**Zihui (Morgan) Qu**

ZQu@lanwanprofessional.com | (951) 867-7799

**Summary**

A professional with progressive IT experience in engineering, deployment administration, integration, configuration, installation and troubleshooting of various technologies which includes proficiency in routing, routing protocols, switching, security, firewalls, voice, wireless and data center technologies.

**Technical Certifications & Skills**

* Cisco Certified Network Professional – Routing/Switching CCNP – R&S
* Certified WAN Professional / Certified WAN Enterprise Administrator CWP / CWEA
* Cisco Security Administrator / Data Center Administrator CSA / CDCA
* Cisco Voice Administrator / Wireless Technician CVA / CWT
* Cisco Certified Network Associate – Routing/Switching CCNA – R&S

**Technical Skills Detail**

**Routing/Switching Technologies –** Networking**, Cisco** Routers (3900, 2900, 1900, 800 Series), **Cisco** Catalyst Switch (6500, 5500, 4900, 4500, 3750, 3560-X, 3100**), Cisco Nexus 1kv, 2k, 5k, 7k Series**, Juniper and HP Routers & Switches - WAN, LAN, TCP/IP, Cisco IOS, Spanning Tree Protocol, BPDU, CDP, ACL, NAT, PAT, RIP, RIPv2**, OSPF, OSPFv3**, EIGRP, **BGP**, MPLS, VTP, SNMP, SMTP, ARP, TCP, UDP, Static Routing, Stub Routing, VLAN, VLAN Trunking, VXLANs, **Multicast routing,** HSRP, SVI, CEF, EtherChannel, PortFast, VSS, VPC.

**Wireless/Voice Technologies – Cisco Prime,** Cisco WLC, IEEE 802.1x & 802.11, WLAN, WAP, AP, SSID, LWAPP, Aironet, Bluetooth, Avaya, AURA - Voice Over Internet Protocol (VoIP), VoIP/SIP, Cisco Call Manager VoIP, CUCM, UCCM, UCCX, MGCP, RTP, SCCP, SRTP, Quality of Service (QoS), PoE, MMDS, LMDS, CCK, DSSS

**Security/Firewalls Technologies -**  Cisco Security Manager Suite, Cisco ASA 5500 series firewalls, Cisco FWSM, Cisco IPS/IDS, Cisco ACS, Advanced Firewall Manager (AFM), Cisco ASA 1000V cloud firewall, Checkpoint Firewall, Juniper SRX series, Palo Alto, **Protocols & Standards** - **TACACS+**, SSH, VPN, IPSec, SSL/IPSec, Data Management Zone, Pretty Good Protection (PGP), Public Key Infrastructure (PKI), Internet Key Exchange Policy, Port Security, MAC Address Filtering

**Monitoring/Data Center/APPS** - Wireshark, Remedy, Cacti, Nagios, VMware, **SolarWinds** **NPM**, Cisco Security Manager Suite, Server, Sniffer, Ethereal, Orion - VMware, F5 Big-IP load balancing (GTM/LTM), Cisco AnyConnect VPN mtg, Cisco Prime, Meraki cloud.based - Splunk Enterprise, SNMP, **DNS, DHCP**, FTP, Telnet, HTTP(S), SMTP, tunneling protocols.

**Applications/Languages** - matlab&simulink, gcc, SQL Developer,qemu, Cadence&Vertruoso, Xilinx ISE,Protel, Visual Studio, VMWare, VirtualBox, C, C++, Python, Verilog, Bash, Assembly, SQL, PLC, Matalab, QTP/QC,LATEX.

**Summary of Professional Experience**

**LANWAN Professional Network Engineer 1 2015-Present**

**Company Overview** - LAN/WAN Professional is a nationwide membership organization of LAN/WAN professionals including administrators, engineers, consultants, analysts, architects located throughout the continental United States.

* Member of a team responsible for onsite LAN/WAN support deployment and configurations of routers, switches, wireless, voice, firewalls and related LAN/WAN technologies.
* Secondary responsibilities including general escalation troubleshooting support and general administration to included LAN/WAN configurations, logical/physical diagrams based on company standards and policies.
* Additional responsibilities included provided timely and accurate updates/reports to technical leads/managers relates to tasks and responsibilities that are assigned and act as subject matter expert on routing, switch related activities.

