



CURSO:
**CCNA 3 ENTERPRISE NETWORKING,
SECURITY, AND AUTOMATION**

70 HORAS



ÍNDICE

1. Descripción	3
2. Público objetivo.....	3
3. Objetivos de aprendizaje	3
<i>Objetivo general</i>	<i>3</i>
<i>Objetivos específicos:.....</i>	<i>3</i>
5. Competencias Previas	4
6. Recursos	4
7. Aspectos metodológicos	4
8. Contenidos del curso.....	5
<i>Unidad 1: Conceptos OSPFV2 SINGLE-AREA</i>	<i>5</i>
<i>Unidad 2: Configuración OSPFV2 SINGLE-AREA.....</i>	<i>5</i>
<i>Unidad 3: Conceptos de seguridad de red</i>	<i>5</i>
<i>Unidad 4: Conceptos de ACL</i>	<i>5</i>
<i>Unidad 5: ACL para la configuración de IPV4</i>	<i>6</i>
<i>Unidad 6: NAT para IPV4</i>	<i>6</i>
<i>Unidad 7: Conceptos de WAN.....</i>	<i>6</i>
<i>Unidad 8: Conceptos de VPN e IPsec.....</i>	<i>6</i>
<i>Unidad 9: Conceptos de QoS</i>	<i>6</i>
<i>Unidad 10: Administración de redes</i>	<i>6</i>
<i>Unidad 11: Diseño de la RED</i>	<i>7</i>
<i>Unidad 12: Solución de problemas de red</i>	<i>7</i>
<i>Unidad 13: Virtualización de RED</i>	<i>7</i>
<i>Unidad 14: Automatización de red</i>	<i>7</i>
9. Criterios de aprobación	7
10. Certificados de aprobación	8



1. Descripción

El presente curso permitirá a los participantes prepararse para iniciar una carrera en redes.

Este es el último de una serie de 3 cursos; el cual presenta temas de arquitectura, componentes, operaciones y seguridad a escala para redes grandes y complejas, incluidas las tecnologías de red de área extensa (WAN).

Este curso se encuentra organizado en catorce capítulos que ofrecen una cobertura integral y completa para aprender:

- Configurar, solucionar problemas y proteger dispositivos de red empresariales,
- Describir las tecnologías de red de área extensa (WAN) y los mecanismos de calidad de servicio (QoS) para el acceso remoto seguro, junto con la red definida por software
- Conceptos de virtualización y automatización que admiten la digitalización de redes.
- Comprender las interfaces de programación de aplicaciones (API) y las herramientas de administración de configuración.

También usted podrá desarrollar un pensamiento crítico y habilidades para resolver problemas mediante equipamientos reales y utilizar el simulador de Cisco llamado Packet Tracer.

Con esta capacitación le permitirá ser uno de las pocas personas que **conocerá cómo configurar y solucionar problemas de redes empresariales, e identificar y protegerse contra las amenazas de ciberseguridad.**

2. Público objetivo

El curso CCNA 3 ENTERPRISE NETWORKING, SECURITY está dirigido a todas las personas que estén interesadas en fortalecer sus conocimientos, habilidades y destrezas relacionadas con Tecnologías de la Información, Ingeniería Electrónica, Ingeniería en Sistemas o afines.

3. Objetivos de aprendizaje

Objetivo general

Adquirir conocimientos para configurar, solucionar problemas y asegurar dispositivos de red empresariales y entender cómo las interfaces de programación de aplicaciones (API) y las herramientas de programación de aplicaciones (API) y las herramientas de administración de configuración permiten la automatización de la red.

Objetivos específicos:

- Configurar OSPFv2 de área única en redes punto a punto y de acceso múltiple.
- Explicar cómo mitigar las amenazas y mejorar la seguridad de la red utilizando
- listas de control de acceso y mejores prácticas de seguridad.
- Implemente ACL IPv4 estándar para filtrar el tráfico y asegurar el acceso administrativo.
- Configure los servicios NAT en el enrutador perimetral para proporcionar escalabilidad de dirección IPv4.



- Indicar las técnicas para proporcionar escalabilidad de direcciones y acceso remoto seguro para WAN.
- Mostrar cómo optimizar, monitorear y solucionar problemas de arquitecturas de red escalables.
- Enseñar cómo los dispositivos de red implementan QoS.
- Implementar protocolos para administrar la red.
- Explique cómo las tecnologías como la virtualización, las redes definidas por software y la automatización afectan las redes en evolución.

4. Duración:

El curso tiene una duración de 70 horas, distribuidas en 50 horas en vivo y 20 horas de estudio autónomo para el desarrollo de actividades de aprendizaje de refuerzo en casa.

5. Competencias Previas

Conocimientos: Es recomendable que los participantes de este curso, hayan aprobado el módulo de CCNA 2 SWITCHING, ROUTING, AND WIRELESS ESSENTIALS o tener conocimientos y experiencia previa.

Habilidades o destrezas: Los participantes deben poseer habilidades para la resolución de problemas técnicos, capacidad de análisis y pensamiento crítico aplicados a redes y tecnologías de la información. Además, se valoran destrezas en la comunicación efectiva.

Valores: Es importante el establecimiento de criterios éticos respecto al manejo y evaluación de los comportamientos observables de las personas.

6. Recursos

- Disponer de una computadora, con sus periféricos bien configurados y funcionales (micrófono, parlantes y cámara).
- Disponer de una conexión estable a internet.
- Tener una cuenta de correo electrónico.
- Facilidad de acceso a la Plataforma NetAcad de CISCO

7. Aspectos metodológicos

La capacitación se desarrollará en la modalidad híbrida, con un componente de horas sincrónicas on line y horas asincrónicas para el estudio autónomo.

