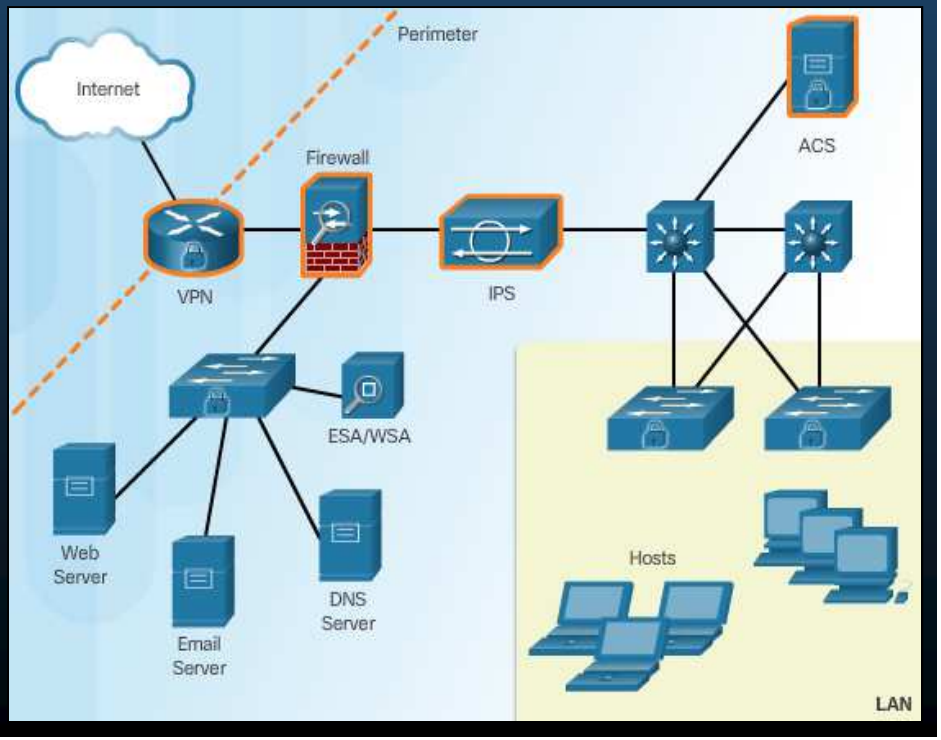
Capítulo 6

Aseguramiento de una Red de Área Local (LAN)

https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#6.1.1.1

6.1 Seguridad de Punto Final

- Aseguramiento de Elementos LAN.
  - Independientemente de las medidas de seguridad perimetrales.
    - Ataques pueden originarse desde el interior de la red.
    - Cualquier host interno infiltrado, puede servir de punto de ataque.
  - Dos principales elementos a asegurar:
    - Puntos Finales: Hosts susceptibles a ataques por malware.
    - Infraestructura de Red: Dispositivos de Interconexión (switches, Aps, IPPhones), susceptibles a ataques LAN (MAC Overflow, Spoofing, Storm, STP, DHCP)



6.1 Seguridad de Punto Final

- Seguridad Tradicional de Puntos Finales.
  - Tradicionalmente computadoras de la empresa dentro del perímetro.
    - Protegidas por un firewall e IPS.

Software instalado en cada host para proteger de virus y malware.

Software instalado en cada host para monitorear y reportar actividad de aplicaciones y configuraciones del sistema.

Software instalado en cada host que restringe las conexiones entrantes y salientes.

6.1 Seguridad de Punto Final

- La Red Sin Frontera.
  - Evolución hacia Puntos Finales Móviles y Ligeros.
  - Acceso a la red puede iniciarse de múltiples lugares y métodos de conexión.

  - Problemas para asegurar puntos finales.
    - Gran variedad de dispositivos.
    - Gran variedad de sistemas operativos.
    - Puntos finales dispares y, usualmente, no comparten información entre ellos.

6.1 Seguridad de Punto Final

- Aseguramiento de Puntos Finales en Redes Sin Frontera.
  - Protección antes, durante y después de un ataque.
    - ¿De donde provino?
    - ¿Cuál fue el método de amenaza y punto de entrada?
    - ¿Qué sistemas fueron afectados?
    - ¿Qué realizó la amenaza?
    - ¿Es posible detener la amenaza y su causa raíz?
    - ¿Cómo recuperarse?
    - ¿Cómo prevenir para que no suceda de nuevo?
  - Protección de Puntos Finales Implica:
    - Anti-Virus / Anti-Malware
    - Filtrado Anti-SPAM
    - Filtrado de URLs
    - Bloqueo de Sitios web en Listas Negras
    - Prevención de Pérdida de Datos (DLP - Data Loss Prevention)

6.1 Seguridad de Punto Final

- Soluciones de Seguridad para Puntos Finales Modernos.
  - Uso de Elementos de Escaneo de Red.
    - AMP – Anti Malware Protection (Protección Anti-Malware).
    - EMA – Email Security Appliance (Dispositivo de seguridad de correo electrónico).
    - WSA – Web Security Appliance (Dispositivo de seguridad web).
    - NAC – Network Admission Control (Control de Admisión de Red).

6.1 Seguridad de Punto Final

- Encriptación de Datos Locales por Hardware/Software.
  - Medidas contra Susceptibilidad a Robo de Datos.
    - Encriptación de Disco Duro >= AES 256bits.
    - OSX brinda opción de encriptación nativa a nivel S.O.
    - Soluciones para Windows:
      - BitLocker, TrueCrypt, Credant, VeraCrypt, etc.

6.1 Seguridad de Punto Final

- Protección contra Malware Avanzada (AMP).
  - Malware es la amenaza mas común a puntos finales.
    - 2013 Cisco compra SourceFire y lo torna un AMP.

      - Busca brindar visibilidad y control para defender contra malware.
        - Antes: Políticas ante violaciones de ciertos tipos de archivos y comunicaciones.
        - Durante: Analiza tráfico de red buscando amenazas que evadan las primeras líneas de defensa.
        - Después: Ayuda a entender, contener y remediar un ataque activo.

      - Utiliza:
        - Reputación de archivos: analiza archivos y bloquea o aplica políticas.
        - Caja de Arena de archivos: Analiza archivos desconocidos y su comportamiento.
        - Retrospección de archivos: Continua analizando archivos en busca de niveles de amenazas.

6.1 Seguridad de Punto Final

- AMP y Defensa contra Amenazas Administrada.
  - Uso de la nube de inteligencia en seguridad de redes (Cisco/Sourcefire).
    - Inteligencia de Seguridad Colectiva (Cisco / Talos).
  - Talos = Cisco Security Intelligence Operations (SIO)
    + SourceFire Vulnerability Research Team (VRT)
    - Detecta y correlaciona amenazas en tiempo real, utilizando red de amenazas.
      - Mas de 600 ingenieros alrededor del mundo trabajando 365 días al año.
      - Gran variedad de fuentes:
        - 1.6 millones de dispositivos de red (Firewalls, IPSs, Aparatos Web / e-mail)
        - 150 millones de puntos finales.
      - Gran cantidad de datos:
        - 100TB de inteligencia de seguridad diaria.
        - 13 billones de solicitudes web al día.
        - 35% del tráfico empresarial del mundo.

6.1 Seguridad de Punto Final

- AMP para Puntos Finales.
  - Existen varios tipos de AMPs:
    - Para Puntos Finales: Integrado en Cisco AMP para proteger puntos finales.
    - Para Redes: Integrado ASA dedicado y FirePower para proteger redes.
    - Para Seguridad de Contenidos: Integrado en Cisco Cloud Web Sec. Protege contra contenidos maliciosos en e-mail y web.
  - Para Puntos Finales.
    - Corre un agente FireAMP que se integra con Cisco AMP para Redes.
    - Brindar protección integral a través de redes extendidas.
    - Usa:
      - Análisis Continuos.
      - Seguridad Retrospectiva.
      - Indicaciones de compromiso de múltiples fuentes.
    - Permite correlacionar eventos de red, con puntos finales para una mejor administración y control.

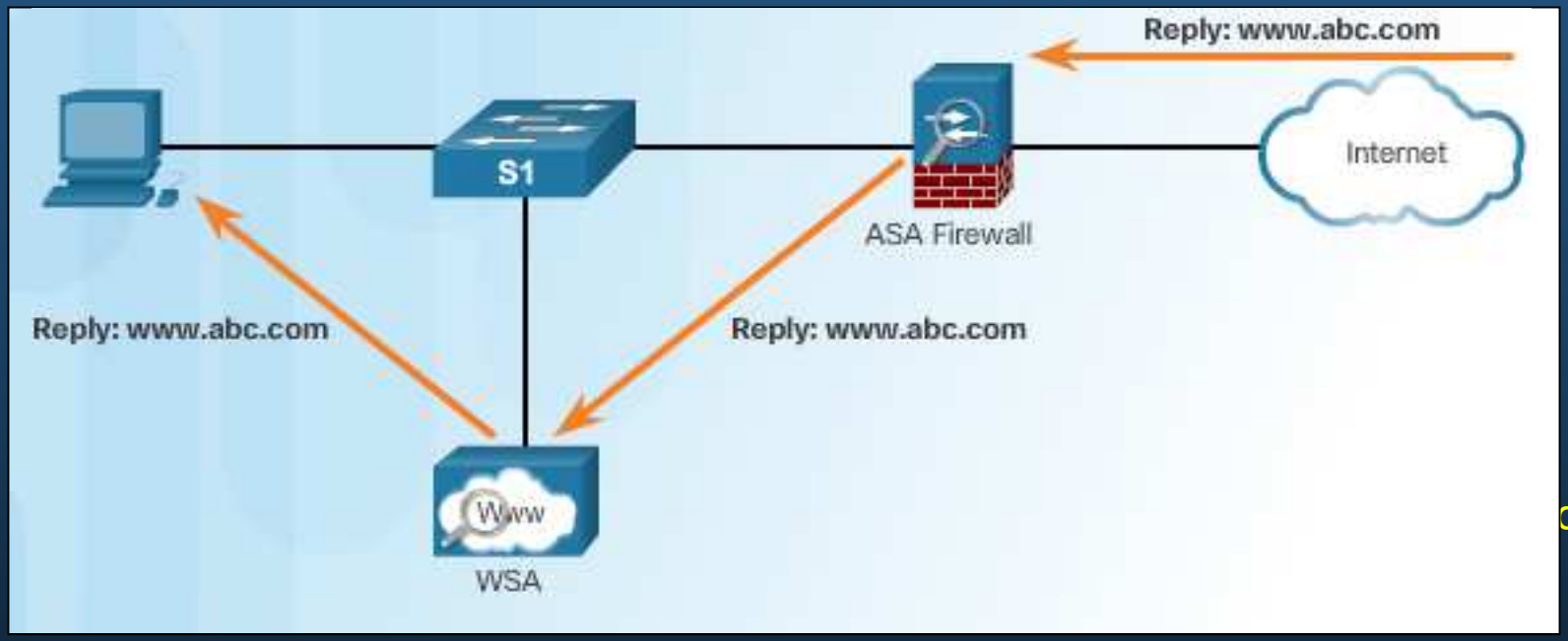
6.1 Seguridad de Punto Final

- Aseguramiento de e-mail y web.
  - El e-mail se ha vuelto la espina dorsal de las comunicaciones empresariales.
  - Más de 100 billones de correos se envían diariamente.
  - Importante asegurarlos.
    - SPAM en masa es la menor de las preocupaciones actuales.
    - Malware en SPAM es parte de una gran imagen de riesgos internos y externos.
  - En 2007 Cisco adquiere IronPort.
    - Ahora incluido en Cisco ESA y Cisco WSA.

6.1 Seguridad de Punto Final

- Dispositivo de seguridad de correo electrónico de Cisco (ESA).
  - Cisco ofrece ESA + Nube virtual y soluciones hibridas.
    - Protección de correo rápida, filtros anti-SPAM.
    - Nube flexible, para desarrollos físicos y virtuales.
    - Control de mensajes salientes + Prevención de pérdidas de datos + cifrado de correo electrónico.
    - Constantemente actualizadas desde Talos.
      - Analiza y retroalimenta cada 3 ó 4 min.
  - Beneficios:
    - Inteligencia global sobre amenazas.
    - Bloqueo de SPAM.
    - Protección contra Malware Avanzada.
    - Control de mensajes salientes + Prevención de pérdidas de datos + cifrado de correo electrónico.

6.1 Seguridad de Punto Final

- Dispositivo de seguridad web de Cisco (WSA).
  - 

  - do de
  - Características y Beneficios:
    - Inteligencia de Seguridad Talos.
    - Controles de Uso Web de Cisco.
    - Protección contra Malware Avanzada.
    - Prevención de Pérdida de Datos.

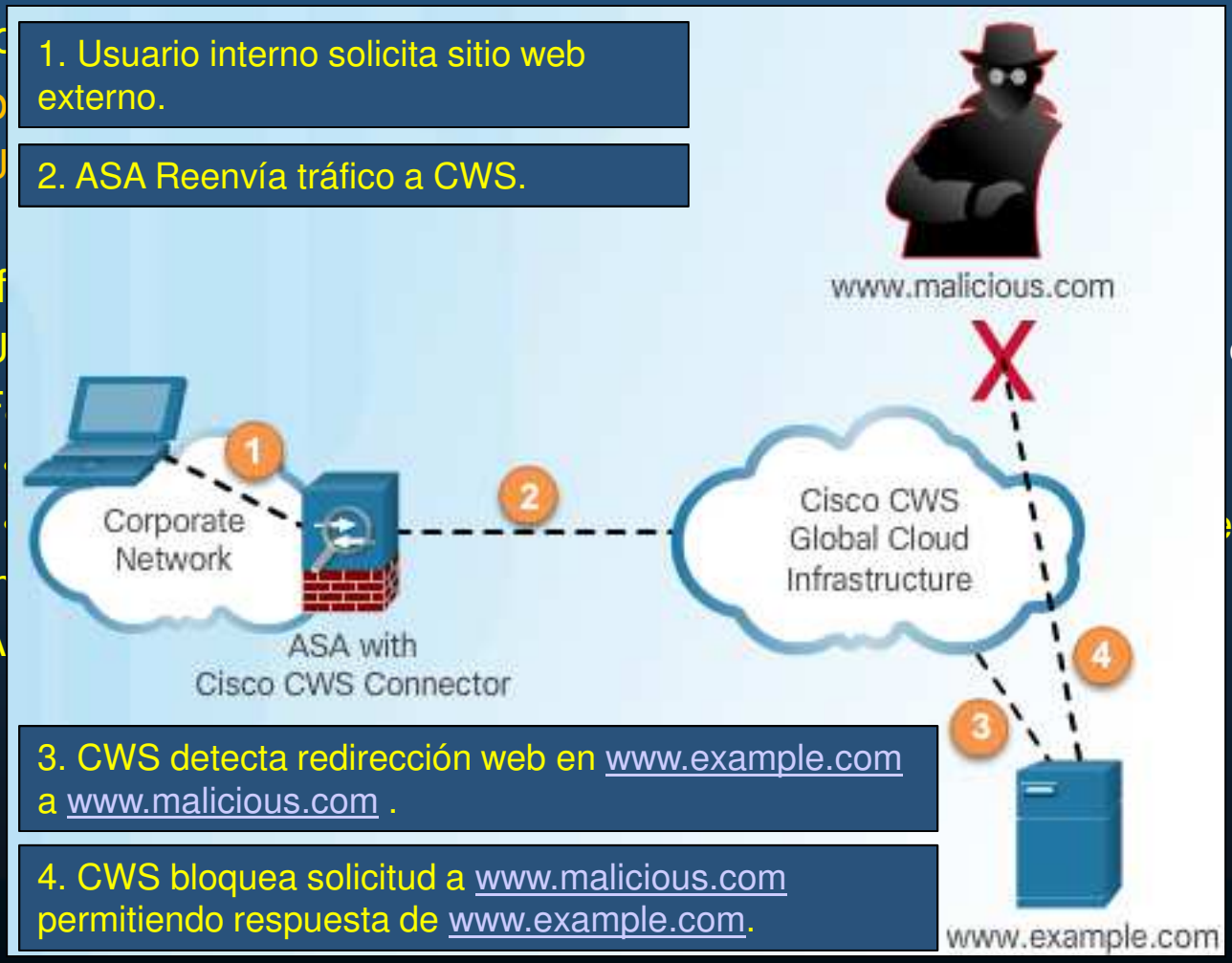
WSA Virtual: Versión de Software de un WSA, requiere hypervisor VMWare o KVM + Servidor de Sistema de cómputo unificado de Cisco.

6.1 Seguridad de Punto Final

- Seguridad Web en la Nube de Cisco (CWS).
  - Servic
  - Usa p
    - U
  - Benef
    - U
    - F
    - Ir
    - A

entorno.

ct.



6.1 Seguridad de Punto Final

- Control de Admisión de Red (NAC) de Cisco.
  - Permitir acceso a la red solo a dispositivos autorizados.
    - Autentica, Autoriza, Audita (AAA). Evalúa cumplimiento de políticas por dispositivo.

Marco de Trabajo NAC (Infraestructura existente + Software)	**Aplicación NAC Cisco** (Funciones NAC en Aparatos Cisco TrustSec)
Módulo de Software embebido en productos con NAC-habilitado.	Puede utilizarse en cualquier switch o router Cisco o no-Cisco.
Marco de trabajo integrado en múltiples productos Cisco y conscientes de NAC.	Solución natural para redes de tamaño medio que requieren una solución autocontenida.
Redes de alto desempeño, con diversos puntos finales, requiriendo soluciones LAN, WAN, Inalámbrico, Extranet, Acceso remoto; que se integren en la infraestructura existente.	Ideal para organizaciones que requieren rastreo de sistema operativo, antivirus, parches de seguridad y vulnerabilidades simplificado e integrado.

  - Permite reconocer usuarios, dispositivos, roles en la red.
  - Evalúa que los dispositivos cumplan con las políticas de seguridad.
  - Bloquea y aísla (remedia), dispositivos que no cumplan (solo autenticados, acceden).
  - Provee fácil acceso a invitados.
  - Simplifica acceso a dispositivos no autenticados.
  - Audita y reporta quién está en la red.

6.1 Seguridad de Punto Final

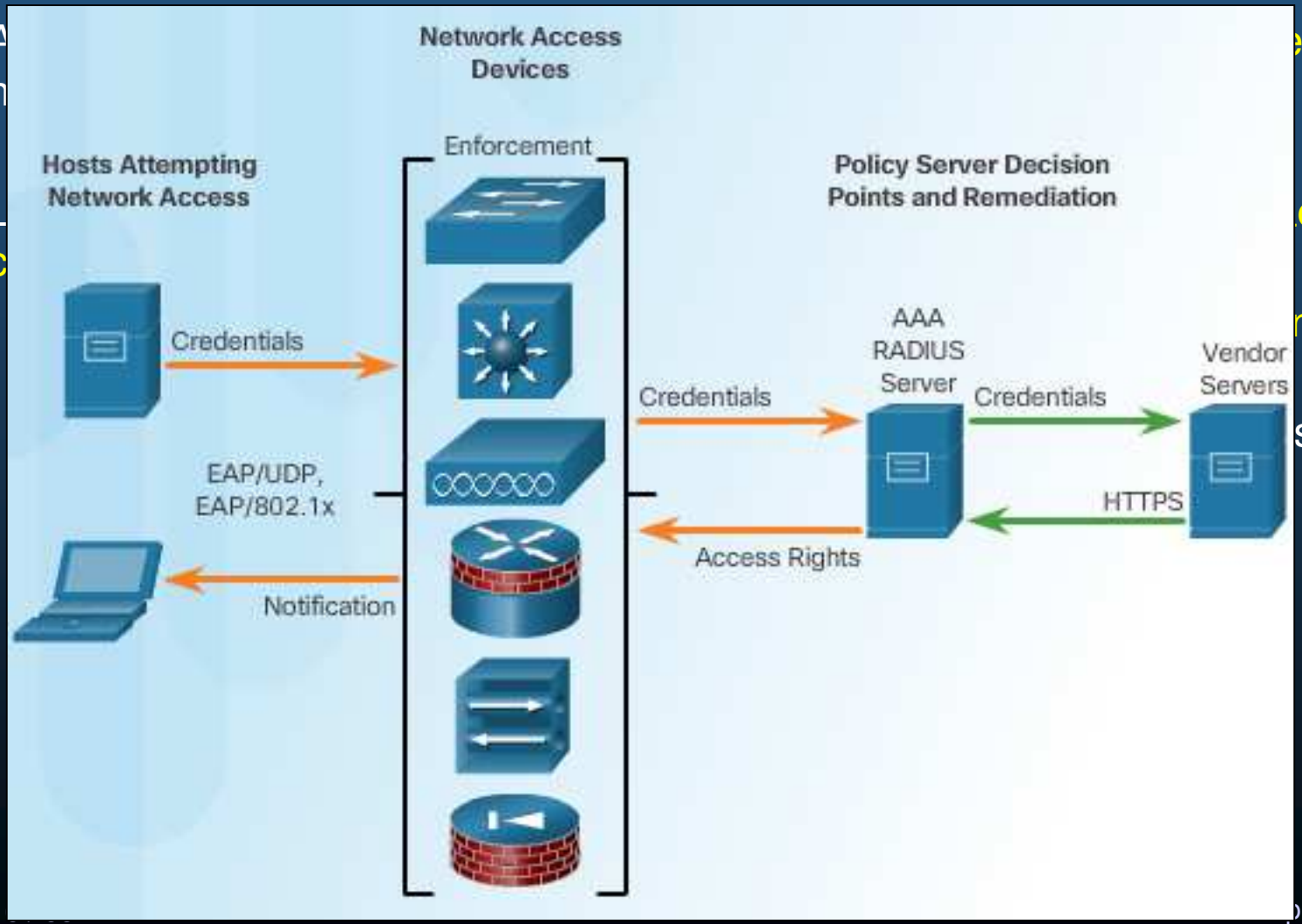
- Funciones de Cisco NAC.
  - A
  - L

eguridad

ción de

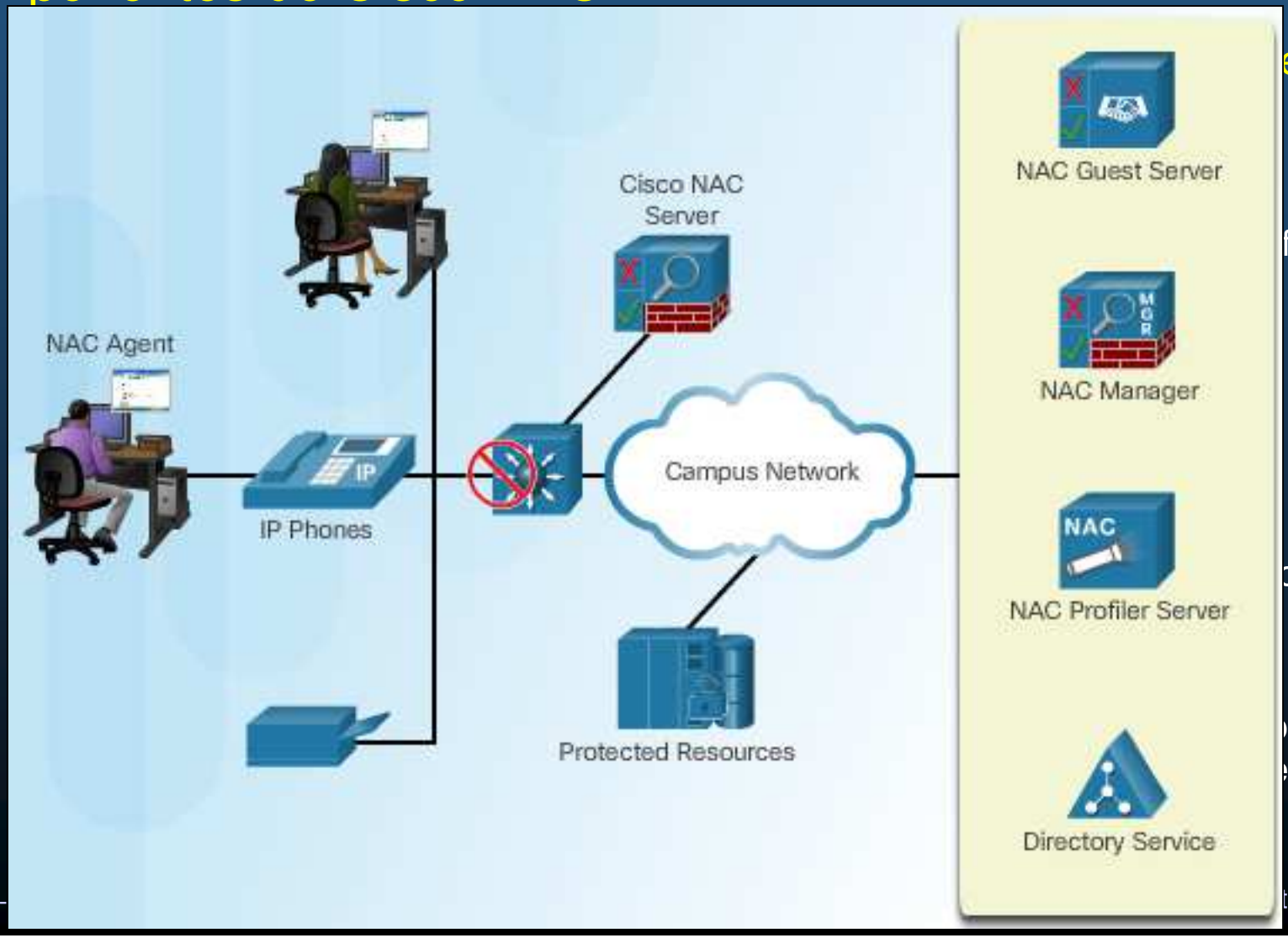
nticar y

servidor



6.1 Seguridad de Punto Final

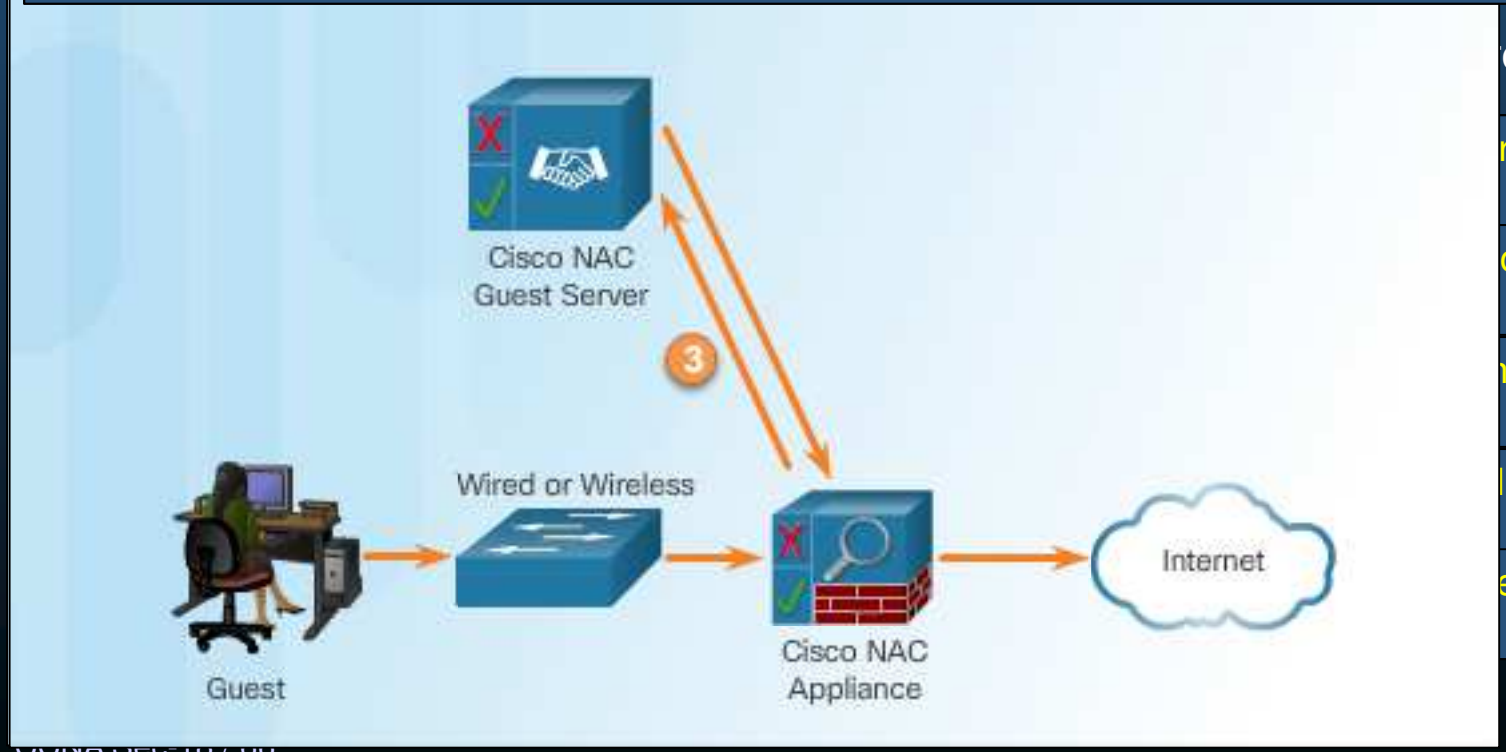
- Componentes de Cisco NAC
  - ec.
  - finales.
  - ortes de
  - locación
    es.



6.1 Seguridad de Punto Final

- Acceso a la Red para Invitados.
  - Un patrocinador en la empresa debe crear cuentas para invitados.

1. El invitado inicia tráfico web, interceptado por en Aparato NAC y le redirige a iniciar sesión.
2. El invitado inicia sesión con las credenciales recibidas del patrocinador. Y ahora puede navegar la web.
3. Se registra el acceso del invitado. Su sesión terminará cuando su tiempo expire.



en invitados.

rvidor de invitados:

con sus

ueva cuenta de

lles sobre cuenta

ee cuenta al

6.1 Seguridad de Punto Final

- Perfilador NAC de Cisco.
  - Habilita descubrimiento dinámico, identificación y monitoreo de puntos finales.
    - Administra dispositivos inteligentemente, basado en políticas.

1. La aplicación colector, recopila datos relevantes para enviar al servidor.

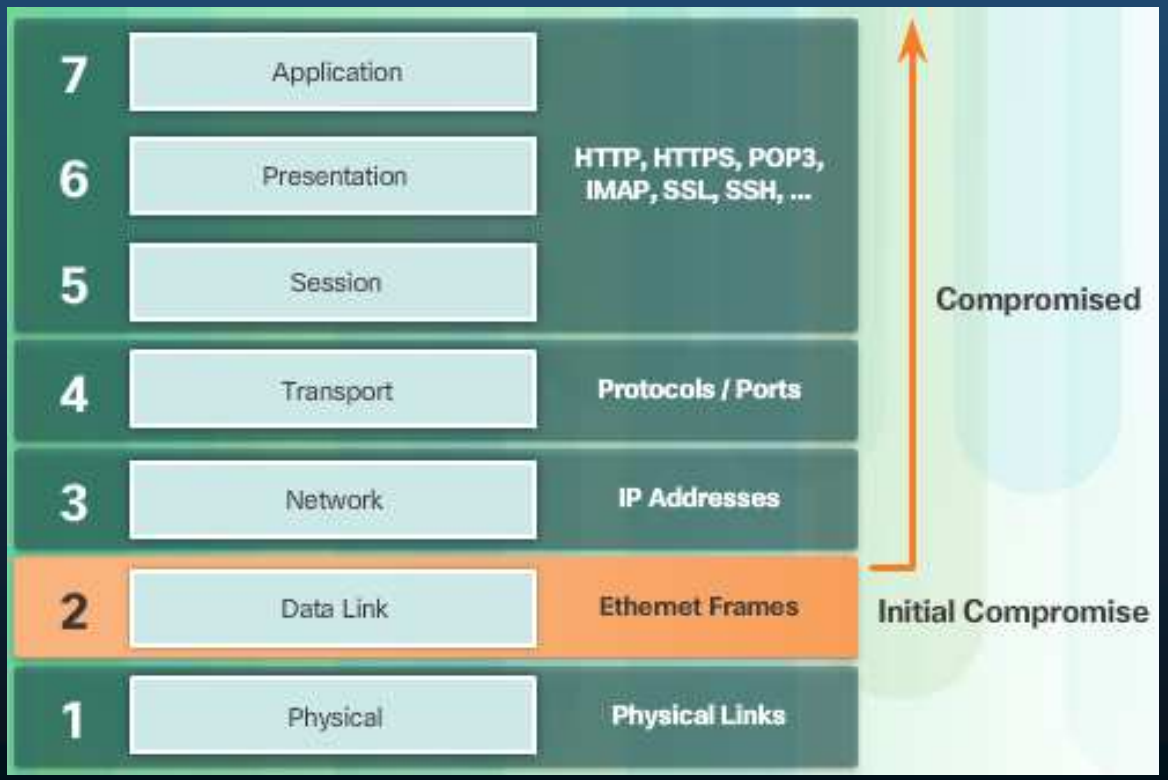
2. El servidor actualiza base de datos de puntos finales (teléfonos, impresoras, etc), con la información recibida del colector.

as en 802.1X
red.
vo.
ticables.

4. El colector monitorea continuamente el comportamiento de dispositivos y actualiza servidor.

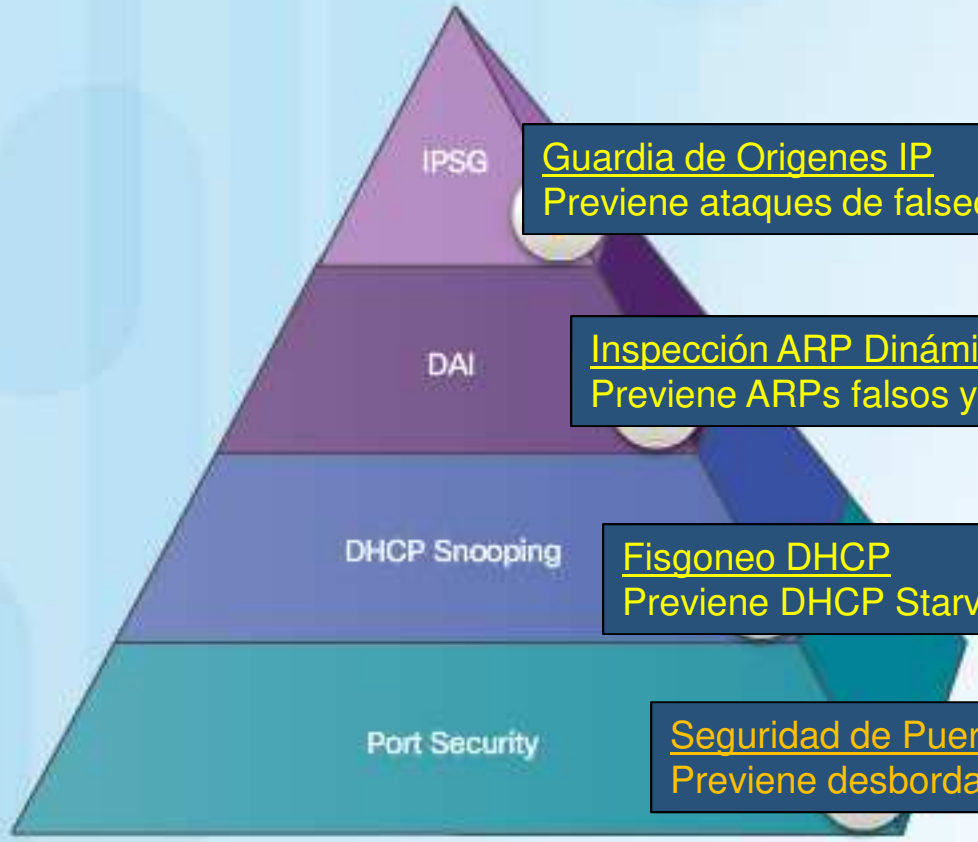
6.2 Consideraciones de Seguridad Capa 2

- Vulnerabilidades en Capa 2.
  - Si la capa 2 se ve comprometida, todas las capas superiores se verán afectadas.



6.2 Consideraciones de Seguridad Capa 2

- Soluciones para Mitigar Ataques en Capa 2.



Guardia de Origenes IP
Previene ataques de falseo de direcciones MAC / IP.

Inspección ARP Dinámica
Previene ARPs falsos y envenenamientos.

Fisgoneo DHCP
Previene DHCP Starvation, y mensajes DHCP falsos.

Seguridad de Puerto
Previene desbordamiento de tablas MAC y DHCP Starvation.

6.2 Consideraciones de Seguridad Capa 2

- Operación Básica de un Switch.
  - Basa sus decisiones de re-envío en la tabla de Memoria Direccionable de Contenido (CAM)
    - Asocia Direcciones MAC / VLAN / puerto físico del switch.
    - El switch busca una dirección destino de trama entrante para elegir el puerto de re-envío.
      - Si la MAC no se encuentra, inunda.
  - Ejemplo de contenido de tabla CAM.

```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

6.2 Consideraciones de Seguridad Capa 2

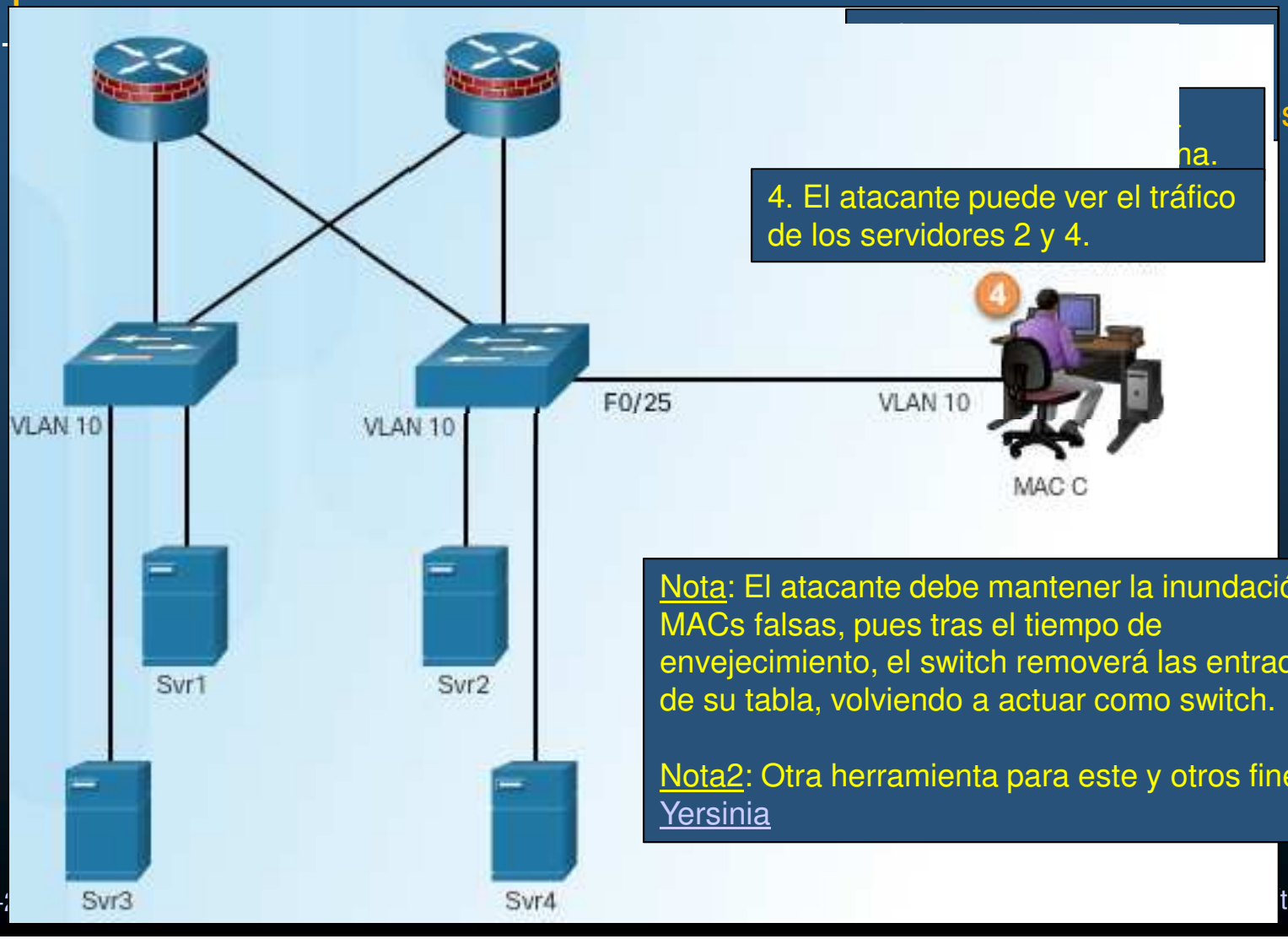
- Ejemplo de Operación de Tabla CAM.

Tras registrar tráfico de todos los puntos finales en la topología:

```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

6.2 Consideraciones de Seguridad Capa 2

- Ataque a Tabla CAM.
  -



s.

na.

4. El atacante puede ver el tráfico de los servidores 2 y 4.

Nota: El atacante debe mantener la inundación de MACs falsas, pues tras el tiempo de envejecimiento, el switch removerá las entradas de su tabla, volviendo a actuar como switch.

Nota2: Otra herramienta para este y otros fines es Yersinia

6.2 Consideraciones de Seguridad Capa 2

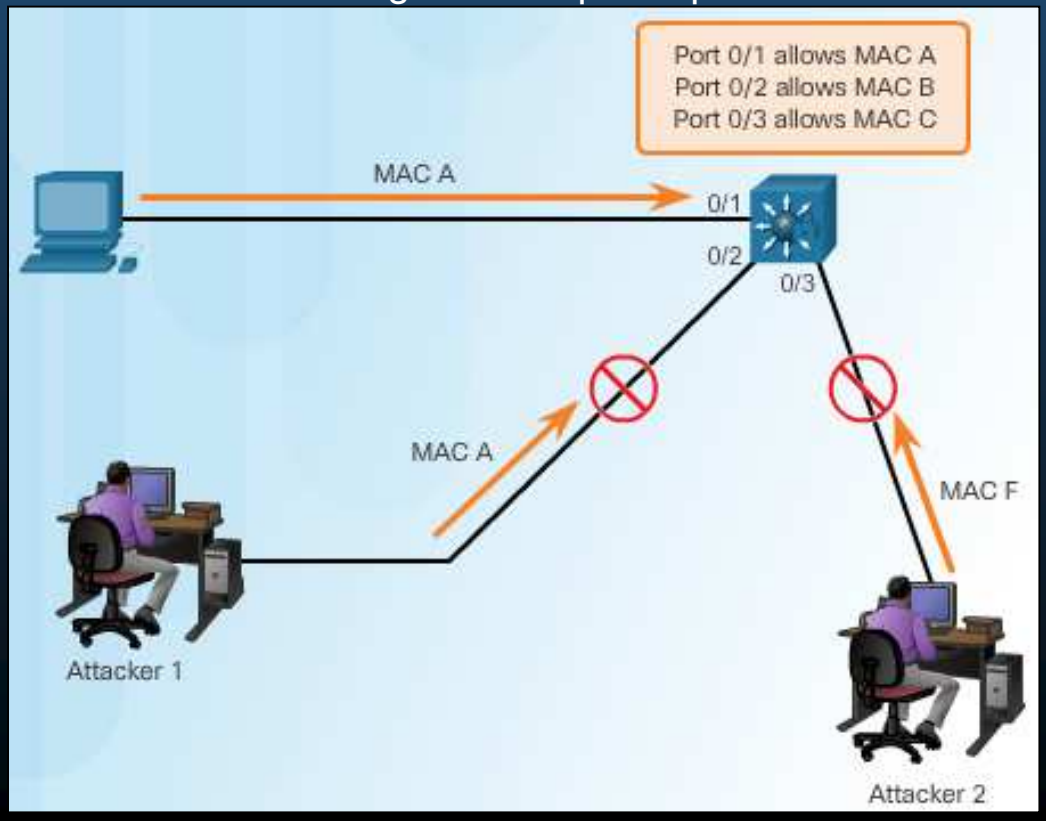
- Herramientas de Ataque a la Tabla CAM.
  - Un switch Catalyst 6500 puede almacenar hasta 132,000 direcciones.
  - macof puede inundar hasta 8,000 direcciones falsas por segundo.

```
# macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

  - Puede afectar a otros switches.
    - Cuando un switch hace broadcast, puede llegar a otros switches conectados a sus puertos.
  - Recomendado implementar seguridad de puerto.

6.2 Consideraciones de Seguridad Capa 2

- Medidas contra Ataques a la tabla CAM.
  - Habilitar seguridad de puerto.
    - Especificar MACs permitidas por puerto, cantidad y mecanismo de aprendizaje.
  - Cuando una MAC se asigna a un puerto seguro, el switch no reenvía marcos que lleguen con otras direcciones origen mas que la permitida.



6.2 Consideraciones de Seguridad Capa 2

- Seguridad de Puerto.
  - Se configura para puertos de acceso como `dynamic auto` por defecto:

```
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#
```

Establece como MAC permitida, la primera de la que escucha tráfico por ese puerto.

  - Verificación (valores por defecto)

```
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#
```

Otros parámetros de configuración disponibles.

```
S1(config)# interface f0/1
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
```

6.2 Consideraciones de Seguridad Capa 2

- Opciones para Habilitar Seguridad de Puerto.
  - Cantidad máxima de direcciones MAC permitidas por puerto.

```
Switch(config-if)
switchport port-security maximum value
```

`value = 1 -` (cantidad de MACs disponibles en la Administración de Base de datos de MACs) (`1` por defecto).

Ejemplos:

```
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#
S1# show port-security interface f0/1
Port Security
Port Status
Violation Mode
Aging Time
Aging Type
SecureStatic Address Agi
Maximum MAC Addresses
Total MAC Addresses
Configured MAC Addresses
Sticky MAC Addresses
Last Source Address:Vlan
Security Violation Count

S1#
```

```
S1# show port-security address
                Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    aaaa.bbbb.1234    SecureConfigured              F0/1          -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

`[ mac-address < sticky | lan | (acces | voice)] > ]`

No soportados en PacketTracer

6.2 Consideraciones de Seguridad Capa 2

- Violaciones de Seguridad de Puerto.
  - Llega trama con MAC origen diferente a la lista de MACs seguras.
  - Llega trama con MAC ya registrada en otro puerto, para la misma VLAN.

No disponible en PacketTracer

  - La configuración de violación determina el comportamiento del switch.

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

```
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#
```

	crementa ntador de olaciones	Apaga el puerto
		No
		No
		Si

, manualmente:

violation global

6.2 Consideraciones de Seguridad Capa 2

- Envejecimiento de la Seguridad de Puerto.

Parámetros subrallados,,
no disponible en PacketTracer

  - Permite establecer tiempo de vida de las MACs seguras.

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

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# exit
S1(config)# snmp-server enable traps port-security trap-rate 5
S1(config)# exit
S1#
S1# show port-security interface f0/1
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

S1#
```

    - **stati**
      - H
    - **time**
      - E
        0
    - **type**
      - T
        li
    - **type**
      - L

nte en el puerto.

vejecer una MAC,

e remueven de la

ificado inactivas.

6.2 Consideraciones de Seguridad Capa 2

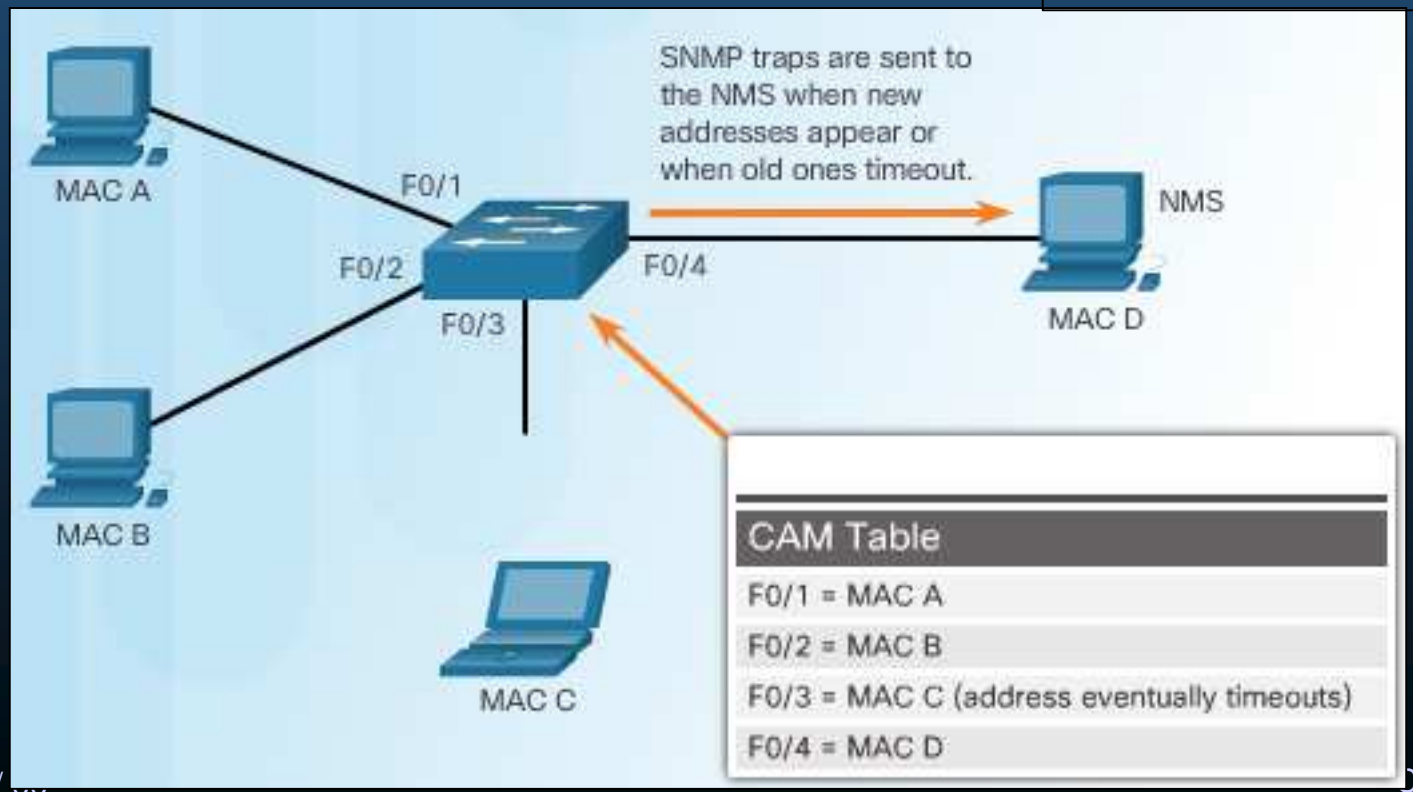
- Seguridad de Puerto con Teléfonos IP.
  - Un puerto de acceso que conecte un teléfono IP y una PC típicamente requiere dos MACs seguras, aunque algunos switches pueden requerir 3:
    - Teléfono IP en la VLAN de voz (No debe ser sticky)
    - Teléfono IP en la VLAN de acceso
    - PC en la VLAN de acceso
  - Ejemplo de configuración típica:

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# switchport port-security aging time 120
S1(config-if)#
```

6.2 Consideraciones de Seguridad Capa 2

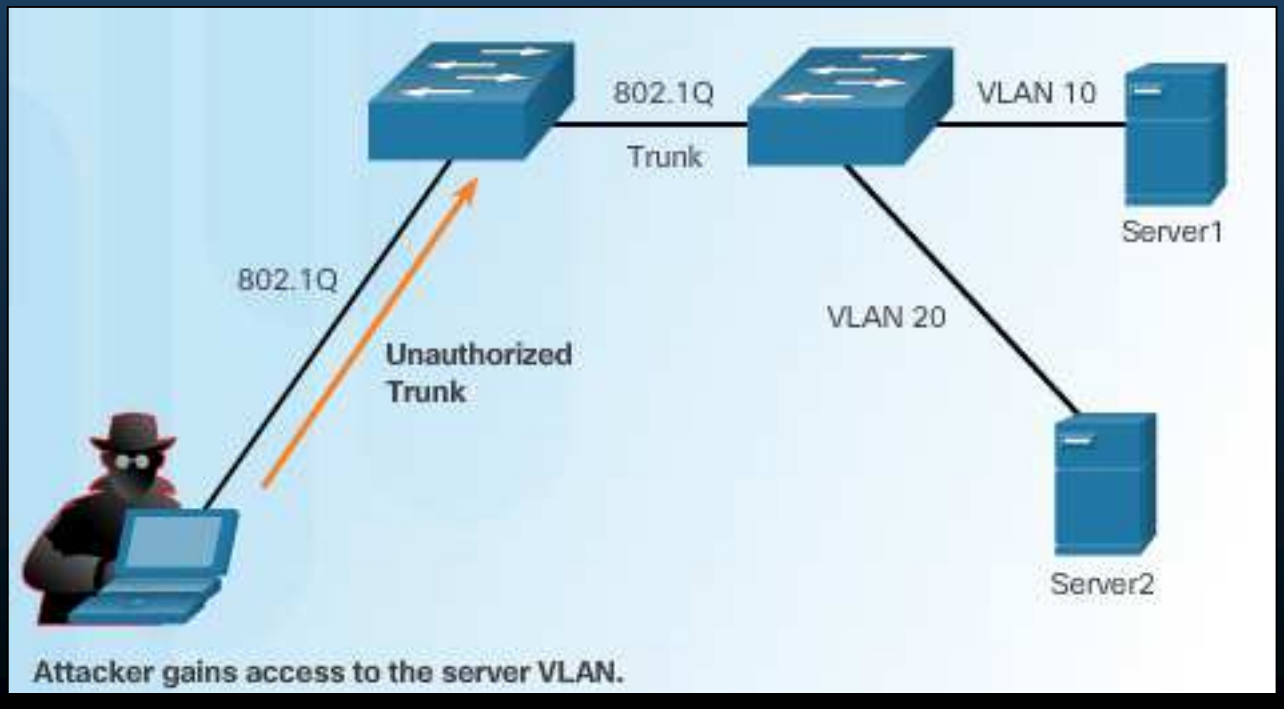
- Notificaciones SNMP de Direcciones MAC.
  - Pueden generarse notificaciones (traps) SNMP cuando se agreguen o eliminen entradas de la tabla de re-envío de un switch (dinámicas/seguras).
    - Permite monitrear MACs aprendidas / envejecidas.
      - `S(config)# mac address-table notification`

Parámetros subrallados,
No disponible en PacketTracer



6.2 Consideraciones de Seguridad Capa 2

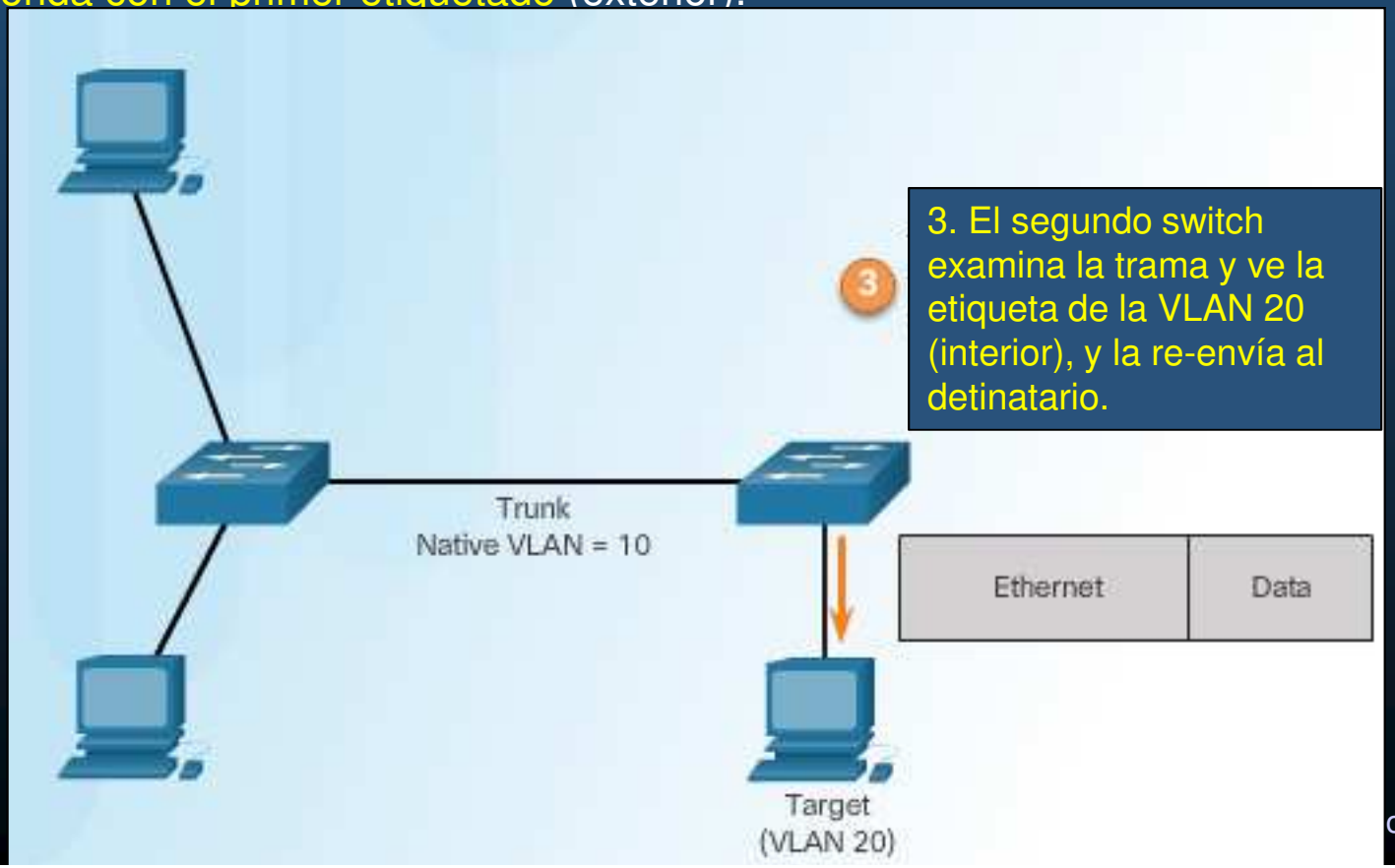
- Ataques VLAN Hopping.
  - Permite ver tráfico de una VLAN en otra.
    - Asume la característica de troncal automático por defecto en los switches.
    - El atacante configura un host para fingir ser un switch
      - Usa señalizaciones 802.1Q y de protocolo de enlace dinámico (DTP) para entablar un troncal (enviar y recibir tramas de y hacia cualquier VLAN).
    - El atacante introduce un switch de ataque, con el cual entablar el troncal.



