⊘ Eskom	Standard	Technology

|		
Title:	**Goods Information for: Standard Networking Devices for the Substation Environment Standard**	Unique Identifier:	**240-68111223**
		Alternative Reference Number:	**474-242**
		Area of Applicability:	**Engineering Transmission and Distribution**
		Documentation Type:	**Standard**
		Revision:	**1**
		Total Pages:	**92**
		Next Review Date:	**N/A**
		Disclosure Classification:	**CONTROLLED DISCLOSURE**

APPROVED FOR AUTHORISATION
☑ TECHNOLOGY ENGINEERING
DOCUMENT CENTRE ☎ X4962

Compiled by

[signature]

M. Mammen
Senior Engineer

Date: 5/8/2013

Functional Responsibility

[signature]
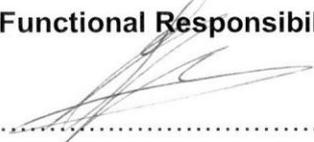
S. Papadopoulos
Control and Automation
Technology & Support Manager

Date: 7/8/2013

**Authorised by**

[signature]
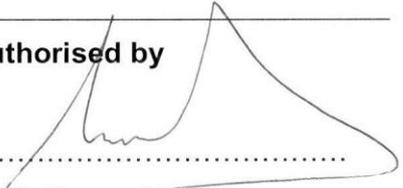
R. McCurrach
Senior Manager: PTMC
Engineering

Date: 7/8/2013

Approved by
(SCOT TC Chairperson)

[signature]
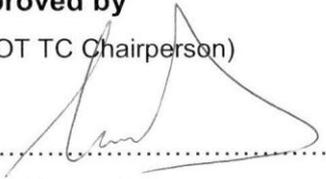
R. McCurrach

Chairperson PTM&C
Technical Committee

Date: 7/8/2013

CONTENTS

Page

FIGURES

TABLES

1. INTRODUCTION

The Goods Information describes the *Purchaser's* (Eskom Holdings SOC Limited) requirements in respect of switches and routers to be applied at various Transmission and Distribution substations.

2. SUPPORTING CLAUSES

2.1 SCOPE

2.1.1 Purpose

The purpose of this document is to provide the *Purchaser's* requirements for substation switches and routers. This document details the aspects of the switches and routers, which consist of the hardware, software and protocols. The invitation calls for the design, manufacture, testing, both at works and site, supply, delivery and possible installation of the routers and switches to be used at the *Purchaser's* substations. The *Supplier* shall be responsible for the tailoring and integration of the *Supplier's* standard switches and routers to meet the *Purchaser's* requirements. Any limitations that prevent the switches and routers from being configured with the different options shall be clearly stated. Furthermore the provision of training, spares, on-going support and the warranties for the entire switch and router, is required.

2.1.2 Applicability

This goods information shall apply throughout the *Purchaser's* substations for new switch and router installations and upgrading of existing systems.

2.2 NORMATIVE/INFORMATIVE REFERENCES

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

The following referenced documents provide the necessary detail to supplement this Goods Information, and should be read in conjunction with this document. In cases of conflict however, this Goods Information takes precedence.

The following standards contain provisions that, through reference in the text, constitute requirements of this Goods Information. At the time of publication the revisions indicated were valid. All standards are subject to review and parties to purchasing agreements, based on this goods information, are encouraged to investigate the possibility of applying the most recent revisions of the standards listed below. Information on currently valid national and international standards may be obtained from the Information Centre at Megawatt Park at cost only.

TESGL0020	Transmission Secondary Plant Technology Development
TTE41-1077	Substation Automation Network Architecture Standard
ISO 9001:2000	Quality Management Systems
EPL 240-55410927	Cyber Security Standard for operational technology
Standard NERC CIP–001–1 — Sabotage Reporting	
Standard NERC CIP–002–3 — Cyber Security — Critical Cyber Asset Identification	
Standard NERC CIP–003–3 — Cyber Security — Security Management Controls	
Standard NERC CIP–004–3 — Cyber Security — Personnel and Training	

Standard NERC CIP–005–3 — Cyber Security — Electronic Security Perimeter(s)

Standard NERC CIP-006-3c — Cyber Security — Physical Security

Standard NERC CIP–007–3 — Cyber Security — Systems Security Management

Standard NERC CIP–008–3 — Cyber Security — Incident Reporting and Response Planning

Standard NERC CIP–009–3 — Cyber Security — Recovery Plans For Critical Cyber Assets

IEC 61850 Ed 1, Parts 1-14, Standard for Communication networks and systems in substations

IEC 60870-2-1:1995, Telecontrol equipment and systems Part 2: Operating conditions - Section 1: Power supply and electromagnetic compatibility

IEC 60870-2-2:1996, Telecontrol equipment and systems Part 2: Operating conditions - Section 2: Environmental conditions (climatic, mechanical and other non-electrical influences)

IEC TS 61000-6-5:2001, Electromagnetic compatibility (EMC) Part 6-5: Generic standards. Immunity for power station and substation environments

IEEE 1613-2009, IEEE Standard for environmental and testing requirements for communications networking devices installed in electric power substations.

IEEE 802-2001, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture

IEEE 802.1AX-2008, IEEE Standard for Local and Metropolitan Area Networks – Link Aggregation

IEEE 802.1D-2004, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges

IEEE 802.1Q-2011, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks

IEEE 802.1X-2010, IEEE Standard for Local and Metropolitan Area Networks: Port-based Network Access Control

IEEE 802.3-2008, IEEE Standard for Information Technology – Telecommunication and Information Exchange between Systems - Local and Metropolitan Area Networks

IEEE C37.238-2011, IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications

2.2.2 Informative

Not Applicable.

2.3 DEFINITIONS

Term	Definition
Substation Automation	A system for managing, controlling and protecting a power system using real-time system data, local and remote control and advanced electrical protection. Core components are local intelligence, data communication and supervisory control and monitoring.
Network Topology	The arrangement of systems on a computer network that defines how the computers, or nodes, within the network are arranged and connected to each other. Some common network topologies include star, ring, line, bus, and tree configurations.

Term	Definition
Bay Level	A bay is a part of a substation containing switchgear and control devices designed for an electrical supply line, transformer, etc. connected to busbar of the substation. These parts of a substation may be managed by devices with the generic name "bay controller" and have protection systems called "bay protection". The bay level represents an additional control level below the overall station level.
Station Level	The station level aggregates the control systems and protection systems that are contained at bay level and includes those systems that are not attributable to a bay.
Gateway	A device that converts one protocol or format to another. In the substation context, a gateway is defined as an application gateway that converts commands and/or data from one format to another.
Head-of-Line (HOL) blocking	HOL blocking occurs when the packet at the head of a queue cannot be transmitted to an output due to a contending packet from another input. At the same time, a packet further back in the queue is blocked although its destination port is free to receive the packet.
RMON	Remote Network Monitoring is a standard monitoring specification that supports monitoring and protocol analysis. It enables various network monitors and console systems to exchange network-monitoring data.
CoS	Class of Service is a 3-bit field that is present in an Ethernet frame header when 802.1Q VLAN tagging is present. The field specifies a priority value between 0 and 7, which can be used by quality of service tools to differentiate, prioritise and shape network traffic. CoS operates only at the data link layer.
GOOSE	Generic Object Oriented Substation Events is a control mechanism for sending event data over a network.
Serial Port Server	A network device containing RS-232 and RS485 ports with the ability to encapsulate serial data into an Ethernet connection. Each serial port typically has a single IP socket mapped to a serial port.
"shall"	Requirements that are defined by the word "shall" must be considered as definite requirements or constraints on the proposal.

2.3.1 Classification

Controlled Disclosure: Controlled Disclosure to external parties (either enforced by law, or discretionary).

2.4 ABBREVIATIONS

Abbreviation	Description
3DES	Triple Data Encryption Algorithm
AAA	Authentication, Authorization and Accounting protocol
ASCII	American Standard Code for Information Interchange
AES	Advanced Encryption Standard
BCU	Bay Controller *or* Bay Control Unit

Abbreviation	Description
BGP	Border Gateway Protocol
BME	Bandwidth Management Equipment
BPDU	Bridge Protocol Data Unit
Cat5e	Category 5E UTP or STP cable
Cat6	Category 6 UTP or STP cable
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CoS	Class of Service
DC	Direct Current
DCE	Data Circuit-terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DTP	Dynamic Trunking Protocol
EMI	Electro Magnetic Interference
eRSTP	Enhanced Rapid Spanning Tree Protocol
FAT	Factory Acceptance Test
FLD	Fast Link Detections
FOBOT	Fibre Optic Break-Out Tray
GARP	Generic Attribute Registration Protocol
GBIC	GigaBit Interface Converter
GMRP	GARP Multicast Registration Protocol
GOOSE	Generic Object Oriented Substation Events
GPS	Global Positioning System
GVRP	GARP Virtual Local Area Network Registration Protocol
HDLC	High-level Data Link Control
HMI	Human Machine Interface
HOL	Head-of-Line blocking
HTTP	HyperText Transfer Protocol
I/O	Input Output
IDS/ IPS	Intrusion Detection and Prevention System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol

Abbreviation	Description
IP	Internet Protocol
IPAM	IP Address Management
IPsec	Internet Protocol Security
IRB	Integrated Routing and Bridging
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
LAN	Local Area Network
LC	Lucent Connector
LFI	Link Fault Indication
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control Address
MMRP	Multiple MAC Registration Protocol
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failure
MVRP	Multiple VLAN Registration Protocol
NAT	Network Address Translation
NERC CIP	North American Electric Reliability Corporation- Critical Infrastructure Protection
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PoE	Power over Ethernet
PSTN	Public Switched Telephone Network
PPP	Point-to-Point Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comments
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SAT	Site Acceptance Test
SC	Subscriber Connector *or* Standard Connector *or* Siemon Connector
SFP	Small Form-factor Gigabit Interface Converter
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOE	Standard Operating Environment / Sequence of Events

Abbreviation	Description
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Straight Tip / Bayonet Fibre Optic Connector
STP	Shielded Twisted Pair / Spanning Tree Protocol
TOS	Type of Service
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

2.5 ROLES AND RESPONSIBILITIES

Not Applicable.

2.6 PROCESS FOR MONITORING

Not Applicable.

2.7 RELATED/SUPPORTING DOCUMENTS

Not Applicable.

3. PROJECT PROGRAMME

The project shall be executed according to a defined project schedule made up of six phases. These phases are governed by the procedures defined under the "System Synthesis" and "Implementation" in TESGL0020 – Transmission Secondary Plant Technology Development.

The *Purchaser* reserves the right to eliminate one or more of the phases, prior to commencing each phase. The *Supplier* is required to provide a detailed work breakdown and the associated costs for the activities in each phase.

3.1 PHASE 1 - FUNCTIONAL DESIGN SPECIFICATION (FDS)

This phase consists of the production of a Functional Design Specification comprising a Functional Specification document and a System Design Report. The intention of this phase is to finalise all requirements and subsequently document the proposed design to form the baseline for the following phases.

The deliverables for this phase included the following:
• A Functional Specification.
• A Systems Design Report.
• Updated Project Programme

3.2 PHASE 2 - DETAILED DESIGN SPECIFICATION (DDS)

This phase consists of the production of a Detailed Design Specification for both hardware and software components of the system and specifies the procedures for testing.

The format of the test descriptions shall be as follows:
• Test Name
• Test Objectives
• Test Description
• Test Procedure with description on all test equipment/simulators to be used
• Expected Test Results

The deliverables for this phase shall be:
• Detailed Design Specification (if applicable);
• FAT Procedure document;
• SAT Procedure document.

The above deliverables shall be individually approved by the *Purchaser* prior to the commencement of Phase 3.

3.3 PHASE 3 - DEVELOPMENT, SYSTEM INTEGRATION AND FACTORY ACCEPTANCE TEST (FAT)

Phase 3 shall commence on completion of Phase 2.
This phase consists of the procurement of hardware required for testing, any required development and supply of software, training of the *Purchaser's* personnel, database population and system integration which is to be followed by formal testing of the system at the *Supplier's* premises, in the presence of the *Purchaser's* personnel.

The deliverable for this phase shall be:
• A signed-off FAT report indicating accepted completion of FAT.

3.4 PHASE 4 - DELIVERY, INSTALLATION, TESTING AND COMMISSIONING

Phase 4 shall commence on completion of Phase 3.
This phase comprises the delivery of hardware, software, documentation and manuals to site, installation in conjunction with the *Purchaser's* personnel and training. Thereafter, the system shall be commissioned in accordance with operating constraints of the power system.

The deliverables for this phase shall be:
• Equipment delivery and installation
• System documentation in triplicate hardcopy and electronic format
• Implementation Report; to be approved by the *Purchaser*
• Commissioned system

3.5 PHASE 5 - SITE ACCEPTANCE TEST (SAT)

The commencement of this phase shall be no later than 1 month after completion of Phase 4.
This phase consists of conducting tests according to the SAT procedure document.

The deliverables for this phase shall be:
• A signed-off SAT report indicating accepted completion of SAT.
• A hand-over Certificate.
• Source code for all software delivered.

3.6 PHASE 6 - ESTABLISHMENT OF SUPPLY CONTRACT

On successful completion and approval of the FAT and SAT on the prototype, by the *Purchaser*, the final phase of this project shall commence.

This phase of the project shall involve the subsequent supply of equipment for purchase and may include the manufacture, delivery, offloading, installation and erection of the purchased equipment.

Provision of training, spares, and on-going support for the product shall also be included in this phase.

4. ARCHITECTURE OVERVIEW

The architecture used is primarily based on a two-tier design. The top tier consists of high capacity; high speed backbone Ethernet switches which provide the physical connectivity only to the lower tier switches. The lower tier switches provide physical connectivity to the bay IEDs, the Gateway(s), HMI(s), router and other equipment. In order to meet high system availability criteria, each lower tier switch connects redundantly to two backbone switches, as shown in Figure 1.

However, for smaller, lower voltage substations, where the above mentioned topology, might not be feasible or practical, other topologies like ring, star and meshed shall be supported.
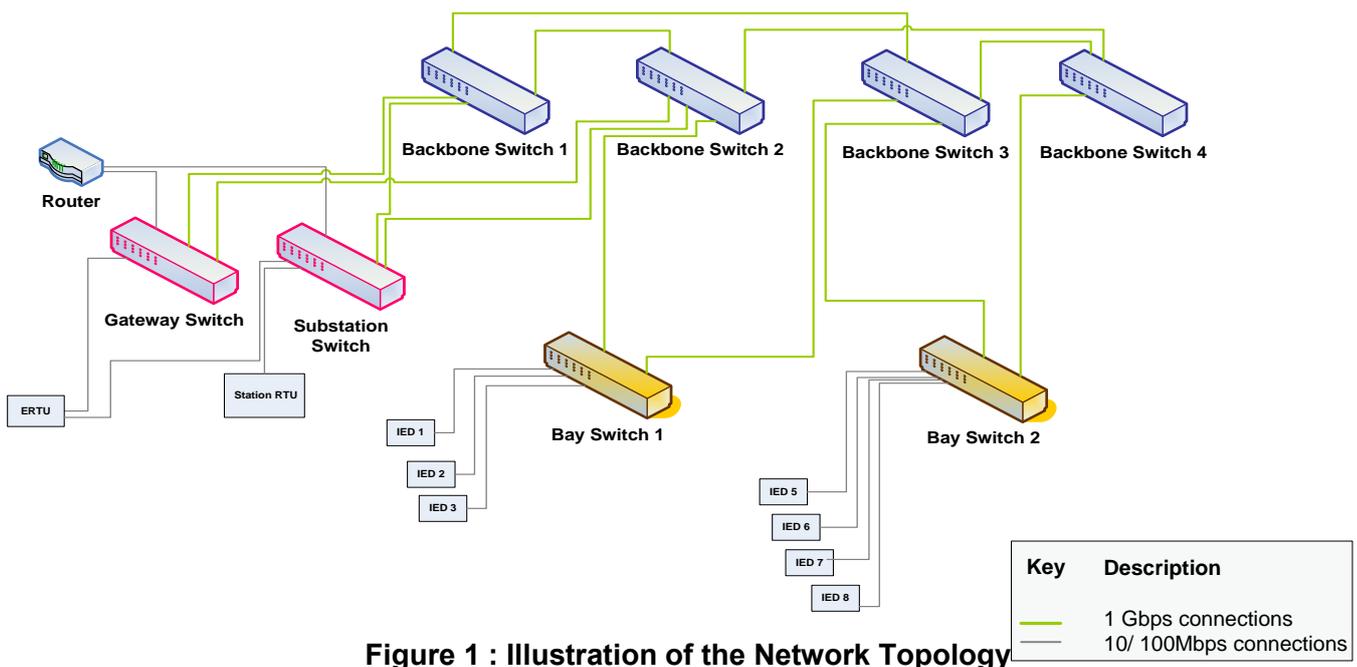
Figure 1 : Illustration of the Network Topology

5. PHILOSOPHY

The design philosophy is that:

- **Proposals shall comprise of the *Supplier's* standard hardware and software with special developments being kept to a minimum and only applying when specifically agreed to and requested by the *Purchaser*.** Such special developments shall be clearly identified and documented as to their nature and depth.

- Essential features of the offered device/s are interoperability with other vendor devices, scalability, modularity, and upgradeability to cater for evolving power system requirements.

6. DESIGN REQUIREMENTS

The *Purchaser's* requirements have been split into the following subsections:
- Gigabit switch requirements;
- Layer 2 switch requirements;
- Router requirements;
- Layer 3 switch requirements;
- Serial Port Server requirements; and
- General requirements.

The sections which follow contain details of each of these.

7. GIGABIT SWITCH REQUIREMENTS

The Gigabit Switch shall perform the function of a backbone switch. Each bay switch shall have dual links to backbone switches, for redundancy. Listed below are the requirements for the Gigabit switch.

7.1 ENVIRONMENTAL, ELECTRICAL AND MECHANICAL REQUIREMENTS

The device shall be substation hardened or ruggedized to be able to withstand the following, without the performance being out of limits, reliability being compromised or the life cycle being shortened.

7.1.1 Environmental

The device shall:

7.1.1.1 Comply with Class C3, as per IEC 60870-2 part 1, Table 1; except for temperature.

7.1.1.2 Operate within a temperature range of -40°C to 85°C, with passive cooling.

7.1.2 Altitude

The device shall operate within an altitude range between 0 – 2500m.

7.1.3 EMI Immunity

The device shall provide error-free operation when exposed to EMI stress and electrical surges, as per Class 2 requirements of IEEE 1613.

7.1.4 Electrical

The device shall:

7.1.4.1 Operate within an electrical interference environment, where equipment is sited within high voltage switching compounds (132 kV or above) such that it is subject to high levels of radiated electrical interference, due to its physical placement or its direct connection to electrical plant.

7.1.4.2 Not be affected by other device frequencies.

7.1.4.3   Not generate any interference, which could hinder its own performance or the performance of the other equipment in its vicinity.

7.1.5   Power Supply

7.1.5.1   The power supply voltages shall be selectable.

7.1.5.2   The voltage options shall be: 48, 110 and 220 volts D.C.

7.1.5.3   The voltage tolerances shall be as per Table 1.

Nominal supply voltage	48 V	110 V	220 V
Normal supply voltage	52,8 V	117 V	234 V
Equipment terminal voltage limits	43 V to 55 V	88 V to 132 V	176 V to 264 V
Connection to earth	Note 1	Note 1	Note 1
NOTE 1: Fully floating supply symmetrically balanced about earth with earth fault detection set to detect 10 mA current from either pole to earth. For the 48 V telecommunications supply, the positive is earthed.			

Table 1: DC supply tolerances

7.1.5.4   Dual, redundant power supplies shall be provided with separate inputs per power supply to be able to draw from separate power sources.

7.1.5.5   The option for a hot swappable power supply is preferred. The *Supplier* shall indicate if available.

7.1.5.6   The power supply connectors shall be pluggable terminal block or screw terminal block.

7.1.6   Mechanical Shock and Vibration

The device shall comply with Class Bm, as per IEC 60870-2 part 1, section 4.2.2.

7.2   HARDWARE

7.2.1   Switching Fabric

7.2.1.1   The switching fabric bandwidth shall be at least twice the total capacity of connecting modules. i.e. the bandwidth shall be double the port rate.

7.2.1.2   The switch shall not allow head of line blocking.

7.2.1.3   The switch shall utilise the store and forward method for switching.

7.2.1.4   The switching latency shall be indicated.

7.2.2 Fibre Ports

The gigabit fibre ports shall:

7.2.2.1   Support multimode communication (1000BaseSx) with a wavelength of 850nm.

7.2.2.2   Support singlemode communication (1000BaseLx) with a wavelength of 1310nm.

7.2.2.3   Support LC connectors.

7.2.2.4   Be modular to allow for future expansion or repairs.

7.2.2.5   Support at minimum of 8 Ethernet gigabit ports.

7.2.3 General

7.2.3.1   The device shall be made of heavy duty steel and supplied with the option to mount on a standard 19" rack panel or a DIN rail, with all associated accessories.

7.2.3.2   The device shall have terminal blocks for power and I/O connections that are rated for industrial applications.

7.2.3.3   There shall be an option to add a protective coating on the circuit board, to protect against dust and moisture.

7.2.3.4   There shall be a dedicated RS232 port for switch management.

7.2.3.5   There shall be an option to use appropriate utility grade Small Form-factor Pluggable (SFP) modules, if and when required.

7.3   REQUIRED FUNCTIONALITY

7.3.1   Virtual Local Area Networks (VLANs)

The device shall:

7.3.1.1   Support as a minimum 30 VLANs.

7.3.1.2   Comply with IEEE 802.1Q-2011.

7.3.1.3   Support the double-tagging of an Ethernet frame/QinQ functionality [refer to IEEE 802.1D-2004].

7.3.1.4   Support the Multiple VLAN Registration Protocol (MVRP) for automatically propagating VLAN information across a network.

7.3.1.5   Support VLAN assignment per port, for untagged traffic.

7.3.2   Spanning Tree Protocol

The device shall:

7.3.2.1   Be able to "heal" the network with a speed of less than 5ms per hop

7.3.2.2   Support mesh topologies of up to 80 devices.

7.3.2.3   Support the Rapid Spanning Tree Protocol (RSTP) [refer to IEEE 802.1D-2004].

7.3.2.4   Support the Multiple Spanning Tree Protocol (MSTP) [refer to IEEE 802.1Q-2011].

7.3.3   Link Aggregation

The device shall:

7.3.3.1   Allow the linking of Ethernet ports into one logical trunk for higher bandwidths.

7.3.3.2   Comply with IEEE 802.1AX-2008.

7.3.4   Traffic Prioritisation

The device shall:

7.3.4.1   Allow for the classification of priorities based on the MAC address, ports, tags and IP Type of Service (TOS).

7.3.4.2   Allow time critical data to be classified as higher priority.

7.3.4.3   Support numerous priority queues for TOS.

7.3.4.4   Comply with the QoS Prioritisation schemes in the IEEE 802.1Q-2011.

7.3.5   Port Configuration

The device shall:

7.3.5.1   Allow for automatic configuration of ports.

7.3.5.2   Allow for automatic crossover detection.

7.3.5.3   Allow for manual configuration of media type state, speed and duplex state.

7.3.5.4   Have the capability to disable ports that are not being used.

7.3.5.5   Allow a port to be configured to a specific VLAN.

7.3.5.6   Be capable of limiting which VLANs are accessible through a trunk port.

7.3.5.7   Allow limiting the number of MAC addresses per port.

7.3.5.8   Allow limiting the number of VLANs per port.

7.3.6   Port Rate Limiting

The device shall:

7.3.6.1   Have the ability to limit traffic on a per-port basis.

7.3.6.2   Allow the choice between Broadcast; Multicast; or Unicast limiting, which is essential for managing network traffic.

7.3.7   Port Based Access Control

The device shall:

7.3.7.1   Provide a means for authenticating and authorising devices attached to the Ethernet ports.

7.3.7.2   Comply with IEEE 802.1x-2010.

7.3.8   Port Mirroring

The device shall support port mirroring that is essential for network monitoring and troubleshooting on live networks.

7.3.9   Time Synchronization

7.3.9.1   The device shall support the Simple Network Time Protocol (SNTP) that is to be used to synchronise the internal system clocks of devices on the network allowing for correct correlation of time stamped events for troubleshooting.

7.3.9.2   The device shall support SNTP client or NTP client.

7.3.9.3   The Supplier shall indicate whether or not the device can support IEEE 1588 version 2 and IEEE C37.238-2011.

7.3.9.4   The *Supplier* shall indicate whether or not the device can function as a NTP server or client.

7.3.10   Other Requirements

The device shall:

7.3.10.1   Provide a Link Fault Indication (LFI) under all failure conditions, to allow devices at the far end of a fibre connection to detect a link failure.

7.3.10.2   Allow for Fast Link Detections (FLD) for quicker discovery of new devices or links in the network.

7.3.10.3   Allow FLD to be automatically turned off, as a failsafe, in the case of a large number of link state changes propagating across the network.

7.3.10.4   Be able to auto-sense the IP version.

7.3.10.5   Support the Link Layer Discovery Protocol (LLDP) [refer IEEE 802.1AB-2009].

7.3.10.6   Support the Internet Group Management Protocol (IGMP) version 3 [refer to RFC 4604] that is used in managing the membership of multicast groups.

7.3.10.7   Be able to perform IGMP snooping.

7.3.10.8   Support the Multiple MAC Registration Protocol (MMRP) that allows multicast traffic in bridged LANs to be confined to areas of the network where it is required. [refer to IEEE 802.1Q-2011]

7.3.10.9   Be able to filter broadcast frames, within user defined thresholds, to prevent broadcast storms.

7.3.10.10 Support Multi-level user password to protect the switch from unauthorised persons.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

7.3.10.11 Allow for logs to be sent to a syslog server.

7.3.11 Switch Security

7.3.11.1 The switch shall comply with North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) security standards, policy 001 - 009, where applicable.

7.3.11.2 The switch shall comply with the Cyber Security Standard for Operational Technology, EST 240 - 55410927.

7.3.11.3 The device shall support Remote Authentication Dial In User Service (RADIUS).

7.3.11.4 The device shall be able to authenticate to AAA (Authentication, Authorization and Accounting) via a RADIUS server.

7.3.11.5 The device shall comply with IEEE 802.1X-2010, port-based network access control.

7.3.11.6 The device shall support multiple levels of privileges per user.

7.3.11.7 All encryption on the device shall be 128 bit AES or better.

7.3.12 Management Tools

7.3.12.1 The switch's management shall be accessible via a web browser that supports HTTPS or via a serial connection.

7.3.12.2 Different web browsers shall be supported i.e. Firefox web browser on Linux or Internet Explorer on Windows.

7.3.12.3 The management Command Line Interface (CLI) shall be accessible via Secure Shell (SSH).

7.3.12.4 The device shall allow remote access for configuration purposes via a physically separated management port.

7.3.12.5 The device shall support the Simple Network Management Protocol (SNMP) version 1, version 2c and version 3.

7.3.12.6 The device shall support the Remote Network Monitoring (RMON) for event logging, viewing of device statistics, proactive monitoring, problem detection and reporting.

8. LAYER 2 SWITCH REQUIRMENTS

The Layer 2 Switch shall perform the function of a bay switch, providing physical connectivity to the bay IEDs, the Gateway(s), HMI(s), router and other equipment. Each bay switch shall also have dual links to backbone switches. Listed below are the requirements for the Layer 2 switch. Two different options are required in this section: a small switch with 4-16 Ethernet ports; and a large switch with 16-32 Ethernet ports.

8.1 ENVIRONMENTAL, ELECTRICAL AND MECHANICAL REQUIREMENTS

The device shall be substation hardened or ruggedized to be able to withstand the following, without the performance being out of limits, reliability being compromised or the life cycle being shortened.

8.1.1 Environmental

The device shall:

8.1.1.1   Comply with Class C3, as per IEC 60870-2 part 1, Table 1; except for temperature.

8.1.1.2   Operate within a temperature range of -40°C to 85°C, with passive cooling.

8.1.2 Altitude

The device shall operate within an altitude range between 0 – 2500m.

8.1.3 EMI Immunity

The device shall provide error-free operation when exposed to EMI stress and electrical surges, as per Class 2 requirements of IEEE 1613.

8.1.4 Electrical

The device shall:

8.1.4.1   Operate within an electrical interference environment, where equipment is sited within high voltage switching compounds (132 kV or above) such that it is subject to high levels of radiated electrical interference, due to its physical placement or its direct connection to electrical plant.

8.1.4.2   Not be affected by other device frequencies.

8.1.4.3   Not generate any interference, which could hinder its own performance or the performance of the other equipment in its vicinity.

8.1.5 Power Supply

8.1.5.1   The power supply voltages shall be selectable.

8.1.5.2   The voltage options shall be: 48, 110 and 220 volts D.C.

8.1.5.3   The voltage tolerances shall be as per Table 1.

8.1.5.4   Dual, redundant power supplies shall be provided with separate inputs per power supply to be able to draw from separate power sources.

8.1.5.5   The option for a hot swappable power supply is preferred. The *Supplier* shall indicate if available.

8.1.5.6   The power supply connectors shall be pluggable terminal block or screw terminal block.

8.1.6 Mechanical Shock and Vibration

The device shall comply with Class Bm, as per IEC 60870-2 part 1, section 4.2.2.

8.2   HARDWARE

8.2.1   Switching Fabric

8.2.1.1   The switching fabric bandwidth shall be at least twice the total capacity of connecting modules. i.e. the bandwidth shall be double the port rate.

8.2.1.2   The switch shall not allow head of line blocking.

8.2.1.3   The switch shall utilise the store and forward method for switching.

8.2.1.4   The switching latency shall be indicated.

8.2.2   Gigabit Fibre Ports

The Gigabit fibre ports shall be used to link to the backbone switches. The Gigabit fibre ports shall:

8.2.2.1   Support multimode communication (1000BaseSx) with a wavelength of 850nm.

8.2.2.2   Support singlemode communication (1000BaseLx) with a wavelength of 1310nm.

8.2.2.3   Support LC connectors.

8.2.2.4   Be modular to allow for future expansion or repairs.

8.2.2.5   Support as a minimum 2 Ethernet gigabit ports on separate modules for the large switch option.

8.2.3   10Base and 100Base Ethernet Ports

The Ethernet ports shall be a combination of numerous copper and or fibre ports, based on the requirements of the connecting bay devices.

8.2.3.1   The fibre ports shall:

8.2.3.1.1   Support multimode communication (10BaseFL) with a wavelength of 850nm.

8.2.3.1.2   Support multimode communication (100BaseFx) with a wavelength of 1300nm.

8.2.3.1.3   Support LC, ST and SC connectors.

8.2.3.2   The copper ports shall:

8.2.3.2.1   Support both 10BaseTx and 100BaseTx.

8.2.3.2.2   Support RJ45 connectors.

8.2.3.3   Ethernet ports shall be modular to allow for future expansion or repairs.

8.2.3.4   The large device option shall support as a minimum a total of 16 Ethernet ports that caters for all combinations of 10/100Base modules.

The combination of 10Base and 100Base Ethernet ports shall range from no 10Base and thirty-two100Base Ethernet ports to thirty-two 10Base and no 100Base Ethernet ports.

8.2.3.5   The small device option shall support as a minimum a total of 8 Ethernet ports and as a maximum have 16 Ethernet ports. The device shall cater for all combinations of 10/100Base modules.

8.2.4   General

8.2.4.1   The device shall be made of heavy duty steel and supplied with the option to mount on a standard 19" rack panel or a DIN rail, with all associated accessories.

8.2.4.2   The device shall have terminal blocks for power and I/O connections that are rated for industrial applications.

8.2.4.3   There shall be an option to add a protective coating on the circuit board, to protect against dust and moisture.

8.2.4.4   There shall be a dedicated RS232 port for switch management.

8.2.4.5   There shall be an option to use appropriate utility grade Small Form-factor Pluggable (SFP) modules, if and when required.

8.3   REQUIRED FUNCTIONALITY

8.3.1   Virtual Local Area Networks (VLANs)

The device shall:

8.3.1.1   Support as a minimum 30 VLANs.

8.3.1.2   Comply with IEEE 802.1Q-2011.

8.3.1.3   Support the double-tagging of an Ethernet frame/QinQ functionality [refer to IEEE 802.1Q-2011].

8.3.1.4   Support the Multiple VLAN Registration Protocol (MVRP) for automatically propagating VLAN information across a network.

8.3.1.5   Support VLAN assignment per port, for untagged traffic.

8.3.2   Spanning Tree Protocol

The device shall:

8.3.2.1   Be able to "heal" the network with a speed of less than 5ms per hop

8.3.2.2   Support mesh topologies of up to 80 devices.

8.3.2.3   Support the Rapid Spanning Tree Protocol (RSTP) [refer to IEEE 802.1D-2004].

8.3.2.4   Support the Multiple Spanning Tree Protocol (MSTP) [refer to IEEE 802.1Q-2011].

8.3.3   Link Aggregation

The device shall:

8.3.3.1   Allow the linking of Ethernet ports into one logical trunk for higher bandwidths.

8.3.3.2   Comply with IEEE 802.1AX-2008.

8.3.4   Traffic Prioritisation

The device shall:

8.3.4.1   Allow for the classification of priorities based on the MAC address, ports, tags and IP Type of Service (TOS).

8.3.4.2   Allow time critical data to be classified as higher priority.

8.3.4.3   Support numerous priority queues for TOS.

8.3.4.4   Comply to the QoS Prioritisation schemes in the IEEE 802.1Q-2011.

8.3.5   Port Configuration

The device shall:

8.3.5.1   Allow for automatic configuration of ports.

8.3.5.2   Allow for automatic crossover detection.

8.3.5.3   Allow for manual configuration of media type state, speed and duplex state.

8.3.5.4   Have the capability to disable ports that are not being used.

8.3.5.5   Allow a port to be configured to a specific VLAN.

8.3.5.6   Be capable of limiting which VLANs are accessible through a trunk port.

8.3.5.7   Allow limiting the number of MAC addresses per port.

8.3.5.8   Allow limiting the number of VLANs per port.

8.3.6   Port Rate Limiting

The device shall:

8.3.6.1   Have the ability to limit traffic on a per-port basis.

8.3.6.2   Allow the choice between Broadcast; Multicast; or Unicast limiting, which is essential for managing network traffic.

8.3.7   Port Based Access Control

The device shall:

8.3.7.1   Provide a means for authenticating and authorising devices attached to the Ethernet ports.

8.3.7.2   Comply with IEEE 802.1X-2010.

8.3.8   Port Mirroring

The device shall support port mirroring that is essential for network monitoring and troubleshooting on live networks.

8.3.9 Time Synchronization

8.3.9.1 The device shall support the Simple Network Time Protocol (SNTP) that is to be used to synchronise the internal system clocks of devices on the network allowing for correct correlation of time stamped events for troubleshooting.

8.3.9.2 The *Supplier* shall indicate whether or not the device can support IEEE 1588 version 2 and IEEE C37.238-2011.

8.3.9.3 The *Supplier* shall indicate whether or not the device can function as a NTP server or client.

8.3.10 Other Requirements

The device shall:

8.3.10.1 Provide a Link Fault Indication (LFI) under all failure conditions, to allow devices at the far end of a fibre connection to detect a link failure.

8.3.10.2 Allow for Fast Link Detections (FLD) for quicker discovery of new devices or links in the network.

8.3.10.3 Allow FLD to be automatically turned off, as a failsafe, in the case of a large number of link state changes propagating across the network.

8.3.10.4 Be able to auto-sense the IP version.

8.3.10.5 Be able to perform auto-negotiation and automatic crossover detection.

8.3.10.6 Support the Link Layer Discovery Protocol (LLDP) [refer to IEEE 802.1AB-2009].

8.3.10.7 Support the Internet Group Management Protocol (IGMP) version 3 [refer to RFC 4604] that is used in managing the membership of multicast groups.

8.3.10.8 Be able to perform IGMP snooping.

8.3.10.9 Support the Multiple MAC Registration Protocol (MMRP) that allows multicast traffic in bridged LANs to be confined to areas of the network where it is required. [refer to IEEE 802.1Q-2011]

8.3.10.10 Support Multi-level user password to protect the switch from unauthorised persons.

8.3.10.11 Allow for logs to be sent to a syslog server.

8.3.11 Switch Security

8.3.11.1 The switch shall comply with North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) security standards, policy 001 - 009, where applicable.

8.3.11.2 The switch shall comply with the Cyber Security Standard for Operational Technology, EST 240 - 55410927.

8.3.11.3 The device shall support Remote Authentication Dial In User Service (RADIUS).

8.3.11.4 The device shall be able to authenticate to AAA (Authentication, Authorization and Accounting) via a RADIUS server.

