

**Network Engineer**

**Vinay**

**Contact: 469-898-0219**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Professional Summary:**

* Overall 10+ years of experience, on networking in-depth knowledge and experience in network architecture, network design, implementation, and support.
* Successful in resolving Routing, Switching and WAN connectivity escalation issues using various ticketing tools.
* Thorough experience in OSI model, TCP/IP, UDP, IPv4/IPv6 sub netting, NAT concepts.
* Expertise in configuring OSPF, BGP and MPLS protocols.
* Proficient in configuring WLAN, VLAN, VLAN Trucking Protocol (VTP), Dynamic Trucking Protocol (DTP), Spanning Tree Protocol (STP), RSTP, and PVST.
* Worked on configuring Juniper MX960, M320, T640, & 3600, 4500, 6500 Cisco Switch series
* Exposure in working on Layer 2 Routing Protocol Configurations as ARP, RARP, and deployment of VPNs over IPsec and GRE.
* Proficient in Cisco IOS installation, Upgradation and configuring, troubleshooting routing protocols like OSPF, BGP (E-BGP, I-BGP).
* Good knowledge and experience in Installation, Configuration and Administration of Windows Servers 2000/2003, Active Directory, FTP, DNS, DHCP, TFTP, Linux OS under various LAN and WAN environments.
* Strong hands-on experience and knowledge of Software Defined WAN (SDWAN).
* Good knowledge in configuration of Voice VLAN’s (VOIP), prioritizing the voice traffic over the data traffic.
* Expertise in diverse on main technologies like Insurance, Ecommerce &Media.
* Tested hardware and software functionality regularly.
* Backed up network regularly & implemented disaster recovery options when needed.
* Diagnosed and resolved hardware and software and networking issues.
* Replaced the hardware when needed.
* Implemented and monitored network security measures including data protection, secured email configuration, and malware spyware and viral protection.
* Effective oral, written communication skills and strong analytical problem-solving capabilities.
* Expertise in troubleshooting and configuring DNS, DHCP, TFTP, TELNET, SSH, FTP and NFS
* Excellent hands-on experience in designing and implementing IP addressing that includes both IPV4and IPV6
* Implementation of Access lists, route maps, and distribute lists.
* Managed and maintained IAM systems, ensuring proper user access controls and adherence to security policies.
* Conducted regular network audits and vulnerability assessments to identify and mitigate security risks.
* Strong fundamental knowledge in implementing Layer-2 level technologies including VLAN's, VTP, STP, RSTP and Trucking.
* Utilize the OSI model as a guide for systematic network troubleshooting.
* Performed LAN, WAN, WLAN and VLAN troubleshooting.
* Design/Implementation and troubleshooting of Cisco Unified Communication.
* Troubleshooting and Maintenance of IPSLA Routers and Voice Gateways.
* Experience in LAN, WLAN, WAN Networking, specifically on Cisco Platform, and to some extent in Juniper.
* Extreme LAN technology. Design expertise in VoIP networks ON Cisco and Nortel interpretability.
* SolarWinds Network Configuration Manager (NCM) to automate and simplify network configuration tasks, ensuring consistency and compliance across the network.
* Conducted performance analysis using SolarWinds reporting and historical data to identify network bottlenecks and optimize resource utilization.
* Designed and configured VoIP networks, including SIP trunks, gateways, and IP-PBX systems, ensuring optimal performance and reliability.
* Provided tier-3 technical support for VoIP systems, diagnosing and resolving complex issues related to call quality, connectivity, and configuration.
* Conducted root cause analysis of VoIP-related incidents, implemented corrective actions, and documented solutions.

