TestOut

TestOut Routing and Switching Pro – English 7.0.x

Objective Mappings:

TestOut Routing and Switching Pro
Cisco 200-301 CCNA

Powered by **LABSIM**

Contents

This document contains four objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to the TestOut Routing and Switching Pro Objectives

Section	Title	Objectives
1.0	**Introduction to Routing and Switching Pro**	
1.1	Introduction	
2.0	**Networking Concepts**	
2.1	TCP/IP Networking Model	
2.2	OSI Networking Model	
2.3	Networking Basics	
2.4	Data Encapsulation and Communications	
2.5	Ethernet	
2.6	Network Devices	
3.0	**Cisco Devices**	
3.1	Cisco Device Connection	
3.2	Command Line Interface (CLI)	1.1 Setup and configure a router • View router configuration information
3.3	IOS Licensing	

3.4	Device Settings	1.1 Setup and configure a router • Configure router hostnames and interface descriptions • Configure router banners 1.2 Setup and configure a switch • Configure switch hostnames and interface descriptions
3.5	Device Passwords	6.1 Configure router security • Configure router passwords 6.2 Configure switch security • Configure switch passwords
3.6	Cisco Discovery Protocol (CDP)	2.1 Configure a router interface • View directly-connected devices using CDP • Manage the CDP Configuration 2.2 Configure a switch interface • Manage the CPD configuration
4.0	**IP Addressing**	
4.1	IPv4 Addressing Overview	
4.2	Subnets	
4.3	Subnet Planning and Design	3.1 Configure device IP settings • Configure router TCP/IP settings
4.4	Route Summarization	
4.5	IPv6 Addressing Overview	
4.6	Dynamic Host Configuration Protocol (DHCP)	5.2 Configure DHCP • Configure the DHCP service on a router • Configure DHCP bindings • Configure a DHCP relay agent

4.7	The Domain Name System (DNS)	5.3 Configure DNS • Configure DNS • Create DNS zones • Create DNS records • Troubleshoot DNS
5.0	**Switching**	
5.1	Layer 2 Switching Overview	
5.2	Switch Interface Configuration	2.1 Configure a router interface • View the status of router interfaces • View directly-connected devices using CDP 2.2 Configure a switch interface • View the status of switch interfaces • Configure interface speed and duplex settings 3.1 Configure device IP settings • Configure router TCP/IP settings • Configure switch TCP/IP settings
6.0	**IPv4 Routing**	
6.1	IPv4 Routing	
6.2	Static Routing	3.2 Implement IP routing • Configure static routes on a router
6.3	Dynamic Routing	3.2 Implement IP routing • View the routing table on a router
6.4	IPv4 Routing Troubleshooting	
6.5	Network Communications Troubleshooting	3.1 Configure device IP settings • Configure router TCP/IP settings • Configure switch TCP/IP settings

7.0	IPv4 Routing Protocols	
7.1	Open Shortest Path First (OSPF) Overview	
7.2	OSPF for IPv4	
7.3	OSPF Configuration	3.3 Configure OSPFv2 routing • Enable OSPF routing • Configure and manage OSPF routing
7.4	OSPF LSA Types and Databases	
7.5	Adjacency Troubleshooting	3.3 Configure OSPFv2 routing • Troubleshoot OSPF routing
7.6	EIGRP for IPv4 Routing	
7.7	EIGRP for IPv4 Configuration	
8.0	IPv6 Routing	
8.1	IPv6 Routing Overview	
8.2	OSPFv3	
8.3	EIGRPv6	
9.0	Wireless Networks	
9.1	Wireless Concepts	
9.2	Wireless Standards	
9.3	Wireless Configuration	4.5 Configure wireless networking • Create a wireless network • Secure a wireless network
9.4	Wireless Network Design	4.5 Configure wireless networking • Design a wireless network

