

	University of the Witwatersrand, Johannesburg
	Wits ICT Networking and Security
Wits ICT Standards Document	

Table of Contents

1. Introduction.....	3
1.1. Background.....	3
1.2. Applicable Standards.....	3
2. Cabling.....	3
3. Cabinets.....	6
4. Uninterruptable Power Supply (UPS).....	7
5. Pathways.....	7
6. Redundant Infrastructure.....	9
7. Wits Cisco Networking and Security Equipment.....	9
8. Wits Equipment Installation Standards.....	10
9. Wits Equipment Configuration Standards.....	10
10. Document Sign-Off.....	15

1. Introduction

1.1. Background

The purpose of the document is to establish Wits ICT installation standards in regards to network related infrastructure installation and configuration. Resulting in guaranteed maintainability, reliability, availability, security and scalability of the Wits University overall network.

1.2. Applicable Standards

1.2.1.Applicable Standards for Infrastructure Build as per CommScope installations specifications

ISO/IEC 11801 Edition 2:2002: ICTI UTP and STP Category 5e, 6 and 7, Transmission performance and fiber cable and connectors

SABS 0142 and SANS 10142-1-:2003: Power Reticulation

SANS 1200 and Telkom Specifications 325R; Civil Works

ANSI/TIA/EIA-559-B: Commercial Building Standards for Telecommunication Pathways and Spaces

ANSI J-STD-607-A: Commercial Building grounding (earthing) and bonding requirements for telecommunications, 2002

ANSI/TIA/EIA-758: Customer owned outside plant telecommunications ICTI standard, 1999

1.2.2.Applicable Standards for Wits Networking and Security Equipment

2. Cabling

2.1. Copper Cabling

2.1.1.Cat6 UTP cabling should be the minimum standard used when new cabling is installed

2.1.2.UTP cabling should comply to CommScope specifications

2.1.3.Original Equipment Manufacturers (OEM) specifications must be adhered to

2.1.4.A standard 3 meter fly lead on user side and a 1 meter patch lead to be supplied with all new point installation, with exceptional requests for different lengths

2.1.5.1 meter patch lead to connect both indoor and outdoor Wireless Access Points

2.1.6.New installations to be done with metallic flush mount terminating outlets. Cables must be enclosed in metal power skating reserved for data cabling and not directly under the power skating.

2.1.7.In areas where is not possible to install flush mounts, a surface mount termination will be used with appropriate trunking for example PVC trunking

2.1.8.Cables inside ceiling must be run in a mesh tray and should overlap on fluorescent light

2.1.9.Termination boxes should not be mounted with adhesives

2.1.10. Only horizontal permanent link will be accepted

2.2. Fiber Optic Cabling

2.2.1.Fiber installed between buildings must be the blown fiber optic type inside 3.5/5mm tubes, configured from 2-way to 24 way tubes

2.2.2.Fiber installed between cabinets in a building could be conventional or blown fiber

2.2.3.When a distance is less than 300m an OM3 fiber will preferably be installed

2.2.4. With a distance between 300m to 500m an OM4 fiber will preferably be installed

2.2.5.With a distance over 500m a single mode fiber must be installed

2.2.6.All fiber cabling on public roads shall comply the appropriate Telecommunications Act

2.2.7.All fibers that are outsides of network cabinets shall be covered with rugged conduits as protection

