CompTIA
Network +

COURSE CONTENT

CompTIA Network+ Introduction

The CompTIA Network+ certification validates your knowledge and skills of installing, managing, and troubleshooting networks on various platforms. This course is composed to help you learn all the required objectives to gain the CompTIA Network+ certification. You will learn the latest networking technologies available, various networks and networking protocols, identify VPN and VLAN features, DNS concepts, and implement wireless networks.
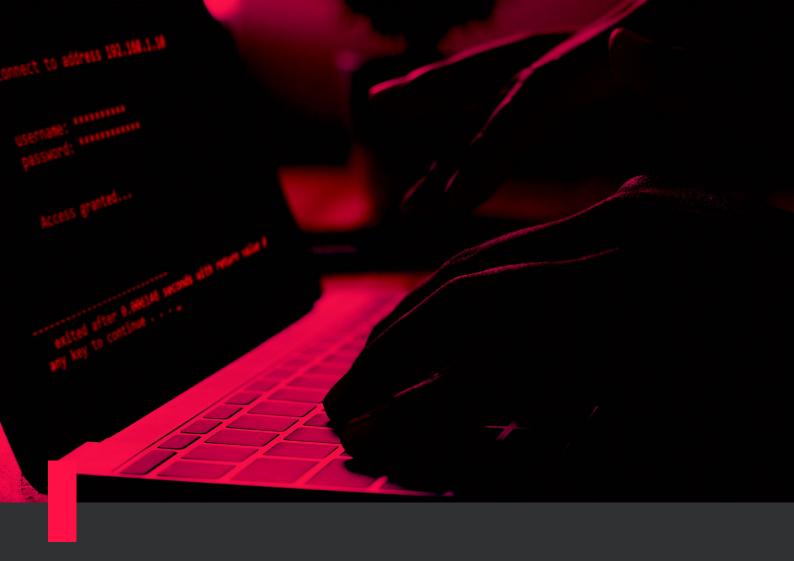
Why CompTIA Network+ with Infosec Train

The IT industry is one of the rapidly growing industries, and it is expected to grow in the future as well. Therefore, the demand for Networking professionals is continuously rising. CompTIA Network+ certification is one of the most preferred credentials by IT professionals. It validates candidate networking skills and emphasizes hands-on practical skills, ensuring that the candidates are well prepared to handle complex networking issues.More employers turn to CompTIA Network+ for baseline networking skills applicable across most of today's job roles. Network+ focuses on the latest trends and methodologies that support connectivity and performance.

Target Audience

- Anyone who wishes to enhance their knowledge and understanding of networking concepts

- Professionals looking forward to acquiring job skills in the network support and administration

- Students who are willing to start their career in cybersecurity

Pre-Requisite

> There are no required pre-requisites for Network+ certification.

> CompTIA A+ certification and/or 9 months of networking experience is recommended.

Exam Information

Exam code	N10-007
Number of Questions	Maximum of 90 questions
Type of Questions	Performance-based and multiple choice
Length of Test	90 minutes
Passing Score	720(on a scale of 100-900)
Languages	English, German, Japanese

CompTIA Network+ Course Objectives

> Explaining the purpose and uses of ports and protocols

> Explaining devices, applications protocols, and services on their appropriate OSI layers

> Explaining the characteristics and concepts of routing and switching

> Understanding to configure the appropriate IP address

> Understanding of network topologies types and technologies

> Implement the appropriate wireless technologies and configurations

> Explained the use cases for advanced networking devices

> Explain various types of networking attacks

Chapter 1: Fundamentals

Module A: Networking concepts

Module B: Classifying networks

Module C: Network models

Module D: The troubleshooting process

Chapter 2: Physical networks

Module A: Connection technologies

Module B: Network devices

Module C: Copper media

Module D: Optical media

Module E: Ethernet standards

Chapter 3: TCP/IP networkst

Module A: IP addressing

Module B: Core protocols

Module C: Network ports and applications

Chapter 4: Internetworking

Module A: Switching

Module B: Routing

Chapter 5: Wireless LANs

Module A: Wireless networks

Module B: Wireless LAN standards

Chapter 6: Wide area networks

Module A: Internet connections

Module B: WAN infrastructure

Chapter 7: Cybersecurity principles

Module A: Goals and threats

Module B: Digital security

Module C: Transport encryption

Chapter 8: Defending networks

Module A: Network security components

Module B: Network authentication systems

Module C: Hardening networks

Chapter 9: Evolving network technologies

Module A: Network convergence

Module B: Virtual and cloud systems

Chapter 10: Network operations

Module A: Monitoring and optimization

Module B: Fault tolerance and disaster recovery

Module C: Incident response

Chapter 11: Network planning

Module A: Network policy design

Module B: Network installation

Module C: Maintenance and upgrades

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com