**Kishan K | Sr Network Engineer**

 **EMAIL:** [**kishan815m@gmail.com**](kishan815m%40gmail.com)**| MOBILE:** [**(779)-379-1686**](%28779%29-379-1686) **| LinkedIn:** [**LinkedIn**](www.linkedin.com/in/kishan815)

**PROFESSIONAL SUMMARY:**

* Configured and managed core network devices including **Cisco Nexus, Catalyst, Meraki, Palo Alto Firewalls, and F5 BIG-IP load balancers**, delivering resilient and high-performing infrastructures.
* Implemented and optimized enterprise-scale data platforms and hybrid WAN solutions by integrating **MPLS, Cisco Viptela/Meraki SD-WAN, AWS Direct Connect, and Azure ExpressRoute**, improving performance and reducing operational costs.
* Conducted **performance tuning, capacity planning, and troubleshooting** to resolve bottlenecks across **WAN, LAN, WLAN (Aruba, Cisco Meraki), and hybrid cloud environments**.
* Acted as the subject matter expert on infrastructure needs, advising leadership and application teams on secure, scalable designs across **Cisco, Palo Alto, Zscaler, and multi-cloud platforms**.
* Developed and maintained detailed documentation using **Microsoft Visio, Confluence, SOPs, and runbooks**, and conducted knowledge transfer sessions for cross-functional teams.
* Strengthened security posture by implementing **Zero Trust, Cisco ISE NAC, IDS/IPS, Palo Alto Firewalls, Zscaler ZIA/ZPA, ACLs, and AES-256 IPSec encryption**, ensuring compliance with **PCI-DSS, HIPAA, and FAA standards**.
* Automated deployments and configuration management with **Ansible, Terraform, and Python scripting**, reducing manual errors and accelerating project timelines.
* Instrumented monitoring and logging with **SolarWinds (NetFlow, VNQM), Splunk, Infoblox, and SNMP traps** to quickly identify routing failures, security threats, and equipment issues.
* Collaborated with vendors (Cisco, Palo Alto, AT&T, Lumen, Verizon, AWS, Azure) and internal stakeholders to improve network resiliency, reduce downtime, and negotiate cost-effective carrier and ISP contracts.
* Led the design, deployment, and optimization of large-scale enterprise networks and hybrid cloud infrastructures using **AWS (VPC, Direct Connect, Transit Gateway), Azure (ExpressRoute, VPN Gateway), and GCP (Cloud DNS, Firewall Rules)**, ensuring secure and scalable solutions aligned with organizational IT strategy.
* Mentored and coached junior engineers on **BGP, OSPF, Cisco SD-WAN, Palo Alto firewall policies, and automation frameworks (Ansible, Python)** to build team capability and operational readiness.
* Delivered enterprise-grade load balancing and application resiliency with **F5 BIG-IP (LTM/GTM) and Citrix NetScaler ADC**, improving uptime and application performance.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **Networking Technologies** | Ethernet, Fast Ethernet, Gigabit Ethernet, & 10 Gigabit Ethernet, Port-channel, VLANS, VTP, STP, RSTP, 802.1Q, Frame Relay, ISDN, ATM, MPLS, leased lines & exposure to PPP, HDLC, and CSU/DSU, CBWFQ, LLQ, WRED, Policing/Shapin, HSRP, RPR, NSF/NSR, Fast Ethernet, Gigabit Ethernet, Serial, HSSI, Sonet (POS), VLAN, VTP, VMPS, ISL, dot1q, DTP, Spanning tree, PVST |
| **Security & Firewalls** | Cisco FWSM/PIX/ASDM, Nokia Checkpoint NG, Juniper SRX, Cisco FWSM/PIX/ASDM, Palo Alto (PA-2k/3k/5k/7k/7050/220/3200), Cisco ASA, Checkpoint, Blue Coat proxy server. Port Security, DHCP Snooping, IP Source Guard (IPSG), Cisco FWSM/PIX/ASDM, Nokia Checkpoint NG, Juniper SRX, Juniper SRX, SSL Decryption, NAT, ACL, IPS/IDS, VPNs (Site-to-Site, IPSEC, DMVPN), TACACS+, RSA SecurID,  |
| **Switches** | T1/E1 – T3/E3/OCX (Channelized, Fractional & full), CEF, MLS, Ether Channel, Cisco 7010, Cisco 7018, Cisco 5020, Cisco 2148, Cisco 2248, EX8200, EX4500, EX4200, EX3200, EX2500, EX2200 Series, Cisco 2960, Cisco 3560, Cisco 3750, Cisco 6500 series, Catalyst 6500, MSFC, MSFC2, 7600, 3700, 3500, ATM, FRAME RELAY, MPLS, VPNs |
| **Routers** | Cisco GSR 12416, 12418, Cisco 7200vxr, Cisco 3640, Cisco 3600, E, J, M and T- Series |
| **Networking Protocols** | IGRP, EIGRP, OSPF, BGPv4, MP-BGP, HDLC, PPP, MLPPP |
| **SDN & SD-WAN** | Cisco SD-WAN (Viptela), Versa, Silver Peak, Cisco ACI, Cisco DNAC, SD-Access |
| **Load Balancers** | F5 BIG-IP (GTM 12.x, ASM 14.x, APM 13.x), A10 Thunder TPS, Citrix NetScaler ADC, F5 BIG-IQ 7.x |
| **Tools & Monitoring** | Infoblox, SolarWinds (NetFlow, LEM), Splunk (MLTK), Cisco ISE (2.6/2.7), Blue Coat, Blue Cat, Cisco Prime |
| **Cloud and Automation Tools** | AWS (Transit Gateway, Direct Connect), Azure (Traffic Manager, DDoS Protection), GCP (Cloud DNS, Firewall Rules), Python, Ansible, Terraform, YAML, REST APIs, Git, CI/CD pipelines. |
| **Wireless**  | Cisco Meraki, Aruba (WPA3, Mobility Master), Ekahau Pro, Cisco Unity, VOIP (CUCM, RTMT, VNQM) |
| **Virtualization & Management** | VMware Horizon, vRealize Ops, UCS, Arista MLAG, VXLAN |

