CompTIA

N10-008 vs N10-007 Exam Objectives Comparison

Organizations and IT professionals face new network challenges and complexities as they navigate through increased security concerns, hybrid working environments, and the need for maximum performance and increased productivity. In today's digital world, it's more important than ever for organizations to trust that their networks are secure, uninterrupted and flexible. Updates to Network+ reflect current skills related to network engineers and prepares professionals to work effectively and efficiently, supporting and optimizing today's network environments.

CompTIA Network+ is updated to address many of the pressing issues organizations face today with their enterprise networks by validating foundational skills and competencies needed to maintain, deploy and troubleshoot essentials networks necessary to support business objectives.

CompTIA Network+ is accredited by ANSI as meeting the ISO/IEC 17024 standard and is approved by U.S. Department of Defense (DoD) to fulfill Directive 8570.01-M/8140 requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA).

CompTIA Network+

Exam Objectives Comparison

The following table aligns exam objectives from N10-008 to N10-007 for comparison. Skills are aligned by best match.

N10-008	N10-007	COMMENTS	MAPPING
1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.	1.2 Explain devices, applications, protocols and services at their appropriate OSI layers.	Data encapsulation added to N10-008.	Content added.
1.2 Explain the characteristics of network topologies and network types.	1.5 Compare and contrast the characteristics of network topologies, types and technologies.	IoT technologies moved.	Content moved.
1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	2.1 Given a scenario, deploy the appropriate cabling solution.	To better address professional specialization and appropriate job roles, cable management and implementations are no longer evaluated at a hands-on cognitive level	Cognitive level change.
1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.	1.4 Given a scenario, configure the appropriate IP addressing components.	Updated to include additional content related to IPv6 addressing.	Updated content.
1.5 Explain common ports and protocols, their application, and encrypted alternatives.	1.1 Explain the purposes and uses of ports and protocols.	No major changes.	
1.6 Explain the use and purpose of network services.	1.8 Explain the functions of network services.	No major changes.	
1.7 Explain basic corporate and datacenter network architecture.		New content that covers the growing impact of datacenters and enterprise use cases for networking professionals, including SDN.	New content.
1.8 Summarize cloud concepts and connectivity options.	1.7 Summarize cloud concepts and their purposes.	Expanded to include deployment models and infrastructure as code.	Content added.
2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.	2.2 Given a scenario, determine theappropriate placement of networking devices on a network and install/configure them.	Updated to include feature sets and address IoT, IPS, and IDS content within a single objective.	Content added.
	2.3 Explain the purposes and use cases for advanced networking devices.		
2.2 Compare and contrast routing technologies and bandwidth management concepts.	1.3 Explain the concepts and characteristics of routing and switching.	Routing and bandwidth is covered in a single objective to ensure greater visibility to the concepts.	
2.3 Given a scenario, configure and deploy common Ethernet switching features.	1.3 Explain the concepts and characteristics of routing and switching.	Switching is covered in its own objective and now appears at a hands-on technical level to ensure mastery of deployments and implementations.	Cognitive level change.

N10-008	N10-007	COMMENTS	MAPPING
2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.	1.6 Given a scenario, implement the appropriate wireless technologies and configurations.	No major changes.	
	4.3 Given a scenario, secure a basic wireless network.		
3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.	3.3 Explain common scanning, monitoring and patching processes and summarize their expected outputs.	Network performance and availability has been highlighted in this objective, with an emphasis on monitoring. The cognitive level is now at a hands-on technical level to better approximate the job role.	Cognitive level change.
3.2 Explain the purpose of organizational documents and policies.	3.1 Given a scenario, use appropriate documentation and diagrams to manage the network.	Documentation updated to reflect the changing nature of network administration within enterprise organizations, especially regarding business directives. The cognitive level is lower to reflect changes in the job role.	Cognitive level change.
	3.5 Identify policies and best practices.	This content area has been grouped under organizational documentation or removed from the exam.	Content changed.
3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.	3.2 Compare and contrast business continuity and disaster recovery concepts.	Content has been expanded to increase emphasis on redundancy and high availability.	Updated content.
4.1 Explain common security concepts..	4.2 Explain authentication and access controls.	Additional defensive security and risk management concepts added.	Updated content.
4.2 Compare and contrast common types of attacks.	4.4 Summarize common networking attacks.	Attacks have been organized to differentiate between social engineering and technology-based attacks.	Updated content.
4.3 Given a scenario, apply network hardening techniques.	4.5 Given a scenario, implement network device hardening.	Updated with additional wireless security measures and IoT access considerations.	Content added.
4.4 Compare and contrast remote access methods and security implications.	3.4 Given a scenario, use remote access methods.	The new objective reflects a security-first approach to the content while updating the cognitive level to better reflect the knowledge required in the job role.	Updated content.
4.5 Explain the importance of physical security.	4.1 Summarize the purposes of physical security devices.	Updated to include the importance of data security.	Updated content.

N10-008	N10-007	COMMENTS	MAPPING
5.1 Explain the network trouble-shooting methodology.	5.1 Explain the network trouble-shooting methodology.	No major changes.	
5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	5.2 Given a scenario, use the appropriate tool.	Content has been refined to more closely examine common connectivity issues due to improper or malfunctioning cables/cabling.	Content changed.
	5.3 Given a scenario, troubleshoot common wired connectivity and performance issues.	Content area included in 5.2 or distributed as appropriate in operational technologies.	Content moved.
5.3 Given a scenario, use the appropriate network software tools and commands.	5.2 Given a scenario, use the appropriate tool.	Objective updated to contain only software tools; hardware troubleshooting mostly moved to objective 5.2.	Content moved.
5.4 Given a scenario, troubleshoot common wireless connectivity issues.	5.4 Given a scenario, troubleshoot common wired connectivity and performance issues.	Reorganized to include specific problems that result in wireless connectivity issues.	Updated content.
5.5 Given a scenario, troubleshoot general networking issues.	5.5 Given a scenario, troubleshoot common network service issues.	Objective broadened to include both issues and considerations.	Content added.