AIRPORTS COMPANY
SOUTH AFRICA

Annexure E – Work package specifications

For

LAN / Wireless / IP Telephony and Network Security Services

Description:

Specifications for the Work Packages related to the Supply, Installation, Commissioning, Support and Maintenance of IT Network, IP Telephony and IT Security Infrastructure Services for a period of 60 Months to Airports Company South Africa

AIRPORTS COMPANY
SOUTH AFRICA

Contents

AIRPORTS COMPANY
SOUTH AFRICA

AIRPORTS COMPANY
SOUTH AFRICA

General Notes

Please take special note of the following items that are applicable to all Work packages.

- **OEM Warranty –**
    - All hardware must be supplied with a 5-year OEM warranty and software with at least next business day replacement, this includes any software for the device to function. Some Work packages have other requirements and should be catered for accordingly.
- **Interoperability –**
    - Any OEM can be used to fulfil any work package as long as FULL interoperability is guaranteed within the existing environment.
    - Efforts are made to describe the current environment for all work packages. Please read this information carefully.
    - The bidder can also include the replacement of the up and downstream devices should they wish/need to provide the guarantee.
    - Note that some switches are in a “stack” and are required to remain in the stack configuration due to limitations on uplink fibre capacity.
- **Management –**
    - All supplied devices must be fully managed.
    - Please refer to the currently deployed management software components as per Annexure A – Section 2: Service environment to determine if the proposed hardware will be able to be managed by the in place management system
    - Should it be needed, the additional management platform must be costed as part of the work package or added to the “Other cost” tab in Annexture C (pricing file)
- **Monitoring –**
    - All supplied devices must be fully monitored.
    - Please refer to the currently deployed monitoring software components as per Annexure A – Section 2: Service environment to determine if the proposed hardware will be able to be monitored by the in place monitoring system
    - Should it be needed, the additional monitoring platform must be costed as part of the work package or added to the “Other cost” tab in Annexure C (pricing file)
- **Support –**
    - Any proposed OEMs must be fully supported by the bidder using OEM certified staff at the equivalent requested certification levels.
- **Wi-Fi roaming –**
    - In the case of Wi-Fi devices, the provider must fully guarantee seamless, near-zero loss to clients while roaming between network segments at each site, should a mix of OEM equipment be proposed.
- **IP Telephony**

- The solution must integrate with existing Cisco Unified Communications Manager (CUCM) version 11.5 or higher, Unity Connection, and Contact Centre platforms.

AIRPORTS COMPANY
SOUTH AFRICA

1.0 WIFI Work Package - Replacement High Spec Access Point

Supply, physically install and configure WIFI Access points that meet enterprise-grade Wi-Fi 6E or latest equivalent standards to replace existing devices that have reached end of life.

The high specification devices for dense areas must have the following features:

- Tri-band Wi-Fi 6E (2.4 GHz, 5 GHz, 6 GHz)
- 4x4 MIMO for high throughput and user density
- Advanced RF management (band steering, interference mitigation)
- Enterprise security (WPA3, secure boot)
- IoT-ready architecture
- Centralised management (cloud/on-prem support)
- Must include all required licenses for full feature activation (connectivity, analytics, location services)
- Include OEM hardware warranty for a period of 5 years, with Next Business Day (NBD) replacement.
- The devices must either be supported by the existing WLAN controllers or separate controllers can be supplied; however, there needs to be seamless roaming between new and existing APs, ensuring no degradation in connectivity or user experience.
- Support for ACSA Wi-Fi portal, or provision of a suitable replacement captive portal with equivalent functionality
- Include decommissioning of existing EOL infrastructure, documentation, asset tagging and validation testing and commissioning of new infrastructure
- Installation should cater for all equipment required for installation at heights, including Skyjacks where required.

2.0 WIFI Work Package - Replacement of Low Spec Access Point

Supply, physically install and configure WIFI Access points that meet enterprise-grade Wi-Fi 6E or latest equivalent standards to replace existing devices that have reached end of life.

The Low specification devices for standard-density environments and general-purpose wireless connectivity must have the following features:

- Tri-band Wi-Fi 6E (2.4 GHz, 5 GHz, 6 GHz)
- 2x2 MIMO antenna configuration, delivering reliable performance for light to moderate client density scenarios.
- Basic RF management features, including automatic channel selection and load balancing to ensure stable operation.
- Enterprise security (WPA3, secure boot)
- IoT-ready architecture
- Centralised management (cloud/on-prem support)
- Must include all required licenses for full feature activation (connectivity, analytics, location services)
- Include OEM hardware warranty for a period of 5 years, with NBD replacement.
- The devices must either be supported by the existing WLAN controllers or separate controllers can be supplied; however, there needs to be seamless roaming between new and existing APs, ensuring no degradation in connectivity or user experience.
- Must be supported by the ACSA WIFI portal, or a suitable replacement portal must be provided.
- Include decommissioning of existing EOL infrastructure, documentation, asset tagging and validation testing and commissioning of new infrastructure
- Installation should cater for all equipment required for installation at heights, including Skyjacks where required.

3.0 WIFI Work Package - Replacement of Outdoor Access Point with external Omnidirectional Antennae

Supply, physically install and configure WIFI Access points that meet enterprise-grade Wi-Fi 6E or latest equivalent standards to replace existing devices that have reached end of life.

