Dohn Nimmo

Network Engineer - 1 Source Consulting, Inc

- Email me on Indeed: indeed.com/r/Dohn-Nimmo/e7115d97aa2207d3

Authorized to work in the US for any employer

WORK EXPERIENCE

Network Engineer

1 Source Consulting, Inc - Washington, DC - July 2016 to Present

• Network Engineer supporting Department of Treasury (TTB) infrastructure.
• Monitoring/Troubleshooting/Upgrading network infrastructure.
(EM7/SolarWinds/CUCM/NETSCOUT Truview/Optiview)
• Mitigates network security vulnerabilities per Dept of Treasury.
• Provide overall network health status to CIO/ACIO, weekly.
• Works with ATT (Provider) for circuit maintenance, troubleshooting and change management. Also to include
EIGRP OTP connectivity between remote sites (hub-spoke) responsible for CE.
• Works with BFS/TIC (Dept. of Treasury) for troubleshooting Internet issues.
• Troubleshoots compressed network infrastructure (Core/Distribution) with Cisco 7k and VDC's, and Cisco
2k (TOR)
• Supporting 2 data centers (OC3 PP connectivity) and 8 remote sites fully meshed MPLS.
• Supporting Multi-blade Cisco floor switches user data and VOIP connectivity. (Switch port configs to include
dot1q/vlan/STP). Parts include Sup 720's and line cards.
• Supporting 4xT1 VOIP PRI solution to PSTN.
• Supporting remote users (SSL VPN - Cisco ASA 55xx)
• Part of TTB team implementing VMWare NSX and micro segmentation of TTB custom applications for
security.
• Evaluates new and existing network products.
• Resolves problems with network infrastructure components and responds to suggestions for improvements
and enhancements.
• Provides network diagrams with Visio Layers 1-4.

Network Engineer

CSC/CSGov/CSRA - Arlington, VA - June 2015 to July 2016

• Full time permanent employee.
• Obtained government security clearance with Computer Sciences Corporation. Also obtained security
clearance from FDIC.
• Network Engineer assigned to internal CSC projects and FDIC client-site.
• Installation/configuration/implementation maintenance/health monitoring/troubleshooting and support of
networking Cisco equipment covering Layers 1-4 for FDIC network infrastructure to include 82 remote sites
(10mg MPLS) 9 Regional sites (100 mg MPLS) and 2 data centers to include all Cisco hardware and IOS.
• Upgraded IOS on 82 remote side Riverbed SH Wan Accelerators as well as Server Side SH (6050)
• Used bypass rules on SH's for troubleshooting FDIC applications issues (ergo FDIC-TV)
• Upgraded 82 remote sites Cisco switches and routers for new VM deployment
(hardware replacement to 3750 stack solutions / dot1q/ACL/GW/routing)
• Migrated FDIC infrastructure from Sprint to ATT responsible for Circuit turn-up with Provider (ATT) for all
sites with new Provider (new IP's/circuit testing/Multicast and BGP configurations).

Proactive monitoring of entire FDIC network infrastructure. (SolarWinds/SPLUNK/Remedy/EM7).
• Network team representative for Change Control Board.
• Worked with internal CSC to help deployment of new data centers. (RTP and Bossiere LA)

Public Trust - Computer Sciences Corporation - 2015 to 2016

Public Trust - Department of Treasury 2106- Present
Military Clearances
Secret - United States Marine Corps

Network Engineer

Experis IT   -   Tysons Corner, VA - August 2014 to February 2015

• Temporary contract position for the upgrade / cutover of SAIC remote sites.
• Network Engineer responsible for configuration / setup of Cisco 2921 and 4451 NG (next generation) routers.
• Part of SAIC's Next Generation Network Architecture team responsible for deployment of router configurations for 85 SAIC remote sites.
• Router configurations include VPLS and DMVPN connectivity for remote sites.
• Configuration to include PFR (performance routing).
• Base configuration / setup of Palo Alto FW PA-200 for management.
• Responsible for configurations of 85 SAIC remote sites.
• Responsible for VSS- 6509 and ASR 1002x maintenance in SAIC headquarters.
• Responsible for base configurations / remote installations of 85 Riverbed Steelhead CX wan acceleration appliances.

