Specification Number: BBH 8048

RAIL NETWORK TELECOMS
TECHNICAL SPECIFICATION

Operational Technology Network Management and Access Control Systems

Author:	Engineer System Integration TRIM Telecommunication	R Kariel
Reviewed:	Act. Senior Engineer System Integration TRIM Telecommunication	O. Matlou
Supported:	Principal Engineer Telecom Network Engineering TRIM Telecommunication	M Mmbengwa

Date: 5 May 2025

Circulation Restricted To:

Transnet Freight Rail

Transnet and Relevant Third Parties

I. Document Authorisation

FUNCTION	NAME	TITLE & DIVISION	SIGNATURE	DATE
Reviewed By:				

II. Distribution

Once updated, a copy of the latest revision will be published on the document management system, “Project Wise”.

III. Document Change History

ISSUE NO.	DATE ISSUED	ISSUED BY	HISTORY DESCRIPTION
1.00	2025-05-08	Systems Integration	Initial Compilation

IV. Changes since Last Revision

CLAUSES	DESCRIPTION

V. List of Abbreviations and Acronyms

ABBREVIATION	DESCRIPTION
AAA	Authentication, Authorisation and Accounting
AC	Alternating Current
CAN	Campus Area Network
CAT	Category
DC	Direct Current
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECIA	Electronic Components Industry Association
ETSI	European Telecommunication Standards Institute
FAT	Factory Acceptance Test
Gbps	Gigabits per second
ICASA	Independent Communications Authority of South Africa
ICMP	Internet Control Message Protocol
IEC	International Electro technical Commission
IP*	Ingress Protection
IP	Internet Protocol
ISO	International Organization for Standardization
JMX	Java Management Extensions
KVA	Kilo-Volt Amperes
LAN	Local Area Network
LV	Low Voltage
NMS	Network Management Software
m	Meters
mm	Millimetre
Mbps	Megabits per second
MPLS	Multiprotocol Label Switching
MPPT	Maximum Power Point Tracking
MSTP	Multiple Spanning Tree Protocol
MTTR	Mean Time to Repair
ODF	Optical Distribution Frame
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection Model
OSPF	Open Shortest Path First
PoE	Power Over Ethernet
QoS	Quality of Services
RU	Rack Units
RSTP	Rapid Spanning Tree Protocol
RTU	Remote Terminal Unit
SABS	South African Bureau of Standards
SAT	Site Acceptance Test
SFP+	Small Form-factor Pluggable
SLA	Service Level Agreement
SNMP	Simple network management protocol
SMTP	Simple Mail Transfer Protocol
SOP	Standard Operating Procedure
SSL	Secure Socket Layer
SSH	Secure Shell
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access-Control System plus
TFR	Transnet Freight Rail
TIPNET	Technical Internet Protocol Network
TIPWAN	Technical Internet Protocol Wide-Area Network
TTP	Transnet Telecoms Personnel
USB	Universal Serial Bus
UPS	Uninterruptable Power Source

ABBREVIATION	DESCRIPTION
UTP	Unshielded Twisted Pair
Vac	Volts Alternating Current
Vdc	Volts Direct Current
VLAN	Virtual Local Area Network
W	Watts
WAN	Wide-Area Network
WMI	Windows Management Instrumentation

VI. Relevant Documentation Applicable

The equipment must comply with the latest issue of the following applicable specifications:

DOCUMENT NO.	DESCRIPTION	LOCATION
CENELEC	European Committee for Electro technical Standardization	External
E.4E	Compliance with the Occupational Health and Safety Act (Act 85 of 1993)	External
ECIA 310-E	Cabinets, Racks, Panels, and Associated Equipment	External
ETSI EN 300 119	Environmental Engineering (EE); European telecommunication standard for equipment practice	External
IEC	International Electro technical Commission	External
IEEE	Institute of Electrical and Electronic Engineers	External
IETF	Internet Engineering Task Force	External
ITU - T	International Telecommunication Union – Telecommunications Standardization Sector	External
ISO/IEC 11801-1:2017	Information technology — Generic cabling for customer premises — Part 1: General requirements	External
ISO 9000	Quality Management Systems.	External
SANS	South African National Standard	External
SANS 10142-1	The wiring of premises Part 1: Low-Voltage installations	External
SANS 60529	Degrees of protection provided by enclosures (IP Codes).	External
SFF INF-8074i	SFP (Small Formfactor Pluggable) Transceiver	External
SFF SFF-8431 4.1	SFP+ High Speed Electrical Interface	External
IEEE 802.1Q	Supporting virtual LANs on an IEEE 802.3 Ethernet Network	External
IEEE 802.3ae – 2002	Media Access Control (MAC) Parameters, Physical Layer, and Management Parameters for 10 Gb/s Operation	External
IEEE 802.3af – 2003	PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350 mA) on each port. Only 12.95 W is assured to be available at the powered device as some power dissipates in the cable.	External
IEEE 802.3at – 2009	PoE standard provides up to 30 W of DC power (minimum 44 V DC and 682 mA) on each port. Only 25.5 W is assured to be available at the powered device as some power dissipates in the cable.	External
IEEE 802.3ba – 2010	Amendment 4: Media Access Control Parameters, Physical Layers, and Management Parameters for 40 Gb/s and 100 Gb/s Operation	External
IEEE 802.3bm – 2015	Amendment 3: Physical Layer Specifications and Management Parameters for 40 Gb/s and 100 Gb/s Operation over Fibre Optic Cables	External
IEEE 802.3cc – 2017	Physical Layer and Management Parameters for Serial 25 Gb/s Ethernet Operation Over Single-Mode Fibre	External
IEEE 802.3z – 1998	Gigabit Ethernet Standard	External

E7/1	Works on, over, under or adjacent to railway lines and near high voltage equipment.	Internal
E.4E	Compliance with the Occupational Health and Safety Act (Act 85 of 1993)	Internal

Background

In modern enterprise and industrial network environments, maintaining operational visibility, ensuring secure access control, and supporting policy-based management are critical for efficient network performance and governance. To meet these needs, a robust Network Management System (NMS) and an integrated Authentication, Authorization, and Accounting (AAA) server are essential components of any network infrastructure.

The Network Management System (NMS) provides centralized monitoring, configuration, and fault management for all networking devices across the organization. It enables administrators to detect network issues in real-time, perform performance analytics, push configuration changes, and maintain inventory control. The NMS must support multi-vendor environments and offer comprehensive protocols such as SNMP, ICMP, and syslog collection to ensure compatibility and scalability.

The AAA server, meanwhile, is responsible for managing user access to network resources. It enforces policies through secure authentication methods, assigns permissions based on defined roles or profiles, and logs all access attempts for audit and compliance purposes. A well-designed AAA system improves security posture by ensuring only authorized users or devices can access the network and provides detailed records to support incident investigation and reporting.

This specification outlines the technical and functional requirements for implementing a scalable, resilient, and secure NMS and AAA solution suitable for deployment in both enterprise and critical infrastructure environments. The solution must align with current best practices and standards, support redundancy, and ensure integration with existing IT and network ecosystems.

Scope

This specification defines the requirements for the procurement, deployment, configuration, and integration of a Network Management System (NMS) and Authentication, Authorization, and Accounting (AAA) server within the organization's network environment. The objective is to enhance the network's operational efficiency, security, and manageability by implementing centralized tools that provide visibility, control, and accountability across all network elements and user access points.

The scope includes the following:

Network Management System (NMS):

1. Centralized monitoring of network devices (routers, switches, firewalls, access points, etc.)
2. Real-time fault detection, alerting, and diagnostics.
3. Performance monitoring and reporting (e.g., bandwidth, latency, availability)
4. Configuration and change management across multi-vendor infrastructure.
5. Inventory management and topology visualization
6. Support for SNMPv2/v3, syslog, NetFlow/sFlow, and API integrations

AAA Server:

7. Centralized user/device authentication for wired and wireless access
8. Role-based access control and policy enforcement
9. Accounting and logging of user sessions for audit and compliance
10. Integration with directory services (e.g., LDAP, Active Directory)
11. Support for RADIUS and TACACS+ protocols
12. High availability and failover capabilities

The system must support deployment in on-premises only and be scalable to accommodate future network growth. It must also be compatible with existing infrastructure and integrate with security, orchestration, and reporting tools in use within the organization.

