Computer Networking Hardware Operations IV

8545/18 weeks

Table of Contents

Acknowledgments 2
Course Description 3
Task Essentials Table 3
Curriculum Framework 6
Describing Single-Area Open Shortest Path First (OSPF)v2 Concepts 6
Configuring Single-Area OSPFv2 7
Analyzing Network Security Concepts 8
Describing Access Control List (ACL) Concepts 10
Exploring ACLs for IPv4 Configuration 11
Configuring Network Address Translation (NAT) for IPv4 12
Explaining Wide Area Network (WAN) Concepts 13
Describing Virtual Private Network (VPN) and IP Security (IPsec) Concepts 14
Analyzing Quality of Service (QoS) Concepts 15
Managing Networks 16
Designing Networks 18
Troubleshooting Networks 18
Exploring Network Virtualization 20
Describing Network Automation 21
SOL Correlation by Task 23
Teacher Resources 27
Appendix: Credentials, Course Sequences, and Career Cluster Information 29

Acknowledgments

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

- Peyton Chichester, Chesterfield Career and Technical Center at Courthouse, Chesterfield County Public Schools
- Kelly Caudle, Program Head: Cisco Academy Support Center (ASC), Instructor Training Center (ITC), VMware Academy, IT Academy Lead Instructor, ITC, Stanly Community College, Albemarle, NC
- Kristen Hudson, Technical Manager US/CAN, Cisco Networking Academy, Buford, GA
- Iris Kutch, Cisco Academy Training and Support Manager, Towson University, Towson, MD
- Brian Stokes, Academies of Loudoun, Loudoun County Public Schools
- Marie Zwickert, Business Development Manager, Cisco Systems, Inc., Monkton, Maryland

Correlations to the Virginia Standards of Learning were reviewed and updated by the following:

- Leslie R. Bowers, English Teacher (ret.), Newport News Public Schools
- Vickie L. Inge, Mathematics Committee Member, Virginia Mathematics and Science Coalition
- Anne F. Markwith, New Teacher Mentor (Science), Gloucester County Public Schools
- Michael L. Nagy, Social Studies Department Chair, Rustburg High School, Campbell County Public Schools

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

- Heather A. Widener, Writer/Editor
- Kevin P. Reilly, Administrative Coordinator

Virginia Department of Education Staff

Lauren-Anne Sledzinski, Specialist, Trade and Industrial Education and Related Clusters
Dr. J. Anthony Williams, Curriculum and Instruction Coordinator
Dr. David S. Eshelman, Director, Workforce Development and Initiatives
George R. Willcox, Director, Operations and Accountability
Office of Career, Technical, and Adult Education
Virginia Department of Education

Course Description

Suggested Grade Level: 11 or 12

The final of three Cisco Networking Academy CCNAv7 courses, this course describes the architecture, components, operations, and security to scale for large, complex networks, including wide area network (WAN) technologies. The course emphasizes network security concepts and introduces network virtualization and automation. Students learn how to configure, troubleshoot, and secure enterprise network devices and understand application programming interfaces (API) and configuration management. Upon completion of this course, students will be prepared to take the Cisco CCNA Unified certification exam.

Task Essentials Table

- 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.

Task No.	Task
Describing Single-Area Open Shortest Path First (OSPF)v2 Concepts	
39 ⊕	Describe the open shortest path first (OSPF) protocol.
40 ⊕	Describe OSPF packets.
41 ⊕	Explain OSPF operation.
Configuring Single-Area OSPFv2	
42 ⊕	Configure an OSPFv2 router ID.
43 ⊕	Configure single-area OSPFv2.
44 ⊕	Describe multiaccess OSPF networks.
45 ⊕	Modify single-area OSPFv2.
46 ⊕	Configure OSPF to propagate a default route.
47 ⊕	Verify single-area OSPFv2.
Analyzing Network Security Concepts	
48 ⊕	Describe cybersecurity.
49 ⊕	Describe threat actors.
50 ⊕	Describe threat actor tools.
51 ⊕	Describe malware.

