



**ACADEMIA CISCO UNIVERSIDAD
CENTRAL DE VENEZUELA - MARACAY**
Cisco Networking Academy
Contenido de curso



CCNP ENCOR v8 Enterprise Network Core Technologies

Información general

En este curso los participantes aprenden, aplican y practican conocimientos y habilidades de CCNP Enterprise a través de una serie de experiencias prácticas en profundidad que refuerzan su aprendizaje. Está diseñado para participantes que buscan trabajos de nivel profesional en el área de las TIC y/o desean cumplir los requisitos previos para obtener las certificaciones CCNP Enterprise.

El curso CCNP Enterprise Core Networking (CCNP ENCOR) enseña a los estudiantes conceptos básicos para configurar routers y switches en entornos empresariales, facilitando la conexión de dispositivos, aplicaciones y datos a través de Internet y de otras redes informáticas. Al final del curso, los estudiantes podrán realizar configuraciones avanzadas para routers y switches; así como diseñar y configurar LAN y WAN de nivel empresarial cableadas y con tecnologías inalámbricas, que integren direccionamiento IP dual stack, protocolos de enrutamiento, switching y seguridad.

Al finalizar el curso, los estudiantes podrán:

- Configurar redundancia L2 en una red empresarial.
- Configurar EIGRP para optimizar el rendimiento en una red empresarial.
- Implementar funciones avanzadas de OSPF para mejorar el rendimiento en redes empresariales IPv4 e IPv6.
- Configure eBGP en una red de acceso remoto desde el hogar.
- Explicar los conceptos de operación multicast y QoS en una red.
- Configure los servicios IP y las VPN para admitir redes seguras, administradas de sitio a sitio y de acceso remoto.
- Explicar cómo las topologías y antenas inalámbricas permiten que los AP se integren con WLC en una red.
- Implementar redes inalámbricas seguras para administrar y admitir roaming inalámbrico.
- Implementar tecnologías avanzadas para obtener una arquitectura de red segura y escalable.
- Configurar tecnologías de red para proporcionar acceso seguro a esta infraestructura.
- Explicar los propósitos y características de la virtualización y la automatización de la red.

Duración:

Este curso se dictará en formato 100% a distancia, con un tiempo previsto de duración de 70 horas para las clases en línea. Además, se desarrollarán actividades fuera de línea que requerirán del participante un tiempo de dedicación estimado de 40 horas.

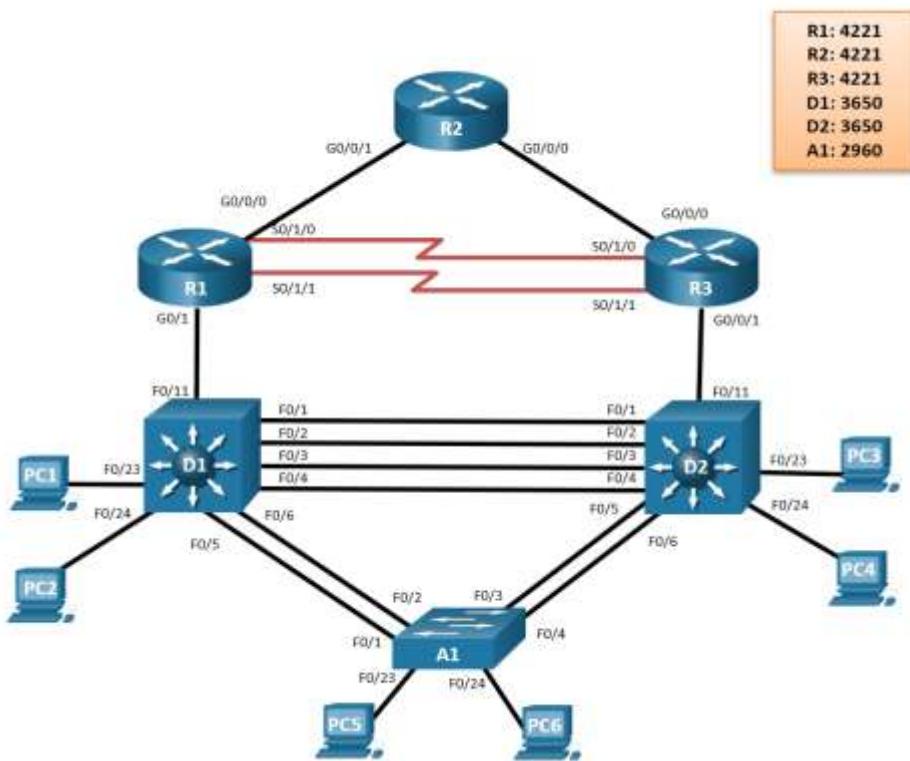
Requisitos para los participantes:

1. Dominio adecuado de lectura de inglés técnico. Los materiales del curso y evaluaciones están disponibles exclusivamente en ese idioma.
2. Haber cursado y aprobado todos los módulos de CCNA R&S versión 5 o superior; o tener conocimientos equivalentes en teoría y práctica de *Routing y Switching*.
3. El curso se desarrolla en base al libro: ***Official Cert Guide. CCNP and CCIE Enterprise Core ENCOR 350-401*** de Cisco Press (En inglés). Es **imprescindible** que cada participante tenga acceso al mismo. Este puede ser adquirido en formato impreso o digital a través de sitios de Internet.
4. Disponer de una conexión a Internet para poder participar en las sesiones en línea y de soporte remoto que se puedan requerir.
5. Instalar en un computador personal los programas *Packet Tracer 8.0* y *GNS3* para actividades prácticas remotas. Este computador debe tener al menos 8 Gbytes de memoria y se recomienda usar Windows 10. Otras opciones para ejecutar prácticas son *VIRL/CML* de Cisco, programa *EVE-NG* y/o acceso a *NetLab* con pods configurados para CCNP ENCOR. *Packet Tracer*, *GNS3* y *EVE-NG* se ejecutan también en ambiente Linux.
6. Debido a las características particulares de la topología a utilizar y los requerimientos para su implementación en un ambiente de emulación de redes como *GNS3* más el software de virtualización para PC (se recomienda *Oracle VirtualBox*), se distribuirá un instructivo base que indicará los sitios desde los cuales se puedan descargar los distintos componentes para estos ambientes con el fin de utilizar versiones comunes y permita además guiar al estudiante en los procesos de instalación y configuración. Está prevista una clase de inducción por parte del instructor sobre estos procesos.

La imagen y aspectos descriptivos que se muestran en la siguiente página, es el correspondiente a la topología utilizada para los cursos CCNP ENCOR y CCNP ENARSI. Cisco Networking Academy señala que se permiten ciertas variaciones en cuanto a equipos físicos. No obstante, si se trabaja a nivel de emulación se recomienda seguir los lineamientos indicados.

CCNP Enterprise Baseline Physical Topology

(for both ENCOR and ENARSI)



CCNP Baseline Equipment Recommendation

- 3x Cisco 4221 with SEC license (2 with NIM-2T)
 - 2x Cisco Catalyst 3650 Switches (WS-C3650-24TS-E)
 - 1x Cisco Catalyst 2960+ Switch (WS-C2960+24TC-L)
 - Ethernet cables as shown in the topology
 - 2x CAB-SS-V35MT= (10' DTE Serial Cable)
 - 2x CAB-SS-V35FC= (10' DCE Serial Cable)

Cisco IOS versions

- Routers: Version IOS-XE 16.9.4 or higher, universal feature set.
 - Layer 3 Switches: Version IOS-XE 16.9.4 or higher, ipservices feature set.
 - Layer 2 Switches: Version IOS 15.2.7 or higher, lanbaseK9 feature set

Computers (Virtual or Physical) requirements

- CPU: Intel Pentium 4, 2.53 GHz or equivalent
 - Operating Systems, Windows, Linux ó Mac OS
 - RAM: 4 GB / Storage: 500 MB of free disk space
 - Display resolution: 1024 x 768 / Latest video card
 - Language fonts supporting Unicode