Attacker gains access to the server VLAN.

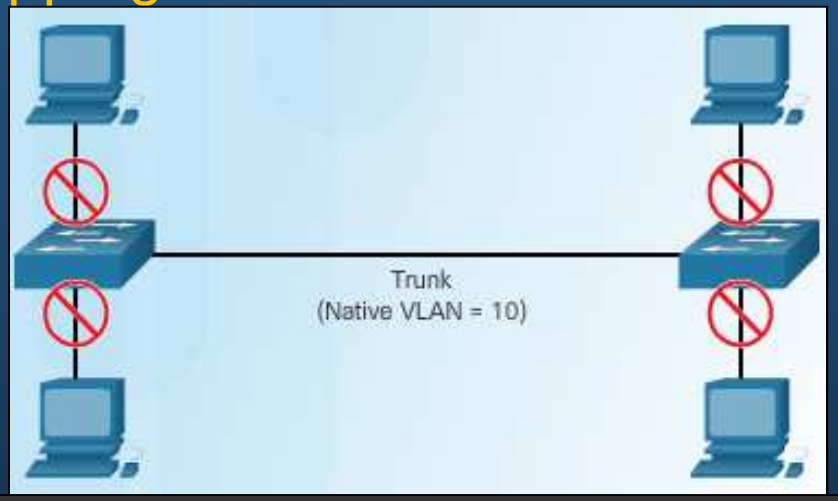
6.2 Consideraciones de Seguridad Capa 2

- Ataque de Doble Etiquetado (Encapsulación) de VLAN.
  - La mayoría de los switches asumen una sola encapsulación de etiquetas VLAN.
  - Un doble etiquetado puede permitir a una trama alcanzar la VLAN del segundo etiquetado (interior), siempre y cuando atraviese por un troncal y la VLAN nativa corresponda con el primer etiquetado (exterior).



6.2 Consideraciones de Seguridad Capa 2

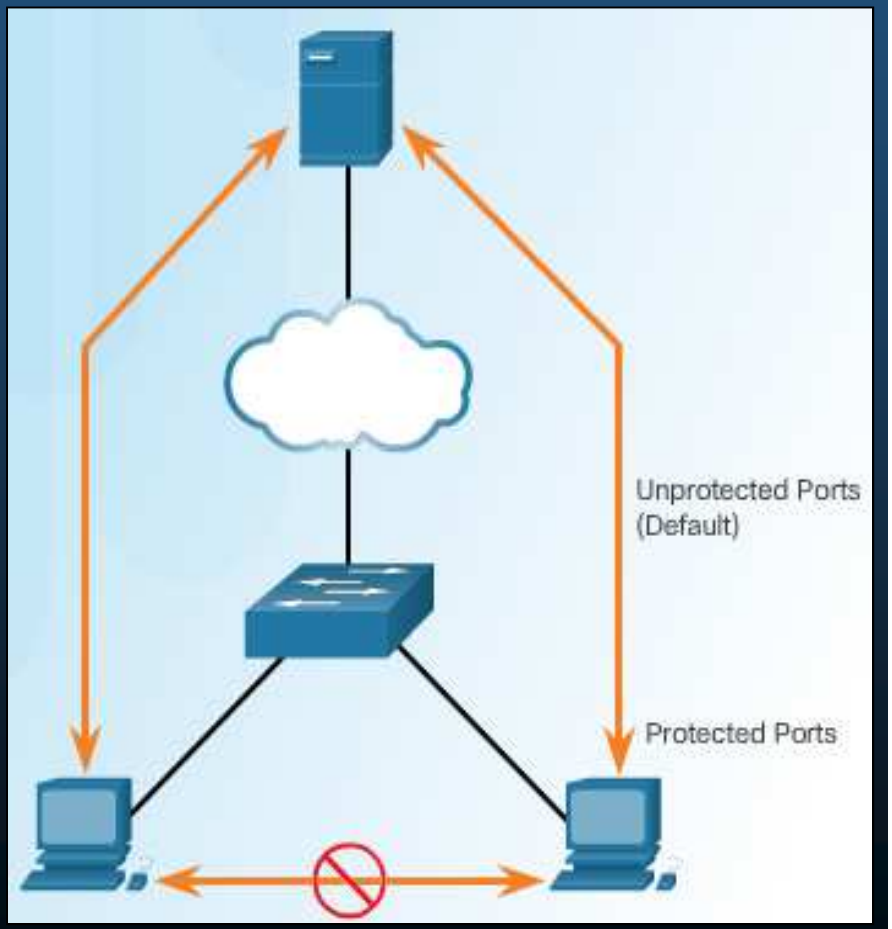
- Mitigación de Ataques VLAN Hopping.
  - Deshabilitar troncales en puertos de acceso (`switchport mode access`).
  - Deshabilitar troncales automáticos (DTP). (`switchport nonegotiate`).
  - Habilitar troncales manualmente. (`switchport mode trunk`).
  - Usar la VLAN nativa solo en los troncales y un valor no usual. (`switchport trunk native vlan` *vlan*).
  - Deshabilitar puertos no utilizados (`shutdown`).
  - Ejemplo:




```
S1(config)# interface range f0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range f0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range f0/21 - 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)# exit
S1(config)#
```

6.2 Consideraciones de Seguridad Capa 2

- Característica de Extremos con VLAN Privada (PVLAN).
  - Asegura que no hay intercambio de datos entre puertos de extremo (puertos protegidos).
  - Características de Puertos Protegidos:
    - No re-envían tráfico de datos a ningún otro puerto protegido.
    - Re-envío normal con puertos no protegidos.
    - Por defecto todos los puertos están como no protegidos.



6.2 Consideraciones de Seguridad Capa 2

- Extremo PVLAN.
  - `Switch(config-if)# switchport protected`
    - Puede configurarse en un puerto físico o EtherChannel.
  - Para verificar:

    `Switch# show interfaces interface-id [switchport]`
  - PVLAN solo tiene significado en el switch local.
  - No es posibile aislar puertos en diferentes switches.

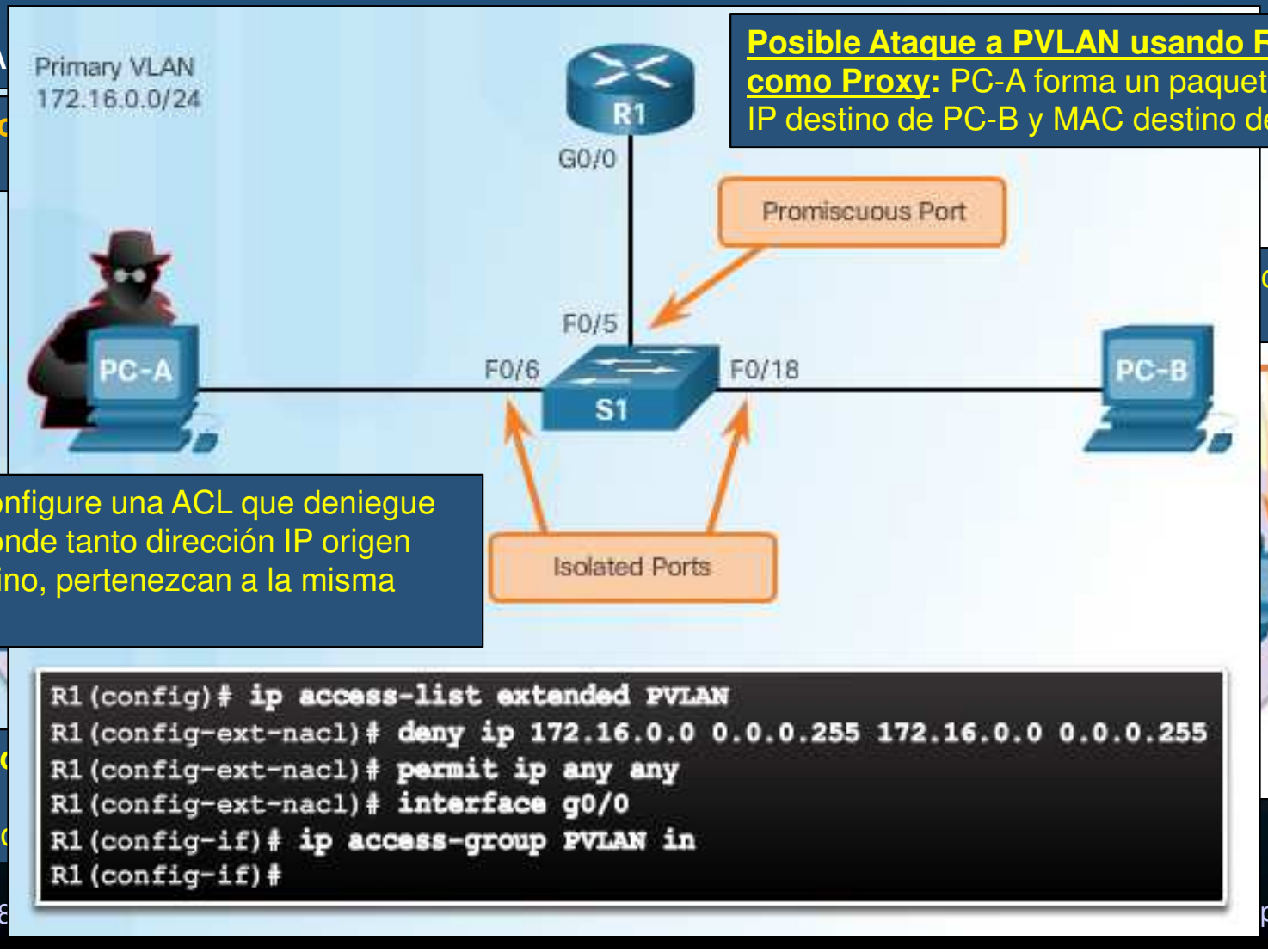
```
Switch# show interfaces gigabitethernet1/0/1 switchport
Name: G1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
<output omitted >
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
```

6.2 Consideraciones de Seguridad Capa 2

- VLANs Privadas.
  - A

Puerto Pr
con todos,

carse solo



Posible Ataque a PVLAN usando Router como Proxy: PC-A forma un paquete con IP destino de PC-B y MAC destino de R1

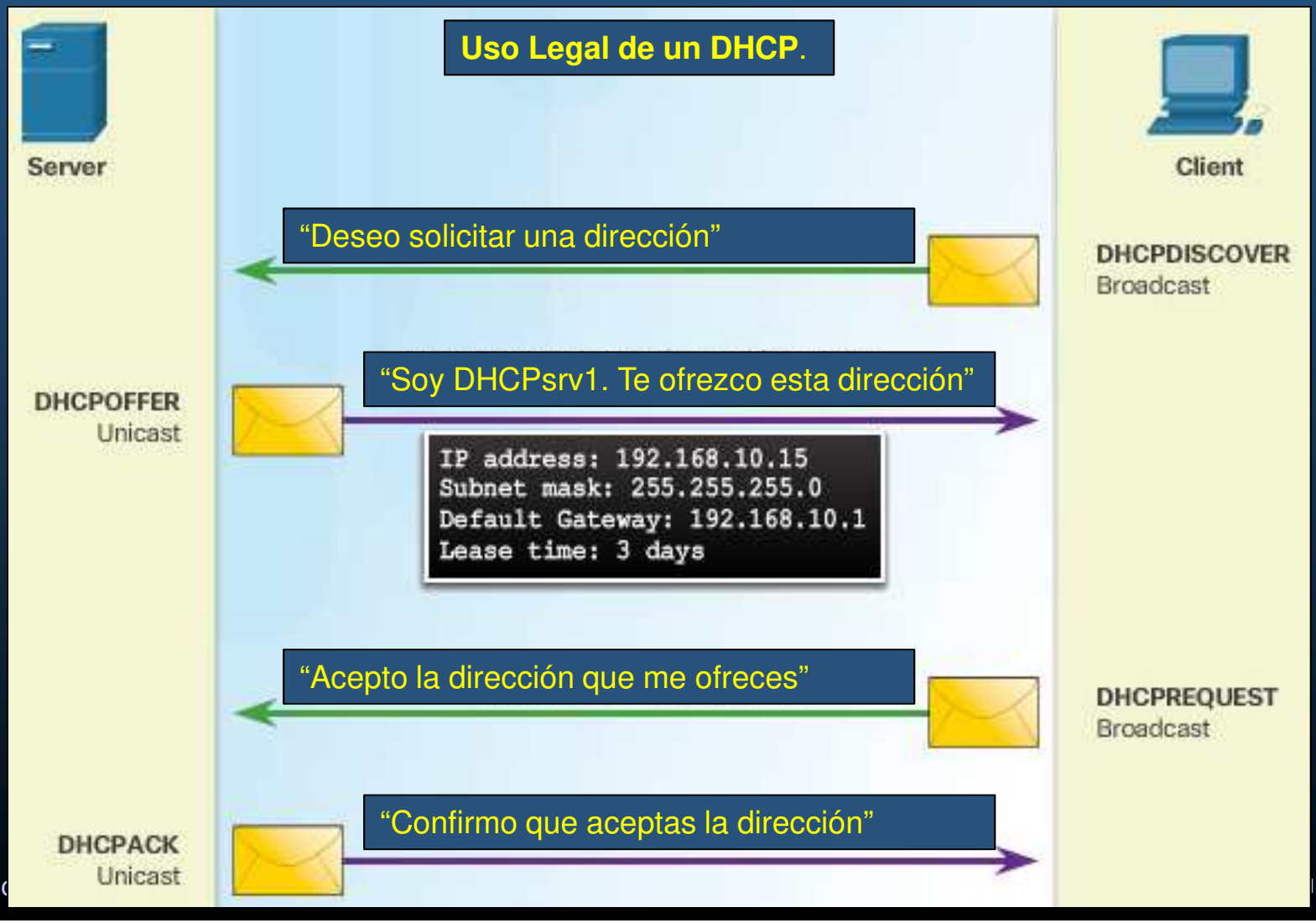
Mitigar: Configure una ACL que deniegue el tráfico donde tanto dirección IP origen como destino, pertenezcan a la misma subred.

```
R1(config)# ip access-list extended PVLAN
R1(config-ext-nacl)# deny ip 172.16.0.0 0.0.0.255 172.16.0.0 0.0.0.255
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)# interface g0/0
R1(config-if)# ip access-group PVLAN in
R1(config-if)#
```

Puerto C
con otros
Promiscuo

6.2 Consideraciones de Seguridad Capa 2

- Ataque DHCP Spoofing (falso).

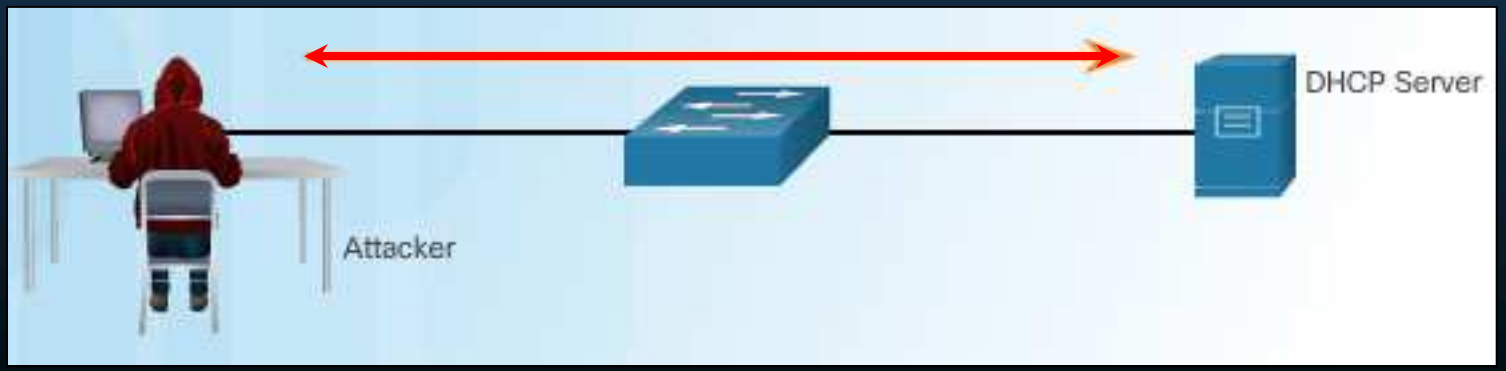


6.2 Consideraciones de Seguridad Capa 2

- Ataque DHCP Spoofing (falso).
  - Servidor DHCP Ilegítimo proporciona parámetros de configuración falsos.
    - Puerta de enlace predeterminada errónea (inexistente o proxy ilegítimo).
    - DNSs erróneos (incorrectos / inexistentes / webs ilegítimas).
    - Dirección IP errónea (inválida → DoS).
  - En una topología con 2 DHCPs (Legítimo/Ilegítimo)
    - Ambos reciben el DHCP Discovery del Cliente DHCP.
    - Ambos generan un DHCP Offer.
    - El cliente difundirá en un DHCP Request, que acepta la primer configuración que le llegue.
    - El Servidor DHCP cuya oferta haya llegado primero al cliente, enviará un acuse de recibo.
  - Un DHCP Ilegítimo colocado estratégicamente, puede llegar a ganar todas las Ofertas.

6.2 Consideraciones de Seguridad Capa 2

- DHCP Starvation (Hambruna).
  - Busca generar DoS, dejando incomunicados a los hosts de la red.
    - Atacante envía muchos DHCP Discoverys.
    - Servidor envía muchos (si no es que todos sus) DHCP Offers.
    - Atacante solicita aceptar todas las ofertas (DHCP Request).
    - Servidor registra todas las ofertas aceptadas (DHCP ACK)
  - Una herramienta para realizar estas acciones es Gobbler
    - Busca consumir la totalidad de las Ips disponibles en un DHCP.
    - Utiliza direcciones MAC falsas.

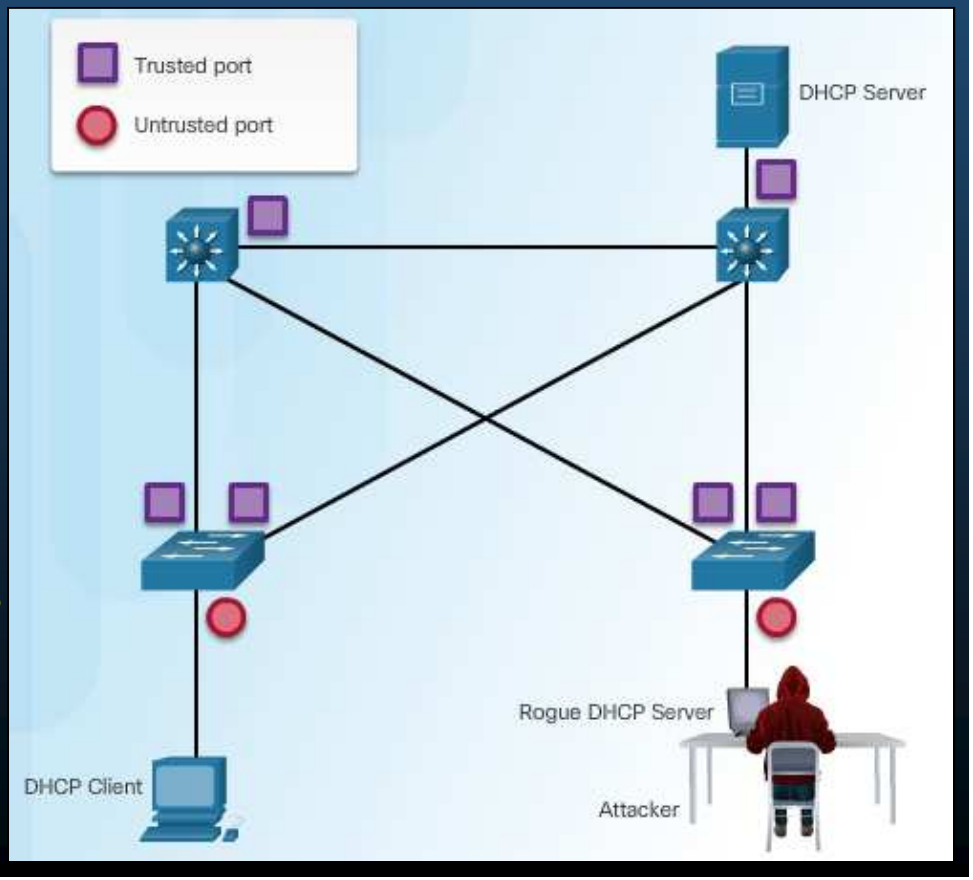


6.2 Consideraciones de Seguridad Capa 2

- Mitigación de Ataques DHCP.
  - DHCP Starvation → Seguridad de Puerto.
  - DHCP Spoofing → Mas complicado… Requiere DHCP SNooping
    - Si Gobbler utiliza diferentes MACs por una misma interfáz → Seguridad de Puerto.
    - Gobler puede utilizar misma MAC en trama, con diferente MAC en DHCP Request.
      - Seguridad de Puerto Inefectivo.
  - DHCP Snooping (Seguimiento de puertos confiables):
    - Permite limitar DHCP Discoverys por puerto.
    - Administra B.D. de asociaciones DHCP, para que el switch pueda filtrar tráfico DHCP.
      - MAC del cliente, Dir. IP, Tiempo de préstamo, tipo de asociación, Num. de VLAN, Interfáz.
    - Analiza tráfico DHCP y desecha si:
      - Identifica tráfico de DHCP no autorizado, en puerto no confiable.
      - Mensajes de clientes DHCP no-autorizados exceden límites, o no se adhieren a la BD de asociaciones.
      - Es paquete de retransmisión DHCP (opción 82) en un puerto no confiable.
      - MAC de la trama no coincide con MAC del DHCP Request.

6.2 Consideraciones de Seguridad Capa 2

- Configuración de DHCP Snooping.
  - Define 2 tipos de puertos.
    - Confiables: Puertos por los que se accede a un servidor DHCP Legítimo.
    - No confiables: Puertos para hosts donde no debería haber servidor DHCP.
  - Configuración:
    1. Habilitar DHCP Snooping.
       ```
       S(conf)# ip dhcp snooping
       ```
    2. Configurar puertos confiables.
       ```
       S(conf-if)# ip dhcp snooping trust
       ```
    3. Habilitar DHCP Snooping x VLAN.
    4. Limitar razón de DHCP Discoverys por segundo en puertos no confiables.
       ```
       S(conf-if)# ip dhcp snooping limit
                                  rate <1-2048>
       ```



6.2 Consideraciones de Seguridad Capa 2

- Ejemplo de Configuración de DHCP Snooping.

```
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:

<output omitted>
```

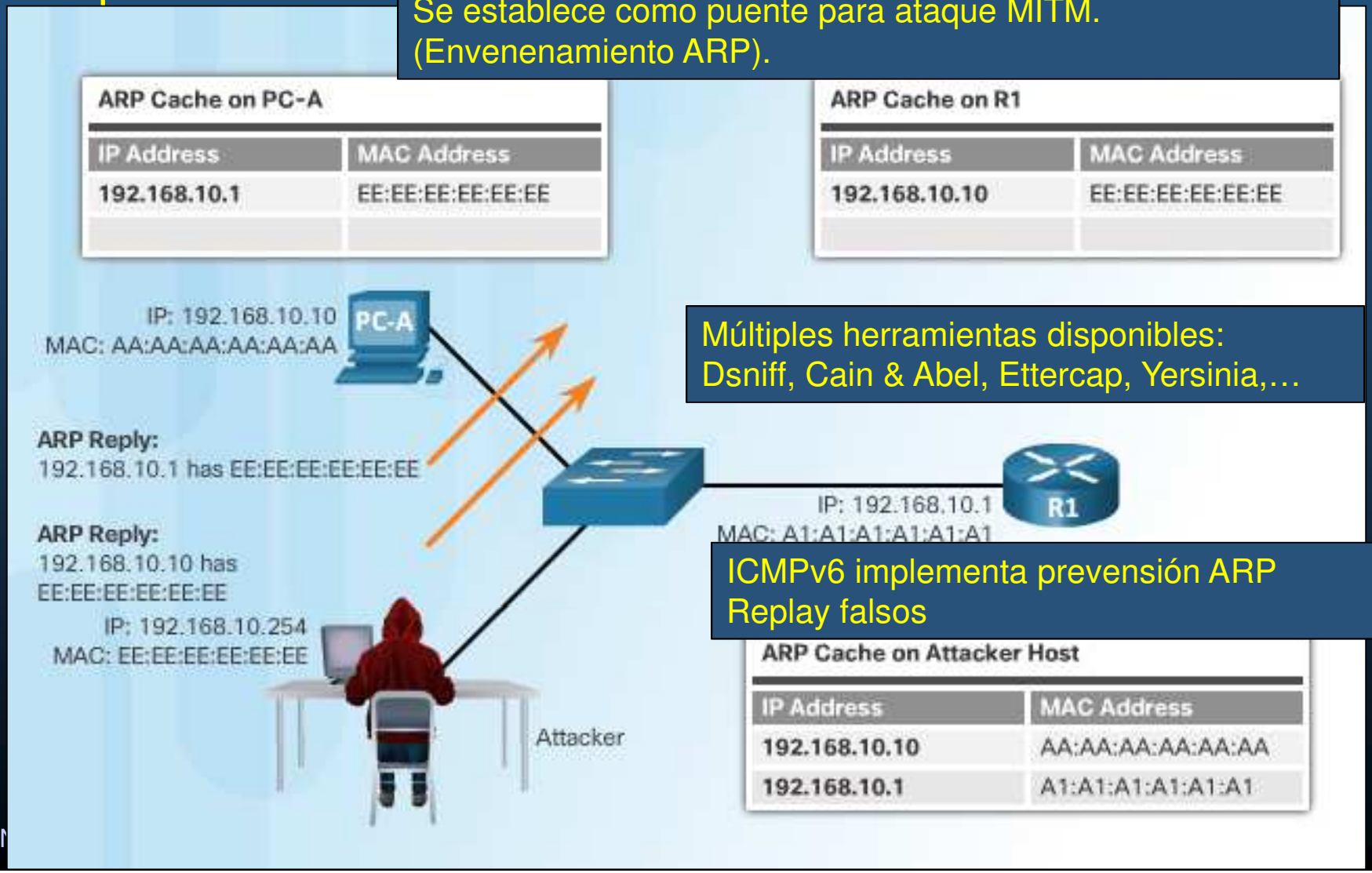
- litar opción 82.

```
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
```

6.2 Consideraciones de Seguridad Capa 2

- Ataques ARP.

Un atacante puede enviar ARP Reply Gratuitos y Falsos.
Se establece como puente para ataque MITM.
(Envenenamiento ARP).

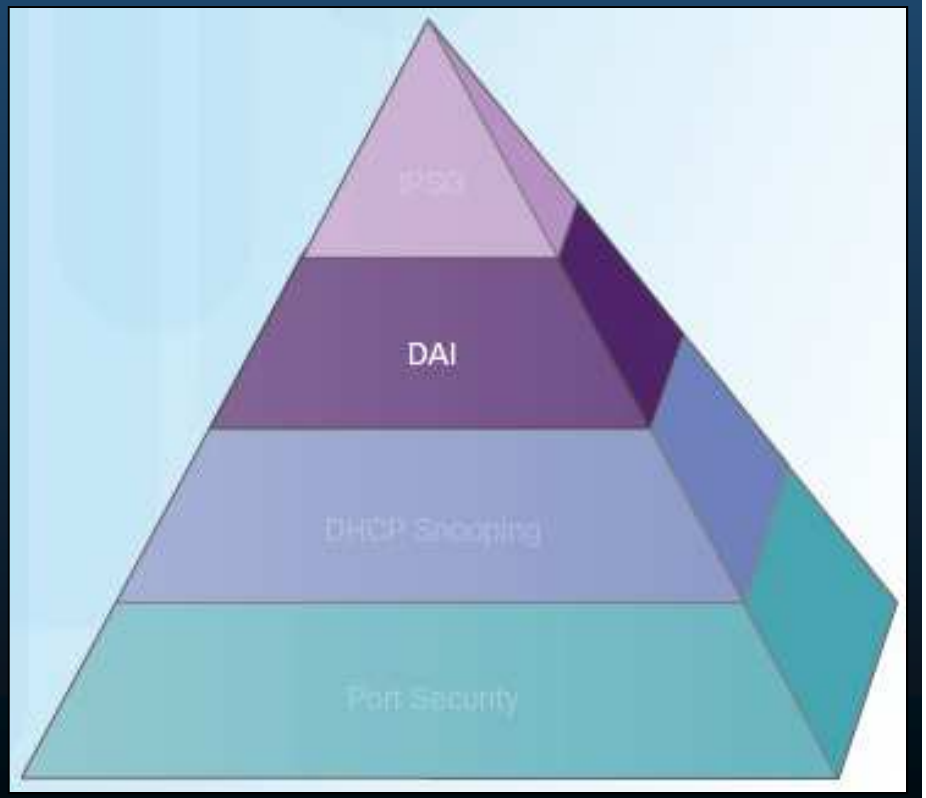


Múltiples herramientas disponibles:
Dsniff, Cain & Abel, Ettercap, Yersinia,…

ICMPv6 implementa prevensión ARP Replay falsos

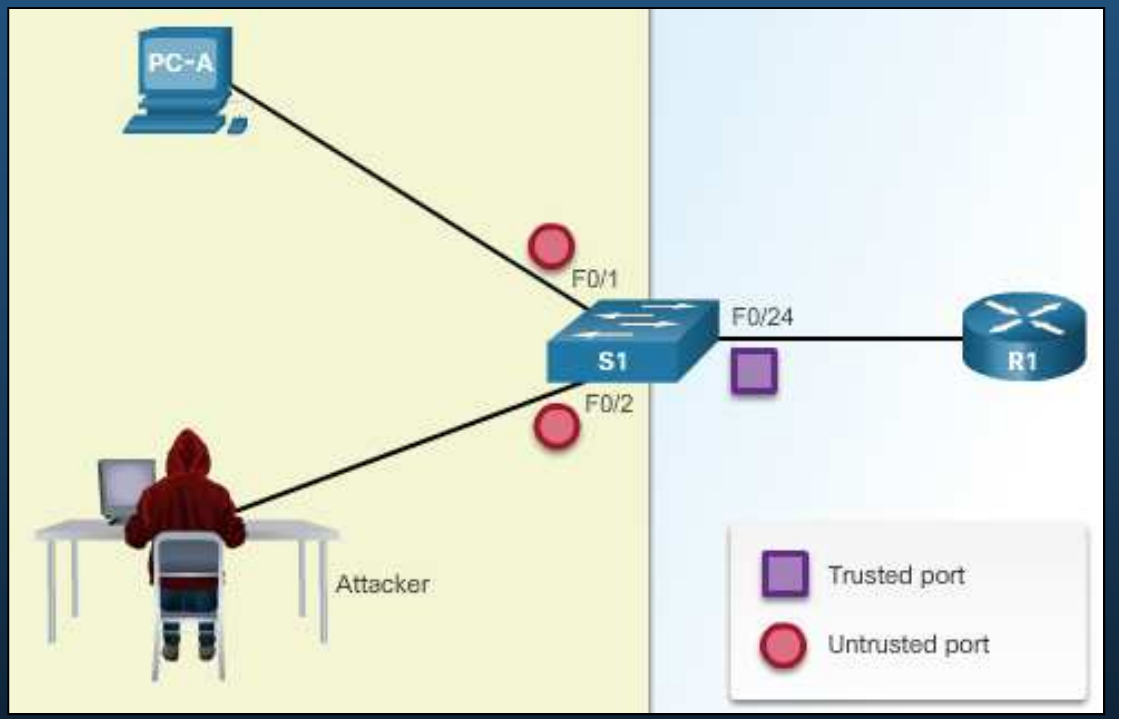
6.2 Consideraciones de Seguridad Capa 2

- Mitigación de Ataques ARP.
  - Inspección Dinámica de ARP (DAI)
    - El switch permite solo los ARP Replays que correspondan con un ARP Request, por VLAN.
    - Requiere DHCP Snooping.
      - Utiliza B.D. de asociaciones MAC-IP.
    - Valida ARPs contra ACLs ARP configuradas por el usuario.



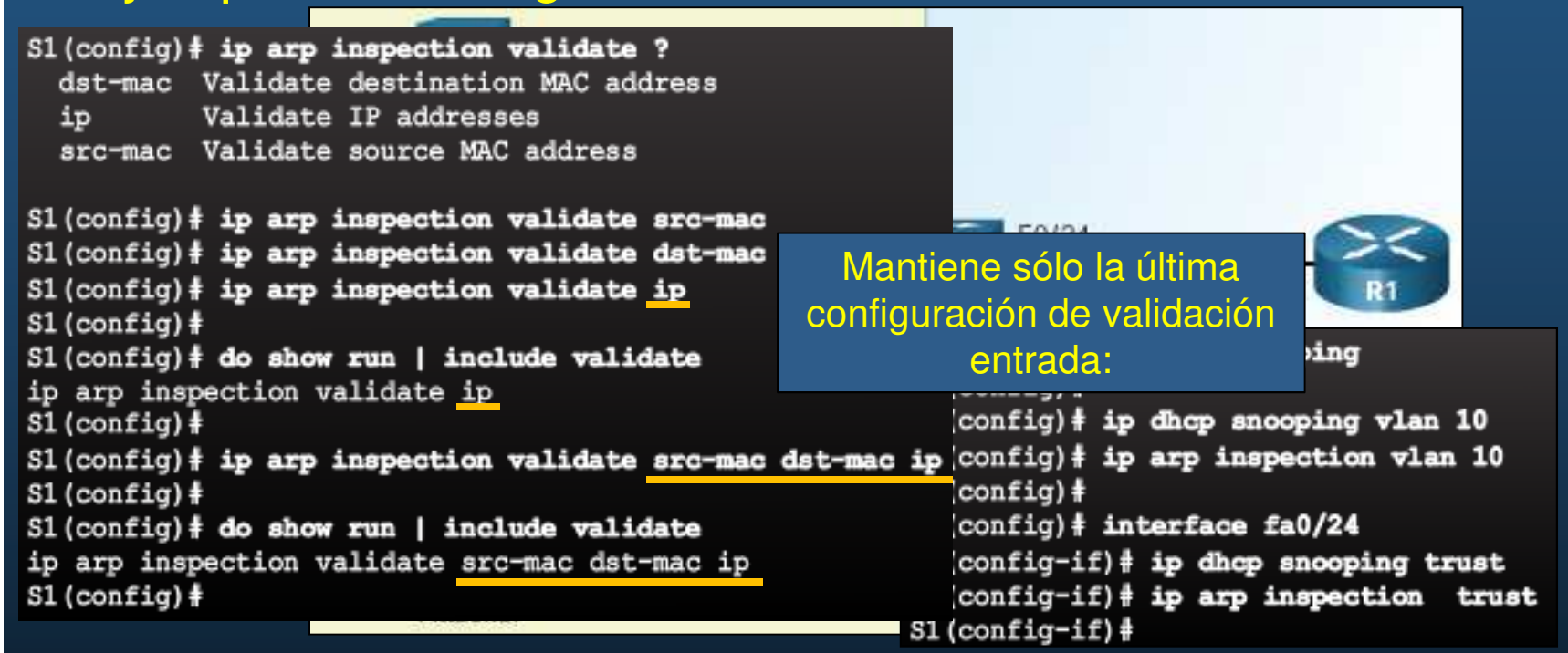
6.2 Consideraciones de Seguridad Capa 2

- Configuración de Inspección Dinámica de ARP.
  - Recomendaciones:
    - Implementar DHCP Snooping globalmente.
    - Habilitar DHCP Snooping por VLANs.
    - Habilitar DAI por VLANs.
    - Configurar interfaces confiables considerando tanto DHCP Snooping como Inspección ARP.
      - Puertos de acceso = No confiables
      - Puertos hacia otros dispositivos de red = Confiables



6.2 Consideraciones de Seguridad Capa 2

- Ejemplo de Configuración de DAI.



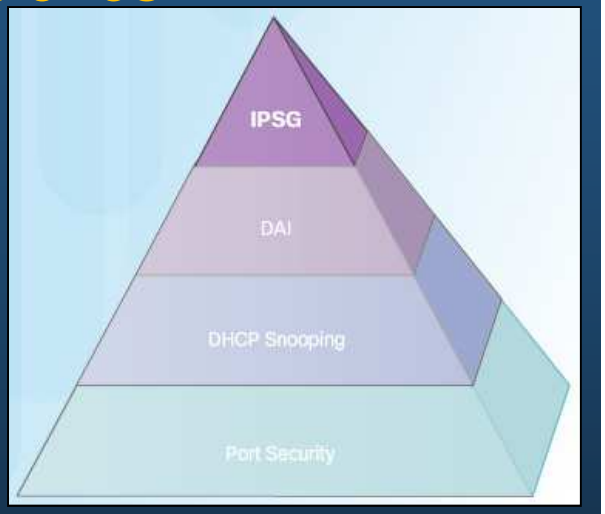
- Adicionalmente DAI puede verificar direcciones IP y MAC origen y destino.
- **S(conf)# ip arp inspection validate {[src-mac] [dst-mac] [ip]}**
  - `src-mac`: Verifica MAC origen en trama contra MAC origen en ARP.
  - `dst-mac`: Verifica MAC destino en trama contra MAC destino en ARP.
  - `ip`: Verifica IP en busca de errores o valores inesperados.

6.2 Consideraciones de Seguridad Capa 2

- Ataque de Suplantación de Direcciones.
  - Un atacante puede falsear tanto IPs como MACs.
  - Falseo de una MAC,
    - Un atacante enviar tramas a un switch con MAC origen de Equipo atacado.
    - El switch re-envía el tráfico destinado al host atacado al atacante.
    - El atacante debe mantener esa entrada en la tabla CAM.
      (tráfico legal (desde el host atacado) regresaría la CAM a su estado legal)
      - Envía tramas falseadas constantemente.
    - No hay mecanismo en Capa 2 para prevenirlo.
  - Falseo de una IP.
    - El atacante utiliza una ip de otro host o una ip aleatoria.
    - Difícil de mitigar.
      - Especialmente cuando se usa en la subred a la que pertenece.

6.2 Consideraciones de Seguridad Capa 2

- Mitigación de Ataques por Falseo de Direcciones.
  - Protector de origen IP (IP Source Guard - IPSG).
    - Desplegado sobre puertos de Acceso no confiables y enlaces troncales.
    - Requiere DAI.
    - Mantiene ACLs por puerto, por VLAN (PVACL)
      - basadas en asociaciones IP-MAC-puerto.

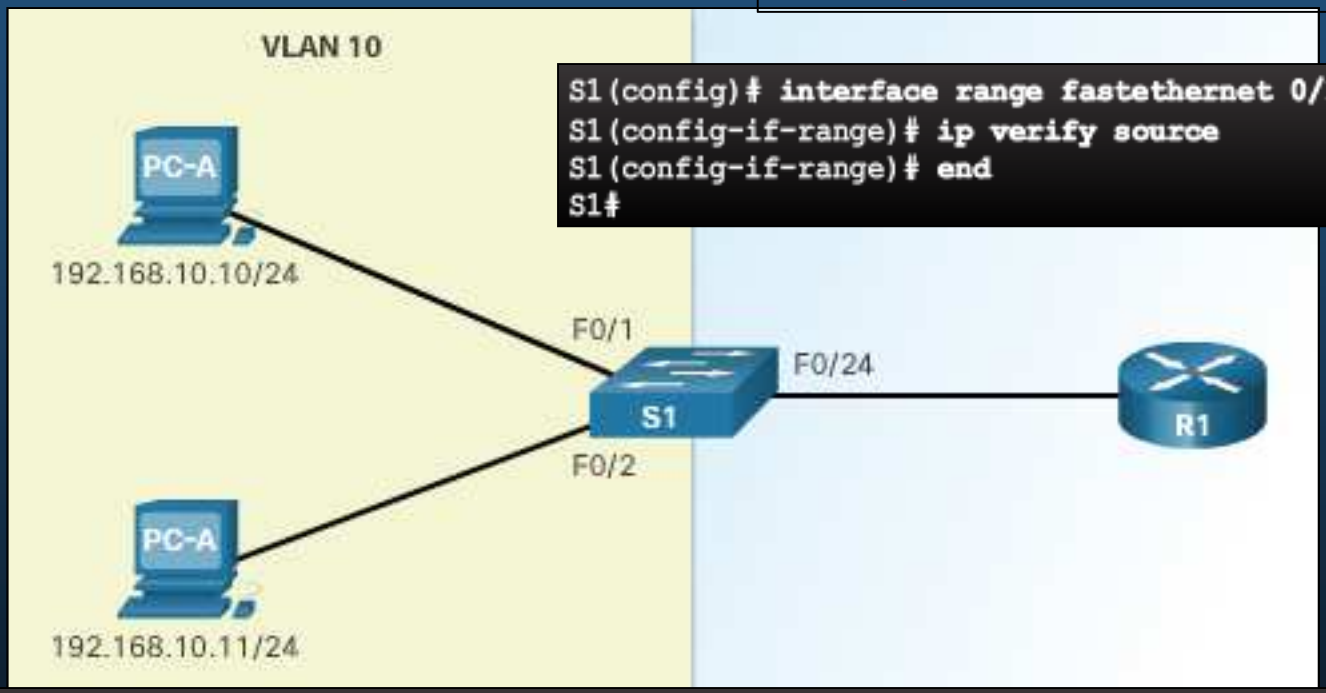


    - Inicialmente bloquea todo el tráfico excepto DHCPs.
    - Se instala PVACL cuando se detecta que un cliente recibe una IP del DHCP, o cuando se configura una asociación estática.
      - Restringe tráfico por ese puerto/VLAN solo a la IP asociada.
      - Un atacante tendría que utilizar forzosamente una IP registrada.
      - Dos posibles filtrados:
        - Dirección IP de origen.
        - Dirección IP y MAC de origen.

6.2 Consideraciones de Seguridad Capa 2

- Configuración de IP Source Guard.
  - **`Switch(conf-if)# ip verify source`**

Comandos subrallados,
No disponible en PacketTracer

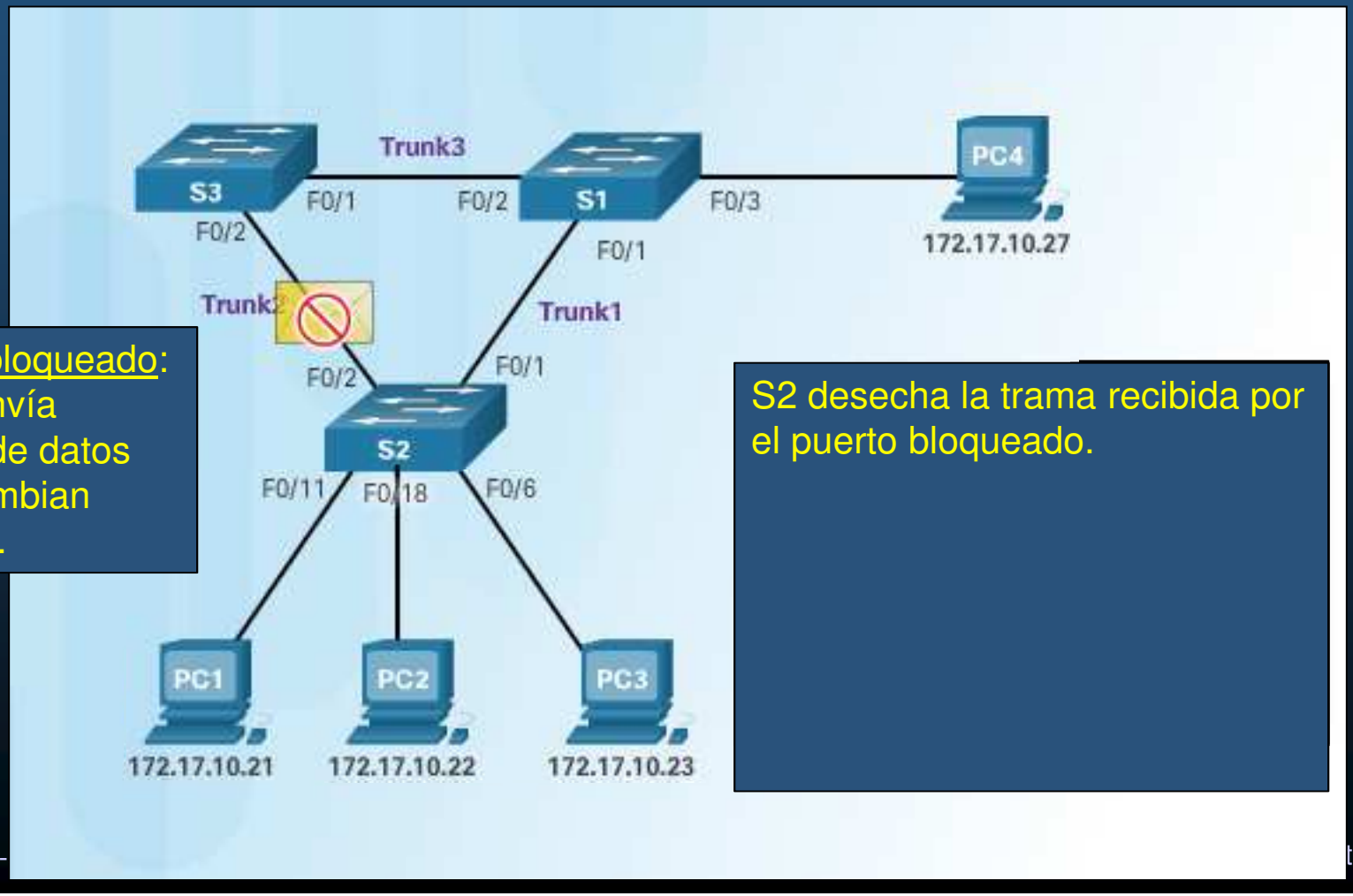



```
S1(config)# interface range fastethernet 0/1 - 2
S1(config-if-range)# ip verify source
S1(config-if-range)# end
S1#
```

```
S1# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
F0/1       ip           active       192.168.10.10                       10
F0/2       ip           active       192.168.10.11                       10
S1#
```

6.2 Consideraciones de Seguridad Capa 2

- Introducción al Protocolo de Árbol de Expansión (STP).
  - STP asegura (bloquea puertos) que enlaces físicos redundantes no generen bucles.