- Tri-band Wi-Fi 6E (2.4 GHz, 5 GHz, 6 GHz)
- 2x2 MIMO antenna configuration, delivering reliable performance for light to moderate client density scenarios
- Outdoor-rated enclosure with N-type connectors for external antennas
- Omni-directional dipole antennas with 4 dBi (2.4 GHz), 8 dBi (5 GHz), and 8 dBi (6 GHz) gain
- Basic RF management features, including automatic channel selection and load balancing to ensure stable operation
- Enterprise security (WPA3, secure boot)
- IoT-ready architecture
- Centralised management (cloud/on-prem support via vendor platform)
- Must include all required licenses for full feature activation (connectivity, analytics, location services)
- Include OEM hardware warranty for a period of 5 years, with NBD replacement.
- Include decommissioning of existing EOL infrastructure, documentation, asset tagging and validation testing and commissioning of new infrastructure
- The devices must either be supported by the existing WLAN controllers or separate controllers can be supplied; however, there needs to be seamless roaming between new and existing APs, ensuring no degradation in connectivity or user experience.
- Support for ACSA Wi-Fi portal, or provision of a suitable replacement captive portal with equivalent functionality
- Installation should cater for all equipment required for installation at heights, including Skyjacks where required.

4.0 WIFI Work Package - Replacement of Outdoor Access Point with Internal Antennae

Supply, physically install and configure WIFI Access points that meet enterprise-grade Wi-Fi 6E or latest equivalent standards to replace existing devices that have reached end of life.

The low specification devices with directional antennae for standard-density environments and general-purpose outdoor wireless connectivity must have the following features:

- Outdoor-rated enclosure with N-type connectors for external antennas
- Directional patch antennas with 8 dBi (2.4 GHz), 9 dBi (5 GHz), and 9 dBi (6 GHz) gain
- Basic RF management features, including automatic channel selection and load balancing to ensure stable operation
- Enterprise security (WPA3, secure boot)
- IoT-ready architecture
- Centralised management (cloud/on-prem support via vendor platform)
- Must include all required licenses for full feature activation (connectivity, analytics, location services)
- Include OEM hardware warranty for a period of 5 years, with NBD replacement.
- The devices must either be supported by the existing WLAN controllers or separate controllers can be supplied; however, there needs to be seamless roaming between new and existing APs, ensuring no degradation in connectivity or user experience.
- Include decommissioning of existing EOL infrastructure, documentation, asset tagging and validation testing and commissioning of new infrastructure
- Support for ACSA Wi-Fi portal, or provision of a suitable replacement captive portal with equivalent functionality
- Installation should cater for all equipment required for installation at heights, including Skyjacks where required.

5.0 WIFI Work Package - Replacement of Small site Wlan controller

Supply, physically install, and configure a enterprise grade WLAN controller to replace the existing controller infrastructure supporting enterprise-grade Wi-Fi 6E or the latest equivalent access points. The controller must have the following features:

- Supports up to 250 access points
- Handles up to 5,000 clients
- Throughput: ~5 Gbps
- Support for Wi-Fi 6E or the latest equivalent and backward compatibility with Wi-Fi 5/6 access points that may still be in operation.
- Centralised management of access points, SSIDs, RF profiles, and security policies
- Integrated security features including WPA3, secure boot, and policy-based access control
- Scalable architecture supporting small to medium enterprise deployments with future expansion capability
- Cloud-managed or on-premises deployment options, compatible with existing network and security infrastructure
- Support for ACSA Wi-Fi portal, or provision of a suitable replacement captive portal with equivalent functionality
- Must support high availability
- Licensing model must include all required features (connectivity, analytics, location services, policy enforcement)
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement
- Include decommissioning of existing controller infrastructure, documentation, asset tagging, and validation testing and commissioning of new controller
- The new controller must be able to support and manage all existing WIFI access points that connect to the existing controller, and retain all existing features.

6.0 WIFI Work Package - Replacement Large Site WLAN controller

Supply, physically install, and configure a enterprise grade WLAN controller to replace the existing controller infrastructure supporting enterprise-grade Wi-Fi 6E or the latest equivalent access points. The controller must have the following features:

- Supports up to 2,000 access points
- Handles up to 32,000 clients
- Throughput: ~40 Gbps
- Support for Wi-Fi 6E or the latest equivalent and backward compatibility with Wi-Fi 5/6 access points that may still be in operation.
- Centralised management of access points, SSIDs, RF profiles, and security policies
- Integrated security features including WPA3, secure boot, and policy-based access control
- Scalable architecture supporting small to medium enterprise deployments with future expansion capability
- Cloud-managed or on-premises deployment options, compatible with existing network infrastructure
- Support for ACSA Wi-Fi portal, or provision of a suitable replacement captive portal with equivalent functionality
- Must support high availability
- Licensing model must include all required features (connectivity, analytics, location services, policy enforcement)
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement
- Include decommissioning of existing controller infrastructure, documentation, asset tagging, and validation testing and commissioning of new controller.
- The new controller must be able to support and manage all existing WIFI access points that connect to the existing controller, and retain all existing features.

7.0 Security Work Package - Replacement of Small Site Firewalls

Supply, physically install, and configure a enterprise grade next-generation firewall and threat prevention appliance to replace the existing small site firewalls, ensuring advanced threat protection, high availability, and centralised security management.

