AIRPORTS COMPANY
SOUTH AFRICA

Annexure D – IT Standards

Tel: +27 (0)11 723 1400 Fax: +27 (0)11 453 9353
The Maples, Riverwoods, 24 Johnson Road, Bedfordview, Gauteng, South Africa, 2007
PO Box 75480, Gardenview, Gauteng South Africa, 2047

www.airports.co.za

Airports Company South Africa SOC Ltd Reg No. 1993/004149/30 VAT no. 4930138393

Contents

TABLES

Glossary of Terms

ACSA	Airport Company South Africa
ASIC	Application-Specific Integrated Circuit
EA	Enterprise Architecture
GDR	Geographically Dispersed Resiliency
GDPS	Geographically Dispersed Parallel Sysplex
HBA	Host Bus Adapter
HSRP	Hot Standby Router Protocol
LAP's	Lightweight Access Points
IT	Information Technology
ITAC	Information Technology Architecture Committee
ITIAS	Information Technology Infrastructure Architecture Standards
IT MANCO	Information Technology Management Committee
ISL	Inter Switch Links
NPIV	N-Port ID Virtualization
NVMe	Non-Volatile Memory express
OS	Operating System
QoS	Quality of Service
LAN	Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network

1.0 Purpose and Objective

The purpose of this document is to define and specify sets of Information Technology Standards for Airports Company South Africa (ACSA) to be adhered to by Potential Service provides. This is done to ensure a compatible, integrated and standardised environment and the optimisation of the technology.

Only the Standards, Technologies, Products and compilation of products described in this document may be purchased, installed, used and supported within the organisation.
Any other products, upgrades and enhancement to the current accepted standards must be approved via Information Technology Architecture Council (ITAC) and noted by Information Management Committee (IT MANCO).

All IT equipment and software maintenance and warranties must be handed over to the current incumbent maintenance service providers of ACSA where a existing contract exists. This is not applicable to completely new services. Costing for this maintenance and warranties must be included into the bid.

2.0 General

2.1 Connectivity to ACSA

Connectivity to the ACSA on-premises systems will be facilitated through either a Site-To-Site or a Point-to-Site VPN.

Point to Site VPN
VPN product:Checkpoint Mobile client for laptops and Checkpoint Capsule for mobile devices
Version: 88.10+

Site-to-Site IPsec VPN
Encryption
Phase 1
IKEv2 only
Encryption Algorithm AES-256 or higher
Data Integrity SHA-255 or higher
DHG Group 14 or higher
Phase 2
Encryption Algorithm AES-256 or higher
Data Integrity SHA-255 or higher
DHG Group 14 or higher

2.2 Authentication and Authorisation

ACSA uses Microsoft Active Directory for User identities. This is a hybrid implementation; therefore the on-premise directory is integrated with Microsoft EntraID.

Any proposed IT system must integrate with ACSA's Active Directory for authentication, ensuring a single identity for each user across the organisation.

Authorisation can be done via Security groups in Active Directory or within the Proposes system.

2.3 Resilience

Resilience should be built into the proposed system to satisfy the SLA/availability requirements as per the Scope of Work.

The relevant resilience for existing infrastructure is described in this document under the various sections. Should the Potential service provider need to expand any of these systems/infrastructure, it should be designed according to the information provided herein.

2.4 Maintenance

Maintenance is a key factor in ensuring the reliability of IT services. IT is of utmost importance to ensure that proper maintenance plans are in place for any newly introduced IT systems/Software/Infrastructure.

Existing systems are usually covered by maintenance contractors already in place. Should there be any expansion of existing IT systems/Software/Infrastructure, the Potential service provider must engage these contractors for the maintenance **handover** of the new hardware/software. The costs should be included in the submitted bid, except when otherwise requested in the Scope of Work.

2.5 IT Security

IT security is to be considered in all aspects of newly installed system. As a minimum ACSA IT security personal to be issued with the master system passwords and long details. ACSA IT administrator to have access to the operating systems and servers (not the system itself)

2.6 Data Sharing

Any Data or information to be shared or saved should be stored in industry-standard formats. Data should be shared in the best resolution possible, where applicable.
E.g.(not limited)
Images: Jpeg, png,Tiff,BMP etc
Documents: Ms Word, PDF etc.
Spread Sheets : Microsoft excel etc.
Video: Mp4, Avi etc
Audio: Mp3, flac etc.

2.7 Deviation

Deviation from any of the listed information requires **approval** and guidance from the ACSA IT division **and must be obtained during the questions and clarifications phase of the RFP**

2.8 Approval

All designs and Bill of materials must be approved by ACS before ordering any equipment or software.

3.0 Existing Standards and Architecture

3.1 End User Computing Platform Standards

Below id the current **minimum** Specification for standard Laptop and desktop devices. Should any **specialised** hardware be required, it should be noted to ACSA during the Questions/Clarifications phase of the RFP.

3.1.1 Desktop

- A 13th Gen i7-13700 (8+8 Cores/30MB/24T/2.1GHz to 5.1GHz/65W)
- 16GB (1X16GB) DDR5 M.2 2280 512GB PCIe NVMe Class 40 Solid State Drive
- M.2 2280 PCIe NVMe Class 40 Solid State Drive as Boot Drive
- Intel Integrated Graphics
- No Optical Drive
- Intel(R) AX211 Wi-Fi 6E 2x2 and Bluetooth
- System Power Cord C13 (South Africa (Red Top Plug))
- Wired Keyboard
- Optical Mouse
- WLAN
- Intel vPro Enterprise
- Trusted Platform Module (Discrete TPM Enabled)
- Dell Additional Software
- Windows 11 Pro
- Warranty - Next Business Day Onsite repair + Accidental Protection - 48 Moths Service
- 20” Screen

3.1.2 Laptop

- 13th Gen Intel Core i7-1365U vPro (12 MB cache, 10 cores, 12 threads, up to 5.2 GHz Turbo)
- Intel 13th Generation Core i7-1365U vPro,Intel Integrated Graphics,TBT4
- Intel vPro Enterprise Technology Enabled
- 16 GB, 2 x 8 GB, DDR4, 3200 MT/s, dual-channel, Non-ECC
- 512 GB, M.2 2230, PCIe NVMe, SSD, Class 35
- 14.0" FHD (1920x1080) Non-Touch, FHD IR Cam,
- WLAN/WWAN(4G)
- FHD/IR Camera, Temporal Noise Reduction, Camera Shutter, Mic
- Single Pointing, Finger Print Reader
- English International backlit keyboard, 79-key
- Intel(R) Wi-Fi 6E (6 if 6E unavailable) AX211, 2x2, 802.11ax, Bluetooth Wireless Card
- E4 Power Cord 1M with red top plug for South Africa
- Latitude 5440 BTO Configuration
- Windows 11 Pro,
- Warranty - Next Business Day Onsite repair + Accidental Protection - 48 Moths Service

3.2 Operating Systems

Operating Systems	
Back end (Servers)	**Linux:** Red Hat Enterprise RHEL 8.10 or better, Ubuntu22.x LTS or better
	Wintel: Windows 2022 64-bit or better
Front end (End-user)	Windows 11 Latest Current Branch

Table 1 – Operating System Standards

3.3 Compute

Servers will be virtualised as standard practice unless this is not supported by the newly proposed system; in this case physical rack server hardware can still be used.

All hardware devices are to be covered by a minimum 5-year extended OEM warranty and 24x7x4 Support Services.

3.3.1 Virtualization

Virtualisation is ACSA's preferred method of deploying servers.

VMware version 8 is the current virtualisation platform standard at ACSA

Virtualisation is achieved on Hyperconverged (HCI) platforms

3.3.1.1 High-level detail of the Virtual server environment.

- Currently, there are about 57 virtual hosts running at the 3 major airports (ORTIA, CTIA and KSIA), PLZ airport and Aero Park office. These hosts currently host a total of over 800 virtual servers.
- On average ACSA 14 virtual servers per host.
- Hypervisor - ESXi
- Clusters of Hypervisors (hosts) for redundancy

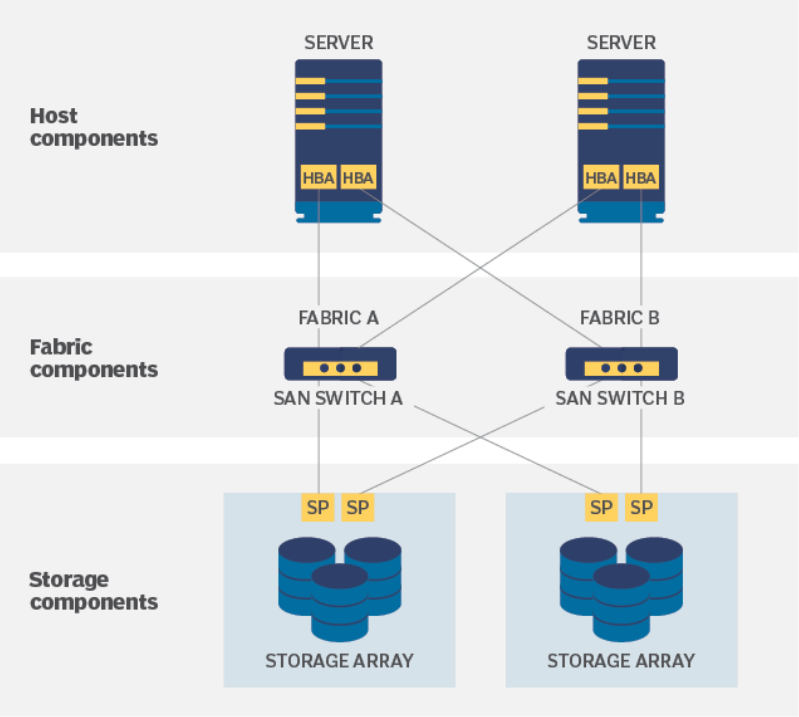
3.3.2 Hyperconverged Server Platform (HCI)

The HCI infrastructure provides the hardware to supply the virtualisation at ACSA. ACSA is currently re-platforming, and the SP should confirm the solution.

3.3.3 Rack Server (Standalone)

Standalone Server Models	
	Two-socket (dual CPU) rack servers offer a wide variety of features to accommodate more demanding workloads and redundancy.
	Four-socket (four CPU) rack servers are the workhorses of the data centre, offering the highest redundancy and performance for the most demanding workloads like data analytics, AI and GPU database acceleration.

Table 2 – Standalone Server Specs



3.4 Databases Platform

Databases
Oracle 12c or latest equivalent
Oracle 11g or latest equivalent
MS SQL 2022 R2 or latest equivalent

Table 3 – Databases

3.5 Messaging Platform

Server	
Software	Microsoft Exchange Online/Hybrid Architecture

Table 4 – Messaging platform

3.6 Data Protection (Backup & Replication) and Storage (SAN)

Data Protection is done via an implementation of DELL/EMC Avamar with DataDomain storage appliances, and replication is done either via Vmware Replication or DELL/ EMC RecoverPoint

Data Storage is achieved via DELL/EMC SAN appliances in the Unity Range.

