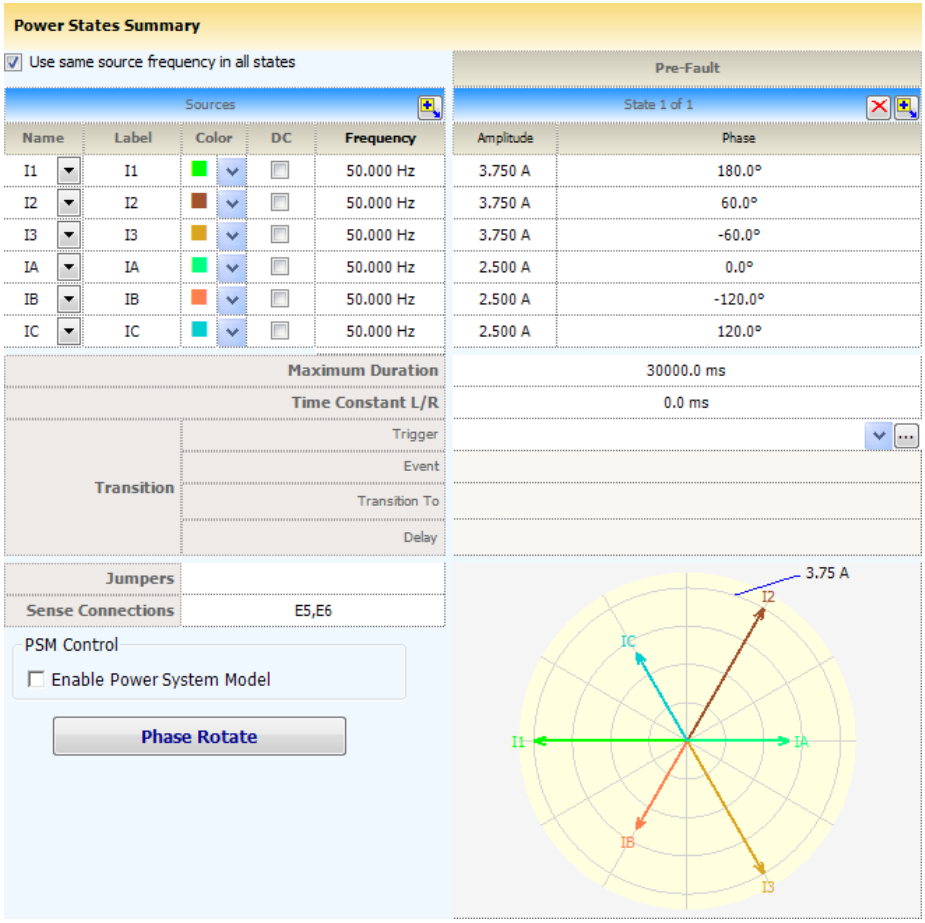



Configuration parameters:

Jitter-buffer – 2ms Payload size – 2 octets

### **7.4.3.1** Forward/Reverse Stability tests

Protection stability tests are performed to prove the current differential scheme behaves correctly under 'system normal' conditions. For the forward stability test standard loads are simulated through the feeder from source bus to load bus using the Doble F6150. The differential current and bias current are sampled from the P541 relay and recorded to prove stability. In the reverse stability test loads are simply reversed so the load bus in now feeding the source bus. Screenshots from the Protection Suite v2.2 software package are shown below depicting the configuration for the Forward Stability test.



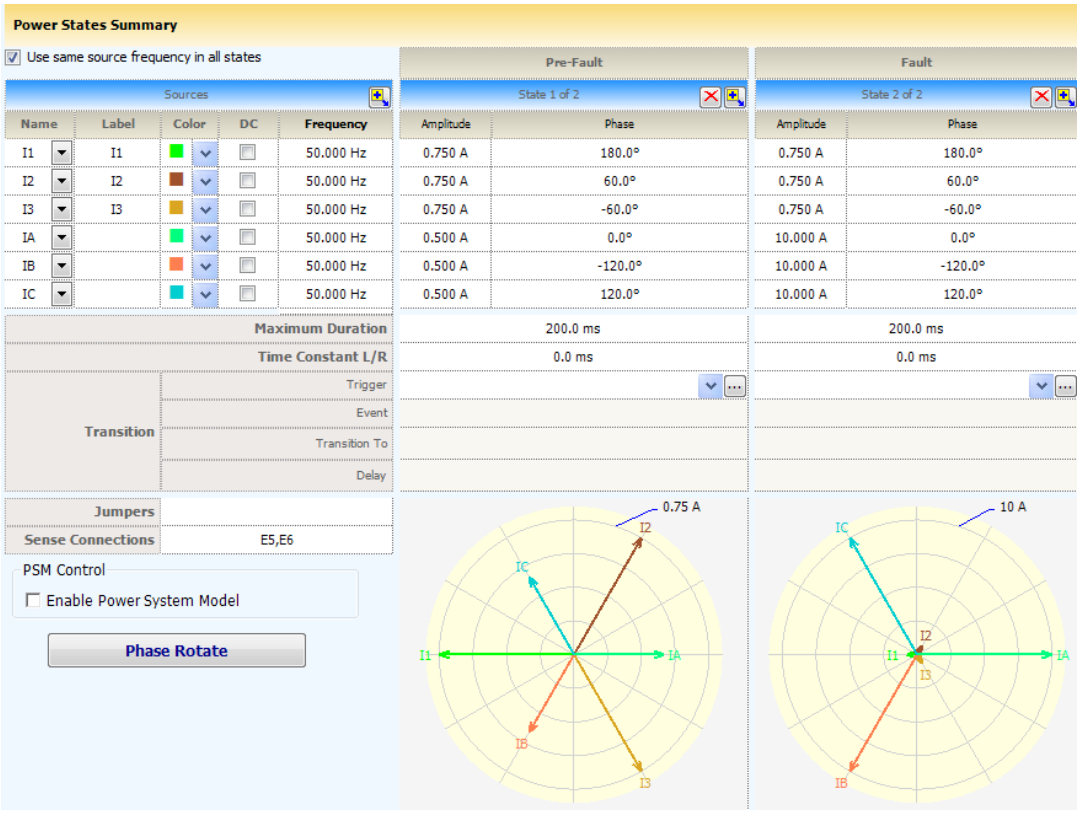

Things of note:

- Currents I1-3 are injected into AGE relay. Currents IA-C are injected into NMK relay.
- Due to the relay CT settings (AGE 1200/5, NMK 800/5) the injected current in the above test plan are different. As such both relays will read 600A primary current.

- The phase angles are reversed at the remote end to simulate a standard load through the feeder.
- The only difference in the Reverse stability test is that the phase angles are configured in the reverse direction.

#### **7.4.3.2** 3 phase In-zone Fault

This test is a two-stage test performed through the Protection Suite v2.2 software controlling the Doble F6150. The system is initially simulated with 'system normal' conditions. The second stage simulates a 3 phase fault injected from one Doble only. This simulates a fault that is on the feeder between the two relays.

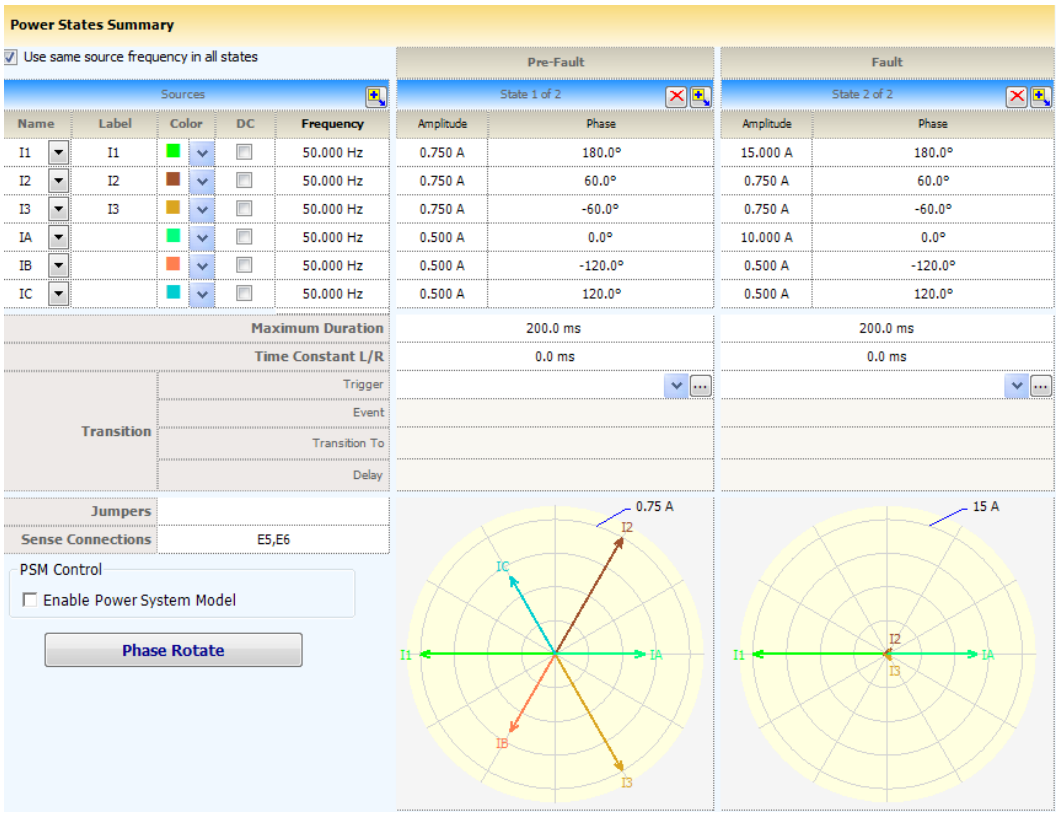



Things of note:

- The test is split into two sections, Pre-fault and Fault.
- During the fault conditions a secondary current to 10A is being injected. This will be seen as 2400A primary current.

### **7.4.3.3** Single phase thru Fault

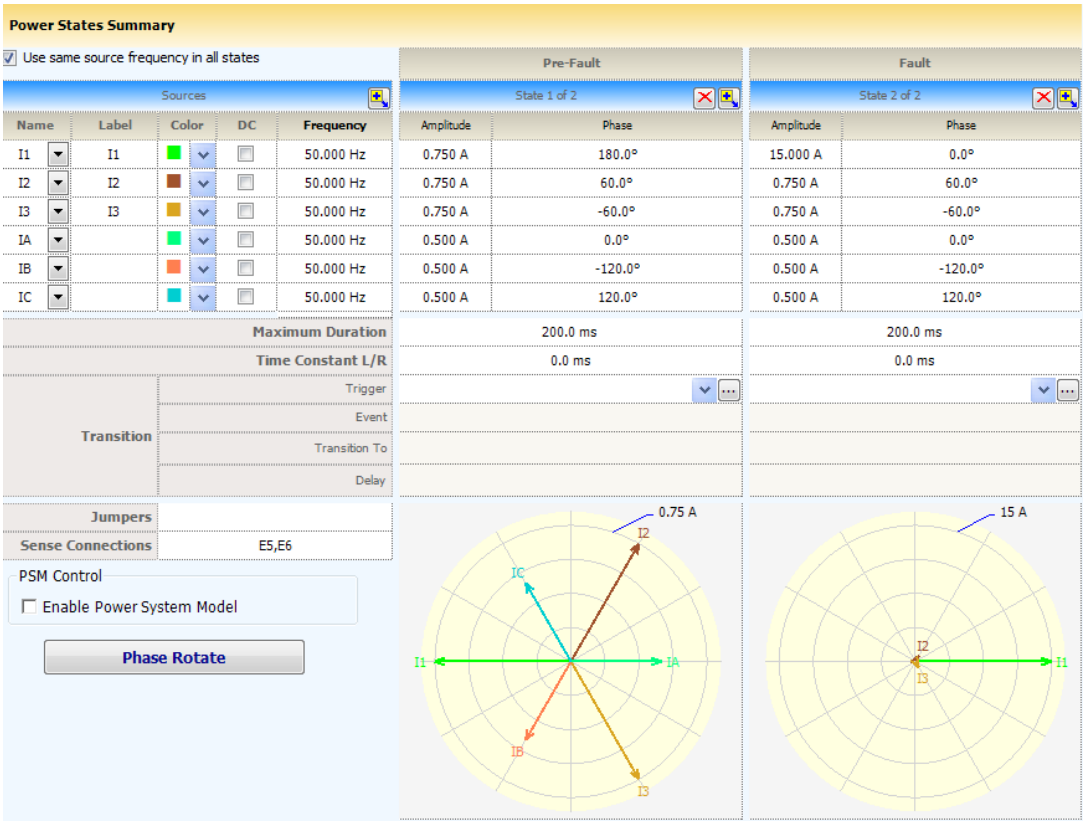
This test simulates a single phase fault current travelling through the feeder. This type of current differential protection scheme is not used to operate under such faults. There are other types of protection that will operate under this fault scenario. As such this is a 'No operation' test, confirming that the relays DO NOT initiate a trip under these circumstances.




- During the Fault stage of the test the currents injected at I1 and IA still match when the primary current is calculated.

### **7.4.3.4** Single phase In-zone Fault

This test is a two-stage test performed through the Protection Suite v2.2 software controlling the Doble F6150. The system is initially simulated with 'system normal' conditions. The second stage simulates a single phase fault injected from one Doble only. This simulates a fault that is on the feeder between the two relays.