The appliance must have the following features:

- Firewall throughput of up to 18 Gbps
- Next-generation firewall (NGFW) throughput of 6.2 Gbps
- Threat prevention throughput of 3.7 Gbps, including IPS, antivirus, anti-bot, URL filtering, DNS security, and sandboxing
- VPN throughput of 4.9 Gbps using AES-256 encryption
- Connection rate of 116,000 connections per second, supporting up to 2 to 8 million concurrent connections depending on memory configuration
- Hardware configuration includes, minimum:
    - 16 GB RAM
    - 240 GB SSD storage
    - Lights-Out Management (LOM) module
    - 10x 1GbE copper ports
    - 4x 10GbE SFP+ ports with transceivers
    - Dual AC power supplies
- Supports Layer 2 and Layer 3 routing, NAT, VRRP, OSPF, BGP, RIP, and multicast protocols
- Supports HTTPS inspection, including TLS 1.3 and HTTP/2 traffic
- Modular chassis, rack mountable with high port density and expansion options
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Includes 5-year license and maintenance, with OEM hardware warranty and 4-hour replacement SLA
- Includes sandboxing subscription Package - for advanced threat prevention, file sanitisation, and zero-phishing
- Include decommissioning of existing security appliance, documentation, asset tagging, and validation testing and commissioning of new appliance with existing firewall rule base.
- The firewall appliance must be integrated with the existing centralised firewall management system to ensure unified policy enforcement, monitoring, and administration across the network.
- SFPs must be supplied, if the existing SFPs are not supported in the proposed OEM models.

8.0 Security Work Package - Replacement of Medium Site Firewalls

Supply, physically install, and configure a enterprise grade next-generation firewall and threat prevention appliance to replace the existing medium site firewalls, ensuring advanced threat protection, high availability, and centralized security management.

The appliance must have the following features:

- Firewall throughput of up to 55 Gbps, with 80 Gbps for large UDP packets (1518B)
- Threat prevention throughput of up to 4.95 Gbps, including IPS, antivirus, anti-bot, and sandboxing
- Next-generation firewall (NGFW) throughput of 18.6 Gbps
- VPN throughput of 22.1 Gbps using AES-256 encryption
- Connection rate of 190,000 connections per second, supporting up to 16.2 million concurrent connections
- Hardware configuration includes:
    - 32 GB RAM
    - 480 GB SSD SATA storage
    - Lights-Out Management (LOM) module
    - 4-port 1GBase-F SFP+ interface card with 4 SFPs
    - Dual AC power supplies
- Supports Layer 2 and Layer 3 routing, NAT, VRRP, OSPF, BGP, RIP, and multicast protocols
- Supports HTTPS inspection, including TLS 1.3 and HTTP/2 traffic
- Modular chassis, rack mountable with high port density and expansion options
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Includes 5-year license and maintenance, with OEM hardware warranty and 4-hour replacement SLA
- Includes sandboxing subscription Package - for advanced threat prevention, file sanitisation, and zero-phishing
- Include decommissioning of existing security appliance, documentation, asset tagging, and validation testing and commissioning of new appliance with existing firewall rule base.
- The firewall appliance must be integrated with the existing centralised firewall management system to ensure unified policy enforcement, monitoring, and administration across the network.
- SFPs must be supplied, if the existing SFPs are not supported in the proposed OEM models.

9.0 Security Work Package - Replacement of Large Site Firewalls

Supply, physically install, and configure an enterprise grade next-generation firewall and threat prevention appliance to replace the existing large site firewalls, ensuring advanced threat protection, high availability, and centralized security management.

The appliance must have the following features:

- Firewall throughput of up to 70 Gbps, with 80.2 Gbps for large UDP packets (1518B)
- Threat prevention throughput of up to 10.5 Gbps, including IPS, antivirus, anti-bot, DNS security, and sandboxing
- Next-generation firewall (NGFW) throughput of 28.2 Gbps
- VPN throughput of 33 Gbps using AES-256 encryption
- Connection rate of 300,000 connections per second, supporting up to 16.2 million concurrent connections
- Hardware configuration includes:
    - 32 GB RAM
    - 480 GB SSD SATA storage
    - Dual AC power supplies for high availability
    - Lights-Out Management (LOM) for remote monitoring and control
    - 8 x RJ45 ports and 8 x 1/10GbE SFP+ ports for high-density connectivity
- Supports Layer 2 and Layer 3 routing, NAT, VRRP, OSPF, BGP, RIP, and multicast protocols
- Supports HTTPS inspection, including TLS 1.3 and HTTP/2 traffic
- Modular chassis, rack mountable with high port density and expansion options
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Includes 5-year license and maintenance, with OEM hardware warranty and 4-hour replacement SLA
- Includes sandboxing subscription Package - for advanced threat prevention, file sanitisation, and zero-phishing
- Include decommissioning of existing security appliance, documentation, asset tagging, and validation testing and commissioning of new appliance with existing firewall rule base.
- The firewall appliance must be integrated with the existing centralised firewall management system to ensure unified policy enforcement, monitoring, and administration across the network.
- SFPs must be supplied, if the existing SFPs are not supported in the proposed OEM models.

10.0 Security Work Package - Replacement of Centralised Firewall Manager

Supply, physically install, and configure a next-generation firewall and security management appliance to manage the small, medium and large site firewalls by replacing the existing management server infrastructure. This appliance will provide centralised security policy management, log aggregation, and reporting for existing distributed firewall gateways.

The appliance must have the following features:

- Support management of up to 10 security gateways
- Log ingestion capacity of up to 25,000 logs per second sustained
- Log indexing and storage optimised for high-throughput environments
- Support for log correlation between all firewalls, event analysis, compliance reporting
- 32 GB RAM (or higher)
- Dual 480 GB SSD in RAID 1 configuration (mirrored storage for log redundancy)
- Centralised management of:
    - Policy Package - (Firewall, NAT, VPN, Threat Prevention)
    - Objects database and global policy layers
- Include 5-year maintenance and support, with OEM hardware warranty and Next Business Day (NBD) replacement SLA
- Include 5-year compliance event and reporting all firewalls.
- Include decommissioning of existing security appliance, documentation, asset tagging, and validation testing and commissioning of new appliance with existing firewall rule base.

