

Sumanth Ravi

Kirkland, Washington, United States | rsumanth1998@gmail.com | (501) 436-9474 | [linkedin.com/in/sumanth-ravi](https://www.linkedin.com/in/sumanth-ravi)

PROFESSIONAL SUMMARY

IT support and network engineer with 4+ years delivering Level 1/2 support across LAN/WAN, VPN, wireless, and endpoint environments, with hands-on experience in ServiceNow, Jira, Remedy, SolarWinds, Splunk, Azure AD, and Microsoft 365. Strong foundation in IT operations including **incident management** and **change management**, plus documentation and troubleshooting playbooks that improve response time and onboarding. Experienced administering Linux systems and supporting identity/access workflows (onboarding/offboarding, MFA, permissions) in Azure and Windows Active Directory. Known for improving uptime (+27%) and incident response speed (+20%) through monitoring, root-cause troubleshooting, and process improvement.

EDUCATION

Northeastern University

Master of science, *Cybersecurity*

Sep 2019 - May 2021

Sreenidhi Institute of Science and Technology

Bachelor of Technology, *Information Technology*

Aug 2015 - May 2019

SKILLS

Tools & Software: Nexus Switches, ServiceNow, Jira, Remedy, Network Administration, Network Security, Cisco Networking, Cisco ACI, Cisco Meraki, Wireless, Aruba, Aruba SD wan, SolarWinds, Net MRI, Wireshark, Infoblox, Splunk, VPN (IPsec/SSL), Firewalls (Palo Alto, FortiGate, Cisco ASA), Routing & Switching (BGP, OSPF, EIGRP, STP), Azure AD, Windows Active Directory, Microsoft 365 (O365, Exchange, Intune, Teams, SharePoint, OneDrive), Remote Desktop Support, Endpoint Security, Web Content Filtering, System/Software Security Compliance, ITIL (familiarity), IT service lifecycle management (incident/problem/change/service level)

Programming Languages: python, bash, PowerShell

Frameworks & Libraries: ansible, puppet

Cloud Platforms: Azure, O365

WORK EXPERIENCE

HCL America | Network Engineer-II

Feb 2024 -

- Verified integrity and availability of network hardware and reviewed device logs across network nodes to maintain operational stability.
- Administered Linux-based systems to support infrastructure operations and troubleshooting.
- Improved the troubleshooting/monitoring process for LAN/WAN activities, increasing the up-time by 27%, and strengthened **incident management** workflows through faster triage and clearer escalation.
- Improved the response time to incoming incident response tickets by 20% by refining runbooks, prioritization, and handoffs between teams.
- Built end-user and engineer documentation for support and operational processes, reducing 2 days of onboarding for new network engineers.
- Monitored system resource utilization and network health using tools such as SolarWinds and Net MRI to proactively detect issues.
- Supported **change management** to ensure success of major changes made to network infrastructure, including planned validation and rollback readiness.
- Monitored, managed, and troubleshot Cisco Wireless devices using Cisco Meraki.
- Performed Wireshark packet capture analysis to isolate network and application connectivity issues affecting end users.
- Evaluated emerging network technologies and provided recommendations to improve reliability and scalability.
- Implemented adds/moves/changes per business requirements in a data center environment, coordinating with stakeholders to minimize downtime.
- Administered switching technologies including creating and managing VLANs, port security, trunking, STP, inter-VLAN routing, and LAN security.
- Supported core/distribution/edge environments including Cisco ASR, Nexus 7K/9K, Arista 7000, and Cisco 7200 platforms in data centers.
- Worked across Layer 2/3 protocols including STP, UDLD, CDP, LLDP, ARP, VTP, BGP, OSPF, EIGRP, and IS-IS to troubleshoot complex connectivity issues.
- Actively involved in design and deployment of a new data center using Cisco Nexus 9000 spine-leaf architecture utilizing VXLAN fabric and BGP-EVPN overlays.
- Conducted regular security compliance audits and risk assessments on network configurations to align with organizational policies and industry security standards.
- Partnered with network planning on IP allocation schemes for routers, switches, workstations, phones, APs, and other devices.
- Used Infoblox, SolarWinds, and other monitoring tools to support DNS/DHCP/IPAM and infrastructure visibility.
- Worked within enterprise ticketing workflows (ServiceNow, Jira, Remedy) to track incidents, changes, and operational requests end-to-end.
- Led stakeholder collaboration to translate business requirements into scalable infrastructure designs aligned to timelines and operational standards.
- Configured new VLANs and extended existing VLANs to enable connectivity between two different data centers.

Bahhwan cybertek | Network engineer (NOC)

Jul 2021 - Dec 2023

- Used SolarWinds for monitoring and analysis of security threats and alerts from network nodes (switches, routers, CCTVs), supporting day-to-day operations.

- Generated uptime and memory utilization status reports from SolarWinds and communicated concise, accurate updates to team leads (supporting **service level management** reporting).
- Supported site-to-site and client VPNs across Cisco ASA/MX, Palo Alto, and FortiGate/Fortinet platforms, troubleshooting connectivity and authentication issues.
- Managed endpoint security by administering FortiClient VPN connected to EMS to ensure employees could establish IPsec tunnels when working remotely.
- Used Forti-Analyzer to monitor traffic flows and investigate anomalous activity for faster incident resolution.
- Performed IAM onboarding/offboarding and account administration: managing/updating user accounts, setting up authentication methods, maintaining permissions, and monitoring access in Azure and Windows Active Directory.
- Administered Linux/Unix operating systems (Kali Linux, Ubuntu) to support troubleshooting, analysis, and operational tasks.
- Applied understanding of TCP/IP and network performance metrics to diagnose LAN/WAN issues affecting corporate users.
- Supported wireless technologies including Cisco DNAC and Aruba wireless for monitoring and troubleshooting.
- Used Ansible and Puppet to automate repetitive network operations and configuration tasks.
- Wrote and maintained scripts in Python and Bash to streamline troubleshooting and operational workflows.
- Performed penetration testing, risk analysis, and compliance testing to strengthen security posture and reduce vulnerabilities.
- Implemented and maintained web content filtering using iBoss, LightSpeed, and Fortinet technologies.
- Secured SSL/VPN configurations and troubleshot Cisco ASA firewalls and related network security controls.
- Worked with network and IDS/IPS tooling such as Splunk, SolarWinds, and FortiGate to investigate events and support incident response.
- Supported Microsoft 365 tooling (Outlook, Word, Excel, PowerPoint, Access, SharePoint, OneDrive, Intune, Teams, Azure AD, MFA authenticator, VPN) for end-user productivity and access.
- Resolved network (LAN/WAN), hardware, and software issues for corporate employees as part of Level 1/2 operations.
- Troubleshot Brocade switches and Cisco routers/switches, created VLANs, monitored switch logs, and restored service during outages.
- Applied OSI/TCP/IP model knowledge and protocols such as BGP to troubleshoot routing and reachability issues.
- Administered Active Directory, configured Group Policies, and used LDAP sync with FortiGate to enforce role-based network access.

CERTIFICATIONS & ACHIEVEMENTS

- CompTIA Security+ certified - CompTIA
- Microsoft Certified Azure Fundamentals - Microsoft
- CCNA - Cisco