- 2.2.8. Both core switches cabinet at SMH and CLM each feeds 12 core fiber links to all 8 distribution cabinets
- 2.2.9. Two distribution cabinets will feed a 12 core fiber each to one mini distribution cabinet
- 2.2.10. All redundant links mentioned on point 2.2.8 and 2.2.9 are on separate fiber cables and are on separate routes
- 2.2.11. The distribution and mini distribution cabinets will feed all access cabinets with a single fiber link
- 2.2.12. Where there is a mini distribution cabinet, all access cabinets in the same vicinity will connect to it with a single fiber link from a 12 core cable
- 2.2.13. Minimum number of fibers cores to be should be 12 cores per cable. All new fibers installations must cater for at least one spare fiber pair per cable
- 2.2.14. In buildings where mini distribution or distribution cabinets doesn't reside in the same buildings as access cabinets, for instance Chris Hani Bara Academic Hospital and Rahima Moosa Hospital The minimum fiber feed to destination building must be 6 pairs in the building. So the fiber will be distributed to one cabinet in the denomination of 12/24/48 or 96 core cable, subsequently, all other building cabinets will feed from it. Fibers will be patched through or spliced through from same cabinet to others in same building to establish connectivity to the distribution/mini distribution.
- 2.2.15. A 5m new fiber cable slack should be allowed at both termination points for future re-splicing.
- 2.2.16. Fiber extensions using mid-couplers is forbidden.
- 2.2.17. Fiber patch leads must be factory assembled certified and terminated as per manufactures standards
- 2.2.18. Both single mode and multimode fibers leads must be duplex from patch panel to the equipment and the length should adhere to required standards
- 2.2.19. LC to LC fiber connectors are current standard, if other types of connectors are required for relevant equipment will be used.
- 2.2.20. Indoor backbone fiber optic cables must have a minimum bend of radius of 10 times the cable outside diameter when under no strain and 15 times the cables outside diameter when pulled
- 2.2.21. The optic fiber cable must be terminated in 19" rack mountable LC 24-way fiber splicing termination tray which shall be LISA metallic splice tray.
- 2.2.22. The fiber cable must be spliced onto unjacketed pigtailed connected to duplex LC mid couplers. The splice tray should always be populated from the left to (for 12 core fibers the first three positions of the top and bottom row should be used, with position 1 being the left top mid-coupler and position 2 the left bottom mid-coupler)
- 2.2.23. The splice tray must always house sufficient splice organizers and all splices must be protected with splice protectors
- 2.2.24. To always adhere to minimum bending radii when routing fibers in the terminating drawers
- 2.2.25. All ends in a cable must be terminated at both ends
- 2.3. Cabling Testing
 - 2.3.1. Copper Cabling to be tested with an approved CommScope tester as follows
 - 2.3.1.1. Cat6 – ISO/IEC11801 – Class E – Permanent Link – NVP: 69%
 - 2.3.1.2. Test results reports must comply with CommScope specifications
 - 2.3.1.3. All tests to be saved with the correct labelling convention that correspond with the data point labels and shall be saved on the tester as follow: Building Name, Outlet Number.
 - 2.3.2. Optic fiber cabling each fiber core must be tested with an OTDR from both sites. Multi-mode cable to be tested at 850nm and single mode cable at 1310nm
 - Maximum connector pair loss must not exceed 0,75dB
 - Maximum connector loss shall not exceed 0,5dB

- Maximum splice loss must not exceed 0,3dB

Test results reports should at minimum include the following information

General Information

- Filename
- Cable ID
- Test Date
- Test Time
- Fiber ID
- Company Name of Splicers
- Customer Name

Location

- Location A & B
- Operator A & B
- Machine Model
- Serial Number
- Calibration Date

Results Field

- MM – supports 850 nm wavelength as per EIE/TIA 568 standard
- SM - supports 1310 nm wavelength as per EIE/TIA 568 standard
- DB Loss
- Length
- Span Loss
- Span ORL (Optical Return Loss)
- Average Loss
- Average Splice Loss
- Maximum Splice Loss

2.4. Earthing and Bonding

- 2.4.1. All materials which form part of earthing and bonding must conform to SANS 10142-1:2003
- 2.4.2. All earthing cabling must be routed into the cabinet
- 2.4.3. All network cabinets must be earthed with a 4mm² flexible insulated copper conductor to the earth bar or ground bar of the power distributions board and a crimped lug must be fitted at the other end for connection to the cabinet. The lug must be fasten to the cabinet with a bolt and nut.

2.5. Electromagnetic Interference (EMI)

- 2.5.1. In order to decrease EMI susceptibility the implementers must
 - 2.5.1.1. Use metal conduit for electrical power circuits and all electrical circuits must be fully enclosed in with solid wall metal conduit
 - 2.5.1.2. Use solid metal conduit for telecommunications circuits and telecommunications circuits should not be installed into conduit containing electrical cables.
- 2.5.2. Isolated grounding circuits mustn't be used unless equipment manufacturers mandates it
- 2.5.3. Adequate physical distance should be maintained between electrical noise sources and susceptible telecommunications circuits or equipment
- 2.5.4. Surge protective devices should be used to reduce transients that emanates from inductive devices that are switched off. Locate external surge protection devices as close as possible to the source of transients.
- 2.5.5. Avoid telecommunication circuits from running in close proximity of any florescent light
- 2.5.6. Grounded conduits and enclosures should be used