**Professional Experience:**

**Senior Network Engineer | Client: Spirit Airlines, FL | July 2024 – Present**

**Project Overview:**

Spirit Airlines’ enterprise-wide WAN transformation initiative, migrating from legacy MPLS to a cloud-enabled SD-WAN architecture across 50+ airports, headquarters, and data Centers. Designed and implemented a high-availability, secure, and cost-efficient WAN backbone that improved resiliency, optimized application performance, and supported the airline’s growing cloud adoption strategy.

**Responsibilities:**

* Led SD-WAN migration across 50+ sites, replacing MPLS with **Cisco Viptela SD-WAN / Cisco Meraki** to improve resiliency and reduce operational costs.
* Designed high-availability WAN architecture using **BGP, OSPF, and IPSec VPNs**, ensuring seamless failover and uninterrupted connectivity for flight scheduling, ticketing, and crew management systems.
* Conducted capacity planning and traffic analysis across WAN links with **SolarWinds & NetFlow**, right-sizing bandwidth allocations to support peak travel seasons and passenger growth.
* Integrated **Azure ExpressRoute and AWS Direct Connect** cloud on-ramps, enabling secure, low-latency access to SaaS/cloud workloads while reducing backhaul through data Centers.
* Implemented **QoS policies** across **WAN** links to prioritize mission-critical airline applications over guest Wi-Fi and non-essential traffic.
* Deployed centralized security policies with **Cisco Firepower (FTD/FMC)** and **Zero Trust (Cisco ISE, ZTNA)** principles, ensuring compliance with **PCI-DSS, FAA, and TSA** standards.
* Hardened WAN security with **ACLs, IDS/IPS, VPN encryption (AES-256/IPSec)**, and micro-segmentation across airport and data Center networks.
* Established disaster recovery (DR) failover strategy between **primary and backup Data Centers (Cisco Nexus/ACI fabric)**, achieving **<30-second** convergence during failover tests.
* Optimized application performance with **intelligent path control (App-Aware Routing)**, reducing average latency by **35%** and improving **SaaS**/**cloud** response times.
* Automated configuration management with **Ansible** and centralized orchestration via **Cisco vManage**, reducing manual changes by 40% and accelerating site deployments.
* Built real-time monitoring dashboards using **SolarWinds, NetFlow, and SNMP traps**, providing visibility into application health, link utilization, and end-to-end WAN performance.
* Collaborated with vendors (**Cisco, AT&T, Lumen, Verizon, Azure, AWS**) to implement a phased rollout with zero downtime during peak travel seasons.
* Negotiated **ISP**/**carrier** contracts, achieving significant cost reductions while enforcing **SLA** guarantees for high-availability circuits.
* Documented network designs with **Visio & Confluence** (topology diagrams, SOPs, runbooks), supporting troubleshooting, audits, and compliance.
* Mentored junior engineers on **Cisco SD-WAN, BGP routing, firewall policies, and automation with Ansible**, improving long-term operational readiness.
* Delivered measurable cost savings by reducing MPLS reliance and enabling **Direct Internet Access (DIA)** with SD-WAN security overlays.