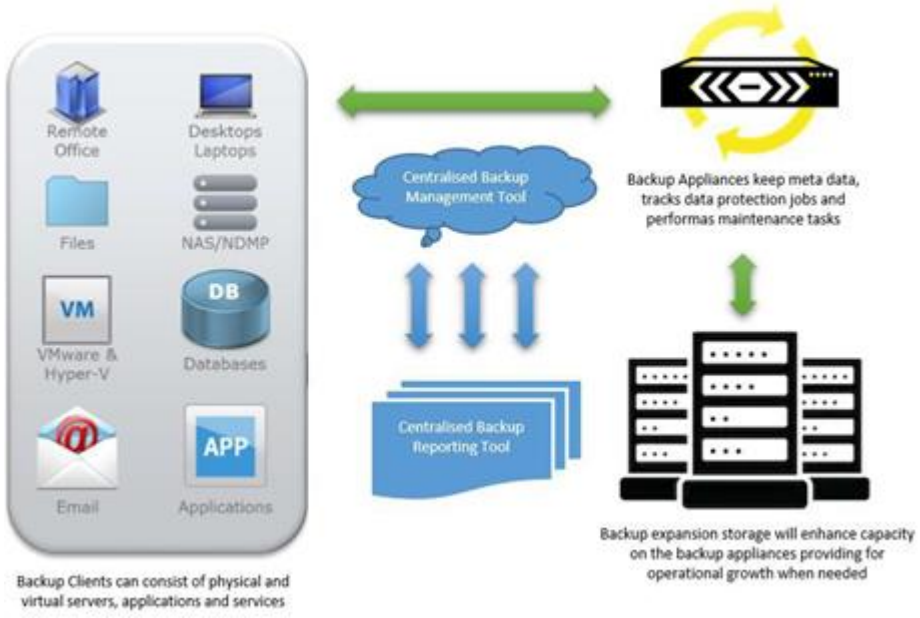
3.6.1 Backups

Backup infrastructure within the ACSA environments has been standardised on DELL/EMC Data Domains (Backup) appliances with Avamar software

Redundancy and High Availability is to be built into the appliances and data protection storage providing **Multiple Shared Uplinks**, **Dual Power Supplies** as well as separate **Processors** per Device.

Large sites **(ORTIA, CTIA, KSIA)** will capture meta and job data on the appliances, whilst backed-up client data will be written to the data protection storage devices. Data protection storage is modular and can be expanded with additional capacities depending on the model of the device. Currently we have 1 large system, 1 medium system and 1 smaller systems at the 3 large campuses.

The diagram below depicts the large airports' standard design (Data Domain backup appliances with expandable storage).



3.6.1.1 Data Domain Backup Device Specification

All data domains (backup) devices are to be covered by minimum 5-year extended OEM warrantee and Dell EMC ProSupport Plus with 4-Hour Mission Critical On-site Response.

PID	PID Description
Standard Datacentre Data (Backup) Appliance	
AVMA1200FG4S	AVAMAR G4S M1200 STORAGE NODE FLD INST
456-104-248	EMC BACKUP SUITE DPA ENABLER=CA
456-104-123	DATA PROT S BACKUP 51-150TB=CA
456-103-951	BACKUP AND RECOVERY MANAGER - NETWORKER
456-104-247	EMC BACKUP SUITE AVAMAR ENABLER=CA
Standard Datacentre Data Domain (Backup) Storage Device Large	
DD4500-2E45	SYSTEM, DD4500+2ES30,3TB SAS HDD, NFS, CIFS
DD4500-CTL-B	SYSTEM, DD4200, CTL, NFS, CIFS
DDRACK-40UN	RACK, DATA DOMAIN,40U
L-BST-4200	LICENSE, BOOST, DD4200
L-REP-4200	LICENSE, REPLICATOR, DD4200

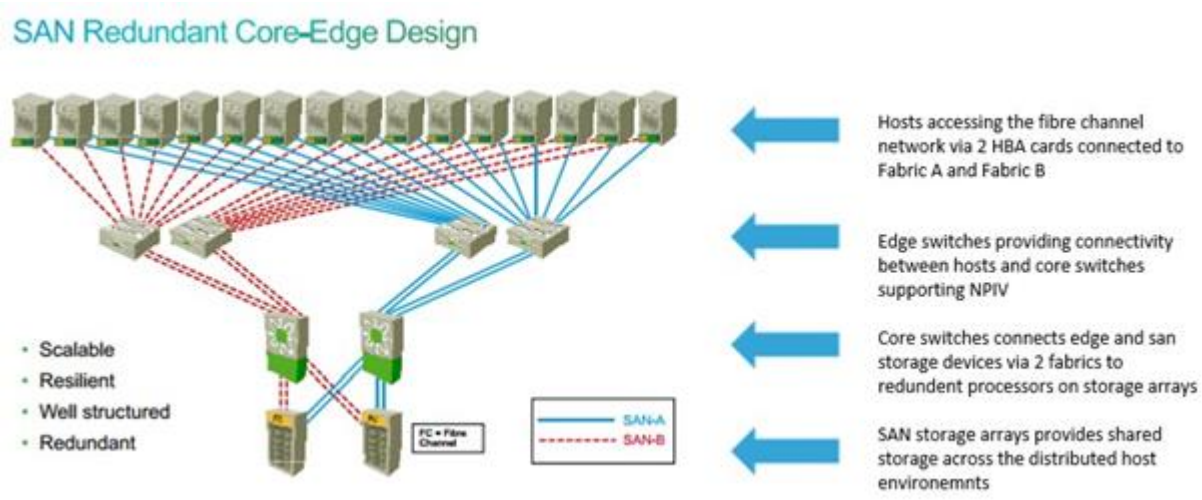
PID	PID Description
U-DDOE-ACT-NC	LICENSE DD OE PER TB UPG ACTIVE=CB
Standard Datacentre Data Domain (Backup) Storage Device Medium	
DD4200-2E45	SYSTEM, DD4200+2ES30,3TB SAS HDD, NFS, CIFS
DD4200-CTL-B	SYSTEM, DD4200, CTL, NFS, CIFS
DDRACK-40UN	RACK, DATA DOMAIN,40U
L-BST-4200	LICENSE, BOOST, DD4200
L-REP-4200	LICENSE, REPLICATOR, DD4200
U-DDOE-ACT-NC	LICENSE DD OE PER TB UPG ACTIVE=CB
Standard Datacentre Data Domain (Backup) Storage Device Small	
DD2500-1E45	SYSTEM, DD2500+1ES45 SAS,81TB, NFS, CIFS
DDRACK-40U	RACK; DATA DOMAIN;40U
L-BST-2500	LICENSE, BOOST, DD2500
L-REP-2500	LICENSE, REPLICATOR, DD2500
L-XCAP2500-B	LICENSE, DD2500 EXP CAP, MORE THAN 66TB

Table 5 – Backup device specs

3.6.2 Storage network

The ACSA storage network infrastructure utilises DELL/EMC or Brocade switches to provide Fibre Channel switching connectivity within the storage environment. This standard is applied to all airports and offices with storage infrastructure spread throughout South Africa. It utilises a **Two-Tier Core-Edge Design** connecting storage units and access hosts via **Fibre Channel Switching Technology**.

The storage network is designed and built to cater for **High Availability and Redundancy** by providing two physically separate fabrics (**A & B**) connecting storage and hosts with multiple paths to utilise. Multi ASIC, Dual Power Supplies, Multiple Link Trunking, Port Virtualisation and 32Gbps SFPs all combine to provide performance within a stable and highly redundant portfolio.



The core switches, located in all main data centres, utilise 48 ports with 4 additional QSFP ports or 96 port with 8 additional QSFP port switches capable of 32Gbps speeds with either single mode or multi model SFP's and cabling. Inter Switch Links (ISL) connectivity between each switch is provided via 4 single-mode fibre links configured as a single trunk.

Edge switches are blade system-based and depend on the system being connected to the SAN network. These switches connect at a minimum speed of 16Gbps and support the Fibre Channel Port Virtualisation (NPIV) standard.

3.6.3 SAN Network Switch Specifications

All storage network devices are to be covered by a minimum 5-year extended OEM warranty and Dell EMC ProSupport with 4-Hour Mission Critical On-site Response

PID	PID Description
Standard Indoor Datacentre Core 96 Port Switch	
DS-6630R-B-EP	DS-6630R-B 96P/96P 32GB RTF ENT SWITCH
BRSFP16G10KLW	BRCD LBL 16GB 10KM LONG WAVE SFP
INTCABPWRCD-B	C14-TO-C13 1M INTERNAL CAB POWER CORDS-B
W-PS-HW-001	PROSUPPORT W/NBD-HARDWARE WARRANTY
M-PSM-HW-E-002	PROSUPPORT W/MISSION CRITICAL-HARDWARE
WU-PSM-HW-001	PROSUPPORT W/MISSION CRITICAL-HW WARRANT
M-PSM-SW-E-002	PROSUPPORT W/MISSION CRITICAL-SOFTWARE
PS-BAS-FCIA	FC INFRA ASSESSMENT
DS-6630B-ENT	DS-6630B ENTERPRISE SW BUNDLE=MA
Standard Indoor Datacentre Core 48 Port Switch	
DS-6620R-B-24	DS-6620R-B 48P/48P 32GB RTF 24SPF ENT SWITCH
BRSFP16G10KLW	BRCD LBL 16GB 10KM LONG WAVE SFP
INTCABPWRCD-B	C14-TO-C13 1M INTERNAL CAB POWER CORDS-B

PID	PID Description
W-PS-HW-001	PROSUPPORT W/NBD-HARDWARE WARRANTY
M-PSM-HW-E-002	*PROSUPPORT W/MISSION CRITICAL-HARDWARE*
WU-PSM-HW-001	PROSUPPORT W/MISSION CRITICAL-HW WARRANT
M-PSM-SW-E-002	PROSUPPORT W/MISSION CRITICAL-SOFTWARE
PS-BAS-FCIA	FC INFRA ASSESSMENT
DS-6620B-ENT	DS-6620B ENTERPRISE SW BUNDLE=MA

Table 6 –Storage Switch specs

3.6.4 SAN Storage

SAN storage forms an integral part of the ACSA infrastructure. The SAN devices are mostly used for the storage of data for Standalone servers. Virtual servers store data in the virtualised SAN as part of the HCI infrastructure; however, in certain cases, External storage is required.

Whether centralised or decentralised, each storage array conforms to the highest levels of **Redundancy and Availability**. Dual Service Processors, Redundant Disk Arrays with spanned raid groups, Dual Power Supplies for each component, Multiple Connectivity Modules and types per processor with 2 or 4 grouped Fibre Uplinks, ensure that downtime is kept to a minimum if not eliminated at all. This includes processes of hardware or even system code upgrades.

