

---

# Tema 2. Gestión de seguridad física

Arturo Zúñiga López  
Departamento de Electrónica

---

# ¿Qué es seguridad física?

---

- Todos aquellos mecanismos (prevención y detección) destinados a proteger físicamente los recursos del sistema.
- Es la primera línea de defensa
- Protección del hardware
  - Acceso físico
  - Alteraciones de entorno (sabotaje)
  - Desastres naturales
- Protección de los datos

# Ejemplo

---

- Temperatura
- Protección contra incendios
- Ubicación
- Acceso físico (acceso a los recursos)

# Amenazas

---

- Tempest
  - Es una tecnología que se refiere a estudios de compromiso emanaciones/emisiones
    - Emisiones magnéticas/eléctricas, acústicas, etc.
  - Medidas de prevencion
    - Jaulas de Faraday y laberintos de radiofrecuencia
    - Técnicas de zoning
    - Ruido electromagnético

# Normativa

---

- ISO 27002 Buenas prácticas para la gestión de la seguridad
- TIA-942 (para Data Centers)
- ANSI/BICSI 002-2011 (redes eléctricas, mecánicas, etc.)

# Elementos que se tienen que considerar

---

- Canales de comunicación
- Repetidores
- Hubs
- Switch
- Routers
- Maquinas utilizadas principalmente servidores

# Switch

---

- VLANs
- Métodos de acceso
  - A través de la consola
  - Remotamente

# Ataques en capa de enlace

---

Funcionamiento de ARP

Sniffing

ARP Poisoning



# Ataques en capa IP

---

- Escaneos
- Fragmentación IP
- IP timestamp
- Robo de direcciones (spoofing)
- Paquetes mal formados de IP
- ICMP flood y Smurf

# Barrido de direcciones IP

---

- Enviar pings a todas las direcciones IP dentro del rango para identificar host que se encuentren activos
- Tipos de barridos
  - Horizontales: busca detectar el mismo puerto abierto en varios host
  - Verticales: Busca detectar todos los puertos abiertos en un mismo host

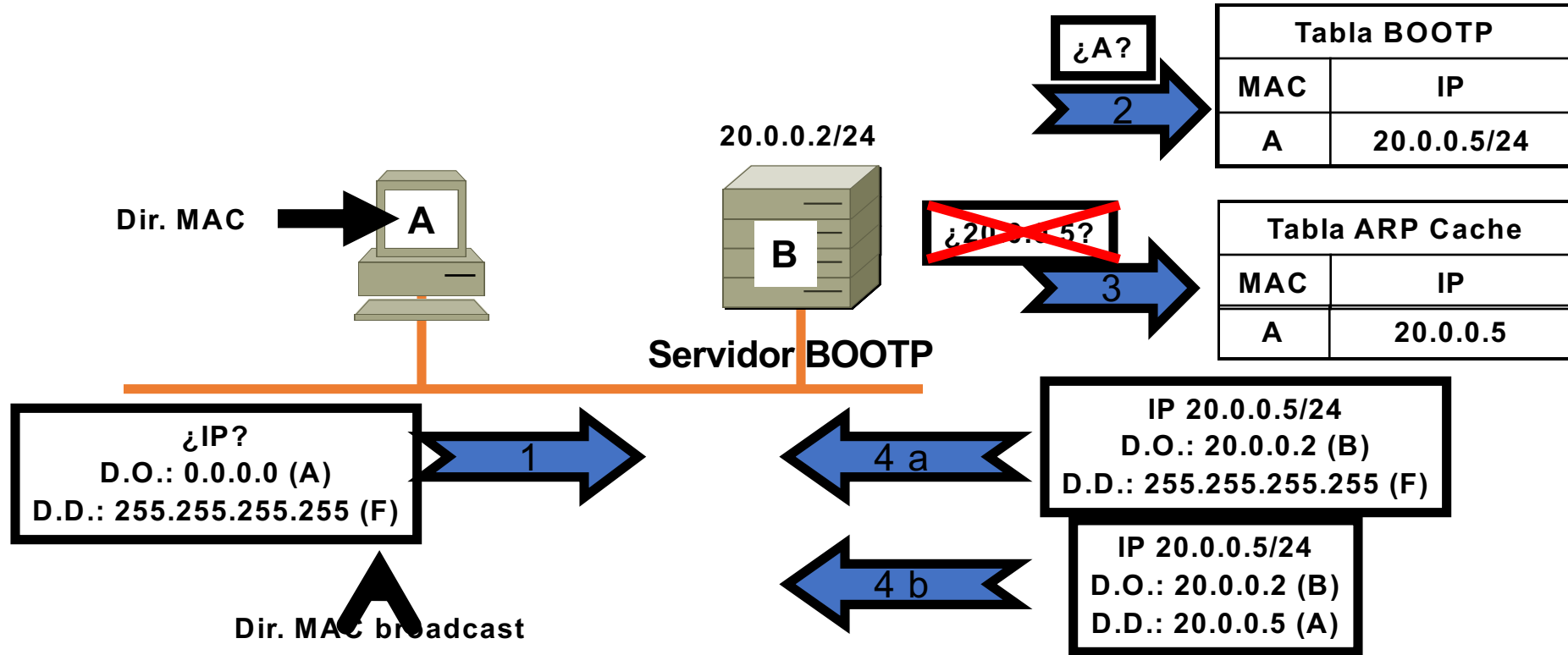
# BOOTP (Bootstrap Protocol)

- Desempeña la misma función que RARP, pero resuelve sus dos problemas principales:
  - Permite suministrar al cliente todos los parámetros de configuración, no solo la dirección IP
  - El servidor y el cliente pueden estar en redes diferentes, ya que los mensajes BOOTP pueden atravesar los routers.
- Si el servidor no está en la misma red que el cliente debe haber un agente en la red del cliente que se encargue de capturar la 'BOOTP Request' para reenviarla al servidor remoto
- Es importante recordar que los mensajes BOOTP viajan siempre en datagramas IP

# Funcionamiento de BOOTP: cliente y servidor en la misma LAN

- Cuando un cliente arranca envía un 'BOOTP request' broadcast (a la dirección 255.255.255.255) poniendo como IP de origen 0.0.0.0 (pues aun no sabe su propia IP)
- El servidor recibe el mensaje, busca en su tabla la MAC del solicitante y si la encuentra prepara el 'BOOTP reply'. Dependiendo de implementaciones la respuesta puede enviarse de dos maneras diferentes:
  - En un paquete IP broadcast (lo más habitual)
  - En un paquete IP unicast dirigido a la MAC del cliente. Al ser un paquete IP la MAC se debería averiguar consultando la ARP cache, pero la MAC no esta allí pues es nueva. Mandar un ARP Request no serviría de nada pues el cliente aún no sabe su IP y no responderá. Es el problema del huevo y la gallina. La solución es permitir que el proceso BOOTP actualice 'ilegalmente' la ARP cache del servidor añadiendo la entrada necesaria sin que se haya recibido un ARP Reply.