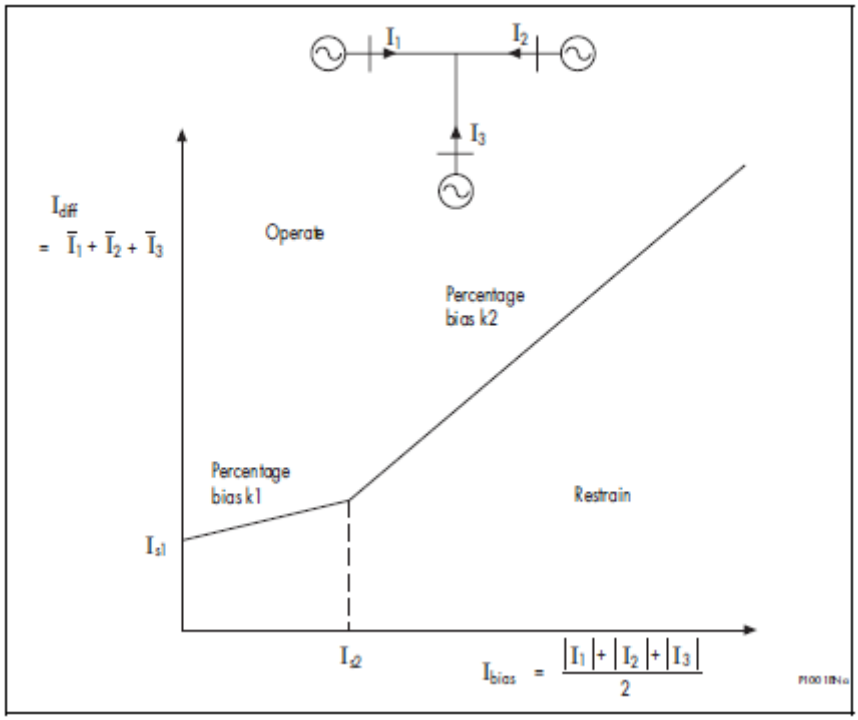

Things to note:

- During the Fault stage of the test I1 injects a fault current level and IA does not. This simulates a fault on the feeder inside the 'protected area'.

### **7.4.3.5** Bias Restraint (In-zone & Out-of-zone)

The basic operating principle of differential protection is to calculate the difference between the currents entering and leaving a protected zone. The protection operates when this difference exceeds a set threshold. Differential currents may also be generated during external fault conditions due to CT saturation. To provide stability for through fault conditions, the relay adopts a biasing technique. This method effectively raises the setting of the relay in proportion to the value of through fault current to prevent relay maloperation. **Figure 7.2** shows the operating characteristics of the P541 phase differential element.

The differential current is calculated as the vector summation of the currents entering the protected zone. The bias current is the average of the measured current at each line end. It is found by the scalar sum of the current at each terminal, divided by two.




The characteristic is determined by four protection settings:

| | |
|---|---|
| Is1 | The basic differential current setting which determines the minimum pick-up level of the relay. |
| k1 | The lower percentage bias setting used when the bias current is below Is2. This provides stability for small CT mismatches, whilst ensuring good sensitivity to resistive faults under heavy load conditions. |
| Is2 | A bias current threshold setting, above which the higher percentage bias k2 is used. |
| k2 | The higher percentage bias setting used to improve relay stability under heavy through fault current conditions. |

**Figure 7.2 – P541 Bias Characteristic Curve**
(Areva MiCOM P54x – Technical Guide, 2005)

The bias restraint tests test a variety of points along the Relay Bias Characteristic Curve in **Figure 7.2**, both inside the *Operate* and *Restrain* regions.

# Chapter 8

# Testing Results and Performance Analysis

## 8.1 Laboratory results

### 8.1.1 Network configuration verification results

#### **8.1.1.1** Verifying OSPF operation with TE support enabled

A:apollo-mg00# show router ospf neighbor

```
===============================================================================
OSPF Neighbors
===============================================================================
Interface-Name                 Rtr Id         State     Pri  RetxQ   TTL
-------------------------------------------------------------------------------
apollo-mg00-ieg1-1-1           172.16.6.6     Full      1    0       16
apollo-mg00-ieg1-2-1           172.16.6.3     Full      1    0       13
-------------------------------------------------------------------------------
No. of Neighbors: 2
===============================================================================
A:apollo-mg00#
```

A:osiris-mg00# show router ospf neighbor

```
===============================================================================
OSPF Neighbors
===============================================================================
Interface-Name                 Rtr Id         State     Pri  RetxQ   TTL
-------------------------------------------------------------------------------
osiris-mg00-ieg1-2-1           172.16.6.8     Full      1    0       16
```

```
osiris-mg00-ieg1-2-2            172.16.6.2      Full      1    0      15
-------------------------------------------------------------------------------
No. of Neighbors: 2
===============================================================================
A:osiris-mg00#

A:apollo-mg00# show router ospf status

===============================================================================
OSPF Status
===============================================================================
OSPF Cfg Router Id          : 0.0.0.0
OSPF Oper Router Id         : 172.16.6.8
OSPF Version                : 2
OSPF Admin Status           : Enabled
OSPF Oper Status            : Enabled
GR Helper Mode              : Disabled
Preference                  : 10
External Preference         : 150
Backbone Router             : False
Area Border Router          : False
AS Border Router            : False
Opaque LSA Support          : True
Traffic Engineering Support : True
RFC 1583 Compatible         : True
Demand Exts Support         : False
In Overload State           : False
In External Overflow State  : False
Exit Overflow Interval      : 0
Last Overflow Entered       : Never
Last Overflow Exit          : Never
External LSA Limit          : -1
Reference Bandwidth         : 100,000,000 Kbps
Init SPF Delay              : 1000 msec
Sec SPF Delay               : 1000 msec
Max SPF Delay               : 10000 msec
Min LS Arrival Interval     : 1000 msec
Init LSA Gen Delay          : 5000 msec
Sec LSA Gen Delay           : 5000 msec
Max LSA Gen Delay           : 5000 msec
Last Ext SPF Run            : Never
Ext LSA Cksum Sum           : 0x0
OSPF Last Enabled           : 04/13/2014 17:40:03
Export Policies             : None
OSPF Ldp Sync Admin Status  : Enabled
LDP-over-RSVP               : Disabled
===============================================================================
A:apollo-mg00#


A:osiris-mg00# show router ospf status

===============================================================================
OSPF Status
===============================================================================
OSPF Cfg Router Id          : 0.0.0.0
OSPF Oper Router Id         : 172.16.6.6
OSPF Version                : 2
OSPF Admin Status           : Enabled
OSPF Oper Status            : Enabled
```

```
GR Helper Mode              : Disabled
Preference                  : 10
External Preference         : 150
Backbone Router             : False
Area Border Router          : False
AS Border Router            : False
Opaque LSA Support          : True
Traffic Engineering Support : True
RFC 1583 Compatible         : True
Demand Exts Support         : False
In Overload State           : False
In External Overflow State  : False
Exit Overflow Interval      : 0
Last Overflow Entered       : Never
Last Overflow Exit          : Never
External LSA Limit          : -1
Reference Bandwidth         : 100,000,000 Kbps
Init SPF Delay              : 1000 msec
Sec SPF Delay               : 1000 msec
Max SPF Delay               : 10000 msec
Min LS Arrival Interval     : 1000 msec
Init LSA Gen Delay          : 5000 msec
Sec LSA Gen Delay           : 5000 msec
Max LSA Gen Delay           : 5000 msec
Last Ext SPF Run            : Never
Ext LSA Cksum Sum           : 0x0
OSPF Last Enabled           : 06/12/2014 03:14:19
Export Policies             : None
OSPF Ldp Sync Admin Status  : Enabled
LDP-over-RSVP               : Disabled
===============================================================================
osiris-mg00#
```

#### **8.1.1.2** Confirm Link LDP sessions established

```
A:osiris-mg00# show router ldp session

===============================================================================
LDP Sessions
===============================================================================
Peer LDP Id       Adj Type   State        Msg Sent  Msg Recv  Up Time
-------------------------------------------------------------------------------
172.16.6.2:0      Link       Established  187586    194232    6d 00:16:40
172.16.6.8:0      Link       Established  187592    217727    6d 00:16:43
-------------------------------------------------------------------------------
No. of Sessions: 2
===============================================================================
A:osiris-mg00#


A:apollo-mg00# show router ldp session

===============================================================================
LDP Sessions
===============================================================================
Peer LDP Id       Adj Type   State        Msg Sent  Msg Recv  Up Time
-------------------------------------------------------------------------------
172.16.6.3:0      Link       Established  187871    193954    6d 00:28:59
```

```
172.16.6.6:0       Link       Established   217318    217732    6d 00:16:53
-------------------------------------------------------------------------------
No. of Sessions: 2
===============================================================================
apollo-mg00#
```

### 8.1.1.3 Confirm MPLS interfaces are operationally up

```
A:apollo-mg00# show router mpls interface

===============================================================================
MPLS Interfaces
===============================================================================
Interface                  Port-id         Adm    Opr    TE-metric
-------------------------------------------------------------------------------
system                     system          Up     Up     None
  Admin Groups                 None
  Srlg Groups                None
apollo-mg00-ieg1-1-1           1/1/1           Up     Up     None
  Admin Groups                 None
  Srlg Groups                None
apollo-mg00-ieg1-2-1           1/2/1           Up     Up     None
  Admin Groups                 None
  Srlg Groups                None
apollo-mg00-ieg1-2-2           1/2/2           Up     Up     None
  Admin Groups                 None
  Srlg Groups                None
-------------------------------------------------------------------------------
Interfaces : 4
===============================================================================
A:apollo-mg00#


A:osiris-mg00# show router mpls interface

===============================================================================
MPLS Interfaces
===============================================================================
Interface                  Port-id         Adm    Opr    TE-metric
-------------------------------------------------------------------------------
system                     system          Up     Up     None
  Admin Groups                 None
  Srlg Groups                None
osiris-mg00-ieg1-1-1           1/1/1           Up     Up     None
  Admin Groups                 None
  Srlg Groups                None
osiris-mg00-ieg1-2-1           1/2/1           Up     Up     None
  Admin Groups                 None
  Srlg Groups                None
osiris-mg00-ieg1-2-2           1/2/2           Up     Up     None
  Admin Groups                 None
  Srlg Groups                None
-------------------------------------------------------------------------------
Interfaces : 4
===============================================================================
osiris-mg00#
```

### 8.1.1.4 Confirm Path definitions are Administratively Up

```
A:osiris-mg00# show router mpls path
===============================================================================
MPLS Path:
===============================================================================
Path Name                    Adm  Hop Index   IP Address      Strict/Loose
-------------------------------------------------------------------------------
to-apollo-mg00-1              Up   1          172.16.6.8      Strict
-------------------------------------------------------------------------------
Total Paths : 1
===============================================================================
A:osiris-mg00#


A:apollo-mg00# show router mpls path
===============================================================================
MPLS Path:
===============================================================================
Path Name                    Adm  Hop Index   IP Address      Strict/Loose
-------------------------------------------------------------------------------
to-osiris-mg00-1              Up   1          172.16.6.6      Strict
-------------------------------------------------------------------------------
Total Paths : 1
===============================================================================
apollo-mg00#
```

### 8.1.1.5 Confirm LSPs are established using lsp-ping & lsp-trace

```
A:apollo-mg00# show router mpls lsp

===============================================================================
MPLS LSPs (Originating)
===============================================================================
LSP Name                     To              Fastfail     Adm   Opr
                                             Config
-------------------------------------------------------------------------------
to-osiris-mg00-lsp            172.16.6.6         No          Up    Up
-------------------------------------------------------------------------------
LSPs : 1
===============================================================================
A:apollo-mg00#

A:osiris-mg00# show router mpls lsp

===============================================================================
```

```
MPLS LSPs (Originating)
===============================================================================
LSP Name                        To              Fastfail     Adm   Opr
                                                Config
-------------------------------------------------------------------------------
to-apollo-mg00-lsp              172.16.6.8      No           Up    Up
-------------------------------------------------------------------------------
LSPs : 1
===============================================================================
A:osiris-mg00#
```

LSP ping and trace

```
A:apollo-mg00# oam lsp-ping to-osiris-mg00-lsp
LSP-PING to-osiris-mg00-lsp: 92 bytes MPLS payload
Seq=1, send from intf apollo-mg00-ieg1-1-1, reply from 172.16.6.6
      udp-data-len=32 ttl=255 rtt=0.462ms rc=3 (EgressRtr)

---- LSP to-osiris-mg00-lsp PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 0.462ms, avg = 0.462ms, max = 0.462ms, stddev = 0.000ms


A:apollo-mg00# oam lsp-trace to-osiris-mg00-lsp
lsp-trace to to-osiris-mg00-lsp: 0 hops min, 0 hops max, 116 byte packets
1  172.16.6.6  rtt=1.03ms rc=3(EgressRtr)
A:apollo-mg00#
-------------------------------------------------------------------------------

A:osiris-mg00# oam lsp-ping to-apollo-mg00-lsp
LSP-PING to-apollo-mg00-lsp: 92 bytes MPLS payload
Seq=1, send from intf osiris-mg00-ieg1-2-1, reply from 172.16.6.8
      udp-data-len=32 ttl=255 rtt=0.414ms rc=3 (EgressRtr)

---- LSP to-apollo-mg00-lsp PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 0.414ms, avg = 0.414ms, max = 0.414ms, stddev = 0.000ms


A:osiris-mg00# oam lsp-trace to-apollo-mg00-lsp
lsp-trace to to-apollo-mg00-lsp: 0 hops min, 0 hops max, 116 byte packets
1  172.16.6.8  rtt=0.463ms rc=3(EgressRtr)
A:osiris-mg00#
```