11.0 Security Work Package - Replacement distributed Denial of Service Protector

Supply, physically install, and configure the enterprise grade Distributed Denial of Service Protector appliance to replace the existing DDOS protector, ensuring protection against denial of service attacks.

The appliance must have the following features:

- Dedicated hardware appliance for DDoS mitigation
- Mitigation throughput of up to 12 Gbps
- Protects against both network-layer and application-layer DDoS attacks
- Supports customised signature creation for evolving threats
- Flexible filter engines to detect and block malicious traffic
- Protection against HTTP floods, bandwidth saturation, and protocol anomalies
- Includes 5-year license and maintenance, with OEM hardware warranty and Next Business Day (NBD) replacement SLA
- Include decommissioning of existing security appliance, documentation, asset tagging, and validation testing and commissioning of new appliance
- The DDOS appliance must be integrated with the centralised firewall management system to ensure unified policy enforcement, monitoring, and administration across the network.

12.0 Security Work Package - Replacement of Existing Perimeter Firewall

Supply, physically install, and configure an enterprise-grade next-generation firewall appliance from a different vendor than the internal firewalls, to replace the current perimeter security infrastructure. The solution must ensure advanced threat protection and high availability, while maintaining vendor diversity to minimise OEM specific vulnerabilities.

The appliance must have the following features:

- Firewall throughput of at least 80 Gbps
- Threat protection throughput of at least 10 Gbps, including IPS, anti-malware, application control, and sandboxing
- SSL/TLS inspection throughput of at least 8 Gbps, with support for TLS 1.3
- VPN throughput of at least 40 Gbps, supporting IPsec and SSL VPN
- Concurrent session capacity of at least 10 million, with a new session rate of 400,000 per second
- Integrated SD-WAN capabilities for link optimisation and application-aware routing
- Advanced routing support including BGP, OSPF, RIP, and multicast
- High port density, including multiple 1G and 10G interfaces for flexible deployment
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Licensing model must include all required features (NGFW, SD-WAN, threat protection, application control, reporting)
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement SLA
- Include decommissioning of existing firewall infrastructure, documentation, asset tagging, and validation testing and commissioning of new appliance
- Centralised management via vendor-supported platform for policy, logging, and analytics

13.0 Security Work Package - Replacement of Existing Public WIFI Firewall

Supply, physically install, and configure an enterprise-grade next-generation firewall appliance from approved vendors to replace the existing perimeter security infrastructure, ensuring advanced threat protection and high availability.

The appliance must have the following features:

- Firewall throughput of at least 40 Gbps
- Threat protection throughput of at least 5 Gbps, including IPS, anti-malware, application control, and sandboxing
- Concurrent session capacity of at least 5 million, with a new session rate of 400,000 per second
- High port density, including multiple 1G and 10G interfaces for flexible deployment
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Licensing model must include all required features (NGFW, SD-WAN, threat protection, application control, reporting)
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement SLA
- Include decommissioning of existing firewall infrastructure, documentation, asset tagging, and validation testing and commissioning of new appliance
- Centralised management via vendor-supported platform for policy, logging, and analytics

14.0 Security Work Package - Replacement of Existing Small Site Web Proxy Solution

Supply, physically install, and configure an enterprise-grade secure web gateway (SWG) appliance from approved vendors to replace the existing web proxy infrastructure, providing advanced web security, URL filtering, malware protection, and policy enforcement capabilities for outbound web traffic.

The solution must have the following features:

- The solution must fit into ACSA's existing architecture or include the costs of any additional requirements including bandwidth
- Solution throughput must support sustained web traffic inspection for the user base per site
- Solution throughput must support concurrent HTTP/HTTPS connections for the userbase per site.
- Comprehensive URL filtering with support for URL categories and real-time updates
- Advanced malware protection with real-time threat intelligence and file reputation scoring
- HTTPS (SSL/TLS) traffic inspection with full certificate validation, policy control, and support for TLS 1.3
- Integrated Data Loss Prevention (DLP) capabilities for web uploads and posts
- Support for ICAP to integrate with external DLP and AV engines
- Must support user quotas for time and bandwidth.
- Authentication integration with Active Directory, LDAP, and SAML
- Policy-based control over user access, applications, content categories, and file types
- Support for Active Directory user, Active Directory group-based and IP-based reporting and policy enforcement
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Support for log forwarding to SIEM systems using syslog, CEF, or LEEF formats
- Must be deployment as a transparent proxy to ensure seamless mobility across sites.
- Centralised management and reporting platform for policy administration and traffic analytics
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement SLA
- Include decommissioning of existing web proxy infrastructure, documentation, asset tagging, and validation testing and commissioning of new appliance

15.0 Security Work Package - Replacement of Existing Large Site Web Proxy Solution

Supply, physically install, and configure an enterprise-grade secure web gateway (SWG) appliance from approved vendors to replace the existing web proxy infrastructure, providing advanced web security, URL filtering, malware protection, and policy enforcement capabilities for outbound web traffic.

