

Certificate in Networking Security Specialist

Program Details

The Networking Security Specialist Certificate is designed for students who are interested in acquiring the skills and knowledge necessary to work in the fields of IT and networking specialists and to pass the Cisco CCNA certification exam. Students will receive hands-on competency-based instruction geared toward entry-level employment in the IT and networking industries. On completion of the program, students will have the skills required for IT and networking careers in industries including healthcare, financial services, fashion, and entertainment and for continued credentialing in Cisco Networking Systems and/or degree programs such as IT, engineering, math, and science.

Additional Information

The Cisco CCNA Certification exam is the responsibility of the student.

Program Outcomes

By the completion of this program, successful students will be able to:

1. Assemble and Configure PC Components: Identify, install, upgrade, and maintain internal computer hardware elements, including motherboards, CPUs, RAM, power supplies, and storage devices—to fulfill client performance specifications.
2. Deploy and Support Mobile Devices: Configure, synchronize, and secure mobile hardware platforms (smartphones, tablets, and laptops) while managing cellular and wireless connectivity.
3. Set Up Basic Network Infrastructures: Implement and configure small office/home office (SOHO) networks, managing physical cabling, TCP/IP ports, wireless protocols, and fundamental networking hardware like switches and routers.
4. Manage Multi-OS Client Environments: Install, configure, and manage diverse client operating systems—including Microsoft Windows, macOS, Linux, ChromeOS, Android, and iOS—utilizing commands and administrative utilities.
5. Apply Physical and Logical Security Safeguards: Deploy foundational cybersecurity countermeasures, including malware remediation, access control permissions, data destruction techniques, and browser security settings, to protect corporate endpoint systems.
6. Troubleshoot Client-Side Faults: Isolate, diagnose, and resolve technical issues spanning hardware devices, operating system software, applications, and local connectivity problems using a systematic, industry-recognized troubleshooting methodology.
7. Leverage Virtualization and Cloud Infrastructures: Differentiate between cloud computing concepts (SaaS, PaaS, IaaS) and configure local client-side virtualization setups to support modern hybrid work environments.
8. Demonstrate Professional Operational Procedures: Practice professional communication, exercise proper safety protocols, adhere to environmental compliance guidelines, implement standard backup procedures, and utilize entry-level scripting basics.
9. Design and Implement IP Addressing Schemes: Calculate and implement efficient IPv4 and IPv6 addressing hierarchies using Variable Length Subnet Masking (VLSM) to meet specific organizational requirements.
10. Configure Layer 2 Switch Infrastructure: Configure and optimize local network components, including VLANs, Trunking, EtherChannel, and Spanning Tree Protocol (STP), to build resilient, loop-free switched networks.
11. Manage Enterprise Routing Mechanisms: Configure and troubleshoot static routing and single-area OSPFv2 across interconnected routers to establish stable IP connectivity.
12. Deploy Network Infrastructure Services: Implement and verify essential network operations services including DHCP, NAT, DNS, NTP, and Quality of Service (QoS) policies.
13. Mitigate Infrastructure Security Threats: Secure network devices using the Cisco CLI and deploy fundamental security countermeasures, including Access Control Lists (ACLs), Layer 2 security features, and secure remote management protocols (SSH).
14. Evaluate Wireless Architectures: Set up and secure a Wireless Local Area Network (WLAN) using Wireless LAN Controllers (WLCs) and modern security frameworks (WPA2/WPA3).
15. Analyze Network Automation and Programmability: Critique modern network management frameworks, distinguishing between traditional networks and controller-based architectures using REST APIs, JSON data structures, and automation tooling.
16. Diagnose and Troubleshoot Network Faults: Isolate and resolve complex connectivity issues across layered network infrastructures using systematic troubleshooting workflows and monitoring applications like Syslog and SNMP.

Academic Map

Certificate in Networking Security Specialist

A minimum of 4 classes and 16 credits is required. At least 8 credits of your program must be taken at Massasoit. Note: Each course completed and passed can only fulfill one program requirement. The same course cannot be used to satisfy multiple program requirements.

Semester 1

4 Credits in ISEC 129
IT Essentials
4 Credits in ISEC 130
Introduction to Networks

Semester 2

4 Credits in ISEC 131
Switching, Routing, and Wireless Essentials

Semester 3

4 Credits in ISEC 132
Enterprise Networking, Security, and Automation

This academic map is a suggested semester-by-semester guide to keep you on a clear path to program completion. Please note that some classes are offered only in certain semesters, have prerequisites, or minimum passing grades. Winter and/or Summer Session classes may be available for some classes. Your [academic advisor](#) will provide you with clear direction needed to stay on course and discuss scheduling options with you. Taking courses not reflected on this map may result in courses not counting toward the completion of your requirements.