### **8.1.1.6** Confirm RSVP sessions are running

```
A:osiris-mg00# show router rsvp session

===============================================================================
RSVP Sessions
===============================================================================
From          To            Tunnel LSP   Name                    State
                            ID     ID
-------------------------------------------------------------------------------
172.16.6.6    172.16.6.8    1      17926 to-apollo-mg00-lsp::to-apol* Up
172.16.6.8    172.16.6.6    1      20998 to-osiris-mg00-lsp::to-osir* Up
-------------------------------------------------------------------------------
```

```
Sessions : 2
===============================================================================
* indicates that the corresponding row element may have been truncated.
A:osiris-mg00#


A:apollo-mg00# show router rsvp session

===============================================================================
RSVP Sessions
===============================================================================
From          To            Tunnel LSP   Name                    State
                            ID     ID
-------------------------------------------------------------------------------
172.16.6.6    172.16.6.8    1      17926 to-apollo-mg00-lsp::to-apol* Up
172.16.6.8    172.16.6.6    1      20998 to-osiris-mg00-lsp::to-osir* Up
-------------------------------------------------------------------------------
Sessions : 2
===============================================================================
* indicates that the corresponding row element may have been truncated.
apollo-mg00#
```

#### 8.1.1.7 Confirm T-LDP sessions have been established for service tunnels

```
A:osiris-mg00>config>router>ldp# show router ldp session

===============================================================================
LDP Sessions
===============================================================================
Peer LDP Id       Adj Type   State        Msg Sent  Msg Recv  Up Time
-------------------------------------------------------------------------------
172.16.6.2:0      Link       Established  187631    194278    6d 00:18:44
172.16.6.8:0      Both       Established  187639    217775    6d 00:18:46
-------------------------------------------------------------------------------
No. of Sessions: 2
===============================================================================
A:osiris-mg00>config>router>ldp#


A:apollo-mg00# show router ldp session

===============================================================================
LDP Sessions
===============================================================================
Peer LDP Id       Adj Type   State        Msg Sent  Msg Recv  Up Time
-------------------------------------------------------------------------------
172.16.6.3:0      Link       Established  187910    193994    6d 00:30:46
172.16.6.6:0      Both       Established  187637    217775    6d 00:18:40
-------------------------------------------------------------------------------
No. of Sessions: 2
===============================================================================
apollo-mg00#
```

#### 8.1.1.8 Confirm SDPs are established and using T-LDP for service tunnels

```
A:osiris-mg00# show service sdp

===============================================================================
Services: Service Destination Points
===============================================================================
SdpId    Adm MTU   Opr MTU   IP address      Adm  Opr        Deliver Signal
-------------------------------------------------------------------------------
5          0                 1550     172.16.6.8      Up   Up         MPLS    TLDP
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
===============================================================================
A:osiris-mg00# show service sdp-using

===============================================================================
SDP Using
===============================================================================
SvcId      SdpId             Type    Far End       Opr S* I.Label  E.Label
-------------------------------------------------------------------------------
20         5:20              Spok    172.16.6.8    Up    131064   131064
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
===============================================================================
* indicates that the corresponding row element may have been truncated.
A:osiris-mg00#


A:apollo-mg00# show service sdp

===============================================================================
Services: Service Destination Points
===============================================================================
SdpId    Adm MTU   Opr MTU   IP address      Adm  Opr        Deliver Signal
-------------------------------------------------------------------------------
5          0                 1550     172.16.6.6      Up   Up         MPLS    TLDP
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
===============================================================================
A:apollo-mg00# show service sdp-using

===============================================================================
SDP Using
===============================================================================
SvcId      SdpId             Type    Far End       Opr S* I.Label  E.Label
-------------------------------------------------------------------------------
20         5:20              Spok    172.16.6.6    Up    131064   131064
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
===============================================================================
* indicates that the corresponding row element may have been truncated.
A:apollo-mg00#
```

### **8.1.1.9** Confirm SAP and Cpipe service are established

```
A:osiris-mg00# show service sap-using

===============================================================================
Service Access Points
===============================================================================
PortId                  SvcId     Ing. Ing.   Egr. Egr.   Adm  Opr
                                  QoS  Fltr    QoS  Fltr
-------------------------------------------------------------------------------
1/5/1.1                 20        1    none    1    none   Up   Up
-------------------------------------------------------------------------------
Number of SAPs : 1
-------------------------------------------------------------------------------
===============================================================================

A:osiris-mg00#

A:apollo-mg00# show service sap-using

===============================================================================
Service Access Points
===============================================================================
PortId                  SvcId     Ing. Ing.   Egr. Egr.   Adm  Opr
                                  QoS  Fltr    QoS  Fltr
-------------------------------------------------------------------------------
1/3/1.1                 20        1    none    1    none   Up   Up
-------------------------------------------------------------------------------
Number of SAPs : 1
-------------------------------------------------------------------------------
===============================================================================

A:apollo-mg00#


A:osiris-mg00# show service service-using

===============================================================================
Services
===============================================================================
ServiceId  Type      Adm  Opr  CustomerId Service Name
-------------------------------------------------------------------------------
3          VPRN      Up   Up   10
20         Cpipe     Up   Up   10
-------------------------------------------------------------------------------
Matching Services : 2
-------------------------------------------------------------------------------
===============================================================================
A:osiris-mg00#

A:apollo-mg00# show service service-using

===============================================================================
Services
===============================================================================
ServiceId  Type      Adm  Opr  CustomerId Service Name
-------------------------------------------------------------------------------
3          VPRN      Up   Up   10
20         Cpipe     Up   Up   10
```

```
--------------------------------------------------------------------------------
Matching Services : 2
--------------------------------------------------------------------------------
================================================================================
A:apollo-mg00#
```

### 8.1.1.10 Sunrise SSMTT-45 IEEE C37.94 Module Test

The G.821 Bit Error Rate Test (BERT) was run for one (1) hour. The results were saved in a .csv format and extracted from the tester. See extracted results are seen below.

| | | | | |
|---|---|---|---|---|
| ---------- | | | | |
| SUNRISE TELECOM Incorporated | | | | |
| Chassis S/N | | : 290978 | | |
| Base SW Version | | : 6.12.02 | | |
| Module SW Version | | : 6.11.03 | | |
| Module Type | | : SSMTT-45 IEEE C37.94 | | |
| Module S/N | | : 101024 | | |
| Module Rev. | | : 1 | | |
| | | | | |
| File Name | | : MEAS0022 | | |
| Date Saved | | : 11:55:36 07/03/14 | | |
| ---------- | | | | |
| | | | | |
| PROFILE | :DEFAULT | | | |
| ---------- | | | | |
| | | | | |
| ET: | 1:00:00 | | RT: | CONTINUE |
| TxHz: | 1x64 | K | TxPAT: | 2.00E+15 |
| | | | | |
| TIME STAMP========== | | | | |
| START TIME : | | 14/07/2003 | 10:55:33 | |
| STOP TIME : | | 14/07/2003 | 11:55:34 | |
| ELAPSED TIME : | | 1:00:00 | | |
| | | | | |
| SUMMARY========== | | | | |
| ERROR DET | | | | |
| BIT : | 747 | | PATL: | 3 |
| POWER: | -16.3 | dBm | FREQ: | 2048033 |
| | | | | |
| BIT ERROR - G.821========== | | | | |
| RxHz: | 1x64 | K | RxPAT: | 2.00E+15 |
| BIT: | 747 | | BER : | 3.20E-06 |
| ES : | 4 | | %ES : | 0.11 |

| | | | | |
|---|---|---|---|---|
| SES: | 4 | | %SES: | 0.11 |
| EFS: | 3596 | | %EFS: | 99.89 |
| AS : | 3600 | | %AS : | 100 |
| UAS: | 0 | | %UAS: | 0 |
| | | | | |
| ALARM/DEFECT========== | | | | |
| LOS : | 0 | | POWER: | 0 |
| LOF : | 0 | | POWER: | 0 |
| AIS : | 0 | | POWER: | 0 |
| YEL : | 0 | | POWER: | 0 |
| PATL: | 3 | | POWER: | 3 |
| | | | | |
| OPTICAL POWER MEASUREMENT========== | | | | |
| POWER: | -16.3 | dBm | | |
| MIN: | -17.5 | dBm | MAX: | -16.1 |

### 8.1.2 Network functionality testing and analysis

#### **8.1.2.1** Latency and Jitter Characterisation – RSVP-TE

**Test Setup 1**

| **LSP path through adjacent routers** | | | |
|---|---|---|---|
| Jitter-buffer (ms) | Payload Size (octets) | Average Latency measured | Maximum Latency variation |
| 32 | 64 | 27.431 | +/- 81 |
| 1 | 2 | 4.267 | +/- 92 |
| 2 | 2 | 4.732 | +/- 65 |
| 2 | 4 | 5.015 | +/- 74 |
| 3 | 2 | 5.245 | +/- 72 |
| 3 | 4 | 5.502 | +/- 77 |
| 3 | 8 | 5.511 | +/- 74 |
| 4 | 2 | 5.770 | +/- 74 |
| 4 | 4 | 6.027 | +/- 77 |
| 4 | 8 | 6.292 | +/- 77 |
| 4 | 12 | 6.547 | +/- 80 |
| 6 | 2 | 6.804 | +/- 75 |
| 6 | 4 | 7.066 | +/- 71 |
| 6 | 8 | 7.324 | +/- 76 |
| 6 | 12 | 7.589 | +/- 72 |
| 8 | 4 | 7.841 | +/- 77 |
| 8 | 6 | 8.101 | +/- 75 |
| 8 | 8 | 8.356 | +/- 71 |
| 8 | 12 | 8.620 | +/- 79 |

| | | | |
|---|---|---|---|
| 8 | 16 | 8.773 | +/- 79 |
| 10 | 4 | 8.896 | +/- 76 |
| 10 | 8 | 9.223 | +/- 73 |
| 10 | 16 | 9.551 | +/- 74 |
| 10 | 24 | 9.877 | +/- 72 |
| 12 | 6 | 10.204 | +/- 72 |
| 12 | 12 | 10.531 | +/- 78 |
| 12 | 24 | 10.858 | +/- 74 |
| 14 | 6 | 11.185 | +/- 77 |
| 14 | 12 | 12.162 | +/- 77 |
| 14 | 24 | 13.452 | +/- 73 |
| 16 | 4 | 11.843 | +/- 75 |
| 16 | 10 | 12.167 | +/- 73 |
| 16 | 32 | 15.376 | +/- 81 |

**Table 8.1 – Latency testing: adjacent routers (Lab)**

**Test Setup 2**

| **LSP path through four (4) routers** | | | |
|---|---|---|---|
| Jitter-buffer | Payload Size | Average latency measured | Maximum Latency variation |
| 32 | 64 | 27.642 | +/- 83 |
| 1 | 2 | 4.352 | +/- 77 |
| 2 | 2 | 4.746 | +/- 71 |
| 2 | 4 | 5.026 | +/- 73 |
| 3 | 2 | 5.252 | +/- 75 |
| 3 | 4 | 5.506 | +/- 76 |
| 3 | 8 | 5.524 | +/- 76 |
| 4 | 2 | 5.784 | +/- 77 |
| 4 | 4 | 6.032 | +/- 78 |
| 4 | 8 | 6.304 | +/- 80 |
| 4 | 12 | 6.594 | +/- 74 |
| 6 | 2 | 6.906 | +/- 78 |
| 6 | 4 | 7.152 | +/- 71 |
| 6 | 8 | 7.479 | +/- 72 |
| 6 | 12 | 7.806 | +/- 74 |
| 8 | 4 | 8.133 | +/- 74 |
| 8 | 6 | 8.462 | +/- 70 |
| 8 | 8 | 8.777 | +/- 75 |
| 8 | 12 | 9.116 | +/- 84 |
| 8 | 16 | 9.442 | +/- 73 |
| 10 | 4 | 9.768 | +/- 79 |
| 10 | 8 | 10.099 | +/- 77 |
| 10 | 16 | 10.421 | +/- 72 |
| 10 | 24 | 10.749 | +/- 74 |
| 12 | 6 | 11.074 | +/- 71 |
| 12 | 12 | 11.405 | +/- 73 |
| 12 | 24 | 11.733 | +/- 77 |

| | | | |
|---|---|---|---|
| 14 | 6 | 12.057 | +/- 77 |
| 14 | 12 | 12.866 | +/- 75 |
| 14 | 24 | 13.461 | +/- 74 |
| 16 | 4 | 12.011 | +/- 74 |
| 16 | 10 | 12.208 | +/- 78 |
| 16 | 32 | 15.469 | +/- 81 |

**Table 8.2 – Latency testing: 4 routers (Lab)**

### **8.1.2.2** Quality of Service Impact Characterisation

| **Test Configuration** | **QoS Markings** | **1 Gbs injected traffic** |
|---|---|---|
| **Setup 1** | No | Nil |
| **Setup 2** | No | Full line speed |
| **Setup 3** | No | Burst traffic 80% duty cycle |
| **Setup 4** | Yes | Full line speed |
| **Setup 5** | Yes | Burst traffic 80% duty cycle |

**Setup 1** – Protection link stable

The link was stable. The results below show that the 'Offered' data is being passed through the default Ingress Queue 1. This queue has a low priority however the link remains stable while there is little other traffic on the router.

