CompTIA Network+ Certification Training

Course Materials

The CompTIA Network+ Certification Training course is developed with CompTIA Approved Quality Content (CAQC) from McGraw-Hill Professional:

Meyers, Mike. *Mike Meyers' CompTIA Network+ Guide to Managing and Troubleshooting Networks (Exam N10-008).* 6th edition, McGraw-Hill, 2022. ISBN: 9781264269037

Meyers, Mike and Jonathan S. Weissman *Mike Meyers' CompTIA Network+ Guide to Managing and Troubleshooting Networks Lab Manual (Exam N10-008).* 6th edition, McGraw-Hill, 2022. ISBN: 9781264274734

130+ video lectures from best-selling author and trainer Mike Meyers and his team at Total Seminars, who have developed educational and entertaining video training. The Total Seminars videos cover important course concepts, exam objectives, and tips and tricks for preparing for the CompTIA Network+ certification exam.

(These texts are available as e-textbooks included in your enrollment. Students may find used, new, or rental print copies online or at local bookstores.)

Course Description

This course provides students with a CompTIA certification path designed to help them prepare for and pass the CompTIA Network+ N10-008 Certification Exam to become CompTIA Network+ certified. The course aligns to CompTIA Network+ competencies, including network architecture, network operations, network security, troubleshooting, industry standards and practices, and network theory. Additionally, the course offers students CompTIA Network+ practice exams and a CompTIA Network+ exam discount for students who complete the course.

NOTE: CompTIA certification exam or exam voucher is not included in the course and must be completed at a Pearson|Vue Test Center.

Course Objectives

After completing this course, you will be able to:

- Describe basic network theory concepts
- Explain the purposes and uses of ports and protocols
- Explain the concepts and characteristics of routing and switching.
- Configure the appropriate IP addressing components given a scenario.

- Compare and contrast the characteristics of network topologies, types and technologies
- Given a scenario, implement the appropriate wireless technologies and configurations
- Summarize cloud concepts and their purposes.
- Explain the functions of network services.
- Understand Infrastructure
- Deploy the appropriate cabling solution given a scenario
- Determine the appropriate placement of networking devices on a network and install/configure them
- Explain the purposes and use cases for advanced networking devices.
- Explain the purposes of virtualization and network storage technologies.
- Compare and contrast WAN technologies.
- Understand Network Operations
- Given a scenario, use appropriate documentation and diagrams to manage the network
- Compare and contrast business continuity and disaster recovery concepts.
- Explain common scanning, monitoring and patching processes and summarize their expected outputs
- Given a scenario, use remote access methods.
- Identify policies and best practices.
- Understand Network Security
- Summarize the purposes of physical security devices.
- Explain authentication and access controls.
- Given a scenario, secure a basic wireless network.
- Summarize common networking attacks.
- Given a scenario, implement network device hardening.
- Explain common mitigation techniques and their purposes.
- Understand Network Troubleshooting and Tools
- Given a scenario, use the appropriate tool.
- Given a scenario, troubleshoot common wired connectivity and performance issues.
- Given a scenario, troubleshoot common wireless connectivity and performance issues.
- Given a scenario, troubleshoot common network service issues.

Course Prerequisites

It is suggested, though not required, that students have their CompTIA A+ Certification and at least 9 to 12 months of networking experience before attempting their CompTIA Net+ certification.

Important Terms

In this course, different terms are used to designate tasks:

- **Lab Manual Exercise**: A non-graded assignment from the course lab manual.
- **Practice Exam:** An ungraded online test.
- **Exam**: A graded online test.

Academic Integrity Statement

Academic integrity is the pursuit of scholarly activity in an honest, truthful and responsible manner. Violations of academic integrity include, but are not limited to, plagiarism, cheating, fabrication and academic misconduct. Failure to comply with the Academic Integrity Policy can result in a failure and/or zero on the attempted assignment/examination, a removal from the course, disqualification to enroll in future courses, and/or revocation of an academic transcript.

Course Completion Policy

In order for a course to be considered complete, all required coursework must be attempted, submitted, and graded. Required coursework consists of graded assignments. Any Academic Integrity Policy violations may prevent a course from being considered complete.

Course Evaluation Criteria

Your score provides a percentage score and letter grade for each course. A passing percentage is **70%** or higher.

There are a total of 1000 points in the course:

Topic	Assessment	Points Available
3	Graded Exam 1	80
6	Graded Exam 2	80
9	Graded Exam 3	80
12	Graded Exam 4	80
12	Graded Midterm Exam	140
15	Graded Exam 5	80
18	Graded Exam 6	80
21	Graded Exam 7	80
22	Graded Final Exam	300
Total		1000