**Core Competencies**

|  |  |
| --- | --- |
| **Tool Knowledge** | **Ticketing**-Service Now.  **Remote Tools-** RDP (Remote Desktop), VNC, Log MeIn, PC anywhere, Team Viewer **Other–** Cisco Packet Tracer, TCP dump, GNS3, Putty. |
| **Routers** | CISCO Routers series–2600,2800,3600,3800,7200,7600 |
| **Switching** | CISCOSwitches-2960,3750,3560,4500,6500series  Firewall Security–Cisco ASA, Check point IP sec, SSL-VPN, Windows Patch Management (WSUS), NAT, PAT |
| **Network Routing**  **Knowledge** | FTP, DHCP, DNS, OSPF, EIGRP, IGRP, BGP, RIP, TCP/IP, Static Routing, VLAN,  STP, VTP, Ether channel |
| **WAN Exposure** | Frame Relay, HDLC, ISDN, PPP, MPLS |
| **Server Operating systems** | Microsoft Windows NT,2000,2003,2008,2008R2,2012, RedHatLinuxES  7/6.7/5/4, Citrix environment servers |
| **Server Models** | Domain servers, Mail Servers, Proxy Servers, Print Servers, Application Servers,  FTP Servers |
| **Wireless Technologies** | Canopy Wireless interface, D-Link Access Point, Linksys Wireless |
| **Webservers** | Apache-tom cat and Apache HTTP Server, VMware, Web Sphere |

