Cybersecurity Systems Technology, Advanced

8629 36 weeks / 280 hours

Table of Contents

Acknowledgments ......................................................................................................................................... 1
Course Description ........................................................................................................................................ 2
Task Essentials List ....................................................................................................................................... 3
Curriculum Framework ................................................................................................................................. 8
Demonstrating Ethical Behavior with Computer Systems Technology ......................................................... 8
Exploring Windows Operating Systems ..................................................................................................... 12
Exploring Other Operating Systems and Technologies .............................................................................. 19
Applying Operational Procedures ............................................................................................................... 25
Understanding Security ............................................................................................................................... 29
Troubleshooting Software ........................................................................................................................... 34
Exploring Network Architecture ................................................................................................................ 39
Exploring Network Operations ................................................................................................................... 48
Understanding Network Security ................................................................................................................ 54
Troubleshooting Networks .......................................................................................................................... 60
Applying Industry Standards, Practices, and Network Theory .................................................................... 66
SOL Correlation by Task ............................................................................................................................ 73
Teacher Resources ...................................................................................................................................... 77
Appendix: Credentials, Course Sequences, and Career Cluster Information ............................................. 79

Acknowledgments

The components of this instructional framework were developed by the following curriculum development team members:

Daviette Anson, Chantilly High School Academy, Fairfax County Public Schools
Jeremiah Doucette, Washington County Career and Technical Education Center,
Washington County Public Schools
Correlations to the Virginia Standards of Learning were reviewed and updated by

Norma J. Bonney, Kempsville High School, Virginia Beach City Public Schools
Anne F. Markwith, New Teacher Mentor, Gloucester County Public Schools
Cathy Nichols-Cocke, PhD, Fairfax High School, Fairfax County Public Schools
Caroline C. Wheeler, M.T., Secondary English

The framework was edited and produced by the CTE Resource Center:

Nathan K. Pope, Writer/Editor
Heather A. Widener, Writer/Editor
Kevin P. Reilly, Administrative Coordinator

J. Anthony Williams, Specialist, Trade and Industrial Education & Related Clusters
Office of Career, Technical, and Adult Education
Virginia Department of Education

Dr. Tricia S. Jacobs, CTE Coordinator of Curriculum and Instruction
Office of Career, Technical, and Adult Education
Virginia Department of Education

Copyright © 2017

Course Description

Suggested Grade Level: 11 or 12
Prerequisites: 8628

This advanced course provides students with training in procedures for optimizing and troubleshooting concepts for computer systems, subsystems, and networks. Students explore the following:

- Basic network design and connectivity
• Network documentation
• Network limitations and weaknesses
• Network security, standards and protocols

Students will gain a basic understanding of emerging technologies including unified communications, mobile, cloud, and virtualization technologies. The course prepares students for postsecondary education and training and a successful career in information technology. Upon successful completion of the course, students may qualify to take CompTIA’s A+ and Network+ certification exams.

Task Essentials List

- Tasks/competencies designated by plus icons (⊕) in the left-hand column(s) are essential
- Tasks/competencies designated by empty-circle icons (○) are optional
- Tasks/competencies designated by minus icons (⊖) are omitted
- Tasks marked with an asterisk (*) are sensitive.

<table>
<thead>
<tr>
<th>Task Number</th>
<th>Tasks/Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>39</td>
<td>⊕ Describe security issues related to computer hardware, software, and data.</td>
</tr>
<tr>
<td>40</td>
<td>⊕ Explain concepts related to copyright, public domain, copy protection, intellectual property, and licensing agreements.</td>
</tr>
<tr>
<td>41</td>
<td>⊕ Describe concepts of cybersecurity, honesty, courtesy, and confidentiality related to information and email systems and social networking (e.g., spam, viruses, and etiquette).</td>
</tr>
<tr>
<td>42</td>
<td>⊕ Analyze Internet privacy issues and computer crimes, including identity theft.</td>
</tr>
<tr>
<td>43</td>
<td>⊕ Comply with copyright and patent laws.</td>
</tr>
<tr>
<td>44</td>
<td>⊕ Comply with policies regarding acceptable use of technology.</td>
</tr>
</tbody>
</table>

Exploring Windows Operating Systems

<table>
<thead>
<tr>
<th>Task Number</th>
<th>Tasks/Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>⊕ Compare features and requirements of Microsoft operating systems.</td>
</tr>
<tr>
<td>Task Number</td>
<td>8629</td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>46</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td></td>
</tr>
</tbody>
</table>

Exploring Other Operating Systems and Technologies

<table>
<thead>
<tr>
<th>Task Number</th>
<th>52</th>
<th>Tasks/Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td></td>
<td>Identify common features and functions of the macOS and Linux OS.</td>
</tr>
<tr>
<td>54</td>
<td></td>
<td>Identify basic cloud concepts.</td>
</tr>
<tr>
<td>55</td>
<td></td>
<td>Describe services provided by networked hosts.</td>
</tr>
<tr>
<td>56</td>
<td></td>
<td>Identify basic features of mobile operating systems.</td>
</tr>
<tr>
<td>57</td>
<td></td>
<td>Set up mobile device network connectivity and email.</td>
</tr>
<tr>
<td>58</td>
<td></td>
<td>Synchronize mobile devices.</td>
</tr>
</tbody>
</table>

Applying Operational Procedures

<table>
<thead>
<tr>
<th>Task Number</th>
<th>59</th>
<th>Tasks/Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>59</td>
<td></td>
<td>Analyze appropriate safety procedures.</td>
</tr>
<tr>
<td>60</td>
<td></td>
<td>Analyze controls and their impact on the environment.</td>
</tr>
<tr>
<td>61</td>
<td></td>
<td>Summarize the process of addressing prohibited content/activity.</td>
</tr>
<tr>
<td>62</td>
<td></td>
<td>Explain privacy, licensing, and policy concepts.</td>
</tr>
<tr>
<td>63</td>
<td></td>
<td>Demonstrate communication techniques and professionalism.</td>
</tr>
<tr>
<td>Task Number</td>
<td>8629</td>
<td>Tasks/Competencies</td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>64</td>
<td></td>
<td>Explain the troubleshooting theory.</td>
</tr>
<tr>
<td>Understanding Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td></td>
<td>Identify common threats and vulnerabilities.</td>
</tr>
<tr>
<td>66</td>
<td></td>
<td>Describe the methods used to make computers and networks more secure.</td>
</tr>
<tr>
<td>67</td>
<td></td>
<td>Configure security settings.</td>
</tr>
<tr>
<td>68</td>
<td></td>
<td>Describe methods for securing mobile devices.</td>
</tr>
<tr>
<td>69</td>
<td></td>
<td>Use data destruction and disposal methods.</td>
</tr>
<tr>
<td>70</td>
<td></td>
<td>Secure SOHO wireless and wired networks.</td>
</tr>
<tr>
<td>Troubleshooting Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td></td>
<td>Troubleshoot PC OS problems.</td>
</tr>
<tr>
<td>72</td>
<td></td>
<td>Troubleshoot common PC security issues.</td>
</tr>
<tr>
<td>73</td>
<td></td>
<td>Troubleshoot mobile OS and application issues.</td>
</tr>
<tr>
<td>74</td>
<td></td>
<td>Troubleshoot mobile OS and application security issues.</td>
</tr>
<tr>
<td>Exploring Network Architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td></td>
<td>Explain the functions and applications of various network devices.</td>
</tr>
<tr>
<td>76</td>
<td></td>
<td>Compare networking services and applications.</td>
</tr>
<tr>
<td>77</td>
<td></td>
<td>Install networking services/applications.</td>
</tr>
<tr>
<td>78</td>
<td></td>
<td>Explain the characteristics and benefits of various wide area network (WAN) technologies.</td>
</tr>
<tr>
<td>79</td>
<td></td>
<td>Install various cable types and connectors.</td>
</tr>
<tr>
<td>Task Number</td>
<td>8629</td>
<td>Tasks/Competencies</td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td>80</td>
<td>+</td>
<td>Differentiate between common network topologies.</td>
</tr>
<tr>
<td>81</td>
<td>+</td>
<td>Differentiate between network infrastructure implementations.</td>
</tr>
<tr>
<td>82</td>
<td>+</td>
<td>Configure addressing schema.</td>
</tr>
<tr>
<td>83</td>
<td>+</td>
<td>Explain basic routing concepts and protocols.</td>
</tr>
<tr>
<td>84</td>
<td>+</td>
<td>Identify the basic elements of unified communication (UC) technologies.</td>
</tr>
<tr>
<td>85</td>
<td>+</td>
<td>Compare technologies that support cloud virtualization.</td>
</tr>
<tr>
<td>86</td>
<td>+</td>
<td>Given a set of requirements, implement a basic network.</td>
</tr>
</tbody>
</table>

Exploring Network Operations
<table>
<thead>
<tr>
<th>87</th>
<th>+</th>
<th>Demonstrate use of monitoring tools.</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>+</td>
<td>Analyze metrics and reports from monitoring and tracking performance tools.</td>
</tr>
<tr>
<td>89</td>
<td>+</td>
<td>Demonstrate use of resources to support configuration management.</td>
</tr>
<tr>
<td>90</td>
<td>+</td>
<td>Explain the importance of implementing network segmentation.</td>
</tr>
<tr>
<td>91</td>
<td>+</td>
<td>Install patches and updates.</td>
</tr>
<tr>
<td>92</td>
<td>+</td>
<td>Configure a switch.</td>
</tr>
<tr>
<td>93</td>
<td>+</td>
<td>Install wireless LAN infrastructure.</td>
</tr>
</tbody>
</table>

Understanding Network Security
<table>
<thead>
<tr>
<th>94</th>
<th>+</th>
<th>Compare risk-related concepts.</th>
</tr>
</thead>
<tbody>
<tr>
<td>95</td>
<td>+</td>
<td>Compare common network vulnerabilities and threats.</td>
</tr>
<tr>
<td>96</td>
<td>+</td>
<td>Demonstrate network hardening techniques.</td>
</tr>
<tr>
<td>Task Number</td>
<td>8629</td>
<td>Tasks/Competencies</td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td>97</td>
<td></td>
<td>Compare physical security controls.</td>
</tr>
<tr>
<td>98</td>
<td></td>
<td>Install a basic firewall.</td>
</tr>
<tr>
<td>99</td>
<td></td>
<td>Explain the purpose of various network access control models.</td>
</tr>
<tr>
<td>100</td>
<td></td>
<td>Describe basic forensic concepts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Troubleshooting Networks</strong></td>
</tr>
<tr>
<td>101</td>
<td></td>
<td>Implement network troubleshooting methodology.</td>
</tr>
<tr>
<td>102</td>
<td></td>
<td>Analyze the output of troubleshooting tools.</td>
</tr>
<tr>
<td>103</td>
<td></td>
<td>Troubleshoot common wireless issues.</td>
</tr>
<tr>
<td>104</td>
<td></td>
<td>Troubleshoot common copper cable issues.</td>
</tr>
<tr>
<td>105</td>
<td></td>
<td>Troubleshoot common fiber cable issues.</td>
</tr>
<tr>
<td>106</td>
<td></td>
<td>Troubleshoot common network issues.</td>
</tr>
<tr>
<td>107</td>
<td></td>
<td>Troubleshoot common security issues.</td>
</tr>
<tr>
<td>108</td>
<td></td>
<td>Troubleshoot common WAN issues.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Applying Industry Standards, Practices, and Network Theory</strong></td>
</tr>
<tr>
<td>109</td>
<td></td>
<td>Describe OSI layers.</td>
</tr>
<tr>
<td>110</td>
<td></td>
<td>Explain the basics of network theory and concepts.</td>
</tr>
<tr>
<td>111</td>
<td></td>
<td>Deploy the appropriate wireless standard.</td>
</tr>
<tr>
<td>112</td>
<td></td>
<td>Deploy wired connectivity standards.</td>
</tr>
<tr>
<td>113</td>
<td></td>
<td>Implement network policies and procedures.</td>
</tr>
<tr>
<td>114</td>
<td></td>
<td>Summarize safety practices.</td>
</tr>
</tbody>
</table>
### Curriculum Framework

