TestOut®

TestOut Routing and Switching Pro - English 7.0.x

MAPPING:

TestOut Routing and Switching Pro mapped to Cisco Network Academy CCNAv7

Modified 2020-05-13

Powered by LABSIM

TestOut Routing and Switching Pro mapped to the Cisco Network Academy CCNAv7 Course Content

Testout Section	Cisco Network Academy Content	Testout Title	Cisco CCNA Objectives
1		Introduction to Routing and Switching Pro	
1.1		Introduction	
2		Networking Concepts	
2.1	CCNA1 3.3 - Protocol Suites 16.4 - Device Security	TCP/IP Networking Model	1.5 Compare TCP to UDP
			4.8 Configure network devices for remote access using SSH
			4.9 Describe the capabilities and function of TFTP/FTP in the network
2.2	CCNA1 3.5 - Reference Models 16.4 - Device Security	OSI Networking Model	4.8 Configure network devices for remote access using SSH
2.3	CCNA1 4.3 - Copper Cabling 4.4 - UTP Cabling 4.5 - Fiber-Optic Cabling	Networking Basics	1.3 Compare physical interface and cabling types
			1.3.a Single-mode fiber, multimode fiber, copper
2.4		Data Encapsulation and Communications	
2.5	CCNA1 4.3 - Copper Cabling 4.4 - UTP Cabling 4.5 - Fiber-Optic Cabling CCNA3 11.3 - Switch Hardware 12.5 - Troubleshooting IP Connectivity	Ethernet	1.3 Compare physical interface and cabling types
			1.3.a Single-mode fiber, multimode fiber, copper
			1.3.b Connections (Ethernet shared media and point-to-point)
			1.3.c Concepts of PoE
			1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)

2.6	CCNA1 1.2 - Network Components 15.2 - Peer-to-Peer 7.2 - Ethernet MAC Address 7.3 - The MAC Address Table CCNA2 1.3 - Secure Remote Access 3.4 - VLAN Trunks 3.5 - Dynamic Trunking Protocol 12.2 - WLAN Components 12.3 - WLAN Operation	Network Devices	1.1 Explain the role and function of network components
			1.1.a Routers
			1.1.b L2 and L3 switches
			1.1.c Next-generation firewalls and IPS
			1.1.d Access points
			1.1.e Controllers (Cisco DNA Center and WLC)
			1.1.g Servers
			1.13 Describe switching concepts
			1.13.a MAC learning and aging
			2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
			2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
			2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings
3		**Cisco Devices**	
3.1	2.1.4 - Access Methods	Cisco Device Connection	4.8 Configure network devices for remote access using SSH
3.2	CCNA1 2.1 - Cisco IOS Access 2.3 - The Command Structure	Command Line Interface (CLI)	
3.3		IOS Licensing	
3.4	CCNA1 2.4 - Basic Device Configuration	Device Settings	

3.5	2.4 - Basic Device Configuration	Device Passwords	5.3 Configure device access control using local passwords
3.6	CCNA3 10.1 - Device Discovery with CDP	Cisco Discovery Protocol (CDP)	2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
4		**IP Addressing**	
4.1	CCNA1 2.6 - Ports and Addresses 2.7 - Configure IP Addressing	IPv4 Addressing Overview	1.6 Configure and verify IPv4 addressing and subnetting
			1.7 Describe the need for private IPv4 addressing
4.2	CCNA1 11.5 - Subnet an IPv4 Network 11.6 - Subnet a Slash 16 and a Slash 8 Prefix 11.7 - Subnet to Meet Requirements	Subnets	1.6 Configure and verify IPv4 addressing and subnetting
			1.7 Describe the need for private IPv4 addressing
4.3	CCNA1 11.5 - Subnet an IPv4 Network 11.6 - Subnet a Slash 16 and a Slash 8 Prefix 11.7 - Subnet to Meet Requirements	Subnet Planning and Design	1.6 Configure and verify IPv4 addressing and subnetting
			1.7 Describe the need for private IPv4 addressing
4.4	CCNA1 11.5 - Subnet an IPv4 Network 11.6 - Subnet a Slash 16 and a Slash 8 Prefix 11.7 - Subnet to Meet Requirements	Route Summarization	1.6 Configure and verify IPv4 addressing and subnetting
4.5	CCNA1 8.3 - IPv6 Packet 12.1 - IPv4 Issues	IPv6 Addressing Overview	1.1 Explain the role and function of network components
			1.1.f Endpoints