8.3.11.5   The device shall comply with IEEE 802.1X-2010, port-based network access control.

8.3.11.6   The device shall support multiple levels of privileges per user.

8.3.11.7   All encryption on the device shall be 128 bit AES or better.

8.3.12   Management Tools

8.3.12.1   The switch's management shall be accessible via a web browser that supports HTTPS or via a serial connection.

8.3.12.2   Different web browsers shall be supported i.e. Firefox web browser on Linux or Internet Explorer on Windows.

8.3.12.3   The management Command Line Interface (CLI) shall be accessible via Secure Shell (SSH).

8.3.12.4   The device shall allow remote access for configuration purposes via a physically separated management port.

8.3.12.5   The device shall support the Simple Network Management Protocol (SNMP) version 1, version 2c and version 3.

8.3.12.6   The device shall support the Remote Network Monitoring (RMON) for event logging, viewing of device statistics, proactive monitoring, problem detection and reporting.

9. ROUTER REQUIREMENTS

The router shall be the single point of entry into the substation LAN. It shall physically be connected to two WAN links. On the LAN side the router shall be physically connected to the Gateway and Substation switches. In addition to routing, the router shall also be able to function as a firewall, Intrusion Detection Service (IDS), NTP server; DHCP server; VPN server and client; and a RADIUS server or client. Listed below are the requirements for the router.

9.1 ENVIRONMENTAL, ELECTRICAL AND MECHANICAL REQUIREMENTS

The device shall be substation hardened or ruggedized to be able to withstand the following, without the performance being out of limits, reliability being compromised or the life cycle being shortened.

9.1.1 Environmental

The device shall:

9.1.1.1   Comply with Class C3, as per IEC 60870-2 part 1, Table 1; except for temperature.

9.1.1.2   Operate within a temperature range of -40°C to 85°C, with passive cooling.

9.1.2   Altitude

The device shall operate within an altitude range between 0 – 2500m.

9.1.3   EMI Immunity

The device shall provide error-free operation when exposed to EMI stress and electrical surges, as per

Class 2 requirements of IEEE 1613.

9.1.4   Electrical

The device shall:

9.1.4.1   Operate within an electrical interference environment, where equipment is sited within high voltage switching compounds (132 kV or above) such that it is subject to high levels of radiated electrical interference, due to its physical placement or its direct connection to electrical plant.

9.1.4.2   Not be affected by other device frequencies.

9.1.4.3   Not generate any interference, which could hinder its own performance or the performance of the other equipment in its vicinity.

9.1.5   Power Supply

9.1.5.1   The power supply voltages shall be selectable.

9.1.5.2   The voltage options shall be: 48, 110 and 220 volts D.C.

9.1.5.3   The voltage tolerances shall be as per Table 1.

9.1.5.4   Dual, redundant power supplies shall be provided with separate inputs per power supply to be able to draw from separate power sources.

9.1.5.5   The option for a hot swappable power supply is preferred. The *Supplier* shall indicate if available.

9.1.5.6   The power supply connectors shall be pluggable terminal block or screw terminal block.

9.1.6   Mechanical Shock and Vibration

The device shall comply with Class Bm, as per IEC 60870-2 part 1, section 4.2.2.

9.2   HARDWARE

9.2.1   Router Fabric

9.2.1.1   The *Supplier* shall indicate the router's maximum throughput, for the following Ethernet frame sizes of 64 bytes; 512 bytes; and 1518 bytes, when all the Ethernet Ports are being utilised.

9.2.1.2   The router latency shall be indicated for frame sizes of 64 bytes; 512 bytes; and 1518 bytes.

9.2.2   Ethernet Ports

The Ethernet ports shall be a combination of copper and fibre ports. It will be used to link to the Gateway Switch and the Substation switch.

9.2.2.1   The fibre ports shall:

9.2.2.1.1   Support multimode communication (1000BaseSx) with a wavelength of 850nm.

9.2.2.1.2　Support singlemode communication (1000BaseLx) with a wavelength of 1310nm

9.2.2.1.3　Support multimode communication (100BaseFx) with a wavelength of 1300nm.

9.2.2.1.4　Support LC and ST connectors.

9.2.2.2　The copper ports shall:

9.2.2.2.1　Support 100BaseTx.

9.2.2.2.2　Support 1000BaseTx.

9.2.2.2.3　Support RJ45 connectors.

9.2.2.3　Ethernet ports shall be modular to allow for future expansion or repairs.

9.2.2.4　The device shall support as a minimum two 1000Base Ethernet ports and two 100Base Ethernet ports.

9.2.3　WAN Ports

The WAN ports shall be used to link to the BME or Telecoms router. This connection shall be X.21 or E1.

9.2.3.1　The router shall support Channelized- E1 connections.

9.2.3.2　The router shall support X.21 connections.

9.2.3.3　WAN ports shall be modular to allow for appropriate selection of WAN module, future expansion or repairs.

9.2.3.4　The device shall support as a minimum 2 WAN ports.

9.2.4　Serial Ports

The serial ports shall be used to link serial devices directly to the router. The serial ports shall:

9.2.4.1　Support RS232

9.2.4.2　Support RS422

9.2.4.3　Support RS485

9.2.4.4　Support RJ45 connectors.

9.2.4.5　Be modular to allow for appropriate module selection, future expansion or repairs.

9.2.4.6　Support as a minimum 2 serial ports.

9.2.5　General

9.2.5.1　The device shall be made of heavy duty steel and supplied with the option to mount on a standard 19" rack panel or a DIN rail, with all associated accessories.

9.2.5.2   The device shall have terminal blocks for power and I/O connections that are rated for industrial applications.

9.2.5.3   There shall be an option to add a protective coating on the circuit board, to protect against dust and moisture.

9.2.5.4   There shall be a dedicated RS232 port for router setup and management.

9.2.5.5   There shall be an option to use appropriate utility grade Small Form-factor Pluggable (SFP) modules, if and when required.

9.3   REQUIRED FUNCTIONALITY

9.3.1   Virtual Private Network (VPN)

The device shall:

9.3.1.1   Support both Layer 2 and Layer 3 VPN.

9.3.1.2   Support the following secure VPN protocols

9.3.1.2.1   Internet Protocol Security (IPsec)

9.3.1.2.2   Secure Socket Layer (SSL)

9.3.1.2.3   Transport Layer Security (TLS)

9.3.1.3   Support the following encryption methods:

9.3.1.3.1   Triple Data Encryption Algorithm (3DES)

9.3.1.3.2   128 bit Advanced Encryption Standard (AES128)

9.3.1.3.3   256 bit Advanced Encryption Standard (AES256)

9.3.1.4   Comply with IEEE 802.1Q-2011 and IEEE 802.1D-2004.

9.3.1.5   Support tunnels to be created to a host, a port on a host or to a whole site.

9.3.1.6   Support Generic Object Oriented Substation Events (GOOSE) tunnels to be created.

9.3.2   Virtual Local Area Networks (VLANs)

The device shall:

9.3.2.1   Support as a minimum 30 VLANs.

9.3.2.2   Comply with IEEE 802.1Q-2011.

9.3.2.3   Support the double-tagging of an Ethernet frame/QinQ functionality [refer to IEEE 802.1Q-2011].

9.3.2.4   Support the Multiple VLAN Registration Protocol (MVRP) for automatically propagating VLAN information across a network.

9.3.2.5   Support VLAN assignment per port, for untagged traffic.

9.3.3   Spanning Tree Protocol

The device shall:

9.3.3.1   Be able to "heal" the network with a speed of less than 5ms per hop

9.3.3.2   Support mesh topologies of up to 80 devices.

9.3.3.3   Support the Rapid Spanning Tree Protocol (RSTP) [refer to IEEE 802.1D-2004].

9.3.3.4   Support the Multiple Spanning Tree Protocol (MSTP) [refer to IEEE 802.1Q-2011].

9.3.4   Link Aggregation

The device shall:

9.3.4.1   Allow the linking of Ethernet ports into one logical trunk for higher bandwidths.

9.3.4.2   Comply with IEEE 802.1AX-2008.

9.3.5   Traffic Prioritisation

The device shall:

9.3.5.1   Allow for the classification of priorities based on the MAC address, type of protocol, ports, tags and Type of Service (TOS).

9.3.5.2   Allow time critical data to be classified as higher priority.

9.3.5.3   Support numerous priority queues for TOS.

9.3.5.4   Comply to the QoS Prioritisation schemes in the IEEE 802.1Q-2011.

9.3.6   Firewall

The device shall:

9.3.6.1   Support a firewall that allows stateful inspection.

9.3.6.2   Support Network Address Translation (NAT) as well as IP Address Masquerading.

9.3.6.3   Be able to perform port forwarding.

9.3.6.4   Be able to filter on source and destination address and ports.

9.3.7   Routing Protocols

The device shall:

9.3.7.1   Support Open Shortest Path First (OSPF) version 2, routing protocol.

9.3.7.2   Support Routing Information Protocol (RIP) and Border Gateway Protocol (BGP).

9.3.7.3   Support Virtual Router Redundancy Protocol (VRRP).

9.3.7.4   Support a Static Routing option.

9.3.7.5   Support Point-to-Point Protocol (PPP).

9.3.7.6   Support High-Level Data Link Control (HDLC).

9.3.7.7   Comply with IEEE 802.1AX-2008.

9.3.8   WAN Authentication protocols

The device shall support the Challenge Handshake Authentication Protocol (CHAP).

9.3.9   Port Configuration

The device shall:

9.3.9.1   Allow for automatic configuration of ports.

9.3.9.2   Allow for automatic crossover detection.

9.3.9.3   Allow for manual configuration of media type state, speed and duplex state.

9.3.9.4   Have the ability to disable ports that are not being used.

9.3.9.5   Allow a port to be configured to a specific VLAN.

9.3.9.6   Be capable of limiting which VLANs are accessible through a trunk port.

9.3.9.7   Allow limiting the number of MAC addresses per port.

9.3.9.8   Allow limiting the number of VLANs per port.

9.3.10   Port Rate Limiting

The device shall:

9.3.10.1   Have the ability to limit traffic on a per-port basis.

9.3.10.2   Allow the choice between Broadcast; Multicast; or Unicast limiting, which is essential for managing network traffic.

9.3.11   Port Based Access Control

The device shall:

9.3.11.1   Provide a means for authenticating and authorising devices attached to the Ethernet ports.

9.3.11.2   Comply with IEEE 802.1X-2010.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

9.3.12 Time Synchronization

9.3.12.1   The device shall support the Simple Network Time Protocol (SNTP) that is to be used to synchronise the internal system clocks of devices on the network allowing for correct correlation of time stamped events for troubleshooting.

9.3.12.2   The device shall be able to perform the function of a Network Time Protocol (NTP) server.

9.3.12.3   The device shall be able to perform the function of a Network Time Protocol (NTP) client.

9.3.12.4   The *Supplier* shall indicate whether or not the device can support IEEE 1588 version 2 and IEEE C37.238-2011.

9.3.12.5   The *Supplier* shall indicate whether an option for a GPS receiver exists.

9.3.13 Other Requirements

The device shall:

9.3.13.1   Be able to perform the function of a Dynamic Host Control Protocol (DHCP) server, with option 82 supported.

9.3.13.2   Allow for centralised password management by means of a RADIUS server.

9.3.13.3   Provide Intrusion Detection and Prevention System (IDS/IPS) services.

9.3.13.4   Support Integrated Routing and Bridging (IRB), which allows a protocol to be bridged as well as routed on the same interface on the router. This can be used to forward VLAN headers.

9.3.13.5   Allow for inter VLAN routing.

9.3.13.6   Allow for IP multicast routing.

9.3.13.7   Support serial IP encapsulation.

9.3.13.8   Provide a fault indication under all failure conditions.

9.3.13.9   Support the Link Layer Discovery Protocol (LLDP) [refer to IEEE 802.1AB-2009].

9.3.13.10 Support the Internet Group Management Protocol (IGMP) version 3 [refer to RFC 4604] that is used in managing the membership of multicast groups.

9.3.13.11 Support Multi-level user password to protect the router from unauthorised persons.

9.3.13.12 Allow for logs to be sent to a syslog server.

9.3.13.13 Allow for WAN and LAN Loopback and Loop-test functions.

9.3.14 Router Security

9.3.14.1   The switch shall comply with North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) security standards, policy 001 - 009, where applicable.

9.3.14.2   The switch shall comply with the Cyber Security Standard for Operational Technology, EST

240 - 55410927.

9.3.14.3   The device shall support Remote Authentication Dial In User Service (RADIUS).

9.3.14.4   The device shall be able to authenticate to AAA (Authentication, Authorization and Accounting) via a RADIUS server.

9.3.14.5   The device shall comply with IEEE 802.1X-2008, port-based network access control.

9.3.14.6   The device shall support multiple levels of privileges per user.

9.3.14.7   All encryption on the device shall be 128 bit AES or better.

9.3.15   Management Tools

9.3.15.1   The router's management shall be accessible via a web browser that supports HTTPS or via a serial connection.

9.3.15.2   Different web browsers shall be supported i.e. Firefox web browser on Linux or Internet Explorer on Windows.

9.3.15.3   The management Command Line Interface (CLI) shall be accessible via Secure Shell (SSH).

9.3.15.4   The device shall allow remote access for configuration purposes via a physically separated management port.

9.3.15.5   The device shall support the Simple Network Management Protocol (SNMP) version 1, version 2c and version 3.

10. LAYER 3 SWITCH REQUIREMENTS

The Layer 3 switch shall be used in cases where it is more practical to use a single device that combines the functionality of a traditional Layer 2 switch and a router. Listed below are the requirements for the Layer 3 switch.

10.1   ENVIRONMENTAL, ELECTRICAL AND MECHANICAL REQUIREMENTS

The device shall be substation hardened or ruggedized to be able to withstand the following, without the performance being out of limits, reliability being compromised or the life cycle being shortened.

10.1.1 Environmental

The device shall:

10.1.1.1   Comply with Class C3, as per IEC 60870-2 part 1, Table 1; except for temperature.

10.1.1.2   Operate within a temperature range of -40°C to 85°C, with passive cooling.

10.1.2   Altitude

The device shall operate within an altitude range between 0 – 2500m.

10.1.3 EMI Immunity

The device shall provide error-free operation when exposed to EMI stress and electrical surges, as per Class 2 requirements of IEEE 1613.

10.1.4 Electrical

The device shall:

10.1.4.1 Operate within an electrical interference environment, where equipment is sited within high voltage switching compounds (132 kV or above) such that it is subject to high levels of radiated electrical interference, due to its physical placement or its direct connection to electrical plant.

10.1.4.2 Not be affected by other device frequencies.

10.1.4.3 Not generate any interference, which could hinder its own performance or the performance of the other equipment in its vicinity.

10.1.5 Power Supply

10.1.5.1 The power supply voltages shall be selectable.

10.1.5.2 The voltage options shall be: 48, 110 and 220 volts D.C.

10.1.5.3 The voltage tolerances shall be as per Table 1.

10.1.5.4 Dual, redundant power supplies shall be provided with separate inputs per power supply to be able to draw from separate power sources.

10.1.5.5 The option for a hot swappable power supply is preferred. The *Supplier* shall indicate if available.

10.1.5.6 The power supply connectors shall be pluggable terminal block or screw terminal block.

10.1.6 Mechanical Shock and Vibration

The device shall comply with Class Bm, as per IEC 60870-2 part 1, section 4.2.2.

10.2 HARDWARE

10.2.1 Switching Fabric

10.2.1.1 The switching fabric bandwidth shall be at least twice the total capacity of connecting modules. i.e. the bandwidth shall be double the port rate.

10.2.1.2 The switch shall not allow head of line blocking.

10.2.1.3 The switch shall utilise the store and forward method for switching.

10.2.1.4 The switching latency shall be indicated.

10.2.2 Gigabit Fibre Ports

The Gigabit fibre ports shall be used to link to the backbone switches. The Gigabit fibre ports shall:

10.2.2.1 Support multimode communication (1000BaseSx) with a wavelength of 850nm.

10.2.2.2 Support singlemode communication (1000BaseLx) with a wavelength of 1310nm.

10.2.2.3 Support LC connectors.

10.2.2.4 Be modular to allow for future expansion or repairs.

10.2.2.5 Support as a minimum 2 Ethernet gigabit ports on separate modules.

10.2.3 Ethernet Ports

The Ethernet ports shall be a combination of numerous copper and or fibre ports, based on the requirements of the connecting bay devices.

10.2.3.1 The fibre ports shall:

10.2.3.1.1 Support multimode communication (10BaseFL) with a wavelength of 850nm.

10.2.3.1.2 Support multimode communication (100BaseFx) with a wavelength of 1300nm.

10.2.3.1.3 Support LC, ST and SC connectors.

10.2.3.2 The copper ports shall:

10.2.3.2.1 Support 10BaseTx

10.2.3.2.2 Support 100BaseTx

10.2.3.2.3 Support 1000BaseTx

10.2.3.2.4 Support RJ45 connectors.

10.2.3.3 Ethernet ports shall be modular to allow for future expansion or repairs.

10.2.3.4 The device shall support as a minimum a total of 16 Ethernet ports that caters for all combinations of 10/100Base modules, with the option to size the switch to a lower port count for smaller installations.

The combination of 10Base and 100Base Ethernet ports shall range from no 10Base and 16 100Base Ethernet ports combination to 16 10Base and no 100Base Ethernet ports.

10.2.4 WAN Ports

The WAN ports shall be used to link to the BME or Telecoms router. This connection shall be X.21 or E1.

10.2.4.1 The router shall support Channelized- E1 connections.

10.2.4.2 The router shall support X.21 connections.

10.2.4.3 WAN ports shall be modular to allow for appropriate selection of WAN module, future expansion or repairs.

10.2.4.4 The device shall support as a minimum 2 WAN ports.

10.2.5 Serial Ports

The serial ports shall be used to link serial devices directly to the switch. The serial ports shall:

10.2.5.1 Support RS232

10.2.5.2 Support RS422

10.2.5.3 Support RS485

10.2.5.4 Support RJ45 connectors.

10.2.5.5 Be modular to allow for appropriate module selection, future expansion or repairs.

10.2.5.6 Support as a minimum 2 serial ports.

10.2.6 General

10.2.6.1 The device shall be made of heavy duty steel and supplied with the option to mount on a standard 19" rack panel or a DIN rail, with all associated accessories.

10.2.6.2 The device shall have terminal blocks for power and I/O connections that are rated for industrial applications.

10.2.6.3 There shall be an option to add a protective coating on the circuit board, to protect against dust and moisture.

