



Title: Principal Network Engineer Position ID: 2026-0021	Type Position: Full Time Level: PL4 Annual Salary: \$138,600 - \$276,000
Primary Location: Colorado Springs, CO / ON-SITE (preferred)	Travel Required: 10% CONUS and HI
Alternate Location: Home office anywhere in USA	Contact: Technical: taxberg@stephensonstellar.org (Thomas Axberg) Human Resource: bmoyer@stephensonstellar.org (Barb Moyer)
Company Background: Stephenson Stellar Corporation (Stellar) is a nonprofit research and development organization focused on assuring our nation remains a global leader in the Space Domain. Our mission is to foster technological innovation and provide secure space-based solutions. Stellar is an equal opportunity employer, and all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, national origin, age, disability status, protected veteran status, or any other characteristic protected by law. Additional information at: www.stephensonstellar.org	
Job Description: In this position, you will serve as a Principal Network Engineer supporting multiple advanced defense and space programs with a primary focus on the Space Development Agency (SDA), U.S. Space Force, and other DoD customers. You will provide technical leadership for engineering teams responsible for designing, integrating, securing, testing, and evaluating space-based network architectures supporting next-generation satellite constellations and mission systems. The ideal candidate possesses extensive experience leading network engineering efforts supporting space systems, satellite communications (SATCOM), mission operations centers, and ground infrastructure. Experience designing secure end-to-end communications across satellites, tactical users, terrestrial networks, cloud environments, and ground stations is highly desirable. Experience working with commercial and government satellite operators, telecommunications providers, cloud service providers, and defense contractors on both technical and contractual matters is required. The candidate must be capable of directly interfacing with customers on highly technical engineering issues, systems architecture, technical risk management, and program execution. Strong leadership, exceptional communication skills, and outstanding analytical and problem-solving abilities are essential. Under the direction of the Program Manager, the candidate will lead engineering efforts supporting research, development, integration, testing, cyber assessments, and operational evaluation of networking technologies. Responsibilities include Secure integration of space communications components and systems; Network modeling and simulation; Technology demonstrations; Prototype evaluations; Mission assurance assessment support; Network performance analysis; Communications resiliency assessments; and Zero Trust implementation across hybrid network environments.	
Requirements Clearance: Active U.S. Security Clearance required; TS/SCI preferred. Citizenship: Candidate must be a United States citizen. Required Education: BS in Computer Science, Computer Engineering, Electrical Engineering, Network Engineering, Information Technology, Cybersecurity, Aerospace Engineering, or related discipline. Desired Education: MS in Computer Science, Electrical Engineering, Network Engineering, Cybersecurity, Systems Engineering, Aerospace Engineering, or related discipline. Required Experience: • 10+ years designing, engineering, integrating, or operating secure network infrastructures supporting space systems and defense communications architectures. • 10+ years of experience supporting space vehicle communications, ground systems, mission operations, and satellite networking. • 10+ years designing enterprise and tactical IP networks including IPv4/IPv6, BGP, OSPF, Ethernet switching, MPLS, SDN, QoS, WAN/LAN/MAN, multicast, and network resiliency. • 5+ years leading technical teams supporting satellite networking, mission operations centers, ground stations, or hybrid terrestrial/non-terrestrial networking. • 5+ years managing technical projects involving telecommunications providers, satellite operators, cloud providers, equipment manufacturers, and government customers. • 3+ years supporting cybersecurity engineering including Zero Trust Architecture, network segmentation, firewalls, IDS/IPS, SIEM, RMF, DoD STIG implementation, vulnerability assessments, and cyber testing. • Experience supporting space networking test events, mission rehearsals, operational demonstrations, or developmental test activities. • Experience integrating commercial and government space systems into resilient mission architectures.	

**Desired Experience:**

- Experience with commercial LEO and MEO constellations and operators (e.g., SpaceX Starlink, OneWeb/Eutelsat, Amazon Kuiper, Telesat Lightspeed, SES/O3b mPOWER, Iridium).
- Experience with space-to-space (inter-satellite) networking and routing across proliferated LEO meshes, including optical inter-satellite links (OISL)/laser crosslinks and RF crosslinks.
- Experience with direct-to-device / direct-to-cell and 3GPP Non-Terrestrial Networks (NTN), including satellite-hosted LTE eNodeB or 5G gNodeB interfaces (e.g., Starlink Direct to Cell, AST SpaceMobile, Lynk).
- Experience with adaptive link management for LEO (e.g., ALMM) and dynamic resource and beam management.
- Experience with Ground-Station-as-a-Service and virtualized ground segments (e.g., AWS Ground Station, Azure Orbital, KSAT, Viasat Real-Time Earth).
- Experience with SDA Transport Layer or similar proliferated LEO architectures.
- Experience supporting U.S. Space Force, Space Systems Command, SDA, Missile Defense Agency, NASA, or commercial satellite operators.
- Experience with Software Defined Satellites.
- Experience with cloud-native networking supporting space missions.
- Experience with network automation using Python, Ansible, Terraform, or REST APIs.
- Experience with digital engineering and Model-Based Systems Engineering (MBSE).
- Experience supporting cyber assessments across satellite and ground infrastructures.
- Ability to clearly communicate highly technical engineering concepts to executive leadership and non-technical stakeholders.

Required Certifications:

- CISSP
- CCNP Enterprise
- CCNP Security
- CCIE Enterprise Infrastructure

Preferred Certifications:

- Security+
- CASP+
- AWS Advanced Networking
- AWS Security Specialty
- DoD 8140-compliant cybersecurity certification

Technical Skills:

The successful candidate will possess deep technical knowledge in:

Space Systems Networking: Space vehicle communications architectures, satellite payload networking, inter-satellite networking concepts, mission data transport architectures, space transport layer networking concepts, and software-defined satellite networking.

Network Engineering: IPv4/IPv6, MPLS, Software Defined Networking (SDN), segment routing, QoS, multicast, network automation, Continuity of Operations (COOP).

Ground Systems: Ground stations, satellite operations centers (SOC) / mission operations centers (MOC) / network operations centers (NOC), ground infrastructure modernization, tactical communications nodes.

Cybersecurity Responsibilities: Zero Trust Architecture, defense-in-depth, least privilege, identity-based networking, SIEM integration, DoD STIG implementation, RMF, NIST 800-53, NIST 800-207, cyber resiliency for satellite and ground networks.