



IT Foundations: Networking Specialist Online – IT106

190 hours

IT Foundations: Networking Specialist program is 190 hours and is designed to provide a quality information and computer technology education that serves as foundation for lifelong learning through the study, design, evaluation, and practical application of best practices in computer technology as it is applied to small, medium, and large size organizations.

In the foundations program, students will demonstrate:

- ✓ best practices and standards in Installation, configuration, and troubleshooting of networks, quality of service, virtual private networks, and broadband technologies for enterprise organizations.
- ✓ an understanding of network and inter-network routing protocols and technologies, network performance considerations, and traffic control over LAN or WAN.
- ✓ an understanding of skills and knowledge needed to plan, install, configure and maintain a variety of servers on any platform according to Industry Standard Server Architecture (ISSA).
- ✓ an understanding of general security concepts, communications security, infrastructure security, basics of cryptography, and operational/organizational security.

A+ Essentials Test 220-601:

Personal Computer Components

Overview/Description

To understand the names and purposes of, and how to install, configure, remove, and troubleshoot personal computer components

Target Audience

The audience for this path includes entry-level computer technicians who will, by the end of studying this path and before taking the exam, have accumulated 500 hours hand-on experience in a lab or in the field

Prerequisites

None

- Identify the features of storage devices, power supplies, and display devices
- Identify the features of motherboards
- Recognize the features of processors
- Recognize the features of memory, ports and cables, adapter cards, and input devices
- Recognize personal computer components and their purposes
- Install, configure, optimize, and upgrade personal computer components
- Identify troubleshooting and preventive maintenance techniques for personal computer components
- Perform basic troubleshooting on personal computer components in a given scenario
- Isolate and solve problems with PC components



Laptop Components, Peripherals, and Networks

Overview/Description

To understand the basic concepts of, and how to troubleshoot problems with, laptops, peripherals and networks connections

Target Audience

The audience for this path includes entry-level computer technicians who will, by the end of studying this path and before taking the exam, have accumulated 500 hours hand-on experience in a lab or in the field

Prerequisites

None

- Identify the features of laptop components, how to remove laptop hardware safely, and how to configure power management
- Recognize basic troubleshooting techniques and preventive maintenance for laptops and portable devices
- Recognize how to perform laptop-specific tasks in given scenarios
- Recognize the features of printers and scanners
- Recognize how to install, configure, and troubleshoot printers and scanners
- Recognize printer technologies and how to perform basic printer installation, configuration, and troubleshooting tasks
- Identify basic networking concepts
- Identify the characteristics of common network cables, connectors, and networking technologies
- Install and configure a network and identify network diagnostic and troubleshooting tools
- Determine how to configure and troubleshoot a wireless network connection on a laptop

Operating Systems

Overview/Description

To recognize the fundamentals of operating system technologies and the basic procedures involved in installing and upgrading operating systems

Target Audience

The audience for this path includes entry-level computer technicians who will, by the end of studying this path and before taking the exam, have accumulated 500 hours hand-on experience in a lab or in the field

Prerequisites

None

- Recognize the differences between operating systems and the basic features of the Windows OS components and system interfaces
- Recognize the names and purposes of operating system files and the basics of disk, file, and directory management
- Identify the location and function of Windows XP system files, navigate the Windows XP interface, and create files and folders
- Recognize how to install, configure, and optimize operating systems in a given scenario
- Recognize how to upgrade operating systems and install a device in a given scenario



- Identify tools, diagnostic procedures, and troubleshooting techniques for operating systems in given scenarios
- Recognize common error messages, codes, operational issues, and preventive maintenance techniques for operating systems in given scenarios
- Troubleshoot operating systems in a given scenario

Security, Safety, and Communication

Overview/Description

To understand the role of security in an organization, the importance of following safety and environmental guidelines, and how to communicate with customers in a professional manner

Target Audience

The audience for this path includes entry-level computer technicians who will, by the end of studying this path and before taking the exam, have accumulated 500 hours hand-on experience in a lab or in the field