- 2.5.7. Maintain a distance of at least 1 meter from electrical power transformers
- 2.5.8. Minimize proximity to radiating antennae and towers
- 2.5.9. Provide common bonding of the grounding point of multiple surge protection devices placed on both the electrical power and signal circuits of the telecommunications unit
- 2.5.10. Use well balanced twisted-pair copper cable
- 2.5.11. Always assume that electrical noise exists in the proximity of any electrical equipment
- 2.5.12. Certificate of Compliance (COC) must be issued for all the dedicated power installed

3. Cabinets

- 3.1. Floor standing cabinets should be more than 800mm deep to be able to accommodate all appropriate equipment. Actual specifications are 600mm x 1000mm for all cabinets
- 3.2. All network cabinets should have a front and side access doors and panels respectively
- 3.3. Front door should be perforated and lockable with keys, embedded fans are optional and will be installed depending on ventilation ability of the hosting room or space
- 3.4. All cabinets should allow all-inclusive 15% future growth
- 3.5. Free standing cabinets will preferably be located in a position where at least two doors can open entirely, except where cabinets are placed alongside to each other. Cabinets should stand securely on the ground and be level and stable
- 3.6. Wall mounted cabinets will only be installed if there are no other options available in a building and must be approved by building manager
- 3.7. Free Standing 47U, 43U and 42U cabinets specifications
 - 3.7.1. 600mm x 1000mm cabinets with perforated and lockable front and rear doors, 4x uprights, 4x screw on feet or plinth and gland plates, Where solid doors would be required due to special circumstances then cabinet should have fans
 - 3.7.2. Removable and lockable side panels
 - 3.7.3. At least 1x vertical side mount cable tray of minimum 150 wide
 - 3.7.4. At least 1x 10-Way C13 IEC PDU to be connected to the UPS, where the UPS is not mounted inside cabinet or the power socket on the UPS is not sufficient

3.8. Free standing 25U cabinet specifications

- 3.8.1. 600mm x 1000mm cabinets with perforated and lockable front and rear doors, 4x uprights, 4x screw on feet or plinth and gland plates, Where solid doors would be required due to special circumstances then cabinet should have fans
- 3.8.2. Removable and lockable side panels
- 3.8.3. At least 1x vertical side mount cable tray of minimum 150 wide
- 3.8.4. At least 1x 6-Way C13 IEC PDU to be connected to the UPS, where the UPS is not mounted inside cabinet or the power socket on the UPS is not sufficient

3.9. Wall mount 16U and wall mount 12U cabinets specifications

- 3.9.1. 550mmx700mm solid wall mount cabinet with perforated front door and 4x uprights and swing frame not allowed
- 3.9.2. Removable and lockable side panels
- 3.9.3. At least 1x Vertical side mount cable tray (minimum 150mm wide)
- 3.9.4. At least 1x 6-Way C13 IEC PDU to be connected to the UPS, where the UPS is not mounted inside cabinet or the power socket on the UPS is not sufficient
- 3.9.5. The cabinets must be mounted at least 2m above finished floor or as high as the ceiling allows
- 3.9.6. The cabinet must be fitted level on solid walls with minimum 4x M8 Rawl bolts
- 3.9.7. Cabinets will absolutely not be fitted to a temporary structures such as dry walls
- 3.9.8. Cabinet shall be mounted in such a position to allow access to at least the front and one side of the cabinet
- 3.9.9. UPS shall preferably not be installed inside the cabinets however where necessary the UPS will be installed inside with a maximum of 1x battery pack.

4. Uninterruptable Power Supply (UPS)

- 4.1. An suitable UPS with sufficient capacity to provide power to all equipment in the cabinet should be installed for each network cabinet and must be able to provide backup power at full load
- 4.2. UPS should be on-line double conversion
- 4.3. The battery power backup time duration required during AC power failure should be 60 minutes at full load
- 4.4. The UPS should be a 19" rack mountable unit and could also be placed outside the cabinet in special cases like insufficient space in the wall mounted cabinets
- 4.5. UPS must have network connectivity module or communication port for UPS monitoring, auto shutdown procedure and UPS battery management
- 4.6. UPS must have at least 5KA/6KV lightning protection
- 4.7. UPS to have pre-warning on key components in case of power supply interruption
- 4.8. The UPS must have a wide input range suitable for poor grid power, range must be equal to or more than 80-280V AC (L-N), 40Hz to 70Hz
- 4.9. The UPS must be ultra-efficient, up to at least 94.5% at full load. Also be efficient at low loads of above 90% at 15% load
- 4.10. All UPS's must comply with the supplier installations standards
- 4.11. All UPS's shall be installed by a qualified technician