Software:

- **Packet Tracer v8.0** (optional for CCNA skills review activities)
 - **Virtualization software:** Oracle VirtualBox, most recent versi0n.
 - **Wireshark** version: latest stable version
 - Open-source server software for various services and protocols, such as HTTP, DHCP, FTP, TFTP, etc.
 - Terminal emulation and SSH client software, such as Tera Term and PuTTy for lab PCs.
 - Terminal emulation software for the installed PC operating system

Evaluaciones:

- Durante el curso se desarrollarán actividades que permitirán evaluar el desempeño de cada estudiante. Estas evaluaciones estarán enmarcadas en distintas categorías: laboratorios y exámenes prácticos, quizzes, participación en foros de discusión, exposición de temas y las evaluaciones en línea desde el sitio de Netacad.
- El instructor indicará en la primera semana del curso, el plan de evaluación y las ponderaciones de cada actividad.
- El instructor indicará las actividades prácticas que deben ser realizadas. El estudiante podrá desarrollar cualquier otra actividad práctica incluida en los contenidos del curso y podrá solicitar soporte al instructor en los mismos.
- Las evaluaciones prácticas que se desarrolle a distancia, requerirán acceso físico a la topología señalada en la figura correspondiente o un ambiente de simulación de red, basado en las recomendaciones.
- Se usará el ambiente de simulación GNS3 para una estandarización que permita un soporte uniforme a todos los estudiantes. Considerar los requisitos de hardware para el uso de esta herramienta y los requerimientos de IOS para los equipos a emular.
- Lo anterior no excluye las otras alternativas de simulación y laboratorios remotos mencionadas, si están disponibles para el estudiante.
- Al culminar el curso, el instructor calificará al estudiante. Aquellos que aprueben el curso podrán descargar el certificado digital de aprobación para su impresión.
- Si un participante requiere sello, firma o autenticación del certificado, deberá comunicarse con la Academia Cisco UCV-Maracay para indicarle los pasos a seguir.

Observaciones finales:

- Al aprobar este curso, el estudiante estará en capacidad de presentar el examen de certificación **CCNP Enterprise Core ENCOR 350-401**, que es parte del proceso de certificación Cisco Certified CCNP Enterprise.
- El curso **CCNP ENCOR** es el primer curso de la serie Enterprise en el programa Cisco Network Academy. Se complementa con el curso **CCNP ENARSI**, como una vía para obtener la **certificación CCNP Enterprise**.
- *La aprobación de este curso, no da derecho a voucher de descuento para el examen de certificación CCNP Enterprise Core 350-40.*
- Las imágenes al final de este documento ilustran las distintas rutas de certificación CCNP existentes.

Contenido del curso CCNP v8.0 ENCOR

Chapter 01. Packet Forwarding

- *Compare hardware and software switching mechanisms.*
 - 1.1 Explain how L2 and L3 devices forward traffic.
 - 1.2 Explain the process of hardware and software Cisco Express Forwarding.

Chapter 02. Spanning Tree Protocol

- *Configure spanning tree protocol in a switched environment.*
 - 2.1 Explain the purpose of the spanning tree protocol in a switched LAN environment with redundant inter-switch links.
 - 2.2 Explain how Rapid PVST+ operates.

Chapter 03. Advanced Spanning Tree

- *Configure STP with protection mechanisms.*
 - 3.1 Explain how to modify the root bridge to control the topology.
 - 3.2 Configure BPDU Guard and LoopGuard to protect an STP installation.

Chapter 04. Multiple Spanning Tree Protocol (MST)

- *Configure multiple versions of the Spanning Tree Protocol.*

Chapter 05. VLAN Trunks and EtherChannel Bundles

- *Troubleshoot EtherChannel on switched networks.*
 - 5.1 Describe Etherchannel technology.
 - 5.2. Configure EtherChannel.
 - 5.3. Troubleshoot EtherChannel
 - 5.4. Configure Dynamic Trunking Protocol (DTP).
 - 5.5. Troubleshoot VLAN and trunk configurations in a switched network.

