Caio B. Franca

Senior Network Engineer | Network Automation | Cloud & On-Prem | L1-L3 Ops | CCNA

braga.caio@outlook.com | LinkedIn | GitHub

Professional Summary

Senior Network Engineer with 10+ years of experience managing global-scale, high-availability infrastructure across enterprise, data center environments. Currently supporting Meta network operations within OCS, focusing on L2/L3 troubleshooting, multi-vendor environments, and operational support.

Proven expertise in L2-L3 troubleshooting, enterprise routing/switching (Cisco, Juniper, Arista, Nexus), and infrastructure operations. Strong collaborator across cross-functional and global teams, streamlining network workflows. Familiar with cloud networking concepts in Azure and AWS, as well as SD-WAN (Velocloud), Palo Alto, Fortinet firewall policies, and F5 load balancing.

Key strengths: Global-scale network operations, SLA-driven incident response, observability tooling, process improvement, configuration hygiene, documentation, and automation-driven support in complex, regulated environments.

Core Competencies

• **Enterprise Networking:** BGP, OSPF, MPLS, VLANs, STP, EtherChannel, VRRP, HSRP

• **Multi-Vendor Environments:** Cisco IOS/NX-OS, Juniper, Nexus, Arista, HP ProCurve

• **Incident Response & Operations:** L1–L3 troubleshooting, RCA, SOP/MOP development, NOC workflows, major incident handling

• **Network Automation:** Python (scripts & tooling), Ansible, Terraform (foundational), REST APIs, Git

• **Monitoring & Diagnostics:** SolarWinds, Wireshark, tcpdump, SNMP, NetFlow, Zabbix, Splunk

• **Cloud & Hybrid Networking:** Azure & AWS – VPC/VNet, VPN, Subnetting, Cloud Peering, Hybrid Integration

• **Security & Access Control:** Palo Alto, Fortinet, Check Point (familiar), ACLs, VPNs, Zero Trust, IDS/IPS

• **Governance & Compliance:** ISO 27001, GDPR, Change Management, Audit Documentation, Risk-aware Ops

Portfolio & Projects

Explore my portfolio and network engineering projects: https://caiofrnca.github.io/

Certifications & Education

• Postgraduate Certificate in Cybersecurity Management – MTU Ireland (2025–2026)
• Higher Diploma in Science in Computing – CCT College, Dublin (2021)
• Amazon Cloud Architect Solution - SAA-C03 (in progress)
• CompTIA Security+ (Valid until Aug 2026)
• Google Professional Certificate (2024)
• BSc (Hons) in Computing Science, Estácio de Sá University (2018)
• Cisco CCNA R&S Coursework (2018)

Work Experience

Network Operations Engineer – Meta (via Astreya), Dublin, Ireland
May 2025 – Present

• Operates and supports Meta's global enterprise and data center networks across a complex multi-vendor stack, including Cisco (IOS/NX-OS), Juniper, Arista, and Nexus platforms.

• Troubleshoot and resolve L1–L3 issues across physical and logical layers, handling faults, escalations, and major incidents to ensure availability and service continuity.

• Collaborate with global operations, engineering, and deployment teams across regions, contributing to backbone and fabric stability within hyperscale environments.

• Drive incident response by performing RCA, impact assessments, and follow-ups, with clear stakeholder communication through internal monitoring and ticketing systems.

• Assist network automation teams by contributing to Python and Ansible scripts used for log parsing, inventory audits, and alert enrichment to reduce manual overhead.

• Improve operational playbooks and MOPs to streamline escalation paths and reduce MTTR.

• Support network observability through dashboard enhancements, metric refinement, and alert tuning.

• Manage VLAN changes, DNS updates, subnet assignments, and vendor RMA coordination.

• Maintain exposure to cloud-native networking via Meta's hybrid infrastructure and tooling, enhancing conceptual knowledge in multi-cloud environments.

• Familiar (theoretical exposure): Velocloud SD-WAN, Palo Alto firewall policy models, F5 load balancing – through documentation review and collaboration with internal teams.

IT Deployment Operations & Asset Management Associate – PwC Ireland, Dublin, Ireland
June 2022 – May 2025

• Led deployment and secure configuration of IT assets across PwC offices, including laptops, mobile devices, and networking hardware, following strict compliance and encryption policies.

• Delivered Tier 1/2 support for VPN, endpoint security, access issues, printers, and OS/application-related tickets.
• Supported global hybrid environments through patch management, system updates, and remote troubleshooting.
• Contributed to IT asset lifecycle management, maintaining clean inventory records and aligning with audit requirements.
• Worked with infrastructure and network teams on escalated cases, assisting in resolving user provisioning and access control challenges.

IT Support Engineer – PFH Technology Group (Clients: PwC, Irish Rail, Dublin Bus), Ireland
Nov 2021 – June 2022

• Provided on-site and remote support for enterprise clients in the public and private sector, focusing on network access, VPN tunnel troubleshooting, and endpoint connectivity.
• Diagnosed hardware, software, and basic network issues, escalating complex cases appropriately.
• Delivered device provisioning and supported secure onboarding processes for users.
• Coordinated with client-side IT departments and vendors for escalations and incident recovery.

Network Operations Centre (NOC) Engineer – RTM – Rede de Telecomunicações para o Mercado, Brazil - April 2012 – April 2019

• Supported the nationwide MPLS backbone used by Brazil's financial sector, managing over 1800 network devices (Cisco, Juniper, Huawei) in high-availability environments.
• Handled L1/L2/L3 incident response and service degradation affecting BGP, OSPF, VLANs, STP, and EtherChannel configurations, ensuring compliance with SLA targets.
• Collaborated with senior engineers on design and implementation of network expansion projects, including new POP integrations, redundancy upgrades, and customer onboarding initiatives.
• Played a key role in executing project rollouts from planning to deployment, assisting in site surveys, device provisioning, and documentation.
• Used monitoring platforms (SolarWinds, SNMP, NetFlow) to proactively identify performance issues and validate fixes.
• Adhered to strict documentation and change control processes as per Central Bank of Brazil operational standards.
• Gained early exposure to ACLs, firewall configurations, and access provisioning for regulated financial customers.

References

Available upon request.