

Likhitha CH

Champaign, Illinois, United States | likhithach1516@gmail.com | (217) 790-7604

PROFESSIONAL SUMMARY

4+ years of experience in network engineering, specializing in the design, implementation, and management of complex network systems. Strong expertise in network troubleshooting, performance and security management for large-scale environments. Proven ability to manage and configure routers, switches, and firewalls to ensure high availability and network efficiency. Hands-on experience in network monitoring tools and performance analysis to identify and resolve potential issues proactively. Expertise in implementing VLANs, VPNs, WAN optimization, and load balancing to enhance network performance and security. Proficient in TCP/IP, DNS, DHCP, and other essential network protocols and extensive knowledge of routing protocols like OSPF, EIGRP, BGP) and switching protocols like STP, VTP. Experience in network security practices, including firewall configurations, VPN setup, and intrusion detection systems (IDS/IPS) and skilled in network automation and scripting using tools like Python, Ansible, and Cisco Prime. Familiar with cloud networking solutions, including integration with AWS, Azure, and Google Cloud platforms. Hands-on experience with Cisco, Juniper, and Huawei devices for routing, switching, and security. Knowledge of data centre networking and SDN (Software-Defined Networking) technologies. Expertise in implementing network virtualization technologies like VMware NSX and Cisco ACI and Proficient in configuring and managing IPsec, SSL VPNs, and MPLS networks for secure data transmission. Experience with network automation platforms such as Cisco DNA Centre and Juniper Contrail. Familiarity with network traffic analysis tools like Wireshark, NetFlow, and SolarWinds for in-depth network performance monitoring.

EDUCATION

Eastern Illinois University

Masters, *Computers Systems Technology*

SKILLS

Technical Skills: Networking & Protocols: LAN/WAN, OSPF, EIGRP, BGP, VLAN, STP, VTP., Network Security: Cisco, FortiGate, IPsec, SSL, ACLs, IDS/IPS., Cloud & Virtualization: AWS, Azure, Google Cloud, VMware NSX, Cisco ACI, cloud server environments., Automation & Monitoring: Python, Ansible, PowerShell, SolarWinds, PRTG, Wireshark, NetFlow, SNMP, Zabbix, Nagios., Wireless Networking: Wi-Fi setup (802.11ac, 802.11ax), Wireless security (WPA2, WPA3)., Performance Optimization: Riverbed, Cisco WAAS, F5, Citrix., Other Skills: VoIP and SIP, DNS, DHCP., Operating Systems & Platforms: Router & Switch configurations (Cisco, Juniper, Huawei), iptables, NFS, SSH, Active Directory, DNS, DHCP, Windows and Linux servers., Endpoint Support: Desktops, laptops, Android/iOS devices, Zebra printers, Level 1/2 support.

Collaboration & Voice: Cisco CUCM, Avaya, Microsoft Teams, Skype, Cisco Webex, Zoom.

Security & Compliance: DDoS, SIEM, SSL/TLS, IPsec Tunnel.

Automation & Configuration Management: Git, CI/CD, Terraform, Salt Stack.

Network Performance & Troubleshooting: Jitter, Latency, BGP Route Maps, tcpdump, Wireshark, Tshark.

Advanced Networking: MPLS, VRRP, LACP, EtherChannel, VPN, HSRP and GLBP, BFD.

TCP/IP Networking Skills: TCP/IP Stack, IPv4, IPv6, Subnetting, ARP, DNS, DHCP, ICMP, NAT, TCP Flags

WORK EXPERIENCE

Cisco Systems | Senior Network Security Engineer

Feb 2026 - Present

- Provided Level 1/2 support for desktops, laptops, and Android/iOS devices across the enterprise, resolving workstation and software issues including installation, upgrade, and maintenance of systems while documenting troubleshooting procedures for end-user knowledge bases.
- Designed, implemented, and supported enterprise-grade network security solutions using Cisco Catalyst, Cisco Nexus, Cisco ASA, Cisco Firepower, and F5 Load Balancers, ensuring high availability and secure architecture.
- Deployed and optimized Routers, Switches, LAN/WAN, and Data Center Networks to deliver scalable enterprise connectivity, configuring and troubleshooting VPNs, switches, routers, firewalls, and wireless access points.
- Configured and maintained VLANs, VRFs, MPLS, IPsec VPN, and DMVPN tunnels for secure multi-site and hybrid connectivity.
- Monitored network performance using Cisco DNA Center, Cisco Prime Infrastructure, SolarWinds, NetFlow, and Wireshark to troubleshoot latency, packet loss, and throughput issues.
- Implemented advanced security controls including Cisco Firepower Threat Defense (FTD), Cisco ISE, IDS/IPS, Zero Trust Architecture, and Network Segmentation to mitigate cyber threats and DDoS attacks.
- Integrated on-prem infrastructure with AWS, Microsoft Azure, and Hybrid Cloud Networking solutions using secure VPN Gateways and SD-WAN connectivity, managing physical, virtual, and cloud server environments.
- Automated network provisioning and compliance validation using Python, Ansible, REST APIs, and Cisco DNA Automation, reducing manual configuration efforts.
- Deployed and managed Cisco SD-WAN (Viptela) to optimize application-aware routing and improve WAN performance across distributed environments.
- Enforced enterprise security compliance through Access Control Lists (ACLs), Encryption Protocols, AAA, RADIUS/TACACS+, and centralized logging.
- Supported enterprise collaboration platforms including Cisco Webex, VoIP, SIP Gateways, and Unified Communications (UC) infrastructure.
- Configured dynamic routing protocols such as BGP, OSPF, and EIGRP, along with high-availability technologies including HSRP, VRRP, and EtherChannel.
- Provided 24/7 operational support, troubleshooting complex network incidents using Packet Capture, Traceroute, tcpdump, and ELK Stack, while coordinating with Cisco TAC for critical escalations.