**Demonstrating Ethical Behavior with Computer Systems Technology**

**Task Number 39**

**Describe security issues related to computer hardware, software, and data.**

**Definition**

Description should include a list of methods for preventing and consequences of dealing with

- theft of equipment or intellectual property
- loss or corruption of data through viruses
- unauthorized entry into the computer system
- accidental loss or corruption of data by a user or company
- loss or theft of private company or customer information.

**Process/Skill Questions**

- What is shoulder surfing?
- What is an acceptable use policy (AUP)?
- What is considered a strong password?
• What is ransomware?

Task Number 40

Explain concepts related to copyright, public domain, copy protection, intellectual property, and licensing agreements.

Definition

Explanation should include, but not be limited to software, media (e.g., music, pictures), and logo requirements. Identification should also include

• a list of terms
• examples of each concept
• laws covering the protection of published information
• legal and ethical issues arising from the infringement of copyright laws and licensing agreements.

Process/Skill Questions

• What is pirated software? Is it true that it isn’t considered stealing if the person didn’t know it was pirated software? Explain.
• How does one determine whether a picture on the Internet is free to use? Explain.
• What are some examples of intellectual property?
• What fines might one expect from a violation of copyright law?

Task Number 41

Describe concepts of cybersecurity, honesty, courtesy, and confidentiality related to information and email systems and social networking (e.g., spam, viruses, and etiquette).

Definition

Description should include

• system security (i.e., ensuring information is transmitted according to approved protocol)
• electronic courtesy (i.e., ensuring the rules of network etiquette are followed)
confidentiality (i.e., ensuring through technology that information remains private and secure).

• technological integrity (i.e., verifying the source of information and ensuring that information on a user’s screen is the same as what was sent)
• availability (i.e., ensuring that data/information remains available and intact).

Process/Skill Questions

• With regard to cybersecurity, what does CIA stand for?
• What does availability mean with regard to cybersecurity?
• Why is data integrity important?

Task Number 42

Analyze Internet privacy issues and computer crimes, including identity theft.

Definition

Analysis should include research to identify computer crimes and privacy issues related to Internet use, such as

• infection of a computer by a virus
• computer hacking
• cyberstalking
• theft of computer equipment
• software piracy
• identity theft

and methods to prevent or protect against each.

Process/Skill Questions

• What physical security issues can be implemented to protect computer systems?
• What are the dangers and ethical considerations involved in software piracy?
• What is the difference between white hat and black hat hacking?

Task Number 43
Comply with copyright and patent laws.

Definition

Compliance should pertain to scanned images and documents, electronic clip art, recorded sounds, recorded and scanned photography, trademarks, and other elements adapted for use in desktop publishing, multimedia, and web documents.

Compliance should include

- identifying applicable copyright and patent laws
- discussing the consequences of illegal use of any images, documents, audio, video, recordings, trademarks, and any other elements adapted for use in desktop publishing, multimedia, and web documents
- discussing the different methods (direct contact with company, copyright clearinghouses) for obtaining permission to use copyrighted materials
- documenting all copyrighted materials used in class assignments.

Process/Skill Questions

- What are the differences between images that are copyright protected and those which are public domain?
- How does one gain permission to use copyrighted materials?
- What images can be used for class PowerPoint presentations?

Task Number 44

Comply with policies regarding acceptable use of technology.

Definition

Compliance should include evaluating the components of various acceptable use policies (AUPs) (e.g., school policies, company policies) and adhering to those policies.

Process/Skill Questions

- When a school acceptable use policy has a guideline not included in state or federal statutes, do you have to comply with the school policy?
- Why do organizations require employee or student signatures on an acceptable use policy? What is the users' responsibility, regardless of whether a signature was obtained?
- How should an employer go about informing workers of changes to the acceptable use policy?
Exploring Windows Operating Systems

Task Number 45

Compare features and requirements of Microsoft operating systems.

Definition

Comparison should include systems such as Windows Vista, Windows 7, Windows 8, Windows 8.1, and Windows 10, and the following:

- Features
  - 32-bit vs. 64-bit
  - Aero, gadgets, user account control, BitLocker, shadow copy, system restore, ready boost, sidebar, compatibility mode, virtual XP mode, easy transfer, administrative tools, defender, Windows firewall, security center, event viewer, file structure and paths, category view vs. classic view
  - Side-by-side apps, Metro UI, Pinning, One Drive, Windows store, multimonitor task bars, charms, Start Screen, PowerShell, Live sign in, Action Center
- Upgrade paths
  - Differences between in-place upgrades, compatibility tools, Windows upgrade operating system (OS) adviser

Process/Skill Questions

- What are the differences between 32 and 64-bit operating systems?
- What is an in-place upgrade?
- How does classic view differ from category view in the Control Panel?
- What does BitLocker do?

Task Number 46

Install Windows PC operating systems.

Definition

Installation should include appropriate methods and the following:

- Boot methods
o Universal Serial Bus (USB)
  o Compact Disc, read-only-memory (CD-ROM)
  o Digital Video Disc or Digital Versatile Disc (DVD)
  o Preboot Execution Environment (PXE)
  o Solid state/flash drives
  o Netboot
  o External/hot swappable drive
  o Internal hard drive (partition)

• Type of installations
  o Unattended installation
  o Upgrade
  o Clean install
  o Repair installation
  o Multiboot
  o Remote network installation
  o Image deployment
  o Recovery partition
  o Refresh/restore

• Partitioning
  o Dynamic
  o Basic
  o Primary
  o Extended
  o Logical
  o Globally Unique Identifier (GUID) Partition Table (GPT)

• File system types/formatting
  o Extended File Allocation Table (exFAT)
  o 32-bit File Allocation Table (FAT32)
  o New Technology File System (NTFS)
  o Compact Disc File System (CDFS)
  o Network File System (NFS)
  o ext3, ext4
  o Quick format vs. full format

• Load alternate third-party drivers when necessary
• Workgroup vs. domain setup
• Time/date/region/language settings
• Driver installation, software and windows updates
• Factory recovery partition
• Properly formatted boot drive with the correct partitions/format

Process/Skill Questions

• How can you change the boot order when installing an operating system from a USB drive?
• What is an International Standards Organization (ISO) file?
• What are the differences between exFAT, FAT32, and NTFS?
• How does a quick format differ from a full format?

Task Number 47

Apply Microsoft command line tools.

Definition

Application should include the following command line tools:

• TASKKILL
• BOOTREC
• SHUTDOWN
• TASKLIST
• MD
• RD
• CD
• DEL
• FORMAT
• COPY
• XCOPY
• ROBOCOPY
• DISKPART
• SFC
• CHKDSK
• GPUPDATE
• GPRERESULT
• DIR
• EXIT
• HELP
• EXPAND
• [command name] /?

Commands available with standard privileges vs. administrative privileges

Process/Skill Questions

• What operating systems use the various, specific command-line interface (CLI) commands?
• What commands require administrative privileges?
• What Linux command is equivalent to the Windows RUNAS command?
• What is the difference between the /scannow and /scanboot parameters of the system file checker (SFC) command?
Task Number 48

Use Microsoft OS features and tools.

Definition

Use should include the following:

- Administrative
  - Computer management
  - Device manager
  - Local users and groups
  - Local security policy
  - Performance monitor
  - Services
  - System configuration
  - Task scheduler
  - Component services
  - Data sources
  - Print management
  - Windows memory diagnostics
  - Windows firewall
  - Advanced security

- MSCONFIG
  - General
  - Boot
  - Services
  - Startup
  - Tools

- Task Manager
  - Applications
  - Processes
  - Performance
  - Networking
  - Users

- Disk Management
  - Drive status
  - Mounting
  - Initializing
  - Extending partitions
  - Splitting partitions
  - Shrink partitions
  - Assigning/changing drive letters
• Adding drives
• Adding arrays
• Storage spaces
• Other
  o User State Migration tool (USMT)
  o Windows Easy Transfer
  o Windows Upgrade Advisor
• System utilities
  o REGEDIT
  o COMMAND
  o SERVICES.MSC
  o MMC
  o MSTSC
  o NOTEPAD
  o EXPLORER
  o MSINFO32
  o DXDIAG
  o DEFRAg
  o System restore
  o Windows Update

Process/Skill Questions

• What components’ performance is displayed in a graph in the Windows Performance Monitor?
• How do you extend a partition in Windows compared to macOS X?
• What is the Graphical User Interface (GUI) version of USMT?

Task Number 49

Use Windows Control Panel utilities.

Definition

Use should include the following:

• Internet options
  o Connections
  o Security
  o General
  o Privacy
  o Programs
  o Advanced
• Display/display settings
  o Resolution
  o Color depth
  o Refresh rate
• User accounts
• Folder options
  o View hidden files
  o Hide extensions
  o General options
  o View options
• System
  o Performance (virtual memory)
  o Remote settings
  o System protection
• Windows firewall
• Power options
  o Hibernate
  o Power plans
  o Sleep/suspend
  o Standby
• Programs and features
• HomeGroup
• Devices and printers
• Sound
• Troubleshooting
• Network and Sharing Center
• Device Manager

Process/Skill Questions

• What is the difference between hibernate and sleep?
• How do you change the default printer for a system?
• How can you see hidden files within a folder?
• What is virtual memory?

Task Number 50

Install Windows networking on a client/desktop.