The solution must have the following features:

- The solution must fit into ACSA's existing architecture or include the costs of any additional requirements including bandwidth
- Solution throughput must support sustained web traffic inspection for the user base per site
- Solution throughput must support concurrent HTTP/HTTPS connections for the userbase per site.
- Comprehensive URL filtering with support for URL categories and real-time updates
- Advanced malware protection with real-time threat intelligence and file reputation scoring
- HTTPS (SSL/TLS) traffic inspection with full certificate validation, policy control, and support for TLS 1.3
- Integrated Data Loss Prevention (DLP) capabilities for web uploads and posts
- Support for ICAP to integrate with external DLP and AV engines
- Must support user quotas for time and bandwidth.
- Authentication integration with Active Directory, LDAP, and SAML
- Policy-based control over user access, applications, content categories, and file types
- Support for Active Directory user, Active Directory group-based and IP-based reporting and policy enforcement
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Support for log forwarding to SIEM systems using syslog, CEF, or LEEF formats
- Must be deployment as a transparent proxy to ensure seamless mobility across sites.
- Centralised management and reporting platform for policy administration and traffic analytics
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement SLA
- Include decommissioning of existing web proxy infrastructure, documentation, asset tagging, and validation testing and commissioning of new appliance

16.0 IPT Work Package - Supply and install a high-spec server for the IP Telephony environment

Supply, install, and configure enterprise-grade server appliances, including applicable call control and telephony application software, to replace end-of-life servers within the IP Telephony infrastructure. The server must support hosting multiple IP Telephony applications such as specified in **Annexure A, table 1.**

Minimum Technical Specifications

- Rack-mountable server appliance (2U)
- Dual high-performance CPUs, minimum 16 cores per CPU (32 cores total), base frequency ≥ 2.8 GHz
- Minimum 192 GB DDR5 RDIMM memory
- 24 × 600 GB SAS 10K RPM SFF HDD, hot-swappable
- RAID controller with minimum 4 GB Flash Backed Write Cache, supporting RAID 0, 1, 5, 6, 10, 50, 60
- Minimum 8 × 10 Gigabit Ethernet ports (SFP+), plus 1 GbE management port
- Dual redundant hot-plug power supplies (minimum 1200W AC Titanium)
- TPM 2.0 module (FIPS 140-2, Common Criteria EAL4+ certified)
- Compatible with VMware ESXi hypervisor
- Enterprise-grade compliance for reliability and security
- Supply, installation, configuration, integration, testing, commissioning, documentation, and removal of old hardware.
- Provide virtualization capability for hosting these applications on a single platform.
- Ensure seamless integration with existing IP Telephony infrastructure.
- Support migration from legacy servers without downtime.
- Minimum 5-year OEM hardware warranty with Next Business Day replacement.

17.0 IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment

Supply, install, and configure enterprise-grade edge routers to replace end-of-life voice gateways, as specified as in **Annexure A, table 1.** Must support SIP voice integration and secure, high-performance connectivity for each airport site. The supplied SIP Voice Gateways must be fully compatible with the existing IP Telephony platform (including call control servers, dial plans, and voice features) and support SIP trunking as currently implemented with external service providers. The solution must allow migration of voice services from legacy gateways without redesign or downtime.

Minimum Technical Specifications

- Rack-mountable, 1RU design with 19" rack-mount kit
- Multicore CPU architecture (minimum 8 cores)
- Minimum 8 GB DRAM memory
- Minimum 16 GB internal flash storage
- Minimum 4 × 1 Gigabit Ethernet WAN ports (RJ45 and SFP)
- USB interface for storage/configuration
- NIM slot with 64-channel DSP capability for voice services
- Embedded IPsec VPN hardware acceleration (≥ 1 Gbps)
- Support for SASE architecture and container-based security services
- Zero-touch provisioning (Plug-and-Play)
- Support for modular OS with SD-WAN capability
- Tamper-resistant hardware with TPM module
- Must integrate with existing IP Telephony infrastructure and SIP trunking.
- Support migration of voice services without downtime.
- Supply, installation, configuration, integration, testing, commissioning, documentation, and removal of old hardware.
- Minimum 5-year OEM hardware warranty with Next Business Day replacement.

18.0 IPT Work Package - Supply and install IP Telephones

Supply, install, and configure new IP telephones to replace end-of-life units at all airport check-in counters, departure gates and iHelp areas.

Minimum Technical Specifications

- Colour: Carbon Black or equivalent
- Dual Ethernet ports (RJ-45) with PoE support
- 100/1000BASE-T Ethernet compliance (IEEE 802.3 standards)
- Compatibility with enterprise UC platforms and SIP-based systems
- Multiline operation (minimum 4 lines)
- Caller ID display
- Full-duplex speakerphone
- High-resolution colour display
- Support for secure SIP signalling and media encryption (TLS/SRTP)
- Must integrate with existing IP Telephony infrastructure without service disruption.
- Support centralized provisioning and firmware upgrades.
- Supply, installation, configuration, integration, testing, commissioning, documentation, and removal of old hardware.

19.0 IPT Work Package - Supply and install single telephone brackets to secure phones

Supply and install telephone brackets at all airport check-in counters, boarding gates and iHelp areas, to securely hold IP telephones and prevent tampering.

Minimum Technical Specifications

- Material: Mild steel, powder-coated for corrosion resistance
- Finish: Matte black
- Dual-purpose design for wall and desk mounting
- Lockable enclosure or tamper-resistant fasteners
- Provision for cable management and securing network/power cables
- Bracket dimensions to be finalized based on IP telephone model
- Supply, installation, secure mounting of IP telephones, removal of old hardware, documentation, and handover.

20.0 NETWORK Work Package - REPLACE ENTERPRISE ACCESS SWITCHES

Enterprise-Grade 48-Port PoE+ Access Switches

Supply, configure and implement Enterprise-Grade 48-Port PoE+ Access Switches at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after every location-specific operating hours and after last flight. Include decommissioning of existing Cisco 3650 switches and asset management in your pricing.

- "Bidders are invited to propose switches that meet or exceed these specifications.
- Port Configuration: 48 Gigabit Ethernet ports with Power over Ethernet Plus (PoE+) support, delivering up to 30W per port.
- PoE Budget: Minimum 700W total PoE power budget
- Switching Capacity: Minimum 200 Gbps switching capacity (non-stacked) with support for stacking to achieve higher throughput (up to 400 Gbps or greater preferred).
- Uplink Ports: Modular or fixed uplinks supporting at least 4x 10 Gigabit Ethernet (10GE) SFP+ ports for high-speed connectivity.
- Layer Support: Layer 2
- Stacking: Include modules and cables for each switch stacking with a minimum stacking bandwidth of 100 Gbps
- Reliability: High availability, including redundant power supplies and hot-swappable components.
- Software Features: Support for enterprise-grade software capabilities, including network analytics, automation, and integration with modern network architectures (e.g., SD-Access or equivalent).
- Form Factor: 1RU rack-mountable design.
- Interoperability: Must interoperate with existing Cisco equipment in mixed environments.
- Warranty and Support: Minimum 5-year warranty with Next Business Day replacement and options for extended support and maintenance services.
- Existing switches that need to be replaced, currently use Cisco SFPs which will be reused, therefore if the existing Cisco SFPs are not supported by proposed OEMs, 2 X10G Long Range Single Mode SFPs per switch need to be supplied

21.0 NETWORK Work Package - REPLACE BRANCH TYPE ACCESS SWITCHES

Stackable 24 or 48 Port Enterprise PoE+ Access Switches

Supply, configure and implement stackable 24 and 48-Port PoE+ Access Switches at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after every location-specific operating hours and after the last flight. Include decommissioning of existing Cisco 2960X switches and asset management in your pricing.

- Bidders are invited to propose switches that meet or exceed these specifications.
- Type: Stackable, managed Layer 2/3 enterprise access switch.
- Minimum 24 or 48 Gigabit Ethernet (GE) ports (RJ45) for client connectivity.
- Minimum 4x 10 Gigabit Ethernet (1/10GE) SFP+ uplink ports
- Support for PoE/PoE+ (IEEE 802.3af/at) on all GE ports.
- Minimum PoE power budget of 370W (for 24-port models) or 740W (for 48-port models), upgradable to higher budgets.
- Modularity: Support for hot-swappable, redundant power supplies and fans.
- Switching Capacity: Minimum 128 Gbps for 24-port models or 176 Gbps for 48-port models.
- Support for physical or virtual stacking of up to 6 switches.
- Dual, hot-swappable AC power supplies (redundant).
- Stacking: Include modules and cables for each switch
- Warranty: Minimum 5-year hardware warranty with next-business-day replacement.
- Include 1x Stack Kit per switch
- Interoperability: Must interoperate with existing Cisco equipment in mixed environments.
- Warranty and Support: Minimum 5-year warranty with Next Business Day replacement and options for extended support and maintenance services.
- Existing switches that need to be replaced, currently use Cisco SFPs which will be reused, therefore if the existing Cisco SFPs are not supported by proposed OEMs, 2 X10G Long Range Single Mode SFPs per switch need to be supplied

22.0 NETWORK Work Package - REPLACE 1U MPLS PE CORE SWITCHES

Enterprise Grade 48 Port 1/10/25/40/100Gbps Core Switch

Supply, configure and implement an Enterprise Grade 48 Port 1/10/25/40/100Gbps Core Switch at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after operating hours and after the last flight. Include decommissioning of existing 9500X switches and asset management in your pricing.

- Bidders are invited to propose switches that meet or exceed these specifications.
- Enterprise-Grade 48-Port 1/10/25/40/100Gbps Core Switch
- Form Factor: 1RU (Rack Unit) fixed configuration switch.
- Minimum 48 ports supporting 25 Gigabit Ethernet (SFP28 or equivalent).
- Minimum 4 to 6 ports supporting 40/100 Gigabit Ethernet (QSFP28 or equivalent).
- All ports must support auto-negotiation and backward compatibility with lower speeds (e.g., 1/10 Gbps).
- Switching Capacity: Minimum 2 Tbps, with preference for higher capacity up to 6.6 Tbps.
- Layer Support: Full Layer 2 and Layer 3 functionality, including VLANs, QoS, and IPv4/IPv6 routing and MPLS.
- Stacking/Virtualisation: Support for switch stacking or virtual chassis technology to enable unified management of multiple switches.
- Programmability: Support for APIs (e.g., NETCONF, RESTCONF, or equivalent) for integration with SDN environments.
- Monitoring: Support for telemetry, sFlow, or equivalent for real-time network analytics.
- Power Supply: Dual redundant AC power supplies, with minimum power consumption efficiency (80 PLUS Platinum or equivalent).
- Must support industry-standard protocols (e.g., IEEE 802.1Q, 802.3ad, OSPF, BGP, MPLS).
- Compatibility with existing Cisco enterprise network infrastructure, including downstream switches
- Minimum 5-year license and OEM warranty with 24/7/4 hardware replacement.
- Existing switches that need to be replaced, currently use Cisco SFPs which will be reused, therefore if the existing Cisco SFPs are not supported by proposed OEMs, then include 112 X10G Long Range Single Mode SFPs per switch.

"

23.0 NETWORK Work Package - NTP SERVER APPLIANCES

SyncServer S650 GNSS-Referenced NTP/PTP Time Server

Supply, configure and implement SyncServer S650 GNSS-Referenced NTP/PTP Time Server at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. Include decommissioning of existing NTP appliances and asset management in your pricing.

- 090-15200-650 "Microchip model SyncServer S650, includes Kit: 75 ft. total length: 50 ft.
- Cable; Lightning Arrestor; 25 ft. Cable; Antenna Kit"
- 090-15201-002 Dual AC Power Supply
- 090-15201-009 SyncServer 10 GbE Module
- 090-15201-013 SyncServer Timing I/O Module with Fiber Outputs

24.0 NETWORK Work Package - REPLACE MODULAR MPLS CORE SWITCHES

Supply, configure and implement 4x Core Switches at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after operating hours and after the last flight. Include decommissioning of existing Cisco 6807 chassis and modules, and asset management in your pricing.

Generic Specification for Modular High-Density Ethernet Switch System. This specification outlines the requirements for a modular, high-performance Ethernet switch system suitable for enterprise core or aggregation network deployments. The system shall provide scalable, non-blocking Layer 2/3 switching with high port density for 10/25 Gigabit Ethernet (GbE) and 40/100 GbE interfaces, dual supervisor redundancy, and N+1 power supply redundancy. The design shall support future scalability to at least 25 Tbps total switching capacity. All components must be hot-swappable for high availability, with support for redundant fans and power inputs. The system shall comply with relevant standards including IEEE 802.3, RoHS, and NEBS Level 3 (if applicable for carrier-grade deployments).1. Chassis Requirements

- Form Factor: Rack-mountable chassis, occupying no more than 8 rack units (RU) height.
- Slot Configuration: Minimum 4 slots for line cards, plus 2 dedicated slots for supervisor modules.
- Switching Capacity: Up to 25 Tbps full-duplex (12.5 Tbps half-duplex) wired switching capacity, with per-slot forwarding bandwidth of at least 6 Tbps.
- Port Density: Capable of supporting up to 96 native 10/25/50 GbE ports or equivalent mix of 40/100 GbE ports across all line cards.
- Backplane/Interconnect: Non-blocking fabric with full-mesh connectivity between all slots, supporting distributed forwarding across line cards.

2. Supervisor Module Requirements

- Quantity: 2 redundant supervisor modules (active/standby or active/active SSO configuration for stateful switchover).
- Performance: Each module shall provide a minimum of 3 Tbps full-duplex switching capacity, based on a programmable ASIC architecture optimized for high-scale routing and security features.
- Processing: Multi-core CPU (at least 2 GHz) with at least 16 GB DRAM and 16 GB flash storage for system software and logging.
- Features:
    - Hardware-based forwarding for IPv4/IPv6 unicast/multicast, MPLS, QoS, and ACLs up to 1 million entries.
    - Integrated security with TrustSec and MACsec encryption.
    - Software-defined networking (SDN) compatibility, including OpenFlow and NETCONF/YANG.
- Redundancy: 1+1 supervisor redundancy with sub-second failover, including redundant clocks and fabric interfaces.

3. Line Card Requirements for 10/25 GbE

- Type: Modular line cards compatible with the chassis slots, supporting 1/10/25 GbE breakout configurations.
- Port Density
    - 2X 24-port line card with SFP28 transceivers, configurable for 1/10/25 GbE per port.
- Performance: Minimum 2.4 Tbps per line card; non-blocking at line rate for all ports simultaneously.
- Interfaces: SFP28 cages supporting multimode/single-mode fiber, DAC, and AOC transceivers; compliant with IEEE 802.3by (25GBASE-SR/CR) and 802.3ae (10GBASE).
- Features:
    - Wire-rate Layer 2/3 forwarding with VXLAN/EVPN support.
    - Per-port QoS with 8 queues, ingress/egress policing up to 100 Gbps.
    - Hardware timestamping for PTP (IEEE 1588v2) and SyncE.
- Power Consumption: Maximum 400W per card under full load.

4. Line Card Requirements for 40/100 GbE

- Type: Modular line cards compatible with the chassis slots, supporting 40/100 GbE with breakout to lower speeds.
- Port Density
    - 2X 24-port line card with QSFP28 transceivers, configurable as 24 x 40 GbE or 12 x 100 GbE (non-blocking).
- Performance: Minimum 2.4 Tbps per line card; non-blocking at line rate, with support for 4:1 oversubscription if hybrid ports are used.
- Interfaces: QSFP28 cages supporting multimode/single-mode fiber, DAC, and AOC; compliant with IEEE 802.3ba (40GBASE) and 802.3bm (100GBASE).
- Features:
    - Flexible port grouping for breakout (e.g., 100 GbE to 4 x 25 GbE).
    - Advanced buffering (minimum 40 MB shared) for bursty traffic.
    - Telemetry and analytics via gRPC and model-driven programmability.
- Power Consumption: Maximum 500W per card under full load.

5. Power System Requirements

- Redundancy Mode: N+1 power supply redundancy, where N is the number of active power supplies required for full system load, and +1 provides hot-standby failover without service interruption.
- Quantity and Type: Minimum 4 hot-swappable power supply units (PSUs) per chassis; support for both AC (100-240V) and DC (-48V) inputs.

- Capacity: Each PSU rated for at least 2500W output; total system power budget supporting full chassis population (up to 10 kW).
- Efficiency: 80 PLUS Platinum certified (minimum 94% efficiency at 50% load).
- Monitoring: Integrated power management with real-time telemetry, fault detection, and automatic load balancing across PSUs.
- Input Safeguards: Independent input circuits per PSU pair, with protection against single-point failures.

6. General System Features

- High Availability: Stateful switchover (SSO), non-stop forwarding (NSF), and graceful restart (GR) for routing protocols (OSPF, BGP, IS-IS).
- Software: Vendor-provided network operating system with unified image across chassis and line cards; support for zero-touch provisioning (ZTP) and automation via Ansible/Python APIs.
- Security: Role-based access control (RBAC), 802.1X authentication, and encrypted management (SSHv2, TLS 1.3).
- Warranty and Support: Minimum 5-year hardware warranty with 4 HOUR advance replacement;
- Compliance and Testing: System shall undergo interoperability testing with standard transceivers (e.g., MSA-compliant) and provide documentation for RFP compliance.