Chapter 06. IP Routing Essentials

- *Configure routers using different algorithms to determine the best path.*
 - 6.1 Compare algorithms used by different routing protocols to forward packets.
 - 6.2 Explain how routers determine the best path.
 - 6.3 Configure static, default, and floating static routes
 - 6.4 Describe virtual routing and forwarding (VRF).

Chapter 07. Enhanced Interior Gateway Routing (EIGRP)

- *Configure EIGRP to improve network performance.*
 - 7.1 Describe the basic features of EIGRP.
 - 7.2 Describe the algorithm used by EIGRP to determine the best path.
 - 7.3 Explain how different types of packets are used to establish and maintain an EIGRP neighbor relationship.
 - 7.4 Configure EIGRP manual summarization.
 - 7.5 Configure EIGRP interface settings to improve network performance.
 - 7.6 Configure EIGRP authentication to ensure secure routing updates.
 - 7.7 Configure a router to propagate a default route in an EIGRP network.
 - 7.8 Configure EIGRP autosummarization.

Chapter 08. Open Shortest Path First (OSPF)

- *Implement multiarea OSPFv2.*
 - 8.1 Explain the features and characteristics of the OSPF routing protocol.
 - 8.2 Configure single-area OSPFv2 in a point-to-point network.
 - 8.3 Configure OSPF to propagate a default route.
 - 8.4 Configure OSPF to improve network performance.
 - 8.5 Configure multiarea OSPFv2 in a routed network.
 - 8.6 Configure summarization between OSPF areas.
 - 8.7 Verify multiarea OSPFv2 operation.

Chapter 09. Advanced OSPF

- *Use advanced OSPF features to optimize network performance.*
 - 9.1 Explain why multiarea OSPF is used.
 - 9.2 Explain how multiarea OSPFv2 uses link state advertisements.
 - 9.3 Explain how to connect discontiguous áreas in OSPFv2.
 - 9.4 Explain how OSPF determines the best path.
 - 9.5 Configure summarization between OSPFareas.
 - 9.6 Explain how to filter routes in OSPFv2 to improve performance.

Chapter 10. OSPFv3

- *Implement single-area OSPFv3.*
 - 10.1 Compare the characteristics and operations of OSPFv2 to OSPFv3.
 - 10.2 Configure single-area OSPFv3.
 - 10.3 Verify single-area OSPFv3.
 - 10.4 Explain how IPv4 traffic is supported in OSPFv3.

Chapter 11. Border Gateway Protocol (BGP)

- *Configure eBGP in a single-homed remote access network.*
 - 11.1 Describe basic BGP features.
 - 11.2 Configure an eBGP branch connection.
 - 11.3 Explain BGP design considerations.
 - 11.4 Configure summarization in BGP to improve performance.
 - 11.5 Configure BGP to support and summarize IPv6 traffic.

Chapter 12. Advanced BGP

- *Explain how advanced BGP features improve performance.*
 - 12.1 Explain how BGP multihoming to ISPs provides resilient internet service.
 - 12.2 Explain how ACLs and prefix matching assist in fine tuning the BGP routing process.
 - 12.3 Explain the purpose of Route-maps in BGP.
 - 12.4 Explain how BGP uses route filtering and manipulation to improve performance.
 - 12.5 Explain the function and purpose of BGP communities.
 - 12.6 Explain what processes are used by BGP for path selection.

Chapter 13. Multicast

- *Explain the concepts and protocols that are required to understand multicast operation.*
 - 13.1 Describe the overall concepts and need for multicasting.
 - 13.2 Describe the address scopes used by multicast to operate at layer 2 and layer 3.
 - 13.3 Explain how IGMP v2 and IGMP v3 allow multicast groups to start receiving multicast traffic.
 - 13.4 Explain the concepts, operation and features of the multicast routing protocol PIM.
 - 13.5 Describe the purpose, function, and operation of a rendezvous point in the multicast network.