Compliance

1. Bidders must comply with all the specifications and requirements as indicated in this document. Any deviation from this (and all inherent) specifications must be clearly indicated in the bidder’s submission document, by use of the technical compliance sheet.
2. All deviations must be disclosed, and Transnet will in its own discretion accept or reject such a deviation.
3. Failure to indicate all deviations will result in a bidder being disqualified from this tender process.
4. Transnet will reserve the right to inspect all network equipment, components and subsystems before adjudication of contract.
5. Transnet will reserve the right to request and check with references of previous contracts.

Service conditions

General Environmental and Electrical Specifications (Applicable to Both NMS and AAA Hardware):

1. Operating Temperature: –10°C to +60°C
2. Storage Temperature: –40°C to +85°C
3. Humidity: 0% to 95% non-condensing
4. Shock and Vibration: Compliant with IEC 60068-2-27 (shock) and IEC 60068-2-6 (vibration)
5. Surge and EMI: Compliant with IEC 61000 series standards for surge, ESD, EFT, and EMI protection
6. Power Input Options:
7. AC: 100–240V, 50/60Hz
8. DC: 12–57V input (for industrial variants)
9. Dual voltage power supply capabilities are required on the devices, i.e., the ability to operate on either a DC (48VDC) or AC (230VAC, 50Hz) power source.
   If native dual power input is not available, the contractor must supply suitable converters or adapters to meet this requirement.

Technical Requirements

This section will describe the requirements needed. The section will focus on the common requirements as standard among all networking devices, regardless of network device function.

1. Network Management System (NMS)

1.1 Hardware Requirements:

- Processor: Minimum 8-core x86_64 CPU
- Memory: Minimum 32 GB ECC RAM
- Storage: RAID-capable with minimum 1 TB usable SSD storage
- Networking: Dual Ethernet interfaces (1 Gbps minimum per port)
- Remote Management: IPMI, iDRAC, or equivalent interface
- Form Factor: 19" rack-mountable; include rails, brackets, and accessories.
- Virtualization Support: Must support virtualization (e.g., Intel VT-x or AMD-V)
- Redundancy: Dual power supplies strongly preferred
- Platform Compatibility: Must support certified Linux distributions (e.g., Ubuntu LTS) as well as Windows Server editions (2016 and up)

1.2 Software Requirements:

- Support for multi-vendor environments (Cisco, Huawei, Juniper, etc.)
- Compatibility with SNMPv2c/v3, ICMP, Syslog, and NetFlow/sFlow
- Topology discovery and visualization
- Fault management: Real-time alerts, event correlation, escalation workflows
- Performance management: Historical trending, SLA monitoring, bandwidth analysis
- Configuration management: Backup/restore, mass configuration deployment, audit trails.
- Reporting engine: Customizable scheduled and ad-hoc reports
- Role-Based Access Control (RBAC) for NOC personnel
- Web-based GUI with secure HTTPS access and optional Multi-Factor Authentication (MFA)
- Integration with existing RADIUS or Active Directory (AD) for user authentication — enabling centralized login credential management.
- API support for integration with ticketing, monitoring, and SIEM platforms
-
- Log retention: Configurable data archiving and compliance export options
- Optional: Containerized or microservice-ready (e.g., Docker, Kubernetes)

2. Authentication, Authorization, and Accounting (AAA) Server

2.1 Hardware Requirements:

- Processor: Minimum 4-core x86_64 CPU (8-core recommended for scaling)
- Memory: Minimum 16 GB ECC RAM
- Storage: Minimum 512 GB SSD (RAID optional)

- Networking: Dual Ethernet ports (1 Gbps minimum), 802.1Q VLAN tagging support
- Remote Management: IPMI/iDRAC or equivalent out-of-band access
- Form Factor: 19” rack-mountable with mounting accessories included.
- Redundancy Support: Clustering or high-availability support (active/passive or load-balanced)
- Platform Compatibility: Must support leading Linux distributions (RHEL, Ubuntu, Debian) and Windows Server (2016 and up)

