

 Eskom	Standard	Technology
--	-----------------	-------------------

Title: **SUBSTATION AUTOMATION – NETWORK ARCHITECTURE AND APPLICATION DESIGN STANDARD FOR TRANSMISSION SUBSTATIONS**

Unique Identifier: **240-61268959**

Alternative Reference Number: **N/A**

Area of Applicability: **Engineering**

Documentation Type: **Standard**

Revision: **3**

Total Pages: **43**

Next Review Date: **November 2023**

Disclosure Classification: **Controlled Disclosure**

Compiled by



Rishi Hariram
Chief Engineer

Date: 23/10/2018

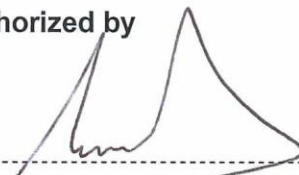
Approved by



Steven Papadopoulos
Control and Automation
Technology and Support
Manager

Date: 24/10/2018

Authorized by



Richard McCurrach
Senior Manager PTMC
Engineering

Date: 25/10/2018

Supported by SCOT/SC



Marlini Sukhnandan
SCOT/SC Chairperson

Date: 23/10/2018

Content

	Page
1. Introduction	6
2. Supporting Clauses	6
2.1 Scope	6
2.1.1 Purpose	6
2.1.2 Applicability	6
2.2 Normative/Informative References.....	6
2.2.1 Normative.....	6
2.2.2 Informative	7
2.3 Definitions.....	7
2.3.1 General	7
2.3.2 Disclosure Classification	8
2.4 Abbreviations.....	8
2.5 Roles and Responsibilities	10
2.6 Process for monitoring	10
2.7 Related/Supporting Documents	10
3. Network architecture.....	10
3.1 Network architecture overview	10
3.1.1 General	10
3.1.2 Objectives	10
3.1.3 Criteria.....	10
3.2 Environmental design parameters	11
3.2.1 Rated for reliable operation in harsh electrical environments.....	11
3.2.2 Rated for error-free operation in high electromagnetic interference environments	11
3.2.3 Rated for operation over a wide temperature range	11
3.2.4 Rated for high availability.....	11
3.2.5 Rated for industrial installations	11
3.3 Network architecture for a single control room	11
3.4 Network architecture for a segregated control room.....	12
4. Network application detailed design	13
4.1 Introduction.....	13
4.2 Physical Environment.....	14
4.2.1 Equipment Housing.....	14
4.2.2 Cable Entry and Termination	14
4.2.3 Cabling.....	14
4.2.4 Fibre Cables and Fibre Termination	14
4.2.5 Fibre Patch Leads.....	15
4.2.6 Cooling	15
4.2.7 Environmental Monitoring	16
4.3 Devices to be connected.....	16
4.3.1 Protection and multifunction intelligent electronic devices	16
4.3.2 Substation gateways.....	16
4.3.3 Station remote terminal units	16
4.3.4 Station IED	16
4.3.5 Global positioning system receivers with embedded network time protocol servers	16

4.3.6	Disturbance recorders.....	16
4.3.7	Under Frequency Load Shedding (UFLS)	16
4.3.8	Meters	16
4.3.9	Engineering laptops	17
4.3.10	Test sets.....	17
4.3.11	Tele-protection systems	17
4.3.12	Condition-based monitoring systems.....	17
4.3.13	Internet protocol cameras (future)	17
4.3.14	Human-machine interfaces	17
4.3.15	IP telephony systems (future)	17
4.3.16	Routers.....	17
4.3.17	Data servers.....	17
4.3.18	Engineering servers	17
4.3.19	Authentication servers	17
4.3.20	Bay level controllers	17
4.3.21	Quality of supply meters	17
4.3.22	Travelling wave fault locators.....	18
4.3.23	Security and access control systems (future)	18
4.3.24	Merging units and intelligent switchgear	18
4.4	Network design parameters	18
4.4.1	Overview	18
4.4.2	Hardware.....	18
4.4.3	Power Supplies	19
4.4.4	Firmware and software versions	19
4.5	Network configuration.....	20
4.5.1	Device Naming.....	20
4.5.2	LAN switch port speed and duplex configuration.....	20
4.5.3	VLAN overview	20
4.5.4	Interface Addressing	24
4.5.5	Interface Allocation	25
4.5.6	Network quality of service policies	26
4.5.7	IP traffic prioritization and differentiated services	27
4.5.8	Spanning tree.....	30
4.5.9	IP Routing	31
4.5.10	Dynamic host configuration protocol.....	32
4.5.11	Trunking/Link Aggregation	32
4.5.12	LAN switch port security settings	33
4.5.13	Power over Ethernet configuration	33
4.5.14	Internet group management protocol.....	34
4.5.15	GARP multicast registration protocol.....	34
4.5.16	Network security enhancements.....	35
4.5.17	Link layer discovery protocol.....	35
4.5.18	Network IP addressing and device allocations	35
4.5.19	IP address management.....	36
4.5.20	Routing requirements and wide area network interfacing	36
4.5.21	Network time synchronization	36
4.5.22	Network time protocol	37
4.5.23	Change control policy	37
4.6	Substation Router.....	37

4.6.1	Overview	37
4.6.2	Hardware.....	37
4.6.3	Ethernet interfaces	38
4.6.4	Device Naming.....	38
4.6.5	Software versions	38
4.6.6	Interface Addressing and Allocation	38
4.6.7	Enabled Services	39
4.6.8	DHCP Server	39
4.6.9	Router Redundancy	39
4.6.10	Shorewall Firewall.....	40
4.6.11	SNMP Configuration	40
4.7	Device management philosophy	41
4.7.1	Management	41
4.7.2	Network alarm and failure notifications.....	41
4.7.3	Network performance monitoring.....	41
4.7.4	Contact procedures and notification policies	41
4.7.5	Network management system	41
4.7.6	Simple network management protocol management and monitoring	42
5.	Authorisation.....	43
6.	Revisions	43
7.	Development team	43
8.	Acknowledgements	43

Figures

Figure 1: Network architecture for a single control room.....	12
Figure 2: Network architecture for a segregated control room	13
Figure 3: Tagged Ethernet Frame	23
Figure 4: Original IPv4 type of service byte.....	28
Figure 5: Differentiated services codepoint field	28
Figure 6: Graphical representation of a typical substation IP address map.....	36

Tables

Table 1: Hardware description.....	19
Table 2: Power termination on the switch.....	19
Table 3: Firmware/Software versions	20
Table 4: Device naming example	20
Table 5: Configuration and duplex settings for substation automation networks	20
Table 6: VLAN allocations	21
Table 7: VLANs and IP addressing example.....	22
Table 8: GOOSE VLAN allocations	22
Table 9: GOOSE message configurations	23
Table 10: VLAN configuration example	24
Table 11: Interfacing addressing example.....	25

ESKOM COPYRIGHT PROTECTED

Table 12: Interface allocation	25
Table 13: Prioritization selection for various applications.....	26
Table 14: Mapping of applications to service levels	27
Table 15: List of differentiated services codepoint field values	28
Table 16: Differentiated services code point to class of service mapping.....	30
Table 17: Spanning tree protocol and multiple spanning tree instances settings	30
Table 18: Multiple spanning tree region	31
Table 19: Bridge priorities example	31
Table 20: IP routing	31
Table 21: Dynamic host configuration protocol server and client.....	32
Table 22: Trunking/Link aggregation example	33
Table 23: Security settings	33
Table 24: Power over Ethernet settings	33
Table 25: Internet group management protocol settings.....	34
Table 26: DHCP.....	35
Table 27: Storm Control.....	35
Table 28: Router hardware example	38
Table 29: Router naming	38
Table 30: Software versions	38
Table 31: Software versions	38
Table 32: Shorewall firewall settings example	40
Table 33: SNMP management information bases applicable to substation devices	42

1. Introduction

Eskom's migration into substation automation systems has necessitated the development of a network architecture that is congruent with the requirements of both current and future technologies. The network technology of choice for the Substation Automation standard, namely [7] IEC 61850, is industrially hardened switched Ethernet.

Switched Ethernet is a flexible networking technology and allows for numerous implementation solutions. Modern substation equipment ranging from Intelligent Electronic Devices (IEDs) to Cameras and Telephony communicate over Ethernet networks.

Real-time messaging for protection tripping needs to be treated differently to typical Supervisory Control and Data Acquisition (SCADA) data or jitter and latency sensitive telephony. Although the various technologies can be accommodated on a single converged networking technology, cognizance shall be taken of the very different requirements pertaining to each technology.

For this reason, a scalable and flexible design shall be considered when designing the network architecture for modern technologies and for solutions that are still on the horizon, taking into account the differing needs of the various technologies. One such requirement is based on Eskom's technology strategy for substation protection and control equipment for the Transmission and Distribution "wires" business that requires the splitting of protection schemes into largely autonomous modules per "main". Modules for Main 1 and Main 2 shall offer fully redundant functionality. This standard shall also cater for the associated network architecture.

2. Supporting Clauses

2.1 Scope

2.1.1 Purpose

The purpose of this document is:

- a) To present a substation automation network architecture standard for Eskom's Transmission substations.
- b) To define design specifications and design quality considerations.
- c) To provide an application design reference to assist users with implementing the most suitable technical solution for specific substation applications.

This document also includes the content intended to supersede the Substation Automation – Network Application Design Guide (TGL 41-684).

2.1.2 Applicability

This document shall apply throughout Eskom Holdings SOC Limited Transmission Division.

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

- [1] ISO 9001 Quality Management Systems.
- [2] IEEE 802, Series of standards
- [3] IEEE 1588, Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
- [4] IEEE 1613, Environmental Standards for Networking Devices Installed in Electric Power Substations

ESKOM COPYRIGHT PROTECTED

- [5] IEC 61000-6-2, Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments
- [6] IEC 61800-3, Adjustable speed electrical power drive systems – Part 3: EMC requirements and specific test methods
- [7] IEC 61850, Communication networks and systems in substations, Parts 1-14
- [8] IEC 61850-9-2, Sampled values over ISO/IEC 8802-3
- [9] TIA/EIA 568A, Building telecom cabling standards
- [10] RFC 2328, Specification of the Open Shortest Path First (OSPF) TCP/IP internet routing protocol
- [11] 240-61224248, Protection, Telecontrol and Substation Automation Technology direction for the Wires business
- [12] 240-75757022, Overview of requirements for Transmission Protection, Telecontrol and Substation Automation equipment
- [13] 240-57855742 Secure Remote Access System Standard Specification for Field IED Access
- [14] 240-46263618, Labelling of Fibre Optic Cables Standard
- [15] 240-46264031, Fibre optic Design Standard – part 2 Substations.
- [16] 240-64100247, Standard for Earthing of Secondary Plant Equipment in Substations
- [17] 01-Auto-Application, Automation Application Design Guide for Conco Solution
- [18] 240-72274830, Multimode Fibre Optic Duct Cable specification
- [19] 240-70733995, Optical Distribution Frame/Patch Panel/Patch Box Standard
- [20] 240-62772955, IP Address Allocation Standard for Substation Based OT Systems

2.2.2 Informative

Not applicable

2.3 Definitions

2.3.1 General

Definition	Description
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.
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.
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.
Station Level	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.

ESKOM COPYRIGHT PROTECTED

Definition	Description
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.