*A:apollo-mg00>config>service>cpipe>sap# show service id 20 sap 1/3/1.1 stats

```
===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id        : 20
SAP               : 1/3/1.1              Encap          : cem
Description       : (Not Specified)
Admin State       : Up                   Oper State     : Up
Flags             : None
Multi Svc Site    : None
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                      Packets                Octets
Ingress Queue 1 (Priority)
Off. HiPrio           : 241746               483492
Off. LoPrio           : n/a                  n/a
Dro. HiPrio           : 0                    0
Dro. LoPrio           : n/a                  n/a
For. InProf           : 241746               483492
For. OutProf          : 0                    0

Egress Queue 1
For. InProf           : n/a                  n/a
For. OutProf          : n/a                  n/a
Dro. InProf           : n/a                  n/a
```

```
Dro. OutProf        : n/a                  n/a
===============================================================================
*A:apollo-mg00>config>service>cpipe>sap#
```

**Setup 2** – Protection link unstable

The protection signalling link fails. As seen below all traffic is being passed in Queue 1 however, due to the low priority the Protection traffic has been given the link cannot remain stable. The relay shows inconsistent propagation delay times for the circuit before failing completely.

```
===============================================================================
Queue Statistics
===============================================================================

-------------------------------------------------------------------------------
Ingress Queue  1           Packets              Octets
    In Profile  forwarded :    0                    0
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    9865148              9957975452
    Out Profile dropped   :    0                    0
Ingress Queue  7           Packets              Octets
    In Profile  forwarded :    0                    0
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    0                    0
    Out Profile dropped   :    0                    0
Ingress Queue CTL          Packets              Octets
    Forwarded :            942                  94768
    Dropped   :            0                    N/A

Egress Queue  1            Packets              Octets
    In Profile  forwarded :    327662               19659720
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    9537770              9938356340
    Out Profile dropped   :    0                    0
Egress Queue  7            Packets              Octets
    In Profile  forwarded :    0                    0
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    0                    0
    Out Profile dropped   :    0                    0
Egress Queue CTL           Packets              Octets
    Forwarded :            1018                 74168
    Dropped   :            0                    N/A
===============================================================================
*A:apollo-mg00#
```

**Setup 3** – Protection link stable

```
A:apollo-mg00# show service id 20 sap 1/3/1.1 stats

===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id        : 20
SAP               : 1/3/1.1              Encap            : cem
Description       : (Not Specified)
Admin State       : Up                   Oper State       : Up
Flags             : None
```

```
Multi Svc Site     : None
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                    Packets              Octets

Ingress Queue 1 (Priority)
Off. HiPrio          : 0                  0
Off. LoPrio          : n/a                n/a
Dro. HiPrio          : 0                  0
Dro. LoPrio          : n/a                n/a
For. InProf          : 0                  0
For. OutProf         : 0                  0

Ingress Queue 7 (Priority)
Off. HiPrio          : 2550518            5101036
Off. LoPrio          : n/a                n/a
Dro. HiPrio          : 0                  0
Dro. LoPrio          : n/a                n/a
For. InProf          : 2550518            5101036
For. OutProf         : 0                  0

Egress Queue 1
For. InProf          : n/a                n/a
For. OutProf         : n/a                n/a
Dro. InProf          : n/a                n/a
Dro. OutProf         : n/a                n/a
===============================================================================
A:apollo-mg00#
```

**Setup 4** – Protection link stable

```
===============================================================================
Queue Statistics
===============================================================================

-------------------------------------------------------------------------------
Ingress Queue  1           Packets              Octets
    In Profile  forwarded :    13323561             13732047276
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    0                    0
    Out Profile dropped   :    0                    0
Ingress Queue  7           Packets              Octets
    In Profile  forwarded :    296837               17810220
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    0                    0
    Out Profile dropped   :    0                    0
Ingress Queue CTL          Packets              Octets
    Forwarded :              1293                 130267
    Dropped   :              0                    N/A

Egress Queue  1            Packets              Octets
    In Profile  forwarded :    13323561             13732047276
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    0                    0
    Out Profile dropped   :    0                    0
Egress Queue  7            Packets              Octets
    In Profile  forwarded :    223874               13432440
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    0                    0
```

```
    Out Profile dropped   :    0                  0
Egress Queue CTL            Packets              Octets
    Forwarded :             1403                 103132
    Dropped   :             0                    N/A
===============================================================================
*A:apollo-mg00>config>service>cpipe>sap#
```

**Setup 5** – Protection link stable

```
===============================================================================
Queue Statistics
===============================================================================

-------------------------------------------------------------------------------
Ingress Queue  1            Packets              Octets
    In Profile  forwarded :    3286659              3424698678
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    0                    0
    Out Profile dropped   :    0                    0
Ingress Queue  7            Packets              Octets
    In Profile  forwarded :    654885               39293100
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    0                    0
    Out Profile dropped   :    0                    0
Ingress Queue CTL           Packets              Octets
    Forwarded :             1874                 187908
    Dropped   :             0                    N/A

Egress Queue  1             Packets              Octets
    In Profile  forwarded :    3287108              3425166536
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    0                    0
    Out Profile dropped   :    0                    0
Egress Queue  7             Packets              Octets
    In Profile  forwarded :    654888               39293280
    In Profile  dropped   :    0                    0
    Out Profile forwarded :    0                    0
    Out Profile dropped   :    0                    0
Egress Queue CTL            Packets              Octets
    Forwarded :             2034                 148832
    Dropped   :             0                    N/A
===============================================================================
A:apollo-mg00#
```

### **8.1.2.3** Traffic Engineering Impact Characterisation

Some basic calculations were performed to establish a precise failover/failback time. As follows:

The JDSU3000c test unit displays TX & RX bytes. The tester is set to run at a constant 1Gbs speed.

1 bit = 0.125 bytes

Example test result:

Tx bytes – 3153803594

Rx bytes – 2876655207

Therefore, 3153803594 – 2876655207 = 277148378

**Convert bytes to bits**

277148378 x 8 = 2217187096

So at 1Gbs,

$$\frac{2217187096}{100000000} = 2217\ milliseconds$$

**Failover Results (in lost bytes)**

| | **Setup 1** | **Setup 2** | **Setup 3** | **Setup 4** |
|---|---|---|---|---|
| **Failover** | No failover | 99519054 | 30005744 | 2125406 |
| **Failback** | No failback | Negligible | Negligible | Negligible |

Using the example calculations above, the failover times were found as:

**Failover Results (in milliseconds)**

| | **Setup 1** | **Setup 2** | **Setup 3** | **Setup 4** |
|---|---|---|---|---|
| **Failover** | N/A | 796 | 240 | 17 |
| **Failback** | N/A | 2877 | 1565 | 395 |

It should be noted that while failback times are given, there was no traffic lost in the process. The failback time is also highly reliant on multiple factors including the configuration of the RSVP hello message interval. The default value of this message timer is set at 3 seconds. Further investigation into optimising this has been considered outside the project scope.

#### **8.1.2.4** Failure Modes

The results of the failure cases are shown in the table below.

| | **Setup 1** | **Setup 2** |
|---|---|---|
| **Line card failure** | Nil | Nil |
| **CSM failure** | Nil | Nil |
| **CSM manual switch** | Nil | Nil |
| **Full node failure** | 2:34 minutes | 21 ms |

**Table 8.3 – Failure Case Test Results**

These results clearly show that failure of redundant hardware in the ALU 7705 SAR-8 does not affect the delivery of any traffic.

### 8.1.3 Protection relay functionality results

#### **8.1.3.1** Forward/Reverse Stability tests

The below results extracted from the P541 relay, show expected values for differential and bias currents.

**Forward Stability Results**

| | |
|---|---|
| IA Magnitude | 596.8 A |
| IA Phase Angle | 0 deg |
| IB Magnitude | 595.2 A |
| IB Phase Angle | −119.7 deg |
| IC Magnitude | 596.5 A |
| IC Phase Angle | 120.1 deg |
| IN Measured Mag | 0 A |
| IN Measured Ang | 0 deg |
| IN Derived Mag | 0 A |
| IN Derived Angle | 0 deg |
| I1 Magnitude | 596.1 A |
| I2 Magnitude | 0 A |
| I0 Magnitude | 0 A |
| IA RMS | 595.1 A |
| IB RMS | 595.7 A |
| IC RMS | 598.7 A |
| Frequency | 50.00 Hz |
| IA Fixed Demand | 0 A |
| IB Fixed Demand | 0 A |
| IC Fixed Demand | 0 A |
| IA Roll Demand | 0 A |
| IB Roll Demand | 0 A |
| IC Roll Demand | 0 A |
| IA Peak Demand | 597.1 A |
| IB Peak Demand | 597.3 A |
| IC Peak Demand | 597.9 A |
| IA local | 591.8 A |
| IA Angle local | 0 deg |
| IB local | 591.8 A |
| IB Angle local | −119.8 deg |
| IC local | 592.7 A |
| IC Angle local | 120.0 deg |
| IA remote 1 | 595.7 A |
| IA Ang remote 1 | −179.0 deg |
| IB remote 1 | 595.7 A |
| IB Ang remote 1 | 61.44 deg |
| IC remote 1 | 595.7 A |
| IC Ang remote 1 | −57.96 deg |
| IA Differential | 12.40 A |
| IB Differential | 14.11 A |
| IC Differential | 12.56 A |
| IA Bias | 593.7 A |
| IB Bias | 593.7 A |
| IC Bias | 594.2 A |
| Ch 1 Prop Delay | 4.625ms |
| Channel Status | 0000000001111 |
| Elapsed Time | 86.32ks |
| Ch1 No.Vald Mess | 17249214 |
| Ch1 No.Err Mess | 6 |

| | |
|---|---|
| Ch1 No.Errored s | 4 |
| Ch1 No.Sev Err s | 0 |
| Ch1 No.Dgraded m | 2 |
| CB Operations | 0 |
| Total IA Broken | 0 A |
| Total IB Broken | 0 A |
| Total IC Broken | 0 A |
| CB Operate Time | 0 s |
| Opto I/P Status | 00000000 |
| Relay O/P Status | 0000000 |
| Test Port Status | 00000000 |
| LED Status | 00000000 |
| Ctrl I/P Status | 00000000000000000000000000000000 |

## Reverse Stability Results

| | |
|---|---|
| IA Magnitude | 597.6 A |
| IA Phase Angle | 0 deg |
| IB Magnitude | 596.6 A |
| IB Phase Angle | −119.9 deg |
| IC Magnitude | 597.2 A |
| IC Phase Angle | 119.9 deg |
| IN Measured Mag | 0 A |
| IN Measured Ang | 0 deg |
| IN Derived Mag | 0 A |
| IN Derived Angle | 0 deg |
| I1 Magnitude | 597.1 A |
| I2 Magnitude | 0 A |
| I0 Magnitude | 0 A |
| IA RMS | 595.1 A |
| IB RMS | 595.8 A |
| IC RMS | 598.5 A |
| Frequency | 50.01 Hz |
| IA Fixed Demand | 9.940 A |
| IB Fixed Demand | 9.929 A |
| IC Fixed Demand | 9.946 A |
| IA Roll Demand | 9.940 A |
| IB Roll Demand | 9.929 A |
| IC Roll Demand | 9.946 A |
| IA Peak Demand | 598.4 A |
| IB Peak Demand | 598.7 A |
| IC Peak Demand | 599.8 A |
| IA local | 592.4 A |
| IA Angle local | 0 deg |
| IB local | 591.4 A |
| IB Angle local | −119.4 deg |
| IC local | 593.5 A |
| IC Angle local | 120.3 deg |
| IA remote 1 | 595.7 A |
| IA Ang remote 1 | −179.7 deg |
| IB remote 1 | 595.7 A |
| IB Ang remote 1 | 59.98 deg |
| IC remote 1 | 595.7 A |
| IC Ang remote 1 | −59.58 deg |
| IA Differential | 4.303 A |
| IB Differential | 5.084 A |
| IC Differential | 3.690 A |
| IA Bias | 593.9 A |
| IB Bias | 593.8 A |
| IC Bias | 594.6 A |
| Ch 1 Prop Delay | 4.787ms |
| Channel Status | 0000000001111 |
| Elapsed Time | 87.21ks |
| Ch1 No.Vald Mess | 17426214 |
| Ch1 No.Err Mess | 6 |
| Ch1 No.Errored s | 4 |
| Ch1 No.Sev Err s | 0 |
| Ch1 No.Dgraded m | 2 |
| CB Operations | 0 |
| Total IA Broken | 0 A |

```
Total IB Broken                 0 A
Total IC Broken                 0 A
CB Operate Time                 17.12 s
Opto I/P Status                 00000000
Relay O/P Status                0000000
Test Port Status                00000000
LED Status                      00000000
Ctrl I/P Status                 00000000000000000000000000000000
```

#### **8.1.3.2** 3 phase In-zone Fault

The results of the 3 phase in-zone fault tests are shown from the protection suite software result window below.

**Timer Results of 2014-08-19 14:22:03**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | NMK | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 24.7 ms | -50.60 % | ✓ |
| 2 | AGE | Fault | LN2 | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 22.8 ms | -54.40 % | ✓ |

Protection operated (tripped) times

- NMK – 24.7ms
- AGE – 22.8ms

#### **8.1.3.3** Single phase thru Fault

The results of the single phase thru fault tests are shown from the protection suite software result window below.

**Timer Results of 2014-08-19 14:27:22**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | NMK | Fault | LN2 | No Op | | | | | Error | NoOp | | | ✓ |
| 2 | AGE | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

The window shows that neither of the relays operated as expected in the test plan.

#### **8.1.3.4** Single phase In-zone Fault

The results of the single phase in-zone fault tests are shown from the protection suite software result window below.

**Timer Results of 2014-08-19 14:31:11**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | NMK | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 24.5 ms | -51.00 % | ✓ |
| 2 | AGE | Fault | LN2 | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 22.6 ms | -54.80 % | ✓ |

Protection operated (tripped) times

- NMK – 24.5ms

- AGE – 22.6ms

#### **8.1.3.5** Bias Restraint (In-zone & Out-of-zone)

Bias restraint testing will only be performed in the field tests and not in the laboratory. Bias restraint test results will be compared to the test results from the TDM production circuit that is currently operational in the field.