5. Pathways

5.1. General

- 5.1.1. In principle horizontal fill ratio for conduit, cable trays and ducts must conform to standards and manufactures recommendations, a maximum of 85% fill after completion should be maintained for all main cable pathways
- 5.1.2. All new cables shall be installed in or on cable pathways at all times
- 5.1.3. When designing horizontal pathways the vendor must consider such pathway's ability to accommodate changes and minimize occupant's disruptions when such pathways are accessed.

5.2. Cabling vendor responsibilities

- 5.2.1. Locate telecommunications pathways away from sources of EMI
- 5.2.2. Consider the aesthetic appearance of the cable pathway within offices and other visible areas
- 5.2.3. Plan outlets to be within 3m from the user workstation or network printer and in close proximity of power outlet

5.3. Ducting

- 5.3.1. Double or single cable tray must be Steel type, single or double, 50mmx75mm x 0.8mm with matching fittings i.e. couplings, corners (90° or diagonal), stoppers and related accessories to be used
- 5.3.2. Metal ducting to be installed in offices for cable routing. Ducting must run against the full length of the wall. Network cable must be placed at the bottom layer of the metal duct. The ducting accessories must be pop riveted or fastened with self-tapping screws. Self-tapping screws must be cut shorter or filed smoother to avoid cabling damage. The ducting colour to be determined by the client and standard colour coding will be recommended. Otherwise the colour must blend with building colours. Where ducting exists the new ducting should match the current ducting colour
- 5.3.3. Ducting must be fastened to permanent structures by means of 6mm Hilti plastic fastener with non-corrosive flat washers and a minimum diameter of 25mm. Fasteners to be placed 1 meter apart and double fastened at end of ducting. Offset of ducting when used in 100mm or more ducting. Methods used can also be discussed during site visits to comply with other buildings specifications in the vicinity. On non-permanent structures like dry walls spring toggles on dry walls and stainless steel bolts and lock nuts on corrugated iron buildings, same washers and spacing's will be used.

- 5.3.4. Grommets/glands must be used for protection of cables that are routed through holes. Cables should be protected from rough and sharp edges by means of rubber grommets or protective material. All burr edges of ducting be neatly filed to protect cabling. Ducting will be routed through walls in a straight line, a section of the lid must be fitted at the points where the ducting is routed through the wall before such a wall is patched and painted. Piece of the lid must protrude 50mm on each side of the wall. Damaged occurring during installations must be repaired to original condition. If damaged cannot be fixed to original condition then an amicable solution will be reached between the installers and Wits University. Block paint to be applied where damaged walls were fixed. Cables should not be visible from the front hence blanks should be fitted in spaces where data terminating socket is not fitted. Where ducting is installed on the roof of a floor with leads facing downwards permanent supporting devices must be supplied to keep wiring in place to prevent the lids from carrying the weight of cables
- 5.4. EGA Trunking
 - 5.4.1. Trunking must be fastened by approved 6mm plastic faster to permanent structures. With spring toggles on dry wall and stainless steel bolts and nuts on corrugated iron buildings. Fasteners to be spaced 1 meter apart
- 5.5. Conduit
 - 5.5.1. Flexible conduit should be in circumstances where it is only the viable option to be used. And the size of the flexible conduit must be increased to over 25mm as per industrial specifications
 - 5.5.2. Conduit runs must be designed to:
 - 5.5.2.1. Installed in the most direct route possible with no more than 90-degree bends
 - 5.5.2.2. Shouldn't have continuous sections that are more than 30 meters. Must be able to withstand the environment which they exposed to
 - 5.5.2.3. If runs are more than 30 meters, draw boxes will be installed at intervals not longer than 30 meters
 - 5.5.2.4. The PVC or metal conduits that are smaller than 25mm in diameter must use matching couplings, adaptors, bends and all related accessories and would conform to environmental factors that prevail in that environment
 - 5.5.2.5. Conduits to be fastened with appropriate saddles, meaning they should be of the correct size, similar material and colour
 - 5.5.2.6. Saddles should be placed 1 meter apart from and must be fastened to permanent structures for example a solid wall using 6mm Hilti plastic fasteners. If there is a dry wall or corrugated iron as non-permanent structure the fastening method used should be spring toggles or stainless steel bolts and lock nuts respectively
 - 5.5.2.7. If the conduit has internal diameter of 50mm or less, the bend radius must be at least 6 times the internal conduit diameter
 - 5.5.2.8. If the conduit has internal diameter of more than 50mm, the bend radius must be at least 10 times the internal conduit diameter
- 5.6. Cable Trays and Baskets
 - 5.6.1. Cable trays and basket must be installed according to manufactures recommendations, it must be in horizontal way rather than vertical posture. Matching internal, external or flat corners should be used when required
 - 5.6.2. At least two supports shall be installed per running length, supports can be suspended from concrete roof by means of threaded rod or steel cable all fastened to the concrete roof with M8 easy-holds
 - 5.6.3. Cable trays and baskets could be mounted on walls by means of cantilever brackets with the correct size, which shall be fastened to permanent structures only with M8 easy-holds
 - 5.6.4. When suspended from the roof a unistrut of correct length should be fastened to the threaded rod with nut and washer on both sides. The basket shall be fastened to the unistrut with a hold-down bracket and spring nut

