CCNA R&S

Objetivo: La currícula de CCNA Routing and Switching (CCNA v5), está diseñada para estudiantes interesados en el aprendizaje de las nuevas tecnologías de la información y comunicación. Aporta algunos de los elementos más representativos de las redes, desde conceptos fundamentales hasta avanzadas aplicaciones y servicios; ofrece, además, la oportunidad de realizar prácticas que ayudan al desarrollo de habilidades esenciales para un profesional de las redes.

CCNA Routing and Switching enseña conceptos de red, desde sus aplicaciones hasta protocolos y servicios realizados para las capas más bajas de la red. Los estudiantes aprenden desde conceptos básicos, hasta complejos sistemas de modelado teóricos

MÓDULO I

INTRODUCCIÓN A LAS REDES

CAPITULO 1:

EXPLORACIÓN DE LA RED

1.1 Conectados globalmente
- 1.1.1 Las redes en la actualidad
- 1.1.2 Provisión de recursos en una red

1.2 LAN, WAN e Internet
- 1.2.1 Componentes de las redes
- 1.2.2 LAN y WAN
- 1.2.3 Internet
- 1.2.4 Conexión a Internet

1.3 La red como plataforma
- 1.3.1 Redes convergentes
- 1.3.2 Red confiable

1.4 El cambiante entorno de red
- 1.4.2 Tecnologías de red para el hogar
- 1.4.3 Seguridad de red para el hogar
- 1.4.4 Seguridad de red
- 1.4.5 Arquitecturas de red

CAPITULO 2:

CONFIGURACION DE UN SISTEMA OPERATIVO DE LA RED

2.1 Entrenamiento intensivo sobre IOS
- 2.1.1 CISCO IOS
- 2.1.2 Acceso a un dispositivo CISCO IOS
- 2.1.3 Navegación de IOS
- 2.1.4 Estructura de comandos

2.2 Información básica
- 2.2.1 Nombres de host
- 2.2.2 Limitación del acceso a las configuraciones de los dispositivos
- 2.2.3 Cómo guardar configuraciones

2.3 Esquema de direcciones
- 2.3.1 Puertos y direcciones
- 2.3.2 Direccionamiento de dispositivos
- 2.3.3 Verificación de la conectividad

CAPITULO 3:

PROTOCOLOS Y COMUNICACIONESDE LA RED

3.1 Reglas de la comunicación
- 3.1.1 Las reglas

3.2 Protocolos y estándares de la red
- 3.2.1 Protocolos
- 3.2.2 Suites de protocolos
- 3.2.3 Organismos de estandarización
- 3.2.4 Modelos de referencia

3.3 Movimiento de datos en la red
- 3.3.1 Encapsulación de datos
- 3.3.2 Acceso a los recursos locales
- 3.3.3 Acceso a recursos remotos
- 3.3.4

CAPITULO 4:

ACCESO A LA RED

4.1 Protocolos de capa física
- 4.1.1 Como realizar la conexión
- 4.1.2 Propósito de la capa física
- 4.1.3 Principios fundamentales de la capa 1

4.2 Medios de red
- 4.2.1 Cableado de cobre
- 4.2.2 Cableado UTP
- 4.2.3 Cableado de fibra óptica
- 4.2.4 Medios inalámbricos

4.3 Protocolos de la capa de enlace de datos
- 4.3.1 Propósito de la capa de enlace de datos
- 4.3.2 Estructura de trama de la capa 2
- 4.3.3 Estándares de la capa 2

4.4 Control de acceso al medio
- 4.4.1 Topologías
- 4.4.2 Topologías de WAN
- 4.4.3 Topologías de LAN
- 4.4.4 Trama de enlace de datos

CAPITULO 5:

ETHERNET

5.1 Protocolo Ethernet
- 5.1.1 Funcionamiento de Ethernet
- 5.1.2 Atributos de la trama de Ethernet
- 5.1.3 MAC de Ethernet
- 5.1.4 MAC e IP

5.2 Protocolo de resolución de direcciones
- 5.2.1 ARP
- 5.2.2 Problemas de ARP

5.3 Switches LAN
- 5.3.1 Conmutación
- 5.3.2 Fija o modular
- 5.3.3 Conmutación de capa 3

CAPITULO 6:

CAPA DE RED

6.1 Protocolos de la capa de red
- 6.1.2 Características del protocolo IP
- 6.1.3 Paquete IPv4
- 6.1.4 Paquete IPv6

6.2 Enrutamiento
- 6.2.2 Tablas de enrutamiento en router

6.3 Routers
- 6.3.1 Anatomía de un router
- 6.3.2 Arranque del router

6.4 Configuración de un router CISCO
- 6.4.1 Configuración inicial
- 6.4.2 Configuración de interfaces
- 6.4.3 Configuración del gateway predeterminado

