CURSOS DE CERTIFICACIÓN
DIPLOMADO DE INTERCONECTIVIDAD

FACULTAD DE INGENIERÍA, DIE, UNAM
DEPARTAMENTO DE TELECOMUNICACIONES

2. CCNP Enterprise

INTRODUCCIÓN:

Este temario se está basado en un diplomado de 120 horas y los temas mencionados en este documento se han basado en las guías de estudio oficiales de Cisco. Para este curso se han tomado en cuenta los temarios de los siguientes exámenes:

- Implementing Cisco Enterprise Network Core Technologies (300-401) examen core
- Implementing Cisco Enterprise Advanced Routing and Services (300-410) examen especialización

Cabe señalar que estos temarios se han juntado y se darán los temas intercalados, ya que se tienen muchas similitudes en los temas.

OBJETIVO:

El presente documento tiene como objetivo plantear un temario para el diplomado orientado a la certificación CCNP Enterprise con la especialización de implementación de enrutamiento avanzado y servicios para redes Enterprise.

ALCANCE:

After Completing the CCNP Course, students will be able to perform the following:
Implement, monitor, and maintain routing and switching services in an enterprise campus network.
Plan, configure, and verify the implementation of complex enterprise LAN and WAN routing solutions

Implement IPv6, RIP, EIGRP, BGP, and OSPF in an enterprise network.
Configure secure routing solutions to support branch offices and mobile workers.
Implement the secure integration of VLANs, WLANs, voice, and video into campus networks.
Plan, configure, and verify the implementation of complex enterprise switching solutions.

CCNP ENTERPRISE

TEMARIO:

1.0 Architecture

1.1 Explain the different design principles used in an enterprise network

- 1.1.a Enterprise network design such as Tier 2, Tier 3, and Fabric Capacity planning
- 1.1.b High availability techniques such as redundancy, FHRP, and SSO

1.2 Analyze design principles of a WLAN deployment

- 1.2.a Wireless deployment models (centralized, distributed, controller-less, controller based, cloud, remote branch)
- 1.2.b Location services in a WLAN design

1.3 Differentiate between on-premises and cloud infrastructure deployments

1.4 Explain the working principles of the Cisco SD-WAN solution

- 1.4.a SD-WAN control and data planes elements
- 1.4.b Traditional WAN and SD-WAN solutions

1.5 Explain the working principles of the Cisco SD-Access solution

- 1.5.a SD-Access control and data planes elements
- 1.5.b Traditional campus interoperating with SD-Access

1.6 Describe concepts of wired and wireless QoS

- 1.6.a QoS components
- 1.6.b QoS policy

1.7 Differentiate hardware and software switching mechanisms

- 1.7.a Process and CEF
- 1.7.b MAC address table and TCAM
- 1.7.c FIB vs. RIB

2.0 Virtualization and VPN Technologies

2.1 Describe device virtualization technologies

- 2.1.a Hypervisor type 1 and 2
- 2.1.b Virtual machine
- 2.1.c Virtual switching

2.2 Configure and verify data path virtualization technologies

- 2.2.a VRF
- 2.2.b GRE and IPsec tunneling

2.3 Describe network virtualization concepts

- 2.3.a LISP
- 2.3.b VXLAN

2.4 Describe MPLS operations (LSR, LDP, label switching, LSP)

2.5 Describe MPLS Layer 3 VPN

2.6 Configure and verify DMVPN (single hub)

- 2.6.a GRE/mGRE
- 2.6.b NHRP
- 2.6.c IPsec
- 2.6.d Dynamic neighbor
- 2.6.e Spoke-to-spoke

3.0 Layer 2

3.1 Troubleshoot static and dynamic 802.1q trunking protocols

3.2 Troubleshoot static and dynamic EtherChannels

3.3 Configure and verify common Spanning Tree Protocols (RSTP and MST)

4.0 Layer 3

4.1 Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. linked state, load balancing, path selection, path operations, metrics)

4.2 Configure and verify simple OSPF environments, including multiple normal areas, summarization, and filtering (neighbor adjacency, point-to-point and broadcast network types, and passive interface)

4.3 Configure and verify eBGP between directly connected neighbors (best path selection algorithm and neighbor relationships)

4.4 Troubleshoot administrative distance (all routing protocols)

4.5 Troubleshoot route map for any routing protocol (attributes, tagging, filtering)

4.6 Troubleshoot loop prevention mechanisms (filtering, tagging, split horizon, route poisoning)

4.7 Troubleshoot redistribution between any routing protocols or routing sources

4.8 Troubleshoot manual and auto-summarization with any routing protocol

4.9 Configure and verify policy-based routing

4.10 Configure and verify VRF-Lite

4.11 Describe Bidirectional Forwarding Detection

4.12 Troubleshoot EIGRP (classic and named mode)

4.12.a Address families (IPv4, IPv6)