2.3.2 Disclosure Classification

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

2.4 Abbreviations

Abbreviation	Description
ACL	Access Control List
AF	Assured Forwarding
BCU	Bay Controller or Bay Control Unit
BPDU	Bridge Protocol Data Unit
Cat6	Category 6 U Unshielded Twisted Pair (UTP) or Shielded Twisted Pair (STP) cable
CoS	Class of Service
CU	Currently Unused
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DSCP	Differentiated Services Code Point
DTR	Delay, Throughput, Reliability
DVR	Digital Video Recorder
EADS	Engineering and Data concentrator Solution
EF	Expedited Forwarding
EMI	Electromagnetic Interference
GARP	Generic Attribute Registration Protocol
GM	General Manager
GMRP	GARP Multicast Registration Protocol
GMT	Greenwich Mean Time
GPS	Global Positioning System
HMI	Human–Machine Interface
I/O	Input/Output
ID	Identifier
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers

Abbreviation	Description
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LAN	Local Area Network
LAP	List of Accepted Products
LLDP	Link Layer Discovery Protocol
M&C	Metering and Control
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
N/A	Not Applicable
NMS	Network Management System
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PC	Personal Computer
PHB	Per-hop Behaviour
PoE	Power over Ethernet
PTM&C	Protection, Telecoms, Metering and Control
PTP	Precision Time Protocol
QoS	Quality of Service
RSTP	Rapid Spanning Tree Protocol
RTU	Remote Terminal Unit
SC	Steering Committee
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
ST	Straight Tip/Bayonet [fibre-optic connector]
STP	Shielded Twisted Pair/Spanning Tree Protocol
ToS	Type of Service
UPS	Uninterruptible Power Supply
UTC	Coordinated Universal Time
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

2.5 Roles and Responsibilities

It is the responsibility of Transmission Grids to ensure compliance to requirements as captured in this document.

This document shall be applied by both Project Engineers and Applications staff for Transmission specific projects.

2.6 Process for monitoring

Not applicable

2.7 Related/Supporting Documents

Not applicable

3. Network architecture

3.1 Network architecture overview

3.1.1 General

The design of the substation automation network architecture as presented in this document is primarily based on a two-tier design. The top tier consists of high-capacity, high-speed backbone Ethernet switches that provide the physical connectivity only to the lower-tier switches. The lower-tier switches consist of lower capacity network switches that provide physical connectivity to the bay Intelligent Electronic Device (IEDs), Gateway(s), Human–Machine Interface(s) (HMI(s)), routers and other equipment.

3.1.2 Objectives

The primary justification for this architecture is to ensure that standardized, cost-effective, reliable and scalable substation automation networks are implemented in Eskom's substations using current technology and are in line with industry best practice.

The objectives are to:

- a) Provide the physical and logical network topologies of all equipment and systems proposed.
- b) Provide for a communications infrastructure for the substation automation network in order to ensure system performance requirements are met and to provide for resilience against possible component or system failures.
- c) Enable the provision of real-time network information to operators and automation engineers, which can also be integrated into the HMI systems.
- d) Provide for a centralized Network Management System (NMS) for the management of the automation network. The NMS is also required to provide configuration management for the network device configurations and the firmware for each network device.
- e) Provide for secure remote and corporate access to the substation automation network for system engineers and specialists [13].

3.1.3 Criteria

The fundamental design criteria for the implementation of the substation automation networks are high availability, high reliability and maintainability:

- a) High availability is achieved by means of a redundant device and cabling design where this is practically achievable.

- b) High reliability is achieved by product selection based on industrial networking principles and guidelines. The products selected have met certain minimum build quality and design quality criteria.
- c) Maintainability is achieved through suitable network monitoring and configuration management.

3.2 Environmental design parameters

The substation automation networks shall be built using ruggedized industrial Ethernet technology, which is compliant with the following requirements:

3.2.1 Rated for reliable operation in harsh electrical environments

- a) Class C3, as per [5] IEC 61000-6-2 part 1 Table 1; except for temperature.

3.2.2 Rated for error-free operation in high electromagnetic interference environments

- a) [4] IEEE 1613 Class 2 error-free performance under Electromagnetic Interference (EMI) stress for fibre-based networking devices.
- b) Fibre-optic ports shall support both short- and long-haul fibre.

3.2.3 Rated for operation over a wide temperature range

- a) Operate within the temperature range of -40 °C to 85 °C (+185 °F), with passive cooling.
- b) CSA/UL 60950 safety approved to +85 °C (+185 °F).

3.2.4 Rated for high availability

- a) Integrated dual redundant power supplies.
- b) Wide input range: $U_{DC} = 48\text{ V}$ (88 V to 300 V).
- c) Dual power supplies shall be powered independently, from different input supplies.

3.2.5 Rated for industrial installations

- a) Galvanized steel enclosure for durability and impact protection.
- b) Heavy-duty steel DIN rail mount or 19" rack mountable.
- c) Industrial terminal blocks for power and Input/Output (I/O) connections.

3.3 Network architecture for a single control room

This topology caters for the application where the Main 1 and Main 2 protection IEDs are integrated into a single scheme. The architecture of the substation automation network is based on a switched Ethernet design using a hierarchical approach and a redundant backbone with redundant cabling between the backbone switches and the lower-tier switches, as shown in Figure 1. This dual-star topology between the lower tier and the backbone switches provide a flexible upgrade path and installation simplicity.

Redundant switches and ethernet links are a core design factor of the network and as such, the minimum number of backbone switches is always two. In this scenario, where possible, effort should be made to create a mirror LAN network using the redundant links.

The dual backbone design offers strong resilience and low failover time. The IEEE 802.1w Multiple Spanning Tree Protocol (MSTP) or Rapid Spanning Tree Protocol (RSTP) is used for redundancy management.

The lower-tier switches are not redundant, as this does not offer sufficient benefit considering (a) the cost of such a solution and (b) that many IEDs do not currently provide for redundant network connections.

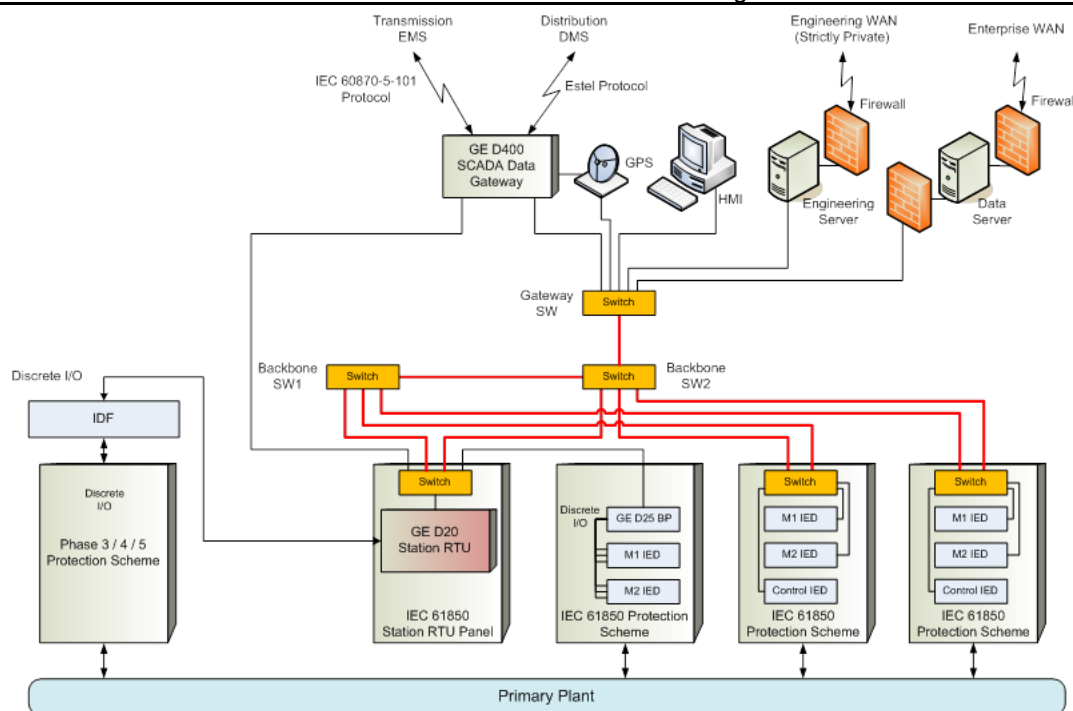


Figure 1: Network architecture for a single control room

3.4 Network architecture for a segregated control room

The new design philosophy for dual main protection and control systems lends itself to the concept of a segregated control room for new substations. The segregated control room includes areas designated for main 1 equipment, main 2 equipment and a central common area for single main and station-level equipment. The intention is that the three control room areas are galvanically separate (as far as is practically possible) with their only interaction being via Ethernet-based communication.

The topology of the substation automation network is basically the duplication of the network topology for the single control room. However there is no redundant cabling between the backbone switches and the lower-tier switches due to the redundancy requirement being catered for by the duplication of the equipment (gateways, GPSs, HMIs, separate protection schemes, etc) in this design. The network resilience to port, cable or switch failure is catered for by the other autonomous main protection scheme.

Detailed information of the application design is shown in the Automation Application Design Guide for Conco Solution [17] and the Automation Application Design Guide for Siemens Solution (still to be developed).

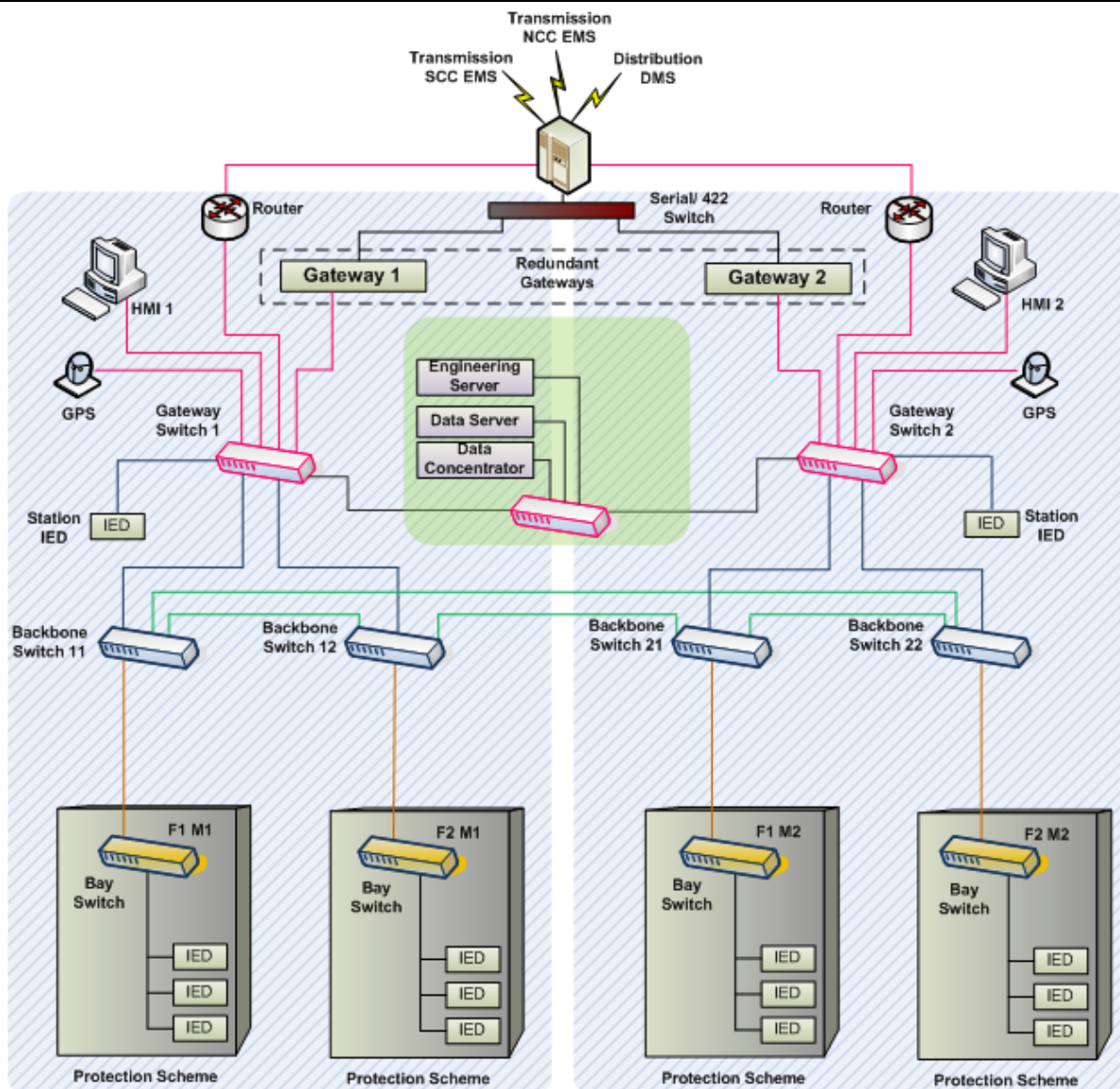


Figure 2: Network architecture for a segregated control room

4. Network application detailed design

4.1 Introduction

The detailed application design provides the specific details of the substation automation network as it would apply to the specific substation application and refers to details that need to be noted to ensure that the equipment is configured, installed and commissioned in line with Eskom standards, guidelines and templates.

