

POSITION DESCRIPTION

Senior Network Engineer



EXECUTIVE POSITION DETAILS

Position Title	Senior Network Engineer
Classification	HEW8
Position Number	NEW
School/Office	Digital Services
Division	Operations

POSITION PURPOSE

The Senior Network Engineer provides advanced technical expertise in the implementation, operation, maintenance and continuous improvement of the University's network infrastructure. The position helps ensure secure, stable and high-performing network services across the University's multi-campus environment, supporting teaching, research and operational needs.

The role is responsible for resolving complex network issues, implementing approved network changes, monitoring service performance, maintaining technical standards and documentation, and supporting infrastructure lifecycle and remediation activities. It works collaboratively with Network, Cybersecurity, Infrastructure, Platform and project teams, as well as external vendors and managed service providers.

The position also contributes to network transformation and project initiatives, including segmentation, network access control, secure connectivity, observability and the transition of new or changed services into reliable BAU operations.

KEY ACCOUNTABILITIES

Network operations and support

- Maintain the availability, performance, security and reliability of network services.
- Diagnose and resolve complex network incidents and recurring network problems.
- Monitor network health, capacity, utilisation and performance trends.
- Participate in operational support and escalation arrangements appropriate to the role.

Engineering and lifecycle management

- Configure and implement approved network changes, upgrades and refresh activities.
- Contribute technical input to network design and planning.
- Address ageing infrastructure, technical debt, stability and lifecycle risks.
- Maintain configurations, standards, procedures and operational records.

Security and compliance

- Implement network security controls aligned with approved architectures and policies.
- Support firewalls, segmentation, NAC, secure access and network telemetry.
- Work with Cybersecurity teams on risk treatment, control uplift and compliance activities.
- Follow incident, problem, change and configuration-management practices.

Projects and service improvement

- Contribute to campus network, Wi-Fi, segmentation and secure connectivity initiatives.
- Support testing, implementation, operational readiness and handover into BAU.
- Identify and implement opportunities for automation, observability and service improvement.
- Coordinate technical delivery with internal teams, vendors and managed service providers.

QUALIFICATIONS, EXPERIENCE AND SKILLS

- Tertiary qualification in Information Technology, Network Engineering, or equivalent experience
- Demonstrated experience in enterprise network implementation, support, and operations
- Experience working within complex or multi-campus environments
- Strong troubleshooting, analytical, and communication skills
- Ability to work collaboratively across technical teams and vendors

Network Transformation Experience

- Experience supporting network segmentation or Zero Trust uplift initiatives in enterprise environments
- Hands on experience implementing or supporting NAC solutions (e.g. Aruba ClearPass)
Experience working with segmentation controls, firewall policies, and access enforcement
Exposure to secure access services (SSE), proxy, or cloud-delivered security controls
Experience supporting large scale network remediation or transformation programs
- Understanding of network-related cyber risk, control uplift, and compliance practices

Technical Proficiency

- Proven experience with enterprise network platforms across a multi-vendor environment, including Cisco, HPE Aruba (switching, wireless and ClearPass), Palo Alto (NGFW and secure access), and Ruckus wireless; experience with application delivery platforms (e.g. Citrix ADC/NetScaler), segmentation and access control technologies, and network security integration is highly regarded
- Network monitoring and management tools (e.g. SolarWinds, NetFlow, SNMP, HP IMC)
- Strong understanding of IPv4/IPv6, VLANs, QoS, and segmentation principles
- Understanding of Zero Trust Architecture and segmentation design concepts
- Experience with segmentation tooling and enforcement technologies (e.g. Illumio or similar)
- Experience integrating network telemetry into monitoring or SIEM platforms

Desirable

- Certifications such as CCNP Enterprise or equivalent, with strong preference for Aruba certifications (e.g. ACMP, ACSP, ClearPass) and Palo Alto certifications (e.g. PCNSE),

particularly where aligned to network access control, segmentation, and secure access platforms

- Experience or certification in Citrix (e.g. ADC/NetScaler) and Ruckus wireless technologies
- Additional certifications or experience in Zero Trust / SASE (e.g. Prisma Access, Zscaler), micro-segmentation technologies (e.g. Illumio), network automation (e.g. Cisco DevNet), DDI/IPAM platforms (e.g. EfficientIP, Infoblox), and cloud networking (e.g. Azure Network Engineer AZ-700)
- Experience in higher education or large enterprise environments
- Familiarity with AARNET or research network environments

KEY RELATIONSHIPS

This position reports to: Manager, Network Operations

This position supervises:

- None

Key internal relationships:

- Network and Infrastructure teams
- Cyber Security Engineering
- IT Operations and Platform Services
- Project delivery teams

Key external relationships:

- Network and security vendors
- Managed service providers

CHALLENGES

- Supporting network performance and reliability across a complex, multi-campus environment
- Managing competing priorities across BAU operations, incidents, and project delivery
- Maintaining consistency across a multi-vendor network ecosystem
- Supporting delivery of a complex, multi-workstream network segmentation and security uplift program
- Balancing project activities with ongoing service stability

UNIVERSITY EXPECTATIONS

The University expects that all employees are aware of, and comply with legislation and Western's policies and procedures relevant to the position, including but not limited to:

- Code of Conduct
- Work Health and Safety and Wellbeing Management System
- Enterprise Agreement or Award
- Anti-discrimination principles, Equal Employment Opportunity and staff and student equity.

Approved by: Chief People Officer

Date: 28 Aug 2026