	12.2 - IPv6 Address Representation 12.3 - IPv6 Address Types 12.4 - GUA and LLA Static Configuration 12.5 - Dynamic Addressing for IPv6 GUAs 12.6 - Dynamic Addressing for IPv6 LLAs 12.7 - IPv6 Multicast Addresses 12.8 - Subnet an IPv6 Network		1.8 Configure and verify IPv6 addressing and prefix
			1.9 Compare IPv6 address types
			1.9.a Global unicast
			1.9.b Unique local
			1.9.c Link local
			1.9.d Anycast
			1.9.e Multicast
			1.9.f Modified EUI 64
4.6	CCNA1 15.4 - IP Addressing Services CCNA2 7.1 - DHCPv4 Concepts 7.2 - Configure a Cisco IOS DHCPv4 Server 7.3 - Configure a DHCPv4 Client 8.1 - IPv6 GUA Assignment 8.2 – SLAAC 8.3 - DHCPv6 8.4 - Configure DHCPv6 Server	Dynamic Host Configuration Protocol (DHCP)	4.3 Explain the role of DHCP and DNS within the network
			4.6 Configure and verify DHCP client and relay
4.7	CCNA1 15.4 - IP Addressing Services 17.7 - Troubleshooting Scenarios	The Domain Name System (DNS)	4.3 Explain the role of DHCP and DNS within the network

	CCNA3 3.8 - IP Services 12.5 - Troubleshooting IP Connectivity		
5		**Switching**	
5.1	CCNA1 16.3 - Network Attack Mitigations CCNA2 1.1 - Configure a Switch with Initial Settings 10.4 - MAC Address Table Attack 10.1 - Endpoint Security CCNA3 13.5 - Controllers	Layer 2 Switching Overview	1.1 Explain the role and function of network components
			1.1.f Endpoints
			1.2 Describe characteristics of network topology architectures
			1.2.a 2 tier
			1.2.b 3 tier
			1.2.c Spine-leaf
			1.3 Compare physical interface and cabling types
			1.3.c Concepts of PoE
			1.13 Describe switching concepts
			1.13.a MAC learning and aging
			1.13.b Frame switching
			1.13.c Frame flooding
			1.13.d MAC address table
5.2	CCNA1 2.4 - Basic Device Configuration 2.5 - Save Configurations	Switch Interface Configuration	
6		**IPv4 Routing**	
6.1	CCNA1 8.5 - Introduction to Routing 11.3 - Types of IPv4 Addresses	IPv4 Routing	3.1 Interpret the components of routing table
			3.1.a Routing protocol code
			3.1.b Prefix
			3.1.c Network mask

	4.1 - Inter-VLAN Routing Operation 4.2 - Router-on-a-Stick Inter-VLAN Routing 4.3 - Inter-VLAN Routing using Layer 3 Switches 4.4 - Troubleshoot Inter-VLAN Routing CCNA2 14.1 - Path Determination 14.2 - Packet Forwarding 14.3 - Basic Router Configuration Review 14.5 - Static and Dynamic Routing		3.1.d Next hop
			3.1.e Administrative distance
			3.1.f Metric
			3.1.g Gateway of last resort
			3.2 Determine how a router makes a forwarding decision by default
			3.2.a Longest match
			3.2.b Administrative distance
			3.2.c Routing protocol metric
			3.3 Configure and verify IPv4 and IPv6 static routing
			3.3.a Default route
			3.3.b Network route
			3.3.c Host route
			3.3.d Floating static
6.2	CCNA2 15.1 - Static Routes 15.2 - Configure IP Static Routes 15.3 - Configure IP Default Static Routes 15.4 - Configure Floating Static Routes 15.5 - Configure Static Host Routes	Static Routing	1.3 Compare physical interface and cabling types
			1.3.b Connections (Ethernet shared media and point-to-point)
			1.6 Configure and verify IPv4 addressing and subnetting
			3.3 Configure and verify IPv4 and IPv6 static routing
			3.3.a Default route
			3.3.b Network route
			3.3.c Host route
			3.3.d Floating static
6.3	CCNA2	Dynamic Routing	