Chapter 14. Quality of Service (QoS)

- *Explain the mechanisms used by QoS to ensure transmission quality.*
 - 14.1 Explain how network transmission characteristics impact quality.
 - 14.2 Describe the different QoS models.
 - 14.3 Describe how QoS classifies and marks traffic based on conditioning policies.
 - 14.4 Explain how policing and shaping algorithms affect excess IP traffic.
 - 14.5 Explain how congestion management and avoidance tools are used to avoid network congestion.

Chapter 15. IP Services

- *Configure IP services for managed networks that provide redundancy, address translation and synchronization.*
 - 15.1 Implement NTP between an NTP client and NTP server.
 - 15.2 Configure HSRP using Cisco IOS commands.
 - 15.3 Configure NAT services on the edge router to provide IPv4 address scalability.

Chapter 16. Overlay Tunnels

- *Configure overlay tunnels to secure site-to-site and remote access connectivity.*
 - 16.1 Configure a site-to-site GRE tunnel.
 - 16.2 Explain how the IPsec framework is used to secure network traffic.
 - 16.3 Explain how the routing architecture, LISP, addresses internet routing scalability problems.
 - 16.4 Explain how a virtual extensible local area network (VXLAN) scheme addresses issues in traditional layer 2 networks.

Chapter 17. Wireless Signals and Modulation

- *Explain the theory of wireless signals and the methods used to carry data wirelessly.*
 - 17.1 Describe the technology and characteristics of radio frequency signals
 - 17.2 Explain methods used to carry data over an RF signal.
 - 17.3 Identify the standards and methods used to maintain AP to client compatibility.
 - 17.4 Explain how to use multiple radio components to scale performance.
 - 17.5 Explain techniques used to maximize AP to client throughput.

Chapter 18. Wireless Architecture Infrastructure

- *Select appropriate wireless topologies and antennas to allow APs to pair with WLCs in an enterprise network.*
 - 18.1 Compare how APs operate in autonomous and lightweight mode.
 - 18.2 Explain how lightweight APs pair with WLCs.
 - 18.3 Select appropriate antennas for APs based on requirements.

Chapter 19. Understanding Wireless Roaming and Location Services

- *Explain how to configure a wireless network to support and manage wireless roaming.*
 - 19.1 Explain how mobile clients roam between autonomous APs and intracontrollers.
 - 19.2 Explain L2 and L3 roaming strategies.
 - 19.3 Describe techniques and business rationale for locating devices in a wireless network.

Chapter 20. Authenticating Wireless Clients

- *Compare different methods to authenticate wireless clients before gaining access to the wireless network.*
 - 20.1 Explain when wireless clients should Access a network using open authentication.
 - 20.2 Explain how to configure secure wireless connections on a WLAN using authentication with a pre-shared key.
 - 20.3 Explain how to configure secure wireless connections on a WLAN using authentication with EAP.
 - 20.4 Explain how to configure secure wireless connections on a WLAN using authentication with WebAuth.

Chapter 21. Troubleshooting Wireless Connectivity

- *Troubleshoot wireless connectivity issues using tools and strategies.*
 - 21.1 Troubleshoot connectivity issues with a single wireless client.
 - 21.2 Explain how to troubleshoot connectivity issues at the AP.

Chapter 22. Enterprise Network Architecture

- *Explain the characteristics of scalable network architectures.*
 - 22.1 Explain how data, voice, and video are converged in a switched network.
 - 22.2 Explain considerations for designing a scalable network.
 - 22.3 Explain how switch hardware features support network requirements.
 - 22.4 Describe the types of routers available for small-to-medium-sized business networks
 - 22.5 Describe the three layers of a hierarchical network and how they are used in network design.
 - 22.6 Explain how enterprise campus architectures can be used to scale from a small environment to a large campus-size network.

