Sai Shruthi Gaddam
Saishruthigaddam@gmail.com|913-991-7679||

EDUCATION

Jawaharlal Nehru Technological University
Bachelor's in computer science- 2017

ABOUT ME

Senior Cloud Network Engineer with 8+ years of hands-on experience architecting, securing, and optimizing enterprise and hybrid cloud networks across AWS, Azure, and GCP. Expert in SD-WAN (Viptela, Silver Peak, Versa), Cisco ACI, Palo Alto Firewalls, and automation tools like Terraform, Ansible, and Python. Proven track record in delivering scalable, high-performance network solutions for Fortune 500 clients including Petsmart and American Express. Adept at zero-trust security, infrastructure as code (IaC), and multi-cloud deployments with a focus on performance, reliability, and compliance (NIST, ISO, SOC2). Certified in CCNP, AWS Solutions Architect, and PCNSE.

PERSONAL DETAILS

LINKS
LinkedIn:
https://www.linkedin.com/in/sai-shruthi-gaddam/

CERTIFICATIONS

CCNA - Cisco Certified Network Associate
CCNA Security – Cisco Certified Network Associate Security
CCNP - Cisco Certified Network Professional
AWS - Solution Architect Associate
PCNSE - Palo Alto Certified Network Security Engineer

TOOLS AND TECHNOLOGIES

Core Networking:
Cisco SD-WAN | Viptela | BGP | OSPF | EIGRP | RIP | HSRP | VRRP | VLAN | VTP | STP | RSTP | MSTP | VXLAN | MPLS | IP SLA | DMVPN | Multicast | Dot1Q Trunking

Switching & Routing:
Cisco Catalyst 2960/3560/3850/4500/9300/9500 | Cisco Nexus 2K/5K/7K/9K | ISR 1000/4000 Series | ASR 1001-X/1002-HX | Juniper EX/MX | Arista 7200 | Cisco ACI Spine-Leaf | Cisco DNA Center | Cisco Virtual Internet Routing Lab (VIRL)

SECURITY TECHNOLOGIES
Palo Alto NGFW (PA-850, PA-3220) | PAN-OS | Cisco ASA 5500-X | Cisco Firepower 2100/4100 | Cisco FTD | Fortinet FortiGate 60–1000 Series | Cisco ISE 2.x/3.x | Duo MFA | Zscaler ZIA/ZPA | SSL VPN | IPSec VPN | VPN Load Balancing | Snort IDS/IPS | ACLs | 802.1X | TrustSec | NAT/PAT | Cisco Umbrella | Cloudflare Access | Blue Coat Proxy

CLOUD & VIRTUALIZATION
AWS (VPC, Transit Gateway, Direct Connect, Route 53, Network Firewall) | Azure (VNet Peering, ExpressRoute, NSG, Azure Firewall, Azure Bastion) | GCP (VPC, Cloud NAT, Cloud VPN) | Hybrid Interconnects | Security Groups | Cloud Load Balancers | Routing Tables | CloudWatch Logs

Platforms & Tools:
Cisco DNA Center | Cisco Prime | Panorama | Infoblox DDI | ServiceNow | F5 BIG-IP (LTM, APM, ASM) | Citrix ADC (NetScaler) | TFTP/SCP | DHCP/DNS/NTP | EVE-NG | GNS3 | OPNET | VMware vSphere/NSX | Cisco CML | Cisco IOL Images

NETWORK MONITORING & MANAGEMENT
SolarWinds NPM/NCM | PRTG | Splunk | ThousandEyes | Cisco Prime Infrastructure | Cisco DNA Assurance | Wireshark | SNMP | NetFlow | ELK Stack | Grafana | Nagios | Zabbix | Azure Monitor | AWS CloudWatch | ServiceNow ITSM

WIRELESS TECHNOLOGIES
Cisco WLC 5520/3504/7240 | Cisco Mobility Express | Cisco Meraki MR Series | Aruba 200/300 Series APs | SSID Segmentation | Rogue Detection | Wireless Intrusion Prevention System (WIPS) | 802.11a/b/g/n/ac/ax | 802.11k/v/r | Fast Roaming | RF Spectrum Analysis | Ekahau Site Survey