4.2 Physical Environment

The physical environment specifically relating to the substation automation system must be taken into account. Typical examples include the number of control systems at the substation; the available DC power supplies present at all the control rooms at the substation as well as any other details that may be pertinent. All networking equipment shall be supplied by dual 50 VDC, 110 VDC, or 220 VDC supplies. Equipment power requirements such as loading shall also be documented to ensure that either the existing battery systems or, in the case of a greenfield substation, the new battery system can adequately cater for the new network equipment loading.

4.2.1 Equipment Housing

Typically, all networking equipment shall be rack mounted in a dedicated cabinet. As a standard installation, the Gateway switch and Router(s) shall be mounted in the Gateway/D400 cabinet, the Station switch in the D20 cabinet or Common Equipment Panel, and the Backbone switches in the Fibre Switching Panels (FSP). All Bay level switches shall be installed in the relevant protection schemes cabinets or condition monitoring cabinets.

All network equipment shall either be 19" rack mountable or din rail mountable and shall be mounted with a minimum of 4 rack screws. Where relevant, exceptions need to be noted and documented.

Due to the nature of networking infrastructure, cable management shall allow for flexibility and changes. Cable management within the cabinet shall be provided by horizontal and vertical cable management. To help support cabling vertically in the rack an enclosed trunking system shall be used.

Grounding/earthing of electronic equipment is essential for safety and to ensure the EMC integrity of the equipment. Equipment shall be directly grounded via the grounding bus bar in the panel via grounding earth points. Grounding wires shall not be looped with other equipment. Refer to the latest revision of the Eskom standard: Standard for Earthing of Secondary Plant Equipment in Substations [16].

A drawing of the layout of equipment shall be provided for each panel. The drawing is to include a cable block indicating power cables and their terminations as well as network cables. Cable numbering and labelling shall be reflected on the cable block diagrams.

4.2.2 Cable Entry and Termination

Typically, all cables are to enter the substation automation system panels from the base of the panels and shall be glanded with double compression type glands complete with necessary armour clamp (for armoured cables) and tapered washer, etc. The cable gland shall match with the different types of power, control and fibre-optic cables with appropriately-sized cable glands. Glanding of fibre optic cables shall conform to The Fibre optic Design Standard – part 2 Substations [15].

Power cable cores shall be lugged with suitably sized crimp lugs and terminated in suitably sized screw terminals. Main 1 and Main 2 DC supplies are to supply equipment within the panel via independent and appropriately rated miniature circuit breakers (MCBs). AC supply to the panel shall also be provided through appropriately rated MCBs.

4.2.3 Cabling

The use of copper cable for Ethernet connections is discouraged and shall be limited to interlinks between switches and devices contained within the gateway panel, and in such cases shall be Category 6 (Cat6) STP cables. Other copper cabling shall only be used for temporal engineering access. Copper patch leads shall be terminated as per [9] TIA/EIA 568A.

4.2.4 Fibre Cables and Fibre Termination

All fibre cables shall adhere to the following guidelines:

- a) The Eskom standard: Fibre optic Design Standard – part 2 substations [15] shall be adhered to for fibre cables that are installed within a control building, fibre cables that are routed between buildings as well as (or) for fibre cables that are terminated in outdoor equipment.

ESKOM COPYRIGHT PROTECTED

-
- b) For interfacing of networking equipment that are in separate cabinets, fibre cables shall be used.
 - c) The network fibre cabling shall be 12 core, 50 μm /125 μm , A1a.2 multimode fibre-optic cable (100BASE-FX) for connections to edge devices; connections are to use LC-type connectors on the switch side and the appropriate connector on the edge device side (typically Straight Tip (ST) connectors). Fibre cable connections between backbone switches are to use 50 μm /125 μm multimode fibre-optic cables (1000BASE-SX)/patch leads with LC-type connectors.
 - d) The connection between the lower-tier switches and the IEDs/Network devices shall make use of multimode fibre patch leads (typically ST connectors on the IED/Network devices side).
 - e) For termination of fibre-optic cables between cabinets, an intermediate patch panel is to be used at both ends. The cables shall be terminated with LC connectors and the patch panel/mid-coupler shall be LC/LC.
 - f) The fibre cables that are installed shall adhere to the Multimode Fibre Optic Duct Cable specification [18].
 - g) Only single length ducts shall be used.
 - h) The patch panel or patch box used shall conform to the requirements stipulated in the Optical Distribution Frame/Patch Panel/Patch Box Standard [19]
 - i) The fibre cables that are installed within the control room shall be installed on a dedicated fibre cable trays that needs to be installed about 500mm below the computer flooring within the Control room, the Diameter Marshalling Kiosk (DMK), or other outdoor buildings. If the installation is being done in an old control room where there are no computer floors, then the installation shall adhere to Fibre optic Design Standard – part 2 Substations [15].
 - j) The identification and labelling of the cables shall be as per the Labelling of Fibre Optic Cables Standard [14].
 - k) Fibre cables details shall be documented on the LAN architecture drawing, the fibre schedule, as well as the Fibre Scope of Work. The fibre cable, number of fibres, termination patch panel, cable number, cable routing, and other relevant information shall be documented.

4.2.5 Fibre Patch Leads

- a) Fibre patch leads shall only be used within panels. No patch leads may be used between panels unless the panels form part of a panel suite and in such cases the fibre patch lead shall be suitably ruggedized and routed in the bus-wiring conduits or fibre cable trays.
- b) Where connections are made between a switch to the patch panels or between patch panels, within the same cabinet, a patch lead with an LC connector on both ends shall be used.
- c) Patch leads shall have the same core and cladding sizing as the cables they shall connect to. In most cases this shall be 50/125 μm multimode fibre.
- d) The patch leads shall preferably have the same connector on both ends to simplify ordering and spares holding. In cases where this is not possible, the “switch side” or “patch panel side” of the fibre patch lead shall use LC-type connectors and the appropriate connector shall be used for the edge device.
- e) Fibre patch leads details shall be documented on the LAN architecture drawing, the fibre schedule, as well as the Fibre Scope of Work. The fibre cable, number of fibres, termination patch panel, cable number, cable routing, and other relevant information shall be documented.

4.2.6 Cooling

All active electronic equipment generates a certain amount of heat that should be effectively removed. Typically all the active equipment shall be cooled via air conditioning units in the substation building.

In order to correctly size air-conditioning units, the amount of heat that the equipment shall produce when in operation shall be documented. The unit of measure is the British Thermal Unit and is expressed as a quantity over time i.e. BTU/hr.

4.2.7 Environmental Monitoring

Where the application warrants environmental monitoring, the details shall be specified. Typically, environmental elements such as ambient air temperature and humidity are not monitored via dedicated sensors however there may be instances where such monitoring is deemed essential. All monitoring equipment specified for such purposes shall be SNMP-manageable.

4.3 Devices to be connected

The devices that have been identified that will require connectivity to the network are listed here. It should be noted that some devices are only to be catered for as and when the requirement for the relevant technologies presents itself within Eskom.

4.3.1 Protection and multifunction intelligent electronic devices

There shall be a single network connection to IEDs via fibre-optic cable. This is due to multiple vendors not yet supporting full redundancy on multiple ports. This will be reviewed once redundant ports are available.

4.3.2 Substation gateways

There shall be dual network connections to substation gateways via fibre-optic cables to two different switches, namely the gateway switch and the station switch.

In the dual control room scenario, there shall be 2 redundant substation gateways; each will be connected to its gateway switch.

4.3.3 Station remote terminal units

There shall be a single network connection to Station Remote Terminal Units (RTUs) via fibre-optic cable.

4.3.4 Station IED

In the dual control room scenario, there shall be no station RTU. The station IED shall perform the function of the station RTU and shall be connected to the gateway switch.

4.3.5 Global positioning system receivers with embedded network time protocol servers

There shall be a single network connection to Global Positioning System (GPS) receivers with embedded Network Time Protocol (NTP) servers via Shielded Twisted Pair (STP) cable or via fibre-optic cable where supported.

4.3.6 Disturbance recorders

There shall be a single network connection to disturbance recorders via fibre-optic cable.

4.3.7 Under Frequency Load Shedding (UFLS)

There shall be a single network connection to UFLS IED via fibre-optic cable.

4.3.8 Meters

There shall be a single network connection to meters via STP cable or via fibre-optic cable where supported.

4.3.9 Engineering laptops

There shall be a single network connection to engineering laptops via STP cable.

4.3.10 Test sets

There shall be a single network connection to test sets via fibre-optic cable or via STP cable when fibre connections are not possible or practical.

4.3.11 Tele-protection systems

There shall be a single network connection to tele-protection systems via fibre-optic cable.

4.3.12 Condition-based monitoring systems

There shall be a single network connection to condition-based monitoring systems via fibre-optic cable.

4.3.13 Internet protocol cameras (future)

There shall be a physically separate network for Internet Protocol (IP) cameras via fibre-optic cable.

4.3.14 Human-machine interfaces

There shall be a single network connection to Human-machine Interfaces (HMIs) via STP cable or via fibre-optic cable where supported.

4.3.15 IP telephony systems (future)

There shall be a physically separate network for IP telephony systems via STP cable or via fibre-optic cable where supported.

4.3.16 Routers

There shall be dual network connections to routers via fibre-optic cables to two different switches, namely the gateway switch and the substation switch.

4.3.17 Data servers

There shall be a single network connection to data servers via STP cable or via fibre-optic cable where supported.

4.3.18 Engineering servers

There shall be a single network connection to engineering servers via STP cable or via fibre-optic cable where supported.

4.3.19 Authentication servers

There shall be a single network connection to authentication servers via STP cable or via fibre-optic cable where supported.

4.3.20 Bay level controllers

There shall be a single network connection to bay level controllers via fibre-optic cable.

4.3.21 Quality of supply meters

There shall be a single network connection to quality of supply meters via fibre-optic cable.

4.3.22 Travelling wave fault locators

There shall be a single network connection to travelling wave fault locators via fibre-optic cable.

4.3.23 Security and access control systems (future)

There shall be a physically separate network for security and access control systems via fibre-optic cable.

4.3.24 Merging units and intelligent switchgear

There shall be dual network connections to merging units and intelligent switchgear via fibre-optic cable.

4.4 Network design parameters

4.4.1 Overview

This section of the document deals with the overall network design parameters.

- a) The core LAN connectivity for the substation automation network is provided by a number of backbone switches. The number shall be determined by the specific design.
- b) The backbone switches shall be ordered to provide for the following minimum requirements:
 - 1 x RJ45 Twisted Pair data port for engineering access
 - 2 x multimode fibre ports with LC connectors for backbone interlinks (operating at 1Gbps)
 - Sufficient multimode fibre ports with LC connectors for bay switch connectivity (operating at 1Gbps).
- c) The gateway and substation switches shall provide for the following:
 - 1 x RJ45 Twisted Pair data port for engineering access,
 - 1 x RJ45 Twisted Pair port for the Time Synchronisation Unit (in the case of the gateway switch for the single control room scenario),
 - 2 x multimode fibre ports with LC connectors for uplink connections to the backbone switches (at 1Gbps), and
 - Sufficient multimode fibre ports with LC connectors for edge device connectivity (e.g. RTUs, HMIs, Gateways, etc).
- d) Bay level, diameter or edge switches shall provide for the following:
 - 2 x RJ45 Twisted Pair ports for engineering access,
 - 1 x RJ45 Twisted Pair per external Disturbance Recorder,
 - 2 x multimode fibre ports with LC connectors for test equipment,
 - 2 x multimode fibre ports with LC connectors for uplink connections to the backbone switches (at 1Gbps),
 - Sufficient multimode fibre ports with LC connectors for IED connectivity.

4.4.2 Hardware

Information pertaining to all the network equipment that is deployed in the substation automation network must be recorded. Typical information includes equipment part number, equipment order code (if different from the part number), the description of the equipment, the quantity and the location of the equipment. An example is shown in Table 1.

Table 1: Hardware description

Part No	Description	Qty	Bay Detail
RSG22200 Backbone Network Switch RSG2200-R-RM-HIP-HIP-FG01-FG01-FG01-FG01-CG01	Backbone Switch 1 (single control room)	1	Fibre Switching Panel
RSG2488 Backbone Network Switch 6GK6024-8GS23-3DA0-Z A0x+B05+C05+D05+E05+F0x+G60+H61	Backbone Switch 1 (segregated control room)	1	Fibre Switching Panel

4.4.3 Power Supplies

Each switch shall be powered by dual station DC supplies for switches installed in schemes and by the dual 48/110/220 VDC supplies for the Gateway, substation and backbone switches. Each switch shall have a dedicated, appropriately rated miniature circuit breaker for the M1 supply and a separate miniature circuit breaker for the M2 supply. An example of the power terminations for a switch is shown in Table 2.

Table 2: Power termination on the switch

Terminal #	Description	Usage
1	PS1 Live / +	PS1 Live / + is connected to the M1 48/110/220 VDC positive (+) terminal via a miniature circuit breaker.
2	PS1 Surge Ground	PS1 Surge Ground is connected to the Chassis Ground via a jumper on the terminal block. Surge Ground is used as the ground conductor for all surge and transient suppression circuitry.
3	PS1 Neutral / -	PS1 Neutral / - is connected to the M1 48/110/220 VDC negative (-) terminal via a miniature circuit breaker.
5	PS2 Live / +	PS2 Live / + is connected to the M2 48/110/220 VDC positive (+) terminal via a miniature circuit breaker.
6	PS2 Surge Ground	PS2 Surge Ground is connected to the Chassis Ground via a jumper on the terminal block. Surge Ground is used as the ground conductor for all surge and transient suppression circuitry.
7	PS2 Neutral / -	PS2 Neutral / - is connected to the M2 48/110/220 VDC negative (-) terminal via a miniature circuit breaker.
4	Chassis Ground	Chassis Ground is connected to the equipment <i>ground bus</i> for DC inputs. Chassis ground connects to both power supply surge grounds via a removable jumper.
8	Relay NO Contact	Normally open, failsafe relay contact.
9	Relay Common	Failsafe relay common contact.
10	Relay NC Contact	Normally closed, failsafe relay contact.

A similar table shall be provided for any other network equipment types such as routers, terminal servers, etc.

4.4.4 Firmware and software versions

All firmware and software version numbers shall be recorded by the equipment type and version number. Table 3 illustrates an example.

Table 3: Firmware/Software versions

Device Type	Model number	Firmware/Software version
Backbone switch	RSG2200	v3.7.1
Bay Level Switches	RSG2100	v3.7.1
Router	RX1100	ROX v1.14.1

4.5 Network configuration

4.5.1 Device Naming

All devices shall be allocated a unique device name. Table 4 illustrates the example below shall be used to document the allocated names. These names shall also be used on network drawings in order to unambiguously identify devices.

Table 4: Device naming example

Device Type	Hostname	Location
Backbone switch	StnA-sas-b-sw01	StnA SAS Backbone Switch 1
Gateway switch	StnA-sas-gw-sw01	StnA SAS Gateway Switch 1
HMI Server 1	StnA-sas-hmi01	StnA SAS HMI 1
Gateway	StnA-sas-gw01	StnA SAS Gateway 1
Data Concentrator	StnA-sas-dc01	StnA SAS Data Concentrator 1
Protection IED	StnA-sas-ma-obj1-ied1	StnA SAS Diameter MA Object 1 M1 IED

4.5.2 LAN switch port speed and duplex configuration

In order to minimize potential problems with device connectivity, the Local Area Network (LAN) speed and duplex settings indicated in Table 15 are recommended:

Table 5: Configuration and duplex settings for substation automation networks

Device	Connection	Speed/Duplex
HMIs, gateways, and engineering servers	All devices fixed	100 Mbps/Full
Backbone interlinks and trunks (uplinks or backhaul links)	Trunk connections	1 000 Mbps/Full
IEDs, BCUs, I/O devices	All devices fixed	100 Mbps/Full
Engineering PCs	All devices set to auto-negotiate	Auto/Auto

4.5.3 VLAN overview

A virtual LAN (VLAN) is a group of devices on one or more LAN segments that communicate as if they were attached to the same physical LAN segment. Configured VLANs are based on logical instead of physical connections. When VLANs are introduced, all traffic in the network must belong to a VLAN. Traffic on one VLAN cannot pass to another, except through an internetwork router or Layer 3 switch. A VLAN tag is the identification information that is present in Ethernet frames in order to support VLAN operation.

4.5.3.1 VLAN numbering and allocations

The automation network shall be configured for at least nine port-based Virtual Local Area Networks (VLANs) as indicated in Table 6:

ESKOM COPYRIGHT PROTECTED

Table 6: VLAN allocations

VLAN	VLAN ID	Description
Network Devices (Management)	VLAN ID (unique substation-specific pre-allocated ID)	Reserved for the network switches and substation router(s).
Substation Automation Devices	VLAN ID (unique substation-specific pre-allocated ID)	Devices that are included in this range are Protection IEDs, Substation Data Gateway(s), Station RTU(s), GPS receivers with embedded NTP servers, Tele-protection devices, HMIs, Bay Level Controllers and Terminal Servers.
IEC 61850 Process Bus Communications	VLAN ID (unique substation-specific pre-allocated ID)	Devices in this range would include intelligent switchgear and merging units.
IP Telephony	VLAN ID 1001	IP Telephones and VoIP gateways (future).
IP Cameras	VLAN ID 1002	IP cameras and Digital Video Recorders (DVRs) (future).
Engineering Purposes	VLAN ID 1003	Includes devices such as Disturbance Recorders, Engineering Workstations, Engineering Laptops, Test Sets, Condition-based Monitoring systems, Dissolved Gas Analysers, Terminal servers, Authentication servers and Travelling Wave fault locators.
Security and Access Control Systems	VLAN ID 1004	Caters for security and Access Control systems (future).
SCADA	VLAN ID 1005	May be used in future for IP-based real-time communications to the control centres.
	VLAN ID 1100-1105	One or more VLANs for WAN links.
	VLAN ID 3	Intra-bay GOOSE messages.
	VLAN ID 4	Inter-bay GOOSE messages.
Engineering Access	VLAN ID 1010	Caters for the engineering access for the Engineering and data concentrator system (EADS). This VLAN will be used in cases where a local Engineering Workstation does not exist and the substation user has to use his laptop to attempt the connection to the Substation Engineering Server using the Remote Desktop Protocol (RDP).
Remote Engineering Access	VLAN ID 1011	Caters for the remote engineering access for the Engineering and data concentrator system (EADS). This VLAN will be used to accommodate remote traffic to the EADS system. This includes traffic between the data concentrator and the enterprise historian, traffic between the data concentrator and the enterprise engineering server and traffic between the substation engineering server and the enterprise engineering server.
Local Engineering Access	VLAN ID 1012	Caters for the local engineering access for the Engineering and data concentrator system This VLAN will be used to accommodate traffic between the EADS system and substation network. This will include all Data Concentrator communication to Substation devices as well as the Job execution and remote engineering access communication.

The “1000” range is used for both the single control room scenario as well as when the dual main protection schemes are used to create the concept of the segregated control room.

ESKOM COPYRIGHT PROTECTED

The unique substation-specific Identifiers (IDs) will be allocated by Protection, Telecoms, Metering and Control (PTM&C) applications.

GOOSE multicast MAC addresses shall be of the form 01-0C-CD-01-ab-cd, where the range for ab is 00 to 01 and cd is 00 to FF. 'ab' shall relate to the feeder number, 'c' is the relay number and 'd' is the GOOSE number.

4.5.3.2 Inter-VLAN routing

In a network which is designed with VLANs as described in 4.5.3, different IP subnets need to be allocated to each VLAN. Routing between VLANs is only possible where a VLAN-aware router is installed in the network environment.

The configuration of the router's virtual interfaces shall associate an IP address with a VLAN interface that is identified by its VLAN ID. Once all these virtual interfaces are defined, routing shall be possible as the router is 'connected' to all the relevant virtual LANs.

4.5.3.3 VLAN definitions and IP Addressing

The substation IP address map shall be documented and displayed on the network architecture drawing. The VLAN ID, the name of the VLAN as configured on the switches, the VLAN description and the IP address range corresponding to the VLAN ID are documented as shown in the example in Table 7. Note that for security reasons, VLAN ID 1 is not used.

Table 7: VLANs and IP addressing example

VLAN ID	VLAN Name	Description	IP Network	Gateway
1	Default	SHUTDOWN – Not used	SHUTDOWN	SHUTDOWN
1016	Man_Vlan	Substation Management VLAN	10.0.16.0 / 23	10.0.16.1
1018	SAS_Vlan	Substation Automation VLAN	10.0.18.0 / 23	10.0.18.1
1003	Eng_Vlan	Engineering VLAN	10.0.21.0 / 26	10.0.21.1
		Unallocated	10.0.21.128 / 25	
		Unallocated	10.0.22.0 / 23	
2201	WAN1_Vlan	Wide Area Network 1 VLAN	10.0.0.48 / 29	10.0.0.49

The VLAN definitions for the GOOSE messages are shown in Table 8.

Table 8: GOOSE VLAN allocations

VLAN ID	VLAN Name	Description	Multicast	Priority
3	GOOSE1_Vlan	Intra-bay GOOSE messages are tagged with this VLAN ID	See GOOSE message configurations section	6
4	GOOSE2_Vlan	Inter-bay GOOSE messages are tagged with this VLAN ID	See GOOSE message configurations section	6

The details of the VLAN definitions and IP addressing are documented in Substation Automation Network Standard (TST 41-1077).

4.5.3.4 VLAN operation

All switches shall be made VLAN aware. Switches add the Port VLAN ID (PVID) to an ingress (incoming from the device) Ethernet frame as per the IEEE 802.1Q standard. Such frames are known as tagged frames and hence carry the relevant VLAN ID as part of the Ethernet frame as shown in Figure 3.