2.2 Software Requirements:

- Full support for RADIUS and TACACS+ for network device access control
- Integration with existing centralized identity services:
- Active Directory (AD) or LDAP for user authentication and group-based policy application
- RADIUS proxying to forward authentication requests to an upstream RADIUS server.
- Support for 802.1X, MAC authentication bypass (MAB), and VPN authentication scenarios
- Accounting logs with timestamped session tracking, exportable in CSV or syslog formats
- Web-based GUI for administration, with RBAC and MFA support
- Support for user session policies (e.g., session timeout, simultaneous login limits)
- RESTful API integration for third-party systems (NMS, NAC, SIEM, ticketing)
- Failover and high availability clustering capabilities (session sync included)
- Support for certificate-based authentication and EAP methods
- Centralized login and audit logs, with syslog forwarding to SIEM or log collectors.

3 Software Feature Set

The descriptions below are guidelines as to how the usability of the services should perform for the NMS (non-exhaustive list):

3.1 Network Management System User Interface

3.1.1 Dashboards and Visualization

- Customizable Dashboards:
    - Users must be able to personalize dashboard layouts based on their role or preference.
    - Widgets and tiles should support drag-and-drop reordering and resizing.
    - Must support multiple dashboard profiles (e.g., for core network, access layer, security events).
- Real-Time Monitoring:
    - Live status indicators for device health, link states, interface utilization, and alert counts.
- Support for geographic and logical topology maps with visual overlays for alarms and bandwidth usage.
- Drill-Down Capabilities:
    - From global overview → region → site → device → interface → metric
- Every dashboard element must allow context-sensitive deep inspection (e.g., clicking on a device shows real-time interface graphs and logs).
- Historical Trend Analysis:
    - Embedded graphs and timelines for CPU, memory, interface utilization, latency, and packet loss.
- Support for exporting graphs to CSV/PDF or embedding in reports.
- Event and Alarm Dashboards:
    - Prioritized alert views with color-coded severity levels.
- Must allow filtering, acknowledgment, assignment, and annotation of alerts.

3.1.2 Customization and Flexibility

- User-Created Views:
    - Users should be able to define custom views based on device types, regions, or tags.
    - Dashboards must support custom filters (e.g., show all access switches in critical alarm state).
- Multi-Tenant Awareness (if required):
    - The system should optionally support segmentation by tenant/business unit/network domain.
- Custom Alert Rules:
    - Thresholds for triggering alerts must be user configurable.
    - Support for compound rules (e.g., alert if CPU > 85% AND interface errors > 10/sec).
- Scripting and Automation:
    - Built-in support for automation scripts (e.g., Python or YAML-based workflows).
    - Scheduling of routine jobs (e.g., daily config backup, weekly interface usage reports).
- Localization and Themes:

    - Support for changing time zones, units (bps/Mbps/Gbps), and UI theme preferences.

3.1.3 Role-Based Access Control (RBAC)

- Granular Permissions:
    - The NMS must support assigning roles with fine-grained privileges down to individual functions (e.g., view-only access to alarms, full access to configuration backups).
    - Roles may be assigned per user or per group.
- Role Examples:
    - NOC Operator: Read-only access to dashboards, acknowledge alarms.
    - Network Engineer: Configuration management, access to device CLI interfaces.
    - Manager/Auditor: View reports, event logs, historical performance data.
    - Super Admin: Full access to system settings, user management, integrations.
- LDAP/AD Integration:
    - RBAC roles must be mappable to LDAP/AD groups, enabling centralized identity management.
    - Changes to roles or group assignments in AD must be reflected automatically in the NMS.
- Audit Logging:
    - All user actions (login, configuration push, script execution, role changes, etc.) must be logged.
    - Logs must include timestamp, username, IP address, and action detail.

3.1.4 Accessibility and Availability

- Mobile-Friendly Interface:
    - The web GUI must be responsive and usable from tablets and mobile devices.
- Multi-Session Support:
    - Must allow multiple simultaneous sessions per user without conflicts.
- Session Timeout and Security Controls:
    - Inactivity timeout, IP whitelisting, and optional 2FA (Two-Factor Authentication) support.

3.2 AAA Server User Interface

The section below will describe the feature set needed for the AAA server.