Definition

Installation should include use and configuration of the following:
- HomeGroup vs. WorkGroup
- Domain setup
- Network shares/administrative shares/mapping drives
- Printer sharing vs. network printer mapping
- Establish networking connections
  - Virtual Private Network (VPN)
  - Dial-ups
  - Wireless
  - Wired
  - Wireless wide area network (WWAN) (Cellular)
- Proxy settings
- Remote Desktop Connection
- Remote Assistance
- Home vs. work vs. public network settings
- Firewall settings
  - Exceptions
  - Configuration
  - Enabling/disabling Windows firewall
- Configuring an alternative IP address in Windows
  - IP addressing
  - Subnet mask
  - Domain Name Server (DNS)
  - Gateway
- Network card properties
  - Half duplex/full duplex/auto
  - Speed
  - Wake-on-LAN
  - Quality of Service (QoS)
  - Basic input/output system (BIOS) (on-board NIC)

Process/Skill Questions

- How does a HomeGroup differ from a WorkGroup?
- What port must be open in the firewall to allow for a remote desktop connection?
- What is the difference between a shared printer and a network printer?
- What are the benefits of a VPN?

---

Task Number 51

Perform common preventive maintenance procedures.

Definition
Performance should include use of appropriate Windows OS tools and the following:

- **Best practices**
  - Scheduled backups
  - Scheduled disk maintenance
  - Windows updates
  - Patch management
  - Driver/firmware updates
  - Antivirus/Anti-malware updates
- **Tools**
  - Backup
  - System restore
  - Recovery image
  - Disk maintenance utilities

**Process/Skill Questions**

- Why is patch management important in a large network?
- What system restore options allow the technician to retain user data files and applications?
- What disk maintenance tool can be used on a hard disk drive but not an SSD?
- How frequently should antivirus and anti-malware signature files be updated?

**Exploring Other Operating Systems and Technologies**

**Task Number 52**

**Identify common features and functions of the macOS and Linux OS.**

**Definition**

Identification should include the following:

- **Best practices**
  - Scheduled backups
  - Scheduled disk maintenance
  - System updates/App Store
  - Patch management
  - Driver/firmware updates
  - Antivirus/anti-malware updates
- **Tools**
• Backup/Time Machine
• Restore/snapshot
• Image recovery
• Disk maintenance utilities
• Shell/Terminal
• Screen sharing
• Force Quit

• Features
  • Multiple desktops/Mission Control
  • Key Chain
  • Spot Light
  • iCloud
  • Gestures
  • Finder
  • Remote Disc
  • Dock
  • Boot Camp

• Basic Linux commands
  • ls
  • grep
  • cd
  • shutdown
  • pwd vs. passwd
  • mv
  • cp
  • rm
  • chmod
  • chown
  • iwconfig/ifconfig
  • ps
  • su/sudo
  • apt-get
  • vi
  • dd
  • update
  • install

Process/Skill Questions

• What commands are the same for Linux CLI and disk operating system (DOS)?
• How do Linux updates differ from Windows updates?
• How does new app installation differ between Windows and Linux?

---

Task Number 53
Set up virtual machines on a host computer.

Definition

Setup should include the following:

• Purpose of virtual machines
• Resource requirements
• Emulator requirements
• Security requirements
• Network requirements
• Hypervisor
• Use of shared resources.
• 32-bit vs. 64-bit operating systems

Process/Skill Questions

• What is the difference between a host computer and a guest computer?
• What method is used to optimize the performance of a virtual machine?
• What is the meaning of the statement, "Virtual machines share the resources of the host computer."?

Task Number 54

Identify basic cloud concepts.

Definition

Identification should include the following:

• Software as a Service (SaaS)
• Infrastructure as a Service (IaaS)
• Platform as a Service (PaaS)
• Public vs. Private vs. Hybrid vs. Community
• Rapid Elasticity
• On-demand
• Resource pooling
• Measured service
• Weaknesses of cloud computing

Process/Skill Questions
• What happens to cloud computing when your network goes down?
• Would you trust a cloud administrator to protect your sensitive data? Explain.
• How is data loss prevented or protected against in the cloud?

---

**Task Number 55**

**Describe services provided by networked hosts.**

**Definition**

Description should include the following:

- Server roles
  - Web server
  - File server
  - Print server
  - Dynamic Host Configuration Protocol (DHCP) server
  - DNS
  - Proxy server
  - Mail server
  - Authentication server

- Internet appliance
  - Unified Threat Management (UTM)
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)

- Legacy/embedded systems

**Process/Skill Questions**

- How do you set up a DHCP or DNS Server on a Windows 2012 R2 Server?
- Why would a network administrator choose to use a Linux Samba server instead of a Windows server?

---

**Task Number 56**

**Identify basic features of mobile operating systems.**

**Definition**
Identification should include the following as it relates to Android vs. iOS vs. Windows vs. Google OS:

- Open source vs. closed source/vendor specific
- App source (Google Play Store, App Store, and Store)
- Screen orientation (accelerometer/gyroscope)
- Screen calibration
- GPS and geotracking
- WiFi calling
- Launcher/GUI
- Virtual assistant
- Software Development Kit/Android Application Package (SDK/APK)
- Emergency notification
- Mobile payment service

Process/Skill Questions

- Why would one mobile OS be more popular than another?
- Where do different operating systems get their applications?
- Who makes applications for mobile devices?

Task Number 57

Set up mobile device network connectivity and email.

Definition

Setup should include the following:

- Wireless/cellular data network (enable/disable)
  - Hotspot
  - Tethering
  - Airplane mode
- Bluetooth
  - Enable Bluetooth
  - Enable pairing
  - Find device for pairing
  - Enter appropriate PIN code
  - Test connectivity
- Corporate and Internet Service Provider (ISP) email configuration
  - POP3
  - IMAP
  - Port and Secure Sockets Layer (SSL) settings
- Exchange, Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Integrated commercial provider email configuration
  - Google/Inbox
  - Yahoo
  - Outlook.com
  - iCloud
- Primary Rate Interface (PRI) updates/Preferred Roaming List (PRL) updates/Baseband updates
- Radio firmware
- International Mobile Equipment Identity (IMEI) vs. International Mobile Subscriber Identity (IMSI)
- VPN

Process/Skill Questions

- Why would a business or office choose to use company email instead of cloud-based email?
- What are the pros/cons of using a WiFi connection in a public location?
- What are the different ways a cellphone can connect to another device wirelessly?

Task Number 58

Synchronize mobile devices.

Definition

Synchronization should include the following:

- Types of data to synchronize
  - Contacts
  - Programs
  - Email
  - Pictures
  - Music
  - Videos
  - Calendar
  - Bookmarks
  - Documents
  - Location data
  - Social media data
  - eBooks
- Synchronization methods
  - Synchronize to the cloud
Synchronize to the desktop
- Mutual authentication for multiple services (Single Sign-ON [SSO])
- Software requirements to install the application on the PC
- Connection types to enable synchronization

Process/Skill Questions

- Why would a person want to synchronize data with other devices?
- What are the possible dangers/drawbacks of synchronization?

Applying Operational Procedures

Task Number 59

Analyze appropriate safety procedures.

Definition

Analysis should include the following:

- Equipment grounding
- Proper component handling and storage
  - Antistatic bags
  - Electrostatic discharge (ESD) straps
  - ESD mats
  - Self-grounding
- Toxic waste handling
  - Batteries
  - Toner
  - Cathode ray tube (CRT)
- Personal safety
  - Disconnect power before repairing PC
  - Remove jewelry
  - Lifting techniques
  - Weight limitations
  - Electrical fire safety
  - Cable management
  - Safety goggles
  - Air filter mask
- Compliance with local government regulations

Process/Skill Questions

- Why is it important to disconnect a PC before repairing it?
• What is the difference between antistatic bags, ESD straps, ESD mats, and self-grounding?
• How is toxic waste (i.e., batteries, toner, and CRT) properly disposed of?
• What personal protective equipment is needed when operating on a computer?

Task Number 60

Analyze controls and their impact on the environment.

Definition

Analysis should include appropriate controls and the following:

• Safety Data Sheets (SDS) documentation for handling and disposal
• Temperature, humidity level awareness and proper ventilation
• Power surges, brownouts, blackouts
  o Battery backup
  o Surge suppressor
• Protection from airborne particles
  o Enclosures
  o Air filters/mask
• Dust and debris
  o Compressed air
  o Vacuums
• Compliance to local government regulations

Process/Skill Questions

• What are SDS and Occupational Safety and Health Administration (OSHA)?
• How do SDS and OSHA relate to local government regulations?
• How is toxic waste (i.e., batteries, toner, and CRT) properly disposed of?
• What safety items are needed to protect from airborne particles, dust, and debris?

Task Number 61

Summarize the process of addressing prohibited content/activity.

Definition
Summary should include the following incident response procedures:

- First response
- Identify
- Report through proper channels
- Data/device preservation
- Use of documentation/documentation changes
- Chain of custody
- Tracking of evidence/documenting process

**Process/Skill Questions**

- What are the stages of the first response stage?
- What are the procedures in an incident response?
- What is the chain of custody for tracking evidence?

---

**Task Number 62**

**Explain privacy, licensing, and policy concepts.**

**Definition**

Explanation should include the following:

- Licensing/Digital Rights Management/End-User Licensing Agreement (DRM/EULA)
  - Open source vs. commercial license
  - Personal license vs. enterprise licenses
- Personally identifiable information
- Follow corporate end-user policies and security best practices

**Process/Skill Questions**

- What is the difference between an open source and a commercial license?
- What is the difference between a personal license and an enterprise license?
- Why is it critical for employees to follow corporate end-user policies?
- What procedures do employers have in practice for security best practices?

---

**Task Number 63**
Demonstrate communication techniques and professionalism.

Definition

Demonstration should include the following:

- Use proper language (i.e., avoid jargon, acronyms and slang when applicable)
- Maintain a positive attitude/project confidence
- Actively listen (take notes) and avoid interrupting the customer
- Be culturally sensitive
  - Use appropriate professional titles, when applicable
- Be on time (if late, contact the customer)
- Avoid distractions
  - Personal calls
  - Texting/social media sites
  - Talking to co-workers while interacting with customers
  - Personal interruptions
- Dealing with difficult customer or situation
  - Do not argue with customers and/or be defensive
  - Avoid dismissing customer problems
  - Avoid being judgmental
  - Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue or question to verify understanding)
  - Do not disclose experiences via social media outlets
- Set and meet expectations/timeline and communicate status with the customer
  - Offer different repair/replacement options if applicable
  - Provide proper documentation on the services provided
  - Follow up with customer/user at a later date to verify satisfaction
- Deal appropriately with customers confidential and private materials (located on a computer, desktop, printer, etc.)

Process/Skill Questions

- Why is it important to use proper language and have a positive attitude?
- In what ways can you be culturally sensitive?
- What should you do if you deal with a difficult customer or situation?
- How would you appropriately handle customers confidential and private materials?

