

SCM SUBMISSION : SPECIFICATION / SCOPE OF WORK

PURPOSE OF SUBMISSION	Appointment of a Service Provider
DESCRIPTION OF GOODS / SERVICES / WORK	Appointment of service provider for Implementation of Enterprise Network for Passenger Rail Agency of South Africa (PRASA) over a 60 months contract period.
REQUEST FOR PROPOSAL NUMBER	HO/ICT/406/06/2021
DIVISION	PRASA Corporate
USER DEPARTMENT	PRASA Corporate ICT
DATE SUBMITTED	2 May 2021

TABLE OF CONTENTS

- 1. INTRODUCTION**
- 2. BACKGROUND INFORMATION**
- 3. OBJECTIVE OF THE PROPOSED PROJECT**
- 4. SCOPE OF WORKS AND AREAS OF FOCUS**
- 5. SPECIFICATION OF THE WORK OR PRODUCTS OR SERVICES REQUIRED**
- 6. TECHNICAL SPECIFICATIONS RELATED TO THIS PROJECT**
- 7. TIME FRAMES / PROGRAMS**
- 8. NEW PREFERENTIAL PROCUREMENT REGULATIONS**
- 9. EVALUATION METHODOLOGY**
- 10. RECOMMENDATIONS**

ACRONYMS

Abbreviation	Description
PBX	Private Branch Exchange
ISP	Internet Service Provider
DMZ	Demilitarized Demilitarised Zone
DNS	Digital Nervous System
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IDPS	Intrusion Detection and Prevention Systems
LTE	Long-Term Evolution
IPSec	IP Security
HAC	Hierarchical Access Control
SNMP	Simple Network Management Protocol
QOS	Quality of Service
APN	Access Point Name
DTMF	Dual-tone multi-frequency
MetroE	Metropolitan-area Ethernet
WAN	Wide Area Network
MLPS	Multiprotocol Label Switching
POE	Power-Over-Ethernet
SSL	Secure Sockets Layer
ICASA	Independent Communications Authority of South Africa
URL	Universal Resource Locator
WEB	Website
LAN	Local Area Network
MOIP	Modem Over Internet Protocol
NAT	Network Address Translation
PRASA	Passenger Rail Agency of South Africa
RADIUS	Remote Authentication Dial-In User Server
RMON	Remote Monitoring
SLA	Service Level Agreement

SNMP	Simple Network Management Protocol
SSH	Secure Socket Shell
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Networks

Annexures

1. ANNEXURE 1 – SITES LIST
2. ANNEXURE 2 – REGIONAL MAPS
3. ANNEXURE 3 – TECHNICAL COMPLIANCE REQUIREMENT
4. ANNEXURE 8 – BILL OF QUANTITIES / PRICING SCHEDULE

1. INTRODUCTION

The purpose of this project is for PRASA to appoint a suitably qualified service provider for the implementation of enterprise network solution for PRASA in all regions. The scope includes Campus, Data Centre, various offices, Stations, Depots, WAN and MAN networks.

The RFP seeks to establish a 60 months contract. It is the target of PRASA to have the project implementation completed within the first 24 months of the contract. The remaining 36 months will be for the support and maintenance.

2. BACKGROUND INFORMATION

PRASA has built a network that allows the convergence of multiple networks to transport all data service information across single coherent network architecture using PRASA-owned optic fibre network that runs along the railway lines. These data services can be broken down into three different classes:

Business Services

These are the services, which allow local and remote user's access to applications, as well as the transport of Datacentre (DC) application data external to the DC for application communication, data backup, Business Intelligence etc.

ICT Services

These are the services that Prasa internal users require to complete their day to day responsibilities. Examples are SAP, email, internal LAN access, file and print functions, Intranet as well as Internet access, and multimedia communication (telephony, video conferencing, document collaboration etc.).

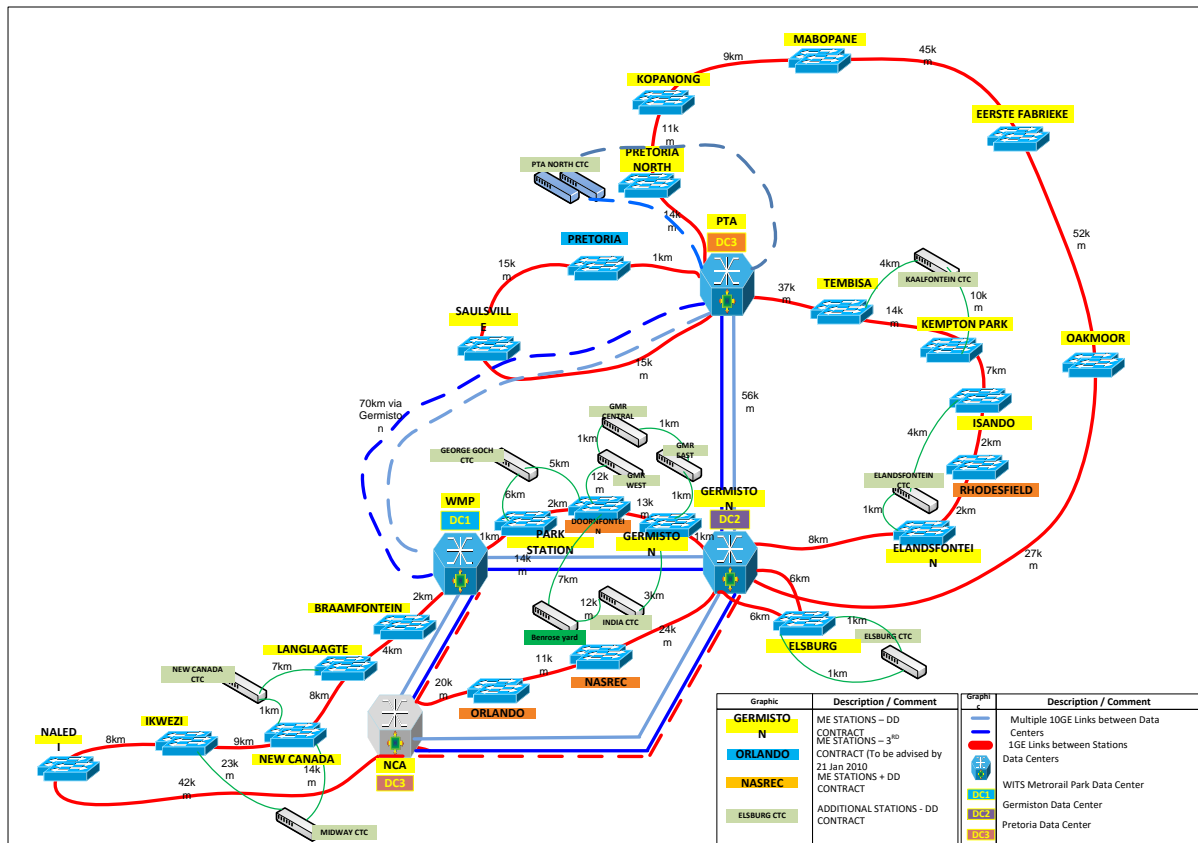
Operational Services

These are the customer facing services which Prasa is deploying to support the business operation and improve the commuter experience. Examples are: Ticketing, CCTV, PA systems, Digital signage, Public Help Points, Access Control, Wireless communications to the new trains etc.

The main objective to bear in mind is to simplify operations and, therefore, lower operating expenses (OPEX), whilst providing the highest levels of services delivery, reliability, bandwidth access, manageability and access to Business Intelligence.

The first phase of the network was commissioned in 2009 and the second phase in 2012.

The network is split into three regions GP, KZN and WC, with each retaining a similar architecture similar to the one below.



The existing Metro Area Network is based on MPLS-IP core with Metro-Ethernet rings connecting Stations and other sites for Gauteng, Western Cape and Kwazulu-Natal regions.

On the backbone, Cisco 7600 nodes run MPLS. The MPLS VPNS are then interworked with VLANs that originate in the metro Ethernet rings that have been formed using the ME3400/ME3600 nodes. These Metro-Ethernet nodes act as CPE on the network. As part of the expansion, 525 IE3000 switches have also been deployed, and they connect to the network via the Metro-Ethernet switches.

The 7600 router is currently acting as MPLS Provider Edge router that performs the following connectivity functions.

- 10G connection to the 6500 switch in the Data centre.
- Aggregates multiple 10G rings
- Aggregates multiple 1G rings.

Unfortunately, these networks have reached end-of-life and end-of-support. As a result, there is a requirement for complete refresh.

3. OBJECTIVE OF THE PROPOSED PROJECT

The objective of the project is the total replacement of the existing PRASA ICT Network environment in all regions. The scope includes Campus, Data Centre, various offices, Stations, Depots, WAN and MAN networks.

The project includes all the Professional Services (Project Management, Consultation, Surveys, Design, Configuration and Training) as well as the supply and implementation of all equipment, software, cabling and associated infrastructure for all the work packages as set out in section 4.

The RFP seeks to establish a 60 months contract. It is the target of PRASA to have the project implementation completed within the first 24 months of the contract. The remaining 36 months will be for the support and maintenance.

The project also includes all the necessary Warranties, Maintenance and Licensing as stipulated. All equipment supplied must be covered with a 3-year warranty and software must be supplied with 3-year software licences. The warranty and software licence term are effective from the milestone sign-off.

The winning bidder will provide the following good and services:

1. Design, Supply and Implement a Next Generation Network
2. Provide Professional Services for
 - a) Architecture and design (high level and Low/Detail level),
 - b) Site surveys WILL be required from the winning bidder.
 - c) Development of network / device configurations.
 - d) Project Management
 - e) Detailed / comprehensive Network Roll-Out Plan.
 - f) Labour for deployment, setup / configuration and commissioning / testing, as well as
 - g) As-built documentation.
3. Provide Cabling and associated services where required (Copper, Fibre and Electrical – Low Voltage)
4. Supply all hardware/software and accessories as may be required.
5. Configure Equipment – Network Staging
6. Deploy and install new network equipment at train stations and other PRASA buildings.
7. Migrate existing Network Services.
8. Decommissioning of Old Equipment.
9. Test and Commission the network, including network services.
10. Provide Detail As-Built Documentation.

4. SCOPE OF WORKS AND AREAS OF FOCUS

The scope of work of the project is subdivided into a number of work packages and the bidder's solution MUST cover all work packages. The summary of the work packages is provided below:

Summary of work packages:

The below work packages are applicable to the regions as follows:

Region	Work Package –A (MAN)	Work Package –B (Datacentres)	Work Package C-H
GP	X	X	X
WC	X		X
KZN	X	X	X
EC			X

4.1 WORK PACKAGE “A”: Next Generation Metro Area Network (MAN) in Gauteng, WC and KZN

Core Layer:

This work package delivers a new Fibre-based Metropolitan Area Network connecting all PRASA stations and depots in the respective regions to the regional Data centres via existing PRASA Fibre infrastructure and redundant DWDM/Dark fibre or third party L2 links.

Aggregation Layer:

This work package delivers a Fibre-based Metropolitan aggregation ring network that connects all PRASA stations and depots in the respective regions and some access rings to the regional MAN Core network via existing PRASA Fibre infrastructure, the redundant underlay transport must be proposed to offer connection redundancy to the stations and Depots

Access Layer:

This work package delivers a Fibre-based Metropolitan access ring network that connects all PRASA stations and sub-stations in the respective regions to the regional MAN Core network via existing PRASA Fibre infrastructure, the redundant underlay transport must be proposed to offer connection redundancy to the stations and sub-stations

4.2 WORK PACKAGE “B”: Next Generation Inter- and Intra- Data Centre Network

This work package delivers a Next Generation Inter- and Intra- Data Centre Network in Gauteng (GNC and Braamfontein) and DR site in Durban. The Next Generation data centre is expected to have the orchestration controller that is able to automate, manage the infrastructure and able to achieve the following:

- hardware discovery

- hardware setup and configuration
- configuration standards and enforcement
- reporting and alerting
- system and application health monitoring
- troubleshooting and resilience tasks

4.3 WORK PACKAGE “C”: Campus/Station Network and WI-FI

This work package seeks the design and replace of all existing ICT network infrastructure in various PRASA campuses/stations across the regions. The network (wired and wireless) should be able to offer data services across single coherent network architecture.

