LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
Class Code 4885
Unit C

WAN SPECIALIST II

DEFINITION

Programs, configures, analyzes, manages and monitors enterprise routers, firewalls, Virtual Private Network (VPN) systems, cache engines, core switches, and auxiliary support devices and systems. Provides specialized data, voice, video, security and systems analysis expertise to ensure integrity and availability of the District's enterprise Wide Area Network (WAN).

TYPICAL DUTIES

Troubleshoots and corrects complex interconnectivity and interoperability WAN issues related to network voice, video, data and security systems and supporting enterprise network devices.

Analyzes, installs, configures, and maintains security infrastructure and/or advanced auxiliary support systems to enterprise network devices, including but not limited to authentication and access control servers and devices, system logging utilities, traffic shaping systems, content filtering systems monitoring and alerting systems, traffic analysis systems, event correlation systems, intrusion detection systems, and vulnerability assessment systems.

Troubleshoots, diagnoses, and corrects internal and external data, and/or security-related network issues utilizing network management systems.

Performs regular system administration, installs software patches, reviews logs, and resolves data and/or security events.

Audits availability and performance of enterprise network devices, including servers and application appliances, to assure service availability.

Implements, configures, upgrades and tests WAN, carrier, or enterprise level network equipment, devices, and systems.

Diagnose, troubleshoots, and corrects network service issues related to Voice over IP (VoIP) systems (including multi-service infrastructure issues), video, and/or security systems.

Assists in the implementation and/or design of voice, video, and/or security solutions.

Develops and maintains documentation and diagrams for network or security environments.

Assesses security threats posed by changes in network hardware or architecture.

Monitor WAN performance and performance of WAN support systems to ensure effective and reliable service availability.

Acts as a liaison with service providers to resolve problems and resume digital service.

Provides technical assistance to other District service provider organizations and District locations.

Uses appropriate applications or appliances to determine and resolve WAN or security issues.

Provides assistance and/or acts as a mentor to lower level information technology staff and new employees.

Performs related duties as assigned.

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

A WAN Specialist II programs, configures, analyzes, and monitors advanced auxiliary WAN support equipment, and/or maintains security infrastructure and provides specialized voice, video, and security expertise to ensure reliability of the District's enterprise network.

The Coordinator of IT, Security is responsible for the planning, development, implementation, and management of computer network security technologies and services for the information services function.

The Design Network Engineer supervises lower-level technicians and contractors assisting in the planning, managing, and implementing current and emerging technologies from an enterprise level.

A WAN Specialist I installs, programs, configures, analyzes and repairs monitors, maintains, services, repairs, basic core WAN equipment and remote site WAN equipment, and diagnoses and repairs hardware/software problems that affect connectivity to within the District’s enterprise network.

SUPERVISION

Supervision is received from ~~a~~ the Coordinator of IT, Security or Director of IT, Network Operations. Work direction may be exercised over technical lower-level personnel

CLASS QUALIFICATIONS

Knowledge of:

Enterprise routing and switching

Current firewall, VPN, content filtering, and intrusion detection methodologies

Common Enterprise digital circuits, including ATM, ADSL, SONET, ADN, ISDN, Frame Relay, T1, DS3, and OC3-OC196

Domain Name System (DNS), including service structure, and server maintenance and operation

Common Authentication, transmission protocols, security procedures, industry standard encryption protocols, and methodologies

Security configuration of Microsoft Windows desktop and server

Common wireless network configuration and network protocols including TCP/IP, SNA, ICMP, STP, 802.1pq, channeling protocols, VLAN trunking protocols, NAT, RADIUS, TACACS+, SNMP, syslog, NTP, SNMP, IPSEC, MPLS, and various implementations of Access Control Lists

Common WAN protocols and routing protocols including RIP, OSPF, BGP, GRE, VPN protocols, and multicast protocols such as BGMP, IGMP, and MBGP

Common VoIP protocols such as H.323, H.235, MGCP, and SIP, and Gateway protocols such as MGCP, and H.261/H.263/H.264 802.11 Wireless protocols

Cisco AVVID (Architecture for Voice, Video and Integrated Data) Solutions

Unity Systems and Unified Messaging

Advanced concepts in data security over TCP/IP networks, such as Intrusion Detection Systems (IDS), Event correlation, DDOS mitigation, content filtering, vulnerability detection and analysis, and layer 7 packet analysis and control

Use of common desktop computer software packages including but not limited to Microsoft Office and Visio

Safety regulations and practices applicable to electrical and electronic repairs

Ability to:

Install, configure, maintain and troubleshoot complex data, voice and video network equipment

Install, configure, maintain, and troubleshoot network security devices, such as authentication appliances, Intrusion Detection Devices, event logging and analysis systems, and/or advanced enterprise network support equipment; Router Access Control Lists and Firewall Rule sets

Understand application protocols and the effect of wide area network issues that affect application availability

Detect and correct security problems that affect wide area network availability and reliability

Design and implement technical modifications to enterprise-wide networks and/or firewall, VPN, content filtering, and intrusion detection rule sets

Learn characteristics of new security threats, vulnerabilities, and countermeasure techniques and technology
Work effectively without supervision
Maintain effective working relationships with District personnel

ENTRANCE QUALIFICATIONS

Education:

Graduation from a recognized college or university with a bachelor's degree in data communications, network engineering, computer science, information systems, electrical engineering, math, telecommunications management, or a related field. Qualifying experience in addition to that listed below, may be substituted for the required education on a year-to-year basis.

Experience:

Three years of general experience in the installation, maintenance, and support of wide area networks, and related equipment. At least two of the three years must include technical experience in at least one of the following areas:

Supporting, implementing, and configuring enterprise voice over IP environments

Support of advanced enterprise security technologies including but not limited to enterprise intrusion detection, enterprise monitoring and alerting systems, authentication/authorization appliances and systems, event correlation and analysis systems, or vulnerability assessment and remediation systems

Supporting videoconferencing with experience with Polycomm and Tandberg systems including MCU's, Gateways and Gatekeepers over IP networks

Supporting a large metropolitan data network with a minimum of 1,000 nodes and 10,000 network components including edge routers, MDF switches, WAN Core switches and distribution routers.

Successful completion of courses in support of wide area networks, security, and digital electronics in the armed forces or equipment manufacturer's training program or recognized trade school or college may be substituted for up to one year of the required experience.

Special:

A valid California Driver License.
Use of an automobile.
A minimum of one of the certifications listed below is required:
Cisco Certified Network Professional (CCNP)
Cisco Certified Security Professional (CCSP)
Cisco Certified Voice Professional (CCVP), or equivalent Avaya certification
Cisco advanced certifications (such as CCIE), or Cisco Specialist Certifications are preferable.

SPECIAL NOTE

Employees in the class are subject to call at any hour.

This class description is not a complete statement of essential functions, responsibilities, or requirements. Requirements are representative of the minimum level of knowledge, skill, and/or abilities. Management retains the discretion to add or change typical duties of a position at any time.

Revised	Reviewed
09-28-11	07-31-13
SJ	SJ