7. Pricing (RFP Guidance)

- Bidders shall provide pricing for a baseline configuration: 1 chassis, 2 supervisor modules, 2 x 10/25 GbE line cards, 2 x 40/100 GbE line cards, 4 x PSUs, and redundant fans.

25.0 NETWORK Work Package - REPLACE FIBRE DISTRIBUTION SWITCHES

Supply, configure and implement Enterprise Grade 12 and 24 Port 1/10/25/Gbps L2/L3 Fibre Distribution Switches at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after operating hours and after the last flight. Include decommissioning of existing Cisco 3850-12S and 3850-24S switches and asset management in your pricing. **All devices to have a 5-year SNTP 24X7X4 warranty.**

The switch shall support modular uplink options for scalability, advanced security features, and model-driven programmability. It must be compatible with open standards (e.g., IEEE 802.3), run on a modular OS supporting NETCONF/RESTCONF/YANG, and provide investment protection through backward compatibility with similar series components. Target use cases include SD-WAN edge, aggregation for access switches, and secure fabric underlay.

Hardware Specifications

- The switch shall be 1RU rack-mountable with field-replaceable units (FRUs) for fans and power supplies.
- Downlink Ports - 12 or 24 multi-rate SFP28 ports supporting 1G/10G/25G fiber (e.g., SR/LR transceivers) - Auto-negotiation for speed and duplex
- Uplink Ports - Modular expansion: 8 x 10G/25G SFP28 via removable network module
- Cooling & Redundancy - 3 x redundant, hot-swappable fans (N+1)
- Power Supplies - Dual hot-swappable AC (1+1 redundant); default 715W AC, scalable to 1,100W for 24 port models.
- Stacking Bandwidth - Up to 1 Tbps bidirectional (e.g., via dedicated StackWise cables: 1m lengths)
- Maximum Stack Members: 4 switches (mixable with compatible access models)
- High Availability: Stateful switchover (SSO), non-stop forwarding (NSF), graceful restart; hitless software upgrades; ISSU support
- Redundancy Protocols: VRRP/HSRP/GLBP for first-hop; LACP/MLAG for link aggregation
- Protocols: SNMPv3, NETCONF/RESTCONF/gRPC, Syslog, sFlow/NetFlow (up to 64K flows)
- Programmability: Python scripting, guest shell for containers/apps (e.g., via Docker)
- Orchestration: gNMI telemetry, OpenConfig support; integration with SDN controllers (e.g., Cisco DNA or open equivalents)
- OS: Modular, patchable network OS with zero-touch provisioning (ZTP)
- Licensing: Perpetual base + optional add-ons for advanced routing/security (e.g., DNA Advantage equivalent)
- Warranty: Minimum 5 years with next-business-day support; optional 24x7 TAC
- Existing switches that need to be replaced, currently use Cisco SFPs which will be reused, therefore if the existing Cisco SFPs are not supported by proposed OEMs, then include 10x 10G Long Range Single Mode SFPs for every 12-port switch.
- Existing switches that need to be replaced, currently use Cisco SFPs which will be reused, therefore if the existing Cisco SFPs are not supported by proposed OEMs, then include 20x 10G Long Range Single Mode SFPs for every 24-port switch.

AIRPORTS COMPANY
SOUTH AFRICA

26.0 NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs

Supply, configure and implement link speed upgrades at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after operating hours and after the last flight. Equipment must be OEM certified

Part Number	Description
SFP-10G-LRM=	10GBASE-LRM SFP Module
SFP-10G-LR-S=	10GBASE-LR SFP Module, Enterprise-Class

27.0 NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G

Supply, configure and implement link speed upgrades at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after operating hours and after the last flight. Equipment must be OEM certified

Part Number	Description
QSFP-100G-LR4-S=	100GBASE LR4 QSFP Transceiver, LC, 10km over SMF
SFP-10/25G-LR-S=	10/25GBASE-LR SFP28 Module

28.0 NETWORK Work Package - PHASED REPLACEMENT ENTERPRISE ACCESS SWITCHES

Enterprise-Grade 48-Port PoE+ Access Switches

Supply, configure and implement Enterprise-Grade 48-Port PoE+ Access Switches at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after every location-specific operating hours and after the last flight. Include decommissioning of existing Cisco 9300 switches and asset management in your pricing.

- Bidders are invited to propose switches that meet or exceed these specifications.
- Port Configuration: 48 Gigabit Ethernet ports with Power over Ethernet Plus (PoE+) support, delivering up to 30W per port.
- PoE Budget: Minimum 700W total PoE power budget
- Switching Capacity: Minimum 200 Gbps switching capacity (non-stacked) with support for stacking to achieve higher throughput (up to 400 Gbps or greater preferred).
- Uplink Ports: Modular or fixed uplinks supporting at least 4x 10 Gigabit Ethernet (10GE) SFP+ ports for high-speed connectivity.
- Layer Support: Layer 2
- Stacking: Include modules and cables for each switch stacking with a minimum stacking bandwidth of 100 Gbps
- Reliability: High availability, including redundant power supplies and hot-swappable components.
- Software Features: Support for enterprise-grade software capabilities, including network analytics, automation, and integration with modern network architectures (e.g., SD-Access or equivalent).
- Form Factor: 1RU rack-mountable design.
- Interoperability: Must interoperate with existing Cisco equipment in mixed environments.
- Warranty and Support: Minimum 5-year OEM warranty with Next Business Day replacement and options for extended support and maintenance services.
- Existing switches that need to be replaced, currently use Cisco SFPs which will be reused, therefore if the existing Cisco SFPs are not supported by proposed OEMs,
  then include 1x 10G Long Range Single Mode SFPs for every 12-port switch.