Network Engineer

Verizon Business   -   Ashburn, VA - November 2011 to June 2014

• Tier II Network Engineer responsible for Verizon Government customers.
• Managed network and security service for government / commercial clients
• Part of a 24/7/365 Network and Security Operations Center monitoring Verizon Government customers' network infrastructure.
• Supporting network infrastructure and remote connectivity for government and commercial clients through MPLS on our PIP cloud.
• CUCM management / monitoring / administration (to include Cisco Emergency Responder and Cisco Unity voice-mail).
• Day to Day issues - configurations/ changes/troubleshooting enterprise managed solutions.
• Secure Web Access Router Management to manage all of the routers/switches of our customers.
• We used TACACS to authenticate with jump boxes in place to separate the customers in domains.
• Implementing new routers / switches and replacement of same.
• Using Citrix to access and manage customers.
• Updating the Juniper IDP signatures weekly for customers, however a different group in Verizon managed them.
• Script and Implement FW changes for 2 customers, 1 commercial 1 government. FWSM in 6509's for 1 customer and Juniper ISG1000. Scripts are peer reviewed and implemented overnight during maintenance windows.
• Support of networking equipment to include Cisco high high end routers, switches, and firewalls, F5 load balancers, Bluecoat Content Filter Appliance, Juniper Firewall ISG1000. QOS implementation on routers.
• Responsible for firewall, routing changes to include scripting and implementation to include VRF's and Break/ Fixes.
• Responsible for Change and Configuration Management for customers. • Responsible for Circuit testing of customer T1 circuits using proprietary Verizon tools (ITS).

• Configuration / troubleshooting of MLFR (multi-link Frame Relay) T1's circuits • Responsible for troubleshooting of DS3 and Optical level circuits and referrals for testing. Worked closely with LEC/IXC's around the country to support customer sites.

• Worked with LEC / IXC for circuit troubleshooting at customer site to include demarc, NIU and CSU on site with CPE. Used proprietary applications for PE side.

• Responsible for reporting network status to customer on daily conference call and addressing any concerns by customer for same.

• Used TACACS+ for remote authentication to devices. Setup and used Out of Band access to sites using various modems with both router con and aux ports.

• Responsible for Security Operations Center validation of customer changes before implementation.

• Responsible for client-site and site-site (business to business) VPN connectivity troubleshooting. (Cisco 2811 /3845)

• Used HP Openview (Java) / Remedy /SMARTS and Verizon Proprietary ETMS as tools for troubleshooting/ ticketing and SNMP.

• LAN responsibilities to include VLAN changes/troubleshooting and switch port configurations and Break/ Fixes.

• Responsible for all Hands/Eyes dispatch to data centers and customer sites for troubleshooting and Break/ Fixes.

• Responsible for Cisco TAC, Juniper, Bluecoat and F5 escalations.

• Responsible for installation of all new network devices into infrastructure and turn-up.

• We take advantage and manage VRF's for 2 customers. So we can take advantage of ip allocation while virtually separating customer applications or programs as well have named for one of our government customers from remote sites on the same circuits terminating on rails in the respective data centers. All this on our MPLS cloud. Actually in some cases, VRF's helps us script firewall changes.

• We also have enabled access on not only the CE but provider edge routers as well.

Public Trust - Verizon - 2011 to 2014

Network Engineer
US Courts / AT&T   -   Oakton, VA - August 2010 to September 2011

• Tier II CSOC (Customer Service Operations Center) in the US Courts NOC. Provided 1st and 2nd level support for the US Courts infrastructure. Full time employee for GTSI contracted to AT&T for US Courts.

• Supported over 1000 remote sites and 3000 circuits in a multi-enterprise environment. Data aggregated through major data centers located strategically in the US. AT&T used several types of proprietary vpn solutions for security. Troubleshot remotely and dispatched major hardware vendors and ATT accordingly for support, circuit troubleshooting /testing, hardware troubleshooting and configuration.

• Performed in depth troubleshooting of routers/switches as well as resolutions

• Supported LAN / WAN and associated network infrastructure at the respective sites.

• Part of NOC team responsible for migration of all sites and circuits from Sprint to AT&T for implementation.

• Supported Cisco 28xx/38xx/72xx routers and Cisco 35xx / 65xx switches and IOS.

• Worked with LEC / IXC for circuit troubleshooting at customer site to include demarc, NIU and CSU on site with CPE. Used proprietary applications for PE side.

• Used "VitalNet" as a front end application for Netflow stats on customer circuits. Also used ip flow cache on routers for determining performance and utilization issues (top talkers)

• MLPPP was used for bundling T1's at the majority of sites. Configured circuits for same and segregated circuits from bundles for troubleshooting and testing (intrusive). 35% of sites had fractional T3 connectivity.

• Worked with remote site POC's (point of contacts) at T3 sites to perform head- to - head testing / troubleshooting.

• Used TACACS+ for remote authentication to devices. Setup and used Out of Band access to sites using various modems with both router con and aux ports.

• Provided RFO (reason for outage) to upper management for all Severity 1 outages. Also provided timeline and solution for same.
• Monitored / troubleshot circuits at data centers as well to include OC speeds. • Worked closely with SOC (security) to troubleshoot network issues (i.e proxies, Bluecoat 404 /503 errors, latency and utilization issues)

Public Trust - US Courts - 2010 to 2011

Civilian Government Clearances - 2006 to 2008

EDUCATION

BS in Computer Science
University of Maryland
2018