Eskom	Standard	Technology

Title: **IP ADDRESS MANAGEMENT SOLUTION FUNCTIONAL SPECIFICATION**

Unique Identifier:	**240-170000369**
Alternative Reference Number:	**N/A**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**1**
Total Pages:	**16**
Next Review Date:	**March 2026**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Bongani Shezi	Cornelius Naidoo	Nelson Luthuli
Senior Engineer Telecoms Technology and Support	Manager Telecomms Technology and Support	Senior Manager PTM&C Engineering (Acting)
Date: 11 February 2021	Date: 2021/02/18	Date: 26/02/2021

Supported by SCOT/SC

Kgomotso Setlhapelo
SCOT/SC Chairperson

Date: 18 February 2021

PCM Reference: **240-53458797**
SCOT Study Committee Number/Name: **Telecommunications Study Committee**

Content

1. Introduction

With the rapid growth of the number of devices being connected to the Eskom Telecommunications' IP network, and the growing list of services being provisioned on this network, it is becoming more difficult for network administrators to manage and maintain the increasing number of IP addresses, devices and services. Along with other network-related responsibilities, network administrators are burdened with additional tasks like allocating, reallocating, assigning, and tracking of IP addresses. This document specifies the minimum functional requirements for an IP Address Management solution for the Eskom Telecommunications network.

2. Supporting clauses

2.1 Scope

This document details the minimum requirements that an IP address management for deployment at the ET NMC shall adhere to.

2.1.1 Purpose

This document is intended for use as part of an enquiry documentation to the market, in procuring an IP address management system/solution for the Eskom Telecommunications network.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited Divisions.

2.2 Normative/informative references

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

2.2.1 Normative

[1] ISO 9001, Quality Management Systems.

[2] 240-55410927 Cyber Security Standard for Operation Technology

[3] 240-86458714 Generic Requirements Specification for a Telecommunications Network Management Solution

[4] 240-135089195 Generic Technical Requirements for Eskom Telecoms Contracts

2.2.2 Informative

[5] TekTools. What is IPAM? How Does It Help With Management of IP Addresses?.[Online] 30 May 2020. [Cited: 23 October 2020] https://www.tek-tools.com/network/best-ipam-tools

[6] Gartner. Definition of Multitenancy – Gartner Information Technology Glossary. [Online] 2020. [Cited: 28 October 2020] https://www.gartner.com/en/information-technology/glossary/multitenancy

[7] Device42. IPAM – Device42 Documentation [Online] 2020. [Cited: 18 November 2020] https://docs.device42.com/ipam/

[8] Infoblox. [Datasheet] Infoblox Trinzic DDI Appliances [Online] 2020. [Cited: 2 December 2020] https://insights.infoblox.com/resources-datasheets/infoblox-datasheet-ddi-appliances

[9] Solarwinds. IP Address Manager Data Sheet [Online] 2020. [Cited: 7 December 2020] https://www.solarwinds.com/-/media/solarwinds/swdcv2/licensed-products/ip-address-manager/resources/datasheets/ipam-datasheet.ashx?rev=8ad84889649242be848fd4bb3ec6a3fc

2.3 Definitions

2.3.1 General

Definition	Description
DHCP	DHCP is a network management protocol used to assign static and dynamic IP addresses to authorized IP devices. DHCP servers automate the process of assigning IP addresses; at the same time, they need to be configured, used, and monitored properly to maintain availability and security of IP addresses. DHCP management also helps with automation and optimization of IP space in the network.
DNS	DNS is one of the most important components of the IP network. It ensures the quick and efficient availability of content for network users. With proper DNS management, administrators can keep DNS servers up to date in accordance with IP address modifications.
IP Inventory Management	IP address inventory management includes planning, collection, allocation, and management of IP addresses. This also includes maintaining real-time updates and the status of the IPs within a network, so an organization's fixed IP space can be used accordingly.
IPAM	The role of an IP Address Management solution (IPAM) is to automate IP address management tasks and allocate data in a centralized, easy-to-access, and user-friendly interface. It helps organizations keep track of IP addresses within a network and helps ensure seamless business connectivity.
Multitenancy	Multitenancy is a reference to the mode of operation of software where multiple independent instances of one or multiple applications operate in a shared environment. The instances (tenants) are logically isolated, but physically integrated. The degree of logical isolation must be complete, but the degree of physical integration will vary.

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ET	Eskom Telecommunications
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPAM	IP Address Management
IPv4	IP version 4
IPv6	IP version 6
LAN	Local Area Network
MAC	Media Access Control

Abbreviation	Description
NAT	Network Address Translation
NMC	Network Management Centre
PTR	Pointer
SCOT	Steering Committee on Technologies
SNMP	Simple Network Management Protocol
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

2.5 Roles and responsibilities

2.5.1 Eskom's responsibilities

a) Create a conducive environment for the supplier by making relevant resources (people and workspace) available

b) Provide network access in accordance with the relevant Eskom security policies/procedures.

c) Provide support functions and services required for the solution

d) Provide technical support and specialist knowledge of the NMC environment (power, cooling, cabling, cabinet space, wiring, Local Area Network (LAN), systems, applications) and the Eskom Telecommunications' Wide Area Network (WAN).

2.5.2 Supplier's responsibilities

a) Design, development, implementation, testing, installation, commissioning, and support of the solution.

b) Training and skills transfer on the operation, administration and maintenance of the solution

c) Handover of solution documents (design, planning, maintenance, administration and operation)

2.6 Process for monitoring

The implementation of this document will primarily be through a procurement/commercial process. Revision to the content of this document will be through the Steering Committee on Technologies (SCOT) governance process. The management of the document will be done according to Eskom's document and records management standards.

2.7 Related/supporting documents

240-86458714 Generic Requirements Specification for a Telecommunications Network Management Solution

240-135089195 Generic Technical Requirements for Eskom Telecoms Contracts

3. IP Address Management Solution

3.1 Solution architecture

The solution architecture and other functional, and integration requirements, except for those specified in this document are as described in [3][3] 240-86458714 Generic Requirements Specification for a Telecommunications Network Management Solution.

3.2 Inventory management functions

IP address inventory management includes planning, collection, allocation, and management of IP addresses. This also includes maintaining real-time updates and the status of the IPs within a network, so an organization's fixed IP space can be used accordingly.

The solution shall support planning, collection, and allocation of IP addresses. At minimum the management functions tools and utilities shall include:

3.2.1 Data collection and discovery:

3.2.1.1 IP discovery is the process of scanning the network for IP devices through one or several methods like SNMP, ICMP, or neighbourhood scanning. The solution shall support network auto-discovery, IP Addresses, MAC Addresses, and DNS Infrastructure. The following methods of adding or discovering IP Addresses and related information should at minimum be supported:

a) SNMP Discovery: SNMP auto-discovery to gather subnets, IP to MAC Address relationships, and MAC Address to Switch Port relationship information.

b) Auto Discovery (or neighbour discovery): Using the auto-discovery (or neighbour discovery tools) to discover multiple multi-vendor devices and systems in the network and establish connections with appropriate resources to collect critical data, including their IP and MAC Address details.

c) Ping Sweep: Ping sweep utility (or similar) to keep the IP Address information up-to-date.

3.2.1.2 Importing of existing IP addresses from Microsoft Excel & CSV spreadsheets.

3.2.1.3 Active scanning of the network for IP devices through one or several methods like SNMP, ICMP, or neighbourhood scanning (and polling of devices to discover subnets from the routing table of the router).

3.2.1.4 Active scanning to discover and track subnets and associated address blocks.

3.2.1.5 Scheduling of automatic scanning for both your IPv4 and IPv6 address space.

3.2.1.6 Adding and importing of IP Addresses and related information.

3.2.2 Problem detection and troubleshooting:

3.2.2.1 Automatic and proactive detection of IP address problems that may result in network disruptions. These include: detection of IP address problems, notification of IP address changes in the network, IP address conflicts and non-availability of IP addresses due to full subnets.