T-Mobile | Network Engineer

Mar 2025 - Jan 2026

- Provided Level 1/2 support for desktops, laptops, and Android/iOS devices across carrier-grade infrastructure, guiding associates in day-to-day operational processes and resolving workstation and software issues including installation, upgrade, and maintenance of systems.
- Managed and optimized carrier-grade network infrastructure across regional data centers and cell site backhaul networks, ensuring high availability, security, and performance for 4G LTE and 5G services using routers, switches, and firewalls while supporting seamless voice and data services for enterprise and retail customers.
- Designed and deployed scalable LAN/WAN and MPLS backbone architectures to support interconnectivity between core network sites, regional hubs, and mobile switching centers (MSCs).
- Implemented secure IPSec and SSL VPN solutions to enable encrypted connectivity for remote engineers, NOC teams, and enterprise clients while maintaining telecom compliance and security standards.
- Automated network provisioning and configuration using Ansible, Cisco DNA Center, and Python scripts, reducing manual errors and accelerating rollout of configuration updates across distributed telecom infrastructure.
- Monitored and troubleshoot network performance using SolarWinds, Wireshark, Nagios, and SNMP tools, ensuring minimal downtime and optimal performance for subscriber voice, data, and messaging services.
- Collaborated with the cybersecurity team to implement advanced firewall policies, DDoS mitigation strategies, and access control mechanisms, aligning with telecom security frameworks and industry best practices.
- Utilized SD-WAN technologies to optimize WAN connectivity for enterprise mobility customers and branch connectivity, improving application performance and network resiliency.
- Deployed and managed Cisco Meraki wireless solutions for enterprise mobility clients, ensuring secure and high-performance Wi-Fi connectivity integrated with carrier backbone services.
- Conducted in-depth traffic analysis using NetFlow and sFlow, implementing QoS policies to prioritize latency-sensitive traffic such as VoLTE, video conferencing, and real-time applications.
- Managed DNS, DHCP, and IP address management (IPAM) services to ensure efficient internal and customer-facing service resolution and deployed Fortinet firewalls with UTM features to provide multi-layered network protection.
- Leveraged VMware NSX for network virtualization and micro-segmentation within telecom data centers and implemented RADIUS and TACACS+ for centralized authentication and secure administrative access control.
- Configured Elastic Stack (ELK) and Zabbix, integrating with Slack and PagerDuty for real-time monitoring and incident response, while automating health checks and compliance reporting using PowerShell and Python, reducing MTTR across telecom operations.

Sanofi India | Network Engineer

Apr 2022 - Jul 2024

- Provided Level 1/2 support for desktops, laptops, and Android/iOS devices across manufacturing plants, R&D labs, and corporate offices, resolving workstation and software issues including installation, upgrade, and maintenance of systems.
- Utilized Cisco DNA Center for automating network configuration management, streamlining deployment processes, and reducing manual errors across manufacturing plants, R&D labs, and corporate offices. Deployed and managed Wi-Fi 6 solutions to enhance secure wireless connectivity across production floors, laboratories, and enterprise environments, ensuring seamless access for research scientists and operational teams.
- Implemented VLAN segmentation to optimize traffic flow, strengthen network security, and isolate critical environments such as manufacturing systems, quality control labs, and enterprise IT networks.
- Applied Quality of Service (QoS) policies to prioritize latency-sensitive applications including ERP systems, clinical research platforms, and real-time production monitoring systems.
- Integrated IoT-enabled manufacturing devices and lab equipment into the corporate network to enable real-time monitoring of production metrics and operational performance, and deployed Cisco Unified Communications Manager (CUCM) to enhance collaboration across regional and global teams.
- Implemented IPSec tunneling to secure sensitive pharmaceutical data between branch offices, manufacturing facilities, and data centers, while leading firmware upgrades and server patch management initiatives to maintain secure and compliant network operations.
- Configured and maintained 802.1X Network Access Control (NAC) to prevent unauthorized device access, integrated disaster recovery solutions using cloud-based backups and replication technologies, and utilized Amazon CloudWatch for real-time cloud infrastructure monitoring.
- Implemented Active Directory (AD) integration with network devices to centralize authentication and role-based access control, and optimized WAN performance using Riverbed WAN optimization to enhance application delivery for global operations.
- Created and maintained detailed network topology diagrams using visualization tools to improve troubleshooting efficiency, capacity planning, and infrastructure scalability.
- Integrated Big Data and analytics platforms (Hadoop ecosystem) within secure network environments to support large-scale pharmaceutical data processing, research analytics, and regulatory reporting requirements.

CERTIFICATIONS & ACHIEVEMENTS

- Cisco Certified Network Associate (CCNA) - Cisco
- Cisco Certified Network Professional (CCNP)-R&S - Cisco
- Cisco Certified Network Professional (CCNP)- Security - Cisco
- Cisco Firewall Security Specialist - Cisco
- PCNSE