Task Number 64

Explain the troubleshooting theory.
Definition

Explanation should include always considering corporate policies, procedures, and impacts before implementing changes. Explanation should also include the steps of the CompTIA troubleshooting theory:

1. Identify the problem. (Question the user and identify user changes to computer and perform backups before making changes.)
2. Establish a theory of probable cause (question the obvious). If necessary, conduct external or internal research based on symptoms.
3. Test the theory to determine cause.
   a. Once theory is confirmed, determine next steps to resolve problem.
   b. If theory is not confirmed, re-establish new theory or escalate.
4. Establish a plan of action to resolve the problem and implement the solution.
5. Verify full system functionality and if applicable implement preventive measures.

Process/Skill Questions

- Why is the troubleshooting theory important?
- Why is it imperative to consider corporate policies, procedures, and impacts before implementing changes?
- What steps are included in CompTIA’s troubleshooting theory?

Understanding Security

Task Number 65

Identify common threats and vulnerabilities.

Definition

Identification should consider that threats are constantly emerging and evolving, and should include the following:

- Malware
  - Spyware
  - Viruses
  - Worms
  - Trojans
  - Rootkits
  - Ransomware
- Phishing
- Spear phishing
• Spoofing
• Social engineering
• Shoulder surfing
• Zero-day attack
• Zombie/botnet
• Brute forcing
• Dictionary attacks
• Non-compliant systems
• Violations of security best practices
• Tailgating
• Man-in-the-middle

Process/Skill Questions

• What distinguishes malware from malicious people on the Internet?
• What social engineering would be effective on a department store as opposed to a military base?
• How does a zero-day attack differ from one that is a month old?

Task Number 66

Describe the methods used to make computers and networks more secure.

Definition

Description should include the following:

• Physical security
  o Lock doors
  o Mantrap
  o Cable locks
  o Securing physical documents/passwords/shredding
  o Biometrics
  o Identification (ID) badges
  o Key fobs
  o Radio Frequency Identification (RFID) badge
  o Smart card
  o Tokens
  o Privacy filters
  o Entry control roster
• Digital security
  o Antivirus/Anti-malware
- Firewalls
- User authentication/strong passwords
- Multifactor authentication
- Directory permissions
- VPN
- Digital light processing (DLP)
- Disabling ports
- Access control lists
- Smart card
- Email filtering
- Trusted/untrusted software sources
- User education/AUP
- Principle of least privilege

Description should also take into account the fact that this list is constantly growing.

**Process/Skill Questions**

- Why is physical security not sufficient to protect a network?
- Why is security not just a job for system administrators?
- What more can be done to train workers about security?
- What are the advantages and disadvantages of multi-factor authentication?

**Task Number 67**

**Configure security settings.**

**Definition**

Configuration should use best practices and the following:

- Password best practices
  - Setting strong passwords
  - Password expiration
  - Changing default user names/passwords
  - Screensaver required password
  - BIOS/UEFI passwords
  - Requiring passwords
- Account management
  - Restricting user permissions
  - Login time restrictions
  - Disabling guest account
  - Failed attempts lockout
Timeout/screen lock

• Disable autorun
• Data encryption
• Patch/update management
• Turn off unused services
• Look at hidden folders
• Study local security policies and what they prevent

Process/Skill Questions

• Why should individual users be trusted to configure their own security settings?
• How might one configure security on a workstation? What should be taken into consideration when doing so?
• Why should the guest account be disabled?
• What are two versions of "security best practices" for the computer you are using right now? Does your computer have all the items covered? Explain.
• What are the advantages and disadvantages of data encryption?

Task Number 68

Describe methods for securing mobile devices.

Definition

Description should include the following:

• Screen locks
  o Fingerprint lock
  o Face lock
  o Swipe lock
  o Passcode lock
• Remote wipes
• Locator applications
• Remote backup applications
• Failed login attempt restrictions
• Antivirus/anti-malware
• Patching/OS updates
• Biometric authentication
• Full device encryption
• Multifactor authentication
• Authenticator applications
• Trusted sources vs. untrusted sources
• Firewalls
• Policies and procedures
  o Bring-Your-Own-Device (BYOD) vs. corporate owned
  o Profile security requirements

Process/Skill Questions

• What method(s) have you used to secure your own mobile device(s)?
• What is the danger when personal cell phones are allowed into high security facilities? Explain.
• What additional security methods could you configure on your mobile device?

Task Number 69

Use data destruction and disposal methods.

Definition

Use should include appropriate methods and the following:

• Physical destruction
  o Shredder
  o Drill/hammer
  o Electromagnetic (Degaussing)
  o Incineration
  o Certificate of destruction
• Recycling or repurposing best practices
  o Low-level format vs. standard format
  o Overwrite
  o Drive wipe

Process/Skill Questions

• Why will formatting a hard drive not help a drug dealer to escape conviction?
• How do Trojans infect a computer? Explain.
• What is a Department of Defense (DOD) wipe of a hard drive?

Task Number 70

Secure SOHO wireless and wired networks.
Definition

Securing the networks should include the following:

- Wireless specific
  - Changing default SSID
  - Setting encryption
  - Disabling SSID broadcast
  - Antenna and access point placement
  - Radio power levels
  - WiFi Protected Setup (WPS)
- Change default usernames and passwords
- Enable Media Access Control (MAC) filtering
- Assign static IP addresses
- Firewall settings
- Port forwarding/mapping
- Disabling ports
- Content filtering/parental controls
- Update firmware
- Physical security
- Have a defined security policy.
- Have a defined security mitigation procedure.

Process/Skill Questions

- In general terms, how would you design an attack on a new department store to feel out vulnerabilities?
- How does the configuration of two wireless routers from different companies in our lab differ in their controls?
- What should a business owner do if it is suspected that the network is breached?

Troubleshooting Software

Task Number 71

Troubleshoot PC OS problems.

Definition

Troubleshooting should include the following symptoms and tools:

- Common symptoms
  - Proprietary crash screens (BSOD/pinwheel)
  - Failure to boot
- Improper shutdown
- Spontaneous shutdown/restart
- Device fails to start/detected
- Missing DLL message
- Services fails to start
- Compatibility error
- Slow system performance
- Boots to safe mode
- File fails to open
- Missing New Technology Loader (NTLDR)
- Missing boot configuration data
- Missing operating system
- Missing graphical interface
- Missing GRand Unified Bootloader/Linux Loader (GRUB/LILO)
- Kernel panic
- Graphical Interface fails to load
- Multiple monitor misalignment/orientation

- Tools
  - BIOS/UEFI
  - SFC
  - Logs
  - System Recovery Options
  - Repair disks
  - Pre-installation environments
  - MSCONFIG
  - DEFRAG
  - REGSRV32
  - REGEDIT
  - Event viewer
  - Safe mode
  - Command prompt
  - Uninstall/reinstall/repair

Process/Skill Questions

- Why is it important to monitor resources on your computer?
- What is the process to determine what is not working in an unexpected shutdown?
- What is the lockup feature?
- What is BIOS and POST?

Task Number 72

Troubleshoot common PC security issues.
Definition

Troubleshooting should include the following symptoms and tools:

- **Common symptoms**
  - Pop-ups
  - Browser redirection
  - Security alerts
  - Slow performance
  - Internet connectivity issues
  - PC/OS lock up
  - Application crash
  - OS updates failures
  - Rogue antivirus
  - Spam
  - Renamed system files
  - Files disappearing
  - File permission changes
  - Hijacked email
  - Responses from users regarding email
  - Automated replies from unknown sent email
  - Access denied
  - Invalid certificate (trusted root CA)

- **Tools**
  - Antivirus software
  - Anti-malware software
  - Recovery console
  - Terminal
  - System restore/Snapshot
  - Pre-installation environments
  - Event viewer
  - Refresh/restore
  - MSCONFIG/Safe boot

Troubleshooting should also follow best practice procedures for malware removal:

1. Identify malware symptoms.
2. Quarantine infected system.
3. Disable system restore (in Windows).
4. Remediate infected systems.
   a. Update anti-malware software.
   b. Scan and removal techniques (safe mode, pre-installation environment)
5. Schedule scans and run updates.
6. Enable system restore and create restore point (in Windows).
7. Educate end user.
Process/Skill Questions

- What are the best practice procedures for malware removal?
- What is the difference between antivirus software and anti-malware software?
- Why is it important to keep your PC secure?

Task Number 73

Troubleshoot mobile OS and application issues.

Definition

Troubleshooting should include the following common symptoms and appropriate tools:

- Common symptoms
  - Dim display
  - Intermittent wireless
  - No wireless connectivity
  - No Bluetooth connectivity
  - Cannot broadcast to external monitor
  - Touchscreen non-responsive
  - Apps not loading
  - Slow performance
  - Unable to decrypt email
  - Extremely short battery life
  - Overheating
  - Frozen system
  - No sound from speakers
  - Inaccurate touch screen response
  - System lockout

- Tools
  - Hard reset
  - Soft reset
  - Close running applications
  - Reset to factory default
  - Adjust configurations/settings
  - Uninstall/reinstall apps
  - Force stop

Process/Skill Questions

- What are some reasons why an application might be running slowly?
• What are some reasons why the battery of a mobile device becomes depleted faster than normal?
• What is the difference between a hard reset and soft reset?

Task Number 74
Troubleshoot mobile OS and application security issues.
Definition
Troubleshooting should include the following common symptoms and appropriate tools:

• Common symptoms
  o Signal drop/weak signal
  o Power drain
  o Slow data speeds
  o Unintended WiFi connection
  o Unintended Bluetooth pairing
  o Leaked personal files/data
  o Data transmission over limit
  o Unauthorized account access
  o Unauthorized root access
  o Unauthorized location tracking
  o Unauthorized camera/microphone activation
  o High resource utilization
• Tools
  o Anti-malware
  o App scanner
  o Factory reset/clean install
  o Uninstall/reinstall apps
  o WiFi analyzer
  o Force stop
  o Cell tower analyzer
  o Backup/restore
  o iTunes/iCloud/Apple Configurator
  o Google Sync
  o One Drive

Process/Skill Questions
• What would be reasons why your monitor goes black after Windows begins to load?
• What is VGA mode and why is it important?
• What happens to hardware when drivers are not up-to-date?
• What are some reasons why personal files or data are leaked?
• Why is a factory reset or clean install beneficial?

Exploring Network Architecture

Task Number 75

Explain the functions and applications of various network devices.

Definition

Explanation should include the following:

• Router
• Switch
• Multilayer switch
• Firewall
• Host Intrusion Detection System (HIDS)
• IDS/IPS
• Access point (wireless/wired)
• Content filter
• Load balancer
• Hub
• Analog modem
• Packet shaper
• VPN concentrator

Process/Skill Questions

• What device allows you to create more than one network?
• What is the difference between an IDS and an IPS?
• In what layer of the OSI does a switch work?

Task Number 76

Compare networking services and applications.