3.2.2.2 Maintenance of historical data on IP address usage to assist in troubleshooting (e.g., which device had the IP first during an IP address conflict and remote shutdown option, to immediately cut-off network connectivity of the conflicting device).

3.2.2.3 Event recording/logging of all IP-related events by keeping detailed activity logs to assist in retracing events leading up to IP conflicts and other IP-related issues.

3.2.2.4 Provision of a single view of IP addresses and corresponding endpoint connection/location details, e.g., switch port details and/or user information. This enables improved troubleshooting and enhanced network access protection with port shutdown. This may assist in proactive maintenance by tracking down and resolving network issues before they cause a major problem.

3.2.3 Administration and management:

3.2.3.1 The solution shall support management of IPv4 and IPv6 addresses. At minimum the following functionality shall be supported: the management functions tools and utilities for DNS Records, DNS Zones, IP Addresses, IP NAT/Map, MAC Addresses, Subnet Tree View, Subnets, Switch Ports, Switch Templates, VLANs and VRF Groups.

3.2.3.2 Assist in the monitoring of suspicious activity in the network and tracking down of rogue devices that may be a threat to the network.

3.2.3.3 Search functions to assist in quick and easy access to IP address data, and to search for available IPs.

3.2.3.4 Resources to assist in the efficient allocation of the managed IP address space into subnets sized appropriately for the extent and traffic of the network.

3.2.3.5 Navigation to a target subnet, viewing, and selecting an available IP address.

3.2.3.6 Identifying transient IP addresses and/or orphaned IP addresses.

3.2.3.7 Creation of an up to date IP address map of the network by directly pulling data from router configurations and connected machines.

3.2.3.8 Access to utilization data on essential metrics that may assist with network and/or resource planning.

3.2.3.9 Automated reporting to track IP requests for compliance or change management purposes.

3.2.3.10 Customizable dashboard to include resources like top 10 data, recent events, IP conflict monitor, etc.

3.3 Multitenancy requirements

Multitenancy is a reference to the mode of operation of software where multiple independent instances of one or multiple applications operate in a shared environment. The instances (tenants) are logically isolated, but physically integrated. The degree of logical isolation must be complete, but the degree of physical integration will vary.

The solution shall support at minimum the following multi-tenancy use cases:

a) Restrict access by geographic location, department, division, corporate entity, and so on.

b) A user to have access to just one department while another user has access to all departments within a division.

c) Allocate subnets to customers or racks to customers.

d) Restrict customer access to the specific subnets and racks assigned to the customer where the service provider can see all subnets and racks:

   1) Buildings, Rooms, Racks

   2) Object Categories, VRF Groups, Subnet Categories

   3) Purchases, Vendors, Customers

3.4 DHCP and DNS Management

3.4.1 DNS management functions

3.4.1.1 The solution shall support monitoring and management of multivendor DNS zones, records and services, including capabilities to track and report on DNS record changes.

3.4.1.2 The solution shall support the monitoring of DNS zones from multiple cloud accounts and displaying them in a single view, with support for search and filter by DNS record type.

3.4.1.3 The solution shall have functions to automatically detect and point out any mismatch in DNS forward and reverse record entries. Disparities in the records should be easily identifiable.

3.4.1.4 The solution shall support functions to automatically create DNS PTR records when registering new devices into DNS zones. This could assist in ensure preventing and eliminating DNS record mismatches and the possible DNS issues due to human error.

3.4.2 DHCP management functions

3.4.2.1 The solution shall support monitoring and management of multivendor DHCP zones, records and services, including capabilities to track and report on DNS record changes

3.4.2.2 The solution shall support functions for DHCP split scope configuration for high availability and load balancing of critical DHCP services. Preferably in a centralized interface with visibility into related scopes and scope distribution across subnets.