Automation & DevOps:
Python | Ansible | Terraform | PowerShell | Bash | Git | Jenkins | GitLab CI/CD | YAML/JSON | REST APIs | RESTCONF | NETCONF | tfsec | Checkov | Configuration Drift Detection | Auto-remediation | Infrastructure as Code (IaC)

CAPACITY & PERFORMANCE
Riverbed | WAN Killer

Standards & Docs:
HIPAA | PCI-DSS | ISO 27001 | NIST 800-53 | Network Audits | SOC 2 | Business Continuity Planning (BCP) | Change Management | HLD/LLD Documentation | Microsoft Visio | Microsoft Office Suite | Agile | Scrum | ITIL Foundation (Basics)

KEY POINTS:

- Experience in **Cisco/Juniper** Networking, and Security which includes designing, Deployment, and providing network support, installation, and analysis for a broad range of **LAN / WAN** protocols.
- Hands-On experience with **Cisco IOS/IOS-XR/NX-OS**, **Juniper JUNOS** for configuration & troubleshooting of routing protocols: **MP-BGP, OSPF, EIGRP, RIP, BGP v4.**
- In-depth knowledge and hands-on experience in **Tier II ISP** Routing Policies, Network Architecture, **IP Subnetting, VLSM**, **TCP/IP, NAT, DHCP, DNS, FT1 / T1 / FT3 / T3 SONET POS OCX / GigE circuits, Firewalls.**
- Involved in troubleshooting of **DNS, DHCP,** and other IP conflict problems.
- Experience of **Palo Alto Firewalls** and the **Panorama** Network Security Management Box.
- Strong knowledge of TACACS+, and RADIUS implementation in Access Control Network.
- Experience in Designing and assisting in deploying enterprise-wide Network Security and High Availability Solutions for ASA.
- Worked with Cisco, Palo Alto, Juniper, **Splunk, Force Point,** Nessus, Stealth watch, Checkpoint, **Zscale**r, and other vendors to provide a stable, high-speed secure network.
- Extensive work experience with Cisco Routers, Cisco Switches, Load Balancers, and Firewalls.
- Experience working with Cisco Nexus 2148 Fabric Extender and Nexus 7010, 5000 series to provide a Flexible Access Solution for a data center access architecture.
- Experience with Zscaler Cloud Proxy Architecture with ZIA, traffic forwarding using GRE tunnels to Zcloud, Azure AD Authentication, Access policies, ZAPP.
- Experience Arista Cloud Vision on a POC. Working on Spine leaf Architecture in Data center. Worked on EVPN, VXLAN, VTEPS, Bridge Domains, MP-BGP etc.
- Responsible for Check Point (Secure Platform R70) and Cisco ASA firewall administration across global networks.
- Experience in working with Cisco Nexus Switches and Virtual Port Channel configuration.
- Implemented and maintained Sourcefire intrusion detection/ prevention (IDS/IPS) system and hardened protection standards, IDS/IPS signatures on Firewall for Fine-tuning of TCP and UDP services.
- Experienced in planning and development of designs for Migrating to AWS cloud.
- Implemented traffic filters using standard and extended access lists, distribution lists, and route maps.
- Experience on implementing and troubleshooting complex layer 2 technologies such as **VLAN** Trunks**, VTP, Ether channel**, **STP, RSTP, and MST**. Implementation of **HSRP, VRRP** for Default Gateway Redundancy.
- Experience as Cloud Administrator on Microsoft Azure, involved in configuring virtual machines, storage accounts, resource groups.
- Proficiency in **Cisco ASAs, ISRs, Catalyst/Nexus**, **HP Switches, Cisco Meraki, Aruba, EIGRP, OSPF, BGP**.
- Experience in testing Cisco routers and switches in a laboratory and deploying them on-site production.
- Experience with configuring **Nexus 2000 Fabric Extender** (FEX) which acts as a remote line card (module) for the **Nexus 5000.**
- Collaborated with cross-functional teams in **Agile environments**, contributing to sprint planning, reviews, and retrospectives for security architecture initiatives
- Deployed, Managed, monitored, and supported **Bluecoat Proxy** for content filtering, internet access between sites and VPN client users, forward proxy scenario and reverse proxy scenario for security, and worked on adding URLs in **Bluecoat Proxy SGs** for URL filtering.
- Worked extensively in Configuring, Monitoring, and Troubleshooting **Cisco's ASA 5500/PIX security appliance, Failover DMZ zoning** & configuring **VLANs/routing/NAT** with the firewalls as per the design.
- Worked extensively on **Cisco Firewalls**, **Cisco PIX (506E/515E/525/)** & **ASA 5500(5510/5540) Series**.
- Experience in preparing Technical Documentation and presentations using Microsoft VISIO/Office.
- Experience of **WAN Optimization** Technology, **Riverbed**.
- Hands on experience on Azure cloud – migrated number of applications from NSX private cloud to Azure.
- Worked on **Cisco Firewalls Cisco ASA 5500(5510/5540) Series and Checkpoint R75, 76, NGX R70 Firewalls.**
- Worked with the **Python 2 & 3 version.**
- Worked with Automation script with Python modules like **Chef & Ansible**.
- Configuring **Cisco Wireless Controllers** and **APs.**
- Configuring the **Network Admission Control (NAC).**
- Configuring **Cisco WAAS.**
- Excellent customer management/resolution, problem-solving, and debugging skills and capable of quick learning, effectively analyzing results, and implementing and delivering solutions as an individual and as part of a team.
- Hands on Experience testing iRules using Browser (IE), **HTTP watch.**