9.5	Wireless Network Implementation	4.5 Configure wireless networking • Implement and configure a wireless network
9.6	SOHO Configuration	4.5 Configure wireless networking • Implement and configure a wireless network
9.7	Wireless Security	4.5 Configure wireless networking • Secure a wireless network
9.8	Wireless Troubleshooting	4.5 Configure wireless networking • Optimize a wireless network • Troubleshoot a wireless network
10.0	**WAN Implementation**	
10.1	WAN Types	
10.2	Leased Line WAN Links	1.1 Setup and configure a router • View router configuration information 2.1 Configure a router interface • Configure Ethernet and serial router interfaces 3.1 Configure device IP settings • Configure router TCP/IP settings
10.3	Network Address Translation (NAT)	5.1 Configure NAT • Configure static NAT on a router • Configure dynamic NAT on a router • Configure PAT on a router
10.4	WAN Troubleshooting	2.1 Configure a router interface • Configure Ethernet and serial router interfaces • Troubleshoot router connections

11.0	Advanced Switching	
11.1	Virtual LANs (VLANs)	4.1 Configure switch VLANs • Configure VLANs on a switch
11.2	Trunking	4.1 Configure switch VLANs • Configure VLANs on a switch • Use trunking to extend VLAN to multiple switches
11.3	Spanning Tree	4.4 Configure EtherChannel • Configure EtherChannel using PAGP • Configure EtherChannel using LACP
11.4	Spanning Tree Configuration	4.3 Configure spanning tree • View STP configuration information • Manually configure a switch as a root bridge • Configure Rapid PVST+
11.5	Router-on-a-Stick InterVLAN Routing	4.2 Configure interVLAN routing • Configure interVLAN routing
11.6	Switch InterVLAN Routing	4.2 Configure interVLAN routing • Configure interVLAN routing • Troubleshoot interVLAN routing issues
11.7	Switch Troubleshooting	4.1 Configure switch VLANs • View information about VLANs configured on a switch • Troubleshoot VLAN issues

12.0	**Access Control Lists**	
12.1	Access Control Lists (ACLs)	6.1 Configure router security • Restrict router remote access 6.3 Configure access control list • Use ACLs to permit allowed network traffic • Use ACLs to block disallowed network traffic
12.2	IPv6 and Extended ACLs	6.3 Configure access control list • Implement standard, extended, and named ACLs • Use wildcard masks in ACLs • Use ACLs to permit allowed network traffic • Use ACLs to block disallowed network traffic • Block disallowed traffic
13.0	**Network Management**	
13.1	Network Time Protocol (NTP)	
13.2	System Message Log	
13.3	Simple Network Management Protocol	
13.4	NetFlow	
13.5	Quality of Service (QoS)	
13.6	Enterprise Networking	
13.7	Cloud Resources	
13.8	Virtual Private Networks and Remote Switch Access	
13.9	Default Gateway Redundancy	
13.10	Network Automation	

14.0	Network Security	
14.1	Network Threats	
14.2	Network Security Best Practices	6.2 Configure switch security • Configure switch passwords
14.3	Switch Security	1.2 Setup and configure a switch • Manage switch configuration files 6.2 Configure switch security • Secure switch access • Enable switch port security • Restrict switch remote access 6.4 Implement security measures • Scan and detect open ports • Implement device hardening
14.4	Malware	
14.5	Combat Malware	6.4 Implement security measures • Implement anti-malware measures • Scan and detect open ports
14.6	Sniffing	6.4 Implement security measures • Analyze network traffic using Wireshark • Analyze network traffic for potential security risks
14.7	Session Hijacking	6.4 Implement security measures • Analyze network traffic using Wireshark • Analyze network traffic for potential security risks
14.8	Denial of Service	6.4 Implement security measures • Analyze network traffic using Wireshark • Analyze network traffic for potential security risks

15.0	Cryptography	
15.1	Cryptography	6.4 Implement security measures • Analyze network traffic for potential security risks
15.2	Cryptanalysis and Cryptographic Attack Countermeasures	6.4 Implement security measures • Implement anti-malware measures
A.0	TestOut Routing and Switching Pro Practice Exams	
A.1	Prepare for Certification	
A.2	TestOut Routing and Switching Pro Domain Review	
B.0	Cisco CCNA 200-301 Practice Exams	
B.1	Prepare for Certification	
B.2	Cisco CCNA 200-301 Practice Exams (20 Questions)	
B.3	Cisco CCNA 200-301 Practice Exams (All Questions)	