3.4.2.3 The solution shall support functions to monitor and manage DHCP failover relationships (load balancing and hot standby configurations) to ensure continuous availability of DHCP services to clients.

3.4.2.4 The solution shall support functions to directly configure standard DHCP options for a multi-vendor DHCP servers without having to log in to the DHCP server or the use of CLI commands.

3.4.2.5 Any DHCP configuration changes made from the solution shall be automatically synced to the respective server

3.4.2.6 The solution shall support DHCP configuration for remoteboot devices.

3.4.3 Integrated DHCP and DNS Configuration Management

3.4.3.1 The solution shall work with multi-vendor DHCP and DNS services. The supplier shall provide a list of the vendors that are supported by their solution.

3.4.3.2 In order for the solution to easily integrate with the installed base, Microsoft DNS and DHCP services shall be supported, as a minimum. The supplier to specify supported versions. If additional proprietary software and/or hardware is required to support the Microsoft DNS and DHCP services, it should be listed, and be included in the solution offering.

3.4.3.3 The DHCP and DNS changes made in the solution should be seamlessly propagated to the respective servers, promoting a single management interface for these services.

3.5 Support and maintenance

The solution support and maintenance requirements and other related requirements, except for those specified in this document are as described in [4] [3]240-135089195 Generic Technical Requirements for Eskom Telecoms Contracts.

4. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Cornelius Naidoo	Telecomms T&S Middle Manager – PTM&C
Barry Clayton	Chief Engineer – Tx Secondary Plant, Work Planning and Centralised Services
Alison Maseko	Senior Manager – Eskom Telecommunications
Lenah Mothata	Senior Manager – Grids
Botse Sikhwitshi	Senior Manager – Group Security (Acting)
Maureen Mokone	Senior Manager – GIT
Prudence Madiba	Senior Manager – Gx
Sikelela Mkhabela	Senior Manager – Dx

5. Revisions

Date	Rev	Compiler	Remarks
March 2021	1	B Shezi	Document required for a management solution for the IP addresses in ET.

6. Development team

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

- Bongani Shezi

7. Acknowledgements

The following people were consulted during the development of this document:

- Joel Mataboge
- Matthew Taljaard
- Nompumelelo Khumalo
- Nontokozo Xulu
- Oscar Ngwenya
- Philla Kgole
- Pieter Mocke
- Sandra Makhatini
- Wicus van Aswegen
- Zwelandile Mbebe

Annex A – Schedule of Compliance

Item	Description	Schedule A	Schedule B	Reference/Comment
3	IP Address Management Solution	(Eskom's requirement statement)	(Supplier's compliance statement)	(Supporting evidence)
3.1	Solution architecture			
	As described in [3] 240-86458714 Generic Requirements Specification for a Telecommunications Network Management Solution.	State Compliance & Provide Evidence		
3.2	Inventory management functions			
	The solution shall support planning, collection, and allocation of IP addresses. At minimum the management functions tools and utilities shall include:	State Compliance		
3.2.1	Data collection and discovery:			
3.2.1.1	IP discovery is the process of scanning the network for IP devices through one or several methods like SNMP, ICMP, or neighbourhood scanning. The solution shall support network auto-discovery, IP Addresses, MAC Addresses, and DNS Infrastructure. The following methods of adding or discovering IP Addresses and related information should at minimum be supported:			
a)	SNMP Discovery: SNMP auto-discovery to gather subnets, IP to MAC Address relationships, and MAC Address to Switch Port relationship information.	State Compliance & Provide Evidence		
b)	Auto Discovery (or neighbour discovery): Using the auto-discovery (or neighbour discovery tools) to discover multiple multi-vendor devices and systems in the network and establish connections with appropriate resources to collect critical data, including their IP and MAC Address details.	State Compliance & Provide Evidence		

