

Technical Lead - Networks

Reports to:	Platforms & Infrastructure Manager	Tenure:	Permanent
Department:	Digital, Systems & Information (DS&I)	Group:	Business Services
Location:	Avalon	Direct Reports:	Nil
Budget:	Nil	Career Path:	Specialist
Job Family:	Operations, Data & Technology	Career Step:	Senior Specialist 1 / Band 8
Date:	May 2025		

Purpose

The Technical Lead – Networks position provides senior network engineering expertise and technical leadership to ensure the reliability, security and continuous improvement of GNS Science's physical and cloud-based network infrastructure. They collaborate closely with service providers, consultants, internal stakeholders, architects and engineers to lead the design, implementation, configuration, monitoring and management of network and firewall systems.

Position Priorities and Responsibilities

Technical Leadership

- Provide technical network leadership, mentoring, direction and advice to the team to lift the technical knowledge, competency and skill levels
- Leads the development, implementation and continuous improvement of network procedures, systems and tools for the team's efficient operation in consultation with other technical leads and architects
- Maintains deep knowledge of network and data telecommunication technologies and works alongside architects and other technical leads and senior engineers to provide technical direction for GNS networks and networked solutions
- Contributes to the development of the technology roadmap for network technologies
- Contribute to the design and implementation of Zero Trust Architecture principles across GNS Science's network infrastructure.
- Plan, prioritise and deliver high availability and performant infrastructure together with capacity growth that matches our organisational need
- Develop and maintain network-related components of business continuity and disaster recovery plans.
- Build effective working relationships with the various technology teams that depend on GNS networks for day-to-day operations
- Collaborate with cybersecurity, DevOps, and platform teams to ensure network infrastructure supports secure and efficient service delivery.

- Supervise specialist external technical consultancy

Network Engineering, Management and Support

- Configure, deploy and maintain LANs, WANs, and wireless networks, including servers, routers, firewalls, switches, UPSs, and other hardware.
- Plan and execute network changes, in coordination with DS&I teams, vendors, and other internal stakeholders with network critical dependencies.
- Monitor the performance of network equipment, initiating action as required.
- Deploy and manage network observability tools (e.g. SNMP, Zabbix, Prometheus, Grafana) to ensure visibility and performance optimization
- Interact with third-party hardware and network providers, ordering changes and requesting support as necessary.
- Maintain network configuration, documentation, and other relevant data stores.
- Maintain firewall configuration, documentation, procedures, and other relevant data stores.
- Implement Infrastructure as Code practices using tools such as Terraform or Ansible to automate network provisioning and configuration.
- Stay current with emerging network technologies and security threats; recommend and pilot innovative solutions to improve network resilience and efficiency.
- Provide second and third level support to the Service Desk on network related issues
- Provide rostered on call after hours support, to respond to high priority incidents raised by our SOC and mitigate accordingly.

InfoSec Support

- Be aware of GNS security guidelines and support others in working on Cyber Security issues and events
- Provide training and support to other IT staff in InfoSec and Cyber Security issues, including in ensuring secure processes.
- Contribute to making GNS Science's software, hardware, networks and data secure by:
 - identifying, reporting and assisting team members and GNS to eliminate InfoSec risks
 - immediately reporting all InfoSec incidents and near misses to DS&I Management
 - promoting a culture where InfoSec is given priority
 - Assist in developing and improving InfoSec policies, processes and procedures

Responsibilities of all Employees

- Comply with the expectations that relate to your career step (you can find these on GNS Online).
- Comply with all GNS Science policies and procedures.
- Contribute to making GNS Science a healthy and safe place to work by complying with the responsibilities and accountabilities outlined in the Health and Safety Management System Framework.
- Have an understanding or interest in Māori relationship and development issues and Te Reo Māori.

- Work effectively as a team member by fostering good relationships and supporting others by providing coverage of other functions as required and ensuring workloads are evenly spread.
- Have the flexibility to adapt and develop as the company and its environment evolves.

Key Working Relationships

- Data Science Platform team, Monitoring and Response Operations Lead, NGMC Staff, External hardware and service vendors and consultants (e.g. Sempre, REANNZ, Kordia, etc)

Person Specification

Skills, Knowledge and Attributes

- Deep understanding of networking technologies and protocols (e.g., BGP, OSPF, VLAN, IPSEC, NAT, QoS).
- Strong knowledge of IP address management, subnetting, and IPv6.
- Experience with enterprise-grade network hardware and firewall systems (preferably including Dell, Juniper and FortiGate).
- Proficiency with Linux environments and command-line tools.
- Familiarity with scripting languages and automation tools.
- Experience with DevOps, configuration management, and software-defined networking.
- Strong understanding of network security principles and practices.
- Skilled in using version control systems (e.g., Git) and peer review tools (e.g. GitLab, GitHub).
- Excellent problem-solving, documentation, and communication skills.
- Ability to interpret and convey complex, detailed technical concepts clearly.
- An ability to absorb information and communicate fast and effectively, both orally face to face and over the phone, and in writing by email, instant messaging and in documentation
- Ability to travel occasionally as required.
- Able to occasionally work outside of regular business hours, to undertake planned service changes.

Qualifications and Experience

Essential

- Bachelor's degree in Information Technology, Computer Science, or a related field, or equivalent industry experience.
- Demonstrated ability to provide technical leadership across a diverse range of network projects/products in an agile environment over the last 3-5 years
- At least five years enterprise networking experience, using a range of wired and wireless technologies and bandwidths
- At least five years of enterprise firewall management experience, preferably using fortigate products.

- In-depth experience with internal and inter-networking service configuration of at least one major public cloud provider, preferably AWS and Azure.

Desirable

- Industry recognised network professional certification, (e.g. CCIE, JNCIE)
- Experience contributing to or leading enterprise network architecture design.
- Demonstrated high level customer service experience (including dealing with complex information and de-escalating conflict)
- Proficiency in incident response and handling, including the ability to analyse and respond to security events and incidents in a timely manner.