Objective Mapping: TestOut Routing and Switching Pro Objectives to LabSim Section

#	Domain	Module.Section
1.0	**Device Setup and Configuration**	
1.1	Setup and configure a router • View router configuration information • Configure router hostnames and interface descriptions • Configure router banners • Manage router configuration files	3.2, 3.4 10.2
1.2	Setup and configure a switch • View switch configuration information • Configure switch hostnames and interface descriptions • Configure switch banners • Manage switch configuration files	3.4 14.3
2.0	**Interface Configuration**	
2.1	Configure a router interface • View the status of router interfaces • View directly-connected devices using CDP • Manage the CDP Configuration • Configure Ethernet and serial router interfaces • Troubleshoot router connections	3.6 5.2 10.2, 10.4
2.2	Configure a switch interface • View the status of switch interfaces • Configure interface speed and duplex settings • View directly-connected network devices using CDP • Manage the CPD configuration	3.6 5.2

3.0	Network Connectivity	
3.1	Configure device IP settings • Configure router TCP/IP settings • Configure switch TCP/IP settings • Troubleshoot LAN communications	4.3 5.2 6.5 10.2
3.2	Implement IP routing • Calculate and configure subnet masks for network hosts • Configure static routes on a router • View the routing table on a router • Manage auto-summarization between networks	6.2, 6.3
3.3	Configure OSPFv2 routing • Enable OSPF routing • Configure and manage OSPF routing • Troubleshoot OSPF routing	7.3, 7.5
4.0	Network Access	
4.1	Configure switch VLANs • View information about VLANs configured on a switch • Manage default VLAN configuration settings • Configure VLANs on a switch • Use trunking to extend VLAN to multiple switches • Troubleshoot VLAN issues	11.1, 11.2, 11.7
4.2	Configure interVLAN routing • Configure interVLAN routing • Troubleshoot interVLAN routing issues	11.5, 11.6
4.3	Configure spanning tree • View STP configuration information • Manually configure a switch as a root bridge • Configure Rapid PVST+	11.4

4.4	Configure EtherChannel • Configure EtherChannel using PAGP • Configure EtherChannel using LACP	11.3
4.5	Configure wireless networking • Create a wireless network • Secure a wireless network • Design a wireless network • Implement and configure a wireless network • Optimize a wireless network • Troubleshoot a wireless network	9.3, 9.4, 9.5, 9.6, 9.7, 9.8
5.0	**Network IP Services**	
5.1	Configure NAT • Configure static NAT on a router • Configure dynamic NAT on a router • Configure PAT on a router	10.3
5.2	Configure DHCP • Configure the DHCP service on a router • Configure DHCP bindings • Configure a DHCP relay agent	4.6
5.3	Configure DNS • Configure DNS • Create DNS zones • Create DNS records • Troubleshoot DNS	4.7
6.0	**Security**	
6.1	Configure router security • Configure router passwords • Secure router access • Restrict router remote access	3.5 12.1

6.2	Configure switch security • Configure switch passwords • Secure switch access • Enable switch port security • Configure Allowed VLANs • Restrict switch remote access	3.5 14.2, 14.3
6.3	Configure access control list • Implement standard, extended, and named ACLs • Use wildcard masks in ACLs • Use ACLs to permit allowed network traffic • Use ACLs to block disallowed network traffic • Block disallowed traffic	12.1, 12.2
6.4	Implement security measures • Implement anti-malware measures • Scan and detect open ports • Implement device hardening • Analyze network traffic using Wireshark • Analyze network traffic for potential security risks	14.3, 14.5, 14.6, 14.7, 14.8 15.1, 15.2

Objective Mapping: LabSim Section to the Cisco 200-301 CCNA Objectives

Section	Title	Objectives
1.0	**Introduction to Routing and Switching Pro**	
1.1	Introduction	
2.0	**Networking Concepts**	
2.1	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	OSI Networking Model	4.8 Configure network devices for remote access using SSH
2.3	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	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	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