Item	Description	Schedule A	Schedule B	Reference/Comment
c)	Ping Sweep: Ping sweep utility (or similar) to keep the IP Address information up-to-date.	State Compliance & Provide Evidence		
3.2.1.2	Importing of existing IP addresses from Microsoft Excel & CSV spreadsheets.	State Compliance & Provide Evidence		
3.2.1.3	Active scanning of the network for IP devices through one or several methods like SNMP, ICMP, or neighbourhood scanning (and polling of devices to discover subnets from the routing table of the router).	State Compliance & Provide Evidence		
3.2.1.4	Active scanning to discover and track subnets and associated address blocks.	State Compliance & Provide Evidence		
3.2.1.5	Scheduling of automatic scanning for both your IPv4 and IPv6 address space.	State Compliance & Provide Evidence		
3.2.1.6	Adding and importing of IP Addresses and related information.	State Compliance & Provide Evidence		
3.2.2	Problem detection and troubleshooting:			
3.2.2.1	Automatic and proactive detection of IP address problems that may result in network disruptions. These include: detection of IP address problems, notification of IP address changes in the network, IP address conflicts and non-availability of IP addresses due to full subnets.	State Compliance & Provide Evidence		
3.2.2.2	Maintenance of historical data on IP address usage to assist in troubleshooting (e.g., which device had the IP first during an IP address conflict and remote shutdown option, to immediately cut-off network connectivity of the conflicting device).	State Compliance & Provide Evidence		
3.2.2.3	Event recording/logging of all IP-related events by keeping detailed activity logs to assist in retracing events leading up to IP conflicts and other IP-related issues.	State Compliance & Provide Evidence		

Item	Description	Schedule A	Schedule B	Reference/Comment
3.2.2.4	Provision of a single view of IP addresses and corresponding endpoint connection/location details, e.g., switch port details and/or user information. This enables improved troubleshooting and enhanced network access protection with port shutdown. This may assist in proactive maintenance by tracking down and resolving network issues before they cause a major problem.	State Compliance & Provide Evidence		
3.2.3	Administration and management:			
3.2.3.1	The solution shall support management of IPv4 and IPv6 addresses. At minimum the following functionality shall be supported: the management functions tools and utilities for DNS Records, DNS Zones, IP Addresses, IP NAT/Map, MAC Addresses, Subnet Tree View, Subnets, Switch Ports, Switch Templates, VLANs and VRF Groups.	State Compliance & Provide Evidence		
3.2.3.2	Assist in the monitoring of suspicious activity in the network and tracking down of rogue devices that may be a threat to the network.	State Compliance & Provide Evidence		
3.2.3.3	Search functions to assist in quick and easy access to IP address data, and to search for available IPs.	State Compliance & Provide Evidence		
3.2.3.4	Resources to assist in the efficient allocation of the managed IP address space into subnets sized appropriately for the extent and traffic of the network.	State Compliance & Provide Evidence		
3.2.3.5	Navigation to a target subnet, viewing, and selecting an available IP address.	State Compliance & Provide Evidence		
3.2.3.6	Identifying transient IP addresses and/or orphaned IP addresses.	State Compliance & Provide Evidence		
3.2.3.7	Creation of an up to date IP address map of the network by directly pulling data from router configurations and connected machines.	State Compliance & Provide Evidence		

Item	Description	Schedule A	Schedule B	Reference/Comment
3.2.3.8	Access to utilization data on essential metrics that may assist with network and/or resource planning.	State Compliance & Provide Evidence		
3.2.3.9	Automated reporting to track IP requests for compliance or change management purposes.	State Compliance & Provide Evidence		
3.2.3.10	Customizable dashboard to include resources like top 10 data, recent events, IP conflict monitor, etc.	State Compliance & Provide Evidence		
3.3	Multitenancy requirements			
	Multitenancy is a reference to the mode of operation of software where multiple independent instances of one or multiple applications operate in a shared environment. The instances (tenants) are logically isolated, but physically integrated. The degree of logical isolation must be complete, but the degree of physical integration will vary.	State Compliance & Provide Evidence		
	The solution shall support at minimum the following multi-tenancy use cases:	State Compliance & Provide Evidence		
a)	Restrict access by geographic location, department, division, corporate entity, and so on.	State Compliance & Provide Evidence		
b)	A user to have access to just one department while another user has access to all departments within a division.	State Compliance & Provide Evidence		
c)	Allocate subnets to customers or racks to customers.	State Compliance & Provide Evidence		
d)	Restrict customer access to the specific subnets and racks assigned to the customer where the service provider can see all subnets and racks:	State Compliance & Provide Evidence		
1)	Buildings, Rooms, Racks	State Compliance & Provide Evidence		

