Alabas Nihad

Baltimore, MD - Email me on Indeed: indeed.com/r/Alabas-Nihad/7bc24942e3a60005

• 12 years' experience in LAN/WAN technologies, Routing/Switching protocols and Wireless Technologies including TCP/IP protocol suite and multi-protocol routing in Cisco, Juniper and FortiNet environment.
• Excellent troubleshooting experience of intricate network and systems issues with RIPv1/v2,OSPF, EIGRP and BGP.
• Experience installing, configuring and troubleshooting Catalyst (2900, 3500, 3700, 4500 and 6500 Series), Nexus (7000, 5000 and 2000 Series) Switches, and Routers (ASR, 2800, 3600, 4400 Series) and Wireless AP's (1260, 3600) using CLI and GUI.
• Knowledge of implementing and troubleshooting complex layer 2 technologies such as VLAN Trunks, VTP, Ether channel, STP, RSTP, and RPVST. Implementation of HSRP, VRRP,GLBP for Default Gateway Redundancy.
• Familiar with IPv6, OSPF v3.
• Network security including NAT/PAT,ACL.
• Configuring Juniper SSG, FortiGate 60D and ASA firewalls 5510 and 5505.
• Working knowledge of network monitoring/management tools like Wireshark, Cisco Prime, Net Flow, Solar Winds.
• Experience in diverse IT disciplines, including networking, technical support, programming, operating systems and system administration.
• Knowledge in preparing Technical Documentation and presentations using Microsoft VISIO/Office.
• Strong written and verbal communication skills, self-motivated, self-managed, result oriented, practical, always looking to learn and contribute.
Authorized to work in the US for any employer

WORK EXPERIENCE

Wireless Network Engineer

Carroll Hospital a Life Bridge Health Center - February 2016 to Present

Wireless
• Assigned WLANs to indoor and outdoor WAPs (each WAP's group has it's own WLAN'), for example: guests WLAN cannot use outdoor WAPs.
• Investigated in Voalte phones/Motorola MC40 models channels bands scanning capabilities and match MC40 channels profile with cisco wireless access points channels/power levels to prevent coverage holes and longtime channel scanning cycle.
• Configured auto QoS on the switch ports that connected to WAPs and QoS of the WLANs.
• Prepared labs using real devices to check the configuration changing impact before making changes in real environment (i.e. on wireless controller 5508, we have DTPC is disabled, I enabled it in the lap to see what this effect on the AP's).
• Deployed monitor mode access point and enable Rogue Location Discovery Protocol (RLDP) on the WLC to prevent rogue access points and clients.
• Designed N+1 Redundancy, N+N Redundancy and N+N+1 Redundancy.
• Wireless site survey in new sites using WLC 2504, WAP 3702 models, and Air Magnet Pro software and positioned WAP in the right place to have wide coverage.
• Designed wireless heat maps and positioned the WAP's on the floor plans using cisco prime infrastructure.
• Created Radio Frequency groups and assign them to specific group of WAP's
• Converted autonomous AP's to lightweight AP's using cisco prime.

• Searching about interfere devices (microwave, cordless phones) in the sites that have interference issues using Air Spectrum Analyzer.
• Deployed additional AP's in sites has poor 802.11 signal coverage after active site survey.
• Gave my recommendation to replace AP 3502-A model with 3700 model
• Upgrade WLC 5508 software version from 8.0.115.0 to the latest code 8.0.140.0 in order to be compatible with WAP 3702I-B domain deployment.
• Minimizing and reducing channel interference and the interference severity by changing the overlapping channels to one of the non-overlapping channels (1,6 or 11)
• Drawing sites floor plans after taking measurements to import them to AirMagnet to perform passive site survey.
• Set and apply RX Sop (Receiver Start of Packet Detection Threshold) for RF profile to minimize co-channel interference, and ensure that the clients are connected to the nearest AP using the heights possible data rates.

Wireless Surveys:
• Obtaining CAD/PDF/JPEG Drawings and use with Air Magnet Survey/Cisco NCS to obtain environment measurements of the building and the floor plan.
• Doing a Preliminary walkthrough survey and basic placement on maps based on a multi-floor plan. Ensure the WAP is properly located to avoid co-channel interference from the floor above and below. Doing an On-Site pre-deployment
• Wireless assessment/Passive site survey for 22 sites (Medical Offices) using AirMagnet Survey Pro.
• Walking around in the coverage area to determine cell size for 2.4GHz and 5GHz.
• Working with the building wiring contractor so that there is a clear understanding of WAP placement and proper placement makes the build to architectural drawings. Make sure appropriate monitoring is set up for alarms and alerts for the wireless infrastructure.
• Post Deployment Site Survey. Verifying coverage with a walk around using a commonly deployed device such as a wireless VOIP phone.
• Doing active survey testing both sending and receiving (transmitting) packets. Fine tune the deployment and troubleshoot if necessary and moving WAP (Wireless Access Points) around.
• Manually adjusting Signal strength on wireless access points and confirm adjustments with walkthrough.
• Making sure the QoS path is trusted on the switch configuration and the packet is being tagged properly. Making sure that a Layer 2 roam across subnets is seamless on a mobile device. Testing mobile clinical wireless devices and clinical application to ensure the appropriate coverage for the mobile device.

