

EDUCACIÓN 

**Redes empresariales,
seguridad y automatización
CCNA3 V7**

Programa de Estudio

Redes empresariales, seguridad y automatización CCNA3 V7

Diseña redes escalables y automatizadas para cualquier empresa u organización. Domina las últimas herramientas en seguridad para blindar tus redes.

Contenido del curso

Comenzaremos aprendiendo a analizar y configurar el protocolo de enrutamiento OSPF, para tener una visión más amplia de cómo nuestros datos son dirigidos por las mejores rutas disponibles en la red. Veremos conceptos como seguridad de redes, automatización, virtualización y troubleshooting tanto de forma teórica, como de forma práctica, en donde el estudiante obtendrá las habilidades necesarias que solicitan hoy en día muchas empresas para los puestos de administradores y analistas de red.

El Curso de Redes Empresariales, Seguridad y Automatización ofrece las mejores prácticas que se deben de tener en cuenta al momento de realizar tareas en una infraestructura de red. También analizaremos los entornos modernos de red para entender cuál es la mejor forma de llevar a cabo su gestión siguiendo conceptos tan claves como lo son la escalabilidad, disponibilidad, seguridad y QoS.

PRÁCTICAS EN CLASE ::

En este módulo los estudiantes usarán la herramienta Packet Tracer para proponer diseños de red y realizar prácticas que resuelvan problemas en determinados escenarios. También haremos prácticas en entornos virtuales para entender las ventajas de tener un entorno virtualizado y así reducir los costos de implementación de servicios.

Requisitos

Es recomendable contar con conocimientos en Generales de Redes o haber realizado el curso de

Curso de Fundamentos de Redes CCNA1 y el curso de Curso de Fundamentos de Enrutamiento y Conmutación CCNA2

Modalidad de cursado

Puedes tomar este curso en modalidad presencial o modalidad online - en vivo

¿Qué aprenderás?

- Fundamentos OSPF
- Paquetes y componentes
- Configuración avanzada OSPF
- Fundamentos de la seguridad en redes
- Tipos de ataques y Malwares
- Análisis de vulnerabilidades
- Uso de procesos criptográficos
- Trabajar con ACLs
- Configuraciones NAT para IPv4
- Arquitectura Redes WAN y VPNs
- Quality of Service (QoS)
- Utilización de Algoritmos de colas
- Técnicas de administración y diseño red
- Troubleshooting de Red
- Métodos de solución de problemas
- Enfoque sistemático de capas
- Virtualización de redes
- Redes automatizadas

Plan de Estudios

A close-up photograph of two men in business attire. The man on the left, wearing glasses and a blue suit with a striped tie, is looking down at a tablet. The man on the right, also in a blue suit, is smiling and pointing at the tablet with a pen. The background is bright and out of focus, suggesting an office environment.

1. OSPF

Definición y características del protocolo OSPF.

Componentes de OSPF.

Paquetes OSPF.

Descripción de las actualizaciones LSA.

Análisis de paquetes de saludo para establecimiento de vecinos.

Topologías multiacceso y definición de DR y BDR

OSPFv3

2. Configuración de OSPF

Configuración de una ID de enrutador OSPFv2.

Configuración de OSPFv2 de área única en una red punto a punto.

Configurar la prioridad de la interfaz OSPF para influir en la elección DR / BDR en una red de acceso múltiple.

Modificaciones para cambiar la operación de OSPFv2 de área única.

Configurar OSPF para propagar una ruta predeterminada.

Verificación de una implementación de OSPFv2 de área única.

3. Concepto de seguridad en redes

Describir las herramientas utilizadas por los actores de amenazas para explotar las redes.

Tipos de malware.

Tipos de ataques de red.

Analizar cómo los agentes de amenazas explotan las vulnerabilidades de IP.

Cómo los actores de amenazas explotan las vulnerabilidades TCP y UDP.

Cómo los servicios de IP son explotados por los actores de amenazas.

Mejores prácticas para proteger una red.

Procesos criptográficos comunes utilizados para proteger los datos en tránsito.

4. ACLs y configuración

Explicar cómo las ACL filtran el tráfico.
Uso de las máscaras comodín.
Explicar cómo crear ACL.
Comparación de las ACL IPv4 estándar y extendidas.
Verificación de las ACLs.

5. NAT para IPv4

Funcionamiento de diferentes tipos de NAT.
Describa las ventajas y desventajas de NAT.
Configurar NAT estática usando la CLI.
Configurar NAT dinámica usando la CLI.
Configure PAT usando la CLI.
Descripción de NAT para IPv6.

6. Redes WAN y VPNs

Propósito de una WAN.
Funcionamiento de una red WAN.
Opciones de conectividad WAN tradicionales.
Opciones modernas de conectividad WAN.
Opciones de conectividad basadas en internet.
Beneficios de la tecnología VPN.
Diferentes tipos de VPN.
Cómo se usa el marco IPsec para proteger el tráfico de red.
Definición y configuración de IPsec

7. QoS.

Explicar cómo las características de transmisión de la red impactan en la calidad.
Algoritmos de colas utilizados por los dispositivos de red.
Describa los diferentes modelos de QoS.
Explicar cómo QoS utiliza mecanismos para garantizar la calidad de la transmisión.

8. Administración y diseño de redes

CDP para mapear una topología de red.

LLDP para mapear una topología de red.

Implementación de NTP entre un cliente NTP y un servidor NTP.

Funcionamiento de SNMP.

Operación de syslog.

Comandos para hacer una copia de seguridad y restaurar un archivo de configuración de IOS.

Implementación de protocolos para administrar la red.

Cómo los datos, la voz y el video convergen en una red conmutada.

Consideraciones para diseñar una red escalable.

Cómo las características de hardware del conmutador admiten los requisitos de red.

Tipos de enrutadores disponibles para redes de pequeñas y medianas empresas.

9. Troubleshooting de red

Explicar cómo se desarrolla y se usa la documentación de red para solucionar problemas de red.

Métodos de solución de problemas que utilizan un enfoque sistemático en capas.

Herramientas de solución de problemas de redes.

Detectar los síntomas y causas de los problemas de red utilizando un modelo en capas.

Solucionar problemas de una red utilizando el modelo en capas.

10. Virtualización de redes

Importancia de la computación en la nube.

Importancia de la virtualización.

Describe la virtualización de dispositivos y servicios de red.

Redes definidas por software.

Controladores utilizados en la programación de red.

11. Redes automatizadas

Formatos de datos JSON, YAML y XML.

Cómo las API permiten las comunicaciones de computadora a computadora.

Cómo REST habilita las comunicaciones de computadora a computadora.

Compare las herramientas de gestión de configuración Puppet, Chef, Ansible y SaltStack.

Explicar cómo Cisco DNA Center permite la creación de redes basadas en la intención.

EDUCACIÓN IT

Centro de Capacitación y Desarrollo Profesional



Lavalle 648 Piso 8, Microcentro, CABA

TEL_PRINCIPAL

info@educacionit.com

EducaciónIT. Copyright 2005-2021