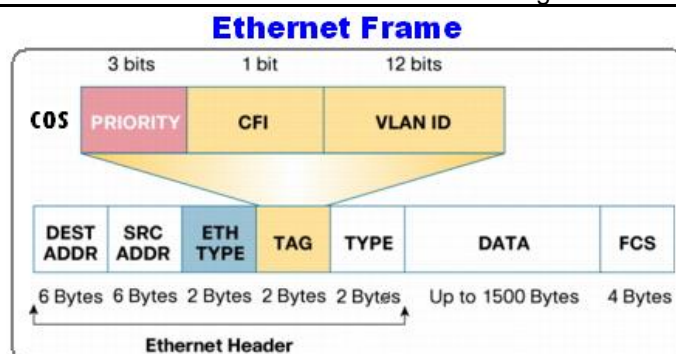


Figure 3: Tagged Ethernet Frame

The VLAN ID is stripped from the Ethernet frame when it is egressed (transmitted) to an edge-device on a port that is configured to be an edge port. If the port is configured as a VLAN trunk port, the Ethernet frame is transmitted with the tag intact.

A port on a switch is defined as an edge port when it attaches to a single end device (such as a HMI or IED) and carries traffic on a single pre-configured VLAN, the native VLAN. Trunk ports are part of the network and carry traffic for all VLANs between switches. Trunk ports are automatically members of all VLANs configured in the switch.

In general, all inter-switch links shall be configured as VLAN trunks. In addition, due to the nature of the IEC 61850 GOOSE messaging where devices tag frames natively, links to Intelligent Electronic Devices (IEDs), Bay Control Units (BCUs), and I/O Units shall be configured as VLAN trunks. All other ports shall have VLAN trunking specifically turned off.

4.5.3.5 GOOSE message configurations

Table 9 lists the typical configuration information that applies to GOOSE messages. The details shall be described in the application document and are intended to assist with commissioning and fault finding.

Table 9: GOOSE message configurations

Field	Description
GOOSE Source Device	This name is as per the network architecture drawings and application documentation, e.g. StnA-sas-ma-obj1-ied1 is the StnA Substation Automation System IED number 1 of Object number 1 within Diameter MA.
Source Device Type	Type of device - preferably an order code to differentiate between similar devices, e.g. ABB REC670.
Message Name	This field is limited to 16 characters. First 5 characters i.e. {1..5} = Substation abbreviation e.g. StnA for StnA, {6..8} = Scheme number / Bay number / Diameter number e.g. scheme 5 is S05, {9..16} = Descriptive reference e.g. PlantIn1.
Description	Free format field for descriptive text.
Goose ID	Similar to Message Name but with underscores separating the fields for easier readability.
Configuration Revision	This number shall be incremented every time a change is made.
Dataset	The dataset containing the signals that is associated with the GOOSE control block.
Multicast MAC Address	The first 4 bytes of the multicast MAC address is fixed (01-0C-CD-01). The fifth byte shall identify the feeder/bay number e.g. 03 is for feeder 3. The first 4 bits of the sixth byte shall identify the IED producing the GOOSE message while the second 4 bits of the sixth byte shall be a sequential number beginning from 1 for each GOOSE message generated by the same IED.

Field	Description
APP ID	The APP ID is a 2 byte field and shall be the same as the fifth and sixth bytes of the Multicast MAC Address.
VLAN ID	The VLAN ID shall be used to manage the flow of GOOSE messages in the substation. The available VLAN ID range is from 1 (0x1) to 4095 (0xFFF). For GOOSE messages the VLAN ID shall be 3 (0x3) for intra-bay GOOSE messages and ID shall be 4 (0x4) for inter-bay GOOSE messages. The remainder IDs in the 2 (0x2) to 50 (0x32) range shall be used for all other GOOSE messages as required.
VLAN Priority	The VLAN priority is a 3 bit field. Higher priority frames have values in the range of 4 to 7 and lower priority frames from 1 to 3. Priority 6 is preferred for high priority GOOSE messages and 0 is not to be used for GOOSE messages.

4.5.3.6 VLAN configurations

The switch port configurations related to the VLAN details are recorded in a separate table for each switch in the network. The example shown in Table 10 lists the port number, the hostname of the attached device, the VLAN ID associated with the attached device (Port VLAN ID), the format of the PVID (tagged or untagged), the VLAN connection type (trunk or edge), the tagged VLAN traffic allowed through a trunk port, and the mode of the GARP VLAN Registration Protocol (GVRP) for the port. GVRP is set to advertise and learn for connections between switches and is disabled for connections to edge devices.

Table 10: VLAN configuration example

Port	Device	Port VLAN ID (PVID)	PVID Format	Type	Permitted VLANs	GVRP
1						
2	StnA-sas-gw-sw01	1016	Tagged	Trunk	All	Adv & Learn
3						
4	StnA-sas-stn-sw01	1016	Tagged	Trunk	All	Adv & Learn
5	StnA-sas-b-sw02	1016	Tagged	Trunk	All	Adv & Learn
6	StnA-sas-ma-sw01	1016	Tagged	Trunk	All	Adv & Learn
7	StnA-sas-b-sw03	1016	Tagged	Trunk	All	Adv & Learn
8						
9						
10						

4.5.4 Interface Addressing

Network equipment interfacing details shall be recorded in a table as shown in the Table 11. The device is identified by the hostname and information related to IP addressing, subnet masks and the VLAN ID.

Table 11: Interfacing addressing example

Hostname	Interface	IP Address	Mask
StnA-sas-b-sw01	Vlan 1016 (Management Interface)	10.0.16.#	255.255.254.0
StnA-sas-ma-sw01	Vlan 1016 (Management Interface)	10.0.16.#	255.255.254.0
Devices connected to StnA-sas-ma-sw01 – interface addressing			
StnA-sas-ma-obj1-ied1	Vlan 1018 (SAS Interface)	10.0.18.#	255.255.254.0
StnA-sas-ma-obj1-ied2	Vlan 1018 (SAS Interface)	10.0.18.#	255.255.254.0
Devices connected to StnA-sas-stn-sw01 – interface addressing			
StnA-sas-rx01	Vlan 1018 (SAS Interface)	10.0.18.#	255.255.254.0
	Vlan 1001 (IP Telephony)	10.0.20.#	255.255.255.128
	Vlan 1002 (IP Cameras)	10.0.20.#	255.255.255.128
	Vlan 1003 (Engineering)	10.0.17.#	255.255.255.192
	Vlan 1004 (Access Control/Security)	10.0.17.#	255.255.255.240
	Vlan 1005 (SCADA)	10.0.17.#	255.255.255.224
	Vlan 1010 (Engineering Access)	10.0.17.#	255.255.255.208
	Vlan 1011 (Remote Engineering Access)	10.0.17.#	255.255.255.192
	Vlan 1012 (Local Engineering Access)	10.0.17.#	255.255.255.176
StnA-sas-stn-rtu1	Vlan 1018 (SAS Interface)	10.0.18.#	255.255.254.0

4.5.5 Interface Allocation

Network switch details shall be recorded for each switch. An example for the interface allocation of a typical backbone switch is shown in Table 12 below. The table shall list the interface module type, the slot number occupied by the interface module, the port number, the device attached to the port, the interface name on the attached device as well as the port description which is configured in the switch port configuration.

Table 12: Interface allocation

Module	Slot	Port	Device	Device Interface	Port Description
FG01	1	1			
FG01	1	3			
FG01	2	2	StnA-sas-gw-sw01	Port 9	StnA-sas-gw-sw01
FG01	2	4	StnA-sas-stn-sw01	Port 9	StnA-sas-stn-sw01
FG01	3	5	StnA-sas-b-sw02	Port 5	StnA-sas-b-sw02
FG01	3	7	StnA-sas-b-sw03	Port 5	StnA-sas-b-sw03
FG01	4	6	StnA-sas-ma-sw01	Port 9	StnA-sas-ma-sw01
FG01	4	8			
1CG01	6	9	Engineering		Engineering
No port	6	11			

4.5.6 Network quality of service policies

The following policies shall be applicable:

- Quality of Service (QoS) is required to ensure appropriate marking and treatment of Substation Automation traffic and normal data across the network. QoS is implemented in tagged Ethernet frames to provide prioritization of traffic on a switched Ethernet network as defined in IEEE 802.1p ([1] ISO 9001 Quality Management Systems.
- IEEE 802).
- QoS is also implemented in the IP header, which is designed to give end-to-end prioritization of traffic which may need to travel over multiple LAN and WAN links.
- The network has been designed to provide 1000 Mbps throughput between the core (backbones) and the lower-tier switches, although an effective 100 Mbps is achievable end-to-end. QoS shall be implemented to prevent oversubscription of backhaul links and prioritize real-time traffic. This is achieved by means of Ethernet prioritization as per the IEEE 802.1Q standard ([1] ISO 9001 Quality Management Systems.
- IEEE 802).
- Class of Service (CoS) is the classification of specific traffic (at Layer 2) by manipulating the CoS bits (in the frame header). It effectively 'marks' the traffic so that QoS can use this identification/classification as a means to actually manipulate the traffic.
- Priority to CoS Mapping is the mechanism whereby the three priority bits in the Ethernet frame as per IEEE 802.1Q ([1] ISO 9001 Quality Management Systems.
- IEEE 802) are mapped to the broader categories of Critical, High, Medium and Normal. The fair-weighted queuing philosophy shall be implemented allowing lower priority frames to be transmitted in a ratio of 8:4:2:1, thereby allowing fair access to all traffic priorities without negatively impacting the higher priority frames. Table 3 shows the prioritization selection for various applications:

Table 13: Prioritization selection for various applications

Priority*	CoS	Typical application
7	Critical	Network management (applied to management VLAN)
6	High	GOOSE messages used for tripping and inter-tripping purposes
5	Medium	GOOSE messages used for interlocking purposes Merging units
4	Medium	GOOSE messaging used for purposes other than tripping or interlocking
3	Medium	Substation Automation purposes (applied to Substation Automation VLAN)
2	Normal	Engineering purposes (applied to Engineering VLAN)
1	Normal	Quality of Supply metering
0	Normal	Security systems, meters, IP cameras
*7 is highest priority and 0 is lowest priority.		

4.5.7 IP traffic prioritization and differentiated services

This solution leverages the new Internet Engineering Task Force (IETF) definition of the IPv4 Type of Service (ToS) octet in the IP header by utilizing the Differentiated Services Code Point (DSCP) field to classify packets into any of the 64 possible classes. The packet classification determines the routers' treatment of the packet as per IETF-defined Per-hop Behaviours (PHBs) including Assured Forwarding (AF) and Expedited Forwarding (EF). Traffic that is characterized as EF shall receive the lowest latency, jitter and assured bandwidth services, which is suitable for applications such as Voice over Internet Protocol (VoIP). AF is a means for offering different levels of forwarding assurances for IP packets received. The AF PHB guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, if available. AF allows carving out the bandwidth between multiple classes in a network according to desired policies.

QoS policies shall allow critical applications to receive the appropriate portion of resources, while ensuring other applications are not neglected. By classifying the application traffic into premium, gold, silver and other classes as shown in Table 14, a baseline methodology is set to provide end-to-end QoS. Differentiated Services (DiffServ) enables this classification by utilizing the DSCP field. Using DiffServ, a properly designed network can deliver assured bandwidth, low latency, low jitter and low packet loss for voice while simultaneously ensuring slices of available bandwidth to other classes.

Table 14: Mapping of applications to service levels

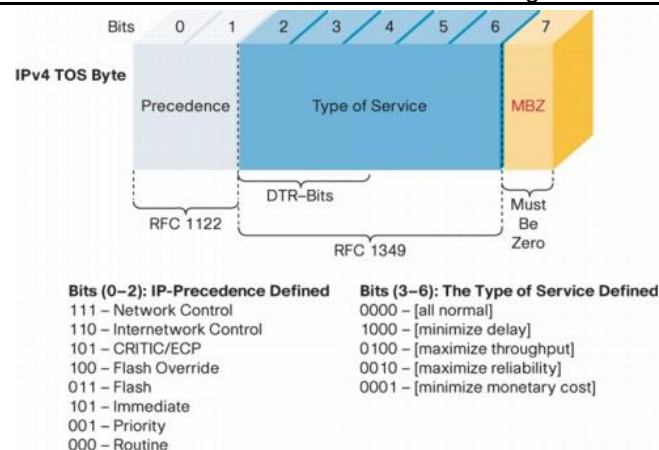
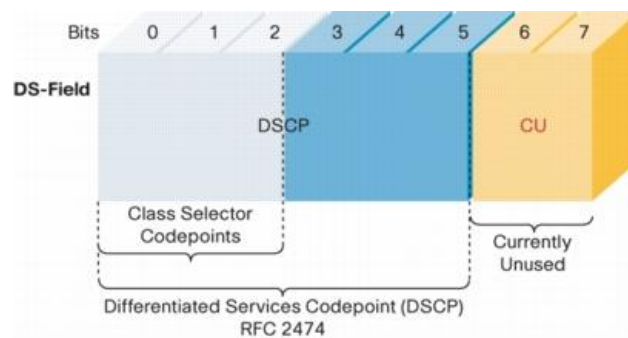
Application	Service
SCADA/Automation	Gold
Management	Silver
Undefined	Bronze
Data	Best Effort

4.5.7.1 Packet classification

Packets entering a DiffServ domain or region (collection of DiffServ routers) can be classified in a variety of ways, including Layer 4 protocol and port numbers, IP precedence and Layer 2 information (such as Ethernet 802.1Q bits). Once these packets are classified on the basis of the criteria mentioned in 4.5.7, they can be processed, conditioned and marked.

4.5.7.2 Packet marking

The IPv4 ToS octet has been redefined from the three-bit IP-precedence to a six-bit DSCP field (Figure 3). Packets can be marked with an arbitrary DSCP value or predefined standard values, corresponding to the appropriate AF (Figure 4), EF or user-defined class. For example, in Table 15, EF is designated by the codepoint '101110'. The codepoint for best-effort traffic shall be set to '000000'.

**Figure 4: Original IPv4 type of service byte****Figure 5: Differentiated services codepoint field****Table 15: List of differentiated services codepoint field values**

Name*	Dec	ToS	Binary
AF11	10	40	001010
AF12	12	48	001100
AF13	14	56	001110
AF21	18	72	010010
AF22	20	80	010100
AF23	22	88	010110
AF31	26	104	011010
AF32	28	112	011100
AF33	30	120	011110
AF41	34	136	100010
AF42	36	144	100100
AF43	38	152	100110
CS1	8	32	001000
CS2	16	64	010000
CS3	24	96	011000

**SUBSTATION AUTOMATION – NETWORK
ARCHITECTURE AND APPLICATION DESIGN
STANDARD FOR TRANSMISSION SUBSTATIONS**

Unique Identifier: **240-61268959**

Revision: **3**

Page: **29 of 43**

Name*	Dec	ToS	Binary
CS4	32	128	100000
CS5	40	160	101000
CS6	48	192	110000
CS7	56	224	111000
EF	46	184	101110
Default	0	0	000000
AF = Assured Forwarding, EF = Expedited Forwarding, CS = Class Selector			

The DSCP mappings shown in Table 6 are typical of VoIP telephony systems. Additional mappings would need to be defined as applications are implemented.

Table 16: Differentiated services code point to class of service mapping

DSCP	CoS
40	6
46	6

4.5.8 Spanning tree

The topology of the substation automation network for a single control room (as shown in Figure 1) and dual control room (as shown in Figure 2) designed to rely on a consistent spanning tree topology to ensure network resilience to port, cable or switch failure.

Spanning tree is also required as a precaution against incorrect patching and future changes, and shall be configured in the following way:

- For point to point links, the Backbone switch shall be the root bridge.
- To counter workstation, IED and Gateway connectivity delay issues, all end-node switch ports shall be configured as an edge port with spanning tree and Bridge Protocol Data Unit (BPDU) guard enabled (if available). All other switch ports, including those not yet in use, shall be configured as edge ports with spanning tree enabled.
- When a switch port is enabled, it shall go through the normal spanning tree process of listening/learning/forwarding. The forwarding and learning performed by each Bridge Port for each spanning tree is dynamically managed by Multiple Spanning Tree Protocol (MSTP) to prevent temporary loops and reduce excessive traffic in the network, while minimizing denial of service following any change in the physical topology of the network.
- For switch ports that are connected to known end stations, this process can be perceived to be superfluous. Setting a port as an edge port with spanning tree disabled allows a port to avoid the listening and learning process so that it moves directly to the forwarding state. The risk with such a setting is that spanning tree loops can be inadvertently created, particularly if a port that has spanning tree disabled is used on a link between switches. This setting is therefore not recommended.
- All edge ports shall be configured as edge ports with Spanning Tree enabled.

4.5.8.1 Multiple spanning tree protocol

The MSTP will be used. MSTP enables VLANs to be grouped into a spanning tree instance and provides for multiple forwarding paths for data traffic. MSTP provides the same redundancy features as RSTP, while providing load balancing across the Multiple Spanning Tree Instances (MSTIs).

The VLAN ID to MSTI mapping is as shown in **Table 7** and is configured as such on all switches:

Table 17: Spanning tree protocol and multiple spanning tree instances settings

VLAN ID	VLAN name	Description	MSTI
Station specific	Mgmt_VLAN	Network Devices VLAN	4
Station specific	SAS_VLAN	Substation Automation Devices VLAN	1
Station specific	Process_VLAN	Process Bus VLAN	6
1001 or 2001	Tel_VLAN	IP Telephony VLAN	5
1002 or 2002	Cam_VLAN	IP Camera VLAN	6
1003 or 2003	Eng_VLAN	Engineering VLAN	2

VLAN ID	VLAN name	Description	MSTI
1004 or 2004	Access_VLAN	Access Control/Security VLAN	6
1005 or 2005	SCADA_VLAN	SCADA VLAN	6
1010 or 2010	EngAccess_VLAN	Engineering Access	5
1011 or 2011	RemoteEng_VLAN	Remote Engineering Access	5
1012 or 2012	LocalEng_VLAN	Local Engineering Access	5
3	IntraBayGOOSE	Intra-bay GOOSE	3
4	InterBayGOOSE	Inter-bay GOOSE	3

The MST Region Identifier for the network is configured as shown in **Table 8** on all the switches:

Table 18: Multiple spanning tree region

Name	Revision Level
“StationName”	0

The settings of the Bridge Priorities are dependent on the number of backbone switches that are installed in the LAN network. **Table 9** shows an example of the bridge priority settings for a network LAN with four backbone switches:

Table 19: Bridge priorities example

MSTI	Bridge with priority 0 (root bridge)	Bridge with priority 4096	Bridge with priority 8192	Bridge with priority 12288	Bridge with priority 32768
1	Backbone Switch 3	Backbone Switch 1	Backbone Switch 2	Backbone Switch 4	All lower-tier switches
2	Backbone Switch 2	Backbone Switch 4	Backbone Switch 1	Backbone Switch 3	
3	Backbone Switch 1	Backbone Switch 3	Backbone Switch 4	Backbone Switch 2	
4	Backbone Switch 4	Backbone Switch 2	Backbone Switch 3	Backbone Switch 1	
5	Backbone Switch 2	Backbone Switch 4	Backbone Switch 1	Backbone Switch 3	
6	Backbone Switch 3	Backbone Switch 1	Backbone Switch 2	Backbone Switch 4	

4.5.9 IP Routing

The information related to inter-VLAN routing and the WAN routing is specified in a table as per the example in Table 20. This configuration applies to the substation router and details the router's hostname, the routing protocol in use for the portion of the routing table described, and the routing entries associated with the portion of the routing table described.

Table 20: IP routing

Device	Routing protocol	Route Entries
StnA-sas-rx01	Connected	VLAN 1016, 1018, 1001, 1002, 1003, 1004, 104, 1010, 1011, 1012
StnA-sas-rx01	Connected	VLAN 2201
StnA-sas-rx01	OSPF	Dynamically learned from neighbouring routers

ESKOM COPYRIGHT PROTECTED

If OSPF shall be used as a WAN routing protocol, the OSPF area to be applied to the router shall be specified.

4.5.10 Dynamic host configuration protocol

The Dynamic Host Configuration Protocol (DHCP) is used to allocate IP addresses dynamically to devices that are not permanently connected to the network. Such devices include engineering laptops and Test sets. The DHCP server ensures that the devices are allocated unique addresses and that there is no risk of duplicate addresses appearing on the network. Typically, the DHCP servers that shall be used in the substation environment are the Engineering Server as the authoritative server and the router as the backup and hence non-authoritative server on the network. In the event that the Engineering Server is not available, then the router becomes the authoritative server. All permanently attached devices shall be allocated static IP addresses.

All devices shall be allocated static IP addresses, as indicated in Table 21, where # is the substation-specific IP addresses as determined by the IP address plan.

Table 21: Dynamic host configuration protocol server and client

Device	Function	Address range	Netmask	Gateway
Router	Server	10.##.129	255.255.255.255	10.##.1
StnA-sas-es01	Server (Authoritative)	10.##.10 (static)	255.255.255.255	10.##.1
Engineering Computers	Clients	10.##.140- 10.##.200	255.255.255.128	10.##.1

4.5.11 Trunking/Link Aggregation

Link aggregation bundles according to IEEE 802.3ad are typically configured across multiple switch ports which have identical configuration (e.g. the same VLAN information and the same trunk information). They are used to increase the backhaul/link capacity.

Each bundle shall be desirable at one end, and auto at the other. The backbone switch shall be configured as the desirable end. If the link is horizontal (e.g. the link between two backbone switches) then the switch with the lower numeric identifier shall be set to desirable.

The group number shall be a unique number on the switch. For a point to point link with a single VLAN the group number should be configured to be the same as the VLAN of the link. If the link is a trunk, then the VLAN ID of the native VLAN should be used. Where the same set of trunked VLANs are configured on multiple bundles on the same switch, then once the native VLAN has been used, all the other VLANs should be used in order.

Link Aggregation Control Protocol (LACP) is required and the reason is to standardise the direction of the LACP negotiation is such that the bundles are all configured consistently on each switch. When trouble shooting, any anomaly should be easier to detect and correct without the need for logging on to both ends of every link.

Care shall be taken that if the group number already exists on the switch that the original ports and the new ports do not end up in the same group.

The details that are recorded for link aggregation are as per the Table 22. The affected switched are listed by hostname in the "Device" columns, the interfaces to be bundled in the "Interfaces" column and the associated channel number in the "Channel Number" column.

Table 22: Trunking/Link aggregation example

Device	Interfaces	Channel Number	Device	Interfaces	Channel Number
StnA-b-sw01	7,9	1	StnA-b-sw02	3,4	2

It shall be noted that there are no envisaged link aggregation applications at this stage.

4.5.12 LAN switch port security settings

The implementation of multiple security layers is considered good practice when implementing substation automation networks. The LAN Switch port security settings shall be as indicated in **Table 1123**:

Table 23: Security settings

Device	Security setting/connection	Option
HMLs, Gateways, Time servers, Data Concentrators and Engineering Servers	No security setting shall be configured on all switch ports which connect to HMLs, Gateways, Time Servers, Data concentrator and the Engineering Server.	Port security MAC Address Autolearn set to 1. MAC Address age upon link loss set true.
Trunks (uplinks or backhaul links)	No security setting shall be configured on trunk ports.	None.
IEDs, BCUs, I/O Devices	No security setting shall be configured on all switch ports which connect to IEDs, BCUs and I/O devices.	Port security MAC Address Autolearn set to 1. MAC Address age upon link loss set true.
Backbone Interlinks	No security setting shall be configured on all backbone interlink switch ports	None.
Engineering PCs	No security setting shall be configured on all switch ports which connect to engineering PCs. Substation users requiring access to IEDs will utilise the Engineering Workstation SCP to first attempt such connection using the Substation Engineering Server (SSC)..	A substation-based Authentication Server is deployed in the form of a Read Only Domain Controller (RODC) which replicates the Enterprise Active Directory infrastructure securely. This server will facilitate authentication requests by users local to the substation and will also synchronise to the Enterprise Active Directory.
Unused Ports	Administratively shutdown.	None.

The Autolearn setting specifies how many MAC addresses the switch should learn on the port. A value of 1 limits the switch to only learning 1 MAC address per port. It is therefore important to set the 'Aging upon Link Loss' option under the 'MAC Address Learning Options' to true.

4.5.13 Power over Ethernet configuration

Power over Ethernet (PoE) is implemented using separate PoE injectors for IP Telephony purposes where necessary. As indicated in **Table 1224**, the Power over Ethernet option will not be used:

Table 24: Power over Ethernet settings

Device	Interfaces	PoE available	PoE power per port	Maximum PoE power per device
-	-	No	0 W	0 W

4.5.14 Internet group management protocol

The Internet Group Management Protocol (IGMP) is a communications protocol that provides a way for an IP host to report its multicast group membership to any immediately neighbouring multicast routers. Multicasting allows one IP host on the Internet to send content to multiple other IP hosts that have identified themselves as interested in receiving the originating IP host's content.

IGMP snooping is a method by which Layer 2 devices can 'listen in' on IGMP conversations between hosts and routers. When a switch hears a 'group join' message from a host, it notes which switch interface it heard the message on, and adds that interface to the group. Similarly, when a Layer 2 switch hears a 'group leave' message or a response timer expires, the switch will remove that host's switch interface from the group.

All switches shall be set up to carry out IGMP snooping. Although the IEC 61850 standard ([7] IEC 61850) does not use IP multicasting (GOOSE uses only Ethernet multicasting), it is considered important to enable the IGMP snooping nonetheless, as there may be other applications which may require IP multicasting at a later stage. The router shall perform the function of the multicast router, and IGMP snooping on the switches shall be configured as passive (i.e. no switch shall be configured as a querier or active).

Table 1325 shows the IGMP settings.

Table 25: Internet group management protocol settings

Device	IGMP configuration
Router	<ul style="list-style-type: none"> Query Interval (1-65535 s) – 30 Max Response Time (1-25 s) – 10 Robustness Value (1-255) – 2 Last Member Query Interval (1-25 s) – 1 Host Timeout (1-16711450 s) – 260 Router Timeout (1-16711450 s) – 260 Leave Timer (0-16711450 s) – 2 Querier State – enabled Querier Router Behaviour – querier State – enabled
Backbone switches	<ul style="list-style-type: none"> Mode: Passive Query Interval: 60 s Router Ports: 9, 11 Router Forwarding: On RSTP Flooding: On Enable IGMP on all statically defined VLANs
Bay/Edge switches	<ul style="list-style-type: none"> Mode: Passive Query Interval: 60 s Router Ports: 1, 2 Router Forwarding: On RSTP Flooding: On Enable IGMP on all statically defined VLANs

4.5.15 GARP multicast registration protocol

The GARP Multicast Registration Protocol (GMRP) shall not be used in this application to perform multicast filtering.

4.5.16 Network security enhancements

4.5.16.1 Dynamic host configuration protocol snooping

DHCP Snooping is used to prevent a rogue DHCP server from issuing IP addresses to clients. Specific interfaces are configured to allow DHCP servers. All other interfaces are configured to deny all DHCP offer messages.

Table 26: DHCP

Device	Port	DHCP server
Gateway switch	3	Substation router
Gateway switch	13	Engineering Server

4.5.16.2 Spanning tree root guard

Root guard provides a way to enforce the root bridge placement in the network. If another switch appears on the network and has a better metric than the current spanning tree root, its port shall be disabled.

Root guard shall be enabled on all compatible switches.

4.5.16.3 Storm control

Storm Control restricts the number of broadcast and/or multicast packets which could inundate a network and degrade its overall performance.

Table 27: Storm Control

Device	Multicast flood level	Broadcast flood level
Switch	Not set	1 000

Storm Control shall be enabled on all compatible switches. The Port Rate Limiting parameter shall be set to an Ingress limit of 1 000 kbps for broadcast frames.

4.5.17 Link layer discovery protocol

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 network protocol that allows connected equipment to share information about other directly connected equipment such as the operating system version and IP address.

LLDP shall be configured on all links between network equipment and disabled on all connections to IEDs, HMIs, time servers, BCUs and Engineering ports.

4.5.18 Network IP addressing and device allocations

The IP Addressing Allocation for the Substation Automation Networks is based on the Eskom IP Address Allocation Standard for Substation Based OT Systems [20].

IP addressing for substation automation devices shall utilize the 10.0.0.0 /8 (8 bit network mask) private IP address range. The following approach shall be applied for address allocation to a substation based on the VLAN allocations described previously.

A substation would be allocated a /21 subnet of the 10.0.0.0/8 IP range. For example, 10.4.80.0/21 may be allocated to Substation A and the IP address ranges are further allocated as follows:

- 10.4.80.0/25 is allocated to the management VLAN for network device addressing.
- 10.4.80.128/25 is allocated for Engineering services.

- 10.4.81.0/27 is allocated to (future) IP-based Supervisory Control and Data Acquisition (SCADA) devices.
- 10.4.81.32/27 is allocated to (future) Access Control and Security systems.
- 10.4.81.64/27 is allocated to Engineering Access.
- 10.4.81.96/27 is allocated to Remote Engineering Access.
- 10.4.81.128/27 is allocated to Local Engineering Access.
- 10.4.81.160/27 is unallocated.
- 10.4.81.192/26 is unallocated.
- 10.4.82.0/23 is allocated to Substation Automation Devices.
- 10.4.84.0/25 is allocated to IP telephony.
- 10.4.84.128/25 is allocated to (future) IP Cameras.
- 10.4.85.0/24 is unallocated.
- 10.4.86.0/23 is allocated to Process Bus devices.

Graphically, this IP address map can be represented as shown in Figure 6.

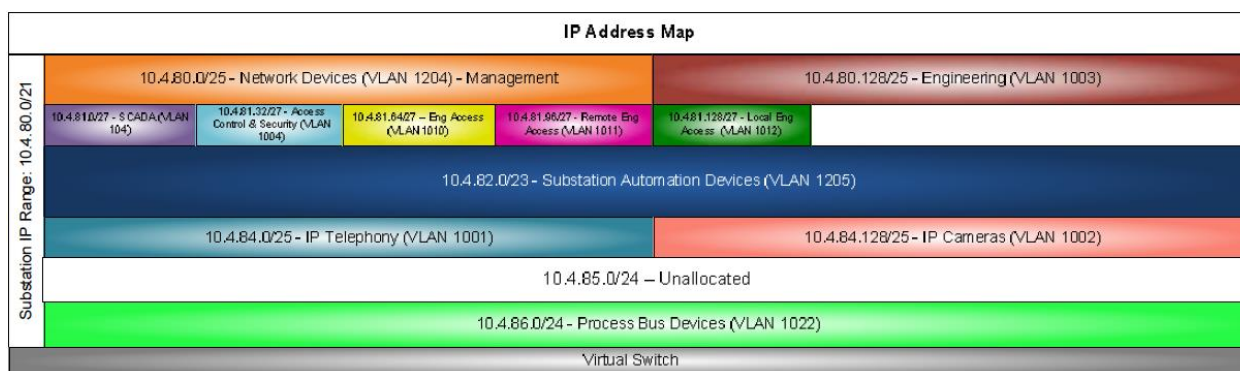


Figure 6: Graphical representation of a typical substation IP address map

4.5.19 IP address management

IP address management is to be handled by the Group Technology PTM&C Applications section.

4.5.20 Routing requirements and wide area network interfacing

The Wide Area Network (WAN) routing standard shall be Open Shortest Path First (OSPF) Version 2, as described in [10] RFC 2328. Dynamic routing is considered essential to managing an enterprise-wide routing environment, as it minimizes the administrative burden of managing routing tables and provides for dynamic path fail-over in cases of link loss or other routing metrics as configured.

4.5.21 Network time synchronization

Eskom's substations are in the time zone 'South African Standard Time' with an offset of +2 h from Greenwich Mean Time (GMT)/Coordinated Universal Time (UTC). Daylight saving is not observed in South Africa and is therefore not considered for time synchronization purposes.

4.5.22 Network time protocol

The Network Time Protocol (NTP) is to be used for device time synchronization for devices that support this mechanism. Devices that do not support NTP shall use direct time synchronization via IRIG signalling from the GPS receiver.

The primary NTP server shall be the GPS receiver if it has an embedded NTP server. The Stratum 0 device (GPS receiver) shall synchronize the Gateway via IRIG-B, which shall in turn be an alternative NTP time source for synchronizing devices within each VLAN.

In cases where the GPS receiver does not support NTP, the GPS shall be required to synchronize the gateway via IRIG-B input, which shall in turn be the network NTP time source. Devices in such a Substation Automation network are to be configured to point to the gateway for NTP.

4.5.22.1 IEEE1588

This standard is also known as the Precision Time Protocol (PTP) and is designed to provide high-precision time to industrial networked applications where NTP does not necessarily provide adequate precision, and where GPS signals may not be directly accessible.

The use of such a timing system is considered a future requirement, as it is expected to be used for Process Bus [8] IEC 61850-9-2 networks and is facilitated by [3] IEEE 1588 Version 2, which allows for transparent clocks through IEEE 1588 aware network equipment.

4.5.23 Change control policy

It is Eskom policy to manage the life cycle of all substation automation systems and networks, as they are critical to meeting business and technical objectives. The management of changes to such production environments is essential to maintaining a quality infrastructure.

The policy shall provide best practice and procedural guidelines that shall be used when making changes to the substation automation system networks.

Before any change can be effected to working systems, the proposed change needs to be evaluated and approved by the PTM&C Applications section.

The change control process needs to meet the following criteria:

- a) A description of the change is required.
- b) An approved plan of action is required, with milestones for implementation of the change showing the sequence of steps required to effect the change; a roll-back plan in case of unforeseen problems; assigned roles and responsibilities; and a post-implementation verification plan.
- c) A test plan is required, showing the results of testing the change in a non-production environment, or providing a reference to a planned feature roll-out plan.
- d) Change approval shall be given by relevant stakeholders, including affected parties such as Control Centres.

4.6 Substation Router

4.6.1 Overview

The substation router shall be configured to subscribe to all VLANs on the network in order to allow traffic from one VLAN to pass through to another VLAN. The application design guide shall document the router configurations and settings as described in the sections below.

4.6.2 Hardware

The router hardware shall be documented as shown in Table 28.

Table 28: Router hardware example

Part No	Hardware Version	Quantity
RX1500-R-RM-HI-HI-XX-XX-TX01-FX11-XXX-XXX	RX1500 V2 (C3)	1
RX1500 - 6GK6015-0AM23-3DC0-Z A03+B06+C00+D00+E01	RX1500 V3	1

4.6.3 Ethernet interfaces

The Ethernet interfaces shall be as follows:

- Ethernet Interface 1 is eth1 (100BASE-TX)
- Ethernet Interface 2 is eth2 (100BASE-TX)
- Ethernet Interface 3 is eth3 (100BASE-FX) – multimode fibre, ST connector
- Ethernet Interface 4 is eth4 (100BASE-FX) – multimode fibre, ST connector

4.6.4 Device Naming

A table such as the example shown in Table 29 shall be used to document the router name.