Wired
• On 7K switches (c7009), provided gateway backup for IP hosts by sharing virtual IP address and MAC's by using GLBP.
• Configuring Destination and Source NAT on Sophos UTM firewall for server located in DMZ.
• Adding IP cameras, printers and supplicants on ISE Server (Authentication Server) after configuring switches (Authenticator) ports with 802.1x MAC Authentication Bypass (MAB)
• Designing new IPv4 addressing scheme by conveting the wired and wirless networks from 10.250.0.0/22 to 10.69.0.0/22 to prevent the overlapping with Sinai, Levendil and Northwest hospitals.
• Maintaining and troupleshooting BGP routing table on ASRs Carroll Hospital routers with ISP.
• Prevented vlan hopping attack (shut down unused ports, assign them to isolated vlan, make the native vlan other than 1 and configure the access ports with nonegotiate.
• Protect the network infrastructure from rogue switches by enabling BPDU guard.
• Upgraded ASA model 5505, 5510, 5520 and 5540 from version (7.x, 8.0, 8.1, 8.2) to 8.3. And migrated old NAT statements to the new ones.
• Built vpn tunnels to connect servers on the Microsoft Azure cloud and created group policies.

• Configured the switches ports with power inline in watt to be compatible with WAP power setting and configured the switches ports with power priorities (high and low), and adjust the power limit that the switch provides to each port
• Configuring 22 remote sites with Dynamic Multipoint VPN (DMVPN) using GRE over IPSec between multiple routers
• IOS maintenance configuration like archiving and build backup configuration on regular basis for cisco switches and routers.
• Trouble shooting ports error disable (i.e. configuring call home technique to receive emails and text message in case sys log get specific messages)
• Trouble shooting switch stack management (i.e. configure auto software update on the master switch to make the software compatible on the whole stack).
• Prevented CAM table overflow attack by using port security feature and limit the mac address on the switch ports and automatically recover the error disabled ports using recovery interval after violations.
• Prevented rogue DHCP server to assign unwanted IP addresses scopes by configuring the switch with DHCP snooping globally and on vlans level.
• Created span port configuration to capture and analyze data using Wireshark.
• Scheduled configuration archive for all managed devices(switches, routers, WLCs) on cisco prime infrastructure.
• Working on SFP 10G LR for single mode fiber cable and SFP 10G LRM for single/multimode mode fiber cable
• Configure the network infrestructure with snmp, tacacs+ and radius protocols to let the network devices send snmp traps to cisco prime, and to have authentication take place on ACS and ISE servers.

Environment: Routers: ASR. Switches: 4510, 3750, 3850 2960, 2k, 5k, 7k. ASA 5555x. AP: 3500,3700A-B, Astaro AP30, AP50. WLC 2504, 5508, 5520. MSE & CMX, Cisco Prime 3.1, ISE 1.2. Firewall: UTM Sophos

Network Engineer

Grupo Bimbo, PA, Horsham - October 2015 to February 2016

• Configured and installed various network devices and services (routers, switches, firewalls, etc.) in conjunction with Grupo Bimbo and/or Bimbo Bakeries USA network engineers.
• Performed network maintenance and network device system upgrades, including service packs, patches, hot fixes and security configurations
• Worked within established configuration and change management policies to ensure awareness, approval and success of changes made to the network infrastructure
• Configure and ship Cisco wireless controllers 2500 and access points 2600 to each plan/site.
• Identify switch port capacity and configure network connectivity for shop floor Instrumentation Devices and special purpose
• Configure and ship Cisco switches for Infrastructure upgrades
• Registered Light Access Points with Wireless Controller.
• Downgrade the WLC to be compatible with centralized WLC.
• Refreshing and upgrading 60 plants (sites) with WLC, AP and cisco switches
• Assign 2.4/5 ghz channels to the AP's based on third party site survey.