Prerequisites

None

- Identify the fundamental principles of security
- Identify the features of data and physical security, incident reporting, and social engineering situations
- Install hardware, software, and data security and identify troubleshooting and preventive maintenance techniques for computer security in given scenarios
- Implement a security policy, install hardware security, and troubleshoot security issues
- Identify safety and environmental measures and procedures
- Recognize how to communicate clearly and respond professionally to customers in given scenarios
- Recognize guidelines for promoting safety and environmental issues, effective communication skills, and job-related professional behavior

A+ IT Technician Test 220-602:

Installing, Configuring, and Troubleshooting PC Components

Overview/Description

To recognize how to install, configure and troubleshoot PC components

Target Audience

The audience for this path includes computer technicians who have accumulated 500 hours hand-on experience in a lab or in the field and, ideally, have completed the A+ Essentials exam (220-601).

Prerequisites

None

Objectives :

Installing, Configuring, and Troubleshooting PC Components

- Recognize how to select and install internal components in given scenarios.
- Recognize how to select, install, and configure display and input devices and adapter cards in given scenarios.
- Install and configure PC components in given scenarios.



- Identify tools, diagnostic procedures, and troubleshooting techniques for personal computer components in given scenarios.
- Identify which tool to use and which steps to take when troubleshooting PC components in given scenarios.
- Recognize common preventive maintenance techniques for personal computer components.
- Troubleshoot operational problems in a given scenario.

Working with Laptops and Portable Devices

Overview/Description

To understand the features of laptops and portable devices, including major components, communication methods, and peripherals

Target Audience

The audience for this path includes computer technicians who have accumulated 500 hours hand-on experience in a lab or in the field and, ideally, have completed the A+ Essentials exam (220-601).

Prerequisites

None

Objectives :

Working with Laptops and Portable Devices

- Identify the major components of the LCD and recognize laptop-specific communication connections, power, and electrical input devices.
- Recognize how to remove laptop-specific hardware and identify how video sharing affects memory.
- Recognize how to use procedures and techniques to diagnose power conditions, video, keyboard, pointer and wireless card issues in given scenarios.
- Troubleshoot laptop issues in a given scenario.

Understanding and Maintaining Networks

Overview/Description

To understand the principles of networking and basic diagnostic and troubleshooting techniques

Target Audience

The audience for this path includes computer technicians who have accumulated 500 hours hand-on experience in a lab or in the field and, ideally, have completed the Essentials exam (220-601).

Prerequisites

None

Objectives :

Understanding and Maintaining Networks

- Recognize the characteristics of networking and Internet protocols.
- Identify characteristics of technologies for establishing network connectivity.
- Recognize networking protocols and technologies for establishing connectivity in given scenarios.



- Install and configure a browser and establish a network connection in a given scenario.
- Recognize how to share network resources in a given scenario.
- Recognize the tools and diagnostic procedures for troubleshooting network problems.
- Recognize how to perform preventative maintenance of networks, including securing and protecting network cabling.
- Configure and troubleshoot a network connection in a given scenario.

Maintaining Operating Systems

Overview/Description

To understand how to manage and optimize operating systems

Target Audience

The audience for this path includes computer technicians who have accumulated 500 hours hand-on experience in a lab or in the field and, ideally, have completed the A+ Essentials exam (220-601)

Prerequisites

None

Objectives :

Maintaining Operating Systems

- Identify the function of commandline functions and utilities for managing operating systems.
- Recognize how to create, view, and manage disks, directories, and files on operating systems.
- Locate and use operating system utilities in given scenarios.
- Recognize procedures and utilities for optimizing operating systems in given scenarios.
- Manage and optimize an operating system in given scenarios.
- Recognize how to use diagnostic and recovery tools for operating systems.
- Recognize howto resolve common operational errors in given scenarios.
- Identify the preventive maintenance measures for operating systems.
- Resolve operational problems in a given scenario.

Installing and Troubleshooting Printers and Scanners

Overview/Description

To recognize how to install and troubleshoot printers and scanners

Target Audience

The audience for this path includes computer technicians who have accumulated 500 hours hand-on experience in a lab or in the field and, ideally, have completed the Essentials exam (220-601).