# Funcionamiento de BOOTP

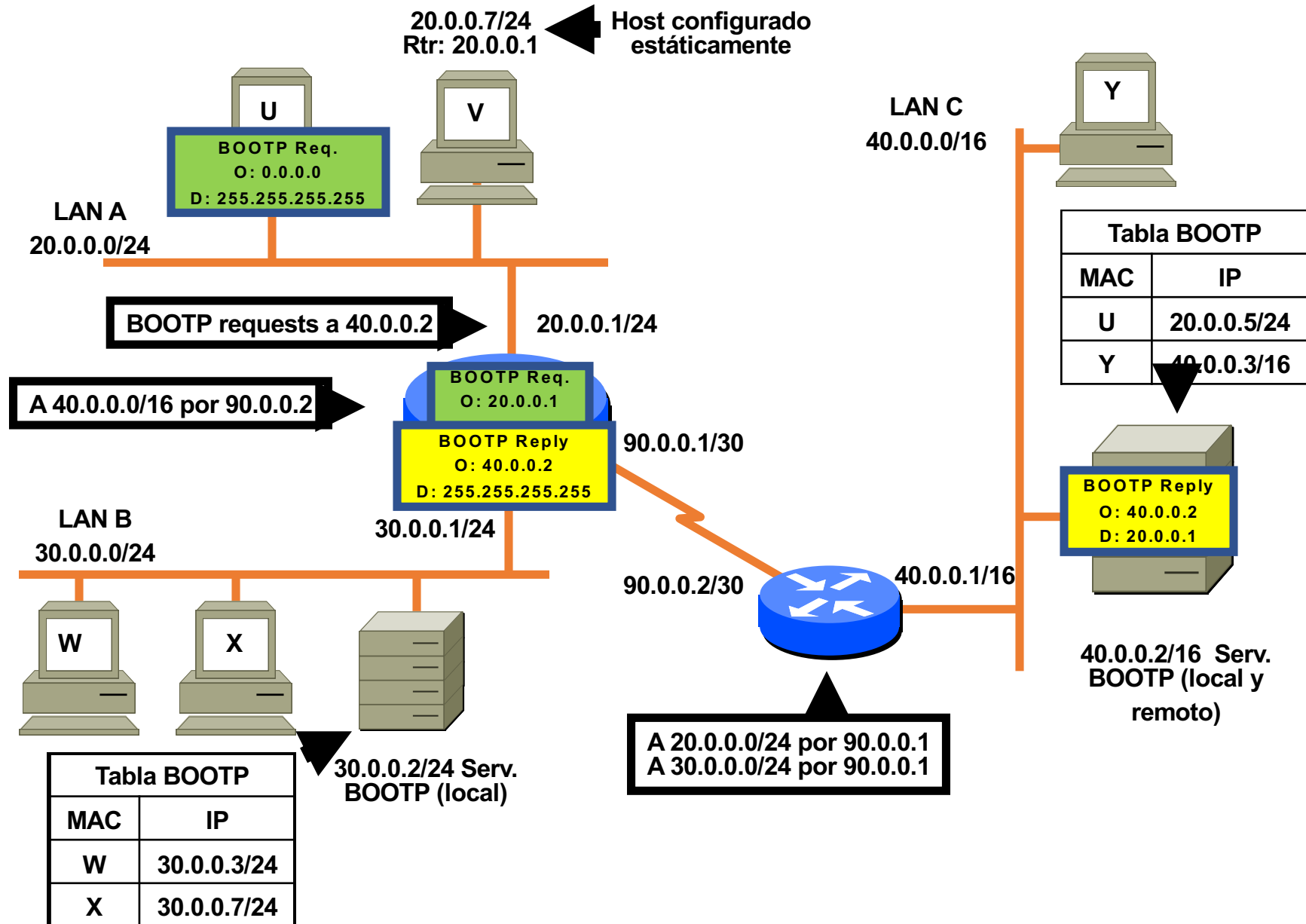


1. A lanza BOOTP request en broadcast preguntando por su IP
2. B busca en su tabla la MAC de A. Encuentra que la IP correspondiente es 20.0.0.5
3. B no puede enviar un datagrama a 20.0.0.5 porque esa IP no esta en su ARP cache; tampoco puede enviar un 'ARP request' pues A no conoce su IP y no responderá
4. a) B lanza BOOTP reply en broadcast, o bien
4. b) El proceso BOOTP de B modifica la ARP cache (si el kernel se lo permite) para incluir la MAC de A y envía el BOOTP reply en unicast

# BOOTP con servidor remoto

- Cuando el servidor BOOTP es remoto alguien en la LAN debe capturar los 'BOOTP Request' y reenviarlos al servidor. El equipo que hace esta función se conoce como 'BOOTP relay agent' y normalmente es un router
- Cuando el BOOTP Request (IP destino broadcast, IP origen 0.0.0.0) llega al agente se convierte en un paquete IP unicast con IP origen la del agente e IP destino la del servidor.
- El BOOTP Reply viaja del servidor al agente también en unicast. Cuando llega a la LAN el Reply se puede enviar en broadcast o en unicast, depende de implementaciones (mismo caso que cuando cliente y servidor estaban en la misma LAN).

# Funcionamiento de BOOTP entre LANs



## Captura Wireshark de un BOOTP Reply

Paquete  
IP

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.100	192.168.2.1	DHCP	DHCP Request - Trans
2	0.005459	192.168.2.1	255.255.255.255	DHCP	DHCP ACK - Trans

Frame 2 (342 bytes on wire, 342 bytes captured)	
+	Ethernet II, Src: SmcNetwo_80:d8:b5 (00:13:f7:80:d8:b5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
+	Internet Protocol, Src: 192.168.2.1 (192.168.2.1), Dst: 255.255.255.255 (255.255.255.255)
+	User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
+	Bootstrap Protocol
Message type: Boot Reply (2)	
Hardware type: Ethernet	
Hardware address length: 6	
Hops: 0	
Transaction ID: 0xaf2650b7	
Seconds elapsed: 0	
+	Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.2.100 (192.168.2.100)	
Your (client) IP address: 192.168.2.100 (192.168.2.100)	
Next server IP address: 192.168.2.1 (192.168.2.1)	
Relay agent IP address: 0.0.0.0 (0.0.0.0)	
Client MAC address: IntelCor_29:86:f8 (00:13:02:29:86:f8)	
Server host name not given	
Boot file name not given	
Magic cookie: (OK)	
+	Option: (t=53,l=1) DHCP Message Type = DHCP ACK
+	Option: (t=54,l=4) Server Identifier = 192.168.2.1
+	Option: (t=51,l=4) IP Address Lease Time = infinity
+	Option: (t=1,l=4) Subnet Mask = 255.255.255.0
+	Option: (t=3,l=4) Router = 192.168.2.1
+	Option: (t=6,l=4) Domain Name Server = 192.168.2.1
End option	