- 5.6.5. The basket could also be suspended by a steel cable as alternative means that is fed through an eye bolt installed in the concrete roof. Ferrules need to be crimped where the cable attaches to either side of the basket also where the cable goes through the eye bolt thus the basket will not move when it gets populated.
- 5.6.6. Basket to be joint together with appropriate splices
- 5.7. P9000 Trunking
 - 5.7.1. P9000 trunking should not be installed with lids facing down. Must be installed according to manufacturer's recommendations preferably horizontal
 - 5.7.2. Matching accessories such as internal, external and flat corners should be used as per requirements.
 - 5.7.3. Two support accessories should be used per running length, supports can be suspended from a concrete roof by means of treaded rod fastened to the concrete roof with M8 easy holds or mounted on walls by means of cantilever bracket with the correct size. subsequently, fastened to permanent structures only with M8 raw-bolts
 - 5.7.4. When suspended from the roof P9000 bracket must be fastened to the threaded rod with a nut and washer on both sides. P9000 needs to be fastened to the bracket and shall be joint together with appropriate splices
- 5.8. Cable Hangers
 - 5.8.1. Cables inside the ceiling voids can be suspended from the concrete roof with cable hangers or S-hooks
 - 5.8.2. Cable hangers or E-hooks must be spaced 1 meter apart and must be fastened to permanent structures by means of 6mm Hilti plastic fasters
 - 5.8.3. Cables bundles should not contain more than 24 cables and cable-tied each 300mm, cables mustn't be fastened to hangers or S-hooks
- 5.9. Ceiling distribution
 - 5.9.1. Ceiling distribution is acceptable if, it is adequate and suitable, there is space in ceiling for cable pathways, it should only be for horizontal cable feed to the floor below, areas used for cable pathways should be accessible from the floor below and ceiling panels or tiles are removable at a maximum height of 3,4m or access available through a trap door
 - 5.9.2. Hardware such as a 10 way disconnect modules or telecommunication equipment mustn't be installed inside ceiling space.
 - 5.9.3. Ceiling space must: allow 75mm of clear vertical space above conduits, cater for 300mm of clear vertical space above the tray or raceway for overhead ceiling cable tray or raceway system
- 5.10. AP Installations
- 5.11. Network Cabinet Layout
- 6. Redundant Infrastructure**
 - 6.1. Infrastructure
 - 6.1.1. All redundant cables, connection hardware, networking devices and pathways that are no longer in use, must be identified and removed from areas they were connected or installed ultimately removed by service providers
 - 6.1.2. All surfaces where redundant infrastructure were removed must be reinstated to original condition by the service provider
 - 6.2. Cisco Devices
 - 6.2.1. All obsolete and out of service devices should be disposed after new equipment is installed
 - 6.2.2. The service provider responsible should dispose devices as per standing agreement with Wits University
- 7. Wits Networking and Security Equipment**
 - 7.1. Core Switches
 - 7.1.1. Cisco Nexus 9516 chassis and accessories
 - 7.2. Distribution Switches
 - 7.2.1. Nexus9000 C9516 and accessories