These data services can be broken down into three different classes:

Business Services

These are the services, which allow user access to applications hosted in the Datacentre (DC) and/or in the cloud.

ICT Services

These are the services that PRASA internal users require to complete their day to day responsibilities. Examples are SAP, email, internal LAN access, file and print functions, Intranet as well as Internet access, and multimedia communication (telephony, video conferencing, document collaboration etc.). The other IP devices should be able to connect to their respective controllers via the same campus network, examples IP cameras, smart tvs, video conferencing devices, access control, etc

Building Management

Various Building Management as well as Physical Security technologies will be deployed including Access Control, Smart CCTV, Power Metering etc

The Campus/Station size would be categorised into the following classes based on the size of site or facility:

Office/Site	Size	Class	Devices
Sub-station / Relay Room	0	Sub-station / Relay Room	12 port industrial switch OR 8 port industrial switch + 8-port low capacity station access switch
Small	0-10	Class A	24 Ports POE Switch + 4 APs (indoor/Outdoor)
Medium	>10	Class B	48 Ports POE Switch + 8 APs (indoor/Outdoor)
Campus/Large	>50	Class C	Site specific

4.4 WORK PACKAGE “D”: Network Security

This work package seeks the design a modern, modular, layered approach shall be followed in assuring network and all IP traffic security. The network security solution should be able to protect OSI layer 3-7. The solution should be a holistic end-to-end security for PRASA network, from the Data Centre to the endpoint, remote and local connectivity.

4.5 WORK PACKAGE “E”: Network Management and monitoring Solutions

This work package sees the supply and implement a Tier 1 Network Management and monitoring solutions that is able to ensure visibility of network and application performance, simplify management, securely accessible from anywhere by the support team. The solution that can facilitate granular control of who can access which network device and change the associated network settings and be able to enforce the policy across all network platforms. Wi-Fi controller should be centralised in the data centres able to control all access point in all regions.

4.6 WORK PACKAGE “F”: Cabling and facilities

The project seeks to establish an “as and when” contract for the provision of cabling and facilities related infrastructure such as UPS, poles, cooling, cabinets, etc.

Bidders will be provided with estimate quantities for these items.

4.7 WORK PACKAGE “G”: Training and Knowledge Transfer

This work package sees the provision of OEM accredited training services that will result in certified PRASA Resources to provide Level 1 and Level 2 support at all tiers of the network, on all products supplied for work packages.

4.8 WORK PACKAGE “H”: Network Maintenance and Support – 60 Months

The project also seeks to establish a maintenance and support contract for of ALL **EQUIPMENT AND SOFTWARE APPLICATIONS** deployed in PRASA during this project. The maintenance contract shall provide for the replacement of network components when they fail and the provision of software patches when they become available.



PRASA aims to build an enterprise network that is based on design guidelines stated below.



Following below is the subset of the list of design requirements and objectives.

High Availability (HA) – It shall be an objective for the PRASA Network Design to recover from most network failures without causing data sessions from timing out. HA must address network resiliency, Hardware and Software design to meet PRASA requirements.

11

Availability %	Downtime per year	Downtime per month	Downtime per week
90% aka "one nine"	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% aka "two nines"	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% aka "three nines"	8.76 hours	43.8 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% aka "four nines"	52.56 minutes	4.32 minutes	1.01 minutes
99.999% aka "five nines"	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% aka "six nines"	31.5 seconds	2.59 seconds	0.605 seconds
99.99999% aka "seven nines"	3.15 seconds	0.259 seconds	0.0605 seconds

High Throughput – The network shall be a non-congested network, i.e. it should "always" have enough bandwidth available. That is, if no failure conditions exist in the network (failed router or link); the throughput in the network should never be blocked by the bandwidth capacity of a link, or processing capacity of a router.

Quality of Service - Not all packets require equal treatment in the network. Several traffic classes will be defined and based on the traffic policy, some traffic will have higher priority (better treatment) than the other.

Low Latency – Low Latency is important. In some Industrial-IoT use cases Ultra-Low Latency is expected. The designed network shall be able to deliver data transmission at low latency and Ultra-low latency levels.

Scalability – Aggregation Network shall be scalable in terms of adding new devices per site, or adding new sites (Horizontal scaling), or adding network modules within a device (Vertical Scaling).

New services, which may become relevant at a later phase of the project, shall be possible to be added without any re-design.

In order to achieve these objectives this design shall be based on industry leading practices with regard to physical topology both in a Point of Presence (POP) and between POP's, logical protocol selection and tuning and finally the management infrastructure required to monitor and optimize the network. Particular attention has to be paid to high availability concepts and convergence objectives.

The increase in network performance shall be proportional to the capacity that has been added.

Flexibility – The network design should have adequate flexibility to accommodate future network business critical services. Flexibility to accommodate new services should be achieved without changing or adding hardware. This excludes instances where additional network throughput is required.

The time required to implement additional services or data flows / routes should be as short as possible.

Security – Cyber Security is a critical aspect to any network, even more so to public transport operators. PRASA requires a network solution that includes a multi-layered security solution that addresses cyber security in line with ISO27000 family of standards. Cyber Security is especially important with the emergence of connected industrial devices and sensors are becoming prevalent with the realisation of the 4IR and Industrial-IoT in the Rail industry.

Maintainability: Ease of Maintenance & Support – The design, technologies, techniques and tools utilised as well as the equipment selection shall deliver a network that is easily maintainable in order to keep the network performing at the levels it was designed to do, within the SLA's set. Preference shall be given to equipment that uses Field-Replaceable-Units (FRU's) for components that are likely to fail, especially due to external factors such as power source related events. Field-based physical / visual and graphic-based troubleshooting and diagnostics is important.

Zero-Touch-Provisioning (ZTP) – Equipment should support Zero-Touch-Provisioning especially in the Data center, Distribution/Aggregation and Access Layers of the network.

All software tools shall be provided in order to realise the aspects of Maintainability as set-out above.

Technology Obsolescence – With the ever-increasing speed with which technology is advancing it is critical that the architecture and technology implemented gives PRASA at least a 7 to 10-year refresh horizon. All equipment proposed in the solution must be supported for a minimum of 7 years from installation.

5.2 TECHNICAL SPECIFICATION FOR WORK PACKAGES:

5.2.1 WORK PACKAGE “A”: Next Generation Metro Area Network (MAN) in Gauteng, WC and KZN

5.2.1.1 Core Layer:

5.2.1.1.1 Current Core Network Topology

Core Nodes are inter-connected in a Ring topology

1. The primary core POP routers are configured (located in each data centre site), this these are currently connected using PRASA optic fibre

5.2.1.1.2 Proposed Core Network Topology

Core Nodes should inter-connected in a Full Mesh topology

1. At least two primary core POP routers should be configured (where the Data Centres are connecting), this can be complemented by secondary core POPS (located at core fibre inter-connects).
2. MAN Core Nodes can be interconnected via DWDM technology using both current Prasa fibre and the redundant 3rd party fibre.

5.2.1.1.3 Network Specifications

These requirements cover the hardware capacity and capabilities of equipment to be used in the Metro Area Network Core layers.

TECHNOLOGY	SPECIFICATION
Routers	<p>MAN Core Routers - High Capacity</p> <ol style="list-style-type: none">a. Multi-chassis device 2 route processor module<ol style="list-style-type: none">a.1 With Redundant AC power supplya.2 Redundant processor modulea.3 total system throughput of at least 2.4Tbpsa.4 Redundant System Controllersa.5 hot swappable fan traysa.6 Fiber line cards with 10G/40G/100G links , the total 100 GE ports should up to 10. The total 10GE ports should up to 20b. Intent based Networking capable<ol style="list-style-type: none">b.1 Automation –programmability, ZTPb.2 Security – segmentation and Policyb.3 Analytics – Flexible Netflow, streaming telemetryc. Capable of Routing & Virtualization<ol style="list-style-type: none">c.1 BGP, OSPF, MPLS L2/L3 VPNd. Flexible Network Segmentation<ol style="list-style-type: none">d.1 VRF, VXLAN, MPLS L2VPN, MPLS L3VPNd.2 Segment Routing & EVPN, Flexible Ethernet feature supportd.3 support SRv6 and SRv6 Policy, support EVPN over SRv6 policy.

	<p>MAN Core Routers - Medium Capacity-option 1 (single process module, deploy dual device in one site)</p> <ul style="list-style-type: none"> a. 1RU (Rack Unit) device with at least 6 ports of 40GE/100GE and 20 ports 10GE <ul style="list-style-type: none"> a.1 With 2 hot-swappable power supplies b. Intent based Networking capable <ul style="list-style-type: none"> b.1 Automation –programmability, ZTP b.2 Security – segmentation and Policy b.3 Analytics – Flexible Netflow, streaming telemetry c. Capable of Routing & Virtualization <ul style="list-style-type: none"> c.1 BGP, OSPF, MPLS L2/L3 VPN d. Flexible Network Segmentation <ul style="list-style-type: none"> d.1 VRF, VXLAN, MPLS L2VPN, MPLS L3VPN d.2 Segment Routing & EVPN, Flexible Ethernet feature support d.3 support SRv6 and SRv6 Policy, support EVPN over SRv6 policy. <p>MAN Core Routers - Medium Capacity-option 2 (dual process module, deploy single device in one site)</p> <ul style="list-style-type: none"> a. Multi-chassis device with 2 route processor module <ul style="list-style-type: none"> a.1 With Redundant AC power supply a.2 Redundant processor module a.3 total system throughput of at least 2.4Tbps a.4 hot swappable fan trays a.5 Fiber line cards with 10G/40G/100G links, the total 100 GE ports should up to 6. The total 10GE ports should up to 20 b. Intent based Networking capable <ul style="list-style-type: none"> b.1 Automation –programmability, ZTP b.2 Security – segmentation and Policy b.3 Analytics – Flexible Netflow, streaming telemetry c. Capable of Routing & Virtualization <ul style="list-style-type: none"> c.1 BGP, OSPF, MPLS L2/L3 VPN d. Flexible Network Segmentation <ul style="list-style-type: none"> d.1 VRF, VXLAN, MPLS L2VPN, MPLS L3VPN d.2 Segment Routing & EVPN, Flexible Ethernet feature support d.3 support SRv6 and SRv6 Policy, support EVPN over SRv6 policy.
Warranty	<p>36 months Manufacturer's Warranty</p> <p>Minimum repair or replace</p>

5.2.1.2 Aggregation Layer:

5.2.1.2.1 Current Aggregation Network Topology

The network is based on a ring (Aggregation) and sub-ring (access) topology.

- a. MAN Rings:
 1. Multiple MAN rings are built between two Core Nodes.
 2. MAN rings are always terminated on two different core node sites
- b. MAN Aggregation Nodes (MAN-ANs):

1. MAN Aggregation Node devices forms MAN rings.
2. MAN-AN also terminate multiple Sub-Rings i.e. Sub-Ring/Access Ring aggregation.
3. In larger, main stations/depot complexes, these MAN-ANs also act as a “local” aggregation switch, providing connectivity to access switches in a campus network style where necessary:
 - i. Local access switches for end-user access connect to these MAN-ANs
 - ii. “3rd party” LAN’s are be able to be connected to the Aggregation Nodes needing upstream connectivity to another site, e.g. control room, Internet breakout etc
 - iii. Other local LAN’s e.g. Public Wi-Fi might need connectivity to a remote internet breakout point. Internet breakouts might be located on aggregation sites connecting into the Ring
4. A Track-side network also terminate between these Aggregation Nodes, providing various services such as IIoT, CCTV extended to the track-side, in addition to Train-To-Ground Wireless connectivity. **The design and implementation of the track-side network is excluded from this project**

5.2.1.2.2 Proposed Aggregation Network Topology

The bidder is encouraged to propose a solution that is able to leverage the current PRASA MPLS rings and any other transport that can either be underlay transports or that are able to offer better redundancy for upstream connectivity.

