**Philbert Mfashingabo**

[PMfashingabo@lanwanprofessional.com](mailto:PMfashingabo@lanwanprofessional.com) | (714) 627 - 5991

**Summary**

IT professional with over several years of professional and progressive technical experience in engineering, supporting business networks, escalation support, on-site support, design, configuration, installation, integration, monitoring, troubleshooting and documentation of various LAN/WAN technologies for enterprise environments and include proficiency in routing, switching, security, voice, wireless and datacenter technologies.

**Technical Certifications & Skills**

* Cisco Certified Network Professional - Routing & Switching **CCNP – R&S**
* Certified WAN Professional **CWP**
* Cisco Certified Design Associate **CCDA**
* Cisco Certified Network Associate – Routing & Switching **CCNA – R&S**
* Cisco Data Center Administrator **CDCA**
* Cisco Voice Administrator **CVA**
* Cisco Security Administrator **CSA**
* Cisco Wireless Technician **CWT**
* Certified WAN Administrator **CWA**

**Technical Skills Detail**

Network Hardware: Cisco Routers (3900, 2900, 1900, 800), Cisco Catalyst Switch (6500, 5500, 4900, 4500, 3000, 3100), Cisco Nexus 5k and 7k Series, Cisco ASA 5500 Series, Cisco WLC, Juniper (E, M, MX, T) Series.

Routing/Switching: WAN, LAN, TCP/IP, Spanning Tree, BPDU, CDP, Frame-relay, PPP, ACL, Network Address Translation (NAT), Port Address Translation (PAT), Access Control List, RIP, OSPF, EIGRP, BGP, MPLS, VTP, SNMP, SMTP, ARP, TCP, UDP, Static Routing, Stub Routing, VLAN Trunking, Multi-Area OSPF, VLAN, VTP, HSRP, SVI, CEF, Etherchannel, Portfast.

Data Center Technologies:  VMware VSphere 5.5, VCenter Server Appliance 5.5, VMware ESXi Hypervisor 5.5, Cisco Nexus 1000v ,Virtual Supervisor Modules (VSM) and Virtual Ethernet Modules (VEMs), Prime Network Services Controller (PNSC), Cisco Cloud Services (CSR 1000v), Port Groups, Routing Profiles, Service Profiles.

Security Technologies: AAA, IPS/IDS, TACACS+, RADIUS, SSH, VPN, Cisco ACS, Data Loss Prevention, IPSec, Data Management Zone, PGP, PKI, Port Security, MAC Address Filtering, IPS/IDS, NPS.

VoIP/Wireless Technologies: 802.11 a/b/g/n, WLAN, WAP, AP, SSID, LWAPP, CSMA/CA, Cisco ACS, VoIP, CUCM, QoS, PoE, CME, CUE, Port Security, MAC Address Filtering, SIP, MGCP, RTP, SCCP, SRTP, UCCM, UCCX, GSM, 3G.

Monitoring Tools/Hardware: Finisar, Wireshark, Remedy, Openview, Cacti, Nagios, VMware, Solarwinds, F5, Cisco Works, LogicMonitor, Cisco Security Manager Suite, DNS Servers, DHCP Servers, NTP Server, TFTP Server, Exchange Server, Blade Servers, Web Servers, Syslog, FTP, SFTP, Sonicwall, watchguard.

Computer Languages: C and C++.

**Summary of Professional Experience**

**Tigo Rwanda Network Engineer 2013 – 2013**

* Member of a team of professionals responsible for the day-to-day maintenance of the IT infrastructure to include onsite administration and support, scheduled installation, configuration and troubleshooting activities.
* Technical responsibilities included, but were not limited to, the installation, configuration, administration, and troubleshooting of LAN/WAN network problems and radio base stations utilizing GSM and 3G technologies.

**New Artel Network Technician 2011 – 2011**

* Member to a team of field engineers responsible for the field support, installation, configuration, and troubleshooting of mission critical technologies within a LAN/WAN network infrastructure.
* Technical responsibilities included, but were not limited to, the installation, configuration, administration, and troubleshooting of various enterprises LAN/WAN technologies which includes Cisco routers and switches, wireless access points and different types of antenna.

**Education**

**Master of Science in Electrical & Computer Engineering Oklahoma Christian University**

**Bachelor of Science in Electronics & Telecommunications Engineering Kigali Institute of Science & Technology**

**Certified WAN Professional Program LANWAN Professional**

**Summary of Technical Accomplishments**

**Routing & Switching**

* Configure secure privileged administrative access to the Cisco IOS system. Enable the encryption of system passwords to prevent unauthorized users access to passwords in the system configuration.
* Configure secure access to the console and vty ports, and set the interval that the EXEC command interpreter waits until user input is detected on the Console and vty ports. Also, configure the console and vty ports log messaging to not interfere with active device configuration.
* Configured and administrated VLAN Trunking Protocol to reduce administrative overhead. Enable secure sharing of VLAN information to prevent the introduction of rogue devices from affecting the VLAN database. Shutdown unused switchports following Layer 2 security best practices.
* Configured VLAN Trunking Protocol to reduce administrative overhead. Enable secure sharing of VLAN information to prevent the introduction of rogue devices from affecting the VLAN database. Shutdown unused switchports following Layer 2 security best practices.
* Administrated Local VLANs based on department function, and configure ports with static VLAN assignment, static 802.1Q trunks, and dynamic ISL trunking using PAgP for layer 2 forwarding. Utilize VLAN Spanning-Tree in conjunction with PVST+ for compatibility between Cisco and Juniper switches. Configure edge ports for fast-transitioning into the forwarding state to fix workstation startup connectivity delays. Modify spanning-tree parameters for manual root bridge assignment. Implement ether-channels between each switch using PAgP for negotiation. Modify ether-channel load balancing method.
* Integrated WAN links between sites using frame-relay point-to-point and multipoint connections to establish connectivity between each of the four sites as required. Establish two frame-relay point-to-point connections between a central site and two remote sites. Configured multipoint connections between three of the sites forming a full-mesh.
* Configured EIGRP MD5 Message Authentication between sites to prevent unauthorized insertion of routes into the domain. Integrate manual EIGRP route summarization to reduce routing protocol demand on CPU resources, memory, and bandwidth used to maintain the routing table.
* Configure and administrated OSPF routing with multiple areas for networks between sites. Implement OSPF MD5 Authentication between each OSPF enabled subnet to prevent unauthorized insertion of routes into the domain.
* Integrated static NAT/PAT to provide access to services located on a server in the private network to the public network. Implement standard and extended access-lists to filter network traffic.
* Configured backup and recovery of Cisco IOS Images. Perform password recovery on Cisco IOS routers/switches and a Juniper EX2200 Series switch to restore administrative access. Backup and Restore startup-config file for disaster recovery.

**Security**

* Configured and administrated an IPSec Site-to-Site VPN between the Cisco ASA5505 at small office location and Cisco 1841 ISR with a security IOS image at the main office. Implementation of the VPN includes the following configurations: Internet Key Exchange Policy using DES and SHA for encryption and authentication, access-lists to define VPN traffic, transform set using esp-des esp-sha-hmacto define how the traffic is protected, crypto-map to associate the previously configured elements to a peer, and application of the crypto map to appropriate interface or VPN endpoint.
* Configured and administrated Zone-Based Policy Firewall on the Cisco 1841 ISR with the following components: three zones, class-maps specifying traffic that must have policy applied as it crosses a zone-pair, policy maps to apply action to the class-maps’ traffic, zone-pairs, and application of policy to zone pairs.

**Voice**

* Configure Cisco 2811 ISR (VoIP) with a Cisco Unity Express Network Module (NM-CUE) installed, Cisco Communications Manager Express, a standard Cisco 3550 Switch, and a Cisco 3550 switch with Power-over-Ethernet. Create and manage Data and Voice VLANs, and configure ports with static VLAN assignment and 802.1Q trunks for layer 2 forwarding. Configure edge ports for fast-transitioning into the forwarding state to fix workstation startup connectivity delays.
* Configure Fast Ethernet main and sub-interface assignments as required for intervlan routing. Implement static routes for local connectivity. Configured NTP server, DHCP server, and TFTP server for support of the VoIP network. Modification of system level parameters including max phones, max directory numbers, display format for date and time, and setting the Time-Zone.
* Integrate Unity Voicemail on the Cisco Unity Express Network Module. Configure a dial-peer on the Cisco 2811 ISR to define the attributes of the packet voice network connection to the Cisco Unity Express Network Module. Enable call forwarding on busy or no answer. Implement Message Waiting Indicators and Voicemail access via SMTP. Daisy-chain PCs to VoIP phones to reduce network cabling costs. Utilize PoE ports for VoIP phones to reduce power infrastructure costs.

**Wireless**

* Administrated a wireless network infrastructure providing access to wired LANs to increase mobility and productivity utilizing the following network elements: Cisco Wireless LAN Controller (WLC) 2106, a Cisco 3550 switch, a Cisco 1130AG series Access Point, and a Cisco 1121G series Access Point. Create wireless LANs and configure interface association, security parameters, and radios used. Utilize the Wireless LAN Controllers web GUI to configure and manage the wireless network. Configure internal DHCP scopes for WLANs.
* Prepare configuration for AP registration on same subnet as management VLAN and for AP registration on different subnet. Implement option 43 for DHCP where necessary. Configure AAA AP policies to allow Self Signed Certifications for APs shipped without a Manufacturer Installed Certificate. Implement AP Grouping to ensure WLAN SSIDs are only broadcast by the APs desired.