- Designed cloud security architectures in alignment with **NIST 800-53 and FedRAMP IL2** compliance for financial and government clients.
- experience of various wireless 802.11 standards, controllers, Access Points, and Wi-Fi analytics from various vendors (**Cisco Meraki, HPE /Aruba, D-Link, and Netgear), SD-WAN** (**MX 65, MX100, MX400**).
- Provided support that included resolving day-to-day operational issues with tickets generated by a server.
- Good understanding of **SNMP, IP SLA,** and Network Monitoring with experience in tools like **PRTG**.

EXPERIENCE

PetSmart | Senior Cloud Network Engineer

Mar 2022 – Present | Remote
Project: Secure Hybrid Cloud Network Deployment
Led the design and deployment of a highly available, secure hybrid cloud network for 1,500+ retail stores and distribution centers by integrating AWS, Azure, and on-prem data centers. Leveraged SD-WAN (Viptela & Versa), Cisco ACI, Palo Alto firewalls, and F5 load balancers to optimize retail operations, inventory systems, and customer Wi-Fi performance.

Responsibilities & Contributions

- Led end-to-end design and deployment of a hybrid network across **AWS**, **Azure**, and **GCP**, supporting secure cloud operations for enterprise applications.
- Migrated **on-prem infrastructure and VMs** to **AWS and GCP** using **Terraform** and **Ansible**, improving scalability and deployment speed.
- Automated infrastructure provisioning with **Azure Bicep**, **Jenkins CI/CD**, and **GitOps**, ensuring consistency across multi-cloud environments.
- Deployed **Cisco Viptela** and **Versa SD-WAN** across branches to optimize bandwidth and ensure **application-aware routing**.
- Designed and configured **Cisco ACI fabric** with **VRFs**, **EPGs**, and **Bridge Domains** to enforce **micro-segmentation** and policy automation.
- Built **Spine-Leaf architecture** using **Arista 7250** switches to enhance scalability and reduce data center bottlenecks.
- Configured **BGP**, **OSPF**, and **EIGRP** for resilient routing and fast failover across global WAN environments.
- Created and maintained **IPSec** and **GRE tunnels** using **Cisco ASA** and **Palo Alto** firewalls for secure multi-site connectivity.
- Migrated from legacy WAN to **GETVPN**, enabling secure multicast and dynamic routing over encrypted links.
- Managed multi-vendor **firewall policies** with **Panorama (Palo Alto)**, **FortiGate**, and **Cisco ASA**, ensuring centralized control and compliance.
- Integrated **Zscaler ZIA/ZPA** for cloud proxy and secure internet access using **user-based policies**.
- Configured **F5 BIG-IP (LTM, ASM, APM)** modules for advanced **L4–L7 load balancing**, SSL offloading, and access control.
- Maintained **Citrix ADC** and **Cisco ACE 4710** for legacy application support and gradual ADC modernization.
- Built **Ansible playbooks** to automate provisioning, load balancer registration, and dynamic infrastructure changes.
- Monitored system health using **AWS CloudWatch**, **GCP Stackdriver**, **Nagios**, **Splunk**, and **Zabbix**.
- Implemented performance dashboards using **New Relic** and **Kibana** to visualize cloud service metrics.