3.6.4.1 Storage Array Specifications

All Storage Array, Hyper-Converged devices are to be covered by a minimum 5-year extended OEM warranty and Dell EMC ProSupport Plus with 4-Hour Mission Critical On-site Response or for out-of-radius devices.

PID	PID Description
Standard Datacentre Shared Storage Array	
40U-RK-DRLKAF	UNITY AFA RACK W/DOOR LOCK
40U-PWR-IECAF	CAB POWER CORD IEC309
D32BD32AD25AF	UNITY 450F 2U DPE 25X2.5 DRIVE EMC RK
D3SL16FAF	UNITY 2X4 PORT 16G FC IO
D3F-2SFXL2-15360	UNITY AFA 15.36TB SSD 25X2.5
D3TX-TWAX-1MAF	1M ACTIVE TWINAX CABLE QTY 4
M-PSM-HWE-005	PROSUPPORT W/MISSION CRITICAL-HARDWARE
458-002-525	UNITY AFA BASE SOFTWARE+ D@RE=IC
M-PSM-SWE-005	PROSUPPORT W/MISSION CRITICAL-SOFTWARE
456-112-850	SRM UNITY 450F=IC
RP-LNX-GPL	RECOVERPOINT LINUX GPLV3 DISTRIBUTION
458-001-574	RP ADV REM FOR UNITY 400F/450F =IC
458-001-573	RP ADV LOC FOR UNITY 400F/450F =IC
M-PSM-SW-D3-001	PROSUPPORT W/MISSION CRITICAL-SOFTWARE
Standard Datacentre Video Security Storage Array	

PID	PID Description
VSS16K-EMCKIT12	VSS1600 INSTALL KIT FOR 12 DRIVE DPE
VNX16K-B12	VNXE1600 ;2XSP DPE;12X3.5, NO SFP, TWIN
VNX16K-DAE-12	2U DAE WITH 12 X 3.5 INCH DRIVE SLOTS
V5-SP-L9X4TB-NL	VNXE1600 3.5 SYSTEM PACK 9X 4TB NLSAS
VNX16K-PWR-13	2 C13 PWRCRD W/ BS546 PLUGS 250V 10A
V5-PS07-040	VNXE1600 4TB NL SAS 12X3.5
VNX16K-16GSFP	16GB SFP QTY 4 FOR FC CONNECTION
W-BASHW-001	BASIC HARDWARE WARRANTY
WU-PS-HWE-003	PROSUPPORT W/NBD HARDWARE WARRANTY UPG
M-PS-HWE-003	PROSUPPORT W/NBD HARDWARE SUPPORT
VNX16K-UNI	BUNDLED FAST CACHE AND REPLICATION=IC
M-PS-SWE-003	PROSUPPORT W/NBD SOFTWARE SUPPORT
458-000-974	VNXE1600 BASE SW+OE DUAL SP ECOSYS =IC

Table 7 – Backup device specs

3.7 LAN Network (Routers and Switches)

The ACSA network infrastructure is made up of Cisco Systems and Huawei networking devices, which have become the standard throughout all sites. Switching infrastructure is broken down into **Access, Distribution/Aggregation** and **Core** (Data Centre).

ACSA currently uses two network infrastructure topologies: **Three-tier** and **Two-tier** hierarchical **Network** models.

Three-tier (Three-layer) - consists of three layers: The **Core layer**, the **Distribution layer**, and the **Access layer**. Three-Layer network model is the preferred approach to network design particularly for large campuses/sites such **ORTIA**, **CTIA**, **KSIA**.

Two-tier (Two-layer)/Collapsed core - consists of two layers: The **Collapsed/Core layer**, and the **Access layer**. The two-layer network model is the preferred approach to network design, particularly for small campuses/sites such **PLZ, ELS, GRJ, BFN, KIM** and **UTN**.

A **"collapsed core"** is when the distribution layer and core layer functions are implemented by a single device. The primary motivation for the collapsed core design is reducing network cost, while maintaining most of the benefits of the three-tier hierarchical model.

The infrastructure to have a high level of redundancy built into the design, leveraging on technologies such as **HSRP, Port Channels**, **Switch Stacking**, **Power Stacking**, **Redundant Power Supplies**, **Dual Fibre Uplinks** and so on.

On the Access layer, ACSA makes use of 24 Port and 48 Port 10/100/1000 POE+ stackable switches with 8-port SPF+ network modules in most standard indoor wiring Centres. The access

stacks link to the distribution switch stacks via dual 1 GB or preferably 10 GB SFP+ single mode fibre uplinks.

Due to increasing rack space restrictions, ACSA may recommend consolidating all 24 port switches and only 48-port switches to be installed in existing wire centres. Depending on the location, wired density and purpose of new wire centres, ACSA will consider the use of 24-port access switches in new/green facilities and only on approval by the relevant structures.
In outdoor or low-density and perimeter standalone wire centres where there might be no cooling and no real growth is expected, the use of 12 Port 10/100/1000 POE+ switches with dual 1 GB fibre uplinks to the distribution switches is permitted.

In certain locations ACSA only allows the installation of intrinsically safe and ruggedized industrial Ethernet switches. This is common in electrical substations, pumping stations, fuel points and air bridges.

NOTE: All configuration of network devices will be supplied by ACSA IT. No service provider is to configure any network device independently

3.7.1 Current Hardware standards (LAN)

Device Type	Manufacturers
MPLS Core routers	Cisco Systems
Data Centre Switches	Cisco Systems / Huawei
LAN Access Switches	Cisco Systems and Huawei
Industrial Ethernet Switches	Cisco Systems and Rockwell Stratix
Data Centre Facilities	Rittal
LAN Management Systems	Cisco Systems
Wireless Access Points	Cisco Systems
Wireless LAN controllers	Cisco Systems
Wi-Fi Management system	Cisco Systems
Telephones – IP and Analogue	Cisco Systems
Voice Recorders	Datavoice Libra, NICE VoIP Logger
Voice Gateways	Cisco Systems
Voice Billing System	PhonexOne, Adapt IT
IP Telephony Management system	Cisco Systems
UCCX Dashboard	2Ring display dashboard
Reporting, Monitoring and inventory management	Variphy Insight, Cisco Prime

Device Type	Manufacturers
In-Path Steelhead Appliances	Riverbed
Internal Firewall	Check Point
Perimeter Firewall	Cisco Systems
DDOS Protector	Check Point
ISE Appliance	Cisco Systems
Web Security Appliances	Cisco Systems
Security Management Appliance	Cisco Systems

Table 8 – Network OEM standards

3.7.2 Network Switches Specifications

Network (LAN)	
Core and Distribution Switches	Cisco Catalyst 9500 Series Switches **(Core devices for regional airports and smaller campus domains)** Cisco Catalyst 9600 Series Switches **(Core devices for large campus domains)** Cisco Catalyst 9300X Series Switches **(Distribution devices for campus sub-domains)**
Access Switches	Cisco Catalyst 9200 and 9200L Series Switches **(Smaller and outdoor wire centres)** Cisco Catalyst 9300 Series Switches **(High density Wire Centres)** Cisco Catalyst 9300UX Series Switches **(High density WI-FI 6 Wire Centres)**
Network ports	Must be Gigabit capable with PoE+ (30 Watt Power over Ethernet) Must be Multi-Gigabit capable with UPoE for WIFI 6 deployments
Data Centre Switches	Cisco Nexus 9300 Series Switches
Industrial Ethernet Switches	Cisco IE3300 Series Switches or latest equivalent Cisco IE3400 Heavy Duty Series or latest equivalent
Wireless LAN Controller	Cisco C9800-40 High Availability – Large sites Cisco C9800-L High Availability – Large sites
Wireless Access Point:	Cisco C9105-AXI – Low density Cisco CW9164i - Medium Density Cisco C9136i -High Density Cisco C9124AXI- Outdoor
Wireless Control System	Cisco Prime Infrastructure

Table 9 – LAN device specs

3.7.3 Network WAN Switches and Devices

Network (WAN)	
Distribution Routers (Large Campuses)	Cisco 7600 Series/6500 Series or latest equivalent

Network (WAN)	
WAN Optimization: Controller and Traffic Analyzer	Riverbed SteelCentral Controller or latest equivalent Riverbed SteelCentral NetEexpress or latest equivalent
WAN Optimization: Appliances	Riverbed Steelhead CX 5070, CX 3070, CX 770 Series or latest equivalent

Table 10 – WAN device specs

3.7.4 Network Cable Specifications

Network (Cabling)	
<100M @ 100MBs	CAT7 plus Patch Lead 1.5m or latest equivalent
<100M @ 1000MBs	CAT7 plus Patch Lead 1.5m or latest equivalent
<412m	Fibre (Multimode)
<2km	Fibre (Multimode)
<20km	Fibre (Single Mode)
>1.5m and <30m	LC-LC Fibre Patch Lead LC-SC Fibre Patch Lead LC-ST Fibre Patch Lead SC-SC Fibre Patch Lead SC-ST Fibre Patch Lead ST-ST Fibre Patch Lead

Table 11 – Network cable specs

3.7.5 Protocols Standards

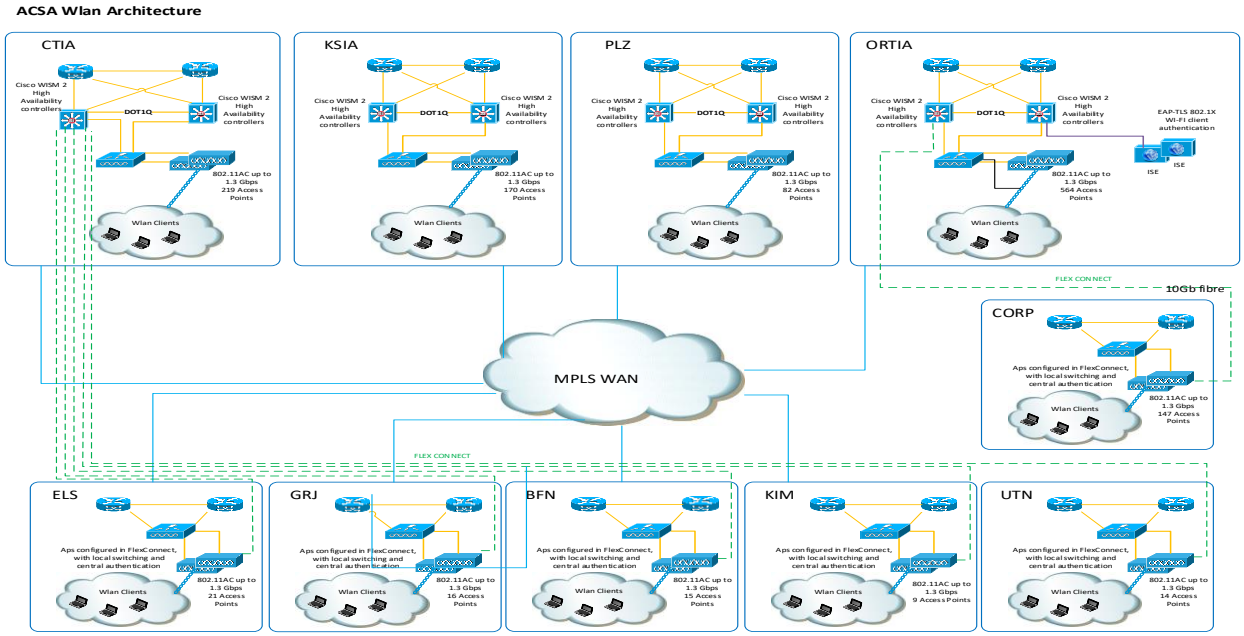
The following standard protocols are deployed at ACSA.