## 8.2 IP/MPLS production network tests

### 8.2.1 Network functionality testing and analysis

#### **8.2.1.1** Latency and Jitter Characteristic – RSVP-TE

**Test Setup**

| **LSP path through production system** | | | |
|---|---|---|---|
| Jitter-buffer (ms) | Payload Size (octets) | Average Latency measured (ms) | Average Jitter measured (µs) |
| 32 | 64 | 27.55 | +/- 80 |
| 1 | 2 | 4.309 | +/- 95 |
| 2 | 4 | 4.529 | +/- 65 |
| 2 | 2 | 4.365 | +/- 66 |
| 3 | 2 | 5.184 | +/- 77 |
| 3 | 4 | 5.444 | +/- 71 |
| 3 | 8 | 5.608 | +/- 85 |
| 4 | 2 | 5.961 | +/- 68 |
| 4 | 4 | 6.209 | +/- 75 |
| 4 | 8 | 6.570 | +/- 72 |
| 4 | 12 | 6.737 | +/- 77 |
| 6 | 2 | 7.010 | +/- 77 |
| 6 | 4 | 7.248 | +/- 81 |
| 6 | 8 | 7.522 | +/- 74 |
| 6 | 12 | 7.767 | +/- 75 |
| 8 | 4 | 7.981 | +/- 77 |
| 8 | 6 | 8.203 | +/- 78 |
| 8 | 8 | 8.537 | +/- 72 |
| 8 | 12 | 8.804 | +/- 82 |
| 8 | 16 | 8.985 | +/- 75 |
| 10 | 4 | 9.058 | +/- 79 |
| 10 | 8 | 9.711 | +/- 72 |
| 10 | 16 | 10.324 | +/- 75 |
| 10 | 24 | 10.944 | +/- 74 |
| 12 | 6 | 11.590 | +/- 77 |
| 12 | 12 | 12.232 | +/- 76 |
| 12 | 24 | 12.865 | +/- 73 |
| 14 | 6 | 13.488 | +/- 75 |
| 14 | 12 | 14.122 | +/- 78 |
| 14 | 24 | 14.754 | +/- 75 |
| 16 | 4 | 14.763 | +/- 77 |
| 16 | 10 | 15.935 | +/- 77 |
| 16 | 32 | 15.626 | +/- 81 |

#### **8.2.1.2** Quality of Service Impact Characterisation

Due to the critical nature of the Production network being used for testing there are constraints on the depth of QoS testing that can be performed. It has been decided that the risk involved with injecting full line rate (1Gbs) traffic is too high as this could affect other mission critical services running on the Production IP/MPLS network. Therefore, protection circuit will not be tested with simulated traffic on the network. The system will be simply tested with the current level of actual traffic in the network at the time of the testing. The test configurations to be used are described below.

| Test Configuration | QoS Markings | Background network traffic |
|---|---|---|
| **Setup 1** | No | Yes |
| **Setup 2** | Yes | Yes |

**Setup 1**

```
B:xssnmk-mg00# show service id 100 sap 1/3/1.1 stats

===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id        : 100
SAP               : 1/3/1.1              Encap            : cem
Description       : (Not Specified)
Admin State       : Up                   Oper State       : Up
Flags             : None
Multi Svc Site    : None
Last Status Change : 08/21/2014 16:12:27
Last Mgmt Change   : 08/21/2014 13:47:23
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                    Packets                Octets

Ingress Queue 1 (Priority)
Off. HiPrio           : 846910               1693820
Off. LoPrio           : n/a                  n/a
Dro. HiPrio           : 0                    0
Dro. LoPrio           : n/a                  n/a
For. InProf           : 846910               1693820
For. OutProf          : 0                    0

Egress Queue 1
For. InProf           : n/a                  n/a
For. OutProf          : n/a                  n/a
Dro. InProf           : n/a                  n/a
Dro. OutProf          : n/a                  n/a
===============================================================================
B:xssnmk-mg00#
```

**Setup 2**

```
*B:xssnmk-mg00>config>service>cpipe>sap# show service id 100 sap 1/3/1.1 stats

===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id        : 100
SAP               : 1/3/1.1              Encap            : cem
Description       : (Not Specified)
Admin State       : Up                   Oper State       : Up
Flags             : None
Multi Svc Site    : None
Last Status Change : 08/21/2014 16:12:27
Last Mgmt Change   : 08/23/2014 11:00:52
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                    Packets                Octets

Ingress Queue 1 (Priority)
Off. HiPrio           : 49853                99706
Off. LoPrio           : n/a                  n/a
Dro. HiPrio           : 0                    0
Dro. LoPrio           : n/a                  n/a
For. InProf           :  49853               99706
For. OutProf          : 0                    0

Ingress Queue 7 (Priority)
Off. HiPrio           : 163903               327806
Off. LoPrio           : n/a                  n/a
Dro. HiPrio           : 0                    0
Dro. LoPrio           : n/a                  n/a
For. InProf           : 163903               327806
For. OutProf          : 0                    0

Egress Queue 1
For. InProf           : n/a                  n/a
For. OutProf          : n/a                  n/a
Dro. InProf           : n/a                  n/a
Dro. OutProf          : n/a                  n/a
===============================================================================
*B:xssnmk-mg00>config>service>cpipe>sap#
```

### **8.2.1.3** Traffic Engineering Impact Characterisation

Due to the critical nature of the Production network Traffic Engineering testing will not be performed on this network. The failing of production links has been considered as too great of a risk to mission critical services. The laboratory testing on traffic engineered paths and failovers provided valuable results in this regard, however further testing is recommended.

#### **8.2.1.4** Failure Modes

Due to critical services running in the Production network Failure modes will not be tested. The test results from the laboratory tests have been deemed as sufficient data proving that failing of redundant hardware in the 7705 SAR-8 chassis has no effect on the protection circuit traffic.

### 8.2.2 Protection relay functionality testing

The following show the results of the testing at both ends of the circuit on both the test and production circuit.

#### **8.2.2.1** Forward/Reverse Stability tests

**IP/MPLS test circuit (AGE-end)**

Forward stability

**Timer Results of 2014-09-10 11:18:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Pre-Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

Data extracted from P541 relay

```
Stability Forward AGE F675
IA Magnitude                597.0 A
IA Phase Angle              0 deg
IB Magnitude                594.3 A
IB Phase Angle              -119.7 deg
IC Magnitude                595.3 A
IC Phase Angle              120.2 deg
IN Measured Mag             0 A
IN Measured Ang             0 deg
IN Derived Mag              0 A
IN Derived Angle            0 deg
I1 Magnitude                595.5 A
I2 Magnitude                0 A
I0 Magnitude                0 A
IA RMS                      596.3 A
IB RMS                      594.6 A
IC RMS                      596.2 A
Frequency                   50.01 Hz
IA Fixed Demand             0 A
IB Fixed Demand             0 A
IC Fixed Demand             0 A
IA Roll Demand              0 A
IB Roll Demand              0 A
IC Roll Demand              0 A
IA Peak Demand              596.9 A
IB Peak Demand              597.7 A
```

| | |
|---|---|
| IC Peak Demand | 597.9 A |
| IA local | 593.1 A |
| IA Angle local | 0 deg |
| IB local | 593.3 A |
| IB Angle local | −119.8 deg |
| IC local | 593.3 A |
| IC Angle local | 120.2 deg |
| IA remote 1 | 593.8 A |
| IA Ang remote 1 | 178.7 deg |
| IB remote 1 | 593.8 A |
| IB Ang remote 1 | 58.39 deg |
| IC remote 1 | 593.8 A |
| IC Ang remote 1 | −61.01 deg |
| IA Differential | 12.55 A |
| IB Differential | 17.28 A |
| IC Differential | 13.57 A |
| IA Bias | 593.4 A |
| IB Bias | 593.5 A |
| IC Bias | 593.5 A |
| Ch 1 Prop Delay | 4.825ms |
| Channel Status | 0000000001111 |
| Elapsed Time | 434.0 s |
| Ch1 No.Vald Mess | 86858 |
| Ch1 No.Err Mess | 0 |
| Ch1 No.Errored s | 0 |
| Ch1 No.Sev Err s | 0 |
| Ch1 No.Dgraded m | 0 |
| CB Operations | 3 |
| Total IA Broken | 11.55MA |
| Total IB Broken | 11.51MA |
| Total IC Broken | 11.54MA |
| CB Operate Time | 13.42 s |
| Opto I/P Status | 00000000 |
| Relay O/P Status | 0000000 |
| Test Port Status | 00000000 |
| LED Status | 00000000 |
| Ctrl I/P Status | 00000000000000000000000000000000 |

## Reverse stability

**Timer Results of 2014-09-10 11:22:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Pre-Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## Data extracted from P541 relay

Stability Reverse AGE F675

| | |
|---|---|
| IA Magnitude | 596.8 A |
| IA Phase Angle | 0 deg |
| IB Magnitude | 596.0 A |
| IB Phase Angle | −119.6 deg |
| IC Magnitude | 595.2 A |
| IC Phase Angle | 120.2 deg |
| IN Measured Mag | 0 A |
| IN Measured Ang | 0 deg |
| IN Derived Mag | 0 A |
| IN Derived Angle | 0 deg |
| I1 Magnitude | 596.0 A |
| I2 Magnitude | 0 A |
| I0 Magnitude | 0 A |
| IA RMS | 596.1 A |
| IB RMS | 596.5 A |
| IC RMS | 596.0 A |
| Frequency | 50.02 Hz |

| | |
|---|---|
| IA Fixed Demand | 0 A |
| IB Fixed Demand | 0 A |
| IC Fixed Demand | 0 A |
| IA Roll Demand | 0 A |
| IB Roll Demand | 0 A |
| IC Roll Demand | 0 A |
| IA Peak Demand | 597.5 A |
| IB Peak Demand | 597.7 A |
| IC Peak Demand | 597.9 A |
| IA local | 591.4 A |
| IA Angle local | 0 deg |
| IB local | 591.9 A |
| IB Angle local | −119.7 deg |
| IC local | 592.4 A |
| IC Angle local | 120.2 deg |
| IA remote 1 | 591.8 A |
| IA Ang remote 1 | −179.8 deg |
| IB remote 1 | 591.8 A |
| IB Ang remote 1 | 60.80 deg |
| IC remote 1 | 591.8 A |
| IC Ang remote 1 | −59.50 deg |
| IA Differential | 3.113 A |
| IB Differential | 4.292 A |
| IC Differential | 4.014 A |
| IA Bias | 591.6 A |
| IB Bias | 591.9 A |
| IC Bias | 592.1 A |
| Ch 1 Prop Delay | 4.809ms |
| Channel Status | 0000000001111 |
| Elapsed Time | 676.0 s |
| Ch1 No.Vald Mess | 135258 |
| Ch1 No.Err Mess | 0 |
| Ch1 No.Errored s | 0 |
| Ch1 No.Sev Err s | 0 |
| Ch1 No.Dgraded m | 0 |
| CB Operations | 3 |
| Total IA Broken | 11.55MA |
| Total IB Broken | 11.51MA |
| Total IC Broken | 11.54MA |
| CB Operate Time | 13.42 s |
| Opto I/P Status | 00000000 |
| Relay O/P Status | 0000000 |
| Test Port Status | 00000000 |
| LED Status | 00000000 |
| Ctrl I/P Status | 00000000000000000000000000000000 |

## TDM production circuit (AGE-end)

Forward stability

**Timer Results of 2014-08-05 10:21:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Pre-Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

Reverse stability

**Timer Results of 2014-08-05 10:25:10**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Pre-Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

## IP/MPLS test circuit (NMK-end)

## Forward

**Timer Results of 2014-09-10 11:18:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Pre-Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## Data extracted from P541 relay

| | |
|---|---|
| Stability Forward NMK F675 | |
| IA Magnitude | 598.3 A |
| IA Phase Angle | 0 deg |
| IB Magnitude | 598.7 A |
| IB Phase Angle | −119.7 deg |
| IC Magnitude | 596.9 A |
| IC Phase Angle | 120.2 deg |
| IN Measured Mag | 0 A |
| IN Measured Ang | 0 deg |
| IN Derived Mag | 4.636 A |
| IN Derived Angle | −70.67 deg |
| I1 Magnitude | 597.9 A |
| I2 Magnitude | 0 A |
| I0 Magnitude | 1.545 A |
| IA RMS | 597.1 A |
| IB RMS | 598.5 A |
| IC RMS | 597.9 A |
| Frequency | 49.99 Hz |
| IA Fixed Demand | 0 A |
| IB Fixed Demand | 0 A |
| IC Fixed Demand | 0 A |
| IA Roll Demand | 0 A |
| IB Roll Demand | 0 A |
| IC Roll Demand | 0 A |
| IA Peak Demand | 598.5 A |
| IB Peak Demand | 598.8 A |
| IC Peak Demand | 599.0 A |
| IA local | 594.7 A |
| IA Angle local | 0 deg |
| IB local | 596.0 A |
| IB Angle local | −119.9 deg |
| IC local | 595.1 A |
| IC Angle local | 120.2 deg |
| IA remote 1 | 591.8 A |
| IA Ang remote 1 | 179.4 deg |
| IB remote 1 | 589.8 A |
| IB Ang remote 1 | 60.01 deg |
| IC remote 1 | 591.8 A |
| IC Ang remote 1 | −60.29 deg |
| IA Differential | 5.834 A |
| IB Differential | 6.461 A |
| IC Differential | 7.189 A |
| IA Bias | 593.3 A |
| IB Bias | 592.9 A |
| IC Bias | 593.5 A |
| Ch 1 Prop Delay | 4.758ms |
| Channel Status | 0000000001111 |
| Elapsed Time | 411.0 s |
| Ch1 No.Vald Mess | 82433 |
| Ch1 No.Err Mess | 0 |
| Ch1 No.Errored s | 0 |
| Ch1 No.Sev Err s | 0 |
| Ch1 No.Dgraded m | 0 |
| CB Operations | 4 |
| Total IA Broken | 5.812MA |
| Total IB Broken | 42.81kA |
| Total IC Broken | 42.01kA |
| CB Operate Time | 185.0ms |

| | |
|---|---|
| Opto I/P Status | 00000000 |
| Relay O/P Status | 0000000 |
| Test Port Status | 00000000 |
| LED Status | 00000000 |
| Ctrl I/P Status | 00000000000000000000000000000000 |