Definition
Comparison should include the following:

- **VPN**
  - Site-to-site/host-to-site/host-to-host
  - Protocols
  - Internet Protocol Security (IPSec)
  - Generic Routing Encapsulation (GRE)
  - SSL VPN
  - Point-to-Point/Point-to-Point Tunneling Protocol (PTP/PPTP)
- **Terminal Access Control Access Control System/Remote Authentication Dial-In User Service (TACACS/RADIUS)**
- Remote Access Service (RAS)
- Web services
- Unified voice services
- Network controllers

**Process/Skill Questions**

- What are the differences between IPSec and SSL VPN protocols?
- What is RAS?
- What is the difference between TACACS and RADIUS?

**Task Number 77**

**Install networking services/applications.**

**Definition**

Installation should include configuration for the following networking services/applications:

- **DHCP**
  - Static vs. dynamic IP addressing
  - Reservations
  - Scopes
  - Leases
  - Options (DNS, suffixes)
  - IP helper/DHCP relay
- **DNS**
  - DNS records (Address; Mail Exchanger; Authentication, Authorization, Accounting, and Address; Canonical Name; Pointer [A, MX, AAAA, CNAME, PTR])
  - Dynamic DNS
- **Proxy/reverse proxy**
- Network Address Translation (NAT)
  - Port Address Translation (PAT)
  - Static Network Address Translation (SNAT)
  - Destination Network Address Translation (DNAT)
- Port forwarding

**Process/Skill Questions**

- What is an IP Lease?
- What is the advantage of dynamic IP addressing?
- What is the purpose of a DNS server?

---

**Task Number 78**

**Explanation**

**Explain the characteristics and benefits of various wide area network (WAN) technologies.**

**Definition**

Explanation should include the following:

- Fiber
  - Synchronous Optical Network (SONET)
  - Dense Wavelength Division Multiplexing (DWDM)
  - Course Wave Division Multiplexing (CWDM)
- Frame relay
- Satellite
- Broadband cable
- DSL/Asymmetric Digital Subscriber Line (ADSL)
- Integrated Services Digital Network (ISDN)
- Asynchronous Transfer Mode (ATM)
- Point-to-Point Protocol (PPP)/multilink PPP
- Multi-Protocol Label Switching (MPLS)
- Global System for Mobile Communications (GSM)/Code Division Multiple Access (CDMA)
  - Long-Term Evolution (LTE)/4G
  - High-Speed Packet Access Plus (HSPA+)
  - 3G
  - Edge
- Dialup
- WiMAX
- MetroEthernet
- Leased lines
• T-1
• T-3
• E-1
• E-3
• OC3
• OC12

• Circuit switch vs. packet switch

Process/Skill Questions

• What is the maximum speed of T-1?
• What is the difference between packet and circuit switching?
• What is a T-line?

Task Number 79

Install various cable types and connectors.

Definition

Installation should include proper termination and the following:

• Copper connectors
  o Registered Jack (RJ)-11
  o RJ-45
  o RJ-48C
  o DB-9/RS-232
  o DB-25
  o UTP coupler
  o Bayonet-Neill-Concelman or British Naval Connector (BNC) coupler
  o BNC
  o F-connector
  o 110 block
  o 66 block

• Copper cables
  o Shielded vs. unshielded
  o CAT3, CAT5, CAT5e, CAT6, CAT6a
  o Permanent Virtual Circuit (PVC) vs. plenum
  o Radio Guide (RG)-59
  o RG-6
  o Straight-through vs. crossover vs. rollover

• Fiber connectors
  o Straight Tip (ST)
- Standard Connector (SC)
- Local Connector (LC)
- Mechanical Transfer-Registered Jack (MT-RJ)
- Fibre Channel (FC)
- Fiber coupler

- Fiber cables
  - Single-mode
  - Multimode
  - Angle Polished Connector (APC) vs. Ultra-Polished Connector (UPC)

- Media converters
  - Single-mode fiber to Ethernet
  - Multimode fiber to Ethernet
  - Fiber to coaxial
  - Single-mode to multimode fiber

Installation should also include using appropriate tools, such as the following:

- Cable crimpers
- Punchdown tool
- Wire strippers
- Snips
- Optical Time Domain Reflectometer (OTDR)
- Cable certifier

Process/Skill Questions

- What tool is used to secure an RJ-45?
- What cable uses an F connector?
- What is the maximum speed for CAT6?

---

**Task Number 80**

Differentiate between common network topologies.

**Definition**

Differentiation should include the following:

- Mesh
  - Partial
  - Full
- Bus
- Ring
• Star
• Hybrid
• Point-to-point
• Point-to-multipoint
• Client-server
• Peer-to-peer

Process/Skill Questions

• What topology is the most redundant?
• What is the major advantage of a star topology?
• What is the difference between star and mesh topologies?

Task Number 81

Differentiate between network infrastructure implementations.

Definition

Differentiation should include the following:

• WAN
• MAN
• LAN
• WLAN
  o Hotspot
• PAN
  o Bluetooth
  o Infrared (IR)
  o Near-Field Communication (NFC)
• Supervisory Control and Data Acquisition/Industrial Control System (SCADA/ICS)
  o ICS server
  o Distributed Control System (DCS)/closed network
  o Remote terminal unit
  o Programmable logic controller
• Medianets
  o Video Teleconferencing (VTC)
  o Integrated Services Digital Network (ISDN)
  o IP/Session Initiation Protocol (SIP)

Process/Skill Questions
• What is the difference between a LAN and a WLAN?
• What technology do PANs use for printing?
• What does a remote terminal allow you to monitor?

Task Number 82

Configure addressing schema.

Definition

Configuration should include the following:

• IPv6
  • Auto-configuration
    ▪ Extended Unique Identifier (EUI) 64
  • DHCP6
  • Link local
  • Address structure
  • Address compression
  • Tunneling 6to4, 4to6
    ▪ Teredo, miredo
  • IPv4
    • Address structure
    • Subnetting
    • Automatic Private Internet Protocol Addressing (APIPA)
    • Classful A, B, C, D
    • Classless
• Private vs. public
• Network Address Translation/Port Address Translation (NAT/PAT)
• Media Access Control (MAC) addressing
• Multicast
• Unicast
• Broadcast
• Broadcast domains vs. collision domains

Process/Skill Questions

• What is the length of the IPV6 address? IPV4?
• What does the IPV4 address 169.254.10.106 represent?
• What class is 255.255.0.0?
Task Number 83

Explain basic routing concepts and protocols.

Definition

Explanation should include the following:

- Loopback interface
- Routing loops
- Routing tables
- Static vs. dynamic routes
- Default route
- Distance vector routing protocols
  - Routing Internet Protocol, version 2 (RIPv2)
- Hybrid routing protocols
  - Border Gateway Protocol (BGP)
- Link state routing protocols
  - Open Shortest Path First (OSPF)
  - Intermediate System to Intermediate System (IS-IS)
- Interior vs. exterior gateway routing protocols
- Autonomous system numbers
- Route redistribution
- High availability
  - Virtual Router Redundancy Protocol (VRRP)
  - Virtual IP
  - Hot Standby Router Protocol (HSRP)
- Route aggregation
- Routing metrics
  - Hop counts
  - Maximum Transmission Unit (MTU), bandwidth
  - Costs
  - Latency
  - Administrative distance
  - Shortest Path Bridging (SPB)

Process/Skill Questions

- How would you characterize a router’s loopback interface? Is it virtual or physical?
- What does a routing table determine?
- What is a hop count? Explain.

Task Number 84
Identify the basic elements of unified communication (UC) technologies.

**Definition**

Identification should include the following:

- Voice over IP (VoIP)
- Video
- Real-time services
  - Presence
  - Multicast vs. unicast
- QoS
  - Differentiated Services Code Point (DSCP)
  - Class of Service (COS)
- Devices
  - UC servers
  - UC devices
  - UC gateways

**Process/Skill Questions**

- What is VoIP?
- What are some examples of unified technologies?
- What is the difference between multicast and unicast?

**Task Number 85**

Compare technologies that support cloud virtualization.

**Definition**

Comparison should include the following:

- Virtualization
  - Virtual switches
  - Virtual routers
  - Virtual firewall
  - Virtual vs. physical Network Interface Cards (NICs)
  - Software-defined networking
- Storage area network
  - Internet Small Computer Systems Interface (iSCSI)
- Jumbo frame
- Fibre Channel
- Network attached storage

- Cloud concepts
  - Public IaaS, SaaS, PaaS
  - Private IaaS, SaaS, PaaS
  - Hybrid IaaS, SaaS, PaaS
  - Community IaaS, SaaS, PaaS

Process/Skill Questions

- What is the advantage of network attached storage (NAS)?
- What is a hypervisor?
- What is the difference between a virtual and a physical router?

Task Number 86

Given a set of requirements, implement a basic network.

Definition

Implementation should include the following:

- List of requirements
- Device types/requirements
- Environment limitations
- Equipment limitations
- Compatibility requirements
- Wired/wireless considerations
- Security considerations

Process/Skill Questions

- What are key considerations when implementing a network?
- What are ease of use vs. security considerations to verify?
- What is the first step when setting up a network?

Exploring Network Operations

Task Number 87
Demonstrate use of monitoring tools.

Definition

Demonstration should include appropriate tools, such as the following:

- Packet/network analyzer
- Interface monitoring tools
- Port scanner
- Top talkers/listeners
- SNMP management software
  - Trap
  - Get
  - Walk
  - Management Information Bases (MIBS)
- Alerts
  - Email
  - Short Message Service (SMS)
- Packet flow monitoring
- System Log (SYSLOG)
- Security Information and Event Management (SIEM)
- Environmental monitoring tools
  - Temperature
  - Humidity
- Power monitoring tools
- Wireless survey tools
- Wireless analyzers

Process/Skill Questions

- What is the purpose of a wireless survey tool?
- How do environmental factors affect networks?
- What tools are available to monitor packet traffic on a network?

Task Number 88

Analyze metrics and reports from monitoring and tracking performance tools.

Definition

Analysis should include the following:
- Baseline
- Bottleneck
- Log management
- Graphing
- Utilization
  - Bandwidth
  - Storage
  - Network device CPU
  - Network device memory
  - Wireless channel utilization
- Link status
- Interface monitoring
  - Errors
  - Utilization
  - Discards
  - Packet drops
  - Interface resets
  - Speed and duplex

Process/Skill Questions

- When using 802.11n or faster, what is typically the cause of network bottlenecks?
- What channels are commonly used in 802.11n?
- What is the advantage/disadvantage of enabling duplexing on a network port?

Task Number 89

Demonstrate use of resources to support configuration management.

Definition

Demonstration should include appropriate use and the following:

- Archives/backups
- Baselines
- On-boarding and off-boarding of mobile devices
- Network Access Control (NAC)
- Documentation
  - Network diagrams (logical/physical)
  - Asset management
  - IP address utilization
  - Vendor documentation
Process/Skill Questions

- What are the differences between a physical and logical network diagram?
- What is the value of a network baseline?
- Who sets the policies that govern the configuration of networks?

Task Number 90

Explain the importance of implementing network segmentation.