**Education**

**Master of Engineering, Computer Engineering Hardware Boston University**

**Bachelor of Science in Electrical Engineering and Automation University of California Riverside**

**Bachelor of Science in Electrical Engineering and Automation Harbin Institute of Technology**

**Summary of Technical Accomplishments**

**Routing & Nexus & Catalyst Switching**

* Implement trunk ports and implement granular control of VLANs and VXLANs using NX-OS to ensure virtual and flexible subnets that can extend further across the network infrastructure than previous generation of switches.
* Implement port-profiles as part of the NX-OS command structure that allows for configuration of multiple ports and port-types via inherited configurations applied via a single command that reduces administrative error and allows for better configuration readability.
* Implement a virtual version of Nexus: Nexus1000v into VMWare to extend Nexus capabilities directly adjacent to virtual machines so that they benefit from Cisco switching capabilities and network topology consistency ensuring VMs maintain their subnet/VLAN relationships during failover.
* Implement 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.
* Implement 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.
* Implement 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.
* Create and manage 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.
* Implement 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 frame-relay point-to-point connections three of the sites creating a full mesh. Implement hub and spoke network between three of the sites with the main office as the hub for redundant connections.
* Implement EIGRP routing for point-to-point and Non Broadcast Multi-Access networks. Ensure that the spoke routers are receiving routing information about each other from the hub. Configure EIGRP unequal-cost load balancing to also use the lower capacity multipoint links when routing packets.
* Prevent neighbor adjacencies from being formed as well as the sending and receiving of routing updates on unnecessary interfaces. Implement EIGRP MD5 Message Authentication between sites to prevent unauthorized insertion of routes into the domain. Implement manual EIGRP route summarization to reduce routing protocol demand on CPU resources, memory, and bandwidth used to maintain the routing table.
* Implement OSPF routing with multiple areas for networks between sites. Implement totally stubby areas to lower the system resource utilization of routing devices for the network. Implement NSSA area to allow injection of external routes into the area and propagation into the OSPF domain.
* Implement 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-comfit file for disaster recovery.
* Configured and verified internal BGP peering using directly connected networks.
* Configured and verified internal BGP peering using loopbacks by using an interior gateway protocol (OSPF) to provide routing information.
* Configured and verified external BGP peering using directly connected networks.
* Configured and verified external BGP peering using loopbacks and ebgp-multihop.
* Configured and verified internal BGP peering using a Route Reflector.
* Used debugging diagnostic commands to monitor BGP events.
* Configured and verified MPLS manually and using automatic configuration via OSPF.
* Configured and verified virtual routing and forwarding (VRF) instances with route-targets and route descriptors.
* Configured and verified MP-BGP to send VRF traffic in an MPLS VPN.
* Redistributed provider edge networks into MP-BGP.
* Verified end-to-end connectivity over the MPLS VPN.

**Security**

 Implement 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.

 Implementation of 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.

 Implement a Clientless SSL VPN (WebVPN) to allow users to establish a secure, remote-access VPN tunnel to the Cisco ASA 5505 using a web browser. Prepare the Cisco ASA with necessary configurations to self-signed certificate generation. Generate a general purpose RSA key-pair for certificate authority identification, configure certificate authority trustpoint for the WebVPN using self enrollment, and configure CA trustpoint interface association.

 Configure Syslog on the Cisco ASA5505 with logging to a host and internal buffer. Forward all logging to an internal Syslog server for monitoring and management. Configure and manage Syslog output generation using custom message lists. Implement FTP backup of internal buffer when it is exceeded.

 Implement Basic Threat-Detection, Advanced TCP Intercept, and Scanning Threat-Detection. Simulate attacks on network to manage threat-detection rates and verify Syslog generation.

 Utilize Cisco ASA5505 Modular Policy Frame-Work to configure and manage layer 3/4 interface service policies, apply inspection and connection limits to services, apply inspection and QoS policing to HTTP traffic. Configure HTTP inspection policy to block restricted sites and file downloads.

**Voice**

 Implement a local voice network with the following network elements: 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. Implement 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.

 Implement 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**

 Implement 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 infrastructure for AP registration on same subnet as management VLAN and for AP registration on different subnet. 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.

**Data Center**

* Configured VLANs and access ports connecting virtual machines using the NX-OS CLI on a Cisco Nexus 1000v virtual machine and VMWare vSphere Client networking.
* Configured routing policies and service profiles for separate levels in an organizational hierarchy using a Cisco Prime Network Services Controller virtual machine. These policies and profiles were applied to Cisco Cloud Service Router 1000v (CSR 1000v) virtual routers.
* Configured a CSR 1000v router using the Cisco IOS 15.4 CLI.

# **Monitoring**

* Used the Cisco Configuration Professional GUI to configure interfaces, passwords, hostnames, DHCP, EIGRP, and SNMP on a Cisco router. Used the CCP monitoring tool to monitor traffic from that router.
* Configured the Nagios XI monitoring tool to monitor routers and switches and customized its dashboard.
* Configured SolarWinds Orion NPM and used it to monitor traffic on a network.
* Configured the CACTI tool to graph traffic from a router and to generate alerts based on a threshold traffic level.
* Used the Wireshark tool to study HTTP, telnet, and SSL traffic.