



# JOB DESCRIPTION

**Post Details:**

Post Title:	<b>Principal Technician (Digital Communications Services)</b>	Organisational Element:	CSU Brunssum
Military/Civilian:	Civilian	Location:	Brunssum, NL

**Organization 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 include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

**Organizational Element Statement of Functions:**

The Directorate of CIS Support Units (DCSU), led by the Director of CIS Support Units (DirCSUs), is the trusted collaborator for the Agency's global operational partners, overseeing the operational support functions essential for the delivery and maintenance of CIS communication and information services that are fundamental to NATO's overall mission and specifically to the local Command's mission. As a Directorate, the DCSU specializes in the delivery of essential CIS support services across the full range of CIS capabilities, operating as integral components of the Agency's service delivery and offering tailored assistance to ensure the effective setup, operation, and maintenance of critical communication and information systems across NATO entities, Nations and the Agency. The DCSU serves as a central hub for on-the-ground technical expertise, service portfolio management, and exercise support within the agency, serving as the face-to-face interface with customers everywhere the Agency operates and as such are attuned to their individual operational needs. DCSU supports its customers through the following delivery-focused value streams: 1) Manage, deliver and maintain assigned Communication and Information System (CIS) products and services for the NCIA's customers including NATO Headquarters (NHQ), NATO Command Structure (NCS), NATO Force Structure (NFS), NATO member Nations and internal Agency users; and 2) Liaison, planning and coordinating functions for Alliance Missions, Operations and Exercises.

The DCSU executes its core business by delivering catalogue services on behalf of the Agency's Business Areas, while delivering tailored non-catalogue services directly through local service agreements. Within this framework the DCSU holds key responsibilities fundamental to NATO's overall mission and specifically to the local Command's mission, providing the Agency's interface for supplying the C2 Catalogue of Services to customers that are planning and/or executing operations and exercises. It ensures that the Agency's responsibilities to deployed operations are met in line with the C2 arrangements, agreed Service Level Agreements (SLAs) and possible additional resources received through the Customer Request Form (CRF)/Price Proposal (PP) process. The unit provides the customer interface in a consultancy capacity to match/estimate customer requirements against those services available from the Agency. OPEX is also responsible for the coordination, with the units and other elements concerned, of the budget committed to

operations support and the coordination related to NCIA personnel's deployment. During major exercises, OPEX leads the execution of customer requested services in coordination with the Enterprise Service Operations Centre (ESOC). The DCSU serves as the primary advisor to the Chief of Staff (COS) on matters related to operational service delivery strategy, and is accountable to the General Manager (GM) for ensuring the Agency's delivery via units in 22 locations, spread across 12 countries and 8 time zones. DCSU Services are delivered in coordination with the ESOC and Agency Business Areas under the Enterprise Service Delivery Model (ESDM).

NCIA CIS Support Unit (CSU) Brunssum, located in Brunssum, NLD, is responsible to manage, deliver and maintain assigned Communication and Information Systems (CIS) products and services for the Agency's customers during peacetime, crisis and war throughout its assigned AoR and as otherwise directed. As the local service provider and Service Management Authority (SMA) for Joint Forces Command Brunssum (JFCBS), it supports the NCIA in delivering secure, reliable end-to-end services under the Enterprise Service Delivery Model (ESDM).

Under the direction of the Head, Service Operations Branch (SOB), the SOB is responsible for the provision of local CIS products and services as required in applicable service agreements. The SOB is responsible to deliver level one and two CIS support to catalogue services as specified in the ESDM under the direction of Agency Service Centers and/or the Enterprise Service Operations Centre (ESOC). The SOB is also responsible to deliver levels one to three CIS support to applicable non-catalogue services as defined in the relevant service agreement(s). The SOB is consulted in relation to the continual improvement program by reporting on key performance indicators in close coordination with the Service Level Management section. The SOB is locally responsible for the installation, operation, maintenance and administration of assigned Information and Communication Technology (ICT) hardware and software.

The SOB is responsible, on behalf of the CSU Commander, for the secure operation of all assigned CIS/ICT as directed by the NATO Cyber Security Centre (NCSC). The SOB is accountable for local actions as part of Agency incident management and service request management processes in coordination with the ESOC and SMB and deployment management in coordination with Service Management and Control (SMC) and the SMB. The SOB is consulted in relation to problem management, release management, event management, service validation and testing, configuration and change management, in support of the responsible Agency Service Centre or the SMB. The SOB comprises the following organizational elements: Technical Coordination Office (TCO), Digital Workplace Services Section, Application Management Section, Infrastructure Services Section (ISS) and the Cyber Security Support Section.

