BCTE
Bureau of Career & Technical Education

NOCTI
State Customized
Credential Blueprint

Computer Systems Networking (PA)

Code: 8148 / Version: 01

General Assessment Information

Blueprint Contents

Test Type: The Computer Systems Networking PA assessment was developed based on a Pennsylvania statewide competency task list and contains a multiple-choice and performance component. This assessment is meant to measure technical skills at the occupational level and includes items which gauge factual and theoretical knowledge.

Revision Team: The assessment content is based on input from Pennsylvania educators who teach in approved career and technical education programs.

CIP Code

11.0901- Computer Systems Networking & Telecommunications

Learning that works for America CTE™

8- Information Technology

NATIONAL COLLEGE CREDIT RECOMMENDATION SERVICE
University of the State of New York - Regents Research Fund

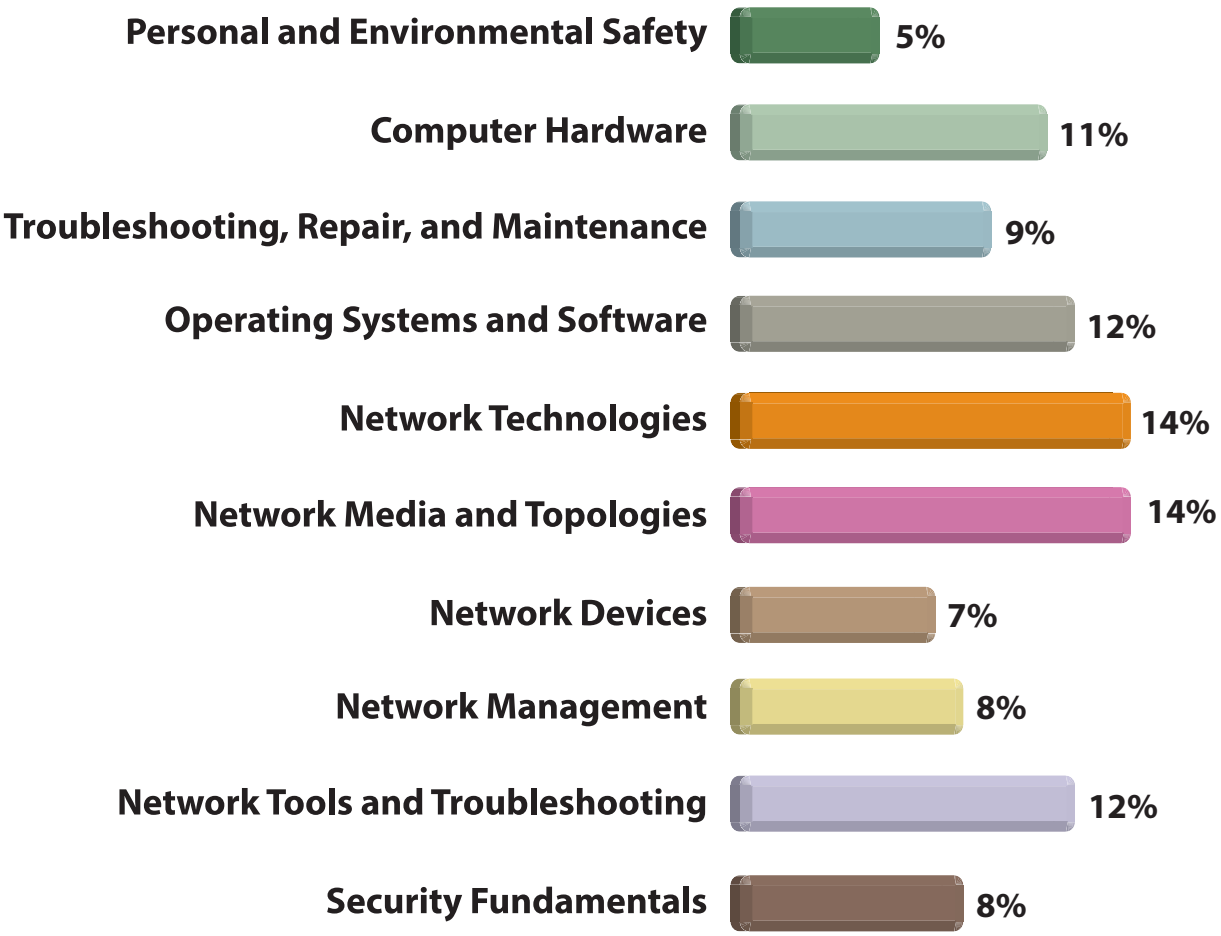
In the lower division baccalaureate/associate degree category, 3 semester hours in Computer Networking, Computer Science, or Computer Information Systems

Written Assessment

NOCTI written assessments consist of questions to measure an individual's factual theoretical knowledge.

