



Criptografía



Objetivos

Título del módulo: Criptografía de Clave Pública

Objetivo del módulo: Explicar el papel de la infraestructura de clave pública (PKI, siglas en inglés) en la seguridad de las redes.

Título del tema	Objetivo del tema
Integridad y autenticidad	Explicar el papel que cumple la criptografía para garantizar la integridad y autenticidad de los datos.
Confidencialidad	Explicar cómo los enfoques criptográficos mejoran la confidencialidad de los datos.
Criptografía de clave pública	Explicar la criptografía de clave pública.
Las autoridades y el sistema de confianza de PKI	Explicar cómo funciona la infraestructura de clave pública.
Aplicaciones e impactos de la criptografía	Explique cómo el uso de la criptografía afecta las operaciones de ciberseguridad.

Integridad y autenticidad

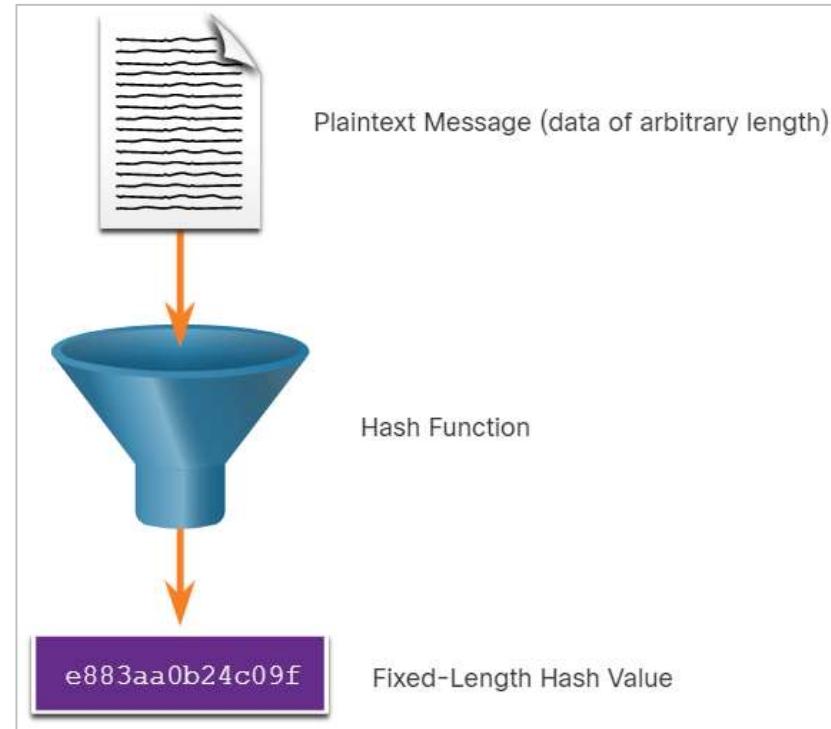
Protegiendo las Comunicaciones

Estos son los cuatro elementos de las comunicaciones seguras:

- **Integridad de los datos:** Garantiza que el mensaje no se haya modificado. Cualquier cambio en los datos en tránsito será detectado. La integridad se garantiza mediante la implementación de los Algoritmos de Seguridad de Hash (Secure Hash Algorithms) SHA-2 o SHA-3. El algoritmo de resumen de mensajes MD5 todavía está en uso, pero debe evitarse ya que es inseguro y crea vulnerabilidades en una red.
- **Autenticación de origen:** Garantiza que el mensaje no sea falso y que el remitente sea el verdadero. Muchas redes modernas garantizan la autenticación con algoritmos, como el Código de Autenticación de Mensaje basado en Hash (HMAC, siglas en inglés).
- **Confidencialidad de los datos:** Garantiza que solamente los usuarios autorizados puedan leer el mensaje. Si se intercepta el mensaje, no se puede descifrar en un plazo razonable. La confidencialidad de los datos se implementa utilizando algoritmos de encriptación simétrica y asimétrica.
- **No repudio de los datos (Data Non-Repudiation):** Garantiza que el remitente no pueda negar ni refutar la validez de un mensaje enviado. No repudio se basa en el hecho de que solamente el remitente tiene las características únicas o una firma de cómo tratar ese mensaje.

Funciones hash criptográficas

- Los "hash" se usan para comprobar y garantizar la integridad de los datos.
- El hashing se basa en una función matemática unidireccional que es relativamente fácil de computar, pero mucho más difícil de revertir.
- Como se ve en la Imagen, una función de hash toma un bloque variable de datos binarios, llamado "mensaje", y produce una representación condensada de longitud fija, denominada hash.
- El hash resultante, a veces, se denomina resumen del mensaje, síntesis o huella digital.

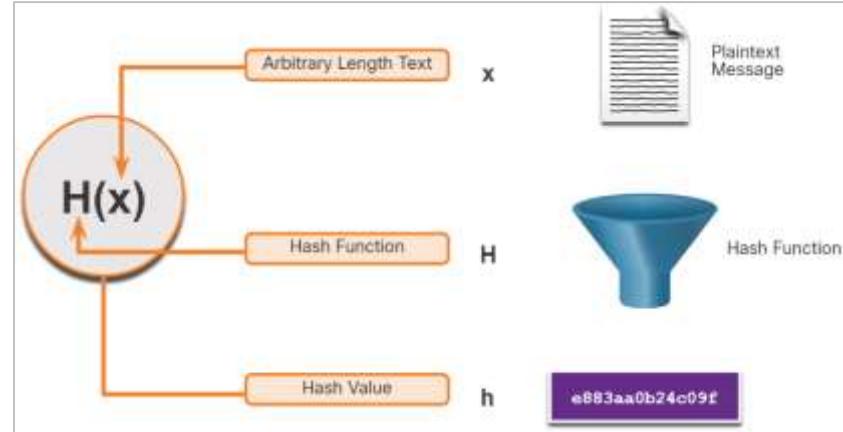


Funciones hash criptográficas

- Con las funciones hash, es computacionalmente imposible que dos conjuntos diferentes de datos tengan el mismo resultado de hash.
- Cada vez que se cambian o se modifican los datos, el valor hash también cambia. Debido a esto, los valores hash criptográficos usualmente se conocen como huellas dactilares digitales.
- Pueden usarse para detectar archivos de datos duplicados, cambios en las versiones de los archivos y otros usos similares.
- Estos valores se utilizan para proteger los datos de un cambio accidental o intencional, o de la corrupción accidental de los datos.
- La función hash criptográfica se aplica en muchas situaciones diferentes con fines de autenticación de entidades, integridad de los datos y autenticidad de los datos.

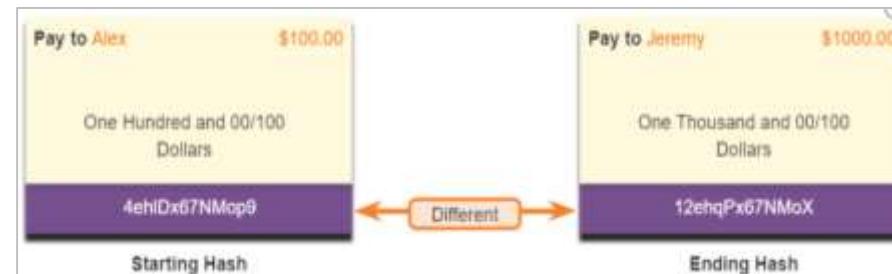
Funcionamiento del hash criptográfico

- Matemáticamente, la ecuación $h = H(x)$ se utiliza para explicar cómo funciona un algoritmo de hash.
- Como se muestra en la imagen, la función de hash H toma un valor de entrada x y arroja una cadena de tamaño fijo con valor de hash h .
- Una función de hash criptográfica tiene las siguientes propiedades:
 - La entrada puede ser de cualquier longitud.
 - La salida tiene una longitud fija.
 - $H(x)$ es relativamente fácil de calcular para cualquier valor dado a x .
 - $H(x)$ es unidireccional y no reversible.
 - $H(x)$ está libre de colisiones, lo que significa que dos valores diferentes de entrada darán como resultado valores diferentes de hash.
 - Si una función de hash es difícil de invertir, se considera un hash unidireccional. Difícil de invertir significa que dado un valor hash de h , es computacionalmente imposible encontrar una entrada para x tal que $h = H(x)$.



MD5 y SHA

- Las funciones de hash se utilizan para garantizar la integridad de un mensaje, garantizando que los datos no hayan sido modificados accidental o intencionalmente.
- En la imagen, el remitente envía una transferencia de \$100 a Alex. El remitente quiere asegurarse de que el mensaje no se modifique accidentalmente en su recorrido hasta el receptor.
- El remitente introduce el mensaje en un algoritmo de hash y calcula el hash de longitud fija.
- Luego, este hash se adjunta al mensaje y se envía al receptor. El mensaje y el hash se transmiten en texto plano.
- El dispositivo receptor elimina el hash del mensaje e introduce el mensaje en el mismo algoritmo de hash. Si el hash calculado es igual al que se adjunta al mensaje, significa que el mensaje no se modificó durante su recorrido. Si los hash son no iguales, ya no es posible garantizar la integridad del mensaje.



MD5 y SHA

Existen tres funciones de hash muy conocidas:

- **MD5 con digest de 128 bits:** Desarrollada por Ron Rivest y utilizada en una variedad de aplicaciones de Internet, MD5 es una función unidireccional que produce un mensaje hash de 128-bits. MD5 es un algoritmo obsoleto y se debe usar solamente cuando no haya mejores alternativas disponibles. Se recomienda utilizar SHA-2 o SHA-3 en su lugar.
- **SHA-1:** Desarrollado por la Agencia Nacional de Seguridad (NSA, siglas en inglés) de los Estados Unidos en 1995. Es muy similar a las funciones de hash MD5. SHA-1 crea un mensaje hash de 160 bits y es un poco más lento que MD5. SHA-1 tiene defectos conocidos y es un algoritmo obsoleto.
- **SHA-2:** Desarrollado por la NSA. Incluye SHA-224, SHA-256, SHA-384 y SHA-512. Si se usa SHA-2, se deben usar los algoritmos SHA-256, SHA-384 y SHA-512.
- **SHA-3:** SHA-3 es el algoritmo hash más nuevo y fue introducido por el instituto NIST como una alternativa para la familia SHA-2 de algoritmos hash. SHA-3 incluye SHA3-224, SHA3-256, SHA3-384 y SHA3-512. La familia SHA-3 es la próxima generación de algoritmos y deben usarse siempre que sea posible.

MD5 y SHA

- Mientras que el hash se puede utilizar para detectar modificaciones accidentales, no brinda protección contra cambios deliberados hechos por un atacante.
- No existe información de identificación única del emisor en el procedimiento de hash.
- Esto significa que cualquier persona puede calcular un hash para los datos, siempre y cuando tengan la función de hash correcta.
- Por lo tanto, el hash es vulnerable a los ataques Man-in-the-middle y no proporciona seguridad a los datos transmitidos. Para proporcionar integridad y autenticación de origen, se necesita algo más.

Nota: Los algoritmos hash solo protegen contra cambios accidentales y no protegen los datos de los cambios realizados deliberadamente por un atacante.

Autenticación de Origen

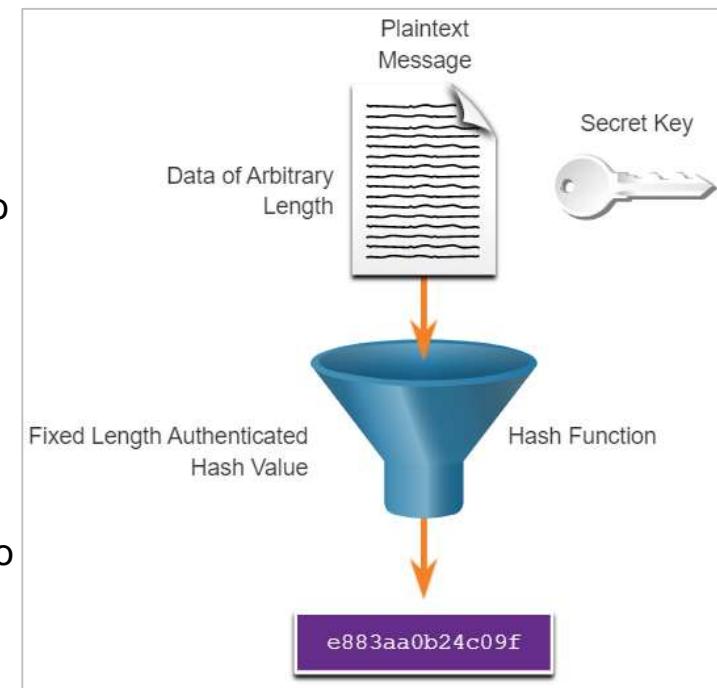
- Para agregar autenticación y control de integridad, se usa un código de autenticación de mensajes hash con clave (Hash-based Message Authentication Code, HMAC).
- Los HMAC utilizan una clave secreta adicional como entrada para la función de hash.

Nota: También se utilizan otros métodos de Código de Autenticación de Mensajes (MAC, siglas en inglés). Sin embargo, HMAC se utiliza en muchos sistemas, incluidos SSL, IPSec y SSH.

Autenticación de Origen

Algoritmo de Hashing de HMAC

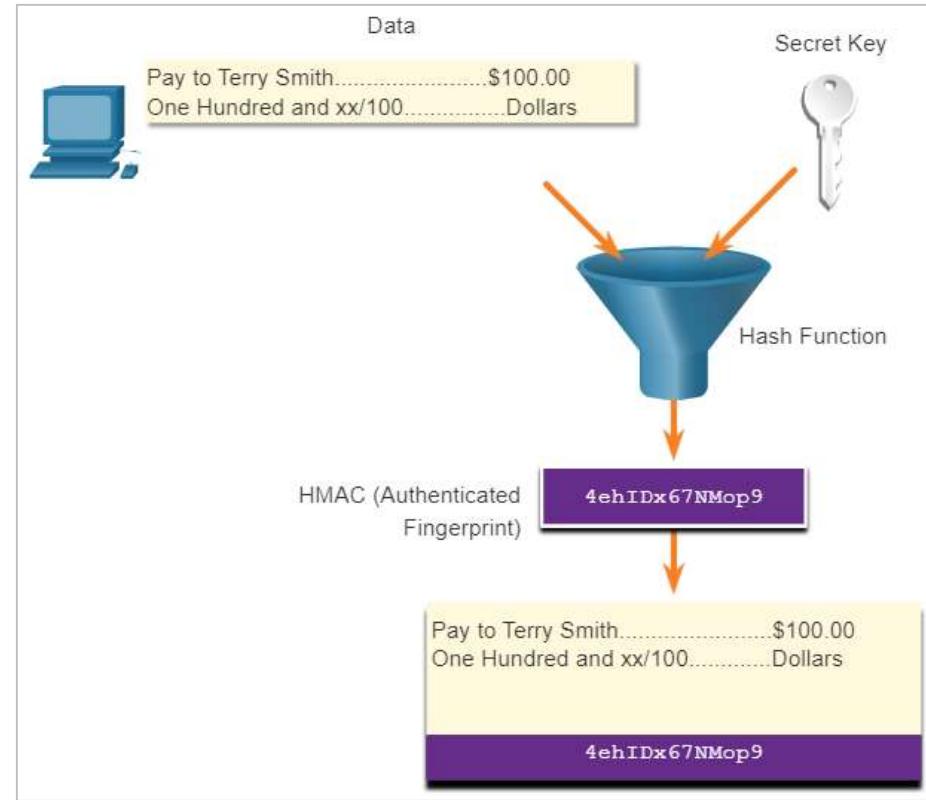
- Como se muestra en la imagen, un HMAC se calcula utilizando cualquier algoritmo criptográfico que combine una función hash criptográfica con una clave secreta. Las funciones de hash son la base del mecanismo de protección de HMAC.
- Solo el emisor y el receptor conocen la clave secreta y el resultado de la función de hash ahora depende de los datos de entrada y la clave secreta. Esta característica derrota los ataques Man-in-the-middle y proporciona autenticación del origen de los datos.
- Si dos personas comparten una clave secreta y utilizan las funciones HMAC para la autenticación, una síntesis de HMAC construida correctamente de un mensaje que ha recibido uno de ellos, indica que la otra persona fue la que originó el mensaje. Esto se debe a que la otra persona posee la clave secreta.



Autenticación de Origen

Creación de un valor HMAC

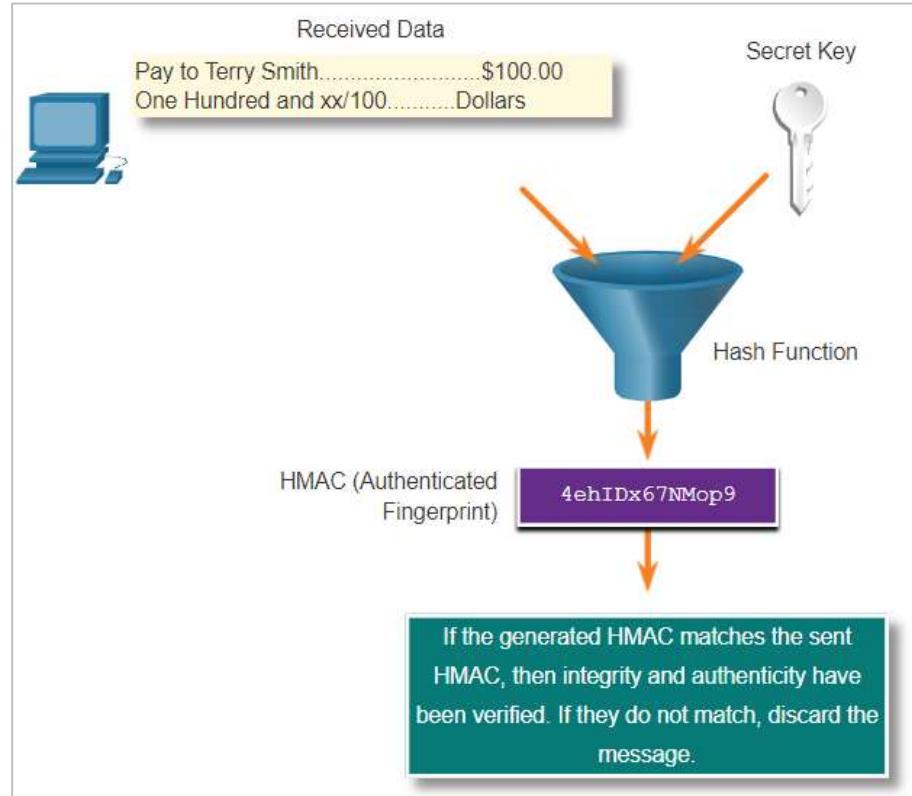
- Como muestra en la imagen, el dispositivo emisor introduce datos en el algoritmo de hash y calcula la síntesis del HMAC de longitud fija.
- Luego, esta síntesis autenticada se adjunta al mensaje y se envía al receptor.



Autenticación de Origen

Verificación de un valor HMAC

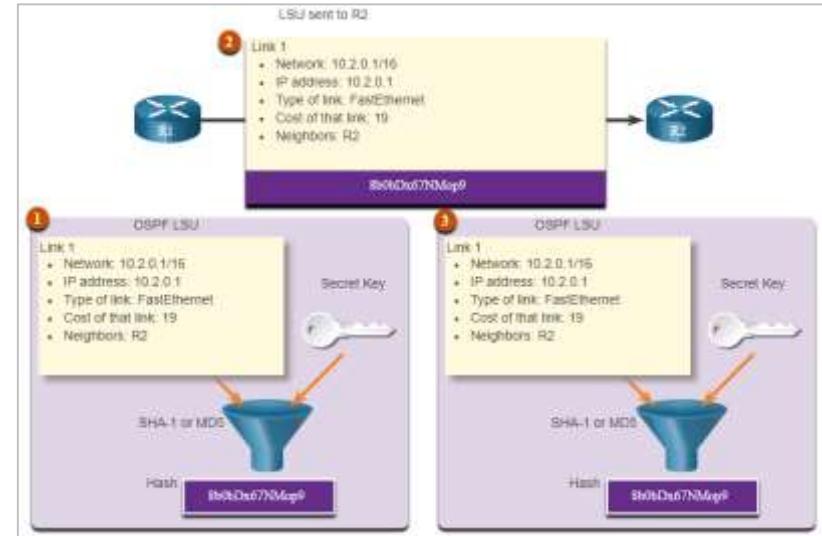
- En la imagen, el dispositivo receptor elimina la síntesis del mensaje y utiliza el mensaje de texto plano con su clave secreta como valor de entrada para la misma función de hash.
- Si la síntesis que calcula el dispositivo receptor es igual a la síntesis que se envió, el mensaje no se modificó.
- Además, el origen del mensaje se autentica porque solamente el emisor posee una copia de la clave secreta compartida. La función de HMAC comprobó la autenticidad del mensaje.



Autenticación de Origen

Ejemplo de HMAC en Router Cisco

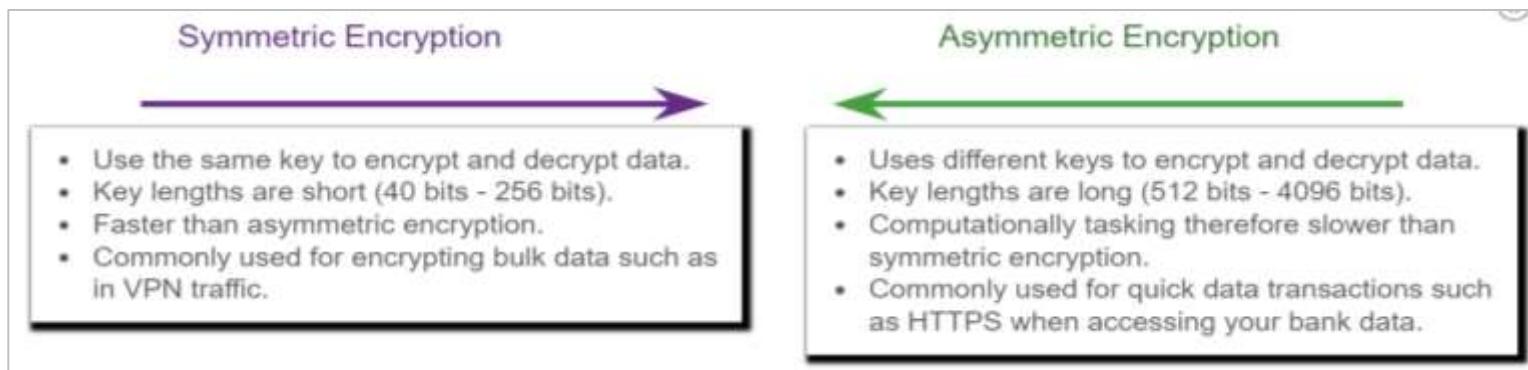
- La figura muestra cómo las HMAC son usadas por los routers Cisco que están configurados para usar autenticación de enrutamiento OSPF.
- R1 esta enviando una actualización de estado de enlace (LSU, siglas en inglés) sobre una ruta hacia la red 10.2.0.0/16:
 - R1 calcula el valor de hash mediante el mensaje de LSU y la clave secreta.
 - El valor de hash resultante se envía con la LSU al R2.
 - R2 calcula el valor de hash mediante la LSU y su clave secreta. R2 acepta la actualización si los valores de hash coinciden. Si no coinciden, R2 descarta la actualización.



Confidencialidad

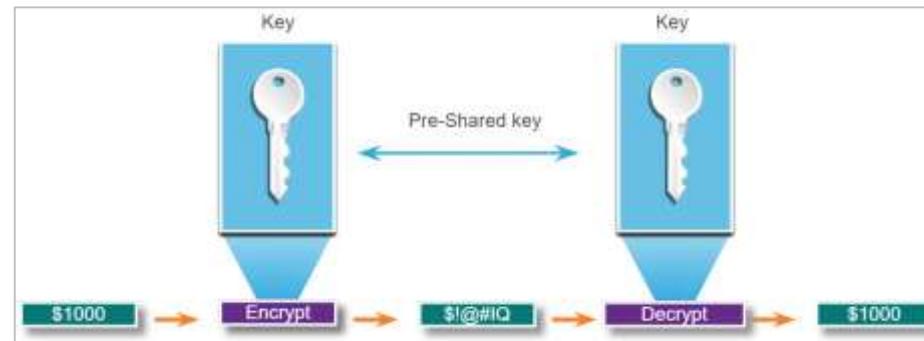
Confidencialidad de los datos

- Hay dos clases de encriptación utilizadas para proporcionar confidencialidad a los datos; simétrica y asimétrica. Estas dos clases se diferencian en cómo utilizan las claves.
- Los algoritmos de encriptación simétrica, como estándar de encriptación de datos (Data Encryption Standard, DES), el DES, y el estándar avanzado de encriptación (Advanced Encryption Standard, AES) se basan en la premisa de que cada parte que se comunica conoce la clave pre-compartida.
- La confidencialidad de los datos también se puede garantizar utilizando algoritmos asimétricos, incluidos Rivest, Shamir y Adleman (RSA) y la infraestructura de clave pública (PKI).
- La imagen destaca las diferencias entre encriptación simétrica y asimétrica.