Definition

Explanation should include the following:

- SCADA systems/industrial control systems
- Legacy systems
- Separate private/public networks
- Honeypot/honeynet
- Testing lab
- Load balancing
- Performance optimization
- Security
- Compliance

Process/Skill Questions

- What is the difference between a honeypot and a honeynet?
- What is the purpose of setting up a separate public network?
- When would it be necessary to implement load balancing?

Task Number 91

Install patches and updates.

Definition
Installation should include application of the following:

- OS updates
- Firmware updates
- Driver updates
- Feature changes/updates
- Major vs. minor updates
- Vulnerability patches
- Upgrading vs. downgrading
  - Configuration backup
- Malware definitions

**Process/Skill Questions**

- What is the difference between a patch and an update?
- Why would someone choose to downgrade an update?
- From what site should device drivers be obtained/downloaded?

**Task Number 92**

**Configure a switch.**

**Definition**

Configuration should include using proper features and the following:

- **VLAN**
  - Native VLAN/default VLAN
  - VLAN Trunk Protocol (VTP)
- **Spanning tree (802.1d)/rapid spanning tree (802.1w)**
  - Flooding
  - Forwarding/blocking
  - Filtering
- **Interface configuration**
  - Trunking/802.1q
  - Tag vs. untag VLANs
  - Port bonding (Link Aggregation Control Protocol [LACP])
  - Port mirroring (local vs. remote)
  - Speed and duplexing
  - IP address assignment
  - VLAN assignment
- **Default gateway**
- **Power over Ethernet (PoE) and PoE+ (802.3af, 802.3at)**
• Switch management
  ◦ User/passwords
  ◦ Authentication, Authorization, and Accounting (AAA) configuration
  ◦ Console
  ◦ Virtual terminals
  ◦ In-band/out-of-band management
• Managed vs. unmanaged

Process/Skill Questions

• What is the benefit of using PoE?
• What is the difference between managed and unmanaged switches?
• What is the purpose of a VLAN?

Task Number 93

Install wireless LAN infrastructure.

Definition

Installation includes configuring and implementing the appropriate technologies in support of wireless-capable devices:

• SOHO wireless router
• Wireless access points
  ◦ Device density
  ◦ Roaming
  ◦ Wireless controllers
  ◦ VLAN pooling
  ◦ Light Weight Access Point Protocol (LWAPP)
• Wireless bridge
• Site surveys
  ◦ Heat maps
• Frequencies
  ◦ 2.4 gigahertz (GHz)
  ◦ 5.0 GHz
• Channels
• Goodput
• Connection types
  ◦ 802.11a-ht
  ◦ 802.11g-ht
• Antenna placement
• Antenna types
- Omnidirectional
- Unidirectional
- Multiple Input, Multiple Output/Multiuser MIMO (MIMO/MU-MIMO)
- Signal strength
  - Coverage
  - Differences between device antennas
- Service Set Identifier (SSID) broadcast
- Topologies
  - Ad hoc
  - Mesh
  - Infrastructure
- Mobile devices
  - Cellphones
  - Laptops
  - Tablets
  - Gaming devices
  - Media devices

Process/Skill Questions

- What is the advantage/disadvantage of using the 5.0 GHz frequency?
- What is the purpose of a unidirectional antenna?
- When would a wireless bridge be implemented?

Understanding Network Security

Task Number 94

Compare risk-related concepts.

Definition

Comparison should include the following:

- Disaster recovery
- Business continuity
- Battery backups/UPS
- First responders
- Data breach
- End user awareness and training
- Single point of failure
  - Critical nodes
  - Critical assets
  - Redundancy
- Adherence to standards and policies
- Vulnerability scanning
- Penetration testing

**Process/Skill Questions**

- What can be done to eliminate single point of failures on a network?
- What type of end user training should be offered to minimize/prevent network vulnerabilities?
- What is the difference between disaster recovery and business continuity?

**Task Number 95**

**Compare common network vulnerabilities and threats.**

**Definition**

Comparison should include the following:

- **Attacks/threats**
  - Denial of Service (DoS)
    - Distributed DoS
      - Botnet
      - Traffic spike
      - Coordinated attack
    - Reflective/amplified
      - DNS
      - Network Time Protocol (NTP)
      - Smurfing
    - Friendly/unintentional DoS
    - Physical attack
      - Permanent DoS
  - Address Resolution Protocol (ARP) cache poisoning
  - Packet/protocol abuse
  - Spoofing
  - Wireless
    - Evil twin
    - Rogue AP
    - War driving
    - War chalking
    - Bluejacking
    - Bluesnarfing
• WiFi Protected Access/Wired Equivalent Privacy/WiFi Protected Setup (WPA/WEP/WPS) attacks
  o Brute force
  o Session hijacking
  o Social engineering
  o Man-in-the-middle
  o VLAN hopping
  o Compromised system
  o Effect of malware on the network
  o Insider threat/malicious employee
  o Zero-day attacks
• Vulnerabilities
  o Unnecessary running services
  o Open ports
  o Unpatched/legacy systems
  o Unencrypted channels
  o Clear text credentials
  o Unsecure protocols
    ▪ Telnet
    ▪ HyperText Transfer Protocol (HTTP)
    ▪ Serial Line Internet Protocol (SLIP)
    ▪ FTP
    ▪ Trivial File Transfer Protocol (TFTP)
    ▪ SNMPv1 and SNMPv2
  o TEMPEST/Radio Frequency (RF) emanation

Process/Skill Questions

• What is a rogue AP?
• What can be done to minimize the effect of a Zero-day attack?
• What are some unsecure protocols?

Task Number 96

Demonstrate network hardening techniques.

Definition

Demonstration should include the following:

• Anti-malware software
  o Host-based
  o Cloud/server-based
• Network-based
  • Switch port security
    o DHCP snooping
    o ARP inspection
    o MAC address filtering
    o VLAN assignments
      ▪ Network segmentation
  • Security policies
  • Disable unneeded network services
  • Use secure protocols
    o Secure Shell (SSH)
    o SNMPv3
    o Transport Layer Security (TLS)/SSL
    o SFTP
    o HyperText Transfer Protocol Secure (HTTPS)
    o Internet Protocol Security (IPSec)
  • Access lists
    o Web/content filtering
    o Port filtering
    o IP filtering
    o Implicit deny
  • Wireless security
    o WEP
    o WPA/WPA2
      ▪ Enterprise
      ▪ Personal
    o Temporal Key Integrity Protocol (TKIP)/Advanced Encryption Standard (AES)
    o 802.1x
    o Transport Layer Security/Tunneled Transport Layer Security (TLS/TTLS)
    o MAC filtering
  • User authentication
    o Challenge Handshake Authentication Protocol (CHAP)/Microsoft CHAP (MSCHAP)
    o Password Authentication Protocol (PAP)
    o Extensible Authentication Protocol (EAP)
    o Kerberos
    o Multifactor authentication
    o Two-factor authentication
    o Single sign-on
  • Hashes
    o MD5
    o Secure Hash Algorithm (SHA)

Process/Skill Questions

• What are some examples of two-factor/multifactor authentication?
• What is the difference between encryption and authentication?
• What is the purpose of a network access list?

Task Number 97

Compare physical security controls.

Definition

Comparison should include the following:

• Mantraps
• Network closets
• Video monitoring
  o IP cameras/Closed Circuit TVs (CCTVs)
• Door access controls
• Proximity readers/key fob
• Biometrics
• Keypad/cipher locks
• Security guard

Process/Skill Questions

• What minimum physical security controls should be put in place on a network closet?
• What are some of the different types of biometric controls that can be used to physically control access to network resources?

Task Number 98

Install a basic firewall.

Definition

Installation should include configuration and the following:

• Types of firewalls
  o Host-based
  o Network-based
  o Software vs. hardware
  o Application aware/context aware
- SOHO firewall
- Stateful vs. stateless inspection
- Unified Threat Management (UTM)

- Settings/techniques
  - Access Control List (ACL)
  - Virtual wire vs. routed
  - DMZ
  - Implicit deny
  - Block/allow
  - Outbound traffic
  - Inbound traffic
  - Firewall placement
  - Internal/external

**Process/Skill Questions**

- What are firewalls used for on networks?
- What are the advantages/disadvantages of software versus hardware firewalls?
- What is the purpose of a DMZ?

**Task Number 99**

**Explain the purpose of various network access control models.**

**Definition**

Explanation should include the following:

- 802.1x
- Posture assessment
- Guest network
- Persistent vs. nonpersistent agents
- Quarantine network
- Edge vs. access control

**Process/Skill Questions**

- What is the difference between persistent versus nonpersistent agents?
- What is the purpose of a quarantine network?
Task Number 100

Describe basic forensic concepts.

Definition

Description should include the following:

- First responder
- Secure the area (escalate when necessary)
- Document the scene
- eDiscovery
- Evidence/data collection
- Chain of custody
- Data transport
- Forensics report
- Legal hold

Process/Skill Questions

- What are responsibilities of a first responder when a network crisis occurs?
- What are the procedures in establishing the chain of custody?

Troubleshooting Networks

Task Number 101

Implement network troubleshooting methodology.

Definition

Implementation should include the following:

- Identify the problem
  - Gather information
  - Duplicate the problem, if possible
  - Question users
  - Identify symptoms
  - Determine whether anything has changed
  - Approach multiple problems individually
- Establish a theory of probable cause
  - Question the obvious
  - Consider multiple approaches
- Top-to-bottom/ bottom-to-top OSI model
- Divide and conquer
- Test the theory to determine cause
  - Once theory is confirmed, determine next steps to resolve problem
  - If theory is not confirmed, reestablish new theory or escalate
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify full system functionality and, if applicable, implement preventative measures
- Document findings, actions and outcomes

**Process/Skill Questions**

- What are the steps in identifying the problem?
- Why do you need to establish a theory of probable cause?
- Why do you need to document the findings, actions and outcomes?

**Task Number 102**

**Analyze the output of troubleshooting tools.**

**Definition**

Analysis should include interpretation of the output and the following:

- Command line tools
  - ipconfig
  - netstat
  - ifconfig
  - ping/ping6/ping -6
  - tracert/tracert -6/ traceroute6/traceroute -6
  - nbtstat
  - nslookup
  - arp
  - mac address lookup table
  - pathping
- Line testers
- Certifiers
- Multimeter
- Cable tester
- Light meter
- Toner probe
- Speed test sites
- Looking glass sites
- WiFi analyzer
- Protocol analyzer
Process/Skill Questions

- What are five command-line tools and the purpose for each?
- What is the purpose of a toner probe and why is it used?

Task Number 103

Troubleshoot common wireless issues.