10.2.6.4 There shall be a dedicated RS232 port for switch setup and management.

10.2.6.5 There shall be an option to use appropriate utility grade Small Form-factor Pluggable (SFP) modules, if and when required.

10.3 REQUIRED FUNCTIONALITY

10.3.1 Virtual Local Area Networks (VLANs)

The device shall:

10.3.1.1 Support as a minimum 30 VLANs.

10.3.1.2 Comply with IEEE 802.1Q-2011.

10.3.1.3 Support the double-tagging of an Ethernet frame/QinQ functionality [refer to IEEE 802.1Q-2011].

10.3.1.4 Support the Multiple VLAN Registration Protocol (MVRP) for automatically propagating VLAN information across a network.

10.3.1.5 Provide the ability to logically segregate traffic between pre-defined ports on switches.

10.3.1.6 Support VLAN assignment per port, for untagged traffic.

10.3.2 Virtual Private Network (VPN)

The device shall:

10.3.2.1   Support both Layer 2 and Layer 3 VPN.

10.3.2.2   Support the following secure VPN protocols

10.3.2.2.1   Internet Protocol Security (IPsec)

10.3.2.2.2   Secure Socket Layer (SSL)

10.3.2.3   Support the following encryption methods:

10.3.2.3.1   Triple Data Encryption Algorithm (3DES)

10.3.2.3.2   128 bit Advanced Encryption Standard (AES128)

10.3.2.3.3   256 bit Advanced Encryption Standard (AES256)

10.3.2.4   Comply to IEEE 802.1Q-2011 and IEEE 802.1D-2004.

10.3.2.5   Support tunnels to be created to a host, a port on a host or to a whole site.

10.3.2.6   Support Generic Object Oriented Substation Events (GOOSE) tunnels to be created.

10.3.3   Spanning Tree Protocol

The device shall:

10.3.3.1   Be able to "heal" the network with a speed of less than 5ms per hop.

10.3.3.2   Support mesh topologies of up to 80 devices.

10.3.3.3   Support the Rapid Spanning Tree Protocol (RSTP) [refer to IEEE 802.1D-2004].

10.3.3.4   Support the Multiple Spanning Tree Protocol (MSTP) [refer to IEEE 802.1Q-2011].

10.3.4   Traffic Prioritisation

The device shall:

10.3.4.1   Allow for the classification of priorities based on the MAC address, type of protocol, ports, tags and Type of Service (TOS).

10.3.4.2   Allow time critical data to be classified as higher priority.

10.3.4.3   Support numerous priority queues for TOS.

10.3.4.4   Comply to the QoS Prioritisation schemes in the IEEE 802.1Q-2011.

10.3.5   Firewall

The device shall:

10.3.5.1   Support a firewall that allows stateful inspection.

10.3.5.2   Support Network Address Translation (NAT) as well as IP Address Masquerading.

10.3.5.3   Be able to perform port forwarding.

10.3.5.4   Be able to filter on source and destination address and ports.

10.3.6   Routing Protocols

The device shall:

10.3.6.1   Support Open Shortest Path First (OSPF) version 2, routing protocol

10.3.6.2   Support Routing Information Protocol (RIP) and Border Gateway Protocol (BGP).

10.3.6.3   Support Virtual Router Redundancy Protocol (VRRP).

10.3.6.4   Support a Static Routing option.

10.3.6.5   Support Point-to-Point Protocol (PPP).

10.3.6.6   Support High-Level Data Link Control (HDLC).

10.3.6.7   Comply with IEEE 802.1AX-2008.

10.3.7   WAN Authentication Protocols

The device shall support the Challenge Handshake Authentication Protocol (CHAP).

10.3.8   Port Configuration

The device shall:

10.3.8.1   Allow for automatic configuration of ports.

10.3.8.2   Allow for automatic crossover detection.

10.3.8.3   Allow for manual configuration of media type state, speed and duplex state.

10.3.8.4   Have the capability to disable ports that are not being used.

10.3.8.5   Allow a port to be configured to a specific VLAN.

10.3.8.6   Be capable of limiting which VLANs are accessible through a trunk port.

10.3.8.7   Allow limiting the number of MAC addresses per port.

10.3.8.8   Allow limiting the number of VLANs per port.

10.3.9   Port Rate Limiting

The device shall:

10.3.9.1   Have the ability to limit traffic on a per-port basis.

10.3.9.2   Allow the choice between Broadcast; Multicast; or Unicast limiting, which is essential for managing network traffic.

10.3.10 Port Based Access Control

The device shall:

10.3.10.1   Provide a means for authenticating and authorising devices attached to the Ethernet ports.

10.3.10.2   Comply with IEEE 802.1X-2010.

10.3.11 Link Aggregation

The device shall:

10.3.11.1   Allow the linking of Ethernet ports into one logical trunk for higher bandwidths.

10.3.11.2   Comply with IEEE 802.1AX-2008.

10.3.12 Port Mirroring

The device shall support port mirroring that is essential for network monitoring and troubleshooting on live networks.

10.3.13 Time Synchronization

10.3.13.1   The device shall support the Simple Network Time Protocol (SNTP) that is to be used to synchronise the internal system clocks of devices on the network allowing for correct correlation of time stamped events for troubleshooting.

10.3.13.2   The device shall be able to perform the function of a Network Time Protocol (NTP) server.

10.3.13.3   The device shall be able to perform the function of a Network Time Protocol (NTP) client.

10.3.13.4   The *Supplier* shall indicate whether or not the device can support IEEE 1588 version 2 and IEEE C27-238-2011.

10.3.13.5   The *Supplier* shall indicate whether an option for a GPS receiver exists.

10.3.14 Other Requirements

The device shall:

10.3.14.1   Be able to perform the function of a Dynamic Host Control Protocol (DHCP) server, with option 82 supported.

10.3.14.2   Allow for centralised password management by means of a RADIUS server.

10.3.14.3   Provide Intrusion Detection and Prevention System (IDS/ IPS) services.

10.3.14.4   Support Integrated Routing and Bridging (IRB), which allows a protocol to be bridged as well as routed on the same interface on the router. This can be used to forward VLAN headers.

10.3.14.5   Allow for inter VLAN routing.

10.3.14.6   Allow for IP multicast routing.

10.3.14.7   Support serial IP encapsulation.

10.3.14.8 Provide a fault indication under all failure conditions.

10.3.14.9 Allow for Fast Link Detections (FLD) for quicker discovery of new devices or links in the network.

10.3.14.10 Allow FLD to be automatically turned off, as a failsafe, in the case of a large number of link state changes propagating across the network.

10.3.14.11 Support the Link Layer Discovery Protocol (LLDP) [refer to IEEE 802.1AB-2009].

10.3.14.12 Support the Internet Group Management Protocol (IGMP) version 3 [refer to RFC 4604] that is used in managing the membership of multicast groups.

10.3.14.13 Be able to perform IGMP snooping.

10.3.14.14 Be able to auto-sense the IP version.

10.3.14.15 Be able to perform auto-negotiation and automatic crossover detection.

10.3.14.16 Support the Multiple MAC Registration Protocol (MMRP) that allows multicast traffic in bridged LANs to be confined to areas of the network where it is required. [refer to IEEE 802.1Q-2011]

10.3.14.17 Support Multi-level user password to protect the switch from unauthorised persons.

10.3.14.18 Allow for logs to be sent to a syslog server.

10.3.14.19 Allow for WAN and LAN Loopback and Loop-test functions.

10.3.15   Switch Security

10.3.15.1 The switch shall comply with North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) security standards, policy 001 - 009, where applicable.

10.3.15.2 The switch shall comply with the Cyber Security Standard for Operational Technology, EST 240 - 55410927.

10.3.15.3 The device shall support Remote Authentication Dial In User Service (RADIUS).

10.3.15.4 The device shall be able to authenticate to AAA (Authentication, Authorization and Accounting) via a RADIUS server.

10.3.15.5 The device shall comply with IEEE 802.1X-2010, port-based network access control.

10.3.15.6 The device shall support multiple levels of privileges per user.

10.3.15.7 The device shall allow for the number of MAC addresses on a port to be limited.

10.3.15.8 All encryption on the device shall be 128 bit AES or better.

10.3.16   Management Tools

10.3.16.1   The switch's management shall be accessible via a web browser that supports HTTPS or via a serial connection.

10.3.16.2   Different web browsers shall be supported i.e. Firefox web browser on Linux or Internet Explorer on Windows.

10.3.16.3   The management Command Line Interface (CLI) shall be accessible via Secure Shell (SSH).

10.3.16.4   The device shall allow remote access for configuration purposes via a physically separated management port.

10.3.16.5   The device shall support the Simple Network Management Protocol (SNMP) version 1, version 2c and version 3.

10.3.16.6   The device shall support the Remote Network Monitoring (RMON) for event logging, viewing of device statistics, proactive monitoring, problem detection and reporting.

11.   SERIAL PORT SERVER REQUIREMENTS

It will be used to provide serial over IP sockets and a means of supporting remote engineering to legacy equipment using propriety protocols and bus architectures. Listed below are the requirements for the Serial Port Server. Three different options shall be provided: small option with 2 serial ports; a medium option with 4-8 serial ports and a large option with 16-32 ports.

11.1   ENVIRONMENTAL, ELECTRICAL AND MECHANICAL REQUIREMENTS

The device shall be substation hardened or ruggedized to be able to withstand the following, without the performance being out of limits, reliability being compromised or the life cycle being shortened.

11.1.1   Environmental

The device shall:

11.1.1.1   Comply with Class C3, as per IEC 60870-2 part 1, Table 1; except for temperature.

11.1.1.2   Operate within a temperature range of -40°C to 85°C, with passive cooling.

11.1.2   Altitude

The device shall operate within an altitude range between 0 – 2500m.

11.1.3   EMI Immunity

The device shall provide error-free operation when exposed to EMI stress and electrical surges, as per Class 2 requirements of IEEE 1613.

11.1.4   Electrical

The device shall:

11.1.4.1   Operate within an electrical interference environment, where equipment is sited within high voltage switching compounds (132 kV or above) such that it is subject to high levels of radiated electrical interference, due to its physical placement or its direct connection to electrical plant.

11.1.4.2   Not be affected by other device frequencies.

11.1.4.3   Not generate any interference, which could hinder its own performance or the performance of the other equipment in its vicinity.

11.1.5   Power Supply

11.1.5.1   The power supply voltages shall be selectable.

11.1.5.2   The voltage options shall be: 48, 110 and 220 volts D.C.

11.1.5.3   The voltage tolerances shall be as per Table 1.

11.1.5.4   Dual, redundant power supplies shall be provided with separate inputs per power supply to be able to draw from separate power sources.

11.1.5.5   The option for a hot swappable power supply is preferred. The *Supplier* shall indicate if available.

11.1.5.6   The power supply connectors shall be pluggable terminal block or screw terminal block.

11.1.6   Mechanical Shock and Vibration

The device shall comply with Class Bm, as per IEC 60870-2 part 1, section 4.2.2.

11.2   HARDWARE

11.2.1   Switching Fabric

11.2.1.1   The switching fabric bandwidth shall be at least twice the total capacity of connecting modules. i.e. the bandwidth shall be double the port rate.

11.2.1.2   The switch shall not allow head of line blocking.

11.2.1.3   The switch shall utilise the store and forward method for switching.

11.2.1.4   The switching latency shall be indicated.

11.2.2   Serial Ports

The serial ports shall:

11.2.2.1   Have surge protection and preferably be optically isolated.

11.2.2.2   Be protected from Electro Static Discharges (ESD) as defined in IEC61000-4-2 Level 1 (2kV) for both contact and air discharges

11.2.2.3   Support DB9 female connectors; RJ45 connectors; and Phoenix type screw terminals.

11.2.2.4   Support Universal Serial Ports where RS232 or RS485 shall be provided on the same physical connector that is software configurable.

11.2.2.5   Allow for the data rate to be selected on a per port basis, in the software.

11.2.2.6   Support the following data rates:

a) 1200

b) 4800

c) 9600

d) 19200

e) 38400

f) 57600

g) 115200

11.2.2.7   Support the following flow control signalling when RS232 is setup:

a) RTS/CTS hardware handshaking

b) Xon/Xoff software handshaking

c) No flow control

11.2.2.8   Allow data Byte frames to be configurable as follows:

a) Seven or eight bits data length

b) Even/odd or no parity bit

c) One or two stop bits

11.2.2.9   Support 120 Ohm terminating resistors as used in RS485 busses. These terminating resistors shall be selectable and preferably by software.

11.2.2.10   Support the following connection types:

11.2.2.10.1   Active - where always on and initiated by the device to the remote host,

11.2.2.10.2   Passive - where connection is initiated from the remote host to the device as required by the remote host, and

11.2.2.10.3   On-Demand - where the connection is initiated from the device to the remote host once serial data has been captured and is ready for transmission, after which a timeout function will be used to disconnect the host.

11.2.2.11   Support an inactivity timeout function on the IP socket that once elapsed will terminate the connection.

11.2.2.12   Support a predefined limitation on the amount of IP socket connections that can be made to a port.

11.2.2.13   Support the use of a terminating character to force the transmission of the serial data.

11.2.2.14   Support any ASCII or bit-based protocol.

11.2.2.15   Support a small device option with 2 serial ports

11.2.2.16   Support a medium device option with 4 to 8 serial ports

11.2.2.17   Support a large device option with 16 to 32 ports that is modular to allow for appropriate module selection, future expansion or repairs.

11.2.3   Ethernet Ports

The Ethernet ports shall be a combination of numerous copper and or fibre ports, based on the requirements of the connecting bay devices.

11.2.3.1   The fibre ports shall:

11.2.3.1.1   Support multimode communication (10BaseFL) with a wavelength of 850nm.

11.2.3.1.2   Support multimode communication (100BaseFx) with a wavelength of 1300nm.

11.2.3.1.3   Support LC, ST and SC connectors.

11.2.3.2   The copper ports shall:

11.2.3.2.1   Support both 10BaseTx and 100BaseTx.

11.2.3.2.2   Support RJ45 connectors.

11.2.3.3   Ethernet ports shall be modular to allow for future expansion or repairs.

11.2.3.4   The device shall support as a minimum 2 Ethernet ports

11.2.4   General

11.2.4.1   The device shall be made of heavy duty steel and supplied with the option to mount on a standard 19" rack panel or a DIN rail, with all associated accessories.

11.2.4.2   The device shall have terminal blocks for power and I/O connections that are rated for industrial applications.

11.2.4.3   There shall be an option to add a protective coating on the circuit board, to protect against dust and moisture.

11.2.4.4   The unit shall have supporting software than can create virtual communication ports on both an windows-based and Linux systems. These virtual ports shall enable transparent communications to the serial ports.

11.2.4.5   There shall be a dedicated RS232 port for device management.

11.2.4.6   There shall be an option to use appropriate utility grade Small Form-factor Pluggable (SFP) modules, if and when required.

11.3 REQUIRED ETHERNET FUNCTIONALITY

11.3.1 Virtual Local Area Networks (VLANs)

The device shall:

11.3.1.1   Support VLAN tagging.

11.3.1.2   Comply with IEEE 802.1Q-2011.

11.3.1.3   Support the double-tagging of an Ethernet frame/QinQ functionality [refer to IEEE 802.1Q-2011].

11.3.1.4   Support the Multiple VLAN Registration Protocol (MVRP) for automatically propagating VLAN information across a network.

11.3.1.5   Support VLAN assignment per port, for untagged traffic.

11.3.2 Link Aggregation

The device shall:

11.3.2.1   Allow the linking of Ethernet ports into one logical trunk for higher bandwidths.

11.3.2.2   Comply with IEEE 802.1AX-2008.

11.3.3 Serial IP Encapsulation

The device shall:

11.3.3.1   Support serial IP encapsulation

11.3.3.2   Be able to handle the serial IP encapsulation of all the protocols listed in the hardware section (11.2.1.14).

11.3.4 Spanning Tree Protocol

The device shall:

11.3.4.1   Support the Rapid Spanning Tree Protocol (RSTP) [refer to IEEE 802.1D-2004].

11.3.4.2   Support the Multiple Spanning Tree Protocol (MSTP) [refer to IEEE 802.1Q-2011].

11.3.5 Traffic Prioritisation

The device shall:

11.3.5.1   Allow for the classification of priorities based on the MAC address, ports, and tags.

11.3.5.2   Allow time critical data to be classified as higher priority.

11.3.5.3   Support numerous priority queues for TOS.

11.3.5.4   Comply with the QoS Prioritisation schemes in the IEEE 802.1Q-2011.

11.3.6 Port Configuration

The device shall:

11.3.6.1   Allow for automatic configuration of ports.

11.3.6.2   Allow for automatic crossover detection.

11.3.6.3   Allow for manual configuration of media type state, speed and duplex state.

11.3.6.4   Have the capability to disable ports that are not being used.

11.3.6.5   Allow a port to be configured to a specific VLAN.

11.3.6.6   Be capable of limiting which VLANs are accessible through a trunk port.

11.3.6.7   Allow limiting the number of MAC addresses per port.

11.3.6.8   Allow limiting the number of VLANs per port.

11.3.7 Port Rate Limiting

The device shall:

11.3.7.1   Have the ability to limit traffic on a per-port basis.

11.3.7.2   Allow the choice between Broadcast; Multicast; or Unicast limiting, which is essential for managing network traffic.

11.3.8 Port Based Access Control

The device shall:

11.3.8.1   Provide a means for authenticating and authorising devices attached to the Ethernet ports.

11.3.8.2   Comply with IEEE 802.1X-2010.

11.3.9 Security Requirements

11.3.9.1   The device shall comply with North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) security standards, policy 001 - 009, where applicable.

11.3.9.2   The switch shall comply with the Cyber Security Standard for Operational Technology, EST 240 - 55410927.

11.3.9.3   The device shall support Remote Authentication Dial In User Service (RADIUS).

11.3.9.4   The device shall be able to authenticate to AAA (Authentication, Authorization and Accounting) via a RADIUS server.

11.3.9.5   The device shall comply with IEEE 802.1X-2010, port-based network access control.

11.3.9.6   The device shall support multiple levels of privileges per user.

11.3.9.7   The device shall support multi-level user password.

11.3.9.8   All encryption on the device shall be 128 bit AES or better.

11.3.10   Management Tools

11.3.10.1   The device's management shall be accessible via a web browser that supports HTTPS or via a serial connection.

11.3.10.2   Different web browsers shall be supported i.e. Firefox web browser on Linux or Internet Explorer on Windows.

11.3.10.3 The management Command Line Interface (CLI) shall be accessible via Secure Shell (SSH).

11.3.10.4   The device shall support the Simple Network Management Protocol (SNMP) version 1, version 2c and version 3.

11.3.10.5   The device shall support the Remote Network Monitoring (RMON) for event logging, viewing of device statistics, proactive monitoring, problem detection and reporting.

12.   GENERAL REQUIREMENTS

12.1   NETWORK MANAGEMENT SOFTWARE (NMS) REQUIREMENTS

The NMS shall:

12.1.1   Be viewable remotely using an encrypted web browser.

12.1.2   Work with Firefox web browser on Linux and not just with Internet Explorer on Windows.

12.1.3   Be accessible via a command line interface via Secure Shell (SSH).

12.1.4   Support scalable licenses for the number of nodes supported with no top limit.

12.1.5   Allow for early detection and repair of faults.

12.1.6   Generate standard and custom reports and graphs on network statistics for the purpose of performance management.

12.1.7   Maintain a log containing the users who logged in, with timestamps for traceability.

12.1.8   Allow for bulk remote uploads of new configurations.

12.1.9   Allow for bulk remote upgrade of firmware.

12.1.10   Provide information on link status throughout the network.

12.1.11   Provide information on device status throughout the network.

12.1.12   Provide information on levels of traffic in different segments of the network.

12.1.13   Provide information on available services on the network.

12.1.14   Support auto discovery, to discover the network that can be configured to include or exclude various ranges or devices.

12.1.15   Provide automatically generated visual maps of the network, showing devices, their links and statuses.

12.1.16   Support SNMP v1, v2c or v3 traps.

12.1.17   Provide support for Remote Monitoring and LLDP.

12.1.18   Support the Linux or Windows operating system.

12.1.19   Have manually configurable thresholds.

12.1.20   Be able to send events by email, SMS or outside programs.

12.1.21   Preferably use SNMP as the protocol.

12.2   SFP MODULE REQUIREMENTS

The *Supplier* shall:

12.2.1   Provide specifications of the all the proposed SFP modules to be supplied and indicated whether the SFP modules are *Supplier* manufactured or third party in origin.

12.2.2   Indicate which standards and what certification the SFP module complies to and provide copies of the certification and/ test results confirming compliance.

12.2.3   Allow for the device to be locked down, to use only specified SFP modules.

12.2.4   Provide a list of recommended third party SFP modules along with their specification and certification, in the case that the device cannot be locked down to use the *Supplier's* SFP module.

12.3   TESTING AND APPROVAL

12.3.1   All equipment shall be pre-built and tested at the *Supplier's* premises before delivery.

12.3.2   Details of tests performed on the equipment shall be submitted for approval. Subsequent to establishment of a contract, test certificates shall be required prior to delivery of any equipment.

12.4   WARRANTY

The *Supplier* shall repair, correct, or replace any defects of any nature that may occur for a period of 5 years from the date of delivery of the device.

12.5   SOFTWARE LICENSES

The *Supplier* shall identify and separately price, all software licence and maintenance agreements required for the switches, routers, serial port servers and management software. The type of license, once-off versus annual, shall be indicated, to enable accurate overall cost calculation.

12.6 DOCUMENTATION

12.6.1 The specifications of the switches and router and detailed drawings, where applicable, shall be supplied in English.

12.6.2 The *Supplier* shall supply at least the following documentation items for each type of switch, router and serial port server:

12.6.2.1 Functional specification documentation

12.6.2.2 Detailed design documentation

12.6.2.3 Factory acceptance test procedure

12.6.2.4 Site acceptance test procedure

12.6.2.5 Commissioning acceptance procedure

12.6.2.6 Hardware maintenance documentation

12.6.2.7 Software maintenance documentation

12.6.2.8 Troubleshooting manual

12.6.3 Detailed procedures on the following topics shall be included:

12.6.3.1 Software installation and operation

12.6.3.2 Device troubleshooting techniques

12.6.3.3 Firmware upgrades

12.6.3.4 Adding and removing modules on the switch, router or serial port server.

12.6.3.5 Performing network management using the management tool

12.6.4 Each of the documents shall have as a minimum, the following: Title; Status; Revision; References; Purpose; Description and Interfaces.

12.6.5 The successful equipment *Supplier* shall be required to supply ten copies in English of each of the installation and operations manual detailing the operation of the switch, router and serial port server, operation of the software and servicing of these devices on delivery of the first items of equipment.

12.7 TRAINING

12.7.1 The *Supplier* shall provide comprehensive training courses to enable the *Purchaser* to configure, install, fully maintain and perform fault finding on switches and routers.

12.7.2 The *Supplier* shall indicate the possibility of getting users trained to add/replace device modules on site, without an impact on the warranty agreement.

12.7.3 The language medium for the training courses shall be English.

12.7.4   The *Supplier* shall state the following:

12.7.4.1   The type of training offered;

12.7.4.2   The course outline;

12.7.4.3   Location of the training centre;

12.7.4.4   The duration and cost of each training course;

12.7.4.5   The maximum and minimum number of students per training course;

12.7.4.6   Prerequisite knowledge for each student

12.7.5   All training documentation shall be supplied both in electronic and hard copy format.

12.8   SPARES

The *Supplier* shall:

12.8.1   Provide prices on a per item basis and a recommended inventory of spare parts sufficient to support the required operational availability of all LAN equipment.

12.8.2   State the spares availability for each module.

12.8.3   Provide a detailed list of all equipment's Mean Time Between Failure (MTBF) to support the recommended inventory of spares.

12.8.4   Commit to a minimum of ten years spares support.

12.8.5   Supply the following information:

12.8.5.1   A detailed spares list for each of the required switches, router and serial port servers

12.8.5.2   The lead times for obtaining spares

12.8.5.3   Whether spares are sourced locally or overseas

12.9   SUPPORT AND MAINTENANCE

The *Supplier* shall:

12.9.1   State their ability to support the equipment, which they provide, both during and after the warranty period/for a period of ten years subsequent to the expiry of the supply contract.

12.9.2   Include details of dedicated support staff that are available.

12.9.3   Indicate the response time to replace and/repair equipment. This shall be specified per module.

12.9.4   State the willingness to enter into support/service level agreements based on guaranteed response time. The *Purchaser* requires a response time of 24 hours after notification of a failure to the *Supplier* for an exchange of any module within the device or the device itself. Any implications to the *Purchaser* of such agreements shall be specified.

12.9.5   Commit to a pre-defined minimum stock holding for each of the modules within a device.

12.9.6   Detail the suggested approach to system maintenance, with due consideration of the *Purchaser's* self-sufficiency requirements.

A high level of after sales support and the promptness of that support shall be important criteria in the evaluation of the tender.

13. AUTHORISATION

This document has been seen and accepted by:

Name	Designation
M Sukhnandan	Chairperson Telecontrol/SCADA Study Committee
P Kara	Protection Technology and Support Manager
R Mccurrach	Senior Manager : PTMC Engineering
S Papadopoulos	Control and Automation Technology and Support Manager
Z Gydien	Chairperson Telecoms Study Committee

14. REVISION

Date	Rev.	Compiler	Remarks
April 2012	0	M Mammen	New Document 474-242
May 2012	0.1	M Mammen	Updated based on comments received
June 2012	1	M Mammen	Final Document for Approval
July 2012	2	M Mammen	Final Document with A/B schedule added
May 2013	2.1	M Mammen	Update the document to reflect the OT security standard and requirements.
August 2013	3	M Mammen	Final Document for Authorisation and Publication as 474-242 Rev 3
August 2013	1	M Mammen	New 240-6111223 document number allocation for Publication

15. DEVELOPMENT TEAM

The following people were involved in the development of this document:

- M Mammen
- J Botha
- T Hyman
- S Seetswane
- I Naicker
- J Hector

16. ACKNOWLEDGEMENTS

Not Applicable.

APPENDIX A:

SCHEDULE OF REQUIREMENTS A/B

FOR

THE PURCHASER'S

STANDARD NETWORKING DEVICES FOR THE SUBSTATION ENVIRONMENT

SCOPE OF SCHEDULE A/B

This document provides a schedule of compliance with regards to, the Goods Information for: Standard Networking Devices for the Substation Environment, as per the Purchaser's requirements. It cross-references all the relevant chapters requiring a response from Tenderers and assists Tenderers in providing a comprehensive proposal.

Tenderers are requested to complete this Schedule A/B as part of the tender submission data package.

INSTRUCTION TO *TENDERERS*

When completing the Schedule of Requirements A/B *Tenderers* are requested to take cognisance of the following:

- It is expected of *Tenderers* to state clearly, for each clause that requires a statement of compliance in the Schedule of Requirements A/B, either "Comply" or "Do not comply".
- It is expected of the *Tenderer* to state the exact location of the evidence in the supporting documentation that is required to validate compliance. References should be in the following format: document name; document reference number; page number; and paragraph number.
  Failure to provide this information will result in the *Tenderer* being deemed non-compliant for that clause in the requirements schedule.
- All supporting documentation shall be provided in electronic format as well as hard copies.
- If a clause in the Schedule of Requirements A/B requires information only, e.g. describe application etc., *Tenderers* are at liberty to provide any information deemed appropriate.