Prerequisites

None

Objectives :



Installing and Troubleshooting Printers and Scanners

- Recognize the processes used by printers and scanners.
- Install, configure, and optimize printers and scanners in given scenarios.
- Install and optimize a printer in a given scenario.
- Identify the symptoms common printer problems and the tools and procedures for troubleshooting printers and scanners.
- Troubleshoot laser printers in a given scenario.
- Identify preventive maintenance measures for printers and scanners.

Managing IT Security

Overview/Description

To understand basic security principles and security software and how to troubleshoot security issues

Target Audience

The audience for this path includes computer technicians who have accumulated 500 hours hand-on experience in a lab or in the field and, ideally, have completed the A+ Essentials exam (220-601).

Prerequisites

None

Objectives :

Managing IT Security

- Identify the characteristics of access control, auditing, and event logging.
- Install and configure security in given scenarios.
- Install and configure software and data security in given scenarios.
- Recognize how to diagnose and troubleshoot software and data security issues in given scenarios.
- Troubleshoot a firewall and a shared folder in a given scenario.
- Identify how to prevent social engineering situations.

Recognizing Safety Procedures, Effective Communication, and Professional Behavior

Overview/Description

To recognize the importance of workplace safety and professional workplace behavior

Target Audience

The audience for this path includes computer technicians who have accumulated 500 hours hand-on experience in a lab or in the field and, ideally, have completed the A+ Essentials exam (220-601)

Prerequisites

None

Objectives :



Recognizing Safety Procedures, Effective Communication, and Professional Behavior

- Recognize potential hazards and how to overcome them with proper safety procedures.
- Recognize guidelines for effective communication in given scenarios.
- Recognize how to respond to given workplace scenarios in a professional manner.
- Recognize proper safety procedures, how to communicate effectively with customers, and how to use job-related professional behavior in given scenarios.

A+ Remote Support Technician Test 220-603:

The CompTIA A+ 220-603 examination is targeted for individuals who work or intend to work in a remote-based work environment where client interaction, client training, operating system and connectivity issues are emphasized. Example job roles include: Remote Support Technician, Help Desk Technician, and Call Center Technician. Ideally, the CompTIA A+ 220-603 candidate has already passed the CompTIA A+ Essentials examination. Candidates who pass both CompTIA A+ Essentials and exam 220-603 exams will be CompTIA A+ certified with the Remote Support Technician designation.

A+ Depot Technician Test 220-604:

The CompTIA A+ 220-604 examination is targeted for individuals who work or intend to work in settings where hardware related activities are emphasized. Example job roles include: Depot Technician, Bench technician. Ideally, the CompTIA A+ 220-604 candidate has already passed the CompTIA A+ Essentials examination. Candidates who pass both CompTIA A+ Essentials and exam 220-604 exams will be CompTIA A+ certified with the Depot Technician designation.

Network+

The Fundamentals of Networking

Overview/Description

To describe basic networking concepts, topologies, the OSI model, and the media used to physically connect a network

Target Audience

Network engineers, network architects, internetworking engineers, LAN and WAN administrators, systems administrators, systems managers, intranet administrators. Network support staff and anybody interested in learning the fundamentals of computer networks.

Lesson Objectives

The Fundamentals of Networking

- identify the primary components of a network and distinguish between the two main network architectures.
- distinguish between the main types of networks
- distinguish between the OSI reference model and the TCP/IP stack.
- distinguish between common network categorizations and identify the characteristics of data encapsulation.
- identify the major components of a network PC and list the resources required to install a NIC.
- identify the functions, features, and operation of network devices used at different layers of the OSI model.
- distinguish between different network topologies
- match network devices to their functions and distinguish between different network topologies.



- differentiate between types of network media.
- recognize the types of cable connectors used in modern networks.
- determine the most appropriate network tool to use in a given scenario.
- determine the appropriate network media and connectors to use in a given scenario.

LAN Technologies

Overview/Description

To describe the operation of the most commonly implemented types of LAN

Target Audience

Network engineers, network architects, internetworking engineers, LAN and WAN administrators, systems administrators, systems managers, intranet administrators. Network support staff and anybody interested in learning the fundamentals of computer networks.