4.12.b Neighbor relationship and authentication

4.12.c Loop-free path selections (RD, FD, FC, successor, feasible successor, stuck in active)

4.12.d Stubs

4.12.e Load balancing (equal and unequal cost)

4.12.f Metrics

4.13 Troubleshoot OSPF (v2/v3)

4.13.a Address families (IPv4, IPv6)

4.13.b Neighbor relationship and authentication

4.13.c Network types, area types, and router types

4.13.c (i) Point-to-point, multipoint, broadcast, nonbroadcast 4.13.c (ii) Area type: backbone, normal, transit, stub, NSSA, totally stub

4.13.c (iii) Internal router, backbone router, ABR, ASBR

4.13.c (iv)Virtual link 1.10.d Path preference

4.14 Troubleshoot BGP (Internal and External)

4,14.a Address families (IPv4, IPv6)

4.14.b Neighbor relationship and authentication (next-hop, mulithop, 4-byte AS, private AS, route refresh, synchronization, operation, peer group, states and timers)

4.14.c Path preference (attributes and best path)

4.14.d Route reflector (excluding multiple route reflectors, confederations, dynamic peer)

4.14.e Policies (inbound/outbound filtering, path manipulation)

5.0 Wireless

5.1 Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference noise, band and channels, and wireless client devices capabilities

5.2 Describe AP modes and antenna types

5.3 Describe access point discovery and join process (discovery algorithms, WLC selection process)

5.4 Describe the main principles and use cases for Layer 2 and Layer 3 roaming

5.5 Troubleshoot WLAN configuration and wireless client connectivity issues

6.0 IP Services

6.1 Describe Network Time Protocol (NTP)

6.2 Configure and verify NAT/PAT

6.3 Configure first hop redundancy protocols, such as HSRP and VRRP

6.4 Describe multicast protocols, such as PIM and IGMP v2/v3

7.0 Network Assurance and Infrastructure service

7.1 Diagnose network problems using tools such as debugs, conditional debugs, trace route, ping, SNMP, and syslog

7.1 Configure and verify device monitoring using syslog for remote logging

7.3 Configure and verify NetFlow and Flexible NetFlow

7.4 Configure and verify SPAN/RSPAN/ERSPAN

7.5 Configure and verify IPSLA

7.6 Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management

7.7 Configure and verify NETCONF and RESTCONF

7.8 Troubleshoot device management

- 7.8.a Console and VTY
- 7.8.b Telnet, HTTP, HTTPS, SSH, SCP
- 7.8.c (T)FTP

7.9 Troubleshoot SNMP (v2c, v3)

7.10 Troubleshoot network problems using logging (local, syslog, debugs, conditional debugs, timestamps)

7.11 Troubleshoot IPv4 and IPv6 DHCP (DHCP client, IOS DHCP server, DHCP relay, DHCP options)

7.12 Troubleshoot network performance issues using IP SLA (jitter, tracking objects, delay, connectivity)

7.13 Troubleshoot NetFlow (v5, v9, flexible NetFlow)

7.14 Troubleshoot network problems using Cisco DNA Center assurance (connectivity, monitoring, device health, network health)

8.0 Security

8.1 Configure and verify device access control

- 8.1.a Lines and password protection
- 8.1.b Authentication and authorization using AAA

8.2 Configure and verify infrastructure security features

- 8.2.a ACLs
- 8.2.b CoPP

8.3 Describe REST API security

8.4 Configure and verify wireless security features

- 8.4.a EAP
- 8.4.b WebAuth
- 8.4.c PSK

8.5 Describe the components of network security design

- 8.5.a Threat defense
- 8.5.b Endpoint security
- 8.5.c Next-generation firewall
- 8.5.d TrustSec, MACsec
- 8.5.e Network access control with 802.1X, MAB, and WebAuth

8.6 Troubleshoot device security using IOS AAA (TACACS+, RADIUS, local database)

8.7 Troubleshoot router security features

- 8.7.a IPv4 access control lists (standard, extended, time-based)
- 8.7.b IPv6 traffic filter
- 8.7.c Unicast reverse path forwarding (uRPF)

8.8 Troubleshoot control plane policing (CoPP) (Telnet, SSH, HTTP(S), SNMP, EIGRP, OSPF, BGP)

8.9 Describe IPv6 First Hop security features (RA guard, DHCP guard, binding table, ND inspection/snooping, source guard)

9.0 Automation

9.1 Interpret basic Python components and scripts

9.2 Construct valid JSON encoded file

9.3 Describe the high-level principles and benefits of a data modeling language, such as YANG

9.4 Describe APIs for Cisco DNA Center and vManage

9.5 Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF

9.6 Construct EEM applet to automate configuration, troubleshooting, or data collection

9.7 Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack