AIR TRAFFIC AND NAVIGATION SERVICES SOC. LTD

REPUBLIC OF SOUTH AFRICA

REQUEST FOR PROPOSALS: ATNS/RFP01/06/2026/27/TIME_SYNC_Dis_2017_234

THE APPOINTMENT OF A SERVICE PROVIDER FOR THE SUPPLY, DELIVERY, INSTALLATION, COMMISSIONING, MAINTENANCE, AND SUPPORT OF GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS) NETWORK TIME PROTOCOL (NTP) TIME CLOCK SYNCHRONISATION SYSTEMS WITH A SYSTEM LIFECYCLE OF FIFTEEN (15)-YEARS.

VOLUME 2

TECHNICAL REQUIREMENTS

JUNE 2026

ABSTRACT

ATNS continually strives towards aligning its operations and services with the fast-evolving technological advances, developments and enhancements within the industry. The quality-of-service provision also hugely depends on the real-time accuracy and integrity of data and information used to provide the best and safest services to all clients. Maintaining accurate time across all ATM and CNS network systems is critical in the real-time aviation industry to ensure all related services are time synchronised for optimal safety and service delivery.

Prevention of collisions by example applying appropriate timed separations and issue timely clearances and instructions that create orderly flow of air traffic and air-traffic services, all are based on accurate date and time data in the strategic, pre-tactical and tactical planning and operational phases. Tactical interventions by the ATCs and direct communication with the flight crews usually during the entire flight, makes time synchronised data in real-time crucial in air-traffic control and all related and associated supporting systems and services to maintain accurate aircraft separations and schedules on a 24/7 basis. Time-synchronised CNS and ATM system networks will ensure accurate control of aircraft and the tracking of flight positions throughout the entire flight for each.

The document herein contains the technical specifications for the replacement of the current time synchronisation obsolete and aged equipment, or to establish a time synchronisation system at sites where such a system does not exist, for all ATM, CNS and local ATC systems at all airports where ATNS provides air traffic services for clients.

REVISION INDEX SHEET

Version	Revision	Date	Reason for Change	Pages Affected
0	1	13/07/2022	Initial Document	All
0	2	02/08/2022	Document Reviewed	All
0	3	17/08/2022	Document Reviewed	All
0	4	14/09/2022	Document Reviewed	All
0	5	18/04/2023	Document Reviewed	All
0	6	05/05/2026	Document Reviewed	All

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ACL	Access Control List
AES-128	Encrypting/decrypting message blocks with a 128-bit key length
AI	Artificial Intelligence
AMP	Advance Malware Protection
ANSP	Air Navigation Service Provider
API	Application Programming Interface
ARP	Address Routing Protocol
ATA	ATNS- Aviation Training Academy
ATC	Air Traffic Control / Air Traffic Controller
ATM	Air Traffic Management
ATNS	Air Traffic and Navigation Services
AVC	Application Visibility and Control
AVF	Active Virtual Forwarder
AVG	Active Virtual Gateway
AX	Application Experience
BCP	Best Current Practice
BFD	Bi-directional Forward Detection
BGP	Border Gateway Protocol
BPDUs	Bridge Protocol Data Units
BRP	Beacon Redundancy Protocol
CAR	Committed Access Rate
CLI	Command Line Interface
CNS	Communication, Navigation and Surveillance
COTS	Commercially-of-the-Shelf
CSF	Critical Success Factor
CVE	Common Vulnerabilities and Exposure
DAN	Dually Attached Node
DANB	Double Attached Node implementing BRP
DANP	Double Attached Node implementing PRP
DC	Direct Current
DDoS	Distribution Denial-of-Service
DDR4	Double Data Rate 4
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial-of-Service

DPI	Deep Packet Inspection
DSCP	Differentiated Service Code Point
EIGRP	Enhanced Interior Gateway Routing Protocol
FABL	Bloemfontein Airport (ICAO Designator)
FACT	Cape Town International Airport (ICAO Designator)
FAEL	East London Airport (ICAO Designator)
FAGC	Grand Central Airport (ICAO Designator)
FAGG	George Airport (ICAO Designator)
FAGM	Rand Airport (ICAO Designator)
FAKM	Kimberley Airport (ICAO Designator)
FAKN	Kruger Mpumalanga International Airport (ICAO Designator)
FALA	Lanseria International Airport (ICAO Designator)
FALE	King Shaka International Airport (ICAO Designator)
FAMM	Mahikeng Airport (ICAO Designator)
FAOR	OR Tambo International Airport (ICAO Designator)
FAPE	Port Elizabeth International Airport (ICAO Designator)
FAPM	Pietermaritzburg Airport (ICAO Designator)
FAPN	Pilanesberg International Airport (ICAO Designator)
FAPP	Polokwane International Airport (ICAO Designator)
FARB	Richards Bay Airport (ICAO Designator)
FAUP	Upington Airport (ICAO Designator)
FAUT	Mthatha Airport (ICAO Designator)
FAVG	Virginia Airport (ICAO Designator)
FAWB	Wonderboom National Airport (ICAO Designator)
FDDI	Fibre Distributed Data Interfaces
FHD	Full High Definition
FHRP	First Hop Redundancy Protocol
FNF	Flexible NetFlow
FOC	Fibre Optic Converter
FRU	Field-Replaceable Unit
FTP	File Transfer Protocol
GLBP	Gateway Load Balancing Protocol
GNSS	Global Navigation Satellite System
GPS	Global Positioning System (USA)
GUI	Graphical User Interface
HDD	Hard Disk Drive
HDMI	High-Definition Media Interface
HSR	High-availability Seamless Redundancy
HSRP	Hot Standby Redundancy Protocol

HTTP	Hyper-Text Transfer Protocol
HTTPS	Hyper-Text Transfer Protocol Secure
HW	Hardware
Hz	Hertz (cycle per second)
ICAO	International Civil Aviation Organisation
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System/Software
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISA	International Society of Automation
ISIS	Intermediate System to Intermediate System
ISP	Information Security and Privacy OR Internet Service Provider
ISR	Integrated Services Routers
IT	Information Technology
L2TP	Layer-2 Tunnelling Protocol
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
LTE	Long-Term Evolution
MAC	Media Access Control
MCS	Monitoring Control and Supervision
MD5	Message-Digest algorithm
MHz	Mega Hertz (1000x cycles per second)
MIB	Management Information Base
MITM	Man-In-The-Middle
ML	Machine Learning
MPLS	Multiprotocol Label Switching
MP-OLSR	Multiple Path Optimized Link State Routing
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failures
NAT	Network Address Translation
NDP	Network Data Platform

NGFW	Next Generation Firewall
NGIPS	Next Generation Intrusion Prevention System
NMAP	Network Management and Automation Platform
NMS	Network Management System
NSW	Network Switch
NTP	Network Time Protocol
NTPD	Network Time Protocol Daemon
NTS	Network Time Security
OEM	Original Equipment Manufacturer
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OT	Operational Technology
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunnelling Protocol
PRP	Parallel Redundancy Protocol
PSU	Power Supply Unit
PTP	Precision Time Protocol
QoS	Quality of Service
RAM	Random Access Memory
RedBox	Redundancy Box
REP	Resilient Ethernet Protocol
RFC	Request for Comments
RIP	Routing Information Protocol
RoHS	Restriction of Hazardous Substances
RPS	Redundant Power Supply
RPVST+	Rapid Per VLAN Spanning Tree Plus
RSPAN	Remote Switch Port Analysis
RSTP	Rapid Spanning Tree Protocol
SAN	Singly Attached Node
SAT	System/Site Acceptance Test
SATA	Serial Advanced Technology Attachment
SD-Access	Secured Device Access
SDR	System Design Review
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SPAN	Switch Port Analysis
SSD	Solid State Drive

SSH	Secure Shell
SSL	Secure Sockets Layer
SSS	System Support Suite (ATNS)
STP	Spanning Tree Protocol
SW	Software
TCP	Transmission Control Protocol
TMH	Time Management Handler
ToS	Type of Service
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
USM	Unified Security Management
UTC	Coordinated Universal Time
VIPA	Virtual IP Address
VLAN	Virtual Local Area Network
VPN	Virtual Private Networks
VRRP	Virtual Router Redundancy Protocol
VSAT	Very Small Aperture Terminal

DEFINITIONS

Definitions are only applicable within this document:

Table 1: Definitions Only Applicable Within This Document

Collective Word/s	Meaning
Clocks	Refers to a time clock that is reliant on an NTP reference time source either as a standalone, display, or wall type of clock.
Host Firewall	Refers to a Software Firewall package installed and activated on a computer node.
Local-Systems	Refers to other ATNS systems that shall synchronise to the Time Synchronisation Systems (the systems described within this document and for this Time Synchronisation Project) at each site.
Main-Sites	References any Regional Airport site that is directly associated with the Major-Sites regarding certain systems inter-dependencies for interconnection and data exchanges from/to the Major-Sites and where ATNS ANSP services are provided.
Major-Site	References any of the two Major Regional International Airport sites, FAOR and FACT, which are regarded as the master sites concerning other regional sites, which are directly inter-dependent on certain data and information provisions and exchanges from/to these two sites and where ATNS ANSP services are provided.
Master-Clock	References an NTP Time Server device.
Next-Gen	Refers to the next generation electronic and other technological advancements and software enhancements implemented/developed as the latest required/preferred and best practices worldwide. For the purpose of this document, it will reference next generation cybersecurity and networking hardware and software advancements and enhancements.
NTP-Client	Refers to a device or node that queries the reference time from one or more NTP-Servers.

Collective Word/s	Meaning
NTP-Peer	Refers to a device or node that compares its own time to that of other peers until all peers agree on the “real/true” time to synchronise to.
NTP-Server	Refers to a server that supplies the reference time source to NTP-Clients.
Obsolete	Refers to equipment already at End-of-Sale and/or End-of-Life at the time of contracting of the Time Synchronisation System as well as equipment that shall not reach End-of-Sale and/or End-of-Life within five years after contracting.
Optional	This word, or the adjective "MAY", mean that an item is truly optional. One bidder may choose to include the item because a particular marketplace requires it or because the bidder feels that it enhances the product while another bidder may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)
Remote-Sites	Refers to the Regional Airport sites that are directly associated with the Main-Sites regarding limited systems dependencies for interconnection and data exchanges from/to Main-Sites where ATNS ANSP services are provided.
Shall	This word, or the terms "REQUIRED" or "MUST", mean that the definition is an absolute requirement of the specification.
Shall not	This phrase, or the phrase "MUST NOT", mean that the definition is an absolute prohibition of the specification.
Should	This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
Should not	This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or

Collective Word/s	Meaning
	even useful, but the full implications should be understood, and the case carefully weighed before implementing any behaviour described with this label.
Sites	Refers collectively to all Major-Sites, Main-Sites and Remote-Sites listed in this document.
System-Components	System-Components refer to all system software and hardware elements and sub-set elements including applications, physical and logical, hardware and software resources, virtualised components and sub-components, devices and interfaces relevant to each of the systems and shall further include, but shall not be limited to; all physical and virtual hardware devices per computer; all physical interfaces of the relevant system; all physical internal and external interfaces per computer; all functional operational logical internal and external interfaces per computer; all main functional applications per computer; all OS functional components per computer; all logical; physical and functional virtualised devices; applications and interfaces per system and per computer; all services per system and per computer; all event logs; all databases; all physical and logical connections; all databases, storage and SSD storage spaces; user access, user actions and events, system events; all which can digitally be monitored, managed, supervised or controlled, all-inclusive where applicable. System-Components shall concern and apply to all Systems (of this project) and shall also include all virtualised systems and their associated relevant System-Components and sub-set components.

1 GENERAL INSTRUCTIONS TO BIDDERS

The Bidder shall submit all responses, diagrams, project management documentation and drawings according to the GENERAL INFORMATION AND INSTRUCTIONS TO BIDDERS document and in the English language.

To assist Bidders only, each paragraph or article has been appended throughout with the letters "(M)", "(D)", "(O)" or "(I)", to indicate whether the requirement is **M**andatory, **D**esirable, **O**ptional or for **I**nformation only.

ALL RESPONSES TO THE REQUIREMENTS IN THIS DOCUMENT SHALL BE PROVIDED AS FOLLOWS:

BIDDERS SHALL RESPOND IN FULL TO EACH ITEM IN THE FORMAT PROVIDED AND REFERENCES (CHAPTER, SECTION, PAGE NUMBER, PARAGRAPH NUMBER) TO DOCUMENTS AND RELEVANT INFORMATION SUPPORTING THE RESPONSES SHALL BE INDICATED IN THE SPACE PROVIDED. THIS INFORMATION WILL BE THE **ONLY RESPONSE USED FOR THE EVALUATION AND ASSESSMENT**.

Responses, provided in the space allowed, that are not clear or inadequate or the lack thereof shall be interpreted as **"Not Compliant"** even though the compliance column is declared as "Comply" and/or the Bidder's offer meets the requirement. Bidders shall ensure that each response correctly addresses the requirement stated. Responses not addressing the requirement of the specific paragraph shall be interpreted as **"Not Compliant"**.

Bidders shall declare compliance to each and every paragraph of this document in the column labelled "Compliance" as follows:

C:	fully compliant	=	2 points
PC:	partly compliant	=	1 point
NC:	not compliant	=	0 points
Noted:	Noted and accepted (applicable to paragraphs marked as "I", not containing requirements)		

Bidders shall, for paragraphs declared "PC" or "NC", include a statement as to the nature of the variation and may supply additional supporting information in the space provided to demonstrate how the proposal may still meet the needs of ATNS.

Paragraphs marked "(M)", indicates that the requirement is mandatory and proposals that do not comply with the requirement **shall** be disqualified for further evaluation.

Paragraphs marked "(D)", indicates that the requirement is desirable, and the Bidder is expected to declare their level of compliance, provide a formal response and reference supporting documents.

Paragraphs marked "(I)", indicates that the requirement is for information, however the Bidder is still expected to respond and provide information if requested. Any information gathered herein may form part of the contractual terms.

Paragraphs marked "(O)", indicates that the requirement is optional, and the Bidder may decide how to respond.

2 PROJECT SCOPE

The scope of this project encompasses the procurement, supply, delivery, installation, commissioning, maintenance, and support of Global Navigation Satellite System (GNSS) / Global Positioning System (GPS) Network Time Protocol (NTP) time clock synchronisation systems with a system lifecycle of 15-years. The aim of this project is to replace the ageing/obsolete local and remote time synchronisation systems, as well as establish new Time Synchronisation systems where necessary. Time Synchronisation Systems shall be provided at the following airports.

2.1 NORTHERN REGION

2.1.1 Sites

- FAOR
- FAOR SSS
- FALE
- FABL
- FALA
- ATA
- FAGM
- FAPN
- FAMM
- FAKN
- FAWB
- FAPP
- FAGC
- FAPM
- FARB
- FAVG
- FAKM
- FAUP

2.2 SOUTHERN REGION

2.2.1 Sites

- FACT
- FACT SSS
- FAPE
- FAEL
- FAGG
- FAUT

The above sites have been divided into 3 types of sites which are Major, Main and Remote sites. Redundant NTP time reference sources will be required at Major-Sites. For Main-Sites, and for the purpose of the project, only a single new NTP time reference source is required since the redundancy will be established using existing NTP Time reference infrastructures. Remote-Sites will have no new redundant equipment installed to save costs. However, the Internet Service Provider (ISP) or Very Small Aperture Terminal (VSAT) links can be utilised as an aggregate medium to establish an alternative NTP time source from the Major and Main-Sites to Remote-Sites.

The new and replacement Time Synchronisation systems will synchronise time with GNSS/GPS NTP time master clocks across all Air Traffic Management (ATM), Communication Navigation and Surveillance (CNS) and local Air Traffic Control (ATC) system networks for all airports at which Air Traffic and Navigation Services (ATNS) provides air traffic services and for remote sites where appropriate aggregate infrastructure exists.

3 PROJECT OVERVIEW

Various Time Synchronisation System design solutions for each Site were considered and the final solutions chosen was based on essential redundancy requirements, security, and cost effectiveness taking into consideration existing network and aggregate infrastructures. The successful solution shall cater for different site types and each site type shall cater for a different Time Synchronisation System design topology.

3.1 FINAL DESIGN CONCEPT

The final design concept entails three different system topology designs according to the different types of sites:

- Major-Site System
- Main-Site System
- Remote-Site System

The design is based on the utilization of the existing Information Technology (IT) network infrastructures at each site. Where possible and for additional redundancy aggregates for an alternative NTP Time reference source the existing IT/ISP or VSAT (where available) shall be utilised. Necessary and essential security measures need to be implemented to ensure that the time synchronisation services are not compromised as well as all systems interfacing to the time synchronisation equipment.

Major-Sites, Main-Sites and their associated Remote-Sites are shown in Table 2.

Table 2: Breakdown of Major-Sites, Main-Sites and Remote-Sites per Region.

Region	Major-Sites	Remote-Sites
Northern	FAOR	FAGM, FAPN, FAMM, FAKN, FAWB, FAPP, FAGC, ATA
Northern	FAOR SSS	N/A
Southern	FACT	N/A
Southern	FACT SSS	N/A
Region	**Main-Sites**	**Remote-Sites**
Northern	FALE	FAPM, FARB, FAVG
Northern	FABL	FAKM, FAUP
Northern	FALA	N/A
Southern	FAPE	N/A
Southern	FAEL	FAUT
Southern	FAGG	N/A

4 BIDDER/CONTRACTOR OBLIGATIONS

[A] The Bidder shall provide a compliance statement to each specification to confirm that, if the Bidder is appointed as the Contractor, all requirements and obligations stated in this specification shall be complied with. (I)

COMPLIANCE (C/PC/NC)	
[THE BIDDER SHALL INSERT FULL RESPONSE FOR EVALUATION HERE]	
[THE BIDDER SHALL INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

5 GENERAL SOFTWARE AND HARDWARE SPECIFIC EXPECTATIONS

[A] The proposed hardware to be provided shall not be obsolete (Refer to the definition), and shall not be past its sell by date, and shall not be unsupported to avoid obsolescence probabilities in the short-term (within the next 5-years after contracting). The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] Equipment shall not be procured before the System Design Review (SDR) signage to further avoid Obsolete (Refer to the definition) equipment. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] The latest Operating System (OS) version, firmware version, Application Programming Interface (API) and Graphic User Interface (GUI) software versions, and hardware drivers, etc. shall be provided for all relevant equipment and System-Components (Refer to definition) before the Site Acceptance Test (SAT) of each system. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] No restore or recovery of any hardware items (such as restoring from a cloned Hard Disk Drive (HDD)) shall rely on the internal equipment batteries being functional. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] Where improvements in the design topology can be made, especially where improvements for security, redundancy and availability of the intended service and application and cost efficiency is concerned, the vendors should recommend such improvements in their proposals with the associated design topology diagrams. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The Network Time Protocol (NTP), Time Management Handler (TMH), Router and Local Area Network (LAN) Switch equipment models to be used shall all cater for the latest technologies, redundancy protocols and security measures. Those included within this document shall be viewed as the minimum requirements unless better features have become available in the IT and Network industry. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

6 SYSTEMS

The effectiveness and value of the resultant Network Time Synchronisation performance, design topologies and implementation of each (for all the required project systems) shall be measured and demonstrated against the following time synchronisation elements:

[A] Stability: Refers to the measure of the automatic adjustment of the clock when observed over a period of time – Maintaining a constant clock frequency. Refer to Figure 1 for the concept of stability.

[B] Accuracy: How the time reference clock compares to international and national standards. (The proximity of the time reference's absolute value to the offset of zero). The clock shall be regarded as accurate when its offset is zero at a particular moment in time. Refer to Figure 1 for the concept of accuracy.

[C] Precision: How precise the time can be resolved/synchronised in each timekeeping system.

[D] Offset: The time difference between two clocks compared to the Coordinated Universal Time (UTC) as well as how precise the re-synchronisation of the clock with an offset/drift can recover according to Original Equipment Manufacturer (OEM) specifications.

[E] Relative Offset: The concept of where true time is replaced by the time as reported by one clock when comparing how 2 clocks compare to each other. E.g., Clock-2's offset relative to Clock-1 at a particular instance of time (Clock-2 minus Clock-1) and the instance difference in time reported by Clock-2 and Clock1.

[F] Resolution: The smallest unit by which a clock's time is updated in terms of seconds and shall be relative to the clock's reported time and not reference time.

[G] Skew: The frequency difference between a clock or the first derivative of its offset with respect to time.

[H] Reliability: The fraction of time that a time reference can be maintained throughout the time synchronisation processes, operations, and connections within the network of each system.

[I] Synchronisation subnet: All time servers on the network capable of each measuring offset between their own local clocks and neighbouring servers and the relative offset must be zero.

[J] Peers: Neighbouring time servers defined as peers to other time servers and refers to an establishment of the NTP protocol on a remote computer connected by a network link from the local node.

[K] Time servers: Timekeeping servers belonging to a time synchronisation subnet where time reference clocks are maintained.

[L] Security: Detection and Mitigations of known latest security vulnerabilities shall be simulated/demonstrated.

[M] Time synchronisation: Setting two clocks to agree at a particular time interval with respect to the Coordinated Universal Time.

[N] Frequency synchronisation: Adjusting clocks on a subnet to operate at the same frequency.

[O] Clock synchronisation: Synchronisation of two clocks in both frequency and time.

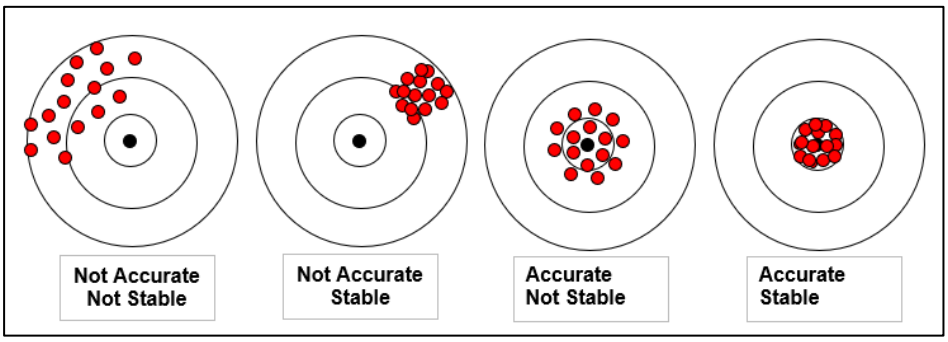


Figure 1: Accuracy and Stability Concept

6.1 SYSTEM DESIGN TOPOLOGIES

[A] All of the designs depict minimum requirements. The Bidder may, as an option, propose a more secure, redundant and mainly cost-effective design topology for each of the three types of designs, not compromising redundancy and security features, at the three different sites and the option might be considered as part of the procurement processes. [O]

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

6.1.1 All Sites

[A] Network Switches (NSW) shall be catered for to distribute the time synchronisation at each Site to other local systems and equipment. (I)

COMPLIANCE (C/PC/NC/Noted)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] It shall be catered for in the design topologies to allow for all Remote-Sites to connect to Major and Main-Sites via the IT, ISP, or even via a VSAT link as well as to the CNS/ATM/Other Systems via secure router and NSW firewalls. (I)

COMPLIANCE (C/PC/NC/Noted)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] It shall be catered for in the design topologies to allow for an aggregate medium as an alternative Time Reference Source as well as for Monitoring Control and Supervision (MCS) services via the ATNS IT Network and associated ISP or VSAT existing infrastructures. (I)

COMPLIANCE (C/PC/NC/Noted)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] Three different system designs for the different sites (Major-Site, Main-Site, Remote-Site) shall be provided as follows. (I)

COMPLIANCE (C/PC/NC/Noted)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

6.1.2 Major Sites

[A] At Major-Sites, a basic design concept shall be catered for that entails the implementation of two GNSS/GPS antennas and two Master-Clocks (NTP Servers), each feeding a Time Management Handler (TMH) server configured in a dual node redundant setup to which all other associated local systems and Remote-Site systems shall synchronise their times. Refer to Figure 2 for the Major-Sites' basic design concept. (I)

COMPLIANCE (C/PC/NC/Noted)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

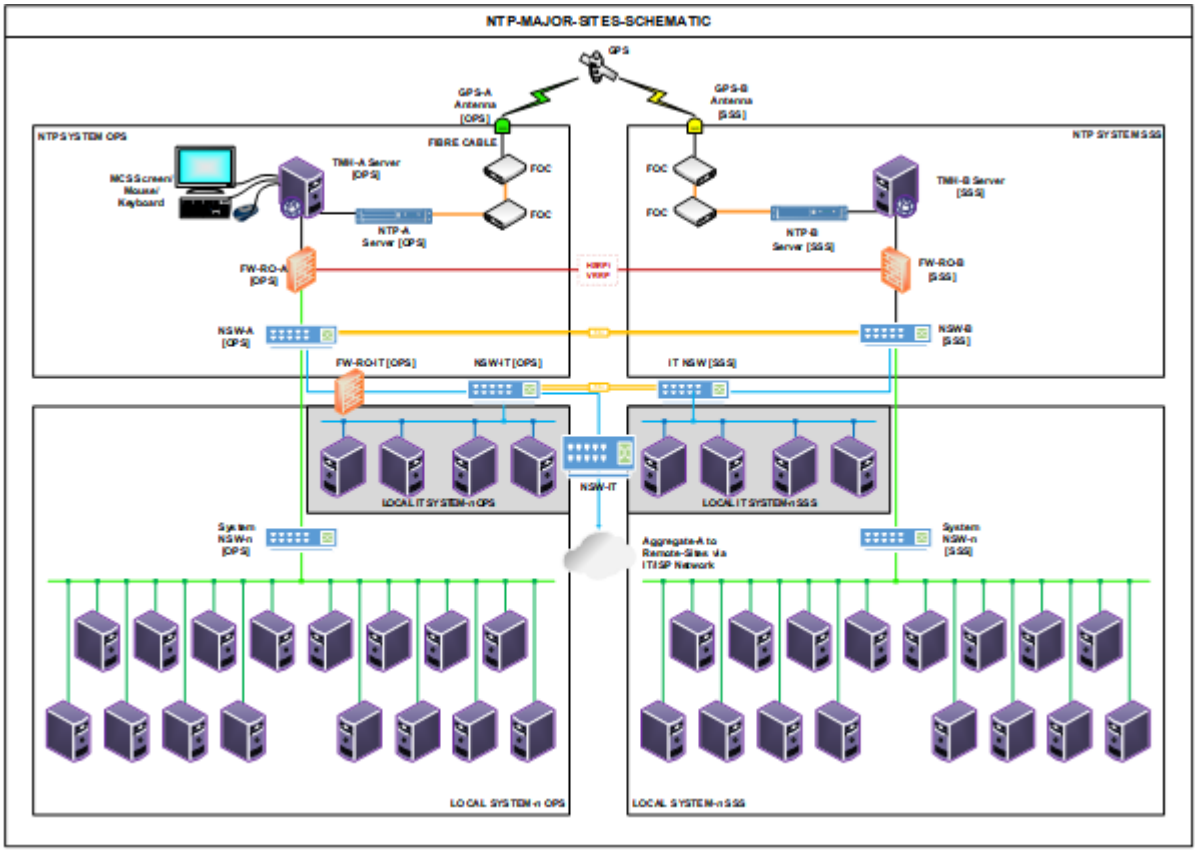


Figure 2: Basic Concept of the GPS NTP Time Synchronisation at Major Sites

6.1.3 Main-Sites

[A] At Main-Sites, a basic design concept shall be catered for that entails the implementation of one GNSS/GPS antenna and one Master-Clock (NTP Server) feeding a Time Management Handler (TMH) server to which all other associated local systems and Remote-Site systems shall synchronise their times. The redundancy shall be achieved using the existing NTP server on the TopSky system as the alternative TMH server. Refer to Figure 3 for the Main-Site's basic design concept. (I)

COMPLIANCE (C/PC/NC/Noted)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

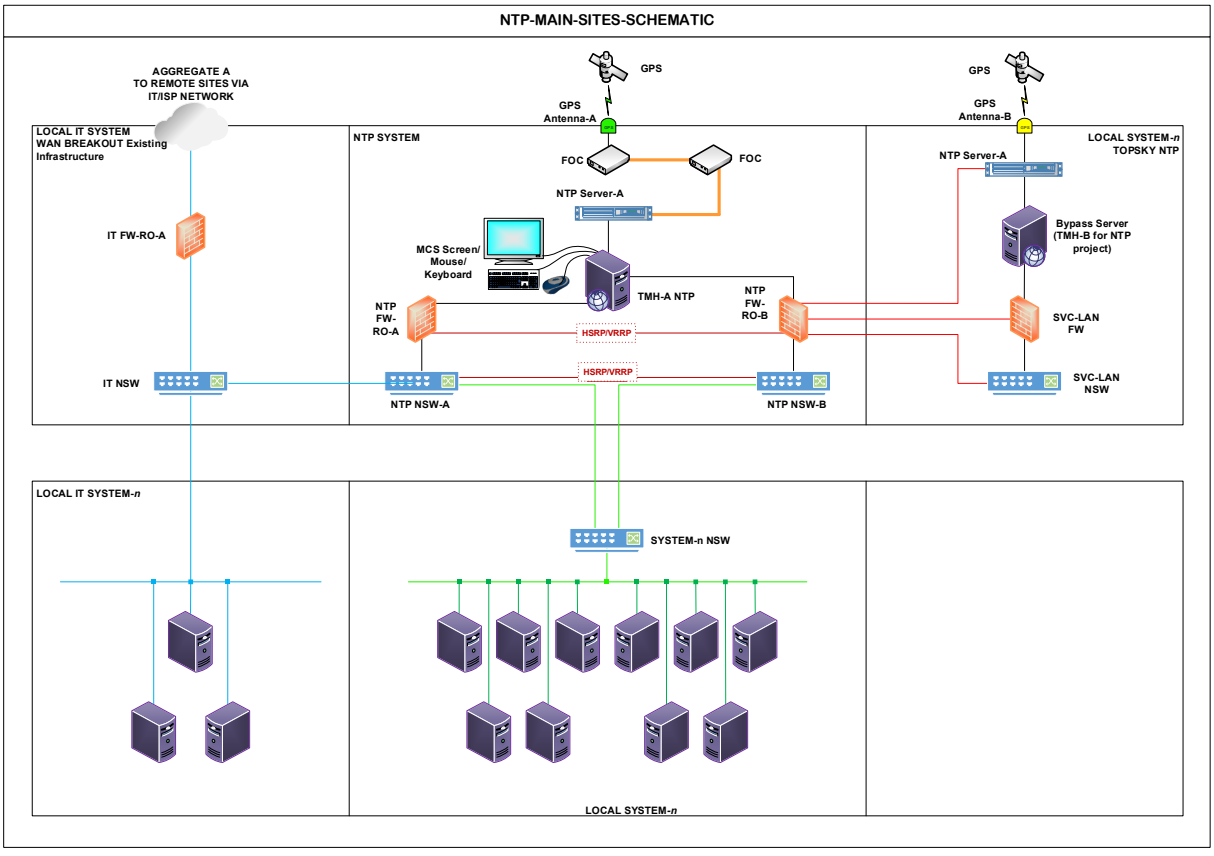


Figure 3: Basic Concept of the GNSS/GPS NTP Master Time Clock Synchronisation at Main-Sites

6.1.4 Remote-Sites

[A] At Remote-Sites, a basic design concept shall be catered for that entails the implementation of one GNSS/GPS antenna and one Master-Clock (NTP Server). (I)

COMPLIANCE (C/PC/NC/Noted)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] Remote-Sites shall have no NTP equipment redundancy, but it shall be catered for to obtain an alternative time reference source input via the ISP/VSAT links for time reference source redundancy. Refer to Figure 4 for the Remote-Sites' basic design concept. (I)

COMPLIANCE (C/PC/NC/Noted)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

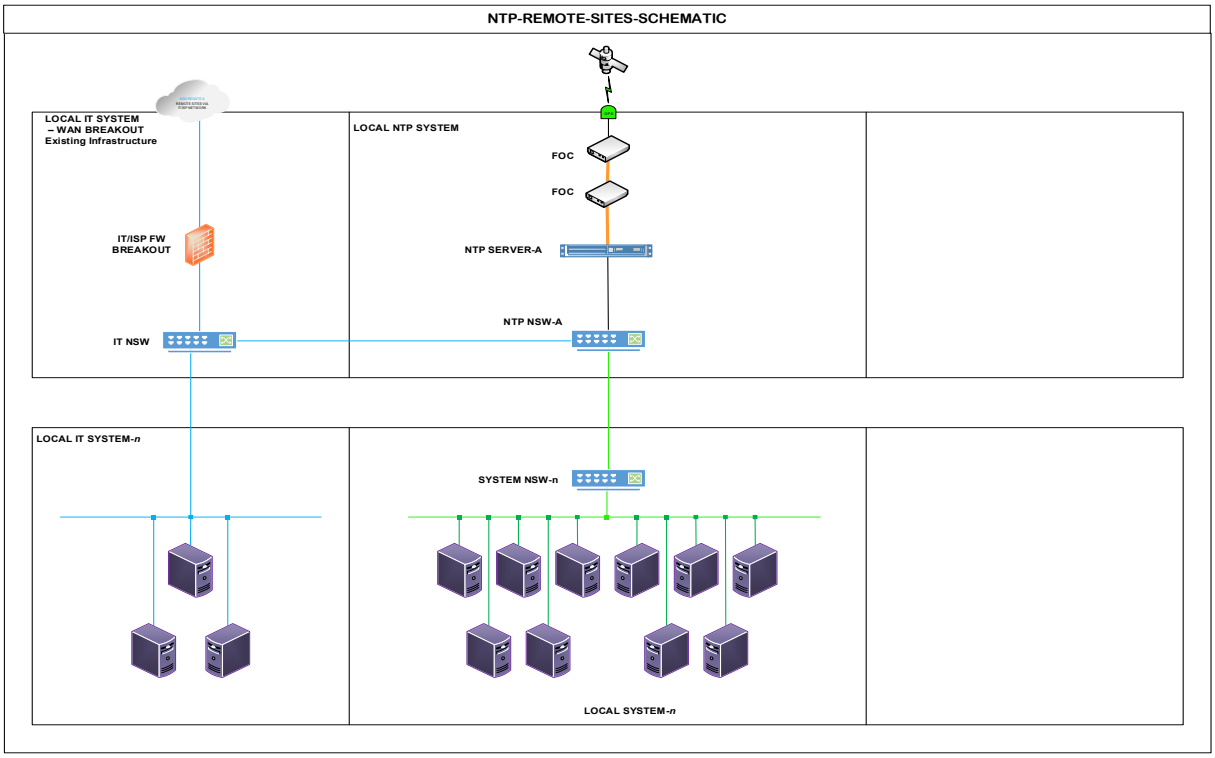


Figure 4: Basic Concept of the GNSS/GPS NTP Master Time Clock Synchronisation at Remote-Sites

7 TECHNICAL FUNCTIONS AND PURPOSE OF EQUIPMENT

7.1 EQUIPMENT LIST

[A] The following equipment list shows the types of equipment required according to the proposed design topologies at the three types of sites but does not clarify equipment per Site. Equipment per site is referenced in section 11.1 Table 3. (I)

- GPS Antennas
- Fibre Optic Converter (FOC)
- NTP Time Servers
- Routers/Firewalls
- Network Switches
- Computers (TMH Servers plus MCS software)

COMPLIANCE (C/PC/NC/Noted)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

7.2 GENERAL FUNCTIONAL REQUIREMENTS

[A] For Major and Main-Sites, the Contractor shall configure a minimum of five upstream time references as peers in the Network Time Protocol Daemon (NTPD) configuration file. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The Contractor shall setup the system such that the NTP Time servers operate at stratum level-1, followed by the Major-Sites and Main-Sites TMH Servers at stratum-2, and so forth. Refer to Figure 5 for a Stratum Level hierarchy example (principle of stratum n + 1). The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] The Contractor shall configure the routers and switches for Major-Sites and Main-Sites as NTP clients in the peer architecture. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] The Contractor shall configure routers and switches at the Remote-Sites such that they shall also run as NTP clients in the peer architecture but shall also use the TMH server in an NTP Symmetric Active Mode, or better type configurations, to synchronise with each other as a backup mechanism when the time reference/source or ISP link is lost. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

7.3 GNSS/GPS ANTENNA GENERAL TECHNICAL FUNCTIONS

[A] The Contractor shall supply and install a total of 24 GPS Antennas at the relevant sites as stated in Table 3. The Bidder shall indicate compliance to this requirement and provide details on the GPS Antennas to be supplied. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] All GPS Antennas shall be fully weather conditions proof against all the harshest known natural environmental elements over the full lifespan (durability) of the Time Synchronisation Systems. The harsh natural environmental conditions shall include lightning, water and humidity, temperature, hail, snow, and shock, all concerning the antenna casing and passive components within. The Bidder shall provide supporting information about the proposed GPS Antennas showing compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] All GNSS Antennas shall allow for a cable connection of at least 300m without the need for a signal booster/amplifier. The Bidder shall provide the minimum cable length of the proposed GNSS Antennas. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] All GNSS Antennas shall cater for a highly effective pre-filter to mitigate inter-modulated signal interference from Long-Term Evolution (LTE) and other cellular bands. The Bidder shall provide details of the proposed pre-filter indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] The Antennas shall receive the GNSS Satellite radio signal frequencies and convert the high frequency phase-modulated signals into an intermediate frequency and into electronic signals for use by the GNSS receiver. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

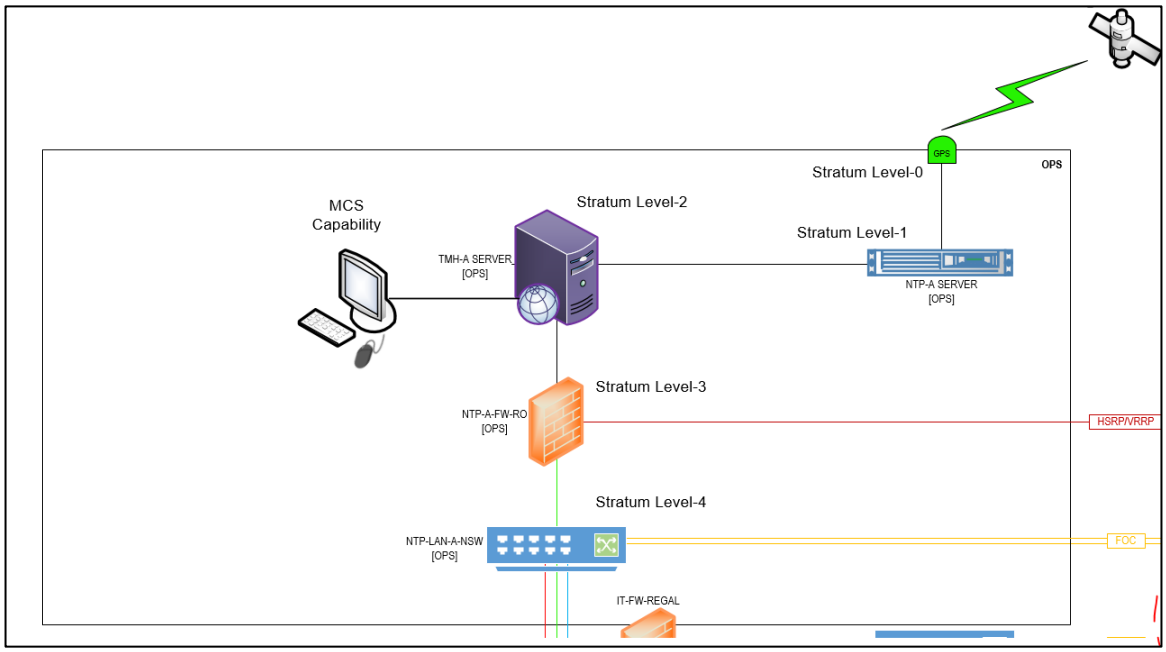


Figure 5: Example of Stratum Levels Hierarchy

7.4 FIBRE OPTIC CONVERTER (FOC) GENERAL TECHNICAL FUNCTIONS

The requirements below are related to the FOC's. Bidders are allowed to propose a solution that may not require the use of FOC's while still complying to the mandatory requirement which states that the connection medium between the antenna and the rest of the system shall be fibre. Should the Bidders proposed solution not require FOC's, the Bidder shall indicate this, and the points allocated to these requirements will be awarded to the Bidder.

[A] The Contractor shall supply and install a total of 48 FOC units at the relevant sites as stated in Table 3. The Bidder shall indicate compliance to this requirement and provide details on the FOC units to be supplied. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] All FOC units shall convert the input frequency from the GNSS antenna into light signals. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] All FOC units shall transport the light signals to the NTP Time servers. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] All FOC units shall supply the Direct Current (DC) bias-T power to the GNSS antennas. Refer to Figure 6 for the FOC units' basic technical functional concept and the specific requirement, respectively. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

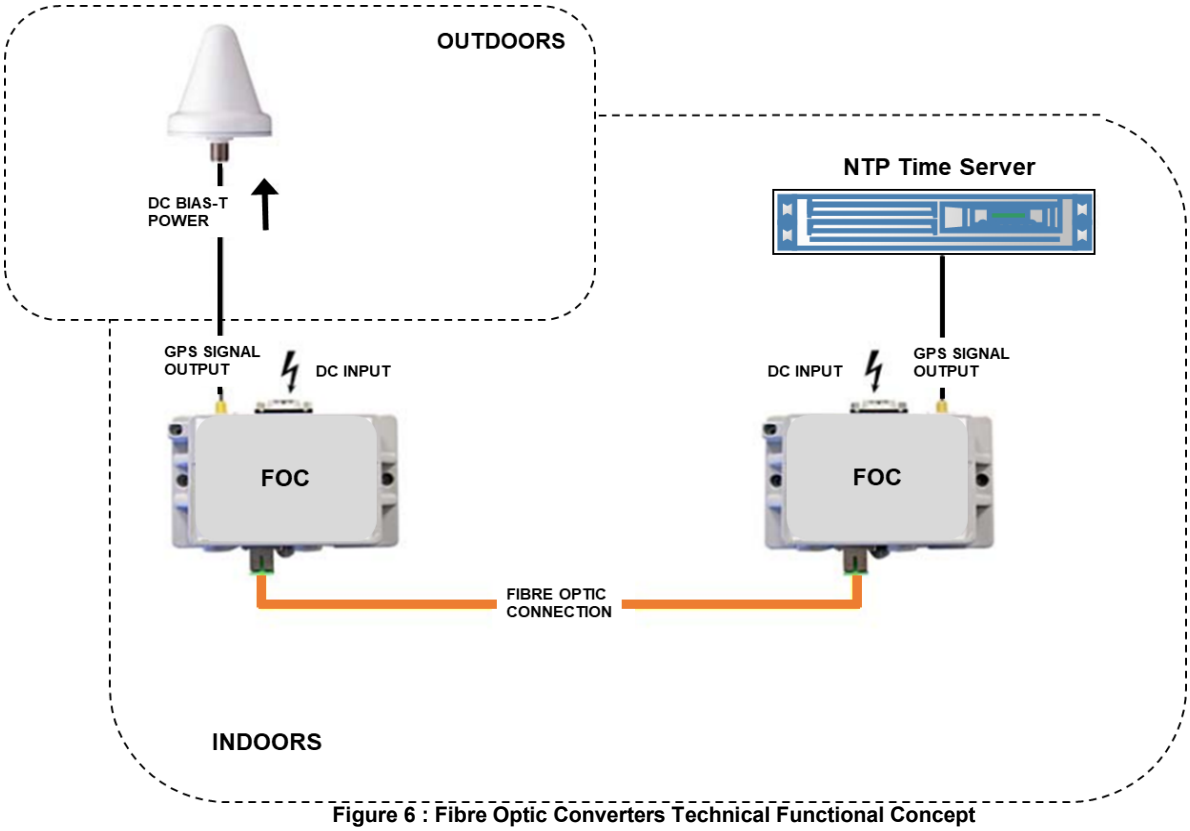


Figure 6 : Fibre Optic Converters Technical Functional Concept

7.5 NTP TIME SERVER GENERAL TECHNICAL FUNCTIONS

[A] The Contractor shall supply and install a total of 24 NTP Time Servers (11 at Major and Main Sites and 13 at Remote Sites) at the relevant sites as stated in Table 3. The Bidder shall indicate compliance to this requirement and provide details on the NTP Time Servers to be supplied. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The proposed NTP Time servers shall serve as Master-Clocks providing accurate time synchronisation to NTP compatible clients. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[C] The proposed NTP Time servers shall use NTPv4 or higher to have better security (Autokey Public Key Authentication Scheme). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] The NTP Time servers at Major-Sites and Main-Sites shall operate in stratum-1 as the Major-Clock time reference. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] The proposed NTP Time servers shall be able to receive GNSS signals. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The proposed NTP Time servers shall utilise High-availability Seamless Redundancy protocols, or an equivalent. Refer to Figure 8 and Figure 9. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[G] The proposed NTP Time servers shall be capable of providing a web-based status and configuration interface and console/dashboard based graphical configuration utility that shall be manageable from the TMH Servers. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[H] The proposed NTP Time servers shall support and provide alarm/alerts notifications of status changes via email, Simple Network Management Protocol (SNMP) and to a monitor screen. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] The proposed NTP Time servers shall support and provide status, configuration, and SNMP trap messages through an SNMP-daemon. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[J] The proposed NTP Time servers shall support the network management systems allowing for monitoring of all relevant System-Components (refer to definition – including operating system parameters, network interface statistics, detailed receiver and NTP status information, and

complete system configuration) and shall also be able to alter the configuration via SNMP set commands and front panel Liquid Crystal Display (LCD). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[K] The proposed NTP Time servers at Major and Main-Sites shall allow for scalability and flexibility. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[L] The proposed NTP Time servers at Major and Main-Sites shall allow for Hot-Plug and Plug & Play modules. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[M] The proposed NTP Time servers at Major and Main-Sites shall allow for remote manageability, monitoring, alerting, reporting and report generation, real-time displaying and configuring of all equipment and network components via an advanced and modern GUI based MCS including for all relevant System Components (refer to definition). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	

[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[N] The proposed NTP Time servers at Major and Main-Sites shall allow for alarm monitoring to be communicated through different protocols including email, SNMP traps, and SYSLOG messages. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[O] The proposed NTP Time servers shall provide an accurate and stable output with a 24/7 operational availability without loss of output provision. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[P] The proposed NTP Time servers shall be high-performance units with the ability to synchronise hundreds of clients on very large networks and shall be able to service a high volume of NTP requests and maintain very high accuracy and availability for all high loads of NTP requests. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[Q] The proposed NTP Time servers at Major and Main-Sites shall allow for advanced modular synchronisation for built-in dual redundancy for input synchronisation of clock reference sources (dual receivers). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[R] The proposed NTP Time servers at Major and Main-Sites shall allow for redundant network links through the assignment of multiple LAN interfaces to a high availability bonding group. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

7.6 TMH SERVERS GENERAL TECHNICAL FUNCTIONS

[A] The Contractor shall supply and install a total of 11 computers to be used as TMH Servers at the relevant sites as stated in Table 3. The Bidder shall indicate compliance to this requirement and provide details on the TMH Servers to be supplied. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The proposed TMH servers shall run the latest supported version of Linux Operating System (OS). The Bidder shall provide information indicating the version of Linux that will be used. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] All TMH servers shall operate at Stratum-2 level receiving the time reference from the Master-Clocks. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] Each TMH Server shall synchronise its time directly with both NTP Servers in a preferred and alternative NTP server configuration with minpoll-4 to maxpoll-7 setup in the NTP configuration file. (e.g., TMH Server-A shall have NTP Server-A as its preferred time synchronisation device with NTP Server-B as the alternative and vice versa for TMH Server-B). The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] For Major and Main sites, each TMH Server shall have the other TMH Server configured as a peer for further redundancy in case a TMH Server loses its synchronisation with both NTP Servers. TMH Server-A shall have TMH Server-B as a peer and vice versa for TMH Server-B. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The TMH Server/s at each site shall become the Master-Clock for all other local systems and devices required to synchronise their times with the NTP time reference. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[G] Each TMH Time server shall have at least 5 peers (unless not possible with the final design topology, then at least 4) defined in the /etc/ntp.conf configuration file where applicable allowing for proper redundancy and allowing for 2 peer failures before the time synchronisation is compromised. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[H] The proposed TMH Servers shall be the host for the monitoring, control, maintenance (MCS) and management software concerning the NTP Network systems and devices. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] The TMH Servers shall host the Management and Monitoring software packages supplied with all relevant devices (NTP equipment and Clocks, Routers, Switches and TMH servers) as well as the relevant additional packages procured as part of the system. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

7.7 ROUTERS & FIREWALL GENERAL TECHNICAL FUNCTIONS

[A] The Contractor shall supply and install a total of 18 Routers at the relevant sites as stated in Table 3. The Bidder shall indicate compliance to this requirement and provide details on the Routers to be supplied. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The proposed Routers shall use data packet source and destination IP addresses (Network Address Translation (NAT)) to find the destination IP address in its routing table and then send each packet on its way in an organised fashion. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] The proposed Routers shall act as a gateway and first line of security to route the NTP time signals safely and protected across to the Remote-Sites from either a Major-Site or Main-Site, as well as to exchange monitoring, management, and status information between sites/systems. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

7.7.1 Performance measures

[A] Implementation of redundancy and security configurations and measures versus normal and effective operations of all time synchronisation and distribution equipment, shall be applied in such a manner to maintain absolute time accuracy and acceptable and optimum performance

(such as for e.g., local and remote monitoring and control). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] All Routers shall cater for best-practice features concerning an integrated network administration dashboard API in Automation & Programmability to reduce time-consuming network troubleshooting tasks and network optimisations, with a Network Management and Automation Platform (NMAP) and Assurance and Network Analysis (or equivalent) features, allowing for every network point to become a sensor that sends continuous streaming telemetry on application performance and user/device connectivity in real time, with the capability of an analytic network API. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] In relation to [B] above, the Automation & Programmability dashboard features shall allow for every device, application, service, and client on the network to provide the user with user-friendly informative insights to the performance and status of the associated item using the latest AI and machine learning technology. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] All routers shall collect data from all different source types, including NetFlow, traceroute, IP SLA, syslog, Web Security Appliance (WSA), RADIUS, Dynamic Host Configuration Protocol (DHCP), Active Directory and users, Command-Line Interface and Secure Shell (CLI/SSH), netconfig, pxGrid, Domain Name System (DNS), Application Visibility and Control (AVC) or any

other Flexible NetFlow (FNF) application service, and Simple Network Management Protocol (SNMP). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] All Network Analysis features mentioned in [D] above shall use a combination of local and remote-based Artificial Interface (AI)-driven analytics engines to interpret all of the data mentioned in [D] above and to automate the process of issue-resolution and performance enhancement. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The Routers shall include application-aware, policy-based routing features that allow it to send traffic over the fastest connection that meets the traffic's security requirements, application needs, and SLA goals. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] The Routers shall include micro-segmentation, URL blacklisting and web filtering capabilities. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	

[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[H] The Routers shall include packet filtering capabilities to control network access by monitoring outgoing and incoming packets and allowing them access based on the source and destination Internet Protocol (IP) addresses, protocols and ports. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] The Routers shall include Deep Packet Inspection capabilities in order to examine the data part of a packet as it passes through it, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may be allowed. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[J] The Router's Deep Packet Inspection capabilities shall ensure that each packet is thoroughly examined to identify malformed packets, errors, known attacks and any other anomalies before they are routed to their destinations. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[K] The Routers shall include a built-in Intrusion Prevention System (IPS). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[L] The built-in IPS shall be able to detect and protect the network efficiently against different kind of attacks like TCP/IP attack, HTTP attack, email attack, FTP Attack, DNS Attack, ICMP Attack, DOS and DDOS Attack and Telnet Attack. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[M] The proposed routers shall be operating in a redundancy configuration that shall prevent frame/packet losses and allow for zero deadtime during failure switchovers including Hot Standby Redundancy Protocol (HSRP) / Virtual Router Redundancy Protocol (VRRP), Rapid Spanning Tree Protocol (RSTP), Beacon Redundancy Protocol (BRP), Parallel Redundancy Protocol (PRP) and Gateway Load Balancing Protocol (GLBP). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[N] The proposed routers shall integrate with ATNS's Active Directory solution for authentication. The Bidder shall indicate compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

7.8 LAN SWITCHES GENERAL AND TECHNICAL FUNCTIONS

[A] The Contractor shall supply and install a total of 33 Network Switches (NSW) (20 x 48 port switches at Major and Main Sites and 13 x 24 port switches at Remote Sites) at the relevant sites as stated in Table 3. The Bidder shall indicate compliance to this requirement and provide details on the NSWs to be supplied. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The proposed NSWs shall cater for best-practice features concerning an integrated network administration dashboard API in Automation & Programmability to reduce time-consuming network troubleshooting tasks and network optimisations, including NMAP Assurance and Network Analysis features, or equivalent, allowing for every network point to become a sensor that sends continuous streaming telemetry on application performance and user/device connectivity in real time, with the capability of an analytic network API that shall be capable of adjusting performance thresholds, reduce alarms and false positives, and automates the process of issue resolution and performance enhancement. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] The Automation & Programmability dashboard features shall allow for every device, application, service, and client on the network to provide the user with user-friendly informative insights to the performance and status of the associated item using the latest AI and machine learning technology. The Bidder shall provide supporting information indicating compliance to this requirement by providing a manual or specification sheet reflecting all of these required capabilities. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	

[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[D] The proposed NSWs shall have a WebUI feature embedded GUI-based device-management tool that provides the ability to administrate the device, simplify device deployment and manageability, and to enhance the user experience. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] The proposed NSWs shall operate utilising the latest and best-practice (industry and proprietary) redundancy features available on the market. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The proposed NSWs shall operate with a dual fan redundancy setup. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] The proposed NSWs shall cater for customised configurations, monitoring and supervision through command line, GUI, and WEB interface means. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[H] The proposed NSWs shall cater for policy-based segmentation. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] The proposed NSWs shall cater for Layer-3 capabilities which shall include:

[a] Open Shortest Path First (OSPF),

[b] Enhanced Interior Gateway Routing Protocol (EIGRP),

[c] Intermediate System to Intermediate System (ISIS),

[d] Routing Information Protocol (RIP),

[e] Routed access,

[f] Full Flexible NetFlow network monitoring,

[g] Secured Device Access (SD-Access),

[h] NMAP network assurance and improved resolution time,

[i] Plug and Play for easy install or expansion,

[j] Model-driven programmability and streaming telemetry,

[k] ACL and Quality of Service (QoS) capabilities.

The Bidder shall provide supporting information indicating compliance to each of these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[J] The proposed NSWs shall allow for a unique selection range of access policy configuration methods to be enforced. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[K] All NSWs shall have a minimum of four (4) 10G SFP ports with 10G transceivers. The Bidder shall provide data sheets for the proposed NSWs indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[L] All NSWs shall have the minimum switching capacity of 96Gbps. The Bidder shall provide data sheets for the proposed NSWs indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[M] All switches shall support 10 000 routing entries and the minimum routing throughput of 100Mpps. The Bidder shall provide data sheets for the proposed NSWs indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

8 TECHNICAL SPECIFICATIONS

8.1 GENERAL TECHNICAL SPECIFICATIONS

[A] All NTP APIs to be loaded on the MCS shall cater for a single software installer and driver package or medium for the latest 64-bit Linux operating systems (OS). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] All NTP equipment shall cater for compatibility between API functions across driver versions and device types. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] All NTP equipment shall cater for all latest API functions to be source code compatible across all latest Linux 64-bit OSs. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] All NTP equipment shall cater for all latest API functions to support the latest new features provided by the latest new devices. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[E] All NTP equipment shall cater for API calls provided by drivers to be thread-safe for multi-tasking environments. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] All NTP equipment shall cater for API calls to the kernel driver where it reads both the reference time from a new Hardware (HW) device and corresponding system time to allow for zero interrupt latencies. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] All source code files required to build own, or customise applications, shall be provided as a pre-installed package. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

8.2 TMH SERVER COMPUTERS TECHNICAL SPECIFICATIONS

[A] The proposed TMH server computers shall be COTS equipment and shall be available in South Africa. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The proposed TMH server computers shall be Desktop type computers. The Bidder shall provide supporting information indicating the type of computer to be supplied. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] The proposed TMH Server computers shall be black in colour. The Bidder shall provide supporting information confirming the colour of the proposed computer. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] The proposed TMH server computers shall be equipped with adequate and effective resources for all intended APIs and functionalities, for future expansion capabilities (scalability), for storage and logging of data, for monitoring, control and management, as well as catering for Next Generation Firewall (NGFW) firewalling capabilities that needs a lot of resources. Not one TMH Server computer shall present with any unacceptable lag in performance and/or compromised capabilities due to a lack of resources. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[E] All TMH servers shall have at least the following minimum specifications:

[a] Processor – 3.6 GHz, i7 generation, multi-core (8+)

[b] Serial Advanced Technology Attachment (SATA) Solid State Drive (SSD) 512GB (Operating System and APIs)

[c] SATA HDD 1TB (Storage)

[d] Random Access Memory (RAM) – Double Data Rate 4 (DDR4) 16GB expandable to 32GB.

The Bidder shall provide supporting information indicating the specifications of the proposed TMH server computers. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

8.3 GNSS ANTENNA TECHNICAL SPECIFICATIONS

[A] The proposed GNSS Antennas at all sites shall use fibre optic multimode type GI50/125µm or GI62.5/125µm fibre as the cable linking the GNSS antenna and GNSS receiver. The Bidder shall provide supporting information indicating the fibre optic multimode type that will be used to link the GNSS antenna to the GNSS receiver. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The proposed Antennas shall have a GNSS signal converter built in. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] The proposed GNSS Antennas shall cater for frequency bands covering from 1164 MHz to 1254 MHz and 1525 MHz to 1606 MHz frequency bands. The Bidder shall provide supporting information indicating the frequency bands that are covered by the proposed GNSS Antennas. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] The proposed GNSS Antennas shall exclude the receiver from the antenna housing. The Bidder shall provide supporting information by providing a specification sheet reflecting this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] The proposed GNSS Antennas shall cater for an external power source. The Bidder shall provide supporting information by providing a specification sheet reflecting this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The proposed GNSS Antennas shall have a gain of +35dB to +40dB. The Bidder shall provide supporting information indicating the gain of the proposed GNSS Antenna. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

8.4 FIBRE OPTIC CONVERTER (FOC) TECHNICAL SPECIFICATIONS

The requirements below are related to the FOC's. Bidders are allowed to propose a solution that may not require the use of FOC's while still complying to the mandatory requirement which states that the connection medium between the antenna and the rest of the system shall be fibre. Should the Bidders proposed solution not require FOC's, the Bidder shall indicate this, and the points allocated to these requirements will be awarded to the Bidder.

[A] The proposed FOC units shall be mounted/situated indoors. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The proposed FOC units shall cater for a coaxial (RG58C/U or RG213/U) cable input from the GNSS Antennas. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] The proposed FOC units shall cater for at least 100 Mbit/s (Fast Ethernet 100BASE-FX) light signal transfer speeds. The Bidder shall provide supporting information indicating transfer speed capabilities of the proposed FOC units. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[D] The proposed FOC units shall cater for Fibre Distributed Data Interfaces (FDDI) of GI50/125µm or GI62.5/125µm multi-mode gradient fibre connections. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] The proposed FOC units shall cater for the prevention of a destructive overvoltage through the antenna cable. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The proposed FOC units shall cater for the prevention of unauthorised or unintentional monitoring and manipulation through the fibre cable. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

8.5 NTP TIME SERVER TECHNICAL SPECIFICATIONS

[A] The proposed NTP Time servers shall cater for a multi-mode optic fibre connection between the GNSS antenna and the TMH receiver. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The proposed NTP Time servers at Major and Main-Sites shall be provided with Redundant Power Supplies (RPS). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] The proposed NTP servers' GNSS receivers shall synchronise the time within < ±100ns of the Coordinated Universal Time (UTC)-second. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] The proposed NTP Time servers shall provide an accurate time synchronisation service to ensure a minimum network time synchronisation latency (typical <500ns to <2ms) for 95% of the time with an allowed offset of no more than a few micro-seconds over LAN networks. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] The proposed NTP Time servers shall cater for time synchronisation over a LAN (Transmission Control Protocol (TCP) / Internet Protocol (IP) over RJ45 and Fibre optic multimode). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The proposed NTP Time servers shall be configured to operate in the following combined Redundancy modes and shall cater for all modes of redundancy where the proposed design or alternative recommended topology permits:

[a] High-availability Seamless Redundancy Protocol (HSRP) or VRRP layer S network redundancy protocol mode.