Lesson Objectives

LAN Technologies

- identify the standards, functions, and operation of Ethernet LAN technologies.
- recognize how Token Ring and FDDI networks function.
- recognize the features of wireless transmission technologies.
- recognize the standards, components, and functionality of wireless LANs.
- identify the features and functionality of common types of LANs.
- identify methods used to extend Ethernet LANs and reduce the size of collision domains.
- recognize the function and composition of Media Access Control (MAC) addresses.
- sequence the steps involved in frame switching.
- differentiate between the features and characteristics of shared and switched LANs.
- identify the benefits, components, and functionality of VLANs.
- determine an appropriate VLAN implementation for a given scenario.

Networking Protocols

Overview/Description

To describe the operation of network protocols TCP/IP, IPX/SPX, AppleTalk, and NetBEUI

Target Audience

Network engineers, network architects, internetworking engineers, LAN and WAN administrators, systems administrators, systems managers, intranet administrators. Network support staff and anybody interested in learning the fundamentals of computer networks.

Networking Protocols

- identify the function and features of TCP/IP.
- distinguish between different network layer protocols and their functions.
- distinguish between the transport layer protocols TCP and UDP.
- recognize the function and usage of common TCP/IP protocols.
- differentiate between the functions of protocols used at the network and transport layers.
- recognize the key characteristics of the IPX/SPX protocol stack.
- recognize the basic functionality and characteristics of NetBEUI and AppleTalk.



- differentiate between IPX/SPX, NetBEUI, and AppleTalk in terms of addressing schemes, routing, naming conventions, and interoperability.

IP Addressing and Subnetting

Overview/Description

To describe the operation of IP addressing, the structuring of addresses using subnets, and the routing of information between networks.

Target Audience

Network engineers, network architects, internetworking engineers, LAN and WAN administrators, systems administrators, systems managers, intranet administrators. Network support staff and anybody interested in learning the fundamentals of computer networks.

Lesson Objectives

IP Addressing and Subnetting

- distinguish between IP address classes and between the types of reserved IP addresses.
- distinguish between public and private IP addresses and identify methods for increasing address availability.
- identify characteristics of a given IP address range.
- recognize how to calculate a subnet address and modify a default subnet mask.
- calculate valid IP subnetwork addresses and mask values in a given scenario.
- perform subnet calculations in a given scenario.
- recognize the basic operations involved in routing.
- distinguish between different routing protocols.
- determine the most appropriate routing protocol to use in a given scenario.

Working with TCP/IP

Overview/Description

To describe the characteristics and operation of TCP/IP applications and utilities, and to describe how to configure TCP/IP on client computers.

Target Audience

Network engineers, network architects, internetworking engineers, LAN and WAN administrators, systems administrators, systems managers, intranet administrators. Network support staff and anybody interested in learning the fundamentals of computer networks.

Lesson Objectives

Working with TCP/IP

- recognize the features and functionality of name resolution services.
- identify the characteristics and functionality of Dynamic Host Configuration Protocol (DHCP).
- recognize how to use common TCP/IP utilities.
- determine the most appropriate TCP/IP utility to use in a given scenario.
- recognize how to configure TCP/IP for Windows, UNIX, and Linux systems.
- configure TCP/IP on a Windows 2000 client.



WANs and Remote Connectivity

Overview/Description

To describe WAN technologies, the devices used to create WAN connections, remote access protocols, and connection methods.

Target Audience

Network engineers, network architects, internetworking engineers, LAN and WAN administrators, systems administrators, systems managers, intranet administrators. Network support staff and anybody interested in learning the fundamentals of computer networks.

Lesson Objectives

WANs and Remote Connectivity

- identify the features and functions of major WAN connection technologies.
- identify the operation and features of common WAN access technologies.
- recognize the characteristics of WAN access devices.
- determine the WAN connection types and access technologies used in a given scenario.
- determine the appropriate remote access protocol to use in a given scenario.
- recognize how to configure remote connections on a client PC.
- create a dial-up Internet connection in Windows 2000.