SCHEDULE A : *PURCHASER'S* PARTICULAR REQUIREMENT
SCHEDULE B : THE *TENDERER'S* COMPLIANCE

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
1.	**INTRODUCTION**	Stated for information only		No response required
2.	**SUPPORTING CLAUSES**	Stated for information only		No response required
2.1	**SCOPE**	Stated for information only		No response required
2.1.1	Purpose	Stated for information only		No response required
2.1.2	Applicability	Stated for information only		No response required
2.2	**NORMATIVE/ INFORMATIVE REFERENCES**	Stated for information only		No response required
2.2.1	Normative	Stated for information only		No response required
2.2.2	Informative	Stated for information only		No response required
2.3	**DEFINITIONS**	Stated for information only		No response required
2.3.1	Classification	Stated for information only		No response required
2.4	**ABBREVIATIONS**	Stated for information only		No response required
2.5	**ROLES AND RESPONSIBILITIES**	Stated for information only		No response required
2.6	**PROCESS FOR MONITORING**	Stated for information only		No response required
2.7	**RELATED/ SUPPORTING DOCUMENTS**	Stated for information only		No response required
3.	**PROJECT PROGRAMME**	State Compliance		
3.1	**Phase 1 - FDS** Functional Specification; System Design Report; Project Programme	State Compliance		
3.2	**Phase 2 - DDS** Detailed Design Specification (if applicable); FAT Procedure; SAT Procedure	State Compliance		
3.3	**Phase 3 – Development, System Integration & FAT** Signed off FAT report	State Compliance		
3.4	**Phase 4 – Delivery, Installation, Testing &**	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
	Commissioning			
	Equipment Delivery & Installation; System Documentation; Approved Implementation Report; Commissioned system			
3.5	**Phase 5 - SAT**	State Compliance		
	Signed off SAT report; Hand-over Certificate; Source code for all software delivered			
3.6	**Phase 6 – Establishment of supply contract**	State Compliance		
4.	**ARCHITECTURE OVERVIEW**	Stated for information only		No response required
5.	**PHILOSOPHY**	State Compliance		
	Standard Hardware and Software Special developments kept to a minimum Interoperability; Scalability; Modularity; Upgradability			
6.	**DESIGN REQUIREMENTS**	Stated for information only		No response required
7.	**GIGABIT SWITCH REQUIREMENTS**	Stated for information only		No response required
7.1	**ENVIRONMENTAL, ELECTRICAL AND MECHANICAL REQUIREMENTS**	State Compliance		
7.1.1	**Environmental**	Stated for information only		No response required
7.1.1.1	Comply to Class 3 of IEC 60870-2 part 1, Table 1	State Compliance		
7.1.1.2	Temperature range of -40°C to 85°C; Passive cooling	State Compliance		
7.1.2	**Altitude**	State Compliance		
	0 – 2500m			
7.1.3	**EMI Immunity**	State Compliance		
	Error-free operation as per Class 2 requirements of IEEE1613			
7.1.4	**Electrical**	Stated for information only		No response required
7.1.4.1	Operate within an electrical interference environment, where equipment is sited within high voltage switching compounds (132 kV or above) such that it is subject to high levels of radiated electrical interference.	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
7.1.4.2	Not affected by other device frequencies	State Compliance		
7.1.4.3	Does not generate any interference that affects its own or other equipment's (within its vicinity) performance.	State Compliance		
7.1.5	**Power Supply**	Stated for information only		No response required
7.1.5.1	Voltage shall be selectable	State Compliance		
7.1.5.2	DC Voltage options: 48 , 110, and 220	State Compliance		
7.1.5.3	Voltage tolerances as per Table 1	State Compliance		
7.1.5.4	Dual redundant power supplies with separate inputs per power supply	State Compliance		
7.1.5.5	Support for hot swappable power supply option	State Compliance		
7.1.5.6	Support pluggable terminal block connectors and screw terminal block connectors	State Compliance		
7.1.6	**Mechanical Shock and Vibration** Comply with Class Bm, as per IEC 60870-2 part 1, section 4.2.2.	State Compliance		
7.2	**HARDWARE**	Stated for information only		No response required
7.2.1	**Switching Fabric**	Stated for information only		No response required
7.2.1.1	Bandwidth = 2 x capacity of connecting modules	State Compliance		
7.2.1.2	Shall not allow head of line blocking	State Compliance		
7.2.1.3	Uses the store and forward method for switching	State Compliance		
7.2.1.4	Switching latency to be indicated	Specify the switching latency		
7.2.2	**Fibre Ports**	Stated for information only		No response required
7.2.2.1	Support Multimode ; 1000BaseSx with wavelength of 850nm	State Compliance		
7.2.2.2	Support Singlemode ; 1000BaseLx with wavelength of 1310nm	State Compliance		
7.2.2.3	Support LC connectors	State Compliance		
7.2.2.4	Modularity	State Compliance		
7.2.2.5	Minimum 8 Ethernet gigabit ports	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
7.2.3	**General**	Stated for information only		No response required
7.2.3.1	Made of heavy duty steel 19"rack panel and DIN rail mount option	State Compliance		
7.2.3.2	Industrial application rated terminal blocks for power and I/O connections.	State Compliance		
7.2.3.3	Option to add a protective coating on the circuit board	State Compliance		
7.2.3.4	Dedicated RS232 port for switch management	State Compliance		
7.2.3.5	Option of a utility grade SFP module	State Compliance		
7.3	**REQUIRED FUNCTIONALITY**	Stated for information only		No response required
7.3.1	**VLANs**	Stated for information only		No response required
7.3.1.1	Minimum 30 VLANs	State Compliance		
7.3.1.2	Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
7.3.1.3	Support double-tagging of Ethernet frame Comply to IEEE 802.1D-2004	State Compliance and provide certification		
7.3.1.4	Support MVRP for automatic propagation of VLAN information across a network	State Compliance		
7.3.1.5	Support VLAN assignment per port, for untagged traffic.	State Compliance		
7.3.2	**Spanning Tree Protocol**	Stated for information only		No response required
7.3.2.1	Network "healing" speed < 5ms per hop	State Compliance		
7.3.2.2	Support mesh topologies with up to 80 devices	State Compliance		
7.3.2.3	RSTP support Comply to IEEE 802.1D-2004	State Compliance and provide certification		
7.3.2.4	MSTP support Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
7.3.3	**Link Aggregation**	Stated for information only		No response required
7.3.3.1	Support trunking of Ethernet ports	State Compliance		
7.3.3.2	Comply to IEEE 802.1AX-2008	State Compliance and provide		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
		certification		
7.3.4	**Traffic Prioritisation**	Stated for information only		No response required
7.3.4.1	Priority classification based on MAC address, ports, tags and Type of Service (TOS)	State Compliance		
7.3.4.2	Higher priority assignment for time critical data	State Compliance		
7.3.4.3	Numerous priority queues for TOS	State Compliance		
7.3.4.4	Comply to QOS prioritisation schemes as per IEEE 802.1Q-2011	State Compliance and provide certification		
7.3.5	**Port Configuration**	Stated for information only		No response required
7.3.5.1	Automatic port configuration	State Compliance		
7.3.5.2	Automatic crossover detection	State Compliance		
7.3.5.3	Manual configuration of media type state, speed and duplex state	State Compliance		
7.3.5.4	Capability to disable ports not being used	State Compliance		
7.3.5.5	Capability to configure specific VLANs to a port	State Compliance		
7.3.5.6	Capability to limit VLANs accessible via trunk port	State Compliance		
7.3.5.7	Capability to limit MAC addresses per port	State Compliance		
7.3.5.8	Capability to limit VLANs per port	State Compliance		
7.3.6	**Port Rate Limiting**	Stated for information only		No response required
7.3.6.1	Ability to limit traffic per-port	State Compliance		
7.3.6.2	Option of : Broadcast ; Multicast; & Unicast Limiting	State Compliance		
7.3.7	**Port Based Access Control**	Stated for information only		No response required
7.3.7.1	Supports authenticating and authorising devices attached to a Ethernet port	State Compliance		
7.3.7.2	Comply to IEEE 802.1x-2010	State Compliance and provide certification		
7.3.8	**Port Mirroring Support**	State Compliance		
7.3.9	**Time Synchronization**	Stated for information only		No response required
7.3.9.1	SNTP support	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
7.3.9.2	SNTP client and NTP client support			
7.3.9.3	IEEE1588 version 2 and IEEE C37.238-2011 support	State Compliance		
7.3.9.4	NTP server and client support	State Compliance		
7.3.10	**Other Requirements**	Stated for information only		No response required
7.3.10.1	Has a Link Fault Indication under all failure conditions	State Compliance		
7.3.10.2	Supports Fast Link Detection (FLD)	State Compliance		
7.3.10.3	FLD can automatically be turned off when large number of link state changes occur.	State Compliance		
7.3.10.4	Auto-sense the IP version	State Compliance		
7.3.10.5	LLDP support Comply to IEEE 802.1AB-2009	State Compliance and provide certification		
7.3.10.6	IGMP version 3 support	State Compliance		
7.3.10.7	Ability to perform IGMP snooping	State Compliance		
7.3.10.8	MMRP support Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
7.3.10.9	Ability to filter broadcast frames to prevent a broadcast storm.	State Compliance		
7.3.10.10	Multi-level user password support	State Compliance		
7.3.10.11	Logs that can be sent to a syslog server	State Compliance		
7.3.11	**Switch Security**	Stated for information only		No response required
7.3.11.1	Comply to NERC CIP security standards, policy 001-009	State Compliance and provide certification		
7.3.11.2	Comply to OT Security Standards; EST 240 - 55410927	State Compliance		
7.3.11.3	RADIUS support	State Compliance		
7.3.11.4	Ability to authenticate to AAA via RADIUS server	State Compliance		
7.3.11.5	Comply to IEEE 802.1X-2010	State Compliance and provide certification		
7.3.11.6	Support multiple levels of privileges per user	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
7.3.11.7	Support 128 AES encryption or better	State Compliance		
7.3.12	**Management Tools**	Stated for information only		No response required
7.3.12.1	Device management accessible via HTTPS or via a serial connection	State Compliance		
7.3.12.2	Support different web browsers Firefox for Linux Internet Explorer for Windows	State Compliance		
7.3.12.3	CLI via SSH	State Compliance		
7.3.12.4	Device allows remote access for configuration via physically separated management port.	State Compliance		
7.3.12.5	SNMP version 1, 2c and 3 support	State Compliance		
7.3.12.6	RMON support	State Compliance		
8.	**LAYER 2 SWITCH REQUIREMENTS** Support for 2 switch options: Small switch; 4-16 Ethernet ports Large switch; 16-32 Ethernet ports	State Compliance		
8.1	**ENVIRONMENTAL, ELECTRICAL AND MECHANICAL REQUIREMENTS**	State Compliance		
8.1.1	**Environmental**	Stated for information only		No response required
8.1.1.1	Comply to Class 3 of IEC 60870-2 part 1, Table 1	State Compliance		
8.1.1.2	Temperature range of -40°C to 85°C; Passive cooling	State Compliance		
8.1.2	**Altitude** 0 – 2500m	State Compliance		
8.1.3	**EMI Immunity** Error-free operation as per Class 2 requirements of IEEE1613	State Compliance		
8.1.4	**Electrical**	Stated for information only		No response required
8.1.4.1	Operate within an electrical interference environment where equipment is sited within high voltage switching	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
	compounds (132 kV or above) such that it is subject to high levels of radiated electrical interference.			
8.1.4.2	Not affected by other device frequencies	State Compliance		
8.1.4.3	Does not generate any interference that affects its own or other equipment's (within its vicinity) performance.	State Compliance		
8.1.5	**Power Supply**	Stated for information only		No response required
8.1.5.1	Voltage shall be selectable	State Compliance		
8.1.5.2	DC Voltage options: 48 , 110, and 220	State Compliance		
8.1.5.3	Voltage tolerances as per Table 1	State Compliance		
8.1.5.4	Dual redundant power supplies with separate inputs per power supply	State Compliance		
8.1.5.5	Support for hot swappable power supply option	State Compliance		
8.1.5.6	Support pluggable terminal block connectors and screw terminal block connectors			
8.1.6	**Mechanical Shock and Vibration**	State Compliance		
	Comply with Class Bm, as per IEC 60870-2 part 1, section 4.2.2.			
8.2	**HARDWARE**	Stated for information only		No response required
8.2.1	**Switching Fabric**	Stated for information only		No response required
8.2.1.1	Bandwidth = 2 x capacity of connecting modules	State Compliance		
8.2.1.2	Shall not allow head of line blocking	State Compliance		
8.2.1.3	Uses the store and forward method for switching	State Compliance		
8.2.1.4	Switching latency to be indicated	Specify the switching latency		
8.2.2	**Gigabit Fibre Ports**	Stated for information only		No response required
8.2.2.1	Support Multimode ; 1000BaseSx with wavelength of 850nm	State Compliance		
8.2.2.2	Support Singlemode ; 1000BaseLx with wavelength of 1310nm	State Compliance		
8.2.2.3	Support LC connectors	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
8.2.2.4	Modularity	State Compliance		
8.2.2.5	Minimum 2 Ethernet gigabit ports for large switch option	State Compliance		
8.2.3	**10Base and 100Base Ethernet Ports**	Stated for information only		No response required
8.2.3.1	**Fibre ports**	Stated for information only		No response required
8.2.3.1.1	Support Multimode ; 10BaseFL with wavelength of 850nm	State Compliance		
8.2.3.1.2	Support Multimode ; 100BaseFx with wavelength of 1300nm	State Compliance		
8.2.3.1.3	Support LC, ST and SC connectors	State Compliance		
8.2.3.2	**Copper ports**	Stated for information only		No response required
8.2.3.2.1	Support 10BaseTx and 100Base Tx	State Compliance		
8.2.3.2.2	Support RJ45 connectors	State Compliance		
8.2.3.3	Modularity	State Compliance		
8.2.3.4	**Large Switch option:** minimum 16 Ethernet ports. Combination of 10Base and 100Base ports	State Compliance		
8.2.3.5	**Small Switch option:** between 6 - 16 Ethernet ports. Combination of 10Base and 100Base ports	State Compliance		
8.2.4	**General**	Stated for information only		No response required
8.2.4.1	Made of heavy duty steel 19"rack panel and DIN rail mount option	State Compliance		
8.2.4.2	Industrial application rated terminal blocks for power and I/O connections.	State Compliance		
8.2.4.3	Option to add a protective coating on the circuit board	State Compliance		
8.2.4.4	Dedicated RS232 port for switch management	State Compliance		
8.2.4.5	Option of a utility grade SFP module	State Compliance		
8.3	**REQUIRED FUNCTIONALITY**	Stated for information only		No response required
8.3.1	**VLANs**	Stated for information only		No response required
8.3.1.1	Minimum 30 VLANs	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
8.3.1.2	Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
8.3.1.3	Support double-tagging of Ethernet frame Comply to IEEE 802.1D-2004	State Compliance and provide certification		
8.3.1.4	Support MVRP for automatic propagation of VLAN information across a network	State Compliance		
8.3.1.5	Support VLAN assignment per port, for untagged traffic.	State Compliance		
8.3.2	**Spanning Tree Protocol**	Stated for information only		No response required
8.3.2.1	Network "healing" speed < 5ms per hop	State Compliance		
8.3.2.2	Support mesh topologies with up to 80 devices	State Compliance		
8.3.2.3	RSTP support Comply to IEEE 802.1D-2004	State Compliance and provide certification		
8.3.2.4	MSTP support Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
8.3.3	**Link Aggregation**	Stated for information only		No response required
8.3.3.1	Support trunking of Ethernet ports	State Compliance		
8.3.3.2	Comply to IEEE 802.1AX-2008	State Compliance and provide certification		
8.3.4	**Traffic Prioritisation**	Stated for information only		No response required
8.3.4.1	Priority classification based on MAC address, ports, tags and Type of Service (TOS)	State Compliance		
8.3.4.2	Higher priority assignment for time critical data	State Compliance		
8.3.4.3	Numerous priority queues for TOS	State Compliance		
8.3.4.4	Comply to QOS prioritisation schemes as per IEEE 802.1Q-2011	State Compliance and provide certification		
8.3.5	**Port Configuration**	Stated for information only		No response required
8.3.5.1	Automatic port configuration	State Compliance		
8.3.5.2	Automatic crossover detection	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
8.3.5.3	Manual configuration of media type state, speed and duplex state	State Compliance		
8.3.5.4	Capability to disable ports not being used	State Compliance		
8.3.5.5	Capability to configure specific VLANs to a port	State Compliance		
8.3.5.6	Capability to limit VLANs accessible via trunk port	State Compliance		
8.3.5.7	Capability to limit MAC addresses per port	State Compliance		
8.3.5.8	Capability to limit VLANs per port	State Compliance		
8.3.6	**Port Rate Limiting**	Stated for information only		No response required
8.3.6.1	Ability to limit traffic per-port	State Compliance		
8.3.6.2	Option of :Broadcast ; Multicast; & Unicast Limiting	State Compliance		
8.3.7	**Port Based Access Control**	Stated for information only		No response required
8.3.7.1	Supports authenticating and authorising devices attached to a Ethernet port	State Compliance		
8.3.7.2	Comply to IEEE 802.1x-2010	State Compliance and provide certification		
8.3.8	**Port Mirroring**	State Compliance		
	Supports port mirroring			
8.3.9	**Time Synchronization**	Stated for information only		No response required
8.3.9.1	SNTP support	State Compliance		
8.3.9.2	IEEE1588 ver. 2 and IEEE C37.238-2011 support	State Compliance		
8.3.9.3	NTP server and client support	State Compliance		
8.3.10	**Other Requirements**	Stated for information only		No response required
8.3.10.1	Has a Link Fault Indication under all failure conditions	State Compliance		
8.3.10.2	Supports Fast Link Detection (FLD)	State Compliance		
8.3.10.3	FLD can automatically be turned off when large numbers of link state changes occur.	State Compliance		
8.3.10.4	Auto-sense the IP version	State Compliance		
8.3.10.5	Perform auto-detection and automatic crossover detection	State Compliance and provide certification		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
8.3.10.6	LLDP support Comply to IEEE 802.1AB-2009	State Compliance and provide certification		
8.3.10.7	IGMP version 3 support	State Compliance		
8.3.10.8	Ability to perform IGMP snooping	State Compliance		
8.3.10.9	MMRP support Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
8.3.10.10	Multi-level user password support	State Compliance		
8.3.10.11	Logs that can be sent to a syslog server	State Compliance		
8.3.11	**Switch Security**	Stated for information only		No response required
8.3.11.1	Comply to NERC CIP security standards, policy 001-009	State Compliance and provide certification		
8.3.11.2	Comply to OT Security Standards; EST 240 - 55410927	State Compliance		
8.3.11.3	RADIUS support	State Compliance		
8.3.11.4	Ability to authenticate to AAA via RADIUS server	State Compliance		
8.3.11.5	Comply to IEEE 802.1X-2010	State Compliance and provide certification		
8.3.11.6	Support multiple levels of privileges per user	State Compliance		
8.3.11.7	Support 128 AES encryption or better	State Compliance		
8.3.12	**Management Tools**	Stated for information only		No response required
8.3.12.1	Device management accessible via HTTPS or via a serial connection	State Compliance		
8.3.12.2	Support different web browsers Firefox for Linux Internet Explorer for Windows	State Compliance		
8.3.12.3	CLI via SSH	State Compliance		
8.3.12.4	Device allows remote access for configuration via physically separated management port.	State Compliance		
8.3.12.5	SNMP version 1, 2c and 3 support	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
8.3.12.6	RMON support	State Compliance		
9.	**ROUTER REQUIREMENTS**	Stated for information only		No response required
9.1	**ENVIRONMENTAL, ELECTRICAL AND MECHANICAL REQUIREMENTS**	State Compliance		
9.1.1	**Environmental**	Stated for information only		No response required
9.1.1.1	Comply to Class 3 of IEC 60870-2 part 1, Table 1	State Compliance		
9.1.1.2	Temperature range of -40°C to 85°C; Passive cooling	State Compliance		
9.1.2	**Altitude** 0 – 2500m	State Compliance		
9.1.3	**EMI Immunity** Error-free operation as per Class 2 requirements of IEEE1613	State Compliance		
9.1.4	**Electrical**	Stated for information only		No response required
9.1.4.1	Operate within an electrical interference environment, , where equipment is sited within high voltage switching compounds (132 kV or above) such that it is subject to high levels of radiated electrical interference	State Compliance		
9.1.4.2	Not affected by other device frequencies	State Compliance		
9.1.4.3	Does not generate any interference that affects its own or other equipment's (within its vicinity) performance.	State Compliance		
9.1.5	**Power Supply**	Stated for information only		No response required
9.1.5.1	Voltage shall be selectable	State Compliance		
9.1.5.2	DC Voltage options: 48 , 110, and 220	State Compliance		
9.1.5.3	Voltage tolerances as per as per Table 1	State Compliance		
9.1.5.4	Dual redundant power supplies with separate inputs per power supply	State Compliance		
9.1.5.5	Support for hot swappable power supply option	State Compliance		
9.1.5.6	Support pluggable terminal block connectors and screw terminal block connectors	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
9.1.6	**Mechanical Shock and Vibration**	State Compliance		
	Comply with Class Bm, as per IEC 60870-2 part 1, section 4.2.2			
9.2	**HARDWARE**	Stated for information only		No response required
9.2.1	**Router Fabric**	Stated for information only		No response required
9.2.1.1	Indicate the router's maximum throughput, when all ports are being utilised, for the following Ethernet frame sizes: 64 bytes, 512 bytes and 1518 bytes	Specify router's maximum throughput		
9.2.1.2	Router latency to be indicated for the following Ethernet frame sizes: 64 bytes, 512 bytes and 1518 bytes	Specify router latency		
9.2.2	**Ethernet Ports**	Stated for information only		No response required
9.2.2.1	**Fibre ports**	Stated for information only		No response required
9.2.2.1.1	Support Multimode ; 1000BaseSx with wavelength of 850nm	State Compliance		
9.2.2.1.2	Support Singlemode ; 1000BaseLx with wavelength of 1310nm	State Compliance		
9.2.2.1.3	Support Multimode ; 100BaseFx with wavelength of 1300nm	State Compliance		
9.2.2.1.4	Support LC and ST connectors	State Compliance		
9.2.2.2	**Copper ports**	Stated for information only		No response required
9.2.2.2.1	Support 100Base Tx	State Compliance		
9.2.2.2.2	Support 1000Base Tx	State Compliance		
9.2.2.2.3	Support RJ45 connectors	State Compliance		
9.2.2.3	Modularity	State Compliance		
9.2.2.4	Minimum 2 x1000BaseEthernet ports and 2x 100Base Ethernet ports	State Compliance		
9.2.3	**WAN Ports**	Stated for information only		No response required
9.2.3.1	Support Channelised-E1 connections	State Compliance		
9.2.3.2	Support X.21 connections	State Compliance		
9.2.3.3	Modularity	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
9.2.3.4	Minimum 2 WAN ports	State Compliance		
9.2.4	**Serial Ports**	Stated for information only		No response required
9.2.4.1	Support RS232	State Compliance		
9.2.4.2	Support RS422	State Compliance		
9.2.4.3	Support RS485	State Compliance		
9.2.4.4	Support RJ45 connectors	State Compliance		
9.2.4.5	Modularity	State Compliance		
9.2.4.6	Minimum 2 serial ports	State Compliance		
9.2.5	**General**	Stated for information only		No response required
9.2.5.1	Made of heavy duty steel 19" rack panel and DIN rail mount option	State Compliance		
9.2.5.2	Industrial application rated terminal blocks for power and I/O connections.	State Compliance		
9.2.5.3	Option to add a protective coating on the circuit board	State Compliance		
9.2.5.4	Dedicated RS232 port for router management	State Compliance		
9.2.5.5	Option of a utility grade SFP module	State Compliance		
9.3	**REQUIRED FUNCTIONALITY**	Stated for information only		No response required
9.3.1	**Virtual Private Network (VPN)**	Stated for information only		No response required
9.3.1.1	Layer 2 and Layer 3 VPN support	State Compliance		
9.3.1.2	**Support the following secure VPN protocols:**	Stated for information only		No response required
9.3.1.2.1	IPsec	State Compliance		
9.3.1.2.2	SSL	State Compliance		
9.3.1.2.3	TLS	State Compliance		
9.3.1.3	**Support the following encryption methods:**	Stated for information only		No response required
9.3.1.3.1	3DES	State Compliance		
9.3.1.3.2	AES128	State Compliance		
9.3.1.3.3	AES256	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
9.3.1.4	VPN shall comply to IEEE 802.1Q-2011 and IEEE 802.1D-2004	State Compliance and provide certification		
9.3.1.5	VPN supports tunnels to be created to: A host; A port on a host; A whole site	State Compliance		
9.3.1.6	VPN supports GOOSE tunnels to be created	State Compliance		
9.3.2	**VLANs**	Stated for information only		No response required
9.3.2.1	Minimum 30 VLANs	State Compliance		
9.3.2.2	Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
9.3.2.3	Support double-tagging of Ethernet frame Comply to IEEE 802.1D-2004	State Compliance and provide certification		
9.3.2.4	Support MVRP for automatic propagation of VLAN information across a network	State Compliance		
9.3.2.5	Support VLAN assignment per port, for untagged traffic.	State Compliance		
9.3.3	**Spanning Tree Protocol**	Stated for information only		No response required
9.3.3.1	Network "healing" speed < 5ms per hop	State Compliance		
9.3.3.2	Support mesh topologies with up to 80 devices	State Compliance		
9.3.3.3	RSTP support Comply to IEEE 802.1D-2004	State Compliance and provide certification		
9.3.3.4	MSTP support Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
9.3.4	**Link Aggregation**	Stated for information only		No response required
9.3.4.1	Support trunking of Ethernet ports	State Compliance		
9.3.4.2	Comply to IEEE 802.1AX-2008	State Compliance and provide certification		
9.3.5	**Traffic Prioritisation**	Stated for information only		No response required
9.3.5.1	Priority classification based on MAC address, type of protocol, ports, tags and Type of Service (TOS)	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
9.3.5.2	Higher priority assignment for time critical data	State Compliance		
9.3.5.3	Numerous priority queues for TOS	State Compliance		
9.3.5.4	Comply to QOS prioritisation schemes as per IEEE 802.1Q-2011	State Compliance and provide certification		
9.3.6	**Firewall**	Stated for information only		No response required
9.3.6.1	Supports a firewall allowing stateful inspection	State Compliance		
9.3.6.2	NAT and IP Address Masquerading support	State Compliance		
9.3.6.3	Ability to perform port forwarding	State Compliance		
9.3.6.4	Ability to filter on source and destination address and ports	State Compliance		
9.3.7	**Routing Protocols**	Stated for information only		No response required
9.3.7.1	OSPF version 2 support	State Compliance		
9.3.7.2	RIP and BGP support	State Compliance		
9.3.7.3	VRRP support	State Compliance		
9.3.7.4	Static routing option	State Compliance		
9.3.7.5	PPP support	State Compliance		
9.3.7.6	HDLC support	State Compliance		
9.3.7.7	Comply to IEEE 802.1AX-2008	State Compliance and provide certification		
9.3.8	**WAN Authentication Protocol** CHAP support	State Compliance		
9.3.9	**Port Configuration**	Stated for information only		No response required
9.3.9.1	Automatic port configuration	State Compliance		
9.3.9.2	Automatic crossover detection	State Compliance		
9.3.9.3	Manual configuration of media type state, speed and duplex state	State Compliance		
9.3.9.4	Capability to disable ports not being used	State Compliance		
9.3.9.5	Capability to configure specific VLANs to a port	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
9.3.9.6	Capability to limit VLANs accessible via trunk port	State Compliance		
9.3.9.7	Capability to limit MAC addresses per port	State Compliance		
9.3.9.8	Capability to limit VLANs per port	State Compliance		
9.3.10	**Port Rate Limiting**	Stated for information only		No response required
9.3.10.1	Ability to limit traffic per-port	State Compliance		
9.3. 10.2	Option of :Broadcast ; Multicast; & Unicast Limiting	State Compliance		
9.3.11	**Port Based Access Control**	Stated for information only		No response required
9.3.11.1	Supports authenticating and authorising devices attached to a Ethernet port	State Compliance		
9.3.11.2	Comply to IEEE 802.1X-2010	State Compliance and provide certification		
9.3.12	**Time Synchronization**	Stated for information only		No response required
9.3.12.1	SNTP support	State Compliance		
9.3. 12.2	NTP server functionality support	State Compliance		
9.3. 12.3	NTP client functionality support	State Compliance		
9.3. 12.4	IEEE1588 version 2 and IEEE C37.238-2011 support	State Compliance		
9.3. 12.5	Option for a GPS receiver	State Compliance		
9.3.13	**Other Requirements**	Stated for information only		No response required
9.3.13.1	Support DHCP server functionality with option 82 support	State Compliance		
9.3.13.2	Support centralised password management via a RADIUS server	State Compliance		
9.3.13.3	IDS/IPS services support	State Compliance		
9.3.13.4	IRB support	State Compliance		
9.3.13.5	Support inter VLAN routing	State Compliance		
9.3.13.6	Support IP multicast routing	State Compliance		
9.3.13.7	Serial IP encapsulation support	State Compliance		
9.3.13.8	Has a Link Fault Indication under all failure conditions	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
9.3.13.9	LLDP support Comply to IEEE 802.1AB-2009	State Compliance and provide certification		
9.3.13.10	IGMP version 3 support	State Compliance		
9.3.13.11	Multi-level user password support	State Compliance		
9.3.13.12	Logs that can be sent to a syslog server	State Compliance		
9.3.13.13	Allow for WAN and LAN loopback and Loop-test functions	State Compliance		
9.3.14	**Router Security**	Stated for information only		No response required
9.3.14.1	Comply to NERC CIP security standards, policy 001-009	State Compliance and provide certification		
9.3.14.2	Comply to OT Security Standards; EST 240 - 55410927	State Compliance		
9.3.14.3	RADIUS support	State Compliance		
9.3.14.4	Ability to authenticate to AAA via RADIUS server	State Compliance		
9.3.14.5	Comply to IEEE 802.1X-2010	State Compliance and provide certification		
9.3.14.6	Support multiple levels of privileges per user	State Compliance		
9.3.14.7	Support 128 AES encryption or better	State Compliance		
9.3.15	**Management Tools**	Stated for information only		No response required
9.3.15.1	Device management accessible via HTTPS or via a serial connection	State Compliance		
9.3.15.2	Support different web browsers Firefox for Linux Internet Explorer for Windows	State Compliance		
9.3.15.3	CLI via SSH	State Compliance		
9.3.15.4	Device allows remote access for configuration via physically separated management port.	State Compliance		
9.3.15.5	SNMP version 1, 2c and 3 support	State Compliance		
10.	**LAYER 3 SWITCH REQUIREMENTS**	Stated for information only		No response required