The current MPLS rings that are interconnected by PRASA fiber suffer a lot of downtime due to fiber cuts that are happening on our over-head fiber on the rail infrastructure. The connectivity that is achieved in the current Aggregation Network should still be achieved

5.2.1.2.3 Network Specifications

These requirements cover the hardware capacity and capabilities of equipment to be used in the Metro Area Network Aggregation layers.

TECHNOLOGY	SPECIFICATION
Switches/ Routers	MAN Aggregation Routers / Switches - Medium Capacity- Option 1 (single process module, deploy dual device in one site) <ol style="list-style-type: none"> a. 1RU (Rack Unit) device with at least 6 ports of 10G SFP and 20 ports 1GE SFP b. With Redundant AC power supply and fan trays c. Intent based Networking capable <ol style="list-style-type: none"> c.1 Automation –programmability, ZTP c.2 Security – segmentation and Policy c.3 Analytics – Flexible Netflow, streaming telemetry d. Capable of Routing & Virtualization <ol style="list-style-type: none"> d.1 BGP, OSPF, MPLS L2/L3 VPN e. Flexible Network Segmentation <ol style="list-style-type: none"> e.1 VRF, VXLAN, MPLS L2VPN, MPLS L3VPN e.2 Segment Routing & EVPN, Flexible Ethernet feature support e.3 support SRv6 and SRv6 Policy, support EVPN over SRv6 policy.

	MAN Aggregation Routers - Medium Capacity-Option 2 (dual process module, deploy single device in one site) <ul style="list-style-type: none"> a. Multi-chassis device with 2 route processor module <ul style="list-style-type: none"> a.1 With Redundant AC power supply a.2 Redundant processor module a.3 hot swappable fan trays a.4 total system throughput of at least 300 Gbps a.5 Support FIBv4/v6 at least 512K/64K a.5 support 10GE/GE interface a.6 Minimum 6 ports of 10G SFP and 20 ports 1GE SFP b. Intent based Networking capable <ul style="list-style-type: none"> b.1 Automation –programmability, ZTP b.2 Security – segmentation and Policy b.3 Analytics – Flexible Netflow, streaming telemetry c. Capable of Routing & Virtualization <ul style="list-style-type: none"> c.1 BGP, OSPF, MPLS L2/L3 VPN d. Flexible Network Segmentation <ul style="list-style-type: none"> d.1 VRF, VXLAN, MPLS L2VPN, MPLS L3VPN d.2 Segment Routing & EVPN, Flexible Ethernet feature support d.3 support SRv6 and SRv6 Policy, support EVPN over SRv6 policy.
Warranty	36 months Manufacturer's Warranty Minimum repair or replace
Software licences	36 months

5.2.1.3 Access Layer:

5.2.1.3.1 Current Access Network Topology

The network is based on a sub-ring (access) topology.

- a. Access Rings (Sub-Rings):
 1. Support multiple sub-rings between two adjacent MAN-ANs.
 2. Main Access Devices (MADs) are connected dual-homed in a ring topology to MAN-ANs.

5.2.1.3.2 Proposed Access Network Topology

The bidder is encouraged to propose a solution that is able to leverage the current PRASA MPLS rings and any other transport that can either be underlay transports or that are able to offer better redundancy for upstream connectivity.

5.2.1.3.3 Network Specifications

These requirements cover the hardware capacity and capabilities of equipment to be used in the Metro Area Network Aggregation layers.

Switches	MAN Access Switches – Low Capacity (Industrial Grade Switches) <ul style="list-style-type: none"> a. Device shall be Fan-less, no moving parts. b. Extended Temperature ranges. At least -40°C to 60°C.
-----------------	--

	<ul style="list-style-type: none"> c. 19" Rack mountable with an option to be mounted using DIN Rail at certain sites where needed. d. Redundant AC and DC power supply options e. Support min 2 x Uplink ports at 1Gbps / 10Gbps f. Support min 2 x downstream SFP ports at 100Mbps / 1Gbps g. Support minimum 8 or 12 Ethernet ports – up to 1Gbps or faster h. Power-Over-Ethernet i. Minimum 802.3at Type 2 "PoE" j. Recommended 802.3bt Type 3 "4PPoE" or 802.3bt Type 4 k. Devices placed in Electrical Sub-Stations have to comply with IEEE 1613 Class-2
Warranty	36 months Manufacturer's Warranty Minimum repair or replace
Software licences	36 months

5.2.1.4 General Requirements for Work Package A:

This work package includes all the Design, Supply and Implementation of the listed categories, including,

Professional Services for:

- b. Architecture and design (high level and Low/Detail level),
 - 1. The Bidder shall provide all the resources required to perform the architecture as well as high level and detail level designs.
 - 2. Relevant industry best-practices and standards shall be followed in the architecture and design of the network.
 - 3. The bidder will generate and prepare all necessary documents for approval by PRASA
 - i. A **General Network Architecture** document shall be compiled covering all topics about the hardware, software, mechanisms, protocols and other techniques utilised in the network.
 - ii. Sample Use-Case configurations, as implemented in the PRASA network will also be included in this document
 - iii. This document will also explain, in detail how each ICT service is configured on the network.
 - iv. The detail of the exact content will be discussed and agreed to during project initialisation.
 - v. A **Detail Low Level Design** document will be compiled, containing all the information for each configurable Item for every site.
 - vi. This will include for example Management IP Addresses, VLAN IDs, Device Names, Port assignments, configuration information for each specific ring etc.
 - vii. This document will have all the information necessary to be able to create a device configuration for a specific site at all layers of the network.

- viii. This document will contain all information required as a singular guide to build the complete network from scratch.
 - ix. Further detail of the exact content will be discussed and agreed to during project initialisation.
 - x. A Site plan indicating where and how equipment shall be installed
 - c. Site surveys WILL be required from the winning bidder.
 - 1. The bidder shall conduct the required site surveys at about listed sites that will host the MAN Core POPs at the respective regions, the list can be found in ANNEXURE 2
 - 2. Regional Maps can be found under ANNEXURE 1
 - 3. Site Survey Reports shall be completed for each site. These reports will inform the detail scope of work to be carried out on each site.
 - 4. Site Survey will focus on all physical requirements for the successful deployment of the new equipment.
 - 5. Resources that will go to site will be subject to safety inductions and substance abuse tests.
 - 6. Labour, travelling and transportation costs associated with these activities shall be included in the offer.
 - d. Development of network / device configurations.
 - 1. Sample Device configuration for each layer of the network shall be compiled.
 - 2. Device and Site-specific configurations files shall be created for each device on the network.
 - e. Project Management (in line with section 5)
 - f. Comprehensive Network Roll-Out Plan.
 - 1. A detailed Network Roll-Out plan shall be developed.
 - 2. This plan will set out in a step-by-step fashion exactly how the network will be deployed
 - i. This will focus on the order in which devices would be installed, commissioned and tested.
 - ii. It shall cover all site visits required.
 - iii. It will cover in detail how services/systems will be migrated.
 - iv. It will cover how the existing network will be decommissioned.
 - v. It will cover all the test plans in detail.
 - g. Labour for deployment, setup, configuration, commissioning, testing, as well as as-built documentation.

5.2.1.5 Technical Assessment of the Solution – Work Package A : Next Generation Metro Area Network (MAN) in Gauteng, WC and KZN

ALL the requirement items in the tables below are **MANDATORY**. Failure to meet all the below products' requirements, bidders will be disqualified automatically under Evaluation Stage 1C.

<i>Item</i>	<i>Minimum Requirement</i>	<i>Compliance Yes/No</i>	<i>Evidence</i>	<i>Reference To Information e.g. File A, Section X, Page Y</i>
1	<i>BIDDER CERTIFICATION / AFFILIATION REQUIREMENTS</i> <i>The bidder must be an OEM or a registered OEM reseller to supply the OEM Infrastructure.</i>		<i>Valid Partnership / Reseller Certificate/ letter</i>	
2	<i>BIDDER CERTIFIED ENGINEERS</i> <i>The bidder must have at least TWO OEM certified Expert level Engineers in the proposed technologies</i>		<i>Valid Expert Level Certificates in Routing</i>	
3	Bidder must provide a concept high-level design that depicts that they understand the requirements. <ul style="list-style-type: none"> - Core layer - 40/100GE - Aggregation layer - 10/25GE - Access layer - 1/10GE 		<i>High-level design concept</i>	

5.2.2 WORK PACKAGE “B”: Next Generation Inter- and Intra- Data Center Network

5.2.2.1 Proposed Core Network Topology

Spine Leaf Topology (applicable to all Data Centres)

- a. The Data Centre Network shall be based on a Spine Leaf Topology as a Data Centre Network underlay.
- b. Leaf and Spine switches shall be connected using single 100Gbps interfaces.
- c. All servers as well as Hyper Converged Infrastructure shall be connected to Leaf switches.
- d. Firewall break-outs shall be connected to Border-Leaf Switches.
- e. A separate Out-of-Band Management network shall be deployed, connecting to all switches in the Data Centre.
- f. Provision shall be made for Application Delivery Controller (ADC's) functionality and shall be included in the solution.

SDN Technology on Data Centre Network (DCN)

- a. Provision shall be made for a Data Centre Overlay network, based on an optimised VXLAN approach, including other associated technologies such as BGP EVPN.
- b. SDN solution for Data Centre that is a policy-driven ecosystem that integrates software and hardware, Fully automated service provisioning and management

Data Centre Network and Interconnection (DCI) – (only applicable to Gauteng Data centres)

- a. PRASA's Data Centres in Gauteng shall be interconnected using modern Data Centre Interconnect techniques and solutions.
- b. The Data Centre Fabric shall be “Stretched” across both Data Centres to provide a seamless virtual data centre.
- c. The DCI solution will enable effortless, automated server migration/mobility, as well as off-site backups.
- d. The DCI solution shall enable VXLAN, BGP-EVPN and Layer-3 DCI.
- e. Shall support Secure Multi-Tenancy

5.2.2.2 Network Specifications

These requirements cover the hardware capacity and capabilities of equipment to be used in the Metro Area Network Core and Aggregation layers, as well as in the Data Centre Spine and Leaf infrastructure.

TECHNOLOGY	SPECIFICATION
Switches	Data Centre SDN Switches <ol style="list-style-type: none">a. For Spine: 2RU (Rack Unit) device with at least 64 ports of 100G QSFP a.1 Which includes Redundant and hot-swappable power supplies, and fansb. For leaf: 1RU (Rack Unit) device with at least 32/48 ports of either 1G/10G/25G/40G with 6 uplink ports of 100GE

	<p>b.1 Which includes Redundant and hot-swappable power supplies, and fans</p> <p>c. Intent based Networking capable</p> <p>b.1 Automation –programmability, ZTP</p> <p>b.2 Security – segmentation and Policy</p> <p>b.3 Analytics – Flexible Netflow, streaming telemetry</p> <p>d. Capable of switching packets at wire speed</p> <p>e. Capable for link aggregation technology (port-channels) and span sessions</p> <p>f. Capable of at least 32 Equal-Cost Multipath (ECMP) paths</p> <p>g. Flexible Network Segmentation</p> <p>d.1 VRF, VXLAN</p> <p>d.2 EVPN feature support</p> <p>h. The Management and orchestration appliance for the switches must have enough storage/RAM and CPU able to manages and operates the devices</p>
Warranty	<p>36 months Manufacturer's Warranty</p> <p>Minimum repair or replace</p>
Software licences	36 months

This work package includes all the Design, Supply and Implementation of a Software Defined Inter- and Intra- Data Centre Network in Gauteng (GNC and Braamfontein) and the DR site in Durban. All equipment and accessories for Routing, Switching, Network Security and Load Balancing shall form part of the design and implementation.

The scope includes all equipment and cabling as well as professional services required.

The Bidder shall carry out a Network Analysis on the current network in order to have an updated view of the existing network, prior to any new works being carried out.

The analysis will include the following as a minimum:

- i. Physical Topology (Device / port level)
- ii. Layer 2 Topology – Configuration
- iii. Layer 3 Topology – Configuration
- iv. Security – Firewall rules, Device vulnerabilities

Any other detail the bidder deems necessary to be able to design and built the new network. This information shall be used in the design of the new network where the data centre layer is separated from the rest of the network.

- i. Physical Topology information shall be used to plan the deployment of the new network. Care should be taken in not decommissioning any existing links until the existing network is officially decommissioned.
- ii. The analysis shall point out any issues at Layer 2 and 3 as well as at a security level. These issues shall be addressed in the design of the new Data Centre network.

- iii. A Network clean-up shall also be done on all network services where required with relation to the Data Centre network.
- iv. This information shall also be used in the development of a comprehensive Network Roll-out plan.

5.2.2.3 Provide Professional Services for

- a. **Architecture and design** (high level and Detail level),
 - 1. The Bidder shall provide all the resources required to perform the architecture as well as high level and detail level designs.
 - 2. Relevant industry best-practices and standards shall be followed in the architecture and design of the network.
 - 3. The outputs / reports from the Network analysis shall be used as input for the architecture and design of the new Data Centre network.
 - 4. The bidder will generate and prepare all necessary documents for approval by PRASA.
 - i. A General Data Centre Network Architecture document shall be compiled covering all topics about the hardware, software, mechanisms, protocols and other techniques utilised in the network.
 - ii. Sample Use-Case configurations, as implemented in the PRASA network will also be included in this document.
 - iii. This document will also explain, in detail how each ICT service is configured on the network
 - iv. The detail of the exact content will be discussed and agreed to during project initialisation.
 - v. A **Detail Low Level Data Centre Design** document shall be compiled, containing all the information for each configurable Item for each data centre site.
 - This will include for example Management IP Addresses, VLAN IDs, Device Names, Port assignments, and configuration information
 - This document will have all the information necessary to be able to create a device configuration for a specific site at all layers of the network.
 - This document will contain all information required as a singular guide to build the complete network from scratch.
 - Further detail of the exact content will be discussed and agreed to during project initialisation.
 - Connectivity to the rest of the PRASA environment shall be addressed in detail.
 - A Site plan indicating where and how equipment shall be installed.
- b. **Site surveys WILL be required from the winning bidder.**
 - 1. The bidder shall conduct the required site surveys at all current 3 Data Centres as well as the 2 Switching Centres in Gauteng.
 - 2. Site Survey Reports shall be completed for each. These reports will inform the detail scope of work to be carried out on each site.
 - 3. Site Survey will focus on all physical requirements for the successful deployment of the new equipment.

4. Resources that will go to site will be subject to safety inductions and substance abuse tests.
5. Information gathered will be used in the Network Roll-out plan.
- c. Development of network / device configurations.**
 1. Sample Device configuration for each layer of the network shall be compiled.
 2. Device and Site-specific configurations files shall be created for each device on the network.
- d. Project Management (in line with section 5)**
- e. Comprehensive Network Roll-Out Plan.**
 1. A detailed Network Roll-Out plan shall be developed.
 2. This plan will set out in a step-by-step fashion exactly how the network will be deployed
 - i. This will focus on the order in which devices would be installed, commissioned and tested.
 - ii. It shall cover all site visits required.
 - iii. It will cover in detail how services/systems will be migrated.
 - iv. It will cover how the existing network will be decommissioned.
 - v. It will cover all the test plans in detail.
- f. Labour for deployment, setup, configuration, commissioning, testing, as well as as-built documentation.**
- g. Provide Cabling and associated services where required (as per Work Package F)**
- h. Supply all hardware and accessories as may be required.**
 1. Equipment shall be supplied and delivered, based on the detail designs, Solution Acceptance and BoM.
 2. As per timelines agreed to during the project meetings.
- i. Configure Equipment**
 1. The contractor shall be responsible for configuring all equipment.
 2. The contractor shall be responsible for Device labelling and Asset tagging, and where applicable, shall be responsible for Packing and shipping the equipment to other areas.
 3. Labour, travelling and transportation costs associated with these activities shall be included in the offer
- j. Deploy and install new network equipment at the respective site.**
 1. All equipment shall be delivered and installed on site after network staging.
 2. Where possible, the new network will be deployed in parallel to the existing network. User migration will then happen on a site-by-site basis. This can only be done where adequate fibre is available to do so.
 3. Where insufficient fibre will not allow parallel deployment, the new devices shall be installed and commissioned in the shortest possible time. Additional resources might be required in those areas.
 4. Labour, traveling and transportation costs related to these activities shall be included in the offer.
- k. Migrate existing Network Services.**
 1. All existing PRASA Network/ICT services shall be migrated by the contractor.
 2. This includes network device configuration where required.
- l. Decommissioning of Old Equipment.**
 1. The contractor shall be responsible for decommissioning old equipment.
 2. This will include recording the asset details.

3. The contractor shall deliver all the old equipment to a storage facility as appointed by PRASA.

m. Test and Commission the network, including network services.

1. Testing of the Network will take place in several stages.
2. Detail Test Plans, User Acceptance Test Scripts shall be developed for each stage of testing.
3. These tests will be carried out on all newly supplied devices
4. Test reports shall be compiled for each device as part of Sign-Off

n. Detail As-Built Documentation.

5.2.2.4 Technical Assessment of the Solution – Work Package B : Next Generation Inter- and Intra-Data Center Network

ALL the requirement items in the tables below are **MANDATORY**. Failure to meet all the below products' requirements, bidders will be disqualified automatically under Evaluation Stage 1C.

<i>Item</i>	<i>Minimum Requirement</i>	<i>Compliance Yes/No</i>	<i>Evidence</i>	<i>Reference To Information e.g. File A, Section X, Page Y</i>
1	<i>BIDDER CERTIFICATION / AFFILIATION REQUIREMENTS</i> <i>The bidder must be an OEM or a registered OEM reseller to supply the OEM Infrastructure.</i>		<i>Valid Partnership / Reseller Certificate / Letter</i>	
2	<i>BIDDER CERTIFIED ENGINEERS</i> <i>The bidder must have at least TWO OEM certified Professional level Engineers in the proposed technologies</i>		<i>Valid Professional Level Certificates in Datacenter Technologies</i>	
3	Bidder must provide a concept high-level design that depicts that they understand the requirements. <ul style="list-style-type: none"> - <i>Spine Leaf Topology as a Data Center Network underlay</i> - <i>Spine 100GE and Leaf 1/10/25/40GE</i> - <i>DCI (Data Center Interconnection) solution should be enabled for VXLAN, BGP-EVPN</i> 		<i>High-level design concept</i>	

5.2.3 WORK PACKAGE “C”: Campus/Station Networks and WI-FI

5.2.3.1 Current & Proposed Campus/Station Network Topology

- a. The Campus Network will typically consist of two layers.
 - 1. The Aggregation/Distribution layer (Main Access Device) will connect back to the Metro Area Network.
 - 2. The Campus Access switches shall connect to the Main Access Device in various topologies such as ring or star.
- b. Large as well as Critical Campus Sites such a large offices or key depots will make use of a redundant pair of Main Access Device.
- c. MAN Aggregation nodes can be used as Campus Aggregation switches.
- d. The Campus Network shall make adequate provision for a Wi-Fi 6 network to be deployed at each site.

5.2.3.2 Current & Proposed Campus/Station Wi-Fi Topology

- a. A centrally managed Wi-Fi 6 network solution shall be deployed at various indoor locations.
- b. The centrally managed Wi-Fi network solution shall deploy Wi-Fi 6 equipment at various outdoor locations.
- c. These will include typical low and medium capacity office environment, low capacity outdoor as well as high capacity outdoor scenarios.
- d. The Wi-Fi network shall support various use cases, including voice, low- latency financial transactions as well as IoT.
- e. Access Points shall be connected to the network via copper, or preferably fibre connections.
- f. Wi-Fi Mesh topology will be used where necessary.
- g. The solution will include adequate redundancy of core elements as to avoid single-points of failure.
- h. The solution shall make provision to replace Wi-Fi 6 devices with Wi-Fi 6 devices in future.

5.2.3.3 Network Specifications

These requirements cover the hardware capacity and capabilities of equipment to be used in the campus Network Core/Distribution and Access layers, as well as in the station and depot enterprise infrastructure.

TECHNOLOGY	SPECIFICATION
Switches	Campus Core/Distribution Switches - High Capacity <ul style="list-style-type: none">a. Multi-chassis device (number of slots based on the size)<ul style="list-style-type: none">a.1 With Redundant AC power supplya.2 Redundant supervisor module, total switching capacity of at least 4.2Tbpsa.3 Chassis line card with at least 320Gbps per slota.4 Redundant System Controllersa.4 hot swappable fan trays

	<table><tr><td>Downstream Ports</td><td>minimum 2 x 1Gbps</td><td>minimum 2x 10Gbps, compatible with 1Gbps</td><td>minimum 2x 10Gbps, compatible with 1Gbps</td></tr></table>	Downstream Ports	minimum 2 x 1Gbps	minimum 2x 10Gbps, compatible with 1Gbps	minimum 2x 10Gbps, compatible with 1Gbps		
Downstream Ports	minimum 2 x 1Gbps	minimum 2x 10Gbps, compatible with 1Gbps	minimum 2x 10Gbps, compatible with 1Gbps				
	<p>Stations Standard switch– Low Capacity Access Switches.</p> <p>Industrial Grade Switches</p> <ul style="list-style-type: none">a. Device shall be Fan-less, no moving parts.b. Extended Temperature ranges. At least -40°C to 60°C.c. 19” Rack mountable with an option to be mounted using DIN Rail at certain sites where needed.d. Redundant AC and DC power supply optionse. Support min 2 x Uplink ports at 1Gbps / 10Gbpsf. Support min 2 x downstream SFP ports at 100Mbps / 1Gbpsg. Support min 8 x Ethernet ports – up to 1Gbps or fasterh. Power-Over-Ethernet<ul style="list-style-type: none">a. Minimum 802.3at Type 2 "PoE+"b. Recommended 802.3bt Type 3 "4PPoE" or 802.3bt Type 4i. Devices placed in Electrical Sub-Stations have to comply with IEEE 1613 Class-2						
Wi-Fi	<p>The Wi-Fi network shall be deployed in the following areas:</p> <ul style="list-style-type: none">a. All office areas, training centre meeting roomsb. Industrial areas such as Running Sheds, Workshops and Warehouses.c. All Staging Yards and lines outside Running and lifting sheds.d. All stations <p>The network shall be designed to provide signal strength of -67dBm minimum. Seamless hand-over of connections between Access Points (AP Handoff).</p> <p>The Wireless Network Controller shall support:</p> <ul style="list-style-type: none">a. Hitless failover – controller clustering or active-standby modeb. Multi-tenancy - Encryption from user to controllerc. Centralised licencing – individual license poold. App aware QoS <p>The wireless solution shall include all the components required to provide a secure and managed “Guest” and “Public” Wi-Fi service</p> <p>WIRELESS MESH</p> <p>The Wi-Fi network in the staging yards shall utilise Wireless Mesh – Based on IEEE 802.11s.</p> <p>The following Wi-Fi standards shall be supported (2.4GHz and 5GHz):</p> <table><tr><td>802.11a/b/g/n/ac</td><td>Legacy Wi-Fi Standards shall be supported</td></tr><tr><td>802.11ac – Wave 2</td><td>Shall be supported on all access points</td></tr><tr><td>802.11ax</td><td>Shall be supported on all access points</td></tr></table> <p>Standard 802.11 ax indoor AP :</p>	802.11a/b/g/n/ac	Legacy Wi-Fi Standards shall be supported	802.11ac – Wave 2	Shall be supported on all access points	802.11ax	Shall be supported on all access points
802.11a/b/g/n/ac	Legacy Wi-Fi Standards shall be supported						
802.11ac – Wave 2	Shall be supported on all access points						
802.11ax	Shall be supported on all access points						

	<ul style="list-style-type: none"> Support two spatial streams at 2.4 GHz (2x2 MIMO) and at 5 GHz (2x2 MIMO) achieving a device rate of up to 1.75Gbps support dual-band smart antenna array <p>High capacity 802.11 ax indoor AP</p> <ul style="list-style-type: none"> Support triple radio frequency at 2.4 GHz (2x2 MIMO) ,5GHz (2x2 MIMO) and 5 GHz (4x4 MIMO) frequency bands, achieving a device rate of up to 6.5Gbps. support smart antenna array 2 x 1 GE electrical <p>802.11 ax outdoor AP</p> <ul style="list-style-type: none"> Support 2.4 GHz (4x4) + 5 GHz (4x4) radios, achieving a maximum rate of 5.95 Gbit/s. support smart antenna array 1 x 5GE electrical, 1 x GE electrical, and 1 x 10GE SFP+. 6 kA/6 kV surge protection for Ethernet ports, IP68 waterproof and dustproof -40° C to + 65° C wide temperature
	<p>Bluetooth Low Energy (BLE) enabled 4.1 shall be supported.</p> <p>Support for MU-MIMO (Multi-User-Multiple-Input and Multiple-Output) Access Points shall support Single Mode fibre where required.</p> <p>All planning and design works shall be included, including RF analysis, channel planning etc.</p>
SDN Control platform	<p>Platform architecture</p> <ul style="list-style-type: none"> Is able to automatically configure large-scale network devices using SDN protocols, such as NETCONF, YANG, and SNMP, collect device performance, alarm data, and user data using Telemetry, as well as perform big data-based statistics collection and analysis, AI-powered network fault prediction and rectification, and intelligent radio calibration. Manages a variety of campus network devices, such as switches, WLAN ACs, APs, firewalls, and routers. Supports high availability deployment mode. The controller supports geographic redundancy regardless of its deployment modes. <p>Underlay network automation</p> <ul style="list-style-type: none"> Support underlay network deployment automation, the controller can directly generate network topologies as well as network and service configurations, and replicate the topologies and configurations to other sites. Is able to automatically configure switches and Wi-Fi devices in batches by templates, such as feature, service, and site templates. <p>Network admission authentication</p> <ul style="list-style-type: none"> Supports an array of authentication technologies, such as 802.1X authentication, MAC address authentication, Portal authentication based on HTTP/2 (HACA) and Portal 2.0, as well as VPN authentication.

	<ul style="list-style-type: none"> ● User access right are decoupled from IP addresses. Security groups are authorized based on user login conditions (5W1H). The UCL policy matrix is used to restrict users' mutual access rights and guarantee that users have the same rights to access network services anytime, anywhere. ● Is able to synchronize with multiple AD or LDAP domain name servers, map account attributes to local roles, and perform network admission authorization by role ● Multiple network attributes for network admission authentication can be automatically bound to users at the first authentication to restrict users' access behavior. ● Is able to authorize and manage network access policies based on a multitude of network attributes, such as the user, user group, role, access location, device group, access time, and access mode. ● Is able to use an array of network attributes as network admission authorization results. The attributes include the VLAN, ACL, dynamic ACL, security group, VIP user, redirection URL, uplink and downlink bandwidth, as well as customized RADIUS attributes. <p>Monitoring and O&M</p> <ul style="list-style-type: none"> ● Provides a default scenario-based dashboard to simplify O&M, and allows customers to flexibly customize dashboards based on their O&M requirements. The controller also supports orchestration of common data sources and correlative data analysis. ● Monitors the overall health, device status, mesh link status, radio frequency information, and topology of each site, and monitors the sites in real time based on the indoor and outdoor maps. ● Monitors the network status and displays collected statistics, including the network traffic statistics, traffic rate, top N device traffic, top N SSID traffic, and number of online users. <p>Displays the list of AP radios at a site, collects statistics on the RF channel utilization, RF interference rate, and RF noise, and displays the RF trend in the past 24 hours.</p>
Warranty	<p>36 months Manufacturer's Warranty</p> <p>Minimum repair or replace</p>
Software licences	<p>36 months</p>

This work package seeks the design and replace of all existing ICT infrastructure in various PRASA campuses across the regions. The network (wired and wireless) should be able to offer data services across single coherent network architecture. The scope includes all equipment, cabling as well as professional services required.

The scope includes all equipment and cabling as well as professional services required.

5.2.3.4 Provide Professional Services for

a. Architecture and design (high level and Detail level),

1. Networks and WI-FI deployed at Campus shall comply to the overall network architecture as developed under work package "A" and "B". The Bidder shall provide all the resources required to perform the high level and detail level designs.

2. Relevant industry best-practices and standards shall be followed in the design of the networks.
3. The bidder will generate and prepare all necessary documents for approval by PRASA.
 - i. A High Level and Detail Low Level Design document will be compiled, containing all the information for each configurable Item for every site.
 - ii. This will include for example Management IP Addresses, VLAN IDs, Device Names, Port assignments, configuration information for each specific layer etc.
 - iii. This document will have all the information necessary to be able to create a device configuration for a specific site at all layers of the network.
 - iv. This document will contain all information required as a singular guide to build the complete network from scratch.
 - v. Further detail of the exact content will be discussed and agreed to during project initialisation.
 - vi. A Site plan indicating where and how equipment shall be installed.
 - vii. Perform Radio Frequency Spectrum Analysis.
 - viii. RF propagation and Carry out Channel Planning
 - ix. Prepare Floorplans indicating AP locations, Signal Quality Heat Maps
- b. Site surveys WILL be required from the winning bidder.**
 1. The bidder shall conduct the required site surveys at Campuses of every region.
 2. These site survey might be conducted separate or in conjunction with other Work Packages.
 3. Site Survey Reports shall be completed for each. These reports will inform the detail scope of work to be carried out on each site.
 4. Site Survey will focus on all physical requirements for the successful deployment of the new equipment.
 5. Resources that will go to site will be subject to safety inductions and substance abuse tests.
- c. Development of network / device configurations**
 1. Sample Device configuration for each layer of the network shall compiled.
 2. Device and Site-specific configurations files shall be created for each device on the network.
 3. The contractor shall be responsible for Device labelling and Asset tagging, and where applicable, shall be responsible for Packing and shipping the equipment to other areas.
- d. Project Management (in line with section 5)**
- e. Comprehensive Network Roll-Out Plan.**
 3. A detailed Network Roll-Out plan shall be developed.
 4. This plan will set out in a step-by-step fashion exactly how the network will be deployed
 - i. This will focus on the order in which devices would be installed, commissioned and tested.
 - ii. It shall cover all site visits required.
 - iii. It will cover in detail how services/systems will be migrated.
 - iv. It will cover how the existing network will be decommissioned.
 - v. It will cover all the test plans in detail.

- f. **Labour for deployment, setup, configuration, commissioning, testing, as well as as-built documentation.**
- g. **Provide Cabling and associated services where required (as per Work Package F)**
- h. **Supply all hardware and accessories as may be required.**
 - 1. Equipment shall be supplied and delivered, based on the detail designs, Solution Acceptance and BoM.
 - 2. As per timelines agreed to during the project meetings.
- i. **Configure Equipment**
 - 1. The contractor shall be responsible for configuring all equipment.
 - 2. The contractor shall be responsible for Device labelling and Asset tagging, and where applicable, shall be responsible for Packing and shipping the equipment to other areas.
 - 3. Labour, travelling and transportation costs associated with these activities shall be included in the offer
- j. **Deploy and install new network equipment at the respective site.**
 - 1. All equipment shall be delivered and installed on site after network staging.
 - 2. Where possible, the new network will be deployed in parallel to the existing network. User migration will then happen on a site-by-site basis. This can only be done where adequate fibre is available to do so.
 - 3. Where insufficient fibre will not allow parallel deployment, the new devices shall be installed and commissioned in the shortest possible time. Additional resources might be required in those areas.
 - 4. Labour, traveling and transportation costs related to these activities shall be included in the offer.
- k. **Migrate existing Network Services.**
 - 1. All existing PRASA Network/ICT services shall be migrated by the contractor.
 - 2. This includes network device configuration where required.
- l. **Decommissioning of Old Equipment.**
 - 1. The contractor shall be responsible for decommissioning old equipment.
 - 2. This will include recording the asset details.
 - 3. The contractor shall deliver all the old equipment to a storage facility as appointed by PRASA.
- m. **Test and Commission the network, including network services.**
 - 1. Testing of the Network will take place in several stages.
 - 2. Detail Test Plans, User Acceptance Test Scripts shall be developed for each stage of testing.
 - 3. These tests will be carried out on all newly supplied devices
 - 4. Test reports shall be compiled for each device as part of Sign-Off
- n. **Detail As-Built Documentation.**

5.2.3.5 Technical Assessment of the Solution – Work Package C : Campus/Station Network and WI-FI

ALL the requirement items in the tables below are **MANDATORY**. Failure to meet all the below products' requirements, bidders will be disqualified automatically under Evaluation Stage 1C.

<i>Item</i>	<i>Minimum Requirement</i>	<i>Compliance Yes/No</i>	<i>Evidence</i>	<i>Reference To Information e.g. File A, Section X, Page Y</i>
1	<i>BIDDER CERTIFICATION / AFFILIATION REQUIREMENTS The bidder must be an OEM or a registered OEM reseller to supply the OEM Infrastructure.</i>		<i>Valid Partnership / Reseller Certificate / letter</i>	
2	<i>BIDDER CERTIFIED ENGINEERS The bidder must have at least TWO OEM certified Professional level Engineers in the proposed technologies</i>		<i>Valid Professional Level Certificates in Datacenter Technologies</i>	
3	Bidder must provide a concept high-level design that depicts that they understand the requirements. <ul style="list-style-type: none"> - Core distribution and access - VLAN design - WiFi design 		<i>High-level design concept depicting the requirements for - Large building Umjantshi House 15 floors)</i>	

5.2.4 WORK PACKAGE “D”: Network Security

5.2.4.1 Proposed Network Security Solution

- a. Network security infrastructure, such as redundant firewalls shall be deployed for:
 1. both internal and external protection
 2. west-east traffic within the Data Centre (DC services FW)
 3. North-South in-out of the Data Centres (DC perimeter firewalling, with IDS capabilities)
 4. inter-VRF routing firewall
- b. Other security appliances shall be implemented as proposed by the bidder, and agreed to by PRASA in order to provide a comprehensive secure network solution that is based on best practices and fit for purpose in the PRASA environment.
- c. Firewalls and other security appliances shall be dual-homed.
- d. The Bidder shall carry out a Security Analysis on the current network in order to have an updated view of the existing security solutions, prior to any new works being carried out.
- e. Any other detail the bidder deems necessary to be able to design and built the new Security Solution may be added.

5.2.4.2 Network Specifications

These requirements cover the solution capabilities to be achieved by the Network Security Solution, below is the subset of the list of design requirements and objectives

TECHNOLOGY	SPECIFICATION
Firewall / Security Devices	<p>Security Device</p> <ol style="list-style-type: none">a. A Modern, modular, layered approach shall be followed in assuring Data Centre Security.b. Generally accepted Data Centre Security best-practices and relevant standards shall form the basis of the proposed solution.c. Security mechanism shall be deployed between the Data Centre network and the Metropolitan Area Network (MAN), as well as campus networks.d. Layers 3 – 7 of the OSI stack shall be protected from a Data Centre Network perspective.<ol style="list-style-type: none">1. This will be further enhanced by End-Point security as well as best practices at an application and database level. This should be covered at a High-Level Design - “Holistic End-to-End Security Plan”e. Independent Security appliances shall be used. Devices shall not be modular units that are slotted into network routers or switches.<ol style="list-style-type: none">1. Software based instances (for HA, redundancy and DR) may be considered however the advantages, limitations and risks associated with this approach has to be clearly indicated.