CAPITULO 7:

CAPA DE TRANSPORTE

7.1 Protocolos de la capa de transporte
- 7.1.1 Transporte de datos
- 7.1.2 Introducción a TCP y UDP

7.2 TCP y UDP
- 7.2.1 Comunicación TCP
- 7.2.2 Confiabilidad y control del flujo
- 7.2.3 Comunicación UDP

CAPITULO 8:

ASIGNACIÓN DE DIRECCIONES IP

8.1 Direcciones de IPv4
- 8.1.1 Estructura de la dirección IPv4
- 8.1.2 Máscara de subred IPv4
- 8.1.3 Direcciones Ipv4 unicast, broadcast y multicast
- 8.1.4 Tipos de direcciones IPv4

8.2 Asignación de direcciones IPv6
- 8.2.1 Problemas de IPv4
- 8.2.2 Asignación de direcciones IPv6
- 8.2.3 Tipos de direcciones Ipv6
- 8.2.4 Direcciones Ipv6 unicast
- 8.2.5 Direcciones ipv6 multicast

8.3 Verificación de conectividad
- 8.3.1 ICMP
- 8.3.2 Prueba y verificación

CAPITULO 9:

DIVISION DE REDES IP EN SUBREDES

9.1 División de un red Ipv4
- 9.1.1 Segmentación de red
- 9.1.2 La división de una red Ipv4 en subredes
- 9.1.3 Determinación de la máscara de subred
- 9.1.4 Beneficios de la máscara de subred de longitud variable

9.2 Esquemas de direccionamiento
- 9.2.1 Diseño estructurado

9.3 Consideraciones de diseño para Ipv6
- 9.3.1 División en subredes de una Ipv6

CAPITULO 10:

CAPA DE APLICACIÓN

10.1 Protocolos de la capa de aplicación
- 10.1.1 Aplicación, sesión y presentación
- 10.1.2 Como interactuan los protocolos con las aplicaciones de usuario final

10.2 Protocolos y servicios de capa de aplicación reconocidos
- 10.2.1 Protocolos de capa de aplcación mas comunes
- 10.2.2 Provisión de servicios de direccionamiento ip
- 10.2.3 Provisión de servicios de intercambio de archivos

CAPITULO 11:

ES UNA RED

11.1 Crear y crecer
- 11.1.1 Dispositivos de una red pequeña
- 11.1.2 Protocolos en redes pequeñas
- 11.1.3 Crecimiento hacia redes mas grandes

11.2 Como mantener la seguridad de la red
- 11.2.1 Medidas de seguridad para dispositivos de red
- 11.2.2 Vulnerabilidades y ataques de red
- 11.2.3 Mitigación de ataques de red
- 11.2.4 Protección de dispositivos

11.3 Rendimiento básico de la red
- 11.3.1 Los comandos
- 11.3.2 Tracert
- 11.3.3 Comandos show
- 11.3.4 Host y comandos de IOS

11.4 Administración de los arcuivos de configuración de IOS
- 11.4.1 Sistemas de archivos del router y del switch
- 11.4.2 Creación de copias de seguridad y restauración de archivos de configuración

11.5 Servicios de enrutamiento integrados
- 11.5.1 Router integrado
- 11.5.2 Configuración de router integrado

MODULO II

PRICIPIOS BÁSICOS DE ROUTING & SWITCHING

CAPITULO 1:

INTRODUCCIÓN A REDES CONMUTADAS

1.1 Diseño LAN
- 1.1.1 Redes convergentes
- 1.1.2 redes conmutadas

1.2 El entorno conmutado
- 1.2.1 Reenvío de tramas
- 1.2.2 Dominios de switching

CAPITULO 2:

CONFIGURACIÓN Y CONCEPTOS BÁSICOS DE SWITCHING

2.1 Configuración básica de switch
- 2.1.1 Configuración de parámetros iniciales de un switch
- 2.1.2 Configuración de puertos de un switch

2.2 Seguridad de switches
- 2.2.1 Acceso remoto seguro
- 2.2.2 Cuestiones de seguridad en redes LAN
- 2.2.3 Prácticas recomendadas de seguridad
- 2.2.4 Seguridad de puertos de switch

CAPITULO 3:

VLAN

3.1 Segmentación de VLAN
- 3.1.1 Descripción general de las VLAN
- 3.1.2 Redes VLAN en un entorno conmutado múltiple

3.2 Implementación de VLAN
- 3.2.1 Asignación de red VLAN
- 3.2.2 Enlaces troncales de la VLAN
- 3.2.3 Protocolo de enlace troncal dinámico
- 3.2.4 Resolución de problemas de VLAN y enlaces troncales

3.3 Seguridad y diseño de redes VLAN
- 3.3.1 Ataques a redes VLAN
- 3.3.2 Prácticas recomendadas de diseño para las VLAN

CAPITULO 4:

CONCEPTOS DE ROUTING

4.1 Configuración inicial de un router
- 4.1.1 Funciones de un router
- 4.1.2 Conexión de los dispositivos
- 4.1.3 Configuración básica de un router
- 4.1.4 Verificación de la conectividad de redes conectadas directamente

4.2 Decisiones de routing
- 4.2.1 Switching de paquetes entre redes
- 4.2.2 Determinación de ruta

4.3 Funcionamiento del router
- 4.3.1 Análisis de la tabla de routing
- 4.3.2 Rutas conectadas directamente
- 4.3.3 Rutas descubiertas estáticamente
- 4.3.4 Protocolos de enrutamiento dinámico

CAPITULO 5:

ENRUTAMIENTO ENTRE VLAN

5.1 Configuración del routing entre VLAN
- 5.1.1 Funcionamiento del routing entre VLAN
- 5.1.2 Configuración de routing entre VLAN antiguo
- 5.1.3 Configurar un enrutamiento router-on-a-stick entre VLAN

5.2 Resolución de problemas de routing entre VLAN
- 5.2.1 Problemas de configuración entre VLAN
- 5.2.2 Problemas de direccionamiento IP

5.3 Conmutación de capa 3
- 5.3.1 Funcionamiento y configuración del switching de capa 3
- 5.3.2 Resolución de problemas de switching de capa 3

CAPITULO 6:

ENRUTAMIENTO ESTÁTICO

6.1 Implementación del routing estático
- 6.1.1 Enrutamiento estático
- 6.1.2 Tipos de rutas estáticas

6.2 Configuración de las rutas estáticas y predeterminadas
- 6.2.1 Configuración de rutas estáticas Ipv4
- 6.2.2 Configuración de rutas predeterminadas Ipv4
- 6.2.3 Configuración de rutas estáticas Ipv6
- 6.2.4 Configuración de rutas Ipv6 predeterminadas

6.3 Revisión de CIDR y VLSM
- 6.3.1 Direccionamiento con clase
- 6.3.2 CIDR
- 6.3.3 VLSM

6.4 Configuración de rutas resumidas Ipv4
- 6.4.1 Configuración de rutas resumidas Ipv4
- 6.4.2 Configuración de rutas resumidas Ipv6
- 6.4.3 Configuración de rutas estáticas flotantes

CAPITULO 7:

ROUTING DINÁMICO

7.1 Protocolos de enrutamiento dinámico
- 7.1.1 Funcionamiento del protocolo de enrutamiento dinámico
- 7.1.2 Tipos de protocolos de routing

7.2 Routing dinámico vector distancia
- 7.2.1 Funcionamiento del protocolo de enrutamiento vector distancia
- 7.2.2 Tipos de protocolos de enrutamiento vector distancia

7.3 Routing dinámico de estado enlace
- 7.3.1 Actualizaciones de estado de enlace

7.3.2 Razones para utilizar protocolos de routing de estado enlace

7.4 La tabla de routing

7.4.1 La tabla de routing

7.4.2 Rutas ipv4 descubiertas en forma dinámica

7.4.3 Proceso de búsqueda de rutas Ipv4

7.4.4 Análisis de una tabla de routing de Ipv6

CAPITULO 8:

OSPF DE AREA UNICA

8.1 Características de OSPF

8.1.1 OSPF

8.1.2 Mensajes de OSPF

8.1.3 Funcionamiento de OSPF

8.2 Configuración de OSPFv2 de área única

8.2.1 ID del router OSPF

8.2.2 Configuración de OSPFv2 de área única

8.2.3 Costo OSPF

8.2.4 Verificación de OSPF

8.3 Configuración de OSPF v3 de área única

8.3.1 Configuración de OSPFv3

8.3.2 Verificación de OSPFv3

CAPITULO 9:

LISTAS DE CONTROL DE ACCESO

9.1 Funcionamiento de ACL de IP

9.1.1 Propósito de los ACLs

9.1.2 Comparación entre ACL de Ipv4 estándar y extendidas

9.1.3 Máscaras wildcard en ACL

9.1.4 Pautas para la creación de ACL

9.1.5 Pautas para la colocación de ACL

9.2 ACL de Ipv4 estándar

9.2.1 Configuración de ACL Ipv4 estándar

9.2.2 Modificación de ACL de Ipv4

9.2.3 Protección de puertos VTY con una ACL de Ipv4 estándar

9.3 ACL de Ipv4 extendidas

9.3.1 Estructura de una ACL de Ipv4 extendida

9.3.2 Configuración de ACL de Ipv4 extendida

9.4 Resolución de problemas de ACL

9.4.1 Procesamiento de paquetes con ACL

9.4.2 Errores comunes de ACL

9.4.3

9.5 ACL de Ipv6

9.5.1 Creación de ACL de Ipv6

9.5.2 Configuración de ACL de Ipv6

CAPITULO 10:

DHCP

10.1 Protocolo de configuración dinámica de host v4
- 10.1.1 Funcionamiento de DHCPv4
- 10.1.2 Configuración de un servidor de DHCPv4 básico
- 10.1.3 Configuración de cliente DHCPv4
- 10.1.4 Resolución de problemas de DHCPv4

10.2 Protocolo de configuración dinámica de host v6
- 10.2.1 SLAAC y DHCP v6
- 10.2.2 DHCPv6 sin estado
- 10.2.3 Servidor DHCPv6 con estado
- 10.2.4 Resolución de problemas de DHCPv6

CAPITULO 11:

TRADUCCIÓN DE DIRECCIONES DE RED PARA IPv4

11.1 Funcionamiento de NAT
- 11.1.1 Características de NAT
- 11.1.2 Tipos de NAT
- 11.1.3 Beneficios de NAT

11.2 Configuración de NAT
- 11.2.1 Configuración de NAT estática
- 11.2.2 Configuración de NAT dinámica
- 11.2.3 Configuración de la traducción de la dirección del puerto (PAT)
- 11.2.4 Reenvío de puertos
- 11.2.5 Configuración de NAT e Ipv6

11.3 Resolución de problemas de NAT

MÓDULO III

ESCALAMIENTO DE REDES

CAPITULO 1:

INTRODUCCIÓN AL ESCALAMIENTO DE REDES

1.1 Implementación de un diseño de red
- 1.1.1 Diseño jerárquico de la red
- 1.1.2 Expansión de la red

1.2 Selección de dispositivos dered
- 1.2.1 Hardware del Switch
- 1.2.2 Hardware de routers
- 1.2.3 Administración de dispositivos

CAPITULO 2:

REDUNDANCIA DE LAN

2.1 Conceptos de árbol de expansión
- 2.1.1 Propósito de árbol de expansión
- 2.1.2 Funcionamiento de STP

2.2 Variedades de protocolos de árbol de expansión
- 2.2.1 Descripción general
- 2.2.2 PVST +
- 2.2.2 PVST + rápido

2.3 Configuración de árbol de expansión
- 2.3.1 Configuración de PVST +
- 2.3.2 Configuración rápida de PVST +
- 2.3.3 Problemas de configuración de STP

2.4 Protocolos de redundancia de primer salto
- 2.4.1 Concepto de protocolos de redundancia de primer salto
- 2.4.2 Variedades de protocolos de redundancia de primer salto
- 2.4.3 Verificación de FHRP

CAPITULO 3:

AGREGACIÓN DE ENLACES

3.1 Concepto de agregado de enlaces
- 3.1.1 Agregación de enlaces
- 3.1.2 Funcionamiento de EtherChannel

3.2 Configuración del agregado de enlaces
- 3.2.1 Configuración de EtherChannel
- 3.2.2 Verificación y resolución de problemas de EtherChannel

CAPITULO 4:

LAN INALAMBRICAS

4.1 Conceptos de tecnología inalámbrica
- 4.1.1 Introducción a la tecnología inalámbrica
- 4.1.2 Componentes de WLANs
- 4.1.3 Topologías de WLAN 802.11

4.2 Operaciones de LAN Inalámbrica
- 4.2.1 Estructura de tramas de 802.11
- 4.2.2 Operación Inalámbrica
- 4.2.3 Administración de canales

4.3 Seguridad de una LAN Inalámbrica
- 4.3.1 Amenazas de WLAN
- 4.3.2 Protección de WLAN

4.4 Configuración de LAN inalámbricas
- 4.4.1 Configuración de un router inalámbrico
- 4.4.2 Configuración de clientes inalámbricos
- 4.4.3 Resolución de problemas de WLAN