[b] RSTP network fault tolerance redundancy protocol mode.

[c] PRP and BRP redundant transport layer 2 protocol mode.

[d] Gateway Load Balancing Protocol (GLBP).

Refer also to Sections 9 and 10 for further requirements. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] The proposed NTP Time servers shall have an SNMP-daemon supporting v1, v2c and v3 SNMP capabilities. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[H] The proposed NTP Time servers shall support an extensive SNMP interface to allow for monitoring of all relevant system parameters and shall also be able to alter the configuration via SNMP set commands. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] The proposed NTP Time servers shall have at least one USB 3.0 port with the capability provided to perform updates, backups and restores of configuration and log files, and front panel locking from a USB device. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[J] The proposed NTP Time Servers shall allow for a Precision Time Protocol (PTP) Client: IEEE 1588-2008 Client Software for Linux. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[K] The proposed NTP Time servers shall have a built-in GNSS Signal receiver. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	

[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[L] All NTP Time Servers shall support IPv4, IPv6, NTP / Simple Network Time Protocol (SNTP) (v2, v3, v4), PRP (IEC 62439-3), Hypertext Transfer Protocol (HTTP) (S), SSH, Telnet, SNMP (v1, v2, v3), File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), DHCP/DHCPv6 protocols. The Bidder shall provide supporting information indicating compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[M] The proposed NTP Time Server shall allow for logical network interfaces (IPv4 and IPv6 addresses). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[N] The proposed NTP Time Servers shall utilise hot-plug modules. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[O] The proposed NTP Time Servers at Major and Main-Sites shall cater for future expansion capabilities (be scalable). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[P] The proposed NTP Time Servers shall allow for front panel configuration and status viewing. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[Q] The proposed NTP Time Servers shall be loaded with the latest firmware version before commissioning of the devices (before SAT execution and after SDR signage). The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[R] The proposed NTP Time servers shall cater for additional network protocols including Hyper-Text Transfer Protocol Secure (HTTPS), SFTP, SSH to allow for remote configuration and status requests from a WEB browser. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[S] The proposed NTP Time servers shall cater for a minimum of two NTP ports. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[T] The proposed NTP Time servers shall cater for two redundant GNSS antenna inputs. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

8.6 ROUTERS TECHNICAL SPECIFICATIONS

Refer also to Sections 9 and 10.

8.6.1 General Technical Specifications

[A] The proposed routers shall be provided with Redundant Power Supplies (RPS). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The proposed routers shall be provided with Advanced Malware Protection (AMP) built-in/loaded. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] The proposed routers shall have the capability to combine the security of a network intrusion protection system with the ability to control access to the network based on detected applications, users, and Uniform Resource Locators (URL). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] The proposed routers shall be able to serve in a switched, routed, or hybrid (switched and routed) environment; to perform NAT; and to build secure virtual private network (VPN) tunnels. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] The proposed routers shall be configured to operate in HSRP/VRRP at the distribution level to provide stateless redundancy for IP routing. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The proposed routers shall be configured to accommodate Resilient Ethernet Protocol (REP), or equivalent, networks in the uplinks to the aggregation to minimise the probability of HSRP/VRRP and routing protocol convergence in the event of a failure in the uplink. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	

[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[G] The proposed routers shall be configured to accommodate redundancy protocols for redundant paths in the network to avoid loops. Resiliency (Redundancy) protocols at Network Layer-2 shall include the following criteria where applicable:

[a] **Network Layer** redundancy protocols – Spanning Tree Protocol (STP) (802.1D), RSTP (802.1W), Multiple Spanning Tree Protocol (MSTP) (802.1s), Rapid Per VLAN Spanning Tree Plus (RPVST+), REP, PRP, EthernetChannel (LACP 802.3ad), Flex Links, StackWise.

[b] **Topology** – ring/star networks and shall include a combination of ring and star networks.

[c] **Industry Standards** – resiliency protocols shall be based on industry standards catering also for multi-vendor equipment and systems.

[d] **Convergence Time** – Resiliency protocols shall be selected to meet the maximum convergence time for the particular application.

The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[H] The proposed routers shall be capable of resiliency (Redundancy) protocols at Network Layer-3 which shall include HSRP/VRRP, GLBP, VRRP (IETF RFC 3768). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] The proposed routers shall accommodate and be configured for Bi-directional Forward Detection (BFD) and all protocols such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), HSRP/VRRP, Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP), etc. shall use BFD for

link failure detection. The Bidder shall provide supporting information indicating compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

8.6.2 Technical Performance Specifications

[A] All routers shall be capable to utilise switching methods based on Exact-Match-Lookup (or equivalent) at interrupt-level. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] All routers shall be capable to utilise Switching Algorithms or Switching Paths to forward packets. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] All routers shall be capable to utilise Optimum Switching to allow for multidimensional tree memory usage. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] All routers shall be capable to utilise Express Forwarding using Forwarding Information Based and Adjacent Based tables (or equivalent) for packet forwarding. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] All routers shall be capable to utilise Distributed Express Forwarding for packet forwarding making use of the so-called Virtual IP Address (VIPA). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] All routers shall be configured to select the best switching path available (from fastest to slowest). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

8.7 LAN NETWORK SWITCH (NSW) TECHNICAL SPECIFICATIONS

Refer also to Sections 9 and 10 for further requirements.

8.7.1 General Technical Specifications

[A] The proposed NSW shall allow for new services to be provided through additional licensing means. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The NMAP software shall provide intent-based networking features in the provisioning, managing, monitoring and troubleshooting of these devices. The NMAP intent-based functions shall include, but not limited to:

[a] Using proximity policy optimisation.

[b] Translating customer intent into the appropriate network configuration for management and provision of multiple devices.

[c] Continuously learn through data flows and adapts data flow to actionable insight to assist in detection of potential issues before it becomes problematic while learning from every incident.

The Bidder shall provide supporting information indicating compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] The proposed NSWs shall cater for Analytics and Assurance software as well as for Network Data Platform (NDP) software to allow for continuous learning and collection of events while implementing these insights into pro-active actions. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] The NMAP software shall allow for an open, extensible, and programmable capability for every network layer including integration of other network devices, open APIs, and a developer

platform. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] The proposed NSWs at Major and Main-Sites shall be provided with Redundant Power Supplies (RPS). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The proposed NSWs shall cater for Gigabit Ethernet (100/1000 Mbps). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] The proposed NSWs at Major and Main-Sites shall cater for 48 ethernet ports. The Bidder shall provide supporting information indicating the number of ports available on the proposed NSWs for Major and Main-Sites. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

8.7.2 Technical Performance Specifications

[A] All LAN switches shall be capable to utilise Logical Network Segmentation using VLANs. The Bidder shall indicate and provide proof of compliance to one or both of this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] All LAN switches shall be capable to forward traffic at Nonblocking Wire Speed to obtain zero packet loss. The Bidder shall indicate and provide proof of compliance to one or both of this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] All LAN switches shall be capable to utilise Link Aggregation Control Protocol (LACP) to increase bandwidth by trunking ports. The Bidder shall indicate and provide proof of compliance to one or both of this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] All LAN switches shall be capable to utilise Stacking to allow for multiple switches to operate as one with one IP address for all. The Bidder shall indicate and provide proof of compliance to one or both of this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] All LAN switches shall be capable to prioritise applications by 802.1p/q tags. The Bidder shall indicate and provide proof of compliance to one or both of this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] All LAN switches shall be capable to prioritise applications by IP header using Differentiated Service Code Point (DSCP)/Type of Service (ToS) at layer 3 switching capability. The Bidder shall indicate and provide proof of compliance to one or both of this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] All LAN switches shall be capable to shape traffic packets making use of bandwidth throttling and/or rate limiting. The Bidder shall indicate and provide proof of compliance to one or both of this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[H] All LAN switches shall be capable to allow for set endpoint ports for optimal performance using storm control, number of devices allowed, Quality of Service (QoS) and VLANs. The Bidder shall indicate and provide proof of compliance to one or both of this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] All LAN switches shall be capable to allow for Discovery Protocol to optimise performance connections, allow for fast problem solving and efficient network management. The Bidder shall indicate and provide proof of compliance to one or both of this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[J] All LAN switches shall be capable to allow for SNMP and/or other monitoring and management tools. The Bidder shall indicate and provide proof of compliance to one or both of this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

8.8 MONITORING, CONTROL AND SUPERVISION (MCS) TECHNICAL SPECIFICATIONS

8.8.1 General MCS Technical Specifications

[A] There shall be a Monitoring Control and Supervision (MCS) software tool installed, configured and deployed on the TMH servers at Major and Main-Sites. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The MCS shall support NTP Control Messages. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[C] The MCS shall support Mode-7 commands for monitoring and control. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] The MCS shall support Mode-7 Authentication Keys configuration and setup. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] The proposed MCS shall include a dashboard and associated/separate GUI tool, as well as a Command Line Interface (CLI) and Web-Browser interface. Refer to Figure 7 for an example. The Bidder shall provide supporting information indicating compliance to this requirement by providing one or more manuals or specification sheets reflecting these features/capabilities. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The proposed MCS shall cater for a comprehensive Next-Gen Network Management Software package using a Management Information Base (MIB) principle to monitor, collect and control interfaces, memory and CPU utilisation, bandwidth utilization, user accounting, buffer and interface statistics (including errors, alerts, discards, octets, etc.). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] The proposed MCS shall cater for fault management to proactively capture, report, and act on SNMP trap occurrences on the network using pre-configured trap filters for hardware including multiple condition-based rules for trap matching and filter definition capabilities. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[H] The proposed MCS shall cater for performance management to determine network, device, and resource utilisation as well as a variety of other critical metrics including predictive modelling algorithms to determine MTBF, cater for capacity planning, for third-party applications and network systems allowing for efficient data collection and delivery for data reporting. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] The proposed MCS shall cater for application management to determine the health and availability of applications concerning protocol utilisation and network traffic on any segment of any of the systems connected to the Time Synchronisation System which shall allow for alerting and reporting of events and detect attacks when they occur. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[J] The proposed MCS shall cater for inventory management to discover network elements and to provide a holistic view of the agents, devices, and network applications regarding communication, interaction, and inter-dependencies allowing for automatic creation of network maps and diagrams from the discovered information and overall dependency information. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[K] The proposed MCS shall cater for event correlation to determine how incongruent events are related and make predictions and provide alerts based on pre-defined (user configurable) and self-discovery heuristics. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[L] The proposed MCS shall operate as a managing server (manager) or NMS (Network Management System) interfacing with all network related devices and applications (managed systems) through SNMP and an enhanced Management Information Base (MIB) feature, or equivalent, using low impact software agents to access all managed systems. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[M] The proposed MCS shall cater for local and remote services including configurations, setups, creation of users and user groups, create API and permission lists, monitor, supervise, control, pull and create reports – automatic and manual, etc. to manage all aspects of all sites regionally. Refer to Figure 7 for an example. The Bidder shall provide supporting information indicating compliance to this requirement by providing one or more manuals or specification sheets reflecting these features/capabilities. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[N] The proposed MCS shall provide a detailed presentation of the performance of any device or client over time and from any application context and System-Component (Refer to definition). Refer to Figure 7 for an example. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[O] The proposed MCS shall cater for a multi-vendor network management, IT and Network Analysis software tool that shall provide a general overview of the operational status of every network device and application provisioned and shall provide detailed information on any issue on a device, connection or application through clicking on it. Refer to Figure 7 for an example. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[P] The proposed MCS shall cater for a multi-vendor network management, IT and Network Analysis software tool that shall allow a user to call up history on any previous network issue. Refer to Figure 7 for an example. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[Q] The proposed MCS shall cater for a multi-vendor network management, IT and Network Analysis software tool that shall provide for on-device analytics to identify critical metrics in advance before an incident occurs allowing for pro-active interventions. Refer to Figure 7 for an example. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[R] The proposed MCS shall cater for a multi-vendor network management, IT and Network Analysis software tool that shall provide for a highly visible application experience measure to track the performance of pre-defined critical applications. Refer to Figure 7 for an example. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[S] The proposed MCS shall cater for a multi-vendor network management, IT and Network Analysis software tool allowing for the user to fine-tune network performance through customisation and through its automated machine learning capabilities allowing for identification and rectification of network noise and performance issues. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	

[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[T] The proposed MCS or associated GUI tool residing on the Major and Main-Sites TMH Servers shall allow for monitoring, logging, reporting, configurations, setups and management aspects of the NGFW and Next Generation Intrusion Prevention System (NGIPS) to be performed. Refer to Figure 7 for an example. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[U] The proposed MCS GUI tools requiring licenses shall be provided with a system life-long license. The Bidder shall provide supporting information indicating how this requirement will be achieved. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[V] All software upgrades relating to any of the MCS GUI tools concerning bug-fixes shall be provided without the need to subscribe or procure further software modules or additional licenses or renewal of licenses. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

Figure 7: MCS Management Centre Example

8.8.2 Specific MCS Technical (Telemetry) Specifications

[A] Time synchronisation telemetry shall be provided. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] Local device traffic statistics shall be provided. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] System status information shall be provided. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] Discovery protocol best common practices shall be provided. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] Syslog logging shall be provided. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] SNMP monitoring and control shall be provided. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] ACL logging shall be provided. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[H] Accounting features shall be provided. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] Archive configuration change control logger features shall be provided. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[J] Packet capture features shall be provided. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[K] Critical Success Factor (CSF) features shall be applied for the network telemetry visibility and awareness. The Bidder shall provide supporting information to the CSF visibility and awareness features that shall be applied indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[L] All logging features shall always be date and time stamped. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[M] Local device statistics shall be implemented as part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[N] Interface statistics per interface shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[O] Interface IP visibility shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	

[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[P] Global IP statistics shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[Q] System status information such as, but not limited to, CPU, memory, processes statistics shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[R] Memory threshold notifications shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[S] Critical system logging reservations shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[T] CPU threshold notification traps via SNMP shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[U] Media Access Control (MAC) address table status shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[V] Open ports and sockets shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[W] Discovery protocol capabilities shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[X] Neighbour device information discovery shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[Y] Syslog messages shall be logged to a central server and shall form part of the telemetry features on the TMH servers. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[Z] SNMP and NetFlow (or equivalent) capabilities to perform traffic profiling and anomaly detection shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[AA] ACL logging for detection of failed and non-authorised accessed attempts to each device shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[BB] Authentication, Authorization and Accounting information logging shall account for four modes for accessing and **configuring** the network devices which shall include user mode sessions, privileged mode sessions, global configuration mode sessions, interface

configuration mode sessions such as, but not limited to, username, date, start and stop times, device IP address, user source address, shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[CC] Configuration changes notification and logging shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[DD] Packet capturing after detection of an anomaly to allow for more detailed analysis and inspection shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[EE] Switch Port Analysis and Remote Switch Port Analysis (SPAN/RSPAN) or equivalent to allow traffic monitoring on one or more specific ports shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[FF] Input/output VLAN mapping (VACL, or equivalent) for packet passing (bridged or routed) for traffic analysis purposes shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[GG] Traffic rate analysis capabilities shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[HH] Link flapping detection monitoring and notification shall form part of the telemetry features. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

9 REDUNDANCY REQUIREMENTS

9.1 GENERAL

[A] Where dual redundant equipment is used in the design architecture, the NSWs and routers shall apply the latest redundancy methods to ensure continuous and seamless operations without packet/frame losses and deadtimes, in case of a network break or failure. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] Where dual redundant equipment is used in the design architecture, RSTP protocols shall be applied in all devices' configurations. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] Where dual redundant equipment is used in the design architecture, the best solution configurations for high availability gateways and routing paths between multiple network devices (such as Multiple Path Optimized Link State Routing (MP-OLSR), MPLS, First Hop Redundancy Protocol (FHRP), HSRP, GLBP or VRRP) shall be applied. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] All redundancy configurations for network equipment shall be optimised to avoid routing loops. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] All redundancy configurations for network equipment shall be optimised to avoid Time Loops. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] Where dual redundant equipment is used in the design architecture, PRP and BRP redundancy topologies and Redundancy Box (RedBox) configurations shall be applied to all network devices to ensure zero deadtime when a Double Attached Node implementing BRP (DANB) / Double Attached Node implementing PRP (DANP) device's one LAN port fails. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] Where dual redundant equipment is used in the design architecture, Bi-directional Forwarding Detection (BFD) detection protocols shall be applied to provide fast forwarding path failure detection times which shall be less than one second. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[H] All redundancy configurations shall be optimised to avoid latency differences between strata and the latency for each shall follow a similar latency scale to ensure all NTP equipment are on the same time rather than just on the right time. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

9.2 NETWORK AND DEVICE REDUNDANCY PROTOCOL TOPOLOGIES

[A] The principles of the redundancy concepts depicted in Sections 9.2.1 to 9.2.6 shall be applied to configurations and interconnections of network devices where applicable on all redundant network equipment but shall not be limited to these concepts if a better proposal can be tabled. The Bidder shall provide supporting information on all the topologies offered. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

9.2.1 Router Hot Standby Redundancy Protocol (HSRP) Concept

HSRP allows for two routers to be standby routers for each other. Only one router is the active router and providing data exchanges at a time. When the active router fails the standby router automatically takes over as the active router until such time that the original active router service is restored. All the routers in one HSRP group share the same MAC and IP address as the gateway for the local network. Refer to Figure 8.