**Client Name: AT&T (Middletown NJ) May 2020 to Present**

**Network Engineer/Administrator**

**Responsibilities:**

* Certification testing of next generation core routers, edge routers, route reflectors, network management and connectivity for Global network (GCBB) network, Layer3 IP transport and security validation, Layer3/Layer2 integrated networks and capacity enhancements in a controlled simulated lab environment.
* Layer3 Data plane Certification using various networking protocols.
* Designed, implemented, and maintained Zero Trust architecture to enhance network security and mitigate risks.
* Conducted network assessments and audits to ensure compliance with Zero Trust principles and industry best practices.
* Collaborated with cross-functional teams to integrate Zero Trust principles into network infrastructure and cloud environments.
* Layer3 Control plane Certification using various networking protocols.
* Worked on QOS testing on customer side interface and verified the flows on the router.
* Worked on Hub & spoke and Route Group and verified flows on the router.
* Layer3 Microservices certification for finished goods automation and deployment.
* Certification testing of network automation tools. Generating test plan and testcases based on design documents - NDR and CCR from system engineering.
* Executing the test cases to certify functional and features as defined in NDR and CCR.
* Authoring test plans and documenting test results.
* Performing hardware installation and turn-up. Generate data traffic using test sets & validating end-to-end connectivity and data flows.
* Create trouble tickets using tools to resolve lab certification issues, authoring installation/turn-up procedure to support field deployment.
* Collaborating with system engineer to perform design validation.
* Experience in network monitoring tools and testing tools such as Wire shark, cisco works and IXIA.
* Collaborating with teams to generate Method of Operating Procedure (MOP) to implement the certified features in the US and Most of World (Mow) networks.
* Assisting field personnel to troubleshoot and performing root-cause analysis of problems found in production network.
* Interfacing with different vendor technical teams to resolve problems found in lab testing. Performing and managing IP address allocation for lab certification.
* Collaborating with IT personnel to assist Business System certification and regression tests.
* Working in lab environments, predominately Linux based.
* Upgrading Cisco OS on Cisco devices, installing SMU, Upgrading JSU on juniper devices Junos installation has per the requirement and testing.
* Configuring BGP with unicast and Label unicast. Testing if routes are being advertised properly to the device.
* Performing hardware installation and turn-up. Cabling and Labeling as the testing.
* Generate data traffic using test sets IXIA, SPIRENT validating end to end connectivity and data flows.
* Successfully implemented Cisco ACI to automate and streamline data center network operations.
* Utilized ACI's policy-based automation features to simplify network provisioning and configuration tasks.
* Automated repetitive tasks, reducing deployment times and minimizing the risk of errors.
* Implemented security policies within the ACI fabric, including micro-segmentation and access controls.
* Worked on the implementation of security groups and policies to enhance network security.
* Worked on Drivnets device for SD Network Multilayer Controller using Cisco Routers.
* Implemented ASA security policies, access control lists (ACLs), and VPN configurations to control network traffic, enforce security policies.
* Configured firewall policies, access control lists (ACLs), and security zones to enforce granular security controls and restrict network traffic based on application, protocol, and user identity.
* Implemented multi-factor authentication (MFA) and certificate-based authentication to enhance VPN security and mitigate unauthorized access risks.
* Generated firewall log reports, analyzed security events, and responded to security incidents in a timely manner to mitigate risks and maintain regulatory.
* Configured firewall load balancing and active-passive failover mechanisms to seamlessly transition traffic between redundant firewalls.
* Established site-to-site VPNs and remote access VPNs using IPsec, SSL/TLS, or other encryption protocols to provide secure connectivity for remote. Configured VPN tunnels, encryption parameters, authentication methods, and VPN routing policies on FortiGate firewalls.
* Integrated Fortinet firewalls with other security technologies such as SIEM (Security Information and Event Management) systems, endpoint protection solutions, and threat intelligence feeds.
* Configuration and Deployment: Designed and implemented Palo Alto Networks firewall solutions to secure corporate networks, including hardware selection, network topology design, and software configuration.
* Integration with Security Ecosystem: Integrated Palo Alto firewalls with SIEM systems, endpoint protection solutions, and threat intelligence platforms to enhance threat detection and response capabilities.
* Performance Optimization: Optimized Palo Alto firewall performance through traffic profiling, load balancing, and resource allocation, improving throughput and network resilience.
* Rule Management: Managed security policies, rules, and objects within Palo Alto firewalls to enforce network segmentation, application control, and threat prevention strategies.
* Implemented and configured AWS networking services such as Amazon Route 53 for DNS management.
* Designed and implemented AWS VPCs to isolate and securely connect AWS resources, ensuring network segmentation and compliance with security.