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
10.1	**ENVIRONMENTAL, ELECTRICAL AND MECHANICAL REQUIREMENTS**	State Compliance		
10.1.1	**Environmental**	Stated for information only		No response required
10.1.1.1	Comply to Class 3 of IEC 60870-2 part 1, Table 1	State Compliance		
10.1.1.2	Temperature range of -40°C to 85°C; Passive cooling	State Compliance		
10.1.2	**Altitude**	State Compliance		
	0 – 2500m			
10.1.3	**EMI Immunity**	State Compliance		
	Error-free operation as per Class 2 requirements of IEEE1613			
10.1.4	**Electrical**	Stated for information only		No response required
10.1.4.1	Operate within an electrical interference environment, where equipment is sited within high voltage switching compounds (132 kV or above) such that it is subject to high levels of radiated electrical interference.	State Compliance		
10.1.4.2	Not affected by other device frequencies	State Compliance		
10.1.4.3	Does not generate any interference that affects its own or other equipment's (within its vicinity) performance.	State Compliance		
10.1.5	**Power Supply**	Stated for information only		No response required
10.1.5.1	Voltage shall be selectable	State Compliance		
10.1.5.2	DC Voltage options: 48 , 110, and 220	State Compliance		
10.1.5.3	Voltage tolerances as per Table 1	State Compliance		
10.1.5.4	Dual redundant power supplies with separate inputs per power supply	State Compliance		
10.1.5.5	Support for hot swappable power supply option	State Compliance		
10.1.5.6	Support pluggable terminal block connectors and screw terminal block connectors	State Compliance		
10.1.6	**Mechanical Shock and Vibration**	State Compliance		
	Comply with Class Bm, as per IEC 60870-2 part 1, section 4.2.2.			

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
10.2	**HARDWARE**	Stated for information only		No response required
10.2.1	**Switching Fabric**	Stated for information only		No response required
10.2.1.1	Bandwidth = 2 x capacity of connecting modules	State Compliance		
10.2.1.2	Shall not allow head of line blocking	State Compliance		
10.2.1.3	Uses the store and forward method for switching	State Compliance		
10.2.1.4	Switching latency to be indicated	Specify switching latency		
10.2.2	**Gigabit Fibre Ports**	Stated for information only		No response required
10.2.2.1	Support Multimode ; 1000BaseSx with wavelength of 850nm	State Compliance		
10.2.2.2	Support Singlemode ; 1000BaseLx with wavelength of 1310nm	State Compliance		
10.2.2.3	Support LC connectors	State Compliance		
10.2.2.4	Modularity	State Compliance		
10.2.2.5	Minimum 2 Ethernet gigabit ports on separate modules	State Compliance		
10.2.3	**Ethernet Ports**	Stated for information only		No response required
10.2.3.1	**Fibre ports**	Stated for information only		No response required
10.2.3.1.1	Support Multimode ; 10BaseFL with wavelength of 850nm	State Compliance		
10.2.3.1.2	Support Multimode ; 100BaseFx with wavelength of 1300nm	State Compliance		
10.2.3.1.3	Support LC, ST and SC connectors	State Compliance		
10.2.3.2	**Copper ports**	Stated for information only		No response required
10.2.3.2.1	Support 10BaseTx	State Compliance		
10.2.3.2.2	Support 100Base Tx	State Compliance		
10.2.3.2.3	Support 1000Base Tx	State Compliance		
10.2.3.2.4	Support RJ45 connectors	State Compliance		
10.2.3.3	Modularity	State Compliance		
10.2.3.4	Minimum of 16 Ethernet ports.	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
	Combination of 10Base and 100Base ports			
10.2.4	**WAN Ports**	Stated for information only		No response required
10.2.4.1	Support Channelised-E1 connections	State Compliance		
10.2.4.2	Support X.21 connections	State Compliance		
10.2.4.3	Modularity	State Compliance		
10.2.4.4	Minimum 2 WAN ports	State Compliance		
10.2.5	**Serial Ports**	Stated for information only		No response required
10.2.5.1	Support RS232	State Compliance		
10.2.5.2	Support RS422	State Compliance		
10.2.5.3	Support RS485	State Compliance		
10.2.5.4	Support RJ45 connectors	State Compliance		
10.2.5.5	Modularity	State Compliance		
10.2.5.6	Minimum 2 serial ports	State Compliance		
10.2.6	**General**	Stated for information only		No response required
10.2.6.1	Made of heavy duty steel 19"rack panel and DIN rail mount option	State Compliance		
10.2.6.2	Industrial application rated terminal blocks for power and I/O connections.	State Compliance		
10.2.6.3	Option to add a protective coating on the circuit board	State Compliance		
10.2.6.4	Dedicated RS232 port for switch management	State Compliance		
10.2.6.5	Option of a utility grade SFP module	State Compliance		
10.3	**REQUIRED FUNCTIONALITY**	Stated for information only		No response required
10.3.1	**VLANs**	Stated for information only		No response required
10.3.1.1	Minimum 30 VLANs	State Compliance		
10.3.1.2	Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
10.3.1.3	Support double-tagging of Ethernet frame Comply to IEEE 802.1D-2004	State Compliance and provide certification		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
10.3.1.4	Support MVRP for automatic propagation of VLAN information across a network	State Compliance		
10.3.1.5	Ability to segregate traffic between pre-defined ports on switches	State Compliance		
10.3.1.6	Support VLAN assignment per port, for untagged traffic.	State Compliance		
10.3.2	**Virtual Private Network (VPN)**	Stated for information only		No response required
10.3.2.1	Layer 2 and Layer 3 VPN support	State Compliance		
10.3.2.2	**Support the following secure VPN protocols:**	Stated for information only		No response required
10.3.2.2.1	IPsec	State Compliance		
10.3.2.2.2	SSL	State Compliance		
10.3.2.3	**Support the following encryption methods:**	Stated for information only		No response required
10.3.2.3.1	3DES	State Compliance		
10.3.2.3.2	AES128	State Compliance		
10.3.2.3.3	AES256	State Compliance		
10.3.2.4	VPN shall comply to IEEE 802.1Q-2011 and IEEE 802.1D-2004	State Compliance and provide certification		
10.3.2.5	VPN supports tunnels to be created to: A host ; A port on a host; A whole site	State Compliance		
10.3.2.6	VPN supports GOOSE tunnels to be created	State Compliance		
10.3.3	**Spanning Tree Protocol**			No response required
10.3.3.1	Network "healing" speed < 5ms per hop	State Compliance		
10.3.3.2	Support mesh topologies with up to 80 devices	State Compliance		
10.3.3.3	RSTP support Comply to IEEE 802.1D-2004	State Compliance and provide certification		
10.3.3.4	MSTP support Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
10.3.4	**Traffic Prioritisation**	Stated for information only		No response required

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
10.3.4.1	Priority classification based on MAC address, type of protocol, ports, tags and Type of Service (TOS)	State Compliance		
10.3.4.2	Higher priority assignment for time critical data	State Compliance		
10.3.4.3	Numerous priority queues for TOS	State Compliance		
10.3.4.4	Comply to QOS prioritisation schemes as per IEEE 802.1Q-2011	State Compliance and provide certification		
10.3.5	**Firewall**	Stated for information only		No response required
10.3.5.1	Supports a firewall allowing stateful inspection	State Compliance		
10.3.5.2	NAT and IP Address Masquerading support	State Compliance		
10.3.5.3	Ability to perform port forwarding	State Compliance		
10.3.5.4	Ability to filter on source and destination address and ports	State Compliance		
10.3.6	**Routing Protocols**	Stated for information only		No response required
10.3.6.1	OSPF version 2 support	State Compliance		
10.3.6.2	RIP and BGP support	State Compliance		
10.3.6.3	VRRP support	State Compliance		
10.3.6.4	Static routing option	State Compliance		
10.3.6.5	PPP support	State Compliance		
10.3.6.6	HDLC support	State Compliance		
10.3.6.7	Comply to IEEE 802.1AX-2008	State Compliance and provide certification		
10.3.7	**WAN Authentication Protocol**	State Compliance		
	CHAP support			
10.3.8	**Port Configuration**	Stated for information only		No response required
10.3.8.1	Automatic port configuration	State Compliance		
10.3.8.2	Automatic crossover detection	State Compliance		
10.3.8.3	Manual configuration of media type state, speed and duplex state	State Compliance		
10.3.8.4	Capability to disable ports not being used	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
10.3.8.5	Capability to configure specific VLANs to a port	State Compliance		
10.3.8.6	Capability to limit VLANs accessible via trunk port	State Compliance		
10.3.8.7	Capability to limit MAC addresses per port	State Compliance		
10.3.8.8	Capability to limit VLANs per port	State Compliance		
10.3.9	**Port Rate Limiting**	Stated for information only		No response required
10.3.9.1	Ability to limit traffic per-port	State Compliance		
10.3.9.2	Option of :Broadcast; Multicast; & Unicast Limiting	State Compliance		
10.3.10	**Port Based Access Control**	Stated for information only		No response required
10.3.10.1	Supports authenticating and authorising devices attached to a Ethernet port	State Compliance		
10.3.10.2	Comply to IEEE 802.1x-2010	State Compliance and provide certification		
10.3.11	**Link Aggregation**	Stated for information only		No response required
10.3.11.1	Support trunking of Ethernet ports	State Compliance		
10.3.11.2	Comply to IEEE 802.1AX-2008	State Compliance and provide certification		
10.3.12	**Port Mirroring**	State Compliance		
	Supports port mirroring			
10.3.13	**Time Synchronization**	Stated for information only		No response required
10.3.13.1	SNTP support	State Compliance		
10.3.13.2	NTP server functionality support	State Compliance		
10.3.13.3	NTP client functionality support	State Compliance		
10.3.13.4	IEEE1588 version 2 and IEEE C37-238-2011 support	State Compliance		
10.3.13.5	Option for a GPS receiver	State Compliance		
10.3.14	**Other Requirements**	Stated for information only		No response required
10.3.14.1	Support DHCP server functionality with option 82 support	State Compliance		
10.3.14.2	Support centralised password management via a RADIUS server	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
10.3.14.3	IDS/IPS services support	State Compliance		
10.3.14.4	IRB support	State Compliance		
10.3.14.5	Support inter VLAN routing	State Compliance		
10.3.14.6	Support IP multicast routing	State Compliance		
10.3.14.7	Serial IP encapsulation support	State Compliance		
10.3.14.8	Has a Link Fault Indication under all failure conditions	State Compliance		
10.3.14.9	Supports Fast Link Detection (FLD)	State Compliance		
10.3.14.10	FLD can automatically be turned off when large numbers of link state changes occur.	State Compliance		
10.3.14.11	LLDP support Comply to IEEE 802.1AB-2009	State Compliance and provide certification		
10.3.14.12	IGMP version 3 support	State Compliance		
10.3.14.13	Ability to perform IGMP snooping	State Compliance		
10.3.14.14	Auto-sense the IP version	State Compliance		
10.3.14.15	Perform auto-detection and automatic crossover detection	State Compliance and provide certification		
10.3.14.16	MMRP support Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
10.3.14.17	Multi-level user password support	State Compliance		
10.3.14.18	Logs that can be sent to a syslog server	State Compliance		
10.3.14.19	Allow for WAN and LAN loopback and Loop-test functions	State Compliance		
10.3.15	**Switch Security**	Stated for information only		No response required
10.3.15.1	Comply to NERC CIP security standards, policy 001-009	State Compliance and provide certification		
10.3.15.2	Comply to OT Security Standards; EST 240 - 55410927	State Compliance		
10.3.15.3	RADIUS support	State Compliance		
10.3.15.4	Ability to authenticate to AAA via RADIUS server	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
10.3.15.5	Comply to IEEE 802.1X-2010	State Compliance and provide certification		
10.3.15.6	Support multiple levels of privileges per user	State Compliance		
10.3.15.7	Ability to limit the number of MAC addresses on a port	State Compliance		
10.3.15.8	Support 128 AES encryption or better	State Compliance		
10.3.16	**Management Tools**	Stated for information only		No response required
10.3.16.1	Device management accessible via HTTPS or via a serial connection	State Compliance		
10.3.16.2	Support different web browsers Firefox for Linux Internet Explorer for Windows	State Compliance		
10.3.16.3	CLI via SSH	State Compliance		
10.3.16.4	Device allows remote access for configuration via physically separated management port.	State Compliance		
10.3.16.5	SNMP version 1, 2c and 3 support	State Compliance		
10.3.16.6	RMON support	State Compliance		
11.	**SERIAL PORT SERVER REQUIREMENTS** Three different options: **Small option**: 2 serial ports **Medium option** : 4-8 serial ports **Large option:** 16-32 ports	State Compliance		
11.1	**ENVIRONMENTAL, ELECTRICAL AND MECHANICAL REQUIREMENTS**	State Compliance		
11.1.1	**Environmental**	Stated for information only		No response required
11.1.1.1	Comply to Class 3 of IEC 60870-2 part 1, Table 1	State Compliance		
11.1.1.2	Temperature range of -40°C to 85°C; Passive cooling	State Compliance		
11.1.2	**Altitude** 0 – 2500m	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
11.1.3	**EMI Immunity**	State Compliance		
	Error-free operation as per Class 2 requirements of IEEE1613			
11.1.4	**Electrical**	Stated for information only		No response required
11.1.4.1	Operate within an electrical interference environment, where equipment is sited within high voltage switching compounds (132 kV or above) such that it is subject to high levels of radiated electrical interference.	State Compliance		
11.1.4.2	Not affected by other device frequencies	State Compliance		
11.1.4.3	Does not generate any interference that affects its own or other equipment's (within its vicinity) performance.	State Compliance		
11.1.5	**Power Supply**	Stated for information only		No response required
11.1.5.1	Voltage shall be selectable	State Compliance		
11.1.5.2	DC Voltage options: 48 , 110, and 220	State Compliance		
11.1.5.3	Voltage tolerances as per Table 1	State Compliance		
11.1.5.4	Dual redundant power supplies with separate inputs per power supply	State Compliance		
11.1.5.5	Support for hot swappable power supply option	State Compliance		
11.1.5.6	Support pluggable terminal block connectors and screw terminal block connectors	State Compliance		
11.1.6	**Mechanical Shock and Vibration**	State Compliance		
	Comply with Class Bm, as per IEC 60870-2 part 1, section 4.2.2.			
11.2	**HARDWARE**	Stated for information only		No response required
11.2.1	**Switching Fabric**	Stated for information only		No response required
11.2.1.1	Bandwidth = 2 x capacity of connecting modules	State Compliance		
11.2.1.2	Shall not allow head of line blocking	State Compliance		
11.2.1.3	Uses the store and forward method for switching	State Compliance		
11.2.1.4	Switching latency to be indicated	Specify the switching latency		
11.2.2	**Serial Ports**	Stated for information only		No response required

