



JOB DESCRIPTION

Post Details:

Post Title:	Engineer (Digital Communications Services)	Organisational Element:	NISC- Network as a Service (NaaS)
		Job Family:	Digital Backbone Engineering
Rank/Grade:	G15		
Military/Civilian:	CIV	Location:	Mons

Organisation context:

This is a position within the NATO Communications and Information Agency (NCIA), an organization of the North Atlantic Treaty Organization (NATO).

To strengthen the Alliance through connecting its forces, the NCIA delivers secure, coherent, cost effective and interoperable communications and information systems in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes to the NATO HQ, the NATO Command Structure and NATO Agencies.

Organisational Element Statement of Functions:

The NATO Infrastructure Service Centre (NISC) Business Area Lead (BAL) is accountable for planning and executing the full lifecycle management activities (design, transition and operations) for the identified area of responsibility. NISC provides generic, domain independent, technical functionality that enables and facilitates the operation and use of Information Technology resources. NISC services (including: subject matter expertise; acquisition; project management, operations and maintenance; and, disposal) are provided in the following technical domains: Network Services (to include routing, switching and transmission services), infrastructure hosting, storage and processing, infrastructure networking, hardware and software management, databases and web platform services, as well as identity management. Services, are provided throughout the lifecycle to both internal and external customers in both static and deployable settings.

The Network as a Service (NaaS) Area of Responsibility (AoR) spans all network infrastructure hardware, software, services, management, and licensing components enabling the provisioning, deployment, network management, maintenance, lifecycle and vendor management of the on-premises, cloud and multi-cloud network infrastructure, services and connectivity.

Job role description:

An Engineer (Digital Communications Services) is a professional responsible for designing, implementing, and maintaining the core network architecture that connects different devices and platforms, establishing a robust and seamless communication backbone that enables data flow and connectivity across various departments and locations, both on premises and cloud internetworking. This involves configuring, troubleshooting and optimizing routers, switches, firewalls, and other hardware/software networking elements to optimize network performance and ensure data integrity and security. They stay updated with emerging technologies and play a crucial role in establishing and maintaining a robust, reliable and efficient digital backbone supporting efficient operations and digital transformation initiatives.

Duties and Responsibilities:**Information security**

- Applies and maintains specific security controls as required by organisational policy and local risk assessments.
- Communicates security risks and issues to business managers and others.
- Performs basic risk assessments for small information systems.
- Contributes to the identification of risks that arise from potential technical solution architectures.
- Suggests alternate solutions or countermeasures to mitigate risks.
- Defines secure systems configurations in compliance with intended architectures.
- Supports investigation of suspected attacks and security breaches.

Systems design

- Designs system components using appropriate modelling techniques following agreed architectures, design standards, patterns and methodology.
- Identifies and evaluates alternative design options and trade-offs.
- Creates multiple design views to address the concerns of the different stakeholders and to handle functional and non-functional requirements.
- Models, simulates or prototypes the behaviour of proposed system components to enable approval by stakeholders.
- Produces detailed design specifications to form the basis for the construction of systems.
- Reviews, verifies and improves own designs against specifications.

Network design

- Specifies the technical configurations and components required for a small network or a network segment in a more complex infrastructure.
- Follows organisational architectures and standards.

Network support

- Carries out agreed network maintenance tasks and specified operational configuration of network components.
- Establish and diagnose network problems/faults using the required troubleshooting methodology and tools.
- Uses network management software and tools to collect agreed performance and traffic statistics.

Systems installation and removal

- Installs or removes hardware or software, using supplied installation instructions and tools, including handover to the clients.

- Uses standard procedures and diagnostic tools to test installations, correct problems, and document results.
- Records details of all components that have been installed and removed.
- Assists users and follows agreed procedures for further help or escalation.
- Contributes to the development of installation procedures and standards.

Additional duties for this post:

Be responsible for implementing, and maintaining network infrastructure. Their duties typically include:

- **Network Design & Implementation** – Plan, configure, and deploy routing protocols (e.g., OSPF, BGP, IS-IS).
- **Routing Optimization** – Optimize routing tables and traffic flow for performance and redundancy.
- **Troubleshooting & Support** – Diagnose and resolve routing issues, including latency, congestion, and failures.
- **Security & Compliance** – Implement route filtering, prefix lists, and security policies to prevent unauthorized access.
- **Capacity Planning** – Monitor network usage and plan for scalability and growth.
- **Documentation & Reporting** – Maintain network diagrams, change logs, and incident reports.
- **Collaboration** – Work with other teams (e.g., security, data center, cloud) to ensure seamless connectivity.
- **Software & Firmware Management** – Upgrade and patch routers to maintain security and stability.
- **Testing & Lab Work** – Conduct network simulations and testing before deploying changes.
- **On-Call Support** – Be available on a rotating basis for after-hours network incidents and escalations.

Enterprise Security Operations Center (ESOC) – Take assigned shifts in the ESOC to monitor and manage network operations in real-time.

Education, Experience and Training (essential):

Education:

A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in a related discipline and 2 years post-related experience.

Or exceptionally, the lack of a university degree may be compensated by the demonstration of a candidate's particular abilities or experience that is/are of interest to NCIA, that is, at least 6 years extensive and progressive expertise in duties related to the function of the post.

Experience:

At least 2 years practical experience with the designing, implementing, and maintaining the core network architecture for large organizations.

Good practical experience configuring, troubleshooting and optimizing routers, switches, firewalls, and other hardware/software networking elements.

Good communication and interpersonal skills.

Good analytical skills and problem-solving attitude.

Training/Certifications:

- Education, Experience and Training (desirable): Knowledge and experience of the following domains
- Routing and Protocol Expertise: Proficiency in dynamic routing protocols (OSPF, BGP, IS-IS) and traffic engineering techniques, with a strong foundation in IPv4/IPv6 networking. MPLS, IPv6, Segment Routing, QoS.
- SD-WAN and Network Virtualization: Hands-on experience deploying, managing, and optimizing SD-WAN solutions for modern enterprise environments. Software Defined (SDx) (e.g. SDN, SD-WAN, SDDC, SASE) Network Functions Virtualization (NFV)
- Troubleshooting and Automation: Advanced troubleshooting skills combined with knowledge of network automation tools (e.g., Python, Ansible) for efficient configuration and monitoring.
- Prior experience of working in an international environment comprising both military and civilian elements
- Knowledge of NATO responsibilities and organization, including ACO and ACT.
- Valid Cisco Professional Certification or other vendor network professional certifications are mandatory. Expired certifications will not be considered.

Behavioural competencies:

- Relating and Networking - Easily establishes good relationships with customers and staff; relates well to people at all levels; builds wide and effective networks of contacts; uses humour appropriately to bring warmth to relationships with others.
- Delivering Results and Meeting Customer Expectations - Focuses on customer needs and satisfaction; sets high standards for quality and quantity; monitors and maintains quality and productivity; works in a systematic, methodical and orderly way; consistently achieves project goals.
- Adapting and Responding to Change - Adapts to changing circumstances; tolerates ambiguity; accepts new ideas and change initiatives; adapts interpersonal style to suit different people or situations; shows an interest in new experiences.

Language:

A thorough knowledge of one of the two NATO languages, both written and spoken, is essential and some knowledge of the other is desirable.

Travel:

NOTE: Most of the work of the NCIA is conducted in the English language.

Business travel to NATO and national (NATO and non-NATO) facilities as well as frequent travel between the NCIA offices;

May be required to undertake duty travel to operational sites and theatres inside and outside NATO boundaries.

Work Environment:

Office Environment