Envío broadcast

Dir. MAC del cliente  
en el paquete BOOTP

Opciones de  
configuración adicionales



# DHCP

## (Dynamic Host Configuration Protocol)

- Muy parecido a BOOTP, permite una asignación más flexible de las direcciones IP, que puede ser:
  - **Manual.** El administrador fija de forma estática en configuración la correspondencia MAC-IP, como en BOOTP.
  - **Dinámica.** A cada MAC se le asigna una IP de un pool por un tiempo limitado. Pasado ese tiempo la IP se retira, salvo que se renueve la petición. Permite un óptimo reaprovechamiento de las direcciones, pero éstas no son fijas.
  - **Automática.** Cada MAC recibe una IP pero el servidor recuerda la IP asignada e intenta darle siempre la misma a cada MAC cuando se conecte en el futuro
- Usa el mismo mecanismo que BOOTP para acceder al servidor cuando éste es remoto (agentes relay)
- DHCP es lo más parecido a la autoconfiguración

# Parámetros configurables por BOOTP/DHCP

- Dirección IP del cliente
- Hostname del cliente
- Máscara de subred
- Dirección(es) IP de:
  - Router(s)
  - Servidor(es) de nombres
  - Servidor(es) de impresión (LPR)
  - Servidor(es) de tiempo
- Nombre y ubicación del fichero que debe usarse para hacer boot (en ese caso el fichero se cargará después por TFTP)

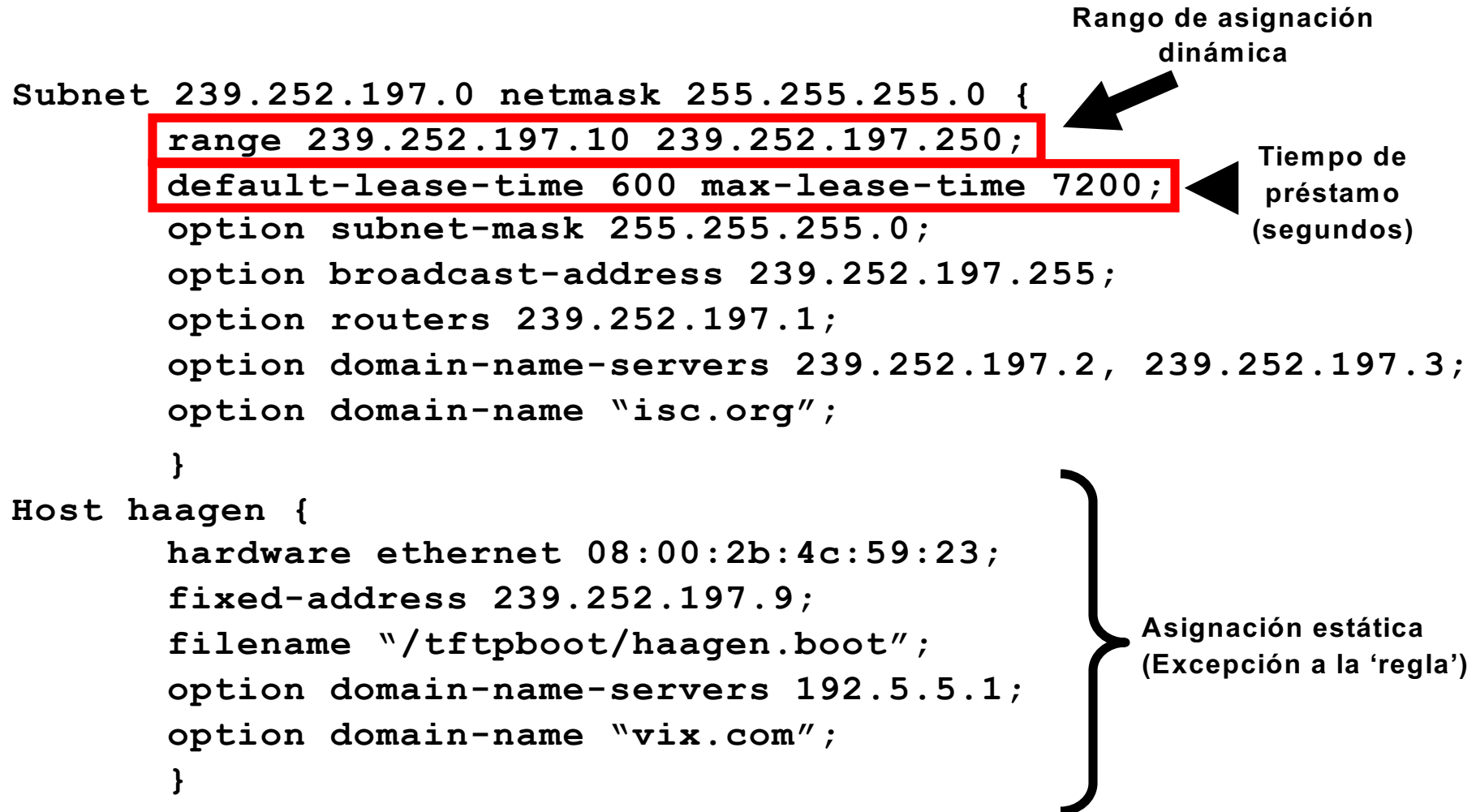
# Servidor DHCP que combina asignación dinámica y estática de direcciones

```
Subnet 239.252.197.0 netmask 255.255.255.0 {  
  range 239.252.197.10 239.252.197.250;  
  default-lease-time 600 max-lease-time 7200;  
  option subnet-mask 255.255.255.0;  
  option broadcast-address 239.252.197.255;  
  option routers 239.252.197.1;  
  option domain-name-servers 239.252.197.2, 239.252.197.3;  
  option domain-name "isc.org";  
}  
Host haagen {  
  hardware ethernet 08:00:2b:4c:59:23;  
  fixed-address 239.252.197.9;  
  filename "/tftpboot/haagen.boot";  
  option domain-name-servers 192.5.5.1;  
  option domain-name "vix.com";  
}
```

Rango de asignación dinámica

Tiempo de préstamo (segundos)

Asignación estática (Excepción a la 'regla')