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
11.2.2.1	Have surge protection ; preferably optically isolated	State Compliance		
11.2. 2.2	Be ESD protected for contact and air discharges, as per IEC 61000-4-2 Level1 (2kV)	State Compliance		
11.2. 2.3	Support DB9 and RJ45 connectors Support Phoenix type screw terminals	State Compliance		
11.2. 2.4	Support Universal Serial Ports for RS232 or RS485, that's software configurable	State Compliance		
11.2. 2.5	Allow data rates to be selected on a per port basis	State Compliance		
11.2. 2.6	**Support these data rates:**	Stated for information only		No response required
11.2. 2.6a	1 200	State Compliance		
11.2. 2.6b	4 800	State Compliance		
11.2.2.6c	9 600	State Compliance		
11.2.2.6d	19 200	State Compliance		
11.2.2.6e	38 400	State Compliance		
11.2.2.6f	57 600	State Compliance		
11.2.2.6g	115 200	State Compliance		
11.2.2.7	**Support for the following flow control signalling for RS232:**	Stated for information only		No response required
11.2.2.7a	RTS/CTS hardware handshaking	State Compliance		
11.2.2.7b	Xon/Xoff software handshaking	State Compliance		
11.2.2.7c	No flow control	State Compliance		
11.2.2.8	**Allow for the data Byte frame to be configured as follows:**	Stated for information only		No response required
11.2.2.8a	Seven or eight bit data length	State Compliance		
11.2.2.8b	Parity: even / odd / no parity	State Compliance		
11.2.2.8c	1 or 2 stop bits	State Compliance		
11.2.2.9	Support for 120 Ohm terminating resistors Terminating resistors shall be selectable in software	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
11.2.2.10	**Support the following connection types:**	Stated for information only		No response required
11.2.2.10.1	Active (always on; initiated by device to remote host)	State Compliance		
11.2.2.10.2	Passive (as required by remote host; initiated by remote host to device)	State Compliance		
11.2.2.10.3	On-Demand (initiated from device to remote host once serial data is captured and ready for transmission; has a timeout function)	State Compliance		
11.2.2.11	Has an inactivity timeout function on the IP socket to terminate connections	State Compliance		
11.2.2.12	Support for a limited number of IP sockets connections to a port	State Compliance		
11.2.2.13	Supports the terminating character to force the transmission of serial data	State Compliance		
11.2.2.14	Support ASCII and bit-based protocols	State Compliance		
11.2.2.15	Small device option support (2 serial ports)	State Compliance		
11.2.2.16	Medium device option support (4 – 8 serial ports)	State Compliance		
11.2.2.17	Large device option support (16 to 32 serial ports)	State Compliance		
11.2.3	**Ethernet Ports**	State Compliance		
11.2.3.1	**Fibre ports**	Stated for information only		No response required
11.2.3.1.1	Support Multimode ; 10BaseFL with wavelength of 850nm	State Compliance		
11.2.3.1.2	Support Multimode ; 100BaseFx with wavelength of 1300nm	State Compliance		
11.2.3.1.3	Support LC, ST and SC connectors	State Compliance		
11.2.3.2	**Copper ports**	Stated for information only		No response required
11.2.3.2.1	Support 10BaseTx and 100Base Tx	State Compliance		
11.2.3.2.2	Support RJ45 connectors	State Compliance		
11.2.3.3	Modularity	State Compliance		
11.2.3.4	Support minimum 2 Ethernet ports	State Compliance		
11.2.4	**General**	Stated for information only		No response required

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
11.2.4.1	Made of heavy duty steel 19"rack panel and DIN rail mount option	State Compliance		
11.2.4.2	Industrial application rated terminal blocks for power and I/O connections.	State Compliance		
11.2.4.3	Option to add a protective coating on the circuit board	State Compliance		
11.2.4.4	Unit shall have supporting software that can create virtual communication ports on both x86 and x64 windows based platforms. Virtual ports shall enable transparent communication to the serial ports.	State Compliance		
11.2.4.5	Dedicated RS232 port for switch management	State Compliance		
11.2.4.6	Option of a utility grade SFP module	State Compliance		
11.3	**REQUIRED ETHERNET FUNCTIONALITY**	Stated for information only		
11.3.1	**VLANs**	Stated for information only		No response required
11.3.1.1	Support for VLAN tagging	State Compliance		
11.3.1.2	Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
11.3.1.3	Support double-tagging of Ethernet frame Comply to IEEE 802.1D-2004	State Compliance and provide certification		
11.3.1.4	Support MVRP for automatic propagation of VLAN information across a network	State Compliance		
11.3.1.5	Support VLAN assignment per port, for untagged traffic.	State Compliance		
11.3.2	**Link Aggregation**	Stated for information only		No response required
11.3.2.1	Support trunking of Ethernet ports	State Compliance		
11.3.2.2	Comply to IEEE 802.1AX-2008	State Compliance and provide certification		
11.3.3	**Serial IP Encapsulation**	Stated for information only		No response required
11.3.3.1	Serial IP encapsulation support	State Compliance		
11.3.3.2	Support the encapsulation of ASCII and bit-based	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
	protocols			
11.3.4	**Spanning Tree Protocol**	Stated for information only		No response required
11.3.4.1	RSTP support Comply to IEEE 802.1D-2004	State Compliance and provide certification		
11.3.4.2	MSTP support Comply to IEEE 802.1Q-2011	State Compliance and provide certification		
11.3.5	**Traffic Prioritisation**	Stated for information only		No response required
11.3.5.1	Priority classification based on MAC address, ports, tags	State Compliance		
11.3.5.2	Higher priority assignment for time critical data	State Compliance		
11.3.5.3	Numerous priority queues for TOS	State Compliance		
11.3.5.4	Comply to QOS prioritisation schemes as per IEEE 802.1Q-2011	State Compliance and provide certification		
11.3.6	**Port Configuration**	Stated for information only		No response required
11.3.6.1	Automatic port configuration	State Compliance		
11.3.6.2	Automatic crossover detection	State Compliance		
11.3.6.3	Manual configuration of media type state, speed and duplex state	State Compliance		
11.3.6.4	Capability to disable ports	State Compliance		
11.3.6.5	Capability to configure specific VLANs to a port	State Compliance		
11.3.6.6	Capability to limit VLANs accessible via trunk port	State Compliance		
11.3.6.7	Capability to limit MAC addresses per port	State Compliance		
11.3.6.8	Capability to limit VLANs per port	State Compliance		
11.3.7	**Port Rate Limiting**	Stated for information only		No response required
11.3.7.1	Ability to limit traffic per-port	State Compliance		
11.3.7.2	Option of :Broadcast ; Multicast; &Unicast Limiting	State Compliance		
11.3.8	**Port Based Access Control**	Stated for information only		No response required
11.3.8.1	Supports authenticating and authorising devices	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
	attached to a Ethernet port			
11.3.8.2	Comply to IEEE 802.1X-2010	State Compliance and provide certification		
11.3.9	**Security Requirements**	Stated for information only		No response required
11.3.9.1	Comply to NERC CIP security standards, policy 001-009	State Compliance and provide certification		
11.3.9.2	Comply to OT Security Standards; EST 240 - 55410927	State Compliance		
11.3.9.3	RADIUS support	State Compliance		
11.3.9.4	Ability to authenticate to AAA via RADIUS server	State Compliance		
11.3.9.5	Comply to IEEE 802.1X-2010	State Compliance and provide certification		
11.3.9.6	Support multiple levels of privileges per user	State Compliance		
11.3.9.7	Support for multi-level user passwords	State Compliance		
11.3.9.8	Support 128 AES encryption or better	State Compliance		
11.3.10	**Management Tools**	Stated for information only		No response required
11.3.10.1	Device management accessible via HTTPS or via a serial connection	State Compliance		
11.3.10.2	Support different web browsers Firefox for Linux Internet Explorer for Windows	State Compliance		
11.3.10.3	CLI via SSH	State Compliance		
11.3.10.4	SNMP version 1, 2c and 3 support	State Compliance		
11.3.10.5	RMON support	State Compliance		
12.	**GENERAL REQUIREMENTS**	Stated for information only		No response required
12.1	**NETWORK MANAGEMENT SOFTWARE (NMS) REQUIREMENTS**	Stated for information only		No response required
12.1.1	Supports remote viewing via encrypted web browser	State Compliance		
12.1.2	Support different web browsers	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
	Firefox for Linux Internet Explorer plus others for Windows			
12.1.3	CLI accessible via SSH	State Compliance		
12.1.4	Support scalable licenses based on the number of nodes, with no upper limit	State Compliance		
12.1.5	Provides the ability for early detect and repair of faults.	State Compliance		
12.1.6	Provide standard and custom reports & graphs on network statistics	State Compliance		
12.1.7	Maintain a comprehensive log of users who logged in and their activities , with accurate timestamps for traceability	State Compliance		
12.1.8	Ability to perform bulk remote uploads of configurations	State Compliance		
12.1.9	Ability to perform bulk remote upgrade of firmware	State Compliance		
12.1.10	Provide link status information throughout the network	State Compliance		
12.1.11	Provide device status information throughout the network	State Compliance		
12.1.12	Provide information on the level of traffic in different segments of the network	State Compliance		
12.1.13	Provide information on the available services on the network	State Compliance		
12.1.14	Support auto-discovery	State Compliance		
12.1.15	Provide automatically generated visual maps of the network, including devices, links and statuses	State Compliance		
12.1.16	SNMP version 1, 2c or 3 traps support	State Compliance		
12.1.17	LLDP and Remote Monitoring support	State Compliance		
12.1.18	Support Linux Operating System	State Compliance		
12.1.19	Have manually configurable thresholds	State Compliance		
12.1.20	Ability to send events by email, SMS or to outside programs	State Compliance		
12.1.21	Preferably use SNMP protocol	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
12.2	**SFP MODULE REQUIREMENTS**	Stated for information only		No response required
12.2.1	SFP module specifications to be supplied. Indicate whether they are *Supplier* manufactured or third party in origin.	State Compliance		
12.2.2	Indicate the standards and certification for the SFP modules.	Specify the standards, certification and test results		
12.2.3	Ability to lock down the device to use specified SFP modules	State Compliance		
12.2.4	If device cannot be locked down: Provide a list of recommended third party suppliers SFP modules; specification and certification	State Compliance and provide certification or test results		
12.3	**TESTING AND APPROVAL**	Stated for information only		No response required
12.3.1	All equipment shall be pre-built and tested before delivery	State Compliance		
12.3.2	Details of tests performed needs to be approved After establishment of a contract, test certificates are required prior to delivery of equipment	State Compliance		
12.4	**WARRANTY** For a period of 5 years from date of delivery: The *Supplier* shall repair, correct or replace any defects of any nature	State Compliance		
12.5	**SOFTWARE LICENSES** The following shall be identified and separately priced: All software licenses & Maintenance agreements Type of licence (once-off or annual) to be indicated	State Compliance and provide information required		
12.6	**DOCUMENTATION**	Stated for information only		No response required
12.6.1	Specification and detailed drawings shall be supplied in English, for switches; router and serial device servers	State Compliance		
12.6.2	**As a minimum, each of these documents need to be supplied for each type of switch, router and serial port server:**	Stated for information only		No response required

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
12.6.2.1	Functional specification	State Compliance		
12.6.2.2	Detailed Design	State Compliance		
12.6.2.3	FAT procedure	State Compliance		
12.6.2.4	SAT procedure	State Compliance		
12.6.2.5	Commissioning acceptance procedure	State Compliance		
12.6.2.6	Hardware maintenance documentation	State Compliance		
12.6.2.7	Software maintenance documentation	State Compliance		
12.6.2.8	Troubleshooting manual	State Compliance		
12.6.3	**Detailed procedures on the following are to be included:**	Stated for information only		No response required
12.6.3.1	Software installation and operation	State Compliance		
12.6.3.2	Device trouble shooting techniques	State Compliance		
12.6.3.3	Firmware upgrades	State Compliance		
12.6.3.4	Detailed procedure on adding and removing modules on switches; routers and serial port servers	State Compliance		
12.6.3.5	Detailed procedure on how to perform network management using the management tool	State Compliance		
12.6.4	Each document must have the following as a minimum: Title; Status; Revision; References; Purpose; Description; Interfaces	State Compliance		
12.6.5	The following had to be provided, on delivery of the first set of equipment: 10 copies in English, of the Installation, operation and servicing manual (of the switch, router, port server, software)	State Compliance		
12.7	**TRAINING**	Stated for information only		No response required
12.7.1	Provide comprehensive training courses	State Compliance		
12.7.2	Indicate possibility training *Purchaser's* staff to add and replace device modules on site without impacting warranty agreements	State Compliance		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
12.7.3	All training shall be in English	State Compliance		
12.7.4	*Supplier* to state the following:	Stated for information only		No response required
12.7.4.1	Type of training offered	State Compliance		
12.7.4.2	Course outline	State Compliance		
12.7.4.3	Location of training centre/s	State Compliance		
12.7.4.4	Duration and cost of each training course	State Compliance		
12.7.4.5	Maximum and minimum number of students per course	State Compliance		
12.7.4.6	Pre-requisites of the course	State Compliance		
12.7.5	All documentation to be provided electronically and on hardcopy format	State Compliance		
12.8	**SPARES**	Stated for information only		No response required
12.8.1	Provide an inventory of spare parts sufficient to support required operation availability. Provide prices on a per item basis.	State Compliance and provided information required		
12.8.2	State the spares availability for each module	State Compliance and provided information required		
12.8.3	Provide a list of all equipment / module MTBF	State Compliance and provided information required		
12.8.4	Commit to a minimum of 10 years spares support	State Compliance		
12.8.5	**Supply information on the following:**	Stated for information only		No response required
12.8.5.1	Provide a detailed spares list for each type of switch, router and serial port server	State Compliance and provided information required		
12.8.5.2	Indicate the lead times for obtaining spares	State Compliance and provided information required		
12.8.5.3	Indicate if spares are sources locally or internationally	State Compliance and provided information required		
12.9	**SUPPORT AND MAINTENANCE**	Stated for information only		No response required
12.9.1	State the ability to support equipment	State Compliance and provided information required		
12.9.2	Indicate details of dedicated support staff	State Compliance and		

CLAUSE	DESCRIPTION	SCHEDULE A	SCHEDULE B	COMMENT(S)
		provided information required		
12.9.3	Indicate the response time to replace and or repair equipment per module	State Compliance and provided information required		
12.9.4	State willingness to enter into support/ service level agreements on guaranteed response times.	State Compliance and provided information required		
12.9.5	Commit to a pre-defined minimum stack holding for each module within a device	State Compliance and provided information required		
12.9.6	Provide a suggested approach to system maintenance.	State Compliance		
13	**AUTHORISATION**	Stated for information only		No response required
14	**REVISION**	Stated for information only		No response required
15	**DEVELOPMENT TEAM**	Stated for information only		No response required
16	**ACKNOWLEDGEMENTS**	Stated for information only		No response required

Signature :

Print Name :

Company :

Date :

APPENDIX B:

SUPPLIER QUESTIONNAIRE FOR

STANDARD NETWORKING DEVICES FOR THE

SUBSTATION ENVIRONMENT

The following questionnaire shall be completed and attached to the *Supplier's* tender proposal for Standard Networking Devices for the Substation Environment. Responses to the questions should state the question number and the question. The response can consist simply of references to specific sections in the body of the *Supplier's* proposal, where applicable.

Company Profile

1. Provide the following information:
    1.1. Name of Company.
    1.2. Company address
    1.3. Date of establishment of Company.

2. Outline the Company's management structure.

3. State the Company's staff compliment
    3.1. Administrative.
    3.2. Design.
    3.3. Software.
    3.4. Production.
    3.5. Drawing Office.
    3.6. Inspection and Quality Assurance.
    3.7. Support
    3.8. Other.

4. Give a brief summary of your present range of equipment and services available.

5. Briefly describe the nature of your resources in the Republic of South Africa e.g. workshop; design; equipment development; testing; and production facilities etc.

Industry Experience

6. If not already detailed in your answers to the above questions, state what experience you have had with substation networking equipment.

7. *Supplier's* comparable sized networking equipment project experience references.
    7.1. State the customer and hardware/software configurations of comparable-sized networking equipment that you have delivered (or that are still in progress) during the past five (5) years.

    7.2. Provide customer references and contract values of the projects indicated in 7.1.

8. Schedule and completion history.
    8.1. Provide the original and actual delivery dates of those networking equipment listed above.

    8.2. Where applicable provide the major reasons for delivery delays for those networking equipment that were delivered more than six (6) months behind the original delivery schedule.

8.3. List and describe the number of networking equipment projects that are currently in progress and/planned to start through 2012/13 versus the number of technical staff directly involved with the production of networking devices.

9. State your level of adherence to International Engineering Standards.

10. Quality Assurance
    10.1. Briefly describe your methods of ensuring that hardware and software ready for customer delivery has been quality assured and tested.

    10.2. Indicate the quality assurance standards that are adhered to and indicate any nationally and internationally recognised body to which the *Supplier* is registered.

11. Manufacturing Capability
    The following additional information is required with respect to the manufacture of networking equipment:

    11.1. Guaranteed lead times for the manufacture and delivery of networking equipment.

    11.2. The quantity of each type of networking equipment that can be produced per month with the *Supplier's* current capability.

    11.3. The implications of increasing the quantity of networking equipment that can be produced per month.

12. Maintenance
    12.1. Describe the maintenance policy for the networking equipment offered, both during and after the warranty period.

    12.2. Will the *Supplier* honour all warranties and guarantees if the *Purchaser's* personnel perform maintenance functions on networking equipment?

    12.3. Will all maintenance or repairs to networking equipment be done locally?

    12.4. Describe any specialised test equipment required for maintenance that is generally not commercially available.

    12.5. *Suppliers* shall provide details of any generalised test equipment, which can be provided to simplify testing and maintenance of networking equipment. It is not the *Purchaser's* intention to fund the development of new specific test devices. However, the *Purchaser* would consider any proposals that are made.

13. Spares
    13.1. Describe the recommended networking equipment spares holdings with respect to the *Purchaser's* geographical locations (substations located throughout the Republic of South Africa) and networking equipment availability requirements.

    13.2. Describe your policy on availability of spare parts and expansion parts for a period of ten years subsequent to the expiry of the supply contract.

14. *Supplier* should state the willingness to provide training on the networking equipment at the *Purchaser's* premises wherever and whenever feasible and practical.

15. Installation and Commissioning
    15.1. *Suppliers* are to indicate if they are willing to install and commission networking equipment at Eskom sites as well as all costs associated with this.

    15.2. *Suppliers* are to specify the lead times required to commence such installation and commissioning and the volume of work, which can be catered for.

16. Telephonic and Local Support
    16.1. *Suppliers* are to indicate if they are willing to provide local support to networking equipment at site, as well as all costs associated with this.

    16.2. *Suppliers* are to specify the turnaround time required to commence such support and the volume of work, which can be catered for, as indicated in 16.1.

    16.3. *Suppliers* are to indicate if they are willing to provide telephonic support, as well as the costs associated with this.