3.0	**Cisco Devices**	
3.1	Cisco Device Connection	4.8 Configure network devices for remote access using SSH
3.2	Command Line Interface (CLI)	
3.3	IOS Licensing	
3.4	Device Settings	
3.5	Device Passwords	5.3 Configure device access control using local passwords
3.6	Cisco Discovery Protocol (CDP)	2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)

4.0	IP Addressing	
4.1	IPv4 Addressing Overview	1.6 Configure and verify IPv4 addressing and subnetting 1.7 Describe the need for private IPv4 addressing
4.2	Subnets	1.6 Configure and verify IPv4 addressing and subnetting 1.7 Describe the need for private IPv4 addressing
4.3	Subnet Planning and Design	1.6 Configure and verify IPv4 addressing and subnetting 1.7 Describe the need for private IPv4 addressing
4.4	Route Summarization	1.6 Configure and verify IPv4 addressing and subnetting

4.5	IPv6 Addressing Overview	1.1 Explain the role and function of network components
		     1.1.f Endpoints
		
		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	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	The Domain Name System (DNS)	4.3 Explain the role of DHCP and DNS within the network

5.0	**Switching**	
5.1	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	Switch Interface Configuration	
6.0	**IPv4 Routing**	
6.1	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 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	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	Dynamic Routing	
6.4	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

7.0	IPv4 Routing Protocols	
7.1	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	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	OSPF Configuration	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
7.4	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	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	

8.0	IPv6 Routing	
8.1	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	OSPFv3	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
8.3	EIGRPv6	
9.0	Wireless Networks	
9.1	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	Wireless Standards	1.11 Describe wireless principles 1.11.a Nonoverlapping Wi-Fi channels
9.3	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	Wireless Network Design	1.11 Describe wireless principles 1.11.b SSID
9.5	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)
9.6	SOHO Configuration	1.2 Describe characteristics of network topology architectures 1.2.e Small office/home office (SOHO)

9.7	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	Wireless Troubleshooting	1.11 Describe wireless principles
		        1.11.a Nonoverlapping Wi-Fi channels
		        1.11.b SSID

10.0	WAN Implementation	
10.1	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	Leased Line WAN Links	1.2 Describe characteristics of network topology architectures 　　1.2.d WAN
10.3	Network Address Translation (NAT)	4.1 Configure and verify inside source NAT using static and pools
10.4	WAN Troubleshooting	1.2 Describe characteristics of network topology architectures 　　1.2.d WAN
11.0	Advanced Switching	
11.1	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	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	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	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	Router-on-a-Stick InterVLAN Routing	
11.6	Switch InterVLAN Routing	
11.7	Switch Troubleshooting	1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)

12.0	Access Control Lists	
12.1	Access Control Lists (ACLs)	5.6 Configure and verify access control lists
12.2	IPv6 and Extended ACLs	5.6 Configure and verify access control lists
13.0	**Network Management**	
13.1	Network Time Protocol (NTP)	4.2 Configure and verify NTP operating in a client and server mode
13.2	System Message Log	4.5 Describe the use of syslog features including facilities and levels
13.3	Simple Network Management Protocol	4.4 Explain the function of SNMP in network operations
13.4	NetFlow	
13.5	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	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	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	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	Default Gateway Redundancy	3.5 Describe the purpose of first hop redundancy protocol 6.1 Explain how automation impacts network management
13.10	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
14.0	**Network Security**	
14.1	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	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	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	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	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	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	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	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)

15.0	**Cryptography**	
15.1	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	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)
A.0	**TestOut Routing and Switching Pro Practice Exams**	
A.1	Prepare for Certification	
A.2	TestOut Routing and Switching Pro Domain Review	
B.0	**Cisco CCNA 200-301 Practice Exams**	
B.1	Prepare for Certification	
B.2	Cisco CCNA 200-301 Practice Exams (20 Questions)	
B.3	Cisco CCNA 200-301 Practice Exams (All Questions)	

Objective Mapping: Cisco 200-301 CCNA Objectives to LabSim Section

#	Domain	Section
1.0	**Network Fundamentals**	
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.f Endpoints 1.1.g Servers	2.6 4.5 5.1
1.2	Describe characteristics of network topology architectures 1.2.a 2 tier 1.2.b 3 tier 1.2.c Spine-leaf 1.2.d WAN 1.2.e Small office/home office (SOHO) 1.2.f On-premises and cloud	5.1 9.6 10.1, 10.2, 10.4 13.7
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	2.3, 2.5 5.1 6.2 10.1
1.4	Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)	2.5 11.7