CAPITULO 5:

AJUSTE Y RESOLUCIÓN DE PROBLEMAS DE OSPF DE AREA UNICA

5.1 Configuraciones avanzadas de OSPF de área única
- 5.1.1 Routing en las capas de distribución y de núcleo
- 5.1.2 OSPF en redes de accesos múltiples
- 5.1.3 Propagación de rutas predeterminadas
- 5.1.4 Ajuste de las interfaces OSPF
- 5.1.5 OSPF segura

5.2 Resolución de problemas de implementaciónes de OSPF de área única
- 5.2.1 Componentes de la resolución de problemas de OSPF de área única
- 5.2.2 Resolución de problemas de routing de OSPFv2 de área única
- 5.2.3 Resolución de problemas de routing de OSPFv3 de área única

CAPITULO 6:

OSPF MULTIAREA

6.1 Funcionamiento de OSPF multiárea
- 6.1.1 ¿Por qué OSPF de diversas áreas?
- 6.1.2 Funcionamiento de LSA de OSPF multiárea
- 6.1.3 Tabla de routing y tipos de rutas OSPF

6.2 Configuración de OSPF de diversas áreas
- 6.2.1 Resumen de rutas OSPF
- 6.2.2 Verificación de OSPF de diversas áreas

CAPITULO 7:

EIGRP

7.1 Características de EIGRP
- 7.1.1 Características básicas de EIGRP
- 7.1.2 Tipos de paquetes EIGRP
- 7.1.3 Mensajes de EIGRP

7.2 Configuración de EIGRP para IPv4
- 7.2.1 Configuración de EIGRP con IPv4
- 7.2.2 Verificación de EIGRP con IPv4

7.3 Funcionamiento de EIGRP
- 7.3.1 Detección inicial de rutas EIGRP
- 7.3.2 Métricas
- 7.3.3 DUAL y la tabla de topología
- 7.3.4 DUAL y la convergencia

7.4 Configuración de OSPF para IPv6
- 7.4.1 Comparación entre EIGRP para IPv4 e IPv6
- 7.4.2 Configuración de EIGP para IPv6
- 7.4.3 Verificación de EIGRP para IPv6

CAPITULO 8:

CONFIGURACIONES AVANZADAS Y RESOLUCIÓN DE PROBLEMAS DE EIGRP

8.1 Configuraciones avanzadas de EIGRP
- 8.1.1 Sumarización automática
- 8.1.2 Sumarización manual
- 8.1.3 Propagación de rutas predeterminadas
- 8.1.4 Ajuste de interfaces EIGRP
- 8.1.5 EIGRP segura

8.2 Resolución de problemas de EIGRP
- 8.2.1 Componentes de la resolución de problemas de EIGRP
- 8.2.2 Resolver problemas de vecinos de EIGRP
- 8.2.3 Resolver problemas de tabla de routing EIGRP

CAPITULO 9:

IMAGENES Y LICENCIAS DEL IOS

9.1 Administración de archivos del sistema IOS
- 9.1.1 Convenciones de nomenclatura
- 9.1.2 Administración de imágenes del IOS de Cisco

9.2 Licencias del IOS
- 9.2.1 Licencia de software
- 9.2.2 Verificación y administración de licencias

MODULO IV

CONEXIÓN DE REDES

CAPITULO 1:

DISEÑO JERARQUICO DE LA RED

1.1 Descripción general del diseño de redes jerárquicas
- 1.1.1 Diseño de campus de red empresarial
- 1.1.2 Diseño jerárquico de la red

1.2 Arquitectura empresarial de CISCO
- 1.2.1 Diseño de red modular
- 1.2.2 Modelo de arquitectura empresarial CISCO

1.3 Arquitecturas de red en evolución
- 1.3.1 Arquitecturas empresariales de red emergentes
- 1.3.2 Arquitecturas de red emergentes

CAPITULO 2:

CONEXION A LA WAN

2.1 Descripción general de las tecnologías WAN
- 2.1.1 Propósito de los WANs
- 2.1.2 Operaciones WAN

2.2 Elección de una tecnología WAN
- 2.2.1 Servicios WAN
- 2.2.2 Infraestructuras WAN privadas
- 2.2.3 Infraestructuras WAN públicas
- 2.2.4 Elección de servicios WAN

CAPITULO 3:

POINT-TOPOINT CONNECTION (CONEXIONES PSTN)