Senior Network Engineer

Amtote International, MD - December 2014 to October 2015

• Refreshed and upgraded Amtote internal network from 2950 cisco switches to 4510R cisco switch.
• Involved in upgrading to the latest IOS images and firmware for cisco routers and switches, Juniper and FortiNet firewalls.
• Opened VPN connections from LINUX boxes and Vyatta firewalls hosted on Amazon Web Services Cloud (AWS) and RackSpace and connected them to Juniper SSG and FortiGate 60D firewalls.

• Created VPCs, subnets and Instances on AWS cloud (virtual networking on private cloud), created route table (routes, subnet association, route propagation) and attached them to Internet gateway then to virtual and actual networks.
• Assigned AWS VPCs to specific zone as well as the instances and its network interfaces.
• Configured Security groups for subnets and instances on Amazon Web Services (AWS) for inbound and outbound traffic.
• Install and setup Shrew Soft on Windows Servers and Linux to open VPN connection to the servers located at Amtote Data Center
• Configured Access HP switches 2530 series and connected them to Amtote terminals.
• Configured Distribution HP switches and connect them to FortiGate and Juniper firewall.
• Configured, setup and install FortiGate 60 D and Juniper SSG 5,20,140 and 320M Firewalls.
• Configured IPSEC VPN through GRE tunnel on firewalls.
• Open VPN connections and configured policies and UTM on Juniper and FortiGate firewalls
• Prepared VISIO diagram for new sites connected with Amtote data center.
• Configuring and troubleshooting NSRP and High Availability on Juniper and FortiGate.
• Creating zones, Virtual Routers VR, routing (Static, Dynamic), policies and addresses or subjects on Juniper and FortiGate firewalls.
• Giving recommendations about what are the recent best firewalls should be used depends on the network environments.
• VPN troubleshooting using tcpdump, show security association, debug VPN ipsec and ike phases, checking aes encryption value, lifetime, preshared key on both VPN sides.
• Upgrading RedHat Linux, Cnetos Linux and Ubuntu Linux with Open Swan software to create IPSEC VPN connection and configure the above Linux boxes for encryption and decryption data between source and destination. Add persistent route on them to keep the route table stable as much as possible and maintain the network interface file as needed.
• Configured Juniper and FortiNet firewalls with zones and controlled zones with incoming and outgoing traffic as permit and deny services like http, https, rdp, icmp, icmp-ech etc.
• Set BGP attributes values (Weight, Local Preference, AS-path, MED) on routers to let AS select the best path for incoming and outgoing traffic.
• Configure OSPF summarization on Area Border Routers and Autonomous System Border Routers.
• Used most powerful troubleshooting tools like tracert, tracerout, routeprint, ping, ipconfig/ifconfig, nslookup, netstat, analysis WireShark Capture file and looking for upnormal ip packet behaviors.

Network Engineer

Fujitsu - Unisys Account, MD - May 2012 to November 2014

• Involved in complete LAN, WAN development (including IP address planning, designing, installation, configuration, testing, and maintenance).
• Provided Tier 2 support for network (Layer 3) related issues for the customer.
• Used Layer 3 protocols like EIGRP, OSPF, and BGP to configure Routers in the network.
• Implemented redundancy /failover using HSRP.
• Performed switching technology administration including VLANs, VDCs, inter-Vlan routing, trunking, link aggregation control protocol (LACP), link negotiation & fex-fabric.
• Configured VPN, ACL, and NAT in the Cisco ASA 5540 firewall to allow only authorized users to access the servers of the internal network
• Involved in troubleshooting various layer 2 and layer 3 issues related to VRF and BGP routing.
• Supported acquisition by merging two different networks.
• Installed and configured Cisco Nexus 2148 T, 2242TP, 5548P, 5548UP, N7KM148GS-11L
• Worked on Nexus deployment methods (Straight through using static pinning and dynamic pinning, and active-active using VPC), and Fabric Path to eliminate STP.

• Used Network monitoring tools to ensure network connectivity and Protocol analysis tools to assess and pinpoint networking issues causing service disruption.
• Preformed IOS upgrades and reconfigured devices afterwards.
• Upgraded 2950 cisco switches to 2960X cisco switches
• Installed wireless routers, operating system, cabling (CAT 5, CAT 6 and termination, connectivity to switch rooms)
• Configured Cisco routers with Radius and TACACS authentication.