	<p>f. Firewall and other security appliances selection shall be based on providing enough processing and port capacity as to not be a bottle-neck in the network.</p> <p>This can be achieved in a number of ways:</p> <ol style="list-style-type: none"> 1. Providing firewalls with multiple 40Gbps or 100Gbps ports, 2. Or by creating firewall pairs that can act as a single firewall in terms of processing and throughput by load balancing the processing and the traffic. <p>Or by using multiple firewalls and configuring the network to pass predefined VLAN's through each firewall</p>
Warranty	<p>36 months Manufacturer's Warranty</p> <p>Minimum repair or replace</p>
Software Licences	<p>36 months</p>

This work package seeks the design a modern, modular, layered approach shall be followed in assuring network and all IP traffic security. The network security solution should be able to protect OSI layer 3-7. The solution should be a holistic end-to-end security for PRASA network, from the Data Centre to the end-point, remote and local connectivity.

The scope includes all equipment and cabling as well as professional services required.

5.2.4.3 Provide Professional Services for

a. Architecture and design (high level and Detail level),

1. The Bidder shall provide all the resources required to perform the architecture as well as high level and detail level designs.
2. Relevant industry best-practices and standards shall be followed in the architecture and design of the network Security solution.
3. The outputs / reports from the Security analysis shall be used as input for the architecture and design of the new Security solution.
4. The bidder will generate and prepare all necessary documents for approval by PRASA.
 - i. A General Security Architecture document shall be compiled covering all topics about the hardware, software, mechanisms, protocols and other techniques utilise.
 - ii. This document will also explain, in detail how network and services will be securely protected.
 - iii. The detail of the exact content will be discussed and agreed to during project initialisation.

b. A High-Level Network Security Design shall be compiled.

1. This design shall cover all aspects of Network Security as per ISO/SANS 27033 Parts 1 to 6. ISO/IEC 27033 consists of the following parts, under the general title Information technology — Security techniques — Network security:
 - i. Part 1: Overview and concepts
 - ii. Part 2: Guidelines for the design and implementation of network security

- iii. Part 3: Reference networking scenarios — Threats, design techniques and control issues
 - iv. Part 4: Securing communications between networks using security gateways
 - v. Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
 - vi. Part 6: Securing wireless IP network access
- 2. A comprehensive Network Security Risk assessment shall be conducted.
- 3. The Data Centre (Equipment, Applications and Data contained within) shall be protected from all other areas of the network.
- 4. All existing Network Security equipment shall be replaced.
- 5. A comprehensive Security Framework with solution building blocks will be developed. This will cover at a high level:
 - i. Network Security – In Detail Information Security Application Security Cybersecurity
 - ii. Internet Security – In Detail
- 6. Included in the scope of this project is the supply and implementation of all security mechanisms, equipment and products in order to address matters related Network Security and Internet Security, including Secure Remote Access and “Trusted” 3rd Party Connections.
- c. Development of Security device configurations.**
 - 1. Sample Device configuration for each layer shall compiled.
 - 2. Device and Site-specific configurations files shall be created for each device.
- d. Project Management (in line with section 5)**
- e. Comprehensive Network Security Roll-Out Plan.**
 - 1. A detailed Security Roll-Out plan shall be developed.
 - 2. This plan will set out in a step-by-step fashion exactly how the network security solution will be deployed
- f. Labour for deployment, setup, configuration, commissioning, testing, as well as as-built documentation.**
- g. Provide Cabling and associated services where required (as per Work Package F)**
- h. Supply all hardware and accessories as may be required.**
 - 1. Equipment shall be supplied and delivered, based on the detail designs, Solution Acceptance and BoM.
 - 2. As per timelines agreed to during the project meetings.
- i. Configure Equipment**
 - 1. The contractor shall be responsible for configuring all equipment.
 - 2. The contractor shall be responsible for Device labelling and Asset tagging, and where applicable, shall be responsible for Packing and shipping the equipment to other areas.
 - 3. Labour, travelling and transportation costs associated with these activities shall be included in the offer
- j. Deploy and install new Security equipment at the respective site.**
- k. Migrate existing Network Services.**
 - 1. All existing PRASA Network/ICT services shall be migrated by the contractor.
- l. Decommissioning of Old Equipment.**
 - 1. The contractor shall be responsible for decommissioning old equipment.
 - 2. This will include recording the asset details.

3. The contractor shall deliver all the old equipment to a storage facility as appointed by PRASA.

m. Test and Commission the Security devices, including network services.

1. Testing of the Security devices and Network services will take place in several stages.
2. Detail Test Plans, User Acceptance Test Scripts shall be developed for each stage of testing.
3. These tests will be carried out on all newly supplied devices
4. Test reports shall be compiled for each device as part of Sign-Off

n. Detail As-Built Documentation.

5.2.4.4 Technical Assessment of the Solution – Work Package D : Network Security

ALL the requirement items in the tables below are **MANDATORY**. Bidders must indicate by either a Yes or No whether they are compliant to requirement items in the table below. Evidence of compliance must be provided where specified – “evidence required” and the evidence must be referenced accordingly in the column provided. Failure to comply with requirement items in the table below will lead to automatic disqualification under Evaluation Stage 1C.

<i>Item</i>	<i>Minimum Requirement</i>	<i>Compliance Yes/No</i>	<i>Evidence</i>	<i>Reference To Information e.g. File A, Section X, Page Y</i>
1	BIDDER CERTIFICATION / AFFILIATION REQUIREMENTS <i>The bidder must be an OEM or a registered OEM reseller to supply the OEM Infrastructure.</i>		<i>Valid Partnership / Reseller Certificate / Letter</i>	
2	BIDDER CERTIFIED ENGINEERS <i>The bidder must have at least TWO OEM certified Professional level Engineers in the proposed technologies</i>		<i>Valid Professional Level Certificates in Security</i>	
3	Bidder must provide a concept high-level design that depicts that they understand the requirements. <ul style="list-style-type: none"> - <i>multi-layered security solution that addresses cyber security in line with ISO27000 family of standards.</i> - <i>Security Solution that protect Layers 3 – 7 of the OSI stack</i> - <i>security appliances that are redundant and have no single point of failure</i> 		<i>Architectural security design concept depicting the requirements</i>	

5.2.5 WORK PACKAGE “E”: Network Management and Monitoring Solutions

5.2.5.1 Proposed Network Management Solution

- a. A centrally managed Network Management System shall be implemented.
- b. The NMS shall be an integral part of the overall Software Defined Network solution.
- c. All network and cyber security elements shall be fully monitored, controlled and maintained using the NMS.
- d. In cases where a single NMS tool is deemed to not be optimal to manage the complete environment a combination of products or software modules will be implemented in a structured well integrated solution that enables end-to-end visibility of network performance, trouble shooting and optimisation. Note: Should the proposed solution consists of various software packages the bidder shall:
 1. Provide all in detail, explain the reason for using multiple different software products.
 2. Clearly indicate the benefits of the proposed solution.
 3. Indicated in detail how the various products shall be integrated to achieve an end-to-end solution.
 4. Provide references and detailed case-studies where to proposed products have been successfully integrated and deployed in a network of similar size and complexity.

5.2.5.2 Solution Specifications

These requirements cover the solution capabilities to be achieved by the Network Management and Monitoring Solutions, below is the subset of the list of design requirements and objectives

TECHNOLOGY	SPECIFICATION
NMS Solution	<p>Capabilities:</p> <ol style="list-style-type: none">a. Network Management System (all Hardware, Software and Licensing) addressing the following (FCAPS):<ol style="list-style-type: none">1. Authentication & Logging2. Change and Configuration Management3. Usage Metering & Billing4. GUI-Based, graphical Network Device and Services Monitoring & Reporting5. GUI-based Service Provisioning6. Network Security Management (pro-active monitoring and risk mitigation)7. Fault Management8. Performance Management9. All necessary software licences for all modules of the suite or independent packages.b. FCAPS capable Network Management System<ol style="list-style-type: none">1. Fault Management;2. Configuration Management;3. Accounting Management;4. Performance Management;5. Security Management;

Warranty	36 months Manufacturer's Warranty Minimum repair or replace
Software licences	36 months

Supply and Implement a Network Management Solution (NMS) in Gauteng. This work package sees the supply and implementation of a Tier 1 Network

Management System. The scope includes all software, licencing, equipment, as well as professional services required to deliver a fully functional Network Management System. The proposed solution shall be in line with ISO – FCAPS and must be implemented in line with ITIL processes.

The proposed product and solution shall be scaled to be extended to manage the networks in all regions (Gauteng, Western Cape, KZN and Eastern Cape) as well.

5.2.5.3 Provide Professional Services for

a. Architecture and design (high level and Detail level),

1. The architectures developed based on best practices, given the operational environment within which the solution shall be deployed.
2. The Bidder shall provide all the resources required for creating the high level and detail level designs.
3. Relevant industry best practices and standards shall be followed in the design of solution.
4. The bidder will generate and prepare all necessary documents for approval by PRASA.
5. A High Level and Detail Low Level Design document will be compiled
 - i. This document will have all the information necessary to be able to setup and deploy all software modules required.
 - ii. This will also include:
 - Compilation of NMS Plans
 - Develop NMS Matrices
 - iii. This document will contain all information required as a singular guide to build the complete NMS Solution from scratch.
 - iv. Further detail of the exact content will be discussed and agreed to during project initialisation.

b. NMS Business processes, in line with ITIL 4

c. Workflow for Alerts and escalations

d. Project Management (in line with section 5)

e. Comprehensive NMS Roll-Out Plan

1. A detailed NMS Roll-Out plan shall be developed.
2. This plan will set out in a step-by-step fashion exactly how the NMS will be deployed.
3. The NMS Roll-out plan has to consider the necessary correlation and sequencing in comparison with the other work packages in this project.

f. Supply all hardware, software and licences as may be required.

1. Equipment, software and licences shall be supplied and delivered, based on the detail designs, Solution Acceptance and BoM.
- g. Configure and Setup all equipment and software**
1. The contractor shall be responsible for configuring all equipment and software.
 2. Labour, travelling and transportation costs associated with these activities shall be included in the offer.
 3. The bidder shall describe in detail how historical and near-real- time network performance data can be shared with 3rd party applications.
 4. The bidder shall describe in detail how near-real-time alerts and escalations can be communicated to 3rd party applications.
- h. Test and Commission the Network Management System**
- i. Detail As-Built Documentation.**

5.2.5.4 Technical Assessment of the Solution – Work Package E : Network Management and Monitoring Solutions

ALL the requirement items in the tables below are **MANDATORY**. Failure to meet all the below products' requirements, bidders will be disqualified automatically under Evaluation Stage 1C.