- Provisioned Wi-Fi and NAC infrastructure using **Aruba ClearPass**, **Cisco ISE**, and **Airwave**, enforcing **802.1X** and **MAC-based auth**.
- Deployed and managed **Cisco Meraki APs**, enabling cloud-managed Wi-Fi across remote offices.
- Enabled **SSO**, **SAML**, and **SCIM** integrations with **Azure AD** and **Zscaler** for identity-based access controls.
- Managed encryption keys and secrets using **Azure Key Vault**, **AWS KMS**, and **GCP Secrets Manager**.
- Deployed **AWS Transit Gateway**, **VPC Peering**, and **Azure ExpressRoute** to interconnect multi-cloud and hybrid resources.
- Integrated **Infoblox** for automated **DNS**, **DHCP**, and **IPAM** services across global environments.
- Applied **ACLs**, **NAT/PAT**, and **zone-based firewall policies** to protect internal and external traffic flows.
- Designed and implemented **Security Groups** and **NSGs** to isolate and protect critical cloud workloads.
- Enforced **CIS Benchmarks** to ensure cloud environment compliance and meet audit and security standards.
- Automated disaster recovery with **AWS Backup**, **Azure Recovery Vault**, and **GCP Snapshots** for critical services.
- Provisioned and maintained **EKS clusters** using **Terraform**, **Helm**, and **Kubernetes network policies** with **Calico**.
- Wrote **Python scripts** for automated health checks, config backups, and compliance audits across network devices.

- Integrated **Okta** with **Azure AD** and **Zscaler** for centralized identity and **role-based access control (RBAC)**.
- Built log monitoring and alerting systems in **Splunk** and **QRadar** to support threat detection and SOC operations.
- Worked with **InfoSec** to remediate vulnerabilities, reducing security risk by **40%** after penetration testing.
- Designed and deployed **SD-Branch architecture** using **Fortinet**, **Cisco**, and **Meraki**, unifying LAN/WAN policy enforcement.
- Segmented internal networks using **VLANs**, **VRFs**, and **Layer 3 interfaces** for DMZ and secure zones.
- Enabled high availability with **HSRP**, **VRRP**, and **LACP** across core routers and switches.
- Standardized **Nexus 7K/9K** switch configs using **Python** and **Ansible**, ensuring consistency in deployments.
- Created and maintained **network diagrams**, **firewall rule matrices**, and **cloud interconnect topologies**.
- Configured **DNS failover**, **geo-routing**, and **GSLB** using **Route 53** and **GCP Load Balancing**.
- Integrated automated backup workflows with scaling events to protect stateful cloud resources.
- Hardened Layer 2 access with **BPDU Guard**, **Port Security**, and **802.1X** on user-facing switches.
- Deployed custom **F5 iRules** for intelligent traffic redirection and enhanced Layer 7 control.
- Created **Terraform-based Jenkins pipelines** for safe infrastructure deployments with change approvals.
- Built alert systems with **CloudWatch Alarms**, **SNS**, and escalation workflows for critical infrastructure.
- Conducted packet capture and latency troubleshooting using **Wireshark** and GCP's **Network Intelligence Center**.
- Aligned network design with DevOps practices by collaborating closely with **cloud architects**, **platform teams**, and **security engineers**.

American Express | Senior Network Engineer

June 2018 – March 2022 |NY
Project: Hybrid Network Modernization for Utility Operations
Engineered and supported a secure, high-performance global enterprise network by modernizing core infrastructure across AWS, GCP, and on-prem environments. Implemented Silver Peak SD-WAN, Cisco ACI, Palo Alto NGFWs, and Cisco DNAC to enhance application availability, improve branch-to-cloud performance, and support PCI-DSS compliance across 200+ global sites.

Responsibilities & Contributions

- Configured and troubleshooted **Cisco 12000, 7500, 3800 routers** and **3560/6500/Nexus switches** for enterprise **LAN/WAN** environments.
- Deployed **Silver Peak SD-WAN** to replace legacy WAN and enable **star topology**, improving site-to-site routing and reducing downtime.
- Designed and implemented **Spine-Leaf architecture** using **Arista 7250QX** and **eBGP**, supporting a new 100G data center consolidation effort.
- Led the **data center migration** and VPN expansion strategy, including secure interconnects between on-prem and cloud.
- Built and maintained **GCP VPCs**, configured **firewall rules**, **cloud CDN**, and routing to isolate workloads and reduce latency.
- Created **Terraform scripts** for provisioning **load balancers**, **S3 buckets**, and automating **infrastructure deployments** in **AWS**.
- Configured **MPLS**, **BGP**, and **OSPF** across enterprise networks to ensure high availability and fast convergence.
- Established **Direct Connect** and **ExpressRoute** links between on-prem environments and **AWS/GCP**, enabling secure hybrid architecture.
- Deployed and segmented **Palo Alto VM-700 firewalls** in **GCP**, managing **prod vs non-prod** zones with Panorama.
- Installed and managed **Cisco ACI**, including **policy enforcement**, **contract creation**, and **endpoint management** via **DNAC**.
- Configured **Azure Hub-and-Spoke topology**, working with Microsoft support to establish scalable routing and connectivity.
- Migrated **200+ sites** from hub-and-spoke WAN to SD-WAN using virtual firewalls, improving routing and policy consistency.
- Deployed **Aruba wireless controllers and APs**, configured **SSID**, **BYOD policies**, **802.1X**, **EAP/PEAP**, and integrated with **Cisco ISE** and **ClearPass**.
- Installed and configured **Cisco Meraki MR series APs** in warehouses, extending secure wireless access in distributed facilities.
- Provisioned and administered **Juniper routers (MX80, MX480, MX960)** for scalable IPv4 network infrastructure and branch integration.

- Migrated workloads to **AWS**, configuring **EC2**, **Route 53**, **RDS**, **Lambda**, and setting up VPC endpoints and NAT gateways.
- Designed secure VPCs and subnets in **AWS** and **GCP**, implementing **Transit Gateways**, **Private Links**, and **Security Groups** for access control.
- Implemented **FortiGate firewall policies**, **CheckPoint ACLs**, and **Juniper SSG-140** configurations to secure inter-office traffic and B2B tunnels.
- Developed **Python scripts** and **Ansible playbooks** to automate configuration, health checks, and compliance audits across Cisco and Juniper platforms.
- Integrated **LDAP and AD authentication** into **Checkpoint** and **F5 APM**, enabling centralized access and policy enforcement.
- Managed **A10** and **F5 BIG-IP LTM (iRules)** load balancers for high-availability application delivery and SSL offloading.
- Monitored network performance using **SolarWinds**, **Splunk**, and **GCP Network Intelligence Center**, diagnosing latency, packet loss, and routing issues.
- Configured and maintained **Site-to-Site IPsec VPNs**, **DMVPN**, and **Cisco ASA tunnels** to support secure regional data center communications.
- Provided **out-of-band management** for disaster recovery setups and fault monitoring using **SNMP**, **SolarWinds**, and Orion tools.
- Collaborated with **cloud architects** and **DevOps teams** to optimize **GCP firewall rules**, **load balancers**, and **subnet design** for high-security zones.
- Created detailed **AWS Security Groups**, acting as virtual firewalls to restrict EC2 access by IP, port, and protocol.
- Deployed **Blue Coat Proxy** for secure internet filtering and web access policy enforcement.
- Configured **Cloud Lifecycle Management (CLM) DNS** to automate IP/DNS assignments during provisioning in AWS and GCP.
- Served as key contributor in enterprise-wide switch upgrades from **Cisco Catalyst to Juniper EX4200/3200**, improving routing flexibility and performance.
- Led troubleshooting efforts using **Wireshark**, **iperf**, and real-time flow tools to optimize application performance and resolve critical outages.