**Tech Stack:** SD-WAN, MPLS, Cisco Viptela, Cisco Meraki, BGP, OSPF, IPSec VPN, Azure ExpressRoute, AWS Direct Connect, QoS, Cisco Firepower (FTD/FMC), Zero Trust, Cisco ISE, ZTNA, ACLs, IDS/IPS, VPN encryption (AES-256), micro-segmentation, Cisco Nexus/ACI, App-Aware Routing, Ansible, Cisco vManage, SolarWinds, NetFlow, SNMP, Visio, Confluence, AT&T, Lumen, Verizon.

**Client: Voya Financials, New York.**

**Role: Senior NETWORK ENGINEER | Jul 2021-** **June 2024**

**Responsibilities:**

* Designed and implemented secure **LAN/WAN architectures** using **OSPF, EIGRP, BGP, RIP, HSRP, VLANs, STP, VTP, QoS**, ensuring high availability and performance across enterprise networks.
* Administered and secured **Cisco ASA firewalls, Catalyst/Nexus switches, ASR 9K routers, and Meraki SD-WAN**, including **ACLs, NAT/PAT, ISE, and NAC** for access control.
* Migrated legacy **Bluecoat/IronPort** proxies to **Zscaler ZIA/ZPA**, enabling **Zero Trust Network Access (ZTNA)** and cloud-first security.
* Deployed and managed **Okta IAM (SSO, MFA, SAML, OAuth)** and **CrowdStrike endpoint protection**, enforcing governance and compliance with **GDPR, HIPAA, PCI DSS**.
* Implemented **AWS networking** solutions including **Transit Gateway, VPC Security Groups, IPSec VPNs, and CloudWatch monitoring** for hybrid cloud environments.
* Delivered enterprise-grade **load balancing and application redundancy** using **F5 BIG-IP LTM/GTM, Radware**, improving uptime for mission-critical applications.
* Provided advanced troubleshooting of **LAN/WAN/WLAN infrastructure**, collaborating across IT teams to resolve incidents and minimize downtime.
* Created detailed **Visio network diagrams, change management documentation**, and supported **data Center operations** (Linux, Windows, OpenStack, NetScaler, F5).

**Tech Stack:** Cisco ASA, Catalyst, Nexus, ASR9K, Meraki, F5 BIG-IP LTM/GTM, Radware, Juniper MX/PTX/EX/SRX, Okta, Zscaler ZIA/ZPA, CrowdStrike, AWS (VPC, Transit Gateway, Security Groups, CloudWatch, EC2), BMC Remedy, Wireshark, SolarWinds, Lucent DWDM, MPLS, IPSec, GETVPN, HSRP, QoS.

**Client: Cigna Health, CT | Jan 2019 – Jun 2021**

**Role: Network Engineer**

**Responsibilities:**

* Designed, deployed, and optimized enterprise network infrastructure supporting digital transformation initiatives across multiple Data Centers.
* Configured and maintained **Cisco routers and switches (Catalyst, Nexus)** for high availability, redundancy, and low-latency connectivity.
* Implemented
* and troubleshot **WAN technologies** including **MPLS, VPNs, IPSec tunnels**, and **site-to-site connectivity**.
* Managed **load balancing** and **traffic distribution** using **F5 BIG-IP** to enhance application performance and reliability.
* Conducted network monitoring, analysis, and troubleshooting using **SolarWinds**, **Wireshark**, and other diagnostic tools.
* Assisted in **cloud network integration** with **Azure** and **AWS**, including **virtual networks**, **VPN gateways**, and **hybrid connectivity**.
* Applied advanced **security configurations**, **firewalls**, and **access controls** to meet healthcare compliance standards (HIPAA).
* Developed network **configuration standards, documentation, and best practices** for enterprise deployments.
* Performed network **capacity planning**, **traffic analysis**, and optimization to support growing workloads.
* Collaborated with **application, server, and security teams** to ensure seamless deployment of enterprise applications and services.
* Participated in **network upgrade projects**, including **firmware updates**, **device replacements**, and architecture improvements.
* Assisted in **disaster recovery** and **business continuity planning** by designing redundant network paths and failover mechanisms.
* Provided mentoring and technical guidance to junior engineers on **network design, troubleshooting, and best practices**.
* Implemented **network automation** and orchestration using **Python, PowerShell, and Ansible** to improve operational efficiency.
* Coordinated with **vendors** for hardware/software support, troubleshooting, and maintenance across enterprise network systems.

**Tech Stack:** Cisco ISR/ASR routers, Cisco Catalyst & Nexus switches, F5 BIG-IP load balancers, enterprise firewalls; MPLS, VPNs, IPSec tunnels, site-to-site connectivity, BGP, OSPF, RIP, VLANs, redundancy protocols; Microsoft Azure (Virtual Networks, VPN Gateways, Hybrid Connectivity), AWS (VPC, VPN, hybrid connectivity); SolarWinds, Wireshark, Python, PowerShell, Ansible, firewalls,

**Client: T-Mobile, WA |Dec 2017 – Dec 2018**

**Role: Network Engineer**

**Responsibilities:**

* Deployed and upgraded **4G LTE networks** across multiple regions, which improved capacity by more than 30% and supported the growing customer base.
* Configured and maintained **Cisco 2600/2900/3600 routers**, setting up **RIP, EIGRP, OSPF, BGP, and MPLS** to improve routing and connectivity.
* Worked on **LAN/WAN technologies** such as **ISDN, Frame Relay, ATM, NAT/PAT, DHCP, TCP/IP, and Radius**, handling day-to-day installation and troubleshooting.
* Set up and managed **Access Control Lists (ACLs)** to allow secure access for users and restrict unauthorized traffic across the network.
* Configured **Spanning Tree Protocol (STP)** to prevent loops and **VTP** for Inter-VLAN routing, ensuring stable and efficient switching.
* Troubleshot connectivity problems using **PING, Traceroute, and SolarWinds**, quickly identifying issues and reducing downtime.
* Installed and upgraded **Checkpoint Security appliances and software**, strengthening the overall security of enterprise systems.
* Wrote and used **Python scripts** to automate routine testing and configuration checks, reducing manual work and saving time.
* Supported **FCoE protocols** for data centers, helping carry Fibre Channel traffic over Ethernet to improve storage networking.
* Monitored and managed **multi-customer ISP environments**, handling alarms, escalations, and ensuring network uptime met SLA requirements.

**Tech Stack:** Cisco 2600/2900/3600 Routers, Catalyst Switches, MPLS, BGP, OSPF, EIGRP, RIP, ISDN, Frame Relay, ATM, NAT/PAT, DHCP, TCP/IP, Radius, ACLs, STP, VTP, FCoE, Checkpoint Security, SolarWinds, Python.

## Client: Sun TV Network (India), Chennai | Mar 2015– Aug 2017

## Role: Network Engineer

## Responsibilities:

* Managed **multicast and broadcast traffic** using **Cisco 5520 WLC and VLAN configurations** for 20+ live events annually, delivering sub-50ms latency for video streams.
* Monitored and maintained **QoS policies on voice and video traffic** with **Cisco Prime and RTMT**, resolving 95%+ of transmission issues before impact.
* Designed and enforced **ACLs and firewall policies** on **ASA and Juniper SRX**, segmenting production, corporate, and guest networks for compliance and security.
* Collaborated with broadcast engineers to troubleshoot **jitter and packet loss** issues at the network layer, leveraging **QoS, BGP routing, and Ekahau tools**.
* Assisted in deployment and configuration of **5 DTH and 2 IPTV head-end systems**, ensuring bandwidth allocation and connectivity for 60K+ subscribers.
* Conducted regular **security audits and vulnerability scans** on devices such as **Websense, Blue Coat, and ASA firewalls** to safeguard content and user data.
* Provided **Level 2/3 support** for 200+ network incidents, leveraging **Cisco Unity, ASA, and Juniper SRX** for troubleshooting while managing 10+ CRQs weekly.
* Planned and executed 50+ **maintenance windows** annually, achieving 99.99% uptime across **24/7 broadcast operations** supported by Cisco/Juniper gear.

**Tech Stack:** Cisco 5520 WLC, ASA Firewalls, VLANs, BGP, QoS, Cisco Prime, Cisco RTMT, Juniper SRX, Ekahau, Cisco Unity, Websense, Blue Coat.

**Education:**

**Bachelor of Engineering** **– Computer Science | 2011-2015**
MVSR Engineering College, India

**Certifications:**

* CCNA – Cisco Certified Network Associate
* CCNP – Cisco Certified Network Professional