



TECHNICAL SPECIFICATIONS

Document Title : **Technical Specifications for Network Equipment, 2026**
Document No: : **CA.TS.520:2026**
Edition: : **Version 1.0**
Effective Date: : **TBD**

Table of Contents

1.	Introduction	3
2.	Objectives.....	3
3.	Scope and Applicability	3
4.	Technical Specifications	4
4.1	Electrical Power.....	4
4.2	Network Protocols	4
4.3	Compatibility and Interoperability	4
4.4	Radiated Emissions.....	5
4.5	Conducted Emissions	5
4.6	Security Features	5
4.7	Environmental Conditions	6
4.8	Safety	6
4.9	RoHS (Restriction of Hazardous Substances)	7
4.10	E-Waste.....	7
4.11	Accessibility for Persons with Disabilities	7
4.12	Quality of Service (QoS)	8
4.13	Artificial Intelligence (AI).....	8
5	Review of Specification	9

1. Introduction

The Communications Authority of Kenya (CA), established under the Kenya Information and Communications Act, 1998, is mandated to regulate and promote the development of the telecommunications sector within the country.

The Authority recognizes the importance of comprehensive technical specifications for Internet Protocol (IP) network equipment in the standardization of equipment to support the national digital transformation, supporting socio-economic development, and enabling effective integration with the global digital communications environment.

The rising adoption of internet-based services and the rapid expansion of digital business applications have underscored the need for network equipment that meets rigorous standards for interoperability, security, reliability, and performance, ensuring seamless transmission of data, voice, and multimedia across connected platforms nationwide.

Accordingly, the increasing deployment and variety of network equipment requires the CA to establish clear technical requirements, ensure compliance with specification and certification processes, and address key regulatory concerns such as equipment type approval, environmental sustainability, network compatibility, and alignment with national and international policy and standards frameworks.

2. Objectives

- 2.1. To facilitate interoperability and compatibility across different network platforms and devices.
- 2.2. To enhance compliance with security requirements of different networks and devices.
- 2.3. To promote reliability and consistency in network operations and service delivery.
- 2.4. Facilitate implementation of the Authority's IPv4 to IPv6 Migration Strategy.

3. Scope and Applicability

- 3.1. This specification covers network devices capable of connecting to public telecommunication networks comprising of Public Switched Telephone Network (PSTN), Public Land Mobile Networks (PLMN), Computer Networks and Broadcasting Networks. The devices covered include; Switches, Routers, Firewalls, Gateways, Servers, Network interface cards, Session border controllers
- 3.2. These technical specifications apply to network devices that utilize network protocols comprising of Management protocols like Simple Network Management Protocol (SNMP), Security Protocols like Secure Socket Layer (SSL) and Communication Protocols like Hypertext Transfer Protocol(HTTP).

- 3.3. These specifications also cover devices that utilize Routed Protocols comprising of AppleTalk, Internetwork Packet Exchange (IPX), Internet Protocol (IP) and Routing Protocols comprising of Border Gateway Protocol (BGP), Routing Information Protocol (RIP) among others.

4. Technical Specifications

The developed specifications for Network Equipment cover input Power, Safety issues, Electromagnetic Compatibility (EMC), Network Protocols, Interoperability, Health and Security issues.

The minimum requirement for each specification are:

4.1 Electrical Power

- 4.1.1. The Network Equipment shall support an operating voltage of 240 VAC $\pm$ 10% at a frequency of 50 Hz $\pm$ 1
[Kenya National Distribution Grid Code, 2024]
- 4.1.2. The efficiency of the Power Supply Unit (PSU) shall have a minimum platinum certification level as per international energy efficient certifications for networking equipment.
[EU Ecodesign for Sustainable Products Regulation, 2024 (EU ESPR)]

4.2 Network Protocols

- 4.2.1 The Network equipment shall support Internet Protocol IPv6 addressing and associated emerging IPv6 Enhanced Innovation ("IPv6+") [IETF RFC 8200, CA IPv4 to IPv6 Migration Strategy]
- 4.2.2 The Network equipment shall support at least one Management protocol, Security Protocol and Communication protocol.
- 4.2.3 The Network equipment shall support at least one Routing and Routed protocol.

4.3 Compatibility and Interoperability

- 4.3.1 The Network equipment shall be compatible and interoperable with the latest switching protocols such as Applications Specific Integrated Circuit (ASIC), Ternary Content Addressable Memory (TCAM) and Content Addressable Memory (CAM)-based switching. [RFC5036, ITU-T G.8121]
- 4.3.2 The Network equipment shall support deployment of MPLS architecture for purposes of core network interoperability [RFC3031]

4.4 Radiated Emissions

- 4.4.1 The radiated emissions from the Network equipment at a 10 metre distance shall be in the range of:

[Européenne Norme (EN) 55022:2006]

4.4.1.1 (40-47) dB μ V/m in the industrial environment

4.4.1.2 (30-37) dB μ V/m in the residential environment.

4.5 Conducted Emissions

- 4.5.1 The conducted emissions from the Network equipment to the mains port shall be in the range of:

[EN55022:2006]

4.5.1.1 (60-66) dB μ V in the industrial environment

4.5.1.2 (46-56) dB μ V in the residential environment.

- 4.5.2 The conducted emissions from the Network equipment to the telecommunications port shall be in the range of :

4.5.2.1 (74-84) dB μ V in the industrial environment

4.5.2.2 (64-74) dB μ V in the residential environment.

4.6 Security Features

- 4.6.1 The Network equipment shall support Access Control Lists (ACLs) and Intrusion Prevention and Detection Systems (IPS/IDS).

[IETF RFC 6632, ITU-T X.1034, ITU-T X.721]

- 4.6.2 The Network equipment shall support the latest version of Internet Protocol Security (IPSec) protocols [IETF RFC 4301].

- 4.6.3 The Network equipment shall support the latest version of Transport Layer Security (TLS) protocols. [IETF RFC 5246]

- 4.6.4 The Network equipment shall support the latest version of secure management protocols including Secure Shell Protocol (SSH) and Secure Network management Protocols

[IETF RFC Nos. 3410, ITU-T X.1034, ITU-T X.721]

- 4.6.5 The network equipment shall support secure update mechanisms, secure access control mechanisms , secure storage mechanisms, secure communication mechanisms and secure network monitoring mechanisms.

[EN 18031-1:2024]

4.7 Environmental Conditions

- 4.7.1 The Network equipment shall support environmental conditions suitable for telecommunications and equipment rooms in Kenya, with an operating temperature range of 5°C to 45°C and relative humidity limits of 80%.
[American National Standards Institute / Telecommunications Industry Association (ANSI/TIA-569-E-1) Addendum]

4.8 Safety

- 4.8.1 Access to energized parts of the Network equipment and their insulation shall be restricted [International Electrotechnical Committee [IEC62368-1]

- 4.8.2 Materials used in the manufacture of Network equipment shall be selected such that surface temperatures do not exceed the touch temperature limits measured at a standardized ambient of 25°C as follows:

- 4.8.2.1 Devices worn directly on the body during normal use for continuous contact exceeding 8 hours:

- 4.8.2.1.1 Metallic elements: 43°C
- 4.8.2.1.2 Glass/porcelain/vitreous elements: 43°C
- 4.8.2.1.3 Plastic/rubber elements: 48°C

- 4.8.2.2 External surfaces held against or worn on the body during normal use for a contact duration greater than 1 minute and up to 8 hours:

- 4.8.2.2.1 Metallic elements: 48°C
- 4.8.2.2.2 Glass/porcelain/vitreous elements: 48°C
- 4.8.2.2.3 Plastic/rubber elements: 48°C

- 4.8.2.3 External surfaces held for short periods or touched occasionally for a contact duration greater than 10 seconds and up to 1 minute:

- 4.8.2.3.1 Metallic elements: 51°C
- 4.8.2.3.2 Glass/porcelain/vitreous elements: 56°C
- 4.8.2.3.3 Plastic/rubber elements: 60°C

- 4.8.2.4 External surfaces touched briefly or an incidental contact duration greater than 1 second and up to 10 seconds:

- 4.8.2.4.1 Metallic elements: 51°C
- 4.8.2.4.2 Glass/porcelain/vitreous elements: 56°C
- 4.8.2.4.3 Plastic/rubber elements: 60°C

- 4.8.2.5 External surfaces accessible to trained users only for a contact duration of up to 1 second, or surfaces not expected to be touched in normal use:

- 4.8.2.5.1 Metallic elements: 70°C
- 4.8.2.5.2 Glass/porcelain/vitreous elements: 80°C
- 4.8.2.5.3 Plastic/rubber elements: 95°C

[International Electrotechnical Committee (IEC) 62368-1]

- 4.8.3 Where the network equipment surface temperatures is required to exceed the limits given in 4.8.2 for functional reasons, the equipment shall be marked with the IEC 60417-5041 warning symbol, and access shall be restricted to trained users [IEC 62368-1]

4.9 RoHS (Restriction of Hazardous Substances)

- 4.9.1 Materials used in the manufacture of Network equipment and accessories shall not contain elements of Lead, Mercury, Cadmium and any other hazardous substance. [Directive 2011/65/EU]

4.10 E-Waste

- 4.10.1 Network equipment imported into the country for marketing shall have a minimum of three (3) years before their end of life (EOL) noting the minimum lifespan of ICT equipment is three (3) years . [ETSI TS 103 199:2011]
- 4.10.2 All Network equipment will be accompanied by a Digital Product Passport (DPP) depicting the product's unique identifier, its precise material composition, and verifiable sustainability metrics, including its environmental footprint and circularity data.
- 4.10.3 the products identity, materials, sustainability
[Eco design for Sustainable Products Regulation (ESPR) Regulation (EU) 2024/1781]
- 4.10.4 The content of the DPP shall entail:
- 4.10.4.1 Product Identity: manufacturer details, model numbers
 - 4.10.4.2 Materials and components: raw materials, recycled content, hazardous substances
 - 4.10.4.3 Environmental Footprint: recyclability, carbon foot print, energy efficiency
 - 4.10.4.4 Compliance and Safety: certifications, Declaration of Conformity (DoC)
 - 4.10.4.5 Life Cycle Data: disposal guidelines, repair instructions
- 4.10.5 The DPP content shall be accessible using either QR Codes, RFID tags, NFC chips, Barcodes or an online portal.

4.11 Accessibility for Persons with Disabilities

- 4.11.1 The Network equipment must support accessibility requirements for persons with disabilities, detailed as:
- 4.11.1.1 For equipment meant for end users, the applicable capabilities shall include:
 - Presence of more than one means of operation besides physical controls namely audio and visual display indicators.

- capability to activate accessibility features using more than one mode of operation.
- tactile markings to identify different parts and components on critical parts and controls.
- support for audible tones indicating port connections and disconnections
- the equipment should have standardized connectors to facilitate assistive device integration.

4.11.2 For equipment meant for usage in the network, they must support user added accessibility features on the end user network device.

[Kenya Standard KS2952]

4.12 Quality of Service (QoS)

4.12.1 The Network equipment should support the various QoS class thresholds as configured in the network defined as:

- IP Packet Transfer Delay (IPTD): $\leq 100\text{ms}$ voice ; 400ms data
- IP Packet Delay Variation (IPDV): $\leq 50\text{ms}$ voice / data
- IP Packet Loss Ratio (IPLR): 0.1%
- IP Packet Error Ratio (IPER): 0.01%

[ITU-T Y.1541]

4.12.2 The Network equipment should support at least two QoS frameworks, namely, Differentiated Services (DiffServ), Integrated Services (IntServ), Multiprotocol Label Switching (MPLS) with QoS and Best effort.

4.12.3 The Network equipment shall support differentiated QoS services for MPLS services [RFC3270]

4.13 Artificial Intelligence (AI)

4.13.1 Network equipment utilizing AI systems/models shall be designed and implemented in such a way that the network equipment safeguards the safety, transparency, privacy and respect for intellectual property rights of the users and data it processes. [EU Artificial Intelligence Act,2024]

4.13.2 Network equipment utilizing AI systems/models categorized as high risk, shall be designed with the appropriate human-machine interface aimed at preventing risks to health, safety and fundamental rights that may emerge when a high-risk AI system is used.

[EU Artificial Intelligence Act,2024]

5 Review of Specification

This Specification is subject to review by the Authority from time to time.

Signed
Director General
Communications Authority of Kenya