- 7.3. Mini Distribution switches
 - 7.3.1. Cisco C3850-24XS and accessories
- 7.4. Data Centre Switches
 - 7.4.1. Cisco Nexus 93128 and accessories
- 7.5. Access Switches
 - 7.5.1. Cisco Catalyst 3650 and 9300
 - 7.5.2. Switches to be scalable and future ready for new technologies i.e. SDN
 - 7.5.3. Cisco small Form-factor Pluggable (SFP) transceivers
 - 7.5.4. Cisco scalable switch power supply's
 - 7.5.5. Cisco data and power stacking cables
- 7.6. Controllers
 - 7.6.1. Cisco 5520 and associated accessories
- 7.7. Access Points
 - 7.7.1. Indoor Access points Cisco AIR-CAP2702I-E-K9 and AIR-AP2802I-E-K9
 - 7.7.2. Outdoor access point Cisco AIR-AP1562E-E-K9
 - 7.7.3. Mounting brackets for indoor APs and key security
 - 7.7.4. Appropriate mounting accessories for outdoor APs and key security
- 7.8. UPS
 - 7.8.1. Vendor should supply UPS management software and configure it for optimal monitoring and power management. Wits ICT will provide a management IP and future monitoring the UPS after commissioning
- 7.9. Firewall
 - 7.9.1. Cisco ASA 5585 firewalls and associated accessories
- 7.10. F5
 - 7.10.1. F5 appliances BIG-IP 10250 and associated accessories
- 7.11. UCS
 - 7.11.1. UCS chassis and associated accessories
- 7.12. Licensing
 - 7.12.1. All Cisco devices must have operating licenses as per agreed terms
 - 7.12.2. All other vendors must provide appropriate licenses for their respective devices

8. Wits Equipment Installation Standards

- 8.1. Cabinets
 - 8.1.1. All equipment installed must be mounted inside network cabinets and should follow the prescribed order, that is: fiber patch panel mounted on the top, followed by copper patch panels, then network devices that are separated by a brush panel, blanking plates where required and UPS control module and battery packs
- 8.2. Equipment installed outside cabinets
 - 8.2.1. Access Points must be mounted on the ceiling with a secure brackets
 - 8.2.2. All outdoor Access Points must be mounted on approved outdoor structures including but not limited to brick walls, concrete walls and approved poles

9. Wits Equipment Configuration Standards

To guide network engineers on how to configure routers, switches, controllers and firewalls as follows

- 9.1. Core switches
 - 9.1.1. Naming convention - **Building Name, Type, Device** an example **SMH-CORE-SW01**
 - 9.1.2. Authentication, Authorization and Accounting (AAA) access must be implemented to control access to the routing switches
 - 9.1.3. Secure Shell (SSH) remote administration protocol should be used to access all routing switches
 - 9.1.4. OSPF routing protocol is the principal protocol used across Wits University's campuses
 - 9.1.5. Port or Ether channeling are configured to aggregate traffic when needed for higher throughput

- 9.1.6. Routing switch consist of chassis, fiber modules and dual power suppliers
- 9.2. Distributions switches
 - 9.2.1.Naming convention - **Building Name, Type, Device** an example **SMH-DIST-SW01**
 - 9.2.2.Authentication, Authorization and Accounting (AAA) access must be implemented to control access to the routing switches
 - 9.2.3. Secure Shell (SSH) remote administration protocol should be used to access all routing switches
 - 9.2.4. OSPF routing protocol is the principal protocol used across Wits University's campuses
 - 9.2.5. Port or Ether channeling are configured to aggregate traffic when needed for higher throughput
 - 9.2.6.Spanning tree protocol is used to manage and optimize virtual local area networks (VLANs)
 - 9.2.7. Routing switch consist of chassis, fiber modules and dual power suppliers.
- 9.3. Mini Distributions
 - 9.3.1.Naming convention - **Building Name, Type, Device** an example **CHB-MD-SW01**
 - 9.3.2.Authentication, Authorization and Accounting (AAA) access must be implemented to control access to the routing switches
 - 9.3.3. Secure Shell (SSH) remote administration protocol should be used to access all routing switches
 - 9.3.4. OSPF routing protocol is the principal protocol used across Wits University's campuses
 - 9.3.5. Port or Ether channeling are configured to aggregate traffic when needed for higher throughput
 - 9.3.6.Spanning tree protocol is used to manage and optimize virtual local area networks (VLANs)
 - 9.3.7. Routing switches consist of chassis, fiber modules and dual power suppliers.
- 9.4. Access Layer switches
 - 9.4.1.Naming convention - **Building Name, Floor, Type-Device** an example **WEC-GH-FLR1-SW01**
 - 9.4.2.Authentication, Authorization and Accounting (AAA) access must be implemented to control access to the routing switches
 - 9.4.3. Secure Shell (SSH) remote administration protocol should be used to access all routing switches
 - 9.4.4.Spanning tree protocol is used to manage and optimize virtual local area networks (VLANs)
 - 9.4.5. Access switch consist of fiber modules, stacking cable where necessary and dual power suppliers.
 - 9.4.6.Appropriate VLANs are configured, inactive VLANs for example 4040 are assigned to inactive switch ports, VTY lines to control inbound telnet connections on legacy devices if needed, Identity Services Engine (ISE) for policy enforcement and security across all access layer switches
 - 9.4.7.Voice Over Internet Protocol (VOIP) configurations using Net1 policy batch file to facilitate voice and data traffic using same switch port
 - 9.4.8. Switch stacking to be implemented to enable multiple switches to be aggregated and managed as on stack
 - 9.4.9.Access layer switched consists of fiber modules, dual power supplies to support POE+ and POE++ technology
- 9.5. Wireless Controllers
 - 9.5.1.Naming convention - **Building Name, Type, Device** an example **WEC-DIST-WLC01**
 - 9.5.2.Two wireless controllers are installed at each distribution in Stateful Switch Over (SSO) mode
 - 9.5.3.Wireless Controllers consists of fiber modules, UTP ports and dual power supplies
 - 9.5.4.CAPWAP tunnel the protocol APs are using to communicate with the controller
 - 9.5.5.AP groupings – grouping of APs per floor that helps with roaming

- 9.5.6.RF groupings – Grouping of RFs per buildings helping with signal propagation
- 9.5.7.Radio Resource Management (RRM) acts as a built-in RF software that consistently provide real-time RF management of the wireless network.
- 9.5.8.Policy enforcement – Authenticating through radius server (ISE)
- 9.5.9.Mobility grouping – helps with intra-controller roaming so that all controller can communicate with each other using same VLANs
- 9.5.10. Quality of Service (QoS) for voice, data and video to ensure seamless connections
- 9.6. Wireless Access Points
 - 9.6.1.Naming convention- **Building Name, Floor, Type-Device, Room** an example **WEC-Girton-FLR2-RM04 and unit mac address**
 - 9.6.2.Configure AP to the correct VLAN on switch and it automatically connects to controller.
 - 9.6.3.Perform Wi-Fi RF scanning to determine number and placement of Wi-Fi access points
 - 9.6.4.Active scanning will be done after the AP installation to optimize connectivity and identify interferences.
 - 9.6.5.

9.7. Services & Security

The Solution will make provision for hardware, software, licenses, cables, ports and other required and/or related components that form part of services & security.

9.7.1.Perimeter Firewall (not relevant for WI-FI installation as there is no new break out point)

- The Perimeter Firewall Solution will:
 - make provision for the current services
 - make provision for the envisaged design principles
 - ensure firewall protection for the institutional infrastructure against external threats from the internet
 - ensure the ability and performance to handle high traffic rates
 - have associated DMZ networks where required
 - have the ability to monitor the day-to-day performance and very quickly adjust in the event of short-term bottleneck, this will be made possible by monitoring tools
 - be capable of performing deep packet inspection at high speed, this will ensure security and performance on the high speed SANREN network
 - include routing failover and appropriate security for the University-supplied secondary internet breakout point, with the appropriate firewall security, associated endpoint internet access, mail and other internet services, independent of the existing ISP link to ensure full redundancy
 - ensure the ability to cater for high speed low latency firewalling with deep packet inspection capability
 - ensure high availability Solution with DR
 - ensure IPS, Application Control , Quality of Service and VPN services, at multi gigabyte speeds without affecting latency
 - ensure at minimum have a 40Gbps connection to the core network as well as a minimum of 40Gbps to the internet and/or exceed these limits to enable large scale projects such as SKA, CERN and Grid initiatives to function and transfer large data sets
 - implement IPv4 and IPv6
 - will ensure logging of all access, based on Active Directory authenticated sessions, is recorded for forensic and legal purposes

9.7.2.VPN Solution (not relevant for WI-FI installation as there is no new break out point)

The VPN Solution will:

- make provision for the current services
- make provision for the envisaged design principles
- have full high availability and redundancy, and will cater for sufficient concurrent connections
- implement IPv4 and IPv6

9.7.3.Mail Gateways (not relevant for WI-FI installation as there is no new break out point)

The Mail Gateways will:

- make provision for the current services
- make provision for the envisaged design principles
- be located at the perimeter and will handle handoff mail to downstream Exchange Servers for incoming mail and handoff to internet destinations for outgoing mail
- process system generated emails from various applications
- Implement IPv4 and IPv6

9.7.4.Network Access Control (NAC)

- The NAC Solution in existence must be considered when extending the WI-FI network, Below are the current NAC considerations in effect:
 -
 - The NAC integrates with the Active Directory (AD) framework
 - The NAC remediates devices before placing them on the network regardless of their type; after remediation the users will be placed into the logical layer in the network that allows the respective access
 - Based on the user profile determined by the AD, the users will be granted the appropriate network, and application access levels
 - It uses IPv4 and IPv6
 - It should have sufficient licensing to cover the total student and staff count and cater for multiple devices, wired and Wi-Fi
 - It integrates into the University's Directory Services to simplify the configuration of the network devices and reduce administrative issues
 - A high number of mobile personal devices (BYOD), such as smart phones and tablets as well as employee's traditional devices, such as laptops and desktops on the network
 - Combine user authentication, user and administrator access control, and policy control in a single Solution. NAC uses a rule-based policy model, which allows for security policies that grant access privileges based on many different attributes and conditions in addition to a user's identity
 - Rule-based mapping of users to identity groups is based on information available in the University's Directory Services
 - Unified Device Authentication authenticates both wired and wireless users using the same system and in the same way
 - Network access control with access servers and management tools
 - Unified Device Authentication:
 - enforces control on all the access layer switches that users use to connect to the network, including both wired and wireless users

- maintain centralized access control policy through integration with the AD
- users are securely authenticated and identified and their transactions are logged with a single Solution for wired, wireless, and remote access
- It Supports:
 - Role-based access control to control access to authorized resources by verifying user privilege level with full integration to wireless, VPN, and LAN switches
 - Endpoint security, enforcement, and remediation to enforce security policies to an endpoint device during connection
 - Silent remediation, auto remediation, and other features to help bring devices into compliance with little to no user impact
 - Guest access and dynamic user provisioning to allow the University to collaborate with confidence by providing secured guest access based on a user's role at the University. Visitors and guests will have the ability to “stay in touch” with their own organisation/company and will not sacrificing the university's security
 - Non-PC device support and data gathering to deliver automated non-PC device support by identifying, tracking, and placing the devices into pre-assigned network segments based on security policy requirements
 - Support different flavours of EAP authentication methods
 - Centralize the network profiles for 802.1x clients for both wired and wireless users

9.7.5.

9.7.6.Firewalls configuration

- Firewall naming convention - Building Name, Type, Device an example SMH-FIRE-01
- Secure and strong password should be created immediately after installation and configuration
- Adopt a principle of least privilege and denying all traffic by default and rulesets to be incrementally opened to allow permissible traffic
- Restricting both inbound and outbound traffic to systems and services that are identified and required
- Avoid using “Any” option in commands in firewalls to allow rules
- If available, turn the intrusion detection and intrusion blocking option and also turn on notifications
- Network Address Translation (NAT) should be turned on to conceal internal addresses from the internet
- Latest firewall updates and patches should be installed to address new vulnerabilities when available.
- Firewall Rulesets and Configurations require annual periodic review to ensure they afford the desired levels of protection.
- Firewall rulesets and configurations must be backed up frequently to alternative storage, on separate device and location
- Multiple generations must be captured and retained in order to preserve the integrity of the data, should restoration be required. Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review
- Network Firewall administration logs (showing administrative activities) and event logs (showing traffic activity) are to be written to alternate storage (not on the same device) and reviewed regularly
- It is recommended that utilities or programs that facilitate the review process be employed. Appropriate access to logs and copies is permitted to those responsible for Firewall and/or system maintenance, support and review.
- Firewall Administrators will execute approved changes to the Firewall Rulesets maintained by Wit ICT following the defined change management procedures.