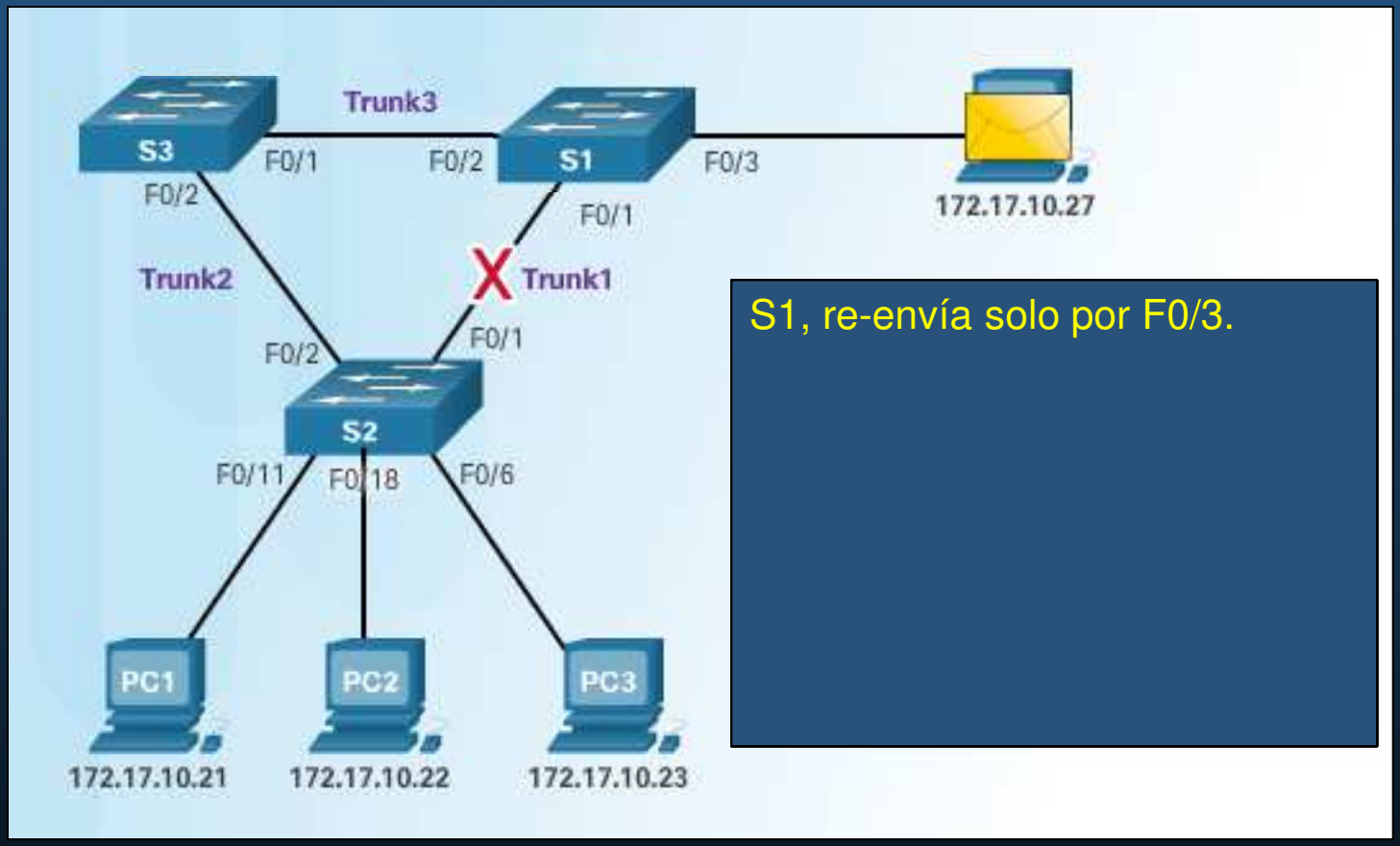


Puerto bloqueado: No re-envía tramas de datos (Intercambian BPDUs).

S2 desecha la trama recibida por el puerto bloqueado.

6.2 Consideraciones de Seguridad Capa 2

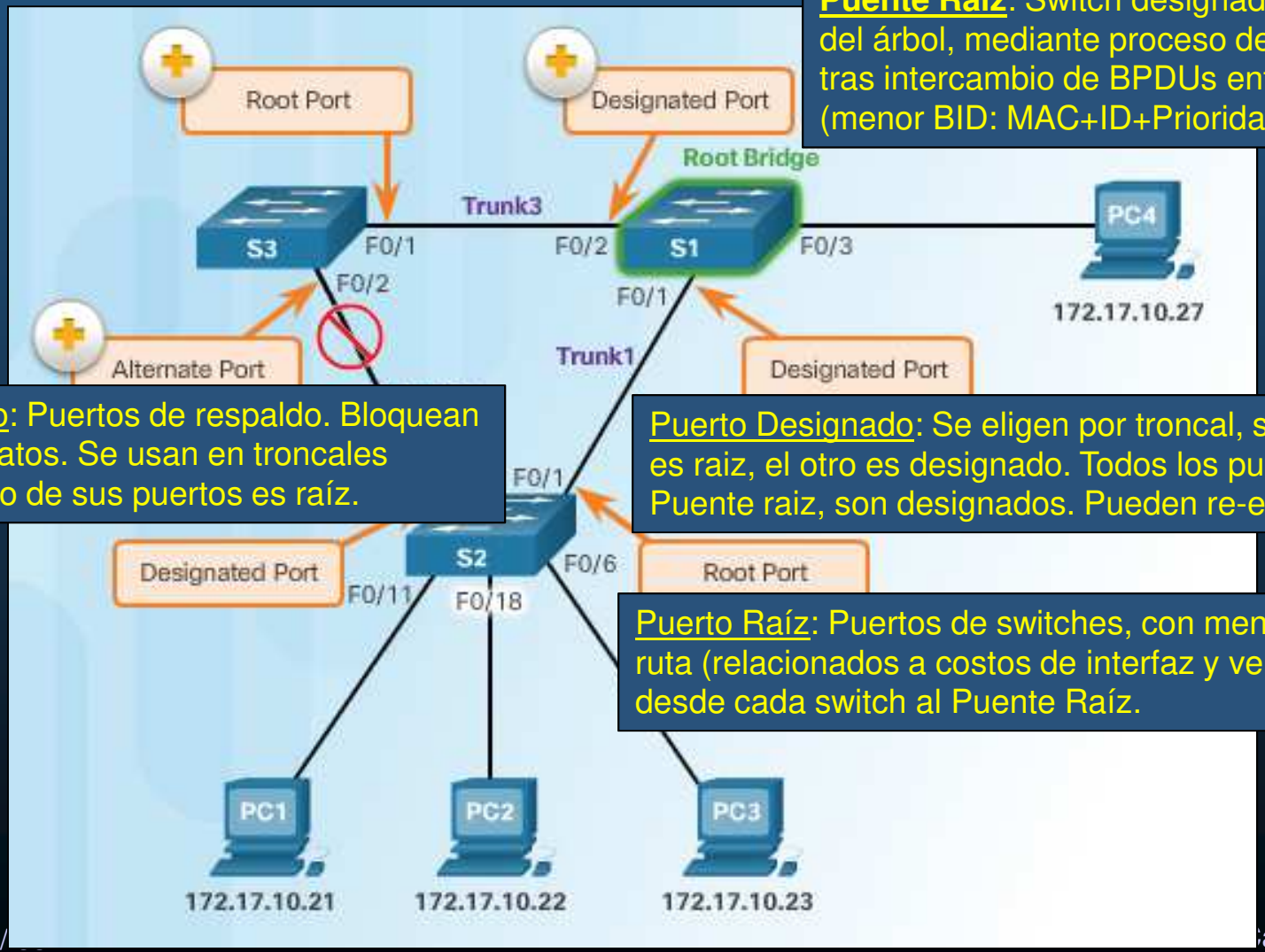
- Varias Implementaciones de STP.



Existen varias implementaciones de STP.
- STP (802.1D) , RSTP (802.1D-2004), MSTP

6.2 Consideraciones de Seguridad Capa 2

- Roles de Puertos STP.



Puente Raíz: Switch designado como raíz del árbol, mediante proceso de elección tras intercambio de BPDUs entre switches (menor BID: MAC+ID+Prioridad).

Puerto Alterno: Puertos de respaldo. Bloquean el tráfico de datos. Se usan en troncales donde ninguno de sus puertos es raíz.

Puerto Designado: Se eligen por troncal, si un puerto es raiz, el otro es designado. Todos los puertos del Puente raiz, son designados. Pueden re-enviar tráfico.

Puerto Raíz: Puertos de switches, con menor costo de ruta (relacionados a costos de interfaz y velocidades) desde cada switch al Puente Raíz.

6.2 Consideraciones de Seguridad Capa 2

- Puente Raíz STP.

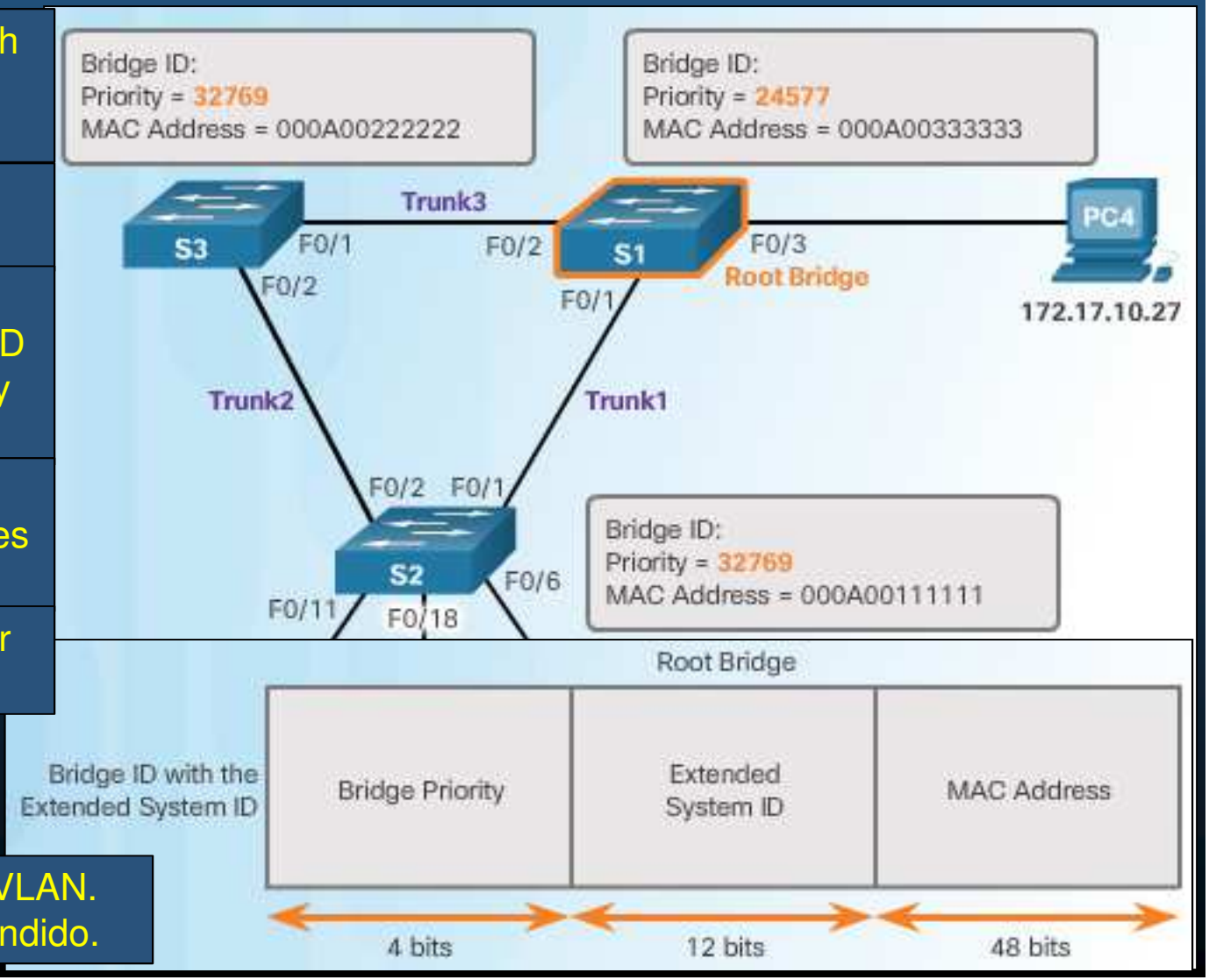
En un principio cada switch consedara que él, es el puente raiz

Evía BPDUs cada 2 segundos BID + RootID

Quién recibe BPDUs compara y actualiza RootID al menor de los recibidos y el propio.

Tras varios intercambios todos coinciden en quién es el Puente Raíz.

Habrá un Puente Raíz, por instancia de STP.

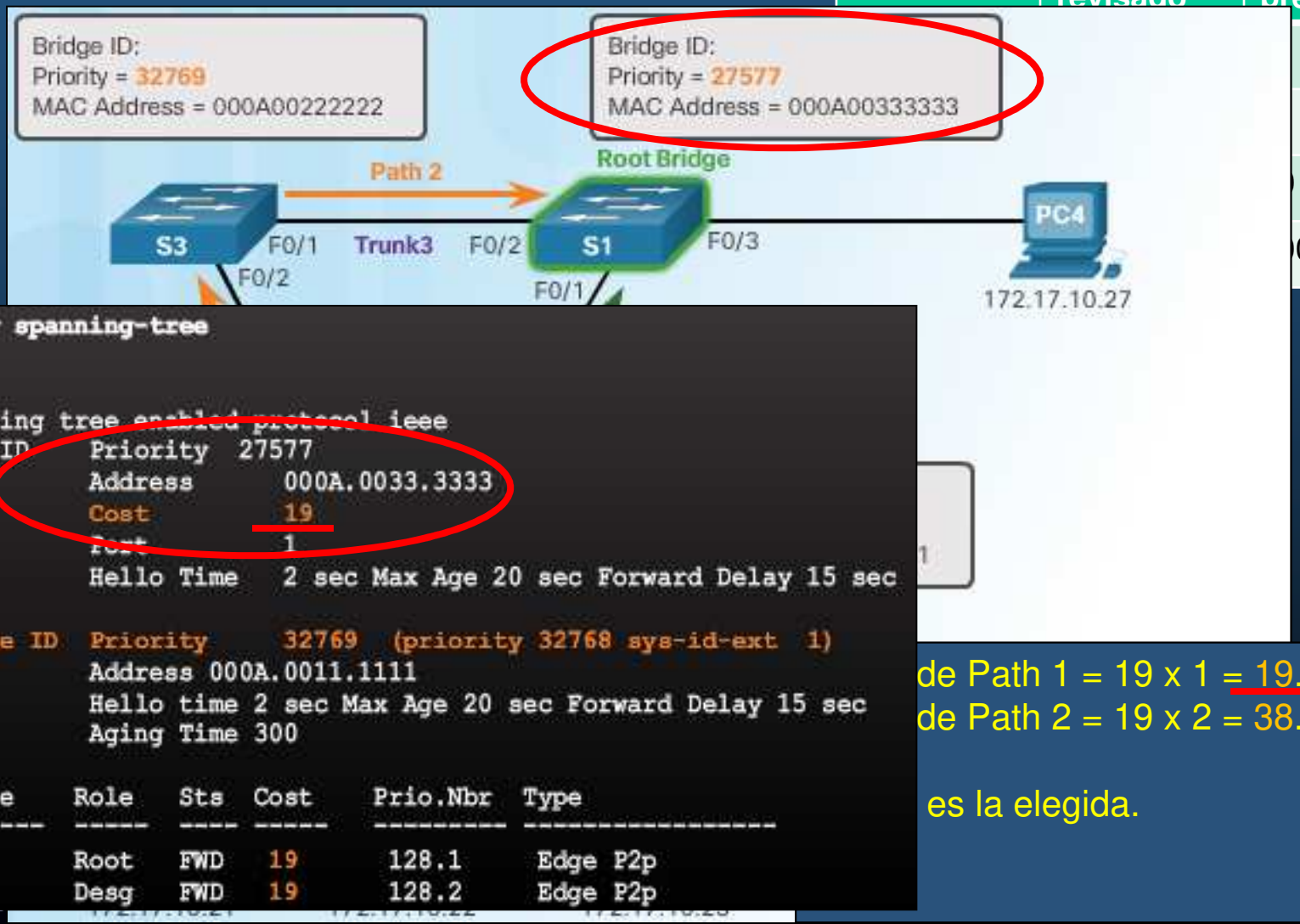


Puede haber un STP por VLAN. Requiere uso de BID Extendido.

6.2 Consideraciones de Seguridad Capa 2

- Costo de Ruta STP.
  -

Enlace	Costo IEEE revisado	Costo IEEE previo
		0




```
S2# show spanning-tree

VLAN001
   Spanning tree enabled protocol ieee
   Root ID     Priority  27577
               Address       000A.0033.3333
               Cost          19
               Port          1
               Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec

   Bridge ID   Priority      32769  (priority 32768 sys-id-ext  1)
               Address 000A.0011.1111
               Hello time 2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time 300

Interface     Role   Sts  Cost     Prio.Nbr  Type
------------  -----  ---- -------  --------- ----------------
F0/1          Root   FWD  19       128.1     Edge P2p
F0/2          Desg   FWD  19       128.2     Edge P2p
```

de Path 1 = 19 x 1 = 19.
de Path 2 = 19 x 2 = 38.

es la elegida.

6.2 Consideraciones de Seguridad Capa 2

- Formato de BPDUs 802.1D.
  - STP intercambia BPDUs para determinar el Puente Raíz y las rutas hacia él.

Field Number	Bytes	Field
1-4	2	Protocol ID
	1	Version

```
Frame 1 (60 bytes on wire, 60 bytes captured)
IEEE 802.3 Ethernet
  Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
  Source: Cisco_9e:93:03 (00:19:aa:9e:93:03)
  Length: 38
  Trailer: 0000000000000000
Logical-Link Control
Spanning Tree Protocol
  Protocol Identifier: Spanning Tree Protocol (0x0000)
  Protocol Version Identifier: Spanning Tree (0)
  BPDU Type: Configuration (0x00)
  BPDU flags: 0x01 (Topology Change)
  Root Identifier: 24577 / 00:19:aa:9e:93:00
  Root Path Cost: 0
  Bridge Identifier: 24577 / 00:19:aa:9e:93:00
  Port identifier: 0x8003
  Message Age: 0
  Max Age: 20
  Hello Time: 2
  Forward Delay: 15
```

Tipo de protocolo utilizado (0).

Versión del protocolo utilizado (0).

e (0).

ología (TC), Acuse de TC (TCA).

C del Puente Raíz.

del switch que envía mensaje.

C del switch que envía mensaje.

le donde se generó el mensaje.

puente raíz generó el mensaje de
se basa el presente mensaje.

erar la configuración como válida (20).

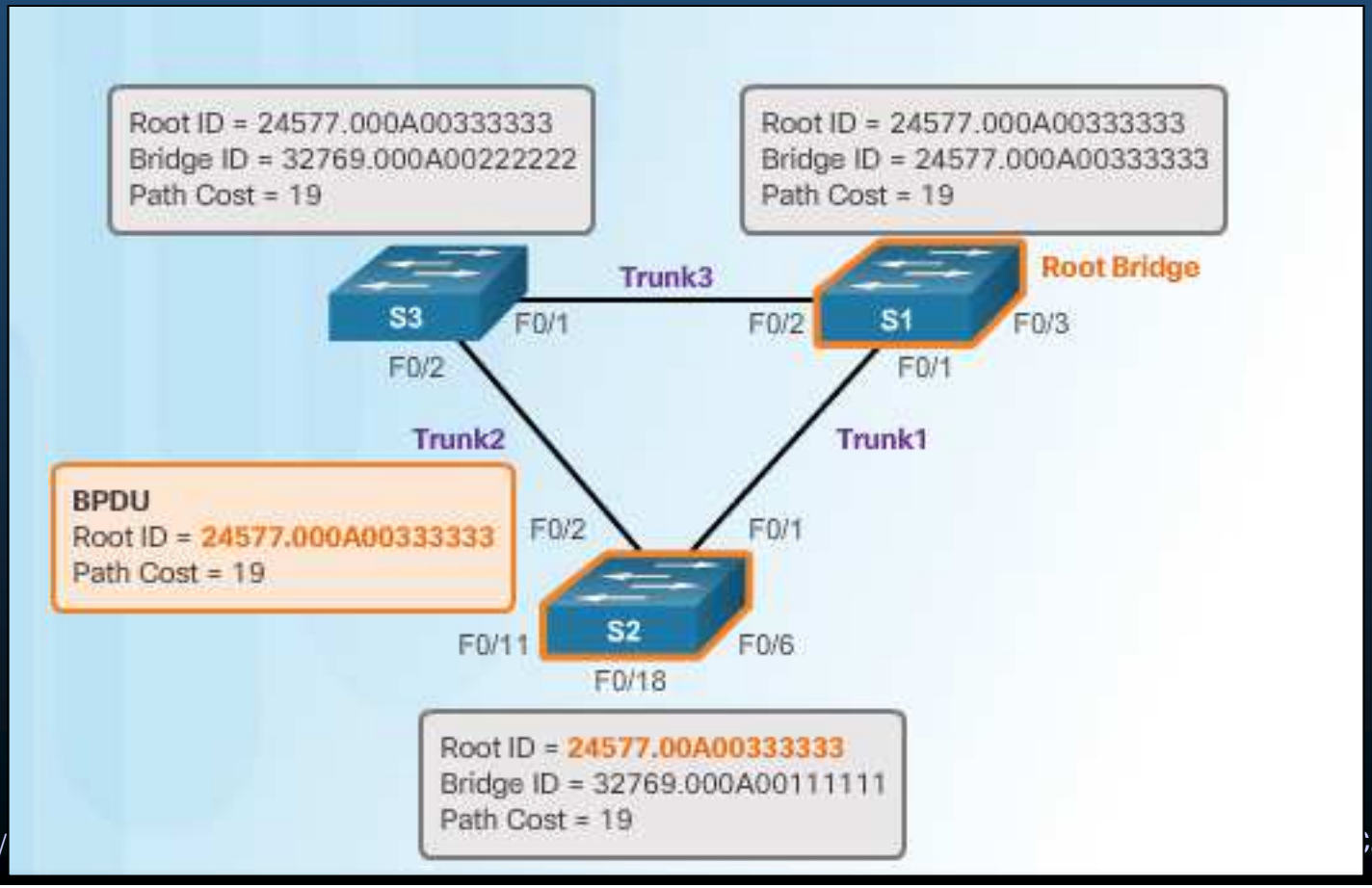
ará el Puente Raíz en enviar BPDUs (2).

cambiar el estado de la topología (15).
a que el resto de switches se enteren.

6.2 Consideraciones de Seguridad Capa 2

- Proceso y Propagación de BPDUs.

S2 compara el RootID del BPDU con el suyo. El recibido es menor.
Actualiza, estableciendo a S1 como el Puente Raíz. Actualiza el costo de Ruta a 19.



6.2 Consideraciones de Seguridad Capa 2

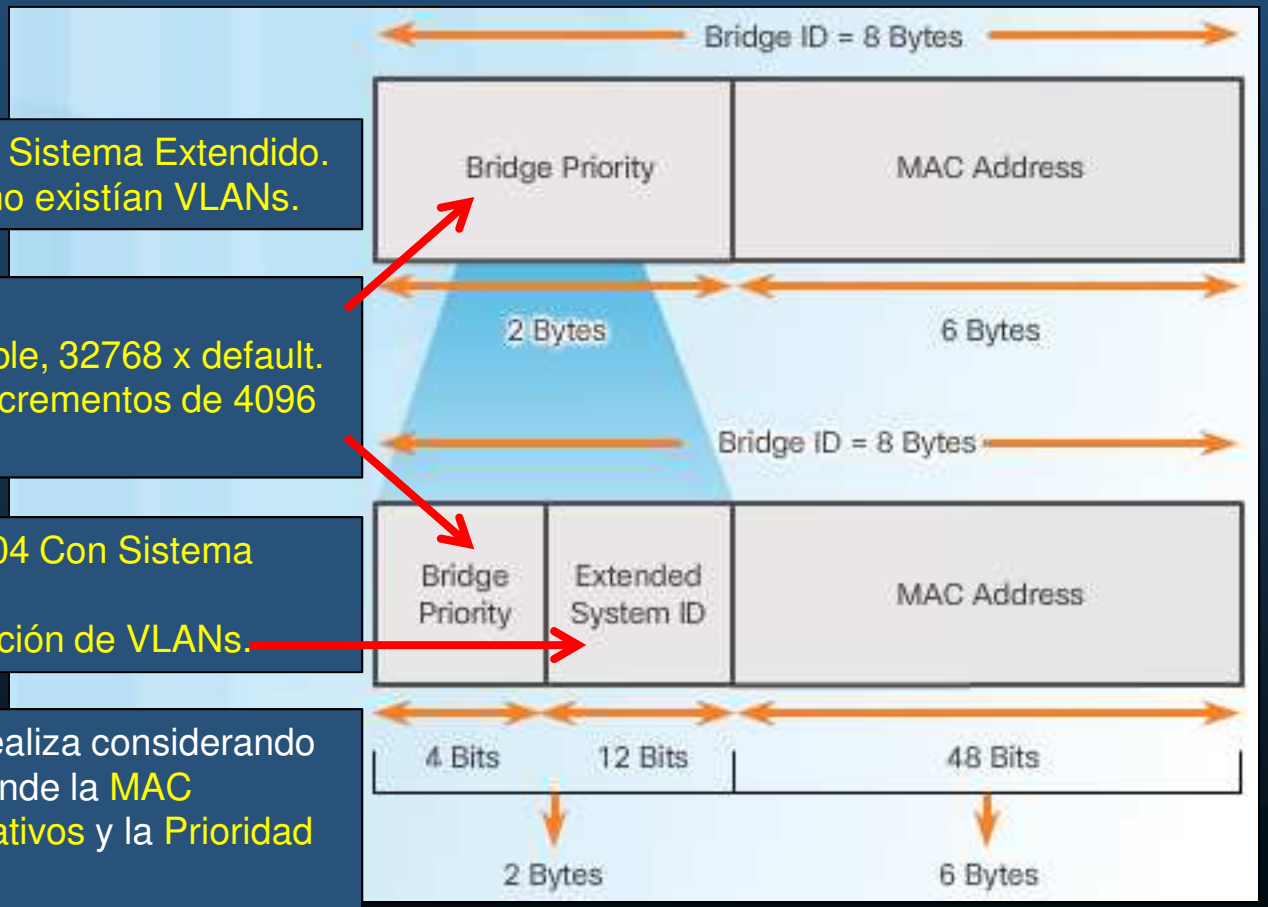
- Sistema de ID Extendido.
  - El ID de Puente (BID) es utilizado para la elección del Puente Raíz.

BID 802.1D Sin Sistema Extendido.
Originalmente no existían VLANs.

Prioridad.
Valor configurable, 32768 x default.
0 – 61440 en incrementos de 4096 (2^12).

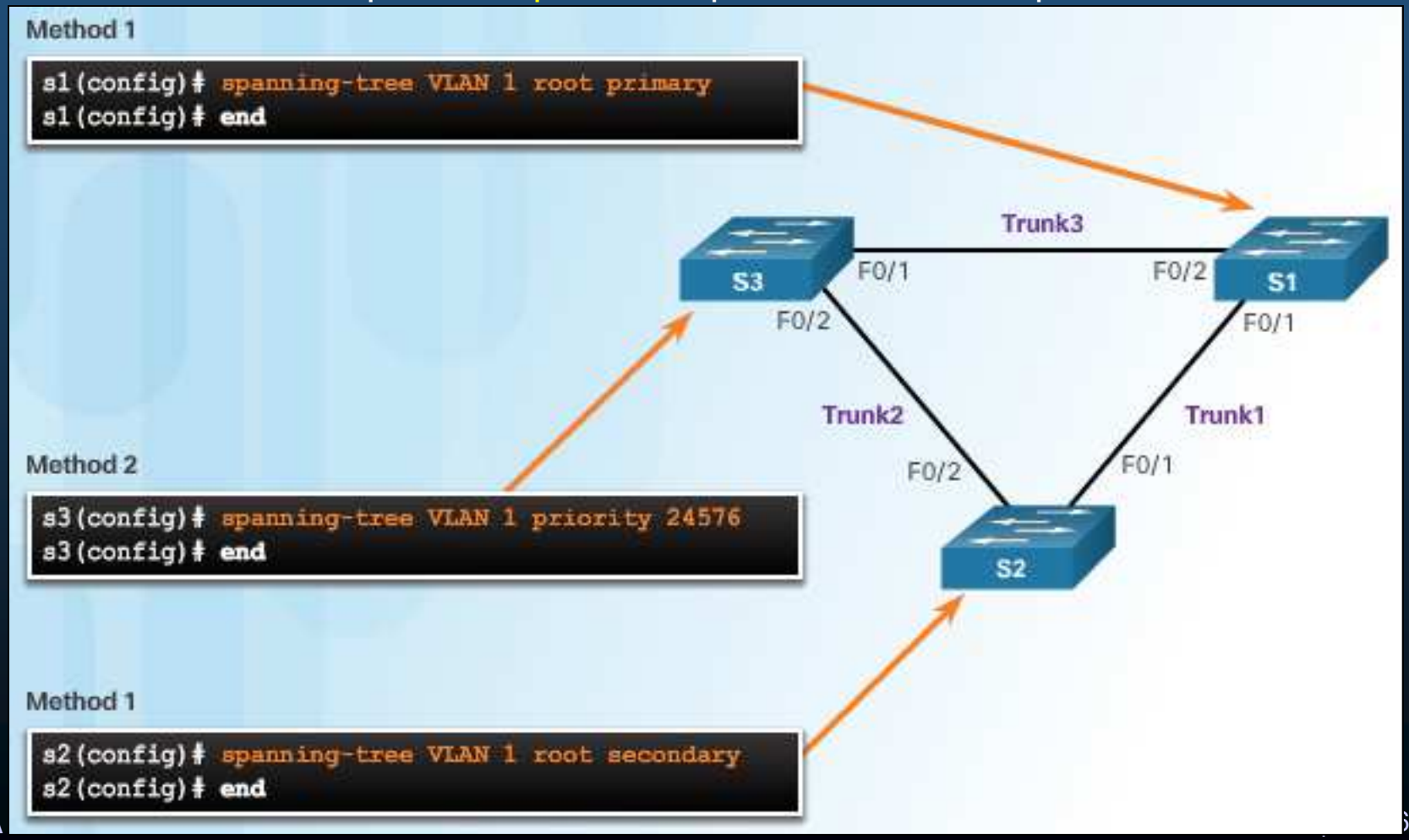
BID 802.1D-2004 Con Sistema Extendido.
Incluye Información de VLANs.

La elección del Puente Raíz, se realiza considerando los 8bytes, como un solo valor, donde la MAC representa los bits menos significativos y la Prioridad los bits mas significativos



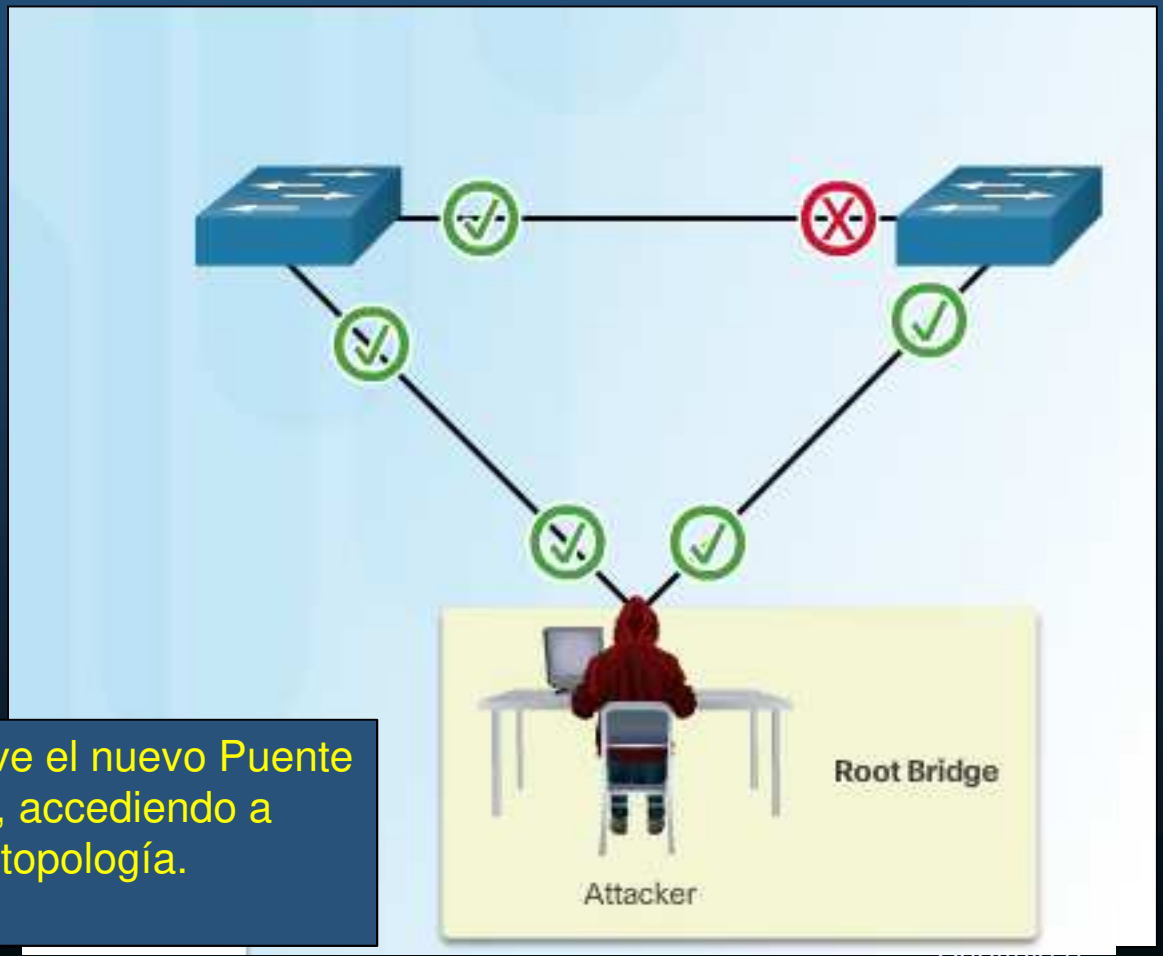
6.2 Consideraciones de Seguridad Capa 2

- Elección del Puente Raíz.
  - El administrador puede especificar que switch desea que sea el Puente Raíz.



6.2 Consideraciones de Seguridad Capa 2

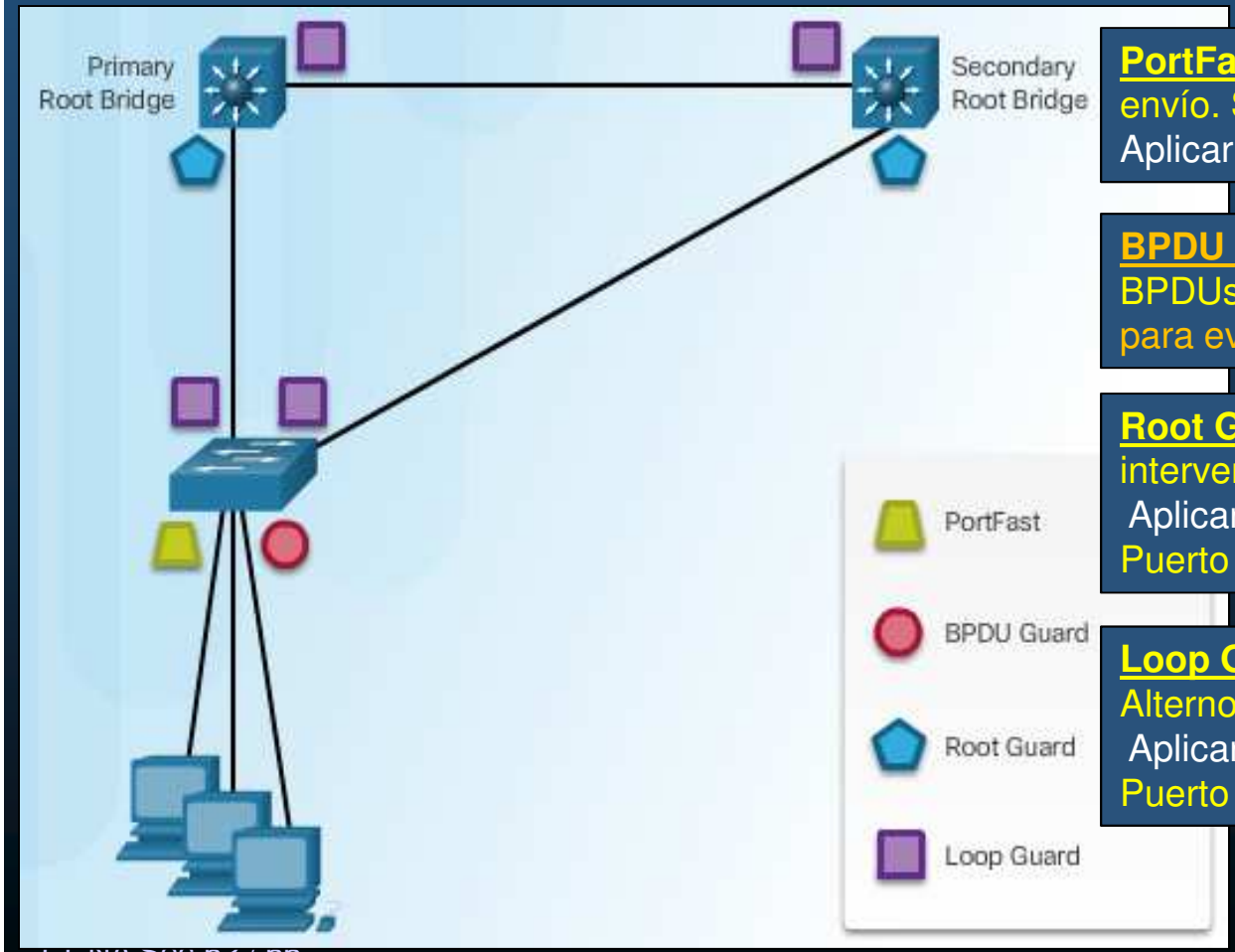
- Ataques por Manipulación de STP.
  - Un atacante puede fingir su host como Puente Raíz y capturar todo el tráfico.



El atacante se vuelve el nuevo Puente Raíz (prioridad = 0), accediendo a todo el tráfico de la topología.

6.2 Consideraciones de Seguridad Capa 2

- Mitigación de Ataques a STP.
  - Mecanismos de estabilidad de STP de Cisco.



PortFast: Cambia de estado de bloqueo a re-envío. Sin pasar por Listening ó Learning. Aplicar solo a puertos de usuario (acceso).

BPDU Guard: Deshabilita puertos que reciban BPDUs. Aplicar a puertos de usuario PortFast para evitar inserción de Switches Espurios.

Root Guard: Limita los puertos que intervendrán en la elección del Puente Raíz. Aplicar a puertos que no deban volverse Puerto Raíz.

Loop Guard: Evita que Puertos Raíz ó Alternos se vuelvan Designados. Aplicar a puertos que sean o puedan volverse Puerto no-Designado (Raíz / Bloqueados).

6.2 Consideraciones de Seguridad Capa 2

- Configuración de PortFast.

Parámetros subrallados,
No disponible en PacketTracer

  - Permite que los Hosts puedan conectarse a la Red mas rápido de lo normal. (Antes de que STP converja)
    - Pasa de estado de bloqueo a re-envío. Sin pasar por Listening ó Learning.
    - Aplicar solo a puertos de usuario (acceso).

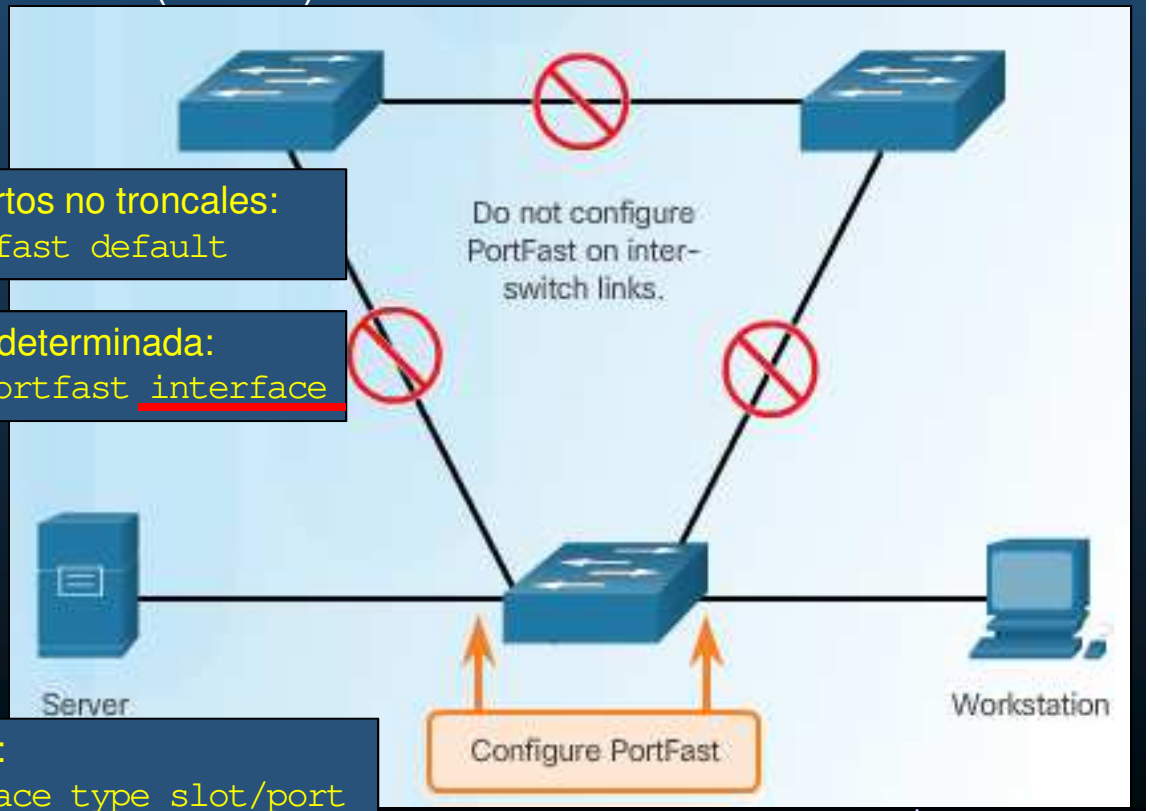
Habilitar PortFast en todos los puertos no troncales:

```
S(config)# spanning-tree portfast default
```

Habilitar PortFast en una interface determinada:

```
S(config-if)# spanning-tree portfast interface
```

- Su uso en troncales puede provocar bucles STP.

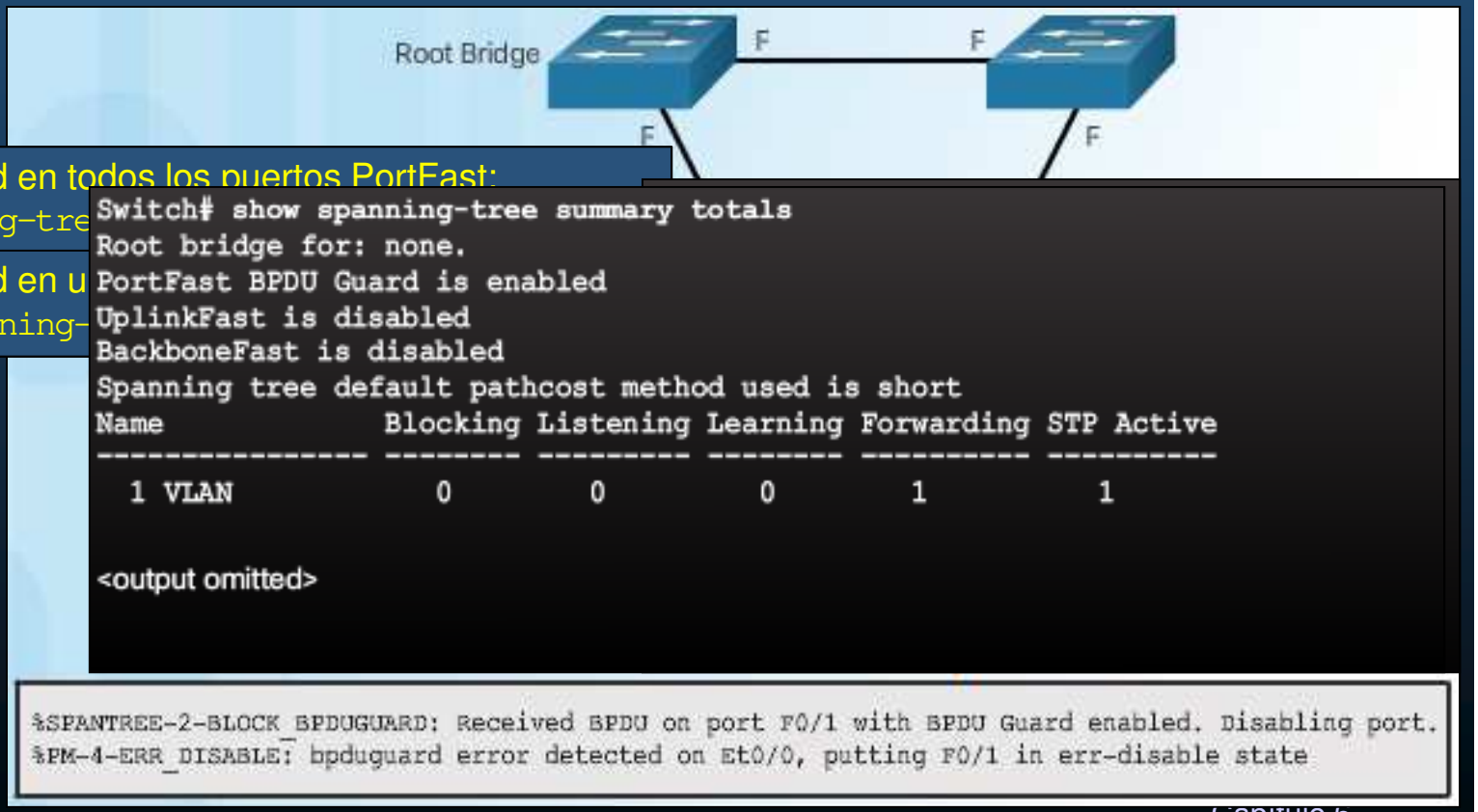


Verificar si PortFast está habilitado:

```
S# show running-config interface type slot/port
```

6.2 Consideraciones de Seguridad Capa 2

- Configuración de BPDU Guard.
  - BPDU Guard coloca el puerto en estado error-disabled, al recibir BPDUs.
    - Protege Puertos PortFast para que no intervengan en convergencia STP.
    - Evita que se agreguen switches adicionales a la topología.



Habilitar BPDU Guard en todos los puertos PortFast:

```
S(config)# spanning-tre
```

Habilitar BPDU Guard en u

```
S(config-if)# spanning-
```

```
Switch# show spanning-tree summary totals
Root bridge for: none.
PortFast BPDU Guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short
Name              Blocking Listening Learning Forwarding STP Active
---------------- -------- --------- -------- ---------- ----------
  1 VLAN             0         0         0         1          1

<output omitted>
```

```
%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa0/1 with BPDU Guard enabled. Disabling port.
%PM-4-ERR_DISABLE: bpduguard error detected on Et0/0, putting Fa0/1 in err-disable state
```

6.2 Consideraciones de Seguridad Capa 2

- Configuración de Root Guard.

Parámetros subrallados,
No disponible en PacketTracer

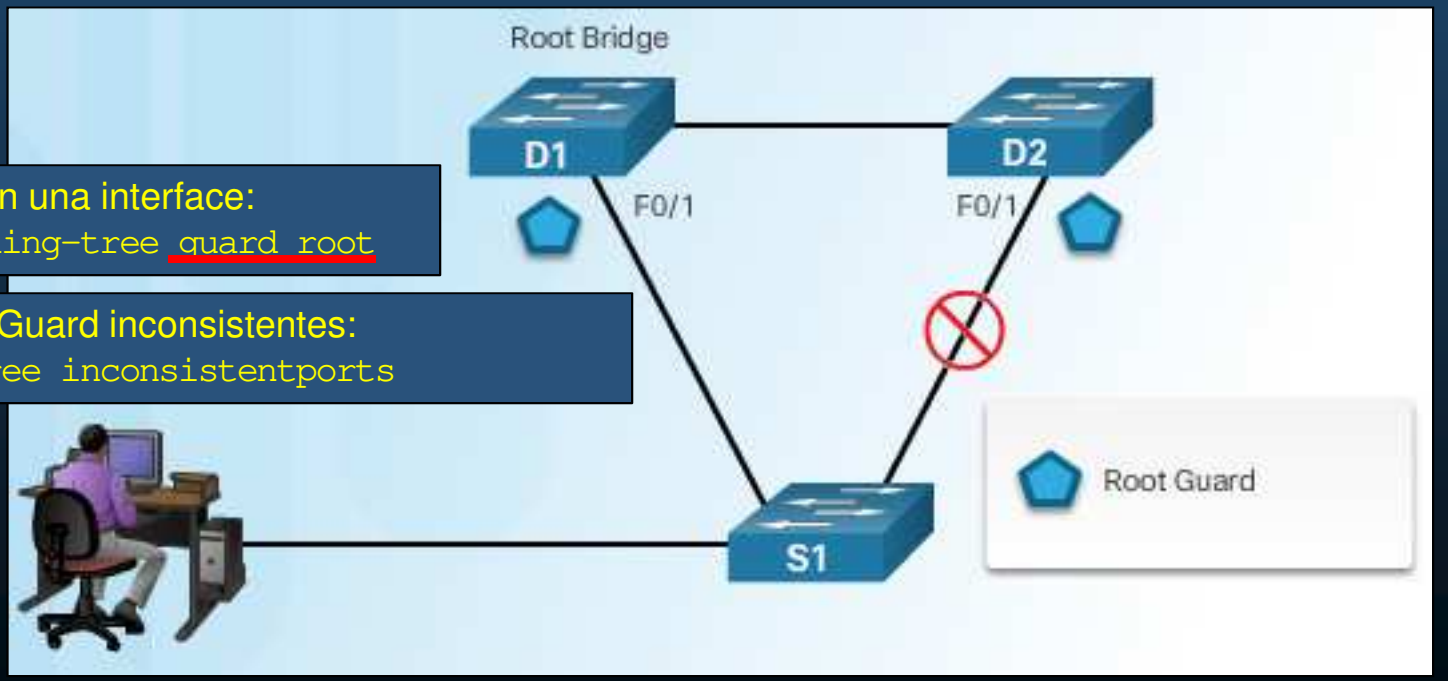
  - Limita los switches que pueden convertirse en Puente Raíz.
    - Se habilita en los puertos que conecten al switch que no deba ser Raíz.
  - Un puerto RootGuard que recibe BPDUs mejores que las suyas se cambia a estado root-inconsistent = STP listening (no re-envía datos)
    - El estado del puerto se reestablece cuando se dejen de recibir BPDUs mejores.

Habilitar Root Guard en una interface:

```
S(config-if)# spanning-tree guard root
```

Verificar puertos Root Guard inconsistentes:

```
S# show spanning-tree inconsistentports
```



6.2 Consideraciones de Seguridad Capa 2

- Configuración de Loop Guard.

No disponible en PacketTracer

  - Un puerto no-designado que deja de recibir BPDUs, cambia a estado Forwarding (Asume que el otro lado se volvió Alterno o Raíz).
    - Si solo falla el enlace en una dirección se crea un bucle Capa 2.
  - Un puerto Loop Guard no-designado que deja de recibir BPDUs cambia a: loo
    y bl

Habilitar L
S(config)

Habilitar L
S(config-

```
S1(config)#  do 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 enabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    1         0        0          5          6
---------------------- -------- --------- -------- ---------- ----------
1 vlan                      1         0        0          5          6
```

Guard

Guard

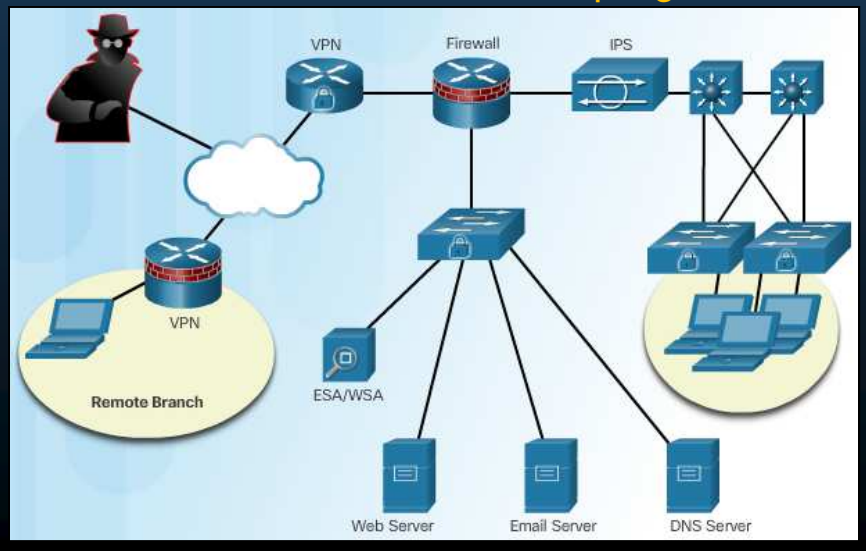
Capítulo 7

Sistemas Criptográficos

https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#7.1.1.1

7.1 Servicios Criptográficos

- Autenticación, Integridad y Confidencialidad.
  - Tras asegurar la topología, es necesario asegurar los datos que viajan a través de varios enlaces.
  - Tres objetivos de asegurar comunicaciones:
    - Autenticación: asegura que el mensaje no haya sido falsificado y que proviene de quién asegura provenir (HMAC).
    - Integridad: Asegura que nadie ha interceptado y/o modificado el mensaje (MD5/SHA).
    - Confidencialidad: Garantiza que si el mensaje es interceptado, no sea descifrado (Criptografía simétrica:DES/3DES/AES; Criptografía asimétrica: RSA/PKI).



7.1 Servicios Criptográficos

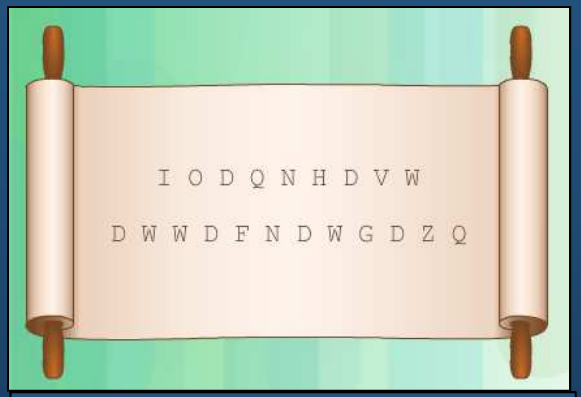
- Autenticación.
  - Garantiza que un mensaje provenga de la fuente que asegura hacerlo.
  - Servicios de Autenticación.
    - Similar a un PIN pre-compartido (simétrico) en secreto (métodos criptográficos).
  - Servicios de No-repudiación de datos.
    - Un emisor utiliza características únicas para firmar cada mensaje.
      - No podrá negar ser el remitente de un mensaje.

7.1 Servicios Criptográficos

- Integridad.
  - Asegura que los mensajes no sean alterados en tránsito.
    - Similar a un sello de cera sin romper.

7.1 Servicios Criptográficos

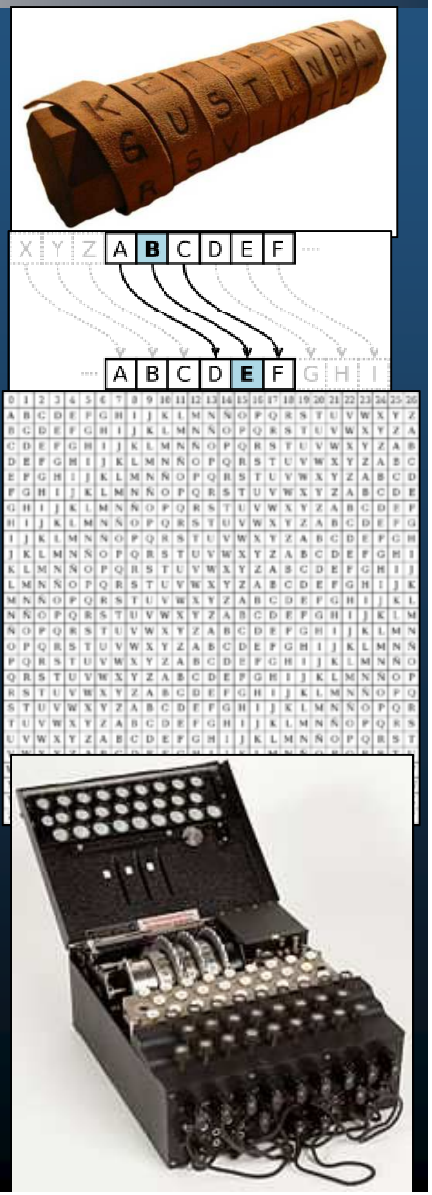
- Confidencialidad de Datos.
  - Asegura que solo el receptor pueda leer el mensaje.
  - Encriptación: Proceso de cifrado de datos para que no pueda ser leído fácilmente por partes no autorizadas.
    - Texto Plano: datos en su forma legible.
    - Texto cifrado: Datos encriptados (ilegibles).
  - Des-encriptación: Proceso de encriptación inverso.
  - Ambos procesos requieren una llave.
  - Encriptación != Hash
    - Encriptación, puede des-cifrarse.
    - Hash es solo un identificador de integridad en un solo sentido.



Cifrado Caesar: desplazamiento de alfabeto

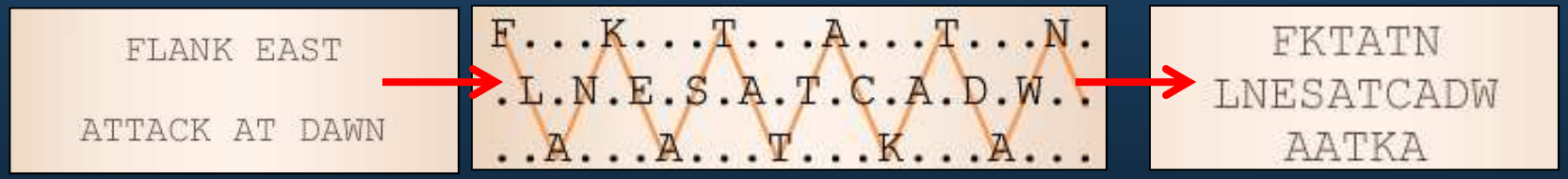
7.1 Servicios Criptográficos

- Creando Cifrado de Texto.
  - Comúnmente utilizado para asegurar secrecía de los mensajes.
    - Escítala: Cifrado militar mas antiguo conocido, usado por Éforos espartanos. Una tira de cuero con letras, al enrollar en un trozo de madera revela palabras/frases (transposición).
    - Cifrado Cesar: Cifrado usado por Julio cesar y sus generales. Técnica de Cifrado mas simple, sustitución de letras, por la correspondiente en un alfabeto desplazado n posiciones (sustitución).
    - Cifrado Vigenère: Cifrado Cesar en 2 dimensiones (tabla de sustitución) Original de Giovan Battista Belasso en 1553.
    - Máquina Enigma: Máquina electromecánica de cifrado rotativo; Uso militar y comercial desde 1920. Mas conocida por ser empleada por los nazis en la segunda guerra mundial.
  - Cada método utiliza algoritmo específico, llamado cifrado:
    - Transposición, Sustitución, bloc de un solo uso.



7.1 Servicios Criptográficos

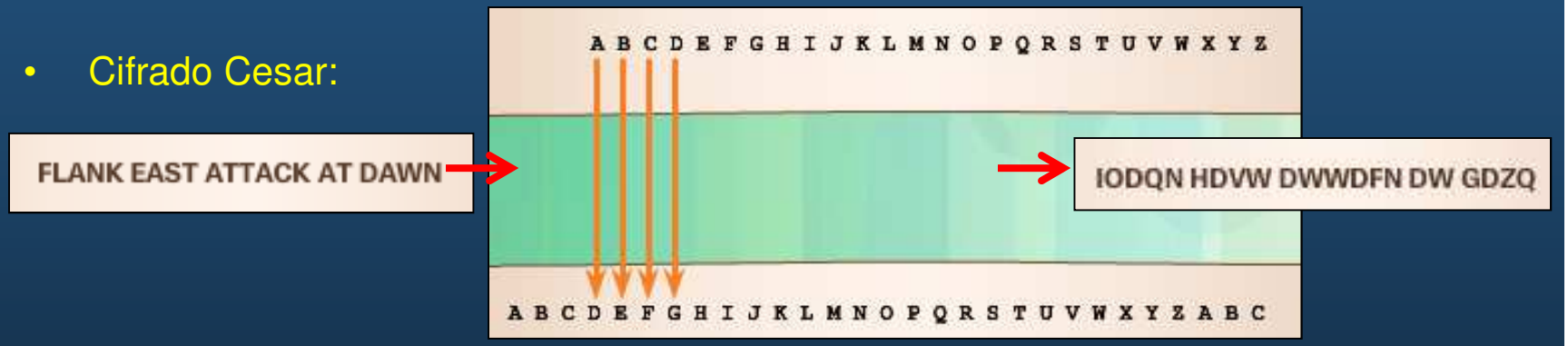
- Cifrados por Transposición.
  - Se reorganizan las letras, no se reemplazan.
    - Vgr; Llave: en orden inverso.
      - FLANK EAST ATTACK AT DAWN → NWAD TAKCATTA TSAE KNALF.
    - Cifrado Rail Fence (Llave, por diagonales descendente y ascendente)



    - Algoritmos modernos como DES y 3DES todavía usan transposición como parte del algoritmo

7.1 Servicios Criptográficos

- Cifrados por Sustitución.
  - Sustituyen letras por otras, mantiene la frecuencia de las letras.
    - Cifrado Cesar:



      - También llamado sustitución monoalfabética (siempre mismo desplazamiento)
      - Fácil de descifrar.
        - Por ello surgen versiones polialfabéticas como:
          - Cifrado Vigenère por Giovan Battista Belasso en 1553 erroneamente atribuido al frances Blaise de Vigenère.

7.1 Servicios Criptográficos

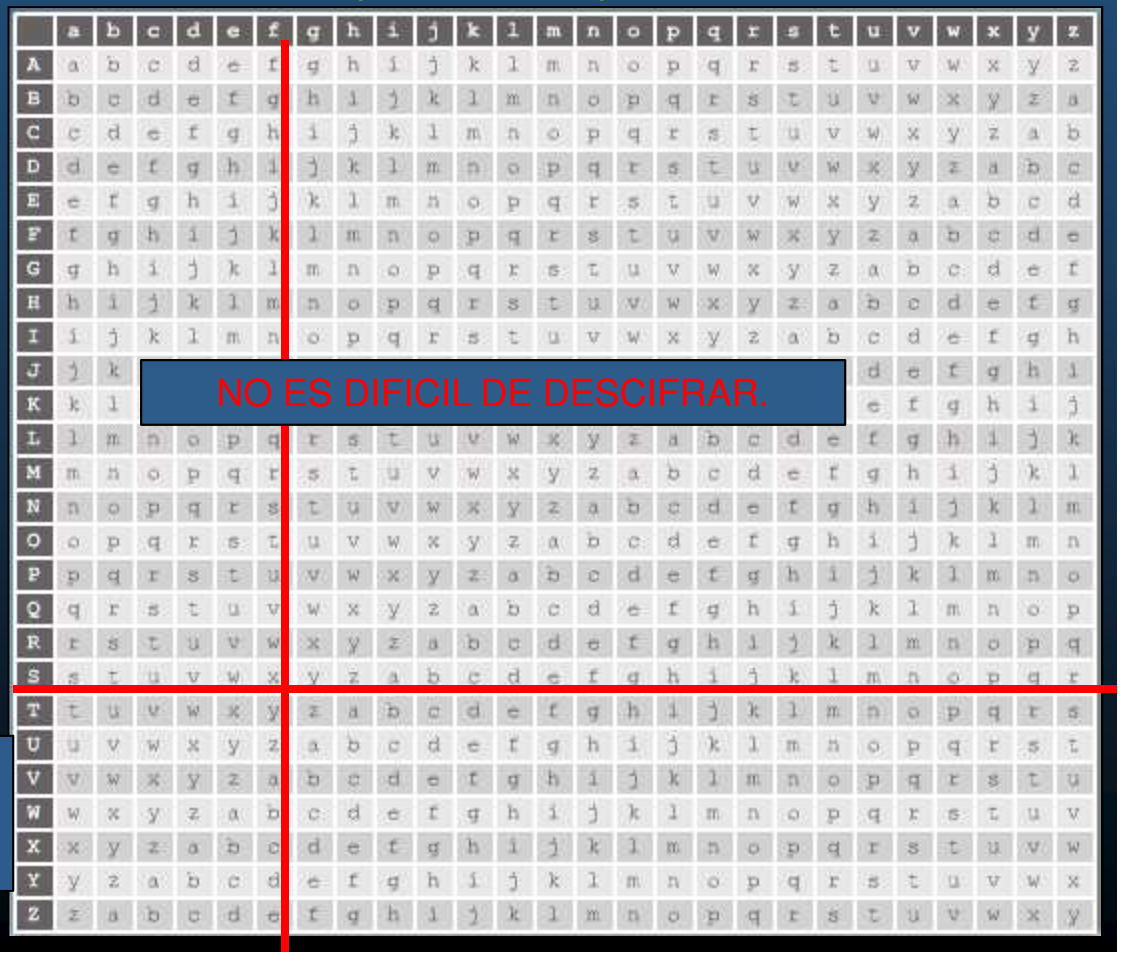
- Cifrados por Sustitución.
  - Sustituyen letras por otras, mantiene la frecuencia de las letras.
    - Cifrado Vigenère: polialfabético (diferente desplazamiento para cada letra).

Emisor y receptor deben conocer llave pre-compartida (SECRETKEY)

Emisor codifica mensaje (flank east attack at dawn)

Intersecta columna del mensaje (f) con fila de la llave (S) = (x)

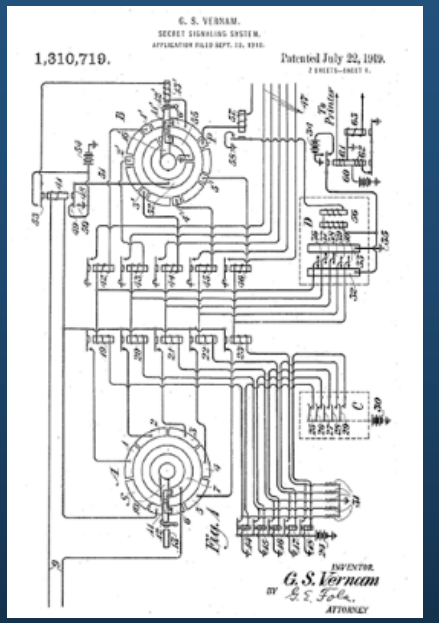
Incrementa índice de llave y mensaje, y repite mientras existan letras en el mensaje (la llave se considera circular, se repite de ser necesario).



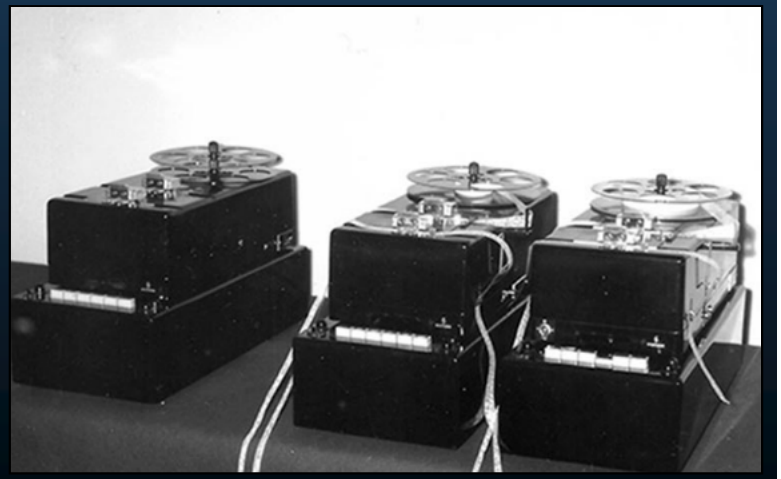

```
Llave Secreta:  SECRE TKEY SECRET KE YSEC
Texto Plano:    FLANK EAST ATTACK AT DAWN
Texto Cifrado:  XPCEO XKUR SXVRGD KX BSAP
```

7.1 Servicios Criptográficos

- Cifrados de Bloc de un Solo Uso.
  - Gilbert Vernam (Ingeniero de AT&T Bell Labs), en 1917
    - Cifrado de flujos:
      - Máquina Teletipo.
      - Cinta con llave de longitud arbitraria de números sin repeticiones.
      - Combinaba carácter por carácter con el mensaje.
    - Para descifrar el mensaje la misma cinta se volvía a combinar carácter por carácter para revelar el texto plano.



  - Inmune a Criptoanálisis siempre que nunca se use la misma cinta mas de una vez.
    - Impráctico generar números realmente aleatorios.
    - RC4 es Implementación en PCs con núms. pseudo-aleatorios.
    - Complicado distribuir la llave.



7.1 Servicios Criptográficos

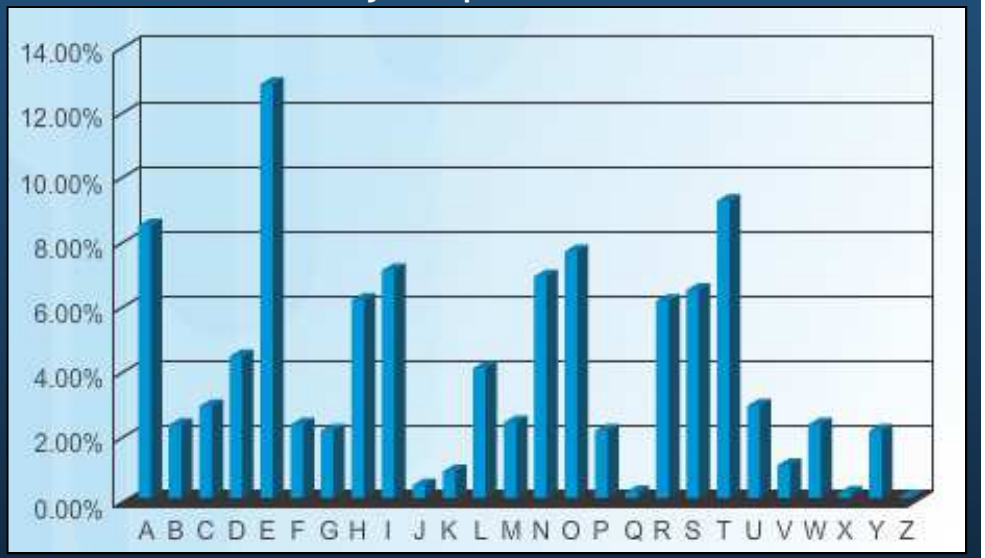
- Romper Cifrados.
  - Desde que existe la Criptografía, existe el Criptoanálisis.
  - Criptoanálisis: estudio para determinar el significado de la información encriptada (sin acceso a la llave secreta).
  - Ejemplos:
    - Cifrado Vigenère (1553), seguro hasta el siglo XIX (Charles Babage).
    - María, Reina de Escocia, buscó derrocar a la Reina Isabel I de Inglaterra (1570). Enviaba mensajes encriptados a sus co-conspiradores, tras descifrarse, fue decapitada (1587).
    - Enigma cifraba comunicaciones alemanas para dirigir barcos en el atlántico. Criptoanalistas Polaco-Britanicos descifraron mediante criptoanálisis y definió la Segunda Guerra Mundial.
  - Requiere muchos intentos antes de dar con el código correcto.

7.1 Servicios Criptográficos

- Métodos para Romper Cifrados.
  - Fuerza Bruta.
    - Intentar todas las posibles llaves.
  - Método Texto-Cifrado.
    - El atacante posee varios mensajes con el mismo cifrado. Busca relación.
  - Texto-Plano Conocido.
    - El atacante analiza el mensaje en Texto-Plano y su Texto-Cifrado resultante.
  - Método Texto-Cifrado Elegido.
    - El atacante puede elegir descifrar determinado Texto-Cifrado.
  - Encuentro a Medio Camino.
    - Determinar la llave a partir de un Texto-Cifrado y su Texto-Plano.
  - Su implementación está fuera del ámbito del presente curso.
  - Premisa: Si hubo alguien lo suficiente inteligente para cifrar algo, habrá otro capaz de descifrarlo
    - El objetivo de la cryptografía es generar llaves lo suficientemente grandes para que descifrar sea los mas costoso y tardado (que ya no sea útil cuando se logre).

7.1 Servicios Criptográficos

- Ejemplo de Rotura de Cifrados (Cifrado Cesar).
  - Cuando las llaves son pocas, Fuerza Bruta es la mejor opción.
  - Cuando no:
    - Análisis de Frecuencia:
      Asumir que algunos caracteres son mas utilizados que otros.
      - Mas frecuentes: E,T,A
      - Menos frecuentes: J,Q,X,Z



IODQN HDVW
DWWDFN DW GDZQ

Mensaje en Ingles con Cifrado Cesar

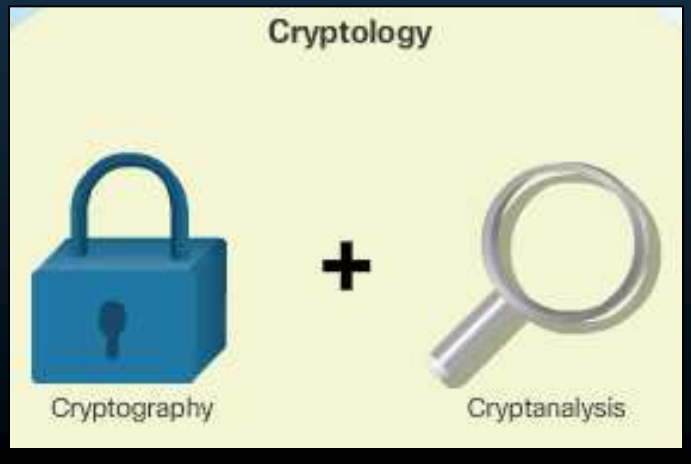
http://nosolomates.es/?page_id=760

- D aparece 6 veces. → Podría ser E,T, ó A
- W aparece 4 veces. → Podría ser E,T, ó A

D → E → desplazamiento de 1 → JPERO IEWX EXXEGO EX HEAR [X]
D → T → desplazamiento de 16 → YETGD XTLM TMMTVD TM WTPG [X]
D → A → desplazamiento de 23 → FLANK EAST ATTACK AT DAWN [OK]

7.1 Servicios Criptográficos

- Creando y Rompiendo Cifrados.
  - Criptología: Ciencia de crear y romper Códigos de Cifrado.
    - Criptografía: Desarrollo de códigos de cifrado.
    - Criptoanálisis: Ruptura de códigos de cifrado.
  - Las organizaciones de seguridad contratan especialistas en ambas ramas y los ponen a competir.
  - Por momentos una disciplina se ubica por delante de la otra.
    - Actualmente se cree que los criptógrafos llevan la delantera.



7.1 Servicios Criptográficos

- Criptoanálisis.
  - Comúnmente utilizado por (criptoanalistas):
    - Gobiernos para vigilancia militar y diplomática.
    - Empresas para proteger propiedad intelectual.
    - Hackers para explotar vulnerabilidades.

NSA

Cryptanalysis

National Security Agency | Fort Meade, MD

Job Description

Cryptanalysis is one of the core technical disciplines necessary for the NSA to accomplish its mission and provide critical intelligence to the nation's leaders. In an ever-changing global environment, the need for Cryptanalysts will remain constant.

Traditionally, Cryptanalysis is the art and science of solving cryptograms (writings in cipher or code) or cryptographic systems (devices for enciphering and deciphering) through analysis without prior knowledge of the encryption method. In a code, a word or phrase is replaced with another word, number, or symbol. In a cipher, each letter is replaced with another letter, number or symbol. Using known techniques and imagination, a Cryptanalyst systematically identifies basic elements in a cipher code that may lead to its solution. Modern Cryptanalysis includes analysis of any type of hidden information, whether a traditional cipher or a telecommunication protocol.

ANSWERING THE TOUGH QUESTIONS:

Cryptanalysts utilize mathematics, computer programming, engineering, and language skills as well as new technologies and creativity to solve tomorrow's problems today. That's why the NSA is looking for people who are intelligent and imaginative, and who can contribute original ideas to the solution of complex challenges. Cryptanalysts must communicate clearly, concentrate long and hard on difficult problems, and not be discouraged if success is elusive. No specific major is targeted for Cryptanalysis; the NSA hires people with technical and non-technical degrees, ranging from mathematics to music, engineering to history, and computer programming to chemistry.

  - Aunque asociado con propósitos dañinos, irónicamente necesario.
    - Permite probar que determinados algoritmos no sean susceptibles a él.

  - Por eso, Matemáticos y Forenses de Seguridad buscan romper mecanismos de seguridad.

7.1 Servicios Criptográficos

- El secreto está en las llaves.
  - Varios algoritmos para diferentes propósitos.

Integridad	Autenticación	Confidencialidad
MD5	HMAC-MD5	DES
SHA	HMAC SHA-1	3DES
	RSA & DSA	AES

    - Cada uno con características diferentes.
  - En la antigüedad basaban su seguridad en la secrecía del algoritmo.
  - Hoy en día, la ingeniería inversa descifra fácilmente los algoritmos.
    - Basar seguridad en la secrecía de las llaves.

7.2 Integridad Básica y Autenticidad

- Funciones Hash Criptográficas.
  - Principalmente usadas para verificar integridad.
    - Generan representación condensada (resumen) del Texto-Plano.
    - Pequeñas variaciones en Texto-Plano produce grandes diferencias de resumen.
  - Similar al cálculo de un CRC.
  - Imposible regenerar Texto-Plano a partir del Hash.
  - Aplicaciones:
    - Autenticidad: autenticación por llave simétrica (IPSec).
    - Autenticación: Generar cadenas de un solo uso (PPP CHAP).
    - Integridad: Certificados en Infraestructura de llave pública (PKI) (certificados https).

7.2 Integridad Básica y Autenticidad

- Propiedades de las Funciones Hash Criptográficas.
  - Matemáticamente: *h=H(x)*
    - Donde:
      - *H* es una función Hash.
      - *x* es la entrada en Texto-Plano.
      - *h* es una cadena de longitud fija llamada valor de hash.
    - Propiedades:
      - *x* puede ser de cualquier longitud.
      - *h* tendrá siempre la misma longitud.
      - *H(x)* debe ser fácil de calcular para cualquier *x*.
        H(x) debe ser en un solo sentido e irreversible (función análisis sin síntesis).
        - O al menos computacionalmente complicado.
      - *H(x)* debe ser libre de colisiones (a dos diferentes *x*, dos diferentes *h*).
        - O al menos muy baja la probabilidad de colisiones.

7.2 Integridad Básica y Autenticidad

- Funciones Hash Bien Conocidas.
  - Las funciones Hash ayudan a asegurar que los datos no hayan cambiado en el tránsito de una comunicación, añadiendo la firma al mensaje.
  - Al llegar un mensaje, al receptor se re-calcula su hash y si coincide con el del mensaje, se considera que no ha sido alterado.
    - Similar a un CRC.
  - No es posible proteger a cambios deliberados (Un atacante podría cambiar tanto el mensaje, como el hash)
    - Vulnerable a Ataques Man-In-The-Middle.
  - Dos funciones Hash bien conocidas son:
    - Firmas de 128bits MD5
    - Firmas de 256bits SHA

7.2 Integridad Básica y Autenticidad

- Algoritmo Firma de Mensaje 5 (MD5).
  - Desarrollado por Ron Rivest.
    - Secuencia compleja de operaciones binarias simples (XOR, corrimientos)

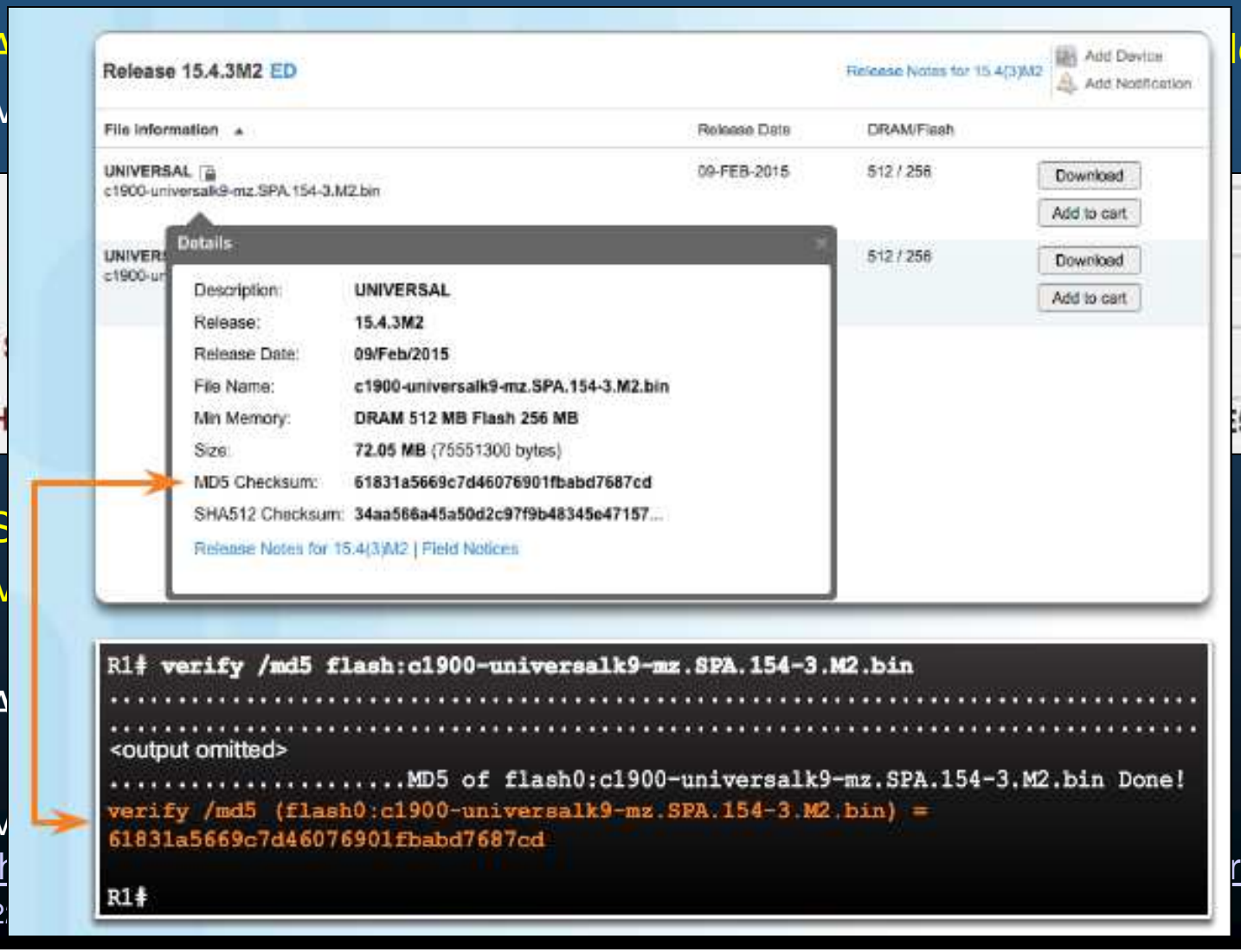
  - Actualmente considerado obsoleto, pero difícil reemplazar por su amplio uso.
    - En lo posible se recomienda reemplazarlo por SHA-2.

7.2 Integridad Básica y Autenticidad

- Algoritmo de Hash Seguro (SHA).
  - Desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos.
    - SHA-1 → 1994 (obsoleto)
    - Toma mensajes de longitud menor a 2^64 y produce Firma de 160bits.
    - Ligeramente mas lento que MD5.
    - A mas bits, mas seguro ante colisiones.
    - SHA-2 (Familia de funciones Hash con firmas de diferente longitud)
      - SHA-224 (224 bit)
      - SHA-256 (256 bit)
      - SHA-384 (384 bit)
      - SHA-512 (512 bit)
      - Requerido por ley para determinadas aplicaciones gubernamentales.
      - Recomendable usar SHA-256, SHA-384, y SHA-512 cuando sea posible.

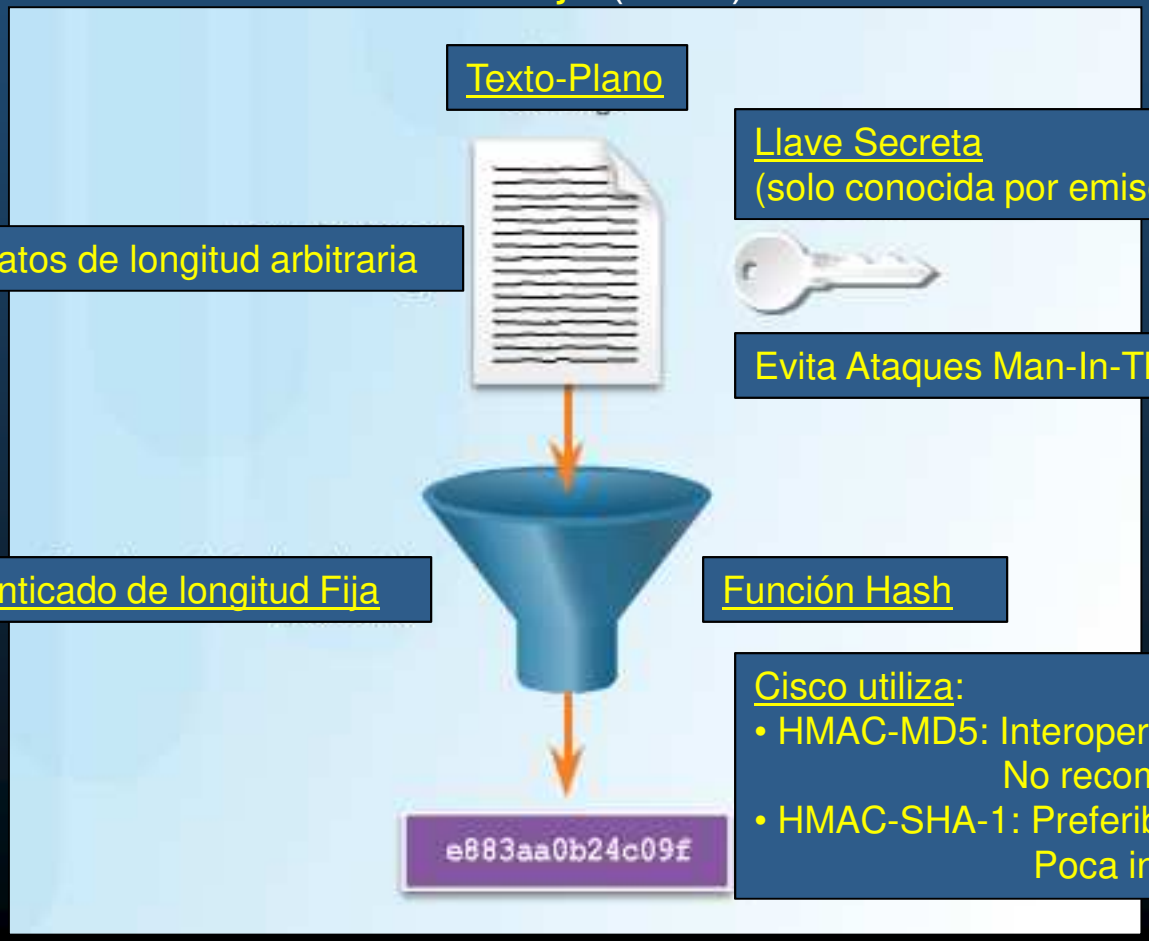
7.2 Integridad Básica y Autenticidad

- MD5 vs SHA.
  - A
  - M
  - S
  - M
  - A
  - M



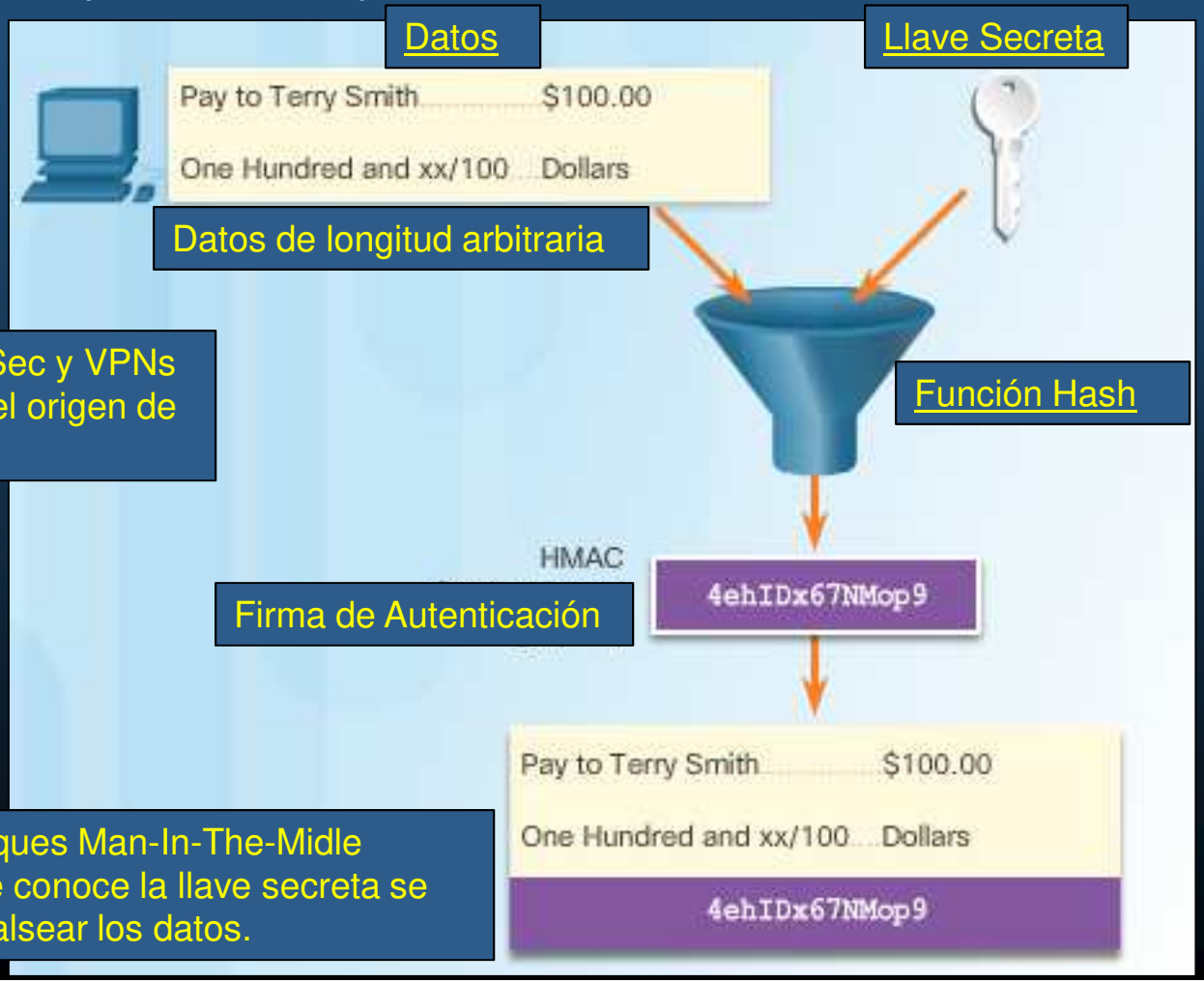
7.2 Integridad Básica y Autenticidad

- Código de Autenticación de Mensajes por Hash de Llave (Keyed-Hash Message Authentication Code - KHMAC).
  - Código de Autenticación de Mensaje (MAC).



7.2 Integridad Básica y Autenticidad

- Operación HMAC.
  - Asegurar que un mensaje no se ha alterado en tránsito.

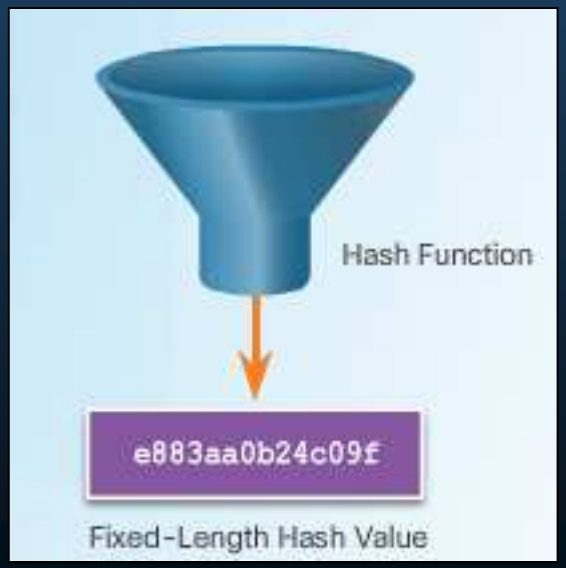


Utilizado por IPSec y VPNs para autenticar el origen de cada paquete

Evita Ataques Man-In-The-Midle
Solo si se conoce la llave secreta se podrían falsear los datos.

7.2 Integridad Básica y Autenticidad

- Hashs en Productos Cisco.
  - Usado para Autenticación de Entidades, Integridad de Datos y otras Autenticaciónes:
    - Hash + Llaves secretas: Autenticar información de enrutamiento.
    - Dispositivos IPSec: Verificar Integridad de Paquetes y Autenticidad en capa 3.
    - Integridad de Imágenes descargadas



  - Nota: Las Firmas Digitales son una alternativa a HMAC

7.2 Integridad Básica y Autenticidad

- Características de Administración de Llaves.
  - Generación: En criptografía moderna generador de números aleatorios. (imprescindible que el atacante no pueda predecir llaves mas utilizadas).
  - Verificación: Imprescindible identificar y evitar utilizar llaves débiles.
  - Intercambio: Acordar de manera segura la llave a utilizar (probablemente por un medio inseguro).
  - Almacenamiento: Cuidar intercambio Disco a Memoria y posibles accesos no autorizados.
  - Tiempos de Vida: Entre mas cortos sean mas seguro.
  - Revocación y Destrucción: Informar de llaves comprometidas y evitar su uso futuro. Al borrar contraseñas, asegurar que no se puedan recuperar.

7.2 Integridad Básica y Autenticidad

- Longitud de Llave y Espacio de Llave.
  - Longitud de Llave: Tamaño de la llave en bits.
  - Espacio de Llave: Posibles llaves que pueden ser generadas dada una longitud de llave.
    - Se incrementa exponencialmente en relación a la longitud de llave.
    - 2^(Longitud de bits) ??

Características AES	
Descripción.	Estándar de Encriptación Avanzada
Línea de Tiempo.	Estándar Oficial desde 2001
Tipo de Algoritmo.	Simétrico
Tamaño de Llave	128b, 192b y 256b
Velocidad	Alta
Tiempo de ruptura. (255 intentos por segundo)	149 trillones de años.
Consumo de Recursos.	Bajo

7.2 Integridad Básica y Autenticidad

- Espacio de Llave.
  - Conjunto de posibles valores de llave 2^n bits.
  - Mientras mayor sea n, las llaves serán mas seguras, pero mas difíciles (computo-intensivo) de generar.
  -

DES Key	Keyspace	# of Possible Keys
56-bit	2^{56} 11111111 11111111 11111111 11111111 11111111 11111111 11111111	72,000,000,000,000,000
57-bit	2^{57} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 1	144,000,000,000,000,000
58-bit	2^{58} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 11	288,000,000,000,000,000
59-bit	2^{59} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 111	576,000,000,000,000,000
60-bit	2^{60} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 1111	1,152,000,000,000,000,000

7.2 Integridad Básica y Autenticidad

- Tipos de Llaves Criptográficas.
  - Llaves simétricas: Pueden intercambiarse entre routers usando VPNs.
  - Llaves asimétricas: Usadas en aplicaciones HTTPs.
  - Firmas digitales: Usadas en conexiones a sitios seguros.
  - Llaves hash: Usadas en la generación de otras llaves.

  - El tiempo para que un atacante pueda encontrar la llave correcta, dependerá del poder de cómputo al que tenga acceso, pero más de la longitud de llave.

Protección	Llave simétrica	Llave asimétrica	Firma digital	Hash
A 3 años.	80 bits	1248 bits	160 bits	160 bits
A 10 años.	96 bits	1776 bits	192 bits	192 bits
A 20 años.	112 bits	2432 bits	224 bits	224 bits
A 30 años.	128 bits	3248 bits	256 bits	256 bits
Contra computo quántico.	256 bits	15424 bits	512 bits	512 bits

7.2 Integridad Básica y Autenticidad

- Elección de Llaves Criptográficas.
  - El procesamiento requerido por un algoritmo criptográfico, es directamente exponencial a la longitud de llave.
    - Algunos algoritmos (RSA), corren lento ante llaves largas.
    - Importante encontrar balance.
    - Evaluar riesgo, estimar recursos, y tiempo que se requiere proteger la información.
      - Romper DES en 2 minutos, requiere computadora de 1 millón de dólares.
        - El valor de la información cifrada con DES debe valer menos que los recursos empleados para obtenerla.
        - De lo contrario, utilizar otro algoritmo.

Llave Corta → Procesamiento Corto

Llave Larga → Procesamiento Largo

7.3 Confidencialidad

- Dos Clases de Algoritmos de Encriptación.
  - Antiguamente se consideraba seguridad a la secrecía del algoritmo empleado.
  - Actualmente todos los algoritmos son públicos → Proteger Llaves.

  - Dos tipos de Algoritmos de Encriptación:
    - Simétricos.
      - Uso de una misma llave pre-compartida para encriptar/desencriptar.
      - Dada la secrecía de la llave se pueden usar llaves cortas / rápidas.
    - Asimétricos.

Simétricos	Asimétricos
Algoritmos de llave-compartida.	Algoritmos de llave pública.
Longitudes de llave de 80 – 256 bits	Longitudes de llave de 512 – 4096 bits
Emisor y receptor conocen la llave secreta.	Emisor y receptor no conocen la llave secreta.
Algoritmos relativamente rápidos.	Algoritmos relativamente lentos.
Ejemplos: DES, 3DES, AES, IDEA, RC2/4/5/6, BlowFish	Ejemplos: RSA, ElGamal, Elliptic Curves, DH

7.3 Confidencialidad

- Encriptación Simétrica.
  - Algoritmos basados en operaciones matemáticas simples.
  - La administración de llaves puede ser un desafío.
    - Emisor y receptor deben conocer la llave secreta (encriptar/desencriptar)
      - Intercambiar por medio seguro.
      - Cualquiera que posea la llave, podrá desencriptar.
  - Ejemplos:

Symmetric Encryption Algorithm	Key Length (in bits)
DES	56
3DES	112 and 168
AES	128, 192, and 256
Software Encryption Algorithm (SEAL)	160
The RC series	RC2 (40 and 64) RC4 (1 to 256) RC5 (0 to 2040) RC6 (128, 192, and 256)

7.3 Confidencialidad

- Cifrados de Bloque y Cifrados de Flujo Simétricos.
  - Técnicas mas utilizadas en el cifrado simétrico.
    - Cifrados de Bloque:
      - Transforma un bloque de Texto-Plano (tamaño fijo) en un bloque de Texto-Cifrado (64 – 128 bits) (Si no se llena el último bloque se rellena con ceros).
      - DES utiliza bloques de 64 bits.
      - AES bloques de 128 bits.

    - Cifrado de Flujo:
      - Encriptan Texto Plano en un byte o bit a la vez (Bloque de un byte o bit).
      - Vigenère.
      - A5 (GSM)
      - RC4
      - DES

7.3 Confidencialidad

- Elección de un Algoritmo de Encriptación.

	DES	3DES	AES
Algoritmo confiable por la comunidad criptográfica.	Reemplazado por 3DES	Si	En Evaluación
Adecuado contra ataques por fuerza bruta.	No	Si	Si

  - Otros criterios a considerar.
    - El algoritmo soporta llaves largas de longitud variable y escalabilidad.
      - A llaves mas largas, mas difícil de romper.
      - Escalabilidad permite elegir que tan seguro y rápido encriptar.
    - El algoritmo no tiene restricciones de importación / exportación.
      - Algunos países no permiten exportar algoritmos de encriptación, o la admiten solo con llaves cortas.
      - Algunos países imponen restricciones para importar algoritmos de encriptación.

7.3 Confidencialidad

- Encriptación Simétrica DES.
  - Estandarizado en 1976
  - Velocidad media.
  - Puede ser roto en 6.4 días asumiendo 255 intentos por segundo.
  - Consumo de recursos medio:
    - Secuencia de permutaciones y sustituciones de bits de datos, combinados con la llave de encriptación.
  - Llave de longitud fija (64 bits):
    - 56 bits para encriptación.
    - 8 bits para verificación de paridad.
    - El bit menos significativo de cada byte indica paridad impar.
    - Encriptación débil de 40 bits.
      - 40 bits secretos + 16 bits públicos = 56 bits

7.3 Confidencialidad

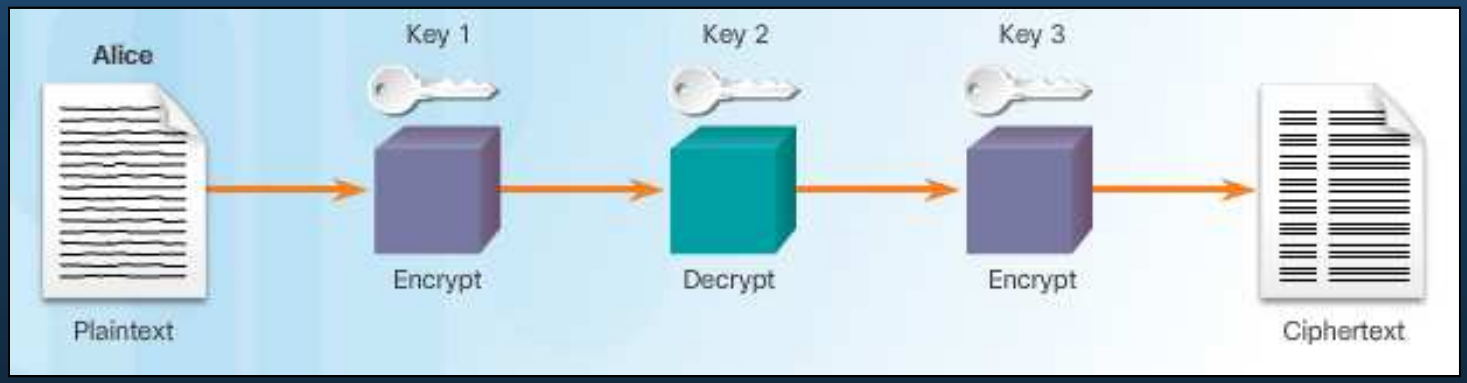
- Resumen DES.
  - Descontinuado, no se debería utilizar.
    - Utilice 3DES o AES siempre que estén disponibles.
  - Si no hay nada mejor:
    - Cambiar llaves frecuentemente.
    - Use un canal seguro para intercambiar llaves.
    - Use el modo CBC (Cipher Block Chaining): La encriptación de cada bloque de 64 bits depende del bloque previo.
    - Verifique que las llaves no sean débiles:
      - 4 llaves débiles
      - 12 semi-débiles

7.3 Confidencialidad

- Mejora de DES → 3DES.
  - Uso del algoritmo DES con diferentes llaves varias veces seguidas.
  - Considerado como no factible de romper.
  - Estandarizado en 1977.
  - Llaves de 112 y 168 bits.
  - Velocidad baja.
  - Tiempo de ruptura: 4.6 billones de años (255 intentos por segundo).
  - Consumo de recursos medio.

7.3 Confidencialidad

- Operación de 3DES.
  - Método Encripta-Desencripta-Encripta (EDE).
    - Utiliza los primeros 56 bits de la llave (k1) y Encripta el mensaje (DES).
    - Utiliza los segundos 56 bits como llave (k2) y Desencripta el mensaje (DES).
    - Utiliza los terceros 56 bits de la llave (k3) y Encripta el mensaje (DES).



    - Mas efectivo que encriptar 3 veces seguidas.
  - Para des-encriptar el mecanismo es inverso
    - Desencripta-Encripta- Desencripta (DED – k3,k2,k1) .
  - Seguro, pero intensivo en cálculos y uso de recursos.
    - AES es tan seguro como 3DES pero más rápido.

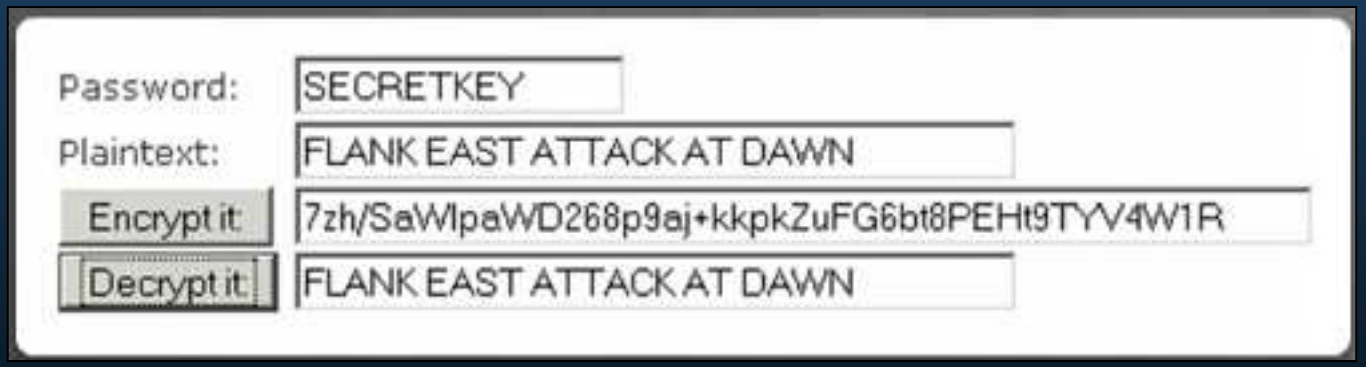
7.3 Confidencialidad

- Orígenes de AES.
  - 1997, Iniciativa AES, busca algoritmo para reemplazar DES.
  - De entre 15 competidores, se elige al cifrado de bloque Rijndael para AES.
    - Autores: Joan Daemen y Vincent Rijmen
    - Longitud de bloque y llave, variables
    - AES incluye solo algunas de las características del cifrado Rijndael:
      - Longitudes de bloque y llave en múltiplos de 32.
      - Versión eficiente.
      - No tan probado como 3DES.
  - Estándar Oficial desde 2001.
  - Algoritmo Simétrico.
  - Tamaños de Llave: 128, 192, y 256 bits.
  - Velocidad alta
  - Tiempo de ruptura: 149 trillones de años (255 intentos por segundo).
  - Consumo de recursos bajo.