Item	Description	Schedule A	Schedule B	Reference/Comment
2)	Object Categories, VRF Groups, Subnet Categories	State Compliance & Provide Evidence		
3)	Purchases, Vendors, Customers	State Compliance & Provide Evidence		
3.4	DHCP and DNS Management			
3.4.1	DNS management functions			
3.4.1.1	The solution shall support monitoring and management of multivendor DNS zones, records and services, including capabilities to track and report on DNS record changes.	State Compliance & Provide Evidence		
3.4.1.2	The solution shall support the monitoring of DNS zones from multiple cloud accounts and displaying them in a single view, with support for search and filter by DNS record type.	State Compliance & Provide Evidence		
3.4.1.3	The solution shall have functions to automatically detect and point out any mismatch in DNS forward and reverse record entries. Disparities in the records should be easily identifiable.	State Compliance & Provide Evidence		
3.4.1.4	The solution shall support functions to automatically create DNS PTR records when registering new devices into DNS zones. This could assist in ensure preventing and eliminating DNS record mismatches and the possible DNS issues due to human error.	State Compliance & Provide Evidence		
3.4.2	DHCP management functions			
3.4.2.1	The solution shall support monitoring and management of multivendor DHCP zones, records and services, including capabilities to track and report on DNS record changes	State Compliance & Provide Evidence		
3.4.2.2	The solution shall support functions for DHCP split scope configuration for high availability and load balancing of critical DHCP services. Preferably in a centralized interface with visibility into related scopes and scope distribution across subnets.	State Compliance & Provide Evidence		

Item	Description	Schedule A	Schedule B	Reference/Comment
3.4.2.3	The solution shall support functions to monitor and manage DHCP failover relationships (load balancing and hot standby configurations) to ensure continuous availability of DHCP services to clients.	State Compliance & Provide Evidence		
3.4.2.4	The solution shall support functions to directly configure standard DHCP options for a multi-vendor DHCP servers without having to log in to the DHCP server or the use of CLI commands.	State Compliance & Provide Evidence		
3.4.2.5	Any DHCP configuration changes made from the solution shall be automatically synced to the respective server	State Compliance & Provide Evidence		
3.4.2.6	The solution shall support DHCP configuration for remoteboot devices.	State Compliance & Provide Evidence		
3.4.3	Integrated DHCP and DNS Configuration Management			
3.4.3.1	The solution shall work with multi-vendor DHCP and DNS services. The supplier shall provide a list of the vendors that are supported by their solution.	State Compliance & Provide Evidence		
3.4.3.2	In order for the solution to easily integrate with the installed base, Microsoft DNS and DHCP services shall be supported, as a minimum. The supplier to specify supported versions. If additional proprietary software and/or hardware is required to support the Microsoft DNS and DHCP services, it should be listed, and be included in the solution offering.	State Compliance & Provide Evidence		
3.4.3.3	The DHCP and DNS changes made in the solution should be seamlessly propagated to the respective servers, promoting a single management interface for these services.	State Compliance & Provide Evidence		

Item	Description	Schedule A	Schedule B	Reference/Comment
3.5	Support and maintenance			
	The solution support and maintenance requirements and other related requirements, except for those specified in this document are as described in [4] 240-135089195 Generic Technical Requirements for Eskom Telecoms Contracts.	State Compliance to Selected Clauses & Provide Evidence		