Task No.	Task
52 ⊕	Describe network attacks.
53 ⊕	Identify Internet Protocol (IP) vulnerabilities and threats.
54 ⊕	Identify transmission control protocol (TCP) and user datagram protocol (UDP) vulnerabilities.
55 ⊕	Identify IP service exploitation.
56 ⊕	Identify network security best practices.
57 ⊕	Explain cryptography.
Describing Access Control List (ACL) Concepts	
58 ⊕	Describe the purpose of access control lists (ACLs).
59 ⊕	Describe wildcard masks.
60 ⊕	Explain ACL creation.
61 ⊕	Compare types of IPv4 ACLs.
Exploring ACLs for IPv4 Configuration	
62 ⊕	Configure standard IPv4 ACLs.
63 ⊕	Modify IPv4 ACLs.
64 ⊕	Secure virtual terminal line (VTY) ports with a standard IPv4 ACL.
65 ⊕	Configure extended IPv4 ACLs.
Configuring Network Address Translation (NAT) for IPv4	
66 ⊕	Describe network address translation (NAT).
67 ⊕	Compare types of NAT.
68 ⊕	Evaluate NAT.
69 ⊕	Configure static NAT.
70 ⊕	Configure dynamic NAT.
71 ⊕	Configure port address translation (PAT).
72 ⊕	Describe NAT64.
Explaining Wide Area Network (WAN) Concepts	
73 ⊕	Describe WANs.
74 ⊕	Explain WAN operations.
75 ⊕	Compare traditional connectivity.
76 ⊕	Compare modern connectivity.
77 ⊕	Compare Internet-based connectivity.
Describing Virtual Private Network (VPN) and IP Security (IPsec) Concepts	

Task No.	Task
78 ⊕	Describe virtual private network (VPN) technology.
79 ⊕	Describe VPNs.
80 ⊕	Describe IP security (IPsec).
Analyzing Quality of Service (QoS) Concepts	
81 ⊕	Explain network transmission quality.
82 ⊕	Describe traffic characteristics.
83 ⊕	Explain queuing algorithms.
84 ⊕	Identify quality of service (QoS) models.
85 ⊕	Define QoS implementation techniques.
Managing Networks	
86 ⊕	Describe device discovery with Cisco Discovery Protocol (CDP).
87 ⊕	Describe device discovery with link layer discovery protocol (LLDP).
88 ⊕	Implement network time protocol (NTP).
89 ⊕	Describe simple network management protocol (SNMP).
90 ⊕	Explain system logging protocol (syslog).
91 ⊕	Maintain router and switch configuration files.
92 ⊕	Manage an IOS image.
Designing Networks	
93 ⊕	Explain hierarchical networks.
94 ⊕	Explain scalable networks.
95 ⊕	Describe switch hardware.
96 ⊕	Describe router hardware.
Troubleshooting Networks	
97 ⊕	Explain network documentation.
98 ⊕	Compare troubleshooting processes.
99 ⊕	Identify troubleshooting tools.
100 ⊕	Determine symptoms and causes of network problems.
101 ⊕	Troubleshoot IP connectivity.
Exploring Network Virtualization	
102 ⊕	Describe cloud computing.
103 ⊕	Describe virtualization.
104 ⊕	Explain virtual network infrastructure.

Task No.	Task
105 ⊕	Describe software-defined networking.
106 ⊕	Describe controllers.
Describing Network Automation	
107 ⊕	Describe automation.
108 ⊕	Compare data formats.
109 ⊕	Explain the function of application programming interfaces (APIs).
110 ⊕	Explain the function of representational state transfer (REST).
111 ⊕	Compare configuration management tools.
112 ⊕	Explain the purpose of the intent-based networking (IBN) and Cisco Digital Network Architecture (DNA) center.