7.3 Confidencialidad

- Resumen AES.
  - Llaves mas fuertes que DES.
  - Más rápido que 3DES.
  - Mas reciente que 3DES.

  - En criptografía, se considera mas confiable un algoritmo mientras mas maduro sea.



  - Probar: http://aesencryption.net/

7.3 Confidencialidad

- Algoritmo de Encriptación Optimizado por Software (SEAL).
  - Alternativa a 3DES y AES.
  - Diseñado por Phillip Rogaway y Don Coppersmith (1993).
  - Llaves de 160 bits
  - Cifrado de Flujo.
  - Más rápido que cifrados de bloque.

  - Versión actual (1997): 3.0
  - Algoritmo simétrico.
  - Velocidad rápida.
  - Tiempo de ruptura desconocido (muy seguro).
  - Consumo de recursos bajo.

7.3 Confidencialidad

- Algoritmos RC.
  - Diseñados por Ronald Rivest (Autor del MD5).

Algoritmo RC	Línea de Tiempo	Tipo de Algoritmo	Tamaño de Llave en bits
RC2	1987	Bloque	40 y 64
RC4	1987	Flujo	1 – 256
RC5	1994	Bloque	0 – 2048
RC6	1998	Bloque	128, 192 ó 256

  - En general se consideran débiles y deben ser evitados.

  - RC2 → Intento de reemplazo para DES.
  - RC4 → WEP.
  - RD5 → Reemplazo para DES.
  - RC6 → Finalista AES.

7.3 Confidencialidad

- Algoritmo Diffie-Hellman (DH).
  - Algoritmo asimétrico diseñado por Whitfield Diffie y Martin Hellman (1976).
    - Base de todos los mecanismos de intercambio de llaves actuales.
    - Base para los sistemas simétricos.
    - Similar a algoritmos asimétricos en uso de dos tipos de llaves: pública, privada.
  - Permite a dos equipos generar la misma llave privada, sin comunicarse.
  - Realiza cálculos con números muy grandes Vgr; 1024bits → 309 cifras decimales.
  - Utilizado en IPSec y VPNs, SSL/TSL
  - Su lentitud hace que en práctica se use para generar llaves a usar con AES o 3DES.
  - Tamaño de Llaves: 512, 1024, 2048, 3072, 4096 bits
  - Velocidad lenta.
  - Tiempo de ruptura desconocido si llave >= 2048bits
  - Consumo de recursos medio.

7.3 Confidencialidad

- Operación DH.
  - Uso de operación aritmética módulo.

1. Acordar 2 números no secretos g y p.

   g - generador
   p - primo

2. Cada extremo genera un número secreto s.
   Alice → 6
   Bob → 15

3. Alice Calcula:
   ma = (g^s) % p.
   Y se lo envía a Bob

4. Bob Calcula:
   mb = (g^s) % p.
   Y se lo envía a Alice

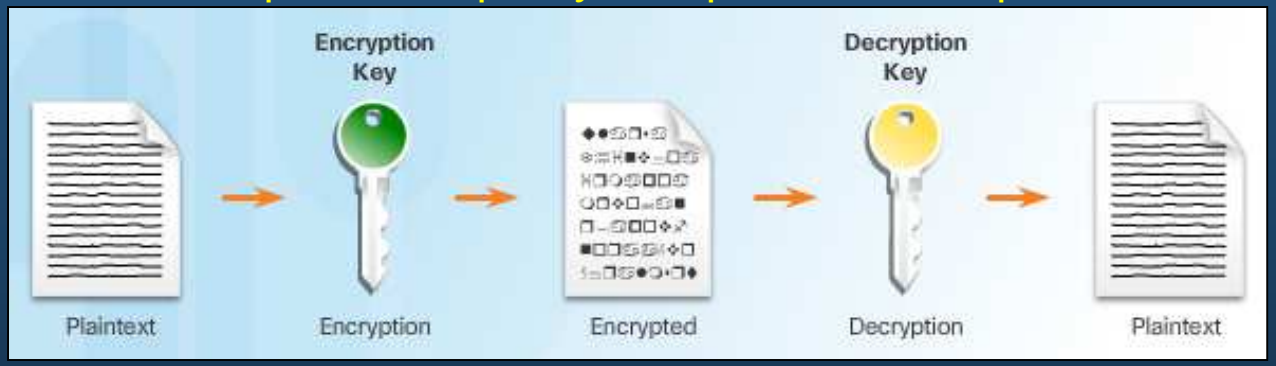
5. Alice repite el proceso utilizando mb en lugar de g

6. Bob repite el proceso utilizando ma en lugar de g

Ambos poseen un secreto compartido

7.4 Criptografía de Llave Pública

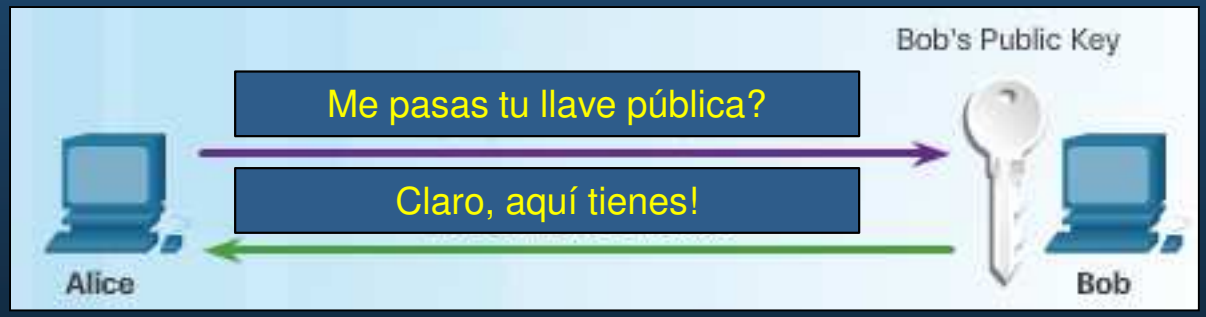
- Algoritmos de Llaves Asimétricas.
  - Utilizan una llave para encriptar y otra para desencriptar.

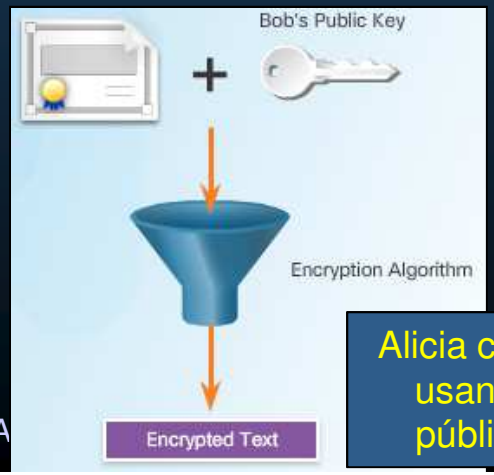


  - La llave para desencriptar no debe ser fácil de calcular a partir de la otra llave.
  - Generan pares de llaves que cumplan las siguientes características:
    - Llave Pública: Se envía al otro extremo para que cifre con ella los mensajes a enviar.
    - Llave Privada: Jamás se envía, se utiliza únicamente para desencriptar mensajes cifrados con llave pública.
  - Cualquiera puede enviar mensajes, solo el destinatario los puedo leer.
  - Utilizan longitudes de llaves de 512 a 4096 bits
  - Vgr; IKE (IPSec, VPNs), SSL (TLS), SSH, PGP

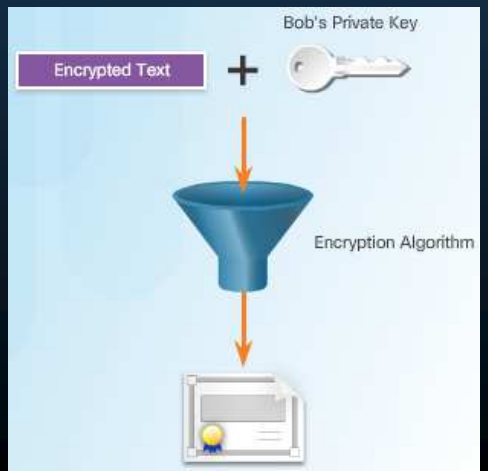
7.4 Criptografía de Llave Pública

- Confidencialidad con Llaves Publica y Privada.
  - Confidencialidad = Llave Pública (Encripta) + Llave Privada (Desencripta).
  - La confidencialidad radica en que solo el receptor conozca la llave privada.
  - Si la llave privada se ve comprometida, se debe generar un nuevo par.





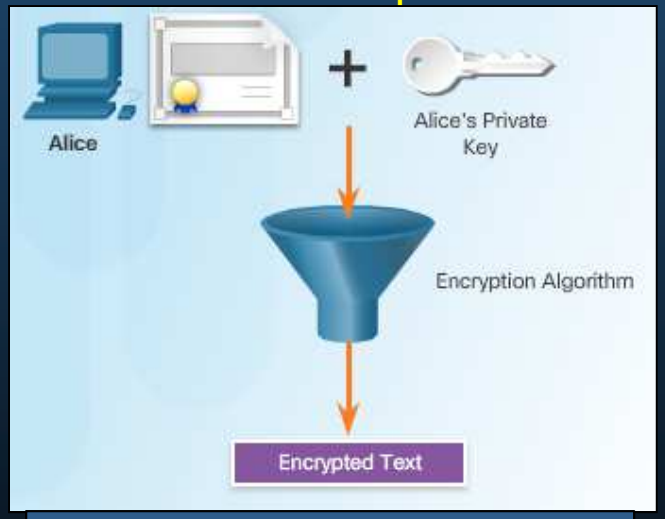
Alicia cifra mensaje usando la llave pública de Bob



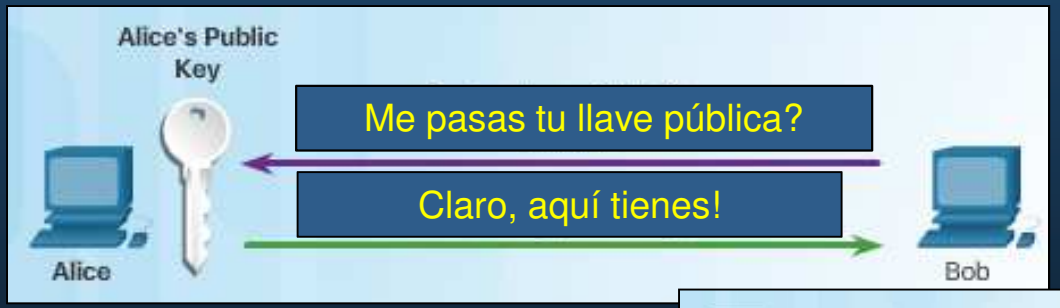
Solo Bob con su llave privada, puede re-generar el Texxto-Plano

7.4 Criptografía de Llave Pública

- Autenticación con Llaves Pública y Privada.
  - Autenticación = Llave Privada (Encripta) + Llave Pública (Desencripta).
  - La autenticación radica en que solo el emisor conozca la llave privada.
    - Cualquiera con la llave pública, podrá autenticar al emisor.
  - Si la llave privada se ve comprometida, se debe generar un nuevo par.



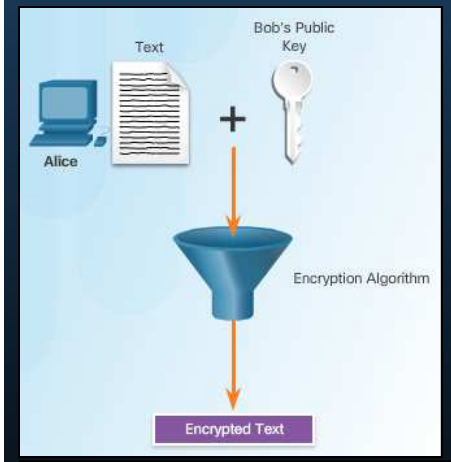
Alicia cifra mensaje usando su llave privada para envíar a Bob



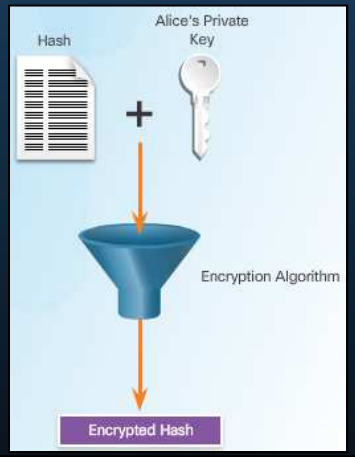
Bob verifica que el mensaje proviene de Alicia al obtener el texto-plano tras descifrar utilizando la llave pública.

7.4 Criptografía de Llave Pública

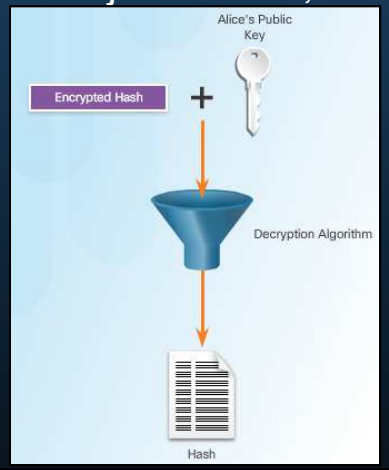
- Algoritmos Asimétricos.
  - Dos fases de encriptación necesarias para asegurar confidencialidad autenticación e integridad:
    1. Confidencialidad: Uso de la llave pública para encriptar / Solo llave privada podrá desencriptar.
    2. Autenticación e Integridad: Uso de llave privada para cifrar un hash del mensaje enviado / Cualquiera con la llave pública puede desencriptar y verificar, si el hash coincide con el calculado del mensaje recibido, se verifica integridad.



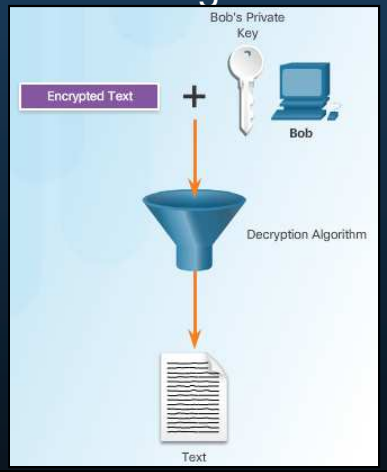
1. Alicia cifra mensaje usando la llave pública de Bob.



2. Alicia cifra Hash del mensaje previo usando su propia llave privada.



Bob usa la llave pública de Alicia para desencriptar el Hash



Bob usa su llave privada para desencriptar el mensaje de Alicia

Bob calcula el Hash del mensaje des-cifrado y compara con el Hash recibido.

7.4 Criptografía de Llave Pública

- Tipos de Algoritmos Asimétricos.

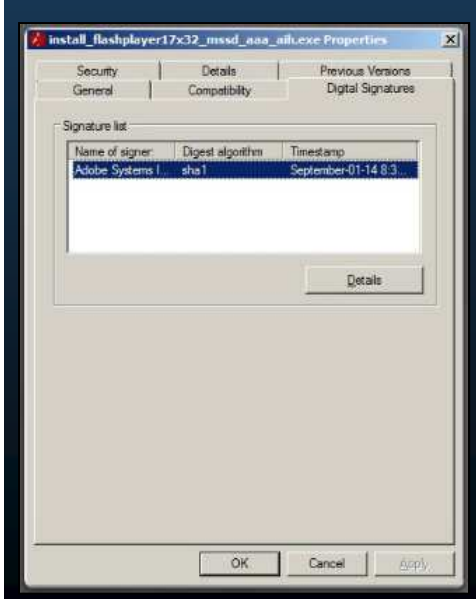
Algoritmo de Encriptación Asimétrica	Longitud de Llave (en bits)	Descripción.
DH	512, 1024, 2048, 3072, 4096	Algoritmo Diffie-Hellman, de llave pública, Whitfield Diffie y Martin Hellman (1976), Permite a dos entidades definir una llave en común. Asume que es fácil elevar un número a una potencia, pero difícil saber que exponente se utilizó dados el número y su potencia.
Estándar y Algoritmo de Firma Digital (DSA / DSS)	512 – 1024	DSS creado por NIST, especifica DSA para firmas digitales. Algoritmo de llave pública basado en ElGamal. Creación de firmas equiparable en velocidad a RCA; de 10 a 40 veces mas lento para verificar.
RSA	512 – 2048	Por Ron Rivest, Adi Shamir, Leonard Adleman en el MIT (1977). Algoritmo de llave pública. Se basa en la dificultad de factorizar números grandes. Usado tanto para firmar como para encriptar. Ampliamente utilizado. Seguro con llaves suficientemente largas.
ElGamal	512 – 1024	Algorítmo asímetrico para criptografía de llave pública, basado en DH. Por Taher ElGamal (1984). Usado en PGP. Desventaja, el mensaje encriptado se vuelve muy grande, casi al doble.
Técnicas de Curvas Elípticas	160	Por Neil Koblitz y Victor Miller (1980s). Pueden usarse para adaptarse a DH, ElGamal, etc. Ventaja de que las llaves pueden ser mas cortas.

7.4 Criptografía de Llave Pública

- Uso de Firmas Digitales.
  - Prueba de Autoría.
  - Técnica matemática para tres servicios básicos de seguridad:
    - Autenticidad: Prueba que se conoce la fuente que firma los datos.
    - Integridad: Garantiza que los datos no han sido alterados desde que se firmaron.
    - No-Repudiación: El receptor lleva datos y firmas a un tercero que certifica el intercambio (el emisor no podrá negar que envió esos datos).
  - Propiedades para autenticación de entidades e integridad de datos.
    - Autenticidad de firma. La firma no se debe poder alterarse.
    - No-Repudiable. Quién firme, no podrá negar que lo hizo.
    - No-Reutilizable. La firma es parte del documento, no podrá moverse a otro documento.
    - Inalterable. Un documento firmado, no podrá ser alterado.
  - Comúnmente usadas para:
    - Firma de códigos: verifica integridad de códigos ejecutables descargados.
    - Certificados digitales: autentica al dueño de un sitio web y cifra comunicación.

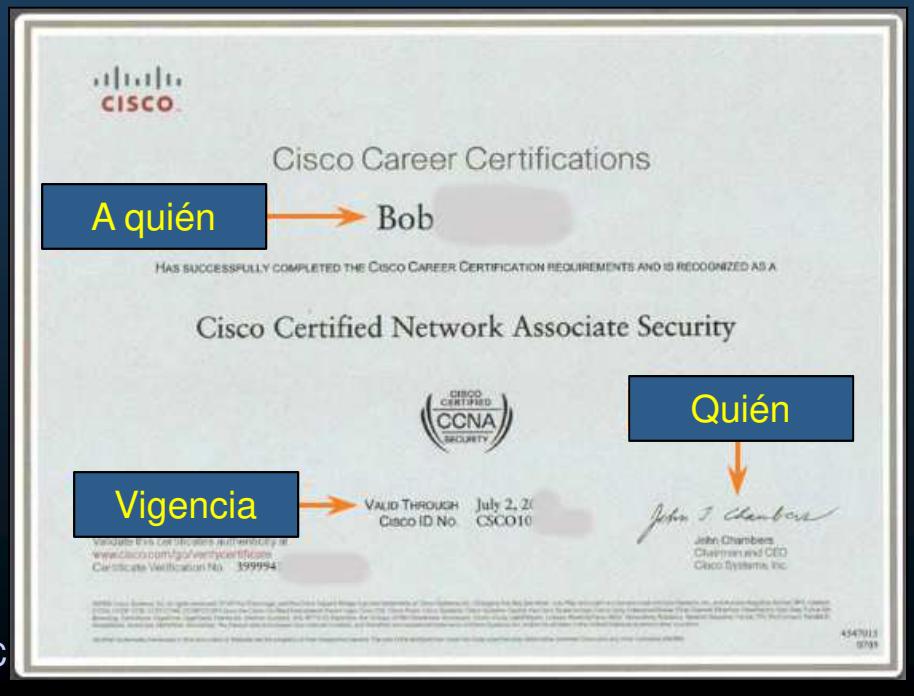
7.4 Criptografía de Llave Pública

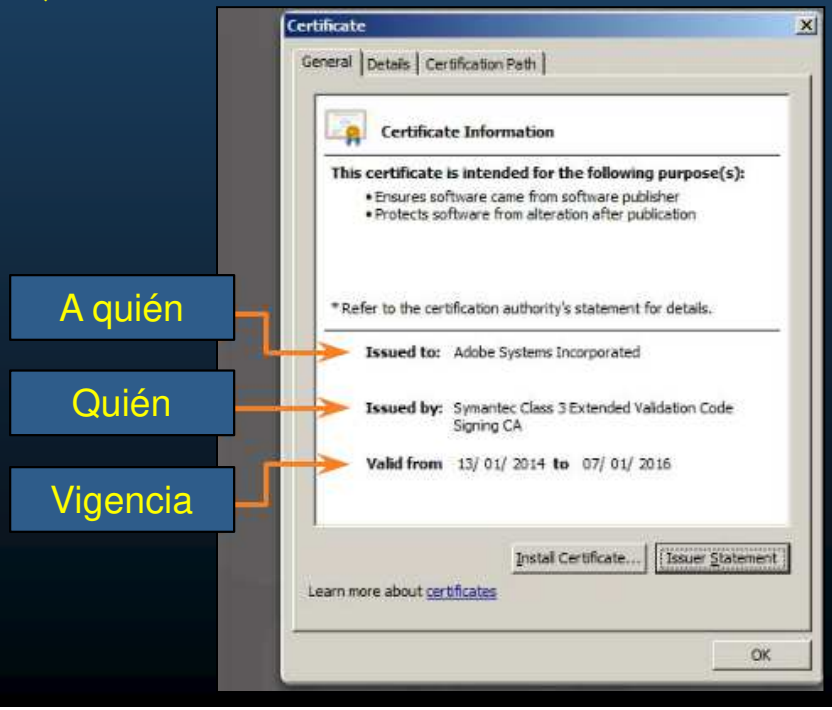
- Firma de Códigos.
  - Asegura autenticidad e integridad de ejecutables descargados de Internet.
    - Sobre con firma digital, que permite verificar firma antes de instalar.
  - Asegura:
    - El código es auténtico y provisto por el distribuidor oficial.
    - El código no ha sido modificado desde que el proveedor lo firmó.
    - El proveedor no puede negar haberlo publicado.



7.4 Criptografía de Llave Pública

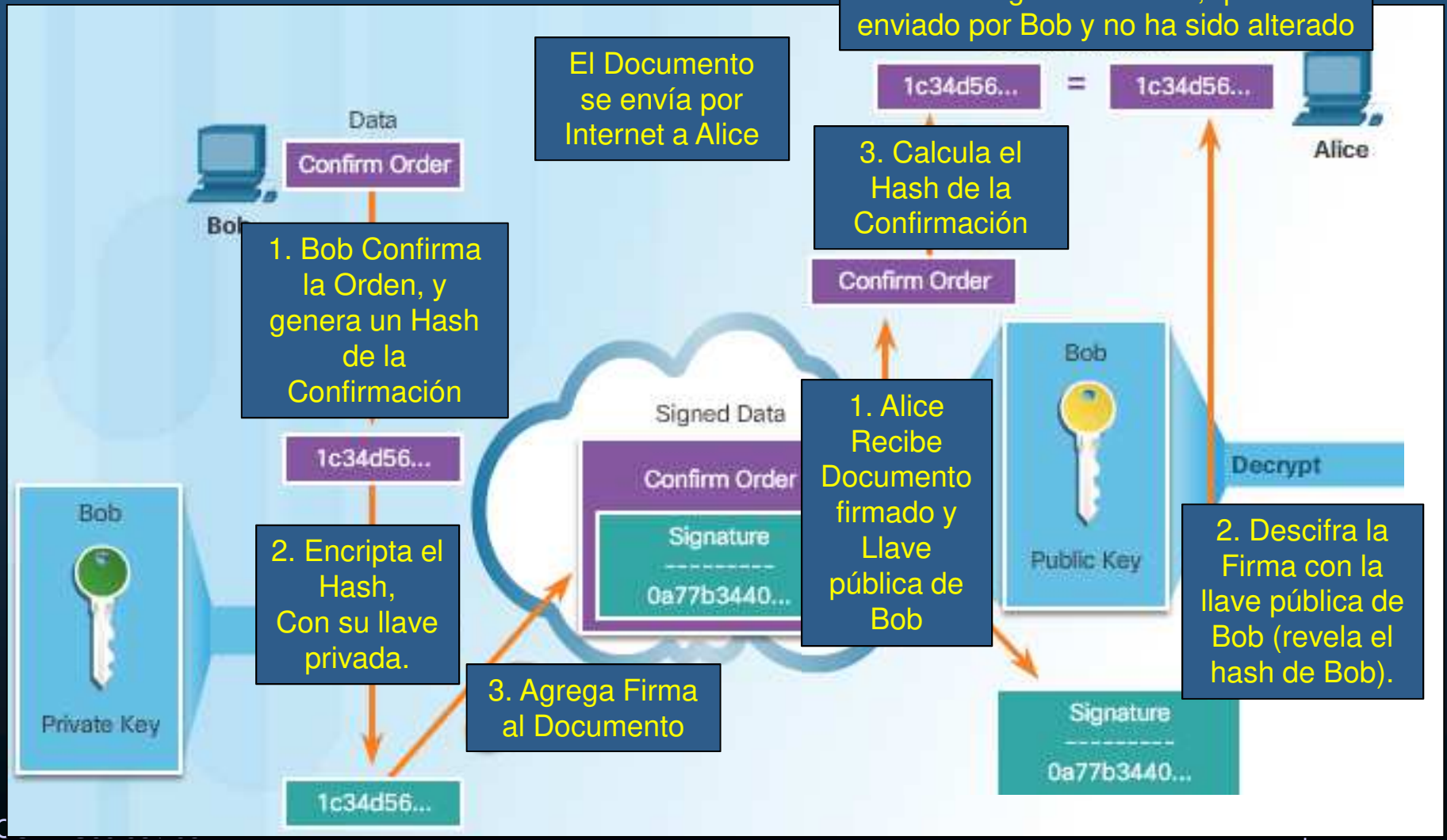
- Certificados Digitales.
  - Equivalente a un pasaporte electrónico.
  - Permiten intercambio seguro de información.
    - Verifica que un usuario es quien dice ser.
  - Similar a un documento de certificación:
    - A quién se certifica / Cuando, Vigencia / Quién lo certifica





7.4 Criptografía de Llave Pública

- Uso de Certificados Digitales.



7.4 Criptografía de Llave Pública

- Algoritmos de Firma Digital.
  - DSA (Algoritmo de Firma Digital)
    - Estándar original para generar y verificar firmas digitales.
    - 1994
    - Generación de firmas rápida
    - Verificación de firmas lenta
  - RSA (Algoritmo Rivest-Shamir Adelman).
    - Comúnmente utilizado para generar y verificar firmas.
    - 1977
    - Verificación de firmas rápida
    - Generación de firmas lenta
  - ECDSA (Algoritmo de Firma Digital por Curvas Elípticas).
    - Nueva variante de DSA computacionalmente eficiente.
    - Firmas pequeñas / Bajos consumo de ancho de banda.

7.4 Criptografía de Llave Pública

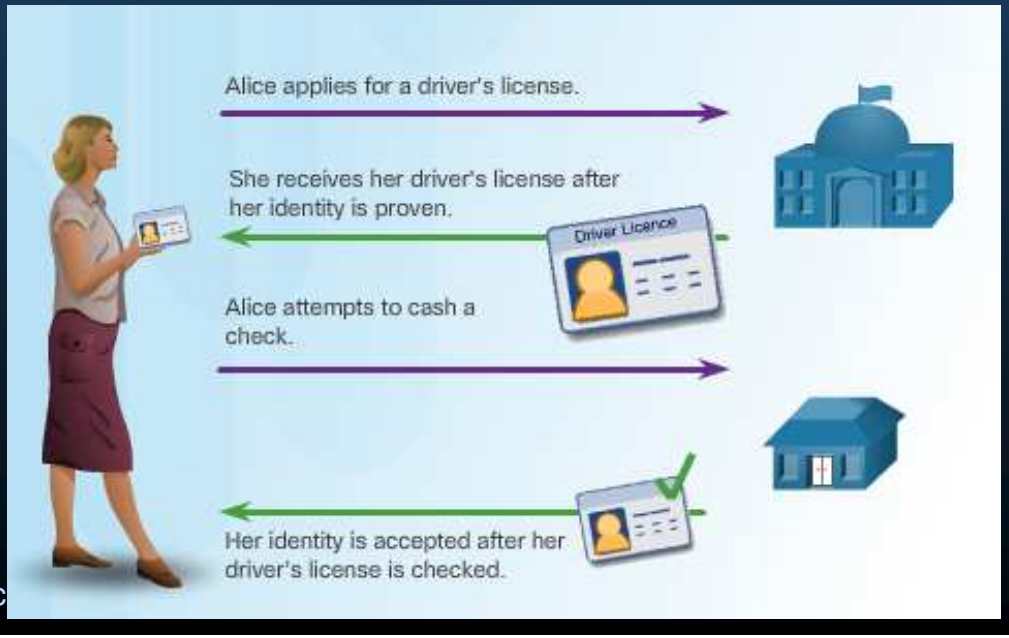
- Software de Cisco Firmado Digitalmente.
  - El Estandar de Procesamiento de Información Federal (FIPS) del Gobierno de los Estados Unidos especifica firmar y verificar el software.
  - Cisco Firma sus imágenes de IOS.
    - Se reconoce por la subcadena `SPA` en su nombre de IOS.
      - Vgr; `c1900-universalk9-mz.SPA.154-3.M2.bin`
      - S: Signed - P: Production - A: Versión de la Llave
    - Verificación de firma digital en router ISR:

No disponible en PacketTracer

```
R1# show software authenticity file flash:c1900-universalk9-mz.SPA.154-3.M2.bin
File Name                       : flash:c1900-universalk9-mz.SPA.154-3.M2.bin
Image type                      : Production
    Signer Information
        Common Name             : CiscoSystems
        Organization Unit       : C1900
        Organization Name       : CiscoSystems
    Certificate Serial Number : 54D56496
    Hash Algorithm              : SHA512
    Signature Algorithm         : 2048-bit RSA
    Key Version                 : A

R1#
```

7.4 Criptografía de Llave Pública

- Introducción a la Infraestructura de Llave Pública (PKI).
  - El intercambio de credenciales particulares en internet resulta impráctico.
  - Se confía en un tercero neutral para validar identidades de las partes.
    - Realiza Investigación exhaustiva de las partes.
    - Emite credenciales difíciles de forjar.
  - Si se confía en el tercero (autoridad de certificación), se confiará en las identidades de todas sus credenciales emitidas.



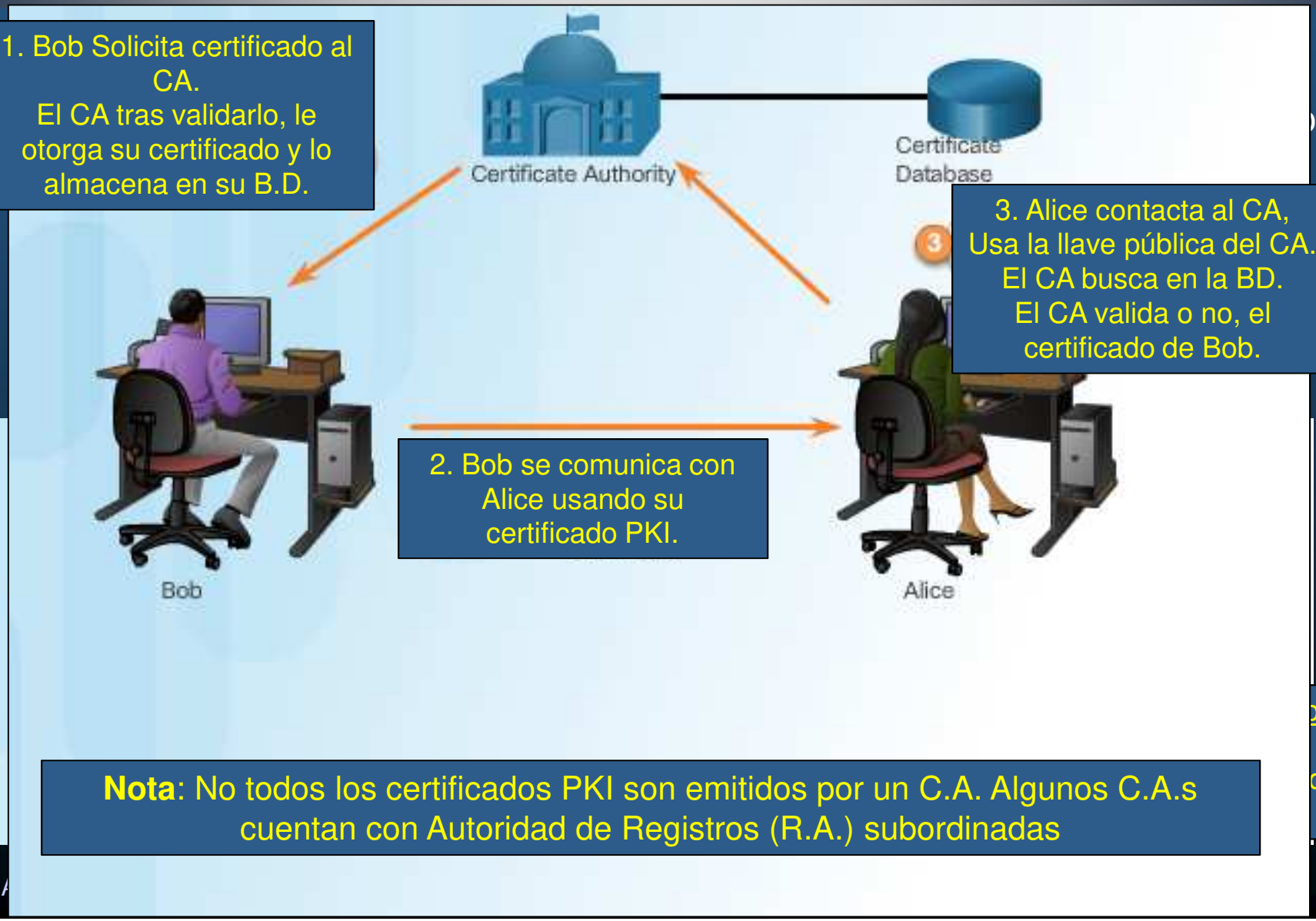
Alicia solicita licencia de conducir, debe acreditar su identidad.

Tras validar identidad de Alicia y aprobar evaluaciones, recibe su licencia.

Alicia va al Banco a retirar efectivo, y presenta su licencia como ID.

El Banco confía en el gobierno (otorga licencias) y acepta como válida la ID de Alicia.

7.4 Criptografía de Llave Pública



Nota: No todos los certificados PKI son emitidos por un C.A. Algunos C.A.s cuentan con Autoridad de Registros (R.A.) subordinadas

7.4 Criptografía de Llave Pública

- Autoridades Certificadoras.
  - Empresas ofrecen servicios de certificación como productos.
    - Symantec Group (VeriSign), Comodo, Go Daddy Group, GlobalSign, DigiCert, etc.
  - Clases de confiabilidad de un certificado:

Clase	Descripción
0	Para pruebas donde no se realizan verificación alguna.
1	Para Individuos con un enfoque, verificación por e-mail.
2	Para Organizaciones, requieren prueba de identidad.
3	Para Servidores y firmado de software independiente, verificación realizada por la C.A.
4	Para negocios en línea o transacciones entre compañías.
5	Para organizaciones privadas o seguridad gubernamental.

  - Nota: Una empresa puede implementar infraestructura PKI para autenticar empleados que accedan la red. La empresa misma funge como C.A.

7.4 Criptografía de Llave Pública

- Interoperabilidad entre PKIs de diferentes Marcas.
  - Proveedores C.A. implementan soluciones propietarias antes del estándar.
  - IETF formó el grupo PKI X.509 (PKIX) para estandarizar PKIs en Internet.
    - Marco de Trabajo para Prácticas de Certificación (RFC2527).
    - Política de Certificados PKI X.509
      - Define formatos básicos PKI para certificados y listas de revocación (CRL).
      - V3 define el formato de un certificado digital.
      - Extensamente utilizado en Internet.
      - Servidores y clientes web usan X.509v3 para autenticación web por SSL/TSL
      - VPNs IPSec usan X.509 al usar certificados como llave pública.
      - Agentes de correo que usan la Extensión de Correo de Internet Multipropósito Seguro (S/MIME) usa X.509
      - Los switches cisco, pueden usar certificados para autenticar hosts conectados a sus puertos mediante un Protocolo de Autenticación Extendida (EAP) y TLS.

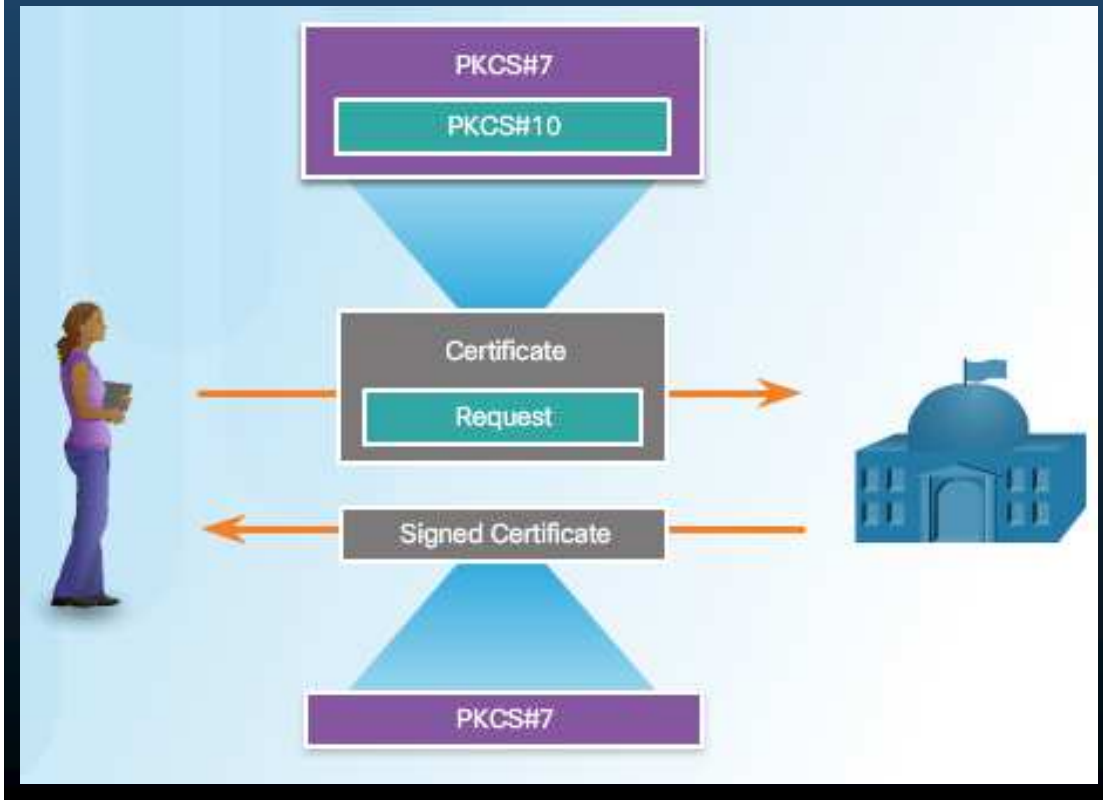
7.4 Criptografía de Llave Pública

- Estándares de Criptografía de Llave Pública (PKCS).
  - Por los Laboratorios RSA.
    - En colaboración con desarrolladores de diferentes marcas.
    - Proporciona interoperabilidad básica.
    - Define formatos de bajo nivel para el intercambio de datos seguro .
    - Buscan acelerar el desarrollo de Criptografía de Llave Pública.

Principales Estándares RSA PKCS
PKCS #3: Estándar de Acuerdo de Llaves DH
PKCS #5: Estándar de Criptografía Basada-en-Contraseña
PKCS #6: Estándar de Sintaxis de Certificados-Extendidos
PKCS #7: Estándar de Sintaxis de Mensajes Criptográficos
PKCS #8: Estándar de Sintaxis de Información de Llave-Privada
PKCS #10: Estándar de Sintaxis de Solicitud de Certificación
PKCS #12: Estándar de Sintaxis de Intercambio de Información Personal
PKCS #13: Estándar de Criptografía de Curvas Elípticas
PKCS #15: Estándar de Formato de Información de Token Criptográfico

7.4 Criptografía de Llave Pública

- Protocolo de Enrolamiento de Certificado Simple (SCEP).
  - Debido al gran uso de certificados PKI, se vuelve necesario un protocolo de administración de certificados, con aplicaciones cliente y servidor.
  - Principales operaciones: Enrolamiento, Revocación, Acceso a CRLs.



1. Un cliente genera un PKCS #10, para iniciar el proceso de enrolamiento

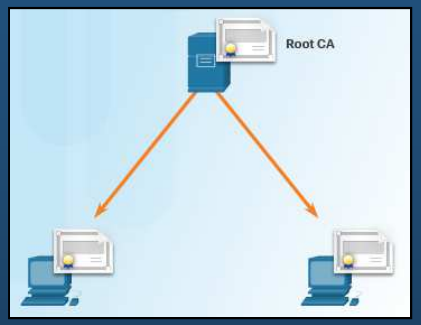
2. Se Encapsula el PKCS #10, en un PKCS #07 (Sintaxis de mensaje criptográfico)

3. Cuando el C.A. (servidor) recibe el mensaje, puede:
   - Aprobar la solicitud
   - **Responder con el certificado.**
   - Indicar esperar autenticación manual.

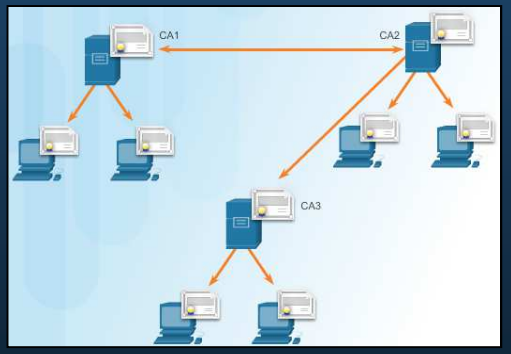
La IETF implementó el SCEP para automatizar y hacer escalable el proceso.

7.4 Criptografía de Llave Pública

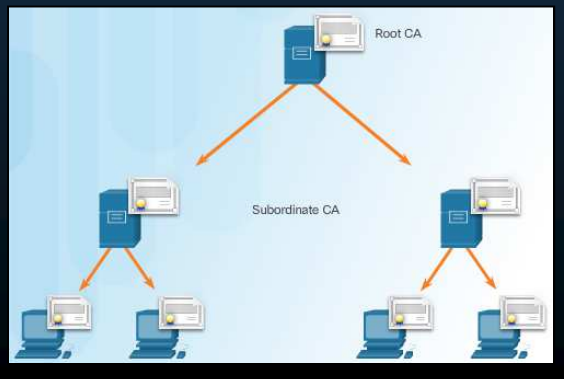
- Topologías PKI.
  - Topología PKI de raíz simple.
    - Un solo CA raíz envía certificados a usuarios finales.
    - Simplicidad de implementación.
    - Dificultad para escalar (único punto de falla).



  - Topología CA con Certificación Cruzada.
    - Modelo Par-a-Par.
    - CAs individuales establecen relaciones de confianza por certificación cruzada.
    - Cada dominio CA confía en los otros.



  - Topología CA Jerárquica.
    - CA raíz certifica subordinados.
    - Sub-CAs certifican sub-dominios.
    - CA raíz establece comunidad de confianza.
    - Incrementa escalabilidad y administración.
    - Difícil determinar cadena de firmados.

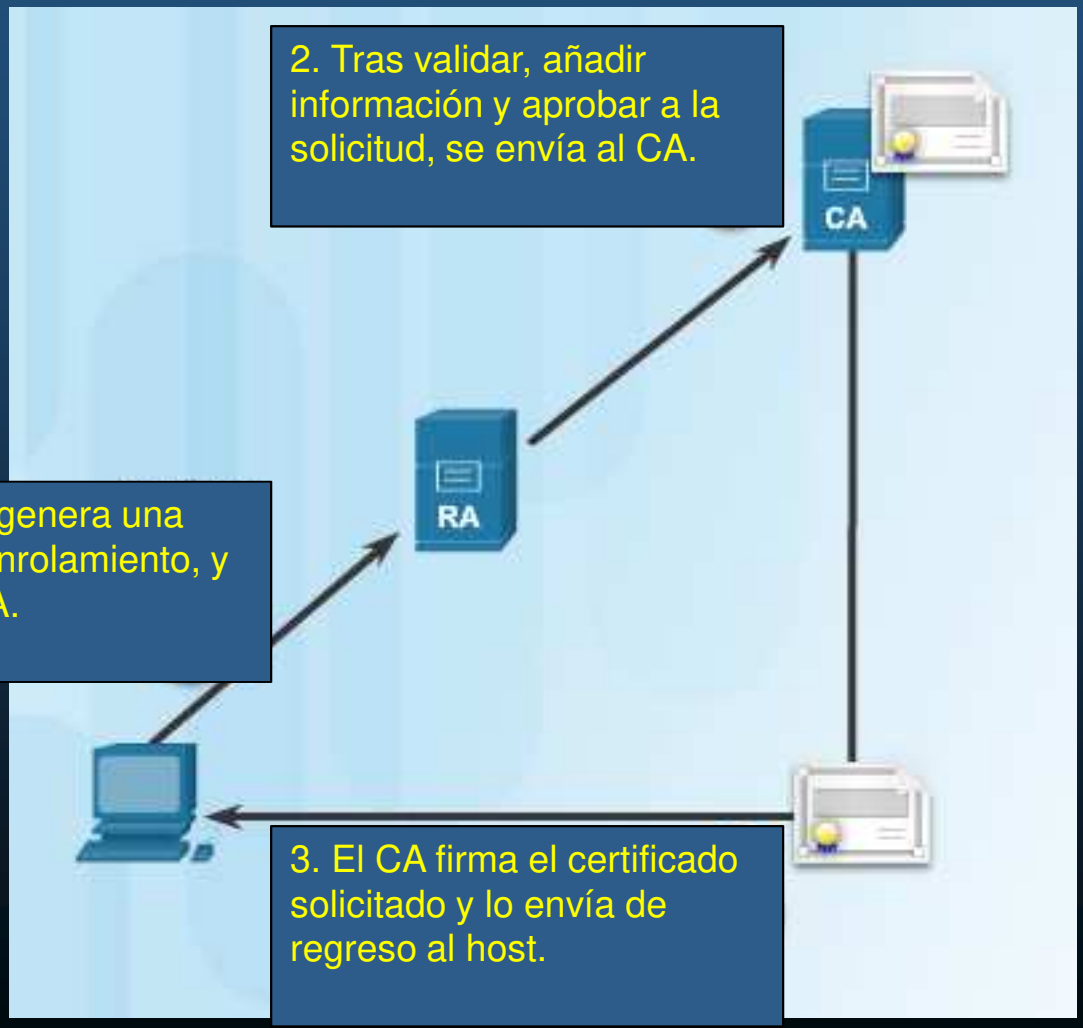


7.4 Criptografía de Llave Pública

- Autoridad de Registro.
  - En una Topología CA Jerárquica, un RA puede aceptar solicitudes de enrolamiento.
    - Ayuda a reducir la carga de los Acs.
    - Responsable de autenticar e identificar suscriptores.
    - No firma ni emite certificados.
    - Realiza tres tareas:
      - Autentica usuarios cuando se enrolan por PKI.
      - Genera llaves para usuarios que no pueden generar los usuarios mismos
      - Distribuye certificados después del enrolamiento.
  - Un RA no emite certificados ni publica CRLs.
    - El CA es responsable de dichas acciones.

7.4 Criptografía de Llave Pública

- Autoridad de Registro.

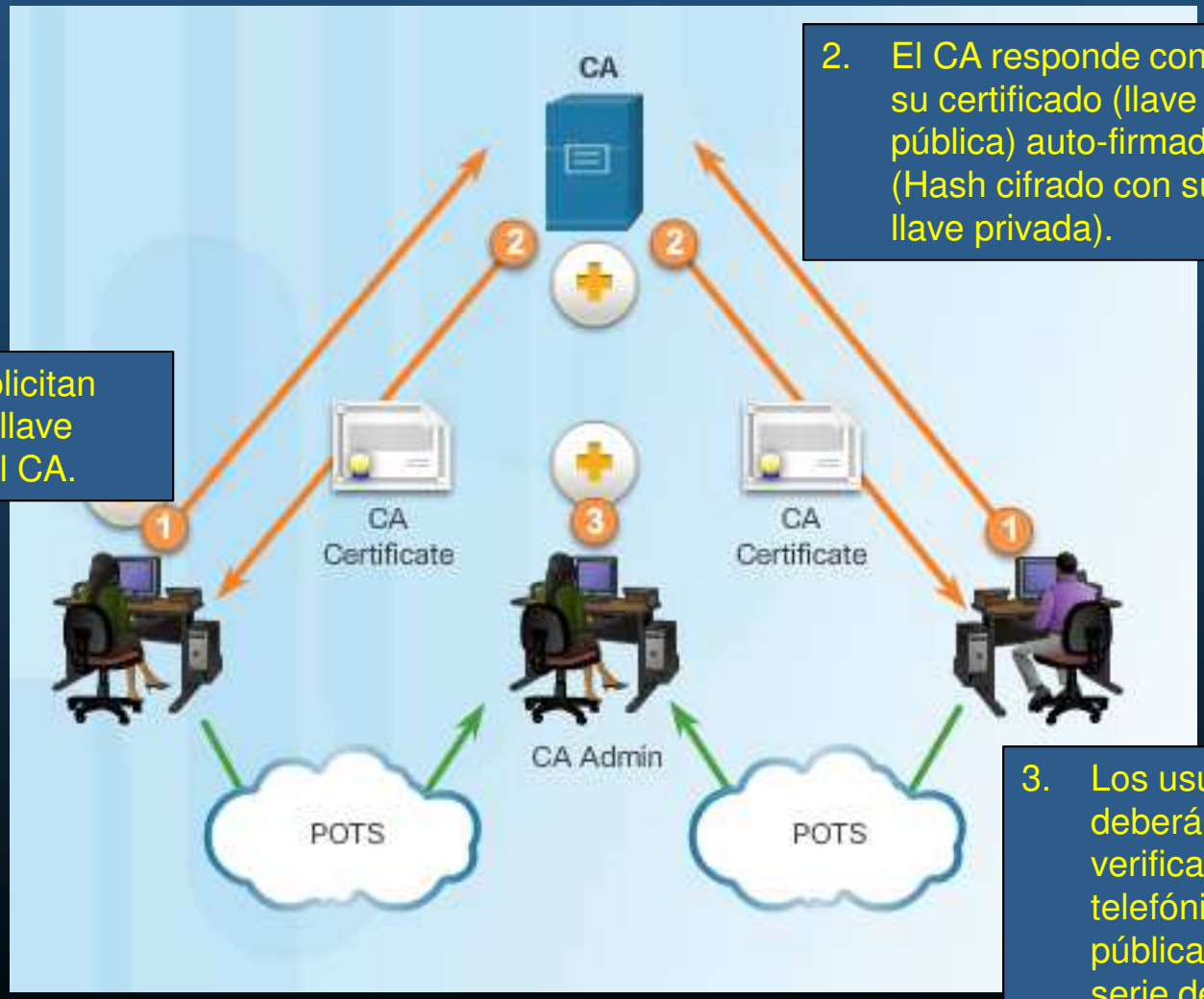


7.4 Criptografía de Llave Pública

- Certificados Digitales y CAs.
  - Obtener de manera segura la llave publica del CA.
    - Servirá para verificar los certificados emitidos por el CA.
    - Certificado auto-firmado (solo CA raíz puede autofirmarse).
    - Los certificados se obtienen en línea por la red.
    - La autorización se realiza vía telefónica fuera de línea.
  - Solicitar Certificados al CA.
    - Enviar solicitud de certificado, incluyendo llave pública (solicitante) y datos de identificación.
    - Cuando CA recibe las solicitudes de certificado, llama al usuario para confirmar su clave pública. Agrega datos a la solicitud, lo firma y emite el certificado.
    - Recuperar manualmente el certificado o automáticamente mediante SCEP.
  - Autenticarse entre usuarios usando certificados.
    - Con certificados emitidos por el mismo CA.
    - La autenticación no requiere la presencia del CA
    - Usuarios intercambian certificados de llave pública.

7.4 Criptografía de Llave Pública

- Certificados Digitales y CAs.