	14.4 - IP Routing Table 14.5 - Static and Dynamic Routing		
6.4	CCNA2 16.1 - Packet Processing with Static Routes 16.2 - Troubleshoot IPv4 Static and Default Route Configuration	IPv4 Routing Troubleshooting	1.6 Configure and verify IPv4 addressing and subnetting
			1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)
			3.3 Configure and verify IPv4 and IPv6 static routing
			3.3.a Default route
			3.3.b Network route
			3.3.c Host route
			3.3.d Floating static
6.5		Network Communications Troubleshooting	1.6 Configure and verify IPv4 addressing and subnetting
7		**IPv4 Routing Protocols**	
7.1	CCNA3 1.1 - OSPF Features and Characteristics 1.2 - OSPF Packets 1.3 - OSPF Operation	Open Shortest Path First (OSPF) Overview	3.4 Configure and verify single area OSPFv2
			3.4.a Neighbor adjacencies
			3.4.b Point-to-point
			3.4.c Broadcast (DR/BDR selection)
			3.4.d Router ID
7.2	CCNA3 1.1 - OSPF Features and Characteristics 1.2 - OSPF Packets 1.3 - OSPF Operation	OSPF for IPv4	3.4 Configure and verify single area OSPFv2
			3.4.a Neighbor adjacencies
			3.4.b Point-to-point
			3.4.c Broadcast (DR/BDR selection)
			3.4.d Router ID
7.3	CCNA3 1.1 - OSPF Features and Characteristics	OSPF Configuration	3.4 Configure and verify single area OSPFv2
			3.4.a Neighbor adjacencies

	1.2 - OSPF Packets 1.3 - OSPF Operation 2.1 - OSPF Router ID 2.2 - Point-to-Point OSPF Networks 2.3 - Multiaccess OSPF Networks 2.4 - Modify Single-Area OSPFv2 2.5 - Default Route Propagation 2.6 - Verify Single-Area OSPFv2		3.4.b Point-to-point
			3.4.c Broadcast (DR/BDR selection)
			3.4.d Router ID
7.4	CCNA3 1.1 - OSPF Features and Characteristics 1.2 - OSPF Packets 1.3 - OSPF Operation 2.1 - OSPF Router ID 2.2 - Point-to-Point OSPF Networks 2.3 - Multiaccess OSPF Networks 2.4 - Modify Single-Area OSPFv2 2.5 - Default Route Propagation 2.6 - Verify Single-Area OSPFv2	OSPF LSA Types and Databases	3.4 Configure and verify single area OSPFv2
			3.4.a Neighbor adjacencies
			3.4.b Point-to-point
			3.4.c Broadcast (DR/BDR selection)
			3.4.d Router ID

7.5	CCNA3 1.1 - OSPF Features and Characteristics 1.2 - OSPF Packets 1.3 - OSPF Operation 2.1 - OSPF Router ID 2.2 - Point-to-Point OSPF Networks 2.3 - Multiaccess OSPF Networks 2.4 - Modify Single-Area OSPFv2 2.5 - Default Route Propagation 2.6 - Verify Single-Area OSPFv2	Adjacency Troubleshooting	3.4 Configure and verify single area OSPFv2
			3.4.a Neighbor adjacencies
			3.4.b Point-to-point
			3.4.c Broadcast (DR/BDR selection)
			3.4.d Router ID
7.6		EIGRP for IPv4 Routing	
7.7		EIGRP for IPv4 Configuration	
8		**IPv6 Routing**	
8.1	CCNA3 1.1 - OSPF Features and Characteristics	IPv6 Routing Overview	1.8 Configure and verify IPv6 addressing and prefix
			1.9 Compare IPv6 address types
			1.9.a Global unicast
			1.9.b Unique local
			1.9.c Link local
			1.9.d Anycast
			1.9.e Multicast
			1.9.f Modified EUI 64
8.2	CCNA3	OSPFv3	1.8 Configure and verify IPv6 addressing and prefix