3.1 Descripción general de conexión serial punto a punto
- 3.1.1 Comunicaciones seriales
- 3.1.2 Encapsulación HDLC

3.2 Funcionamiento de PPP
- 3.2.1 Ventajas de PPP
- 3.2.2 LCP y NCP
- 3.2.3 Sesiones para PPP

3.3 Configuración de PPP
- 3.3.1 Configuración de PPP
- 3.3.2 Autenticación de PPP

3.4 Resolver problemas de conectividad de PPP
- 3.4.1 Resolución de problemas de PPP

CAPITULO 4:

FRAME RELAY

4.1 Introducción a Frame Relay
- 4.1.1 Beneficios de Frame-Relay
- 4.1.2 Operación de Frame Relay

4.2 Configurar Frame Relaay
- 4.2.1 Configuración básica de Frame Relay
- 4.2.2 Configuración de subinterfaces

4.3 Resolución de problemas de conectividad
- 4.3.1 Resolución de problemas de Frame Relay

CAPITULO 5:

TRADUCCIÓN DE DIRECCIONES DE RED PARA IPv4

5.1 Funcionamiento de NAT
- 5.1.1 Características de NAT
- 5.1.2 Tipos de NAT
- 5.1.3 Beneficios de NAT

5.2 Configuración de NAT
- 5.2.1 Configuración de NAT estática
- 5.2.2 Configuración de NAT dinámica
- 5.2.3 Configuración de la traducción de la dirección del puerto (PAT)

CAPITULO 6:

CONECTIVIDAD DE SITE-TO-SITE

6.1 VPN
- 6.1.1 Aspectos básicos de las VPN
- 6.1.2 tipos de VPN

6.2 Túneles GRE Site-to-Site
- 6.2.1 Aspectos básicos de la encapsulación de routing genérico
- 6.2.2 Configuración de túneles GRE

6.3 Presentación de Ipsec
- 6.3.1 Seguridad de protocolo de Internet
- 6.3.2 Estructura Ipsec

6.4 Acceso remoto
- 6.4.1 Soluciones VPN de acceso remoto
- 6.4.2 VPN de acceso remoto con Ipsec

CAPITULO 7:

SUPERVISION DE LA RED

7.1 SYSLOG
- 7.1.1 Funcionamiento de syslog
- 7.1.2 Configuración de syslog

7.2 SNMP
- 7.2.1 Funcionamiento de SNMP
- 7.2.2 Configuración de SNMP

7.3 NetFlow
- 7.3.1 Funcionamiento de NetFlow
- 7.3.2 Configuración de NetFlow
- 7.3.3 Análisis de patrones de tráfico

CAPITULO 8:

RESOLUCIÓN DE PROBLEMAS DE RED

9.1 Resolución de problemas mediante un enfoque sistemático
- 9.1.1 Documentación de red
- 9.1.2 Proceso de resolución de problemas
- 9.1.3 Aislamiento del rpobelma mediante modelos de capas

9.2 Resolución de problemas de red
- 9.2.1 Herrmaientas para la resolución de problemas
- 9.2.2 Sintomas y causas de la resolución de problemas
- 9.2.3 Resolución de problemas de conectividad IP

CCNA SECURITY 2.0

Objetivo: El programa de estudios Cisco CCNA Security ofrece el siguiente paso para los estudiantes que quieran mejorar sus conocimientos de nivel CCNA y ayuda a satisfacer la creciente demanda de profesionales de seguridad de la red. El programa de estudios proporciona una introducción a los conceptos básicos de seguridad y los conocimientos necesarios para la instalación, resolución de problemas y supervisión de los dispositivos de red para mantener la integridad, confidencialidad y disponibilidad de los datos y los dispositivos. CCNA Security ayuda a preparar a los alumnos para las oportunidades profesionales de nivel básico relacionadas con la seguridad y para la certificación Cisco CCNA Security, reconocida internacionalmente.

Se trata de una solución de aprendizaje práctica y orientada hacia el ámbito profesional que hace hincapié en la experiencia práctica para ayudar a los alumnos a desarrollar habilidades especializadas de seguridad, así como el pensamiento crítico y las habilidades de resolución de problemas complejos. CCNA Security es un programa de estudios que combina el aprendizaje online con las clases presenciales. Los alumnos que se matriculan en el curso CCNA Security deben tener un conocimiento de los conceptos de redes y unas habilidades de nivel CCNA, además de conocimientos informáticos y de navegación en Internet básicos.