<i>Item</i>	<i>Minimum Requirement</i>	<i>Compliance Yes/No</i>	<i>Evidence</i>	<i>Reference To Information e.g. File A, Section X, Page Y</i>
1	<p>Bidder must provide a proposal design that depicts that they understand the requirements. The proposal must cover:</p> <ul style="list-style-type: none"> - <i>Solution that is centrally managed</i> - <i>Solution that is able to manage and monitor all network and security elements.</i> - <i>Zero Touch Provisioning</i> 		<i>Network Management proposal</i>	

5.2.6 WORK PACKAGE “F”: CABLING AND FACILITIES (COOLING, UPS, POLES, etc.)

STRUCTURED CABLING

5.2.6.1. NETWORK CABINETS

Item	Minimum Specifications
Product description	Rack - ventilated (42U, 22U, 18U,15U, 9U as per the BOQ)
Product type	Ventilated rack
Rack sized	19"
Dimensions	Minimum 600mm x 600mm to fit the active components
Construction	<ul style="list-style-type: none">• The front Clear Glass door, back door mesh door.• Front/rear locking double section door, enable ventilation and reliable operation.• Wire path on the top and bottom can be closed.
Power	<ul style="list-style-type: none">• Pre-wired 240V AC conditioned grounded power circuit• 6 Outlet Power Distribution Unit Included• Supplied with Earth Bond Kit and Cage nuts

5.2.6.2. CABLES

i) HORIZONTAL CABLING AND PATCH/FLY LEADS

	Category 6A UTP 4-Pair Cable
Item	Minimum specifications
Industry Compliance	<ul style="list-style-type: none">• ISO/IEC 11801 Ed. 2.2 (Class EA)• ISO/IEC 61156-5 (Category 6A)• TIA-568-C.2 (Category 6A)• LSOH: ISO/IEC 60332, IEC 60754, IEC 61034

ii) CAT 6A UTP PATCH PANELS

Item	Minimum specifications	Proposed Solution
Ports	24/48 Ports	
Characteristics	For 19" rack size	
Warranty	36 months End-to-End Manufacturer's Warranty on Cabling System (Attach Manufacturer's Warranty Statement)	

5.2.6.3. FIBRE CABLING

i) BACKBONE MULTIMODE FIBRE OPTIC CABLE

Item	Minimum Specifications	Proposed Solution	Meet Requirements
Armour	Corrugated Steel Tape Armour		
Cable characteristics	- Support for 10G - Multimode - 2 cores		

5.2.6.4. UTILITY POLES



	Solar powered utility Pole solution for mounting of Wifi Access Points.
Item	Minimum Specifications

Features	<ul style="list-style-type: none"> • Solar panels and batteries and other accessories must be configured to support up to 4 outdoor APs per pole with operating times of 24 hours in bad weather conditions. • With waterproof cabinet for batteries and accessories • Poles must be Hot Dip Galvanised by a SABS approved Galvaniser in accordance to SANS 121 / SABS 1461 Specification. • Poles up to 15m height
Support	Locally Available Technical Support Services (Manufacturer's Letter of Authorization Mandatory)
Warranty	Minimum 3 years

5.2.6.5. CABINET COOLING (As and when required)

Item	Minimum Specifications
Features	<ul style="list-style-type: none"> • Bidder must provide appropriate cooling for the operation of the proposed network equipment unless if the equipment are deployed in PRASA's existing server rooms or datacenters. • The cooling capacity must specified in line with the OEM's equipment requirements
Support	Locally Available Technical Support Services (Manufacturer's Letter of Authorization Mandatory)
Warranty	Minimum 3 years

5.2.6.6. RACK MOUNT UPS

Item	Minimum Specifications
Features	<p>Output power capacity: 2.1kWatts / 3.0kVA</p> <p>Rack Height: 2U</p> <p>Nominal Output Voltage: 230V</p> <p>Nominal Input Voltage: 230V</p> <p>Output Frequency (sync to mains): 50 Hz Sync to mains</p> <p>Topology: Line interactive</p> <p>Waveform type: Sine wave</p> <p>Batteries & Runtime</p> <ul style="list-style-type: none"> ➤ Battery Type: Maintenance-free sealed Lead-Acid battery with suspended electrolyte : leakproof ➤ Typical recharge time: 3 hour(s) ➤ Replacement Battery: YES ➤ RBC Quantity: 1 ➤ Runtime: Minimum 3 hours

Management	<ul style="list-style-type: none"> ➤ Interface Port(s): USB ➤ Control panel: Multi-function LCD status and control console ➤ Audible Alarm: Alarm when on battery <ul style="list-style-type: none"> : distinctive low battery alarm : configurable delays
Support	Locally Available Technical Support Services (Manufacturer's Letter of Authorization Mandatory)
Warranty	Manufacturer's Limited Lifetime Warranty Minimum 3 years- repair or replace

5.2.6.6. Technical Assessment of the Solution – Work Package F

ALL the requirement items in the tables below are **MANDATORY**. Failure to meet all the below products' requirements, bidders will be disqualified automatically under Evaluation Stage 1C.

<i>Item</i>	<i>Minimum Requirement</i>	<i>Compliance Yes/No</i>	<i>Evidence</i>	<i>Reference To Information e.g. File A, Section X, Page Y</i>
1	Bidder must provide proof of accreditation for the cabling technologies proposed, for both copper and fibre optic cabling.		<i>Letter of accreditation from OEM / Certified / Letter / Authorised Installer</i>	
2	Bidder must provide proof that they are authorized to supply and support proposed UPS equipment and Cooling cabinets (where applicable)		<i>Authorization letter / certification</i>	

5.2.7 WORK PACKAGE “G”: Training and Knowledge Transfer

5.2.7.1 Work Package Requirements

This work package sees the provision of OEM accredited training services that will result in certified PRASA resources to provide Level 1 and Level 2 support at all tiers of the network, on all products supplied for work packages

- a. Provide detail information on certification programs of each OEM.
 1. List all courses / training modules.
 - List the relevant certification track for each Work Package.

- Provide the breakdown for Level 1 and level 2 support.
 - Detail description of each course / module
 - Indicated the duration of each
2. Provide the detail of the proposed accredited training centre.
- b. Provide OEM Accredited Technical Certification to PRASA personnel to provide level 1 and Level 2 support, at all tiers of the network, on all products supplied.
 - c. Provide OEM Accredited / Certified operator and administration training for all Application Software supplied.
 - d. The bidder shall include all costs related to certification of PRASA personnel to achieve level 1 and 2 support.
 1. Provision shall be made for six (6) PRASA resources to be certified, for each work package.
 2. Not more than three PRASA resources shall be scheduled at given training timeslot.
 3. The bidder shall assume that all resources identified for training has basic network and network security as well as ITIL foundation knowledge.
 - e. Provide a high-level training plan as part of the Project Management submission.

5.2.7.2 Technical Assessment of the Solution – Work Package G: Training and Knowledge Transfer

ALL the requirement items in the tables below are **MANDATORY**. Failure to meet all the below products' requirements, bidders will be disqualified automatically under Evaluation Stage 1C.

<i>Item</i>	<i>Minimum Requirement</i>	<i>Compliance Yes/No</i>	<i>Evidence</i>	<i>Reference To Information e.g. File A, Section X, Page Y</i>
1	Bidder must provide detailed training plan that indicate that they understand the requirements		<i>Training package proposal</i>	

5.2.8 WORK PACKAGE “H”: Network Maintenance and Support – 60 months

The project also seeks to establish a maintenance and support contract for of ALL EQUIPMENT AND SOFTWARE APPLICATIONS deployed in PRASA during this project. The maintenance contract shall provide for the replacement of network components when they fail and the provision of software patches when they become available

5.2.8.1 LEVEL 3 - Network Engineer - Onsite

- a. The project also seeks Level 3 support services by OEM certified network engineer for estimated 2496 hours over the five years contract term. The support hours to be consumed on “as and when” basis.
- b. This resource will ensure the design changes and modifications (Move, Add, Change or Delete – MACD) are approved and the implementation managed.
- c. This engineer will also manage, monitor and maintain all the network equipment and associated software in PRASA using the NMS and other specialised tools.
- d. This engineer will furthermore advise and guide the PRASA team in identifying and resolving network related issues.
- e. Travelling costs associated with these activities shall be included in the offer.
- f. Engineers shall undergo security vetting.

5.2.8.2 LEVEL 3 - Network Security Engineer – Onsite

- a. The project also seeks Level 3 support services by OEM certified network security engineer for estimated 2496 hours over the five years contract term. The support hours to be consumed on “as and when” basis.
- b. This resource will ensure that the ICT network security levels are maintained at all times.
- c. The engineer will define and review security policies, the design changes and modifications (Move, Add, Change or Delete – MACD) are approved and the implementation managed.
- d. This engineer will also manage, monitor and maintain all aspects of network security, both internally as well as inbound/outbound traffic.
- e. The engineer will be responsible for directing the hardening of both equipment and associated software in PRASA using the NMS and other specialised tools.
- f. This engineer will furthermore advise and guide the PRASA team in identifying and resolving network security related issues.
- g. The engineer will be responsible for maintaining wireless security.
- h. The engineer will be responsible for directing security tests (ethical hacking), analysing the results and making recommendations on how to improve the security.
- i. The engineer will furthermore guide the realisation of the total information security function.
- j. Travelling costs associated with these activities shall be included in the offer.
- k. Engineers shall undergo security vetting.

5.2.8.3 LEVEL 3 – Network and Security Engineer – Service Level Support

- a. This engineer (or a qualified, substitute engineer who knows the PRASA network) will be available remotely via telephone, email and VPN to assist the PRASA team in break-fixes when required.
 1. The engineer will be available to assist remotely within 1 hour of the company being informed of any problems.
 2. The company shall therefore operate a 24 hour 365 days/year call centre.
 3. If a call cannot be resolved remotely, within 1 hour from responding, the company shall dispatch an engineer to site.
 4. The engineer shall arrive onsite within 2 hours from the time it has been determined that the problem cannot be resolved remotely.
 5. Travelling costs associated with these activities shall be included in the offer.

5.2.8.4 Technical Assessment of the Solution – Work Package H: Network Maintenance and Support – 60 Months

ALL the requirement items in the tables below are **MANDATORY**. Failure to meet all the below products' requirements, bidders will be disqualified automatically under Evaluation Stage 1C.

<i>Item</i>	<i>Minimum Requirement</i>	<i>Compliance Yes/No</i>	<i>Evidence</i>	<i>Reference To Information e.g. File A, Section X, Page Y</i>
1	<i>Bidder must provide a support proposal that include</i> <ul style="list-style-type: none">- Network Engineer for 2496 hours- Security Engineer for 2496 hours and- Service Level Support		<i>Support proposal</i>	

5.6 GENERAL TECHNICAL COMPLIANCE REQUIREMENTS (ANNEXURE 3)

The bidder must commit to the items in ANNEXURE 3 and ensure that the requirements in ANNEXURE 3 are costed in the bidder's solution.

Failure to commit to the items in ANNEXURE 3 will lead to automatic disqualification.

6. TIME FRAMES / PROGRAMS

KEY MILESTONES

Activity	Duration	Start Date	End Date
Bid Advertising	21 Days	18 Aug 2021	17 Sep 2021
Non-Compulsory Briefing (Microsoft Teams) @ 10H30	1 Day	25 Aug 2021	25 Aug 2021
Written Q&A	3 Days	25 Aug 2021	27 Aug 2021
Bid Closing	1 Days	17 Sep 2021	17 Sep 2021
Evaluation of Proposals (Bidders note that PRASA may call for Presentation of bidders offers at any stage of the evaluation process)	TBA		
Sitting of Bid Evaluation Committee	TBA		
Bid Adjudication Committee	TBA		
FCIP	TBA		
Approval of FCIP Recommendation	TBA		
Award	TBA		
Contract Finalization and Loading	TBA		

7. MANDATORY SUBCONTRACTING

Subcontracting as per Section 9 of the Preferential Procurement Regulations: PRASA expects the bidders to subcontract 30% of the value of this contract in compliance with Section 9 of the Preferential Procurement Regulations. Failure to comply with this requirement will result in automatic disqualification.

The successful tenderer must subcontract a minimum of 30% of the value of this contract to:

1. An EME or QSE
2. An EME or QSE which is at least 51% owned by black people
3. An EME or QSE which is at least 51% owned by black people who are youth
4. An EME or QSE which is at least 51% owned by black people who are women
5. An EME or QSE which is at least 51% owned by black people with disabilities
6. An EME or QSE which is at least 51% owned by black people living in rural or underdeveloped areas or townships
7. A cooperative which is at least 51% owned by black people
8. An EME or QSE which is at least 51% owned by black people who are military veterans or
9. More than one of the categories referred to in paragraphs 1 to 8.

The bidders may subcontract any company provided that the company is registered on the National Treasury CSD database and is within the designated groups provided above. Or choose from the list provided under Annexure 5.

8. EVALUATION PROCESS

Interested bidders for this project shall be evaluated in terms for their administrative responsiveness, substantive responsiveness, technical/functional (capacity testing) evaluation and preference points. The evaluation committee shall use the following Evaluation Criteria depicted in table below for the selection of the preferred bidder that shall render / deliver the required works, goods and / or services.