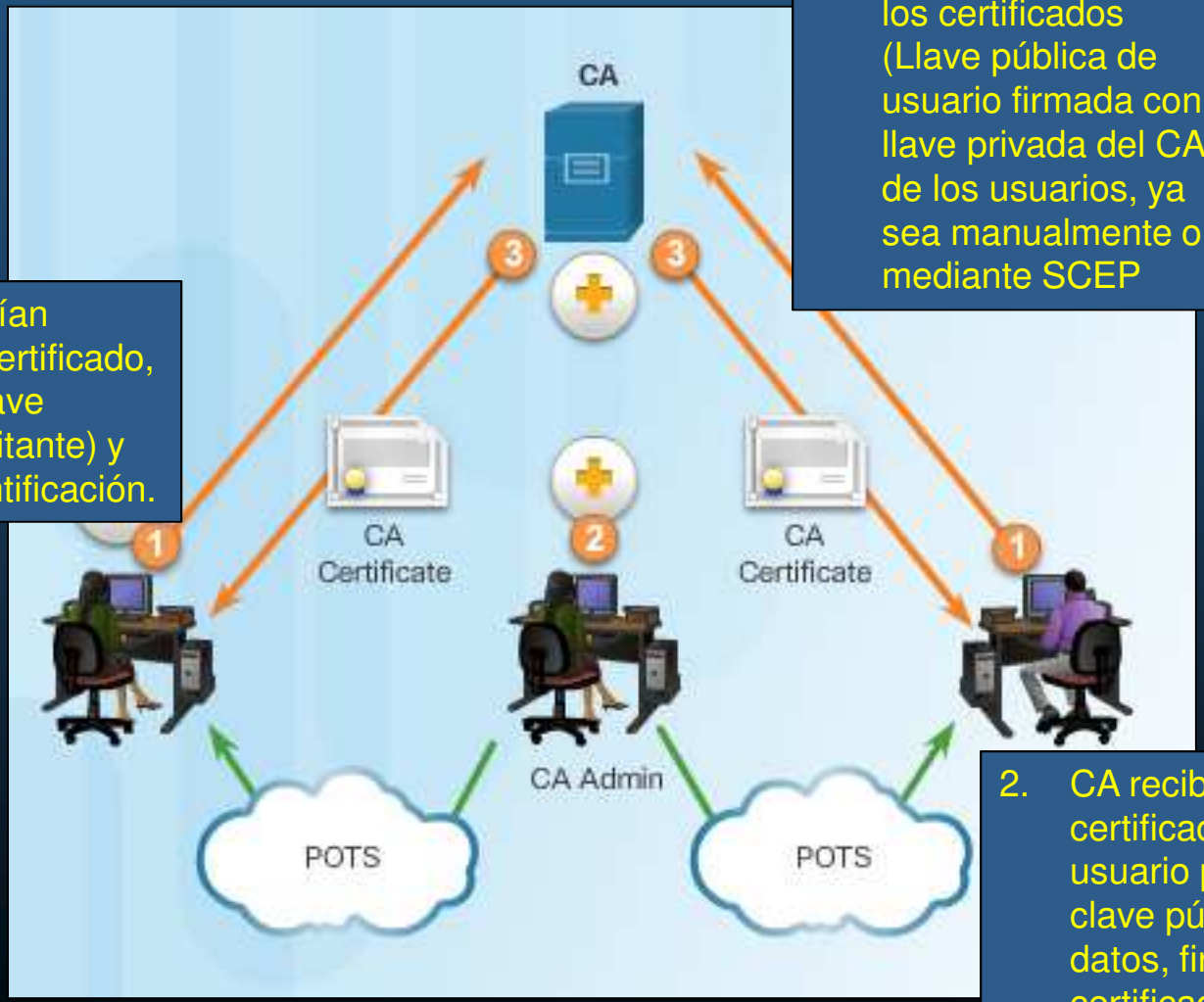
1. Usuarios solicitan certificado (llave pública), del CA.

2. El CA responde con su certificado (llave pública) auto-firmado (Hash cifrado con su llave privada).

3. Los usuarios deberán realizar una verificación telefónica de la clave pública y número de serie del certificado.

7.4 Criptografía de Llave Pública

- Certificados Digitales y CAs.



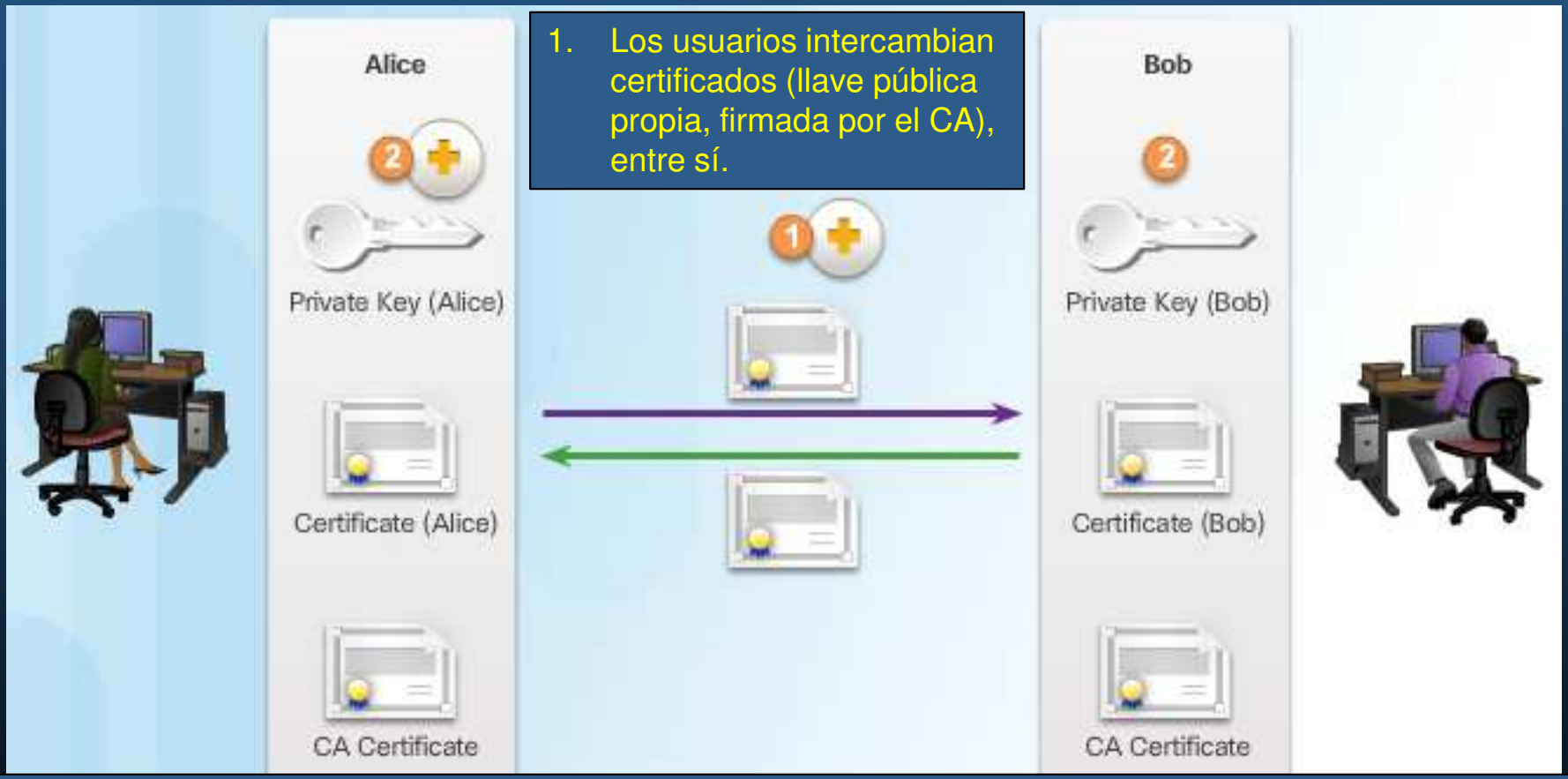
1. Usuarios envían solicitud de certificado, incluyendo llave pública (solicitante) y datos de identificación.

3. El CA responde con los certificados (Llave pública de usuario firmada con llave privada del CA) de los usuarios, ya sea manualmente o mediante SCEP

2. CA recibe solicitudes de certificado, llama al usuario para confirmar clave pública, agregar datos, firmar y emitir el certificado

7.4 Criptografía de Llave Pública

- Certificados Digitales y CAs.



2. Cada usuario verifica la firma digital
   Compara Hash del texto plano del certificado (llave pública del usuario remoto) con el resultado de de-encriptar la firma con la llave pública del CA.
   Si coinciden, CA certifica que el mensaje lo emitió el Usuario que afirma haberlo hecho.

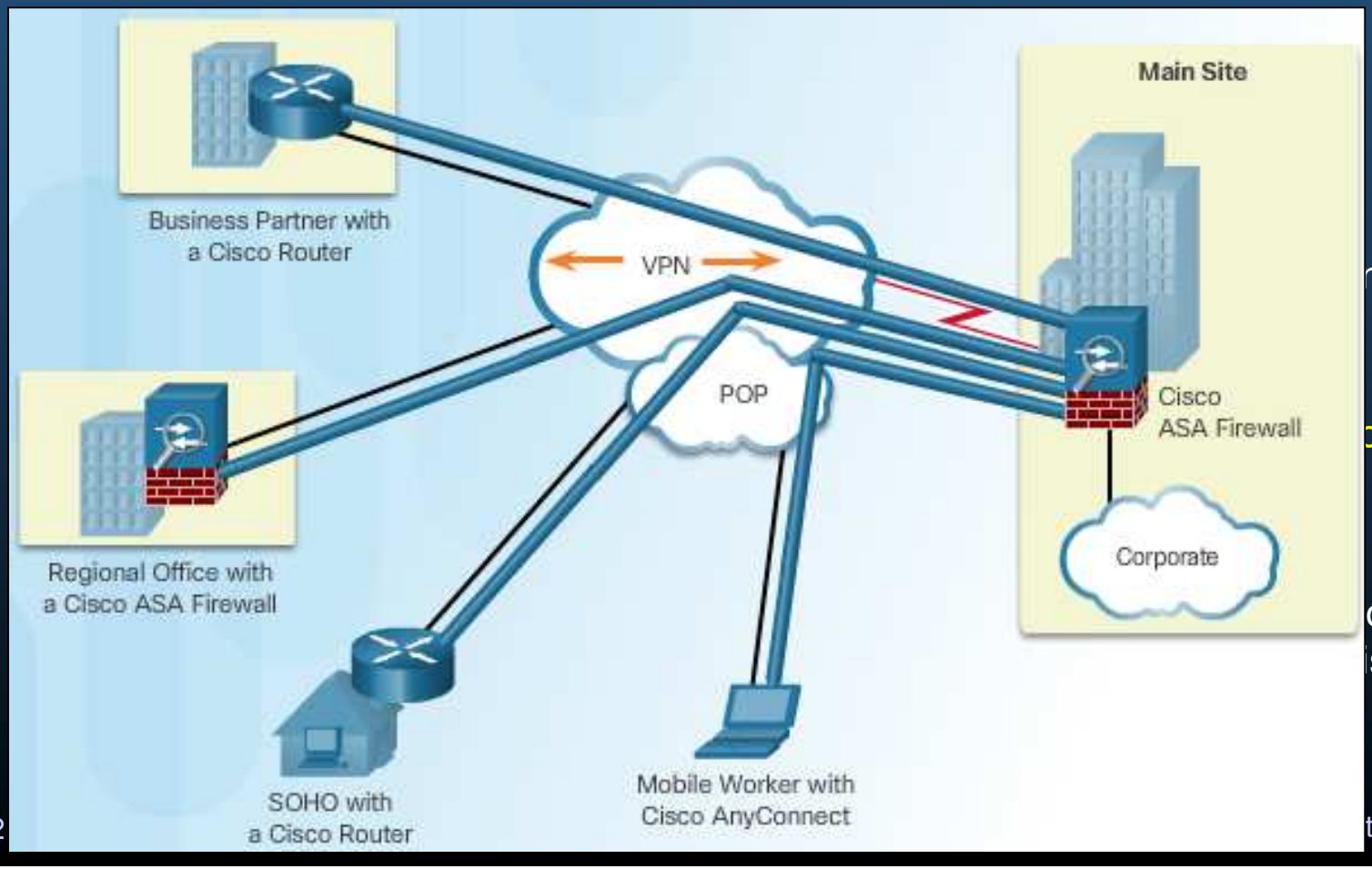
Capítulo 8

Implementación de VPNs

https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#8.1.1.1

8.1 VPNs

- Introducción.
  - Una Red Privada Virtual (VPN), utiliza conexiones enrutadas por Internet para simular una red local y segura entre sitios remotos.



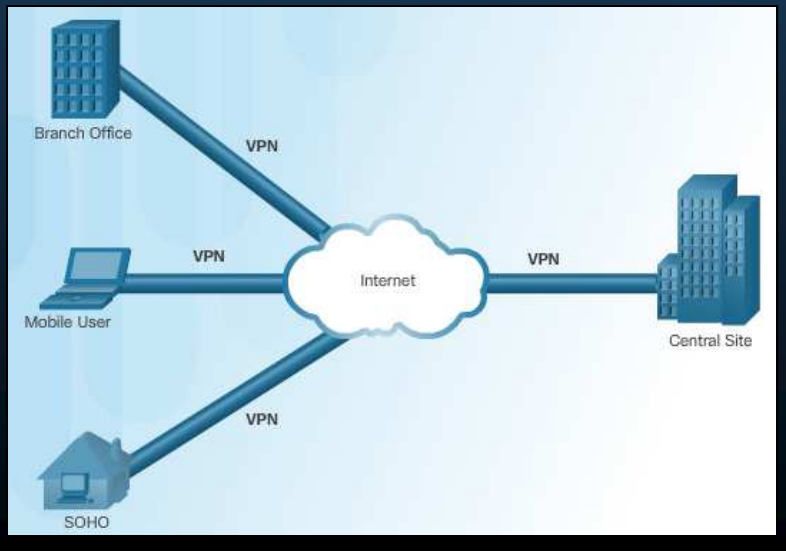
n líneas

otos, sin

orte por
istración

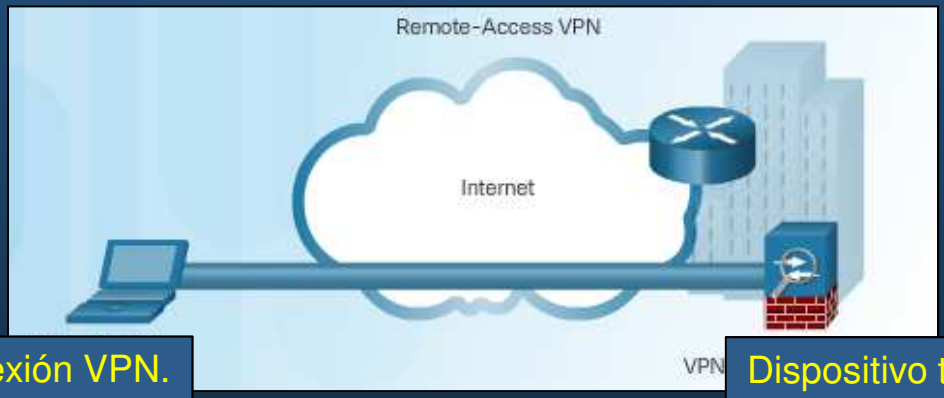
8.1 VPNs

- VPNs IPSec Capa 3.
  - Puede realizar la conexión lógica en Capas 2 ó 3.
    - El presente capítulo se centra solo en VPNs capa 3 (Opera sobre Capa 2).
      - Vgr; GRE, MPLS, IPSec.
  - Pueden ser conexiones entre sitios punto-a-punto (GRE, IPSec) ó cualquiera-a-cualquiera (MPLS, DMVPNGE, TVPN).
    - El presente curso se enfoca solamente en IPSec.
  - IPSec es una suite de protocolos y estándares (respaldados por IETF), para entablar servicios seguros sobre redes IP.
    - Admiten: autenticación, integridad, control de acceso, y confidencialidad.
    - Admite VPNs punto-a-punto y de acceso-remoto.



8.1 VPNs

- Dos tipos de VPNs.
  - De acceso-remoto: La información de conexión VPN no se establece estáticamente, sino de forma dinámica.



Cliente inicia la conexión VPN.

Dispositivo teminal de VPN.

  - Sitio-a-sitio: Configuración estática entre dispositivos en ambos extremos de la conexión (transparente a los hosts internos).

El cliente desconoce la existencia de la VPN.

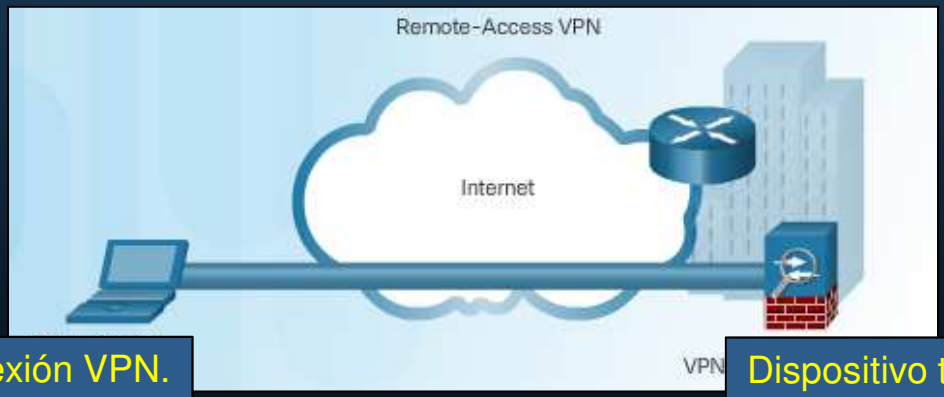
Dispositivo teminal de VPN.

Dispositivo teminal de VPN.

8.1 VPNs

- Componentes de las VPNs de Acceso-Remoto.
  - Los Dispositivos Móviles solo ocupan una conexión a Internet.
  - Los Trabajadores a distancia no requieren estar todo el tiempo conectados.

  - En cualquier caso:
    - El equipo movil es responsable de establecer la conexión VPN.
      - Su IP, cambiará continuamente, dependiendo de donde se encuentre.



Cliente inicia la conexión VPN.

Dispositivo teminal de VPN.

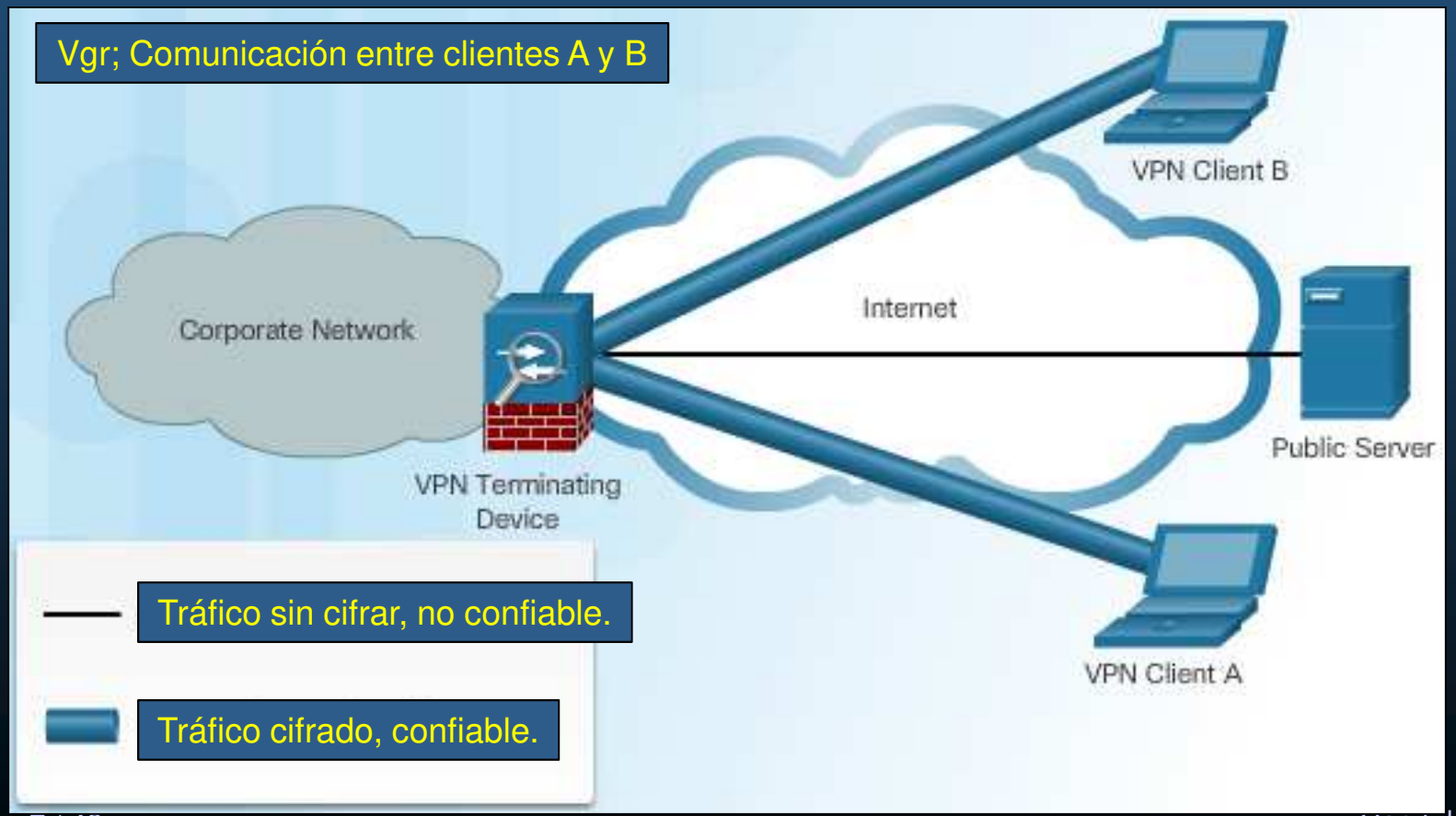
8.1 VPNs

- Componentes de las VPNs Sitio-a-Sitio.
  - Los hosts envían tráfico por puerta de enlace VPN (router, firewall, concentrador VPN, ASA).
  - La puerta de enlace encapsula y cifra el tráfico saliente y envía por internet al gateway par en el otro extremo; quien desencapsula y descifra el tráfico, para entregar al host en la red interna.

  - Otras Topologías VPN sitio-a-sitio:
    - MPLS: conjunto de sitios interconectados mediante proveedor MPLS. Cada extremo cuenta con un dispositivo Customer Edge y uno Provider Edge.
    - DMVPN: auto-proporciona VPNs IPSec sitio-a-sitio, (Cisco NHRP+GRE+IPSec)
    - GETVPN: establece grupo de confianza para evitar túneles punto a punto. Lo miembros (GM) comparten asociación segura (SA). Cualquier GM puede descifrar tráfico de otro GM. No requiere túneles punto-a-punto entre GMs

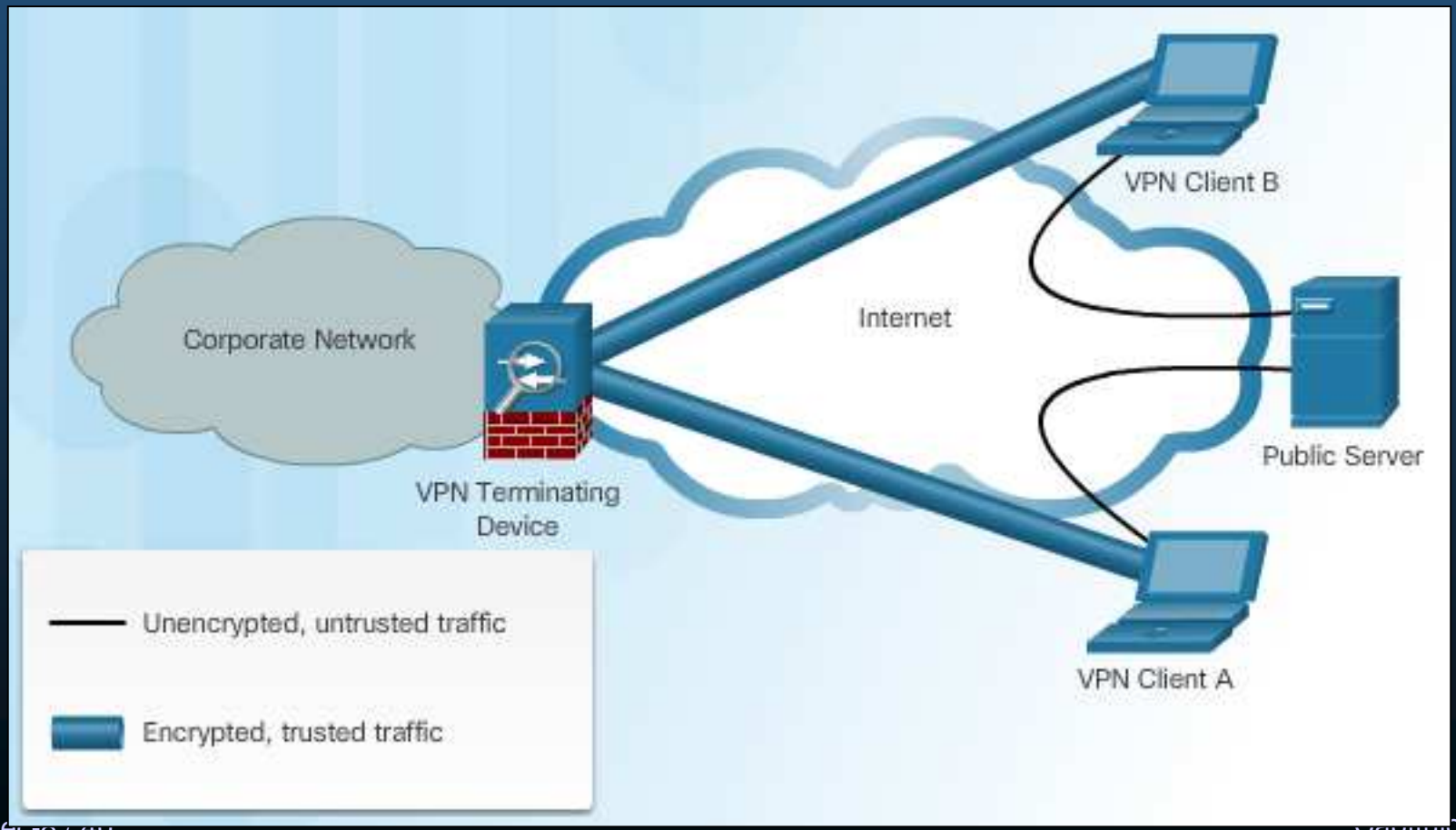
8.1 VPNs

- Horquilla (Hairpinning).
  - Necesidad de enrutar tráfico por la misma interfaz que llega (Topología Hub & Spoke).



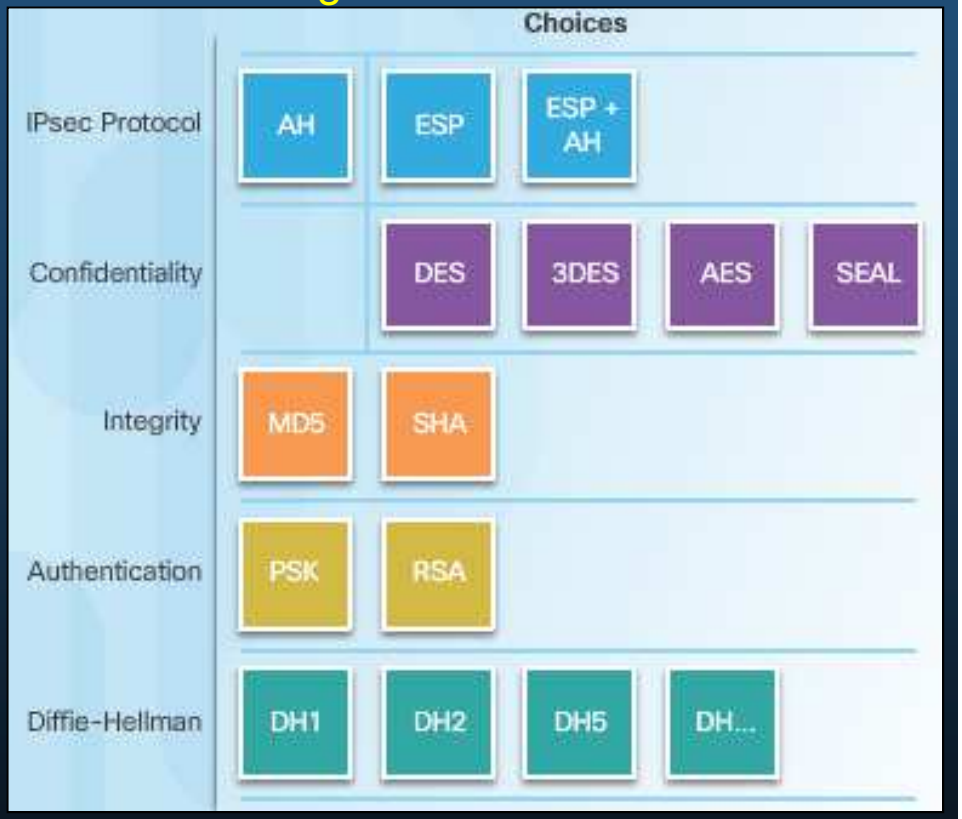
8.1 VPNs

- Túneles divididos.
  - Separa el tráfico interno (seguro mediante VPN), del inseguro (público por Internet).



8.2 Componentes y Operación VPNs IPSec

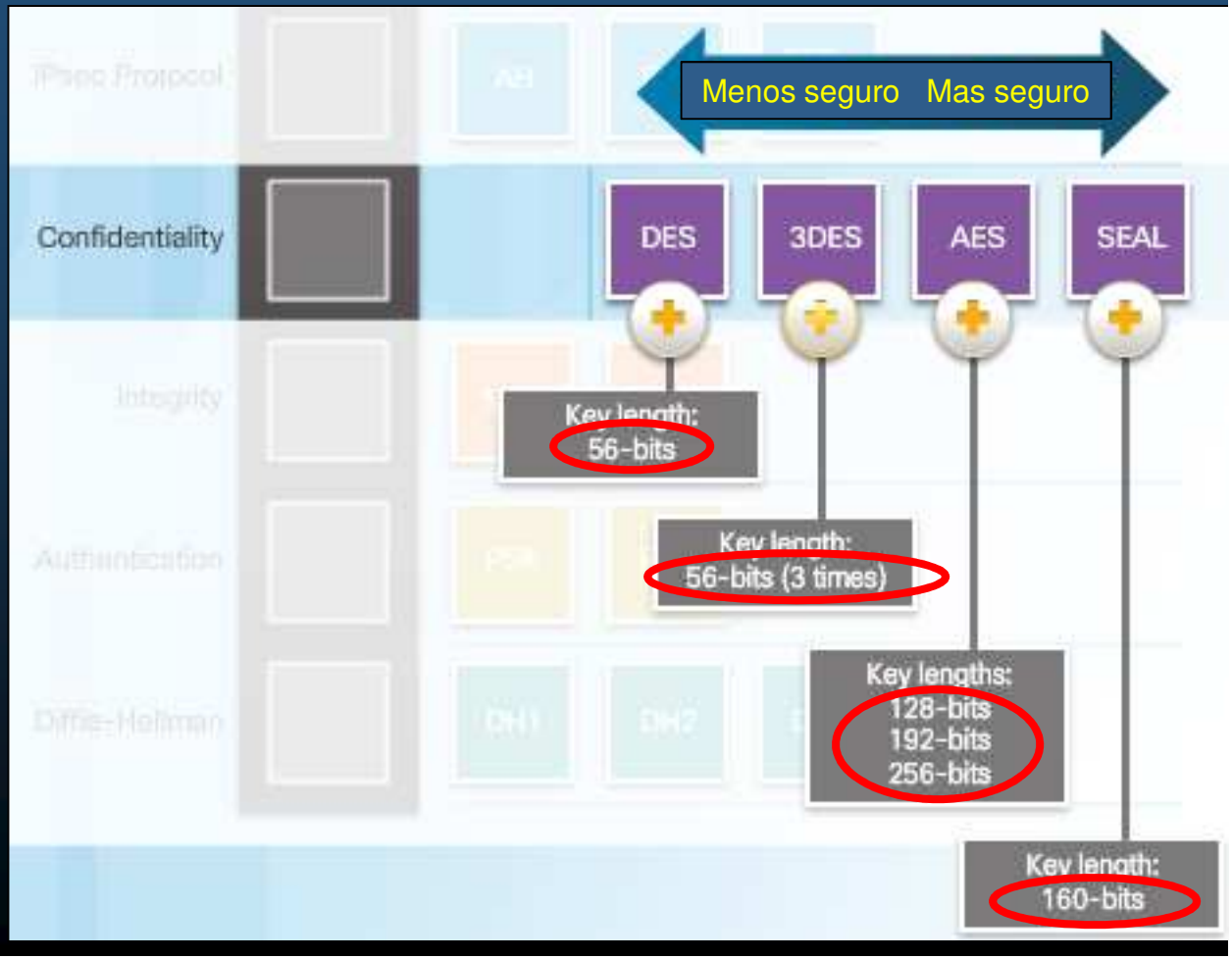
- Tecnologías IPSec.
  - IPSec: Estándar RFC 2401-2412, define cómo asegurar VPNs en redes IP.
  - Protege tráfico de capa 4 a capa 7.
  - Opciones IPSec:
    - Cabecera de Autenticación (AH)
    - Protocolo de Encapsulación de Seguridad (ESP)
  - Provee funciones:
    - Confidencialidad: cifrado.
    - Integridad: algoritmos hash.
    - Autenticación: Intercambio de llaves de Internet (IKE)
    - Intercambio de Llaves seguro: Diffie-Hellman (DH).



  - No está limitado a opciones de componentes, el estandar admite inclusión de nuevas tecnologías.

8.2 Componentes y Operación VPNs IPSec

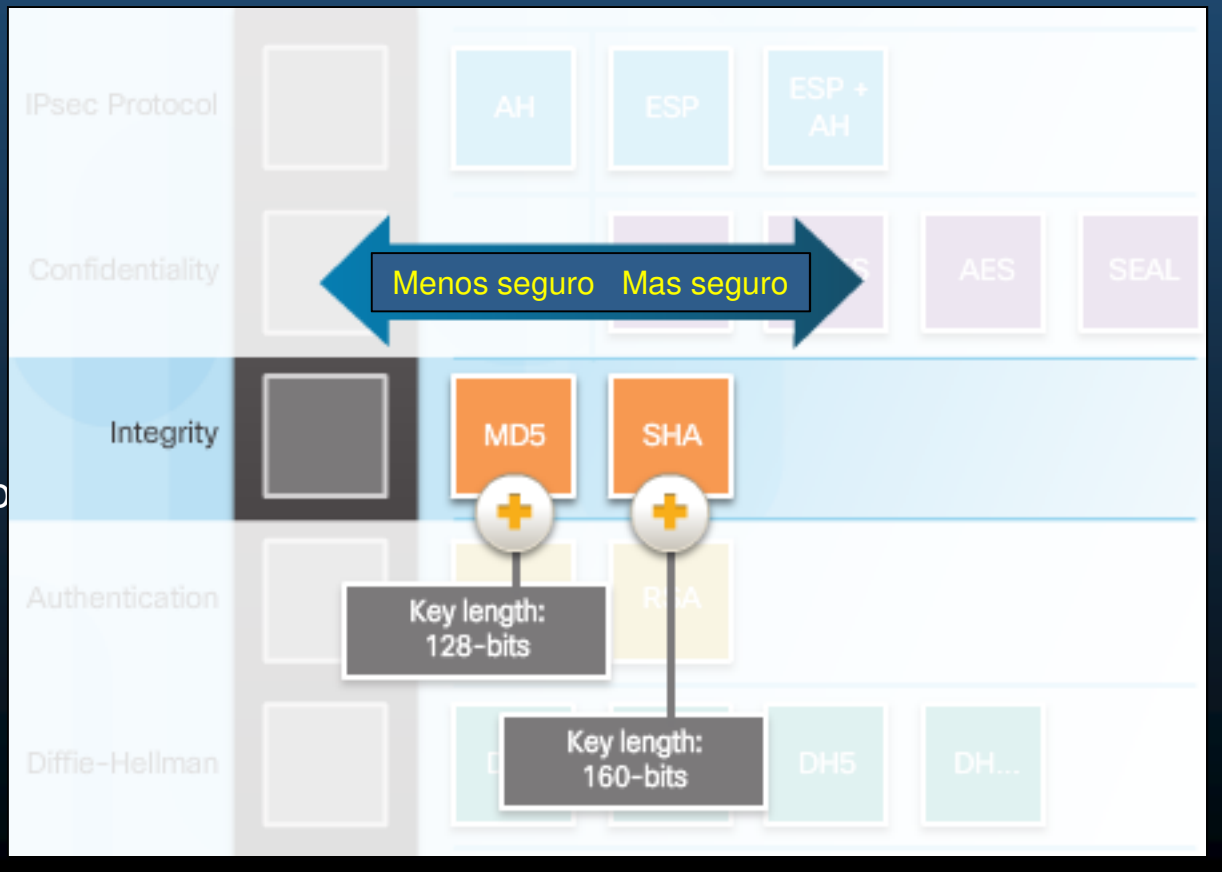
- Confidencialidad.
  - Se alcanza mediante cifrado.
  - El grado de seguridad depende de la longitud de la llave.
    - Vgr;
      - 64 bits puede tomar un año en romperla por fuerza bruta.
      - 128 bits puede tomar hasta 10^19 años.



8.2 Componentes y Operación VPNs IPSec

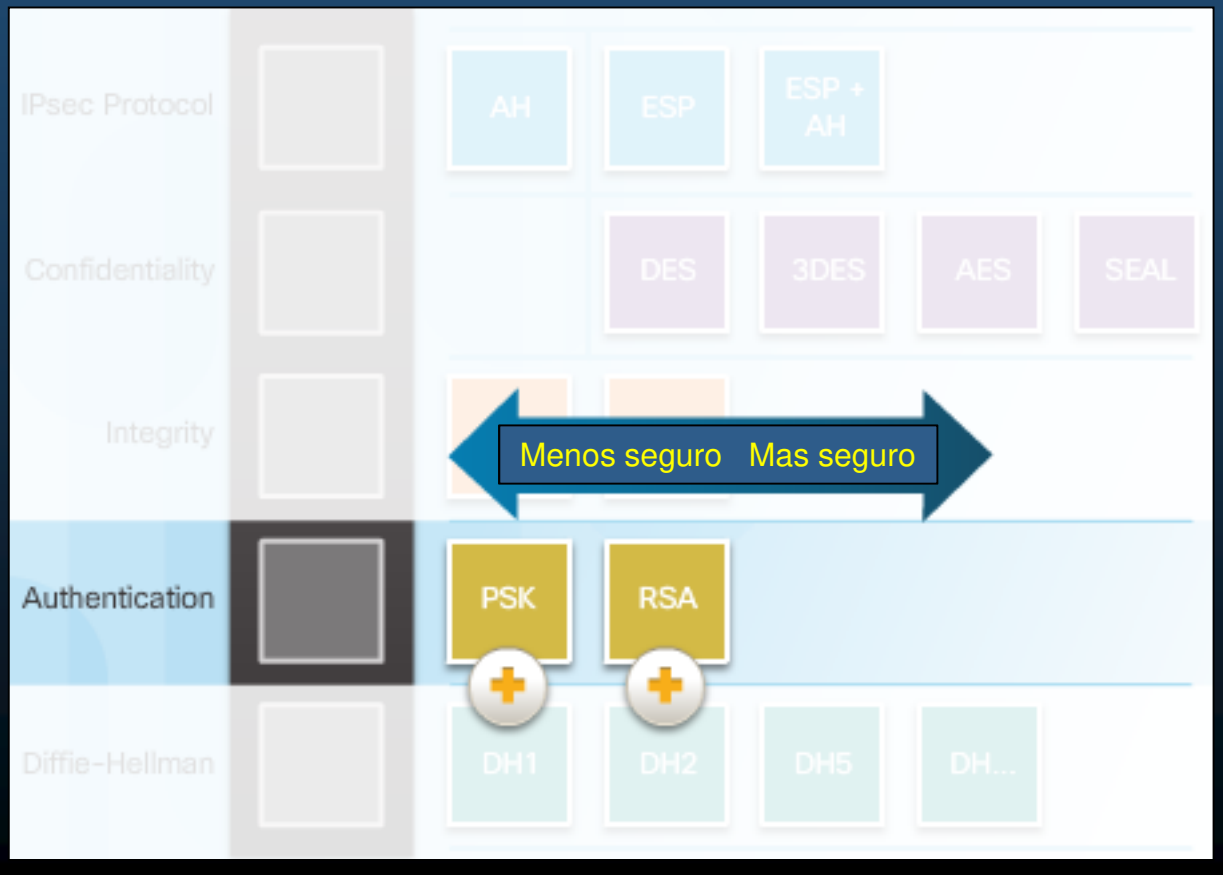
- Integridad.
  - Datos recibidos corresponden con los enviados (No se alteraron en tránsito).
  - VPN utiliza redes públicas, debe asegurar que los datos no se alteren.
    - IPSec emplea Código de Autenticación de Mensaje por Hash (HMAC)
      - Comúnmente:
        MD5 / SHA
      - Entre mas largo el hash, mas seguro.
      - Cisco considera SHA-1 como obsoleto

        Recomienda:
        SHA-256



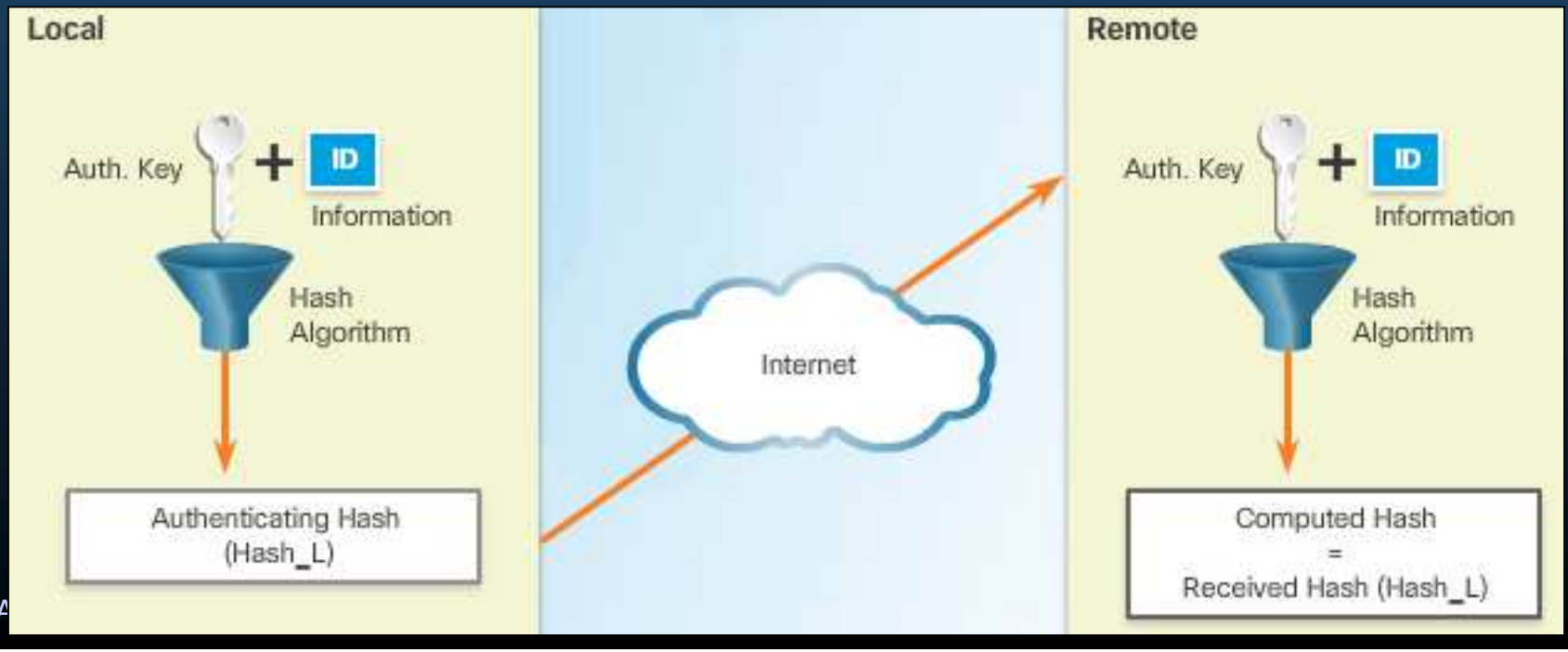
8.2 Componentes y Operación VPNs IPSec

- Autenticación.
  - Cada dispositivo en un extremo de la VPN debe autenticarse.
    - No se da entrada a la red segura a cualquiera.
  - IPSec se utiliza comúnmente con: PSK / RSA.



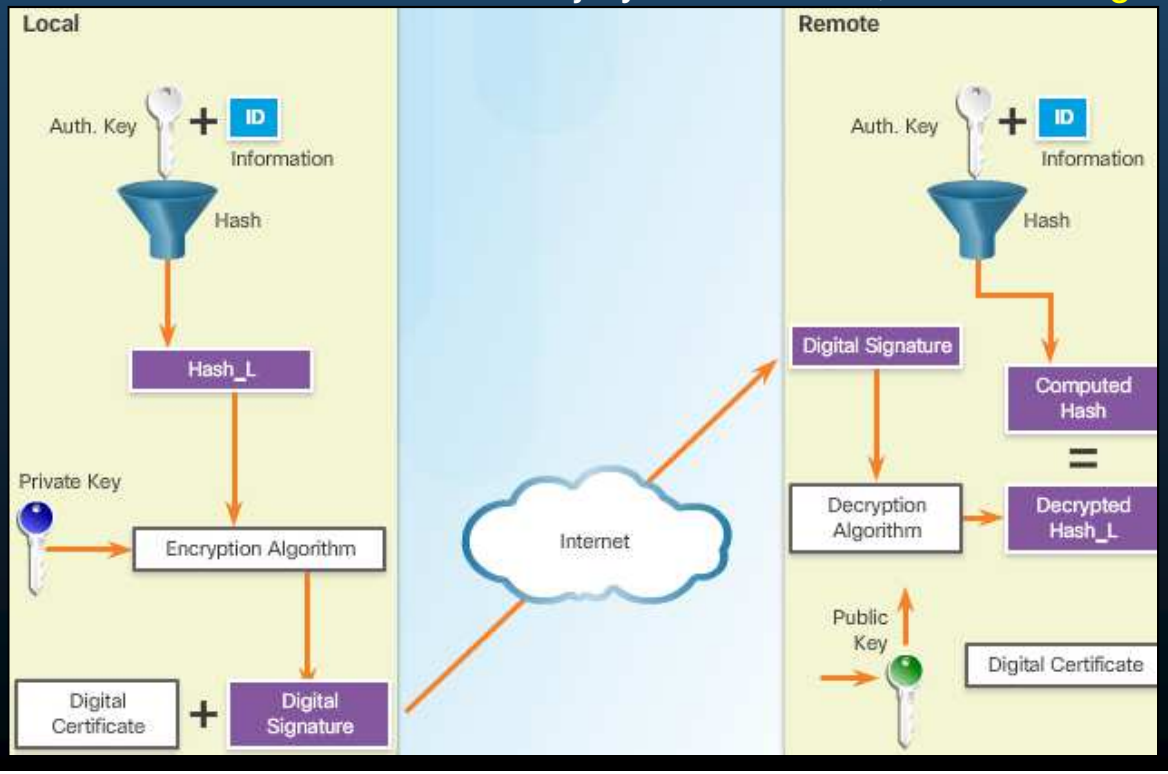
8.2 Componentes y Operación VPNs IPSec

- Autenticación por PSK.
  - Utiliza una llave secreta pre-compartida en cada extremo.
  - La llave se combina con el Id de extremo mediante un Hash → Hash_L.
    - El otro extremo, conoce la llave, del otro extremo, calcula Hash y compara con el recibido
  - Fáciles de configurar, Difíciles de Escalar
    - Requiere pre-configurar cada dispositivo VPN con la llave.



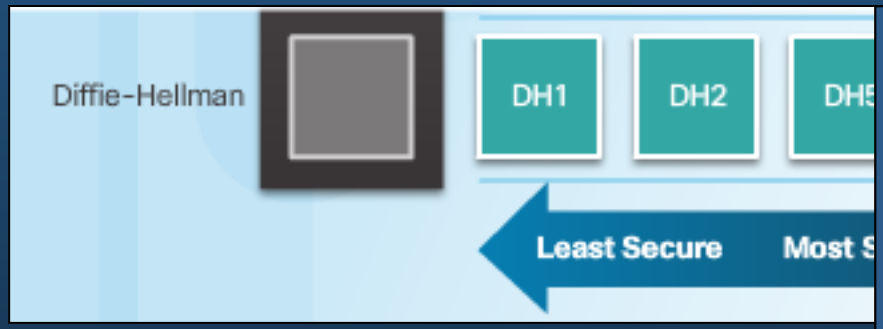
8.2 Componentes y Operación VPNs IPSec

- Autenticación RSA.
  - Autentica extremos mediante intercambio de certificados.
    - El dispositivo local deriva un Hash del mensaje y lo cifra con su llave privada.
    - El hash se adjunta al mensaje y envía al extremo remoto como firma.
    - En el extremo remoto, el hash se descifra con la llave pública del extremo local.
      - Recaulcula el Hash del mensaje y si coinciden, la firma es genuina.



8.2 Componentes y Operación VPNs IPSec

- Intercambio Seguro de Llaves.
  - DH, permite a dos pares establecer una llave secreta compartida (para cifrar).



Estándar RFC 4869 para cifrar Información Clasificada (NSA)
- Cifrado: AES-(128 ó 256)
- Hash: SHA-2
- Firmas Digitales: ECDSA (256 +o 384)
- Intercambio de Llaves: ECDH

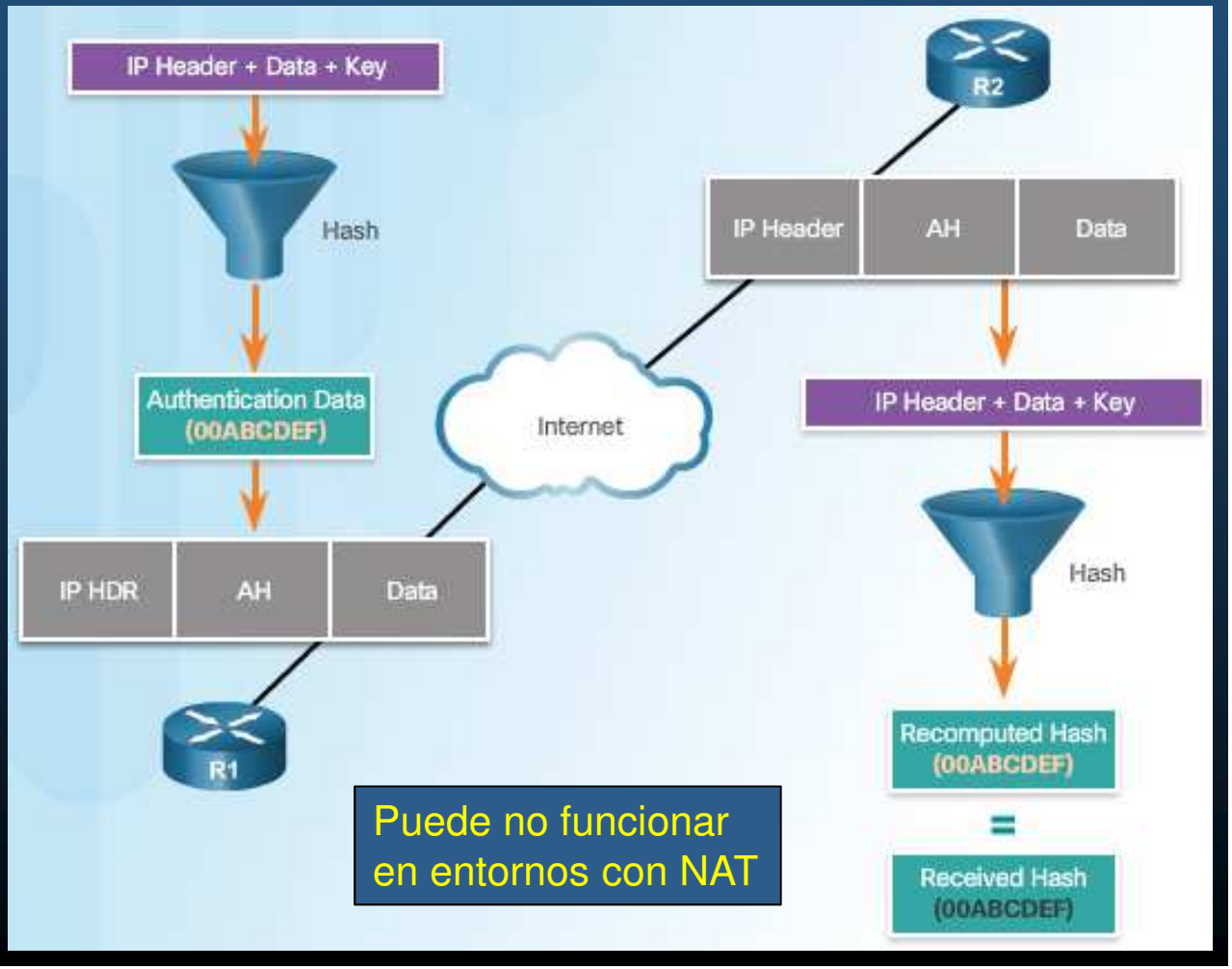
  - Variantes/Grupos:
    - DH 1,2 y 5: Soporta exponenciación sobre un modulo principal y genera llaves de 768, 1024 y 1536 bits respectivamente (obsoletos desde 2012).
    - DH 14, 15 y 16: Uso de llaves mas largas de 2048, 3072 y 4096 bits respectivamente (recomendados hasta 2030).
    - DH 19, 20, 21 y 24: Uso de llaves de 256, 384, 521 y 2048 bits con soporte de criptografía de curvas elípticas (ECDH) (DH24 para siguiente generación).
  - Utilizar uno que corresponda en longitud de llave con la del algoritmo de cifrado a emplear.

