

SANDEEP GUVVALA

Network Engineer

Montgomery, AL | sandeep@careerattainment.com | +1 (773) 684-4649



SUMMARY

Network Engineer with 4+ years of experience supporting enterprise environments using Cisco Catalyst, Cisco Nexus, ISR/ASR routers, and Juniper switches, with strong capability in OSPF, EIGRP, BGP, STP variants, VLANs, and subnetting. Skilled in securing networks through Palo Alto and Fortinet firewalls, IPSec/SSL VPNs, authentication controls, and traffic management. Experienced in troubleshooting with Wireshark, monitoring with SolarWinds and CloudWatch, and working with AWS, Docker, and Kubernetes for cloud and containerized networking. Adept at creating network documentation, maintaining configuration standards, coordinating with vendors, and improving reliability through redundancy and incident resolution.

TECHNICAL SKILLS

Networking Fundamentals:	OSI Model, TCP/IP, routing & switching concepts, VLANs, subnetting, network troubleshooting
Switching Equipment & Protocols:	Cisco Catalyst Series, Cisco Nexus Series, Juniper switches, Multi-Layer Switching (MLS), STP, PVST, MST, VTP, Inter-VLAN routing, VPC, VSS
Routing Equipment & Protocols:	Cisco ISR & ASR routers, Cisco Gateways, OSPF, EIGRP, BGP, HSRP/VRRP, static routing, load balancing
Network Protocols:	TCP/IP, ARP, ICMP, NAT, PAT, DNS, DHCP, HTTP/HTTPS, SNMP, NTP, SSH
Network Security:	Palo Alto Firewalls, Fortinet Firewalls, VPNs (IPSec/SSL), IDS/IPS, Zero Trust Architecture, access control & authentication
Monitoring & Reliability:	Wireshark, SolarWinds, AWS CloudWatch, disaster recovery planning, auto-configuration servers
Cloud & Virtualization:	AWS, Cloud Networking, Docker, Kubernetes
Architecture & Operations:	Network design, vendor management, documentation & diagrams, SOPs, incident reporting

PROFESSIONAL EXPERIENCE

Network Engineer | HCL Tech, USA

| Jul 2024 – Present

- Architected hybrid cloud gateway infrastructure connecting 15 data centers across AWS, Azure, and GCP using Cisco ISR/ASR routers with BGP multi-cloud routing, achieving 99.99% uptime and sub-100ms inter-cloud latency across 5 availability zones.
- Designed zero-trust security framework at cloud entry points using Palo Alto firewalls with IDS/IPS and HSRP-based redundancy, implementing granular access control policies that reduced unauthorized access attempts by 87% while maintaining SOC2 compliance.
- Optimized network architecture through Multi-Layer Switching on Cisco Nexus Series switches with PVST optimization, enabled inter-VLAN routing with VPC peering and OSI model segmentation, improving application response time by 34% across 3 cloud providers.
- Implemented OSPF and static routing protocols with VLAN segmentation and subnetting strategy for hybrid cloud networks, reducing broadcast domains by 65% and enhancing network troubleshooting efficiency across all regions.
- Automated cloud resource provisioning through infrastructure-as-code frameworks with auto-configuration servers and SOP documentation, reducing gateway provisioning time from 8 hours to 45 minutes and enabling 1200+ cloud instance scaling.
- Established end-to-end monitoring using AWS CloudWatch and SolarWinds with SNMP traps and SSH management access, achieving 99.2% first-contact incident resolution with comprehensive network documentation and disaster recovery planning.
- Deployed IPSec VPN tunnels with NTP synchronization and DHCP management, established 2-hour RTO disaster recovery procedures, managed Cisco, Palo Alto and AWS vendor relationships, and containerized deployment using Docker.

Network Engineer | Lumen Technologies, India

| Dec 2019 – Jul 2022

- Engineered enterprise-scale VPN mesh supporting 10,000+ concurrent remote users across 6 continents with redundant IPSec and SSL-VPN tunnels, leveraging VRRP-based failover mechanisms maintaining sub-50ms latency for 6,000+ concurrent sessions.
- Strengthened enterprise security by deploying Fortinet Firewalls with IDS/IPS threat prevention, implemented hardware token MFA and zero-trust authentication frameworks with dynamic role-based policy updates, reducing security audit findings by 76% achieving HIPAA compliance.
- Configured switching infrastructure using Juniper switches with VSS clustering and Multi-Layer Switching for intelligent VPN traffic classification, deployed VLAN-based segmentation aligned with OSI layers and MST optimization, handling 850 Gbps daily traffic across 4 regional hub sites.
- Built network resilience through comprehensive disaster recovery planning with failover procedures for 12 VPN gateway pairs, implemented sub-30-second failure detection and incident reporting workflows, improving MTTR from 90 minutes to 35 minutes.
- Deployed Wireshark packet analysis for troubleshooting and baseline establishment, integrated SNMP monitoring with AWS CloudWatch dashboards across 500+ VPN endpoints, reducing tunnel diagnosis time by 64% enabling faster issue resolution.
- Ensured regulatory compliance across VPN operations by enforcing TCP/IP encryption standards, implementing PAT for traffic masking, configuring SSH management protocols, and maintaining comprehensive documentation passing HIPAA/SOC2 audits with zero findings.
- Optimized routing intelligence by deploying EIGRP and BGP protocols for multi-path routing optimization, implemented traffic-aware load balancing algorithms distributing sessions across 28 VPN gateways with intelligent session affinity management.
- Developed comprehensive network design documentation and SOP frameworks for tunnel provisioning and MFA onboarding, trained 12 network administrators on DNS configuration, ICMP troubleshooting, ARP protocol handling, and Kubernetes scaling, reducing onboarding from 6 weeks to 3 weeks with 89% knowledge retention.

EDUCATION

Masters in Computer Science | Auburn University at Montgomery – Montgomery, AL

| Jan 2023 - May 2024

CERTIFICATION

Certificate: Cisco Certified Network Associate (CCNA) – CISCO