1.5	Compare TCP to UDP	2.1
1.6	Configure and verify IPv4 addressing and subnetting	4.1, 4.2, 4.3, 4.4 6.2, 6.4, 6.5
1.7	Describe the need for private IPv4 addressing	4.1, 4.2, 4.3
1.8	Configure and verify IPv6 addressing and prefix	4.5 8.1, 8.2

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
		4.5
		8.1, 8.2

1.10	Verify IP parameters for Client OS (Windows, Mac OS, Linux)	6.4

1.11	Describe wireless principles
	
	       1.11.a Nonoverlapping Wi-Fi channels
	       1.11.b SSID
	       1.11.c RF
	       1.11.d Encryption
		9.1, 9.2, 9.3, 9.4,
		9.7, 9.8

1.12	Explain virtualization fundamentals (virtual machines)	13.7

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
		2.6
		5.1

2.0	Network Access	
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	11.1, 11.2 14.3
2.2	Configure and verify interswitch connectivity 2.2.a Trunk ports 2.2.b 802.1Q 2.2.c Native VLAN	11.1, 11.2 14.3
2.3	Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)	3.6
2.4	Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)	11.3
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	11.3, 11.4
2.6	Compare Cisco Wireless Architectures and AP modes	9.1, 9.5
2.7	Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)	2.6 9.1 11.2, 11.3
2.8	Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)	2.6 9.5, 9.7 14.1
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	2.6 9.3

3.0	IP Connectivity	
3.1	Interpret the components of routing table 3.1.a Routing protocol code 3.1.b Prefix 3.1.c Network mask 3.1.d Next hop 3.1.e Administrative distance 3.1.f Metric 3.1.g Gateway of last resort	6.1
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	6.1
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	6.1, 6.2, 6.4

3.4	Configure and verify single area OSPFv2	7.1, 7.2, 7.3, 7.4, 7.5
	3.4.a Neighbor adjacencies 3.4.b Point-to-point 3.4.c Broadcast (DR/BDR selection) 3.4.d Router ID	
3.5	Describe the purpose of first hop redundancy protocol	13.9
4.0	**IP Services**	
4.1	Configure and verify inside source NAT using static and pools	10.3
4.2	Configure and verify NTP operating in a client and server mode	13.1
4.3	Explain the role of DHCP and DNS within the network	4.6, 4.7
4.4	Explain the function of SNMP in network operations	13.3
4.5	Describe the use of syslog features including facilities and levels	13.2
4.6	Configure and verify DHCP client and relay	4.6
4.7	Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping	13.5
4.8	Configure network devices for remote access using SSH	2.1, 2.2 3.1 13.8
4.9	Describe the capabilities and function of TFTP/FTP in the network	2.1
5.0	**Security Fundamentals**	
5.1	Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)	14.1, 14.2, 14.4, 14.5, 14.6, 14.7, 14.8 15.1, 15.2
5.2	Describe security program elements (user awareness, training, and physical access control)	14.4, 14.5, 14.6, 14.7, 14.8 15.1, 15.2

5.3	Configure device access control using local passwords	3.5
5.4	Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)	14.2 15.1
5.5	Describe remote access and site-to-site VPNs	13.8
5.6	Configure and verify access control lists	12.1, 12.2
5.7	Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)	14.3
5.8	Differentiate authentication, authorization, and accounting concepts	14.1
5.9	Describe wireless security protocols (WPA, WPA2, and WPA3)	9.7
5.10	Configure WLAN using WPA2 PSK using the GUI	9.3
6.0	**Automation and Programmability**	
6.1	Explain how automation impacts network management	13.9, 13.10
6.2	Compare traditional networks with controller-based networking	13.6, 13.10
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	13.6, 13.10
6.4	Compare traditional campus device management with Cisco DNA Center enabled device	13.10
6.5	Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)	13.10
6.6	Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible	13.10
6.7	Interpret JSON encoded data	13.10