Network Operating Systems and Clients

Overview/Description

To describe the features and functions of different network operating systems, and the software clients and tools which enable them to interoperate

Target Audience

Network engineers, network architects, internetworking engineers, LAN and WAN administrators, systems administrators, systems managers, intranet administrators. Network support staff and anybody interested in learning the fundamentals of computer networks.

Network Operating Systems and Clients

- identify the key features and functionality of Windows NT and Windows 2000.
- recognize the features and architecture of Novell NetWare.
- recognize the functions and features of UNIX and Linux operating systems.
- recognize features of the Apple Mac operating system.
- identify the characteristics of network operating systems.
- install network client software in Windows 2000.
- recognize the structure and characteristics of network directory services.
- install Client Services for NetWare in Windows 2000.



Network Security

Overview/Description

To describe protocols and authentication methods used to maintain network security, and commonly used network security devices and tools.

Target Audience

Network engineers, network architects, internetworking engineers, LAN and WAN administrators, systems administrators, systems managers, intranet administrators. Network support staff and anybody interested in learning the fundamentals of computer networks.

Lesson Objectives

Network Security

- identify common security risks for network computers.
- identify the characteristics of common Internet security protocols.
- identify the characteristics of wireless security protocols.
- recognize the key characteristics and functionality of common authentication protocols.
- determine the appropriate security or authentication protocol to use in a given scenario.
- identify the characteristics and components of firewalls and proxy servers.
- recognize the features and functionality of antivirus programs.
- distinguish between different encryption and decryption techniques.
- recognize tools and techniques for protecting network data.

Network Troubleshooting

Overview/Description

To describe a working methodology and tools and utilities that can be used to diagnose and troubleshoot network problems

Target Audience

Network engineers, network architects, internetworking engineers, LAN and WAN administrators, systems administrators, systems managers, intranet administrators. Network support staff and anybody interested in learning the fundamentals of computer networks.

Lesson Objectives

Network Troubleshooting

- recognize the types of documentation and technical support options available for troubleshooting networks.
- recognize the features and functionality of common network troubleshooting tools.
- recognize how log files and network diagnostics utilities are used in network troubleshooting.
- determine the most appropriate network troubleshooting tool to use in a given scenario.
- sequence the steps in a network troubleshooting methodology.
- troubleshoot Internet connectivity and name resolution problems on a network.
- troubleshoot LAN communication issues and problems with local hosts.
- use a systematic troubleshooting methodology to resolve a network problem.



Fault Tolerance and Disaster Recovery

Overview/Description

To describe how to implement fault tolerance and recovery processes in a network

Target Audience

Network engineers, network architects, internetworking engineers, LAN and WAN administrators, systems administrators, systems managers, intranet administrators. Network support staff and anybody interested in learning the fundamentals of computer networks.

Lesson Objectives

Fault Tolerance and Disaster Recovery

- identify common fault tolerance and disaster recovery strategies.
- distinguish between different methods of providing fault tolerance for computer disk systems.
- identify the media and utilities used to back up network data.
- identify common power management devices.
- identify practical disaster recovery strategies.

TestPrep N10-003 Network+ 2005

Overview/Description

Generally taken near the end of a program of certification-orientated study, the N10-003 Network+ 2005 TestPrep enables the learner to test their knowledge in a simulated certification testing environment. Learners can take TestPrep in two different modes: Study and Certification. Study mode is designed to maximize learning by providing feedback, while Certification mode is designed to mimic a certification exam.

Target Audience

Individuals seeking practice in a simulated testing environment, covering the skills and competencies being measured by the actual certification exam.

Lesson Objectives

TestPrep N10-003 Network+ 2005

- Media and Topologies
- Protocols and Standards
- Network Implementation
- Network Support

Security+

General Security Concepts



Overview/Description

To introduce the key principles of security for the enterprise

Target Audience

Network administrators, firewall administrators, system administrators, application developers, and IT security officers

Lesson Objectives

General Security Concepts

- describe how to achieve CompTIA Security + Certification.
- discuss access control concepts.
- discuss access control types and models.
- discuss resource access control and system access control.
- identify the requirements for system access control and resource access control.
- explain how to implement resource access control and system access control.
- define the principles of authentication and discuss authentication methods.
- explain the features and operation of Kerberos.
- explain the authentication mechanisms used in PPP.
- describe threats to information security and network infrastructure.
- explain how different types of denial-of-service attacks affect a network.
- describe some of the common attacks that are carried out on networks.
- detail threats that arise specifically from hackers.
- set up and monitor a Telnet session using a protocol analyzer.
- discuss the threat of social engineering.
- describe how passwords are stored and explain why they are vulnerable to attack.
- explain why a strong password policy is important and what can be done to protect password files on UNIX and Windows systems.
- use the password cracking utility LC4 and employ it to audit passwords from a number of locations.

Communications Security

Overview/Description

To introduce the key issues in communications security

Target Audience

Network administrators, firewall administrators, system administrators, application developers, and IT security officers

Lesson Objectives

Communications Security

- explain the technologies used to implement VPNs for secure WAN communications.
- detail the features of a VPN solution for secure remote connectivity.
- implement a VPN solution for secure remote access.
- outline the RADIUS authentication mechanism.



- outline the TACACS+ authentication mechanism and compare it to the RADIUS authentication mechanism.
- describe WEP and the differences between the various wireless LAN standards.
- describe wireless LAN security attacks and explain how to prevent them.
- identify the strengths and weaknesses of various wireless LAN security techniques.
- identify appropriate security solutions for wireless LANs.
- explain corporate security policies and outline the procedures involved in performing a site survey.
- conduct a wireless LAN site survey.
- describe the WAP protocol and discuss mechanisms for protecting the WAP gateway.
- provide an overview of the various threats to web security.
- describe how Gnutella and peer-to-peer networks work and outline the security issues that arise from their use.
- understand the FTP protocol and outline the measures used to secure FTP.
- discuss the security implications of popular instant messaging applications.
- identify the various components of LDAP.
- describe the security methods associated with LDAP.

Infrastructure Security

Overview/Description

To describe how to detect and respond to network intruders, understand operating system security, and describe LAN devices and topology

Target Audience

Network administrators, firewall administrators, system administrators, application developers, and IT security officers

Lesson Objectives

Infrastructure Security

- discuss the principles of detecting network intruders.
- describe how to distract network intruders and limit the damage they can cause.
- set up a decoy account and monitor both failed and successful login attempts.
- describe the characteristics and features of intrusion detection systems.
- describe the different types of intrusion detection mechanisms.
- discuss the deployment of intrusion detection systems.
- discuss how to respond to and manage computer-related security incidents.
- recognize the functionality and deployment issues of intrusion detection.
- describe network components and their application.
- explain the role of bridges, switches, and routers in a network.
- describe the basic operation of firewalls and proxy servers.
- describe the various frauds that are carried out on PBX systems.
- identify the different types of networking media that are used at the physical layer of the OSI model.
- describe Windows NT and Windows 2000 security issues.
- identify the threats to system security, both intentional and unintentional.
- run a security scan on a networked workstation.
- outline the main components of OS security.
- explain changes that can be made to an OS to make it more secure.
- discuss Windows 2000 Registry security.



- perform tasks to improve the security of the Windows OS.
- describe how VLANs operate.
- list the components of NAT and explain when NAT should be implemented.

Encryption Technologies

Overview/Description

To discuss techniques for encrypting information

Target Audience

Network administrators, firewall administrators, systems administrators, application developers, and IT security officers

Lesson Objectives

Encryption Technologies

- outline the history of encryption and the reasons why encryption is important.
- outline the principles of symmetric encryption.
- explain what a block cipher is and identify the algorithms that use them.
- discuss the fundamentals of asymmetric encryption.
- explain the functionality of hashes and message functions in protecting the integrity of encrypted data.
- describe the processes involved in symmetric and asymmetric encryption.
- outline the different methods of managing encryption keys.
- discuss some practical applications of encryption.
- implement a secure encryption scheme on a computer.
- exchange encrypted e-mails.
- explain the use of certificates for trusted secure public-key implementation.
- describe revocation and nonrepudiation of public-key certificates.
- discuss the X.509 standard for public-key certificates.
- describe public-key infrastructure and Secure Electronic Transactions (SETs).
- outline certificate practices, policies, and paths.

Operational and Organizational Security

Overview/Description

To present the key issues and policy requirements for organizational and operational security

Target Audience

Network administrators, firewall administrators, system administrators, application developers, and IT security officers

Lesson Objectives

Operational and Organizational Security

- discuss the reason for business continuity plans.
- discuss the reason for and the process involved in creating a disaster recovery plan.



- discuss the reasons why business continuity plans are used and how to create them.
- describe how to develop a business impact assessment and a business continuity plan.
- discuss the process involved in maintaining and testing a disaster recovery plan.
- explain the underlying concepts and principles of security management.
- list and explain the recognized industry standards and recommendations that address information and network security.
- define security policy and identify issue-specific security policy documents.
- design a security policy document.
- discuss employment practices in the workplace.
- describe the controls that are available to protect resources, restrict privileges, and limit the risk of access abuse in a network environment.
- describe the technologies and controls that make a working environment secure.
- describe the technologies and controls that make a safe working environment.
- identify the environmental safeguards and security strategies required to make a site secure.
- describe the technologies and controls that restrict access to a working environment and control data confidentiality.
- discuss risk management and its requirements with reference to security issues.
- describe the processes involved in implementing information risk management.
- explain how computer crime investigations are conducted.

TestPrep SY0-101 Security+

Overview/Description

Generally taken near the end of a program of certification-orientated study, the SY0-101 Security+ TestPrep enables the learner to test their knowledge in a simulated certification testing environment. Learners can take TestPrep in two different modes: Study and Certification. Study mode is designed to maximize learning by providing feedback, while Certification mode is designed to mimic a certification exam.

Target Audience

Individuals seeking practice in a simulated testing environment, covering the skills and competencies being measured by the actual certification exam.

TestPrep SY0-101 Security+

- General Security Concepts
- Communication Security
- Infrastructure Security
- Basics of Cryptography
- Operational/Organizational Security



Server +

Servers and their Components

Overview/Description

To identify the functions, features, and components of servers

Target Audience

Service managers, technicians, systems engineers/administrators, help desk staff, service and repair professionals, system analysts and integrators, PC support specialists, network engineers/administrators/analysts/architects/managers/specialists

Lesson Objectives

Servers and their Components

- identify the characteristics of servers and recognize the features of the key server categories.
- identify various roles that can be assigned to network servers.
- identify server categories and assign roles to servers.
- recognize the features and functions of motherboards and expansion buses.
- recognize the features and functions of specified PCI system bus architectures.
- identify memory types and best practices for managing server memory.
- identify the specifications of the main server processors and recognize how multiprocessing works.
- select memory types and processors in given scenarios.

IDE, SCSI, and Server Storage

Overview/Description

To identify critical server storage technologies and the functions and features of IDE and SCSI

Target Audience

Service managers, technicians, systems engineers/administrators, help desk staff, service and repair professionals, system analysts and integrators, PC support specialists, network engineers/administrators/analysts/architects/managers/specialists

Lesson Objectives

IDE, SCSI, and Server Storage

- identify the features of Fibre Channel technology and differentiate between SAN and NAS.
- deploy RAID levels in a given scenario.
- choose appropriate server storage technologies in a given scenario.
- differentiate between physical and logical disks.
- recognize the different IDE technologies and configuration best practices.
- identify the different SCSI types and the benefits of SCSI over IDE.
- identify best practices for installing and configuring SCSI technologies.
- add components using IDE and SCSI best practices.



Installation and Configuration

Overview/Description

To identify best practices for installing and configuring servers

Target Audience

Service managers, technicians, systems engineers/administrators, help desk staff, service and repair professionals, system analysts and integrators, PC support specialists, network engineers/administrators/analysts/architects/managers/specialists

Lesson Objectives

Installation and Configuration

- identify pre-installation planning activities.
- identify key considerations for evaluating remote management requirements.
- identify key considerations and best practices for installing server hardware.
- create server planning and hardware installation best practice checklists.
- identify considerations involved in installing and configuring a network operating system.
- identify best practices for installing service tools on the server and measuring baseline performance.
- create NOS and service tool installation best practice checklists.