## Reverse

**Timer Results of 2014-09-10 11:22:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Pre-Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## Data extracted from P541 relay

| | |
|---|---|
| Stability Reverse NMK F675 | |
| IA Magnitude | 597.3 A |
| IA Phase Angle | 0 deg |
| IB Magnitude | 597.7 A |
| IB Phase Angle | −119.8 deg |
| IC Magnitude | 598.3 A |
| IC Phase Angle | 120.2 deg |
| IN Measured Mag | 0 A |
| IN Measured Ang | 0 deg |
| IN Derived Mag | 0 A |
| IN Derived Angle | 0 deg |
| I1 Magnitude | 597.8 A |
| I2 Magnitude | 0 A |
| I0 Magnitude | 0 A |
| IA RMS | 597.8 A |
| IB RMS | 597.8 A |
| IC RMS | 598.5 A |
| Frequency | 50.01 Hz |
| IA Fixed Demand | 0 A |
| IB Fixed Demand | 0 A |
| IC Fixed Demand | 0 A |
| IA Roll Demand | 0 A |
| IB Roll Demand | 0 A |
| IC Roll Demand | 0 A |
| IA Peak Demand | 598.5 A |
| IB Peak Demand | 599.0 A |
| IC Peak Demand | 599.0 A |
| IA local | 592.5 A |
| IA Angle local | 0 deg |
| IB local | 593.1 A |
| IB Angle local | −119.9 deg |
| IC local | 592.3 A |
| IC Angle local | 120.4 deg |
| IA remote 1 | 591.8 A |
| IA Ang remote 1 | 178.5 deg |
| IB remote 1 | 589.8 A |
| IB Ang remote 1 | 59.13 deg |
| IC remote 1 | 589.8 A |
| IC Ang remote 1 | −60.23 deg |
| IA Differential | 5.016 A |
| IB Differential | 3.472 A |
| IC Differential | 5.702 A |
| IA Bias | 591.0 A |
| IB Bias | 591.3 A |
| IC Bias | 591.2 A |
| Ch 1 Prop Delay | 4.737ms |
| Channel Status | 0000000001111 |
| Elapsed Time | 643.0 s |
| Ch1 No.Vald Mess | 128634 |
| Ch1 No.Err Mess | 0 |
| Ch1 No.Errored s | 0 |

| | |
|---|---|
| Ch1 No.Sev Err s | 0 |
| Ch1 No.Dgraded m | 0 |
| CB Operations | 4 |
| Total IA Broken | 5.812MA |
| Total IB Broken | 42.81kA |
| Total IC Broken | 42.01kA |
| CB Operate Time | 185.0ms |
| Opto I/P Status | 00000000 |
| Relay O/P Status | 0000000 |
| Test Port Status | 00000000 |
| LED Status | 00000000 |
| Ctrl I/P Status | 00000000000000000000000000000000 |

**TDM production circuit (NMK-end)**

Forward

**Timer Results of 2014-08-05 10:21:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Pre-Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

Reverse

**Timer Results of 2014-08-05 10:25:10**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Pre-Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

#### **8.2.2.2** 3 phase In-zone Fault

Full set of screenshots of results is shown in **Appendix C – Protection test results screenshots**. A snapshot and comparison of these results is provided in **Section 8.3**.

#### **8.2.2.3** Single phase thru Fault

Full set of screenshots of results is shown in **Appendix C – Protection test results screenshots**. A snapshot and comparison of these results is provided in **Section 8.3**.

#### **8.2.2.4** Single phase In-zone Fault

Full set of screenshots of results is shown in **Appendix C – Protection test results screenshots**. A snapshot and comparison of these results is provided in **Section 8.3**.

#### **8.2.2.5** Bias Restraint (In-zone & Out-of-zone)

Full set of screenshots of results is shown in **Appendix C – Protection test results screenshots**. A snapshot and comparison of these results is provided in **Section 8.3**.

## 8.3 System results analysis and comparison

### 8.3.1 Latency and jitter comparison

**Table 8.4** below shows the latency and jitter testing results. With an optimal jitter buffer and payload size configured at the Cpipe service, the IP/MPLS protection circuit latency slightly outperforms the current TDM network running PDH architecture. The total jitter introduced by both systems could be considered similar using the results that the testing provided. It should also be noted that adding routers into the circuit path adds around 50 µs per router.

| | IP/MPLS network | TDM network |
|---|---|---|
| Round-trip Latency | 4.365 ms | 4.876 ms |
| Jitter | +/- 72 µs | +/- 75 µs |

**Table 8.4 – Latency and Jitter Test Results**

### 8.3.2 Operation comparison

The three (3) tables below show the protection testing results formatted in a way for ease of comparison across the systems. **Table 8.4** shows correct and consistent operation for all test cases we no false operations.

| Site Circuit | Forward | Reverse | A phase | B phase | C phase |
|---|---|---|---|---|---|
| AGE test | No Op | No Op | No Op | No Op | No Op |
| AGE prod | No Op | No Op | No Op | No Op | No Op |
| NMK test | No Op | No Op | No Op | No Op | No Op |
| NMK prod | No Op | No Op | No Op | No Op | No Op |

**Table 8.5 – Stability and Thru Faults Test Results**

**Table 8.5** outlines all tested operation times for both circuits at both ends of the protection scheme. It clearly shows the IP/MPLS test circuit operating faster than the TDM network results. While these operation times are only slight in their advantage over the current TDM

network, the consistency in which the IP/MPLS network delivers these results is the most important to take from this table.

| Site Circuit | 3 phase in-zone | A phase in-zone | B phase in-zone | C phase in-zone |
|---|---|---|---|---|
| AGE test | 23.4ms | 25.1ms | 22.3ms | 23.7ms |
| AGE prod | 29.2ms | 27.1ms | 24.8ms | 26.3ms |
| ***Difference*** | ***-5.8ms*** | ***-2.0ms*** | ***-2.5ms*** | ***-2.6ms*** |
| NMK test | 25.1ms | 26.3ms | 22.3ms | 24.4ms |
| NMK prod | 27.9ms | 30.4ms | 28.0ms | 30.4ms |
| ***Difference*** | ***-2.8ms*** | ***-4.1ms*** | ***-5.7ms*** | ***-6.0ms*** |

**Table 8.6 – In-zone Fault Test Results**

**Table 8.6** provides the results for the bias restraint tests. It can be seen that the operation times are again consistent across both systems for the in-zone fault tests. All out-of-zone faults where recognised correctly and no operation occurred.

| Site Circuit | Test 1 In-zone | Test 1 Out-zone | Test 2 In-zone | Test 2 Out-zone | Test 3 In-zone | Test 3 Out-zone |
|---|---|---|---|---|---|---|
| AGE test | 45.1ms | No Op | 47.5ms | No Op | 38.7ms | No Op |
| AGE prod | 50.1ms | No Op | 46.2ms | No Op | 38.0ms | No Op |
| ***Diff*** | ***-5.0ms*** | **N/A** | ***1.3ms*** | **N/A** | ***0.7ms*** | **N/A** |
| NMK test | 45.9ms | No Op | 47.4ms | No Op | 39.0ms | No Op |
| NMK prod | 45.8ms | No Op | 48.5ms | No Op | 34.9ms | No Op |
| ***Diff*** | ***0.1ms*** | **N/A** | ***-1.1ms*** | **N/A** | ***4.1ms*** | **N/A** |

**Table 8.7 – Bias Restraint Test Results**

Chapter 9

# Conclusions and Further Work

## 9.1 Conclusions

A number of direct major and minor conclusions can be made from this project. To ensure compatibility with existing systems latency characteristics of the system are of critical importance. The two (2) most important conclusions that have been made, relate to the jitter and QoS findings. The primary minor conclusion that the project makes is related to the resiliency of the designed circuit. Adding weight and credibility to these conclusions is the research and testing performed by Blair et al. (2014). These findings tightly parallel the findings and conclusions that this research project has made, primarily in regards, the latency and jitter characteristics of a C37.94 MPLS-run circuit.

The testing proved the latency of the circuit closely matched the latency of existing TDM circuits running over PDH architecture. The latency of the circuit can be adjusted with the use of the jitter buffer settings in the Cpipe service. Latency variation is minimal and thus C37.94 protection Cpipe service is considered very stable. Latency does not change a noticeable amount when adjusting either the jitter buffer or payload size, staying consistently around +/- 72 µs. This meets the Requirements Analysis sub-section **4.4.1 – Major system capabilities**. Furthermore, adding routers into the path increases the circuit latency by around 50 µs per router.

Correctly configured QoS markings were essential to reliability and stability of the circuit. With QoS markings correctly set at the MDA, port, interface and SAP the circuit remained stable under all test scenarios. This testing showed complete isolation between the low priority an high priority teleprotection traffic. Under high levels of network congestion and without QoS configured, the circuit became unstable and would eventually fail. Analyse showed that while the protection circuit data was not being dropped by the router, the latency and PDV was great enough to not meet the P541 communications link requirements, and thus the link failed. Furthermore, testing proved that incorrectly configuring QoS markings in any number of ways had major negative effects on the performance on the circuit. Thus, it is concluded that without the correct implementation and configuration of QoS within the entire IP/MPLS network, the migration of existing C37.94 teleprotection circuits would not be possible.

Traffic engineering and resiliency cases proved that failover to alternative paths were possible in sub-30ms speeds and did not cause any incorrect tripping functions. The failover was stable and failing back to the primary path was also successful. While an automatic failover system was not part of the Requirement Analysis it is seen as an added benefit that the MPLS circuit brings. If this system was to be implemented on a live HV feeder, it is recommended that the tested MPLS resiliency features would be left shutdown initially. It was also proven that the resiliency features worked correctly when failing various redundant cards in the ALU 7705 SAR-8. This testing also proved there was no traffic lost and no unexpected relay behaviour.

The project concludes that using IP/MPLS technology to migrate protection relays that do not support native IP communications is a possible intermediate step for power utilities looking to migrate teleprotection services onto their next generation telecommunications network. While the proven results are positive, there is still considerable further work to be completed before a large scale rollout should be undertaken.

Overall, this project has concluded that an IP/MPLS network could be used to run a C37.94 teleprotection signalling circuits using the Areva P541 Current Differential Relay.

## 9.2 Further Work

Limitations in available test equipment made detailed analysis at high resolution speeds (µs) on the single-way delay and PDV of the circuit not possible. For further understanding of the latency characteristics of the IP/MPLS network, this analysis needs to be completed. While the teleprotection service packet structure was researched, decoding these packets during testing to confirm their contents would also be highly beneficial.

The relays were configured using their internal time stamping for synchronisation. The P541 relay can also be synchronised to a GPS clock. Using such a GPS time synchronisation system could further minimise PDV in the circuit and thus, this is considered important further work.

This project focused solely on a single relay and a single vendor for network equipment. To this end, it is recommended that a variety of protection devices using a variety of communications standards, including G.703 and SEL MB should be tested. A variety of network equipment, over a range of vendors, should also be tested in the future.

The project was only focused on a single feeder-ended type of current differential protection scheme. It should be noted that there are many different types including;

- multiple Feeder-ended;
- single transformer-ended; and,
- dual transformer-ended.

Testing of all of these types of schemes should also be completed to provide the ability for analysis and comparison of them.

Chapter 10

# References


Gers, J & Holmes, E. J 2011, *Protection of Electircity Distribution networks*, 3rd Edition, Institution of Engineering and Technology, 2011.

Alstom 2011, 'Network Protection & Automation Guide', Alstom Grid.

Kerven, D 2011, *Planning Guidelines for Distribution Network Protection*, Energex, Brisbane.

Ebrecht, W 2013, Young Power Equipment, 'Teleprotection Schemes and Equipment', Scottsdale.

IEEE 2013, *IEEE Guide for Power System Protective Relay Applications Over Digital Communications Channels*, New York.

IEEE 2013, *IEEE Standard C37.94 - Standard for N time 64 kilobit per second optical fiber interfaces between teleprotection and multiplexer equipment*, New York.

Made-IT 2011, ‘RS232 - V.24/V.28 - IS2110 - X20 bis (for Async) - X.21 bis (for Sync),’ Made-IT; Connectivity Knowlege Platform, viewed 13 May 2014, <http://ckp.made-it.com/rs232.html>.

Schweitzer, E. O., Whitehead, D, Fodero, K & Robertson, P 2012, *Merging SONET and Ethernet Communications for Power System Applications*, Schweitzer Engineering Laboratories, Washington.

Sollecito, L 2009, ‘Protection and Control Journal’, *Smart Grid: The Road Ahead*, no. 8, pp. 15-20.

Mackiewicz, R.E 2006, “Overview of IEC 61850 and Benefits,” IEEE, New York.

Kastenny, B, Whatley, J, Urden, E, Burger, J, Finney, D & Adamiak, M, ‘IEC 61850 - A Practical Application Primer for Protection Engineers’, *IEEE*, New York.

CISCO 2013, ‘Multiprotocol Label Switcing for the Utility Wide Area Network’, *CISCO*, San Jose, California.

Hunt, L 2011, ‘Drivers for Packet-Based Utility Communications Networks – Teleprotection’, *in The International Conference on Advanced Power System Automation and Protection*, pp. 2453 - 57.

RAD Communications 2012, ‘Carrier-Grade Ethernet for Power Utilities’, RAD Data Communications Limited, Tel Aviv.

Dean, T 2003, *Guide to Telecommunications Technology*, Thomson, Massachusetts.

Hundley, K 2009, *Alcatel-Lucent Scalable IP Networks Self-Study Guide: Preparing for the Network Routing Specialist I (NRS 1) Certification Exam (4A0-100)*, Wiley Publishing, Indianapolis.

Halsall, F 2002, *Data Communications, Computer Networks and Open Systems 3rd ed.*, Addison-Wesley, New York.

Chappell, L & Tittel, E 2005, *Guide to TCP/IP 2nd ed.*, Thomson, Massachusetts.