Polygon |Network Engineer

April 2017 – June 2018 | India

Project: Enterprise Network Optimization for Asset Management

Implemented a secure and scalable network for logistics and asset management using **SD-WAN**, **Juniper SRX**, **Cisco Catalyst**, **BGP**, **OSPF**, and **Cisco DNAC** to support distributed operations.

Responsibilities & Contributions

- Configured and managed **Cisco 2620, 1900, 2950, and 3500 series routers and switches**, supporting enterprise LAN/WAN infrastructure.
- Used **TFTP servers** to back up and restore Cisco device configurations during planned changes and outages.
- Supported network expansion by provisioning new users, assigning subnets, and extending VLAN configurations.
- Designed IP addressing schemes using **FLSM** and **VLSM** to optimize IP space allocation across departments and applications.
- Configured **Spanning Tree Protocol (STP)** on Cisco Catalyst switches to prevent Layer 2 loops and ensure stable switching paths.
- Deployed and managed **VLAN Trunking Protocol (VTP)** to centralize VLAN management and simplify switch configuration.
- Set up **Inter-VLAN Routing** to enable secure communication between different departmental networks.
- Implemented access control using **ACLs**, routing redistribution, and **dynamic routing protocols** to manage internal traffic efficiently.
- Enabled switch-level security by configuring **Port Security**, **Sticky MAC**, and **Violation Modes** as per internal policy.
- Segmented the network using **VLANs** to isolate HR, Finance, and Engineering traffic for better security and control.
- Configured **IPSec VPN tunnels** on **Juniper SRX firewalls** to establish secure connectivity between branch locations.
- Deployed **EIGRP** on Cisco routers to optimize convergence and support fast failover in LAN environments.
- Tuned **BGP** and **OSPF** on **Juniper M-series routers** to ensure high availability for asset and logistics platforms.
- Implemented **MPLS** on Cisco switches for optimized WAN routing and load-balanced connectivity across remote sites.

- Deployed **DMVPN** on Juniper SRX devices, enabling scalable, encrypted branch-to-branch communication.
- Implemented **SD-WAN** for remote office traffic optimization, integrated with **Cisco Meraki** to improve cloud application performance.
- Used **Cisco DNA Center (DNAC)** for policy-based automation, managing VLAN deployment and STP configurations across the campus network.
- Installed and configured **Juniper SRX firewalls**, applying security policies to protect sensitive data within inventory and tracking systems.
- Configured **802.1Q trunking** and **ISL** to enable VLAN communication between Cisco Catalyst switches.
- Utilized **Wireshark (formerly Ethereal)** to analyze network packet flow, detect anomalies, and identify root causes of latency.
- Resolved connectivity issues using tools like **PING**, **Traceroute**, and **NetFlow** data for real-time troubleshooting.
- Performed **hardware replacements and firmware upgrades** to keep network infrastructure compliant and stable.
- Conducted **routine virus checks and software updates** on all desktops and servers to maintain endpoint security.
- Supported **LAN implementation and maintenance**, handling cabling, port activation, and switch provisioning for new offices.
- Worked with **SNMP**, **DNS**, and **DHCP** services to maintain reliable IP address management and network visibility.
- Created and maintained access lists to enforce **traffic filtering**, especially for inter-VLAN and internet-bound traffic.
- Coordinated with vendors and internal teams to plan and execute **Layer 2 and Layer 3 changes** during maintenance windows.
- Documented network topology diagrams, configuration changes, and operational checklists for internal knowledge base.
- Assisted in **troubleshooting WAN links**, collaborating with ISPs to resolve outages and monitor SLAs.
- Ensured all configurations adhered to internal **security and compliance standards**, particularly for asset-sensitive data flows.