TEMARIO

CAPÍTULO 1:

AMENAZAS MODERNAS DE SEGURIDAD DE RED

1.1 Introducción.
1.2 Principios fundamentales de una Red Segura
- 1.2.1 La evolución de Seguridad de la Red
- 1.2.2. Controladores para Seguridad de Redes
- 1.2.3 Organizaciones de Seguridad de Red
- 1.2.4 Dominios de la Red de Seguridad
- 1.2.5 Dominios de la Red de Seguridad
- 1.2.6 Políticas de Seguridad de Red

1.3 Virus, gusanos, tecnologías de ataque
- 1.3.1 Virus
- 1.3.2 Gusanos
- 1.3.3 Caballo de Troya
- 1.3.4 Mitigando Virus, gusanos y Troyanos

1.4 Metodologías de ataque.
- 1.4.1 Ataques de reconocimiento
- 1.4.2 Ataque de Acceso
- 1.4.3 Ataques de denegación de servicio

1.5 Cisco Network Foundation Protection Framework
1.6 Resumen

CAPÍTULO 2:

SEGURIDAD DE DISPOSITIVO DE ACCESO

2.1 Introducción.
2.2 Seguridad de Dispositivos de Red
2.3 Asignación de Roles Administrativos.
- 2.3.1 Configurando Privilegios
- 2.3.2 Configurando Roles de Acceso

2.4 Monitorizando y gestionando dispositivos.
- 2.4.1 Asegurando IOS Cisco y Ficheros de Configuración
- 2.4.2 Una gestión segura y reportando
- 2.4.3 Utilizando syslog en la Seguridad de la Red
- 2.4.4 Utilizando NTP

2.5 Automatizando las funciones de seguridad
- 2.5.1 Haciendo una auditoría de seguridad
- 2.5.2 Bloqueo de un router con Autosecure
- 2.5.3 Bloqueo de un router con Cisco SDM

2.6 Resumen.

CAPÍTULO 3:

AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD

3.1 Reglas de la comunicación
3.2 Propósito de AAA.
- 3.2.1 Descripción de AAA
- 3.2.2 Características de AAA

3.3 Autenticación Local de AAA
- 3.3.1 Configuración de autenticación local AAA con CLI
- 3.3.2 Configuración de autenticación local AAA con SDM
- 3.3.3 Solución de problemas de autenticación local AAA

3.4 Server-based AAA.
- 3.4.1 Características Server-Based AAA
- 3.4.2 Protocolos de comunicación Server-Based AAA
- 3.4.3 Cisco Secure ACS
- 3.4.4 Configuración de Seguridad de Cisco ACS
- 3.4.5 Configuración de Seguridad de Cisco ACS Usuarios y grupos

3.5 Autenticación Server Based AAA
- 3.5.1 Configuración del servidor de autenticación Server-Based AAA con CLI
- 3.5.2 Configuración de autenticación Server-Based AAA con SDM
- 3.5.3 Solución de problemas del servidor de autenticación basado en la AAA

3.6 Server-Based AAA, Autorización y Contabilidad
- 3.6.1 Configuración del servidor basado en AAA Autorización
- 3.6.2 Configuración de Contabilidad Server-Based AAA

3.7 Resumen

CAPÍTULO 4:

IMPLEMENTACIÓN DE TECNOLOGÍAS FIREWALL

4.1 Introducción
4.2 Listas de control de acceso
- 4.2.1 Configuración de ACLs Estándar y Extendidas de la CLI
- 4.2.2 Utilización de ACLs estándar y extendidas
- 4.2.3 Tipología y flujo para las ACL
- 4.2.4 Configuración de ACLs estándar y extendidas son SDM
- 4.2.5 Configuración de ACLs reflexivas y TCP Established
- 4.2.6 Configuración de ACLs Dinámicas
- 4.2.7 Configuración de ACLs basadas en tiempo
- 4.2.8 Resolución de problemas de implementaciones con ACL complejas
- 4.2.9 Mitigación de ataques con ACLs

4.3 Tecnologías Firewall
4.4 Zone-Based Policy Firewall
4.5 Resumen

CAPÍTULO 5:

IMPLEMENTACIÓN DE PREVENCIÓN DE INTRUSIONES

5.1 Introducción
5.2 IPS Tecnologías
- 5.2.1 IDS y IPS Características
- 5.2.2 Implementación e IPS basados en Host
- 5.2.3 Implementado IPS basado en Red.