* Configured VPC subnets, route tables, internet gateways, NAT gateways, and VPC peering connections to establish connectivity between on-premises infrastructure and AWS cloud resources.
* Implemented AWS CloudWatch for monitoring network performance metrics, such as network traffic, latency, and packet loss, and set up alarms for proactive alerting.
* Configured and deployed SolarWinds Network Performance Monitor (NPM) to monitor network devices, interfaces, and traffic metrics in real-time.
* Configured alerting thresholds and notifications in SolarWinds to proactively detect and respond to network issues, outages, and performance degradations.
* Integrated SolarWinds Application Performance Monitor (APM) to monitor and analyze application performance, transaction latency, and user experience.
* Deployed and configured DHCP servers on various platforms, including Windows Server, Linux, and network devices such as routers and switches.
* Configured DHCP relay agents on routers or Layer 3 switches to forward DHCP messages between clients and remote DHCP servers in different subnets or VLANs.
* Deployed and managed Zscaler Internet Access (ZIA) for secure internet gateway (SIG) services, including web filtering, SSL inspection, and threat protection.
* Configured and maintained Zscaler Private Access (ZPA) for zero-trust network access, enabling secure access to applications regardless of user location.
* Implemented Zscaler Cloud Firewall policies to enforce network security and control access to cloud-based resources.
* Configured VNet peering and virtual network gateways to establish connectivity between Azure VNets and on-premises networks.
* Defined and configured IP address ranges, subnets, and network security groups (NSGs) within Azure VNets to segment and secure network traffic.
* Implemented address spaces, subnet masks, and CIDR notation to optimize IP address allocation and subnetting strategies.
* Deployed Azure Firewall to secure inbound and outbound traffic to Azure resources and enforce network security policies.
* Implemented security measures to protect wireless networks from unauthorized access and attacks.
* Designed and implemented wireless network architectures for small, medium, and large-scale deployments.
* Implemented network monitoring tools and techniques to proactively monitor wireless network performance, utilization, and security.
* Implemented load balancing algorithms such as round-robin, least connections, or weighted round-robin to optimize traffic distribution based on server capacity and availability.
* Developed and implemented Windows device drivers for various hardware components, including but not limited to network adapters, graphics cards, audio devices, and storage controllers.
* Utilized SD-WAN management interfaces and APIs to automate provisioning, configuration, and monitoring tasks, reducing manual effort.
* Configuring firewall rules, access control lists (ACLs), security zones, and NAT (Network Address Translation) policies to control traffic flow and protect against unauthorized access and cyber threats.
* Configuring and tuning intrusion prevention system (IPS) policies to detect and block network-based attacks, exploits, and vulnerabilities in real-time.
* Monitoring security events, alerts, and logs generated by Cisco FTD devices using SIEM (Security Information and Event Management) tools and security analytics platforms
* Enabling and tuning intrusion prevention system (IPS) features on Cisco ASA devices to detect and block network-based attacks, exploits, and vulnerabilities in real-time.
* Integrating Cisco ASA with advanced malware protection (AMP) solutions to provide comprehensive threat detection, sandboxing, and file reputation analysis capabilities.
* Developed and implemented security policies, access control rules, and authentication protocols on Cisco ISE to enforce network access policies and compliance requirements.
* Deployed and configured self-registration portals and guest access workflows on Cisco ISE to provide secure and streamlined onboarding for guest users and devices.
* Implemented load balancing algorithms such as Round Robin, Least Connections, and Weighted Least Connections to achieve optimal resource utilization and performance.
* Implemented health monitors, failover triggers, and synchronization mechanisms to maintain session persistence and data integrity across redundant load balancer instances.
* Implemented SSL profiles, cipher suites, and certificate management policies to ensure secure communication.
* Configured F5 GTM (Global Traffic Manager) to perform DNS-based load balancing and global server load balancing (GSLB) across geographically dispersed data centers and cloud regions.
* Designed, deployed, and configured Wi-Fi 5 networks for enterprise, campus, or public environments to provide high-speed wireless connectivity to users and devices.
* Configured Wi-Fi 5 access points (APs) with optimal settings, including channel selection, transmit power levels, and antenna configurations, to minimize interference and maximize coverage.
* Implemented Wi-Fi 5 security features such as WPA2-Enterprise or WPA3 encryption, 802.1X authentication, and captive portal authentication to protect wireless networks.
* Implemented Layer 3 routing on Cisco Catalyst switches using features such as SVI (Switched Virtual Interface), VLAN routing, and static routing to enable inter-VLAN communication and route traffic between network segments.
* Configured QoS policies on Cisco Catalyst switches to prioritize critical traffic flows, such as voice or video, over best-effort traffic and ensure optimal performance for latency-sensitive applications.