	1.1 - OSPF Features and Characteristics		
			1.9 Compare IPv6 address types
			1.9.a Global unicast
			1.9.b Unique local
			1.9.c Link local
			1.9.d Anycast
			1.9.e Multicast
			1.9.f Modified EUI 64
8.3		EIGRPv6	
9		**Wireless Networks**	
9.1	CCNA1 4.6 - Wireless Media CCNA2 12.1 - Introduction to Wireless 12.2 - WLAN Components 12.3 - WLAN Operation 12.4 - CAPWAP Operation 12.5 - Channel Management 12.6 - WLAN Threats 12.7 - Secure WLANs 13.1 - Remote Site WLAN Configuration 13.2 - Configure a Basic WLAN on the WLC 13.3 - Configure a WPA2 Enterprise WLAN on the WLC	Wireless Concepts	1.11 Describe wireless principles
			1.11.a Nonoverlapping Wi-Fi channels
			1.11.b SSID
			1.11.c RF
			2.6 Compare Cisco Wireless Architectures and AP modes
			2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
9.2	CCNA2	Wireless Standards	1.11 Describe wireless principles

	12.1 - Introduction to Wireless 12.5 - Channel Management		
			1.11.a Nonoverlapping Wi-Fi channels
9.3	CCNA1 4.6 - Wireless Media CCNA2 12.1 - Introduction to Wireless 12.2 - WLAN Components 12.3 - WLAN Operation 12.4 - CAPWAP Operation 12.5 - Channel Management 12.6 - WLAN Threats 12.7 - Secure WLANs 13.1 - Remote Site WLAN Configuration 13.2 - Configure a Basic WLAN on the WLC 13.3 - Configure a WPA2 Enterprise WLAN on the WLC	Wireless Configuration	1.11 Describe wireless principles
			1.11.b SSID
			2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings
			5.10 Configure WLAN using WPA2 PSK using the GUI
9.4	CCNA1 4.6 - Wireless Media CCNA2 12.1 - Introduction to Wireless	Wireless Network Design	1.11 Describe wireless principles
			1.11.b SSID

	12.2 - WLAN Components 12.3 - WLAN Operation 12.4 - CAPWAP Operation 12.5 - Channel Management 12.6 - WLAN Threats 12.7 - Secure WLANs 13.1 - Remote Site WLAN Configuration 13.2 - Configure a Basic WLAN on the WLC 13.3 - Configure a WPA2 Enterprise WLAN on the WLC		
9.5	CCNA1 4.6 - Wireless Media CCNA2 12.1 - Introduction to Wireless 12.2 - WLAN Components 12.3 - WLAN Operation 12.4 - CAPWAP Operation 12.5 - Channel Management 12.6 - WLAN Threats 12.7 - Secure WLANs 13.1 - Remote Site WLAN Configuration	Wireless Network Implementation	2.6 Compare Cisco Wireless Architectures and AP modes
			2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)

	13.2 - Configure a Basic WLAN on the WLC 13.3 - Configure a WPA2 Enterprise WLAN on the WLC		
9.6	CCNA1 4.6 - Wireless Media CCNA2 12.1 - Introduction to Wireless 12.2 - WLAN Components 12.3 - WLAN Operation 12.4 - CAPWAP Operation 12.5 - Channel Management 12.6 - WLAN Threats 12.7 - Secure WLANs 13.1 - Remote Site WLAN Configuration 13.2 - Configure a Basic WLAN on the WLC 13.3 - Configure a WPA2 Enterprise WLAN on the WLC	SOHO Configuration	1.2 Describe characteristics of network topology architectures
			1.2.e Small office/home office (SOHO)
9.7	12.7 - Secure WLANs	Wireless Security	1.11 Describe wireless principles
			1.11.b SSID
			1.11.d Encryption

			2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
			5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
9.8	CCNA2 13.4 - Troubleshoot WLAN Issues	Wireless Troubleshooting	1.11 Describe wireless principles
			1.11.a Nonoverlapping Wi-Fi channels
			1.11.b SSID
10		**WAN Implementation**	
10.1	CCNA3 7.1 - Purpose of WANs 7.2 - WAN Operations 7.3 - Traditional WAN Connectivity 7.4 - Modern WAN Connectivity 7.5 - Internet-Based Connectivity	WAN Types	1.2 Describe characteristics of network topology architectures
			1.2.d WAN
			1.3 Compare physical interface and cabling types
			1.3.b Connections (Ethernet shared media and point-to-point)
10.2	CCNA3 7.1 - Purpose of WANs 7.2 - WAN Operations 7.3 - Traditional WAN Connectivity 7.4 - Modern WAN Connectivity 7.5 - Internet-Based Connectivity	Leased Line WAN Links	1.2 Describe characteristics of network topology architectures
			1.2.d WAN
10.3	CCNA3 6.1 - NAT Characteristics	Network Address Translation (NAT)	4.1 Configure and verify inside source NAT using static and pools