3.2.1 Administrative Dashboard

- **Policy Overview Dashboard:**
    - Summary of currently enforced policies (e.g., wired/wireless access, VPN, 802.1X)
    - Real-time indicators for active sessions, recent login attempts, and policy violations
    - Quick stats for accepted/denied authentications over time.
- **Session Viewer:**
    - Live view of active RADIUS/TACACS+ sessions, device details, MAC/IP mapping, and session duration
    - Support for session search and filtering by username, IP address, access point, or device
- **User Access Timeline:**
    - Historical tracking of user access attempts with timestamps, access type (wired, wireless, VPN), and result (granted, rejected)

3.2.2 Policy Configuration and Management

- **Role-Based Access Policies:**
    - Define access rights based on user roles or AD group memberships.
    - Assign VLANs, ACLs, or downloadable access control lists (dACLs) dynamically based on user/device attributes.
- **Flexible Policy Builder:**
    - Visual or form-based rule engine for defining access conditions (e.g., time of day, endpoint posture, authentication method)
    - Support for nested conditions and fallback logic (e.g., fallback to MAC auth if 802.1X fails)
- **Device Profiling:**
    - Classify endpoint types based on MAC OUIs, DHCP fingerprints, or manual tagging.
    - Apply policies based on device class (e.g., IP phone, printer, laptop, contractor device)
- **Guest Access Management:**
    - Built-in captive portal editor with customizable branding and access duration
    - Self-registration and sponsor-based guest approval workflows

3.2.3 User and Identity Integration

- **Directory Synchronization:**
  - Integrate with existing Active Directory, LDAP, or RADIUS proxying systems for centralized credential management.
  - Schedule synchronization intervals and apply filters (e.g., only sync users from specific AD OU)
- **Credential Methods:**
  - Support for password-based, certificate-based (EAP-TLS), and token-based authentication (e.g., OTP, SAML)
  - Enforce password policies, MFA, and account lockout thresholds based on failed attempts.
- **Self-Service Options:**
  - Optional web portal for users to manage their own passwords, certificates, or see recent access history (subject to policy)

3.2.4 RBAC and User Management

- **Administrator Roles:**
  - Support for fine-grained administrative roles (e.g., policy editor, session auditor, user manager)
  - Role inheritance and restrictions must be definable via GUI or LDAP group mapping.
- **Secure Access Control:**
  - Admin access to AAA UI must be HTTPS-only, with session timeout and login IP whitelisting.
  - Support for multi-factor authentication for administrative users
- **Audit Logging:**
  - Every admin activity must be logged, including policy edits, user account changes, and login attempts.
  - Logs must capture timestamp, username, IP address, and action summary.
  - Export to syslog, SIEM, or secure archive

3.2.5 Alerting and Reporting

- **Real-Time Alerts:**
  - Configurable thresholds to trigger alerts for high authentication failures, policy violations, or unknown devices.
  - Alerts via email, syslog, or webhook to incident management systems
- **Custom Reports:**

  - Generate scheduled or on-demand reports on access trends, user behavior, and policy usage.
  - Export formats: CSV, PDF, JSON
  - Option to anonymize or mask PII data for privacy compliance.

- **Compliance Support:**

  - Audit trails must meet industry regulatory requirements (e.g., ISO 27001, NIST 800-53, POPIA, GDPR)
  - Data retention policies must be configurable per site or region.

4. Service Level Agreement

Transnet requires a service level agreement (SLA) with the contractor. This agreement shall focus on training, hardware and software support, guarantee and warranty policies related to the components that make up the NMS and AAA server. The agreement must run immediately after the components system is handed over to Transnet. Details of the SLA are described below.

4.1 Training

Transnet will require training where the devices will be placed. Transnet will thus require training for 12 people; however, this number is subject to change depending on the need of the business. If this does change, Transnet will formally request that the bidder provide the required training, including the updated number of employees. Transnet will also determine what type of training the specific individuals need.

For each of the different training requirements listed below, a standard operating procedure (SOP) document must be supplied. The contractor must work with Transnet Academy to develop the specific OEM training and SOP, tailored to the network device maintenance and troubleshooting.

The training portion of the SLA must run immediately after the contract is awarded to the contractor, and a purchase order is issued – provided it is needed. The contractor must be able to provide training in at least two of the following manners:

- Online instructor led and self-paced training
- On premise training at one of 3 Transnet (Transnet Academy) venues
  - Johannesburg is compulsory
  - Cape town is compulsory
  - Durban is optional
- On premise training at the contractor offices
- On premise training at a recognised IT institute of learning and skill development

The types of training required are listed below:

- Maintenance training

  Transnet requires first line maintenance training to be deployed to designated personnel.

- Fault finding training.

  Transnet requires first and second line fault-finding training to be given to designated personnel. This training must focus on fixing basic faults that occur with the the network devices.

- Operator training

  Transnet requires up to professional level training to refine the design, operate, configure and administer the networking devices.

Transnet may require maintenance, fault finding and operator training for the optional components, systems and software listed in this spec. These additional training requests will be sent to the bidder by Transnet when it is required.

4.2 Software Updates

During the provision of Maintenance and Support Services period, the contractor will use commercially reasonable efforts to correct or modify any operating software (for the betterment), which must conform in all material respects with the then-current documentation for the network devices.
For the network devices, the update must be pushed through the TFTP server or the *optional SD-controller (if implemented).*

4.3 Hardware Warranty

The contractor must provide a warranty on the components based on the OEM warranty period. The warranty period, of the hardware, is valid from the date of the handover of the components in a phased approached. Maintenance support (on the hardware) must consist of telephonic and onsite response depending on the criticality of the fault. The bidder must provide proof of same day response should the need arise. When necessary for escalated hardware support issues - the bidder will coordinate collaboration between TTP and the hardware vendor staffed by senior-level analysts, for troubleshooting assistance of hardware (and/or software issues). During this period the bidder will remain involved and in contact with Transnet to ensure timely resolution.

All hardware (that falls within the warranty period) failures that cannot be rectified must be replaced with the same or similar model. The bidder must take note not to hinder or fail to maintain the same level management system with the replaced hardware. A new warranty certificate must also be issued once the hardware has been replaced.
s

4.4 Incident Management and Support

The bidder must provide a fault reporting support portal (online tickets or fault logging service) by which Transnet can receive assistance from the bidder relating the troubleshooting of issues with the software.

The bidder must also provide telephonic support (or equivalent) during working days in the event of emergency faults.
Service hours 08:00 – 17:00

Severity clarification:

Severity Level	Severity Description	Response Time	MTTR
High	You have encountered a problem with the product that prevents its main features from working. The product cannot be used as described in its documentation. *Example: "I am unable to access the server, but it is running."*	4 Hours	8 Hours
Critical	The device is unresponsive/down. *Example: "It does not power on and no connectivity is shown."*	2 Hours	4 Hours

Proprietary Configurations

None of the equipment/systems/components supplied (including the optional ones), must have any proprietary configurations that disable it from being able to operate/communicate or be part of a network that has network elements (routers, switches and NMS and other) from a different supplier/ original equipment manufacturer.

Evaluation, and Performance Testing and Handover Documents

Acceptance tests on site must be conducted, and a test report must be submitted to Transnet for review and acceptance. The system shall be tested at the factory and on site; these tests must be satisfactory to Transnet's requirements. FAT and SAT tests must be conducted for all components.
The Transnet Quality Assurance team will give final word of verification of correctly installed equipment and correctly selected equipment described in this document.
Transnet will approve all integration points between systems.
Transnet will receive all performance and operation results and conduct an optional site acceptance test if needed.

1.7 Handover Documents

Handover documents for the project must be supplied to Transnet after the successful installation and commission of the system. There should be handover documents per sub system installed, subsystems include the power requirements and networking requirements. The following document must be provided showing the following:

- A section showing the successful results of the installation as per the requirements of Transnet.
- All certification documents needed to install the components must be included.
- The contractor shall conduct all necessary tests and supply a certificate of compliance (CoC).
- All components, which needs calibration - certificates must be provided.
- Full, detailed and updated as built/last mile diagrams and designs.
- Project power supply documents, these documents must show where and how the different network components are powered.
- Network documentation and all designs/diagrams.
- Successful network communication documents. These documents must show that communication between all the components of the network is successful, whether being a wireless or physical link where applicable.

END OF SPECIFICATION