Upgrading

Overview/Description

To identify best practices for upgrading servers

Target Audience

Service managers, technicians, systems engineers/administrators, help desk staff, service and repair professionals, system analysts and integrators, PC support specialists, network engineers/administrators/analysts/architects/managers/specialists

Lesson Objectives

Upgrading

- identify critical steps and considerations involved in planning a server upgrade.
- identify best practices and troubleshooting procedures for adding memory and processors.
- identify best practices and troubleshooting procedures to be employed when upgrading hard disks, adaptors, and peripherals.
- identify key considerations, best practices, and troubleshooting procedures for software upgrades.
- identify best practices and troubleshooting procedures that should be employed when upgrading servers.

Disaster Recovery and Server Backups



Overview/Description

To identify server backup and disaster recovery best practices

Target Audience

Service managers, technicians, systems engineers/administrators, help desk staff, service and repair professionals, system analysts and integrators, PC support specialists, network engineers/administrators/analysts/architects/managers/specialists

Disaster Recovery and Server Backups

- identify backup strategies and select appropriate media types.
- identify best practices for framing backup plans, restoring data, and troubleshooting common backup problems.
- choose and implement backup strategies.
- identify risks for a disaster recovery plan and create strategies to deal with them.
- identify components and considerations aimed at ensuring redundancy, scalability, and high availability.
- identify key considerations for creating and maintaining a disaster recovery plan.
- identify key considerations and best practices in creating a disaster recovery plan.

Maintenance and Environment

Overview/Description

To identify best practices in maintaining servers and their environments

Target Audience

Service managers, technicians, systems engineers/administrators, help desk staff, service and repair professionals, system analysts and integrators, PC support specialists, network engineers/administrators/analysts/architects/managers/specialists

Maintenance and Environment

- identify key considerations when monitoring servers.
- identify how data can be gathered to monitor server performance.
- identify the features and functions of SNMP and discuss its relationship with RMON.
- identify best practices for maintaining a server.
- identify methods to mitigate common environmental issues that may affect server performance.
- identify measures and best practices for physically securing the server room and server hardware.
- manage environmental and physical security issues.

Troubleshooting Servers

Overview/Description

To identify server-related troubleshooting best practices

Target Audience

Service managers, technicians, systems engineers/administrators, help desk staff, service and repair professionals, system analysts and integrators, PC support specialists, network engineers/administrators/analysts/architects/managers/specialists

Lesson Objectives

- identify the steps in the troubleshooting process and discuss how to prioritize problems.
- identify methods for gathering information to determine the origins of problems.
- identify best practices and resources for fixing and documenting server-related problems.
- identify best practices and procedures for troubleshooting problems in a given scenario.
- identify strategies for dealing with common server-related problems.
- identify best practices and guidelines for using documentation and log files to solve server-related problems.
- identify the troubleshooting features of specified diagnostic tools.
- select diagnostic tools and techniques in a given scenario.

TestPrep SK0-002 Server+ 2005

Overview/Description

Generally taken near the end of a program of certification-orientated study, the SK0-002 Server+ 2005 TestPrep enables the learner to test their knowledge in a simulated certification testing environment. Learners can take TestPrep in two different modes: Study and Certification. Study mode is designed to maximize learning by providing feedback, while Certification mode is designed to mimic a certification exam.

Target Audience

Individuals seeking practice in a simulated testing environment, covering the skills and competencies being measured by the actual certification exam.

Lesson Objectives

TestPrep SK0-002 Server+ 2005

- General Server Hardware Knowledge
- Installation
- Configuration
- Upgrading
- Proactive Maintenance
- Environment
- Troubleshooting and Problem Determination
- Disaster Recovery

****Students who successfully complete all requirements of the IT Foundations: Networking Specialist program will also be prepared to independently take the internationally recognized exams by CompTIA for A+, Network+, Security+ and Server+. These designations prepare students for the workforce to complete such tasks as: repair and maintain a variety of PCs, install, manage and troubleshoot a variety of networks on any platform, plan, install, configure and maintain a variety of servers on any platform according to Industry Standard Server Architecture (ISSA), and to secure network services, network devices and network traffic.***