Accountable to Head ISS, the Digital Communications Services Principal Technician is responsible for local support to Infrastructure as a Service (IaaS) and their associated hardware on behalf of the NATO Infrastructure Services Centre. This support includes the installation and maintenance of internal networking infrastructure. The ISS provides level one and two CIS support on behalf of NISC and in coordination with the service centre and/or the ESOC, and full-stack support to locally deployed networks supporting local services. ISS is consulted in relation to problem management, deployment management, configuration and change management in support of the respective service owner and the SMB.

**Job role description:**

A Principal Technician (Digital Communications Services) supports the implementation, and maintaining of the core network architecture that connects different devices and platforms. They ensure that all systems are operating efficiently and securely, and that they are aligned with the organization's overall goals and objectives. He/she are configuring, troubleshooting and optimizing routers, switches and other hardware/software networking elements to optimize network performance and ensure data integrity and security. This role requires expertise in network architecture, cloud computing, cybersecurity, and data management. A Communications Services Principal Technician works closely with other IT professionals to ensure that the organization's digital infrastructure is optimized for performance and efficiency.

**Duties and Responsibilities:****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**

- Responsible for the full lifecycle management of LAN infrastructure, including provisioning, maintenance, inventory, operations, troubleshooting, and decommissioning.
- Design, deploy, and maintain campus LAN environments
- Monitor and troubleshoot network performance and connectivity issues
- Collaborate with cross-functional teams to ensure network reliability and security

**Systems integration and build**

- Configures the hardware and software environment as required by the system being integrated.
- Produces integration test specifications, conducts tests and records and reports on outcomes.
- Diagnoses faults and records and reports on the results of tests.
- Produces system integration reports.

**Additional duties for this post:**

- Leads the Digital Communications Services Team and provides SME guidance within the CSU AoR on all network related matters.
- Administers and implements technical solutions relating to Local Area Network (LAN) infrastructure and network security issues and manages the daily operations.
- Produces and maintains documentation related to daily activity logs, active and passive network configuration, network mapping, processes, Standard Operating Procedures (SOP) and service records within the AoR.
- Performs fault diagnosis and troubleshooting with the approved available network management toolset (e.g. Cisco ISE, Catalyst Center, DX Spectrum, LAN Sweeper) and maintain daily operations logs and uptimes in accordance with the Service Level Agreements (SLAs).

- Designs, proposes and completes routine maintenance schedules in accordance with the Agency and manufacture guidelines and monitors operational performance of the CSU network infrastructure.
- Carries out LAN infrastructure analysis and configuration in support of the Incident and Problem Management Processes.
- Investigates and proposes long-term solutions to re-occurring problems, and identify areas for greater efficiency.
- Routinely conducts in-depth technical analysis to assess network capacity, improves network performance, contributes to Business Continuity and Disaster Recovery Plans and, where necessary, submits Requests for Change to improve the LAN.
- Responsible for the installation, management, inventory and lifecycles programs of Switches, Routers and Wireless Controllers.
- Supervises work of contractors in Class 1 server rooms
- Maintains an awareness of all ongoing network infrastructure configuration and maintenance activities to build and maintain an up-to-date picture.
- Establishes, monitors and conducts On-The-Job Training (OJT) to ensure all personnel are proficient in their duties.
- Ensures compliance with NATO network security standards.
- Provides collaboration and assistance to other work sections within Service Operations Branch in support of mission requirements.
- Supports physical task requirements with the ability to lift up to 25 lbs.
- Deputises for higher grade staff as required.
- Performs other duties as required.

**Education, Experience and Training (essential):**

**Education:**

Higher vocational training in a relevant discipline with 3 years post-related experience. Or a secondary educational qualification with 5 years post-related experience.

**Experience:**

At least 3 years hands-on experience with the designing, implementing, and maintaining the core network architecture for large organizations.

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

Good communication and interpersonal skills.

Good analytical and problem-solving skills.

**Training/Certifications:**

**Education, Experience and Training (desirable):**

**Required Technical Skills & Experience**

- Strong expertise in campus routing and switching technologies based on Cisco IOS-XE and NX-OS platforms
- Hands-on experience with Cisco SD-Access, IS-IS, and LISP routing protocols
- Familiarity with Cisco Catalyst Center (formerly Cisco DNA Center)
- Demonstrated expertise in Cisco IOS-XE security technologies across enterprise routing and switching platforms, including segmentation, access control, infrastructure protection, and secure management
- Proficiency with Cisco Identity Services Engine (ISE)
- Solid understanding of multicast technologies and IGMP
- Good understanding of Cisco controller-based wireless networks

**Training/Certifications:**

- valid Cisco CCNA certification  
ITIL Foundation
- Cisco CCNP certification (Enterprise, Service Provider, Wireless, or Security)  
Cisco CCIE certification

**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.
- *Achieving Personal Work Goals and Objectives* - Accepts and tackles demanding goals with enthusiasm; works hard and puts in longer hours when it is necessary; seeks progression to roles of increased responsibility and influence; identifies own development needs and makes use of developmental or training opportunities

**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.

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