Legend: ⊕Essential ○Non-essential ⊖Omitted

Curriculum Framework

Describing Single-Area Open Shortest Path First (OSPF)v2 Concepts

Task 39

Describe the open shortest path first (OSPF) protocol.

Definition

Description should include basic OSPF features and characteristics.

Task 40

Describe OSPF packets.

Definition

Description should include the OSPF packet types, link state updates (LSUs), and link state advertisements (LSAs) used in single-area OSPF.

Task 41

Explain OSPF operation.

Definition

Explanation should include how single-area OSPF operates.

Configuring Single-Area OSPFv2

Task 42

Configure an OSPFv2 router ID.

Definition

Configuration should include an explanation of how the router will select its own OSPFv2 router ID if one is not configured.

Task 43

Configure single-area OSPFv2.

Definition

Configuration should include point-to-point OSPF networks.

Task 44

Describe multiaccess OSPF networks.

Definition

Description should include configuration of the OSPF interface priority to influence the designated router/backup designated router (DR/BDR) election in a multiaccess network.

Task 45

Modify single-area OSPFv2.

Definition

Modification should include changing the operation of single-area OSPFv2.

Task 46

Configure OSPF to propagate a default route.

Definition

Configuration should include a description of default route propagation.

Task 47

Verify single-area OSPFv2.

Definition

Verification should include a single-area OSPFv2 implementation.

Analyzing Network Security Concepts

Task 48

Describe cybersecurity.

Definition

Description should include the current state of cybersecurity and vectors of data loss.

Task 49

Describe threat actors.

Definition

Description should include threat actors who exploit networks.

Task 50

Describe threat actor tools.

Definition

Description should include tools used by threat actors to exploit networks.

Task 51

Describe malware.

Definition

Description should include types of malware.

Task 52

Describe network attacks.

Definition

Description should include examples of common network attacks.

Task 53

Identify Internet Protocol (IP) vulnerabilities and threats.

Definition

Identification should include a description of how IP vulnerabilities are exploited by threat actors.

Task 54

Identify transmission control protocol (TCP) and user datagram protocol (UDP) vulnerabilities.

Definition

Identification should include a description of how TCP and UDP vulnerabilities are exploited by threat actors.

Task 55

Identify IP service exploitation.

Definition

Identification should include how IP services are exploited by threat actors.

Task 56

Identify network security best practices.

Definition

Identification should include a description of best practices for protecting a network.

Task 57

Explain cryptography.

Definition

Explanation should include common cryptographic processes used to protect data in transit.

Describing Access Control List (ACL) Concepts

Task 58

Describe the purpose of access control lists (ACLs).

Definition

Description should include how ACLs filter traffic.

Task 59

Describe wildcard masks.

Definition

Description should include how ACLs use wildcard masks.

Task 60

Explain ACL creation.

Definition

Explanation should include guidelines for ACL creation.

Task 61

Compare types of IPv4 ACLs.

Definition

Comparison should include standard and extended IPv4 ACLs.

Exploring ACLs for IPv4 Configuration

Task 62

Configure standard IPv4 ACLs.

Definition

Configuration should include standard IPv4 ACLs to filter traffic to meet networking requirements.

Task 63

Modify IPv4 ACLs.

Definition

Modification should use sequence numbers to edit existing standard IPv4 ACLs.

Task 64

Secure virtual terminal line (VTY) ports with a standard IPv4 ACL.

Definition

Securing should include configuring a standard ACL to secure VTY access.

Task 65

Configure extended IPv4 ACLs.

Definition

Configuration should include extended IPv4 ACLs to filter traffic according to network requirements.

Configuring Network Address Translation (NAT) for IPv4

Task 66

Describe network address translation (NAT).

Definition

Description should include the characteristics, purpose, and function of NAT.

Task 67

Compare types of NAT.

Definition

Comparison should include the operation of various types of NAT.

Task 68

Evaluate NAT.

Definition

Evaluation should include the advantages and disadvantages of NAT.

Task 69

Configure static NAT.