Definition

Troubleshooting should include an explanation of how to resolve the issue, and the following:

- Signal loss
- Interference
- Overlapping channels (mismatched channels)
- Signal-to-noise ratio
- Device saturation
- Bandwidth saturation
- Untested updates
- Wrong SSID
- Power levels
- Open networks
- Rogue access point
- Wrong antenna type
- Incompatibilities
- Wrong encryption
- Bounce
- MIMO
- Access Point (AP) placement
- AP configurations
  - LWAPP
  - Thin vs. thick
- Environmental factors
  - Concrete walls
  - Window film
  - Metal studs
- Wireless-standard-related issues
  - Throughput
  - Frequency
  - Distance
  - Channels

Process/Skill Questions
• What environmental issues are under your control?
• How would you alleviate bandwidth saturation?

Task Number 104

Troubleshoot common copper cable issues.

Definition

Troubleshooting should include an explanation of how to solve the problem, and the following:

• Shorts
• Opens
• Incorrect termination (mismatched standards)
  o Straight-through
  o Crossover
• Cross-talk
  o Near end
  o Far end
• Electromagnetic Interference (EMI)/Radio Frequency Interference (RFI)
• Distance limitations
• Attenuation/Decibel (Db) loss
• Bad connector
• Bad wiring
• Split pairs
• Tx/Rx reverse
• Cable placement
• Bad Small Form-factor Pluggable (SFP)/Gigabit Interface Converter (GBIC)
  o cable or transceiver

Process/Skill Questions

• What methods can be used to mitigate EMI/RFI?
• What is cross-talk? What are some methods to eliminate it?

Task Number 105

Troubleshoot common fiber cable issues.

Definition

Troubleshooting should include an explanation of how to resolve the problem, and the following:

• Attenuation/Db loss
• SFP/GBIC
  o cable mismatch
• Bad SFP/GBIC
  o cable or transceiver
• Wavelength mismatch
• Fiber type mismatch
• Dirty connectors
• Connector mismatch
• Bend radius limitations
• Distance limitations

Process/Skill Questions

• What problems can be caused by dirty connections?
• What are the distance limitations with a fiber cable?

Task Number 106

Troubleshoot common network issues.

Definition

Troubleshooting should include an explanation of how to resolve the issue, and the following:

• Incorrect IP configuration/default gateway
• Broadcast storms/switching loop
• Duplicate IP
• Speed and duplex mismatch
• End-to-end connectivity
• Incorrect VLAN assignment
• Hardware failure
• Misconfigured DHCP
• Misconfigured DNS
• Incorrect interface/interface misconfiguration
• Cable placement
• Interface errors
• Simultaneous wired/wireless connections
• Discovering neighboring devices/nodes
• Power failure/power anomalies
• Maximum Transmission Unit (MTU)/MTU black hole
• Missing IP routes
• NIC teaming misconfiguration
  o Active-active vs. active-passive
  o Multicast vs. broadcast
Process/Skill Questions

- How would you determine an incorrect IP configuration/default gateway and what are the steps to correct the issue?
- How do you resolve an incorrect VLAN assignment?

Task Number 107

Troubleshoot common security issues.

Definition

Troubleshooting should include an explanation of how to resolve the issue, and the following:

- Misconfigured firewall
- Misconfigured ACLs/applications
- Malware
- DoS
- Open/closed ports
- ICMP-related issues
  - Ping of death
  - Unreachable default gateway
- Unpatched firmware/OSs
- Malicious users
  - Trusted
  - Untrusted users
  - Packet sniffing
- Authentication issues
  - TACACS/RADIUS misconfigurations
  - Default passwords/settings
- Improper access/backdoor access
- ARP issues
- Banner grabbing/Organizationally Unique Identifier (OUI)/TCP ports
- Domain/local group configurations
- Jamming

Process/Skill Questions

- What are common methods used to control malware issues?
- What are three types of malicious users?
Task Number 108

Troubleshoot common WAN issues.

Definition

Troubleshooting should include an explanation of how to resolve the issue, and the following:

- Loss of Internet connectivity
- Interface errors
- Split horizon
- DNS issues
- Interference
- Router configurations
- Customer premise equipment
  - Smart jack/Network Interface Unit (NIU)
  - Demarc
  - Loopback
  - Channel Service Unit (CSU)/Data Service Unit (DSU)
  - Copper line drivers/repeaters
- Company security policy
  - Throttling
  - Blocking
  - Fair access policy/utilization limits
- Satellite issues (latency)

Process/Skill Questions

- What is your school's WAN security policy?
- What methods can be used to alleviate DNS issues?

Applying Industry Standards, Practices, and Network Theory

Task Number 109

Describe OSI layers.

Definition

Description should include the following OSI layers:
• Layer 1 – Physical
• Layer 2 – Data link
• Layer 3 – Network
• Layer 4 – Transport
• Layer 5 – Session
• Layer 6 – Presentation
• Layer 7 – Application

Process/Skill Questions

• What are the seven layers of the OSI model?
• What activities are controlled at the physical layer?

Task Number 110

Explain the basics of network theory and concepts.

Definition

Explanation should include the following:

• Encapsulation/de-encapsulation
• Modulation techniques
  o Multiplexing
  o De-multiplexing
  o Analog and digital techniques
  o Time Division Multiplexing (TDM)
• Numbering systems
  o Binary
  o Hexadecimal
  o Octal
• Broadband/baseband
• Bit rates vs. baud rates
• Sampling size
• Code Division Multiple Access (CDMA)
• Carrier Sense Multiple Access/Collision Detection (CSMA/CD) and Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
• Carrier detect/sense
• Wavelength
• TCP/IP suite
  o ICMP
  o UDP
  o TCP
Process/Skill Questions

- What is encapsulation and how does it relate to network traffic?
- What methods are used to prevent a collision on the network?

Task Number 111

Deploy the appropriate wireless standard.

Definition

Deployment should include the following:

- 802.11a
- 802.11b
- 802.11g
- 802.11n
- 802.11ac

Process/Skill Questions

- Compare two different wireless standards; how are they alike and different?
- Which standard you would use for a SOHO network located in a large city? Explain.

Task Number 112

Deploy wired connectivity standards.

Definition

Deployment should include the following:

- Ethernet standards
  - 10BaseT
  - 100BaseT
  - 1000BaseT
  - 1000BaseTX
  - 10GBaseT
• 100BaseFX
• 10Base2
• 10GBaseSR
• 10GBaseER
• 10GBaseSW
• Institute of Electrical and Electronics Engineers (IEEE) 1905.1-2013
• Ethernet over HDMI
• Ethernet over power line

• Wiring standards
  • Electronic Industries Alliance/Telecommunication Industries Association (EIA/TIA) 568A/568B
• Broadband standards
  • Data-Over-Cable Service Interface Specification (DOCSIS)

Process/Skill Questions

• What Ethernet standard would you use for a home network and why?
• What Ethernet standard would be appropriate for a large office (200 employees) located in one building and why?

Task Number 113

Implement network policies and procedures.

Definition

Implementation should include the following:

• Security policies
  • Consent to monitoring
• Network policies
• AUP
• Standard business documents
  • Service Level Agreement (SLA)
  • Memorandum of Understanding (MOU)
  • Master Service Agreement (MSA)
  • Statement of Work (SOW)

Process/Skill Questions

• What security policies are used at your school?
• What is an AUP?
Task Number 114

Summarize safety practices.

Definition

Summary should include the following:

- Electrical safety
  - Grounding
- ESD
  - Static
- Installation safety
  - Lifting equipment
  - Rack installation
  - Placement
  - Tool safety
- SDS (formerly known as MSDS)
- Emergency procedures
  - Building layout
  - Fire escape plan
  - Safety/emergency exits
  - Fail open/fail close
  - Emergency alert system
- Fire suppression systems
- HVAC

Process/Skill Questions

- What type of fire suppression is appropriate for a computer room?
- What are the emergency procedures for your building?

Task Number 115

Install equipment.

Definition

Installation of equipment should be in an appropriate location, include configuration, and should use best practices. Installation should include the following:
• Intermediate distribution frame
• Main distribution frame
• Cable management
  o Patch panels
• Power management
  o Power converters
  o Circuits
  o UPS
  o Inverters
  o Power redundancy
• Device placement
• Air flow
• Cable trays
• Rack systems
  o Server rail racks
  o Two-post racks
  o Four-post racks
  o Free-standing racks
• Labeling
  o Port labeling
  o System labeling
  o Circuit labeling
  o Naming conventions
  o Patch panel labeling
• Rack monitoring
• Rack security

Process/Skill Questions

• Why is labeling and documenting an important activity when installing equipment?
• Why is device placement important when planning an installation?

Task Number 116

Explain the basics of change management procedures.

Definition

Explanation should include the following:

• Document reason for a change
• Change request
  o Configuration procedures
- Rollback process
- Potential impact
- Notification

- Approval process
- Maintenance window
  - Authorized downtime
- Notification of change
- Documentation
  - Network configurations
  - Additions to network
  - Physical location changes

**Process/Skill Questions**

- Why are change requests an important step in management procedures?
- Why is network documentation a vital part of management procedures?

**Task Number 117**

**Compare ports and protocols.**

**Definition**

Comparison should include the following:

- 80 HTTP
- 443 HTTPS
- 137-139 NetBIOS
- 110 POP
- 143 IMAP
- 25 SMTP
- 5060/5061 Session Initiation Protocol (SIP)
- 2427/2727 Media Gateway Control Protocol (MGCP)
- 5004/5005 Real-Time Protocol (RTP)
- 1720 H.323
- TCP
  - Connection-oriented
- UDP
  - Connectionless

**Process/Skill Questions**

- What is the difference between TCP and UDP?
• What protocols are used for email?

Task Number 118

Configure ports and protocols.

Definition

Configuration should include the following:

• 20, 21 FTP
• 161 SNMP
• 22 SSH
• 23 Telnet
• 53 DNS
• 67, 68 DHCP
• 69 TFTP
• 445 SMB
• 3389 RDP

Process/Skill Questions

• What is the FTP protocol used for?
• When and why is the SSH protocol used?