Network Engineer

Verizon - December 2010 to April 2012

• Installed and configured Cisco 2600, 2800, 3600, 3800 routers and 2950, 3700, 6500 switches.
• Maintained and managed networks running EIGRP and BGP routing protocols.
• Configured peer-link to create VPC
• Configured route redistribution between OSPF and EIGRP in a multi-area OSPF network.
• Daily monitoring of network traffic using sniffers and access logs to troubleshoot and identify network issues.
• Performed Layer 2 administration including VLANs, Private VLANs, inter-VLAN routing, trunking, port aggregation
• Route redistribution and route update manipulation using route-maps, distribute lists and AD manipulation and link negotiation.
• Used network monitoring tools to ensure network connectivity and protocol analysis tools to assess and pinpoint networking issues causing service disruption.
• Worked with engineering team to resolve tickets and troubleshoot L3/L2 problems efficiently.
• Preformed IOS upgrades and reconfigured devices afterwards.
• Updated documentation as necessary.
• Mapped, Network Diagrams and physical identification in MS Visio.
• Worked with Radius and TACACS
• Worked with policy based routing in a MPLS routing environment.

Network Engineer

DATA POINT, MD - November 2008 to November 2010

• Configuring and troubleshooting HSRP, BGP, OSPF, EIGRP, MPLS WAN, QoS and Route Maps.
• Troubleshoot connectivity issues involving VLAN's, EIGRP, QoS etc.
• Support, monitor and manage the IP network.
• Performance monitoring of various applications and web servers to maintain quality of service and network stability.
• Maintained core switches, creating VLAN's and configuring VTP.
• Designed IP Addressing schemes, VLAN tables and Switchport assignments, Trunking and Ether-channel implementation.
• Gained hands on experience with VRF, VLSM, STP, VTP, VLAN Trunking.
• Installed and set up Cisco routers and switches according to deployment plans.
• Applied access lists and NAT configurations based on implementation guidelines.
• Developed network projects designed to strengthen network continuity and deploy security elements in an attempt to meet and exceed contract requirements, including system analysis and troubleshooting.
• Change management, monitoring network performance with network tools.
• IP Distribution for existing devices and new devices as they were added.
• Preformed maintenance on equipment as necessary, performing device upgrades, modification of configurations, password changes and diagnostic testing.
• Worked with vendors and Engineering team to test new hardware and procedures.
• Coordinated with higher-level support and external vendors for resolution.

• Prepared and maintained documentation using MS Visio.

Network Engineer

UNICEF - January 2005 to July 2008

• Involved in network upgrades and implementation.
• Diagnosed problems through troubleshooting skills, logic, research, and isolation steps.
• Performed routine maintenance of network hardware and software of LAN/WAN (NAT, DHCP, SNMP)
• Configured ACL to allow only authorized users to access the servers.
• Implemented VLANs, DHCP server, DNS configuration, NAT/PAT in a small network environment.
• Configured Routing Protocol: single-area OSPF, RIPv2.
• Performed technical support, troubleshooting and maintenance of network equipment, installed and upgraded software and hardware equipment.
• Implemented WAN technologies like Frame relay, HDLC and PPP in the branch office network connectivity.

EDUCATION

BSc in Computer Science and Information System

University of Technology
2004

SKILLS

BGP (8 years), cisco (8 years), IOS (6 years), OSPF (10+ years), vlan (7 years)

PUBLICATIONS

Upgrading cisco WLC to have new code

https://www.linkedin.com/pulse/upgrading-cisco-wlc-have-new-code-alabas-n-abbas
April 2017
Let's assume you have critical mission wireless network deployment, and you are not sure how the wireless devices will behave if you upgrade cisco wireless controller code from 8.0.xxx.0 to 8.0.xxy.0 following cisco recommendation to handle vulnerabilities affecting multiple products.
Please follow URL for more info.

ADDITIONAL INFORMATION

TECHNICAL SKILLS
• Cisco Routers: 2800, 3600, 4400, […] 3900, 7600
• Cisco Switches: 2900, 3500, 3700, 5000, 4500, 6500
• Cisco Wireless: 1260 AP, 3600 AP, 2602 AP, 3700 AP, […] 5520, MSE 3365 10.0 with CMX
• Other Hardware: Juniper SSG […] and 320M, Juniper SRX210, Vyatta Firewall, F5 BIG-IP LTM Load Balancer
• Networking: TCP/IP, UDP, ICMP, LAN, WAN, DHCP, DNS, FTP, TFTP, SNMP, ARP
• Other Protocols: HSRP, NSRP, HA, GLBP, VRRP, QoS, IPv4, IPv6, IP SLA
• Security: ACL, NAT/PAT, Juniper, FG 60D, ASA (5505, 5510) Firewall,
• Routing: EIGRP, OSPF, BGP, MPLS
• Switching: VLAN, VTP, STP/RSTP/RPVST
• Operating Systems: MS Windows XP/Vista/Windows 7, Linux (Centos, Ubuntu, RedHat), CISCO IOS.
• Applications: Wireshark, Cisco Prime Infrastructure, Solar Winds, MS Office and MS Visio

- Languages: Matlab, C ,Labview,Pspice
- Microsoft Office (Excel, Access, Power Point)