

#PUETrainingTalk



Amador Gabaldón

Senior Technical Trainer en PUE



Novedades curso Cisco CCNA v7

Workshop seguridad e identidad en la LAN

Agenda

➤ **Novedades en CCNA v7:**

- Motivación
- Certificación
- Estructura
- Organización y Orientación
- Curso Bridge**
- Contenidos nuevos

➤ **Seguridad e identidad en la LAN (WKSP):**

- Dispositivos finales
- Dispositivos de red
- Servicios
- AAA

Seguridad, automatización y programabilidad de las operaciones de TI

Liderazgo de Cisco



Red Intuitiva

Usuarios, Dispositivos, Apps,
Seguridad y Políticas



Redes de Dominio múltiple

Empresa, Centro de Datos,
Proveedor, Cloud



Programable mediante APIs

Automatización, Agilidad,
DevOps

El equipo de IT del futuro

Mundo de los
Ingenieros de infraestructura



Mundo de los
Desarrolladores de Software

Cisco ayudará a construir esto

Recorrido curricular:
Ingenieros de
Networking



Certificación Previa CCNA 200-125

Se mantiene en el nuevo CCNA

Desaparece
o se incorpora a CCNP

Nuevo examen de certificación CCNA 200-301

Nuevos
Temas

CCNA v7 - Actualización Temas Certificación – 200-301



Automatización y programabilidad

Automatización y Programabilidad de la Red 10%

Seguridad 15%



Fundamentos de seguridad

Fundamentos de IP 75%



Fundamentos de red



Acceso a la red



Conectividad IP



Servicios IP

1.0 Network Fundamentals	20%
2.0 Network Access	20%
3.0 IP Connectivity	25%
4.0 IP Services	10%
5.0 Security Fundamentals	15%
6.0 Automation and Programmability	10%

Cambios en el examen de Certificación

- Ampliación – teoría – de áreas temáticas. Ser capaz de describir.
- Duración del examen incrementada a 120 minutos
- Menos énfasis en configuraciones avanzadas
- Habilidades de resolución → Reubicadas en el nivel de CCNP

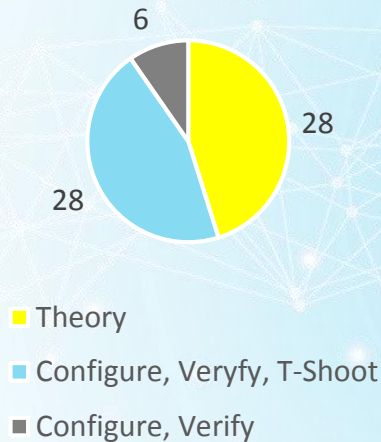
Cambios en el curso de preparación en Netacad

- Se mantiene una sólida base de fundamentos de IP y su conectividad
- Se mantiene aproximadamente el 55% del curriculum de CCNA R&S
- Existen algunos tópicos de fundamentos que, aunque no se incluyen en el examen, son necesarios para el desarrollo del curso. Ej. Topologías WAN
Topologies, IPSec, metodologías de resolución...

Balance Teoría /Práctica

- Orientación representativa según número y objeto de los enunciados y tareas
- Aproximación. A tener en cuenta la diversidad de temas.

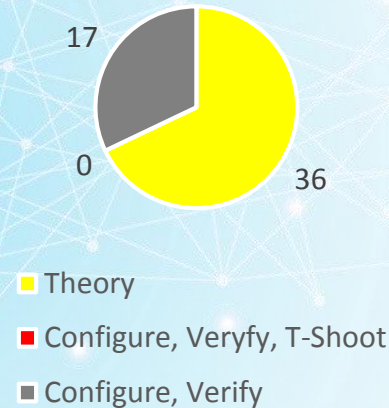
CCNA Routing & Switching



...más centrado en resolución de problemas

34 Tareas de Configuración o Resolución

CCNA v7



...más centrado en amplitud de conocimientos

17 Tareas de configuración (no Resolución)

Temas relevantes / clave que desaparecen

- VTP (1,2)
- Multi-area OSPF
- OSPFv3
- HSRP
- NetFlow
- EIGRP
- RIP, RIPv2
- BGP
- PPP, PPOE, HDLC
- GRE

CCNA v7 vs CCNA v6 - Comparativa Estructura

CCNA Routing & Switching – v6 (200 - 125)

CCNA – v7 – (200 – 301)

4 Módulos – 280 horas

Carga curricular estimada

3 Cursos ~ 210 horas

CCNA R&S – Introducción a las redes

CCNAv7 - ITN
Introducción a las redes

CCNA R&S – Fundamentos de enrutamiento y conmutación

CCNAv7 - SRWE
Fundamentos de conmutación, enrutamiento y comunicaciones inalámbricas

CCNA R&S – Escalado de redes

Estructura

CCNA R&S – Interconexión de redes

CCNAv7 - ENSA
Redes empresariales, seguridad y automatización

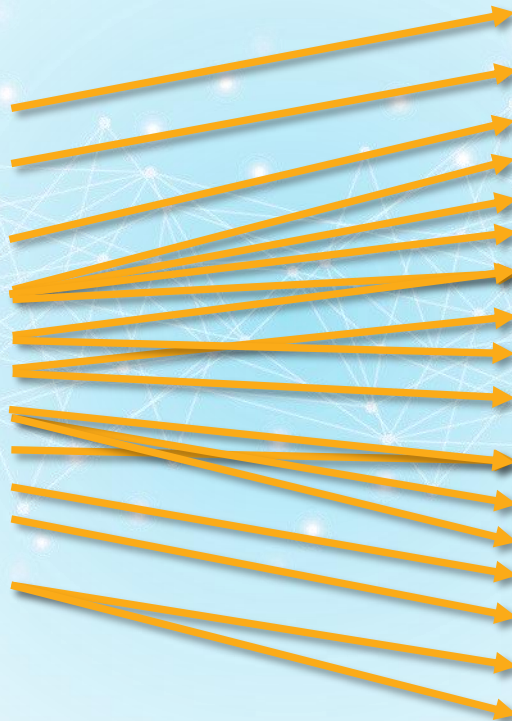
CCNA v7: Conformación de los cursos

CCNA v7 ITN	CCNA v7 SRWE	CCNA v7 ENSA
<p>Basado en el contenido de fundamentos de:</p> <p>CCNA R&S v6 Intro to Networks (ITN)</p>	<p>Selección Temas de de CCNA 6.0:</p> <ul style="list-style-type: none">- Fundamentos de enrutamiento y conmutación (RSE)- Escalado de redes (ScaN) <p>+ *Nuevos Temas</p>	<p>Selección de Temas de CCNA 6.0:</p> <ul style="list-style-type: none">- Fundamentos de enrutamiento y conmutación (RSE)- Escalado de redes (ScaN)- Interconexión de redes (CN) <p>+ **Nuevos temas</p>
<p>Ajustes menores y refinamientos</p>	<p>*Adición de temática: Seguridad y WLANs</p>	<p>**Adición de temática: Automatización, Programabilidad, VPNs y Seguridad</p>

CCNA v7 – ITN - Introducción a las redes

11 Capítulos

CCNA v6 - ITN
Exploración de las redes
Configuración de un sistema operativo de red
Protocolos de red y comunicaciones
Acceso a la red
Ethernet
Capa de Red
Direccionamiento IP
División en subredes IP
Capa de Transporte
Capa de Aplicación
Implementación básica de una red



17 Módulos

CCNA v7 - ITN

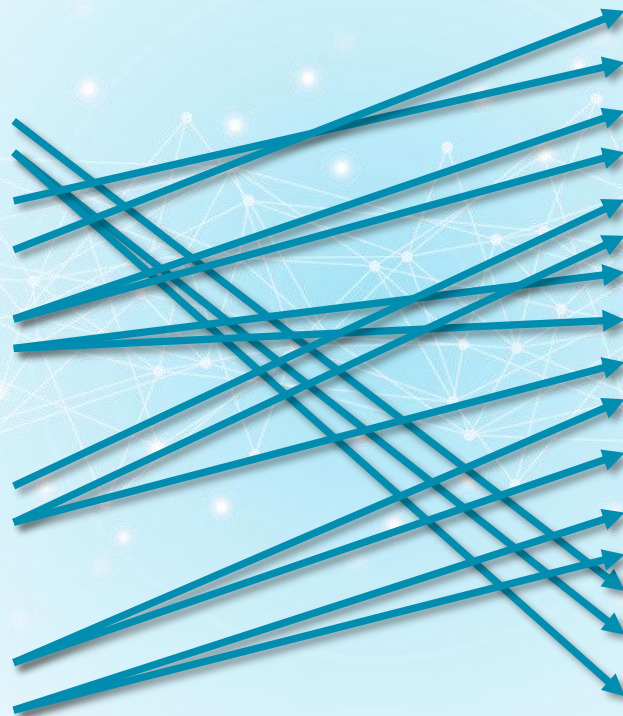
Las redes en la actualidad
Configuración básica de switches
Protocolos y modelos
Capa física
Sistemas numéricos
Capa de enlace de datos
Switching Ethernet
Capa de red
Resolución de dirección
Configuración básica de un router
Asignación de direcciones IPv4
Asignación de direcciones IPv6
ICMP
Capa de transporte
Capa de aplicación
Fundamentos de seguridad en la red
Cree una red pequeña

CCNA v7 – SRWE – Fundamentos enrutamiento, conmutación y comunicaciones inalámbricas

CCNA v6 - RSE
1 - Conceptos de enrutamiento
2 - Enrutamiento estático
3 - Redes conmutadas
5 - Configuración básica de conmutación
6 - VLANs
8 - DHCP

CCNA v6 - ScaN
3 - STP
4 - Etherchannel y HSRP


Nuevo Contenido*
Seguridad
WLANS



16 Módulos

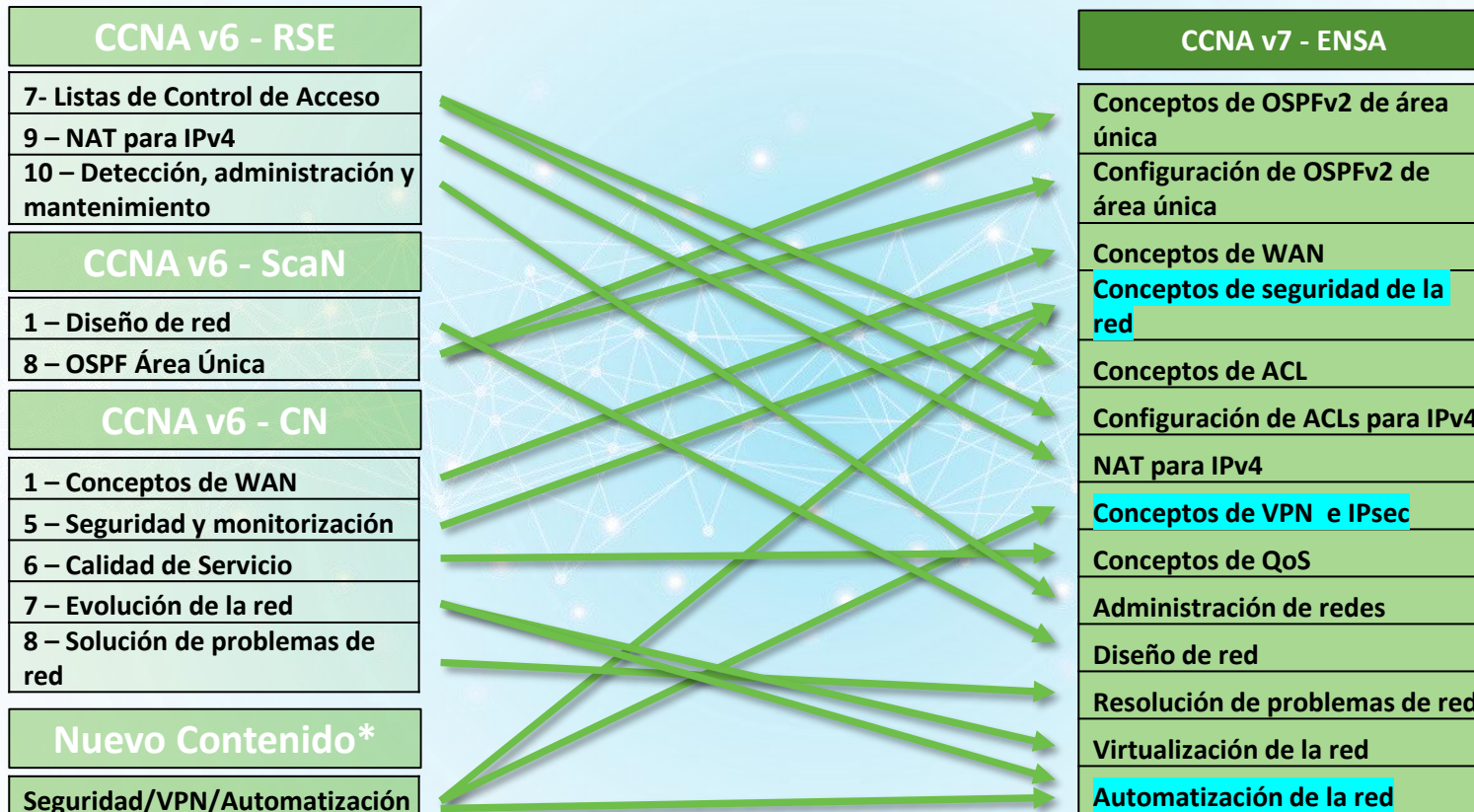
CCNA v7 - SRWE

Configuración básica de dispositivos
Conceptos de Switching
VLANs
Enrutamiento entre VLAN
STP
Etherchannel
DHCPv4
Conceptos SLAAC y DHCPv6
Conceptos de FHRP
Conceptos de seguridad de LAN
Conceptos de seguridad de Switch
Concepto WLAN
Configuración WLAN
Conceptos de enrutamiento
Rutas IP estáticas
Resuelva problemas de rutas estáticas y predeterminadas

 *Contenido nuevo o con cambios significativos

CCNA v7 – ENSA – Redes Empresariales, Seguridad y Automatización

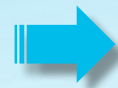
14 Módulos



*Contenido nuevo o con cambios significativos

CCNA v7 – Cada Curso → Constituidos por Módulos

- **Orientación** a la adquisición y entrenamiento de habilidades más definidas
 - ❖ Completar **Tareas**
- **Implicación** → Nuevo **arreglo** de contenidos en **Módulos**
 - ❖ Enfocado en el conocimiento (**auto-contenido**) para la realización de tareas
 - ❖ Unidad **integrada** de aprendizaje → Desarrollar un conjunto de **competencias**
- **Implicación** → Nuevo **nomenclatura** de las entidades formativas
 - ❖ CCNA v6
 - Módulos constituidos por **capítulos**
 - ❖ CCNA v7
 - Cursos constituidos por **módulos**



Capítulos



Módulos

CCNA v7 – Curso Bridge

- ❖ Recopilación contenidos diferenciales
- ❖ Nuevos y Complementarios
- ❖ Herramienta de soporte
- ❖ Indicado para instrucciones/ iniciadas basadas en CCNA R&S v6
- ❖ Agrupado por temática
- ❖ Referenciando nuevo curriculum

7 Módulos

CCNA v7 – Bridge
SRWE – Conceptos de Seguridad LAN
SRWE - Configuración de Seguridad en el Switch
SRWE – Conceptos de WLANs
SRWE – Configuración de WLANs
ENSA - Conceptos de Seguridad en red
ENSA – Conceptos de VPN e IPSEC
ENSA – Automatización de la red

Curso Bridge

Nuevos Contenidos

➤ SRWE:

- Conceptos de Seguridad LAN
- Configuración de Seguridad en el Switch
- Conceptos de redes Inalámbricas
- Configuración de WLANs

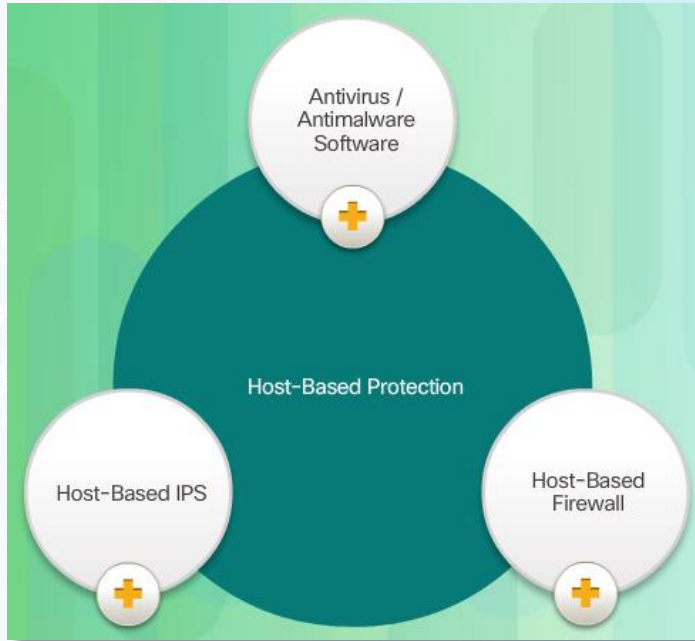
➤ ENSA:

- Conceptos de Seguridad en red
- Conceptos de VPN e IPSec
- Automatización de la Red

SRWE - Conceptos de Seguridad en la LAN

Tema	Objetivo del tema
Seguridad de punto de finales	Explique cómo usar la seguridad de punto de finalización para mitigar los ataques.
Control de acceso - AAA	Explique cómo se utilizan AAA y 802.1x para autenticar los terminales y los dispositivos LAN.
Amenazas a la seguridad de capa 2	Vulnerabilidades de la capa 2
Ataque a las tablas de direcciones MAC	Explique cómo un ataque de tablas de direcciones MAC compromete la seguridad de LAN.
Ataques a la LAN	Explique cómo los ataques a la LAN comprometen la seguridad de LAN.

Aproximación a la seguridad de Puntos finales



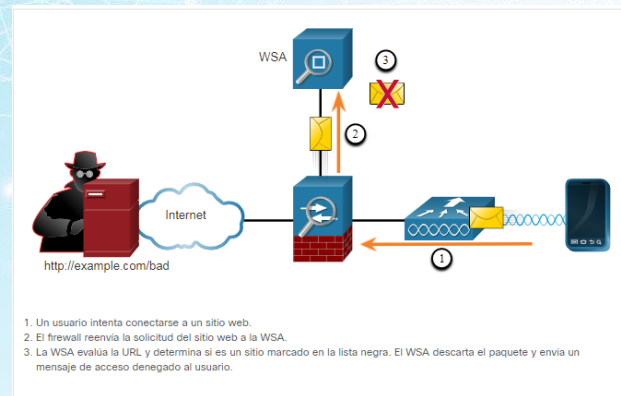
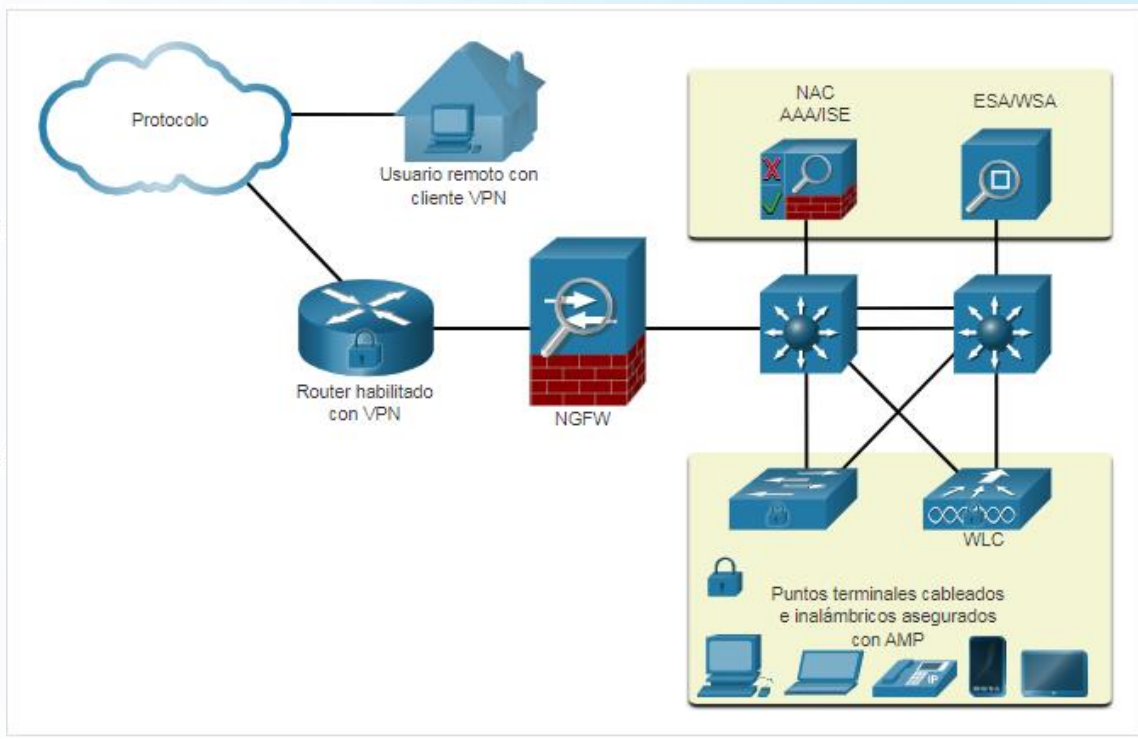
Tradicional



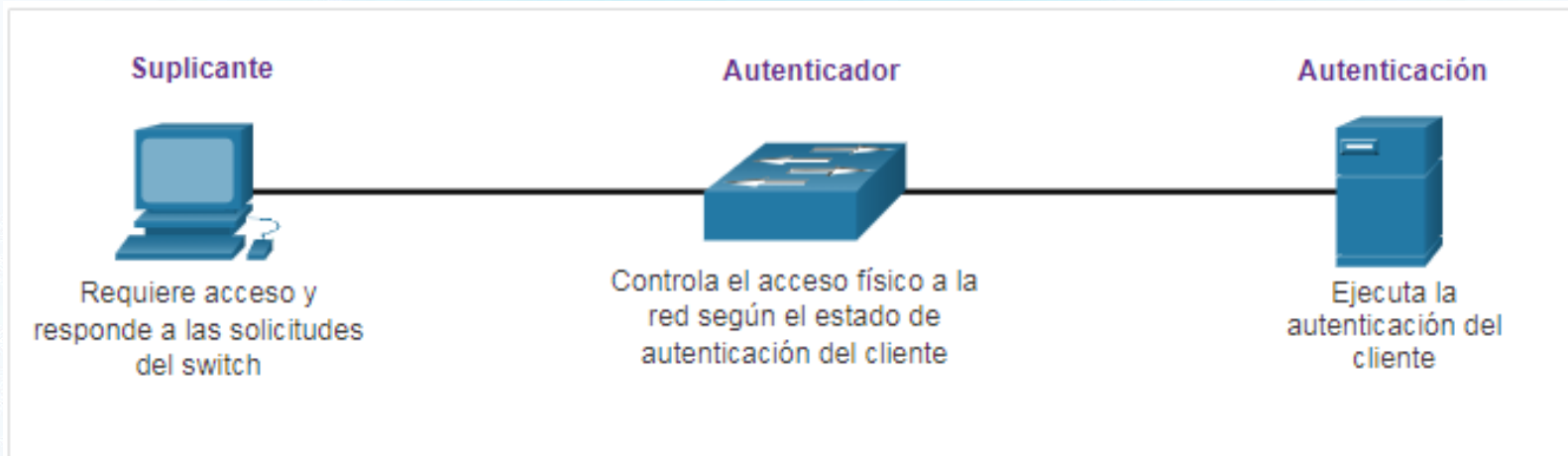
vs

Moderna

Protecciones - NAC/AMP/ESA/WSA/NGFW/VPN

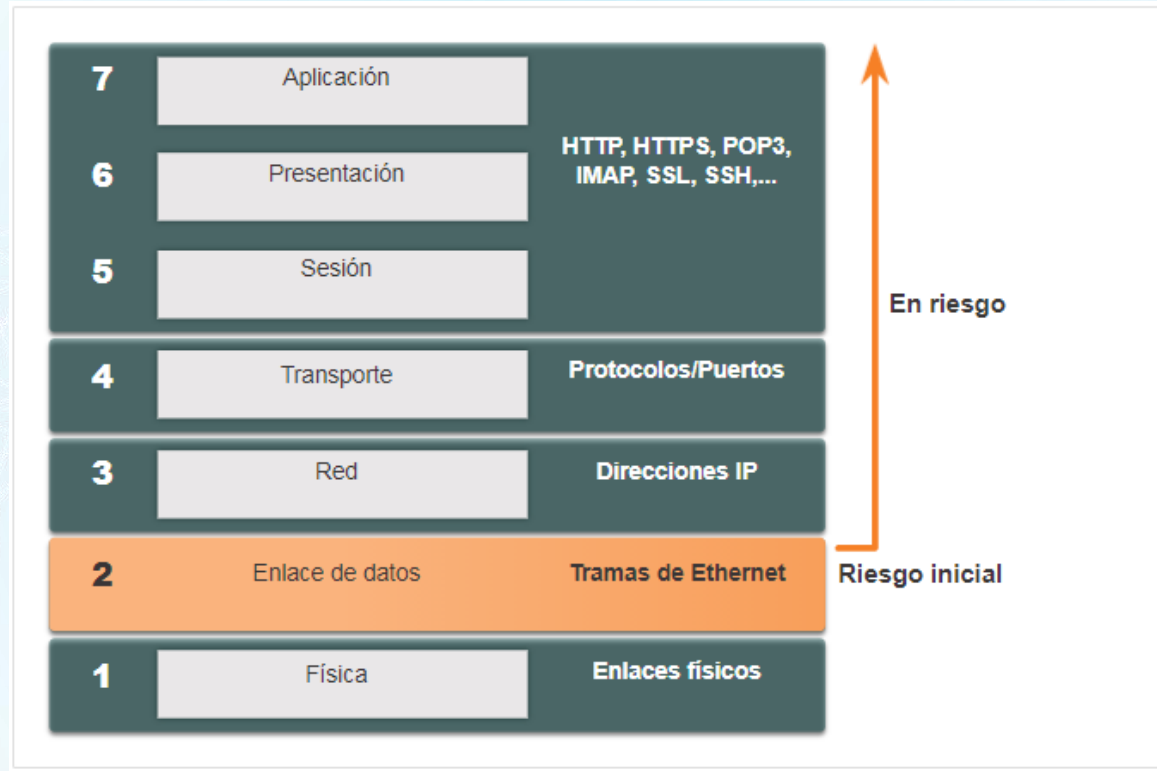


Control de Acceso basado en AAA – 802.1x - Elementos → IBNS – NAC



- **Cliente (suplicante)** - Este es un dispositivo ejecutando software de cliente 802.1X, el cual está disponible para dispositivos conectados por cable o inalámbricos.
- **Switch (Autenticador)** - El switch funciona como un agente intermediario (proxy) entre el cliente y el servidor de autenticación. Solicita la identificación de la información del cliente, verifica dicha información al servidor de autenticación y transmite una respuesta al cliente. Otro dispositivo que puede actuar como autenticador es un punto de acceso inalámbrico.
- **Servidor de autenticación** El servidor valida la identidad del cliente y notifica al switch o al punto de acceso inalámbrico si el cliente está o no autorizado para acceder a la LAN y a los servicios del Switch.

Seguridad desde Capa 2



Amenazas a la seguridad de Capa 2

Ataques de Capa 2

Categoría	Ejemplos
Ataques a la tabla MAC	Incluye ataques de saturación de direcciones MAC.
Ataques de VLAN	Incluye ataques VLAN Hopping y VLAN Double-Tagging. Esto también incluye ataques entre dispositivos en una misma VLAN.
Ataques de DHCP	Incluye ataques de agotamiento y suplantación DHCP.
Ataques ARP	Incluye la suplantación de ARP y los ataques de envenenamiento de ARP.
Ataques de Suplantación de Direcciones	Incluye los ataques de suplantación de direcciones MAC e IP.
Ataque de STP	Incluye ataques de manipulación al Protocolo de Árbol de Extensión.

Soluciones* para Mitigación de ataques en Switches

Mitigación de ataques en Capa 2.

Solución	Descripción
Seguridad de Puertos	Previene muchos tipos de ataques incluyendo ataques MAC address flooding Ataque por agotamiento del DHCP
DHCP Snooping	Previene ataques de suplantación de identidad y de agotamiento de DHCP
Inspección ARP dinámica (DAI)	Previene la suplantación de ARP y los ataques de envenenamiento de ARP.
Protección de IP de origen (IPSG)	Impide los ataques de suplantación de direcciones MAC e IP.

* Adicionales a la protección por buenas prácticas de los protocolos de gestión:
SSH, SCP, SFTP, SSL/TLS

SRWE - Configuración de Seguridad en Switches

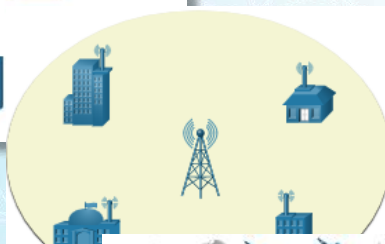
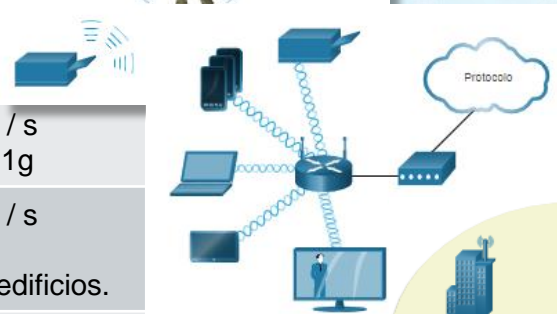
Tema	Objetivo del tema
Implementación de seguridad de puertos	Implemente la seguridad de puertos para mitigar los ataques de tablas de direcciones MAC.
Mitigación de ataques de VLAN	Explique cómo configurar DTP y la VLAN nativa para mitigar los ataques de VLAN.
Mitigación de ataques de DHCP	Explique cómo configurar el snooping de DHCP para mitigar los ataques de DHCP.
Mitigación de ataques de ARP	Explique cómo configurar ARP para mitigar los ataques de ARP.
Mitigación de ataques de STP	Explicar cómo configurar PortFast y BPDU Guard para mitigar los ataques STP.

SRWE - Conceptos de redes Inalámbricas - WLANs

Tema	Objetivo del Tema
Introducción a la Tecnología Inalámbrica	Describa la tecnología y los estándares WLAN.
Componentes de las WLAN	Describa los componentes de una infraestructura WLAN.
Funcionamiento de WLAN	Explique cómo la tecnología inalámbrica permite el funcionamiento de WLAN.
Funcionamiento de CAPWAP	Explique cómo un WLC utiliza CAPWAP para administrar múltiples AP.
Administración de Canales	Describa la administración de canales en una WLAN.
Amenazas a la WLAN	Describa las amenazas a las WLAN.
WLAN Seguras	Describa los mecanismos de seguridad de WLAN.

Clasificación / Tecnologías / Estándares

Estándar IEEE	Frecuencias de radio	Descripción
802.11	2,4 GHz	Velocidades de datos de hasta 2 Mb/s
802.11a	5 GHz	Velocidades de datos de hasta 54 Mb / s No interoperable con 802.11b o 802.11g
802.11b	2,4 GHz	Velocidades de datos de hasta 11 Mb / s Mayor alcance que 802.11a y mejor penetración en las estructuras de los edificios.
802.11g	2,4 GHz	Velocidades de datos de hasta 54 Mb / s Compatible con versiones anteriores de 802.11b
802.11n	2,4 Hz y 5 GHz	Velocidades de datos 150 - 600 Mb/s Requiere múltiples antenas con tecnología MIMO
802.11ac	5 GHz	Velocidades de datos 450 Mb/s – 1.3 Gb/s Admite hasta ocho antenas
802.11ax	2,4 GHz y 5 GHz	High-Efficiency Wireless (HEW) Capaz de usar frecuencias de 1 GHz y 7 GHz



WPAN

WLAN

WMAN

WWAN

Bluetooth

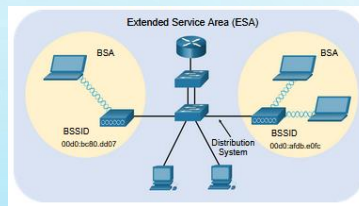
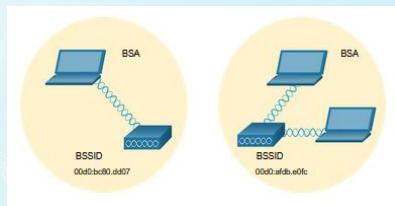
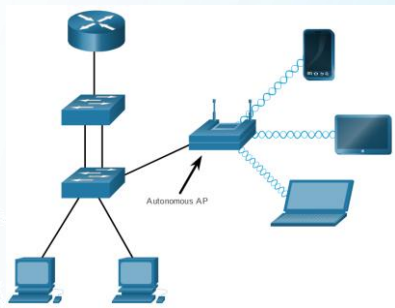
WiMAX

Ancho de banda celular.

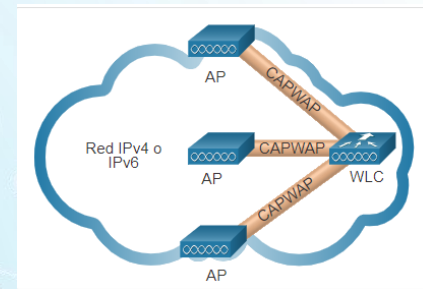
Banda ancha satelital (Satellite Broadband)

Conceptos de redes Inalámbricas

Aps Autónomos

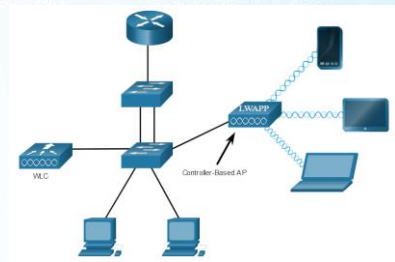


BSS ← Modos → ESS

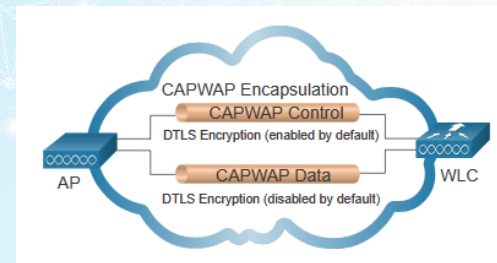
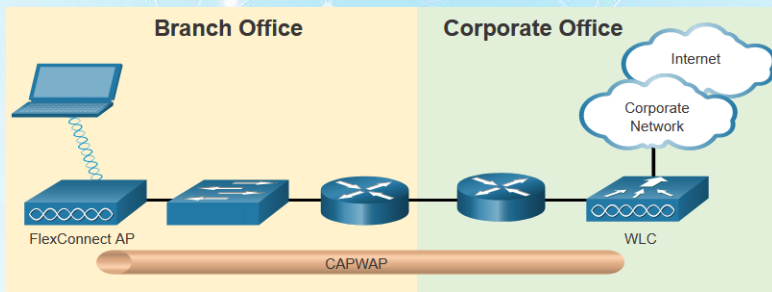


WLC → CAPWAP → AP

Aps basados en WLC



FlexConnect AP – Arquitectura Split MAC



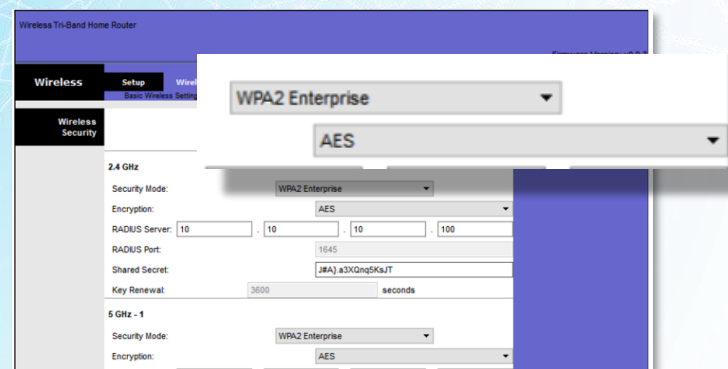
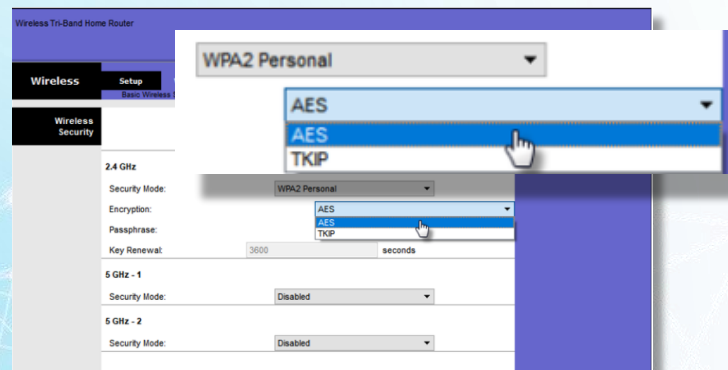
LWAPP + DTLS → CAPWAP

Redes Inalámbricas Seguras

Métodos

Método de Autenticación	Descripción
Privacidad Equivalente al Cableado (WEP)	La especificación original 802.11 diseñada para proteger los datos utilizando el método de cifrado Rivest Cipher 4 (RC4) con una clave estática. WEP ya no se recomienda y nunca debe usarse.
Acceso Protegido Wi-Fi (WPA)	Un estándar de Wi-Fi Alliance que usa WEP pero asegura los datos con el algoritmo de cifrado del Protocolo de integridad de clave temporal (TKIP) mucho más fuerte. El TKIP cambia la clave para cada paquete, lo que hace que sea mucho más difícil de descifrar.
WPA2	Utiliza el Estándar de Cifrado Avanzado (AES) para el cifrado. AES actualmente se considera el protocolo de cifrado más sólido.
WPA3	Próxima generación de seguridad Wi-Fi. Los dispositivos habilitados para WPA3 usan los últimos métodos de seguridad, no permiten protocolos heredados y requieren el uso de marcos de administración protegidos (PMF).

Personal / Empresarial – AAA + Radius



SRWE - Configuración de redes Inalámbricas

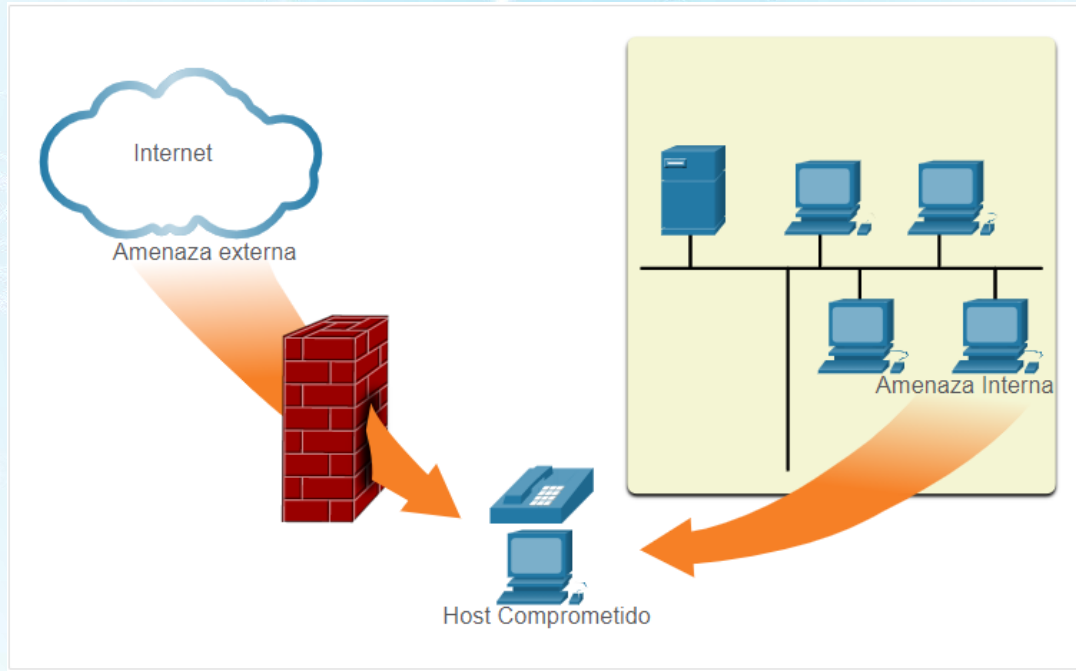
Tema	Objetivo del tema
Configuración de WLAN del sitio remoto	Configure una WLAN para admitir un sitio remoto.
Configure a WLAN Básico en el WLC	Configure un WLC de red inalámbrica WLAN para que use la interfaz de administración y la autenticación WPA2 PSK.
Configure una red inalámbrica WLAN WPA2 Enterprise en el WLC	Configure un WLC de red inalámbrica WLAN para que use una interfaz VLAN, un servidor DHCP, y autenticación WPA2 Enterprise.
Solución de problemas de WLAN	Resolver problemas comunes de la configuración inalámbrica.

ENSA - Conceptos de Seguridad en Red

Tema	Objetivo del tema
Estado Actual de la Ciberseguridad	Describa el estado actual de la ciberseguridad y los vectores de pérdida de datos.
Agentes de amenazas	Describa las herramientas que utilizan los agentes de amenazas para explotar las redes.
Malware	Describa los tipos de malware.
Ataques de red habituales	Describa los ataques de red habituales.
Vulnerabilidades y amenazas de IP	Explique cómo los agentes de amenazas explotan las vulnerabilidades de IP.
Vulnerabilidades de TCP y UDP	Explique cómo los agentes de amenazas explotan las vulnerabilidades de TCP y UDP.
Servicios IP	Explique cómo los agentes de amenazas explotan los servicios IP.
Mejores Prácticas en Seguridad de Redes	Describa las mejores prácticas para proteger una red.
Criptografía	Describa los procesos criptográficos comunes utilizados para proteger los datos en tránsito.

Aproximación a los métodos de defensa ante ataques

Clasificación de Amenazas – Internas y Externas



Terminología de Seguridad

Términos de seguridad	Descripción
Activos	Un activo es cualquier cosa de valor para la organización. Incluye personas, equipos, recursos y datos.
Vulnerabilidad	Una vulnerabilidad es una debilidad en un sistema, o su diseño, que podría ser explotada por una amenaza.
Amenaza	Una amenaza es un peligro potencial para los activos, los datos o la funcionalidad de la red de una empresa.
Exploit	Un exploit es un mecanismo para tomar ventaja de una vulnerabilidad.
Mitigación	La mitigación es la contra-medida que reduce la probabilidad o la severidad de una posible amenaza o riesgo. La seguridad de Redes consiste en técnicas de mitigación múltiples.
Riesgo	El riesgo es la probabilidad de que una amenaza explote la vulnerabilidad de un activo, con el objetivo de afectar negativamente a una organización. El riesgo se mide utilizando la probabilidad de ocurrencia de un evento y sus consecuencias.

Vectores de pérdida de datos	Descripción
Correo electrónico / Redes sociales	El correo electrónico o los mensajes de mensajería instantánea interceptados podrían capturarse y descifrar el contenido.
Dispositivos no encriptados	Si los datos no se almacenan utilizando un algoritmo de cifrado, entonces el ladrón puede extraer datos confidenciales de valor.
Dispositivos de almacenamiento o en la nube	Los datos confidenciales se pueden perder si el acceso a la nube se ve comprometido debido a ajustes débiles en la seguridad.
Medios extraíbles	Un riesgo es que un empleado pueda realizar una transferencia no autorizada de datos a un dispositivo USB. Otro riesgo es que el dispositivo USB que contiene datos corporativos de valor se puede extraviar.
Respaldo físico	Los datos confidenciales deben triturarse cuando ya no sean necesarios.
Control de Acceso Incorrecto	Las contraseñas o contraseñas débiles que se hayan visto comprometidas pueden proporcionar al atacante un acceso fácil a los datos corporativos.

Clasificación de Actores Amenaza y Hackers



Término de Piratería	Descripción
Script kiddies	Estos son adolescentes o hackers inexpertos que corren scripts, ejecutan herramientas y exploits existentes para ocasionar daño, pero generalmente no para obtener ganancias.
Agentes de Vulnerabilidad	Son generalmente hackers de sombrero gris que intentan descubrir los exploits e informarlos a los proveedores, a veces a cambio de premios o recompensas.
Hacktivistas	Estos son hackers de sombrero gris que protestan en público contra las organizaciones o gobiernos mediante la publicación de artículos, videos, la filtración de información confidencial y la ejecución de ataques a la red.
Delincuentes cibernéticos	Son hackers de sombrero negro que independientes o que trabajan para grandes organizaciones de delito cibernético.
Patrocinados por el estado	Son hackers de sombrero blanco o sombrero negro que roban secretos de gobierno, recopilan inteligencia y sabotean las redes. Sus objetivos son los gobiernos, los grupos terroristas y las corporaciones extranjeras. La mayoría de los países del mundo participan en algún tipo de hacking patrocinado por el estado.

Herramientas de Actores Amenaza

Decodificadores de Contraseñas	Las herramientas para descifrar contraseñas a menudo se denominan herramientas de recuperación de contraseñas y se puede usar para descifrar o recuperar una contraseña. Esto se logra ya sea eliminando la contraseña original, después de omitir los datos cifrado, o por descubrimiento directo de la contraseña. Decodificadores de contraseñas hacer conjeturas repetidamente para descifrar la contraseña. Ejemplos de las herramientas para descifrar contraseñas incluyen a John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack y Medusa.
Herramientas de Hacking Inalámbrico	Las herramientas de piratería inalámbrica se utilizan para piratear intencionalmente red para detectar vulnerabilidades de seguridad. Ejemplos de piratería inalámbrica las herramientas incluyen Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep y NetStumbler.
Escaneo de redes y Herramientas de Hacking	Las herramientas de análisis de red se utilizan para sondear dispositivos de red, servidores y hosts para puertos TCP o UDP abiertos. Ejemplos de herramientas de escaneo incluyen Nmap, SuperScan, Angry IP Scanner y NetScanTools
Herramientas para conformar Paquetes de Prueba	Estas herramientas se utilizan para sondear y probar la robustez de un cortafuegos utilizando paquetes forjados especialmente diseñados. Los ejemplos incluyen Hping, Scapy, Socat, Yersinia, Netcat, Nping y Nemesis.
Analizadores de protocolos de paquetes	Estas herramientas se utilizan para capturar y analizar paquetes dentro de redes tradicionales Ethernet LANs y WLANs. Las herramientas incluyen Wireshark, Tcpcdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, y SSLstrip.
Detectores de Rootkits	Este es un verificador de integridad de directorios y archivos utilizado por los sombreros blancos para detectar grupos de raíz instalados. Las herramientas de ejemplo incluyen AIDE, Netfilter, y PF: OpenBSD Packet Filter.
Fuzzers para Buscar Vulnerabilidades	Los fuzzers son herramientas utilizadas por los actores de amenazas para descubrir una computadora y sus aspectos vulnerables de la seguridad Algunos ejemplos de fuzzers: Skipfish, Wapiti y W3af.

Herramientas de Actores Amenaza – Cont.

Herramientas de Informática Forense	Los hackers de sombrero blanco utilizan estas herramientas para detectar cualquier rastro de evidencia existente en una computadora. Ejemplos de herramientas incluyen un equipo de Sleuth, Helix, Maltego, y Encase.
Depuradores	Los hackers de sombrero negro utilizan estas herramientas para aplicar ingeniería inversa en archivos binarios cuando escriben debilidades. También las utilizan los sombreros blancos cuando analizan malware. Algunas herramientas de depuración son las siguientes: GDB, WinDbg, IDA Pro e Immunity Debugger. Depuradores
Sistemas Operativos para Hacking	Estos son sistemas operativos especialmente diseñados precargados con herramientas optimizado para hackear. Ejemplos de operaciones de piratería especialmente diseñadas Los sistemas incluyen Kali Linux, Knoppix, BackBox Linux.
Herramientas de Cifrado	Las herramientas de cifrado utilizan esquemas de algoritmos para codificar los datos para evitar acceso no autorizado a los datos encriptados. Ejemplos de estas herramientas incluyen VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN y Stunnel.
Herramientas para Atacar Vulnerabilidades	Estas herramientas identifican si un host remoto es vulnerable a un ataque de seguridad ataque. Ejemplos de herramientas de explotación de vulnerabilidades incluyen Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit y Netsparker.
Escáneres de Vulnerabilidades	Estas herramientas analizan una red o un sistema para identificar puertos abiertos. Ellos pueden también usar para escanear vulnerabilidades conocidas y escanear máquinas virtuales, BYOD dispositivos y bases de datos de clientes. Ejemplos de herramientas incluyen Nipper, Secunia Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT u Open VAS.

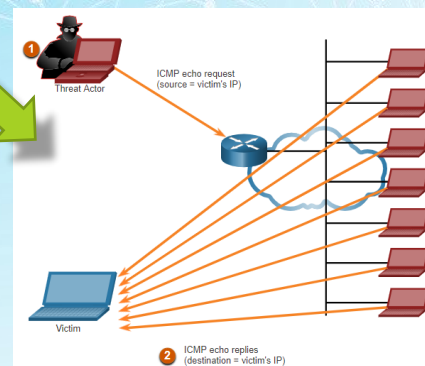
Tipos de Ataque

Tipo de ataque	Descripción
Ataque de interceptación pasiva (eavesdropping)	Esto es cuando un actor de amenaza captura “escucha” a tráfico de red. Este ataque también se conoce como sniffing o snooping.
Ataque de Modificación de Datos	Si los actores de la amenaza han capturado el tráfico empresarial, pueden alterar los datos en el paquete sin el conocimiento del remitente o receptor.
Ataque de suplantación de dirección IP	Un actor de amenaza construye un paquete IP que parece originarse de un dirección válida dentro de la intranet corporativa.
Ataques Basados en Contraseñas	Si los actores de amenazas descubren una cuenta de usuario válida, los actores de amenazas tienen los mismos derechos que el usuario real. Los actores de amenazas podrían usar como válida la cuenta para obtener listas de otros usuarios, información de red, cambio de configuraciones de servidores y redes, y modificar, redireccionar o eliminar datos.
Ataque por Denegación de Servicio	Un ataque de DoS impide el uso normal de una computadora o red por parte de usuarios válidos usuarios. Un ataque DoS puede inundar una computadora o toda la red con tráfico hasta que se produzca un apagado debido a la sobrecarga. Ataque de DoS también puede bloquear el tráfico, lo que resulta en una pérdida de acceso a la red recursos por usuarios autorizados.
Ataque man-in-the-middle	Este ataque ocurre cuando los actores de amenaza se han posicionado entre el origen y destino. Ahora pueden monitorear, capturar y controlar la comunicación de forma transparente.
Ataque de Claves Comprometidas	Si un actor de amenaza obtiene una clave secreta, esa clave se conoce como clave en riesgo. Se puede usar una clave comprometida para obtener acceso a un comunicación segura sin que el remitente o el receptor sean conscientes del ataque.
Ataque de analizador de protocolos	Un detector es una aplicación o dispositivo que puede leer, monitorear y capturar intercambios de datos de red y leer paquetes de red. Si los paquetes no están cifrados, un analizador de protocolos permite ver por completo los datos que están dentro del paquete.

Vulnerabilidades y amenazas de IP

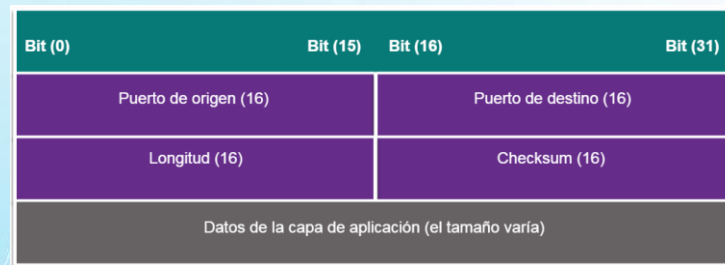
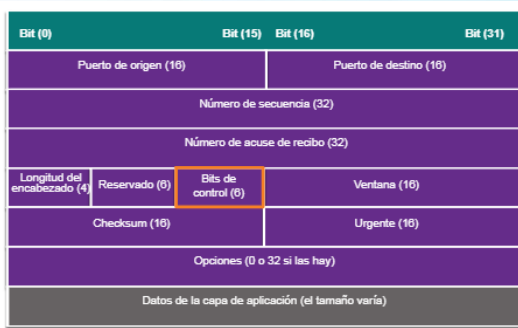
Técnicas de Ataque IP	Descripción
Ataques ICMP	Los atacantes utilizan paquetes de eco (pings) del protocolo de mensajería de control de Internet (ICMP) para detectar subredes y hosts en una red protegida para generar ataques de saturación DoS y para modificar las tablas de routing de los hosts.
Ataques de Amplificación y reflexión	Los atacantes intentan impedir que usuarios legítimos tengan acceso a información o servicios.
Ataques de suplantación de direcciones	Los atacantes suplantan la dirección IP de origen en un paquete de IP para realizar suplantación blind o non-blind.
Ataques man-in-the-middle (MITM)	Los atacantes se posicionan entre un origen y un destino para monitorear, capturar y controlar la comunicación en forma transparente. Simplemente pueden escuchar en silencio mediante la inspección de paquetes capturados o modificar paquetes y reenviarlos a su destino original.
Secuestros de sesiones	Los atacantes obtienen acceso a la red física y, luego, usan un ataque de MITM para secuestrar una sesión.

Mensajes ICMP utilizados por los Hackers	Descripción
"Echo request" y "echo reply" de ICMP	Esto se utiliza para realizar la verificación del host y los ataques DoS.
"Unreachable" de ICMP	Se usa para realizar ataques de reconocimiento y análisis de la red.
"Mask reply" de ICMP	Se utiliza para alcanzar una red IP interna.
"Redirect" de ICMP	Se utiliza para lograr que un host de destino envíe todo el tráfico a través de un dispositivo atacado y crear un ataque de MITM.
"Router discovery" de ICMP	Se usa para inyectar rutas falsas en la tabla de routing de un host de destino.



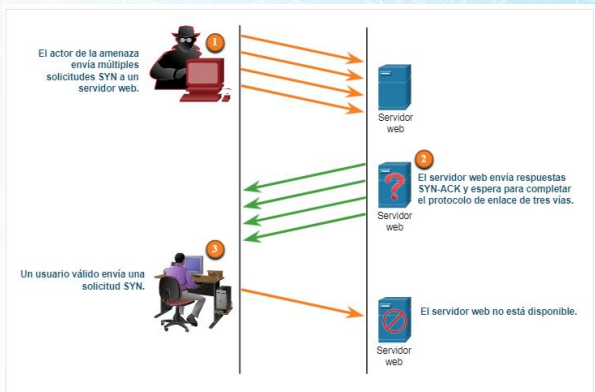
Amplificación y Reflexión

Vulnerabilidades TCP y UDP [y servicios IP*]



Cabecera TCP (↑) y ataque SYN (↓)

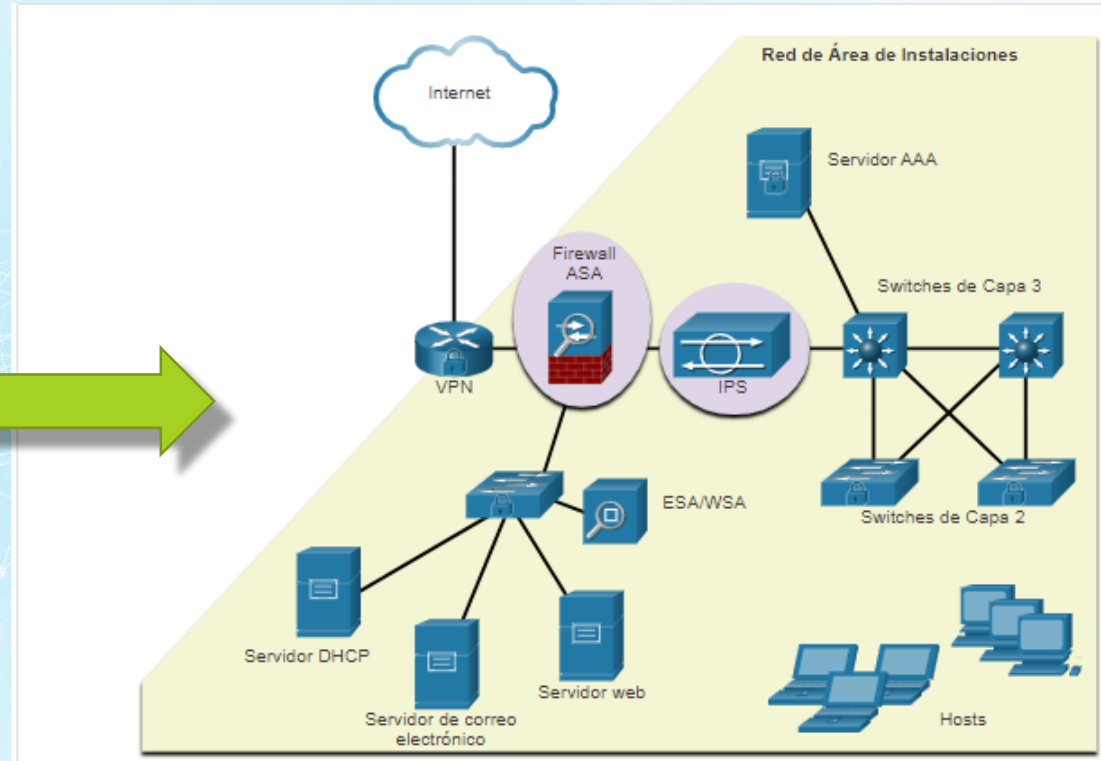
Cabecera UDP (↑)



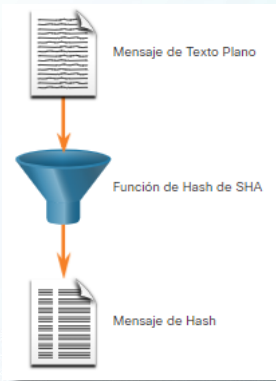
Usualmente se traduce en:

- Ataques inundación a servicios basados en UDP:
 - ➔ Para saturar un servicio (incluso protegido)
 - ➔ Para provocar respuestas amplificadas (similar a ICMP)
- Barrido de puertos

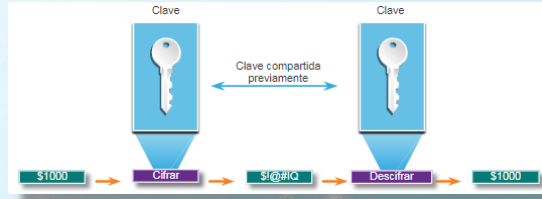
Mejores Prácticas en Seguridad de Redes



Criptografía



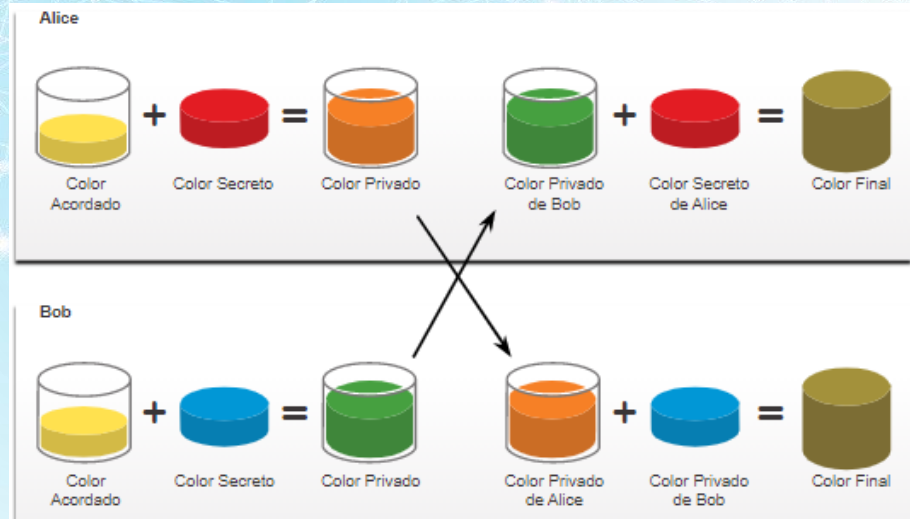
HASH (↑) vs HMAC (↓)



Cifrado Simétrico (↑)



Cifrado Asimétrico (↑)



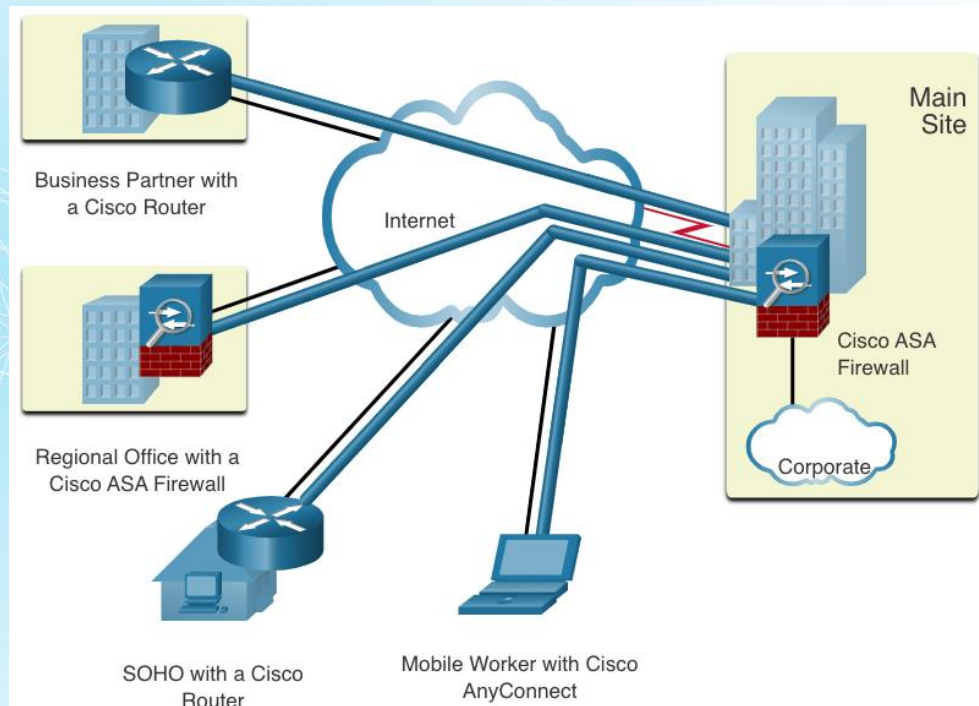
Intercambio Diffie - Hellman

ENSA - Conceptos de VPN e IPsec – Seguridad en comunicaciones

Tema	Objetivo del tema
Tecnología VPN	Describa los beneficios de la tecnología VPN.
Tipos de VPN	Describa los diferentes tipos de VPN
IPSec	Explique cómo se utiliza el framework IPsec para proteger el tráfico de red.

Tecnología VPN y Beneficios

Ventaja	Descripción
Ahorro de costos	Las organizaciones pueden usar VPN para reducir sus costos de conectividad y al mismo tiempo aumentar el ancho de banda de la conexión remota.
Seguridad	Los protocolos de encriptación y autenticación protegen los datos del acceso no autorizado.
Escalabilidad	Las VPN proporcionan escalabilidad, lo que permite a las organizaciones usar Internet, lo que facilita agregar nuevos usuarios sin agregar una infraestructura significativa.
Compatibilidad	Las VPN se pueden implementar en una amplia variedad de opciones de enlace WAN, incluidas las tecnologías de banda ancha. Los trabajadores remotos pueden usar estas conexiones de alta velocidad para obtener acceso seguro a las redes corporativas.

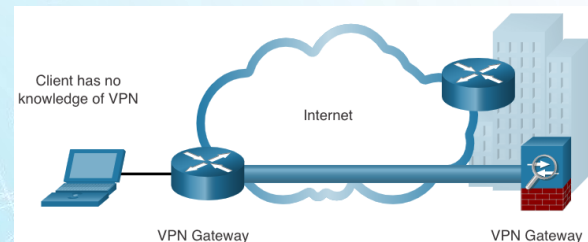


Tipos de VPN – Básicos

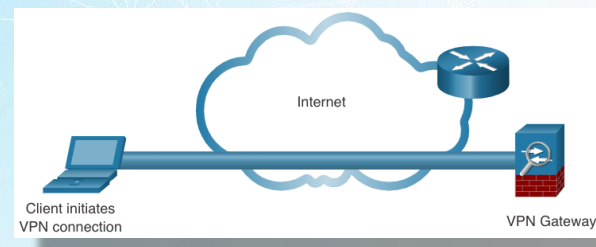
IPsec vs SSL

Característica	IPsec	SSL
Aplicaciones compatibles	Extensiva – Todas las aplicaciones basadas en IP son compatibles.	Limitada – Solo aplicaciones y archivos compartidos basados en la web
Nivel de autenticación	Fuerte : – autenticación bidireccional con claves compartidas o certificados digitales	Moderado – Uso de autenticación unidireccional o bidireccional
Nivel de encriptación	Fuerte – Longitudes de clave 56 - 256 bits	Moderado a fuerte – Longitudes de clave 40 - 256 bits
Complejidad de conexión	Medio : – Requiere un cliente VPN instalado en un host	Bajo : – Requiere un navegador web en un host
Opción de conexión	Limitado : – Solo se pueden conectar dispositivos específicos con configuraciones específicas	Extenso : – Cualquier dispositivo con un navegador web puede conectarse

VPN – Sitio a sitio

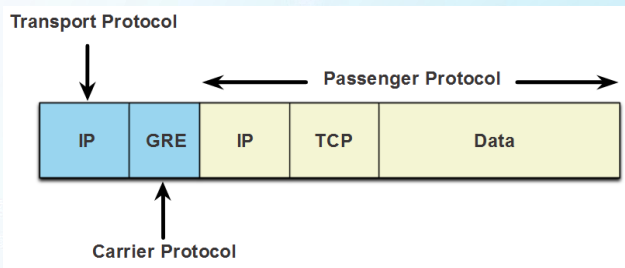


VPN – Acceso Remoto

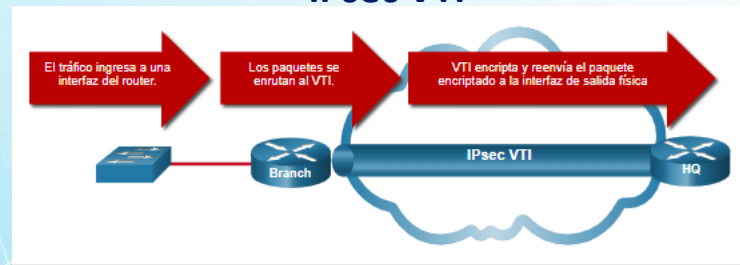


Tipos de VPN – Túneles

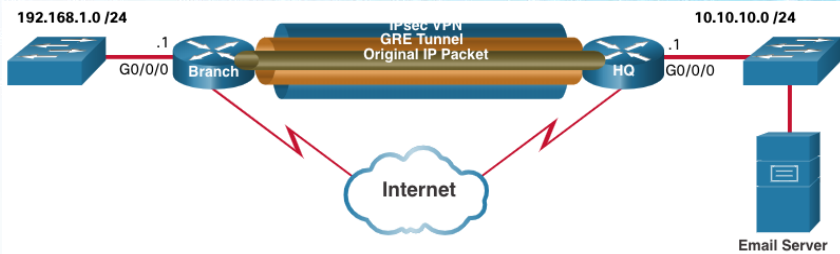
Túnel GRE



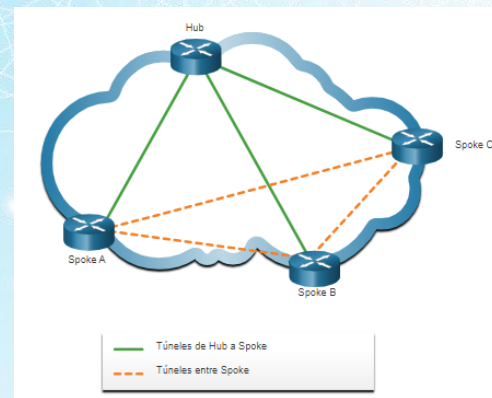
IPsec VTI



Túnel GRE sobre IPsec

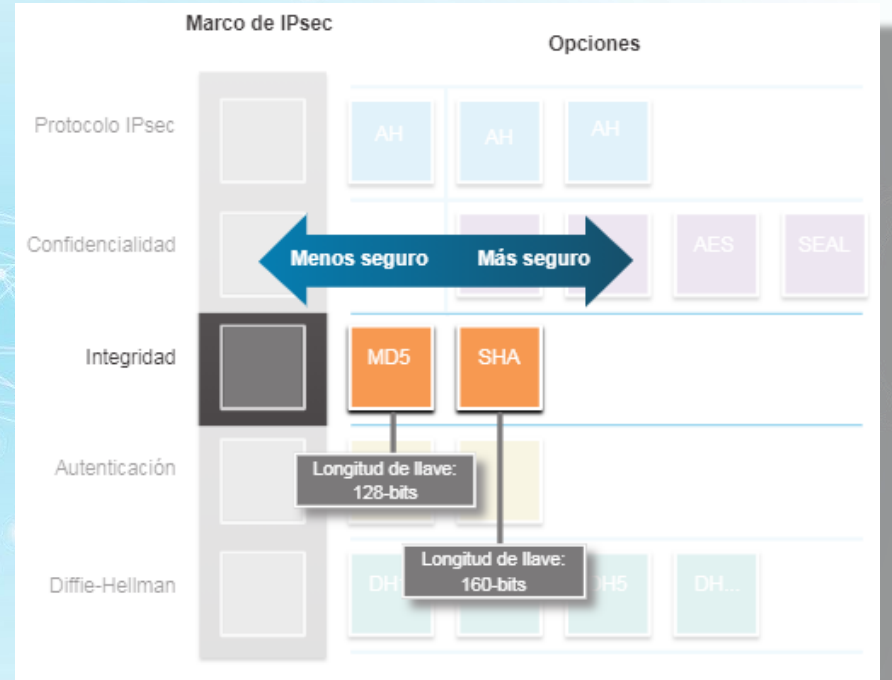
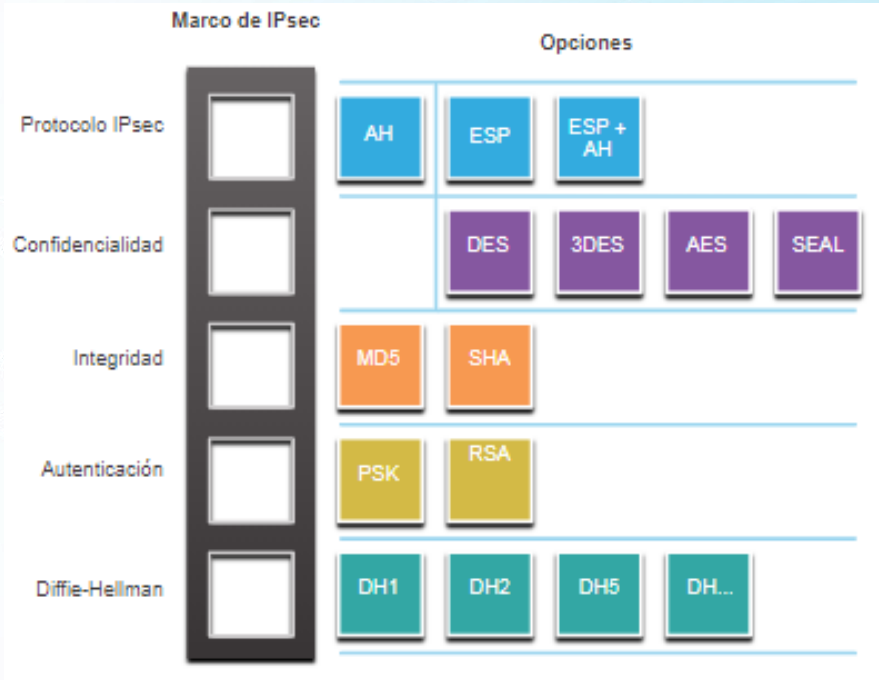


VPN Dinámica Multipunto - NHRP + mGRE

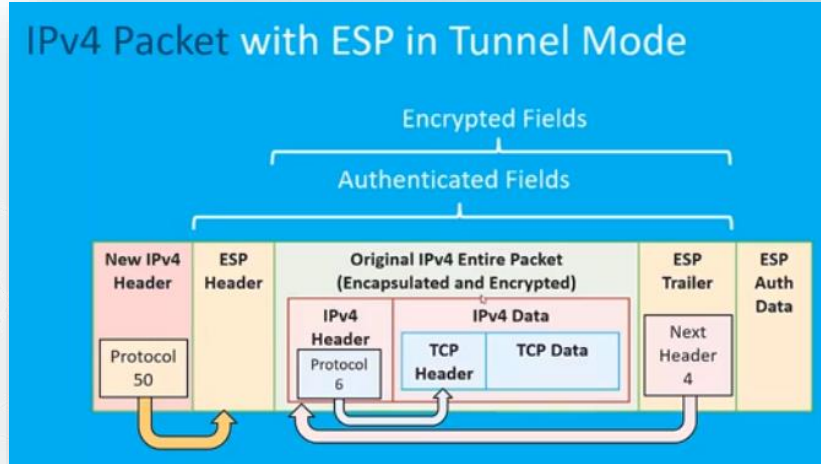


*Además ➔ VPN de Proveedor – MPLS Layer 3 / Layer2

Framework IPsec → Protocolos AH y ESP

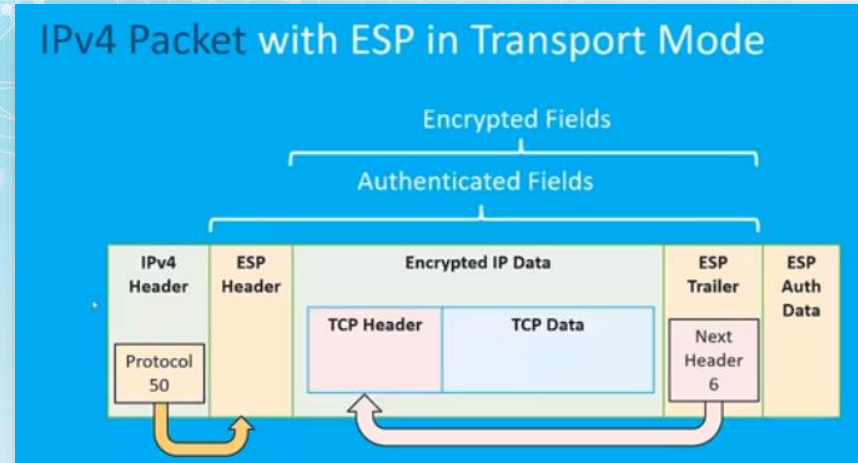


Framework IPsec → Encapsulaciones



Modo transporte →
Usual si el VPN Gateway es destino

← Modo túnel. Por defecto
Usual en sitio a sitio



ENSA - Automatización de red

Tema	Objetivo del tema
Visión General	Explique los beneficios de la automatización de red
Formato de Datos	Explique la necesidad y tipos
API	Describir usos de una API
REST	Describir y caracterizar APIs RESTfu
Herramientas de Administración y Configuración	Describa los controladores utilizados en la programación de redes.
IBN y Cisco DNA Center	

Automatización de red

Beneficios de la automatización:

- Las máquinas pueden trabajar las 24 horas sin interrupciones → brindan una mayor producción.
- Las máquinas proporcionan un resultado más uniforme.
- La automatización permite la recolección de grandes cantidades de datos →
 - **Análisis**
 - **Obtención de información → Guiado o disparador de un evento o proceso.**
- Los robots se utilizan en condiciones peligrosas como la minería, la lucha contra incendios y la limpieza de accidentes industriales → Reducción del riesgo para las personas.
- Bajo ciertas circunstancias, los dispositivos inteligentes (con lógica o programación integrada) pueden alterar su uso de energía, realizar diagnósticos médicos y mejorar la conducción de los automóviles para que sea más segura.

Formatos de Datos – HTML – JSON – XML - YAML

- Modo de almacenar e intercambiar datos de una manera estructurada. P.ej HTML es un estándar que describe la estructura de páginas web
- Formatos de datos comunes usados en muchas aplicaciones incluidas automatización de la red y programación:
 - **Notación de objeto de JavaScript (JavaScript Object Notation - JSON)**
 - **Lenguaje de marcado extensible (XML)**
 - **YAML no es un lenguaje de marcado (YAML)**

```
mensaje: éxito
marca de tiempo: 1560789260 iss_position:
  latitud: '25.9990' longitud: '-
132.6992'
```

Formato YAML

```
{
  "mensaje": "éxito",
  "marca de tiempo":
1560789260,
  "iss_position": {
    "latitud": "25.9990",
    "longitud": "-132.6992"
  }
}
```

Formato JSON

```
<?xml version="1.0" encoding="UTF-8" ?> <root>
<message>success</message>
<timestamp>1560789260</timestamp>
<iss_position>
  <latitude>25.9990</latitude>
  <longitude>-132.6992</longitude> </iss_position>
</root>
```

Formato XML

Tipos de APIs de servicios Web

Cuatro tipos:

- Protocolo Simple de Acceso a Objetos (SOAP)
- Transferencia de Estado Representacional (REST)
- Llamada a procedimiento remoto de lenguaje de marcado extensible (XML-RPC)
- Llamada a procedimiento remoto de notación de objetos JavaScript (JSON-RPC)

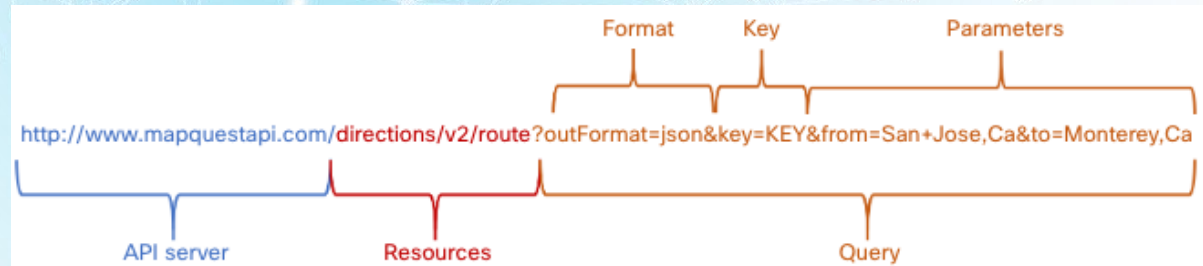
Característica	SOAP	REST	XML-RPC	JSON-RPC
Formato de datos	XML	JSON, XML, YAML y otros	XML	JSON
Año de lanzamiento	1998	2000	1998	2005
Puntos fuertes	Bien establecido	Formateo flexible y más utilizado	Bien establecida, simplicidad	Simplicidad

REST Y RESTful APIS

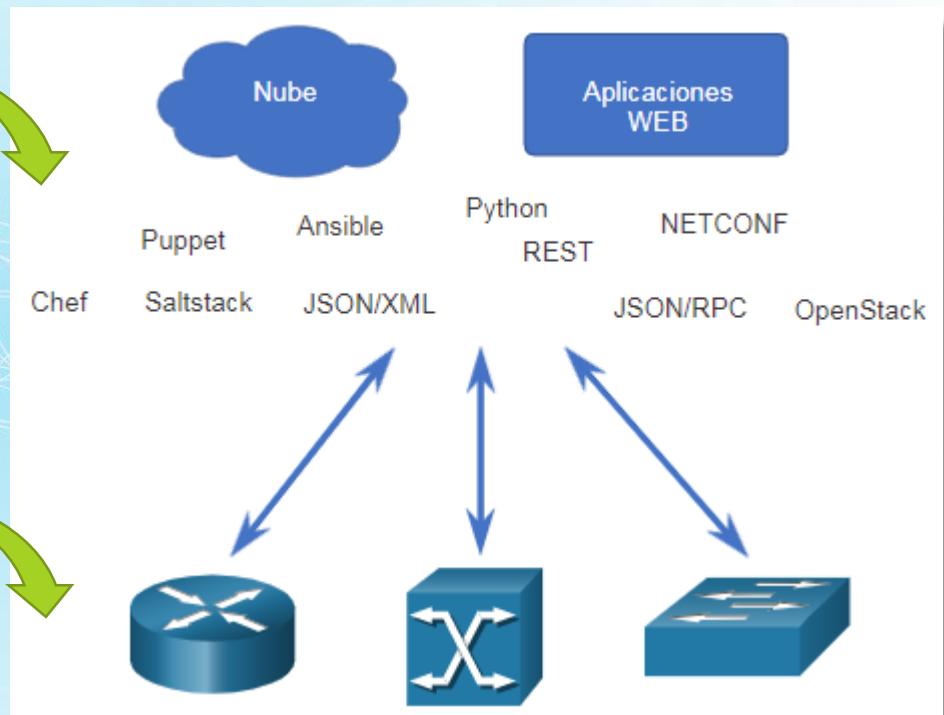
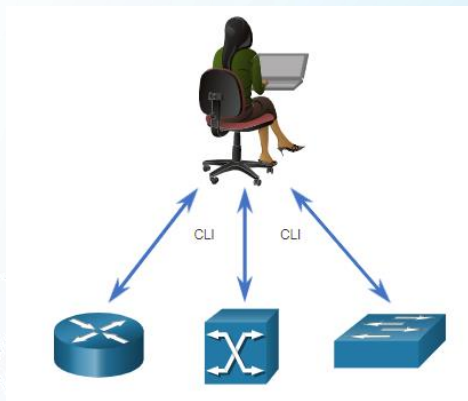
- API REST → API que funciona sobre HTTP.
- Conforme a las restricciones de la arquitectura REST (API Restful)
 - Modelo Cliente – Servidor (intercambiable)
 - Sin estado. Sin datos del cliente en el servidor
 - Cacheable. Orientado a mejora en el rendimiento
 - Operaciones definidas
 - URI (Identifier) // URN (Name) //URL (Localizador)

Anatomía de una solicitud RESTful

Método HTTP	Operación RESTful
POST	Crear (Create)
GET	lectura (Read)
PUT/PATCH	Actualizar (Update)
DELETE	Eliminar (Delete)



Herramientas de Gestión y Configuración + Evolución

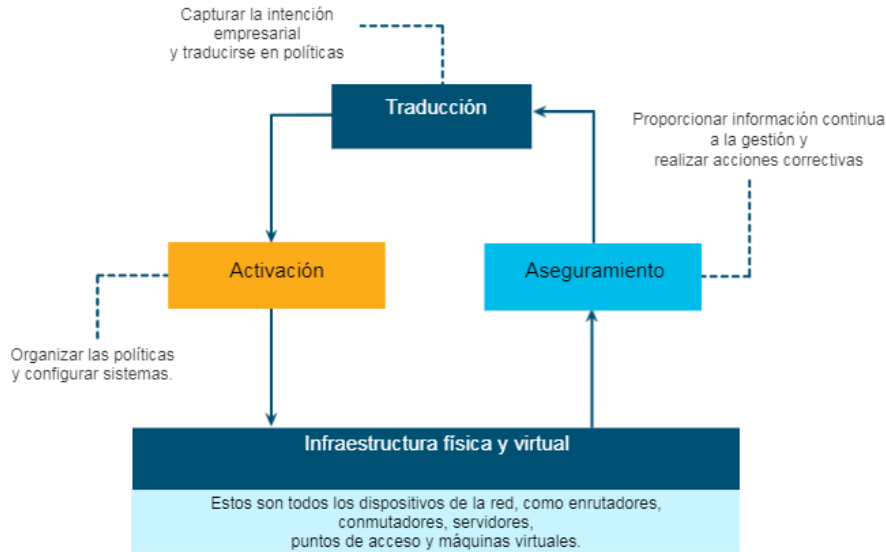


Herramientas de Gestión y Configuración - Comparativa



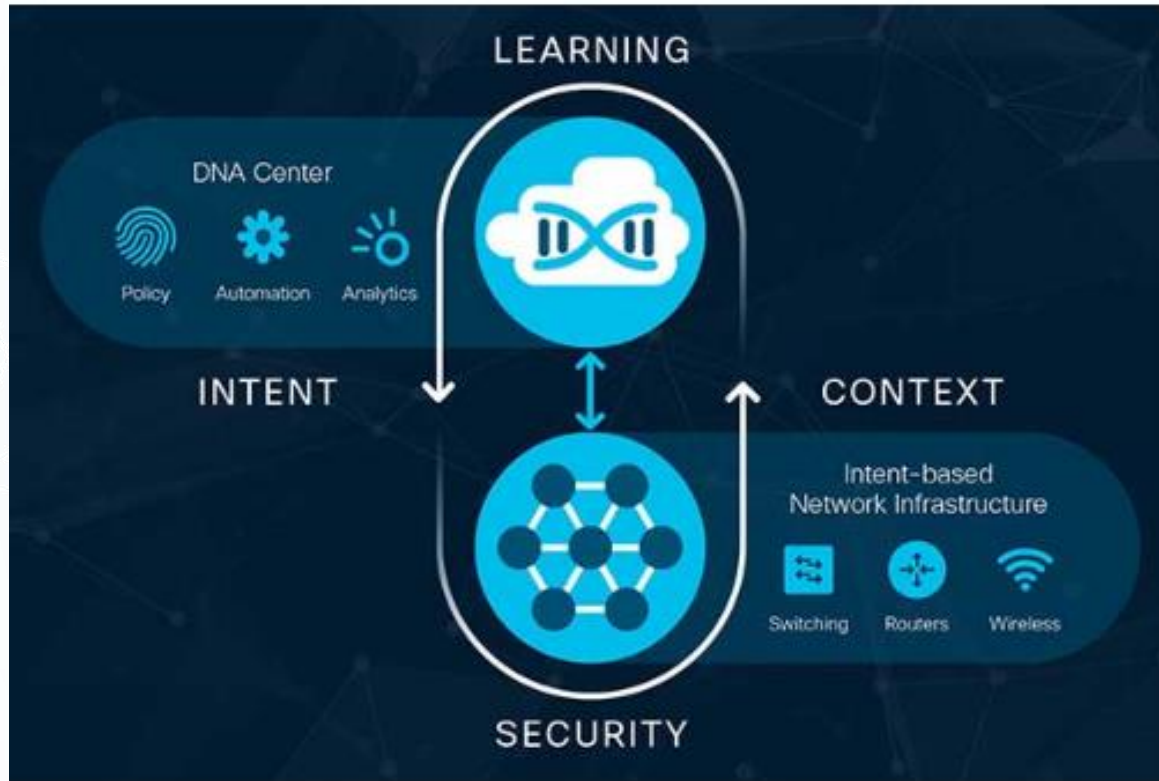
Característica	Ansible	Chef	Puppet	SaltStack
Lenguaje de programación	Python + YAML	Ruby	Ruby	Python
¿Basado en agentes o sin agente?	Sin agente	Basado en agentes	Soporta ambos	Soporta ambos
¿Cómo se administran los dispositivos?	Cualquier dispositivo puede ser "controlador"	Chef Master	Puppet Master	Salt Master
¿Qué crea la herramienta?	Cuaderno de estrategias	Cookbook	Manifiesto	Pilar

IBN (Intent Based Networks)



- **Traducción:** - la función de traducción permite al administrador de red expresar el comportamiento de red esperado que mejor admitirá la intención empresarial.
- **Activación:** - la intención capturada debe interpretarse en directivas que se pueden aplicar a través de la red. La función de activación instala estas directivas en la infraestructura de red física y virtual mediante la automatización en toda la red.
- **Aseguramiento:** - Para comprobar continuamente que la red respeta la intención expresada en cualquier momento, la función de aseguramiento mantiene un bucle continuo de validación y verificación.

Cisco DNA (Digital Network Architecture) Center



Acceso definido por software

Utiliza una estructura de red única a través de LAN y WLAN para crear una experiencia de usuario consistente y altamente segura.

SD-WAN

Utiliza una arquitectura segura entregada en la nube para administrar centralmente las conexiones WAN.

Cisco DNA Assurance

Análisis y ML para mejorar el rendimiento y la resolución de problemas, y realizar predicciones de aseguramiento

Cisco DNA Center Security

Uso de la red como sensor para análisis e inteligencia en tiempo real. control granular para aplicar políticas y contener amenazas en toda la red.

Seguridad e identidad en la LAN (WKSP)

➤ Seguridad e identidad en la LAN (WKSP):

- Dispositivos finales
- Dispositivos de red
- Servicios
- AAA

Primero → Buenas prácticas – Casos Básicos

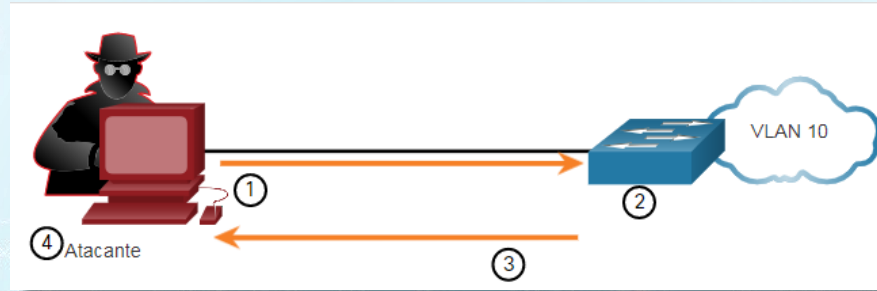
- Proteger accesos al dispositivo y al modo privilegiado:
 - Accesos controlados desde única/s LAN/s (OOB).
 - Solo tráfico de Gestión LAN/VLAN dedicada
 - NO establecer VLAN nativa para tráfico de usuario
 - Nombrado y Protección modo privilegiado

- Acceso seguro a la gestión y configuración de dispositivos de red
 - Habilitar SSH

- Deshabilitar puertos no utilizados

Realizar o comprobar

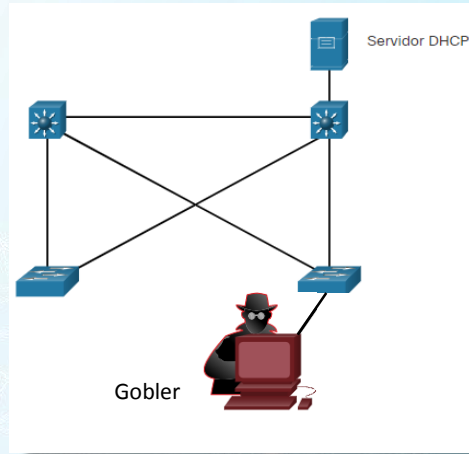
Ataques - 1 – Saturación de las tablas CAM



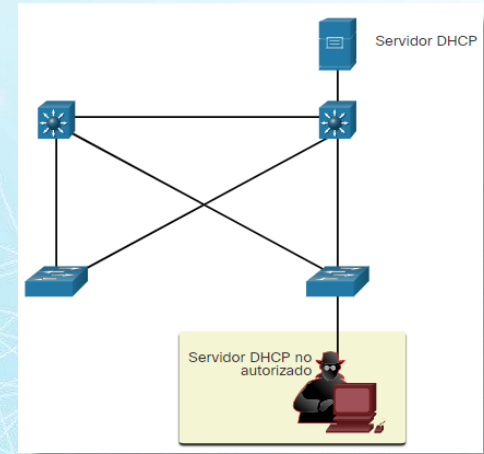
- Herramienta típica de ataque → macof
- Crea tráfico continuo direcciones MAC aleatorias
- Al saturar la tabla con direcciones falsas → Siempre falla el reenvío → Inunda
- Acotado al dominio de Broadcast / VLAN
- EL atacante ve en su puerto el tráfico de todos los dispositivos de la LAN/VLAN
- A efectos prácticos el **SWITCH → HUB**
- **Identidad → El switch no se comporta como switch → No segmenta tráfico**

Ataques - 2 – DHCP Starvation (Ahogamiento o agotamiento) & DHCP Spoofing

Ahogamiento de DHCP



Suplantación de DHCP



- Herramienta típica de ataque → Gobler
- Ahogamiento → es la preparación aunque no tiene porqué ser necesario
 - Se consumen los recursos legítimo (es una DoS)
- Suplantación → Se activa un servidor DHCP no autorizado
 - Control de la información ofrecida a los clientes que soliciten
 - IP - Máscaras – DNS
- Identidad → Suposición Falsa → Mi DHCP ya no es mí DHCP legítimo

Mitigación – Saturación CAM & Ahogamiento de DHCP → Port Security

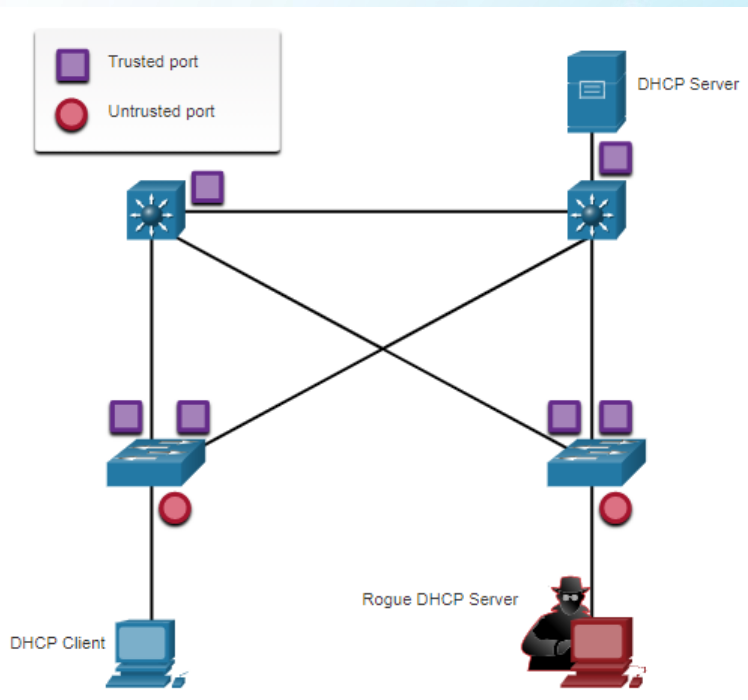
- ¿Dónde? En switches de acceso = en los puertos de acceso
- ¿Cómo? (Usar Interface o interface range)
 - S1(config-if)# **switchport mode access**
 - S1(config-if)# **switchport port-security**

Por defecto – Solo 1 dirección MAC y Modo de violación = Shutdown
Comprobar con → **show port-security interface <>**

- Opciones más específicas: aging / mac-address / máximo / violation:
 - **switchport port-security aging { static | time time | type {absolute | inactivity}}**
 - **switchport port-security mac-address {<mac-address> | sticky }**
 - **switchport port-security maximum <value>**
 - **switchport port-security violation { protect | restrict | shutdown}**
- Recuperación de violación: Shutdown/No shutdown ó “errdisable recovery cause psecure-violation”

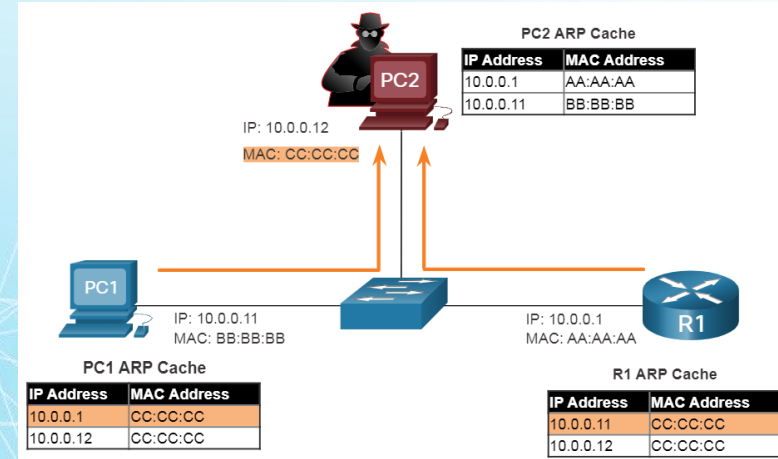
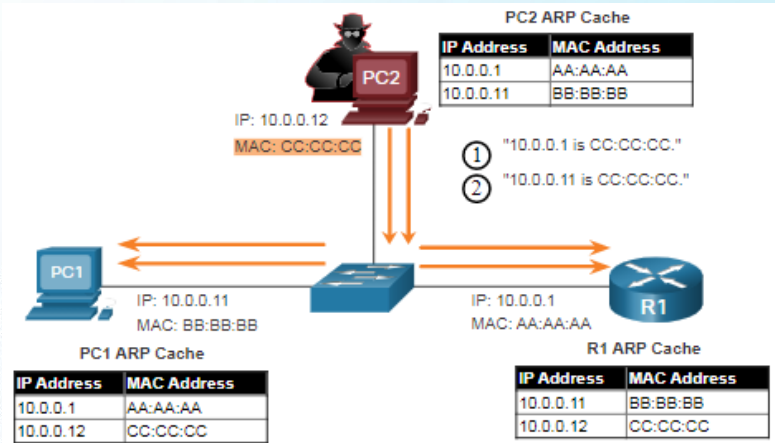
Port Security – No protege del DHCP Spoofing → ¿Entonces? → DHCP Snooping

- DHCP Snooping – IDEA – Conocer el proceso y las topología de servicio de DHCP



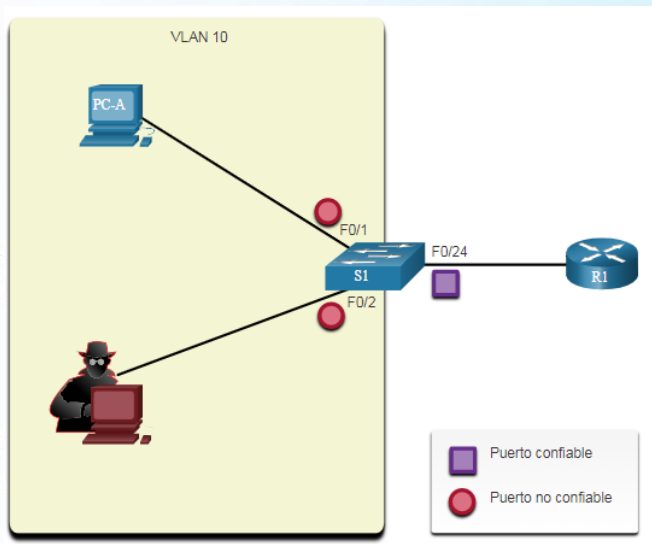
- Habilitar DHCP Snooping globalmente (modo global)
 - `ip dhcp snooping`
- Determinar los interfaces que legítimamente pueden recibir mensajes del servidor → DHCP a Cliente (OFFER)
 - Marcarlos como confiables → `trusted`
 - `ip dhcp snooping trust`
- Los no confiables es posible limitar su rate (conf interface)
 - `ip dhcp snooping limit rate 6`
- Habilitar snooping en las vlans de interés
 - `ip dhcp snooping vlan <vlans>`

Ataques - 3 – ARP Spoofing // ARP Poisoning → Man In The Middle



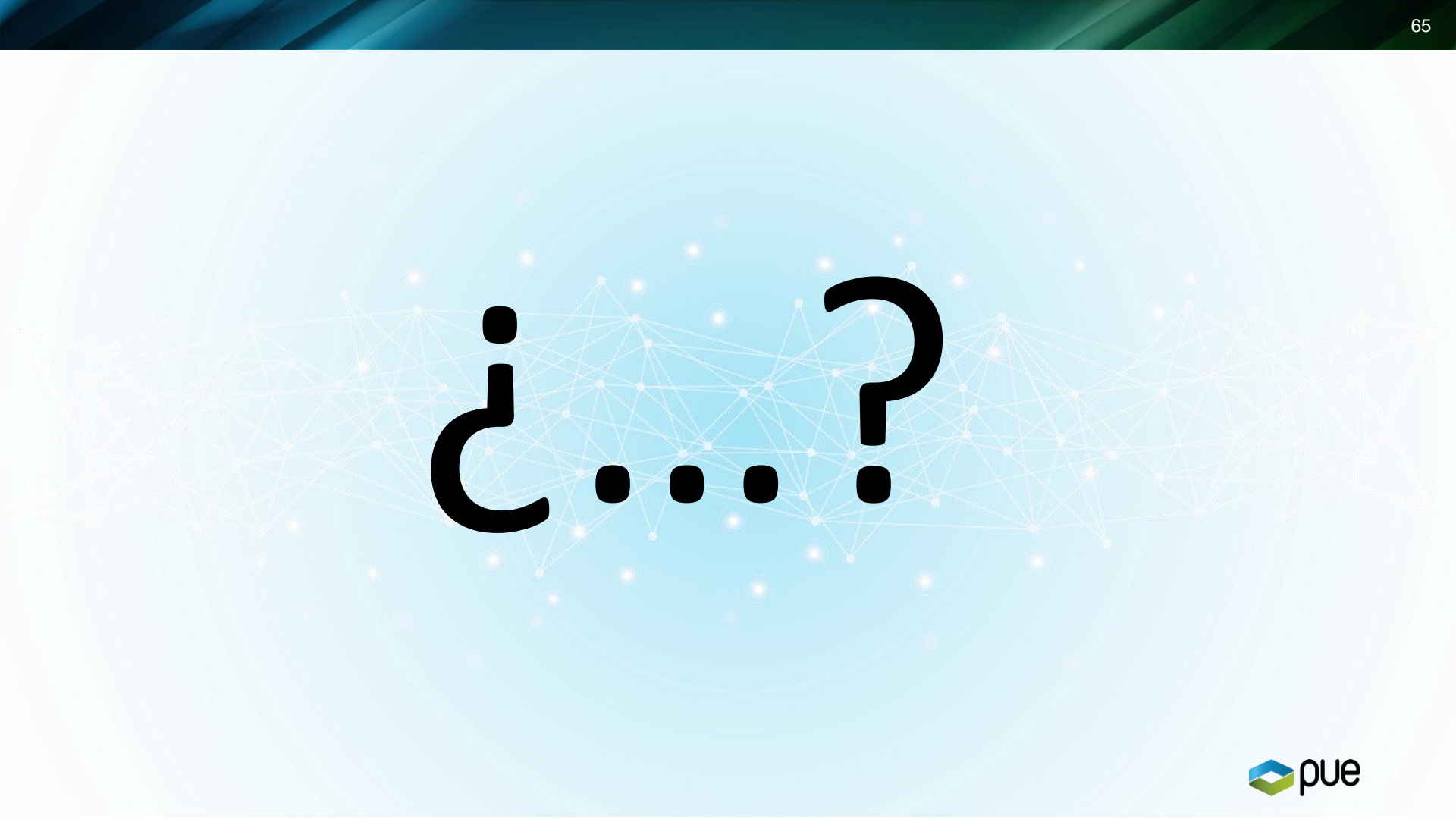
- Por RC se permite a un cliente el envío de ARP gratuitos
- Los clientes que lo ven actualizan sus caches de ARP con dicha información
- Es posible alegar ser cualquier combinación de IP a MAC
- Ejemplo → Suplantar al Gateway de la red
- **Identidad** → **El Gateway de la red no es quien se está informando que es.**

Mitigación - DAI – Dynamic ARP Inspection (basada en DHCP Snooping)



- Habilitar DHCP Snooping
- Habilite DHCP Snooping en las VLAN seleccionadas
- Habilite el DAI en las VLANs seleccionadas (config global)
 - **ip arp inspection vlan <vlan>**
- Configurar DHCP Snooping y DAI en las interfaces confiables (config interface)
 - **ip dhcp snooping trust**
 - **ip arp inspection trust**

- No retransmite ARPs inválidas o gratuitas en otros puertos de la misma VLAN
- Intercepta peticiones y respuestas en puertos no confiables y las valida con los bindings existentes
- Deshabilita la interfaz si se excede el número de paquetes ARP configurado
- Es posible validaciones adicionales – MACs en la Trama vs MACs en el cuerpo de ARP e incluso IP



ج...؟



¡Muchas gracias!

 www.pue.es

 Blog

blog.pue.es



[@ticPUE](https://www.instagram.com/ticPUE)

PUE Services

 sales@pue.es

PUE Training

 training@pue.es

PUE Academy

 pueacademy@pue.es

Certification

 exams@pue.es