Filename: cisco-ccna200301-2022-0-0-0-overview-exam-objectives
ShowName: Cisco CCNA (Exam 200-301).
SubTitle: Modern Networking Skills
Topic: 0.0 Overview Exam Objectives
EpisodeName: Overview
Description: The Cisco CCNA show is produced to to help candidates prepare for the 200-301 exam. The show examines the fundamentals of a variety of IT careers. It will prepare any one who achieves CCNA certification the knowledge and skills need to start any IT career he or she chooses. The show will cover networking fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability

There are no formal prerequisites for CCNA certification, but you should have an throughly review each exam topic before taking the exam. CCNA candidates also are expected to have:

- Hands-on experience implementing and administering Cisco solutions
- Knowledge of basic IP addressing theory
- A commanding knowledge of network fundamentals

1.0 Networking Fundamentals

Networking Components (Roles and Functions)

- 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

Networking Topologies Architectures

- 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

Physical Networking Concepts

- 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)

Netoworking Connections

- 1.5 Compare TCP to UDP

IP Addressing

- 1.6 Configure and verify IPv4 addressing and subnetting
- 1.7 Describe the need for private IPv4 addressing
- 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
- 1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)

Virtualization Fundamentals

- 1.12 Explain virtualization fundamentals (virtual machines)

2.0 Network Access

Switches and Switching [Moved to Cisco Switching-Complet]

- 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

Basic VLAN Configuration

- 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

Interswitch Connectivity

- 2.2 Configure and verify interswitch connectivity
    - 2.2.a Trunk ports
    - 2.2.b 802.1Q
    - 2.2.c Native VLAN

L2 Discovery Protocols

- 2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)

Etherchannel Configuration

- 2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)

Spanning Tree Protocol

- 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

Cisco Wireless

- 1.11 Describe wireless principles
    - 1.11.a Nonoverlapping Wi-Fi channels
    - 1.11.b SSID
    - 1.11.c RF
    - 1.11.d Encryption
- 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)
- 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
- 5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)

3.0 IP Connectivity

Routing 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)

Routing Tables

- 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

Routing Decisions

- 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

Configure Static Routing

- 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

Dynamic Routing Protocols, an introduction (RIP, EIGRP, OSPF, BGP)

- not exam objective but helpful to contextualize configuration

Configure Dynamic Routing: OSPFv2

- 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

Describe FHRP

- 3.5 Describe the purpose of first hop redundancy protocol

4.0 IP Services

Network Address Translation

- 4.1 Configure and verify inside source NAT using static and pools

Network Time Protocol

- 4.2 Configure and verify NTP operating in a client and server mode

DHCP and DNS

- 4.3 Explain the role of DHCP and DNS within the network
- 4.6 Configure and verify DHCP client and relay

SNMP

- 4.4 Explain the function of SNMP in network operations

Syslog

- 4.5 Describe the use of syslog features including facilities and levels

PHB for QoS

- 4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping

Remote Access SSH

- 4.8 Configure network devices for remote access using SSH

FTP/TFTP

- 4.9 Describe the capabilities and function of TFTP/FTP in the network

5.0 Security Fundamentals

Security Concepts

- 5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)

Security Programs

- 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)
- 5.8 Differentiate authentication, authorization, and accounting concepts

Configure security controls

- 5.3 Configure device access control using local passwords
- 5.5 Describe remote access and site-to-site VPNs
- 5.6 Configure and verify access control lists
- 5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- 5.10 Configure WLAN using WPA2 PSK using the GUI

6.0 Automation and Programmability

Automation and Network Management

- 6.1 Explain how automation impacts network management
- 6.2 Compare traditional networks with controller-based networking

Controller-based and Software-Defined Architectures

- 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

Device Management

- 6.4 Compare traditional campus device management with Cisco DNA Center enabled device management

REST-based APIs

- 6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)

Configuration Management

- 6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible

JSON encoded data

- 6.7 Interpret JSON encoded data