Encriptación simétrica

- Los algoritmos simétricos utilizan la misma clave pre-compartida para encriptar y desencriptar datos.
- Antes de que ocurra cualquier comunicación encriptada, el emisor y el receptor deben conocer la clave pre-compartida, también llamada clave secreta.
- Para exemplificar cómo funciona la encriptación simétrica, consideremos un ejemplo en el que Alice y Bob viven en diferentes lugares y quieren intercambiar mensajes secretos entre sí mediante el sistema de correo.
- En la figura, Alice y Bob tienen claves idénticas y pre-compartidas. Alice escribe un mensaje secreto y lo coloca en una caja pequeña que ella cierra con el candado y su propia clave. Le envía la caja a Bob. Cuando Bob recibe la caja, utiliza su clave para desbloquear y recuperar el mensaje. Bob puede utilizar la misma caja y la misma clave para enviar una respuesta secreta a Alice.



Encriptación simétrica

- Los algoritmos de encriptación simétrica suelen utilizarse con el tráfico de VPN.
- Esto se debe a que los algoritmos simétricos utilizan menos recursos de CPU que los algoritmos de encriptación asimétrica.
- Esto permite encriptar y desencriptar datos rápidamente cuando se utiliza una VPN.
- Al utilizar algoritmos de encriptación simétrica, mientras más larga sea la clave, más tiempo demorará alguien en descubrirla. La mayoría de las claves de encriptación tienen entre 112 bits y 256 bits.
- Para garantizar que la encriptación sea segura, se recomienda una longitud mínima de clave de 128 bits. Para comunicaciones más seguras, se aconseja el uso de claves más prolongadas.
- Los algoritmos de encriptación simétrica a veces son clasificados como cifrados por bloques o cifrados de flujo.

Encriptación simétrica

Cifrado por bloques

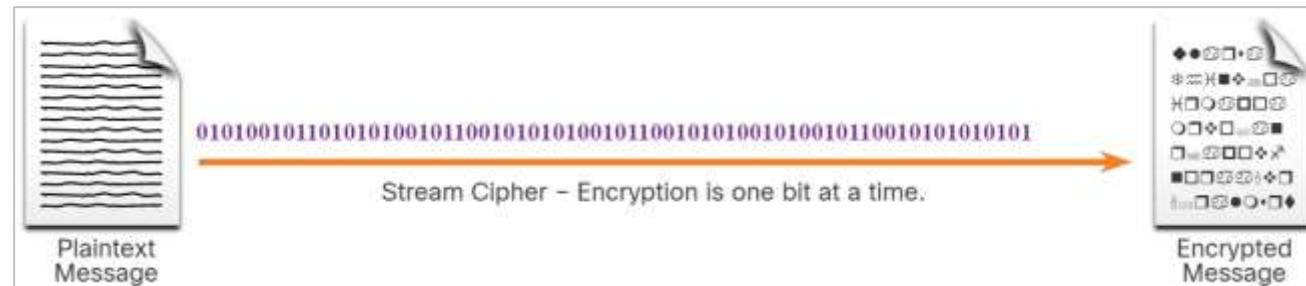
- Los cifrados por bloques transforman un bloque de texto plano de longitud fija en un bloque común de texto cifrado de 64 o 128 bits.
- Los cifrados por bloques comunes incluyen DES con un bloque de tamaño de 64-bits y AES con un bloque de tamaño de 128-bits.



Encriptación simétrica

Cifrado de flujo

- Los cifrados de flujo encriptan el texto plano byte por byte, o bit por bit.
 - Los cifrados de flujo son básicamente un cifrado por bloques con un tamaño de bloque de un byte o bit.
 - Los cifrados de flujo suelen ser más rápidos que los cifrados por bloques, debido a que los datos se encriptan continuamente.
 - Algunos ejemplos del cifrado de flujo son RC4 y A5, que se utiliza para encriptar comunicaciones de telefonía celular GSM.



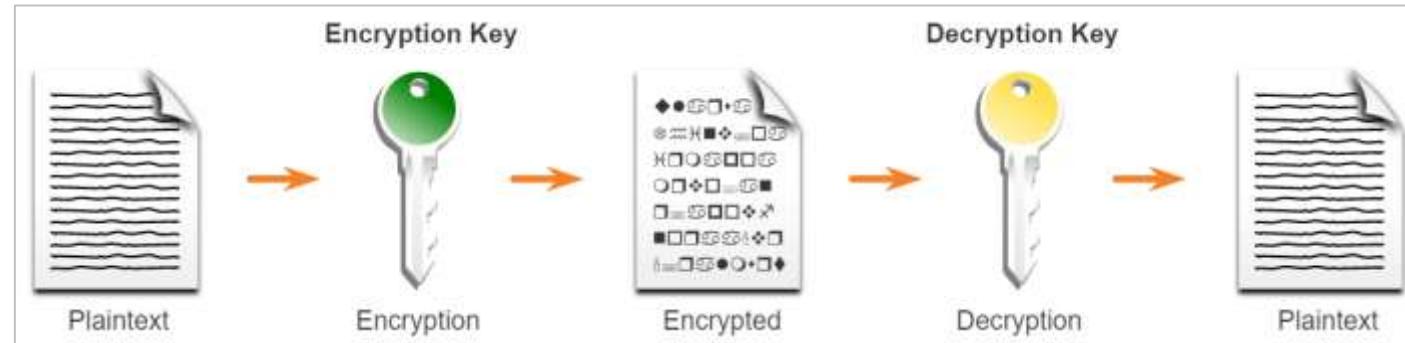
Encriptación simétrica

Los algoritmos de encriptación simétrica bien conocidos se describen en la tabla.

Algoritmos de encriptación simétrica	Descripción
Estándar de encriptación de datos (Data Encryption Standard, DES)	Este es un algoritmo obsoleto. Utiliza una longitud de clave corta, lo cual lo hace inseguro.
3DES (Triple DES)	Este es el reemplazo para DES y repite el algoritmo DES tres veces. Debe evitar usarse, ya que está previsto retirarlo en 2023. Si se implementa, se deben usar claves de muy poco tiempo de vida.
Estándar de encriptación avanzada (Advanced Encryption Standard, AES)	Es un algoritmo de encriptación simétrica popular y recomendado. Ofrece combinaciones de claves de 128, 192 o 256 bits para encriptar bloques de datos de 128, 192 o 256 bits de longitud.
Algoritmo de encriptación optimizado por software (Software-Optimized Encryption Algorithm, SEAL)	Este es un algoritmo más rápido, alternativo a AES. SEAL es un cifrado de flujo que usa un clave de encriptación de 160 bits y tiene un menor impacto en la CPU en comparación con otros algoritmos basados en software.
Algoritmos de Rivest ciphers (RC)	Este algoritmo fue desarrollado por Ron Rivest. RC4 es un cifrado de flujo y se utiliza para proteger el tráfico web. Se ha encontrado que tiene múltiples vulnerabilidades que lo han hecho inseguro. No se debe usar RC4.

Encriptación asimétrica

- Los algoritmos asimétricos, también llamados algoritmos de claves públicas, están diseñados para que la clave de encriptación y la de desencriptación sean diferentes, como se muestra en la imagen.
- Los algoritmos asimétricos utilizan una clave pública y una privada. Ambas claves son capaces de encriptar, pero se requiere la clave complementaria para desencriptar.
- El proceso también es reversible. Los datos encriptados con la clave pública requieren la clave privada para desencriptarse. Los algoritmos asimétricos logran confidencialidad y autenticidad mediante la utilización de este proceso.



Encriptación asimétrica

- La encriptación asimétrica puede utilizar longitudes de claves entre 512 y 4096 bits.
- Longitudes de clave mayores o iguales a 2048 bits son confiables, y mientras que las claves de 1024 bits o más cortas se consideran insuficientes.
- Entre algunos de los ejemplos de protocolos en los que se utilizan algoritmos de claves asimétricos se incluyen los siguientes:
 - **Internet Key Exchange (IKE):** Es un componente fundamental de las VPN con IPsec.
 - **Secure Socket Layer (SSL):** Ahora se implementa como un estándar de Seguridad de la capa de transporte (TLS) de IETF.
 - **Secure Shell (SSH):** Este protocolo proporciona una conexión segura de acceso remoto a dispositivos de red.
 - **Pretty Good Privacy (PGP):** Este programa de computadora proporciona privacidad y autenticación criptográfica. A menudo, se utiliza para aumentar la seguridad de las comunicaciones por correo electrónico.
- Los algoritmos asimétricos son sustancialmente más lentos que los simétricos.

Encriptación asimétrica

En la tabla, se incluyen ejemplos comunes de algoritmo de encriptación asimétrica.

Algoritmos de encriptación asimétrica	Longitud de la Clave	Descripción
Diffie-Hellman (DH)	512, 1024, 2048, 3072, 4096	Permite que ambas partes acuerden una misma clave que pueden utilizar para encriptar los mensajes que quieren enviarse. La seguridad de este algoritmo está basada en que resulta sencillo elevar un número a una determinada potencia, pero difícil calcular qué potencia fue utilizada conociendo solamente el número y el resultado.
Estándar de firmas digitales (Digital Signature Standard, DSS) y Algoritmo de firmas digitales (Digital Signature Algorithm, DSA)	512 – 1024	Especifica a DSA como el algoritmo para firmas digitales. DSA es un algoritmo de clave pública basado en el esquema de firmas El Gamal. La velocidad de creación de firma es similar a la de RSA, pero es de 10 a 40 veces más lenta para la verificación.
Algoritmos de encriptación Rivest, Shamir, Adleman (RSA)	Entre 512 y 2048	Utilizado para criptografía de clave pública, se basa en la dificultad actual de factorización de números muy grandes. Es el primer algoritmo apto tanto para firmas como para encriptación. Es ampliamente utilizado en protocolos de comercio electrónico y se considera seguro si se utilizan claves suficientemente prolongadas e implementaciones actualizadas.

Encriptación asimétrica

Algoritmos de encriptación asimétrica	Longitud de la Clave	Descripción
EIGamal	512 – 1024	Un algoritmo de encriptación de claves asimétrico para criptografía de claves públicas basado en el acuerdo de claves Diffie-Hellman. Una desventaja del sistema EIGamal es que el mensaje encriptado se vuelve muy grande, aproximadamente el doble del tamaño del mensaje original y por ello sólo se utiliza con mensajes pequeños como claves secretas.
Técnicas de curvas elípticas.	224 o superior	Se puede utilizar para adaptar muchos algoritmos criptográficos, como los de Diffie-Hellman o EIGamal. La principal ventaja es que las claves pueden ser mucho más pequeñas.

Encriptación asimétrica

- Los algoritmos asimétricos se usan para brindar confidencialidad sin compartir previamente una contraseña.
- El objetivo de confidencialidad de los algoritmos asimétricos se inicia cuando comienza el proceso de encriptación con la clave pública.
- El proceso puede resumirse con la fórmula:

Clave pública (Encriptar) + Clave privada (Desencriptar) =

Confidencialidad

- Cuando se utiliza la clave pública para encriptar los datos, debe utilizarse la clave privada para desencriptarlos.
- Solamente un host tiene la clave privada; por lo tanto, se logra la confidencialidad.
- Si la clave privada está en riesgo, se debe generar otro par de claves para reemplazar la clave comprometida.

Encriptación asimétrica - Confidencialidad

Veamos cómo se pueden utilizar las claves privadas y públicas para proporcionar confidencialidad al intercambio de datos entre Bob y Alice.

Alice adquiere la clave pública de Bob.

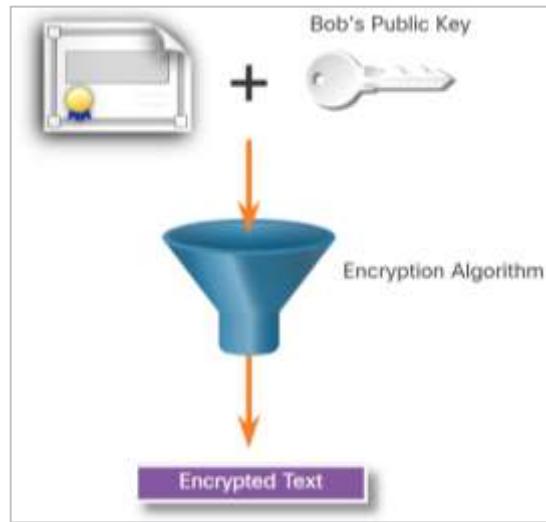
Alice solicita y obtiene la clave pública de Bob.



Encriptación asimétrica - Confidencialidad

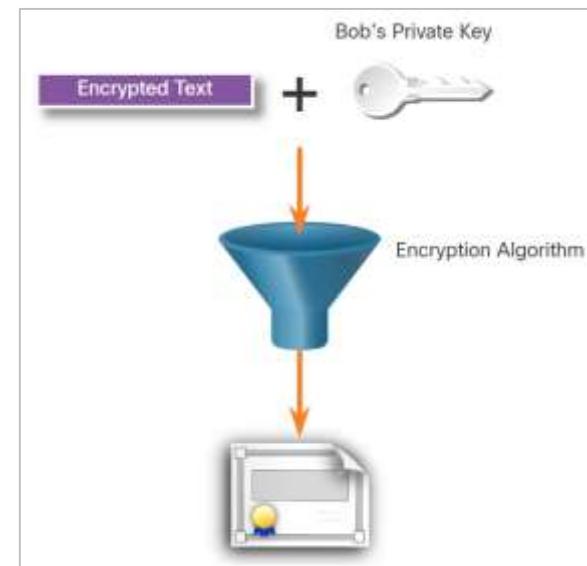
Alice utiliza la clave pública

Alice utiliza la clave pública de Bob para encriptar un mensaje con un algoritmo acordado. Alice le envía el mensaje encriptado a Bob.



Bob desencripta el mensaje utilizando su clave privada

Bob utiliza su clave privada para desencriptar el mensaje, dado que Bob es el único con la clave privada, el mensaje de Alice solo puede ser desencriptado por Bob y así se logra la confidencialidad.



Encriptación asimétrica - Autenticación

- El objetivo de autenticación de los algoritmos asimétricos se inicia cuando comienza el proceso de encriptación con la clave privada.
- El proceso puede resumirse con la fórmula:

Clave privada (Encriptar) + Clave pública (Desencriptar) = Autenticación

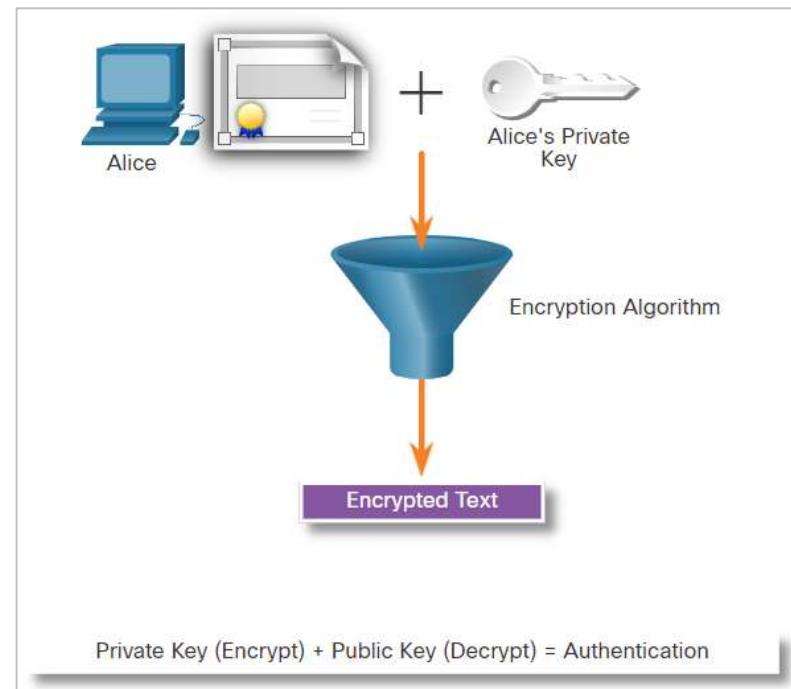
- Cuando se utiliza la clave privada para encriptar los datos, debe utilizarse la clave pública correspondiente para desencriptarlos.
- Debido a que un solo host tiene la clave privada, ese host es el único que puede haber encriptado el mensaje, lo que proporciona autenticación del remitente.
- Por lo general, no se intenta preservar el secreto de la clave pública, por lo que muchos hosts pueden desencriptar el mensaje.
- Cuando un host desencripta correctamente un mensaje con una clave pública, se confía en que la clave privada encriptó el mensaje y permite verificar quién es el remitente. Esta es una forma de autenticación.

Encriptación asimétrica - Autenticación

Veamos cómo se pueden usar las claves privadas y públicas para proporcionar autenticación al intercambio de datos entre Bob y Alice.

Alice utiliza su clave privada

- Alice encripta el mensaje utilizando su clave privada
- Alice le envía el mensaje encriptado a Bob.
- Bob necesita autenticar que el mensaje realmente provino de Alice.



Encriptación asimétrica - Autenticación

Bob solicita la clave pública de Alice

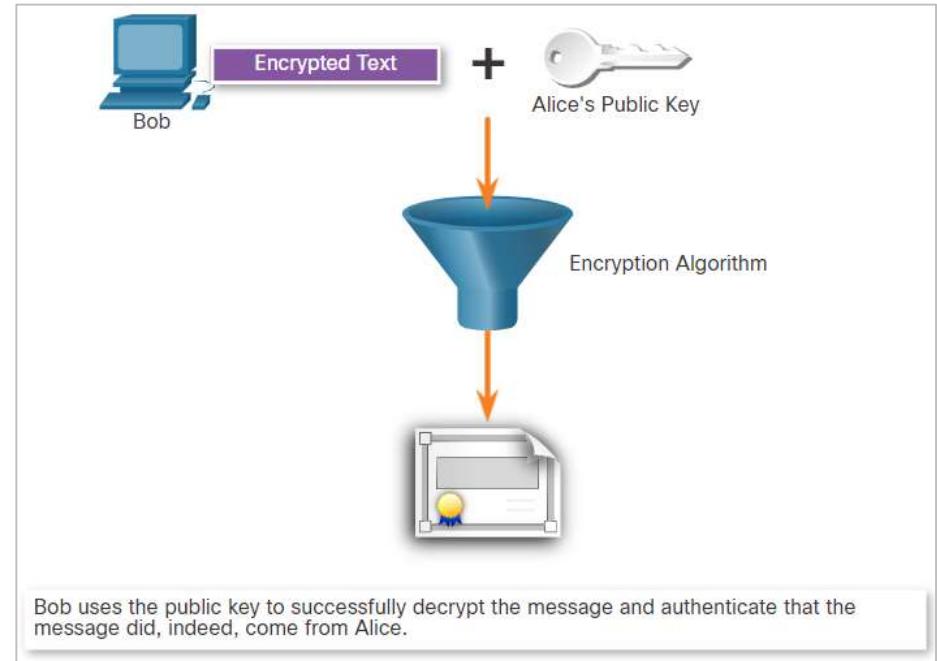
Para autenticar el mensaje, Bob solicita la clave pública de Alice.



Encriptación asimétrica - Autenticación

Bob desencripta usando la clave pública

Bob utiliza la clave pública de Alice para desencriptar el mensaje.



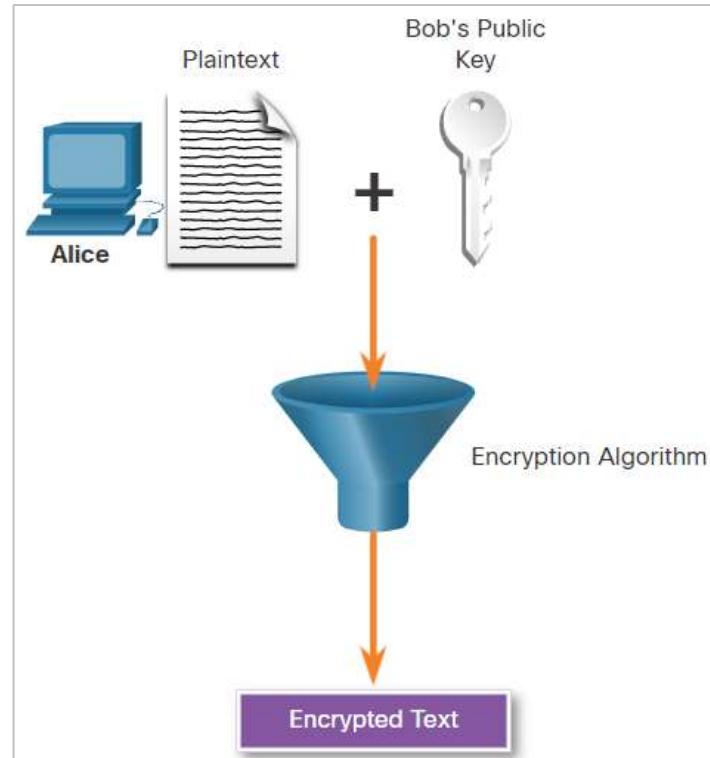
Encriptación asimétrica - Integridad

Combinar los dos procesos de encriptación asimétrica proporciona confidencialidad, autenticación e integridad.

En este ejemplo, se cifrará un mensaje con la clave pública de Bob y se encriptará un hash cifrado con la clave privada de Alice para proporcionar confidencialidad, autenticidad e integridad.

Alice utiliza la clave pública de Bob

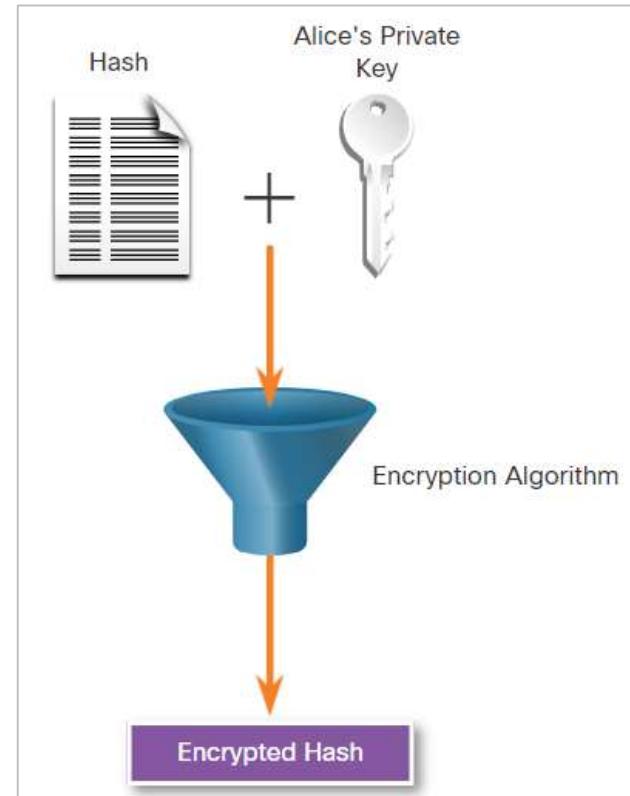
Alice quiere enviar un mensaje a Bob con la seguridad de que solo él podrá leerlo. Alice quiere garantizar la confidencialidad del mensaje. Alice utiliza la clave pública de Bob para cifrar el mensaje. Solo Bob podrá descifrarlo usando su propia clave privada.



Encriptación asimétrica - Integridad

Alice encripta un hash con su propia clave privada

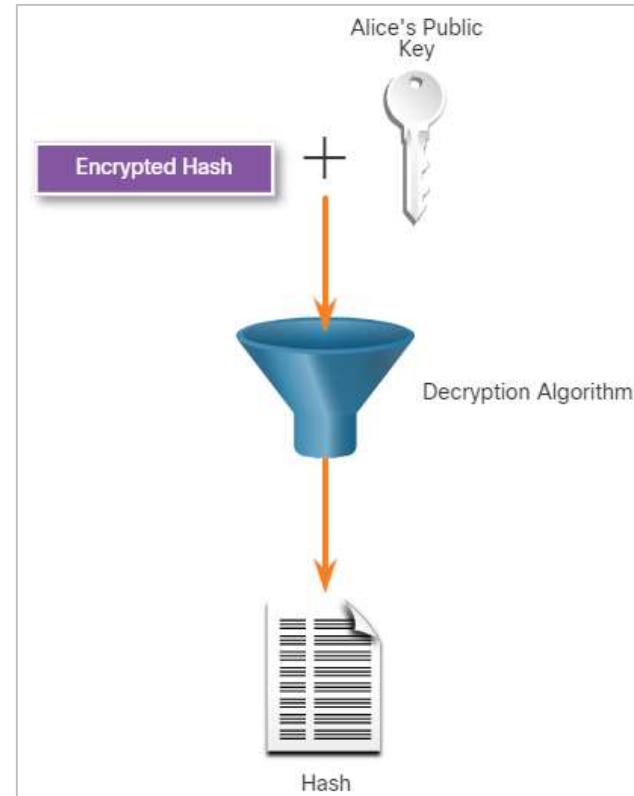
- Alice también quiere garantizar la integridad y autenticación de los mensajes.
- La autenticación le garantiza a Bob que el documento fue enviado por Alice y la integridad asegura que no se modificó.
- Alice utiliza su clave privada para cifrar un hash del mensaje.
- Alice envía el mensaje encriptado con su hash encriptado a Bob.



Encriptación asimétrica - Integridad

Bob utiliza la clave pública de Alice para desencriptar el hash

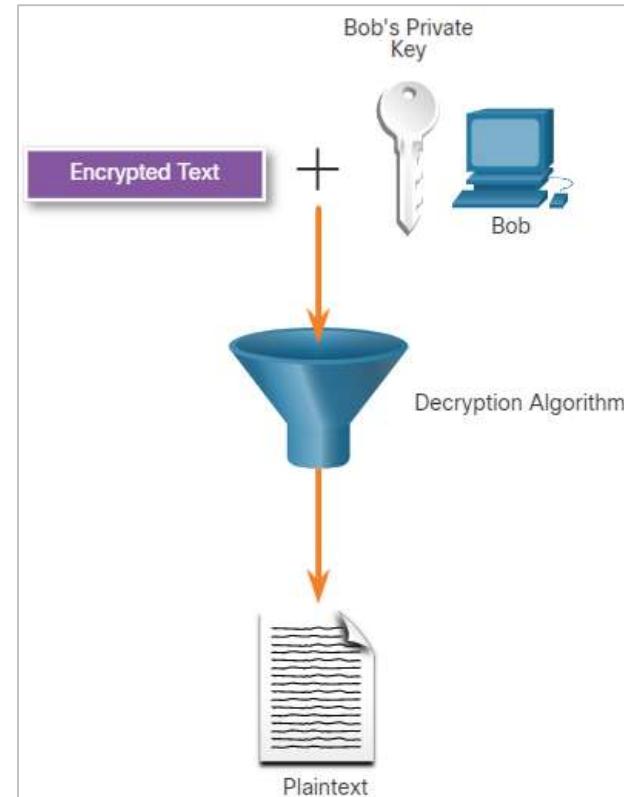
- Bob utiliza la clave pública de Alice para verificar que no se modificó el mensaje.
- El hash recibido equivale al hash determinado localmente según la clave pública de Alice.
- Además, esto verifica que Alice definitivamente es la remitente del mensaje, porque nadie más tiene la clave privada de Alice.



Encriptación asimétrica - Integridad

Bob utiliza su clave privada para desencriptar el mensaje

Bob utiliza su clave privada para descifrar el mensaje

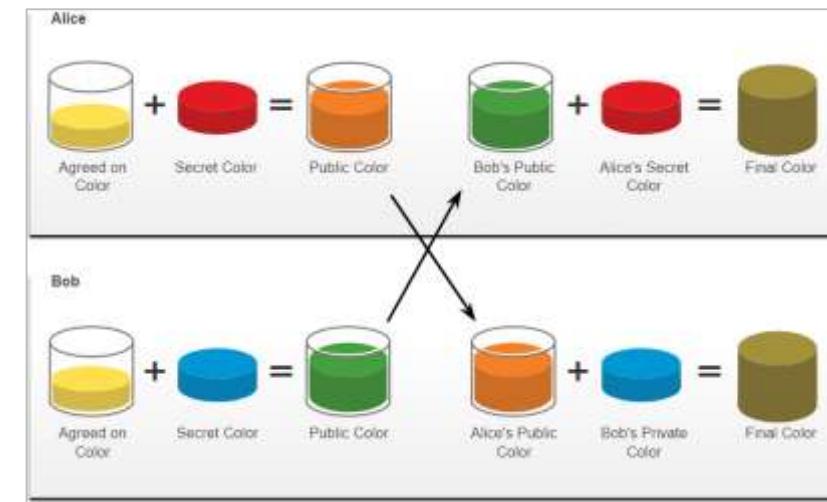


Diffie-Hellman

- Diffie-Hellman (DH) es un algoritmo matemático asimétrico que permite a dos computadoras generar un secreto compartido idéntico sin antes haberse comunicado.
- El emisor y el receptor nunca intercambian realmente la nueva clave compartida.
- Sin embargo dado que ambos participantes la conocen, la clave puede ser utilizada por un algoritmo de encriptación para encriptar tráfico entre los dos sistemas.
- Estos son dos ejemplos de casos en los que el algoritmo de DH suele utilizarse:
 - Se intercambian datos mediante una VPN con IPsec
 - Se intercambian datos de SSH

Diffie-Hellman

- La imagen muestra como funciona DH. Los colores son utilizados en lugar de números largos y complejos para simplificar el proceso de acuerdo de claves del algoritmo DH.
- El intercambio de claves DH comienza con Alice y Bob acordando un color, en este caso el amarillo.
- Luego, Alice y Bob seleccionan un color secreto cada uno. Alice eligió rojo y Bob, azul.
- Ahora, Alice y Bob mezclan el color común compartido (amarillo) con su color secreto respectivo para producir un color público.
- Alice envía su color público (anaranjado) a Bob y Bob le envía el suyo (verde) a Alice.
- Alice y Bob mezclan cada uno el color que recibieron con su propio color secreto original (rojo para Alice y azul para Bob). El resultado es una mezcla final de color marrón que es idéntica para Bob y Alice. El color marrón representa la clave secreta que comparten Bob y Alice.



Diffie-Hellman

- La seguridad del algoritmo de DH se basa en el hecho de que utiliza números increíblemente grandes en sus cálculos.
- Diffie-Hellman utiliza grupos de DH diferentes para determinar la solidez de la clave que se utiliza en el proceso de acuerdo de clave. Los grupos superiores de números son más seguros, pero requieren tiempo adicional para calcular la clave.
- A continuación, se identifican los grupos de DH compatibles con el software Cisco IOS y su valor asociado de número primo:
 - DH Grupo 1: 768 bits
 - DH Grupo 2: 1024 bits
 - DH Grupo 5: 1536 bits
 - DH Grupo 14: 2048 bits
 - DH Grupo 15: 3072 bits
 - DH Grupo 16: 4096 bits

Nota: Un acuerdo de clave de DH también puede estar basado en la criptografía de curva elíptica. Los grupos de DH 19, 20 y 24, si se basan en la criptografía de curva elíptica, son compatibles con el software Cisco IOS.

Criptografía de clave pública

Criptografía de clave pública

Uso de firmas digitales

- Las firmas digitales son una técnica matemática empleada para brindar autenticidad, integridad, y no repudio.
- Las firmas digitales tienen propiedades específicas que permiten la autenticación de entidades y la integridad de los datos. Además, las firmas digitales proporcionan no repudio a la transacción.
- En otras palabras, la firma digital sirve como prueba legal de que el intercambio de datos tuvo lugar. Las firmas digitales usan criptografía asimétrica.
- Las propiedades de las firmas digitales son las siguientes:
 - **Auténtica:** La firma no puede ser falsificada y permite demostrar que el firmante fue el único que firmó el documento.
 - **Inalterable:** Despues de firmar un documento, no puede modificarse.
 - **No reutilizable:** La firma del documento no se puede transferir a otro documento.
 - **No repudiado:** Se considera que el documento firmado es el mismo que un documento físico. La firma es una prueba de que el documento ha sido firmado por la persona real.

Uso de firmas digitales

- Las firmas digitales se utilizan comúnmente en las siguientes dos situaciones:
 - **Firma de código :** Se utiliza para fines de integridad y autenticación de datos. La firma de código se utiliza para verificar la integridad de los archivos ejecutables descargados del sitio web de un proveedor. También utiliza certificados digitales firmados para autenticar y verificar la identidad del sitio de donde provienen los archivos.
 - **Certificados digitales:** Son similares a una tarjeta ID de identificación virtual y se usan para autenticar la identidad del sistema con un sitio web de un proveedor, además de establecer una conexión encriptada para intercambiar datos confidenciales.

Uso de firmas digitales

Se utilizan tres algoritmos del estándar de firmas digitales (Digital Signature Standard, DSS) para generar y verificar firmas digitales:

- **Algoritmo de Firma Digital (Digital Signature Algorithm, DSA)** : DSA es el estándar original para generar pares de claves públicas y privadas, y para generar y verificar firmas digitales.
- **Algoritmo de Rivest-Shamir-Adelman (RSA)**: Es un algoritmo asimétrico que se utiliza comúnmente para generar y verificar firmas digitales.
- **Algoritmo de firma digital de curva elíptica (Elliptic Curve Digital Signature Algorithm, ECDSA)**: Es una nueva variante de DSA y proporciona autenticación de firma digital y no repudio, con los beneficios agregados de eficiencia informática, tamaños de firma pequeños y ancho de banda mínimo.

En los noventa, RSE Security Inc. comenzó a publicar estándares de criptografía de clave pública (Public-Key Cryptography Standards, PKCS). Hubo 15 PKCS, aunque se ha retirado 1 desde el momento en que se escribió el presente contenido.

Firmas digitales para la firma de código

Las firmas digitales suelen usarse para proporcionar certeza de la autenticidad e integridad del código de software.

Los archivos ejecutables están dentro de un sobre firmado digitalmente, lo que le permite al usuario final verificar la firma antes de instalar el software.

Firmar código en forma digital proporciona varias garantías con respecto al código:

- El código es auténtico y realmente es provisto por el editor.
- El código no se ha modificado desde que salió del editor de software.
- El editor definitivamente editó y publicó el código. Esto proporciona no repudio de la acción de publicación.

El propósito del software firmado digitalmente es asegurar que no se alteró y que, como se dice, proviene de una fuente de confianza.

Las firmas digitales sirven como verificación de que el código no ha sido manipulado por atacantes y que un tercero no insertó código malicioso en el archivo.

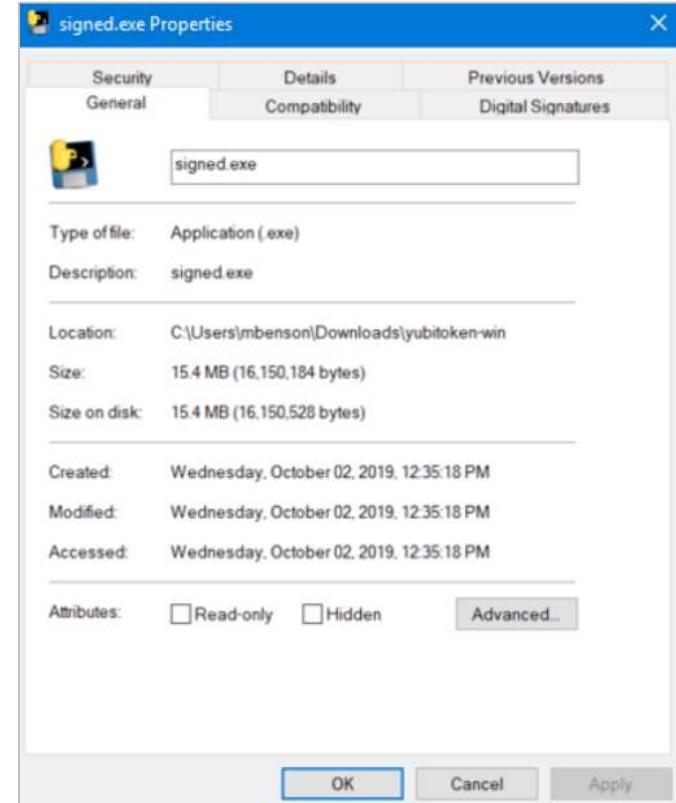
Criptografía de clave pública

Firmas digitales para la firma de código

Las propiedades de un archivo que tiene un certificado firmado digitalmente son las siguientes:

Propiedades de archivo

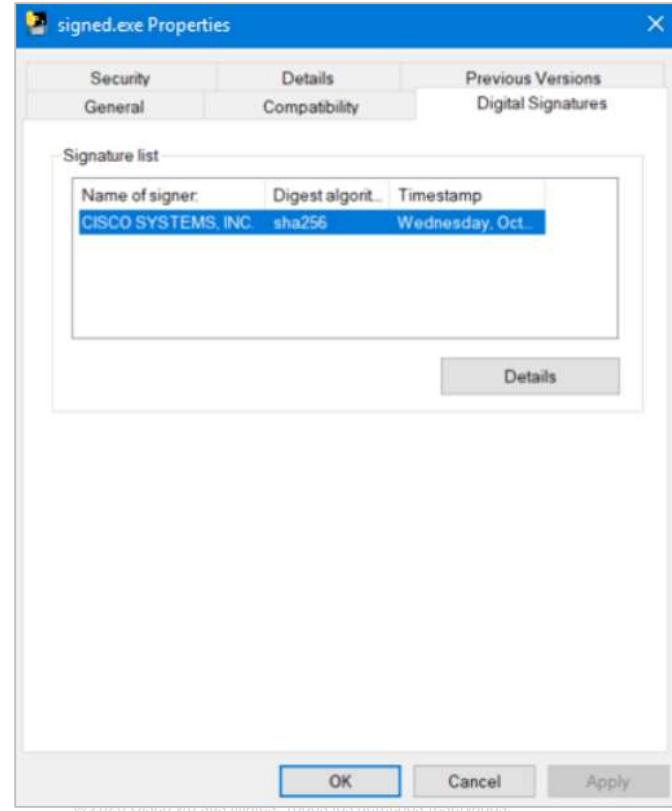
El archivo ejecutable fue descargado de internet. El archivo contiene una herramienta de software de Cisco Systems.



Firmas digitales para la firma de código

Firmas digitales

- Hacer clic en la pestaña **Firmas digitales** revela que el archivo procede de una organización de confianza, Cisco Systems Inc. El resumen (digest) del archivo fue creado con el algoritmo sha256.
- También se proporciona la fecha en la que se firmó el archivo.
- Al hacer clic en **Detalles** se abre la ventana Detalles de firmas digitales.

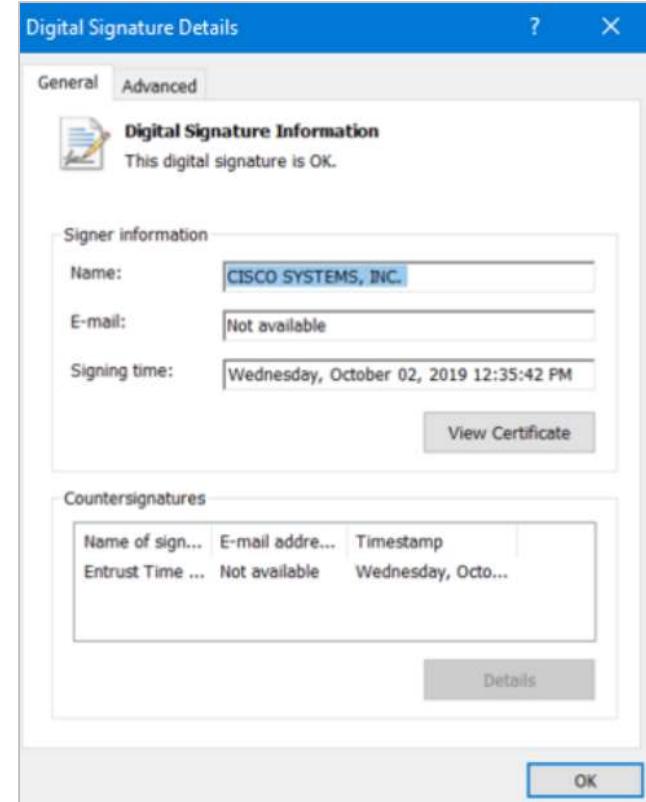


Criptografía de clave pública

Firmas digitales para la firma de código

Detalles de la Firma Digital

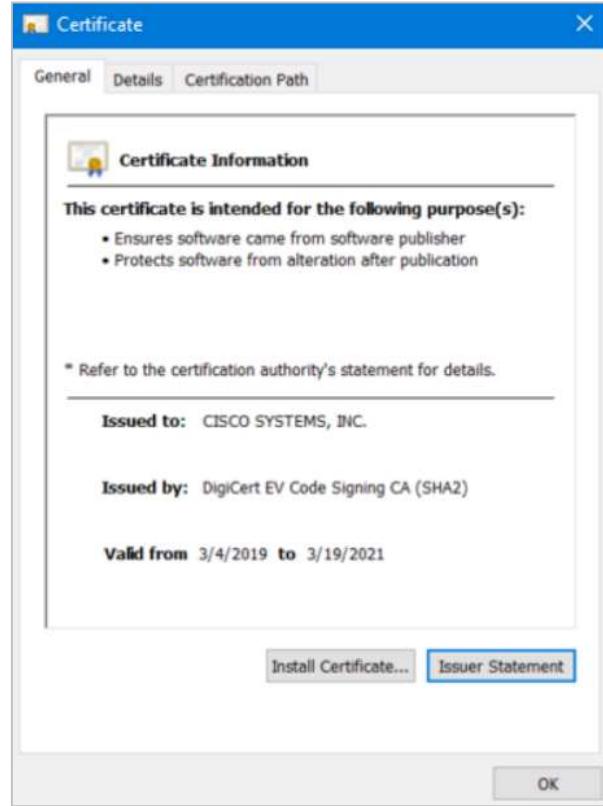
- La ventana Detalles de la firma digital revela que el archivo fue firmado por Cisco Systems, Inc en octubre de 2019.
- Esto se verificó mediante un refrendo proporcionado por Entrust Time Stamping Authority el mismo día en que fue firmada por Cisco.
- Haga clic en **Ver certificado** para ver los detalles del propio certificado.



Firmas digitales para la firma de código

Información sobre Certificados

- La pestaña **General** proporciona los propósitos del certificado, a quién se emitió el certificado y quién lo emitió.
- También muestra el período para el que el certificado es válido. Los certificados no válidos pueden impedir que se ejecute el archivo.



Firmas digitales para la firma de código

Ruta de Certificación

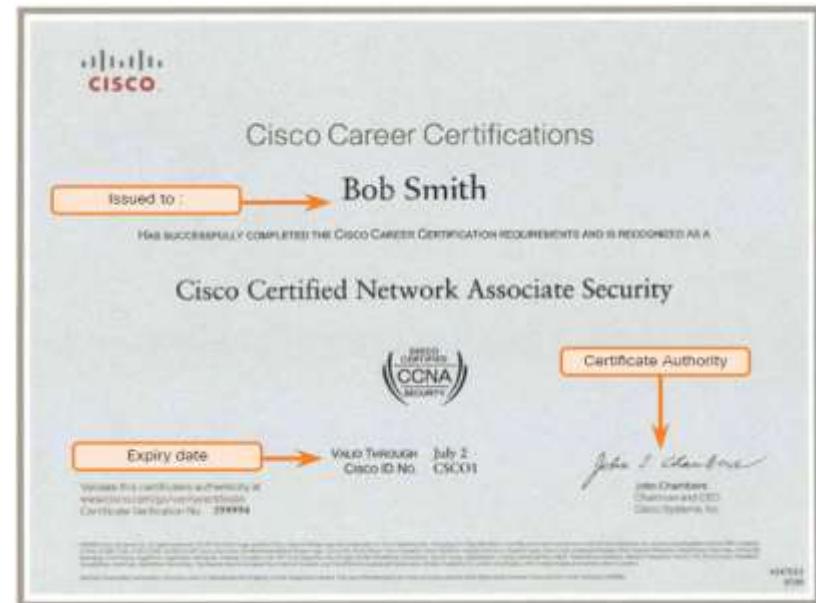
- Haga clic en la pestaña **Ruta de certificación** para ver que el archivo fue firmado por Cisco Systems, como se verificó en DigiCert.
- En algunos casos, una entidad adicional puede verificar independientemente el certificado.



Criptografía de clave pública

Firmas digitales para certificados digitales

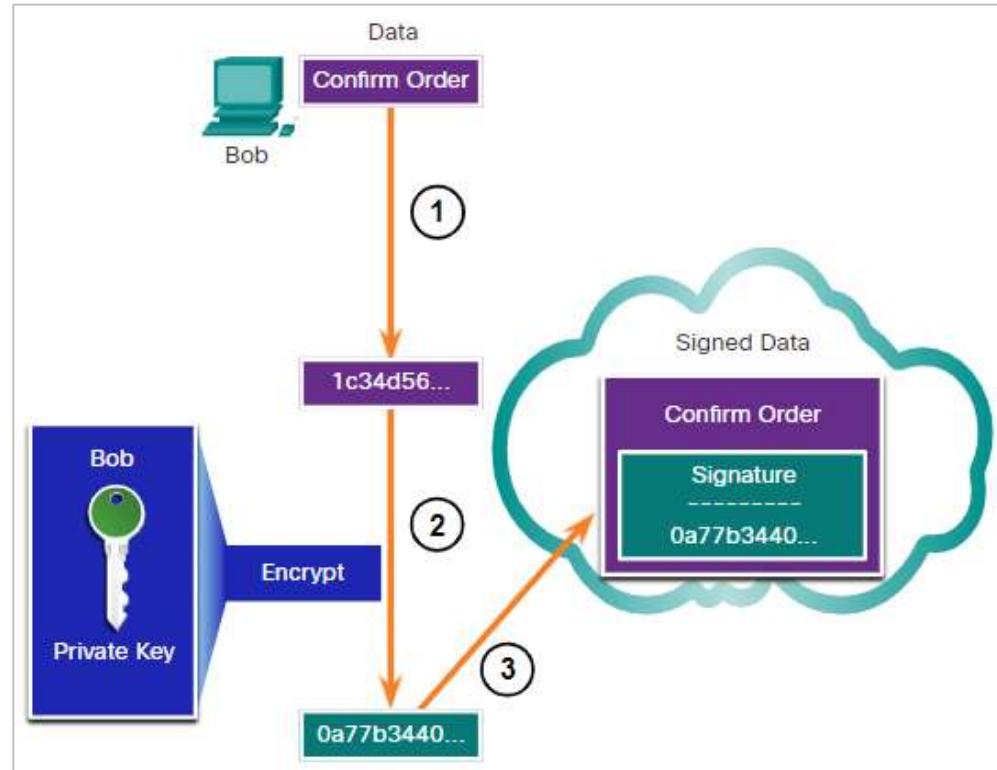
- Un certificado digital es utilizado para autenticar y verificar que el usuario que está enviando el mensaje sea verdaderamente quien afirma ser.
- Los certificados digitales también pueden usarse para proporcionar confidencialidad a un receptor con los medios necesarios para encriptar una respuesta.
- Los certificados digitales son similares a los certificados físicos, como se muestra en la imagen.
- El certificado digital verifica de forma independiente una identidad.
- En resumen, un certificado verifica la identidad, mientras que una firma verifica que algo proviene de esa identidad.



Firmas digitales para certificados digitales

Este ejemplo le ayudará a comprender cómo se utiliza una firma digital.

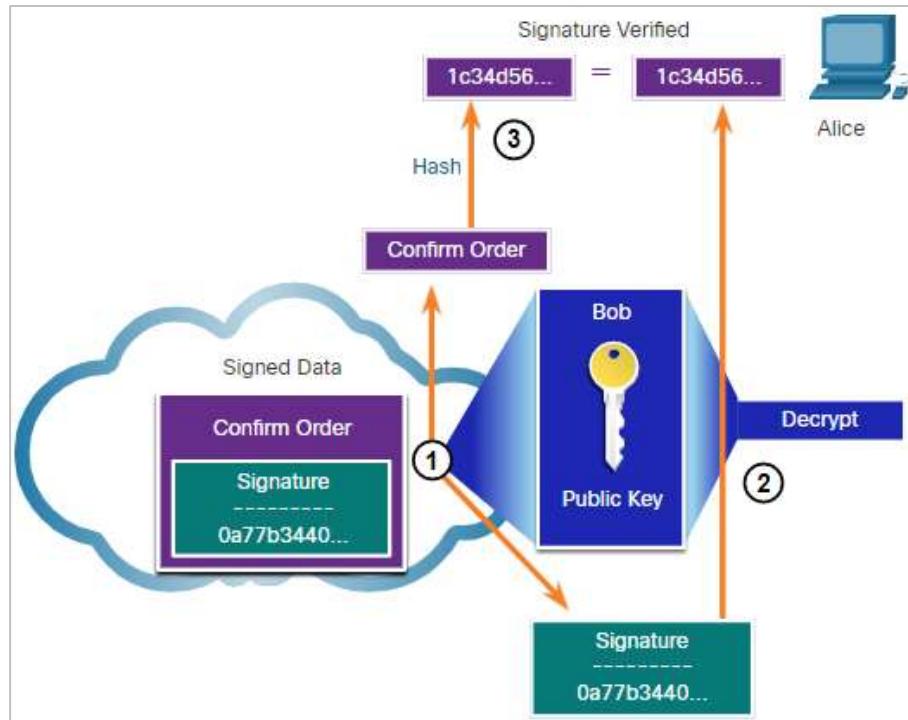
- Bob confirma un pedido con Alice. Alice está ordenando desde el sitio web de Bob.
- Bob confirma la orden y su computadora crea un hash de la confirmación.
- La computadora encripta el hash con la clave privada de Bob.
- El hash encriptado, conocido como la firma digital, se adjunta al documento.
- La confirmación del pedido se envía a Alice por medio de Internet.



Firmas digitales para certificados digitales

Cuando Alice recibe la firma digital, se produce el siguiente proceso:

- La computadora de Alice acepta la confirmación del pedido con la firma digital y obtiene la clave pública de Bob.
- La computadora de Alice desencripta la firma usando la clave pública de Bob que revela el valor hash asumido del dispositivo de envío.
- La computadora de Alice crea un hash del documento recibido, sin su firma, y lo compara con el hash desencriptado.
- Si los hashes coinciden, el documento es auténtico. Esto significa que la confirmación fue enviada por Bob y no ha cambiado desde que se firmó.



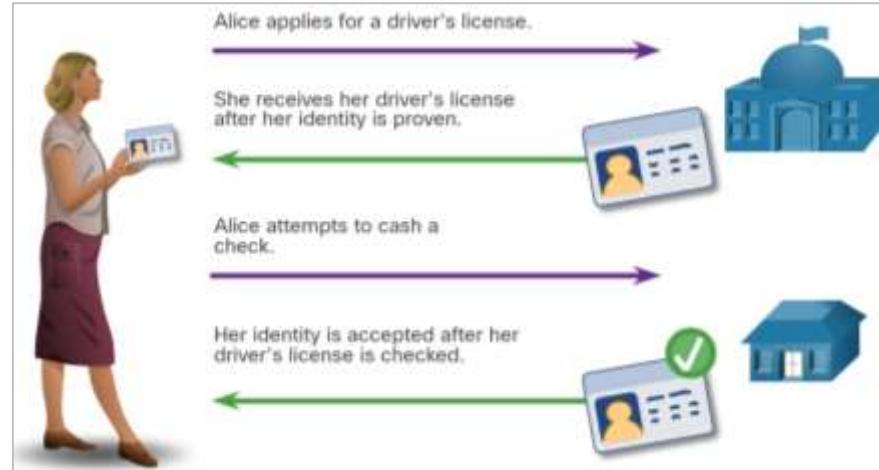
Autoridades y sistema de confianza de la PKI (PKI Trust System)

Administración de claves públicas

- El tráfico de Internet se compone de tráfico entre dos participantes. Cuando se establece una conexión asimétrica entre dos hosts, estos intercambian su información de clave pública.
- Un certificado SSL es un certificado digital que confirma la identidad de dominio de un sitio web.
- Para implementar SSL en un sitio web, el usuario compra un certificado SSL para el dominio de un proveedor de certificados SSL.
- El tercero de confianza realiza una investigación exhaustiva antes de emitir las credenciales. Despu  s de la investigaci  n exhaustiva, el tercero emite las credenciales que son dif   iles de falsificar.
- Cuando las computadoras intentan conectarse a un sitio web a trav  s de HTTPS, el navegador web comprueba el certificado de seguridad del sitio web y comprueba que es v  lido y se origin   con una CA confiable.
- Esto valida que la identificaci  n del sitio web es verdadera. El certificado se guarda localmente por el navegador web y luego se utiliza en transacciones posteriores. La clave p  blica del sitio web se incluye en el certificado y se utiliza para verificar futuras comunicaciones entre el sitio web y el cliente.

Administración de claves públicas

- Estos terceros de confianza ofrecen servicios similares a las agencias gubernamentales de concesión de licencias.
- En la figura, se muestra la analogía entre una licencia de conducir y un certificado digital.
- La infraestructura de claves públicas (Public Key Infrastructure, PKI) consiste en especificaciones, sistemas, y herramientas que se utilizan para crear, administrar, distribuir, utilizar, almacenar, y revocar certificados digitales.
- La autoridad de certificación (Certificate Authority, CA) es una organización que crea certificados digitales vinculando una clave pública a una identificación confirmada, como un sitio web o un individuo.
 - La PKI es un sistema intrincado que está diseñado para salvaguardar las identidades digitales contra el hacking, incluso por los atacantes más sofisticados, o estados nacionales.



La Infraestructura de Claves Públicas

- La PKI es necesaria para admitir la distribución e identificación a gran escala de claves de encriptación públicas.
- El framework de la PKI permite una relación de confianza altamente escalable.
- Se compone del hardware, el software, las personas, las políticas y los procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar certificados digitales.

Las autoridades y el sistema de confianza PKI

La Infraestructura de Claves Públicas

- La figura muestra los principales elementos de la PKI.
- Los certificados PKI contienen una clave pública de una entidad, su propósito, la autoridad de certificación (CA) que validó y emitió el certificado, el plazo durante el cual el certificado se puede considerar válido y el algoritmo utilizado para crear la firma.
- El almacén de certificados reside en una computadora local y almacena certificados emitidos y claves privadas.
- La autoridad de certificación (CA) es un tercero de confianza que emite certificados PKI a entidades y personas luego de verificar sus respectivas identidades. Este firma esos certificados usando su clave privada.
- En la base de datos de certificados se almacenan todos los certificados aprobados por la CA.

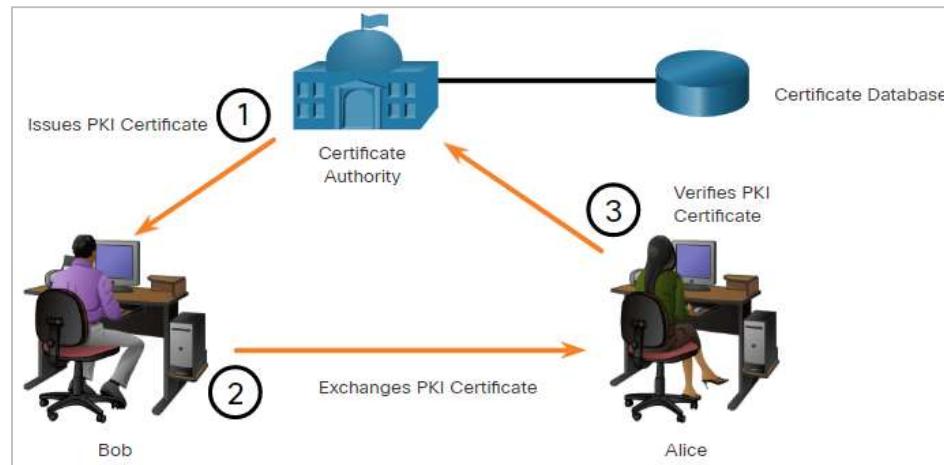


Las autoridades y el sistema de confianza PKI

La Infraestructura de claves públicas

La figura muestra cómo interoperan los elementos de la PKI:

- Emisión del certificado PKI: Bob pide inicialmente un certificado de la CA. La CA autentica a Bob y almacena el certificado de PKI de Bob en la base de datos de certificados.
- Intercambio de certificado PKI: Bob se comunica con Alice utilizando su certificado de PKI.
- Verificación de certificado PKI: Alice se comunica con la CA de confianza usando la clave pública de la CA. La CA consulta a la base de datos de certificados para validar el certificado PKI de Bob.



Nota: No todos los certificados de PKI se reciben directamente de una CA. Una autoridad de registro (Registration Authority, RA) es una CA secundaria y está certificada por una CA principal para emitir certificados para usos específicos.

Las autoridades y el sistema de confianza PKI

El sistema de autoridades de la PKI

- Muchos proveedores proporcionan servidores de CA como un servicio administrado o como un producto para usuarios finales. Algunos de estos proveedores son: Symantec Group, Comodo, Go Daddy Group, GlobalSign, entre otros.
- Las organizaciones también pueden implementar PKI privadas utilizando Microsoft Server u Open SSL.
- Las CA, especialmente aquellas tercerizadas, emiten certificados basados en clases que determinan cuán confiable es un certificado.
- La tabla proporciona una descripción de las clases. Cuanto mayor sea el número de clase, más confiable será el certificado. Un certificado de clase 5 es mucho más confiable que un certificado de una clase inferior.

Clase	Descripción
0	Se utiliza con fines de pruebas en situaciones en las que no se ha realizado ninguna comprobación.
1	Utilizado por personas que requieren verificación de correo electrónico.
2	Se utiliza por organizaciones en las que se requiere demostrar la identidad.
3	Se utiliza para la firma de servidores y software.
4	Se utiliza para transacciones comerciales en línea entre empresas.
5	Se utiliza para organizaciones privadas o agencias de seguridad gubernamentales.

Las autoridades y el sistema de confianza PKI

El sistema de autoridades de la PKI

- Algunas claves públicas de la CA están precargadas, como las que aparecen en los navegadores web.
- La imagen muestra varios certificados de VeriSign que están guardados en el almacén de certificados en el host.
- El navegador considerará como legítimo cualquier certificado firmado por cualquiera de las CA de la lista y confiará automáticamente.

The screenshot shows a Windows Certificates dialog box with the title 'Certificates'. At the top, there is a dropdown menu set to '<All>'. Below it, there are three tabs: 'Intermediate Certification Authorities' (selected), 'Trusted Root Certification Authorities' (highlighted in blue), and 'Trusted Publishers'. The main area is a table listing certificates:

Issued To	Issued By	Expiration Date	Friendly Name
AAA Certificate Ser...	AAA Certificate Services	12/31/2028	Sectigo (AAA)
AddTrust External ...	AddTrust External CA...	5/30/2020	Sectigo (AddTrust)
AffirmTrust Comme...	AffirmTrust Commercial	12/31/2030	AffirmTrust Com...
Baltimore CyberTru...	Baltimore CyberTrust ...	5/12/2025	DigiCert Baltimor...
Certigna	Certigna	6/29/2027	Certigna
Certum CA	Certum CA	6/11/2027	Certum
Certum Trusted Ne...	Certum Trusted Netw...	12/31/2029	Certum Trusted ...
Cisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<None>
Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<None>

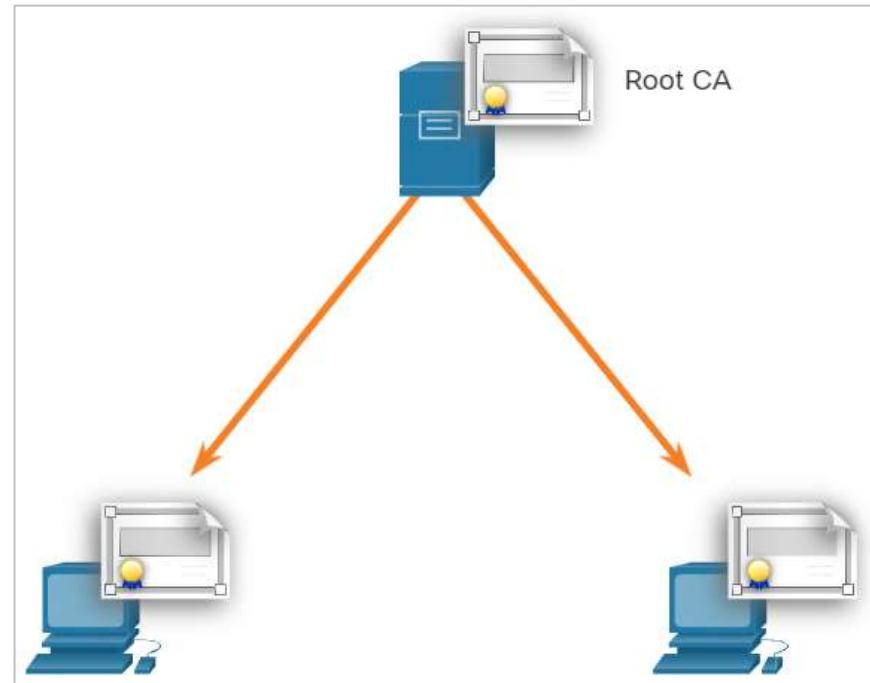
Below the table are buttons for 'Import...', 'Export...', 'Remove', and 'Advanced'. A section titled 'Certificate intended purposes' lists: Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user. There is a 'View' button next to this list. At the bottom right are 'Close' and 'OK' buttons.

El sistema de confianza PKI

Las PKIs pueden formar distintas topologías de confianza, como las siguientes:

Topología de PKI de raíz única

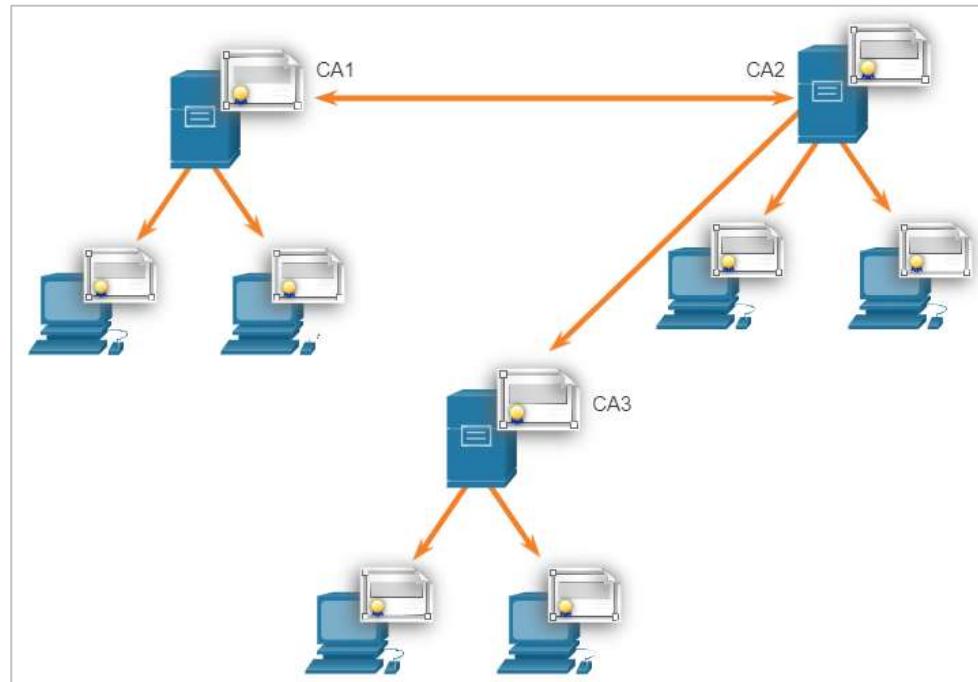
- Una sola CA, llamada la CA raíz, emite todos los certificados a los usuarios finales, que suelen encontrarse dentro de la misma organización.
- El beneficio de este enfoque es su simplicidad.
- Es difícil llevar esta estructura a un entorno grande, ya que requiere una administración estrictamente centralizada que crea un único punto de falla.



El sistema de confianza PKI

Topologías de CA con certificación cruzada

- Este es un modelo peer-to-peer (par a par) en el que las CA individuales establecen relaciones de confianza con otras CA mediante la certificación cruzada de certificados de CA.
- Los usuarios de cualquiera de los dos dominios de CA pueden estar seguros de que pueden confiar en el otro.
- Esto proporciona redundancia y elimina el punto único de falla.

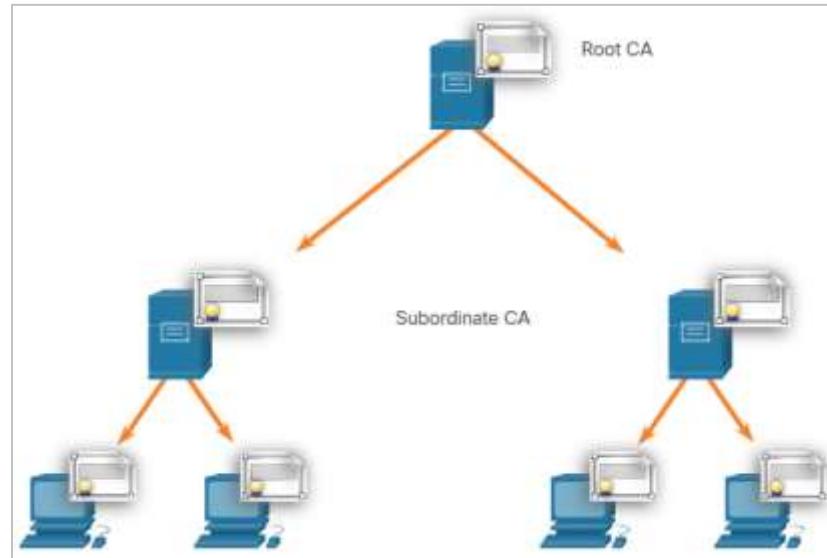


Las autoridades y el sistema de confianza PKI

El sistema de confianza PKI

Topologías de CA jerárquicas

- La CA de nivel más alto es la CA raíz que emite certificados a los usuarios finales y a una CA subordinada.
- Las CA subordinadas (sub-CAs) pueden crearse para respaldar diversas unidades de negocio, dominios o comunidades de confianza.
- La CA raíz mantiene la “comunidad de confianza” establecida al asegurar que cada entidad de la jerarquía respete un conjunto mínimo de prácticas.
- Los beneficios de esta topología incluyen el aumento en la escalabilidad y capacidad de administración.
- Una topología jerárquica y de certificación cruzada pueden ser combinadas para crear una infraestructura híbrida.



Interoperabilidad de los diferentes proveedores de PKI

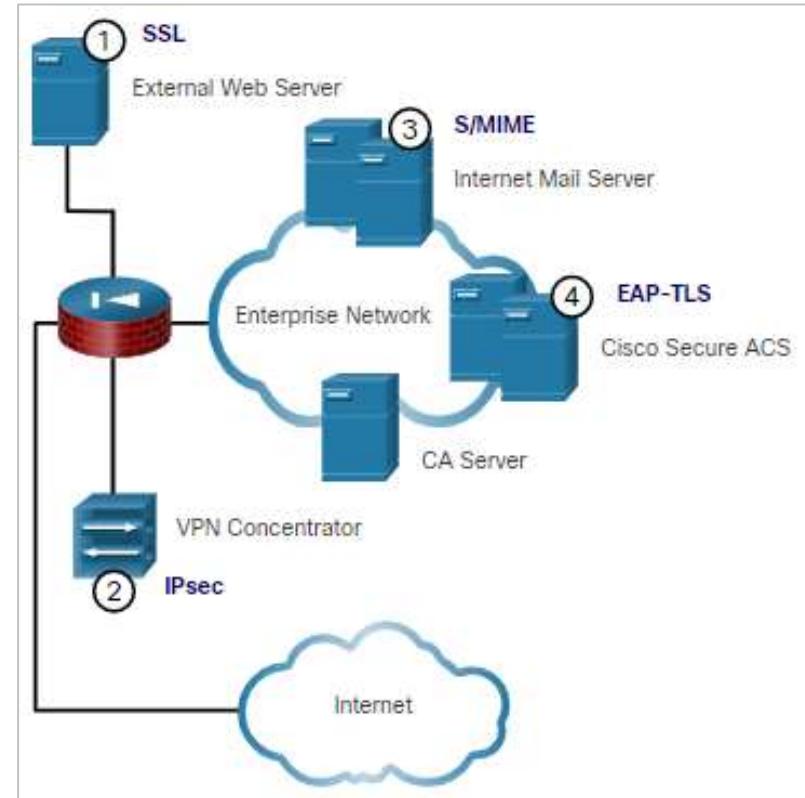
- Existe una preocupación acerca de la interoperabilidad entre una PKI y sus servicios de respaldo, por ejemplo el protocolo Lightweight Directory Access Protocol (LDAP) y los directorios X.500, dado que muchos proveedores de CA han propuesto e implementado soluciones propias en lugar de esperar a que se desarrollen estándares.
- Para dar solución a esta preocupación sobre la interoperabilidad, la IETF publicó el framework de prácticas y políticas de certificación de PKI, de Internet X.509 (RFC 2527).
- El estándar X.509 versión 3 (X.509v3) define el formato de un certificado digital.

Nota: *LDAP y X.500 son protocolos que se utilizan para consultar un servicio de directorios, como Microsoft Active Directory, para verificar un nombre de usuario y una contraseña.*

Interoperabilidad de los diferentes proveedores de PKI

Aplicaciones de X.509v3

- **SSL:** Los servidores web seguros utilizan X.509 v3 para la autenticación de sitios web en los protocolos SSL y TLS mientras que los web browsers utilizan X.509 v3 para implementar certificados de clientes HTTPS.
- **IPsec:** Las redes VPN IPsec utilizan X.509 cuando los certificados se pueden utilizar como mecanismo de distribución de claves públicas (IKE) para la autenticación basada en RSA.
- **S/MIME:** Los agentes de correo de usuario que admiten la protección de correo con el protocolo S/MIME utilizan certificados X.509.
- **EAP-TLS:** Los switches pueden utilizar certificados para autenticar dispositivos finales que se pueden proporcionar a un ACS central a través del Protocolo de Autenticación Extensible con TLS (EAP-TLS).



Inscripción, Autenticación y Revocación de Certificados

- En el procedimiento de autenticación de CA, el primer paso es obtener una copia segura de la clave pública de la CA.
- Todos los sistemas que utilizan el PKI deben tener la clave pública de la CA, que se llama certificado autofirmado.
- La clave pública de la CA verifica todos los certificados emitidos por la CA y es vital para el correcto funcionamiento del PKI.
- Para muchos sistemas, como los navegadores web, la distribución de los certificados de CA se maneja automáticamente. El navegador web trae preinstalado un conjunto de certificados raíz de CA públicos.
- Un sistema de host utiliza el proceso de inscripción de certificado para inscribirse en una PKI. Para hacerlo, se obtienen los certificados de CA mediante la transmisión en banda en una red y la autenticación se realiza mediante la transmisión fuera de banda (Out-of-band, OOB) utilizando el teléfono.

Nota: Sólo una CA raíz puede emitir un certificado autofirmado que sea reconocido o verificado por otras CA dentro de la PKI.

Inscripción, Autenticación y Revocación de certificados

- El sistema que se inscribirá en la PKI se pone en contacto con una CA para solicitar y obtener un certificado de identidad digital para sí mismo y para obtener el certificado firmado automáticamente de la CA.
- En la etapa final, se verifica la autenticidad del certificado de CA utilizando un método fuera de banda como POTS (Plain Old Telephone System), para obtener la huella digital del certificado de identidad válido de la CA.
- La autenticación ya no requiere la presencia del servidor de CA y cada usuario intercambia sus certificados que contienen las claves públicas.
- A veces, se debe revocar el certificado. Estos son dos de los métodos más comunes de revocación:
 - **Lista de revocación de certificados (Certificate Revocation List, CRL):** Una lista de números de serie de certificados revocados que ya no son válidos porque caducaron. Las entidades de PKI sondan periódicamente el repositorio de CRL para recibir la CRL más actual.
 - **Protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP):** Un protocolo de Internet utilizado para consultar un servidor de OCSP y comprobar el estado de revocación de un certificado digital X.509. La información sobre revocación se publica inmediatamente en una base de datos en línea.

Aplicaciones e impacto de la criptografía

Aplicaciones de PKI

A continuación, se detalla una breve lista de usos comunes de las PKI:

- Autenticación de pares basada en certificados SSL/TLS
- Asegurar tráfico de red utilizando redes VPN IPsec
- Tráfico web HTTPS
- Control de acceso a la red mediante la autenticación 802.1x
- Protección de correo electrónico utilizando el protocolo S/MIME
- Protección de mensajería instantánea
- Aprobación y autorización de aplicaciones con firma de código
- Protección de datos de usuarios con el sistema de archivos de encriptación (EFS)
- Implementación de autenticación de dos factores con tarjetas inteligentes
- Protección de dispositivos de almacenamiento USB

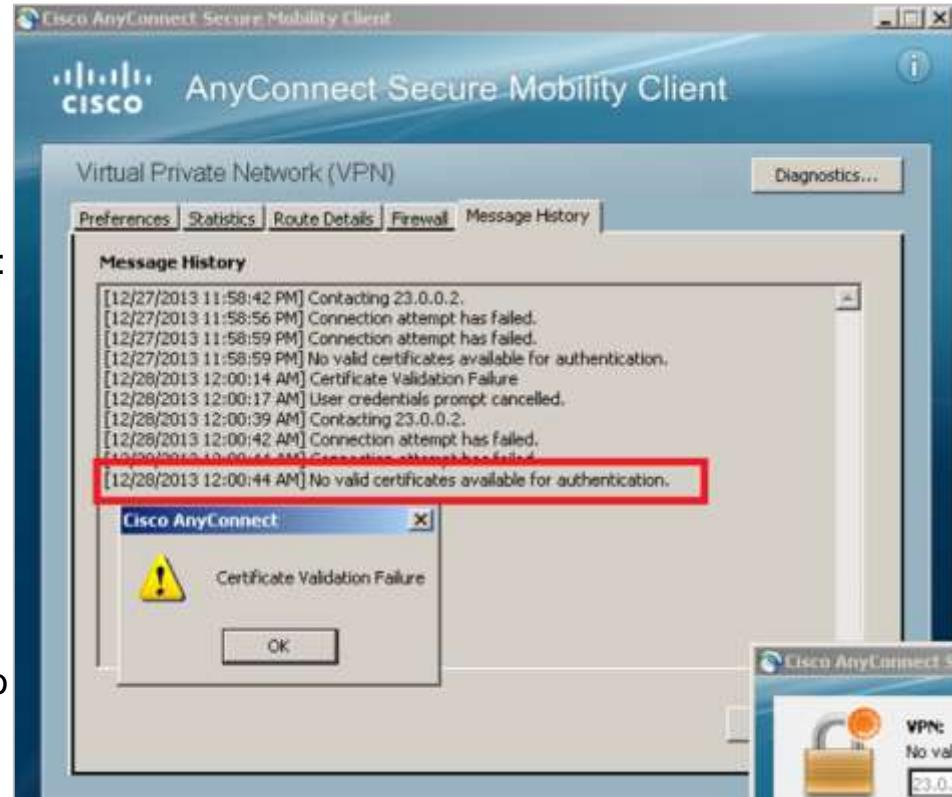
Transacciones encriptadas en la red

- Un analista de seguridad debe ser capaz de reconocer y resolver problemas potenciales vinculados a permitir el uso de soluciones relacionadas con PKI en la red empresarial.
- Tenga en cuenta la manera en que el crecimiento del tráfico de SSL/TLS constituye un mayor riesgo de seguridad para las empresas, ya que el tráfico está encriptado y no puede interceptarse ni monitorearse con los métodos normales. Los usuarios pueden introducir malware o filtrar información confidencial en una conexión SSL/TLS.
- Otros problemas relacionados con SSL/TLS pueden vincularse a la validación del certificado de un servidor web. Cuando esto ocurre, los navegadores web muestran una advertencia de seguridad. Algunos de los problemas relacionados con la PKI que están vinculados con advertencias de seguridad son los siguientes:
 - **Plazo de validez:** Los certificados X.509v3 especifican fechas de validez. Si la fecha actual está fuera del rango, el navegador web muestra un mensaje.
 - **Error de validación de firma:** Si un navegador no puede validar la firma en el certificado, no hay ninguna garantía de que la clave pública en el certificado sea auténtica. Ocurrirá un error con la validación de la firma si el certificado raíz de la jerarquía de la CA no está disponible en el almacén de certificados del navegador.

Transacciones encriptadas en la red

Error de validación de firma

- Algunos de estos problemas pueden evitarse debido a que los protocolos SSL/TLS son extensibles y modulares. Esto se conoce como un conjunto de cifrado (cipher suite).
- Los componentes clave del conjunto de cifrado son: El algoritmo de código de autenticación de mensajes (Message Authentication Code, MAC), el algoritmo de encriptación, el algoritmo de intercambio de claves y el algoritmo de autenticación.
- A medida que el criptoanálisis sigue revelando defectos en estos algoritmos, el conjunto de cifrado se puede actualizar para colocar parches en estos defectos. Cuando las versiones del protocolo dentro del conjunto de cifrado cambian, el número de versión de SSL/TLS también lo hace.



Encriptación y monitoreo de seguridad

- El monitoreo de red se vuelve más difícil cuando los paquetes están encriptados.
- Los analistas de seguridad deben conocer esas dificultades y abordarlas lo mejor posible.
- Por ejemplo, cuando se utilizan VPN de sitio a sitio, el IPS debe colocarse de modo que pueda monitorear el tráfico sin encriptar. Sin embargo, el aumento de HTTPS en la red empresarial supone nuevos desafíos.
- Los analistas de seguridad deben saber cómo evitar y resolver estos problemas. Aquí vemos una lista de algunas de las medidas que podría tomar un analista de seguridad:
 - Configurar reglas para distinguir entre tráfico SSL y no SSL, o entre tráfico SSL HTTPS y no HTTPS.
 - Aumentar la seguridad mediante la validación de certificados de servidor usando CRL y OCSP.
 - Implementar protección antimalware y filtrado URL de contenido HTTPS.
 - Implementar un dispositivo Cisco SSL Appliance para desencriptar el tráfico SSL y enviarlo a dispositivos de un sistema de prevención de intrusiones (IPS) para identificar riesgos normalmente ocultos para SSL.

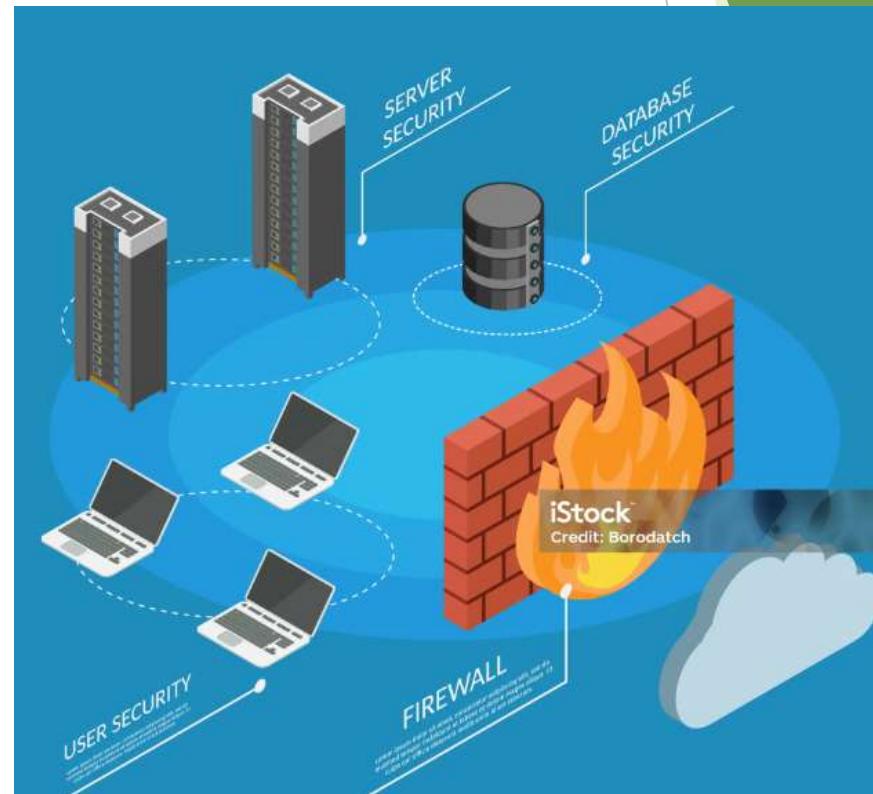
Encriptación y monitoreo de seguridad

- La criptografía es dinámica y siempre cambia. Un analista de seguridad debe comprender bien los algoritmos y las operaciones criptográficas para poder investigar los incidentes de seguridad relacionados con la criptografía.
- Hay dos maneras principales en las que la criptografía afecta las investigaciones de seguridad.
- En primer lugar, los ataques pueden dirigirse específicamente a los algoritmos de encriptación propiamente dichos.
- Después de que el algoritmo es hackeado y el atacante obtiene las claves, es posible desencriptar y leer todos los datos encriptados que recopile el atacante, lo que expone los datos privados.
- Luego de esto, la investigación de seguridad también se ve afectada porque los datos se pueden ocultar a plena vista, encriptándolos.

Firewall

¿Qué es un Firewall?

- ▶ Un firewall es una barrera de seguridad diseñada para proteger una red de computadoras, controlando el tráfico entrante y saliente según un conjunto de reglas predefinidas.
- ▶ Puede ser una combinación de hardware y software o simplemente un software que se ejecuta en un servidor.
- ▶ Su objetivo principal es prevenir o limitar el acceso no autorizado desde y hacia una red privada mientras permite la comunicación autorizada.



Tipos de FireWall

- ▶ **Firewall de red:** Opera a nivel de capa 3 del modelo OSI y examina los paquetes de datos que entran y salen de la red. Puede basarse en reglas de filtrado de paquetes, donde se bloquean o permiten paquetes según direcciones IP, puertos, protocolos, etc.
- ▶ **Firewall de aplicación:** Opera a nivel de capa 7 y es capaz de inspeccionar el contenido de los paquetes y tomar decisiones basadas en el contenido de las aplicaciones. Puede filtrar tráfico basado en el comportamiento de las aplicaciones y detectar amenazas avanzadas como intrusiones y malware.

Importancia de los Firewall

- ▶ **Comprender la Arquitectura de Redes:** El estudio del firewall ayuda a los estudiantes a entender cómo se diseñan y se aseguran las redes informáticas. Les brinda conocimientos sobre la segmentación de redes, el enrutamiento seguro y las mejores prácticas de configuración.
- ▶ **Defensa contra Amenazas:** Los firewalls son una primera línea de defensa contra diversas amenazas cibernéticas, como malware, ataques de denegación de servicio (DDoS) e intrusiones.
- ▶ Aprender sobre firewalls proporciona a ustedes las habilidades necesarias para configurar reglas efectivas y proteger los sistemas contra tales amenazas.

- ▶ **Cumplimiento de Normativas:** Muchas normativas y estándares de seguridad, como PCI DSS (Payment Card Industry Data Security Standard) y HIPAA (Health Insurance Portability and Accountability Act), requieren la implementación de firewalls para cumplir con los requisitos de seguridad. Ustedes deben estar familiarizados con estas regulaciones y cómo los firewalls ayudan en el cumplimiento.
- ▶ **Investigación de Incidentes:** En un entorno corporativo, los firewalls son una fuente crucial de registros de actividad de red. Aprender a analizar los registros de firewall puede ayudarles a investigar incidentes de seguridad, identificar patrones de tráfico malicioso y fortalecer la postura de seguridad de una organización.

- ▶ **Firewalls de Packet Filtering (Filtrado de Paquetes):** Estos firewalls examinan los encabezados de los paquetes de datos y aplican reglas predefinidas para permitir o denegar el paso de paquetes según criterios como dirección IP, puerto y protocolo. Son eficientes y rápidos, pero tienen limitaciones en la inspección de contenido.
- ▶ **Firewalls de Estado (Stateful Firewalls):** Estos firewalls no solo examinan los encabezados de los paquetes, sino que también realizan un seguimiento del estado de la conexión. Esto significa que pueden determinar si un paquete pertenece a una conexión establecida y, por lo tanto, si debe permitirse o denegarse. Esto mejora la seguridad al reducir la posibilidad de ataques de denegación de servicio.
- ▶ **Firewalls de Aplicaciones (Application Firewalls):** Estos firewalls operan a nivel de aplicación (Capa 7) y pueden inspeccionar el contenido de los paquetes para detectar amenazas específicas, como intrusiones o malware. Son ideales para proteger aplicaciones web y servidores de correo electrónico, ya que pueden identificar y bloquear actividades maliciosas a nivel de aplicación.

Funcionalidades Avanzadas

- ▶ **Inspección Profunda de Paquetes (Deep Packet Inspection, DPI):** Esta técnica permite a los firewalls examinar el contenido de los paquetes en busca de patrones específicos asociados con amenazas ciberneticas. DPI es especialmente útil para detectar y bloquear malware y ataques avanzados que pueden pasar desapercibidos para otros métodos de filtrado.
- ▶ **VPN (Virtual Private Network) Firewalls:** Estos firewalls se utilizan para proteger las conexiones VPN, garantizando que el tráfico que fluye a través de la red privada virtual esté seguro y protegido contra intrusiones y ataques.
- ▶ **Prevención de Intrusiones (Intrusion Prevention System, IPS):** Algunos firewalls incorporan funcionalidades de IPS para identificar y bloquear activamente intentos de intrusión en tiempo real. Esto ayuda a fortalecer la seguridad de la red al detener los ataques antes de que causen daño.

- ▶ **Evasión de Firewalls:** Los atacantes constantemente buscan formas de eludir las defensas del firewall, como utilizando técnicas de evasión de paquetes o explotando vulnerabilidades en los propios firewalls. Los estudiantes de seguridad informática deben estar al tanto de estas técnicas y aprender cómo mitigarlas.
- ▶ **Firewalls en la Nube:** Con el aumento de las implementaciones en la nube, los firewalls basados en la nube están ganando popularidad. Estos firewalls protegen las infraestructuras en la nube y proporcionan capacidades de seguridad escalables y flexibles.
- ▶ **Automatización y Orquestación:** La automatización y la orquestación están transformando la gestión de firewalls, permitiendo a las organizaciones implementar y mantener políticas de seguridad de manera más eficiente y consistente a través de múltiples dispositivos y entorno

Firewalls y Seguridad Perimetral

- ▶ Los firewalls tradicionalmente se han utilizado como una medida de seguridad perimetral, protegiendo el borde de una red contra amenazas externas. Sin embargo, con la evolución de las amenazas cibernéticas y los entornos de red cada vez más complejos, el enfoque de seguridad ha cambiado hacia modelos más centrados en los datos y las aplicaciones. Esto ha llevado al desarrollo de firewalls más avanzados y a la adopción de estrategias de seguridad en profundidad.

Firewalls de Próxima Generación (Next-Generation Firewalls, NGFW)

- ▶ Los firewalls de próxima generación van más allá de las capacidades de filtrado de paquetes tradicionales y ofrecen funcionalidades avanzadas, como inspección de contenido, detección de aplicaciones, prevención de intrusiones y visibilidad y control avanzados del tráfico. Estos firewalls son capaces de identificar y bloquear amenazas en tiempo real, así como de aplicar políticas de seguridad granulares basadas en el contexto del tráfico y las aplicaciones.

Seguridad en Entornos Distribuidos y Cloud

- ▶ Con la adopción generalizada de la nube y los entornos distribuidos, la seguridad de red se ha vuelto más compleja. Los estudiantes de seguridad informática deben comprender cómo implementar firewalls en entornos de nube pública, privada e híbrida, así como en redes distribuidas que abarcan múltiples ubicaciones geográficas. Esto incluye la configuración de políticas de seguridad coherentes en todos los entornos y la integración de firewalls con otras soluciones de seguridad, como sistemas de detección y respuesta a incidentes (IDS/IPS) y herramientas de gestión de identidades y accesos (IAM).

Automatización y Orquestación

- ▶ La automatización y la orquestación juegan un papel crucial en la gestión eficiente de firewalls en entornos dinámicos y escalables. Los estudiantes deben familiarizarse con herramientas y lenguajes de automatización, como Ansible, Puppet y Chef, para automatizar tareas de configuración, implementación y mantenimiento de firewalls. La orquestación de firewalls permite la coordinación y el control centralizado de políticas de seguridad en toda la infraestructura de red, facilitando la implementación de políticas coherentes y el cumplimiento de los estándares de seguridad.

Análisis de Registros y Respuesta a Incidentes

- ▶ El análisis de registros de firewall es una habilidad fundamental para la detección y respuesta a incidentes de seguridad. Los estudiantes deben aprender a interpretar los registros de firewall para identificar patrones de tráfico malicioso, realizar análisis forenses y tomar medidas correctivas adecuadas. Además, deben estar familiarizados con los procedimientos y mejores prácticas para la gestión de incidentes de seguridad, incluida la coordinación con equipos de respuesta a incidentes internos y externos.

Pruebas de Penetración y Evaluación de Firewalls

- ▶ Realizar pruebas de penetración y evaluaciones de seguridad es una parte integral del proceso de aseguramiento de firewalls. Los estudiantes deben adquirir habilidades en el uso de herramientas y técnicas de prueba de penetración para identificar vulnerabilidades y evaluar la efectividad de las defensas del firewall. Esto incluye la realización de pruebas de intrusión simuladas para validar la resistencia de los firewalls ante diferentes escenarios de ataque.

VPN

- ▶ Una VPN es una tecnología que establece una conexión segura y cifrada entre dos puntos de una red, generalmente a través de Internet. Esto permite a los usuarios enviar y recibir datos de manera segura a través de una red pública como si estuvieran conectados directamente a una red privada.

Funcionamiento

- ▶ Una VPN utiliza protocolos de cifrado para proteger los datos mientras viajan a través de la red. Cuando un usuario se conecta a una VPN, su dispositivo establece una conexión cifrada con un servidor VPN. A partir de ese momento, todo el tráfico de datos entre el dispositivo y el servidor se cifra, lo que garantiza la confidencialidad e integridad de los datos.

Importancia

- ▶ **Privacidad y Seguridad en la Conexión:** Las VPN proporcionan un nivel adicional de seguridad y privacidad al cifrar el tráfico de Internet, lo que protege contra la interceptación de datos y los ataques de hackers, especialmente en redes Wi-Fi públicas.
- ▶ **Acceso Remoto Seguro:** Las VPN permiten a los usuarios acceder de forma segura a recursos de red internos desde ubicaciones remotas, lo que es crucial en un entorno donde el trabajo remoto es cada vez más común. Los estudiantes pueden aprender a configurar y administrar VPN para garantizar un acceso remoto seguro a los recursos de la organización.
- ▶ **Evitar la Censura y las Restricciones Geográficas:** Las VPN pueden utilizarse para eludir la censura en Internet y las restricciones geográficas al cambiar la ubicación virtual del usuario. Esto es útil para acceder a contenido restringido geográficamente y para proteger la libertad de expresión en entornos donde Internet está censurado.
- ▶ **Investigación y Desarrollo:** Los estudiantes de seguridad informática pueden utilizar VPN para realizar investigaciones sobre seguridad en redes y comunicaciones cifradas. Esto les permite experimentar con diferentes configuraciones de VPN, protocolos de cifrado y medidas de seguridad para comprender mejor sus características y limitaciones.

Tipos

- ▶ **VPN de Acceso Remoto:** Permiten a los usuarios individuales conectarse de forma segura a una red corporativa desde ubicaciones remotas, como el hogar o un café.
- ▶ **VPN de Sitio a Sitio:** Establecen conexiones seguras entre redes geográficamente separadas, como sucursales de una empresa o datacenters.
- ▶ **VPN de Acceso por Capas (Layer 2 y Layer 3):** Ofrecen diferentes niveles de acceso a los usuarios, permitiendo una segmentación más granular de la red y un control más preciso sobre quién puede acceder a qué recursos.

Consideraciones

- ▶ **Velocidad y Rendimiento:** El cifrado y la encapsulación de datos pueden afectar el rendimiento de la red, especialmente en conexiones de alta velocidad. Los estudiantes deben comprender cómo optimizar el rendimiento de la VPN sin comprometer la seguridad.
- ▶ **Gestión y Mantenimiento:** Configurar y mantener una infraestructura de VPN puede ser complejo, especialmente en entornos empresariales con múltiples usuarios y dispositivos. Los estudiantes deben aprender las mejores prácticas para la gestión de VPN, incluida la configuración de políticas de seguridad, la administración de usuarios y la resolución de problemas.

Tecnologías Subyacentes de las VPN

- ▶ **Protocolos de Cifrado:** Las VPN utilizan protocolos de cifrado para proteger la confidencialidad e integridad de los datos transmitidos. Algunos de los protocolos comunes incluyen IPsec (Protocolo de Seguridad de Internet), SSL/TLS (Secure Socket Layer/Transport Layer Security) y OpenVPN. Los estudiantes deben comprender las diferencias entre estos protocolos, sus fortalezas y debilidades, y cómo configurarlos correctamente para garantizar la seguridad de la conexión VPN.
- ▶ **Túneles VPN:** Las VPN establecen túneles virtuales a través de la infraestructura de red pública, encapsulando y cifrando los datos que viajan entre los puntos finales. Los túneles VPN pueden ser de capa 2 (túneles de enlace) o de capa 3 (túneles de red), cada uno con sus propias aplicaciones y consideraciones de configuración.

Seguridad y Provacidad

- ▶ **Confidencialidad de los Datos:** La principal función de una VPN es garantizar la confidencialidad de los datos transmitidos a través de la red pública. Esto se logra mediante la aplicación de cifrado a nivel de paquete o de conexión, asegurando que los datos no sean legibles para terceros no autorizados.
- ▶ **Integridad de los Datos:** Además de la confidencialidad, las VPN también garantizan la integridad de los datos, asegurando que no sean modificados o manipulados durante la transmisión. Los algoritmos de hash y firma digital se utilizan para verificar la integridad de los paquetes de datos.
- ▶ **Anonimato y Privacidad:** Al enrutar el tráfico a través de servidores VPN, los usuarios pueden ocultar su dirección IP real y mantener su anonimato en línea. Esto es especialmente útil para proteger la privacidad y evitar la vigilancia en línea.

Implementación y Configuración

- ▶ **Servidores VPN:** Los estudiantes deben comprender cómo configurar y administrar servidores VPN, ya sea en hardware dedicado o en software basado en servidor. Esto incluye la instalación y configuración de software de servidor VPN, la gestión de certificados digitales y la definición de políticas de seguridad.
- ▶ **Clientes VPN:** Además de los servidores VPN, los estudiantes también deben estar familiarizados con la configuración y el uso de clientes VPN en dispositivos de usuario final. Esto implica la instalación de software cliente VPN, la configuración de perfiles de conexión y la autenticación de usuarios.

Seguridad de la Infraestructura de VPN

- ▶ **Auditoría y Monitoreo:** Los estudiantes deben aprender a realizar auditorías de seguridad en la infraestructura de VPN para identificar posibles vulnerabilidades y riesgos de seguridad. Esto implica el monitoreo de registros de eventos, la detección de intrusiones y la evaluación de la configuración de seguridad.
- ▶ **Actualizaciones y Parches:** Mantener la infraestructura de VPN actualizada es crucial para garantizar la seguridad y la estabilidad de la red. Los estudiantes deben entender la importancia de aplicar regularmente parches de seguridad y actualizaciones de software para mitigar vulnerabilidades conocidas.

Detección de intrusos

- ▶ La detección de intrusos (IDS, por sus siglas en inglés) es un proceso de vigilancia y análisis del tráfico de red o de los registros de actividad de sistemas para detectar y responder a actividades maliciosas o sospechosas. Los IDS identifican patrones de comportamiento que pueden indicar intrusiones o intentos de acceso no autorizado.

Funcionamiento de los Sistemas de Detección de Intrusos

- ▶ **Basados en Firmas:** Estos IDS comparan el tráfico de red o los registros de actividad con una base de datos de firmas conocidas de ataques. Si se encuentra una coincidencia, se activa una alerta.
- ▶ **Basados en Comportamiento:** Estos IDS analizan el comportamiento normal del tráfico o de los usuarios en la red y generan alertas cuando se detectan desviaciones significativas que pueden indicar actividades maliciosas.
- ▶ **Híbridos:** Algunos IDS combinan técnicas de detección de firmas y de comportamiento para proporcionar una detección más completa y precisa de intrusiones.

Importancia

- ▶ **Detección Temprana de Amenazas:** Los IDS permiten detectar y responder a intrusiones de manera proactiva, lo que ayuda a minimizar el tiempo de exposición a las amenazas y reduce el impacto de los ataques.
- ▶ **Comprendión del Paisaje de Amenazas:** Estudiar y trabajar con IDS proporciona a los estudiantes una comprensión profunda del panorama de amenazas ciberneticas y de las tácticas utilizadas por los atacantes para comprometer la seguridad de una red.
- ▶ **Investigación de Incidentes:** Los IDS generan alertas cuando se detectan actividades sospechosas, lo que permite a los estudiantes investigar y responder a incidentes de seguridad de manera eficiente. Esto incluye el análisis de registros de eventos, la identificación de vectores de ataque y la mitigación de riesgos.

Tipos de IDS

- ▶ **IDS de Red:** Monitorizan el tráfico de red en busca de actividades maliciosas, como escaneos de puertos, intentos de intrusión y tráfico anómalo. Pueden ser implementados como dispositivos físicos o software en un servidor.
- ▶ **IDS de Host:** Se ejecutan en sistemas individuales para analizar registros de actividad del sistema operativo y detectar comportamientos sospechosos, como modificaciones de archivos, acceso no autorizado y actividad de malware.

Consideraciones

- ▶ **Falsos Positivos y Negativos:** Los IDS pueden generar falsas alertas (falsos positivos) o no detectar actividades maliciosas (falsos negativos). Los estudiantes deben comprender cómo mitigar estos desafíos mediante la calibración y ajuste de los IDS, así como el análisis manual de alertas.
- ▶ **Rendimiento y Escalabilidad:** Implementar IDS en entornos de red grandes y de alta velocidad puede ser desafiante debido a la cantidad de tráfico y la necesidad de procesar datos en tiempo real. Los estudiantes deben aprender a optimizar el rendimiento y la escalabilidad de los IDS para garantizar una detección efectiva.



Módulo 11: Configuración de seguridad en el Switch

Switching, Routing y Wireless
Essentials (SRWE)



Objetivos del módulo

Título de módulo: Configuración de seguridad en el Switch

Objetivo del módulo: Configurar la seguridad en el Switch para mitigar los ataques de LAN

Título del tema	Objetivo del tema
Implementación de seguridad de puertos	Implementar la seguridad de puertos para mitigar los ataques de tablas de direcciones MAC.
Mitigación de ataques de VLAN	Explicar cómo configurar DTP y la VLAN nativa para mitigar los ataques de VLAN.
Mitigación de ataques de DHCP	Explicar cómo configurar el snooping de DHCP para mitigar los ataques de DHCP.
Mitigación de ataques de ARP	Explicar 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.

11.1 – Implementar Seguridad de Puertos (Port Security)

Asegure los puertos no utilizados

Los ataques de Capa 2 son de los más sencillos de desplegar para los hackers, pero estas amenazas también pueden ser mitigadas con algunas soluciones comunes de capa 2.

- Se deben proteger todos los puertos (interfaces) del switch antes de implementar el dispositivo para la producción. ¿Cómo se asegura un puerto dependiendo de su función?.
- Un método simple que muchos administradores usan para contribuir a la seguridad de la red ante accesos no autorizados es inhabilitar todos los puertos del switch que no se utilizan. Navegue a cada puerto no utilizado y emita el comando de apagado **shutdown**de Cisco IOS. Si un puerto debe reactivarse más tarde, se puede habilitar

```
Switch(config)# interface range type module/first-number - last-number
```

- Para configurar un rango de puertos, use el comando **interface range**.

Mitigar los ataques de la tabla de direcciones MAC

El método más simple y eficaz para evitar ataques por saturación de la tabla de direcciones MAC es habilitar el port security.

- La seguridad de puertos limita la cantidad de direcciones MAC válidas permitidas en el puerto. Permite a un administrador configurar manualmente las direcciones MAC para un puerto o permitir que el switch aprenda dinámicamente un número limitado de direcciones MAC. Cuando un puerto configurado con port security recibe un trama, la dirección MAC de origen del trama se compara con la lista de direcciones MAC de origen seguro que se configuraron manualmente o se aprendieron dinámicamente en el puerto.
- Al limitar a uno el número de direcciones MAC permitidas en un puerto, port security se puede utilizar para controlar el acceso no autorizado a la red.

Activar Port Security

Port security se habilita con el comando **switchport port-security** de la interfaz de puerto

Observe que en el ejemplo, el comando **switchport port-security** fue rechazado. Esto se debe a que port security solo se puede configurar en puertos de acceso o trunks configurados manualmente. Los puertos capa 2 del switch están definidos como dynamic auto (troncal encendido), de manera predeterminada. Por lo tanto, en el ejemplo, el puerto se configura con el comando **switchport mode access** de la interfaz

Nota: La configuración de port security troncal va mas allá del alcance de este curso.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

Implementar Seguridad de puertos (Port Security) Activar Port Security (Cont.)

Use el **comando show port-security interface** para mostrar la configuración de seguridad del puerto actual para FastEthernet 0/1.

- Note que port security está habilitado, el modo de violación esta apagado, y que el número máximo de direcciones MAC permitidas es 1.
- Si un dispositivo está conectado al puerto, el switch automáticamente agregará la dirección MAC de este dispositivo como una dirección MAC segura. En este ejemplo, no existe ningún dispositivo conectado al puerto.

Nota: Si un puerto activo está configurado con el comando **switchport port-security** y hay más de un dispositivo conectado a ese puerto, el puerto pasará al estado de error desactivado.

```
S1# show port-security interface f0/1
Port Security          : Enabled
Port Status             : Secure-shutdown
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 0
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
S1#
```



Activar Port Security (Cont.)

Una vez que se activa port security, se pueden configurar otras funciones específicas de port security, como se muestra en el ejemplo.

```
S1(config-if)# switchport port-security ?
  aging          Port-security aging commands
  mac-address   Secure mac address
  maximum        Max secure addresses
  violation      Security violation mode
<cr>
S1(config-if)# switchport port-security
```

Implementar Seguridad de Puertos (Port Security) Limitar y aprender direcciones MAC

Para poner el número máximo de direcciones MAC permitidas en un puerto, utilice el siguiente comando

```
Switch(config-if)# switchport port-security maximum valor
```

- El valor predeterminado de port security es 1.
- El número máximo de direcciones MAC seguras que se puede configurar depende del switch y el IOS.
- En este ejemplo, el máximo es 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
      <1-8192> Maximum addresses
S1(config-if)# switchport port-security maximum
```

Limitar y Aprender MAC Addresses (Cont.)

El switch se puede configurar para aprender direcciones MAC en un puerto seguro de tres maneras:

1. Configuración manual: el administrador configura manualmente una dirección MAC estática mediante el siguiente comando para cada dirección MAC segura en el puerto:

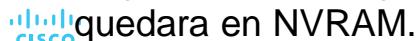
```
Switch(config-if)# switchport port-security mac-address dirección MAC
```

2. Aprendizaje dinámico: cuando se ingresa el comando **switchport port-security** la fuente MAC actual para el dispositivo conectado al puerto se asegura automáticamente pero no se agrega a la configuración en ejecución. Si el switch es reiniciado, el puerto tendrá que re-aprender la dirección MAC del dispositivo.

3. Aprendizaje dinámico – Sticky: el administrador puede configurar el switch para aprender dinámicamente la dirección MAC y "adherirla" a la configuración en ejecución mediante el siguiente comando:

```
Switch(config-if)# switchport port-security mac-address sticky
```

Al guardar la configuración en ejecución la dirección MAC aprendida automáticamente se

 quedara en NVRAM.

Limitar y Aprender direcciones MAC (Cont.)

El ejemplo muestra una configuración de seguridad de puerto completa para FastEthernet 0/1.

- El administrador especifica una cantidad máxima de 4 direcciones MAC, configura una dirección MAC segura, y luego configura el puerto para que aprenda más direcciones MAC de manera automática hasta un máximo de 4 direcciones MAC.
- Use los comandos **show port-security interface** y el **show port-security address** para verificar la configuración.

```

S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 4
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security      : Enabled
Port Status        : Secure-up
Violation Mode    : Shutdown
Aging Time        : 0 mins
Aging Type        : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 4
Total MAC Addresses  : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan  : 0000.0000.0000:0
Security Violation Count : 0
S1# show port-security address
          Secure Mac Address Table
-----+-----+-----+-----+-----+
Vlan  Mac Address     Type       Ports      Remaining Age
              (mins)
-----+-----+-----+-----+-----+
      1  aaaa.bbbb.1234  SecureConfigured  Fa0/1      -
-----+-----+-----+-----+-----+
Total Addresses In System (excluding one mac per port) : 8
Max Addresses Limit in System (excluding one mac per port) : 8192
S1#

```

Implementar Seguridad de Puertos (Port Security) activar Port Security

El vencimiento del port security puede usarse para poner el tiempo de vencimiento de las direcciones seguras estáticas y dinámicas en un puerto.

- **Absoluta**- Las direcciones seguras en el puerto se eliminan después del tiempo de caducidad especificado.
- **Inactiva**- Las direcciones seguras en el puerto se eliminan si están inactivas durante un tiempo específico.

Utilice el vencimiento para remover las direcciones MAC seguras en un puerto seguro sin necesidad de eliminar manualmente las direcciones MAC existentes.

- El vencimiento de direcciones seguras configuradas estáticamente puede ser habilitado o deshabilitado por puerto.

```
Switch(config-if)# switchport port-security aging {static | time time | type {absolute | inactivity}}
```

vencimiento estático para el puerto seguro, o para establecer el tiempo o el tipo de vencimiento.

Implementar Seguridad de Puertos (Port Security) Vencimiento de Port Security (Cont.)

El ejemplo muestra a un administrador configurando el tipo de vencimiento a 10 minutos de inactividad.

El comando **show port-security** confirma los cambios.

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security          : Enabled
Port Status             : Secure-shutdown
Violation Mode         : Restrict
Aging Time              : 10 mins
Aging Type              : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 4
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0050.56be.e4dd:1
Security Violation Count : 1
```

Implementar Seguridad de Puertos (Port Security)

Modos de violación de Port Security

Si la dirección MAC de un dispositivo conectado a un puerto difiere de la lista de direcciones seguras, se produce una violación del puerto y el puerto entra en estado de error desactivado.

```
Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}
```

La siguiente tabla muestra cómo reacciona un switch en función del modo de infracción configurado.

Modo	Descripción
shutdown (predeterminados)	El puerto pasa al estado de error desactivado de inmediato, apaga el LED del puerto y envía un mensaje de registro del sistema. Aumenta el contador de violaciones. Cuando un puerto seguro se encuentra en estado de error desactivado, un administrador debe volver a habilitarlo ingresando los comandos shutdown y no shutdown .
restrict (Restricción)	El puerto descarta paquetes con direcciones de origen desconocidas hasta que elimine un número suficiente de direcciones MAC seguras para caer por debajo del valor máximo o aumentar el valor máximo. Este modo hace que el contador de Infracción de seguridad se incremente y genera un mensaje de syslog.
protect (protección)	Este modo es el menos seguro de los modos de violaciones de seguridad. El puerto descarta paquetes con direcciones de origen MAC desconocidas hasta que elimine un número suficiente de direcciones MAC seguras para colocar por debajo del valor máximo o aumentar el valor máximo. No se envía ningún mensaje syslog.

Implementar Seguridad de Puertos (Port Security) Modos de violación de Security (Cont.)

El ejemplo muestra a un administrador cambiando la violación de seguridad a "Restrict"

El resultado del comando **show port-security interface** confirma que se ha realizado el cambio.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security           : Enabled
Port Status              : Secure-shutdown
Violation Mode          : Restrict
Aging Time               : 0 mins
Aging Type               : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses    : 4
Total MAC Addresses       : 1
Configured MAC Addresses : 1
Sticky MAC Addresses      : 0
Last Source Address:Vlan : 0050.56be.e4dd:1
Security Violation Count : 1
S1#
```

Implementar Seguridad de Puertos (Port Security) Puertos en estado de error-disabled

Cuando un puerto está apagado y puesto en modo error-desabilitado, no se envía ni se recibe tráfico a través de ese puerto.

En la consola, se muestra una serie de mensajes relacionados con la seguridad del puerto.

Nota: El protocolo del puerto y el estado del enlace se cambian a inactivo y el LED del puerto se apaga.

```
*Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting Fa0/18 in  
err-disable state  
*Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC  
address 000c.292b.4c75 on port FastEthernet0/18.  
*Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface FastEthernet0/18, changed state  
to down  
*Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

Puertos en estado error-disabled (Cont.)

- En el ejemplo, el comando **show interface** identifica el estado del puerto como **err-disabled**. La salida del comando **show port-security interface** ahora muestra el estado del puerto como **secure-shutdown**. El contador de violación incrementa en uno.
- El administrador debe determinar que causó la violación de seguridad, si un dispositivo no autorizado está conectado a un puerto seguro, la amenazas de seguridad es eliminada antes de restablecer el puerto.
- Para volver a habilitar el puerto, primero use el **shutdown** luego, use el comando **no shutdown**.

```
S1# show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)

S1# show port-security interface fa0/18
Port Security          : Enabled
Port Status             : Secure-shutdown
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses: 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : c025.5cd7.ef01:1
Security Violation Count : 1
S1#
```

Verificar Port Security

Después de configurar la seguridad de puertos en un switch, revise cada interfaz para verificar que la seguridad de puertos y las direcciones MAC estáticas se configuraron correctamente.

Para mostrar la configuración de seguridad del puerto para el conmutador, use el comando **show port-security**.

- El ejemplo indica que las 24 interfaces están configuradas con el comando **switchport port-security** porque el máximo permitido es 1 y el modo de violación está apagado.
- No hay dispositivos conectados, por lo tanto, el CurrentAddr (Count) es 0 para cada interfaz.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)      (Count)      (Count)
-----
Fa0/1           1            0            0     Shutdown
Fa0/2           1            0            0     Shutdown
Fa0/3           1            0            0     Shutdown
(output omitted)
Fa0/24          1            0            0     Shutdown
-----
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Implementar Seguridad de Puertos (Port Security) Verificar Port Security (Cont.)

Use el comando **show port-security interface** para ver detalles de una interfaz específica, como se mostró anteriormente y en este ejemplo.

```
S1# show port-security interface fastethernet 0/18
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0025.83e6.4b01:1
Security Violation Count : 0
S1#
```

Implementar Seguridad de Puertos (Port Security) Verificar Port Security (Cont.)

Para verificar que las direcciones MAC están configuradas “sticking” (pegadas) a la configuración, use el comando **show run** como se muestra en el ejemplo de FastEthernet 0/19.

```
S1# show run | begin interface FastEthernet0/19
interface FastEthernet0/19
switchport mode access
switchport port-security maximum 10
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0025.83e6.4b02
(output omitted)
S1#
```

Implementar Seguridad de Puertos (Port Security)

Verificar Port Security (Cont.)

Para mostrar todas las direcciones MAC seguras que son configuradas manualmente o aprendidas dinámicamente en todas las interfaces del switch use el comando **show port-security address** como se muestra en el ejemplo.

```
S1# show port-security address
Secure Mac Address Table
-----
Vlan   Mac Address      Type        Ports      Remaining Age
                                         (mins)
----  -----  -----  -----  -----
1      0025.83e6.4b01  SecureDynamic Fa0/18    -
1      0025.83e6.4b02  SecureSticky  Fa0/19    -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

11.2 - Mitigación de los ataques de VLAN

Revisión de ataques de VLAN

Un ataque de salto de VLAN se puede iniciar de una de tres maneras:

- La suplantación de mensajes DTP del host atacante hace que el switch entre en modo de enlace troncal. Desde aquí, el atacante puede enviar tráfico etiquetado con la VLAN de destino, y el switch luego entrega los paquetes al destino.
- Introduciendo un switch dudoso y habilitando enlaces troncales. El atacante puede acceder todas las VLANs del switch víctima desde el switch dudoso.
- Otro tipo de ataque de salto a VLAN es el ataque doble etiqueta o doble encapsulado. Este ataque toma ventaja de la forma en la que opera el hardware en la mayoría de los switches.

Pasos para mitigar los ataques de salto de VLAN

Use los siguiente pasos para mitigar ataques de salto

Paso 1: Deshabilitar las negociaciones DTP (enlace automático) en los puertos que no son enlaces mediante el comando **switchport mode access** en la interfaz del switch.

Paso 2: Deshabilitar los puertos no utilizados y colocarlos en una VLAN no utilizada.

Paso 3: Habilitar manualmente el enlace troncal en un puerto de enlace troncal utilizando el comando **switchport mode trunk**.

Paso 4: Deshabilitar las negociaciones de DTP (enlace automático) en los puertos de enlace mediante el comando **switchport nonegotiate**.

Paso 5: Configurar la VLAN nativa en una VLAN que no sea la VLAN 1 mediante el comando **switchport trunk native vlan** *vlan_number*.

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```

11.3 - Mitigación de ataques de DHCP

Revisión de ataque de DHCP

El objetivo de un ataque de agotamiento DHCP es que una herramienta de ataque como Gobbler cree una Denegación de servicio (DoS) para conectar clientes.

Recuerde que los ataques de agotamiento de DHCP pueden ser efectivamente mitigados usando seguridad de puertos, porque Gobbler usa una dirección MAC de origen única para cada solicitud DHCP enviada. Sin embargo mitigar ataques DHCP de suplantación de identidad requiere mas protección.

Gobbler podría configurarse para usar la dirección MAC de la interfaz real como la dirección Ethernet de origen, pero especifique una dirección Ethernet diferente en la carga útil de DHCP. Esto haría que la seguridad del puerto sea ineficaz porque la dirección MAC de origen sería legítima.

Los ataques de suplantación de DHCP se pueden mitigar mediante el uso de detección DHCP en puertos confiables.



Mediante detección de DHCP

La inspección de DHCP filtra los mensajes de DHCP y limita el tráfico de DHCP en puertos no confiables.

- Los dispositivos bajo control administrativo (por ejemplo, switches, routers y servidores) son fuentes confiables.
- Las interfaces confiables (por ejemplo, enlaces troncales, puertos del servidor) deben configurarse explícitamente como confiables.
- Los dispositivos fuera de la red y todos los puertos de acceso generalmente se tratan como fuentes no confiables.

Se crea una tabla DHCP que incluye la dirección MAC de origen de un dispositivo en un puerto no confiable y la dirección IP asignada por el servidor DHCP a ese dispositivo.

- La dirección MAC y la dirección IP están unidas.
- Por lo tanto, esta tabla se denomina tabla de enlace DHCP snooping.

Pasos para implementar DHCP Snooping

Utilice las siguientes pasos para habilitar DHCP snooping:

Paso 1. Habilite DHCP snooping usando el comando **ip dhcp snooping** en modo global

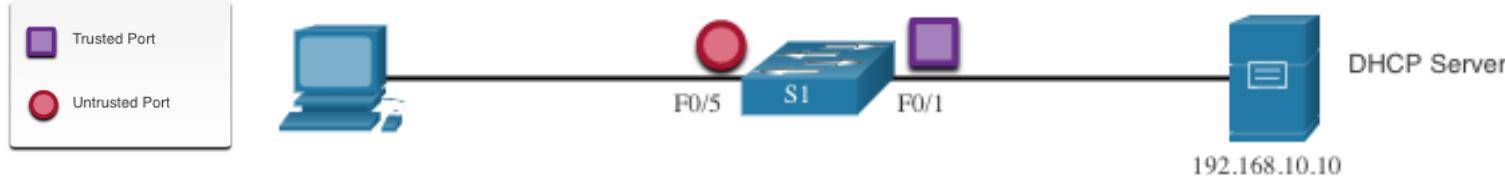
Paso 2. En los puertos de confianza, use el comando **ip dhcp snooping trust**.

Paso 3: En las interfaces que no son de confianza, limite la cantidad de mensajes de descubrimiento de DHCP que se pueden recibir con el comando **ip dhcp snooping limit rate packets-per-second** .

Paso 4. Habilite la inspección DHCP por VLAN, o por un rango de VLAN, utilizando el comando **ip dhcp snooping vlan**.

Ejemplo de configuración de DHCP Snooping

Consulte la topología de ejemplo de indagación DHCP con puertos confiables y no confiables



- La inspección DHCP se habilita primero en S1.
- La interfaz ascendente al servidor DHCP es explícitamente confiable.
- F0/5 a F0/24 no son de confianza y, por lo tanto, su velocidad se limita a seis paquetes por segundo.
- Finalmente, la inspección DHCP está habilitada en VLANS 5, 10, 50, 51 y 52.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

Ejemplo de configuración de DHCP Snooping (Cont.)

Utilice el comando **show ip dhcp snooping** para verificar la configuración de inspección DHCP.

Use el comando **show ip dhcp snooping binding** para ver los clientes que han recibido información de DHCP.

Nota: DHCP snooping también requiere Dynamic ARP Inspection (DAI).

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface      Trusted     Allow option    Rate limit (pps)
-----
FastEthernet0/1   yes        yes            unlimited
  Custom circuit-ids:
FastEthernet0/5   no         no             6
  Custom circuit-ids:
FastEthernet0/6   no         no             6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN Interface
-----
00:03:47:B5:9F:AD  192.168.10.10  193185    dhcp-snooping  5   FastEthernet0/5
```

11.4 - Mitigación de ataques de ARP

Inspección dinámica de ARP

En un ataque típico el atacante puede enviar respuestas ARP no solicitadas, a otros hosts en la subred con la dirección MAC del atacante y la dirección IP de la puerta de enlace predeterminada. Para evitar la suplantación de ARP y el envenenamiento por ARP resultante, un interruptor debe garantizar que solo se transmitan las Solicitudes y Respuestas de ARP válidas.

La inspección dinámica(DAI) requiere de DHCP snooping y ayuda a prevenir ataques ARP así:

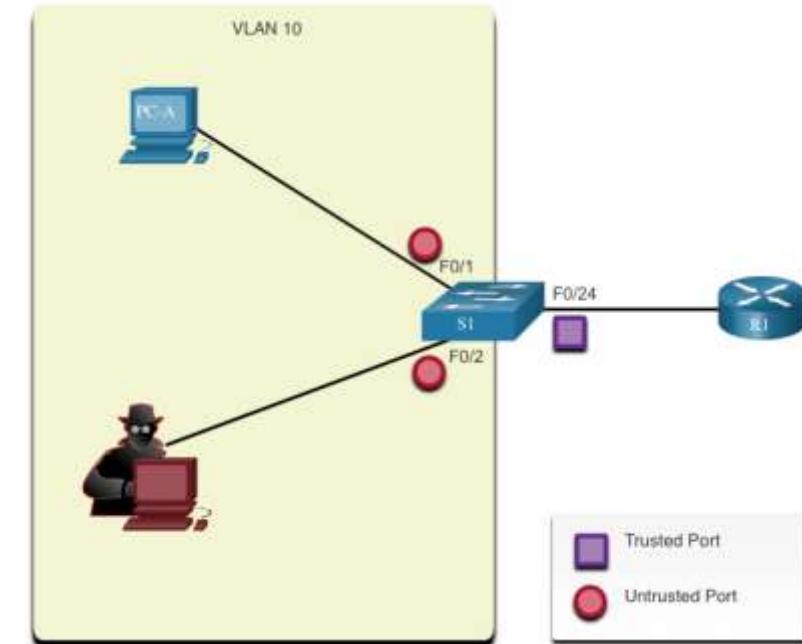
- No retransmitiendo respuestas ARP invalidas o gratuitas a otros puertos en la misma VLAN.
- Intercepta todas las solicitudes y respuestas ARP en puertos no confiables.
- Verificando cada paquete interceptado para una IP-to-MAC Binding válida.
- Descarte y registre ARP Replies no válidos para evitar el envenenamiento de ARP.
- Error-disabling deshabilita la interfaz si se excede el número DAI configurado de paquetes ARP.

Pautas de implementación de DAI

Para mitigar las probabilidades de ARP spoofing y envenenamiento ARP, siga estas pautas de implementación DAI:

- Habilite la detección de DHCP.
- Habilite la detección de DHCP en las VLAN seleccionadas.
- Habilite el DAI en los VLANs seleccionados.
- Configure las interfaces de confianza para la detección de DHCP y la inspección de ARP ("no confiable" es la configuración predeterminada).

Generalmente, es aconsejable configurar todos los puertos de switch de acceso como no confiables y configurar todos los puertos de enlace ascendente que están conectados a otros switches como confiables.



Ejemplo de configuración de DAI

En la topología anterior S1 está conectado a dos usuarios en la VLAN 10.

- DAI será configurado para mitigar ataques ARP spoofing y envenenamiento ARP.
- La inspección DHCP está habilitada porque DAI requiere que funcione la tabla de enlace de inspección DHCP.
- Continua, la detección de DHCP y la inspección de ARP están habilitados para la computadora en la VLAN 10.
- El puerto de enlace ascendente al router es confiable y, por lo tanto, está configurado como confiable para la inspección DHP y ARP.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

Ejemplo de configuración de DAI (Cont.)

DAI se puede configurar para revisar si hay direcciones MAC e IP de destino o de origen:

- **MAC de destino** Comprueba la dirección MAC de destino en el encabezado de Ethernet con la dirección MAC de destino en el cuerpo ARP.
- **MAC de origen**- Comprueba la dirección MAC de origen en el encabezado de Ethernet con la dirección MAC del remitente en el cuerpo ARP.
- **Dirección IP**- Comprueba el cuerpo ARP para direcciones IP no válidas e inesperadas, incluidas las direcciones 0.0.0.0, 255.255.255.255 y todas las direcciones de multidifusión IP.

Ejemplo de configuración de DAI (Cont.)

El comando de configuración global: **ip arp inspección validate {[src-mac] [dst-mac] [ip]}** se utiliza para configurar DAI para descartar paquetes ARP cuando las direcciones IP no son válidas.

- Se puede usar cuando las direcciones MAC en el cuerpo de los paquetes ARP no coinciden con las direcciones que se especifican en el encabezado Ethernet.
- Note como en el siguiente ejemplo, sólo un comando de validación de inspección de arp sobre escribe el comando anterior.
- Para incluir más de un método de validación, ingréselos en la misma línea de comando como se muestra y verifíquelo en la siguiente salida.

```
S1(config)# ip arp inspection validate ?
dst-mac  Validate destination MAC address
ip      Validate IP addresses
src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#

```

11.5 - Mitigar ataques STP

PortFast y protección de BPDU

Recuerde que los atacantes de red pueden manipular el Protocolo de árbol de expansión (STP) para realizar un ataque falsificando el puente raíz y cambiando la topología de una red.

Para mitigar los ataques STP, use PortFast y la protección de la unidad de datos de protocolo de puente (BPDU):

PortFast

- PortFast lleva inmediatamente un puerto al estado de reenvío desde un estado de bloqueo, sin pasar por los estados de escucha y aprendizaje.
- Aplica a todos los puertos de acceso de usuario final.

Protección de BPDU

- El error de protección de BPDU deshabilita inmediatamente un puerto que recibe una BPDU.
- Al igual que PortFast, la protección BPDU sólo debe configurarse en interfaces conectadas a dispositivos finales.

Configurar PortFast

PortFast omite los estados de escucha y aprendizaje de STP para minimizar el tiempo que los puertos de acceso deben esperar a que STP converja.

- Sólo habilite PortFast en los puertos de acceso.
- PortFast en enlaces entre comutadores puede crear un bucle de árbol de expansión.

PortFast se puede habilitar:

- **En una interfaz:** – utilice el comando de **spanning-tree portfast**.
- **Globalmente:** – use el comando de **spanning-tree portfast default** para habilitar PortFast en todos los puertos de acceso.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
should now disable portfast explicitly on switched ports leading to hubs,
switches and bridges as they may create temporary bridging loops.
S1(config)# exit
```

Configurar PortFast(Cont.)

Para verificar si PortFast está habilitado globalmente, puede usar:

- Comando **show running-config | begin span**
- Comando **show spanning-tree summary**

Para verificar si PortFast tiene habilitada una interfaz, use el comando **show running-config interface type/number** .

El comando **show spanning-tree interface type/number detail** también se puede utilizar para la verificación.

Configure BPDU Guard

Un puerto de acceso podría recibir un BPDU inesperado accidentalmente o porque un usuario conectó un switch no autorizado al puerto de acceso.

- Si se recibe una BPDU en un puerto de acceso habilitado para BPDU Guard, el puerto se pone en estado de error deshabilitado.
- Esto significa que el puerto se cierra y debe volver a habilitarse manualmente o recuperarse automáticamente a través del comando **errdisable recovery cause psecureViolation**.

BPDU Guard se puede habilitar:

- **En una interfaz:** – use el comando **spanning-tree bpduguard enable** .
- **Globalmente:** – use el comando de configuración **spanning-tree portfast bpduguard default** para habilitar BPDU Guard en todos los puertos de acceso.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID      is enabled
Portfast Default        is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is disabled
EtherChannel misconfig guard is enabled
UplinkFast              is disabled
BackboneFast             is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```



Conceptos de WLAN

Switching, Routing y Wireless Essentials v7.0
(SRWE)



Objetivos del Módulo

Título del módulo: Conceptos de WLAN

Objetivo del módulo: Explivar cómo las WLAN habilitan la conectividad de red.

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

12.1 - Introducción a la Tecnología Inalámbrica

Beneficios de la Tecnología Inalámbrica

- Una LAN Inalámbrica (WLAN) es un tipo de red inalámbrica que se usa comúnmente en hogares, oficinas y entornos de campus.
- Las WLAN hacen posible la movilidad dentro de los entornos domésticos y comerciales.
- Las infraestructuras inalámbricas se adaptan a las necesidades y tecnologías que cambian rápidamente.



Introducción a la Tecnología Inalámbrica

Tipos de Redes Inalámbricas

- **Red Inalámbrica de Área Personal (WPAN)** – Baja potencia y corto alcance (20-30 pies o 6-9 metros). Basado en el estándar IEEE 802.15 y una frecuencia de 2.4 GHz. Bluetooth y Zigbee son ejemplos de WPAN.
- **LAN Inalámbrica (WLAN)** – Redes de tamaño mediano de hasta aproximadamente 300 pies. Basado en el estándar IEEE 802.11 y una frecuencia de 2.4 GHz o 5.0 GHz.
- **Wireless MAN (WMAN)** – Gran área geográfica, como ciudad o distrito. Utiliza frecuencias específicas con licencia.
- **WAN inalámbrica (WWAN)** – Área geográfica extensa para la comunicación nacional o global. Utiliza frecuencias específicas con licencia.

Introducción a la Tecnología Inalámbrica

Tecnologías Inalámbricas

Bluetooth – Estándar IEEE WPAN utilizado para emparejar dispositivos a una distancia de hasta 300 pies (100 m).

- Bluetooth de Baja Energía (BLE) - Admite topología de malla para dispositivos de red a gran escala.
- Bluetooth velocidad básica/mejorada (BR / EDR) - Admite topologías punto a punto y está optimizada para la transmisión de audio.

WiMAX (Interoperabilidad mundial para acceso por microondas) – Conexiones alternativas a Internet de banda ancha por cable. IEEE 802.16 WLAN estándar para hasta 30 millas (50 km).



Introducción a la Tecnología Inalámbrica

Tecnologías Inalámbricas (Cont.)

Banda Ancha celular – Transporte de voz y datos. Usado por teléfonos, automóviles, tabletas y computadoras portátiles.

- Global System of Mobile (GSM) – Reconocido internacionalmente
- Code Division Multiple Access (CDMA) – Principalmente utilizado en los Estados Unidos.

Banda ancha satelital – Utiliza una antena parabólica direccional alineada con el satélite en órbita geoestacionaria. Necesita una línea clara del sitio. Normalmente se usa en ubicaciones rurales donde el cable y el DSL no están disponibles.



Introducción a la Tecnología Inalámbrica

Estándares 802.11

Los estándares 802.11 WLAN definen cómo se usan las frecuencias de radio para los

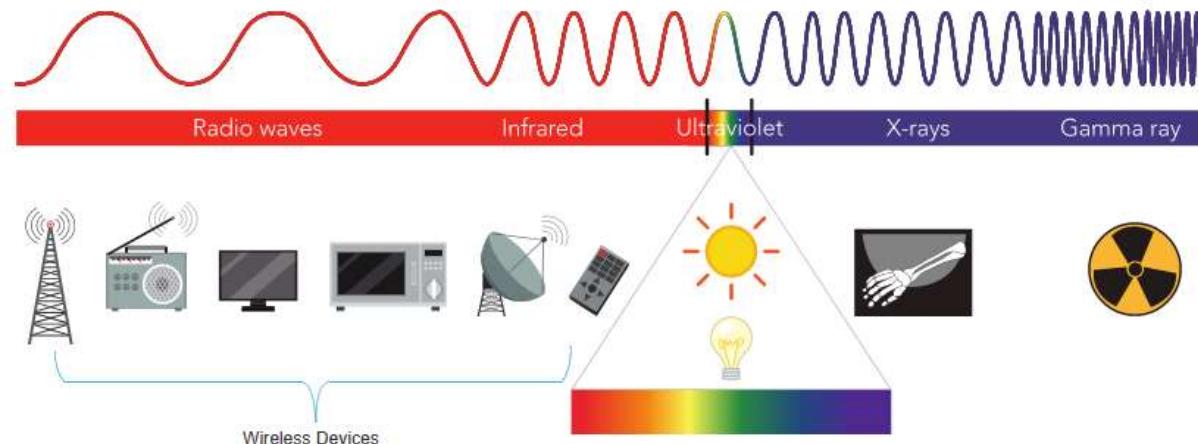
Estándar IEEE	Frecuencias de radio	Descripción
802.11	2,4 GHz	Velocidades de datos de hasta 2 Mb/s
802.11a	5 GHz	Velocidades de datos de hasta 54 Mb / s No interoperable con 802.11b o 802.11g
802.11b	2,4 GHz	Velocidades de datos de hasta 11 Mb / s Mayor alcance que 802.11a y mejor penetración en las 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

Introducción a las frecuencias de radio

Radio Frecuencias

Todos los dispositivos inalámbricos funcionan en el rango del espectro electromagnético. Las redes WLAN funcionan en bandas de frecuencia de 2,4 y 5 GHz.

- 2.4 GHz (UHF) - 802.11b/g/n/ax
- 5 GHz (SHF) – 802.11a/n/ac/ax



Organizaciones de Estándares Inalámbricos

Los estándares aseguran la interoperabilidad entre dispositivos fabricados por diferentes fabricantes. A nivel internacional, las tres organizaciones que influyen en los estándares WLAN:

- **International Telecommunication Union (UIT)**: – Regula la asignación del espectro radioeléctrico y las órbitas satelitales.
- **Institute of Electrical and Electronics Engineers (IEEE)** – Especifica cómo se modula una frecuencia de radio para transportar información. Mantiene los estándares para redes de área local y metropolitana (MAN) con la familia de estándares IEEE 802 LAN / MAN.
- **Alianza Wi-Fi** – Promueve el crecimiento y la aceptación de las WLAN. Es una asociación de proveedores cuyo objetivo es mejorar la interoperabilidad de los productos que se basan en el estándar 802.1

12.2 - Componentes de la WLAN

Componentes WLAN NICs inalámbrica

Para comunicarse de forma inalámbrica, las computadoras portátiles, tabletas, teléfonos inteligentes e incluso los últimos automóviles incluyen NIC inalámbricas integradas que incorporan un transmisor / receptor de radio.

Si un dispositivo no tiene una NIC inalámbrica integrada, se puede utilizar un adaptador inalámbrico USB.



Router de Hogar Inalámbrico

Un usuario doméstico generalmente interconecta dispositivos inalámbricos utilizando un pequeño router inalámbrico.

Los routers inalámbricos sirven de la siguiente manera:

- **Punto de acceso** – Para proporcionar acceso por cables
- **Switch** – Para interconectar dispositivos cableados
- **Router** - Para proporcionar una puerta de enlace predeterminada a otras redes e Internet



Punto de acceso inalámbrico

Los clientes inalámbricos usan su NIC inalámbrica para descubrir puntos de acceso cercanos (APs).

Los clientes luego intentan asociarse y autenticarse con un AP.

Después de la autenticación, los usuarios inalámbricos tienen acceso a los recursos de la red.



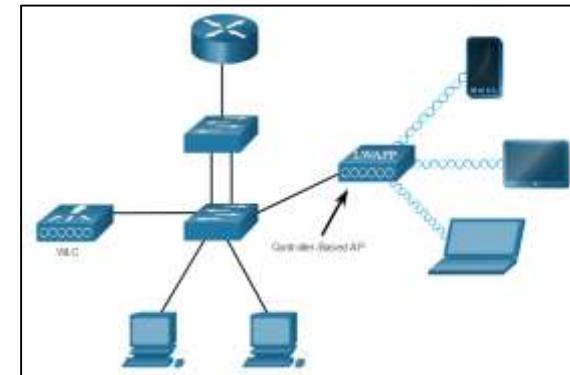
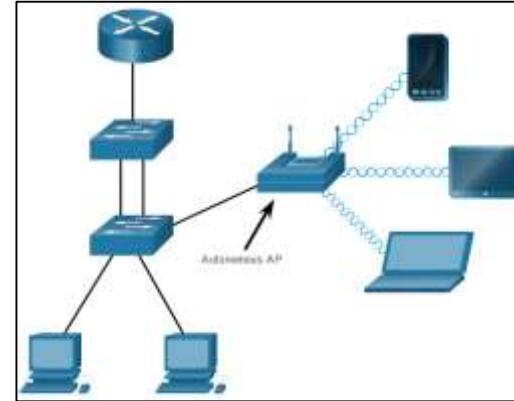
Puntos de acceso Cisco
Meraki Go

Componentes WLAN

Categorías AP

Los AP se pueden categorizar como AP autónomos o AP basados en controladores.

- **AP autónomos** – Dispositivos independientes configurados a través de una interfaz de línea de comandos o GUI. Cada AP autónomo actúa independientemente de los demás y es configurado y administrado manualmente por un administrador.
- **APs basados en controlador** – También conocidos como AP ligeros (LAPs). Utilice el Protocolo de punto de acceso ligero (LWAPP) para comunicarse con un controlador LWAN (WLC). Cada LAP es configurado y administrado automáticamente por el WLC.



Componentes WLAN

Antenas Inalámbricas

Tipos de antenas externas:

- **Omnidireccional**– Proporcionan cobertura de 360 grados. Ideal en áreas de viviendas y oficinas.
- **Direccional**– Enfoca la señal de radio en una dirección específica. Ejemplos son el Yagi y el plato parabólico.
- **Multiple Input Multiple Output (MIMO)** – Utiliza múltiples antenas (hasta ocho) para aumentar el ancho de banda.



12.3 – Funcionamiento de la WLAN

802.11 Modos de topología inalámbrica

Modo ad hoc - Se utiliza para conectar clientes de igual a igual sin un AP.



Modo de infraestructura - Se usa para conectar clientes a la red utilizando un AP.



Tethering - La variación de la topología ad hoc es cuando un teléfono inteligente o tableta con acceso a datos móviles está habilitado para crear un punto de acceso personal.



Operación de WLAN BSS y ESS

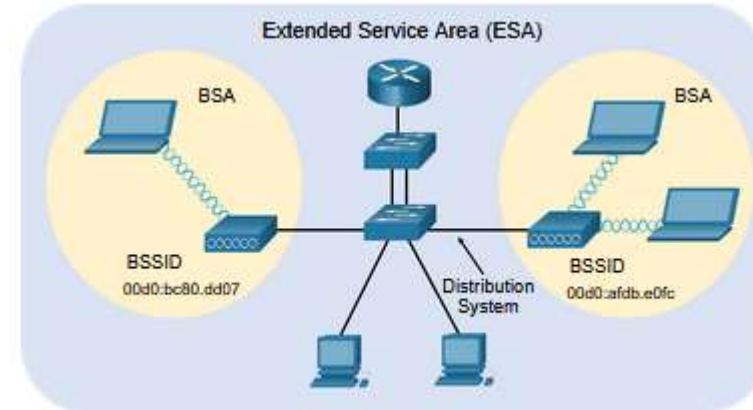
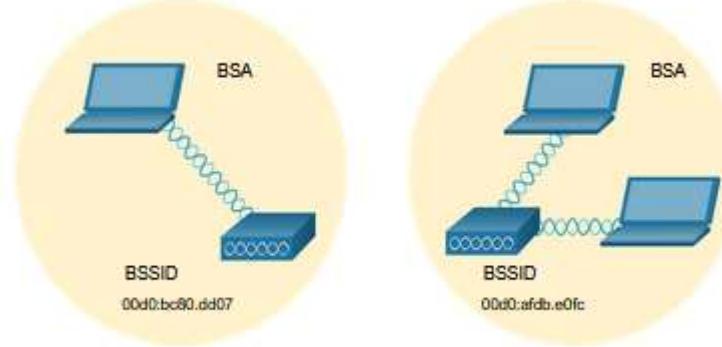
El modo de infraestructura define dos bloques de topología:

Conjunto de Servicios Básicos (BSS)

- Utiliza un AP único para interconectar todos los clientes inalámbricos asociados.
- Los clientes en diferentes BSS no pueden comunicarse.

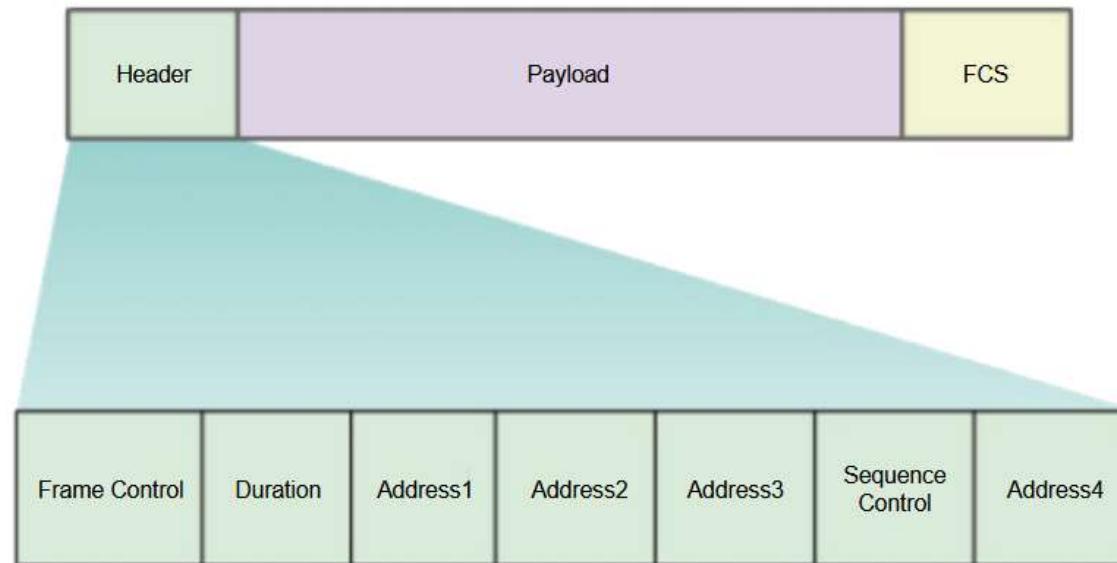
Conjunto de Servicios Extendidos (ESS)

- Una unión de dos o más BSS interconectados por un sistema de distribución por cable.
- Los clientes en cada BSS pueden comunicarse a través del ESS.



802.11 Estructura de trama

El formato de trama 802.11 es similar al formato de trama de Ethernet, excepto que contiene más campos.



Operación de WLAN CSMA/CA

Las WLAN son semidúplex y un cliente no puede "escuchar" mientras envía, por lo que es imposible detectar una colisión.

Las WLAN utilizan el acceso múltiple con detección de operador con evitación de colisiones (CSMA / CA) para determinar cómo y cuándo enviar datos. Un cliente inalámbrico hace lo siguiente:

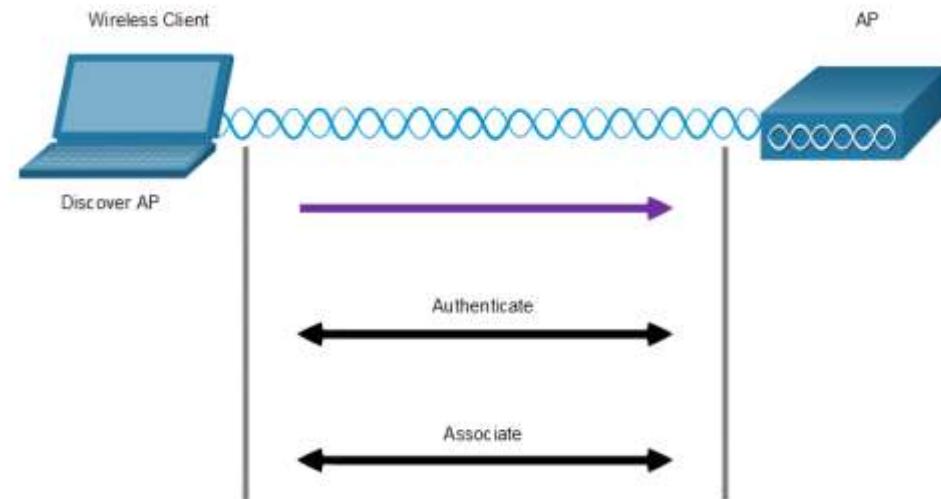
1. Escucha el canal para ver si está inactivo, es decir, no hay otro tráfico actualmente en el canal.
2. Envía un mensaje Ready to Send (RTS) al AP para solicitar acceso dedicado a la red.
3. Recibe un mensaje Clear to Send (CTS) del AP que otorga acceso para enviar.
4. Espera una cantidad de tiempo aleatoria antes de reiniciar el proceso si no se recibe un mensaje CTS.
5. Transmite los datos.
6. Reconoce todas las transmisiones. Si un cliente inalámbrico no recibe el reconocimiento, supone que ocurrió una colisión y reinicia el proceso.

Cliente Inalámbrico y Asociación AP

Para que los dispositivos inalámbricos se comuniquen a través de una red, primero se deben asociar a un AP o un router inalámbrico.

Los dispositivos inalámbricos completan las tres etapas del siguiente proceso:

- Descubre un AP inalámbrico
- Autenticar el AP
- Asociarse con el AP



Cliente Inalámbrico y Asociación AP(Cont.)

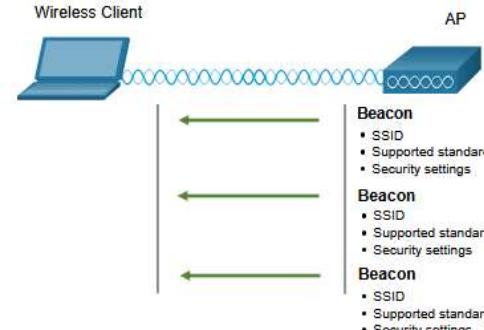
Para lograr una asociación exitosa, un cliente inalámbrico y un AP deben aceptar parámetros específicos:

- **SSID** – El cliente necesita saber el nombre de la red para conectarse.
- **Contraseña** – Esto es necesario para que el cliente se autentique en el AP.
- **Modo de red** – El estándar 802.11 en uso.
- **Modo de Seguridad** – La configuración de los parámetros de seguridad, es decir, WEP, WPA o WPA2.
- **Configuraciones de canal** – Las bandas de frecuencia en uso.

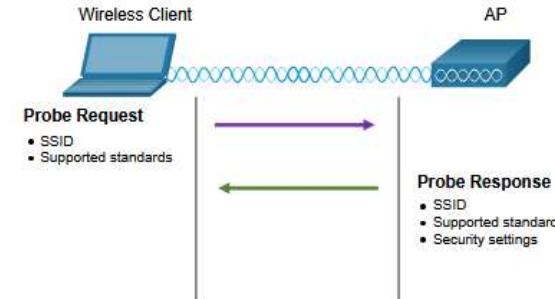
Modo de entrega Pasiva y Activa

Los clientes inalámbricos se conectan al AP mediante un proceso de escaneo (sondeo) pasivo o activo.

- **Modo pasivo:** el AP anuncia abiertamente su servicio enviando periódicamente tramas de señal de difusión que contienen el SSID, los estándares admitidos y la configuración de seguridad.
- **Modo activo :** los clientes inalámbricos deben conocer el nombre del SSID. El cliente inalámbrico inicia el proceso al transmitir por difusión una trama de solicitud de sondeo en varios canales.



Modo pasivo



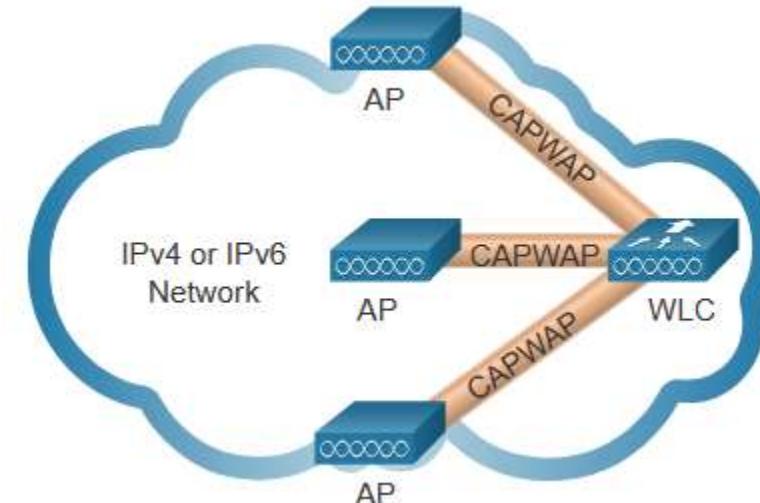
Modo activo

12.4 - Funcionamiento de la CAPWAP

Operación de la CAPWAP

Introducción a CAPWAP

- CAPWAP es un protocolo estándar IEEE que permite que un WLC administre múltiples AP y WLAN.
- Basado en LWAPP pero agrega seguridad adicional con Datagram Transport Layer Security (DLTS).
- Encapsula y reenvía el tráfico del cliente WLAN entre un AP y un WLC a través de túneles utilizando los puertos UDP 5246 y 5247.
- Opera sobre IPv4 e IPv6. IPv4 usa el protocolo IP 17 e IPv6 usa el protocolo IP 136.



Operación de la CAPWAP Arquitectura MAC dividida

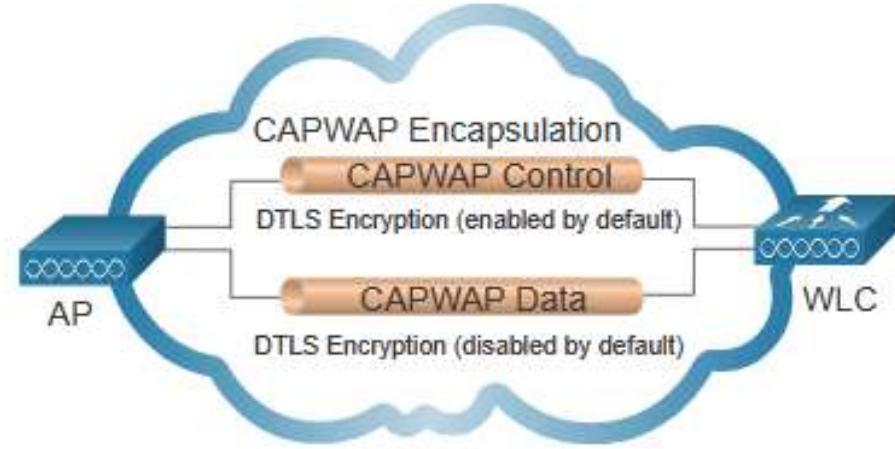
El concepto CAPWAP split MAC realiza todas las funciones que normalmente realizan los AP individuales y las distribuye entre dos componentes funcionales:

- AP Funciones MAC
- Funciones WLC MAC

AP Funciones MAC	Funciones WLC MAC
Beacons y respuestas probe	Autenticación.
Reconocimientos de paquetes y retransmisiones	Asociación y re-asociación de clientes itinerantes.
Cola de Frame y priorización de paquetes	Traducción de Frames a otros protocolos.
Cifrado y descifrado de datos de capa MAC	Terminación del tráfico 802.11 en una interfaz cableada.

Operación de CAPWAP Cifrado DTLS

- DTLS proporciona seguridad entre el AP y el WLC.
- Está habilitado de manera predeterminada para proteger el canal de control CAPWAP y cifrar todo el tráfico de administración y control entre AP y WLC.
- El cifrado de datos está deshabilitado de manera predeterminada y requiere que se instale una licencia DTLS en el WLC antes de que se pueda habilitar en el AP.



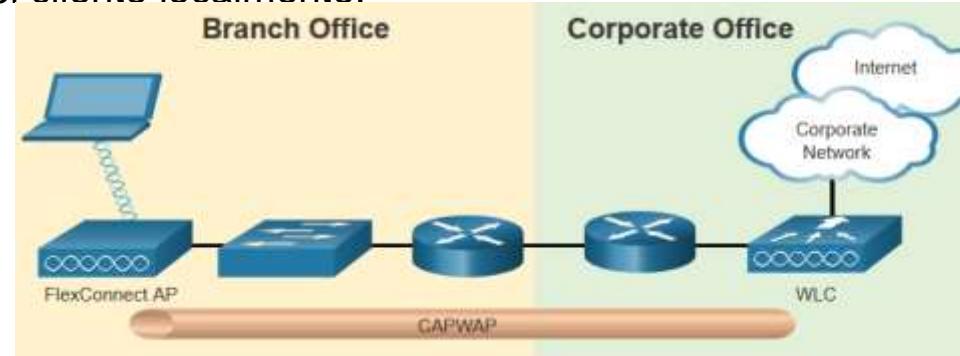
Operación de CAPWAP

Conexión flexible a AP

FlexConnect permite la configuración y el control de Aps a través de un enlace WAN.

Hay dos modos de opción para la Conexión flexible a AP:

- **Modo conectado** – El WLC es accesible. La Conexión flexible a AP tiene conectividad CAPWAP con el WLC a través del túnel CAPWAP. El WLC realiza todas las funciones CAPWAP.
- **Modo independiente** – El WLC es inalcanzable. La Conexión flexible a AP ha perdido la conectividad CAPWAP con el WLC. La Conexión Flexible a AP puede asumir algunas de las funciones de WLC, como cambiar el tráfico de datos del cliente localmente y realizar la autenticación del cliente localmente.



12.5 - Gestión de Canales

Canal de Frecuencia de Saturación

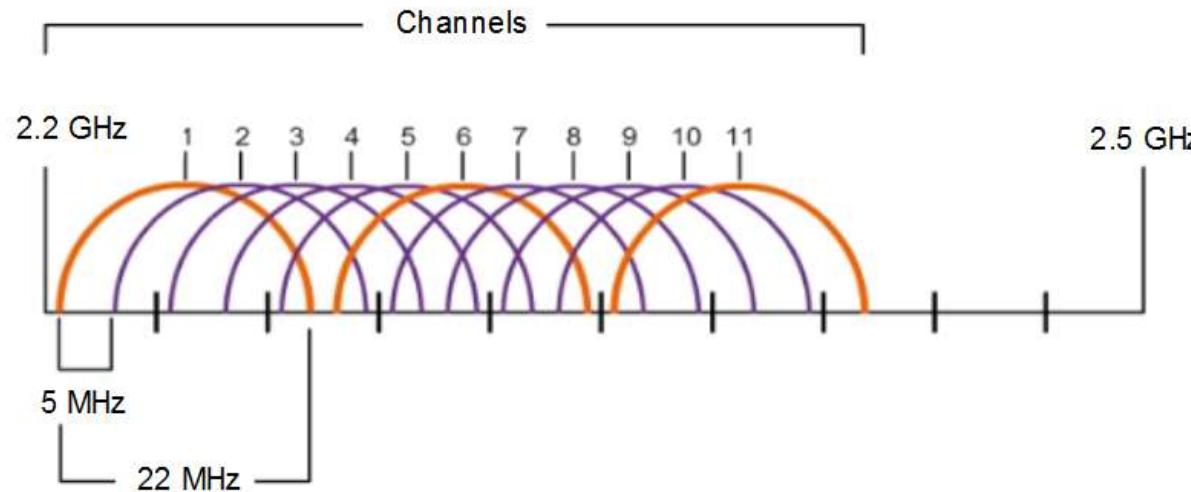
Si la demanda de un canal inalámbrico específico es demasiado alta, el canal puede sobresaturarse, degradando la calidad de la comunicación.

La saturación de canales se puede mitigar utilizando técnicas que usan los canales de manera más eficiente.

- **Direct-Sequence Spread Spectrum (DSSS)** - Una técnica de modulación diseñada para extender una señal sobre una banda de frecuencia más grande. Usado por dispositivos 802.11b para evitar interferencias de otros dispositivos que usan la misma frecuencia de 2.4 GHz.
- **Frequency-Hopping Spread Spectrum (FHSS)** - Transmite señales de radio cambiando rápidamente una señal portadora entre muchos canales de frecuencia. El emisor y el receptor deben estar sincronizados para "saber" a qué canal saltar. Usado por el estándar 802.11 original.
- **Orthogonal Frequency-Division Multiplexing (OFDM)** - Subconjunto de multiplexación por división de frecuencia en el que un solo canal utiliza múltiples subcanales en frecuencias adyacentes. Una serie de sistemas de comunicación, incluidos los estándares 802.11a/g/n/ac, usa OFDM.

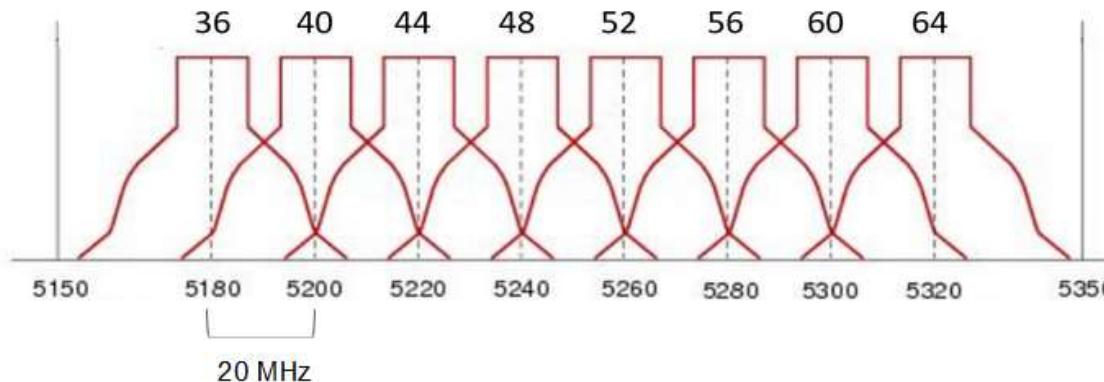
Selección del canal

- La banda de 2,4 GHz se subdivide en múltiples canales, cada uno de los cuales tiene un ancho de banda de 22 MHz y se separa del siguiente canal en 5 MHz.
- Una práctica recomendada para las WLAN 802.11b/g/n que requieren múltiples AP es utilizar canales no superpuestos, como 1, 6 y 11.



Selección de canales (Cont.)

- Para los estándares de 5 GHz 802.11a/n/ac, hay 24 canales. Cada canal está separado del siguiente canal por 20 MHz
- Los canales no superpuestos son 36, 48 y 60.

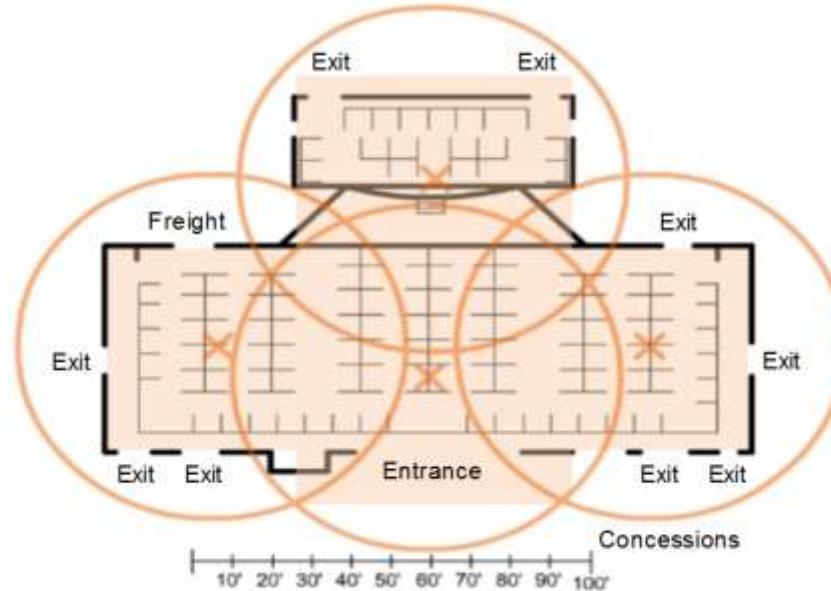


Planifique la Implementación de WLAN

El número de usuarios admitidos por una WLAN depende de lo siguiente:

- El diseño geográfico de la instalación.
- La cantidad de cuerpos y dispositivos que pueden caber en un espacio.
- Las tasas de datos que los usuarios esperan.
- El uso de canales no superpuestos por múltiples AP y configuraciones de potencia de transmisión.

Al planificar la ubicación de los puntos de acceso, el área de cobertura circular aproximada es importante.



12.6 – Amenazas en la WLAN

Resumen de seguridad inalámbrica

Una WLAN está abierta a cualquier persona dentro del alcance de un AP con las credenciales correspondientes para asociarse a él.

Las personas ajenas a la empresa, los empleados insatisfechos e incluso otros empleados, involuntariamente, pueden generar los ataques. Las Redes Inalámbricas son específicamente susceptibles a varias amenazas, incluidas las siguientes:

- Intercepción de datos.
- Intrusos inalámbricos.
- Ataques de denegación de servicio (DoS).
- AP dudosos.

Amenazas en la WLAN

Ataques DoS

Los ataques DoS inalámbricos pueden ser el resultado de lo siguiente:

- Dispositivos mal configurados
- Un usuario malintencionado que interfiere intencionalmente con la comunicación inalámbrica
- Interferencia accidental.

Para minimizar el riesgo de un ataque DoS debido a dispositivos mal configurados y ataques maliciosos, fortalezca todos los dispositivos, mantenga las contraseñas seguras, cree copias de seguridad y asegúrese de que todos los cambios de configuración se incorporen fuera de horario.

Puntos de acceso no autorizados

- Un AP falso es un AP o un router inalámbrico que se ha conectado a una red corporativa sin autorización explícita y en contra de la política corporativa.
- Una vez conectado, el AP falso puede ser usado por el atacante para capturar direcciones MAC, capturar paquetes de datos, obtener acceso a recursos de red o lanzar un ataque intermedio.
- Un punto de acceso a la red personal también podría usarse como un AP no autorizado. Por ejemplo, un usuario con acceso seguro a la red habilita su host de Windows autorizado para que se convierta en un AP Wi-Fi.
- Para evitar la instalación de puntos de acceso no autorizados, las organizaciones deben configurar WLC con políticas de puntos de acceso no autorizados y utilizar software de monitoreo para monitorear activamente el espectro de radio en busca de puntos de acceso no autorizados.

Ataques intermediarios

En un ataque intermedio (MITM por su sigla en inglés), el pirata informático se coloca entre dos entidades legítimas para leer o modificar los datos que pasan entre las dos partes. Un popular ataque MITM inalámbrico se denomina “ataque con AP de red intrusa”, en el que un atacante introduce un AP no autorizado y lo configura con el mismo SSID que el de un AP legítimo.

La derrota de un ataque MITM comienza con la identificación de dispositivos legítimos en la WLAN. Para hacer esto, se deben autenticar los usuarios. Una vez que se conocen todos los dispositivos legítimos, se puede monitorear la red para detectar los dispositivos o el tráfico anormal.

12.7 – WLAN seguras

Encubrimiento SSID y filtrado de direcciones MAC

Para abordar las amenazas de mantener alejados a los intrusos inalámbricos y proteger los datos, se utilizaron dos características de seguridad tempranas que aún están disponibles en la mayoría de los enrutadores y puntos de acceso:

Encubrimiento SSID

- Los AP y algunos enrutadores inalámbricos permiten deshabilitar la trama de baliza SSID, (Beacon frame SSID). Los clientes inalámbricos deben configurarse manualmente con el SSID para conectarse a la red.

Filtrado de Direcciones MAC

- Un administrador puede permitir o denegar manualmente el acceso inalámbrico de los clientes en función de su dirección física de hardware MAC. En la figura, el router está configurado para permitir dos direcciones MAC. Los dispositivos con diferentes direcciones MAC no podrán unirse a la WLAN de 2.4GHz.

802.11 Métodos de Autenticación Originales

La mejor manera de proteger una red inalámbrica es utilizar sistemas de autenticación y cifrado. Se introdujeron dos tipos de autenticación con el estándar 802.11 original:

Autenticación abierta

- No se requiere contraseña. Normalmente se usa para proporcionar acceso gratuito a Internet en áreas públicas como cafeterías, aeropuertos y hoteles.
- El cliente es responsable de proporcionar seguridad, como a través de una VPN.

Autenticación de clave compartida

- Proporciona mecanismos, como WEP, WPA, WPA2 y WPA3 para autenticar y cifrar datos entre un cliente inalámbrico y AP. Sin embargo, la contraseña se debe compartir previamente entre las dos partes para que estas se conecten.

Métodos de autenticación de clave compartida

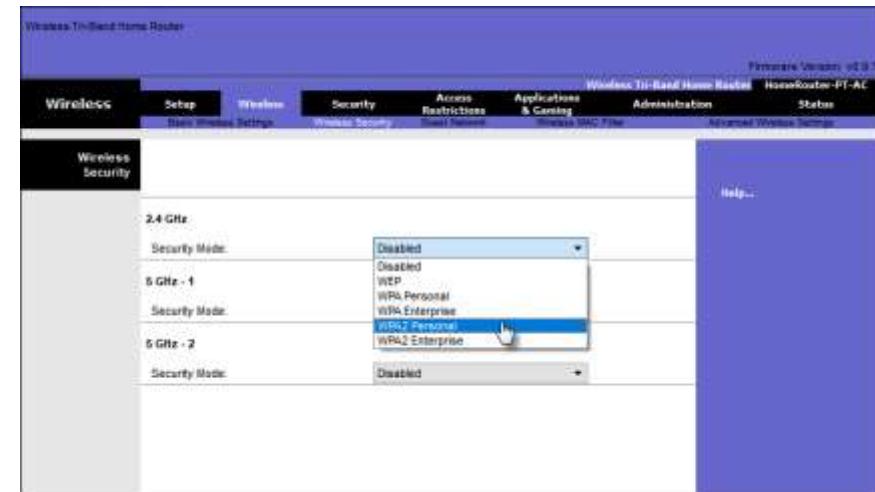
Actualmente hay cuatro técnicas de autenticación de clave compartida disponibles, como se muestra en la tabla.

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	Esta es la próxima generación de seguridad Wi-Fi. Todos los dispositivos habilitados para WPA3 utilizan los últimos métodos de seguridad, no permiten protocolos heredados obsoletos y requieren el uso de marcos de administración protegidos (PMF).

Autenticando a un Usuario Doméstico

Los routers domésticos suelen tener dos opciones de autenticación: WPA y WPA2. Con WPA2 tenemos dos métodos de autenticación.

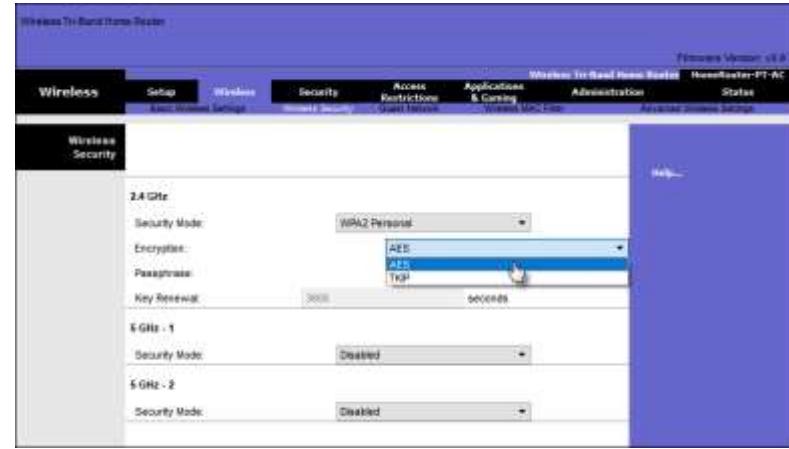
- **Personal** – Destinados a redes domésticas o de pequeñas oficinas, los usuarios se autentican utilizando una clave precompartida (PSK). Los clientes inalámbricos se autentican con el enrutador inalámbrico utilizando una contraseña previamente compartida. No se requiere ningún servidor de autenticación especial.
- **Empresa** – Destinado a redes empresariales. Requiere un servidor de autenticación de Servicio de usuario de acceso telefónico de autenticación remota (RADIUS). El servidor RADIUS debe autenticar el dispositivo y, a continuación, se deben autenticar los usuarios mediante el estándar 802.1X, que usa el protocolo de autenticación extensible (EAP).



Métodos de encriptación

WPA y WPA2 incluyen dos protocolos de encriptación:

- **Protocolo de integridad de clave temporal (Temporal Key Integrity Protocol (TKIP))** – Utilizado por WPA y proporciona soporte para equipos WLAN heredados. Hace uso de WEP pero encripta la carga útil de Capa 2 usando TKIP.
- **Estándar de cifrado avanzado (Advanced Encryption Standard (AES))** – Utilizado por WPA2 y utiliza el modo de cifrado de contador con el protocolo de código de autenticación de mensajes de encadenamiento de bloque (CCMP) que permite a los hosts de destino reconocer si los bits cifrados y no cifrados han sido alterados.

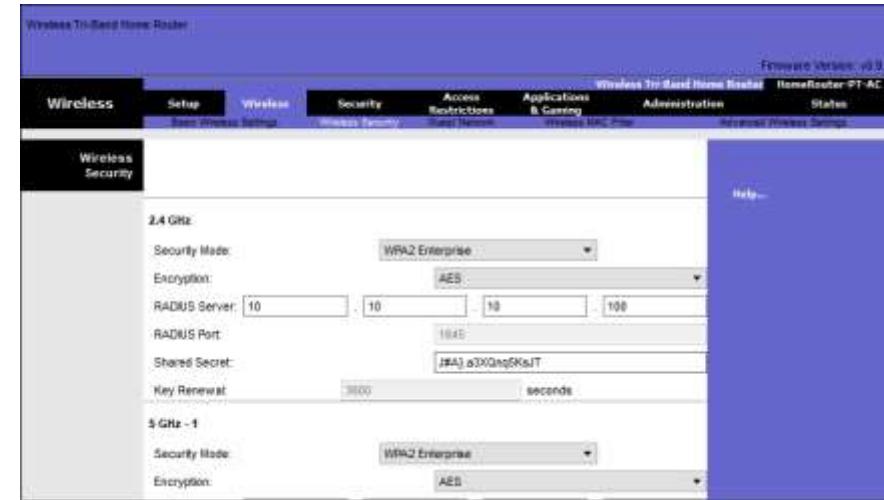


Autenticación en la empresa

La elección del modo de seguridad empresarial requiere un servidor RADIUS de autenticación, autorización y contabilidad (AAA).

Allí se requieren piezas de información:

- **Dirección IP del servidor RADIUS** – Dirección IP del servidor.
- **Números de puerto UDP**–Los puertos UDP 1812 para la autenticación RADIUS y 1813 para la contabilidad RADIUS, pero también pueden funcionar utilizando los puertos UDP 1645 y 1646.
- **Llave compartida** – Se utiliza para autenticar el AP con el servidor RADIUS.



Nota: La autenticación y autorización del usuario se maneja mediante el estándar 802.1X, que proporciona una autenticación centralizada basada en el servidor de los usuarios finales.

© 2016 Cisco y/o sus filiales. Todos los derechos reservados.
Información confidencial de Cisco.

WLAN seguras

WPA 3

Debido a que WPA2 ya no se considera seguro, se recomienda WPA3 cuando esté disponible. WPA3 incluye cuatro características:

- **WPA3 - Personal:** Frustra los ataques de fuerza bruta mediante el uso de la autenticación simultánea de iguales (Simultaneous Authentication of Equals, SAE).
- **WPA3 - Empresa:** Utiliza la autenticación 802.1X / EAP. Sin embargo, requiere el uso de una suite criptográfica de 192 bits y elimina la combinación de protocolos de seguridad para los estándares 802.11 anteriores.
- **Redes Abiertas:** No usa ninguna autenticación. Sin embargo, utiliza el cifrado inalámbrico oportunista (OWE) para cifrar todo el tráfico inalámbrico.
- **Incorporación de IoT :** Utiliza el Protocolo de aprovisionamiento de dispositivos (DPP) para incorporar rápidamente dispositivos IoT.

Gestión de Parches y Actualizaciones

Consiste en el proceso de mantener actualizados todos los programas, sistemas operativos y dispositivos con las últimas correcciones de seguridad y mejoras proporcionadas por los fabricantes. Esta práctica ayuda a mitigar vulnerabilidades conocidas y proteger los sistemas contra ataques cibernéticos.

Microsoft Windows Update

Microsoft proporciona actualizaciones periódicas para sus sistemas operativos Windows.

Los administradores de sistemas pueden configurar Windows Update para descargar e instalar automáticamente las últimas actualizaciones de seguridad y correcciones de errores.

Por ejemplo, una actualización de seguridad para cerrar una vulnerabilidad en el protocolo SMB (Server Message Block) que podría ser explotada por un ataque de ransomware.

Para Windows 10:

KB5034763 (versiones del SO 19044.4046 y 19045.4046): Esta actualización se lanzó el 13 de febrero de 2024 e incluye varias correcciones de seguridad y mejoras. Se conoce que esta actualización causa problemas en algunos usuarios, como la detención de la instalación sin razón aparente. Microsoft ha publicado soluciones tanto automáticas como manuales para este problema.

Para Windows 11:

KB5034765 (versiones del SO 22511.4115 y 22621.4115): Esta actualización también se lanzó el 13 de febrero de 2024 e incluye correcciones de seguridad y mejoras similares a la actualización de Windows 10. Al igual que la actualización de Windows 10, se ha informado que esta causa problemas en algunos usuarios, como fallos en la barra de tareas y en el Explorador de archivos. Microsoft está investigando estos problemas.

Actualizaciones de seguridad de Adobe Flash Player: Adobe Flash Player solía ser una herramienta comúnmente utilizada para contenido multimedia en la web. Sin embargo, también fue un objetivo frecuente para los ciberataques debido a sus numerosas vulnerabilidades de seguridad.

Adobe proporcionaba actualizaciones regulares para abordar estas vulnerabilidades y los administradores de sistemas tenían que asegurarse de instalar estas actualizaciones de forma oportuna para proteger los sistemas contra exploits.

Parches de seguridad de Linux: Los sistemas basados en Linux también requieren actualizaciones regulares para mantener la seguridad. Los administradores de sistemas deben estar al tanto de las actualizaciones de seguridad proporcionadas por los desarrolladores del kernel de Linux y otras aplicaciones de software de código abierto utilizadas en el entorno. Por ejemplo, un parche para corregir una vulnerabilidad en el protocolo de red TCP/IP que podría permitir a un atacante realizar ataques de denegación de servicio.

Al 22 de abril de 2024, las últimas actualizaciones críticas de seguridad para Debian son las siguientes:

Debian 11 ("Bullseye")

CVE-2023-5717: Una vulnerabilidad de escritura fuera de los límites del montón en el sistema de eventos de rendimiento del kernel de Linux, descubierta por Budimir Markovic. Esta vulnerabilidad podría permitir a un atacante local obtener privilegios de root. La actualización linux-lts-5.15.54-1 corrige esta vulnerabilidad.

CVE-2023-5178 y CVE-2023-6121: Fallos en el subsistema NVMe-oF/TCP, capaces de provocar una denegación de servicio, una escalada de privilegios o una fuga de información. Las actualizaciones nvme-of-tcp-2.3.2-1 y linux-lts-5.15.54-1 corren estas vulnerabilidades.

CVE-2021-44879: Una desviación del puntero NULL en la implementación del sistema de archivos F2FS. La actualización f2fs-tools-1.86-1 corrige esta vulnerabilidad.

Debian 12 ("Bookworm")

Las mismas vulnerabilidades que se encuentran en Debian 11 también afectan a Debian 12, y las actualizaciones correspondientes también están disponibles para esta versión.

**Página de seguridad de
Debian:** <https://www.debian.org/security/>

Actualizaciones de firmware de dispositivos de red: Los dispositivos de red, como routers, switches y firewalls, también requieren actualizaciones periódicas de firmware para corregir vulnerabilidades de seguridad y mejorar el rendimiento. Por ejemplo, una actualización de firmware para un firewall que parchea una vulnerabilidad de desbordamiento de búfer que podría permitir a un atacante eludir las reglas de filtrado de paquetes.

Seguridad de Sistemas Operativos

Nivel básico:

Actualizaciones del sistema: Instalar todas las actualizaciones de seguridad tan pronto como estén disponibles. Esto es fundamental para corregir vulnerabilidades conocidas y proteger tu servidor de ataques.

Fortalecimiento de contraseñas: Utilizar contraseñas seguras y únicas para todas las cuentas de usuario. Evitar contraseñas fáciles de adivinar o basadas en palabras del diccionario.

Firewall: Configurar un firewall para restringir el acceso al servidor solo a los servicios y puertos necesarios. Deshabilitar los servicios no utilizados y bloquear el acceso no autorizado.

Desactivación de inicio de sesión root: Evitar iniciar sesión directamente como root. Utilizar cuentas de usuario con privilegios limitados para las tareas diarias y solo elevar los privilegios cuando sea necesario.

Monitoreo del sistema: Implementar un sistema de monitoreo para detectar actividades inusuales o intentos de intrusión. Existen herramientas gratuitas como Fail2ban e intrusion detection systems (IDS) que pueden ayudarte en esto.

Nivel medio:

Criptografía: Cifrar los datos sensibles en reposo y en tránsito. Utilizar protocolos seguros como HTTPS para las comunicaciones web y SSH para el acceso remoto.

Segmentación de red: Segmentar la red para aislar los servidores críticos y limitar el impacto de un posible compromiso. Implementar VLANs o redes privadas virtuales (VPN) para una mayor seguridad.

Copias de seguridad: Realizar copias de seguridad regulares de los datos del servidor y almacenarlas en un lugar seguro fuera del sitio. Probar las copias de seguridad periódicamente para garantizar su correcta restauración.

Pruebas de penetración: Realizar pruebas de penetración regulares para identificar y corregir vulnerabilidades de seguridad en el servidor. Esto puede ayudarte a encontrar puntos débiles antes de que sean explotados por los atacantes.

Conciencia sobre seguridad: Educar a los usuarios sobre las mejores prácticas de seguridad y los riesgos potenciales. Implementar políticas de seguridad claras y procedimientos de respuesta a incidentes.

<https://www.debian.org/doc/manuals/securing-debian-manual/index.es.html>