Definition

Configuration should include static NAT using the command line interface (CLI).

Task 70

Configure dynamic NAT.

Definition

Configuration should include dynamic NAT using the CLI.

Task 71

Configure port address translation (PAT).

Definition

Configure PAT using the CLI.

Task 72

Describe NAT64.

Definition

Description should include NAT for IPv6.

Explaining Wide Area Network (WAN) Concepts

Task 73

Describe WANs.

Definition

Description should include the purpose of WANs.

Task 74

Explain WAN operations.

Definition

Explanation should include how WANs operate.

Task 75

Compare traditional connectivity.

Definition

Comparison should include traditional WAN connectivity options.

Task 76

Compare modern connectivity.

Definition

Comparison should include modern WAN connectivity options.

Task 77

Compare Internet-based connectivity.

Definition

Comparison should include Internet-based WAN connectivity options.

Describing Virtual Private Network (VPN) and IP Security (IPsec) Concepts

Task 78

Describe virtual private network (VPN) technology.

Definition

Description should include the benefits of VPN technology.

Task 79

Describe VPNs.

Definition

Description should include different types of VPNs.

Task 80

Describe IP security (IPsec).

Definition

Description should include how the IPsec framework is used to secure network traffic.

Analyzing Quality of Service (QoS) Concepts

Task 81

Explain network transmission quality.

Definition

Explanation should include an analysis of how network transmission characteristics affect quality.

Task 82

Describe traffic characteristics.

Definition

Description should include minimum network requirements for voice, video, and data traffic.

Task 83

Explain queuing algorithms.

Definition

Explanation should include the queuing algorithms used by networking devices.

Task 84

Identify quality of service (QoS) models.

Definition

Identification should include a description of various QoS models.

Task 85

Define QoS implementation techniques.

Definition

Definition should include how QoS uses mechanisms to ensure transmission quality.

Managing Networks

Task 86

Describe device discovery with Cisco Discovery Protocol (CDP).

Definition

Description should include using CDP to map a network topology.

Task 87

Describe device discovery with link layer discovery protocol (LLDP).

Definition

Description should include using LLDP to map a network topology.

Task 88

Implement network time protocol (NTP).

Definition

Implementation should include NTP between an NTP client and NTP server.

Task 89

Describe simple network management protocol (SNMP).

Definition

Description should include operation and traps, daemons, and the need for securing SNMP communications.

Task 90

Explain system logging protocol (syslog).

Definition

Explanation should include operation and the various levels of syslog messages and how to configure logging within the Cisco Internetwork Operating System (IOS).

Task 91

Maintain router and switch configuration files.

Definition

Maintenance should include using commands to back up and restore a Cisco IOS configuration file.

Task 92

Manage an IOS image.

Definition

Management should include performing an upgrade of an IOS system image.

Designing Networks

Task 93

Explain hierarchical networks.

Definition

Explanation should include how data, voice, and video converge in a switched network.

Task 94

Explain scalable networks.

Definition

Explanation should include considerations for designing a scalable network.

Task 95

Describe switch hardware.

Definition

Description should include how switch hardware features support network requirements.

Task 96

Describe router hardware.

Definition

Description should include the types of routers available for small-to-medium-sized business networks.

Troubleshooting Networks

Task 97

Explain network documentation.

Definition

Explanation should include how network documentation is developed and used to troubleshoot network issues.

Task 98

Compare troubleshooting processes.

Definition

Comparison should include troubleshooting methods that use a systematic, layered approach.

Task 99

Identify troubleshooting tools.

Definition

Identification should include networking troubleshooting tools.

Task 100

Determine symptoms and causes of network problems.

Definition

Determination should include identifying symptoms and causes of network problems using the layered model.

Task 101

Troubleshoot IP connectivity.

Definition

Troubleshooting should include using the layered model.

Exploring Network Virtualization

Task 102

Describe cloud computing.

Definition

Description should include the importance of cloud computing.

Task 103

Describe virtualization.