Administration Time: 3 hours
Number of Questions: 200
Number of Sessions: This assessment may be administered in one, two, or three sessions.

Areas Covered



Specific Standards and Competencies Included in this Assessment

Personal and Environmental Safety

- Wear personal protective equipment
- Review Material Safety Data Sheets (MSDS) and explain their requirements in handling hazardous materials
- Describe the importance of safety as it relates to environmental issues
- Identify potential hazards when working with power supplies
- Identify proper disposal procedures for batteries and display devices
- Identify and prevent electrostatic discharge (ESD) conditions
- Configure a computer's power management settings to maximize energy efficiency
- Maintaining a safe work area to avoid common accidents and injuries

Computer Hardware

- Categorize storage devices and backup media
- Explain motherboard components, types, and features
- Categorize power supplies types and characteristics
- Explain the purpose and characteristics of CPUs and their features
- Compare and contrast memory types, characteristics, and their purpose
- Summarize the function and types of adapter cards
- Install and configure peripherals and input devices
- Install, configure, and optimize laptop components and features
- Install and configure printers
- Given a scenario, install, configure, and maintain personal computer components
- Given a scenario, detect problems, troubleshoot, and repair/replace desktop and laptop computer components
- Given a scenario, diagnose and repair common printer issues

(Continued on the following page)

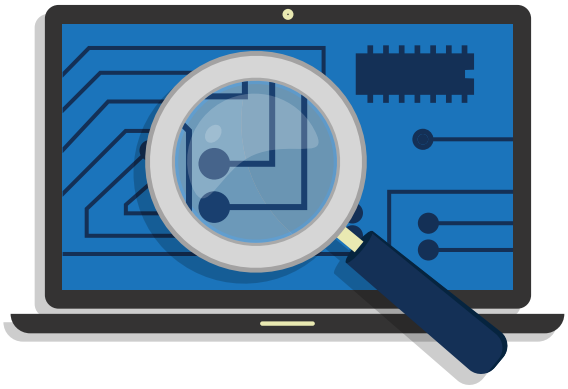
Specific Standards and Competencies (continued)

Troubleshooting, Repair, and Maintenance

- Describe and explain the troubleshooting theory
- Describe, explain, and interpret common hardware and operating system symptoms and their causes
- Describe and determine the troubleshooting methods and tools for printers
- Describe and interpret common laptop issues and determine the appropriate basic troubleshooting method
- Compare and contrast network troubleshooting and hardware/software troubleshooting

Operating Systems and Software

- Compare and contrast the different operating systems and their features
- Given a scenario, demonstrate proper use of user interfaces
- Explain the process and steps to install and configure an operating system
- Explain the basics of boot sequences, methods, and startup utilities
- Select the appropriate commands and options to troubleshoot and resolve problems
- Differentiate between various operating system directory structures
- Identify and use system utilities/tools and evaluate the results
- Evaluate and resolve common OS and software issues
- Explain the administration of local users/groups, and institute local security policy
- Compare and contrast a network operating system (NOS) with a workstation operation system (OS)



(Continued on the following page)

Specific Standards and Competencies (continued)

Network Technologies

- Explain the function of common networking protocols, such as FTP, TCP/IP suite, DHCP, DNS, etc.
- Identify commonly used TCP and UDP default ports, including TCP ports; FTP-20, 21, SSH-22, TELNET-23, HTTP-80, etc.
- Identify address formats, including IPv6, IPv4, and MAC addressing
- Given a scenario, evaluate the proper use of addressing technologies and addressing schemes, including Subnetting: Classful vs. classless, NET, PAT, SNAT, Public vs. Private, DHCP, addressing schemes: Unicast, Multicast, Broadcast, etc.
- Identify common IPv4 and IPv6 routing protocols, including link state, distance vector, and hybrid protocols
- Explain the purpose and properties of routing, including IGP vs. EGP, static vs. dynamic, next hop, interpret routing tables and how they pertain to path selection.
- Explain convergence (steady state)
- Compare the characteristics of wireless communication standards, including 802.11 standards: Speeds, distance, channels, frequency, authentication, and encryption

(Continued on the following page)

Specific Standards and Competencies (continued)

Network Media and Topologies

- Categorize standard cable types and their properties, including UTP, STP, coaxial, fiber: Plenum vs. non-plenum properties: transmission speeds, distance, duplex, noise immunity, frequency
- Identify common connector types, including UTP, STP, coaxial, and fiber
- Identify common physical network topologies
- Given a scenario, differentiate and implement appropriate wiring standards, including 568A, 568B, and loopback
- Categorize common WAN technology types and properties
- Categorize common LAN technology types and Ethernet properties: CSMA/CD, broadcast, collision, bonding, speed, distance
- Explain common logical network topologies and their characteristics, including peer-to-peer and client/server
- Install components of wiring distribution, including vertical and horizontal cross-connects, verify installation and termination

Network Devices

- Install, configure, and differentiate between common network connectivity devices
- Identify the functions of specialized network devices, such as multilayer switch, content switch, IDS/IPS, load balancer, multifunction network devices, DNS server, bandwidth shaper, proxy server, CSU/DSU
- Explain the advanced features of a switch, such as PoE, spanning tree, VLAN trunking, port mirroring, port authentication, etc.
- Implement a basic wireless network, including client configuration, access point placement, and installation

(Continued on the following page)

Specific Standards and Competencies (continued)

Network Management

- Explain, compare, and contrast the layers of the TCP/IP and OSI models
- Identify types of configuration management documentation, such as wiring schematics, physical and logical network diagrams, baselines, policies, procedures and configurations, regulations
- Conduct network monitoring to identify performance and connectivity issues, such as packet sniffers, connectivity software, load testing, throughput testers, system logs, history logs, event logs

Network Tools and Troubleshooting

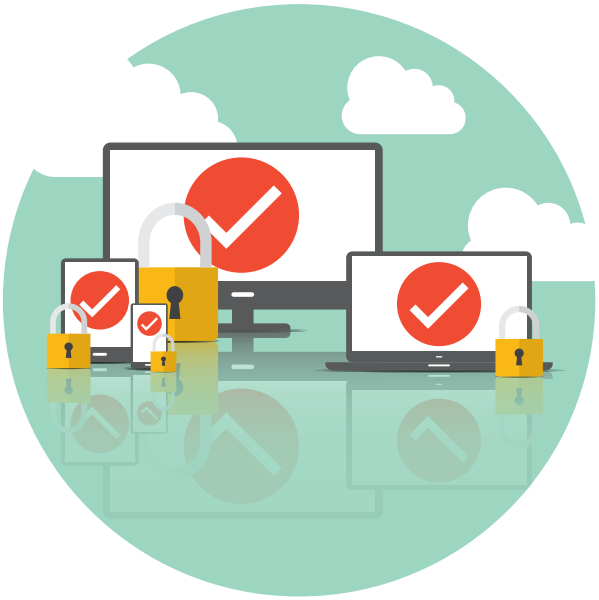
- Given a scenario, select the appropriate command line/graphical tools, interpret the output to verify functionality such as Traceroute, Ipconfig, Ifconfig, ping, arp ping, arp, Nslookup, hostname, dig, Mrt, route, Nbstat, Netstat
- Explain the purpose of network scanners, such as packet sniffers, intrusion detection software, intrusion prevention software, port scanners
- Given a scenario, select the appropriate hardware tools, such as cable testers, protocol analyzer, certifiers, TDR, OTDR, multimeter, toner probe, butt set, punch down tool, cable stripper, snips, voltage event recorder, temperature monitor
- Given a scenario, implement network troubleshooting methodologies, including information gathering – identify symptoms and problems, identify the affected areas of the network
- Given a scenario, troubleshoot common wired and wireless connectivity issues and select an appropriate solution to include physical and logical issues

(Continued on the following page)

Specific Standards and Competencies (continued)

Security Fundamentals

- Explain, compare, and contrast the function of hardware and software security devices such as network-based firewall, host-based firewall, DMZ, IDS, IPS, VPN concentrator
- Explain common features of a firewall, such as application layer vs. network layer, stateful vs. stateless, scanning services, content filtering, signature identification, zones
- Explain issues that affect device security, such as physical security, restricting local and remote access, secure methods vs. unsecure methods: SSH, HTTPS, SNMPv3, SFTP, SCP, TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2
- Identify common security threats and mitigation techniques
- Identify security features, including BIOS security, password management, locking workstations, and biometrics



Sample Questions

A single-sided, single-density DVD recordable disk has a capacity of

A. 1.8 GB
B. 2.3 GB
C. 4.7 GB
D. 9.4 GB

The ipconfig/all command is used to view a PCs

A. MAC addressing information
B. IP addressing information
C. network connectivity
D. Internet connection status

A unique "network number" used in routing is contained in the

A. MAC address
B. physical address
C. logical address
D. NIC

Peer-to-peer networks

A. do not share resources
B. allow workstations to share and access resources without a dedicated server
C. are optimized for sharing resources from a single computer with many users
D. are remotely administered

A port scanner may be used to

A. probe a network host for open ports
B. probe a PC for unused USB ports
C. scan a hub, switch, or router for unused physical ports
D. scan a hub, switch, or router for active physical ports

(Continued on the following page)

Sample Questions (continued)

A properly attached wrist strap decreases the chance of

A. VPN
B. ESP
C. PAN
D. ESD

Which of the following operating systems is considered open source?

A. Windows® 7
B. OS X
C. UBUNTU
D. UNIX

Router IP interface addresses can be configured

A. hexadecimally or binary
B. orthographically
C. statically or dynamically
D. categorically

Which of the following protocols is found in the transport layer?

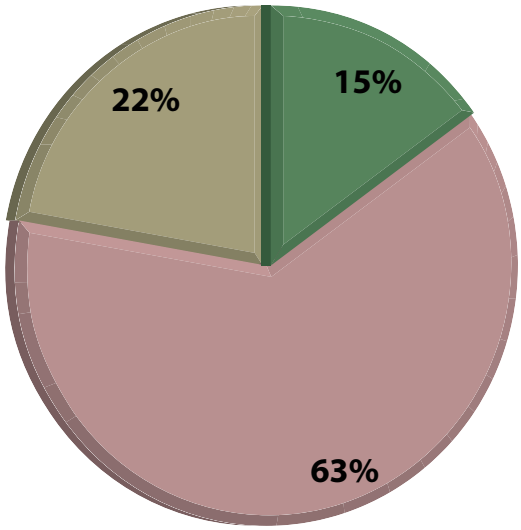
A. IP
B. TCP
C. HTTP
D. FTP

A firewall is best described as a

A. physical wall that protects a data center from catching on fire
B. system or group of systems that scans an environment for viruses, spyware, and spam
C. system or group of systems that enforces an access control policy between two networks
D. system used to connect two different networks to each other

Performance Assessment

NOCTI performance assessments allow individuals to demonstrate their acquired skills by completing actual jobs using the tools, materials, machines, and equipment related to the technical area.



Administration Time: 2 hours
Number of Jobs: 3

Areas Covered:

15% Identify Cables and Usage
Participants will identify cable types and usage and will test one cable to determine the nature of a fault.

63% Set Up a Simple LAN with Two Workstations and Hardware Installation
Participants will select correct tools for the job and demonstrate appropriate safety procedures. This job will measure the participant's ability to check for warnings or conflicts in the Device Manager, remove and replace a non-functioning NIC, verifying an onboard NIC is disabled through BIOS or Device Manager, and PING loopback address to establish the NIC functionality. Participants will then create a simple LAN with two workstations, configure the IP addresses, verify IP connectivity between the workstations, and verify the network is correctly set up and functions according to specifications provided.

22% Wireless Configuration
Participants will demonstrate the ability to configure a wireless router by logging in, changing the default password and wireless router name, configuring DHCP according to the specifications provided, renaming the wireless configuration SSID, and setting up wireless security.

(Continued on the following page)

Sample Job

Identify Cables and Usage

Maximum Time: 30 minutes

Participant Activity: Using the information provided, the participant will identify cable types A, B, and C, and record their usage, test Cable D and determine the nature of the fault, and give completed form to evaluator.