5.3 IPS Firmas
- 5.3.1 IPS Características de las Firmas
- 5.3.2 Alarmas de la Firma
- 5.3.3 Tuning IPS signature Alarms
- 5.3.4 Acciones de las firmas IPS
- 5.3.5 Gestión y Monitoreo del IPS

5.4 Implementación IPS
5.5 Verificación y supervisión IPS
5.6 Resumen

CAPÍTULO 6:

ASEGURANDO LA RED DE ÁREA LOCAL

6.0 Introducción
6.1 Seguridad Endpoint
- 6.1.1 Introducción a la Seguridad de los Dispositivos finales
- 6.1.2 Asegurando los Dispositivos finales con IronPort
- 6.1.3 Asegurando los Dispositivos finales con NAC
- 6.1.4 Asegurando la red con el Agente de Seguridad Cisco

6.2 Consideraciones de Seguridad de Capa 2

6.2.1 Introducción a la Seguridad de Capa 2
6.2.2 Ataques de Suplantación de Direcciones MAC
6.2.3 Ataques de desbordamiento a la Tabla de direcciones MAC
6.2.4 Ataques de Manipulación de STP
6.2.5 Ataques de Tormentas LAN
6.2.6 Ataques de VLANs
6.3 Configurando Seguridad de Capa 2
6.3.1 Configurando Port Security
6.3.2 Verificando Seguridad de Puerto (Port Security)
6.3.3 Configurando BPDU Guard y Root Guard
6.3.4 Configurando Control de Tormentas
6.3.5 Configurando Troncales Seguras para las VLANs
6.3.6 Configurando CISCO SPAN (Switched Port Analyzer)
6.3.7 Configurando CISCO RSPAN (Remote Switched Port Analyzer)
6.4 Wireless, VoIP, y Seguridad SAN
6.4.1 Consideraciones de Seguridad de la Tecnología Avanzada Empresarial
6.4.2 Consideraciones de Seguridad para Redes Inalámbricas
6.4.3 Consideraciones de Seguridad en Redes Inalámbricas
6.4.4 Consideraciones de Seguridad para VoIP
6.4.5 Soluciones de Seguridad para VoIP
6.4.6 Consideraciones de Seguridad para la SANs
6.4.7 Soluciones de Seguridad para las SANs
6.5 Resumen

CAPÍTULO 7:

SISTEMAS CRIPTOGRÁFICOS

7.0 Introducción
7.1 Servicios Criptográficos
7.1.1 Comunicaciones Seguras
7.1.2 Criptografía
7.1.3 Criptoanálisis
7.1.4 Criptología
7.2 Integridad y autenticidad básica
7.2.1 Critographic Hashes
7.2.2 Integridad con MD5 y SHA-1
7.2.3 Autenticación con HMAC
7.2.4 Administración de claves
7.3 Confidencialidad
7.4 Criptografía de clave pública
7.4.1 Simétrica versus encriptación asimétrica
7.4.2 Firmas Digitales
7.4.3 Rivest, Sahdir y Alderman

7.4.4 Infraestructura de llave pública
7.4.5 Estándares PKI
7.4.6 Autoridades de certificación
7.4.7 Los certificados digitales y Cas

CAPÍTULO 8:

IMPLEMENTACIÓN DE REDES PRIVADAS VIRTUALES

8.0 Introducción
8.1 VPNs
- 8.1.1 Descripción general de una VPN
- 8.1.2 Topologías VPNs
- 8.1.3 Soluciones VPNs

8.2 GREE VPNs
- 8.2.1 Configurando un túnel GRE sitio a sitio

8.3 Componentes y Operación de VPN IPsec
- 8.3.1 Introducción a IPsec
- 8.3.2 Protocolos de seguridad IPsec
- 8.3.3 Intercambio de claves en Internet

8.4 Implementando VPNs Sitio-a-Sitio con CLI
8.5 Implementando VPNs Sitio-a-Sitio con CCP
8.6 Implementando VPNs de Acceso-Remoto
- 8.6.1 El entorno empresarial cambiante
- 8.6.2 Introduciendo a las VPN de acceso remoto
- 8.6.3 VPNs SSL
- 8.6.4 Cisco Easy VPN
- 8.6.5 Configurando un VPN Server con SDM
- 8.6.6 Conectándose con un VPN Cliente

8.7 Resumen

CAPÍTULO 9:

IMPLEMENTACIÓN DE CISCO ADAPTIVE SECURITY APPLIANCE (ASA)

9.0 Introducción
9.1 Introducción al ASA
9.2 Configuración de firewall ASA
9.3 Configuración VPN ASA
9.4 Resumen

CAPÍTULO 10:

LA GESTIÓN DE UNA RED SEGURA