Definition

Description should include the importance of virtualization.

Task 104

Explain virtual network infrastructure.

Definition

Explanation should include the virtualization of network devices and services.

Task 105

Describe software-defined networking.

Definition

Description should include the characteristics of software-defined networking.

Task 106

Describe controllers.

Definition

Description should include controllers used in network programming.

Describing Network Automation

Task 107

Describe automation.

Definition

Description should include how automation is enabled and why it is important.

Task 108

Compare data formats.

Definition

Comparison should include

- JavaScript object notation (JSON)
- yet another markup language (YAML)
- extensible markup language (XML).

Task 109

Explain the function of application programming interfaces (APIs).

Definition

Explanation should include how APIs enable computer-to-computer communication.

Task 110

Explain the function of representational state transfer (REST).

Definition

Explanation should include how REST enables computer-to-computer communication.

Task 111

Compare configuration management tools.

Definition

Comparison should include

- Puppet
- Chef
- Ansible
- SaltStack.

Task 112

Explain the purpose of the intent-based networking (IBN) and Cisco Digital Network Architecture (DNA) center.

Definition

Explanation should include how the Cisco DNA center enables IBN.

SOL Correlation by Task

Task No.	Task	SOL Correlations
Describing Single-Area Open Shortest Path First (OSPF)v2 Concepts		
39	Describe the open shortest path first (OSPF) protocol.	English: 11.5, 12.5
40	Describe OSPF packets.	English: 11.5, 12.5
41	Explain OSPF operation.	English: 11.5, 12.5
Configuring Single-Area OSPFv2		
42	Configure an OSPFv2 router ID.	
43	Configure single-area OSPFv2.	
44	Describe multiaccess OSPF networks.	English: 11.5, 12.5
45	Modify single-area OSPFv2.	
46	Configure OSPF to propagate a default route.	
47	Verify single-area OSPFv2.	
Analyzing Network Security Concepts		
48	Describe cybersecurity.	English: 11.5, 12.5 History and Social Sciences: WG 17; WHII 14; VUS 14; Govt 9, 12, 16
49	Describe threat actors.	English: 11.5, 12.5 History and Social Sciences: WG 17; WHII 14; VUS 14; Govt 9, 12, 16
50	Describe threat actor tools.	English: 11.5, 12.5 History and Social Sciences: WG 17; WHII 14; VUS 14; Govt 9, 12, 16
51	Describe malware.	English: 11.5, 12.5 History and Social Sciences: WG 17; WHII 14; VUS 14; Govt 9, 12, 16
52	Describe network attacks.	English: 11.5, 12.5

Task No.	Task	SOL Correlations
		History and Social Sciences: WG 17; WHII 14; VUS 14; Govt 9, 12, 16
53	Identify Internet Protocol (IP) vulnerabilities and threats.	English: 11.5, 12.5 History and Social Sciences: WG 17; WHII 14; VUS 14; Govt 9, 12, 16
54	Identify transmission control protocol (TCP) and user datagram protocol (UDP) vulnerabilities.	English: 11.5, 12.5 History and Social Sciences: WG 17; WHII 14; VUS 14; Govt 9, 12, 16
55	Identify IP service exploitation.	English: 11.5, 12.5 History and Social Sciences: WG 17; WHII 14; VUS 14; Govt 9, 12, 16
56	Identify network security best practices.	English: 11.5, 12.5 History and Social Sciences: WG 17; WHII 14; VUS 14; Govt 9, 12, 16
57	Explain cryptography.	English: 11.5, 12.5 History and Social Sciences: WG 17; WHII 14; VUS 14; Govt 9, 12, 16
Describing Access Control List (ACL) Concepts		
58	Describe the purpose of access control lists (ACLs).	English: 11.5, 12.5
59	Describe wildcard masks.	English: 11.5, 12.5
60	Explain ACL creation.	English: 11.5, 12.5
61	Compare types of IPv4 ACLs.	English: 11.5, 12.5
Exploring ACLs for IPv4 Configuration		
62	Configure standard IPv4 ACLs.	
63	Modify IPv4 ACLs.	English: 11.5, 12.5
64	Secure virtual terminal line (VTY) ports with a standard IPv4 ACL.	

Task No.	Task	SOL Correlations
65	Configure extended IPv4 ACLs.	
Configuring Network Address Translation (NAT) for IPv4		
66	Describe network address translation (NAT).	English: 11.5, 12.5
67	Compare types of NAT.	English: 11.5, 12.5
68	Evaluate NAT.	English: 11.5, 12.5
69	Configure static NAT.	
70	Configure dynamic NAT.	
71	Configure port address translation (PAT).	
72	Describe NAT64.	English: 11.5, 12.5
Explaining Wide Area Network (WAN) Concepts		
73	Describe WANs.	English: 11.5, 12.5
74	Explain WAN operations.	English: 11.5, 12.5
75	Compare traditional connectivity.	English: 11.5, 12.5
76	Compare modern connectivity.	English: 11.5, 12.5
77	Compare Internet-based connectivity.	English: 11.5, 12.5
Describing Virtual Private Network (VPN) and IP Security (IPsec) Concepts		
78	Describe virtual private network (VPN) technology.	English: 11.5, 12.5
79	Describe VPNs.	English: 11.5, 12.5
80	Describe IP security (IPsec).	English: 11.5, 12.5
Analyzing Quality of Service (QoS) Concepts		
81	Explain network transmission quality.	English: 11.5, 12.5
82	Describe traffic characteristics.	English: 11.5, 12.5
83	Explain queuing algorithms.	English: 11.5, 12.5
84	Identify quality of service (QoS) models.	English: 11.5, 12.5
85	Define QoS implementation techniques.	English: 11.3, 11.5, 12.3, 12.5
Managing Networks		
86	Describe device discovery with Cisco Discovery Protocol (CDP).	English: 11.5, 12.5
87	Describe device discovery with link layer discovery protocol (LLDP).	English: 11.5, 12.5
88	Implement network time protocol (NTP).	
89	Describe simple network management protocol (SNMP).	English: 11.5, 12.5

Task No.	Task	SOL Correlations
90	Explain system logging protocol (syslog).	English: 11.5, 12.5
91	Maintain router and switch configuration files.	
92	Manage an IOS image.	
Designing Networks		
93	Explain hierarchical networks.	English: 11.5, 12.5
94	Explain scalable networks.	English: 11.5, 12.5
95	Describe switch hardware.	English: 11.5, 12.5
96	Describe router hardware.	English: 11.5, 12.5
Troubleshooting Networks		
97	Explain network documentation.	English: 11.5, 12.5
98	Compare troubleshooting processes.	English: 11.5, 12.5
99	Identify troubleshooting tools.	English: 11.5, 12.5
100	Determine symptoms and causes of network problems.	English: 11.5, 12.5
101	Troubleshoot IP connectivity.	English: 11.5, 12.5
Exploring Network Virtualization		
102	Describe cloud computing.	English: 11.5, 12.5
103	Describe virtualization.	English: 11.5, 12.5
104	Explain virtual network infrastructure.	English: 11.5, 12.5
105	Describe software-defined networking.	English: 11.5, 12.5
106	Describe controllers.	English: 11.5, 12.5
Describing Network Automation		
107	Describe automation.	English: 11.5, 12.5
108	Compare data formats.	English: 11.5, 12.5
109	Explain the function of application programming interfaces (APIs).	English: 11.5, 12.5
110	Explain the function of representational state transfer (REST).	English: 11.5, 12.5
111	Compare configuration management tools.	English: 11.5, 12.5
112	Explain the purpose of the intent-based networking (IBN) and Cisco Digital Network Architecture (DNA) center.	English: 11.5, 12.5