Course Topics and Objectives

Topic	Topic Title	Subtopics	Objectives
1	Network Models	• Working with Models • The OSI Seven-Layer Model in Action • The TCP/IP Model • The Tech's Troubleshooting Tools	• Describe how models such as the OSI seven-layer model and the TCP/IP model help technicians understand and troubleshoot networks • Explain the major functions of networks with the OSI seven-layer model • Describe the major functions of networks with the TCP/IP model
2	Cabling and Topology	• Network Topologies • Cabling and Connectors • Networking Industry Standards - IEEE	• Explain the different parts of network topologies • Describe the different types of network cabling and connectors • Describe the IEEE network standards
3	Ethernet Basics	• Ethernet • Early Ethernet Networks • Expanding and Enhancing Ethernet Networks	• Define and describe Ethernet • Explain early Ethernet implementations • Describe ways to extend and enhance Ethernet networks
4	Ethernet Standards	• 100-Megabit Ethernet • Gigabit Ethernet • Ethernet Evolutions • Beyond Network+	• Describe the varieties of 100-megabit Ethernet • Discuss copper- and fiber-based Gigabit Ethernet • Discover and describe Ethernet varieties beyond Gigabit
5	Installing a Physical Network	• Understanding Structured Cabling • Installing Structured Cabling • NICs • Diagnostics and Repair of Physical Cabling	• Recognize and describe the functions of basic components in a structured cabling system • Explain the process of installing structured cable • Install a network interface card • Perform basic troubleshooting on a structured cable network
6	TCP/IP Basics	• The TCP/IP Protocol Suite • CIDR and Subnetting • IP Address Assignment	• Describe how the TCP/IP protocol suite works • Explain CIDR and subnetting • Describe the functions of static and dynamic IP addresses
7	Routing	• How Routers Work	• Explain how routers work

Topic	Topic Title	Subtopics	Objectives
		• Dynamic Routing • Working with Routers	• Describe dynamic routing technologies • Install and configure a router successfully
8	TCP/IP Applications	• Transport Layer and Network Layer Protocols • The Power of Port Numbers • Common TCP/IP Applications	• Describe common Network and Transport layer protocols • Explain the power of port numbers • Define common TCP/IP applications such as HTTP, HTTPS, Telnet, SSH, email (SMTP, POP3, and IMAP4), and FTP
9	Network Naming	• Before DNS • DNS • Diagnosing TCP/IP Networks	• Analyze and configure early name resolution solutions • Describe the function and capabilities of DNS • Use common TCP/IP utilities to diagnose problems with DNS
10	Securing TCP/IP	• Making TCP/IP Secure • TCP/IP Security Standards • Secure TCP/IP Applications	• Discuss the standard methods for securing TCP/IP networks • Compare TCP/IP security standards • Implement secure TCP/IP applications
11	Switch Features	• Virtual Private Networks • Switch Management • Virtual LANs • Multilayer Switches	• Describe the features and functions of VPNs • Define the capabilities and management of managed switches • Configure and deploy VLANs • Implement advanced switch features
12	IPv6	• IPv6 Basics • Using IPv6 • Moving to IPv6	• Discuss the fundamental concepts of IPv6 • Describe IPv6 practices • Implement IPv6 in a TCP/IP network
13	WAN Connectivity	• Telephony and Beyond • The Last Mile • Using Remote Access • WAN Troubleshooting Scenarios	• Describe WAN telephony technologies, such as SONET, T1, and T3 • Compare last-mile connections for connecting homes and businesses to the Internet • Discuss and implement various remote access connection methods • Troubleshoot various WAN scenarios

Topic	Topic Title	Subtopics	Objectives
14	Wireless Networking	• Wi-Fi Standards • Implementing Wi-Fi • Troubleshooting Wi-Fi	• Explain wireless networking standards • Describe the process for implementing Wi-Fi networks • Describe troubleshooting techniques for wireless networks
15	Virtualization and Cloud Computing	• Concepts of Virtualization • Virtualization Benefits • Virtualization in Modern Networks • To the Cloud	• Describe the concepts of virtualization • Explain why PC and network administrators have widely adopted virtualization • Describe how virtualization manifests in modern networks • Describe the service layers and architectures that make up cloud computing
16	Data Centers	• Mobile Network Technologies • Deployment Models • Scenarios	• Explain the capabilities of different mobile networking technologies • Describe common deployment schemes for mobile devices • Deal with sample security issues with mobile devices
17	Integrating Network Devices	• Designing a Basic Network • Unified Communication • ICS	• Explain the concepts of basic network design • Describe unified communication features and functions • Describe the function and major components of an ICS/SCADA network
18	Network Operations	• Risk Management • Contingency Planning • Safety	• Describe the industry standards for risk management • Discuss contingency planning • Examine safety standards and actions
19	Protecting Your Network	• Network Threats • Common Vulnerabilities • Hardening Your Network • Firewalls	• Discuss common security threats in network computing • Discuss common vulnerabilities inherent in networking • Describe methods for hardening a network against attacks • Explain how firewalls protect a network from threats

Topic	Topic Title	Subtopics	Objectives
20	Network Monitoring	• SNMP • Monitoring Tools • Putting It All Together	• Explain how SNMP works • Describe network monitoring tools • Discuss a scenario that uses management and monitoring tools
21	Network Troubleshooting	• Troubleshooting Tools • The Troubleshooting Process • Resolving Common Network Service Issues	• Describe appropriate troubleshooting tools and their functions • Analyze and discuss the troubleshooting process • Resolve common network issues
22	Course Final Examination		• Take your Final Exam • Take your CompTIA Certification Exam

Back to Top