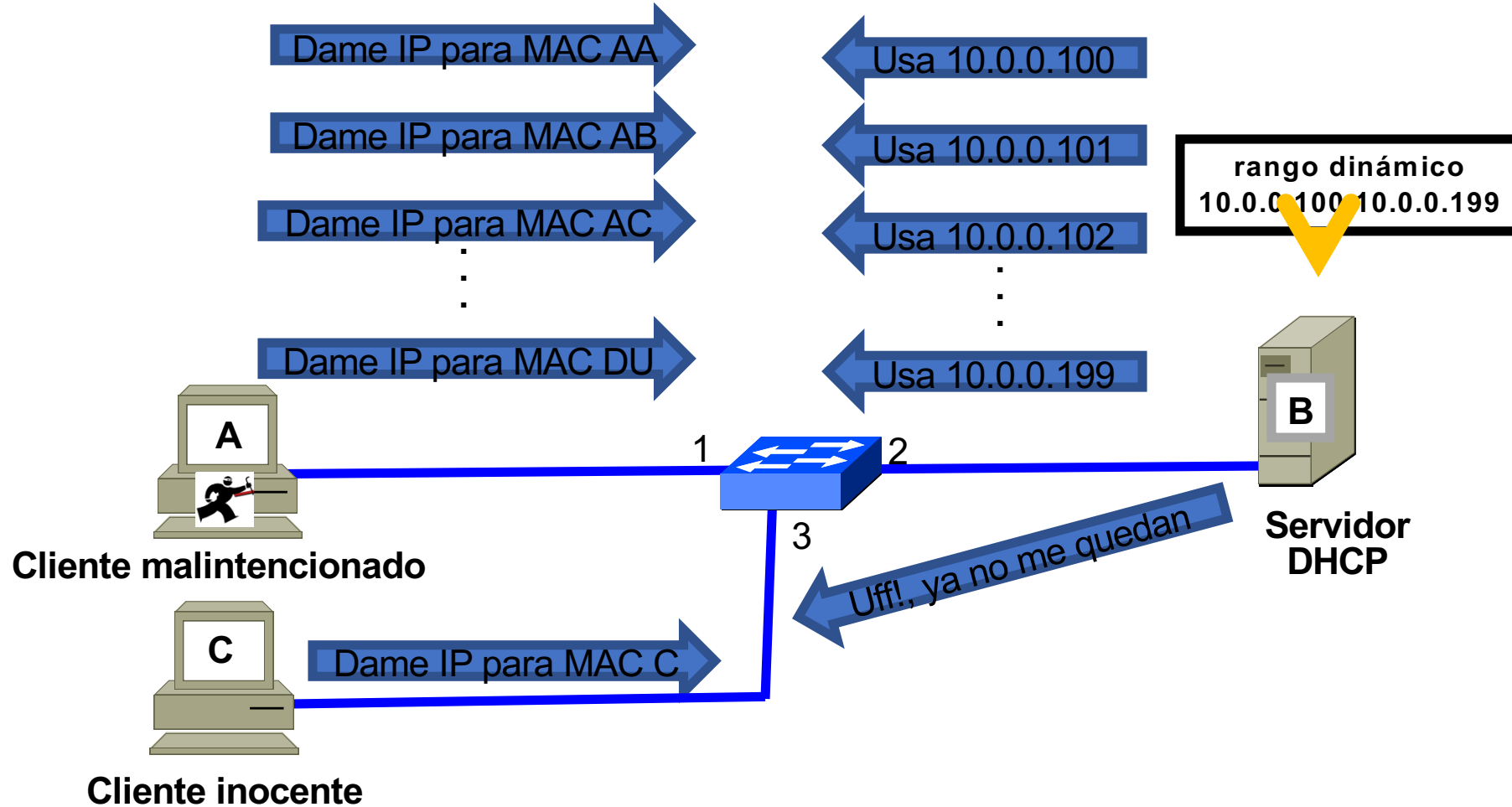


# Ataques de DHCP

- Cuando se utilizan servidores BOOTP/DHCP pueden ocurrir dos tipos de ataques:
  - Agotamiento de direcciones (DHCP 'starvation'): ocurre cuando se utiliza asignación dinámica o automática y un cliente intenta consumir todas las direcciones disponibles en el servidor
  - Servidores DHCP furtivos ('rogue'): se da cuando hay en la red servidores no autorizados que compiten con el legítimo

# Agotamiento de direcciones en DHCP

A puede falsear las MACs que utiliza al mandar los DHCP Request



# Solución al ataque de agotamiento de direcciones DHCP

- Si limitamos el número de MACs que pueden aparecer por puerto con el comando:

**switchport port-security maximum 1**

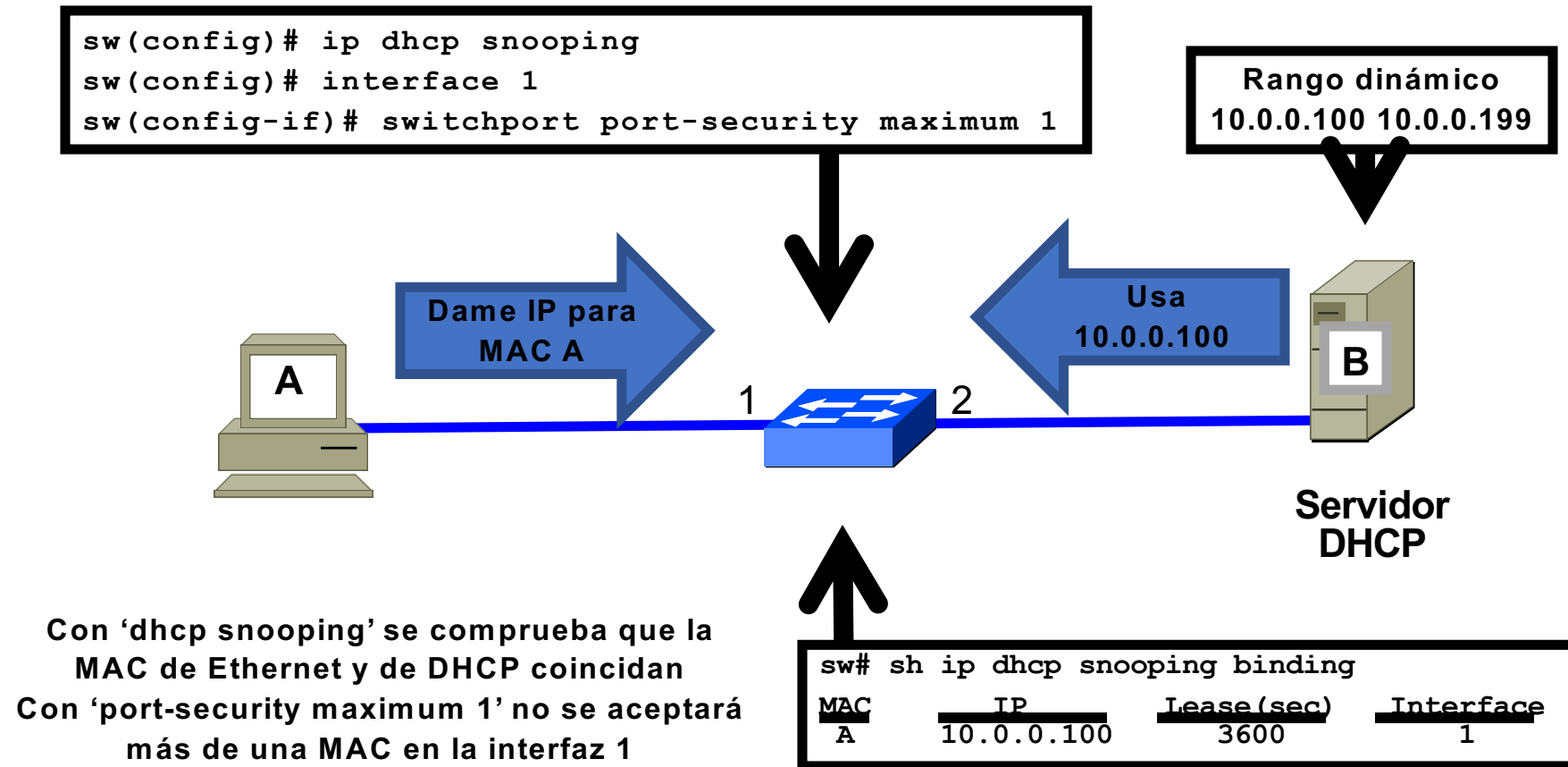
podríamos evitar el problema. El presunto atacante quedaría bloqueado (puerto shutdown) cuando intentara utilizar más de una dirección MAC

- Pero esto por sí solo no evita el ataque, ya que los servidores DHCP no utilizan la dirección MAC de la trama Ethernet para asignar direcciones, sino la que aparece dentro del paquete BOOTP/DHCP, que no es vista por el switch
- Algunos switch tienen una función denominada 'DHCP Snooping' (snooping = husmear) que les permite inspeccionar información contenida dentro de los paquetes DHCP

# Solución al ataque de agotamiento de direcciones DHCP

- Con DHCP snooping activado el switch comprueba que la dirección MAC dentro del paquete DHCP coincida con la de la cabecera Ethernet, en caso contrario el paquete se descarta (o el puerto se deja en shutdown).
- Además el switch aprovecha esto para construir una tabla, llamada 'DHCP binding table' (parecida a la ARP Cache) que le permite saber la correspondencia entre las direcciones MAC e IP asignadas.
- El DHCP snooping solo está disponible en switches modernos, normalmente de gama alta.

# Uso de DHCP snooping

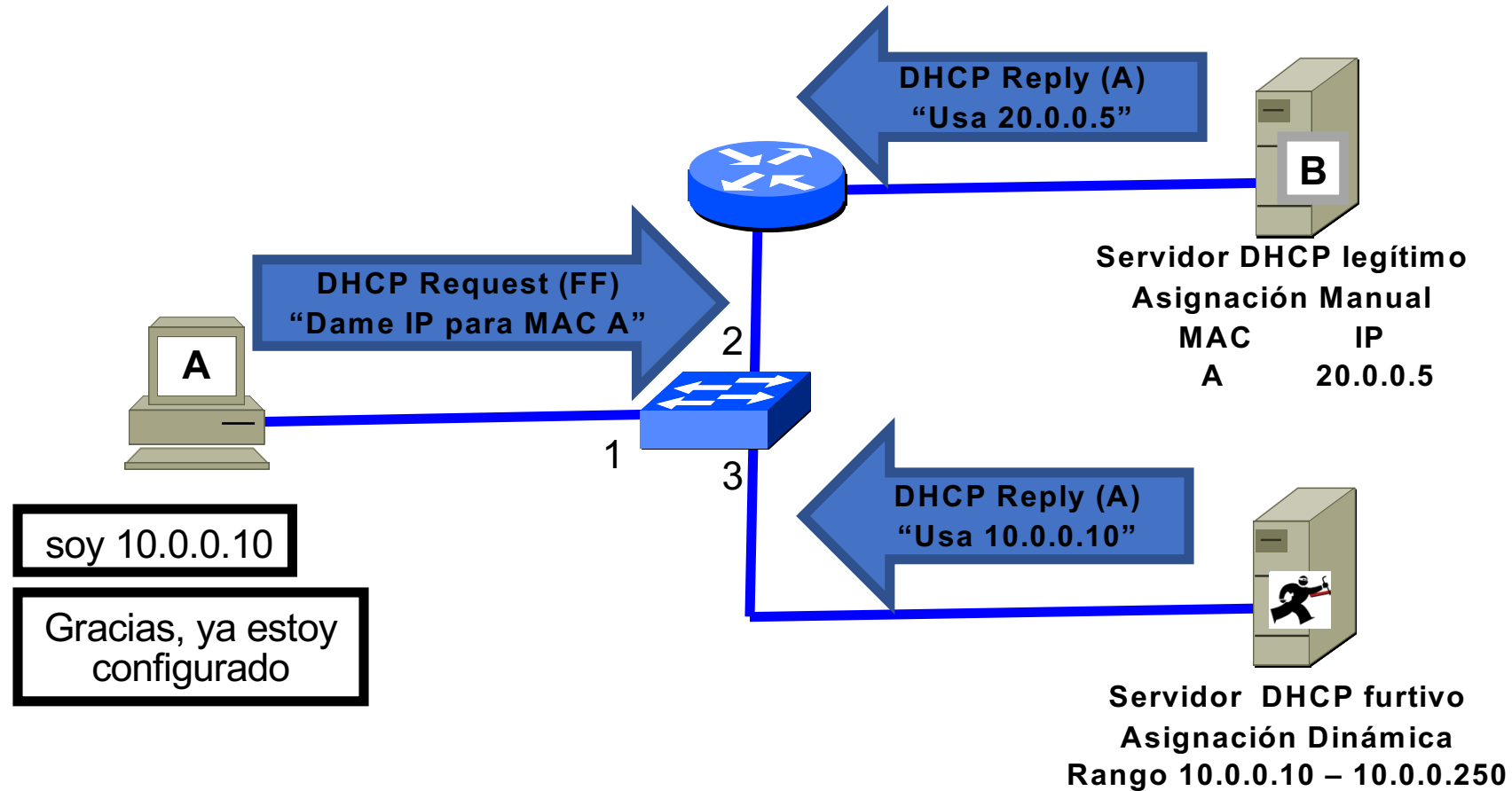




# Ataque Servidor DHCP furtivo ('rogue')

- Los mensajes DHCP Request que envían los clientes se mandan a la dirección broadcast
- Si en la LAN hay un servidor furtivo éste recibirá también el DHCP Request y si responde antes que el legítimo el host atenderá sus mensajes
- Cuando el DHCP furtivo está en la misma LAN que el cliente y el legítimo está remoto el furtivo normalmente responde antes
- El servidor furtivo puede controlar por completo al cliente ya que la configuración DHCP que le manda incluye:
  - La dirección IP del cliente
  - El router por defecto
  - El servidor DNS
- Asignando un router y un DNS falsos se pueden llevar a cabo ataques muy sofisticados

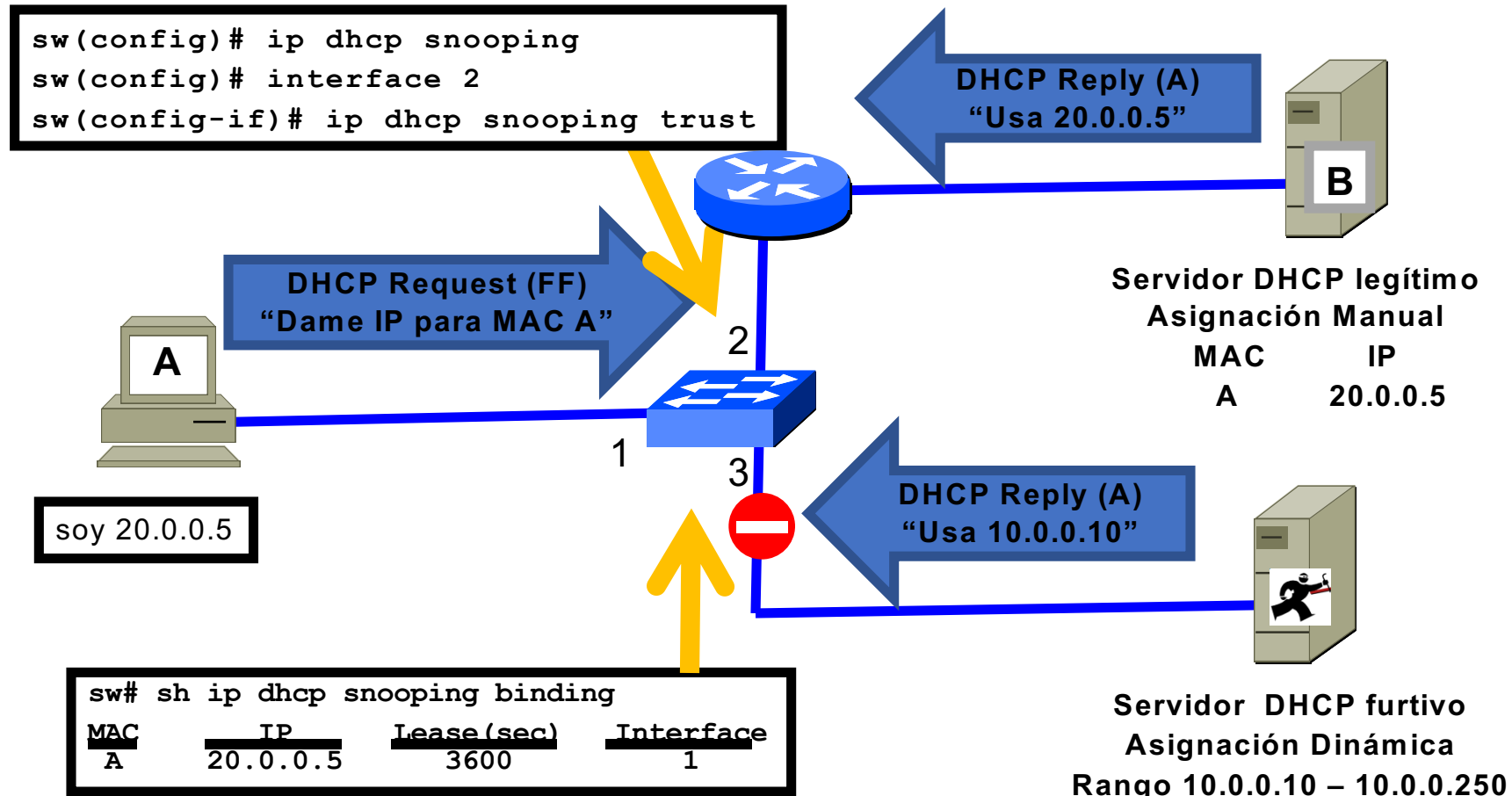
# Ataque servidor DHCP furtivo



# Solución al ataque servidor DHCP furtivo

- Para evitar este ataque hay que configurar los switches para que **solo** acepten los mensajes DHCP Reply cuando vengan de puertos donde se sabe que hay servidores legítimos. Esto es posible si los switch soportan DHCP snooping
- Los puertos por los que se espera recibir mensajes DHCP Reply deben configurarse como puertos 'trust' (de confianza) en el switch
- Normalmente la configuración por defecto es 'no trust' para todos los puertos. Solo deberían configurarse como 'trust' los puertos por los que previsiblemente deban llegar mensajes DHCP Reply

# Ataque servidor DHCP furtivo configuración protegida



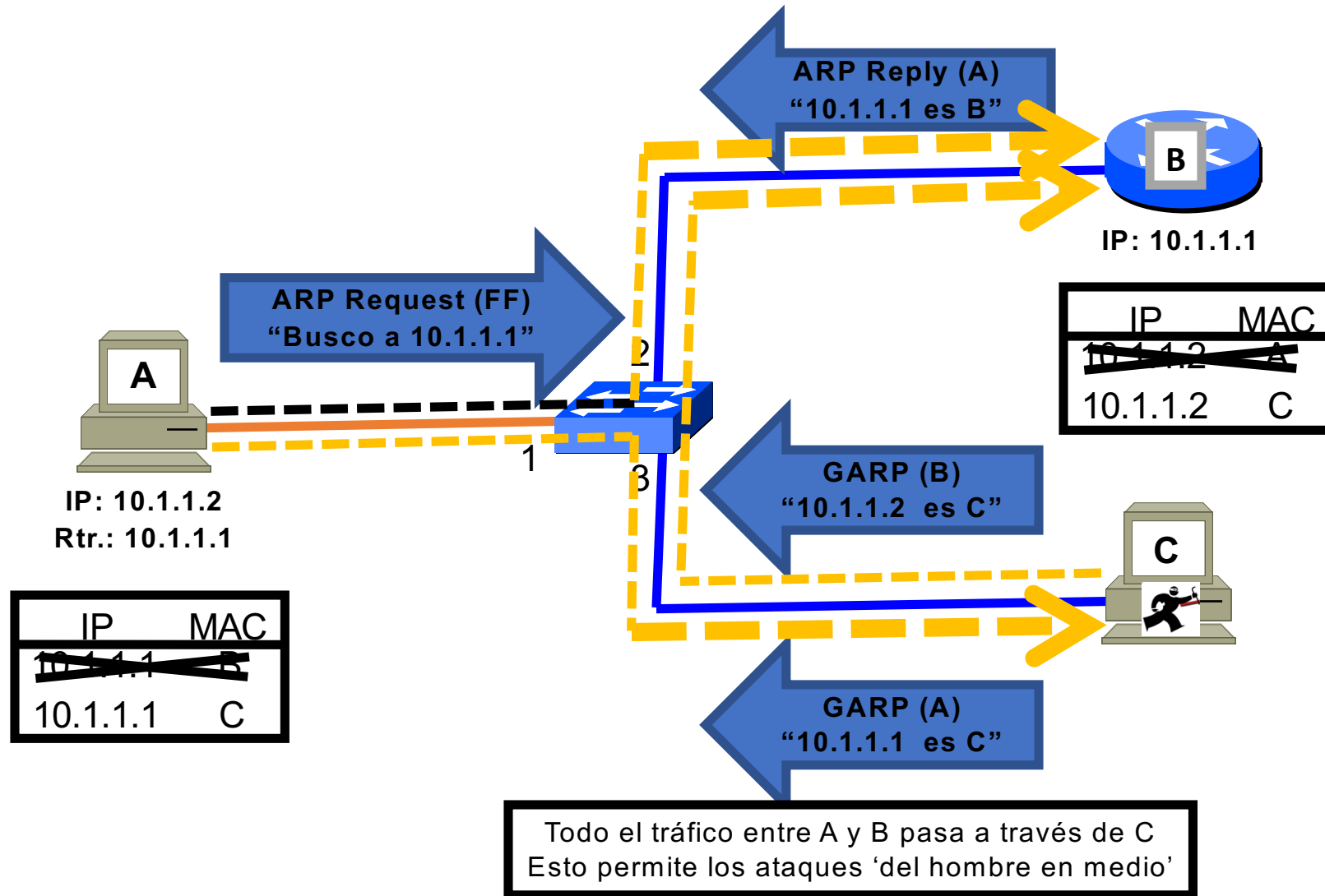
# Ataques de 'spoofing' (suplantación de identidad)

- Consisten en utilizar una dirección falsa para acceder a algún recurso haciéndose pasar por otro host. Se pueden hacer de diferentes maneras:
  - ARP spoofing: se falsea la información de la tabla ARP cache mediante el envío de mensajes ARP falsos
  - IP spoofing: un equipo utiliza la dirección IP de otro. En determinadas circunstancias este ataque puede hacerse a máquinas de otra LAN
  - MAC spoofing: un equipo utiliza la dirección MAC de otro
  - Diversas combinaciones de los tres anteriores

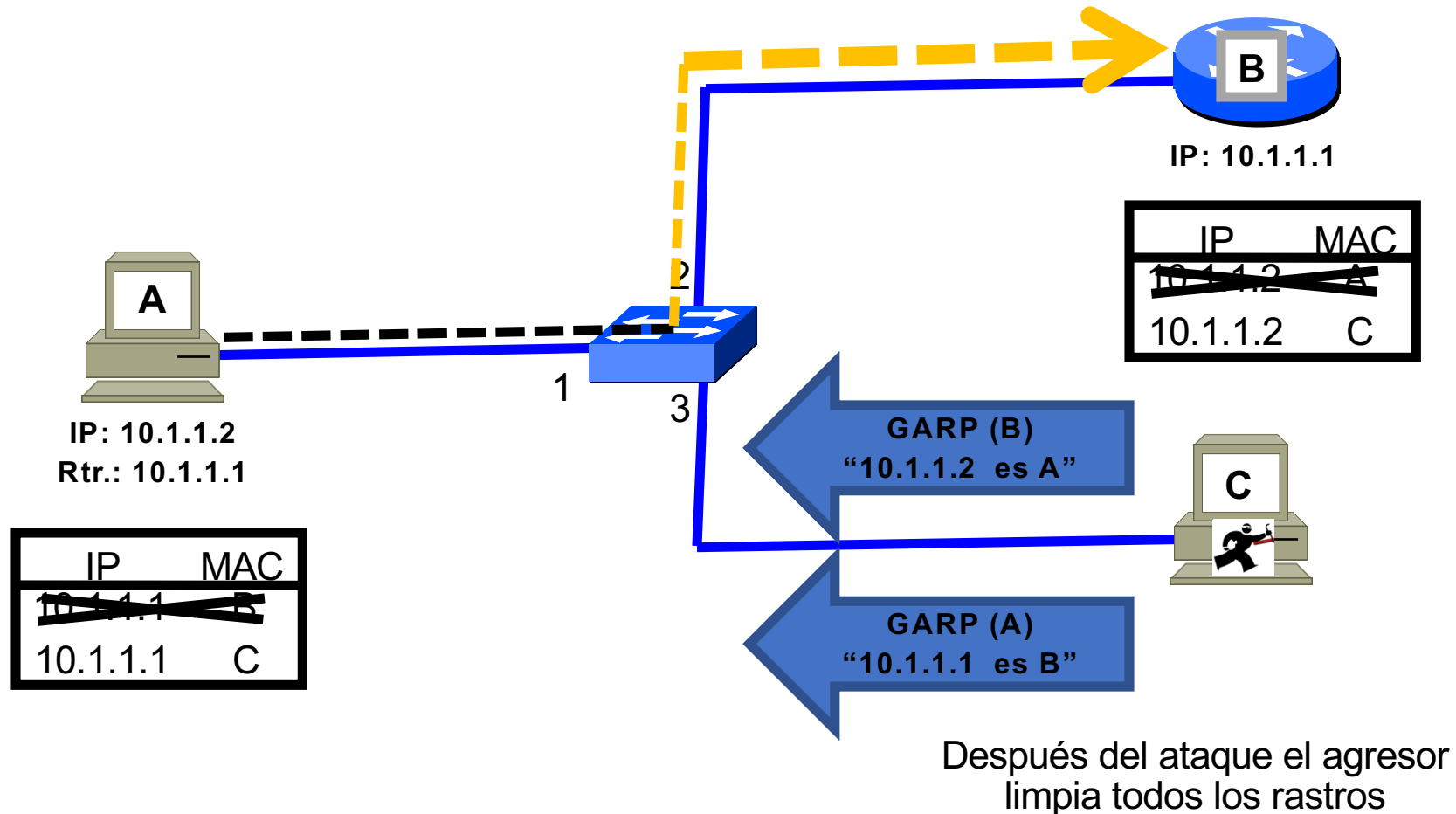
# Ataque de ARP spoofing, o envenenamiento de ARP

- Para averiguar una dirección IP un host envía un ARP Request en broadcast preguntando por la dirección IP buscada
- Todos los Hosts en la LAN reciben y procesan el ARP Request; el dueño de la IP buscada responde con un ARP Reply
- Pero el protocolo ARP no es seguro, cualquier host puede responder a un ARP Request diciendo poseer cualquier dirección IP, sea o no cierto. En condiciones normales los hosts se fían de los ARP que reciben, nadie se encarga de verificar la veracidad de la información
- Enviando mensajes ARP gratuitos (GARP; Gratuitous ARP) un host se puede poner entre otro host y el router, pudiendo inspeccionar o modificar todo el tráfico intercambiado entre ambos.

# ARP spoofing, ataque



# ARP spoofing, limpieza

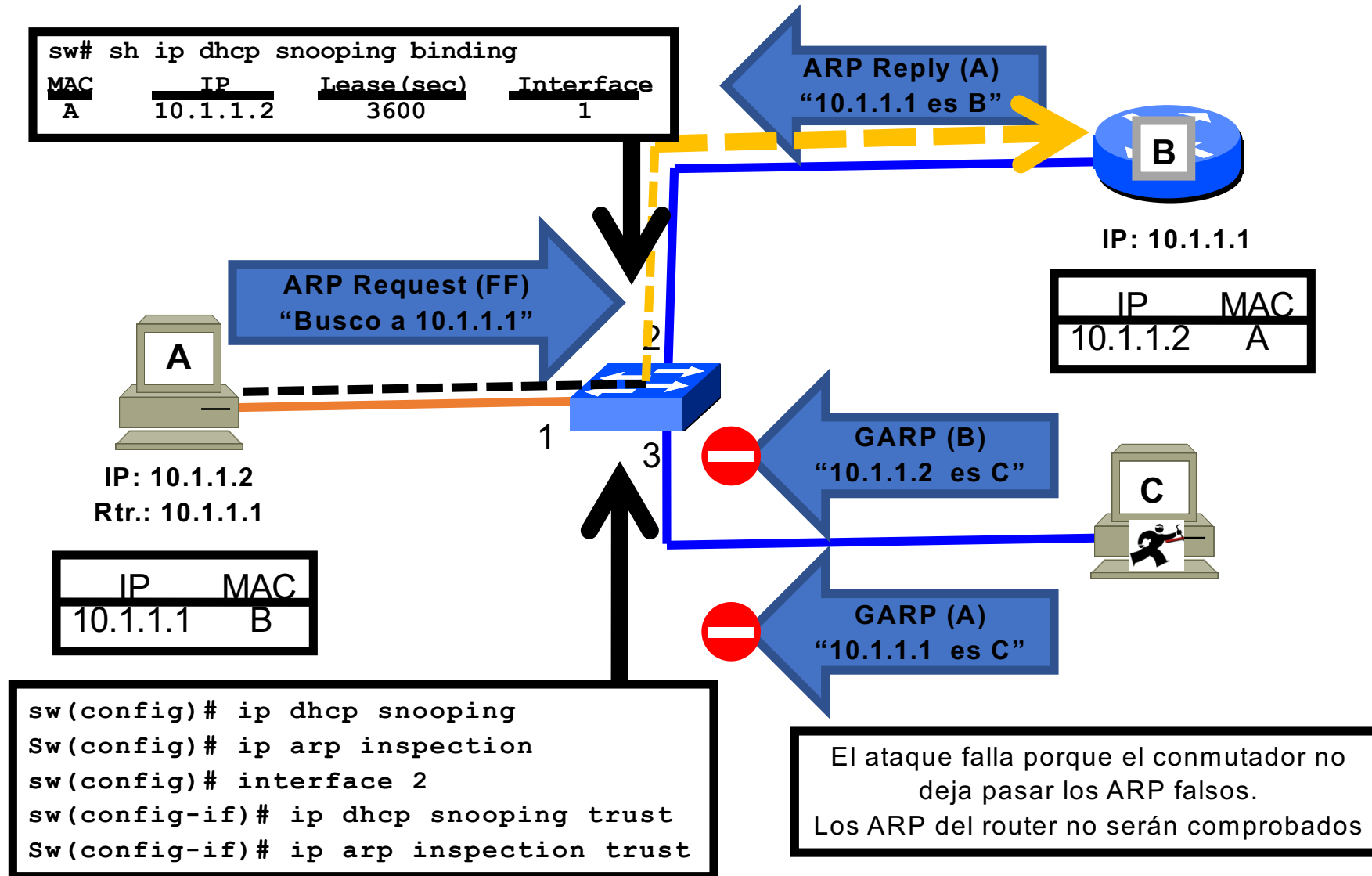




# Solución al ARP spoofing

- Los switches tienen que 'husmear' los paquetes ARP (parecido a lo que hacían con DHCP) para comprobar que la información que lleva es correcta. En este caso no se llama 'ARP Snooping' sino **'ARP Inspection'** o **'ARP Security'**
- ARP Inspection hace uso de la DHCP 'binding table', por lo que requiere tener activado el DHCP Snooping
- Cuando un ARP pasa por el switch éste comprueba que la MAC e IP se correspondan con la binding table; si no el mensaje se descarta.
- Se pueden configurar puertos de confianza (trust) en los que no se aplica el ARP Inspection. Por defecto todos los puertos son 'no trust'
- Otra forma de evitar el ataque ARP es llenar a mano la ARP cache con entradas estáticas. Esto requiere mucha labor administrativa por lo que no suele hacerse.

# ARP spoofing, configuración protegida



# IP spoofing

- El host envía paquetes IP poniendo una dirección de origen falsa. Generalmente esto lo hacen los atacantes para evitar ser perseguidos. Muchos ataques de denegación de servicio se basan en desbordar recursos de servidores usando múltiples direcciones IP, todas falsas, desde un mismo host.
- Podemos distinguir dos tipos de spoofing:
  - IP Spoofing ciego: el host impostor y el suplantado están en LANs diferentes. En este caso el impostor no recibe las respuestas a los paquetes de ataque. Suele utilizarse para ataques de denegación de servicio.
  - IP Spoofing con visibilidad: el impostor y el suplantado están en la misma LAN, de forma que el impostor puede fácilmente obtener los paquetes de respuesta (con ARP spoofing, por ejemplo). Esto le permite controlar la sesión y potencialmente le da acceso a recursos reservados.

# AAA

- Introducción

- La forma más simple de autenticación son las contraseñas, sin embargo son muy vulnerables a ataques de fuerza bruta, además no ofrece registro de auditoria de ningún tipo.
- AAA (Authentication, Authorization, Accounting) provee una mejor solución al hacer que todos los dispositivos accedan a la misma base de datos de usuarios y contraseñas en un servidor central.

# AAA

- Authentication. Se encarga de verificar que el usuario es quien dice ser.
- Authorization. Determina a qué recursos tiene acceso el usuario una vez que se ha autenticado.
- Accounting. Se encarga de registrar la actividad realizada por el usuario una vez que haya sido autenticado.

# AAA

- Autenticación AAA
  - La autenticación puede ser local, sin embargo este método no es muy seguro.
  - Método basado en servidor, donde se utilizan recursos de bases de datos a través de protocolos
    - RADIUS (Remote Dial-in User Services)
    - Diameter
    - TACACS+ (Terminal Access Control Access Control Server Plus)
  - Algunos métodos de autenticación
    - Autenticación de sistema
    - Los protocolos PAP (Password Authentication Protocol) y CHAP (Challenge Handshake Authentication Protocol)
    - LDAP (Lightweight Directory Access Protocol), es un protocolo a nivel de aplicación (TCP/IP)
    - Kerberos
    - EAP (Extensible Authentication Protocol)

# AAA

- Autorización
  - La autorización consiste básicamente en que los que un usuario puede y no puede hacer en la red, parecido a los niveles de privilegios.
  - Utiliza un grupo de atributos creado que describe el acceso del usuario a la red.
  - Métodos de autorización
    - LDAP
    - Bases de datos SQL
    - Archivos de configuración local del servidor

# AAA

- Auditoría
  - El registro de auditoria recolecta y reporta datos de uso para que puedan ser empleados para auditoria.
  - Estas estadísticas pueden ser extraídas para crear reportes detallados sobre la configuración de la red.



# NAS

- Un Network Access Server (NAS) es un sistema que proporciona acceso a la red. En algunos casos también se conoce como RAS (Remote Access Server) o Terminal Server
- En general NAS es un elemento que controla el acceso a un recurso protegido.