Lammle, T, Hales, K & Porter, D 2008, *CCNP Advanced Cisco Router Configuration*, Sybex, San Francisco.

Warnock, G & Nathoo, A 2011, *Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide: Preparing for the NRS II Cerification Exams*, Wiley Publishing, Indianapolis.

Hudson, K, Caudle, K & Cannon, K 2003, *CCNA Guide to Cisco Networking 2nd ed.*, Thomson, Massachusetts.

Alcatel-Lucent University 2012, '*Quality of Service – Course Notes'*.

Alcatel-Lucent University 2013, *'MPLS – Course Notes'*.

Alcatel-Lucent University 2012, '*Services Architecture – Course Notes'*.

Alcatel-Lucent 2013, '*7705 Service Aggregation Router OS – Release 6.0.R4: Services Guide*', Wiley Publishing, Indianapolis.

CIGRE 2012, 'Line and System Protection Using Digital Circuit and Packet Communications', CIGRE, Paris.

Alcatel-Lucent 2012, 'Deploying IP/MPLS Communications Networks for Smart Grids', Alcatel Lucent, Canada.

CIGRE 2012, 'Communication Architecture for IP-Based Substation Applications', CIGRE, Paris.

Van Wyk, C 2011, 'Teleprotection Services over an Alcatel-Lucent IP/MPLS infrastructure', Canada.

Levrau, L 2011, ‘Teleprotection Over an IP/MPLS Network - Technical Validation’, Alcatel Lucent.

AEMC 2014, ‘National Electricity Rules Version 65’, Sydney.

IEC 1993, ‘IEC 60834-2: Performance and testing of teleprotection equipment of power systems – Part 2: Analogue comparison systems’, IEC.

Avara Technologies 2010, ‘*C37.94 Optical Data Interface Unit – Product brochure’*, Victoria.

MiCOM 2005, P54x Current Differential Relay – Technical Manual, Wiltshire, UK.

Doble 2012, F6150sv Technical Specification, Massachusetts.

Doble 2011, Protection Suite v2.2 – Protection testing software, Massachusetts.

JDSU 2012, HST3000c Handheld Services Tester – Platform Overview, Massachusetts.

Sunrise Telecom 2007, IEEE C37.94 Module SSMTT-45 – Data Sheet, San Jose.

ITU-T 2002, ‘G.821 – Error performance of an international digital connection operating at a bit rate below the primary rate and forming part of an Integrated Services Digital Network’, Geneva.

Blair, S, Coffele, F, Booth, C, De Valck, B, Verhulst, D 2014, ‘Demonstration and analysis of IP/MPLS communications for delivering power system protection solutions using IEEE C37.94, IEC 61850 Sampled Values, and IEC 61850 GOOSE protocols’, *at CIGRE Session 45*, Paris.

# Appendix A - Project Specification

University of Southern Queensland

## FACULTY OF HEALTH, ENGINEERING AND SCIENCES

## ENG 4111/4112 Research Project
## PROJECT SPECIFICATION

FOR: **Nigel Anthony John McDOWELL**

TOPIC: Teleprotection signalling over an IP/MPLS network

SUPERVISORS: Dr. Alexander Kist

PROJECT AIM: The project aims to investigate core aspects of an IP/MPLS network as a communications technology to be used in teleprotection signalling.

**PROGRAMME: Issue A, 4 March 2014**

1. Research information on current protection signalling schemes, their interface to current communications equipment and on IP/MPLS as a mature industry telecommunication technology.

2. Complete a basic requirements analysis to establish the deliverable for this project.

3. Undertake a comprehensive literature review covering all aspects of this project including IP/MPLS networking in High Voltage substations and other similar environments.

4. Design the system at a conceptual level.

5. Evaluate the design and appropriate electrical and telecommunications test equipment required for the testing of an IP/MPLS protection signalling scheme.

6. Build a testbed to test IP/MPLS teleprotection signalling as a service. This includes complete router and switch configurations.

7. Fully configure, test and evaluate a C37.94 protection signalling scheme.

As time permits:

8. Fully configure, test and evaluate a serial SEL MB protection signalling scheme.

9. Fully configure, test and evaluate a G.703 protection signalling scheme.

AGREED:_____ (student) _____ (Supervisor)

__/__ /__ __/__ /__ (date)

# Appendix B – Router configuration dump

```
# TiMOS-B-6.0.R4 both/hops ALCATEL-LUCENT SAR 7705
# Copyright (c) 2000-2013 Alcatel-Lucent.
# All rights reserved. All use subject to applicable license agreements.
# Built on Thu Sep 5 12:10:24 EDT 2013 by csabuild in /rel6.0/b1/R4/panos/main

# Generated WED JUN 25 22:35:33 2014 UTC

exit all
configure
#--------------------------------------------------
echo "System Configuration"
#--------------------------------------------------
    system
        name "apollo-mg00"
        location "apollo-mg00"
        snmp
            engineID "172016006008172016006008"
            packet-size 9216
        exit
        login-control
            pre-login-message "|-------------------------------------------------
------------------|\n| WARNING: This system and any other ENERGEX system (regardless
of|\n| how access is obtained, including through any mobile device)      |\n| must only be
accessed and used by authorised users for           |\n| legitimate corporate business purposes.
|\n| Your access and use of any ENERGEX system may be monitored.       |\n| By accessing any
ENERGEX system, you consent to this monitoring,|\n| and agree to comply with all ENERGEX
policies      relating      to      access|\n|      and      use      of      the      system.
|\n| Unauthorised access and use of the system may result in legal    |\n| proceedings against
you.                                          |\n|---------------------------------
---------------------------------|\n"
        exit
        time
            ntp
                no authentication-check
                authentication-key 3 key "HpeBI8pW.N/8criS.QMD1." hash2 type message-digest
                authentication-key 4 key "HfSMacH2BPCHzh0lBSzyd." hash2 type message-digest
                authentication-key 7 key "Ime0DEKdIPsZI/b5oMt00E" hash2 type message-digest
                authentication-key 8 key "k/wcgVadQXxB47cJgtda4k" hash2 type message-digest
                server 10.3.2.16 key 3
                server 10.3.2.22 key 7
                server 10.3.34.16 key 4
                server 10.3.34.22 key 8
                no shutdown
            exit
            sntp
                shutdown
            exit
            zone AEST
        exit
        thresholds
            rmon
            exit
            cflash-cap-alarm cf3-A: rising-threshold 5468750 falling-threshold 3906250 interval
900
            cflash-cap-alarm cf3-B: rising-threshold 5468750 falling-threshold 3906250
interval 900
        exit
    exit
#--------------------------------------------------
echo "System Security Configuration"
#--------------------------------------------------
    system
        security
            ftp-server
            password
                no health-check
            exit
```

```
            user "admin"
                password ".wwBSCf55BeJQsICA8BrJ." hash2
                access console ftp
                console
                    member "administrative"
                exit
            exit
            user "lab-snmpv3-7705"
                password "Yq.zcGZ/I8dSFLRITwCw0tWggemK.kpo" hash2
                access snmp
                snmp
                    authentication hash md5 899ece445f7bde1f73a26c7bbf34b76b privacy des
899ece445f7bde1f73a26c7bbf34b76b
                    group "nmsPriv"
                exit
            exit
            snmp
                access group "nmsPriv" security-model usm security-level privacy read "iso"
write "iso" notify "iso"
            exit
            ssh
                preserve-key
            exit
        exit
    exit
#--------------------------------------------------
echo "Log Configuration"
#--------------------------------------------------
    log
        event-control "vrtr" 2034 generate
        syslog 1
            description "Syslog server VPK"
            address 10.3.2.18
            facility local5
            log-prefix "anubismg00"
        exit
        syslog 2
            description "Syslog server WFS"
            address 10.3.34.18
            facility local5
            log-prefix "anubismg00"
        exit
        snmp-trap-group 98
            description "5620sam"
            trap-target "172.16.16.2:162" address 172.16.16.2 snmpv3 notify-community "lab-
snmpv3-7705" security-level privacy
            trap-target "172.16.17.2:162" address 172.16.17.2 snmpv3 notify-community "lab-
snmpv3-7705" security-level privacy
        exit
        log-id 91
            description "Log syslog VPK"
            time-format local
            from main security change
            to syslog 1
        exit
        log-id 92
            description "Log syslog WFS"
            time-format local
            from main security change
            to syslog 2
        exit
        log-id 98
            from main security
            to snmp 1024
        exit
    exit
#--------------------------------------------------
echo "System Security Cpm Hw Filters Configuration"
#--------------------------------------------------
    system
```

```
        security
        exit
    exit
#--------------------------------------------------
echo "QoS Policy Configuration"
#--------------------------------------------------
    qos
        network-queue "4001" create
            queue 1 create
                high-prio-only 10
            exit
            queue 7 create
                rate 10 cir 10
                high-prio-only 10
            exit
            queue 8 create
                rate 10 cir 10
                high-prio-only 10
            exit
            queue 9 multipoint create
                high-prio-only 10
            exit
            fc h1 create
                multicast-queue 9
                queue 7
            exit
            fc nc create
                multicast-queue 9
                queue 8
            exit
        exit
        fabric-profile 3 aggregate-mode create
            description "7705 SAR-8 Fabric QoS"
            aggregate-rate 1000000 unshaped-sap-cir 0
        exit
    exit
#--------------------------------------------------
echo "QoS Policy Configuration"
#--------------------------------------------------
    qos
        sap-ingress 4000 create
            queue 1 create
            exit
            queue 7 create
                rate 256 cir 256
                mbs 8
                cbs 2
                high-prio-only 10
            exit
            fc "h1" create
                queue 7
            exit
            default-fc "h1"
            default-priority high
        exit
        mc-mlppp
        exit
        network 4002 create
            ingress
                dscp nc2 fc nc profile in
                lsp-exp 6 fc h1 profile in
            exit
            egress
                fc nc
                    dscp-in-profile nc1
                exit
            exit
        exit
    exit
#--------------------------------------------------
```

```
echo "Card Configuration"
#--------------------------------------------------
    card 1
        card-type iom-sar
        mda 1
            mda-type a8-1gb-v2-sfp
            network
                ingress
                    fabric-policy 3
                    queue-policy "4001"
                exit
            exit
            access
                ingress
                    fabric-policy 3
                exit
            exit
        exit
        mda 2
            mda-type a8-1gb-v2-sfp
            network
                ingress
                    fabric-policy 3
                exit
            exit
            access
                ingress
                    fabric-policy 3
                exit
            exit
        exit
        mda 3
            mda-type a8-vt
            network
                ingress
                    fabric-policy 3
                exit
            exit
            access
                ingress
                    fabric-policy 3
                exit
            exit
        exit
        mda 5
            mda-type a12-sdi
        exit
        mda 6
            mda-type a16-chds1v2
        exit
    exit
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
    port 1/1/1
        description "to osiris-mg00"
        ethernet
            mode network
            network
                queue-policy "4001"
            exit
            autonegotiate limited
            ssm
                no shutdown
            exit
        exit
        no shutdown
    exit
    port 1/1/2
        shutdown
```

```
        ethernet
        exit
    exit
    port 1/1/3
        ethernet
        exit
        no shutdown
    exit
    port 1/1/4
        shutdown
        ethernet
        exit
    exit
    port 1/1/5
        shutdown
        ethernet
        exit
    exit
    port 1/1/6
        shutdown
        ethernet
        exit
    exit
    port 1/1/7
        shutdown
        ethernet
        exit
    exit
    port 1/1/8
        description "to apollo-mc00"
        ethernet
            encap-type dot1q
            autonegotiate limited
        exit
        no shutdown
    exit
    port 1/2/1
        description "to apollo-mb00"
        ethernet
            mode network
            autonegotiate limited
            ssm
                no shutdown
            exit
        exit
        no shutdown
    exit
    port 1/2/2
        description "to seth-mg00"
        ethernet
            mode network
            autonegotiate limited
        exit
        no shutdown
    exit
    port 1/2/3
        shutdown
        ethernet
        exit
    exit
    port 1/2/4
        shutdown
        ethernet
        exit
    exit
    port 1/2/5
        shutdown
        ethernet
        exit
    exit
```

```
port 1/2/6
     shutdown
     ethernet
     exit
exit
port 1/2/7
     shutdown
     ethernet
     exit
exit
port 1/2/8
     description "to apollo-mc01"
     ethernet
          encap-type dot1q
          autonegotiate limited
     exit
     no shutdown
exit
port 1/3/1
     tdm
          tpif
               channel-group 1
                    encap-type cem
                    no shutdown
               exit
               no shutdown
          exit
     exit
     no shutdown
exit
port 1/3/2
     shutdown
     tdm
     exit
exit
port 1/3/3
     shutdown
     tdm
     exit
exit
port 1/3/4
     shutdown
     tdm
     exit
exit
port 1/3/5
     shutdown
     voice
     exit
exit
port 1/3/6
     shutdown
     voice
     exit
exit
port 1/3/7
     shutdown
     voice
     exit
exit
port 1/3/8
     shutdown
     voice
     exit
exit
port 1/5/1
     shutdown
     serial
     exit
exit
```

```
port 1/5/2
     shutdown
     serial
     exit
exit
port 1/5/3
     shutdown
     serial
     exit
exit
port 1/5/4
     shutdown
     serial
     exit
exit
port 1/5/5
     shutdown
     serial
     exit
exit
port 1/5/6
     shutdown
     serial
     exit
exit
port 1/5/7
     shutdown
     serial
     exit
exit
port 1/5/8
     shutdown
     serial
     exit
exit
port 1/5/9
     shutdown
     serial
     exit
exit
port 1/5/10
     shutdown
     serial
     exit
exit
port 1/5/11
     shutdown
     serial
     exit
exit
port 1/5/12
     shutdown
     serial
     exit
exit
port 1/6/1
     shutdown
     tdm
     exit
exit
port 1/6/2
     shutdown
     tdm
     exit
exit
port 1/6/3
     shutdown
     tdm
     exit
exit
```

```
    port 1/6/4
        shutdown
        tdm
        exit
    exit
    port 1/6/5
        shutdown
        tdm
        exit
    exit
    port 1/6/6
        shutdown
        tdm
        exit
    exit
    port 1/6/7
        shutdown
        tdm
        exit
    exit
    port 1/6/8
        shutdown
        tdm
        exit
    exit
    port 1/6/9
        shutdown
        tdm
        exit
    exit
    port 1/6/10
        shutdown
        tdm
        exit
    exit
    port 1/6/11
        shutdown
        tdm
        exit
    exit
    port 1/6/12
        shutdown
        tdm
        exit
    exit
    port 1/6/13
        shutdown
        tdm
        exit
    exit
    port 1/6/14
        shutdown
        tdm
        exit
    exit
    port 1/6/15
        shutdown
        tdm
        exit
    exit
    port 1/6/16
        shutdown
        tdm
        exit
    exit
#-------------------------------------------------
echo "External Alarm Configuration"
#-------------------------------------------------
    external-alarms
    exit
```

```
#----------------------------------------------------
echo "Management Router Configuration"
#----------------------------------------------------
    router management
    exit

#----------------------------------------------------
echo "Router (Network Side) Configuration"
#----------------------------------------------------
    router
        interface "apollo-mg00-ieg1-1-1"
            address 172.16.0.25/31
            description "to osiris-mg00"
            port 1/1/1
            bfd 100 receive 100 multiplier 3
        exit
        interface "apollo-mg00-ieg1-2-1"
            address 172.16.0.21/31
            description "to apollo-mb00"
            port 1/2/1
            bfd 100 receive 100 multiplier 3
        exit
        interface "apollo-mg00-ieg1-2-2"
            address 172.16.0.26/31
            description "to seth-mg00"
            port 1/2/2
            bfd 100 receive 100 multiplier 3
        exit
        interface "system"
            address 172.16.6.8/32
        exit
        autonomous-system 65400
#----------------------------------------------------
echo "OSPFv2 Configuration"
#----------------------------------------------------
        ospf
            traffic-engineering
            area 0.0.0.0
                interface "system"
                exit
                interface "apollo-mg00-ieg1-1-1"
                    interface-type point-to-point
                    hello-interval 4
                    dead-interval 17
                    bfd-enable
                exit
                interface "apollo-mg00-ieg1-2-1"
                    interface-type point-to-point
                    hello-interval 4
                    dead-interval 17
                    bfd-enable
                exit
            exit
        exit
#----------------------------------------------------
echo "MPLS Configuration"
#----------------------------------------------------
        mpls
            interface "system"
            exit
            interface "apollo-mg00-ieg1-1-1"
            exit
            interface "apollo-mg00-ieg1-2-1"
            exit
            interface "apollo-mg00-ieg1-2-2"
            exit
        exit
#----------------------------------------------------
echo "RSVP Configuration"
#----------------------------------------------------
```

```
        rsvp
            interface "system"
            exit
            interface "apollo-mg00-ieg1-1-1"
            exit
            interface "apollo-mg00-ieg1-2-1"
            exit
            interface "apollo-mg00-ieg1-2-2"
            exit
            no shutdown
        exit
#--------------------------------------------------
echo "MPLS LSP Configuration"
#--------------------------------------------------
        mpls
            path "to-osiris-mg00-1"
                hop 1 172.16.6.6 strict
                no shutdown
            exit
            path "to-osiris-mg00-2"
                hop 1 172.16.6.3 strict
                hop 2 172.16.6.2 strict
                hop 3 172.16.6.6 strict
                no shutdown
            exit
            lsp "to-osiris-mg00-lsp"
                to 172.16.6.6
                cspf
                fast-reroute facility
                    no node-protect
                exit
                primary "to-osiris-mg00-1"
                exit
                secondary "to-osiris-mg00-2"
                    standby
                exit
                no shutdown
            exit
            lsp "to-osiris-mg00-traffic-lsp"
                to 172.16.6.6
                primary "to-osiris-mg00-1"
                exit
                no shutdown
            exit
            no shutdown
        exit
#--------------------------------------------------
echo "LDP Configuration"
#--------------------------------------------------
        ldp
            peer-parameters
                peer 172.16.6.6
                exit
            exit
            interface-parameters
                interface "apollo-mg00-ieg1-1-1"
                exit
                interface "apollo-mg00-ieg1-2-1"
                exit
            exit
            targeted-session
                peer 172.16.6.3
                exit
                peer 172.16.6.6
                exit
            exit
        exit
    exit

#--------------------------------------------------
```

```
echo "Service Configuration"
#------------------------------------------------------
    service
        customer 1 create
            description "Default customer"
        exit
        customer 10 create
            description "Control plane and management services"
        exit
        customer 20 create
            description "Corporate services"
        exit
        customer 30 create
            description "Control zone traffic services"
        exit
        customer 40 create
            description "Measurement zone traffic services"
        exit
        customer 50 create
            description "Distribution zone traffic services"
        exit
        customer 60 create
            description "Site security services"
        exit
        customer 70 create
            description "PDH transport services"
        exit
        customer 80 create
            description "Teleprotection services"
        exit
        customer 90 create
            description "Powerlink"
        exit
        sdp 5 create
            far-end 172.16.6.6
            lsp "to-osiris-mg00-lsp"
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        sdp 15 create
            far-end 172.16.6.6
            lsp "to-osiris-mg00-traffic-lsp"
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        vprn 3 customer 10 create
            route-distinguisher 65400:10000001
            auto-bind ldp
            vrf-target target:65400:10000001
            interface "apollo-mg00-ieg1-1-8-v2010" create
                address 172.16.2.13/30
                sap 1/1/8:2010 create
                    collect-stats
                exit
            exit
            interface "apollo-mg00-ieg1-2-8-v2011" create
                address 172.16.3.13/30
                sap 1/2/8:2011 create
                exit
            exit
            no shutdown
        exit
        cpipe 20 customer 10 vc-type cesopsn create
            sap 1/3/1.1 create
                cem
                    packet jitter-buffer 2 payload-size 2
```

```
                    exit
                    ingress
                        qos 4000
                    exit
                exit
                spoke-sdp 5:20 create
                exit
                no shutdown
            exit
            epipe 30 customer 10 create
                sap 1/1/3 create
                exit
                spoke-sdp 5:30 create
                exit
                no shutdown
            exit
        exit
#--------------------------------------------------
echo "Router (Service Side) Configuration"
#--------------------------------------------------
        router
#--------------------------------------------------
echo "OSPFv2 Configuration"
#--------------------------------------------------
            ospf
            exit
        exit
#--------------------------------------------------
echo "System Sync-If-Timing Configuration"
#--------------------------------------------------
        system
            sync-if-timing
                begin
                ref-order ref1 ref2 external
                ref1
                    source-port 1/1/1
                    no shutdown
                exit
                ref2
                    source-port 1/2/1
                    no shutdown
                exit
                external
                    input-interface
                        shutdown
                    exit
                exit
                revert
                commit
            exit
        exit
#--------------------------------------------------
echo "System Time Configuration"
#--------------------------------------------------
        system
            time
                ntp
                exit
            exit
        exit
#--------------------------------------------------
echo "OAM Tests Configuration"
#--------------------------------------------------
        test-oam
            twamp
                server
                    shutdown
                exit
            exit
        exit
```

