

**A close-up of a logo

Description automatically generated****A logo with text and a circle

Description automatically generated with medium confidence**

|  |  |  |
| --- | --- | --- |
|  | **V. Chalama Reddy** |  |

   Network Engineer

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Contact   |  |  | | --- | --- | |  | crvenna25@gmail.com |  |  |  | | --- | --- | |  | +1 (872)-256-2202 |   LinkedIn **:** <https://www.linkedin.com/in/crvenna/>  Skills  TECHNICAL SKILLS    Networking Protocols    RIP, OSPF, EIGRP, BGP, STP, RSTP, VLANs, VTP, PAGP, LACP, MPLS, HSRP, VRRP, GLBP, TACACS+, RADIUS, AAA, SNMP, VPC, VDC, MLAG    Switches    Cisco Catalyst Series (9400, 9300, 9200, 8500, 8300, 8200), Cisco Nexus Series (9500, 9300, 3000, 5000, 7700 [7706, 7710, 7718]), Cisco Meraki Series (MS390, MS250-48P), Arista 7000 Series (Cloud-grade switches).    Routers    Catalyst 8300 and 8200 Series Edge Platforms, ASR 9000 Series (9006, 9010,920), Juniper MX960, Arista 7800R Series, Cisco ISR 4000 Series, IR 809 and IR 1101.    Wireless    Cisco WLC, 802.11 a/b/g/n/ac/ax, 802.1X Authentication, EAP/PEAP, Aruba ClearPass, Ekahau, Cisco ISE, Air Magnet, AirWatch (VMware Workspace ONE), Aruba Central, Cisco DNA Spaces.    Firewalls    Palo Alto Networks (PA-2K, PA-3K, PA-5K, PA-7K Series), Cisco (Firepower, ASA 5500 Series), Fortinet (FortiGate 6000 Series), Symantec Blue Coat (ProxySG), Check Point Firewalls.    Load Balancers    F5 Networks (BIG-IP LTM, BIG-IP GTM), Citrix NetScaler ADC, Cisco (CSM, ACE), A10 Networks ADC, Azure Load Balancer (Cloud-native).    WAN technologies    MPLS, SD-WAN, PPP, OC3, SONET, L2VPN, L3VPN, VPLS.    LAN technologies    Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, 40 & 100 GBE, Port- channel, VLANs, VTP, STP, RSTP, MST, 802.1Q    Security Protocols    IKE, IPSEC, SSL-VPN, ACL, NAT, PAT, URL Filtering, SSL Forward Proxy, Blocklists, VPN, Port-Security, SSH, AAA, Prefix-Lists, Zone-Based Firewalls, HIPAA Standards, Ingress & Egress Firewalls, Content Filtering, Load Balancing, IDS/IPS, SNMP Trap.    Cloud & Virtualization Technologies    AWS (Transit Gateway, Direct Connect, Network Load Balancer), Microsoft Azure (Traffic Manager, DDoS Protection, Load Balancer), Zscaler (ZIA, ZPA), VMware (vSphere, NSX, ESXi), Citrix ADC, Cisco ACI, and Cisco Nexus Cloud.    Operating Systems    CAT IOS, IOS XE, XR, NX-OS, Junos, PANOS, F5 BIG-IP OS, Linux, Windows    Network Monitoring & Management Tools    Wireshark, Splunk, SolarWinds (NPM, NCM, SAM), Cisco DNA Center, NetScout, Thousand Eyes, Nagios, Zabbix, Infoblox, ManageEngine OpManager, Dynatrace, Datadog, Logic Monitor, Grafana, Prometheus, PRTG Network Monitor.    Education  Master' s  Computer Science Western Illinois University | Macomb, USA  Bachelor' s  computer science | Vignan University | India  Certifications   * Cisco Certified Network Associate (CCNA) * Cisco Certified Network Professional (CCNP) * AWS Certified Solutions Architect (AWS) | PROFESSIONAL SUMMARY   * Experienced Network Engineer with a strong background in designing, deploying, and managing multi-vendor network infrastructures in enterprise and data center environments. * Expert in Software-Defined Networking (SDN), implementing Cisco ACI with APIC controllers, VXLAN EVPN, and multi-site fabric integration. * Extensive SD-WAN expertise, deploying Cisco Viptela, Versa Networks, and Silver Peak Unity Edge Connect for branch connectivity and optimized WAN performance. * Strong proficiency in cloud networking, configuring AWS Transit Gateway, Direct Connect, Azure Traffic Manager, DDoS Protection, and Load Balancer for secure and efficient cloud connectivity. * Advanced expertise in routing and switching, configuring BGP (underlay/overlay, route policies), OSPFv3 (IPv6), VXLAN, VLANs, STP, and VTP on Cisco Nexus 9000, Catalyst 9000, and ASR routers. * Experience in network automation, using Ansible, Terraform, and Python scripting to automate data center deployments, firewall configurations, and network provisioning. * Hands-on experience in enterprise firewall security, configuring and managing Palo Alto (PA-5K, PA-7K, Panorama), Cisco Firepower, Check Point, and FortiGate 6000 series firewalls. * Implemented advanced VPN solutions, deploying IPsec, SSL VPNs, and Palo Alto GlobalProtect for secure remote access and site-to-site connectivity. * Expertise in load balancing and application delivery, configuring F5 BIG-IP (LTM, GTM) and Citrix NetScaler ADC for global traffic balancing, SSL offloading, and web acceleration. * Configured and secured cloud-based web filtering solutions, including Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), and Cisco Umbrella. * Implemented high availability (HA) and redundancy solutions, including HSRP, VRRP, GLBP, and Fortinet HA clusters for failover and reliability. * Experience in enterprise wireless networking, deploying and managing Cisco and Aruba 500 series access points with Aruba ClearPass authentication. * Utilized monitoring and analysis tools, including Wireshark, SolarWinds NetFlow, Splunk, NetScout, and Cisco DNA Center, for real-time network performance monitoring and troubleshooting. * Configured and managed DNS and traffic routing solutions, including Windows DNS, Infoblox, F5 GTM, and Akamai DNS, for intelligent traffic steering and global failover. * Secured applications using Akamai Kona WAF, F5 ASM, Site Shield, and API & App Protector, mitigating DDoS attacks, OWASP Top 10 threats, and bot-based security risks. * Hands-on experience integrating networking solutions across Cisco, Juniper, Palo Alto, F5, and Fortinet, ensuring seamless multi-vendor deployments. * Passionate about network automation, cybersecurity, performance optimization, and cloud security, driving efficient and scalable networking solutions.   Work History  March 2024 - Current  Network Engineer  **Verizon, Irving, TX**   * Deployed and configured Cisco ACI in a Spine-Leaf topology using Nexus 9500 and 9300 Series switches, integrating BGP underlay and VXLAN EVPN overlay for centralized management * Implemented ACI tenant segmentation, Application Network Profiles (ANPs), bridge domains, Endpoint Groups (EPGs), and contracts for automated provisioning and policy enforcement * Configured ACI multi-site connectivity (MSO), Layer 2/3 external integrations, and policy-driven automation * Deployed Cisco SD-WAN (Viptela) on ISR 1000 and Catalyst 8000 routers, leveraging vManage for centralized policy and template management, integrating with Azure for optimized cloud connectivity * Configured Versa Networks SD-WAN, Silver Peak Unity EdgeConnect, and Cisco SD-Access for secure and scalable enterprise segmentation * Utilized Cisco v Manage, Versa Director, and Silver Peak Orchestrator for centralized policy configuration, monitoring, and troubleshooting * Automated SDN and SD-WAN deployments with Ansible and Terraform, ensuring consistent configuration management * Configured and managed Palo Alto Networks PA-3K, PA-5K, PA-7K Series firewalls, Panorama 10.0, and Wildfire for threat prevention * Migrated from Cisco ASA to Palo Alto, optimizing URL filtering, IPSec/SSL VPNs, and zone-based security policies * Integrated Palo Alto PA-7050 with LDAP and Active Directory for user-based security policies * Designed and deployed FortiGate 6000 Series NGFWs, configuring intrusion prevention, application control, and advanced security policies * Integrated FortiClient with FortiGate and FortiManager for centralized endpoint security management * Configured Cisco ISE (802.1X authentication) on Catalyst 9300 switches, enforcing role-based network access * Implemented Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) for secure cloud web filtering and remote access * Configured F5 BIG-IP ASM for web application firewall (WAF) protection against SQL injection, XSS, and DDoS attacks, utilizing automated learning mode for policy tuning * Managed F5 LTM and GTM for global application traffic distribution, developing iRules for traffic redirection, SSL offloading, and security enhancements * Configured Cisco Nexus 9500, Catalyst 9400, and 9000 Series switches for enterprise infrastructure upgrades * Implemented dynamic routing protocols (OSPF, BGP, EIGRP) for WAN connectivity, ensuring optimal path selection and failover * Established BGP peering with external ASNs on Arista 7800R switches and Juniper MX960 routers, optimizing traffic flow * Migrated legacy Cisco switches to Aruba CX Series (8320, 8400), leveraging AOS-CX OS automation for cost reduction and scalability * Configured AWS Transit Gateway and Direct Connect for multi-VPC and on-premises network connectivity * Implemented Azure Traffic Manager for DNS-based load balancing and Azure DDoS Protection for cloud security * Designed and deployed Cisco Meraki MX85 Security Appliance and MS250-48P switches, integrating with Cisco Umbrella for threat prevention * Configured VMware vSphere and ESXi hosts for high availability and resource management in virtualized environments * Utilized SolarWinds NetFlow Traffic Analyzer for network traffic monitoring and bandwidth utilization insights * Integrated Splunk with AWS and Azure for hybrid cloud security monitoring * Automated firewall and network device configurations with Ansible and Terraform for infrastructure as code (IaC) * Developed Python scripts and Ansible playbooks to streamline configuration management and device provisioning * Used ServiceNow for incident, change, and configuration management in network operations * Configured and managed Infoblox DDI (DNS, DHCP, IPAM) for automated IP address management and security enforcement * Automated DNS and DHCP provisioning using Infoblox APIs and Ansible * Managed Akamai CDN, Edge DNS, and GTM for global traffic steering and optimized content delivery * Deployed Akamai API Gateway to secure enterprise APIs from bot attacks and injection threats * Configured Aruba Mobility Controllers and Access Points to deploy WiFi-6 (802.11ax) networks, supporting over 1,500 devices * Integrated Aruba ClearPass for role-based network access control and cloud-managed networking with Aruba Central * Implemented BPDU Guard, Root Guard, and VTP authentication to enhance switch security   Jan 2023 - Mar 2024  Network Engineer  **UHG, Hanover Park, IL**   * Integrated Palo Alto Networks PA-850 firewalls with Splunk SIEM, leveraging Python automation for log management and real-time threat detection * Managed Palo Alto Firewalls (PA-220, PA-3200, PA-5200) through Panorama, implementing centralized security policies, firewall rule management, and VPN configurations * Configured Cisco ASA 5500-X (9.14) firewalls, deploying advanced security policies, IPS, VPN services, and traffic filtering * Executed migration from Check Point to Cisco ASA, ensuring secure and efficient VPN policy transitions * Implemented A10 Thunder TPS for DDoS protection, configuring advanced threat detection and mitigation technologies * Deployed Symantec Blue Coat ProxySG as a Secure Web Gateway (SWG), integrating web filtering, SSL inspection, and malware protection * Integrated Cisco ISE with Active Directory and RSA SecurID, enabling multi-factor authentication for critical network access * Configured Aruba ClearPass with RADIUS authentication, enforcing secure and efficient user authentication for wired and wireless networks * Deployed Cisco ACI in a multi-site environment, configuring APIC controllers and fabric switches for application-based networking and centralized management * Monitored Cisco ACI health scores to track network performance, detect faults, and optimize policy enforcement * Configured Silver Peak Unity EdgeConnect for SD-WAN, leveraging dynamic path control and WAN optimization for improved application performance * Implemented Viptela SD-WAN on vEdge routers, establishing secure, scalable WAN fabric for distributed sites * Provisioned Versa Networks SD-WAN and Secure Access Service Edge (SASE) solutions, enhancing branch connectivity and security * Designed and implemented LAN/WAN architectures, utilizing MPLS, Ethernet, and broadband technologies for optimal connectivity * Configured BGP (EBGP, IBGP) on Cisco ASR 9000 Series routers, optimizing route selection and high availability * Implemented OSPF sham-links on ASR 9000 to support MPLS VPNs and maintain routing integrity * Deployed AWS Direct Connect, establishing high-bandwidth, low-latency connectivity between on-premises networks and AWS * Configured Google Cloud VPCs, implementing secure segmentation, firewall rules, and route tables for efficient cloud networking * Optimized AWS Network Load Balancer (NLB) and Route 53 policies, ensuring high availability and fault tolerance across cloud environments * Administered F5 BIG-IP LTM/GTM, performing licensing, provisioning, firmware upgrades, and health monitoring * Executed migration from A10 to F5 load balancers, implementing advanced traffic steering and SSL offloading * Developed F5 iRules for traffic redirection, security enhancements, and custom filtering policies * Configured Akamai CDN for optimized content delivery, caching policies, and latency reduction * Implemented Akamai Kona Site Defender for WAF protection, tuning security policies to mitigate OWASP Top 10 threats and DDoS attacks * Deployed Akamai API Gateway, enforcing rate limiting, authentication, and SIEM integration for real-time threat monitoring * Automated SSL/TLS certificate deployment across F5 and Akamai, ensuring secure communication and compliance * Configured Splunk Enterprise for real-time log analysis, developing custom dashboards and alerts for network security events * Monitored OSPF neighbor relationships using SolarWinds NCM, proactively identifying routing issues * Automated firewall and network device configurations with Ansible and Python, reducing manual efforts * Integrated ServiceNow for incident, change, and configuration management, streamlining IT workflows * Managed Aruba 300 Series (802.11ac) and 500 Series (802.11ax) wireless access points, ensuring high-performance connectivity in enterprise environments * Deployed Aruba Wireless LAN Controllers (WLCs), optimizing AP performance, user density handling, and security policies * Integrated Aruba ClearPass for network access control, enabling policy-based user authentication   May 2019 - May 2022  Network Support Engineer/ Technical Analyst  Capgemini | Hyderabad , India   * Managed VLANs, inter-VLAN routing, and trunking (802.1Q) on Cisco Catalyst 3560, 3750, and 4500 Series switches, optimizing network segmentation and security * Configured Layer 2 technologies, including VLAN Trunks, EtherChannel, and Spanning Tree Protocol (STP) to prevent loops and enhance LAN performance * Performed Cisco IOS upgrades, password recovery, and TFTP-based configurations, ensuring secure and updated switch firmware * Implemented routing protocols such as EIGRP, OSPF, RIPv2, and static routes on Cisco routers (2800, 3800, 7200 Series) for optimized path selection and network stability * Troubleshot WAN connectivity issues, including BGP route reflectors on Nexus 7000 switches and DMVPN solutions for secure site-to-site communication * Configured Cisco ASA 5500 series firewalls, deploying SSL VPN and IPSec VPNs for secure remote connectivity * Implemented NAT, Access Control Lists (ACLs), and firewall logging, ensuring secure resource access and network monitoring * Utilized SolarWinds and Wireshark for real-time network monitoring, detecting anomalies and security threats * Configured AWS Security Groups, Network ACLs, and Azure Traffic Manager, ensuring secure and efficient cloud connectivity * Assisted in VMware vSphere and NSX to support virtualized networking environments, including cloud-based VPN solutions * Configured Citrix NetScaler Gateway for VPN services and multi-factor authentication, troubleshooting traffic distribution issues * Managed enterprise wireless networks, troubleshooting 2.4 GHz/5 GHz connectivity, and configuring EAP and PEAP authentication for secure access * Monitored networking protocols (OSPF, RSTP, EIGRP, BGP) using SolarWinds NCM, proactively identifying and resolving connectivity issues * Utilized Wireshark and Splunk for protocol analysis and traffic flow monitoring, identifying performance bottlenecks * Provided hands-on technical support, including network installations, racking, stacking, and cabling, ensuring efficient LAN/WAN administration |