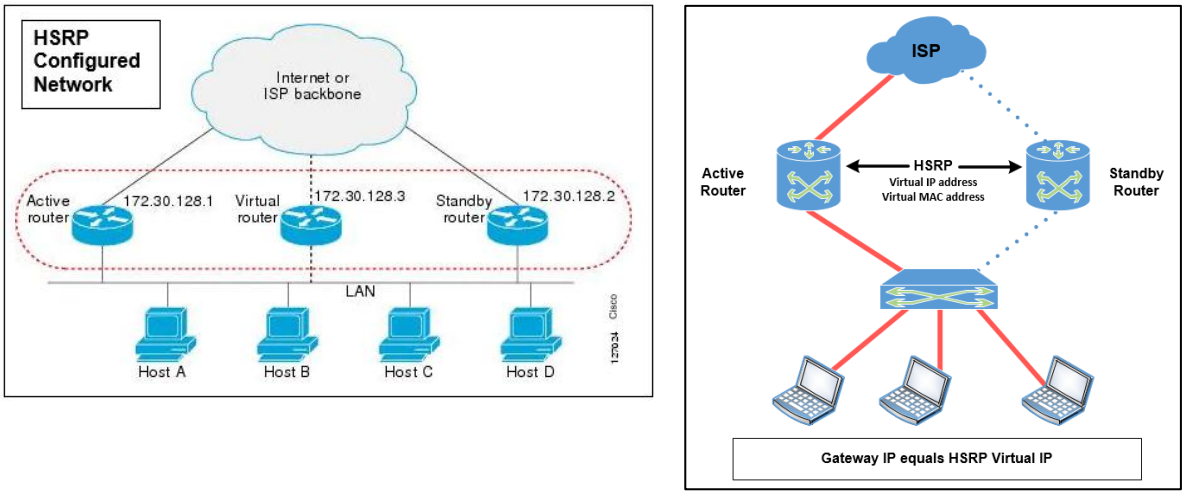


Figure 8: Example of HSRP Design Topology

9.2.2 Virtual Router Redundancy Protocol (VRRP)

VRRP is very similar to HSRP but is an open standard. VRRP allows for router group configuration with one router within the group being the master. The master router's physical IP address of the interface connecting the subnet is used by the clients as a default gateway. The backup members of the VRRP group will communicate with the master gateway and take over the duties of forwarding traffic, should the master fail. The IP address used always belongs to the master router which is referred to as the IP address owner. When the master router recovers, it will take back the duties of routing for that IP address. Refer to Figure 9.

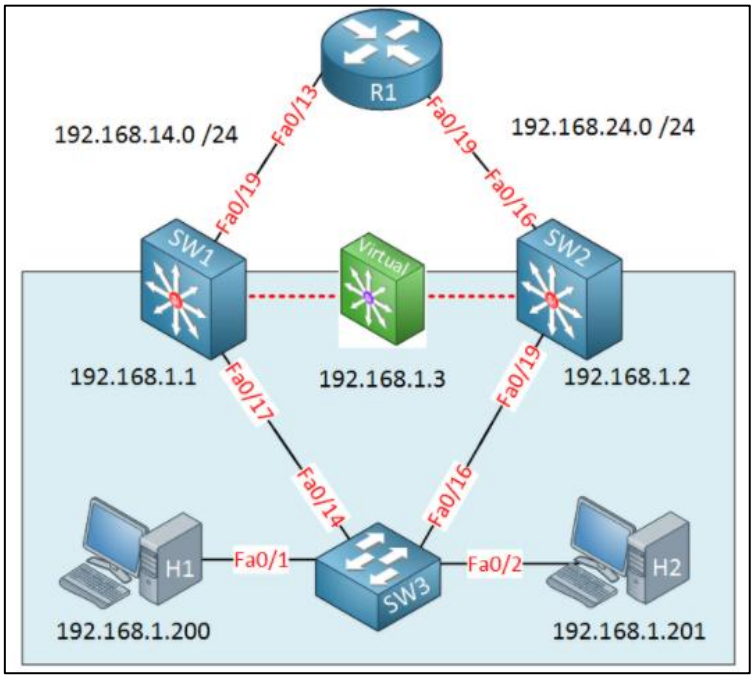


Figure 9: Example of the VRRP concept.

9.2.3 Gateway Load Balancing Protocol (GLBP)

GLBP provides redundancy for data traffic in the event of a failed router or network circuit, while allowing packet load sharing between a group of redundant routers. It allows for automatic selection and simultaneous traffic forwarding from first hop routers within a router group. GLBP provides load balancing over multiple (router) gateways using a single virtual IP address as the default gateway address and multiple virtual MAC addresses. Each host is configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets. GLBP does not use a single virtual MAC address for the entire group, but the Active Virtual Gateway (AVG) assigns different virtual MAC addresses to each of the physical routers in the group. Two types of GLBP routers exist within a router group. One acts as the AVG and handles the operation of the protocol with the highest priority value or main IP address within the router group and responds to all ARP requests for MAC addresses to be forwarded to the virtual router IP address. The second type of GLBP router within a router group is the Active Virtual Forwarder (AVF) router. The AVF is responsible for forwarding data packets sent to the MAC address returned by the AVG router. Many AVF routers can exist in each GLBP router group on a network. Refer to **Error! Reference source not found.**.

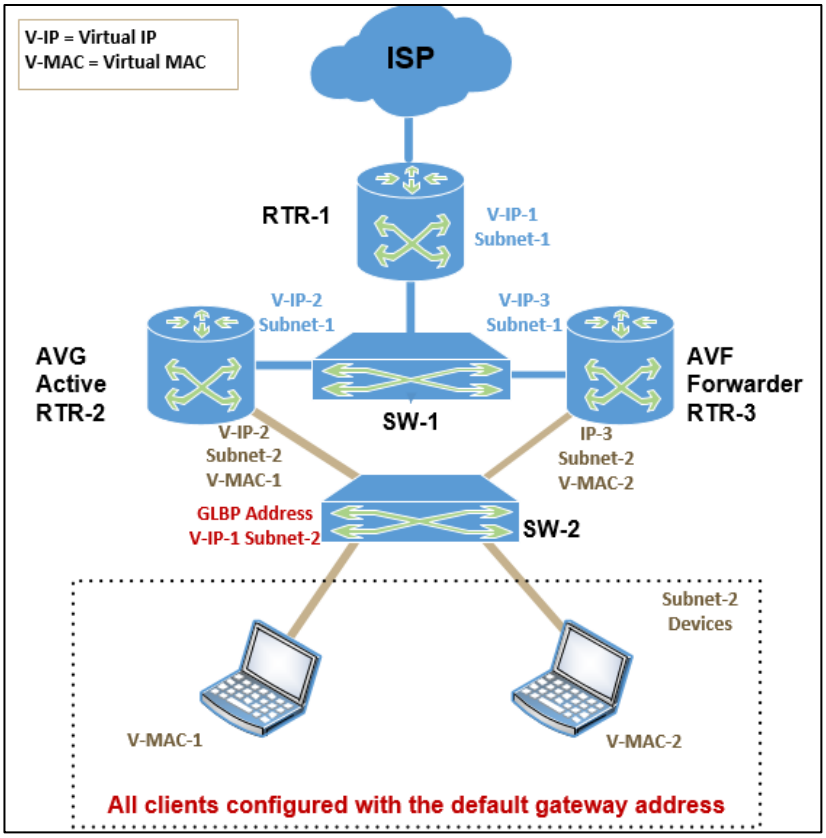
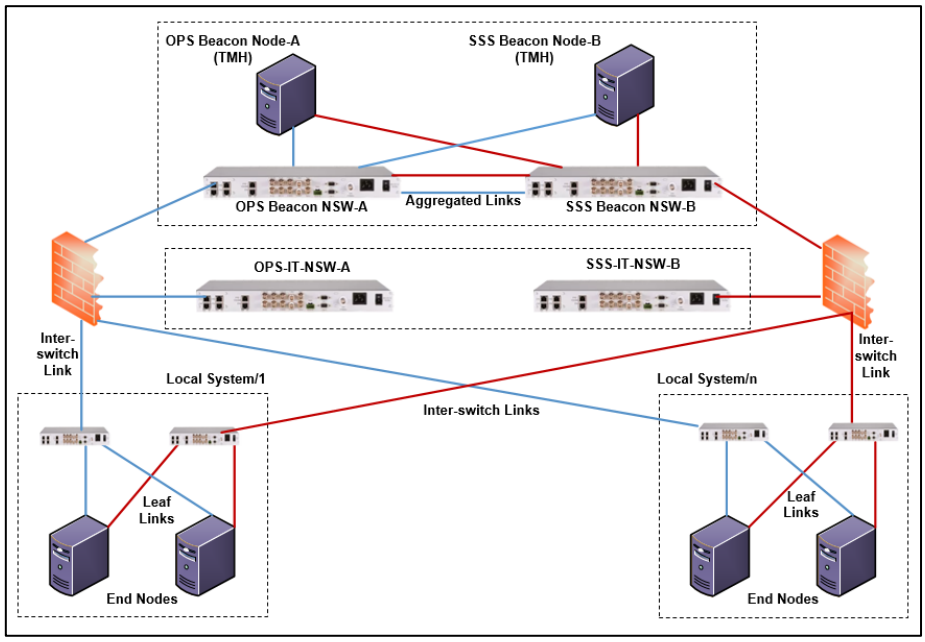


Figure 10. Figure 10: Example of the GLBP Concept

9.2.4 Beacon Redundancy Protocol (BRP)

BRP network topology basically refers to two computer nodes (Beacon nodes) connected to two interconnected switches (Beacon switches), each switch having internal underlying star, line and/or ring network topology capabilities. The rest of the network system and associated end nodes shall effectively connect to these Beacon switches and the Beacon nodes. Refer to Figure 11 for a basic BRP concept example.



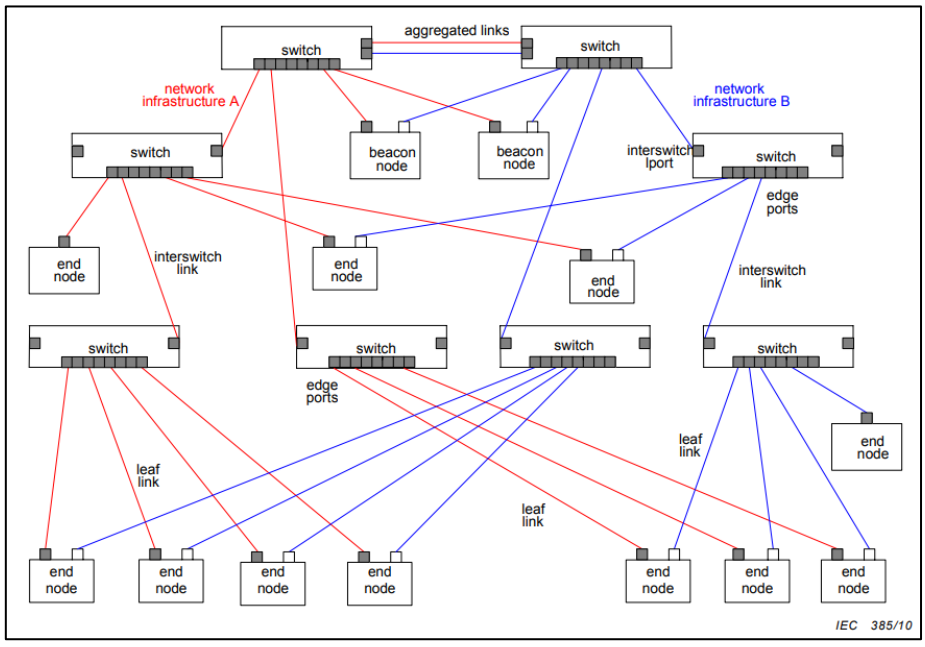
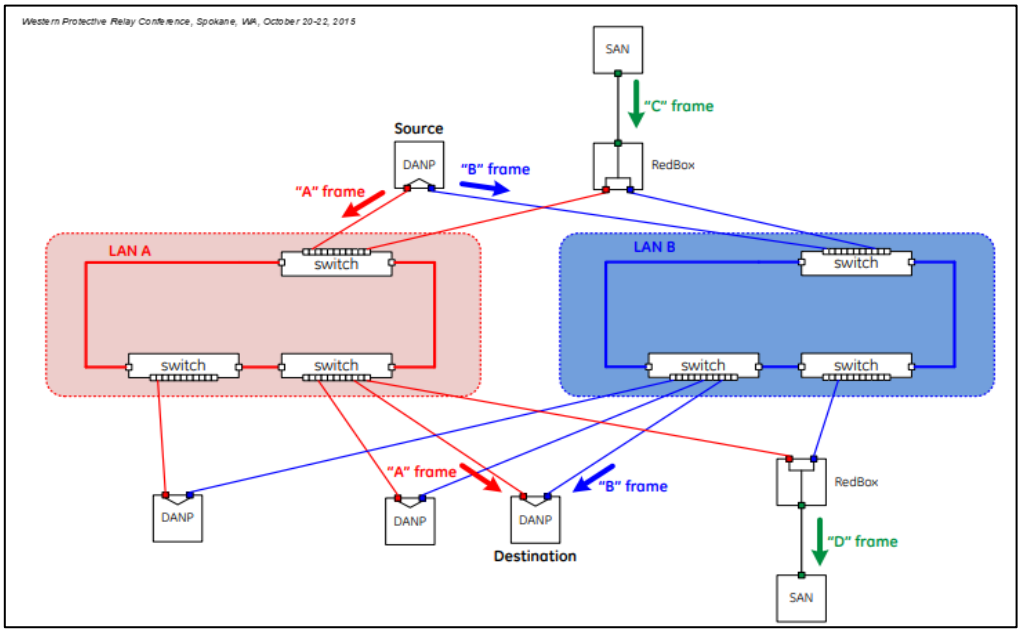


Figure 11: Examples of BRP Redundancy Concept

9.2.5 Parallel Redundancy Protocol (PRP)

In order to ensure that no device network deadtime is experienced, hence no deadtime for data output, it is required to implement a means whereby zero recovery time for data output is experienced when one device's network port fails. This can be achieved by implementing PRP allowing for both network ports of a device to be active in parallel allowing for simultaneous transmission of mirror data. For this purpose, two totally independent (not inter-linked) networks must exist to prevent network loops. The dual LAN port nodes become the actual network redundancy instead of the network elements and are referred to as Dually Attached Nodes (DANs). Networks utilising PRP redundancy need to be in a ring or mesh network layout. If devices have only a single network port (Singly Attached Node (SAN)) a LAN switch, called a Redundancy Box (RedBox), acting as a dual redundant port on behalf of the single port device can be used to maintain network redundancy throughout the network.



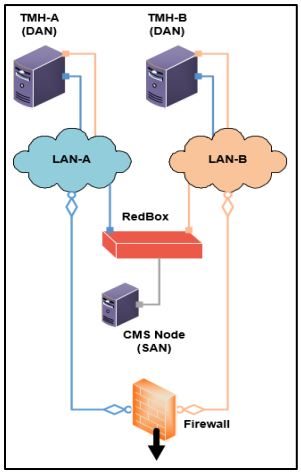


Figure 12: PRP Concept

9.2.6 Bidirectional Forwarding Detection (BFD)

BFD is a detection protocol formulated to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols (BGP, EIGRP, ISIS, and OSPF), hence for all adjacent routers, including the interfaces, data links, and forwarding planes. In addition, BFD provides a consistent failure detection method for network administrators. The network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol 'alive' mechanisms. BFD allows for easier network profiling and planning, and re-convergence time will be consistent and predictable. BFD greatly reduces overall network convergence time. Refer to Figure 13 for OSFP and BFD behavioural examples.

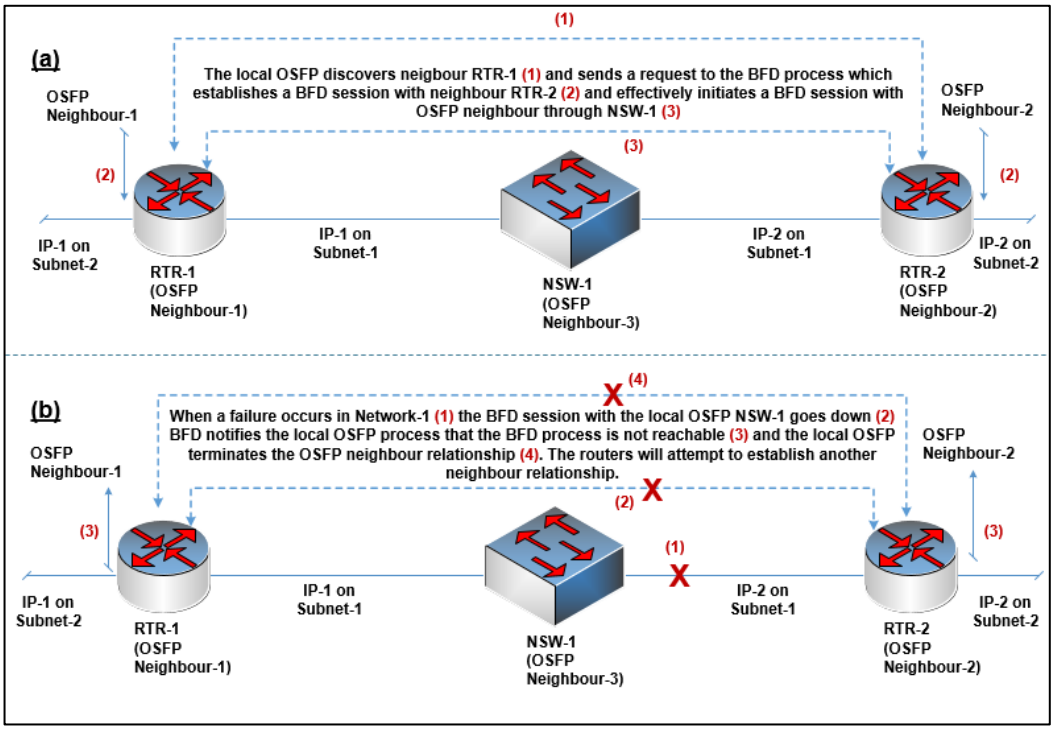


Figure 13: Examples of OSPF and BFD Behaviour (a) Neighbouring (b) Network Link Failure

9.3 NTP Time Synchronisation Redundancy

[A] All NTP Time Servers shall be equipped with and configured for dual Power Supply Units (PSU). The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] All Routers shall be equipped with and configured for dual PSUs. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] All Switches shall be equipped with and configured for dual PSUs. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] For all of the sites where the capability exists for a cluster configuration for NTP Time servers and associated equipment, these shall be configured as such, including configurations to achieve an effective GLBP or BRP and PRP redundancy group setup. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] NTP Time servers at Major-Sites shall be synchronised with both GNSS Antenna sources. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] The two GNSS Antennas and NTP Time Servers at FAOR and FACT shall be installed at separate buildings rendering it ideal for full redundancy NTP networks with all relevant redundancy protocols applied. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] Bonding of two LAN ports on NTP Time Servers, and possibly on other network equipment as well, shall be applied to achieve HSR (High-availability Seamless Redundancy) on the network. Refer to Figure 14 for a simple example of NTP Time Server port bonding. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

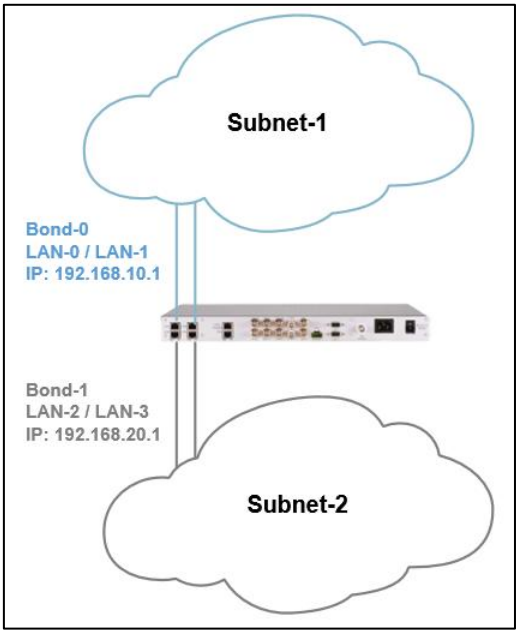


Figure 14: Simple Example of NTP Server Port Bonding for Two Subnets

10 SECURITY

All the NTP Network devices used in the design topologies (for Major, Main and Remote sites) shall cater/implement/apply the latest and best practice security features available at the time of responding to this bid document, including the following:

10.1 NTP SERVER SECURITY

[A] Network Time Security (NTS) security key mechanisms shall be applied as per the topology presented in Error! Reference source not found. to prevent the manipulation of time information by an attacker. The Bidder shall indicate and provide proof of compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

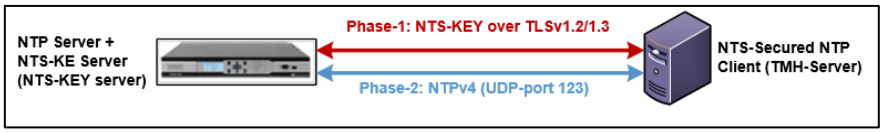


Figure 15: NTS over Separate Communication Paths between Client and Server

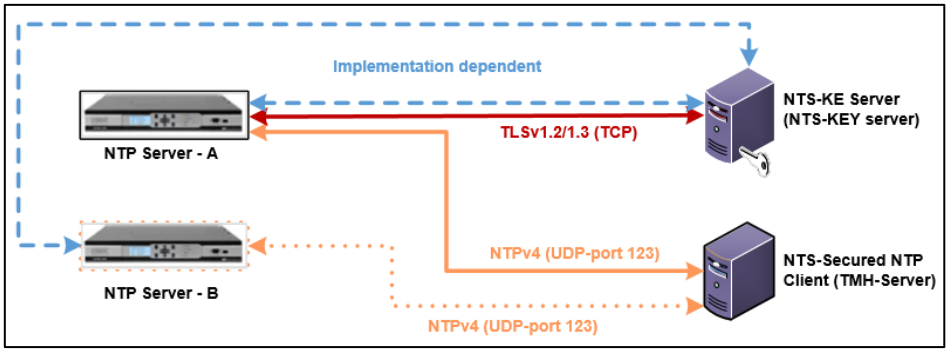


Figure 16: Separation of NTS-KE Server and NTP Time Server

[B] If the topology method as per **Error! Reference source not found.** is not possible in the ATNS proposed or vendor recommended design topology for one or more of the systems, then the option of an additional KEY-server (NTS-KE) shall be used for the NTS instead, and shall be added to the design topology for each Site System as depicted in **Error! Reference source not found.**. The Bidder shall indicate and provide proof of compliance to this requirement if it becomes applicable. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] Hardware timestamping shall be implemented and shall cater for real-time hardware based NTP packet identification and timestamping to protect the device from excessive network traffic denial of service attacks and notify the operator if NTP traffic is above expected levels. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] Where applicable, CPU-based bandwidth limiting shall be introduced to allow for only a pre-determined number of packets to reach the NTP server CPU. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] HTTPS/ Secure Sockets Layer (SSL) security measures shall be implemented to encrypt management traffic between server and the web GUI application and interface. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] A password shall be required before NTP server management shall be allowed. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] NTP authentication and NTP autokey shall be applied to provide key based hashed NTP packet exchanges between clients and servers. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[H] TACACS+, RADIUS, and Lightweight Directory Access Protocol (LDAP) authentication shall be introduced to limit who has access to the NTP server through credentials based on industry-leading access management systems. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] These features, [H] above, shall also allow for server management through the MCS central management system as part of the network-wide access management system and shall allow for remote management of each device. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[J] All the NTP Time Servers shall be configured to use encrypted SSH, HTTPS or SNMPv3 channels. The Bidder shall indicate and provide proof of compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[K] Non-applicable, unused or unwanted protocols that shall not interfere with fault-finding, performance, logging, status monitoring, and overall management of the network and System-Components (refer to definition), analysis, configurations and setup, shall be disabled to reduce possible points of attack. The Bidder shall indicate clearly which protocols shall be disabled and which protocols shall be activated with proof of compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[L] All NTP Time Servers shall be protected against GNSS spoofing. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[M] All NTP Time Servers shall be protected against GNSS jamming. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[N] All NTP Time Servers shall be protected against accidental interference including nearby antennas transmitting in adjacent frequency bands bleeding into the GNSS bands. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

10.2 ROUTER SECURITY FEATURES

[A] All routers shall have the latest and best practice security protection and as a minimum shall provide/implement/apply protection against and/or prevention regarding Sniffing-Based attacks including, but not limited to:

[a] Man-In-The-Middle (MITM) attacks such as Traffic Redirect, Traffic Sent to a Black Hole. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[b] Distributed Denial-of-Service (Memcached DDoS) protection against Internet Control Message Protocol (ICMP) Flood, User Datagram Protocol (UDP) Flood, and TCP-Flood, Unauthorised Route Prefix Origination covert networks attacks, Bogus attacks, Wiretap attacks, replay attacks of Duplicate and Old Duplicate packets, Cut-and-paste attacks, Passive attacks, Middleman attacks, Masquerade attacks, Delay attacks, and DoS attacks. The Bidder shall indicate and provide proof of compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The Bidder shall indicate and provide proof of compliance that all routers shall have the latest and best practice security protection and as a minimum shall implement and apply, including, but not limited to:

[a] Routing Protocol Messaging Authentication for Plain Text Password Authentication and Message-Digest algorithm (MD5) Authentication. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[b] EIGRP or equivalent. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[c] Network Time Security (NTS) in Unicast mode. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[d] Load Balancing per Flow for upstream traffic. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[e] State-Sharing Security Devices. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[f] Router configuration methods to manipulate Return Packet Flows by using Routing or Network Address Translation (NAT). (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[g] Filtering of inbound and outbound Internet Control Messaging Protocol (ICMP) traffic to allow how much ICMP traffic (Committed Access Rate (CAR)), which message types will be allowed (ping, etc.) and blocking of fragmented ICMP messages using ACL by applying the principle of "Expressly permit, implicitly deny." (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[h] Protection against and/or prevention regarding replay attacks at the on-wire protocol layer. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

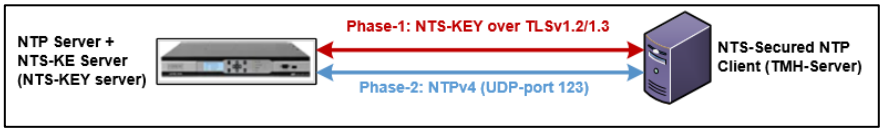
[i] Protection against and/or prevention regarding all relevant Common Vulnerabilities and Exposure (CVE) attacks as depicted in Table 4. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[j] NTP encryption and/or Access Control Lists (ACL). (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	



[k] Address Resolution Protocol (ARP) inspection. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[l] IP Source Guard. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[m] Dynamic Host Configuration Protocol (DHCP) to counter snooping attacks. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[C] Additional security features shall include prevention, threat-hunting, and remediation capabilities against endpoint attacks such as software equivalent to AMP or Endpoint Detection and Response, and shall provide the following functions:

[a] Continuous analysis. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[b] Retrospective security. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[c] FireSIGHT Management Centre. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[d] Collective Security Intelligence. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[e] Indications of compromise. The Bidder shall indicate and provide proof of compliance to one or both of these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[f] File reputation. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[g] File analysis and sandboxing (isolation). The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[h] Retrospective detection. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[i] File trajectory. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[j] Integrated SSL Decryption. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[k] Integration with AMP for Endpoints. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

10.3 LAN SWITCH SECURITY FEATURES

[A] All switches shall have the latest and best practice security protection, and as a minimum shall provide/implement/apply protection against and/or prevention including, but not limited to, Border Gateway Protocol (BGP) attacks using Public Key Infrastructure (PKI) and IP-sec. The Bidder shall indicate and provide proof of compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] All switches shall have the latest and best practice security protection and as a minimum shall provide/implement/apply protection against and/or prevention regarding Sniffing-Based attacks including, but not limited to:

[a] Man-In-The-Middle (MITM) attacks such as Traffic Redirect, Traffic Sent to a Black Hole. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[b] Denial-of-Service (DoS). The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[c] Distributed Denial-of-Service (Memcached DDoS) protection against ICMP-Flood, UDP-Flood, and TCP-Flood, Unauthorised Route Prefix Origination covert networks attacks, Bogus attacks, Wiretap attacks, replay attacks of Duplicate and Old Duplicate packets, Cut-and-paste attacks, Passive attacks, Middleman attacks, Masquerade attacks, Delay attacks, and DoS attacks. The Bidder shall indicate and provide proof of compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	

[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[C] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply Routing Protocol Messaging Authentication for, but not limited to, Plain Text Password Authentication and MD5 Message-Digest Authentication. The Bidder shall indicate and provide proof of compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, Enhanced Interior Gateway Routing Protocol (EIGRP) or equivalent. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, Network Time Security (NTS) in Unicast mode. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[F] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, Load Balancing per Flow for upstream traffic. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, State-Sharing Security Devices. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[H] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, VRRP and HSRP. The Bidder shall indicate and provide proof of compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply and cater for, but not limited to, router configuration methods to manipulate Return Packet Flows by using Routing or Network Address Translation (NAT). The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[J] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, filtering of inbound and outbound Internet Control

Messaging Protocol (ICMP) traffic to allow how much ICMP traffic (Committed Access Rate (CAR)), which message types will be allowed (ping, etc.) and blocking of fragmented ICMP messages using ACL by applying the principle of "Expressly permit, implicitly deny." The Bidder shall indicate and provide proof of compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[K] All switches shall have the latest and best practice security protection and as a minimum shall provide/implement/apply, but not limited to, protection against and/or prevention regarding replay attacks at the on-wire protocol layer. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[L] All switches shall have the latest and best practice security protection and as a minimum shall provide/implement/apply, but not limited to, protection against and/or prevention regarding all relevant Common Vulnerabilities and Exposure (CVE) attacks as depicted in Table 4. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[M] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, NTP encryption and Access Control Lists (ACL). The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[N] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, Spanning Tree Protocol protection preventing Bridge Protocol Data Units (BPDUs). The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[O] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, security protection for the Discovery Protocol. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[P] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, Address Resolution Protocol (ARP) inspection. The Bidder shall indicate and provide proof of compliance to these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[Q] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, Address Resolution Protocol (ARP) inspection. The Bidder shall indicate and provide proof of compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[R] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, IP Source Guard. The Bidder shall indicate and provide proof of compliance to one or both of these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[S] All switches shall have the latest and best practice security protection and as a minimum shall implement and apply, but not limited to, Dynamic Host Configuration Protocol (DHCP) to counter snooping attacks. The Bidder shall indicate and provide proof of compliance to one or both of these requirements. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

10.4 TMH SERVERS SECURITY

[A] The proposed TMH Servers shall be equipped with software firewall applications that shall apply multi-layer security measures. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[B] The proposed TMH Servers shall have a software firewall activated/installed and configured to protect against unauthorised network access on a per-application basis and shall control and manage incoming and outgoing traffic. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[C] Each TMH Server software firewall shall perform International Society of Automation (ISA) data packet flow, circuit and application filtering and inspection at the boundary of the network to give enhanced security. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[D] Each TMH Server software firewall shall authenticate all communications passing through the firewall. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[E] All traffic passing through the software firewall shall be logged to allow identification of the source of an attack or unauthorised attempt to access the network. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	

[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[F] All software firewalls shall apply the latest available data encryption methods where necessary. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[G] All software firewalls shall apply intrusion security measures including rule-based and behaviour-based monitoring to eliminate suspicious network activity. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[H] The proposed TMH servers shall be provided with centralised management system software to allow for control, configuration, setup of security measures and policies, as well as aggregated reporting of all network devices from the Desktop environment of the TMH servers. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[I] All software firewalls shall apply circuit-level gateways at the session layer of the OSI model to monitor connections and sessions to ensure that the established connections are legit and safe. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

[J] All software firewalls shall apply stateful inspection firewall capabilities creating a dynamic firewall rules state table to keep track of the state of a connection through TCP 3-way handshake to ensure that the entire connection from start to end permits only expected return of inbound traffic. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[K] All software firewalls shall apply NGFW to automatically implement threat protection, full SSL visibility through inspection, gateway anti-virus, intrusion prevention, application and web control, etc. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[L] All software firewall NGFW measures shall be carefully optimised such that they do not considerably impact on data throughput speeds and performance. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[M] Automatic and Manual email sending (outgoing only to ATNS Exchange Email server address) shall be made available on the TMH Servers running the systems management software which shall be secured through encryption. No incoming email shall be allowed to the TMH servers. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[N] The proposed TMH servers shall have Trusted Platform Module (TPM 2.0) secure crypto processors. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[O] The proposed TMH servers shall implement a Self-healing BIOS backup. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[P] The proposed TMH servers shall implement Supervisor, SMP and power-on passwords. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[Q] The proposed TMH servers shall implement electronic lock support. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[R] The proposed TMH servers shall implement Chassis intrusion detection. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[S] The proposed TMH servers shall implement Unified Extensible Firmware Interface (UEFI) secure boot support. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[T] The proposed TMH servers shall implement HDD and SSD password protection for Data. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[U] The proposed TMH servers shall implement Linux UEFI firmware update support. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

[V] The proposed TMH servers shall implement hypervisor security. The Bidder shall provide supporting information indicating compliance to this requirement. (D)

COMPLIANCE (C/PC/NC)	
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

11 NUMBER OF EQUIPMENT REQUIRED

Depending on the final design topology for each site type, the following shall remain in place if the design topology has not changed.

11.1 NUMBER OF EQUIPMENT REQUIRED PER SITE

As per current design topologies for each site type:

Where: M = Major and Main-Sites

R = Remote-Sites

Table 3: Number of Equipment Required

	Site Name	GPS Antenna	FOC	TMH Server	NTP Server-M	NTP Server-R	NSW-M	NSW-R	RTR-M	WAN MCS Capabilities	LOCAL MCS Capabilities
1	FAOR	1	2	1	1	0	2	0	1	Y	Y
2	FAOR SSS	1	2	1	1	0	2	0	1	Y	Y
3	FALE	1	2	1	1	0	2	0	2	Y	Y
4	FABL	1	2	1	1	0	2	0	2	Y	Y
5	FALA	1	2	1	1	0	2	0	2	N	N
6	ATA	1	2	1	1	0	2	0	2	N	Y
7	FAGM	1	2	0	0	1	0	1	0	N	N
8	FAPN	1	2	0	0	1	0	1	0	N	N
9	FAMM	1	2	0	0	1	0	1	0	N	N
10	FAKN	1	2	0	0	1	0	1	0	N	N
11	FAGC	1	2	0	0	1	0	1	0	N	N
12	FAWB	1	2	0	0	1	0	1	0	N	N
13	FAPP	1	2	0	0	1	0	1	0	N	N
14	FAPM	1	2	0	0	1	0	1	0	N	N
15	FARB	1	2	0	0	1	0	1	0	N	N
16	FAVG	1	2	0	0	1	0	1	0	N	N
17	FAKM	1	2	0	0	1	0	1	0	N	N
18	FAUP	1	2	0	0	1	0	1	0	N	N
	Region	**GPS Antenna**	**FOC**	**TMH Server**	**NTP Server-M**	**NTP Server-R**	**NSW-M**	**NSW-R**	**RTR-M**		
	Northern Region Equipment Totals	**18**	**36**	**6**	**6**	**12**	**12**	**12**	**10**		

	Site Name	GPS Antenna	FOC	TMH Server	NTP Server-M	NTP Server-R	NSW-M	NSW-R	RTR-M	WAN MCS Capabilities	LOCAL MCS Capabilities
1	FACT	1	2	1	1	0	1	0	1	Y	Y
2	FACT SSS	1	2	1	1	0	1	0	1	Y	Y
3	FAPE	1	2	1	1	0	2	0	2	N	Y
4	FAEL	1	2	1	1	0	2	0	2	N	Y
5	FAGG	1	2	1	1	0	2	0	2	N	Y
6	FAUT	1	2	0	0	1	0	1	0	N	N
	Region	**GPS Antenna**	**FOC**	**TMH Server**	**NTP Server-M**	**NTP Server-R**	**NSW-M**	**NSW-R**	**RTR-M**		
	Southern Region Equipment Totals	**6**	**12**	**5**	**5**	**1**	**8**	**1**	**8**		

12 REFERENCES

[A] The reference list, as provided below, is not intended to be comprehensive but shall be used by the Bidder to comply and conform to requirements and/or recommendations stipulated within these referenced documents for relevant aspects of the NTP Time Synchronisation Project. The conformance and compliance shall especially be in respect to all Industry Standards and Recommended Practices and Operational Safety Standards.

[B] Where references have been omitted but have relevance to industry standards and requirements or recommendations, the Bidder shall comply and conform to those as well.

[C] The Bidder shall always use the latest version of all relevant and applicable references, as well as for those as depicted below in Table 4.

[D] Some of the reference in Table 4 are informative references and shall be used by the bidder as a guideline to implement optimal features as proposed and recommended by these references.

Table 4: Applicable References and Informative Guideline references

1.	Attacking the Network Time Protocol, NDSS'16, San Diego, CA. , 2016.
2.	BCP 105, RFC 4085, DOI 10.17487/RFC4085, June 2005.
3.	BCP 126, RFC 4786, DOI 10.17487/RFC4786, December 2006.
4.	BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.
5.	BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017.
6.	BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000.
7.	BCP 78, RFC 5378, Rights Contributors Provide to the IETF Trust, NOVEMBER 2008.
8.	BCP 79, RFC 8179, Intellectual Property Rights in IETF Technology, MAY 2017.
9.	BCP 9, RFC 2026, DOI: 10.17487/RFC2026, The Internet Standards Process – Revision 3, OCTOBER 1996.
10.	Computer network time synchronisation: the Network Time Protocol, CRC Press , 2006.
11.	Control Messages Protocol for Use with Network Time Protocol Version 4, Internet-Draft draft-ietf-ntp-mode-6-cmds-06, September 2018. (As described in RFC 1305)
12.	CVE-2015-7979 2021/04/15 Modified date
13.	CVE-2015-8138 2021/11/17 Modified date
14.	CVE-2015-8138, CERT VU#357792, NETWORK TIME PROTOCOL ORIGIN TIMESTAMP CHECK IMPERSONATION VULNERABILITY, 2016.

15.	CVE-2015-8139 2017/11/21 Modified date
16.	CVE-2015-8139. CERT VU#357792, NETWORK TIME PROTOCOL NTPQ AND NTPDC ORIGIN TIMESTAMP DISCLOSURE VULNERABILITY, 2016.
17.	CVE-2015-8140 2017/11/21 Modified date
18.	CVE-2015-8158 2018/01/05 Modified date
19.	CVE-2016-1547 2021/11/17 Modified date
20.	CVE-2016-1548 2021/11/17 Modified date
21.	CVE-2016-1549 2018/03/28 Modified date
22.	CVE-2016-1550 2021/11/17 Modified date
23.	CVE-2016-1550, Xleave Pivot: NTP Basic Mode to Interleaved, 2016. NTP Authentication Potential Timing Vulnerability.
24.	CVE-2016-1551 2017/11/21 Modified date
25.	CVE-2016-2516 2017/11/21 Modified date
26.	CVE-2016-2517 2017/11/21 Modified date
27.	CVE-2016-2518 2021/06/10 Modified date
28.	CVE-2016-2519 2017/11/21 Modified date
29.	CVE-2016-4953 2021/07/16 Modified date
30.	CVE-2016-4954 2021/07/16 Modified date
31.	CVE-2016-4955 2021/07/16 Modified date
32.	CVE-2016-4956 2021/07/16 Modified date
33.	CVE-2016-4957 2020/06/18 Modified date
34.	CVE-2016-7426 2020/06/18 Modified date
35.	CVE-2016-7427 2019/01/24 Modified date
36.	CVE-2016-7428 2019/01/24 Modified date
37.	CVE-2016-7429 2018/01/05 Modified date
38.	CVE-2016-7431 2021/07/12 Modified date
39.	CVE-2016-7433 2021/07/16 Modified date
40.	CVE-2016-7434 2020/06/18 Modified date
41.	CVE-2016-9042 2022/04/19 Modified date
42.	CVE-2016-9310 2019/01/24 Modified date
43.	CVE-2016-9311 2019/01/24 Modified date
44.	CVE-2017-6451 2017/10/24 Modified date
45.	CVE-2017-6452 2017/10/24 Modified date
46.	CVE-2017-6455 2017/10/24 Modified date
47.	CVE-2017-6458 2021/07/12 Modified date
48.	CVE-2017-6459 2017/10/24 Modified date
49.	CVE-2017-6460 2017/10/24 Modified date
50.	CVE-2017-6462 2019/01/24 Modified date

51.	CVE-2017-6463 2019/01/24 Modified date
52.	CVE-2017-6464 2018/04/12 Modified date
53.	CVE-2018-12327 2020/08/24 Modified date
54.	CVE-2018-7170 2020/06/18 Modified date
55.	CVE-2018-7182 2019/10/31 Modified date
56.	CVE-2018-7183 2021/07/20 Modified date
57.	CVE-2018-7184 2020/08/24 Modified date
58.	CVE-2018-7185 2020/08/24 Modified date
59.	CVE-2018-8956 2020/07/19 Modified date
60.	CVE-2019-11331 2020/08/24 Modified date
61.	CVE-2019-8936 2020/10/07 Modified date
62.	CVE-2020-11868 2022/04/26 Modified date
63.	CVE-2020-13817 2022/03/29 Modified date
64.	CVE-2020-15025 2021/01/20 Modified date
65.	CVE-2021-22212 2022/06/03 Modified date
66.	Message Authentication Code for the Network Time Protocol, Internet-Draft draft-ietf-ntp-mac-06, January 2019.
67.	Network Time Security for the Network Time Protocol", Internet-Draft draft-ietf-ntp-using-nts-for-ntp-17, February 2019 and approved in March 2020.
68.	NTP Client Data Minimization, Internet-Draft draft-ietf-ntp-data-minimization-04, March 2019. Updates: 5905 in conformance to BCP78 and BCP79.
69.	Payment Card Industry Data Security Standard (PCI DSS) 10.4
70.	RFC 1059, Network Time Protocol (Version 1) Specification and Implementation.
71.	RFC 1119, Network Time Protocol (Version 2) Specification and Implementation.
72.	RFC 1305, DOI 10.17487/RFC1305, March 1992, Network Time Protocol (Version 3) Specification, Implementation and Analysis.
73.	RFC 5905, DOI 10.17487/RFC5905, June 2010.
74.	RFC 5906, DOI 10.17487/RFC5906, June 2010, Network Time Protocol Version 4: Autokey Specification.
75.	RFC 6151, DOI 10.17487/RFC6151, March 2011, Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms.
76.	RFC 7094, DOI 10.17487/RFC7094, January 2014, Architectural Considerations of IP Anycast.
77.	RFC 7384, DOI 10.17487/RFC7384, October 2014, Security Requirements of Time Protocols in Packet Switched Networks.
78.	RFC 7384, DOI 10.17487/RFC7384, October 2014.
79.	RFC 8729, DOI: 10.17487/RFC8729, The RFC Series and RFC Editor, FEBRUARY 2020.

80.	RFC 8915, October 2021, Network Time Security protocol (NTS)
81.	RFC 958, Network Time Protocol (NTP).
82.	SIGCOMM Computer Communications Review (CCR) , 2016.
83.	Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks, Internet Measurement Conference , 2014.