**Client Name: Sercomm Corporation (Fremont CA) Sep 2016 to Apr 2020 Network Engineer/Administrator**

**Responsibilities:**

* Hands on experience with the configuration and implementation of various Cisco Routers and L2 Switches.
* Configuring IP address, providing static routes, authentication, creating VLAN'S, providing inter VLAN routing, trunk ports 802.1q tagging, assigning Spanning tree to VLAN'S, configuring SNMP.
* Supported core network consisting of Cisco7200 series routers running multi area OSPF.
* Configuration of EIGRP and OSPF as interior gate way protocol with route filtering and route redistribution.
* Implemented stub/Totally stub areas and various OSPF features like route-summarization and SPF throttling.
* Single point of contact for VLANs, Virtual port channel (VPC) and configuration on Nexus7k.
* Responsible for service request tickets generated by the help desk such as troubleshooting, maintenance, upgrades, patches, and fixes with all around technical support.
* Supporting EIGRP and BGP for problems of L2/L3 in internal teams & external customers.
* Providing daily network support for national wide area network consisting of MPLS, VPN and point-to point site.
* Upgrading Used DHCP to automatically assign reusable IP addresses to DHCP clients.
* Negotiate VPN tunnels using IPsec encryption standards and configured and implemented site-to-site VPN, Remote VPN.
* Configuring STP for switching loop prevention and VLANs for data and voice along with Configuring port security for users connecting to the switches.
* Worked on commissioning and decommissioning of the MPLS circuits for various field offices.
* Network Cabling, dressing, labeling, and troubleshooting various network drops onsite.
* Assisted with deployment of various network devices and services, including SD-WAN, Load Balancers, Cisco routers, switches & firewalls.
* worked on migration project from traditional data center to spine Leaf.
* Developed infrastructure as code using AWS CloudFormation and Terraform, automating deployment processes and ensuring consistency across environments.
* Implemented security best practices on AWS, including IAM policies, encryption at rest and in transit, and VPC configurations, to ensure compliance with industry standards and regulations.
* Monitored and optimized AWS environments using CloudWatch, CloudTrail, and other monitoring tools, identifying and addressing performance bottlenecks and cost inefficiencies.
* Developed infrastructure as code using AWS CloudFormation and Terraform, automating deployment processes and ensuring consistency across environments.
* Monitored DHCP server performance, utilization, and lease status using monitoring tools or built-in DHCP management consoles.
* Optimized DNS server settings, caching, and TTL (Time-To-Live) values to improve DNS query performance, reduce latency, and enhance DNS resolution speed.
* Integrated Zscaler with identity providers such as Azure AD and Okta for user authentication and single sign-on (SSO) capabilities.
* Conducted threat analysis and incident response using Zscaler's advanced security features, including sandboxing and threat intelligence.
* Developed and implemented patch testing procedures to evaluate the compatibility, stability, and performance impact of Windows patches on diverse hardware and software configurations.
* Generated compliance reports and executive summaries to communicate patch management effectiveness, security posture, and risk mitigation efforts to stakeholders and management.
* Used Visio to document and visualize IT infrastructure components, including servers, switches, routers, and network connections.
* Integrated Visio diagrams and project plans with other Microsoft Office applications, such as Excel and Project, for seamless project management and reporting.
* Maintained and updated desktop images on a regular basis to incorporate software updates, patches, and new application releases.
* Conducted compatibility testing of desktop images with hardware platforms, device drivers, and peripheral devices to ensure seamless deployment and functionality.
* Documented desktop imaging procedures, workflows, and best practices to create comprehensive documentation and knowledge base resources for IT staff and end-users.

**Environment:** Cisco2990/3550 switches, Cisco7200/3845/3600/2800routers, EIGRP, RIP, OSPF, BGP, VPN, Ether Channels, and Sniffer, Data center.

**R2 Technologies, India May 2012 to May 2015**

**Network Engineer**

**Responsibilities:**

* Configured Cisco Routers for OSPF, IGRP, RIPv2, EIGRP, Static and default route.
* Worked on HSRP for ho redundancy and load balancing.
* Configured the Cisco router as IP Firewall and for NATing Configured RSTP, MST and used VTP with802.1q trunk encapsulation.
* Designed ACLs, VLANs, troubleshooting IP addressing issues and taking back up of the configurations on switches and routers.
* Provided testing for network connectivity before and after installation/upgrade.
* Switching related tasks included implementing VLANS and configuring ISL trunk on Fast-Ethernet and Gigabit Ethernet channel between switches.
* Experience in Cisco switches and routers: Physical cabling, IP addressing, Wide Area Network configurations.
* Performed troubleshooting, while maintaining trouble ticket tracking, following internal/external.
* Basic Knowledge on HSRP.

**Environment:** Cisco Routers 2900, 2600, 3600; Cisco Switches1900, 2900, 3500, 3700and450Series; LAN/WAN: Frame relay, NAT, DHCP, TCP/IP