El curso se desarrolla totalmente desde internet, el Sistema de Gestión del Aprendizaje LMS Moodle; donde se realizan actividades teórico prácticas con un enfoque dinámico y participativo centrado en los y las participantes.

Los contenidos del curso estarán a su disposición las 24 horas del día y los 7 días de la semana dentro del tiempo establecido para la duración del curso, por lo que, todos los participantes pueden organizar su propio horario de estudio.



Se realizarán actividades sincrónicas y asincrónicas a través de herramientas de comunicación como: vídeo conferencias, chat, foros, mensajería interna, entre otras; que son empleadas por el Facilitador para mediar el aprendizaje. El seguimiento tutorial efectuado será constante y proactivo; lo que garantiza el éxito en el proceso de aprendizaje de los participantes.

El curso es teórico – práctico, por cuanto el estudiante se apoyará en la plataforma de NetAcad, para lo cual se creará un nombre de usuario y contraseña para el acceso.

Cada día se presentan contenidos que son estructurados con actividades individuales y colaborativas, recursos complementarios y herramientas que estarán disponibles en formatos para navegar.

8. Contenidos del curso

Unidad 1: Conceptos OSPFV2 SINGLE-AREA

- 1.1. OSPF Features and Characteristics
- 1.2. Características y características de OSPF
- 1.3. Paquetes OSPF
- 1.4. Operación OSPF

Unidad 2: Configuración OSPFV2 SINGLE-AREA

- 2.1. ID de enrutador OSPF
- 2.2. Redes OSPF Point-to-Point
- 2.3. Redes OSPF de acceso múltiple
- 2.4. Modificar OSPFv2 Single-Área
- 2.5. Propagación de ruta predeterminada
- 2.6. Verificar OSPFv2 Single-Área

Unidad 3: Conceptos de seguridad de red

- 3.1. Estado actual de ciberseguridad
- 3.2. Actores de amenaza
- 3.3. Herramientas para actores de amenazas
- 3.4. Malware
- 3.5. Ataques de red comunes
- 3.6. Vulnerabilidades y amenazas de IP
- 3.7. Vulnerabilidades de TCP y UDP
- 3.8. Servicios de IP
- 3.9. Mejores prácticas de seguridad de red
- 3.10. Criptografía

Unidad 4: Conceptos de ACL

- 4.1. Propósito de las ACL
- 4.2. Máscaras Wildcard en ACL



4.3. Pautas para la creación de ACL

4.4. Tipos de ACL IPv4

Unidad 5: ACL para la configuración de IPV4

5.1. Configurar ACL IPv4 estándar

5.2. Modificar las ACL de IPv4

5.3. Puertos VTY seguros con una ACL IPv4 estándar

5.4. Configurar las ACL IPv4 extendidas

Unidad 6: NAT para IPV4

6.1. Características de NAT

6.2. Tipos de NAT

6.3. Ventajas y desventajas de NAT

6.4. NAT estático

6.5. NAT dinámico

6.6. PAT

6.7. NAT 64

Unidad 7: Conceptos de WAN

7.1. Propósito de las WAN

7.2. Operaciones WAN

7.3. Conectividad WAN tradicional

7.4. Conectividad WAN moderna

7.5. Conectividad basada en internet

Unidad 8: Conceptos de VPN e IPsec

8.1. Tecnología VPN

8.2. Tipos de VPN

8.3. IPsec

Unidad 9: Conceptos de QoS

9.1. Calidad de transmisión de red

9.2. Características del tráfico

9.3. Algoritmos de cola

9.4. Modelos de QoS

9.5. Técnicas de implementación de QoS

Unidad 10: Administración de redes

10.1. Descubrimiento de dispositivos con CDP

10.2. Descubrimiento de dispositivos con LLDP

10.3. NTP

10.4. SNMP

10.5. Syslog

10.6. Mantenimiento de enrutadores y conmutadores

10.7. Administración de la imagen del IOS



Unidad 11: Diseño de la RED

- 11.1. Redes jerárquicas
- 11.2. Redes escalables
- 11.3. Switch Hardware
- 11.4. Router Hardware

Unidad 12: Solución de problemas de red

- 12.1. Documentación de red
- 12.2. Proceso de resolución de problemas
- 12.3. Herramientas de solución de problemas
- 12.4. Síntomas y causas de problemas de red
- 12.5. Solucionar problemas de conectividad IP

Unidad 13: Virtualización de RED

- 13.1. Computación en la nube
- 13.2. Virtualización
- 13.3. Infraestructura de red virtual
- 13.4. Redes definidas por software
- 13.5. Controladores

Unidad 14: Automatización de red

- 14.1. Resumen de automatización
- 14.2. Formatos de datos
- 14.3. APIs
- 14.4. REST
- 14.5. Herramientas de administración y configuración
- 14.6. IBN y Cisco DNA Center

9. Criterios de aprobación

Aprobar los exámenes electrónicos por capítulo, estos exámenes pueden presentarlos con base en la planificación académica del instructor en el horario de las clases presenciales o fuera de ellas.

Prácticas de laboratorio por cada capítulo y práctica final (skills).

- Examen Final Teórico
- Examen Final Práctico
- Examen Feedback (Satisfacción del Cliente)

Todas las evaluaciones son calificadas sobre 100 puntos, por lo que para aprobar cada uno de los módulos el participante debe obtener una nota promedio de todas las evaluaciones descritas de 70/100 puntos y registrar una asistencia mínima del 70% a las sesiones presenciales.



10. Certificados de aprobación

El participante que cumpla con los criterios de aprobación, recibirá un certificado con el **aval** **CISCO NETWORKING ACADEMY y ESPE - INNOVATIVA E.P.**

¡Actualice sus competencias profesionales con nosotros!