	6.2 - Types of NAT 6.3 - NAT Advantages and Disadvantages 6.4 - Static NAT 6.5 - Dynamic NAT 6.6 – PAT 6.7 - NAT64		
10.4	CCNA3 7.1 - Purpose of WANs 7.2 - WAN Operations 7.3 - Traditional WAN Connectivity 7.4 - Modern WAN Connectivity 7.5 - Internet-Based Connectivity	WAN Troubleshooting	1.2 Describe characteristics of network topology architectures
			1.2.d WAN
11		**Advanced Switching**	
11.1	CCNA2 3.1 - Overview of VLANs 3.2 - VLANs in a Multi-Switched Environment 3.3 - VLAN Configuration	Virtual LANs (VLANs)	2.1 Configure and verify VLANs (normal range) spanning multiple switches
			2.1.a Access ports (data and voice)
			2.1.b Default VLAN
			2.1.c Connectivity
			2.2 Configure and verify interswitch connectivity
			2.2.b 802.1Q
11.2	CCNA2 3.4 - VLAN Trunks 3.5 - Dynamic Trunking Protocol	Trunking	2.1 Configure and verify VLANs (normal range) spanning multiple switches
			2.1.a Access ports (data and voice)
			2.1.b Default VLAN
			2.1.c Connectivity

			2.2 Configure and verify interswitch connectivity
			2.2.a Trunk ports
			2.2.b 802.1Q
			2.2.c Native VLAN
			2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
11.3	CCNA2 5.1 - Purpose of STP 5.2 - STP Operations 5.3 - Evolution of STP	Spanning Tree	2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
			2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
			2.5.a Root port, root bridge (primary/secondary), and other port names
			2.5.b Port states (forwarding/blocking)
			2.5.c PortFast benefits
			2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
11.4	CCNA2 5.1 - Purpose of STP 5.2 - STP Operations 5.3 - Evolution of STP	Spanning Tree Configuration	2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
			2.5.a Root port, root bridge (primary/secondary), and other port names
			2.5.b Port states (forwarding/blocking)
			2.5.c PortFast benefits
11.5	CCNA2 4.1 - Inter-VLAN Routing Operation 4.2 - Router-on-a-Stick Inter-VLAN Routing	Router-on-a-Stick InterVLAN Routing	

11.6	CCNA2 4.1 - Inter-VLAN Routing Operation 4.4 - Troubleshoot Inter-VLAN Routing	Switch InterVLAN Routing	
11.7	CCNA3 12.2 - Troubleshooting Process	Switch Troubleshooting	1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
12		**Access Control Lists**	
12.1	CCNA3 4.1 - Purpose of ACLs 4.2 - Wildcard Masks in ACLs 4.3 - Guidelines for ACL Creation 4.4 - Types of IPv4 ACLs 5.1 - Configure Standard IPv4 ACLs 5.2 - Modify IPv4 ACLs 5.3 - Secure VTY Ports with a Standard IPv4 ACL 5.4 - Configure Extended IPv4 ACLs	Access Control Lists (ACLs)	5.6 Configure and verify access control lists
12.2	CCNA3 4.1 - Purpose of ACLs 4.2 - Wildcard Masks in ACLs 4.3 - Guidelines for ACL Creation 4.4 - Types of IPv4 ACLs 5.1 - Configure Standard IPv4 ACLs	IPv6 and Extended ACLs	5.6 Configure and verify access control lists

	5.2 - Modify IPv4 ACLs 5.3 - Secure VTY Ports with a Standard IPv4 ACL 5.4 - Configure Extended IPv4 ACLs		
13		**Network Management**	
13.1	CCNA3 10.3 - NTP	Network Time Protocol (NTP)	4.2 Configure and verify NTP operating in a client and server mode
13.2	CCNA3 10.5 - Syslog	System Message Log	4.5 Describe the use of syslog features including facilities and levels
13.3	CCNA3 10.4 - SNMP	Simple Network Management Protocol	4.4 Explain the function of SNMP in network operations
13.4		NetFlow	
13.5	CCNA3 9.1 - Network Transmission Quality 9.2 - Traffic Characteristics 9.3 - Queuing Algorithms 9.4 - QoS Models 9.5 - QoS Implementation Techniques	Quality of Service (QoS)	4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
13.6	CCNA3 13.1 - Cloud Computing 13.2 – Virtualization 13.3 - Virtual Network Infrastructure 13.4 - Software-Defined Networking 13.5 – Controllers	Enterprise Networking	6.2 Compare traditional networks with controller-based networking
			6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric)
			6.3.a Separation of control plane and data plane
			6.3.b North-bound and south-bound APIs