Protocols	
Application Protocol	Transmission Control Protocol/Internet Protocol (TCP/IP), SSH, IPsec, SSL/TLS
Database Protocol	Transmission Control Protocol/Internet Protocol (TCP/IP)
Data link Protocol	Border Gateway Protocol **(BGP),** Routing Information Protocol (RIP), Open Short Path First **(OSPF),** Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System to Intermediate System **(IS-IS**) and Multiprotocol Label Switching **(MPLS)**
Wireless Protocol	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k,802.11n, 802.11r,802.11u, 802.11w, 802.11ac, 802.11ax
Wired/Switching/Routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T. 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q Tagging, and IEEE 802.1AX Link Aggregation.
Storage connectivity protocols	Fibre Channel over Ethernet (FCoE) FCoE Initialization Protocol (FIB)
System Protocol	SNMP v3.x, RFC 3411 or latest equivalent
Network Protocols	TCP/IPv4, UDP, IPSec, SSLv3 or latest equivalent
Authentication protocol	LDAPS, Kerberos, SSH, NTLM v2.x, EAP-TLS, TACACS+ or latest equivalent
Remote Access protocol	TLS 1.x, VPN Protocol: IPSEC, VPN (UDP/TCP modes)
All servers should have Gig connectivity, preferably 10 Gigs per connection for interface Fibre	

Table 12 – Network protocols

3.8 Wireless LAN

The ACSA Wireless Architecture is based on Cisco's Unified Wireless Network. ACSA uses Cisco Wireless LAN controllers at each of the Major International Airports as a standard. Wireless LAN controllers are responsible for system-wide WLAN functions, such as security policies, intrusion prevention, RF management, quality of service **(QoS),** and mobility. Only Cisco Lightweight Access points, **(LAPs)** are used in the environment and are configured and managed centrally on the WLAN Controllers at the bigger airports. These Airports use locally switched Access Points, and the remaining Airports uses **Flex-Connect Technology** mode Access Points, which is locally switched and centrally managed.



Access Points are chosen based on the environmental conditions. All environments with high number of clients must support a **High-Density AP Configuration**. The different models used are shown below, as well as the Outdoor access Points. All installations must be planned and approved by the ACSA IT Change Management Framework. In certain cases, device licenses will be required if the AP counts increase on the WLAN controllers. The same will apply to Cisco Prime Infrastructure device licenses. These will have to be supplied with the Access Points if there is insufficient capacity to support the additional infrastructure.

Access Points have different power requirements, and part of the ACSA requirements is to ensure that if the power requirements to supply full power to the Access Point are not met by the switch that the AP has to have its own power supply, either by a **Power Injector**, **Power Adapter**, or **AC Power** cord. The specifications of these devices are shown below.

3.8.1 Access Points and WLAN Controllers Specification

All Access Points are to be covered by minimum 5-years extended OEM warrantee and either 24x7 Cisco Partner Support Services or Cisco SmartNet Support.

Wireless Access Point:	Cisco C9105-AXI – Low density
	Cisco CW9164i - Medium Density
	Cisco C9136i -High Density
	Cisco C9124AXI- Outdoor

Table 13 – WLAN Devices

Wireless LAN Controller	Cisco C9800-40 High Availability – Large sites Cisco C9800-L High Availability – Large sites
Wireless Control System	Cisco Prime Infrastructure

Table 14 – WLAN controllers

3.9 Firewall

Firewall	
Firewall	Checkpoint 6600, 5400, 7000 Security Gateway Appliance Cisco Perimeter FW's and Checkpoint DDOS
Firewall Management	Checkpoint Smart-1 600 M Security management Sender or latest equivalent specification
ORTIA Perimeter (Data Centre Firewall)	Cisco ASA 5545X HA or latest equivalent specification DDoS Protector or to latest equivalent specification Cisco Identity Service Engine (ISE) or latest equivalent specification
Firewall Software and Functionality	Security Management – Monitoring Blade (MNTR) Mobile access Blade, User Directory Blade, Endpoint Security Secure access package, IPv6 capability, Anti bot, Identity Awareness, IPS, URL Filtering, Application Control, Site to Site VPN

Table 15 – Firewalls

3.10 Physical infrastructure and Data Centres

3.10.1 Categorisation and Rating

IT facilities are categorised into 3 types depending on functionality

	1 - WIRE CENTRE	2 - CORE CENTRE	3 - DATA CENTRE
	Wire Centre / Fibre Distribution Centres	**Core Equipment**	**Primary Data Centre / Disaster Recovery Centre OR Secondary Data Centres**
Note	Low Heat Generating Equipment	High Heat Generating equipment	High-heat-generating equipment
Function	Copper Distribution	Data Distribution/ Copper Distribution	Data Distribution
Function	Fibre Distribution	Fibre Distribution/ WC backbone distribution	Data Processing
Function	End User connectivity	End User connectivity	Data Storage
Function			Disaster Recovery
TIA ref	Floor Distributer	Building Distributer	Campus Distributer
Cables	Cat7 SFTP Cables	Cat7 SFTP Cables	Cat7 SFTP Cables
Cables	RF Cable	RF Cable	

	1 - WIRE CENTRE	2 - CORE CENTRE	3 - DATA CENTRE
Cables	Co Axial Cables	Co Axial Cables	
Cables	Fiber Cables	Fiber Cables	Fiber Cables
Network	Access layer switches	Access layer switches	Access layer switches
Network		Distribution Layer	Distribution layer
Network		Core Layer	Core Layer
Network			Routers
Network			Firewalls
Servers			Blade Enclosures
Servers			Rack Mount Servers
Servers			
Storage			SAN
Storage			Backups
Storage			DR
Radio	RF Boosters	Repeaters	
Radio	Base Stations	Base Stations	
Equipment	Fiber / Copper Distribution/panels	Fibre / Copper Distribution/panels	Fibre / Copper Distribution/panels
Equipment	CCTV: field/end components	CCTV: field/end components	
Equipment	Access Control: field/end components	Access Control: field / end components	
Equipment		Audio/Visual: field/end components.	
Equipment		Parking systems: field/end components	
Equipment		Telecoms: Analogue Gateways	
Equipment		National Radio system field end devices	
Equipment	Fire Systems: field/end components	Fire Systems: field/end components	Fire Systems: field/end components
Equipment	BMS: field/end components / Sensors / Door contacts		BMS Server : field / end components / Sensors / Door contacts
Equipment		PABX	

3.10.2 **IT Facility Ratings**

Rooms are rated into 8 types, focusing on the availability and expectation of the infrastructure

	Availability	Recommended for Room Category	Room Function	Hosted System Description	Location
A	99.999%	DATA CENTRE	Disaster Recovery Centres. Primary Data Centres and Secondary Data Centres	Business Critical Systems. Core Network Devices. Backups. Storage. Primary Virtual hosting. Independent server hosting. Data Recovery systems.	Secured Facility on Landside
B	99.98%	CORE CENTRE	Regional Core Rooms Functions as a Campus Distribution	Campus Distribution Business Critical Systems. Core and Distribution Devices. Cute / Baggage / Comms	Secured Facility inside the terminal building
C	99.67%	WIRE CENTRE	Data Distribution Centres	Access Devices. Data Distribution to end devices	Secured Facility inside the terminal building
D	99.67%	WIRE CENTRE	Data Distribution Centres	Access Devices. Data Distribution to	Landside OUTDOOR – Outside the terminal buildings Inside Parade Areas (MSP)

The above ratings are guided by the TIA942 & the Uptime Institute standards for physical infrastructure, but not confined to all specifications, as it is suited to and defined by ACSA. Availability considers maintenance schedules.

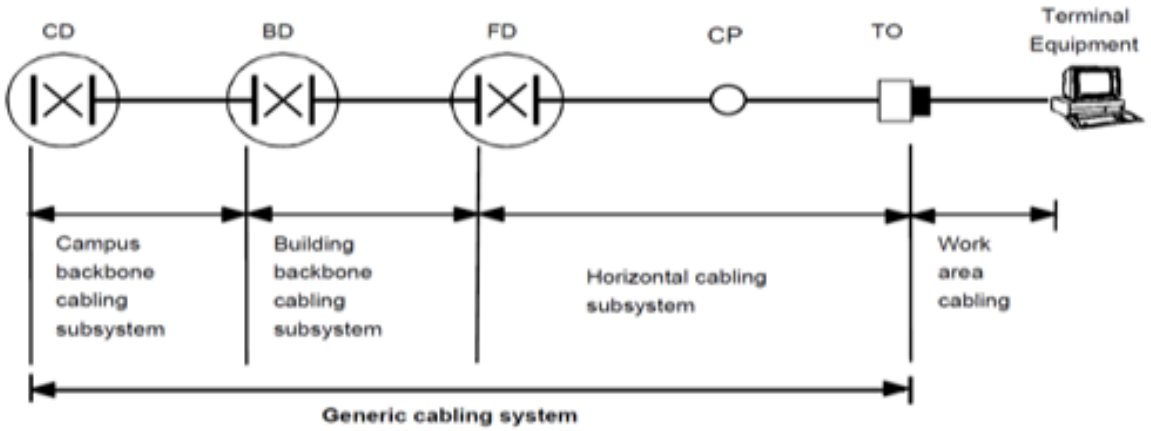
3.10.3 Cabling Standards

3.10.3.1 Network Cabling Schema

The functional elements of generic cabling are as follows:

- campus distributor (CD)
- campus backbone cable
- building distributor (BD)
- building backbone cable

- floor distributor (FD)
- horizontal cable
- consolidation point (CP)
- consolidation point cable (CP cable)
- multi-user telecommunications outlet (MUTO)
- telecommunications outlet (TO)