# Appendix C – Protection test result screenshots

3 phase In-zone Fault

## IP/MPLS test circuit (AGE-end)

**Timer Results of 2014-09-10 11:31:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 23.4 ms | -53.20 % | ✓ |

## TDM production circuit (AGE-end)

**Timer Results of 2014-08-05 10:29:10**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 29.2 ms | -41.60 % | ✓ |

## IP/MPLS test circuit (NMK-end)

**Timer Results of 2014-09-10 11:31:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 25.1 ms | -49.80 % | ✓ |

## TDM production circuit (NMK-end)

**Timer Results of 2014-08-05 10:29:10**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 27.9 ms | -44.20 % | ✓ |

Single phase thru Fault

## IP/MPLS test circuit (AGE-end)

A phase

**Timer Results of 2014-09-10 11:32:30**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

B phase

**Timer Results of 2014-09-10 11:35:30**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

C phase

**Timer Results of 2014-09-10 11:38:30**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## TDM production circuit (AGE-end)

A phase

**Timer Results of 2014-08-05 10:30:50**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

B phase

**Timer Results of 2014-08-05 10:33:40**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

C phase

**Timer Results of 2014-08-05 10:36:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## IP/MPLS test circuit (NMK-end)

A phase

**Timer Results of 2014-09-10 11:32:30**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

B phase

**Timer Results of 2014-09-10 11:35:30**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

C phase

**Timer Results of 2014-09-10 11:38:30**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## TDM production circuit (NMK-end)

A phase

**Timer Results of 2014-08-05 10:30:50**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

B phase

**Timer Results of 2014-08-05 10:33:40**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

C phase

**Timer Results of 2014-08-05 10:36:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

Single phase In-zone Fault

## IP/MPLS test circuit (AGE-end)

A phase

**Timer Results of 2014-09-10 11:34:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 25.1 ms | -49.80 % | ✓ |

B phase

**Timer Results of 2014-09-10 11:37:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 22.3 ms | -55.40 % | ✓ |

C phase

**Timer Results of 2014-09-10 11:40:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 23.7 ms | -52.60 % | ✓ |

## TDM production circuit (AGE-end)

A phase

**Timer Results of 2014-08-05 10:32:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 27.1 ms | -45.80 % | ✓ |

B phase

**Timer Results of 2014-08-05 10:34:50**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 24.8 ms | -50.40 % |

C phase

**Timer Results of 2014-08-05 10:37:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 26.3 ms | -47.40 % |

## IP/MPLS test circuit (NMK-end)

A phase

**Timer Results of 2014-09-10 11:34:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 26.3 ms | -47.40 % |

B phase

**Timer Results of 2014-09-10 11:37:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 22.3 ms | -55.40 % |

C phase

**Timer Results of 2014-09-10 11:40:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 24.4 ms | -51.20 % |

## TDM production circuit (NMK-end)

A phase

**Timer Results of 2014-08-05 10:32:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 30.4 ms | -39.20 % |

B phase

**Timer Results of 2014-08-05 10:34:50**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 28.0 ms | -44.00 % |

C phase

**Timer Results of 2014-08-05 10:37:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Value | 50.0 ms | 99.00 % | 0.00 % | Percent | Error | Op | 30.4 ms | -39.20 % |

Bias Restraint (In-zone & Out-of-zone)

Bias Restraint 1 In-zone

**IP/MPLS test circuit (AGE-end)**

**Timer Results of 2014-09-10 11:43:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 45.1 ms | |

**TDM production circuit (AGE-end)**

**Timer Results of 2014-08-05 10:42:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 50.1 ms | |

**IP/MPLS test circuit (NMK-end)**

**Timer Results of 2014-09-10 11:43:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 45.9 ms | |

**TDM production circuit (NMK-end)**

**Timer Results of 2014-08-05 10:42:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 45.8 ms | |

Bias restraint 1 Out-of-zone

**IP/MPLS test circuit (AGE-end)**

**Timer Results of 2014-09-10 11:45:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

**TDM production circuit (AGE-end)**

**Timer Results of 2014-08-05 10:43:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## IP/MPLS test circuit (NMK-end)

**Timer Results of 2014-09-10 11:45:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## TDM production circuit (NMK-end)

**Timer Results of 2014-08-05 10:43:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

Bias restraint 2 In-zone

## IP/MPLS test circuit (AGE-end)

**Timer Results of 2014-09-10 11:46:30**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 47.5 ms | |

## TDM production circuit (AGE-end)

**Timer Results of 2014-08-05 10:44:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 46.2 ms | |

## IP/MPLS test circuit (NMK-end)

**Timer Results of 2014-09-10 11:46:30**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 47.4 ms | |

## TDM production circuit (NMK-end)

**Timer Results of 2014-08-05 10:44:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 48.5 ms | |

Bias restraint 2 Out-of-zone

## IP/MPLS test circuit (AGE-end)

**Timer Results of 2014-09-10 11:48:15**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## TDM production circuit (AGE-end)

**Timer Results of 2014-08-05 10:45:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## IP/MPLS test circuit (NMK-end)

**Timer Results of 2014-09-10 11:48:15**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

## TDM production circuit (NMK-end)

**Timer Results of 2014-08-05 10:45:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | |

Bias restraint 3 In-zone

## IP/MPLS test circuit (AGE-end)

**Timer Results of 2014-09-10 11:50:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 38.7 ms | |

## TDM production circuit (AGE-end)

**Timer Results of 2014-08-05 10:46:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 38.0 ms | |

## IP/MPLS test circuit (NMK-end)

**Timer Results of 2014-09-10 11:50:00**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 39.0 ms | |

## TDM production circuit (NMK-end)

**Timer Results of 2014-08-05 10:46:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error |
| 1 | VA | Fault | LN1 (VA) | Op | | | | | Error | Op | 34.9 ms | |

Bias restraint 3 Out-of-zone

## IP/MPLS test circuit (AGE-end)

**Timer Results of 2014-09-10 11:51:30**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

## TDM production circuit (AGE-end)

**Timer Results of 2014-08-05 10:47:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

## IP/MPLS test circuit (NMK-end)

**Timer Results of 2014-09-10 11:51:30**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |

## TDM production circuit (NMK-end)

**Timer Results of 2014-08-05 10:47:20**

| Timer | Label | Start State | Stop Event | Expected Result | | Tolerance | | | | Measured Result | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Op | Time | Minus | Plus | Type | Severity | Op | Time | Error | |
| 1 | VA | Fault | LN1 (VA) | No Op | | | | | Error | NoOp | | | ✓ |