13.7	CCNA3 13.1 - Cloud Computing 13.2 – Virtualization 13.3 - Virtual Network Infrastructure 13.4 - Software-Defined Networking 13.5 – Controllers	Cloud Resources	1.2 Describe characteristics of network topology architectures
			1.2.f On-premises and cloud
			1.12 Explain virtualization fundamentals (virtual machines)
13.8	CCNA3 8.1 - VPN Technology 8.2 - Types of VPNs 8.3 - IPsec	Virtual Private Networks and Remote Switch Access	4.8 Configure network devices for remote access using SSH
			5.5 Describe remote access and site-to-site VPNs
13.9	CCNA2 9.1 - First Hop Redundancy Protocols 9.2 - HSRP	Default Gateway Redundancy	3.5 Describe the purpose of first hop redundancy protocol
			6.1 Explain how automation impacts network management
13.1	CCNA3 14.1 - Automation Overview 14.2 - Data Formats 14.3 – APIs 14.4 – REST 14.5 - Configuration Management Tools 14.6 - IBN and Cisco DNA Center	Network Automation	6.1 Explain how automation impacts network management
			6.2 Compare traditional networks with controller-based networking
			6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric)
			6.3.a Separation of control plane and data plane
			6.3.b North-bound and south-bound APIs
			6.4 Compare traditional campus device management with Cisco DNA Center enabled device

			6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)
			6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible
			6.7 Interpret JSON encoded data
14		**Network Security**	
14.1	CCNA3 3.1 - Current State of Cybersecurity 3.2 - Threat Actors 3.3 - Threat Actor Tools CCNA2 10.2 - Access Control	Network Threats	2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
			5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
			5.8 Differentiate authentication, authorization, and accounting concepts
14.2	CCNA3 3.1 - Current State of Cybersecurity 3.2 - Threat Actors 3.3 - Threat Actor Tools	Network Security Best Practices	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
			5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
14.3	CCNA2 10.1 - Endpoint Security 10.2 - Access Control 10.3 - Layer 2 Security Threats 10.4 - MAC Address Table Attack 10.5 - LAN Attacks	Switch Security	2.1 Configure and verify VLANs (normal range) spanning multiple switches
			2.1.a Access ports (data and voice)
			2.1.c Connectivity
			2.2 Configure and verify interswitch connectivity
			2.2.a Trunk ports
			2.2.c Native VLAN

			5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
14.4	CCNA3 3.4 - Malware	Malware	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
			5.2 Describe security program elements (user awareness, training, and physical access control)
14.5	CCNA3 3.4 – Malware 3.5 - Common Network Attacks	Combat Malware	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
			5.2 Describe security program elements (user awareness, training, and physical access control)
14.6	CCNA3 3.5 - Common Network Attacks 3.6 - IP Vulnerabilities and Threats 3.7 - TCP and UDP Vulnerabilities 3.8 - IP Services 3.9 - Network Security Best Practices	Sniffing	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
			5.2 Describe security program elements (user awareness, training, and physical access control)
14.7	CCNA3 3.5 - Common Network Attacks 3.6 - IP Vulnerabilities and Threats 3.7 - TCP and UDP Vulnerabilities 3.8 - IP Services 3.9 - Network Security Best Practices	Session Hijacking	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
			5.2 Describe security program elements (user awareness, training, and physical access control)

14.8	CCNA3 3.5 - Common Network Attacks 3.6 - IP Vulnerabilities and Threats 3.7 - TCP and UDP Vulnerabilities 3.8 - IP Services 3.9 - Network Security Best Practices	Denial of Service	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
			5.2 Describe security program elements (user awareness, training, and physical access control)
15		**Cryptography**	
15.1	CCNA3 3.10 - Cryptography	Cryptography	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
			5.2 Describe security program elements (user awareness, training, and physical access control)
			5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
15.2	CCNA3 3.10 - Cryptography	Cryptanalysis and Cryptographic Attack Countermeasures	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
			5.2 Describe security program elements (user awareness, training, and physical access control)