Chapter 23. Fabric Technologies

- *Explain how fabric networks allow traditional networks to be more manageable, flexible, secure, and scalable.*
 - 23.1 Explain how SD-Access is effective for configuration and maintenance in growing and ever-changing networks.
 - 23.2 Describe the two main components of SD-Access.
 - 23.3 Explain the functions of the four layers of SD-Access architecture.
 - 23.4 Describe the benefits of utilizing an SD-WAN.
 - 23.5 Describe Cisco's current solutions for SD-WAN.
 - 23.6 Explain how the SD-WAN Cloud ONRamp solution addresses optimal cloud SaaS application access and IaaS connectivity.

Chapter 24. Network Assurance

- *Troubleshoot an enterprise network using common tools and techniques.*
 - 24.1 Configure NetFlow to monitor traffic in a business network.
 - 24.2 Explain the features and characteristics of SPAN.
 - 24.3 Troubleshoot common and advanced network problems.
 - 24.4 Explain how to configure SPAN to capture packets on local switch ports.
 - 24.5 Compare the use of local SPAN and RSPAN.
 - 24.6 Explain how to configure ERSPAN to monitor traffic in one area of the network and route the SPAN traffic to a traffic analyzer in another area of the network.
 - 24.7 Use an ICMP echo-based IP SLA to troubleshoot network connectivity issues.
 - 24.8 Explain how Cisco DNA center enable intent-based networking.

Chapter 25. Secure Access Control

- *Compare secure solutions for different places in the network*
 - 25.1 Describe Cisco SAFE, a security architectural framework, that helps design secure solutions for PINs.
 - 25.2 Explain how to design endpoint security that will detect the rapidly evolving threats to organizations.
 - 25.3 Compare current and next generation network access control technologies.

Chapter 26. Network Device Access Control and Infrastructure Security

- *Configure network access control using tools and features that provide device and infrastructure security.*
- 26.1 Verify the functionality of a configured ACL in relation to the network topology.
- 26.2 Explain techniques that secure and control access to VTY lines on network devices.
- 26.3 Configure access control using the local database and AAA server.
- 26.4 Explain how to configure zone-based firewalls to provide stateful network security.
- 26.5 Configure ACLs with CoPP policies that protect the CPU from unexpected extreme rates of traffic.
- 26.6 Configure network devices with device hardening features to mitigate security threats.

Chapter 27. Virtualization

- *Explain the purpose and characteristics of network and server virtualization.*
- 27.1 Explain the importance of cloud computing.
- 27.2 Explain the importance of virtualization.
- 27.3 Describe the virtualization of network devices and services.
- 27.4 Describe software-defined networking.
- 27.5 Describe controllers used in network programming.
- 27.6 Explain how the Network Functions Virtualization (NFV) architectural framework decouples network functions from hardware-based appliances.

Chapter 28. Foundational Network Programmability Concepts

- *Explain common network programmability concepts and programmatic methods of management.*
- 28.1 Explain the pros and cons of using the CLI to manage devices on a network.
- 28.2 Explain how APIs enable computer to computer communications.
- 28.3 Describe tools and resources related to using APIs and REST functions.
- 28.4 Compare JSON and XML data formats.
- 28.5 Explain how Cisco DNA center enable intent-based networking.
- 28.6 Compare the use of vManage APIs to Cisco DNA Center APIs.
- 28.7 Describe data models and tools used in a programmatic approach.
- 28.8 Explain how DevNet encourages communities of network programmers.
- 28.9 Explain how GitHub tracks changes in your files and facilitates collaboration and code sharing.
- 28.10 Use Python to access and manipulate values in lists and dictionaries.

Chapter 29. Introduction to Automation Tools

- Explain the benefits and operation of various automation tools.
- 29.1 Explain how the Embedded Event Manager is used to automate configuration, troubleshooting, and data collection.
- 29.2 Compare the configuration management tools Puppet, Chef, Ansible, and SaltStack.

Rutas de Certificación CCNP



Certification paths

Professional and Specialist certifications