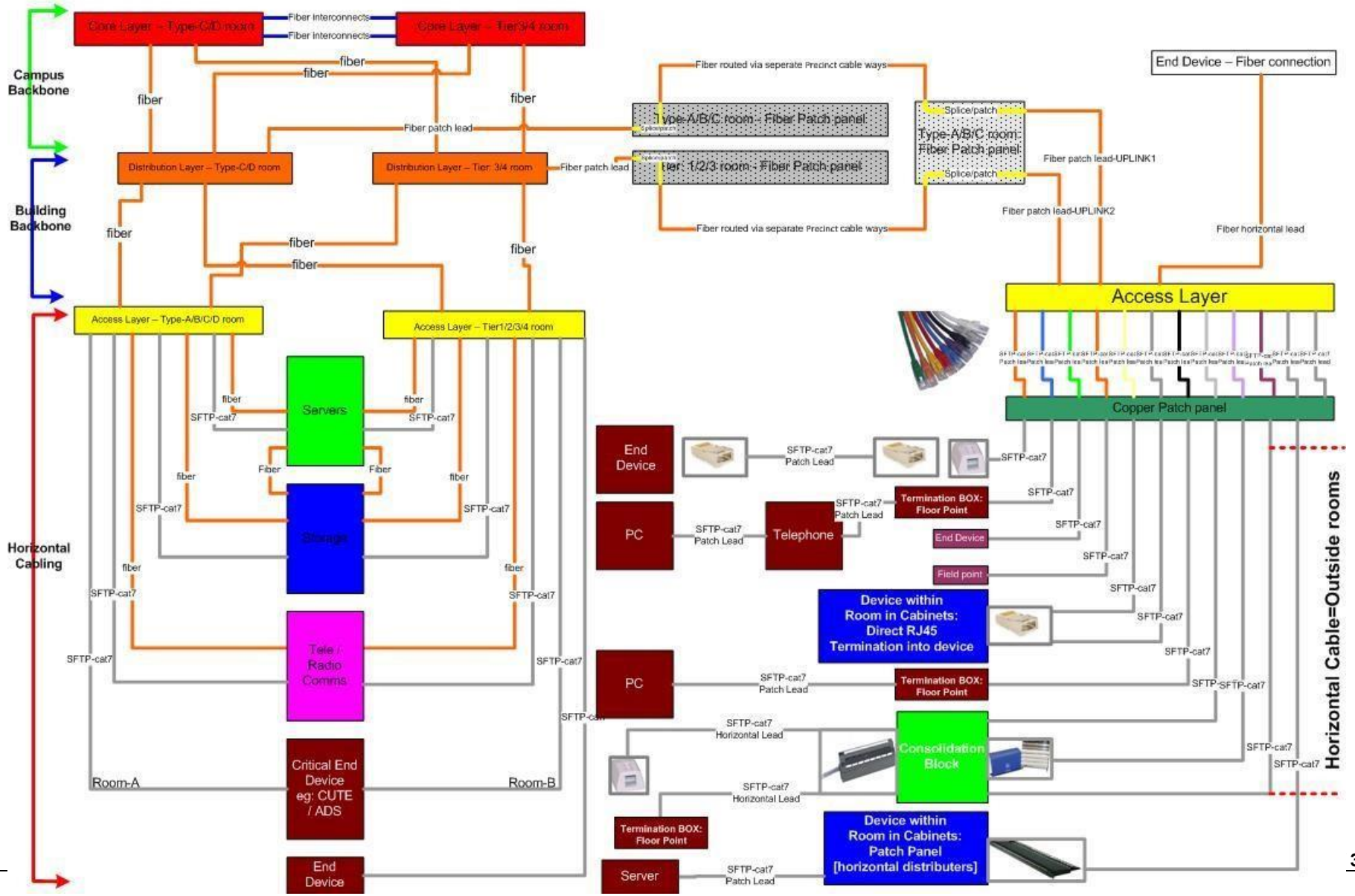


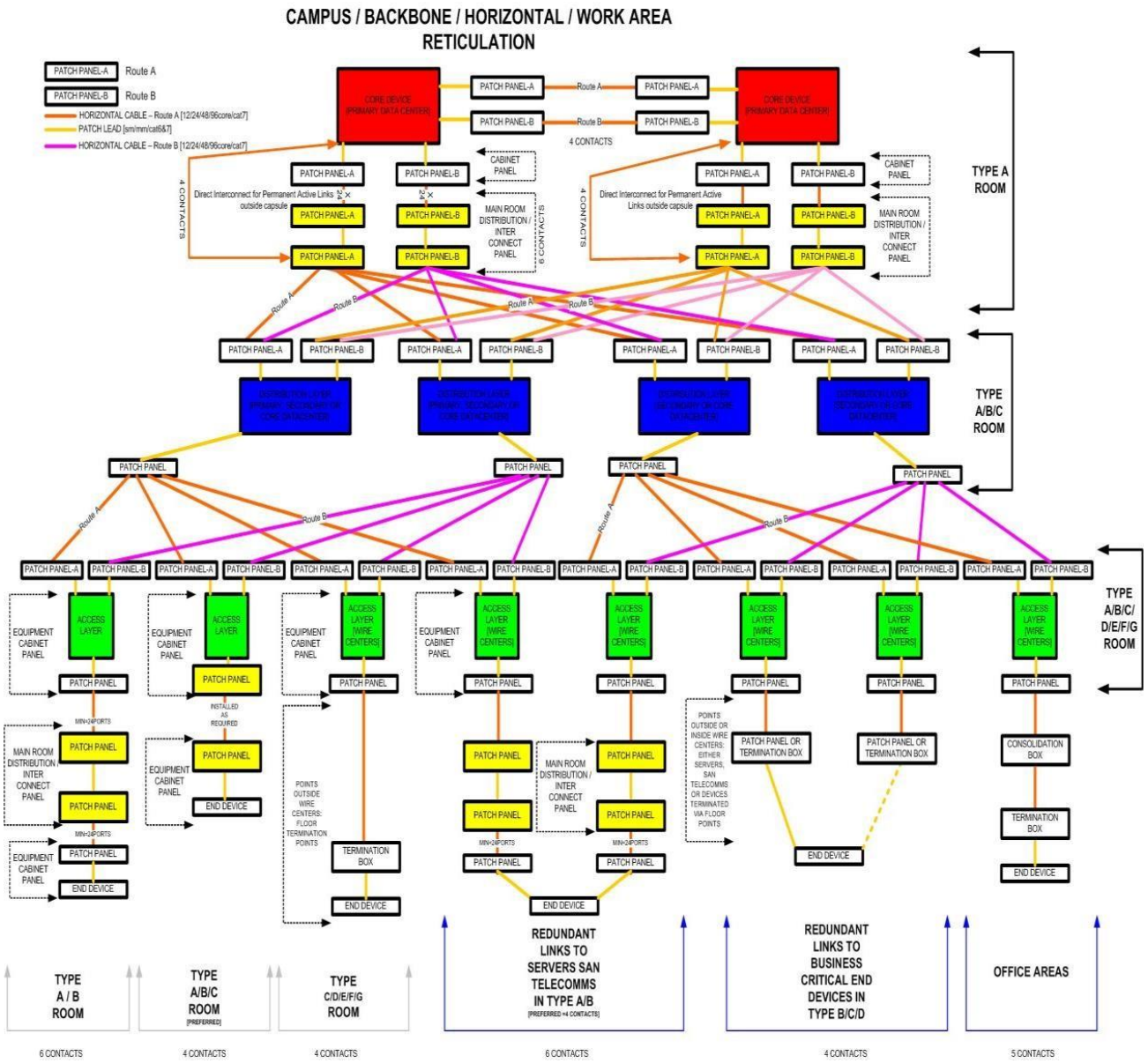
***Consolidation points:** Shall only contain passive connecting hardware and shall not be used for cross-connections. A consolidation point should be located in accessible locations [but not to the public]. The consolidation point shall be located so that there is at least 15 m from it to the outlet.

***The main distribution area (MDA)** is the central space where the point of distribution for the structured cabling system in the data centre is located. The data centre shall have at least one main distribution area. The core routers and core switches for the data centre networks are often located in or near the main distribution area.

***The horizontal distribution area (HDA)** is the space that supports cabling to the equipment distribution areas. The LAN, SAN, console, and KVM switches that support the end equipment are also typically located in the horizontal distribution area.

Network Cabling Schema




CAMPUS / BACKBONE / HORIZONTAL / WORK AREA RETICULATION
PATCH PANEL-A
Route A
PATCH PANEL-B
Route B
HORIZONTAL CABLE – Route A [12/24/48/96core/cat7]
PATCH LEAD [sm/mm/cat6&7]
HORIZONTAL CABLE – Route B [12/24/48/96core/cat7]
CORE DEVICE (PRIMARY DATA CENTER)
4 CONTACTS
CABINET PANEL
MAIN ROOM DISTRIBUTION / INTER CONNECT PANEL
6 CONTACTS
Direct Interconnect for Permanent Active Links outside capsule
TYPE A ROOM
TYPE A/B/C ROOM
PATCH PANEL
ACCESS LAYER (WIRE CENTERS)
EQUIPMENT CABINET PANEL
INSTALLED AS REQUIRED
END DEVICE
TERMINATION BOX
POINTS OUTSIDE WIRE CENTERS: FLOOR TERMINATION POINTS
PATCH PANEL OR TERMINATION BOX
CONSOLIDATION BOX
TYPE A/B/C/ D/E/F/G ROOM
TYPE A / B ROOM
TYPE A/B/C ROOM [PREFERRED]
TYPE C/D/E/F/G ROOM
REDUNDANT LINKS TO SERVERS SAN TELECOMMS IN TYPE A/B [PREFERRED =4 CONTACTS]
REDUNDANT LINKS TO BUSINESS CRITICAL END DEVICES IN TYPE B/C/D
OFFICE AREAS
6 CONTACTS
4 CONTACTS
4 CONTACTS
6 CONTACTS
4 CONTACTS
5 CONTACTS

3.10.3.2 **Fibre Cabling**

- Covering Sheath Colour: ORANGE
- Flame retardant cables or Low smoke zero halogen protective outer casing.
- Installations to adhere to TIA/EIA568-B standards.
- UPC connectors are deployed in transport systems designed for digital signal transport, while APC connectors are preferred for RF video signal transport.
- For systems such as RF video and high fibre sensitivity applications, the APC connector is preferred because these particular systems are extremely sensitive to any back reflections from connectors within the network.
- Number of patches to be kept to a minimum at all times.
- Max number of connection points per permanent link on campus backbone[core – core]: 4
    - [core device→patch cable→patch panel→horizontal cable→patch panel→patch cable→distribution device].
- Max number of connections points per permanent link on campus backbone[core - distribution]: 4
    - [core device→patch cable→patch panel→horizontal cable→patch panel→patch cable→distribution device].
    - [core device→patch cable→patch panel→horizontal cable→patch panel→patch lead →patch panel →horizontal cable→patch panel→patch cable→distribution device].
- Max number of connections points per permanent link on building backbone[distribution – access – end device]: 6
    - [core device→patch cable→patch panel→horizontal cable→patch panel□patch lead →patch panel →horizontal cable→patch panel→patch cable□distribution device].
- Max number of splices/joints on a channel link before replacement: 3 [subject to confirmation of db loss on cable]
- Standard campus backbone/building backbone / horizontal cabling: Optical Single mode 2 (OS2) Orange Sleeve.
- Patch Leads: OS2 Yellow and Optical Multimode 4 (OM4) Purple and Aqua Blue only [less impurities in core].
- Indoor fibre must have warning labels every 15m along its route and at every cable entry and exit point.
- Outdoor fibre must have warning labels every 15m along its route and at visible points (i.e. Manhole & Junction box, cable entry and exit point) along its route.
- As a minimum standard, all campus distribution layers, the cabling must be as per the below Fibre Spec:

    Indoor Blown Fibre Standard:

    - Option A = 12 core single mode
    - Option B = 24 core single mode
    - Option C = 48 core single mode
    - Option D = 96 core single mode
    - Option E = 192 core single mode
- Standard duct size and Colour Orange:
    - Option A = 4 way Micro-duct

  - Option B = 7 way Micro-duct
  - Option C = 12 way Micro-duct

- As a minimum standard, all conventional fibre cores from distribution lay to the end point termination cabinet the cabling must be as per the below Fibre Spec:
  - Option A = 12 core single mode
  - Option B = 24-core single-mode
  - Option C = 48-core single-mode
  - Option D = 96-core single-mode
  - Option E = 192 core single mode
- Long runs indoor: Single Mode=9 micron core. Cladding diameter = 125um. Min supported length=5000m @1G / 10G
- Devices within a room: Multi mode = +50 micron core [OM4]. Multi-mode = 62.5 micron core [OM1]. Cladding diameter = 125um.
- Max 300m distance @10g. Orange jackets =OM1/OM2. Aqua Jackets=OM3/OM4.
- Open trenching: heavy-duty duct construction, cable and armoured cable required. Inner ducts [rodent-free] must be used for all fibre in open trenching. Use 3 x 32mm inner ducts hosted in a 110mm PVC duct [capable of carrying 3x96core cables].
- Covering Sheath: UV-resistant. High impact resistant. Flame retardant. Water resistant, rodent-free.
- Usage at Roadway crossings – 110mm Corrugated PVC Rodent-free.
  - Minimum of 250 depth and covered with concrete.
- Ceramic tip connectors, UV curable, <3Db loss with load on fibre axial. Ip44.
- Fibre-inter connections or distribution units: Preferably 40-degree angled connection panels (stress relief on bend). 24-port patch panels.
- Dust covers or dust caps for unused slots
- Operating temp: -40degrees to 70degrees
- Test docs: continuity and maintenance of polarity, length, propagation delay, optical attenuation of link (2 wave lengths/2 directions) using light source and power meters. Test to be performed at 10G ratings. Test results must be recorded by power meter and not handwritten [FLUKE
- meter required]. Using ODF's. (Fibre Frame)
- Return loss max: - 45db
- No incomplete splicing in Manholes where restriction of closing runways may affect works.
- Use bend control accessories during installation: min bend radius = 20 X cable diameter
- With Long run fibre Tank Dome Joints are required to be used.
- Dome Joints need to be fixed with a bracket/s inside Manholes.

3.10.3.3 Fiber Splicing And Termination

3.10.3.3.1 Indoor Fibre Requirements

- Arc fusion splicing.
- Splice loss = <0.03db.
- Loss per 200m = <0.07db.
- 30mm sheath visible past the end of the entry gland for the fibre patch panel.
- 925mm of removed outer sheath coiled in clockwise direction on spool.
- 300mm slack before the entry gland to allow the removal of the fibre panel.
- Pigtails to be wrapped counter clockwise.
- All splices must be covered by splice protection sleeves.

- Buffer lengths are per cable manufacturers' specifications.
- Fibres must be organised into a fibre splice chip by colours or numbers for future amendments. Chip cover to be labelled appropriately.
- Splicing done within a proof / external particle-free environment.
- All fibre joints to be enclosed within water-tight / air–tight housing. Housing to have durable labels.
- Sufficient slack in every manhole – mounted coil boxes at each manhole to coil up slack cabling.
- All ports to be cleaned by Isopropyl alcohol.
- Dome joint junction boxes are required for ring networks and outdoor usage. Fully updated documentation/legends per patch station.
- Termination boxes in office spaces: LC 6 port termination boxes. IP66 rated +-200mmX200mmX30mm
- Plug and play 12port termination LC OEM-4 units only acceptable. Rack mountable.

3.10.3.3.2 **Outdoor Fibre Requirements**

- No Through Splices at individual WC's or Termination Points
- Direct Splicing required on 2 separate Fibre panels (Route A & B)

3.10.3.4 **Copper Cabling (Cat7** ORANGE **SOLID CABLE)**

- Colour: Orange for horizontal runs within Type A/B/C rooms.
- Colour: Orange for patch leads.
- Within Type A rooms = Cat7 S-Ftp LSZH 10G 750MHZ
- Within Type B rooms = Cat7 S-Ftp LSZH 10G 750MHZ
- Within Type C rooms = Cat7 S-Ftp LSZH 10G 750MHZ
- Between Servers, Storage and network device uplinks to the network = Cat7 S-Ftp LSZH 10G 750MHz
- Horizontal Cables = Cat7-SFTP LSZH = Supportive of 10 000mb/s (10G)@>750MHz
- Current revision date – June 2011. Next revision – Jan 2014
- Meet or exceed ISO/IEC 11801 Cat6a or Cat7 component requirements.
- CAT7-SFTP = 4 pair-23 American Wire Gauge (AWG) copper cable wires, 100 ohms, shielded twisted pairs, RJ45 connectors. Foiled twisted Pairs – each pair enclosed in laminated aluminium foil, minimising crosstalk. Outer braiding minimises alien cross-talk.
- Cable properties to ensure maximum resistance against electromagnetic interference and alien crosstalk
- LSZH - Low smoke. Zero halogen cable properties. FRNC- Flame-retardant and non-corrosive cable properties.
- Max cable diameter: less than 7.5mm
- Outdoor Cabling must have UV protection and IP66-rated connections and junction points.
- Operating temperatures: -20degrees to + 60degrees
- Use conduit/trunking if exposed to sunlight or higher than 50-degree temperatures. Use conduit/trunking for all outdoor applications.
- Max number of connections between access layer switch and end device from a wire centre: 4
    - [switch→patch lead→patch panel→horizontal cable→termination box→patch lead→device].
- Max number of connections between access layer switch and end device within a secondary data center or core centre: 4
    - [switch→patch lead→patch panel→horizontal cable→patch panel→patch lead→device].

- Max number of connections between access layer switch and end device within a primary data centre: 6
    - [switch→patch lead→patch panel→horizontal cable→patch panel→horizontal cable→patch panel→horizontal cable→patch panel→patch lead→device].
- Max single copper run (between patch panel and termination box): 90m
- Max patch lead length for workspaces: 10m
- Max total distance for copper run = 100m, including patch and fly leads.
- Each cable run from the patch panel to the floor connectors must be continuous with no breaks or joints. No joints will be accepted.
- 7-strand patch leads will only be used in workspace areas [no more than 20%db loss on channel performance allowed].
- Solid Conductor patch cables [horizontal cables] to be used as patch leads in data rooms.
- Note: Possible 20% loss on permanent links. -4db =80% loss. 7 strand patch cable=20% dB loss.
- Test docs: wire map/length/attenuation / near-end cross-talk loss on permanent links and not channel links.
- Only “Permanent Link” test results will be accepted
- Avoid interferences like routing around air conditioning units.
- Patch leads loses 20% dB – made up of 7 cables only. Consider using Horizontal cables for patch leads only.
- Link Runner test is only for troubleshooting and to determine the VLAN and the Connection
- FLUKE Copper test results required for new installations and to be submitted with handover/sign-off.

3.10.3.5 **Patching**

- Leads to adhere to latest ANSI/TIA/EIA-569-B standards – with factory fitted 8 pin connectors.
- Each Cabinet will be represented by a patch panel with Primary and Secondary datacentres.
- Every Primary data centre must have a distribution interconnect cabinet. (Passive Cabinet) Dedicated Fibre and Copper Cabinet, e.g. ODF
- Wire Centres will run from the patch panel directly to the switch– single cross connections.
- Copper Patch leads to be factory terminated and distance specific – minimum slack.
- Factory-supplied patch leads to be used only at the work area cabling zones [user end].
- Fibre patch leads to be factory terminated - supplied with distances closest to requirements - min slack.
- Fibre patch runs will be above cabinets – 1st fibre panel will be mounted at the top of the cabinet.
- Patching: Overhead fibre trays for fibre cables between cabinets.
- Copper patch runs will be overhead, if possible, be under cabinets – 1st copper panel will be at the bottom of the cabinet.
- Should fibre and copper be in the same cabinet – Fibre panels will be mounted first from top, and the first copper panel will be mounted from bottom up.
- All cables to be patched downwards into brush panels below in wall mount cabinets and outdoor cabinets only.
- Labels on the patch panel to be visible as per labelling standards.
- Looms/ bundles of 24 to start from the patch panel. Jacket removal point to be kept to a minimum - not to compromise cable integrity. Jackets to remain up to connecting block – twists to remain up to connecting points [0mm untwist].
- Patch connectors to be positioned correctly into patch panels without any stress on the cable or additional twists– no forcing connectors to place.

- Cable bending not exceeding 35mm radius in fibre and 65mm in copper. 10 x outer diameter for fibre.
- Strain relief boot clips must be used

3.10.3.6 Patch Panels And Consolidation Points

- Copper: 24 port panels. Shielded patch panels where applicable.
- Fiber: 24-port panels. Environment temperature: -40~+80° C. Insulated Resistance: ≥ 21χ 0MΩ /500V (DC). Fibre bending radius: ≥ 40mm
- Consolidation points: 8 / 16 / 24 blocks installed along cable route FOR OFFICE SPACES ONLY [horizontal cabling outside the room].
- Every consolidation block will have a unique number per site. Used for office spaces where 1 point for every 4m2.
- Horizontal Distribution Points: In a room, they must be centrally located between active equipment, allowing patch leads to be connected.
- 1rack unit (1U) rack-mounted patch panels.19-inch wide. > 1,000 repeated wire insertions without incurring permanent deformations.
- Fibre: Interchangeable adapter plates - LC adapter only.
- Copper: RJ45 patch panels. CAT 7 shielded sockets. Gold-plated contact elements.
- Cables to be routed from patch panels in bundles of 24.
- Panels to be mounted >150mm from the front door of the cabinet.
- Adequate label space above for each port
- Patch cables loop below/downwards from the patch panel into the brush panels
- Colour: Black Patch panels
- To be earthed. Gold contacts.
- Entry Glands/support guiders on the rear left and rear right sides of panels.
- Fibre panels will be above copper panels if in the same cabinets.
- Type-A Room: Passive Cabinets – shielded copper patch panels. Separate copper and separate fibre distribution cabinets.
- Type-B Room: Passive Cabinets – shielded copper patch panels. Separate copper and separate fibre distribution cabinets.
- Type-C Room: Active and Passive Cabinets - shielded copper patch panels where applicable if STP cables are used

3.10.3.7 Floor / Terminations Boxes / Plugs Or End Point Connections

Indoor Cabling Installations

- Offices: dual port recessed panels fixed against floor trunking [RJ45]. Blanking panels for unused ports.
- Ceilings/areas with no trunking: single port surface mount boxes [RJ45].
- Gold-plated contact elements.
- Shielded keystones where applicable – compulsory where SFTP cables are required.
- Termination Panels [1U patch panel – to be located centrally to active equipment requiring copper connectivity] required if devices are in the same wire centre as the access switch.