EVALUATION CRITERIA	WEIGHTING
Stage 1A	Mandatory Compliance Requirements
Stage 1B	Basic Compliance Requirements
Stage 1C	Technical Mandatory Compliance Requirements – Section 5. All mandatory requirements in section 5 must be met, failure to meet all the mandatory requirements will lead to disqualification.
Stage 2	Technical/Functionality
Technical/Functional Requirements	Threshold of 80%
Stage 3	Price and BBBEE
Price	90
BBBEE	10
TOTAL	100

Table: Evaluation Process

9.1 STAGE 1A – Mandatory Requirements (Substantive Responsiveness)

If you do not submit the following documents your tender will be automatically disqualified:

No.	Description of requirement
a)	Completion of ALL RFP documentation (includes ALL declarations, ALL Standard Bidding Documents (SBD) and Commissioner of Oath signatures required)

No.	Description of requirement
b)	<p>In compliance with the compulsory subcontracting requirement as per Preferential Procurement Regulation, bidders must submit an MOU or Letter of intent signed by all parties indicating the names of companies that it intends subcontracting to, the nature of the works to be subcontracted and contract % that will be subcontracted.</p> <p>The successful bidder will be expected to submit a formal subcontracting agreement signed by all parties within 14 days of the award.</p>

9.2 STAGE 1B - Basic Compliance Requirements (Administrative Responsiveness)

If you do not submit the following basic compliance documents and should an award be made, these basic compliance documents must be made available within seven (7) days, failing of which the award will be recalled.

No.	Description of requirement
a)	Original or certified B-BBEE certificate issued by SANAS or Affidavit for QSEs and EMEs.
b)	In cases of JVs or consortiums, a combined B-BBEE certificate in the name of the JV/Consortium must be submitted
c)	CSD supplier registration number
d)	A valid and Original Tax Clearance Certificate (valid as at the closing date of this RFP) Or supply SARS Pin
e)	Company registration documents
f)	Copies of Directors' ID documents
g)	Signed Joint Venture, Consortium Agreement or Partnering Agreement (whichever is applicable) if the bidder is bidding as such

9.3 STAGE 1C - TECHNICAL MANDATORY COMPLIANCE

Technical Mandatory Compliance Requirements – Section 5. All mandatory requirements in section 5 must be met, failure to meet all the mandatory requirements will lead to disqualification.

9.4 STAGE 2 - Technical / Functionality Requirements

Qualified bidders from Stage 1 shall be evaluated on technicality / functionality after meeting all compliance requirements outlined above. The minimum threshold for the technical/functionality requirements is 80%. Bidders who score below the minimum requirement shall not be considered for further evaluation in stage 3.

Summary of the technical/functional requirements are presented in the table 19 below.

Table: Technical Evaluation Criteria

No.	CRITERIA	WEIGHT	SCORES
1	Project Management Skills and Experience	15	<p>The bidder is required to provide the detailed Curriculum Vitae of the Project Manager who will be assigned to the project who has acquired the following certification and skills:</p> <ul style="list-style-type: none"> a. Experience in management of IT Network Infrastructure projects that span across multiple buildings in multiple areas for installation and commission of at least 50 Routers or Switches, b. PMP Certification must be provided with the CV in order to be awarded points for this evaluation criteria. <p>Note:</p> <ul style="list-style-type: none"> i. PMP or Prince2 Certificates (or equivalent) must be provided with the Project Managers' CV in order to be considered to be awarded points for this evaluation criteria; in addition to ii. Relevant post certification experience which can be verified. <ul style="list-style-type: none"> 1: 0-2 Years Post Certification Experience in the management of projects of scope and size as highlighted in Point "a" above and supporting of services in the scope of the project 2: 3-4 Years Post Certification Experience in the management of projects of scope and size as highlighted in Point "a" above and supporting of services in the scope of the project 3: 5-6 Years Post Certification Experience in the management of projects of scope and size as highlighted in Point "a" above and supporting of services in the scope of the project 4: 7-8 Years Post Certification Experience in the management of projects of scope and size as highlighted in Point "a" above and supporting of services in the scope of the project 5: 9 Years and above Post Certification Experience in the management of projects of scope and size as highlighted in Point "a" above and supporting of services in the scope of the project.

2	<p>Experience and Track Record for <u>Provision and Maintenance of WAN and MAN Services</u></p> <p>Case Studies and References</p>	20	<p>In order to prove experience and understanding of the scope, size and scale of this project for WAN and MAN Services, the bidder is required to provide a minimum of three (3) successfully implemented and completed detailed case studies of:</p> <ul style="list-style-type: none"> a. MAN nodes in at least 2 metro area that covers the distance of at least 30 kilometre across the connected sites successfully implemented and completed. With at least 50 access nodes. b. WAN nodes in at least 3 sites connected in the WAN network. <p>Contactable references must be provided for each case study.</p> <ul style="list-style-type: none"> 1 : Requirements not met: Has not presented evidence of relevant experience and/ or one case study presented and/ or partial and/ or no reference as per points “a” and “b” above 2: Requirements partially met: Has implemented projects as per points “a” and “b” above of WAN and MAN services and one case studies presented and reference verification 3: Requirements partially met: Has implemented projects as per points “a” and “b” above of WAN and MAN services and two case studies presented and reference verification 4: Requirements partially met: Has implemented projects as per points “a” and “b” above of WAN and MAN services and three case studies presented and reference verification – on current and completed projects 5: Requirements fully met: Has implemented projects as per points “a” and “b” above of WAN and MAN services and three case studies presented and or reference verification – all projects completed
---	--	----	--

3	<p>Experience and Track Record for <u>Provision and Maintenance of LAN and Wi-Fi</u></p> <p>Case Studies and References</p>	20	<p>In order to prove experience and understanding of the scope, size and scale of this project for LAN and Wi-Fi Services, the bidder is required to provide a minimum of three (3) successfully implemented and completed detailed case studies of:</p> <ul style="list-style-type: none"> a. LAN network that connected the at least 500 users in the same enterprise building. b. WIFI network that serves at least 1,000 users in the enterprise campus and at least 10 remote areas centrally managed by the Wi-Fi controller <p>Contactable references must be provided for each case study.</p> <ul style="list-style-type: none"> 1 : Requirements not met: Has not presented evidence of relevant experience and/ or one case study presented and/ or partial and/ or no reference 2: Requirements partially met: Has implemented projects as per points “a” and “b” above of LAN and Wi-Fi services and one case studies presented and reference verification 3: Requirements partially met: Has implemented projects as per points “a” and “b” above of LAN and Wi-Fi services and two case studies presented and reference verification 4: Requirements partially met: Has implemented projects as per points “a” and “b” above of LAN and Wi-Fi services and three case studies presented and reference verification – on current and completed projects 5: Requirements fully met: Has implemented projects as per points “a” and “b” above of LAN and Wi-Fi services and three case studies presented and or reference verification – all projects completed
---	---	----	---

4	<p>Experience and Track Record for <u>Provision and Maintenance of Data Centre Network</u></p> <p>Case Studies and References</p>	10	<p>In order to prove experience and understanding of the scope, size and scale of this project for Data Center network, the bidder is required to provide a minimum of three (3) successfully implemented and completed detailed case studies of:</p> <ol style="list-style-type: none"> Data Center network that connected at least 20 servers in the same data center Pod Data Center network that connected to the Data Recovery site (DR) Data center that is at least 20 Kilometre away. <p>Contactable references must be provided for each case study.</p> <ol style="list-style-type: none"> 1 : Requirements not met: Has not presented evidence of relevant experience and/ or one case study presented and/ or partial and/ or no reference 2: Requirements partially met: Has implemented projects as per points “a” and “b” above of all the elements of Data Center network and one case studies presented and reference verification 3: Requirements partially met: Has implemented projects as per points “a” and “b” above of Data Center network and two case studies presented and reference verification 4: Requirements partially met: Has implemented projects as per points “a” and “b” above of all the elements of Data Center network and three case studies presented and reference verification – on current and completed projects 5: Requirements fully met: Has implemented projects as per point points “a” and “b” of Data Center network and three case studies presented and or reference verification – all projects completed
---	---	----	--

5	<p>Experience and Track Record for Provision and Maintenance of Network Security solution</p> <p>Case Studies and References</p>	10	<p>In order to prove experience and understanding of the scope, size and scale of this project for Network Security solution, the bidder is required to provide a minimum of three (3) detailed successfully implemented and completed case studies of:</p> <p>a. Network security infrastructure: Redundant firewalls shall be deployed for:</p> <ul style="list-style-type: none"> • internal and external data traffic protection • Protection of between the servers/applications within the datacentre. Data Center (DC services FW) for 3 tiered-application stack traffic (e.g Web-Application-Database) • Protection of in and out of the datacentre. The Data Centers (DC perimeter firewalling, with IDS capabilities or out of the trusted internal network (like peering with 3rd party links) <p>Contactable references must be provided for each case study.</p> <p>1 : Requirements not met: Has not presented evidence of relevant experience and/ or one case study presented and/ or partial and/ or no reference</p> <p>2: Requirements partially met: Has implemented projects as per point “a” above of all the elements of Network Security solution and one case studies presented and reference verification</p> <p>3: Requirements partially met: Has implemented projects as per point “a” above of all the elements of Network Security solution and two case studies presented and reference verification</p> <p>4: Requirements partially met: Has implemented as per point “a” above of all the elements of Network Security solution and three case studies presented and reference verification – on current and completed projects</p> <p>5: Requirements fully met: Has implemented projects as per point “a” above of Network Security solution and three case studies presented and or reference verification – all projects completed</p>
6	<p>Project Methodology and Plan</p>	15	<p>Project Schedule/Program</p> <p>1: Project schedule not provided;</p> <p>2: Project schedule shows estimated start and finish dates.</p> <p>3: Project schedule shows estimated start and finish dates and major milestones</p> <p>4: Project schedule shows estimated start and finish dates, major milestones and estimated duration to reach works completion; and</p> <p>5: Project schedule shows estimated start and finish dates, major milestones and estimated duration to reach works</p>

			completion. Project schedule also contains information on mitigations for unforeseen delays or occurrences.
7	Financial Capability Using Current Ratio Bidders to submit their latest financial statement.	10	<p>The current ratio is a liquidity ratio which estimates the ability of a company to pay back short-term obligations. This ratio is also known as cash asset ratio, cash ratio, and liquidity ratio. A higher current ratio indicates the higher capability of a company to pay back its debts. The formula used for computing current ratio is: Current Assets / Current Liabilities.</p> <p>1: Current ratio of less than 0.5 2: Current ratio of 0.5 or more 3: Current ratio of 0.75 or more 4: Current ratio of 1 or more 5: Current ratio of 1.5 or more</p>
	Total	100	

1 = Poor information submitted, 2 = Fair/average, 3 = Good, 4 = acceptable or very good and 5 = Excellent.

9.5 STAGE 3 - PRICING AND BBBEE

Include or attach detailed pricing schedule

The following formula shall be used by the Bid Evaluation Committee to score potential bidders on pricing:

$$P_s = 90 \left[1 - \frac{P_t - P_{\min}}{P_{\min}} \right]$$

Where:

P_s = Points scored for the price of tender under consideration;

P_t = Rand value of the tender under consideration;

P_{\min} = Rand value of the lowest acceptable tender.

The minimum qualifying criteria for pricing is 90 points as per the standard Evaluation Criteria presented in figure above.

The BBBEE component of the evaluation process is weighted at 10 points in figure above of the standard Evaluation Criteria outlined above. Bidders will be awarded points based on the level of the BBBEE status presented in the BBBEE Certificate issued by an approved agency certified by SANAS. Details of the allocation of points by the Evaluation Committee are presented in figure below.

B-BBEE STATUS LEVEL OF CONTRIBUTOR	NUMBER OF POINTS(90/10 SYSTEM)
1	10
2	9
3	6
4	5
5	4
6	3
7	2
8	1
Non-Compliant Contributor	0

Figure : BBBEE Evaluation Criteria