SOL Correlation by Task

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>English:</th>
</tr>
</thead>
<tbody>
<tr>
<td>39</td>
<td>Describe security issues related to computer hardware, software, and data.</td>
<td>11.5, 12.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>History and Social Science: GOVT.16, VUS.14, WHII.14</td>
</tr>
<tr>
<td>40</td>
<td>Explain concepts related to copyright, public domain, copy protection, intellectual property, and licensing agreements.</td>
<td>11.5, 12.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>History and Social Science: GOVT.16, VUS.1, WG.1, WHI.1, WHII.1</td>
</tr>
<tr>
<td>41</td>
<td>Describe concepts of cybersecurity, honesty, courtesy, and confidentiality related to information and email systems and social networking (e.g., spam, viruses, and etiquette).</td>
<td>11.5, 12.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>History and Social Science: GOVT.16, VUS.14, WHII.14</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>42</td>
<td>Analyze Internet privacy issues and computer crimes, including identity theft.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>43</td>
<td>Comply with copyright and patent laws.</td>
<td>History and Social Science: GOVT.16, VUS.1, VUS.14, WG.1, WHL.1, WHII.1</td>
</tr>
<tr>
<td>44</td>
<td>Comply with policies regarding acceptable use of technology.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>45</td>
<td>Compare features and requirements of Microsoft operating systems.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Science: PH.1a</td>
</tr>
<tr>
<td>46</td>
<td>Install Windows PC operating systems.</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Apply Microsoft command line tools.</td>
<td>Mathematics: COM.10</td>
</tr>
<tr>
<td>48</td>
<td>Use Microsoft OS features and tools.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td>49</td>
<td>Use Windows Control Panel utilities.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td>50</td>
<td>Install Windows networking on a client/desktop.</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Perform common preventive maintenance procedures.</td>
<td>Mathematics: COM.16</td>
</tr>
<tr>
<td>52</td>
<td>Identify common features and functions of the macOS and Linux OS.</td>
<td>Mathematics: COM.7, COM.16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Science: PH.1a</td>
</tr>
<tr>
<td>53</td>
<td>Set up virtual machines on a host computer.</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Identify basic cloud concepts.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td>55</td>
<td>Describe services provided by networked hosts.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>56</td>
<td>Identify basic features of mobile operating systems.</td>
<td>Science: PH.1a</td>
</tr>
<tr>
<td>57</td>
<td>Set up mobile device network connectivity and email.</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>Synchronize mobile devices.</td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>Analyze appropriate safety procedures.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>History and Social Science: GOVT.16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Science: CH.1b, CH.1c</td>
</tr>
</tbody>
</table>
| 60 | Analyze controls and their impact on the environment. | English: 11.5, 12.5  
History and Social Science: GOVT.16  
Science: CH.1b, CH.1c |
| 61 | Summarize the process of addressing prohibited content/activity. | English: 11.5, 12.5  
History and Social Science: GOVT.16  
Mathematics: COM.16, COM.18 |
| 62 | Explain privacy, licensing, and policy concepts. | English: 11.5, 12.5  
History and Social Science: GOVT.16, VUS.14 |
| 63 | Demonstrate communication techniques and professionalism. | English: 11.1, 11.2, 12.1, 12.2  
History and Social Science: GOVT.16, VUS.14 |
| 64 | Explain the troubleshooting theory. | English: 11.5, 12.5  
Science: CH.1f |
| 65 | Identify common threats and vulnerabilities. | Mathematics: COM.2, COM.18 |
| 66 | Describe the methods used to make computers and networks more secure. | English: 11.5, 12.5  
History and Social Science: VUS.14 |
| 67 | Configure security settings. | English: 11.5, 12.5  
History and Social Science: VUS.14  
Mathematics: COM.1, COM.16 |
| 68 | Describe methods for securing mobile devices. | English: 11.5, 12.5  
History and Social Science: VUS.14 |
<p>| 69 | Use data destruction and disposal methods. |  |
| 70 | Secure SOHO wireless and wired networks. |  |</p>
<table>
<thead>
<tr>
<th></th>
<th>Troubleshoot PC OS problems.</th>
<th>Mathematics: COM.10, COM.11, COM.17, COM.18</th>
</tr>
</thead>
<tbody>
<tr>
<td>72</td>
<td>Troubleshoot common PC security issues.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td>73</td>
<td>Troubleshoot mobile OS and application issues.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td>74</td>
<td>Troubleshoot mobile OS and application security issues.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td>75</td>
<td>Explain the functions and applications of various network devices.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>76</td>
<td>Compare networking services and applications.</td>
<td></td>
</tr>
<tr>
<td>77</td>
<td>Install networking services/applications.</td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>Explain the characteristics and benefits of various wide area network (WAN) technologies.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>79</td>
<td>Install various cable types and connectors.</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>Differentiate between common network topologies.</td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>Differentiate between network infrastructure implementations.</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>Configure addressing schema.</td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>Explain basic routing concepts and protocols.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>84</td>
<td>Identify the basic elements of unified communication (UC) technologies.</td>
<td>Mathematics: COM.13</td>
</tr>
<tr>
<td>85</td>
<td>Compare technologies that support cloud virtualization.</td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>Given a set of requirements, implement a basic network.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>87</td>
<td>Demonstrate use of monitoring tools.</td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>Analyze metrics and reports from monitoring and tracking performance tools.</td>
<td>Science: PS.1, PS.2, PS.3, PS.4, PS.5</td>
</tr>
<tr>
<td>89</td>
<td>Demonstrate use of resources to support configuration management.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>90</td>
<td>Explain the importance of implementing network segmentation.</td>
<td>Mathematics: COM.16</td>
</tr>
<tr>
<td>91</td>
<td>Install patches and updates.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td>92</td>
<td>Configure a switch.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td>93</td>
<td>Install wireless LAN infrastructure.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td>94</td>
<td>Compare risk-related concepts.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>95</td>
<td>Compare common network vulnerabilities and threats.</td>
<td>History and Social Science: VUS.14</td>
</tr>
<tr>
<td>96</td>
<td>Demonstrate network hardening techniques.</td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>Compare physical security controls.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>98</td>
<td>Install a basic firewall.</td>
<td>Mathematics: COM.1</td>
</tr>
<tr>
<td>99</td>
<td>Explain the purpose of various network access control models.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>100</td>
<td>Describe basic forensic concepts.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>101</td>
<td>Implement network troubleshooting methodology.</td>
<td>Mathematics: A.8, AII.10</td>
</tr>
<tr>
<td>102</td>
<td>Analyze the output of troubleshooting tools.</td>
<td>Mathematics: A.8, AII.10, COM.15</td>
</tr>
<tr>
<td>103</td>
<td>Troubleshoot common wireless issues.</td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>Troubleshoot common copper cable issues.</td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>Troubleshoot common fiber cable issues.</td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>Troubleshoot common network issues.</td>
<td>Mathematics: COM.18</td>
</tr>
<tr>
<td>107</td>
<td>Troubleshoot common security issues.</td>
<td>Mathematics: COM.18</td>
</tr>
<tr>
<td>108</td>
<td>Troubleshoot common WAN issues.</td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>Describe OSI layers.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>110</td>
<td>Explain the basics of network theory and concepts.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>111</td>
<td>Deploy the appropriate wireless standard.</td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>Deploy wired connectivity standards.</td>
<td></td>
</tr>
<tr>
<td>113</td>
<td>Implement network policies and procedures.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>114</td>
<td>Summarize safety practices.</td>
<td>English: 11.5, 11.6, 12.5, 12.6</td>
</tr>
<tr>
<td>115</td>
<td>Install equipment.</td>
<td>History and Social Science: GOVT.16</td>
</tr>
<tr>
<td>116</td>
<td>Explain the basics of change management procedures.</td>
<td>English: 11.5, 12.5</td>
</tr>
<tr>
<td>117</td>
<td>Compare ports and protocols.</td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>Configure ports and protocols.</td>
<td>Mathematics: COM.1</td>
</tr>
</tbody>
</table>

**Teacher Resources**

**CompTIA**

The Virginia Cyber Range is a Commonwealth of Virginia initiative with a mission to enhance cybersecurity education for students in the Commonwealth’s public high schools, colleges, and universities. The Virginia Cyber Range seeks to increase the number of fully prepared students entering the cybersecurity workforce in operations, development, and research. The Virginia
Cyber Range provides an extensive Courseware Repository for educators and a cloud-hosted Exercise Area environment for hands-on cybersecurity labs and exercises for students.

**AFA CyberPatriot** the National Youth Cyber Education Program created by the Air Force Association to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future. At the core of the program is the National Youth Cyber Defense Competition, the nation's largest cyber defense competition that puts high school and middle school students in charge of securing virtual networks.
Appendix: Credentials, Course Sequences, and Career Cluster Information

Industry Credentials: Only apply to 36-week courses

- A+ Certification Examination
- Apple Certified Support Professional Examination
- Business Information Processing Assessment
- Cisco Certified CyberOps Associate Examination
- Cisco Certified DevNet Associate Examination
- Cisco Certified Networking Associate (CCNA) Examination
- Cisco Certified Networking Professional (CCNP) Automation for Cisco Enterprise Solutions Examination
- Cisco Certified Networking Professional (CCNP) Cisco Enterprise Networks Examination
- Cisco Certified Networking Professional (CCNP) Cisco SD-WAN Solutions Examination
- Cisco Certified Networking Professional (CCNP) Designing Enterprise Wireless Networks Examination
- Cisco Certified Networking Professional (CCNP) Enterprise Advanced Routing and Services Examination
- Cisco Certified Networking Professional (CCNP) Enterprise Network Core Technologies Examination
- Cisco Certified Networking Professional (CCNP) Implementing Enterprise Wireless Networks Examination
- College and Work Readiness Assessment (CWRA+)
- Computer Maintenance Technology Examination
- Computer Networking Fundamentals Assessment
- Computer Repair Technology Assessment
- Computer Service Technician (CST) Examination
- Computer Technology Assessment
- Customer Service Examination
- Customer Service Specialist (CSS) Examination
- IC3 Digital Literacy Certification Examination
- IT Fundamentals+ Certification Examination
- Microsoft 365 Fundamentals Examination
- Microsoft Certified Azure Fundamentals Examination
- Microsoft Dynamics 365 Fundamentals Examination
- Microsoft Office Specialist (MOS) Examinations
- National Career Readiness Certificate Assessment
- Network Administration Certification Tests
- Network+ Certification Examination
- Professional Communications Certification Examination
- Security+ Certification Examination
- Technical Support Certification Tests
- Workplace Readiness Skills for the Commonwealth Examination

Concentration sequences: A combination of this course and those below, equivalent to two 36-week courses, is a concentration sequence. Students wishing to complete a specialization may take additional courses based on their career pathways. A program completer is a student who has met the requirements for a CTE concentration sequence and all other requirements for high school graduation or an approved alternative education program.
- Cybersecurity Systems Technology (8628/36 weeks, 140 hours)

### Career Cluster: Information Technology

<table>
<thead>
<tr>
<th>Pathway</th>
<th>Occupations</th>
</tr>
</thead>
</table>
| Information Support and Services | Computer Support Specialist  
Computer Systems Engineer, Architect  
Information Systems Analyst  
Maintenance Technician  
Network Systems and Data Communication Analyst  
Systems Analyst |
| Network Systems                  | Computer Operator  
Computer Security Specialist  
Computer Support Specialist  
Computer Systems Engineer, Architect  
Information Security Analyst  
Network and Computer Systems Administrator  
Network Architect  
Network Systems and Data Communication Analyst  
Systems Analyst  
Telecommunications Equipment Installer, Repairer  
Telecommunications Specialist |
| Programming and Software Development | Computer Software Engineer  
Network Systems and Data Communication Analyst |
| Web and Digital Communications   | Computer Support Specialist  
Computer Systems Engineer, Architect  
Systems Analyst |