Outdoor Cabling Installations

- IP66-rated interchangeable keystones and connection joints for outdoor points.
- IP66 IP66-rated junction boxes to house Wall boxes and Keystones.
- All Wall boxes and Junction boxes to be fixed to permanent structure or pole with a Stainless-Steel Banded Strap to secure.
- All entry and exit points into junction boxes need to be installed facing down, with the holes facing the floor.
- All entry and exit points need to have entry grommets installed.

- Critical system termination points must be enclosed in a secure IP66 IP66-rated PVC box with entry and exit glands via bosal or PVC Piping [CCTV cameras/access control].
- Termination Panels [1U patch panel – to be located centrally to active equipment requiring copper connectivity] required if devices are in the same wire centre as the access switch.
- All Outdoor equipment and cabinets need to be properly earthed.

3.10.3.8 **Brush Panels [All Rooms]**

- To BE USED ONLY UPON APPROVAL IN Type E / F / G /H FACILITIES ONLY.
- To be located below patch panels and switches.
- Colour: White or black.
- 1.5mm thick metal framework.
- 1U height.
- 341mm x 21.5mm opening for brushes.
- 4 x mounting holes per panel.

3.10.3.9 **Cable Management, Routing And Trenching**

- Max bend - Fibre patch leads: 25mm
- Max bend – Co Axial leads: 50.5mm radius[Rj11]
- Max bend – Co Axial leads: 33 mm radius[Rj16]
- Max bend – Copper looms: 100mm radius
- Max bend – Fiber cased covered: 150mm radius
- Copper loom of 24 = 40mm diameter.
- PVC Conduit or Sprague for single cable: 25mm
- Trench Sleeve: >110mm (Material to be used, Dependent on Requirement).
- Distance for data cables from shielded electrical cables [greater than 5Kva] = 300mm.
- Distance for data cables from unshielded electrical cables [greater than 5Kva] = 600mm.
- Each U-space to be separately maintained/managed vertically and horizontally in the cabinet through the cable routing cycle.
- Velcro cable ties on all routes. No Plastic Cable ties. No glue guns/staples. Risks are too high when cutting cable ties locked around a cable. Only Velcro strips are allowed to be used in the Data Centre and Disaster Recovery Centre
- Velcro to be installed at every 500mm inside Wire Centres and Core Rooms. Velcro at every 3000mm in cable ways. Both must be finger tight.
- Avoid slack in cabinets. If required, then do not exceed 3m / 4 coils and maintain max bends.
- Cable bundles not to exceed 24 cables per bundle or loom.
- Cable managers in cabinets must NOT EXCEED HEIGHT OF patch panel: e.g. 1rack unit patch panel = 1 rack unit of a plastic cable manager. The cabinet cable manager must be plastic.
- Cables to be locked in place within a room and outside a room using Velcro.
- Cable routing to be guided as per building design, preliminary investigations and discretion of ACSA tender-approved/certified / qualified cabling teams.
- Shortest distance for routing must always be investigated, and capacity planning along routes must be considered.
- Preferred [Stainless Steel Bollard] Figure 10 – Figure 12.
- Sleeves: min diameter - 110mm to accommodate capacity planning as per cable tray / cable duct distribution routing diagrams.
- PVC sleeves [Concrete sleeves]: Rodent Free, UV resistant, weatherproof, accidental damage protection and self-draining.
- Min trench depth: 0.5m. Min trench width: 200mm (ensure safe distance between services). Special Requirements require formal approval from the Client.

- Avoid interferences like routing around air conditioning units.
- Prior to any trenching, a full investigation of the route must be provided to stakeholders – to ensure that no services will be disrupted during trenching.
- Cabinet Cable Manager
    - A: 43U spacer (2x45mm=90mm wide, 12x45mm=540mm depth) o Cabinet Cable Manager
    - B: 42U spacer (2x45mm=90mm wide, 10x45mm=450mm depth) Cabinet Cable Manager
    - C: 20U spacer (2x45mm=90mm wide, 5x45mm=225mm depth) o Cabinet Cable Manager D: 16U spacer (2x45mm=90mm wide,

3.10.3.10 **Maintenance holes:**

- Min: 1000mmx1000mm wide.
- Min: 50mm exposed sleeves.
- Min: 400mm sleeve height entry
- Double brick construction hole facility. Preferably: Concrete.
- Lockable Metal (Preferably: high-density Plastic) manhole cover
- Maintenance holes to be sealed with bitumen inside and outside
- To be bag-washed with Cement slush before backfilling.
- Mounted coil boxes – hot galvanised dipped.
- Sleeve installations first, then bricking.
- Preferably: Ladder facility into the manhole
- Available at each site: Water Pump to remove water in manholes.
- External water seal to be above the regional water table.

3.10.3.11 **Cable Trays / Cable Ducts And Flooring**

- Suspended Ceilings / overhead fibre management trays made up of shatterproof lightweight plastic / PVC, maintaining a 50mm max bend radius.
- Overhead fibre management trays should be made up of lightweight Metal Material.
- Self-extinguishing or non-flammable. 100mm above cabinets – 100mm above the highest cabinet, maintained if cabinet heights vary.
- Cable bends in trays and ducts > 110degrees bend radius.
- Hot-dipped galvanised before fabrication. Zinc is electroplated after fabrication. Wire-mesh cable trays for exterior and corrosive environmental applications. Non-water retention. Welded at intersections – 50 x 50mm grid patterns. U-shaped with equal height side walls.
- All cable trays must be earthed.
- Supports attached to ceilings, walls or floors. Punched hole pattern that accepts tray attachment hardware. Steel supports.
- Cable Tray
    - Cable Tray SPEC1: width=100mm. height=40mm. support weight per 1000mm=40kgx2 o
    - Cable Tray SPEC2: width=200mm. height=45mm. support weight per 1000mm=60kgx2 o
    - Cable Tray SPEC3: width=300mm. height=50mm. support weight per 1000mm=80kgx2
    - Cable Tray SPEC4: width=400mm. height=60mm. support weight per 1000mm=100kgx2
    - Cable Tray SPEC5: width=600mm. height=60mm. support weight per 1000mm=120kgx2
- 3-layered ceiling suspended cabled tray systems preferred. (Power, Fibre, UTP). Formal approval required from the Client in special circumstances.

- All suspended ceilings / mounted or floor cable trays must allow for multi layered installations – first installation must start at lowest layer. (Power, Fibre, UTP). Formal approval required from the Client in special circumstances.
- Horizontal cable tray separations [data tray parallel to electrical] preferred over multi-layered tray systems in raised floors to minimise resistance and maximise air flow.
- All suspension nuts (if applicable) must be installed above the lowest layer to accommodate future cable tray installations above the lowest layer.
- Multi-layered cabled trays: min distance between trays = 60mm allowing air flow.
- Bend radius = width of cable tray (width of larger cable tray if two are interlinked).
- Max stacked height of cables in a cable tray: 120%
- Minimum height above ground for floor trays: 60mm for air flow
- Min distance from ceiling for ceiling suspended trays: 60mm
- Suspension bars: 1000mm apart. Dual support beams. Adjustable with butterfly lockable nuts (ceiling and floor trays for multi-tray installations and height adjustments). Wall L-shape brackets where applicable.
- Data Cable Trays: Preferred Overhead / under cabinets possible.
- Electrical Cable Trays: Rear of cabinets Overhead
- Incoming routes to be located furthest from air con locations – preferably the centre of rooms
- Cross-connect cable trays [trays linking rows] should run centrally through the room at an equal distance between cabinets.
- Min dist. bet electrical cables and copper data/telecoms cables: 300mm.
- Radio frequency transmission cables to be separated at a distance of 600mm from data cables.
- Radio frequency transmission cables to be separated at 300mm away from electrical cables
- Conduits in offices - preferably located on solid walls opposite doors/entrances - away from feet when seated. Data with voice to be separated from power. Separate conduits for power and data. (P801)
- No Cabling on ceiling tiles - ensure cables run through a conduit or cable tray to the termination point/end device.
- Copper cables must run in looms or bundles of 24 in cable trays.
- No sharp edging – Grommets and polishing required where applicable.
- Cable trays should not exceed 60% for the first installation for certification.
- Sleeves: min diameter- 110mm to accommodate capacity planning.
- Flexible PVC sleeves [Preferably: Concrete sleeves]: Rodent Free, UV resistant, weatherproof, accidental damage protection and self-draining.
- Min trench depth: 0.5m. Min trench width: 200mm (ensure safe distance between services). Special Requirements require formal approval from the Client.

3.10.3.12 Cabinet Specifications

- **Type-A Room:** External height=+-2200mm (with castors) External width=600mm. Internal height= 42U high / +-2000mm. 600mm x 1070mm. Support weight: 1400kg.
- **Type-B Room**: External height=+-2210mm (with castors) External width=800mm. Internal height= 42U high / +-2000mm. 600mm x 1070mm. Support weight: 1200kg.
- Type-C Room: External height=+-2200mm (with castors) External width=600mm. Internal height= 42U high / +-2000mm. 600mm x 1070mm. Support weight: 1400kg.
- **Type-D Room:** Indoor Environmental Cabinet - External height=+-1985mm (with castors) External width=600mm. Internal height=42U/42U high / +-1866mm. 600mm x 1070mm. Support weight: 1400kg.
- **Outdoor IP66 Rated Cabinet** – External height (Including Canopy) = 1400mm External Width = 1800mm Depth = 998,45mm / Internal Height = 25U Internal Width = 1200mm / Bottom Plinth Height – 200mm Support Weight = 850kg

3.11 Systems Integration

3.11.1 Enterprise Service Bus

ACSA has deployed the IBM Enterprise Service Bus (ESB) for system integration. The ESB architecture is designed to facilitate seamless communication between various IT systems, including but not limited to airport management solutions, sort allocation computers (SOC), fuel networks, emigration gates (E-gates), flight information through a mobile application, baggage reconciliation systems (BRS), hotel flight information, etc., within airport operations. IBM's ESB solutions provide a robust framework for integrating services and applications, enabling them to interact in a flexible, scalable, and reliable manner.