Table 29: Router naming

Device Type	Hostname	Location
	StnA-sas-rx01	StnA Control Room – Gateway panel 1

4.6.5 Software versions

A table such as the example shown in Table 30 shall be used to document the software version.

Table 30: Software versions

Device	Software version	Role
		Substation Router

4.6.6 Interface Addressing and Allocation

For individual VLAN referencing, the interface is of the form [Ethernet Interface Name].[VLAN ID]. A table such as the example shown in Table 31 shall be used to document the interfacing addressing and allocations.

Table 31: Software versions

Hostname	Interface Type	Interface	IP Address	Mask
StnA-sas-rx01	LAN – VLAN 1001	eth3.1001	10.0.20.#	255.255.255.128
	LAN – VLAN 1002	eth3.1002	10.0.20.#	255.255.255.128
	LAN – VLAN 1003	eth3.1003	10.0.21.#	255.255.255.192
	LAN – VLAN 1004	eth3.1004	10.0.21.#	255.255.255.224
	LAN – VLAN 1016	eth3.1016	10.0.16.#	255.255.254.0
	LAN – VLAN 1018	eth3.1018	10.0.18.#	255.255.254.0
	LAN – VLAN 104	eth3.104	10.0.21.#	255.255.255.240
	WAN – VLAN 2201	eth4.2201	10.0.0.#	255.255.255.248

4.6.7 Enabled Services

The following services shall be enabled on the router via the “Bootup and Shutdown” menu:

- a) dhcp3-server (DHCP Server)
- b) keepalived (VRRP Server)
- c) ntp (NTP Server)
- d) quagga (Routing Protocols including OSPF)
- e) snmpd (SNMP)
- f) snort (Intrusion Detection)
- g) ssh (SSH Server)
- h) webmin (Web Management Interface)

4.6.8 DHCP Server

The following settings shall be changed on the router's DHCP server and documented in the application guide. Settings not specified shall use default values.

- a) Subnet Description: Engineering VLAN
- b) Network Address
- c) Address Ranges
- d) Server is Authoritative for this subnet? Yes

The Client Options setting shall be:

- a) Subnet Mask
- b) Domain name: eskom.co.za
- c) Time Servers
- d) NTP Servers
- e) Default Routers
- f) DNS Servers
- g) NetBIOS Name Servers

In the case of the segregated control room, the pool of IP addresses will be split between the primary and secondary VRRP routers. This will ensure that should the primary router fail; the secondary router will continue serving as a DHCP server.

4.6.9 Router Redundancy

Not used at substation using only a single router.

In the case of the segregated control room, the routers shall be configured with the Virtual Router Redundancy Protocol (VRRP) which is a mechanism that allows the two routers to be configured in a redundant fashion. The primary router (Main 1 system) will service routing while active. If the primary router fails the secondary router (Main system) of the VRRP setup will resume the routing responsibility, in a manner that is transparent to the end devices. This is accomplished by creating a virtual router (which includes a virtual IP address and MAC address). If the primary router fails, the secondary will take over control of the virtual IP and MAC address for the VRRP virtual router.

VRRP in the network design will be implemented as follows:

ESKOM COPYRIGHT PROTECTED

- **Virtual IP:** The IP address for the virtual router will be the first IP in the subnet for each subnet
- **Primary Physical Router:** Will be assigned the second IP in the subnet for each subnet
- **Secondary Physical Router:** Will be assigned the third IP in the subnet for each subnet

4.6.10 Shorewall Firewall

Default firewall policy shall be to deny everything that is not explicitly allowed. Table 3 shows an example of the settings that shall be documented if the firewall capability is used.

Table 32: Shorewall firewall settings example

From	To	Direction	Service	Action	Description
{IP address}	{IP address}	Incoming	TCP/2404	Allow	Allow IEC 60870-5-104 access to gateway 1
{IP address}	{IP address}	Incoming	TCP/2404	Allow	Allow IEC 60870-5-104 access to gateway 2
{IP address}	{IP address}	Incoming	TCP/3389	Allow	Allow remote desktop to Engineering Server
{IP address}	{IP address}	Incoming	TCP/22	Allow	Allow SSH to Engineering Server
{IP address}	{IP address}	Incoming	TCP/22	Allow	Allow SSH to firewall
{IP address}	{IP address}	Incoming	TCP/443	Allow	Allow HTTPS to firewall
{IP address}	{IP address}	Incoming	OSPF	Allow	Allow OSPF to router
{IP address}	{IP address}	Incoming	IPSec	Allow	Allow VPN to firewall
{IP address}	{IP address}	Incoming	IPSec	Allow	Allow VPN to firewall
{IP address}	{IP address}	Outgoing	TCP/25	Allow	Allow outgoing email access only to Eskom email servers
{IP address}	Any	Outgoing	TCP/25	Deny	Deny outgoing email access (prevent spam)
{IP address}	Any	Outgoing	Any	Allow	Allow all other outgoing access
Any	{IP address}	Incoming	Any	Deny	Deny All

All rules that are required shall be developed in conjunction with the Eskom corporate security policies.

For the case of the segregated control room, it is important that all routers in the substation VRRP configuration have the exact same firewall configurations. In the event a primary VRRP router fails and passes control to the secondary router, the secondary router will use its own firewall configuration. This means that if both routers have different firewall configurations, they will each handle traffic differently, which can lead to unexpected issues.

4.6.11 SNMP Configuration

The following settings shall be defined for SNMP and documented in the application guide.

- System Configuration
 - System Name: [Substation Name] Substation Router 1
 - System Location: [Substation Name]
 - System Contact: Eskom Control
 - System Description: [Substation Name] Substation Router 1
- Addresses to listen on:

ESKOM COPYRIGHT PROTECTED

- eth3.1016
- eth3.1003

All other interfaces shall be disabled.

c) **SNMP Trap Configuration**

- Enable authentication traps
- Enable link up/down traps

4.7 Device management philosophy

4.7.1 Management

- a) The managed switches shall provide for Simple Network Management Protocol (SNMP) Version 2c as a minimum. SNMP traps are to be sent to the substation gateway for processing and retransmission to the control centres.
- b) All switches shall have the facility enabled to detect a failure in a single channel on a communications circuit connecting to another switch or to an end device. Twisted pair cables and fibre-optic cables typically employ a separate transmit and receive channel. The switch shall therefore not only be able to detect a complete device disconnection, but also a single channel failure.
- c) SNMP shall be used to collect information and alarms related to environmental, security and performance.

4.7.2 Network alarm and failure notifications

The integration of event, alarm and monitoring data that is collected via the Gateway using SNMP is described in 4.7.6. This shall allow such information to be collected using typical SCADA protocols, and routed to the appropriate alarming point within the relevant control centre such as the 'Comms Desk'. This is the recommended notification path, as the technician dispatch procedures can be adhered to as for any other substation equipment fault.

4.7.3 Network performance monitoring

Network performance monitoring is typically the function of a dedicated NMS as described in 4.7.5. Critical links that would typically require monitoring are the backbone 'uplinks' from the bay level switches to the backbone switches. These connections are required to be high capacity links. Any strain experienced on these links shall highlight the need for possible further optimization or upgrading of capacity.

4.7.4 Contact procedures and notification policies

As described in 4.7.2, the contact procedures and notification policies shall follow the Service Level Agreements as documented between the control centres and the various service providers within the organization. It is expected that network-related faults shall be dispatched to the Grid field staff.

4.7.5 Network management system

The management of the Substation Automation Networks from a centralized point is considered essential. The enterprise-grade NMS platform performs the monitoring, configuring and maintaining of the Substation Automation networks and facilitates the proper management of the networks. The NMS performs a centralized SNMP monitoring service that is also capable of monitoring services on servers and other devices with an SNMP agent. The NMS has the facility to email and/or send SMS notifications as required.

The NMS provides for:

- a) a mechanism to manage all the switch configurations and firmware images;

- b) centralized management and monitoring of network and networked devices to achieve the highest possible desired level of network availability and performance;
- c) a scalable system architecture;
- d) events, alarms and notifications – display network visibility details to enable proactive corrective actions and improved capacity utilization;
- e) pre-packaged reports for availability metrics and performance metrics as well as for providing the tools to create user-defined reports;
- f) have manually configurable thresholds
- g) automated network discovery; and
- h) support for SNMP v1, v2c and v3.

4.7.6 Simple network management protocol management and monitoring

- a) The integration of event, alarm and monitoring data for devices that are ancillary to the automation system (IEDs, etc.) into the SCADA monitoring system is of importance to operational staff.
- b) The devices that provide the network infrastructure, power infrastructure, etc. that can provide data via SNMP shall be visible in the relevant displays, alarm lists and event lists in the SCADA system and the Engineering Server, e.g. Environment Monitoring Equipment, Managed Industrial Ethernet Switches, Routers, Uninterruptible Power Supplies (UPSs), Linux and Windows-based PCs and Servers.
- c) Unmanaged device availability can normally be confirmed by means of device 'pings'.
- d) SNMP shall also be used as a core system status metric. The information to be extracted is as follows:
 - 1) Real data download throughput of each of the backhaul trunks.
 - 2) Real data upload throughput of each of the backhaul trunks.
 - 3) Uptime statuses of all of the edge switch hardware.
 - 4) Packet statistics for each of the switch ports.
 - 5) Packet loss for each of the switch ports.

Table 1433 lists the SNMP Management Information Bases (MIBs) to be employed when communicating with a device:

Table 33: SNMP management information bases applicable to substation devices

Role	Device	SNMP
Client	Gateway	Linux MIBS
Server	Engineering Server	Linux and WinXP MIBS
Client	HMI	Linux and WinXP MIBS
Router	RuggedCom RX1100	RuggedCom MIBS
Switch	Backbone Switches	RuggedCom MIBS
Switch	Lower-tier Switches	RuggedCom MIBS

- e) The SNMP server shall at the very least support SNMP v2c. Other features that are of value would include:
 - 1) Device Auto Discovery (including managed and unmanaged devices).

- 2) MIB Import – provide the facility to import device specific MIB files to allow convenient mapping from MIB addresses to OPC tag names. MIBs would typically be required to access data that may be specific to a device, e.g. the status of a redundant power supply.
- 3) Calculate metrics such as bandwidth utilization and network error rate statistics from raw SNMP data.
- 4) SNMP Traps Support – many SNMP-manageable devices can be configured to send unsolicited data to network management software systems such as NMSs and SNMP servers. This reduces the need for the management systems to continuously poll the devices.

5. Authorisation

This document has been seen and accepted by:

Name and surname	Designation
Sham Dhrampal	Group IT: Corporate Specialist
Prince Moyo	General Manager: Power Delivery Engineering
Mervin Mottian	Dx SCADA Managers Forum Convenor
Prudence Madiba	Senior Manager: Electrical and Control & Instrumentation
Joe Manyisa	Senior Manager: Telecommunications (Acting)
Comfort Masike	Senior Manager: System Operator
Danie Conradie	Senior Manager: Distribution
Lenah Mothata	Senior Manager: Transmission

6. Revisions

Date	Rev	Compiler	Remarks
Nov 2018	3	R Hariram	Document edited to include the dual control rooms design and the Engineering and Data Server solution.
Nov 2013	2	R Hariram	Document edited to include the dual control rooms design. New document template used.
July 2012	1	R Hariram	Document edited to include as-built configurations.
Dec 2009	0	P Diamandis	Initial draft version issued for review.

7. Development team

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

- Peter Diamandis

8. Acknowledgements

Not applicable