Teacher Resources

Acronym Glossary

AAA	authentication, authorization, and accounting
ACL	access control list
API	application programming interfaces
ARP	Address Resolution Protocol
BIOS	basic input/output system
BPDU	bridge protocol data unit
BYOD	bring your own device
CAPWAP	control and provisioning of wireless access points
CDP	Cisco Discovery Protocol
CLI	command-line interface
DHCP	dynamic host configuration protocol
DNA	(Cisco) Digital Network Architecture
DNS	Domain Name Service
DR/BDR	designated router/backup designated router
DTP	Dynamic Trunking Protocol
FHRP	first hop redundancy protocol
FTP	file transfer protocol
GUA	global unicast address
HSRP	Hot Standby Router Protocol
IBN	intent-based networking
ICMP	Internet Control Messaging Protocol
ICT	information and communications technology
IOS	(Cisco) Internetwork Operating System
IoT	Internet of Things
IP	Internet Protocol

IPsec	IP security
IT	information technology
JSON	JavaScript object notation
LAN	local area network
LLA	link-local address
LLDP	link layer discovery protocol
LSA	link state advertisement
LSU	link state update
MAC	media access control
NAT	network address translation
NTP	network time protocol
OSI	Open Systems Interconnection
OSPF	open shortest path first
PAT	port address translation
PC	personal computer
PDU	protocol data unit
PSK	pre-shared key
QoS	quality of service
REST	representational state transfer
SLAAC	stateless address autoconfiguration
SMB	service message block
SNMP	simple network management protocol
STP	spanning tree protocol
STP	Shielded Twisted Pair
syslog	System Logging Protocol
TCP	transmission control protocol
UDP	user datagram protocol
UEFI	Unified Extensible Firmware Interface

UTP	unshielded twisted pair
VLAN	virtual local area network
VLSM	variable-length subnet masking
VPN	virtual private network
VTY	virtual terminal line
WAN	wide area network
WLAN	wireless local area network
WLC	wireless LAN controller
WPA	Wi-Fi protected access
XML	extensible markup language
YAML	yet another markup language

Appendix: Credentials, Course Sequences, and Career Cluster Information

Industry Credentials: Only apply to 36-week courses

- A+ Certification 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 Networking Fundamentals Assessment
- Customer Service Specialist (CSS) Examination
- Internetworking Examination

- IT Fundamentals+ Certification Examination
- Microsoft 365 Fundamentals Examination
- Microsoft Certified Azure Fundamentals Examination
- Microsoft Dynamics 365 Fundamentals Examination
- Microsoft Office Specialist (MOS) Examinations
- Microsoft Technology Associate (MTA) Examinations
- 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.

- Computer Networking Hardware Operations I (8542/18 weeks, 70 hours)
- Computer Networking Hardware Operations II (8543/18 weeks, 70 hours)
- Computer Networking Hardware Operations III (8544/18 weeks, 70 hours)

Career Clusters, Pathways, and Occupations

Career Cluster: Information Technology	
Pathway	Occupations
Information Support and Services	Applications Integrator Computer Support Specialist Computer Systems Engineer, Architect Database Administrator Database Analyst Information Systems Analyst Information Systems Security Developer Information Systems Security Manager Maintenance Technician Network Systems and Data Communication Analyst Software Test Engineer Systems Analyst Technical Writer

Network Systems	Computer and Information Systems Administrator Computer Operator Computer Security Specialist Computer Software Engineer Computer Support Specialist Computer Systems Engineer, Architect Database Analyst Information Security Analyst Network and Computer Systems Administrator Network Architect Network Systems and Data Communication Analyst Software Test Engineer Systems Analyst Telecommunications Equipment Installer, Repairer Telecommunications Specialist
Programming and Software Development	Computer Software Engineer Information Security Analyst Network Systems and Data Communication Analyst Programmer Project Manager Software Applications Engineer Software Test Engineer Systems Analyst
Web and Digital Communications	Computer Support Specialist Computer Systems Engineer, Architect Project Manager Software Test Engineer Systems Analyst