8.2 Componentes y Operación VPNs IPSec

- Introducción a los Protocolos IPSec.
  - Protocolo es el primer bloque del Marco de Trabajo IPSec
    - Indica que otros bloques estarán incluidos.
  - Cabecera de Autenticación - AH:
    - Protocolo IP 51.
    - Sin Confidencialidad, solo Autenticación e Integridad.
    - Transmisión en Texto Plano.
  - Encapsulación de la Carga-útil Segura – ESP:
    - Protocolo IP 50.
    - Confidencialidad (cifrado) + Autenticación (Opcionales, al menos una) + Integridad.
    - Encripta paquete IP.
    - Autentica el paquete IP Interno y la cabecera ESP.

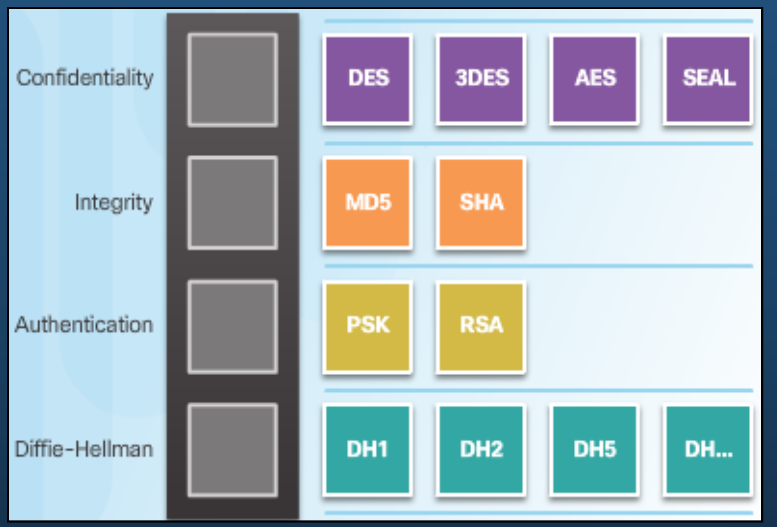
8.2 Componentes y Operación VPNs IPSec

- Cabecera de Autenticación (AH).
  - Realiza Hash a Cabecera, Datos y Llave Compartida, e incluye como firma.
    - Involucra: Integridad, Autenticación Diffie-Hellman
    - Calcula Hash de: Cabecera IP + Datos + Llave → Firma
    - Genera nueva Cabecera AH con la Firma.
    - Transmite
    - Re-Calcula Hash.
    - Compara.



8.2 Componentes y Operación VPNs IPSec

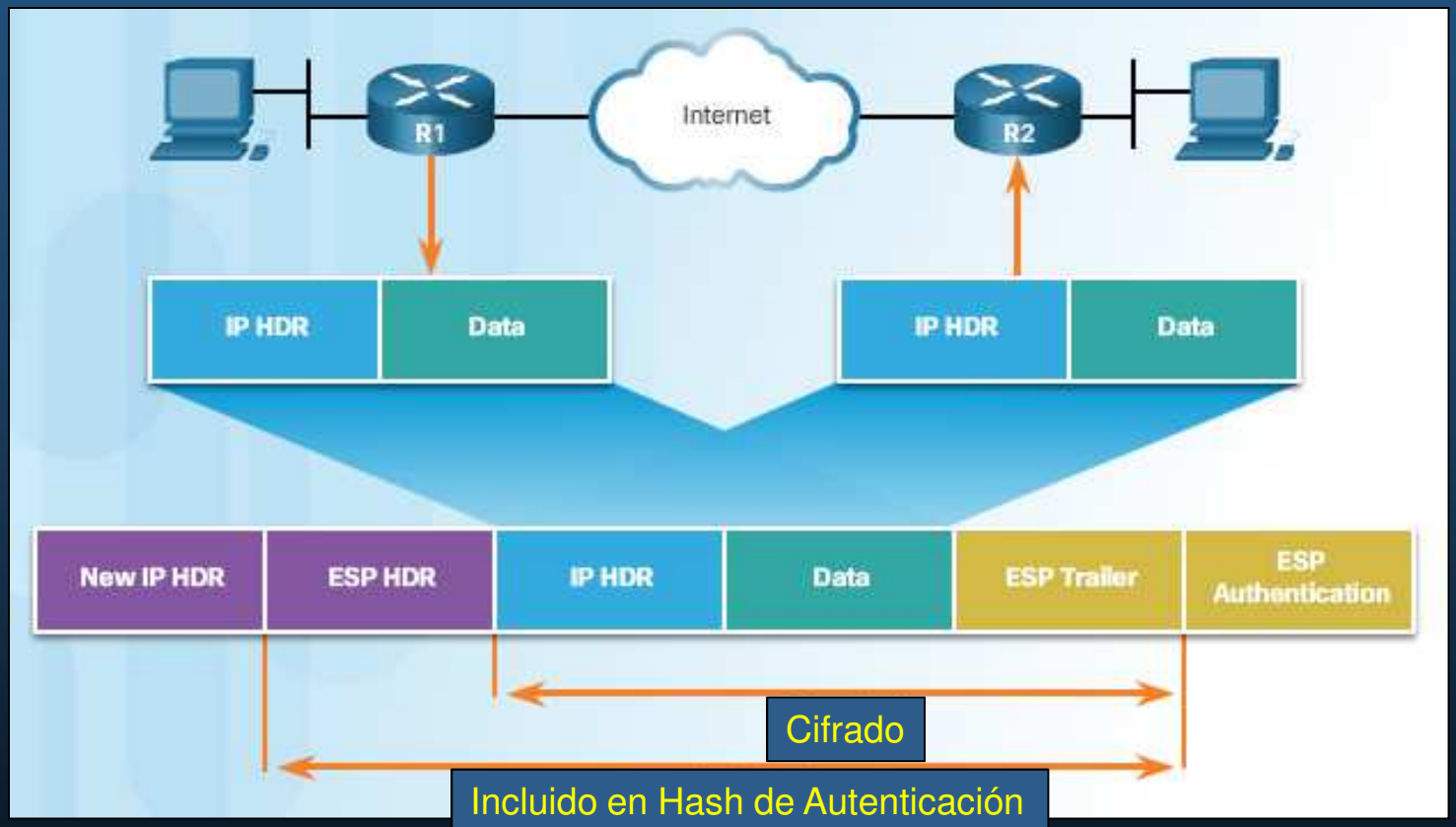
- Encapsulación de la Carga-útil Segura – ESP.
  - Cifra carga-útil (DES 56bits por defecto).
    - Provee Confidencialidad.
  - Calcula Hash de la información cifrada.
    - Provee Integridad y Autenticación (opcional).



  - Puede proveer protección anti-contestación.
    - Verificar unicidad de paquetes (no duplicados).
    - Asegura que hackers no insertan paquetes alterados al flujo mediante ventana deslizante.
    - Aunque es típicamente utilizado en ESP, puede hacerse también en AH.

8.2 Componentes y Operación VPNs IPSec

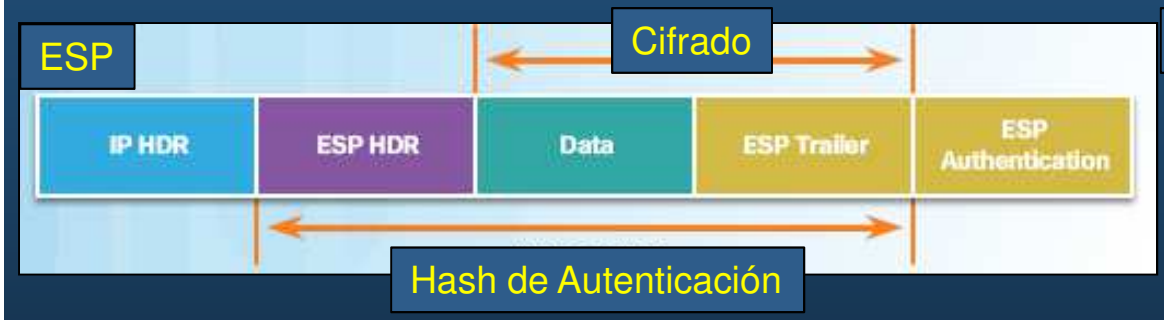
- ESP Cifra y Autentica.



  - Modelo considerando IPv4, para IPv6 en lugar de cabeceras independientes, se utilizan extensiones de cabecera IPv6 con valores 50 (ESP) y 51 (AH), para el campo siguiente cabecera .

8.2 Componentes y Operación VPNs IPSec

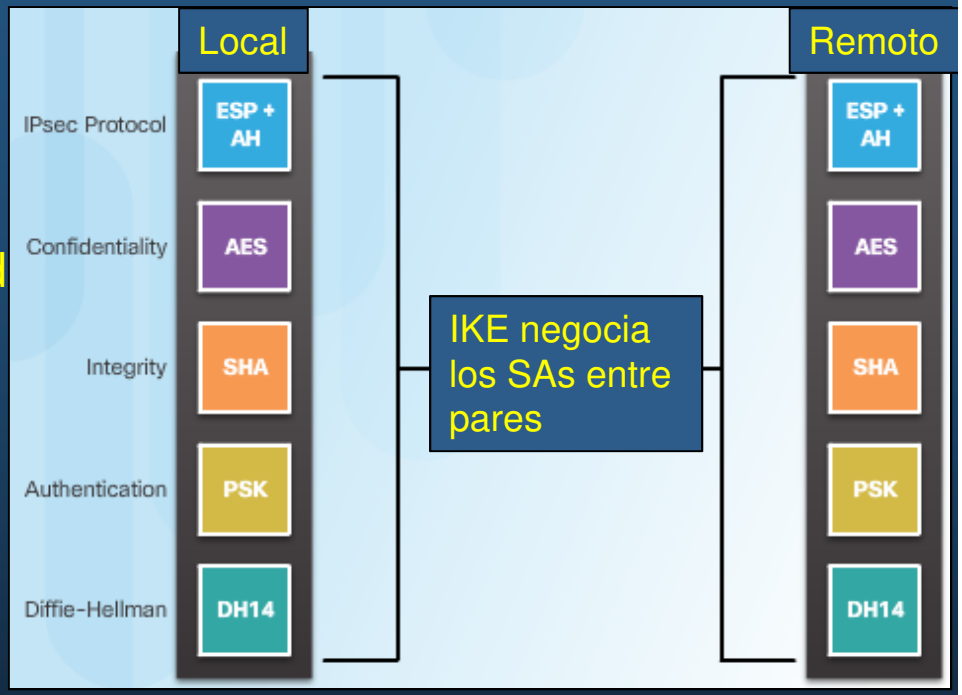
- Modos de Transporte y Tunel.
  - Transporte (Entre Hosts / Acceso Remoto).
    - Cifra solo de capa de transporte en adelante (IP en texto-plano).



  - Tunel (Acceso-Remoto / Sitio-a-Sitio).
    - Asegura de capa de red en adelante (todo el paquete).
      - Re-encapsula en otro paquete nuevo.

8.2 Componentes y Operación VPNs IPSec

- El Protocolo IKE.
  - Estándar de administración de llaves.
  - Negocia Asociaciones de Seguridad (SA).
  - Simplifica configuraciones IPSec.
  - Parte del marco de trabajo del: Protocolo de Administración de Llaves de Asociación de Seguridad de Internet (ISAKMP).
    - Define: formato de mensaje; mecanismos de intercambio; proceso de negociación.
  - Basado en Oakley (intercambio) y SKEME (cifrado de llave pública).
    - RFC 2409
  - Calcula llaves en base al intercambio de varios paquetes.
  - Usa puerto UDP 5000 para intercambio de mensajes.



8.2 Componentes y Operación VPNs IPSec

- Fases IKE.
  - Fase 1: Negociación de (llave) Asociación de Seguridad (SA) para Fase 2.
    - Negocia políticas ISAKMP (políticas IKE).
      - Vgr; Política 10 (AES, SHA, PSK, DH14, tiempo de vida)
    - Intercambia llave por DH.
    - Verifica Identidad de Pares (Autentica).
    - Establece tunel seguro.
    - Dos modos:
      - Principal.
        - Oculta identidad de los pares.
      - Agresivo.
        - Mas rápido (No cifra identidad de pares).
        - Vulnerable a ataques por fuerza bruta.
  - Fase 2: Negociación de (llaves) Asociación de Seguridad (SA) para otras aplicaciones (IPSec).
    - Negocía politicas IPSec.

8.2 Componentes y Operación VPNs IPSec

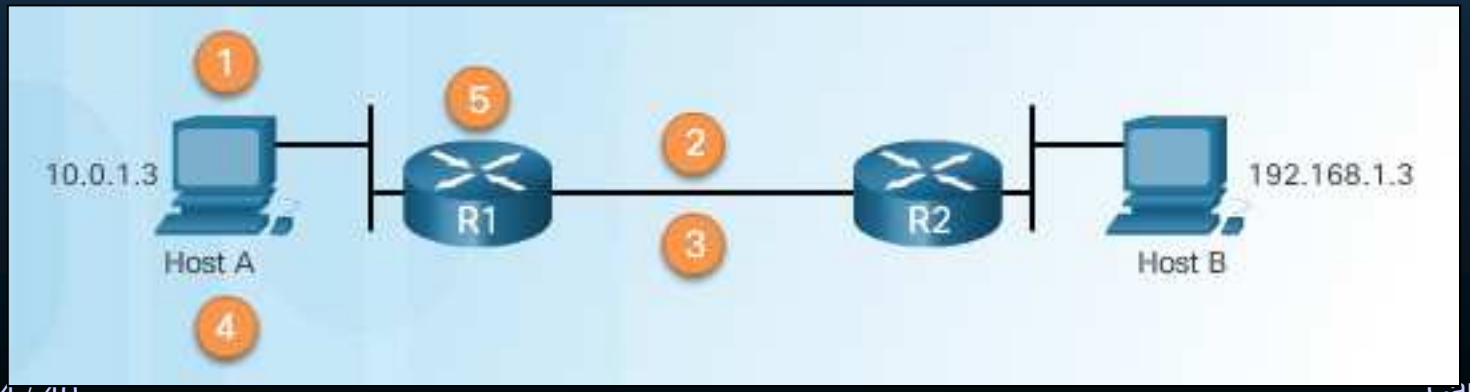
- Fase 2 IKE: Negociación de SAs.
  - Negocia los parámetros de seguridad que se usarán en el tunel IPSec.
  - También llamada: modo rápido.
  - IKE negocia los parámetros de seguridad necesarios por IPSec
  - Negocia una nueva asociación de seguridad cuando su tiempo de vida previo caduca.

  - IKE v2 (RFC 4306). Mejora IKE.
    - Soporta detección de NAT con NAT-T
      - NAT-T encapsula paquetes ESP en UDP:4500 para que puedan atravesar un NAT.

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Negociación IPSec.

1. Host A quiere enviar tráfico “interesante” al Host B Eso inicia un túnel ISAKMP
2. R1 y R2 negocian una sesión de fase 1 IKE.
3. R1 y R2 negocian una sesión de fase 2 IKE.
4. Intercambio de información por el tunel IPSec.
5. Elimina el tunel IPSec.



8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Topología Base para VPN Sitio-a-Sitio.


```
R1# show run
<output omitted>

!
interface GigabitEthernet0/0
 ip address 10.0.1.1 255.255.255.0
!
interface Serial0/0/0
 ip address 172.30.2.1 255.255.255.0
!
ip route 192.168.1.0 255.255.255.0 Serial0/0/0
!

R1# ping ip 192.168.1.1 source 10.0.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#
```

```
R2# show run
<output omitted>

!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
 ip address 172.30.2.2 255.255.255.0
!
ip route 10.0.1.0 255.255.255.0 Serial0/0/0
!

R2#
```

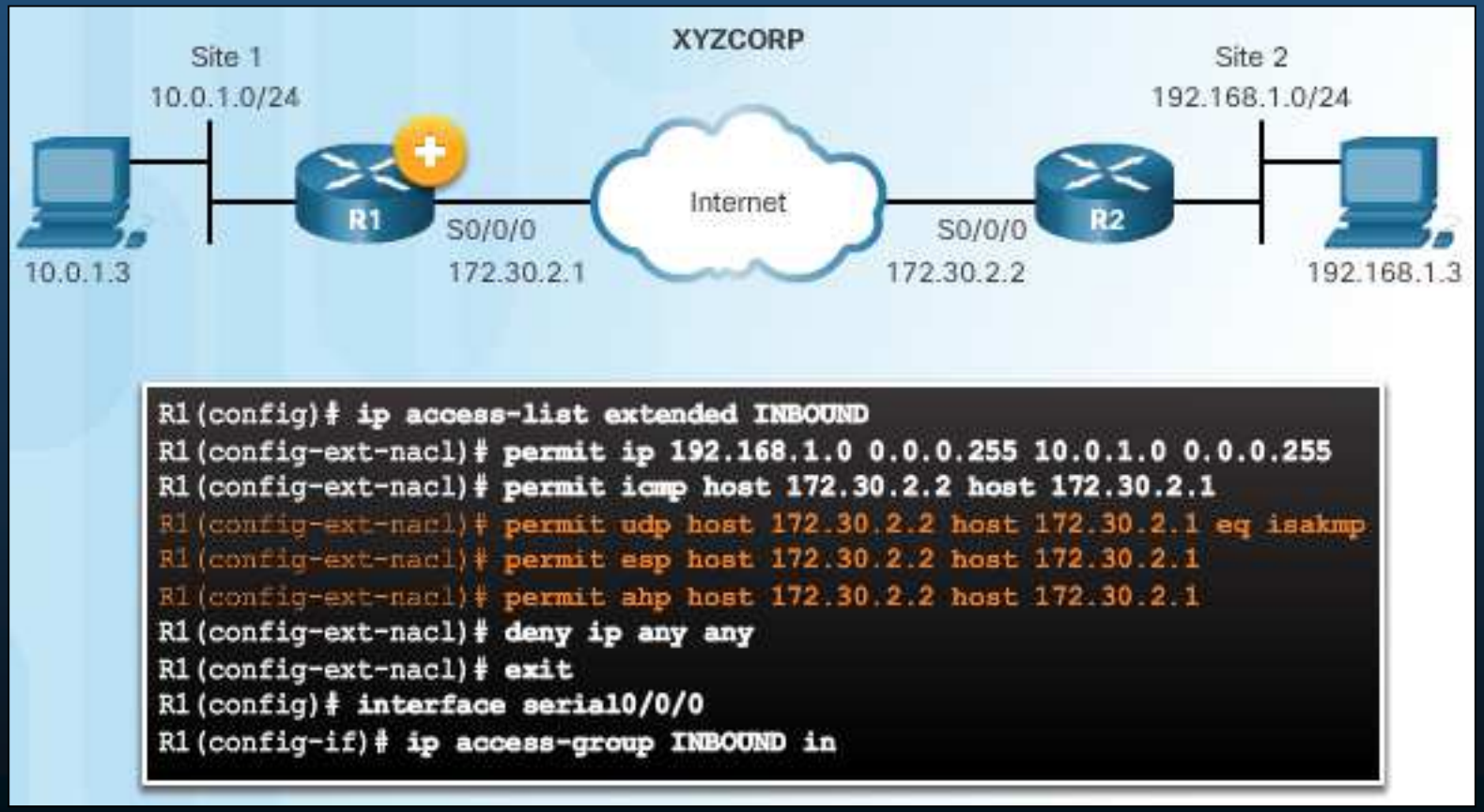
8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Tareas a configurar en le VPN IPSec de ejemplo.
  - Requerimientos.
    - Cifrar tráfico con AES 256 y SHA
    - Autenticar con PSK
    - Intercambiar claves con el grupo 24
    - La duración del túnel ISAKMP es de 1 hora
    - El túnel IPsec utiliza ESP con una duración de 15 minutos

  - Tareas para cubrir requerimientos:
    - Configurar la directiva ISAKMP para IKE Fase 1
    - Configurar la directiva IPsec para IKE fase 2
    - Configurar un mapa de cifrado para la directiva Ipsec
    - Aplicar la directiva Ipsec
    - Verificar que el túnel IPsec es operativo

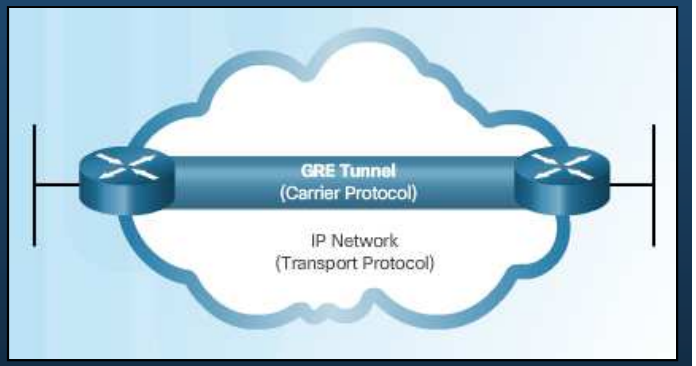
8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Configuraciones ACL Existentes.
  - Asegurarse que ACLs existentes admitan el tráfico necesario por IPSec.



8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Manejo de Tráfico Multicast y Broadcast.
  - IPSec solo soporta tráfico unicast.
  - Encapsulación de Enrutamiento Generica (GRE), admite tráfico de enrutamiento (unicast, multicast, broadcast) en una VPN sitio a sitio.
    - Soporta tuneling multiprotocolo.
      - Puede encapsular múltiples protocolos capa 3 en redes IP.
      - Añade cabecera GRE adicional entre la carga útil e IP.
    - No provee cifrado.



    - Está fuera del alcance del curso.

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

Requiere habilitar licencia securityk9

- Políticas ISAKMP por defecto.
  - **R# show crypto isakmp default policy**


```
R1# show crypto isakmp default policy

Default IKE policy
Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
```

7 políticas por defecto policy (65507 – 65514)

Si no se especifica, cada router buscará utilizar la mas segura disponible.

Si concuerdan ambos extremos, se establecerá el tunel, sin mas configuración.

Subrallado No disponible en PacketTracer

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Políticas ISAKMP por defecto (655010 - 655014).

```
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

Ninguna cumple requisitos del ejemplo solicitado

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Configurar una nueva política ISAKMP.
  - `R(config)# crypto isakmp policy …`


```
R1(config)# crypto isakmp policy ?
  <1-10000>  Priority of protection suite

R1(config)# crypto isakmp policy 1
R1(config-isakmp)# ?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
```

Menor Valor → Mayor Prioridad

Configura IKE Fase 1

Recuerde HAGLE
- **H**ash
- **A**utenticación
- **G**rupo
- **L**ifetime
- **E**ncriptación

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Ejemplo de configurar una nueva política ISAKMP.
  - `R(config)# crypto isakmp policy …`

Recuerde HAGLE
- **H**ash
- **A**utenticación
- **G**rupo
- **L**ifetime
- **E**ncriptación


```
R1(config)# crypto isakmp policy 1
R1(config-isakmp)# hash sha
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 24
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# end
R1# show crypto isakmp policy
Global IKE policy
Protection suite of priority 1
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #24 (2048 bit, 256 bit subgroup)
        lifetime:                3600 seconds, no volume limit
R1#
```

PacketTracer sólo soporta grupos 1, 2 y 5

R2 deberá tener una configuración equivalente

Verificar la configuración

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Configurar una llave pre-compartida.

```
Router(config)#
crypto isakmp key keystring address <peer-address | peer-hostname>
```

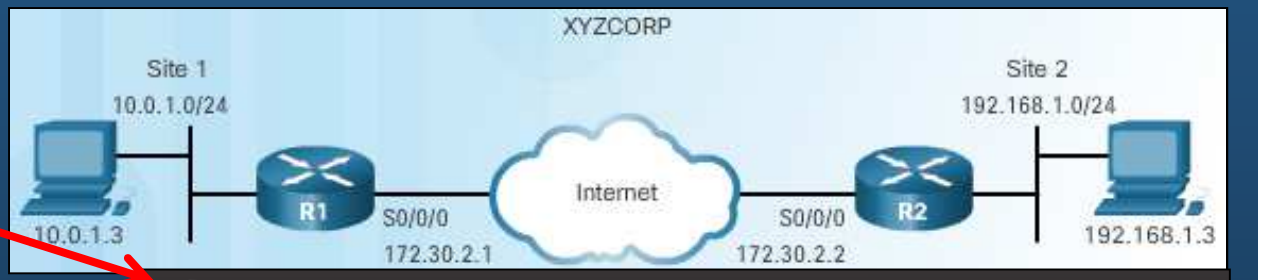
  - El ejemplo, requiere el uso de llave pre-compartida entre pares:


```
R1# conf t
R1(config)# crypto isakmp key cisco12345 address 172.30.2.2
R1(config)#
```

```
R2# conf t
R2(config)# crypto isakmp key cisco12345 address 172.30.2.1
R2(config)#
```

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Definiendo Tráfico “Interesante”.
  - Aunque se haya configurado, el túnel aún no existe.
    - El tunel se crea al detectar tráfico “interesante”.
    - Un tunel para cada tipo de tráfico interesante.




```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA

R1#
```

  - Tráfico Interesante se define mediante ACLs que permitan dicho tráfico.
    - Tráfico que no admita la ACL no es interesante y se envía sin cifrar.
    - Vgr; Tráfico de una LAN a otra.

```
R1# conf t
R1(config)# access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#
```

Se usarán en la configuración del criptomapa, para indicar que iniciará IKE Fase 1

```
R2# conf t
R2(config)# access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255
R2(config)#
```

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Configurar conjunto de transformaciones IPsec.
  - Especificar algoritmos a ser utilizados por IPSec en IKE Fase 2.
    - Para proteger el tráfico "interesante".


```
R1(config)# crypto ipsec transform-set ?
  WORD  Transform set tag

R1(config)# crypto ipsec transform-set R1-R2 ?
  ah-md5-hmac       AH-HMAC-MD5 transform
  ah-sha-hmac       AH-HMAC-SHA transform
  ah-sha256-hmac    AH-HMAC-SHA256 transform
  ah-sha384-hmac    AH-HMAC-SHA384 transform
  ah-sha512-hmac    AH-HMAC-SHA512 transform
  comp-lzs          IP Compression using the LZS compression algorithm
  esp-3des          ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes           ESP transform using AES cipher
  esp-des           ESP transform using DES cipher (56 bits)
  esp-gcm           ESP transform using GCM cipher
  esp-gmac          ESP transform using GMAC cipher
  esp-md5-hmac      ESP transform using HMAC-MD5 auth
  esp-null          ESP transform w/o cipher
  esp-seal          ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac      ESP transform using HMAC-SHA auth
  esp-sha256-hmac   ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac   ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac   ESP transform using HMAC-SHA512 auth
```

Nombre del conjunto de transformación.

Algoritmos.

```
R1(config)# crypto ipsec transform-set R1-R2 esp-aes esp-sha-hmac
R1(config)#
```

```
R2(config)# crypto ipsec transform-set R1-R2 esp-aes esp-sha-hmac
R2(config)#
```

Permiten definir algoritmos de cifrado e integridad a ser utilizados en el tunel IPSec.

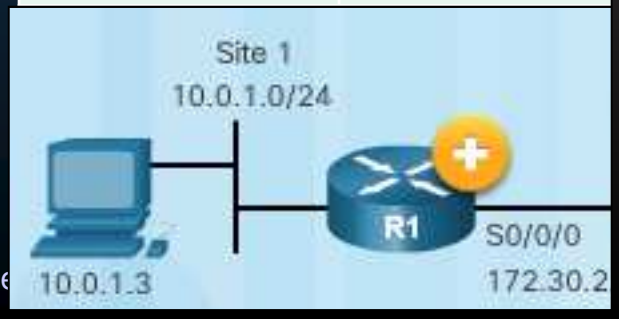
No todos disponibles en PacketTracer

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Sintaxis para Configurar un Mapa de Cifrado (Crypto-Map).
  - Un Mapa de Cifrado asocia el tráfico interesante y el conjunto de transformaciones al resto de políticas IPSec.

```
Router(config)#
crypto map map-name seq-num [ipsec-isakmp | ipsec-manual]
```

Parámetro	Descripción
map-name	Nombre que identifica al mapa de cifrado
seq-num	Número de secuencia para cada entrada del mapa. Use sin palabra clave, para modificar la entrada
ipsec-isakmp	Usar IKE para establecer SAs de IPSec para esta entrada.
ipsec-manual	No usar IKE para establecer SAs de IPSec para el tráfico especificado por esta entrada




```
R1(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)# ?
Crypto Map configuration commands:
  default          Set a command to its defaults
  description      Description of the crypto map statement policy
  dialer           Dialer related commands
  exit             Exit from crypto map configuration mode
  match            Match values.
  no               Negate a command or set its defaults
  qos              Quality of Service related commands
  reverse-route    Reverse Route Injection.
  set              Set values for encryption/decryption
```

Configuraciones disponibles

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Configuración de un Mapa de Cifrado (Crypto-Map).

- 1: A
  c
  t
  r
- 2: E
- 3: C
- 4: C
  vid
- 5: V
  R#

```
R1# show crypto map
    Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "R1-R2_MAP" 10 ipsec-isakmp
    Peer = 172.30.2.2
    Extended IP access list 101
        access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
    Security association lifetime: 4608000 kilobytes/900 seconds
    Responder-Only (Y/N): N
    PFS (Y/N): Y
    DH group:  group24
    Mixed-mode : Disabled
    Transform sets={
        R1-R2:  { esp-aes esp-sha-hmac  } ,
    }
    Interfaces using crypto map R1-R2_MAP:

R1#
```

ntil a peer

PacketTracer sólo soporta grupos 1, 2 y 5

fetime seconds 900

ntil a peer

fetime seconds 900

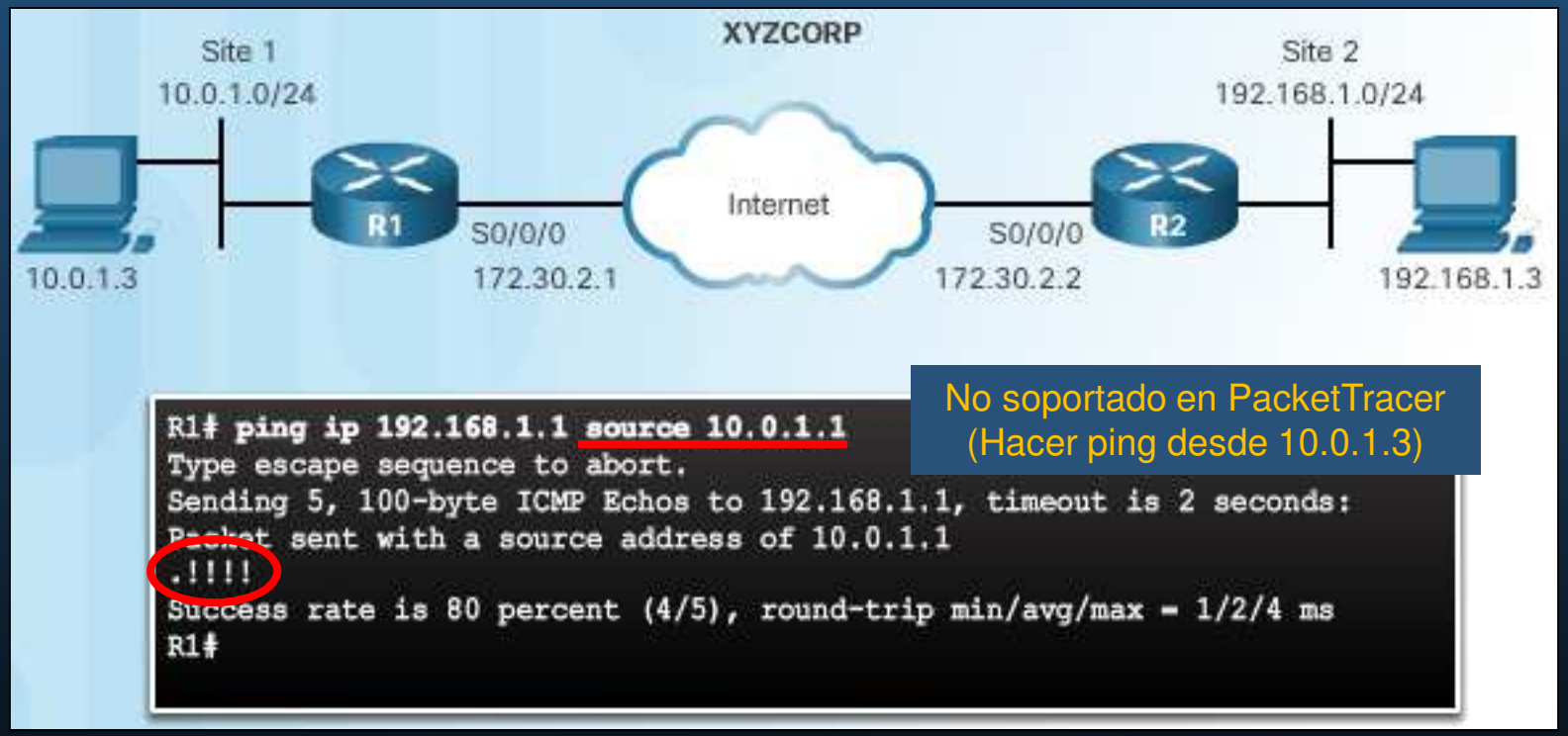
8.3 Implementación de VPNs IPSec Sitio-a-Sitio

- Aplicar el Mapa de Cifrado.
  - Se aplica en la interface de salida con: `R(conf-if)# crypto map map-name`.
  - Se verifica con: `R# show crypto map`.


```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map R1-R2_MAP
R1(config-if)#
*Mar 19 19:36:36.273: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)# end
R1# show crypto map
          Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "R1-R2_MAP" 10 ipsec-isakmp
          Peer = 172.30.2.2
          Extended IP access list 101
              access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
          Security association lifetime: 4608000 kilobytes/900 seconds
          Responder-Only (Y/N): N
          PFS (Y/N): Y
          DH group:  group24
          Mixed-mode : Disabled
          Transform sets={
                    R1-R2:  { esp-aes esp-sha-hmac  } ,
          }
          Interfaces using crypto map R1-R2_MAP:
                    Serial0/0/0
```

8.3 Implementación de VPNs IPSec Sitio-a-Sitio

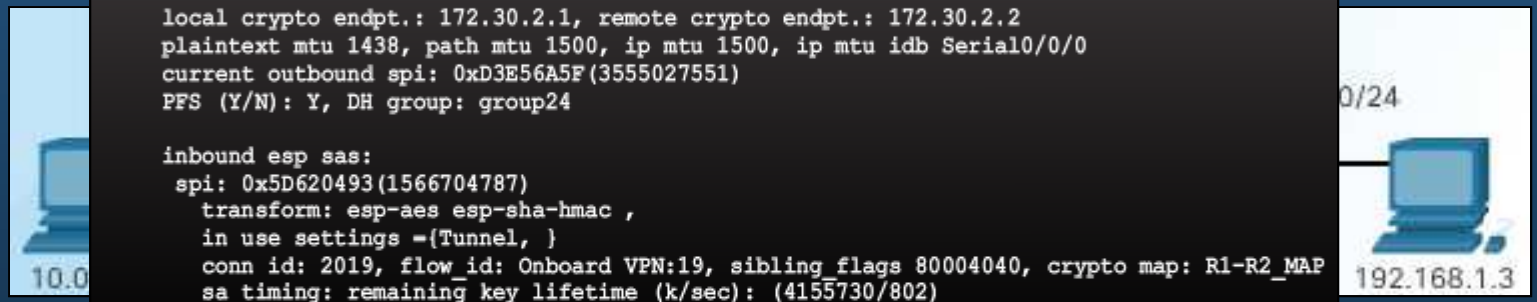
- Envío de Tráfico Interesante.
  - Para probar el túnel, basta con enviar tráfico IP de una LAN a otra.
    - Que coincida con la ACL definida.



  - En el ejemplo, el primer ping falla debido a los milisegundos que tardan en establecerse los túneles ISAKMP e IPSec

8.3 Imp...-a-Sitio

- Verificar ...
  - Él tráfi... KMP e IPSec.
  - Verifica... psec sa




```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: R1-R2_MAP, local addr 172.30.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 172.30.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.30.2.1, remote crypto endpt.: 172.30.2.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xD3E56A5F(3555027551)
     PFS (Y/N): Y, DH group: group24

     inbound esp sas:
      spi: 0x5D620493(1566704787)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2019, flow_id: Onboard VPN:19, sibling_flags 80004040, crypto map: R1-R2_MAP
        sa timing: remaining key lifetime (k/sec): (4155730/802)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xD3E56A5F(3555027551)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2020, flow_id: Onboard VPN:20, sibling_flags 80004040, crypto map: R1-R2_MAP
        sa timing: remaining key lifetime (k/sec): (4155730/802)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
R1#
```

Capítulo 9

Implementación de ASAs

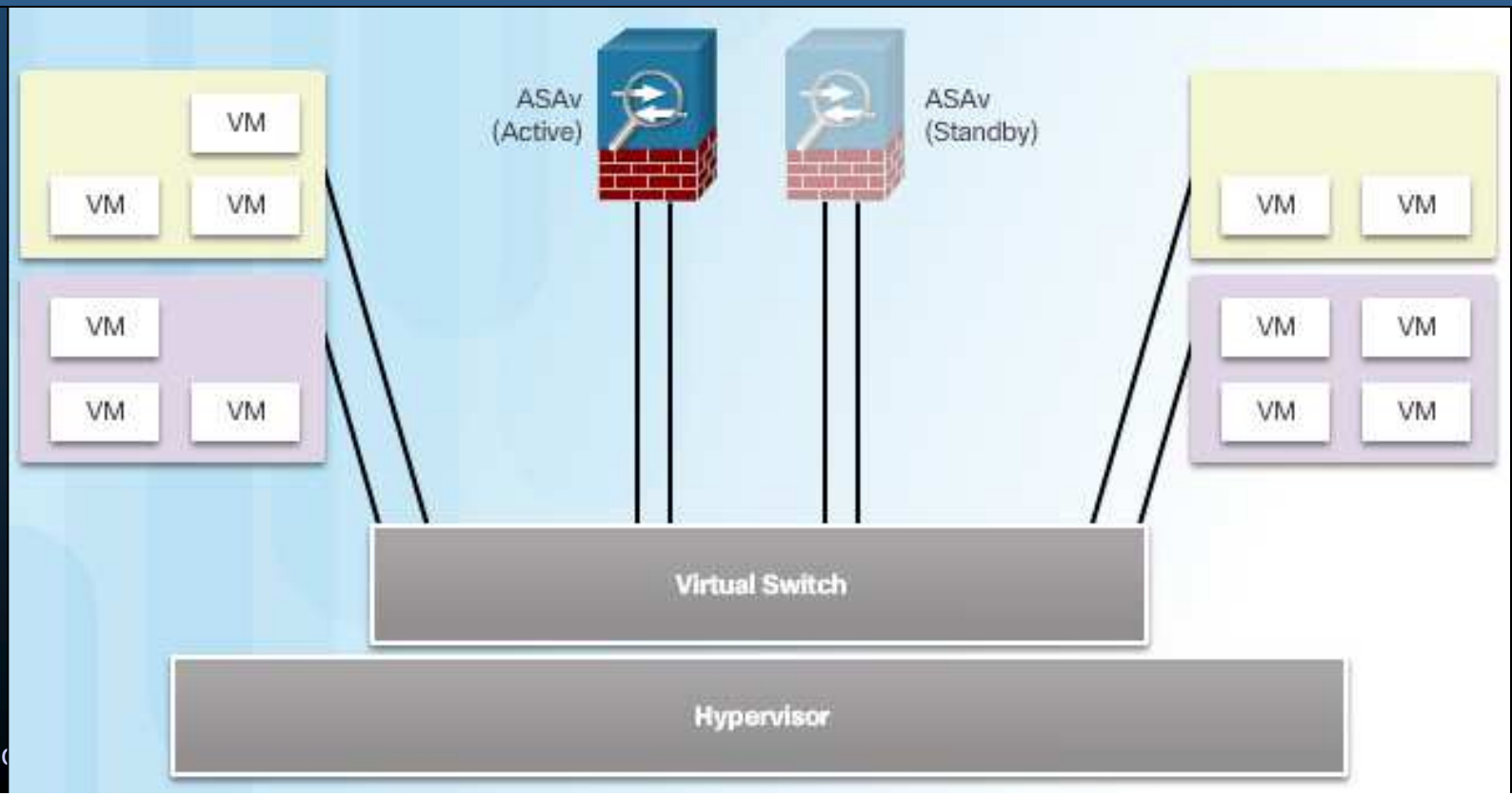
https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#9.1.1.1

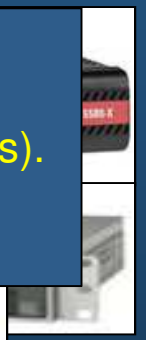
9.1Introducción a ASA.

- Modelos de Firewalls ASA.

Alternativa: ASA vitualizado.

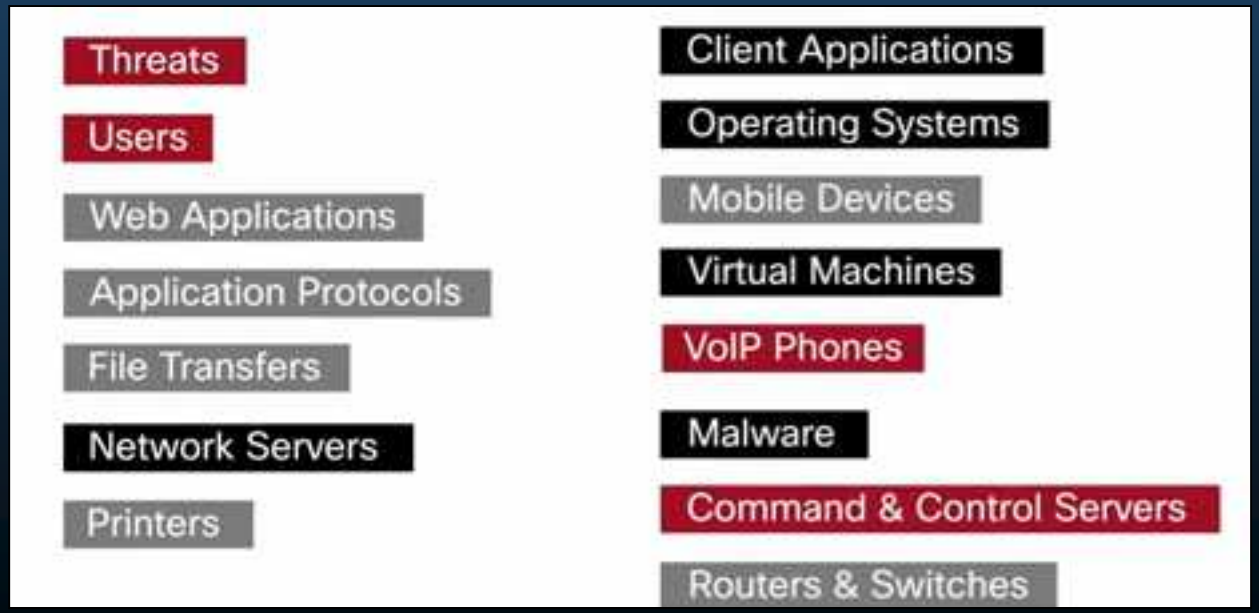
- Hypervisor crea switch virtual para interconectar ASAv y Hosts Virtuales (VMs todos).
- Soporta VPNs Sitio-a-Sitio y de Aceso-Remoto.
- No admite clústeres y múltiples contextos.





9.1Introducción a ASA.

- ASA de Siguiente Generación (con servicios FirePower).
  - Combina Firewall + Concentrador VPN + IPS en un mismo software.
    - Previamente, se tenían en tres difetrentes softwares/dispositivos.
  - Incrementa la Visibilidad (saber que sucede en cada momento)
  - Detecta y Prioriza Amenaza.
  - Simplifica Operaciones.
    - Centro de Administración Unificado:



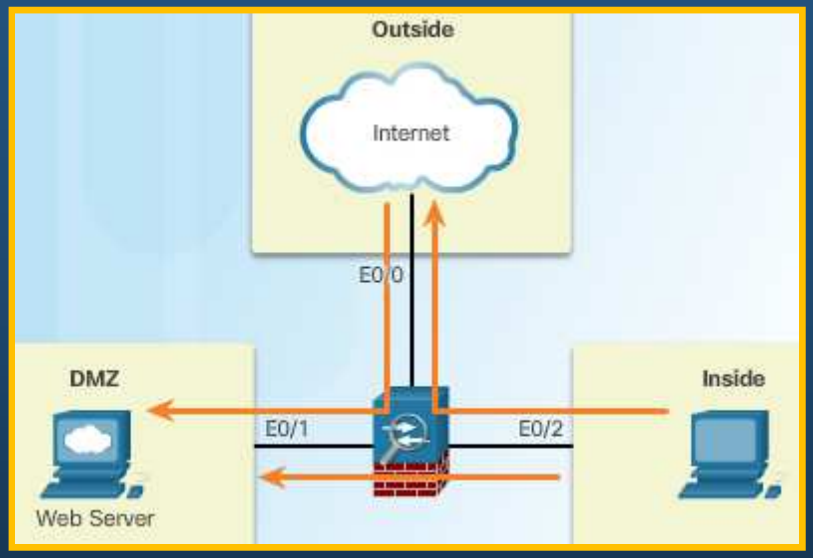
- https://static-course-assets.s3.amazonaws.com/CCNAS2/en/course/files/Introducing%20Cisco%20ASA%20with%20FirePOWER%20Services.pdf

9.1Introducción a ASA.

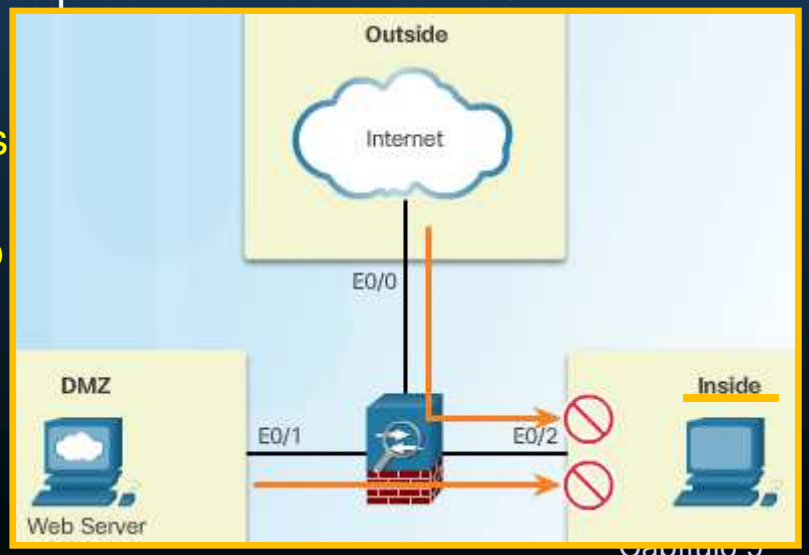
- Características Avanzadas de Firewall ASA.
  - Virtualización: Un solo ASA puede particionarse en varios.
    - Cada partición se denomina Contexto de seguridad.
    - Independientes entre sí, con sus propias políticas de seguridad.
    - Funciones no soportadas: VPNs y Enrutamiento dinámico.
  - Alta disponibilidad con conmutación por error: Dos ASAs redundantes.
    - Requiere sean idénticos en software, licenciamiento, memoria interfaces, módulos.
  - Firewall de Identidad. Control de Acceso por IP + Windows Active Directory.
    - Requiere autenticar mediante Active Directory para atravesar el firewall.
    - Puede intercalarse sin restricciones con reglas IP.
  - Control de Amenazas y Servicios de Contención: IPS básico.
    - IPS avanzado requiere módulos de hardware
      - AIP (Prevención e Inspección Avanzada)
      - Antimalwarare requiere módulos CSC (Control y Seguridad de Contenidos)
    - Incluyen mecanismos de detección para amenazas conocidas y desconocidas.
  - Fuera del alcance de este curso.

9.1Introducción a ASA.

- Firewall en un Diseño de Red.
  - Términos a Considerar:
    - Exterior. Zona fuera de la protección del firewall.
    - Interior: Zona protegida por firewall.
    - DMZ: Zona protegida, accesible tanto del exterior como del interior.

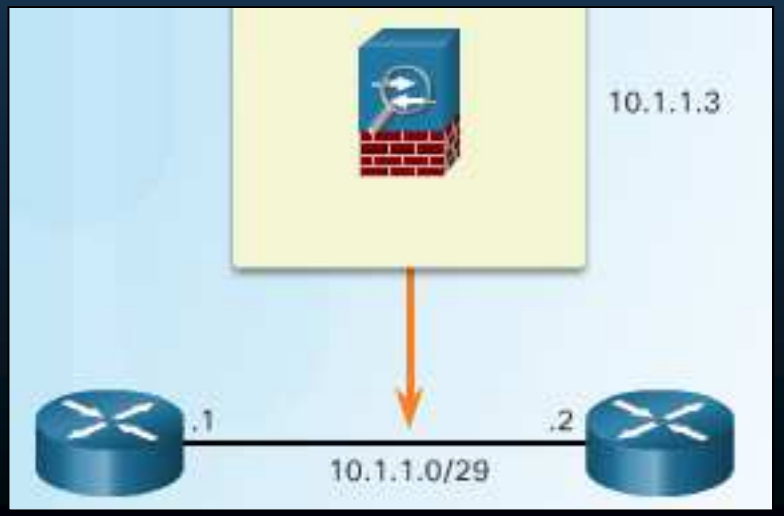


  - Firewall Protege usuarios internos de ataques internos/externos.
  - Características Router ISR:
    - Firewall por Pilíticas Basadas en Zonas (ZPF).
    - Control de Acceso basado en Contexto (CBAC).
  - ASA ofrece mismas características
    - Su configuración es diferente.
    - Diferentes Niveles de Seguridad.



9.1Introducción a ASA.

- Modos de Operación de un Firewall.
  - Enrutado.
    - Dos o más interfaces separan redes capa 3.
    - El ASA se considera un salto (router).
    - Puede realizar NAT.
    - Aplica políticas al tráfico que fluye por el firewall.
    - Se considera la implementación tradicional.
  - Transparente.
    - Conocido como “bache en el cable” o “cortafuegos furtivo”.
    - ASA actúa como dispositivo Capa 2, y no como un salto o router.
    - Se le asigna IP solo con propósitos administrativos.
    - Útil para no alterar direccionamiento IP.
    - No soporta enrutamiento dinámico, VPNs, QoS, o DHCP Relay.
    - Fuera del alcance de este capítulo.



9.1Introducción a ASA.

Licenses	Description (Base Lice	Licenses	Description (Security Plus Lic. in Plaintext)		
Firewall Licenses		**Firewall Licenses**			
Botnet Traffic Filter				Available	
Firewall Conns, Concurrent					
GTP/GPRS					
Intercompany Media Engine					
Unified Comm. Sessions					
VPN Licenses					
Adv. Endpoint Assessment					
AnyConnect Essentials					
AnyConnect Mobile					
AnyConnect Premium (sessions)					25
Combined VPN sessions of all types, Maximum					
Other VPN (sessions)					
VPN Load Balancing					
General Licenses					
Encryption					
Failover					
Interfaces of all types, Max.					
Security Contexts					
Users, concurrent					Unlimited
VLANs/Zones, Maximum				ilover link)	
VLAN Trunk, Maximum	No Support	VLAN Trunk, Maximum	8 trunks		

```
CCNAS-ASA# show version

<output omitted>

Licensed features for this platform:
Maximum Physical Interfaces       : 8              perpetual
VLANs                             : 3              DMZ Restricted
Dual ISPs                         : Disabled       perpetual
VLAN Trunk Ports                  : 0              perpetual
Inside Hosts                      : 10             perpetual
Failover                          : Disabled       perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 10             perpetual
Total VPN Peers                   : 12             perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual

This platform has a Base license.
```

9.1Introducción a ASA.

- Introducción al Cisco ASA 5505.
  - Ideal para pequeños negocios, trabajador a distancia y sucursales.
    - Firewall, VPN SSL, VPN IPsec, Servicios Modulares Plug&Play.

ASA 5505:
256/ 512 Mb RAM
128Mb Flash

Ranura SSC: Para Añadir funcionalidad IPS mediante AIP-SSC (Security Service Card).

Puerto Serie: Para configurar el ASA mediante consola.

Ranura de seguridad: Para colocar un cable de seguridad.

Conector de Energía: Para alimentar 48Vcd.

Puertos PoE 10/100: Para Conectar teléfonos o APs PoE.

Puertos Fast Eth 10/100: Para interconexión de hasta 3 zonas (VLANs).

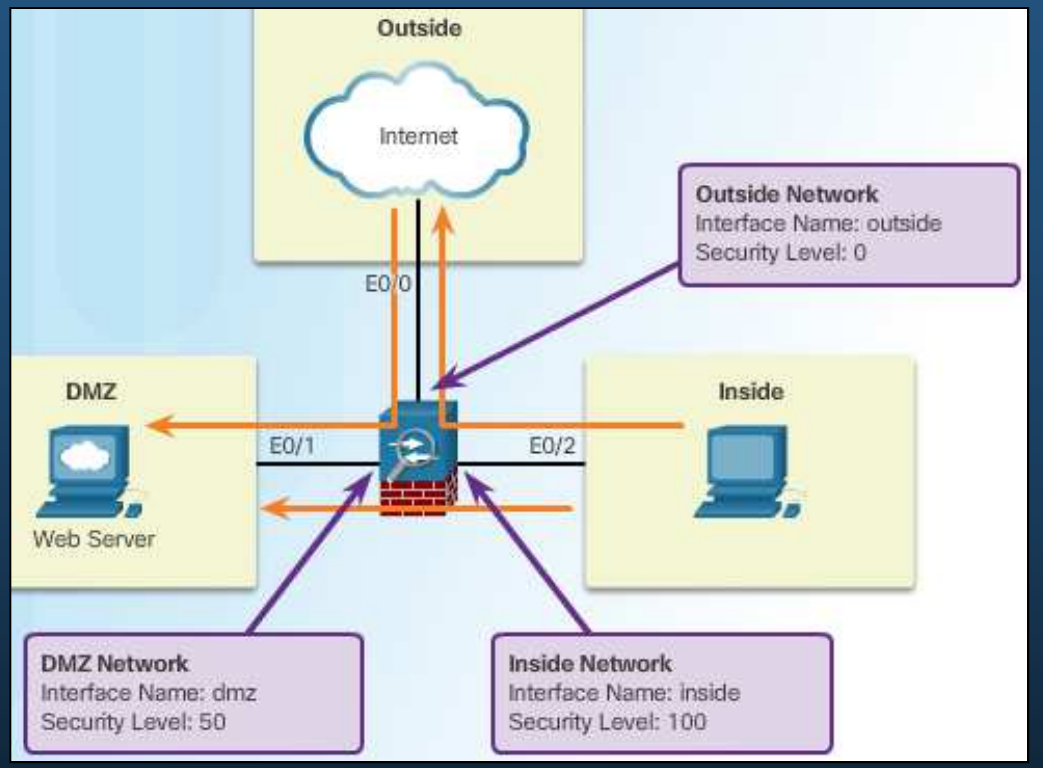
Botón Reset: Reinicia el dispositivo

Puertos USB v2: Incrementa capacidades y servicios

SSC(Security Service Card): Permite incorporar tarjetas para inspección y prevención avanzada.

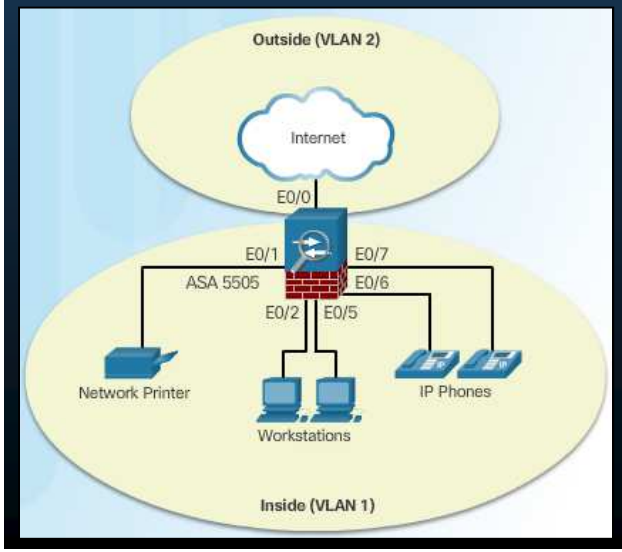
9.1Introducción a ASA.

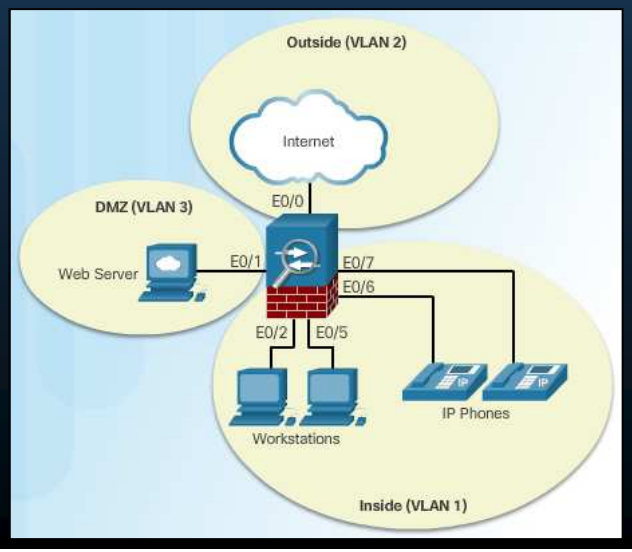
- Niveles de Seguridad ASA.
  - ASA establece niveles para definir el nivel de confiabilidad.
    - Desde 0 → No confiable, hasta 100 → Totalmente confiable.
    - Cada interface operacional debe tener un nombre y nivel de seguridad.
    - Ayudan a Controlar el tráfico de Red:
      - Acceso a la Red: Permite acceso a niveles superiores o iguales (=s solo si se especifica, si no bloquea x default).
      - Motor de inspección: define cuando inspeccionar tráfico en base a niveles, Vgr; mismo nivel, inspecciona tráfico en ambas direcciones.
      - Filtro de Aplicaciones: Filtra solo para conexiones salientes de un nivel superior a un inferior. Para mismo nivel puede filtrarse en una u otra dirección.
        - Requiere configurar ACL para permitir tráfico de nivel inferior a superior.

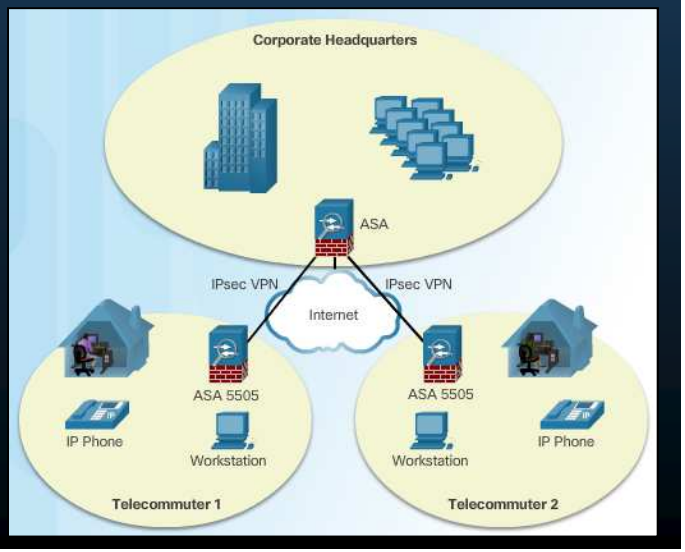


9.1Introducción a ASA.

- Escenarios de Implementación de ASA 5055.
  - Dispositivo de Seguridad de Frontera.
    - Conecta red Interna (VLAN 1 – Nivel Seg 100) con ISP (VLAN 2 – Nivel de Seg 0).
  - Pequeña Sucursal (3 Segmentos).
    - Red Interna (VLAN 1 – Nivel Seg. 100)
    - DMZ (VLAN3 – Nivel Seg. 50)
    - ISP (VLAN 2 – Nivel Seg. 0)
  - Desarrollo Empresarial.
    - Usado por trabajadores a distancia para acceder a red empresarial por VPN.







9.2 Configuración de ASA.

- Configuracion

Comandos Exclusivos de ASA

```
ciscoasa# conf t
ciscoasa(config)# show password encryption
Password Encryption: Disabled
Master key hash: Not set(saved)
ciscoasa(config)#
ciscoasa(config)# help write

USAGE:
          write erase|terminal|standby
          write net [<tftp_ip>]:<filename>
          write [memory]

DESCRIPTION:

write           Write config to net, flash, or terminal, or erase flash.
                Write without argument defaults to write memory

SYNTAX:

erase           Clears the flash memory configuration

terminal        Display the current active configuration, not necessarily
                the saved configuration

mem             Save the active configuration to the flash, so that it will
                be the active configuration after a reload

standby         Save the active configuration on the active unit to the
                flash on the standby unit

<--- More --->
```

Los comandos show ASA, pueden ejecutarse, sin importar el modo de configuración actual, incluso sin utilizar “do” como en un router/switch

El comando ASA “help” proporciona descripción básica sobre un comando y su sintaxis.

Comandos no disponibles en PacketTracer.

Para interrumpir el comando show, presione Q (No funciona Ctrl+C)

En PacketTracer se utiliza `interface` en lugar de `interfaces`.

9.2 Configuración de ASA.

- Configuración ASA por Defecto.

Nombre de dispositivo: `ciscoasa`
Contraseñas de linea y privilegiado: no configuradas (`Enter`).
E 0/0: VLAN 2 Exterior
E 0/1-7: VLAN 1 Interior

VLAN 1: Interior / NivSeg 100 / 192.168.1.1/24

VLAN 2: Exterior / NoivSeg 0 / IP por Cliente DHCP.

PAT Habilitado para traducir IPS Internas por la Externa obtenida por DHCP.

Acceso http habilitado para ASDM (GUI java para administrar ASA desde red interior).

Cliente dhcp debe configurar interface exterior.

Servidor dhcp debe proporcionar configuración IP a clientes Internos.

```
ciscoasa(config)#  configure factory-default
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
<output omitted>
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
<output omitted>
object network obj_any
 nat (inside,outside) dynamic interface
<output omitted>
http server enable
http 192.168.1.0 255.255.255.0 inside
<output omitted>
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
<output omitted>
```

9.2 Configuración de ASA.

- Asistente de Configuración ASA.
  - Configuración mediante Instrucciones Interactivas.
    - Desplegadas cuando el ASA es vaciado y reiniciado (**`write erase`** / **`reload`**)
      - Preguntará si se desea entrar al modo de configuración interactivo.
        - Responder "no", lleva directo a la CLI.
        - Responder "yes", Inicia las instrucciones interactivas:
        - Presionar ENTER, acepta la respuesta por defecto entre corchetes [ ]
        - Tras configurar, mostrará resumen y pedirá confirmar.

```
The following configuration will be used:
Enable password: cisco
Allow password recovery: yes
Clock (UTC): 12:00:00 April 1 2015
Firewall Mode: Routed
Management IP address: 192.168.1.1
Management network mask: 255.255.255.0
Host name: CCNAS-ASA
Domain name: ccnasecurity.com
IP address of host running Device Manager: 192.168.1.2

Use this configuration and save to flash? [yes]yes
INFO: Security level for "management" set to 0 by default.
WARNING: http server is not yet enabled to allow ASDM access.
Cryptochecksum: 81b18adc 335be94e 833731d1 b02031c1

2564 bytes copied in 1.480 secs (2564 bytes/sec)

Type help or '?' for a list of available commands.
CCNAS-ASA>
```

9.2 Configuración de ASA.

- Modo de Configuración Global (Configuración Inicial).

```
ciscoasa> enable
Password:
ciscoasa#
ciscoasa# clock set 12:00:00 1 April 2015
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)#

***************************** NOTICE *****************************

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: A
You will be reminded again in 7 days.

If you would like to enable this feature, issue the command
"call-home reporting anonymous".

Please remember to save your configuration.

ciscoasa(config)#
```

`enable` → Modo Privilegiado
`Password:` → `ENTER` (Por default, ninguno)

Imperativo establecer fecha y hora manualmente o mediante NTP.

`configure terminal` → Modo de configuración global

Al entrar por primera vez aal modo de configuración global, ASA ofrece diagnósticos y alertas en tiempo real.

Requiere ID de cisco.com
Y registro en SMARTnet

En PacketTracer, para establecer fecha y hora, debe entrarse primero al modo de configuración global

9.2 Configuración de ASA.

- Configuraciones Básicas.

```
ciscoasa(config)# hostname CCNAS-ASA
CCNAS-ASA(config)# domain-name ccnasecurity.com
CCNAS-ASA(config)# enable password class
CCNAS-ASA(config)#
CCNAS-ASA(config)# banner motd ------------------------------------------
CCNAS-ASA(config)# banner motd     Authorized access only!
CCNAS-ASA(config)# banner motd     You have logged into a secure device.
CCNAS-ASA(config)# banner motd ------------------------------------------
CCNAS-ASA(config)# bann
CCNAS-ASA(config)# exit
CCNAS-ASA# exit

Logoff

----------------------
    Authorized access o
    You have logged int
----------------------


Type help or '?' for a
CCNAS-ASA>
```

acteres.
gito y contener caracteres

```
CCNAS-ASA# show password encryption
Password Encryption: Disabled
Master key hash: Not set(saved)
CCNAS-ASA#
CCNAS-ASA# conf t
CCNAS-ASA(config)# key config-key password-encryption cisco123
CCNAS-ASA(config)# password encryption aes
CCNAS-ASA(config)# exit
CCNAS-ASA#
CCNAS-ASA# show password encryption
Password Encryption: Enabled
Master key hash: 0x45ebef8e 0x77a0f287 0x90247f80 0x2a184246 0xe85cbcc4(not saved)
CCNAS-ASA#
CCNAS-ASA# write
Building configuration...
Cryptochecksum: 99934042 e6c6b12b 607a9920 89d8a181

2359 bytes copied in 1.340 secs (2359 bytes/sec)
[OK]
CCNAS-ASA#
```

No disponibles en P.T.:

```
(config)# banner motd
(config)# key ...
(config)# password ...
# show password encryption
```

9.2 Configuración de ASA.

- Configuración de Interfaces VLAN Lógicas.
  - La Mayoría de ASAs serie 5500 tratan interfaces como router (Capa 3).
  - ASA 5505 trata sus 8 interfaces como switch (Capa 2).
    - Interfaces VLAN lógicas – SVI (Capa 3)
      - Nombre, nivel de seguridad, IP
    - Puertos Físicos Switcheados (Capa 2)
      - Se asignan a las interfaces VLAN lógicas.
      - Aplica políticas de seguridad para el tráfico Inter-VLAN

Comando ASA	Descripción
`interface vlan` *`vlan-num`*	Entra al modo de configuración SVI.
`nameif` *`if-name`*	Da nombre a la interface (48 caracteres, insensible a mayusculas).
`security-level` *`vlue`*	Establece nivel de seguridad (0 - 100).

    - Licencia Base no admite tres Interfaces VLAN completamente funcionales.
    - Admite tercera con funcionalidad limitada.
      - **`no forward interface vlan`** *`number`*
        - Antes del comando *`nameif`*
        - No puede iniciar tráfico a otra VLAN (Uso común para red Interna).

9.2 Configuración de ASA.

- Configuración de Interfaces VLAN Lógicas (Cont.).
  - Configuración de IP en interfaces para ASA 5505.

Configuración	Comando ASA	Descripción
Manual	`ip address` *`dirección-ip mascara`*	Asigna IP y mascara a la interface.
Mediante DHCP	`ip address dhcp`	Configura mediante DHCP.
	`ip address dhcp setroute`	Configura mediante DHCP y establece ruta por defecto hacia el dispositivo superior.
Mediante PPPOE	`ip address pppoe`	Configura mediante PPPOE.
	`ip address pppoe setroute`	Configura mediante PPPOE y establece ruta por defecto hacia el dispositivo superior.

```
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA(config-if)# security-level 100
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA(config-if)# security-level 0
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
```

9.2 Configuración de ASA.

- Acceso a VLANs en Puertos Capa 2.
  - Por defecto, todos los puertos se asignan a VLAN 1.
  - Pueden cambiarse similar a un Switch Cisco (importante `no shut` en `SVI` e `if`).

```
CCNAS-ASA(config)# interface e0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config-if)# interface e0/1
CCNAS-ASA(config-if)# switchport access vlan 1
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
```

Verificación de configuraciones VLAN

```
CCNAS-ASA# show switch vlan
VLAN Name            Status    Ports
---- --------------- --------- -------------------------------
1    inside          up        Et0/1, Et0/2, Et0/3, Et0/4
                               Et0/5, Et0/6, Et0/7
2    outside         up        Et0/0
CCNAS-ASA#
```

Despliega estado de todas las interfaces

```
CCNAS-ASA# show interface ip brief
Interface              IP-Address      OK? Method Status    Protocol
Ethernet0/0            unassigned      YES unset  up        up
Ethernet0/1            unassigned      YES unset  up        up
Ethernet0/2            unassigned      YES unset  up        up
Ethernet0/3
Ethernet0/4
Ethernet0/5
Ethernet0/6
Ethernet0/7
Internal-Data
Internal-Data
Vlan1
Vlan2
Virtual0
CCNAS-ASA#
```

Despliega información de interfaces Capa 3

```
CCNAS-ASA# show ip address
System IP Addresses:
Interface              Name            IP address      Subnet mask     Method
Vlan1                  inside          192.168.1.1     255.255.255.0   manual
Vlan2                  outside         209.165.200.226 255.255.255.248 manual
Current IP Addresses:
Interface              Name            IP address      Subnet mask     Method
Vlan1                  inside          192.168.1.1     255.255.255.0   manual
Vlan2                  outside         209.165.200.226 255.255.255.248 manual
CCNAS-ASA#
```

9.2 Configuración de ASA.

- Configuración de Rutas Estáticas.
  - Como cliente DHCP puede recibir ruta por defecto de un dispositivo superior.
  - De otro modo de configurarse manualmente y verificarse:
    - **ASA(config)# route** *interface-name* **0.0.0.0 0.0.0.0** *next-hop-ip-address*
    - **ASA# show route**

```
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
CCNAS-ASA(config)#
CCNAS-ASA(config)# show route | begin Gateway
Gateway of last resort is 209.165.200.225 to network 0.0.0.0

S*    0.0.0.0 0.0.0.0 [1/0] via 209.165.200.225, outside
C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside
C        209.165.200.224 255.255.255.248 is directly connected, outside
L        209.165.200.226 255.255.255.255 is directly connected, outside

CCNAS-ASA(config)#
```

9.2 Configuración de ASA.

- Configuración de Servicios de Acceso Remoto.
  - Telnet:

Comando ASA	Descripción
[**passwd** | **password**] *contraseña*	Establece contraseña de logueo (hasta 80 caracteres).
telnet {*dir_ipv4 mascara* | *dir_ipv6/prefijo*} *nombre_if*	Identifica que Ips pueden hacer telnet al ASA. Y desde qué interface. Remover con: **clear configure telnet**
telnet timeout *minutos*	Por defecto las sesiones telnet inactivas por 5 minutos se cierran. El comando altera la cantidad de minutos.
aaa authentication telnet console LOCAL	Indica a telnet autenticar contra la base de datos local.
clear configure telnet	Elimina conexiones telnet de la configuración.

```
CCNAS-ASA(config)# password cisco
CCNAS-ASA(config)# telnet 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)# telnet timeout 3
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run telnet
telnet 192.168.1.3 255.255.255.255 inside
telnet timeout 3
CCNAS-ASA(config)#
```

No disponible en P.T.

9.2 Configuración de ASA.

- Configuración de Servicios de Acceso Remoto (Cont.).
  - SSH:

Comando ASA	Descripción
username *nombre* **password** *contraseña*	Crea entrada en la base de datos local.
aaa authentication ssh console LOCAL	
crypto key generate rsa modulus *tamaño_modulo*	
ssh {*dir_ipv4 mascara* | *dir_ipv6/prefijo*} *nombre_if*	
ssh version *versión*	
ssh timeout *minutos*	
clear configure ssh	

No disponible en P.T.

```
CCNAS-ASA(config)# username ADMIN password class
CCNAS-ASA(config)#
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
CCNAS-ASA(config)#
CCNAS-ASA(config)# crypto key generate rsa modulus 2048
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
CCNAS-ASA(config)#
CCNAS-ASA(config)# ssh 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)# ssh 192.168.1.4 255.255.255.255 inside
CCNAS-ASA(config)# ssh 172.16.1.3 255.255.255.255 outside
CCNAS-ASA(config)#
CCNAS-ASA(config)# ssh version 2
CCNAS-ASA(config)#
CCNAS-ASA(config)# show ssh
Timeout: 5 minutes
Version allowed: 2
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
172.16.1.3 255.255.255.255 outside
CCNAS-ASA(config)#
```

9.2 Configuración de ASA.

- Configuración de Network Time Protocol - NTP.
  - ASA cuenta con cliente NTP para obtener fecha y hora.

Comando ASA	Descripción
ntp authenticate	Habilita autenticación con el servidor NTP.
ntp trusted-key *id-llave*	Especifica un identificador de llave para autenticar con el servidor NTP.
ntp authentication-key *id-llave* **md5** *llave*	Asocia una llave al identificador de llave indicado, para autenticar con el servidor NTP.
ntp server *dir_ip* [**key** *id_llave*]	Especifica el servidor NTP y credenciales para autenticar.

```
CCNAS-ASA(config)# ntp authenticate
CCNAS-ASA(config)# ntp trusted-key 1
CCNAS-ASA(config)# ntp authentication-key 1 md5 cisco123
CCNAS-ASA(config)# ntp server 192.168.1.254
CCNAS-ASA(config)#
```

9.2 Configuración de ASA.

No disponible en P.T.

- Configuración de Servicios DHCP.
  - Servidor DHCP.

Verificación:
- `show dhcpd status`
- `show dhcpd binding`
- `show dhcpd statistics`

Comando ASA	Descripción
dhcpd address *dir_ip_1 [-dir_ip_2] nombre_if*	Crea un rango de IPs a ofertar por DHCP en una interface. El rango debe coincidir con la subred configurada en la interface.
dhcpd dns *dns1 [dns2]*	Especifica la dirección de hasta 2 servidores DNS.
dhcpd lease *segundos*	Cambia la cantidad de segundos en el que un cliente podrá utilizar su configuración IP (1 hora por defecto) (0 – 1,048,575).
dhcpd domain *nombre_dominio*	Especifica el nombre de dominio asignado al cliente.
dhcpd enable *nombre_if*	Habilita demonio DHCP en interface especificada (interna, usualmente).

Habilitar Cliete DHCP en outside
`dhcpd auto_config outside`

```
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.100
ERROR: % Incomplete command
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.100 inside
Warning, DHCP pool range is limited to 32 addresses, set address range as:
192.168.1.10-192.168.1.41
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.41 inside
CCNAS-ASA(config)# dhcpd lease 1800
CCNAS-ASA(config)#
```

Licencia Base admite solo 32 IPs en Pool DHCP y salida solo a 10 clientes simultáneos.

9.2 Configuración de ASA.

- Introducción a Objetos y Grupos de Objetos.
  - Los objetos se crean para usarse en lugar de direcciones IP.
    - Pueden ser: rangos de direcciones, protocolos, o rangos de puertos.
    - Pueden usarse en múltiples configuraciones.
    - Alterar un objeto, altera automáticamente todas las reglas que usen el objeto.
    - Los objetos pueden añadirse o retirarse de grupos de objetos.
    - Pueden usarse en NAT, ACLs y grupos de objetos.
    - Dos tipos principales:
      - Network: IP y mascara.
      - Service: Protocolo y opcionalmente rango de puertos.
  - En ASA la configuración de NAT requiere el uso de objetos `network`.

En P.T. sólo están disponibles `network` para `object` y `service` para `object-group`

```
CCNAS-ASA(config)# object ?

configure mode commands/options:
  network  Specifies a host, subnet or range IP addresses
  service  Specifies a protocol/port
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group ?

configure mode commands/options:
  icmp-type  Specifies a group of ICMP types, such as echo
  network    Specifies a group of host or subnet IP addresses
  protocol   Specifies a group of protocols, such as TCP, etc
  service    Specifies a group of TCP/UDP ports/services
  user       Specifies single user, local or import user group
CCNAS-ASA(config)#
```

9.2 Configuración de ASA.

- Configuración de Objetos "network".
  - Creación del objeto network:
    - **ASA(config)# object network** nombre-objeto
    - **ASA(config-network-object)#**
  - Cada objeto network puede contener solo una definición de las mostradas:
    - Una segunda entrada sobre-escribe la anterior.

Comando ASA	Descripción
host	
subnet	
range	

```
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.3
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object network EXAMPLE-1
 host 192.168.1.3
CCNAS-ASA(config)#
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.4
CCNAS-ASA(config-network-object)# range 192.168.1.10 192.168.1.20
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object network EXAMPLE-1
 range 192.168.1.10 192.168.1.20
CCNAS-ASA(config)#
```

  - Eliminación de un objeto
    - **ASA(config)# no**
  - Eliminación de todos lo
    - **ASA(config)# cl**

9.2 Configuración de ASA.

- Configuración de Objetos "`service`". No disponible en P.T.
  - Creación del objeto `service`:
    - **`ASA(config)# object service`** `nombre-objeto`
    - **`ASA(config-service-object)#`**
  - Cada objeto `service` puede contener solo una definición de las mostradas:
    - Una segunda entrada sobre-escribe la anterior.

Comando ASA	Descripción
service protocolo [**source** [*operador port*]] [**destination** [*operador port*]]	Especifica un protocolo IP por nombre o número.
service tcp [**source** [*operador port*]] [**destination** [*operador port*]]	Especifica objeto servicio para el protocolo TCP.
service udp [**source** [*operador* [**destination** [*operador port*]]	
service icmp *tipo_icmp*	
service icmp6 *tipo_icmp6*	

```
CCNAS-ASA(config)# object service SERV-1
CCNAS-ASA(config-service-object)# service tcp destination eq ftp
CCNAS-ASA(config-service-object)# service tcp destination eq www
CCNAS-ASA(config-service-object)# exit
CCNAS-ASA(config)# show running-config object service
object service SERV-1
 service tcp destination eq www
CCNAS-ASA(config)#
```

  - Operadores disponibles
    - `eq` (=), `neq` (!=), `lt` (<), `gt`(>), `range` (rango)

9.2 Configuración de ASA.

- Grupos de Objetos.
  - Los grupos de objetos pueden usarse en reglas/politicas, en lugar de poner una por cada objeto.
  - Tipos:
    - Network: lista de IPs, subredes, o rangos de direcciones.
    - Service: agrupación de protocolos y puertos variados.
    - Security: Para usarse con TrustSec, al incluir el grupo en ACLs.
    - ICMP-Type: Para definir tipos de icmp necesarios.
    - User: Para grupos de usuarios por Active Dorectory (firewall de identidad).
  - Guias y Limitaciones:
    - Objetos y Grupos de Objetos comparten el espacio de nombres entre si.
    - Los grupos de objetos deben tener nombres únicos.
    - Un grupo de objetos no puede ser removido o vaciado si está siendo usado.
    - ASA no soporta grupos de objetos anidados IPv6.

9.2 Configuración de ASA.

- Configuración Común de Grupos de Objetos.

```
CCNAS-ASA(config)# object-group network ADMIN-HOST
CCNAS-ASA(config-network-object-group)# description Administrative hosts
CCNAS-ASA(config-network-object-group)# network-object host 192.168.1.3
CCNAS-ASA(config-network-object-group)# network-object host 192.168.1.4
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)# object-group network ALL-HOSTS
CCNAS-ASA(config-network-object-group)# description All inside hosts
CCNAS-ASA(config-network-object-group)# network-object 192.168.1.32 255.255.255.240
CCNAS-ASA(config-network-object-group)# group-object ADMIN-HOST
```

```
CCNAS-ASA(config)# object-group service SERVICES-1
CCNAS-ASA(config-service-object-group)# service-object tcp destination eq www
CCNAS-ASA(config-service-object-group)# service-object tcp destination eq https
CCNAS-ASA(config-service-object-group)# service-object tcp destination eq pop3
CCNAS-ASA(config-service-object-group)# service-object udp destination eq ntp
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service SERVICES-2 tcp
CCNAS-ASA(config-service-object-group)# port-object eq www
CCNAS-ASA(config-service-object-group)# port-object eq smtp
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service SERVICES-3 tcp
CCNAS-ASA(config-service-object-group)# group-object SERVICES-2
CCNAS-ASA(config-service-object-group)# port-object eq ftp
CCNAS-ASA(config-service-object-group)# port-object range 2000 2005
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
```

P.T. sólo soporta números de puerto

```
MP-ALLOWED
ject echo
ject time-exceeded

-group id ICMP-ALLOWED
```

inición}

o

lefinición}

9.2 Configuración de ASA.

- ACLs en ASA.
  - Similares a ACLs de routers en:
    - Ambas se componen de ACEs .
      - Las ACEs se aplican a protocolo, IP origen/destino, red, puertos origen/destino.
    - Se procesan secuencialmente de arriba hacia abajo.
    - Una coincidencia sale y termina la verificación del resto de ACEs.
    - `deny any` implícito al final.
    - Pueden agregarse comentarios.
    - Una sola ACL por interface, por protocolo y por dirección.
    - Pueden habilitarse/deshabilitarse por rangos de tiempo.
  - Diferentes a ACLs de routers en:
    - Uso de mascaras en lugar de wildcards.
    - Las ACLs son nombradas, en lugar de numeradas.
    - Por defecto, los niveles de seguridad aplican control de acceso sin necesidad de configurar una ACL.

9.2 Configuración de ASA.

- Tipos de Filtrados ACLs en ASA.
  - Filtrado a-través: Filtra tráfico que pasa de una interface a otra del ASA.
    - Crear ACL, asignar a una interface.
  - Filtrado a la caja: Filtra tráfico destinado al ASA.
  - ASAs se diferencian de otros dispositivos por los niveles de seguridad.
    - Controlan tráfico sin necesidad de ACLs.
      - Admite tráfico a interfaces de niveles mas seguros.
      - Bloquea tráfico de interfaces de niveles menos seguros.
  - Permitir tráfico entre niveles de seguridad iguales:
    - `ASA(config)# same-security-traffic permit inter-interface`
  - Permitir que tráfico entre y salga por la misma interface:
    - `ASA(config)# same-security-traffic permit intra-interface`

No disponibles en P.T.

9.2 Configuración de ASA.

- Tipos de ACLs en ASA.
  - Extendidas.
    - Contiene una o mas ACEs para especificar direcciones origen y destino, protocolos y puertos.
  - Estándar.
    - Identifican solo direcciones IP **destino**. Típicamente para filtrar redistribución OSPF. No pueden asignarse a interfaces para controlar tráfico.
  - EtherType.
    - Solo para aparatos que trabajan en modo transparente (Capa 2).
  - WebType.
    - Para configuraciones que soportan filtrado VPN SSL sin clientes.
  - IPv6.
    - Para determinar que tráfico IPv6 bloquear y/o permitir en interfaces enrutadas.
  - Consultar Sintaxis: `ASA# help access-list`
  - Solo Extendidas en este curso.

9.2 Configuración de ASA.

- Configuración de ACLs.
  - Sintaxis con demasiados parámetros.
    - Versión condensada:

Nombre de la ACL, puede ser un número

Vgr; IP, TCP, UDP

Origen del tráfico a filtrar: any, host, objeto network o nombre de interface (solo para filtrado a la caja)

```
access-list id extended {deny | permit} protocol
{source_addr source_mask | any | host src_host | interface src_if_name}
[operator port [port]]
{dest_addr dest_mask} | any | host dst_host | interface dst_if_name}
[operator port [port]]
```

Operador de puerto origen, usado en conjunto con un puerto origen, `eq` (=), `neq` (!=), `lt` (<), `gt`(>), `range` (rango)

Destino del tráfico a filtrar: any, host, objeto network o nombre de interface (solo para filtrado a la caja)

    - Adicionalmente
      - `log`: permite colocar elementos SysLog, como severidad, e intervalo de log.
      - `time range`: especifica un rango de tiempo para la ACE.

No disponibles en P.T.

9.2 Configuración de ASA.

- Aplicación de ACLs.

```
access-group id { in | out } interface if_name [ per-user-override | control-plane ]
```

Sintaxis
access-group
id
in
out
interface
if_name
per-user-override
control-plane

ACL, evita que 192.168.1.0/24 accese a 209.165.201.0/27.
A los hosts internos se les permite accede a cualquier otra dirección.
Cualquier otro tráfico es denegado.

```
access-list ACL-IN extended deny tcp 192.168.1.0 255.255.255.0 209.165.201.0
255.255.255.224
access-list ACL-IN extended permit ip any any
access-group ACL-IN in interface inside
```

ACL, permite que 192.168.1.0/24 accese a 209.165.201.0/27.
Cualquier otro tráfico es denegado.

```
access-list ACL-IN extended permit ip 192.168.1.0 255.255.255.0 209.165.201.0
255.255.255.224
access-group ACL-IN in interface inside
```

ACL, evita que hosts internos accedan al servidor web 209.165.201.29.
A los hosts internos se les permite acceder a cualquier otro servicio en 209.165.201.29.
A hosts internos se les permite acceder a cualquier otra dirección
Cualquier otro tráfico es denegado.

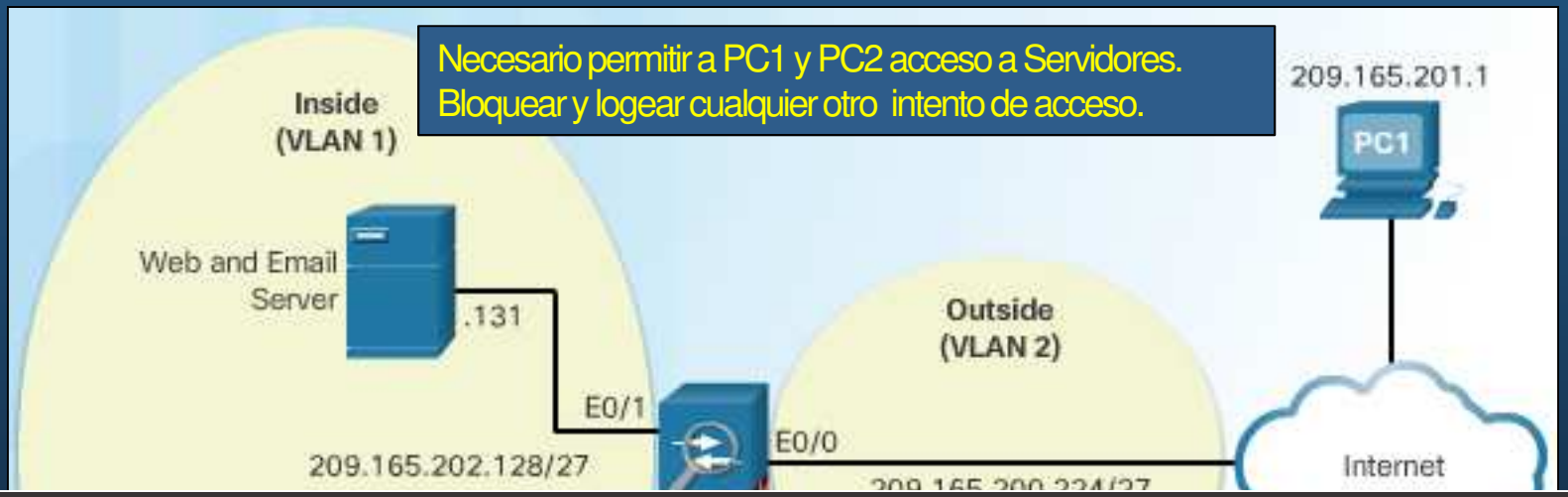
```
access-list ACL-IN extended deny tcp any host 209.165.201.29 eq www
access-list ACL-IN extended permit ip any any
access-group ACL-IN in interface inside
```

ACL, permite a todos los hosts de la red interna pasar por el ASA.

```
access-list ACL-IN extended permit ip any any
access-group ACL-IN in interface inside
```

9.2 Configuración de ASA.

- ACLs y Grupos de Objetos.




```
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-1 -> Server A for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-1 -> Server B for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-2 -> Server A for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-2 -> Server B for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq smtp
CCNAS-ASA(config)# access-list ACL-IN extended deny ip any any log
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-group ACL-IN in interface outside
CCNAS-ASA(config)#
```

Dos ACEs para acceso de cada PC.

9.2 Configuración de ASA.

- Ejemplos de ACLs usando Grupos de Objetos.
  - E

```
CCNAS-ASA(config)# show running-config access-list
access-list ACL-IN remark Only permit PC-A / PC-B -> Internal Servers
access-list ACL-IN extended permit tcp object-group NET-HOSTS object-group SERVERS
object-group HTTP-SMTP
CCNAS-ASA(config)#
```

No disponibles en P.T. (sólo object)

sts externos
cios.

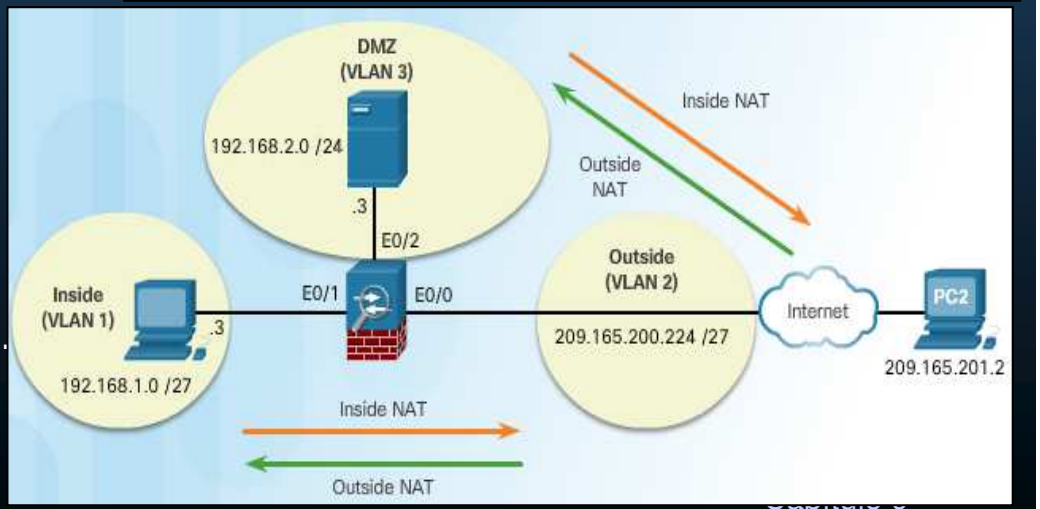
```
CCNAS-ASA(config)# object-group network NET-HOSTS
CCNAS-ASA(config-network-object-group)# description OG matches PC-A and PC-B
CCNAS-ASA(config-network-object-group)# network-object host 209.165.201.1
CCNAS-ASA(config-network-object-group)# network-object host 209.165.201.2
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group network SERVERS
CCNAS-ASA(config-network-object-group)# description OG matches Web / Email Servers
CCNAS-ASA(config-network-object-group)# network-object host 209.165.202.131
CCNAS-ASA(config-network-object-group)# network-object host 209.165.202.132
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service HTTP-SMTP tcp
CCNAS-ASA(config-service-object-group)# description OG matches SMTP / WEB traffic
CCNAS-ASA(config-service-object-group)# port-object eq smtp
CCNAS-ASA(config-service-object-group)# port-object eq www
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-list ACL-IN remark Only permit PC-A / PC-B -> Internal Servers
CCNAS-ASA(config)#  access-list ACL-IN extended permit tcp object-group NET-HOSTS
object-group SERVERS object-group HTTP-SMTP
```

9.2 Configuración de ASA.

- Introducción de NAT para ASA.
  - NAT Interno.
    - Tráfico de interface de alto nivel de seguridad destinado a interface de bajo nivel de seguridad.
    - Traduce dirección del host interno a dirección global. Restaura IP original al retornar el tráfico.
  - NAT Externo.
    - Tráfico de interface de bajo nivel de seguridad destinado a interface de alto nivel de seguridad.
    - Permite que un host externo aparentar pertenecer a la red interna.
  - NAT Bidireccional.
    - Uso de NAT Interno y Externo en conjunto.

Dos veces NAT (Twice): Identifica origen y destino en una sola regla. Usado al configurar VPNs. Fuera del alcance del curso.

  - Tipos de NAT (Network Object).
    - NAT Dinámico: Muchos a muchos.
    - PAT Dinámico: Muchos a uno.
    - NAT Estático: Uno a uno.
    - NAT Política: Basado en reglas. Solo ciertos orígenes a ciertos destinos serán traducidos.



9.2 Configuración de ASA.

- Configuración de NAT Dinámico.
  - Requiere unir dos objetos network.
    - Pool de direcciones públicas a traducir por internas (`range` | `subnet`).
    - Direcciones internas a ser traducidas (`range` | `subnet`).
      - Establece unión: (**`nat`** (*`real-ifc`*, *`mapped-ifc`*) **`dynamic`** *`mapped-obj`*)

No disponible en P.T. (sólo interface)

Los hosts internos (192.168.1.0/27) serán traducidos a

248).

Verificación de traducciones.

```
CCNAS-ASA(config)# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

NAT from inside:192.168.1.3 to outside:209.165.200.242 flags i idle 0:00:02 timeout 3:00:00
CCNAS-ASA(config)#
CCNAS-ASA(config)# show nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic DYNAMIC-NAT PUBLIC
    translate_hits = 1, untranslate_hits = 1
CCNAS-ASA(config)#
CCNAS-ASA(config)# show nat detail

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic DYNAMIC-NAT PUBLIC
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.1.0/27, Translated: 209.165.200.240-209.165.200.248
CCNAS-ASA(config)#
```

9.2 Configuración de ASA.

- Configuración de PAT Dinámico.
  - Variante con sobrecarga: **`nat`** (*`real-ifc`*, *`mapped-ifc`*) **`dynamic interface`**

Los hosts internos (192.168.1.0/27) serán traducidos a la dirección pública de E0/0 (`outside`).

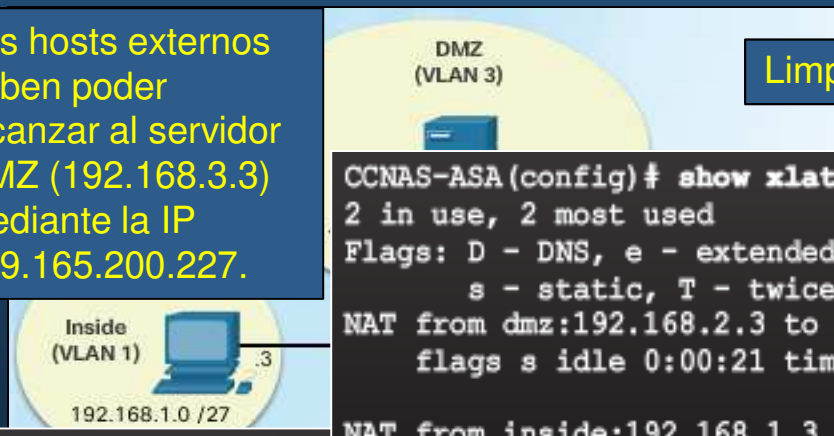
```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```

```
CCNAS-ASA# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

ICMP PAT from inside:192.168.1.3/1 to outside:209.165.200.226/1 flags ri idle
 0:00:02 timeout 0:00:30
CCNAS-ASA#
```

9.2 Configuración de ASA.

- Configuración de NAT Estático.
  - Mapeo de una dirección interna a una dirección externa.
    - `ASA(conf-net-obj)# nat (real-ifc,mapped-ifc) static mapped-inline-host-ip`

Los hosts externos deben poder alcanzar al servidor DMZ (192.168.3.3) mediante la IP 209.165.200.227.



Limpiar contadores NAT: `ASA(config)#clear nat counters`

Muestra de traducciones y detalles

```
CCNAS-ASA(config)# show xlate
2 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from dmz:192.168.2.3 to outside:209.165.200.227
    flags s idle 0:00:21 timeout 0:00:00

NAT from inside:192.168.1.3 to outside:209.165.200.242 flags i idle 0:09:06 timeout
 3:00:00
CCNAS-ASA(config)#
CCNAS-ASA(config)# show nat detail

Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static DMZ-SERVER 209.165.200.227
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.2.3/32, Translated: 209.165.200.227/32
2 (inside) to (outside) source dynamic DYNAMIC-NAT PUBLIC
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.1.0/27, Translated: 209.165.200.240-209.165.200.248
CCNAS-ASA(config)#
```

```
CCNAS-ASA(config)# int
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)#
INFO: Security level
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)#
CCNAS-ASA(config)#
CCNAS-ASA(config)# int
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)#
CCNAS-ASA(config)#
```

```
CCNAS-ASA(config)#
```

9.2 Configuración de ASA.

- AAA en ASA.
  - Asegura que solo usuarios autenticados y autorizados puedan conectarse al ASA.
  - Autenticación: Requiere credenciales válidas de usuarios (¿Quién es?).
    - Usuario y Contraseña: Telnet, SSH, Consola, ASDM – HTTPS, Modo Privilegiado.
    - Puede usarse independiente o con Autorización y Auditoria de cuenta.
  - Autorización: Controla los permisos de usuarios autenticados (¿Qué puede hacer?):
    - Controla accesos de red, accesos VPN, servicios, comandos disponibles.
    - Requiere Autenticación previa.
  - Auditoria de cuentas: Registra actividades de usuarios (¿Qué hizo?).
    - Registra: Inicio y fin de sesión, nombre de usuario, bytes transmitidos al ASA, servicios utilizados, duración de la sesión.
    - Puede usarse independiente o con Autenticación y Autorización.

9.2 Configuración de ASA.

Parámetros subrayados, No disponibles en P.T.

- Base de Datos Local y Servidores.
  - AAA puede autenticar contra base de datos local o externa.
    - Local (Base de Datos en el Dispositivo, Ideal para redes pequeñas)
      - ASA requiere AAA para autenticar.
      - Administración de usuarios:
        - ASA(conf)# **username** *name* **password** *password* [**privilege** *priv-level*]
        - ASA
        - ASA
    - Servidor RA

Comando ASA
aaa-server *et… protocolo*
aaa-server *et… [(nombre_inte… {ip_servidor*

```
CCNAS-ASA(config)# username Admin password class privilege 15
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run username
username Admin password obYXcKAuUW.jT5NE encrypted privilege 15
CCNAS-ASA(config)#
CCNAS-ASA(config)# aaa-server TACACS-SVR protocol tacacs+
CCNAS-ASA(config-aaa-server-group)# aaa-server TACACS-SVR (dmz) host 192.168.2.3
CCNAS-ASA(config-aaa-server-host)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run aaa-server
aaa-server TACACS-SVR protocol tacacs+
aaa-server TACACS-SVR (dmz) host 192.168.2.3
 key *****
CCNAS-ASA(config)#
```

- Eliminar configuraciones de servidor: ASA(conf)# **clear config aaa-server**
- Ver configuración: ASA# **show running-config aaa-server**

9.2 Configuración de ASA.

- Configuración AAA.
  - Autenticación.

P.T. sólo admite:
telnet | ssh
LOCAL

```
ASA(config)# aaa authentication { serial | enable | telnet | ssh | http } console
                                { LOCAL | server-group [ LOCAL ]}
```

```
CCNAS-ASA(config)# aaa authentication http console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication enable console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication http console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication serial console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication ssh console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication telnet console TACACS-SVR LOCAL
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run aaa
aaa authentication enable console TACACS-SVR LOCAL
aaa authentication http console TACACS-SVR LOCAL
aaa authentication serial console TACACS-SVR LOCAL
aaa authentication ssh console TACACS-SVR LOCAL
aaa authentication telnet console TACACS-SVR LOCAL
CCNAS-ASA(config)# exit
CCNAS-ASA# disable
CCNAS-ASA> exit

Logoff

Username: Admin
Password: *****
Type help or '?' for a list of available commands.
CCNAS-ASA>
```

Eliminar parámetros AAA:

No disponible en P.T.

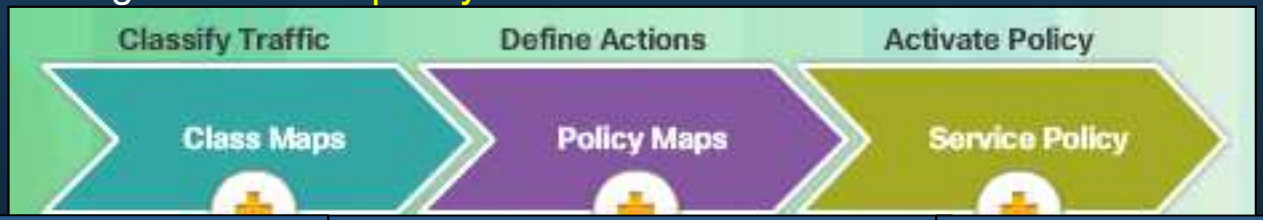
```
ASA(config)# clear config aaa
```

Ver cuentas de usuario:

```
ASA(config)# show running-config username
```

9.2 Configuración de ASA.

- Introducción a MPF.
  - Marco de Trabajo de Políticas Modular (MPF).
    - Define un conjunto de reglas para aplicar características de firewall (filtrar tráfico).
    - Clasifica granularmente flujos de tráfico, para aplicación de políticas.
    - Usado con módulos de hardware (redirigir tráfico a módulos)
  - Pasos para configurar:
    - 1. Configurar ACLs; 2. Configurar class-map; 3. Configurar policy-map; 4. Configurar service-policy



Mapas de Clases:
Identifica tráfico en el que trabaja MPF (interesante).
Crea un mapa de clases Capas 3 / 4 con criterios de concordancia.

`class-map` *`nombre-clase`*

Mapas de Políticas:
Define políticas para tráfico de Capas 3 - 7.
Crea un mapa de políticas para múltiples mapas de clases con acciones asociadas.

`policy-map` *`nombre-politica`*

Servicio de Políticas:
Activa mapa de políticas en interfaces.
Crea un servicio de políticas aplicando mapas de políticas a interfaces.

`Service policy` *`nombre`*
`interface` *`nombre_if`*

9.2 Configuración de ASA.

- Configuración de Mapas de Clases.
  - Identifican tráfico en capas 3-4.
  - Crea
    -
    -
    -
  - Verif
    -

Subrayados, No disponibles en P.T.

Nombres de Clases Reservados:

```
CCNAS-ASA(config)# access-list UDP permit udp any any
CCNAS-ASA(config)# access-list TCP permit tcp any any
CCNAS-ASA(config)# access-list SERVER permit ip any host 10.1.1.1
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-TCP
CCNAS-ASA(config-cmap)# description "This class-map matches all TCP traffic"
CCNAS-ASA(config-cmap)# match access-list TCP
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-UDP
CCNAS-ASA(config-cmap)# description "This class-map matches all UDP traffic"
CCNAS-ASA(config-cmap)# match access-list UDP
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-HTTP
CCNAS-ASA(config-cmap)# description "This class-map matches all HTTP traffic"
CCNAS-ASA(config-cmap)# match port TCP eq http
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map TO-SERVER
CCNAS-ASA(config-cmap)# description "Class map matches traffic    10.1.1.1"
CCNAS-ASA(config-cmap)# match access-list SERVER
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
```

9.2 Configuración de ASA.

- Definir y Activar una Política.
  - Los Mapas de Políticas asocian mapas de clases con acciones.
    - Creación: `ASA(conf)#` **`policy-map`** *`nombre-mapa-política`*
    - Descripción: `ASA(conf-pmap)#` **`description`** *`descripción`*
    - Liga Clase: `ASA(conf-pmap)#` **`class`** *`nombre-mapa-clase`*
    - Acciones:
      ```
      ASA(conf-pmap-c)# set connection
      ASA(conf-pmap-c)# inspect
      ASA(conf-pmap-c)# police
      ```
    - Verificar: `ASA#` **`show running-config policy-map`**
    - Vaciar configuración: `ASA#` **`clear configure policy-map`**
    - Activar Políticas: `ASA(conf)#` **`service-policy`** *`policy-map-name`* [**`global`** | **`interface`** *`intf`*]

Subrayados, No disponibles en P.T.

Nombres de 40 caracteres

64 mapas de políticas máximo

Varias clases x política

Varias acciones x clase

```
CCNAS-ASA(config)# access-list TFTP-TRAFFIC permit udp any any eq 69
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map CLASS-TFTP
CCNAS-ASA(config-cmap)# match access-list TFTP-TRAFFIC
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# policy-map POLICY-TFTP
CCNAS-ASA(config-pmap)# class CLASS-TFTP
CCNAS-ASA(config-pmap-c)# inspect tftp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-pmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# service-policy POLICY-TFTP global
CCNAS-ASA(config)#
```

9.2 Configuración de ASA.

- Políticas por Defecto en ASA.

No disponible en P.T.

  - Política global que inspecciona tráfico de todas las aplicaciones por defecto.

```
<output omitted>

class-map inspection_default
 match default-inspection-traffic

policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp

service-policy global_policy global

<output omitted>
```

Mapa de clase de una sentencia que concuerda con la palabra clave `default-inspection-traffic`.

Verificación:

```
ASA# show service-policy
ASA# show running-config service-policy
```

Limpieza total de estadísticas políticas de servicio:

```
ASA(conf)# clear configure service-policy
```

Mapa de políticas que asocia acciones para el tráfico identificado en el mapa de clase.

Los Servicios de Política por interface tienen precedencia sobre el global.

Solo una política global.
Para alterar Política global, es necesario editar o sustituir.

Servicio de Política que aplica el mapa de políticas a todas las interfaces (`global`).