Some of the key features provided by this EBS include:

- **Interoperability:** Supports a wide range of communication protocols and data formats, ensuring compatibility across diverse systems.
- **Scalability:** Easily scalable to accommodate growing data volumes and transaction loads.
- **Reliability:** High availability and fault-tolerant mechanisms to ensure uninterrupted operations.
- **Security:** Comprehensive security features including encryption, authentication, and authorisation to protect data integrity and confidentiality.

3.11.1.1 Software Layer

Software integration within the ACSA ESB system leverages IBM's middleware solutions, primarily IBM MQ and IBM Integration Bus (IIB), also known as IBM App Connect Enterprise.
IBM MQ:

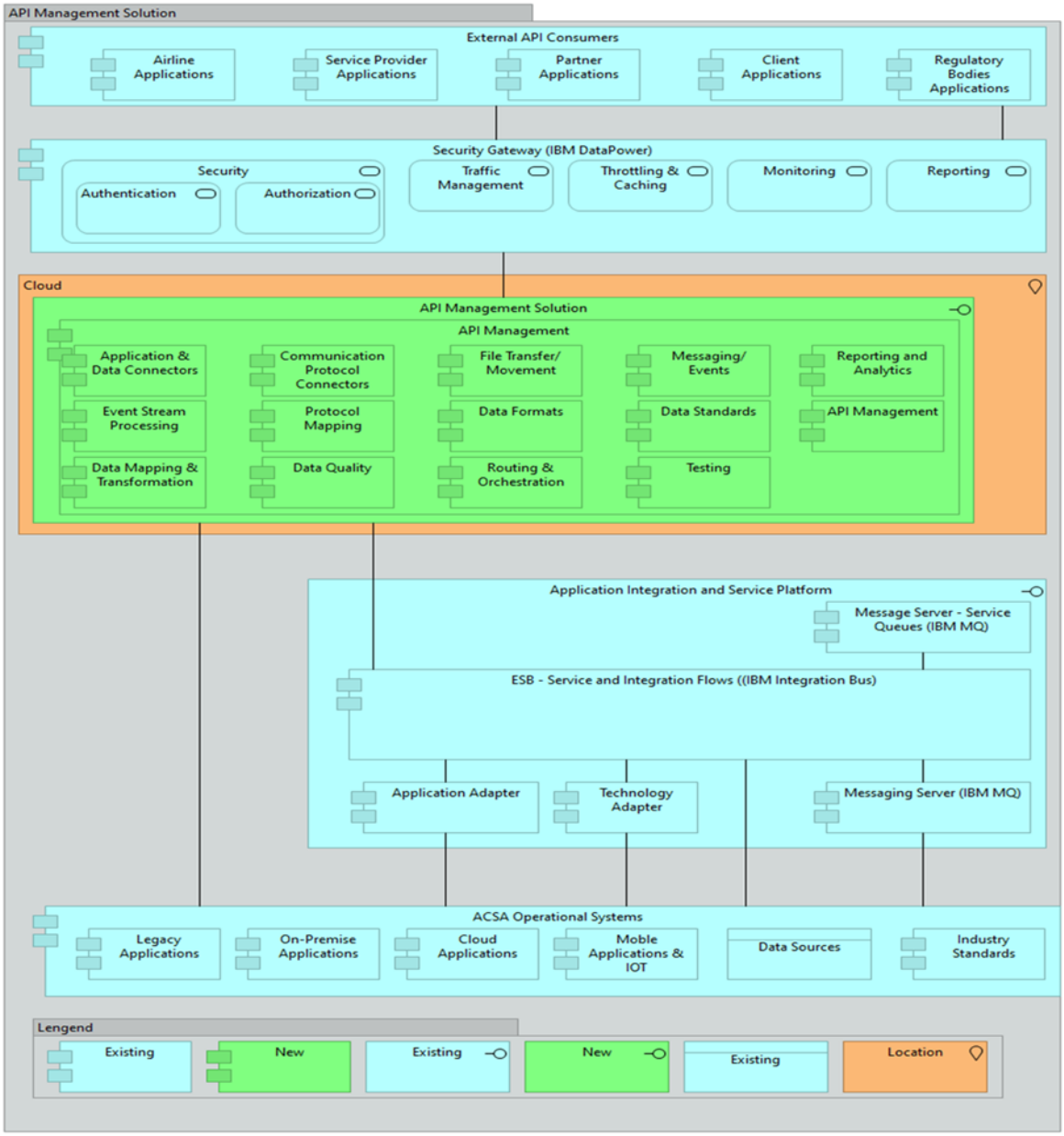
- **Messaging Backbone:** Acts as a messaging backbone for data exchange between applications, ensuring message delivery, reliability, and security.
- **Decoupling:** Decouples applications to allow them to communicate asynchronously, improving system flexibility and resilience.
- **Transaction Management:** Supports complex transaction management and ensures data consistency across distributed systems.
- **Routing and Mediation:** Routes messages based on content and business rules and mediates between different services.
- **Service Orchestration:** Orchestrates composite services by coordinating interactions between multiple applications and services.

3.11.1.2 Data Transmission

Data transmission within the ESB is managed through IBM MQ and IBM Integration Bus, which provide reliable and secure message delivery mechanisms. The following data transmission mechanisms are configured:

- **Message Queues:** IBM MQ uses message queues to store messages until they can be safely delivered to the receiving application. This ensures reliable data transmission even in the event of network or application failures.
- **Message Brokers:** IBM Integration Bus acts as a message broker that processes, routes, and transforms messages as they pass through the ESB. This allows for efficient data exchange and integration across different systems.
- **Real-time Processing:** Supports real-time data processing to meet the needs of time-sensitive applications and services.

The table below depicts an IBM EBS high-level integration architecture in our environment.



3.11.2 Quickwork API

ACSA is in the process of implementing the Quickworks API management platform to enable the creation, deployment, and management of APIs in a secure and scalable environment. This platform will sit on top of the IBM ESB to enhance the integration capabilities with additional layers of API management, automation, and analytics. Quickwork provides a unified platform for API lifecycle management, including the creation of API collections and endpoints, faster deployment, better security, and comprehensive monitoring. This architecture will support the efficient management of complex workflows and ensure high levels of service availability and security across all integration points.

3.11.2.1 Guidelines and Compliance

To ensure that our systems remain secure, reliable, and interoperable with other technologies and services, all service providers must strictly adhere to the following sections that guide the IT architecture for integration at ACSA.

A. Design and Development

- **API Design:** all API designs must follow RESTful principles, ensuring stateless communication, and use standard HTTP methods (GET, POST, PUT, DELETE).
- **Versioning:** the service provider must ensure that they implement version control for APIs to manage changes and maintain backward compatibility.
- **Documentation:** the service provider must provide comprehensive API documentation using standardised formats such as OpenAPI/Swagger.
- **MQ and Message Broker:** the service provider should use IBM MQ and Message Broker for reliable message queuing and data integration.
- **Service-Oriented Architecture (SOA):** the service provider must implement SOA principles for modular and reusable services.

B. Security

- **Authentication:** authentication should use secured API keys, OAuth, and other token-based authentication mechanisms.
- **Authorisation:** the service providers should implement role-based access control (RBAC) and least privilege principles.
- **Encryption:** the service provider should ensure all data in transit is encrypted using the latest TLS.
- **Logging:** the service provider should maintain detailed logs of API requests and responses for audit and troubleshooting purposes.

C. Compliance and Governance

- **Integration standards:** The service provider should ensure all API activities comply with relevant international standards (ISO/IEC 27001, IEEE 1471) and local regulations (e.g., POPIA for data protection).

3.12 Service Management (Service Desk)

The ACSA IT Service Desk utilises the ITIL framework and serves as the first line of support for users experiencing issues or requesting IT services. Acting as a central point of contact, the service desk resolves issues, fulfils requests, and ensures the smooth operation of technology within the organisation. Key responsibilities include:

- **Incident Reporting and Escalation:** The ACSA IT Service Desk documents all user interactions, tracking trends in reported issues, and escalating complex problems to higher-level IT support (internal or external) when needed.

- **Fulfilling Service Requests:** The ACSA IT Service Desk handles requests for new software installations, hardware replacements, access permissions, and other IT-related needs.

- **IT Change Management:** All required changes follow the ACSA IT Change Process. Changes are requested and implemented by internal or external parties.

- **Communication and Customer Service:** The ACSA IT Service Desk effectively communicates with users from diverse technical backgrounds, clearly explaining solutions, and keeping users updated on the progress of their issues and requests.

To fulfil these responsibilities, the ACSA IT Service Desk monitors tickets logged and assigned to third-party Service Providers (SPs). Achieving SLA targets and minimising

breaches requires collaboration among all parties. The following aspects support this collaboration:

- **Ticketing Systems:** The ACSA IT Service Desk utilises an ITSM tool (ServiceNow) for ticket logging. Any Service Provider contracted to ACSA IT is required to integrate into the ITSM tool using the REST API Explorer method. These details on how to set up the integration are found on the following URL

  https://docs.servicenow.com/bundle/vancouver-api-reference/page/integrate/inbound-rest/task/t_GetStartedAccessExplorer.html

  This integration allows for seamless information flow, where incidents can be routed to the appropriate technician (internal IT or SP) based on the issue. It also creates a central repository for tracking issue resolution and maintaining communication history.

- **Clearly Defined Roles and Responsibilities:** A documented Service Level Agreement (SLA) outlines the specific services provided by the SP, communication protocols for issue escalation, and response time expectations.

- **Troubleshooting and Problem-Solving:** IT service desk agents diagnose and resolve a wide range of user issues at the first level, from fixing printer problems to resetting passwords to tackling software glitches. The contract defines the roles and responsibilities, specifying the extent of first-level troubleshooting within the Service Desk.

- **Knowledge Management:** The ACSA IT Service Desk maintains a knowledge base or self-service portal containing solutions to common issues and guides for users to troubleshoot problems themselves. Sharing a centralised knowledge base is highly beneficial, with the SP contributing solutions to common issues they handle, and the Service Desk leveraging this information to assist users or direct them to self-service solutions.

- **Regular Communication:** Maintaining open communication channels is essential. This involves scheduled meetings, dedicated communication channels, or utilizing features within the ticketing system for updates and discussions.

Overall, the ACSA IT Service Desk plays a vital role in keeping an organisation's technology running smoothly and ensuring a positive user experience. They are the first line of defence for user issues and the bridge between users and the broader IT department and its Service Providers.