	For the entry-level employee, all tasks are typically done under supervision for as much as the first year and then with some independence with verification after the employee has more experience.	
	Task	**Key Performance Indicators**
	INSTALL	
T-1	Configure and optimize network, routers, and switches (e.g., higher-level protocols, tunneling).	Installation or upgrade plan is complete and accurate and company guidelines are followed. All components and devices (including IoT) are properly connected. Operating system and application software and upgrades are installed and configured according to specifications. Required network protocols are correctly installed and tested. System hardware and software are configured to specification. Network interfaces (e.g. LAN to WAN) are correctly connected and configured. Network security devices and software (e.g., firewall, routers, anti-virus software) are correctly installed by peer reviews or supervisor. Accounts are set up following standard operating procedures. Final overall tests to ensure full network resilience and functionality are properly performed. Current software upgrades including operating system patches anti-virus database are installed. Requirements for systems security are properly identified, by peer reviews or supervisor. Communication regarding changes in procedures is distributed to all necessary parties in a timely manner.
T-3	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware) which would include patch network vulnerabilities to safeguard information.	
T-4	Install or replace network, routers, and switches.	
T-9	Implement group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	
T-12	Validate/update baseline system security according to organizational policies.	
T-15	Install, update, and troubleshoot systems/servers.	
T-21	Installation, implementation, configuration, and support of system components.	
	TROUBLESHOOT	
T-2	Diagnose network connectivity problem.	Appropriate data analysis and troubleshooting techniques per organizational standard are used to diagnose the problem. Problem is correctly identified and causes are isolated per organizational standard. Solutions are thoroughly tested and implemented with minimal risk to network performance per organizational standard. Problems, solutions and implementation processes are thoroughly documented and clearly communicated per organizational standard.
T-22	Troubleshoot faulty system/server hardware.	
T-24	Troubleshoot hardware/software interface and interoperability problems.	
	DOCUMENT	
T-11	Follow SOP and validate/update documentation of compliance.	New configuration, system specifications and installation and test results are clearly and completely documented. Systems security procedures are properly documented and approved in accordance with company guidelines. Documentation follows company format and standards and is at the appropriate level of detail. Inventory of parts includes accurate identification, tagging and location. Accurate and up-to-date records (e.g., device configuration and user accounts) are maintained to ensure system integrity.
	MONITOR, MAINTAIN, OPERATE	
T-5	Integrate new systems into existing network architecture.	Integration and testing are performed according to project and company schedules, priorities and guidelines. Preventive maintenance plan and monitoring procedures are updated. Documented performance requirements are used to monitor network and recommend system improvement. System configuration is optimized to meet user needs with minimal disruption. Performance is monitored according to procedures and is compared to baseline performance for discrepancies; reports are generated. Traffic capacity and performance characteristics are monitored, and technician knows how to involve others to handle concerns. Component and connectivity problems are monitored and reported. Functional verifications, system audits and backups are performed according to proper procedures Patches are applied to affected software and hardware in a timely manner, and are properly tested. Disruptions, outages, security violations and attacks of network services are monitored, recognized, and escalated in a timely manner according to company procedures. Diagnostic software is run to verify that the components are operating, and tests are performed. System backups and other maintenance tasks are performed and documented according to scope, schedule and procedure. System back-ups are verified and periodic test restores are performed. Components are correctly programmed, integrated into the system and backed up and all security procedures are followed. Tests for functionality and safety of equipment and systems are completed. Communication regarding changes in procedures is distributed to all necessary parties in a timely manner.
T-6	Monitor network capacity and performance.	
T-7	Test and maintain network infrastructure including software and hardware devices.	
T-8	Conduct functional and connectivity testing to ensure continuing operability.	
T-10	Support group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	
T-13	Manage accounts, network rights, and access to systems and equipment.	
T-14	Provide ongoing optimization and problem-solving support.	
T-16	Check system hardware availability, functionality, integrity, and efficiency.	
T-17	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	
T-18	Implement local network usage policies and procedures.	
T-19	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	
T-20	Monitor and maintain system/server configuration.	
T-23	Perform repairs on faulty system/server hardware.	