

GRUPO:9

EXPOSICIÓN DHCP-ARP

INTEGRANTES:

Iara Ale

Valeria Panigo

Omar mareco

Lucas Silvestri



DHCP

¿Que es DHCP?

Overview

DHCP es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas

Historia

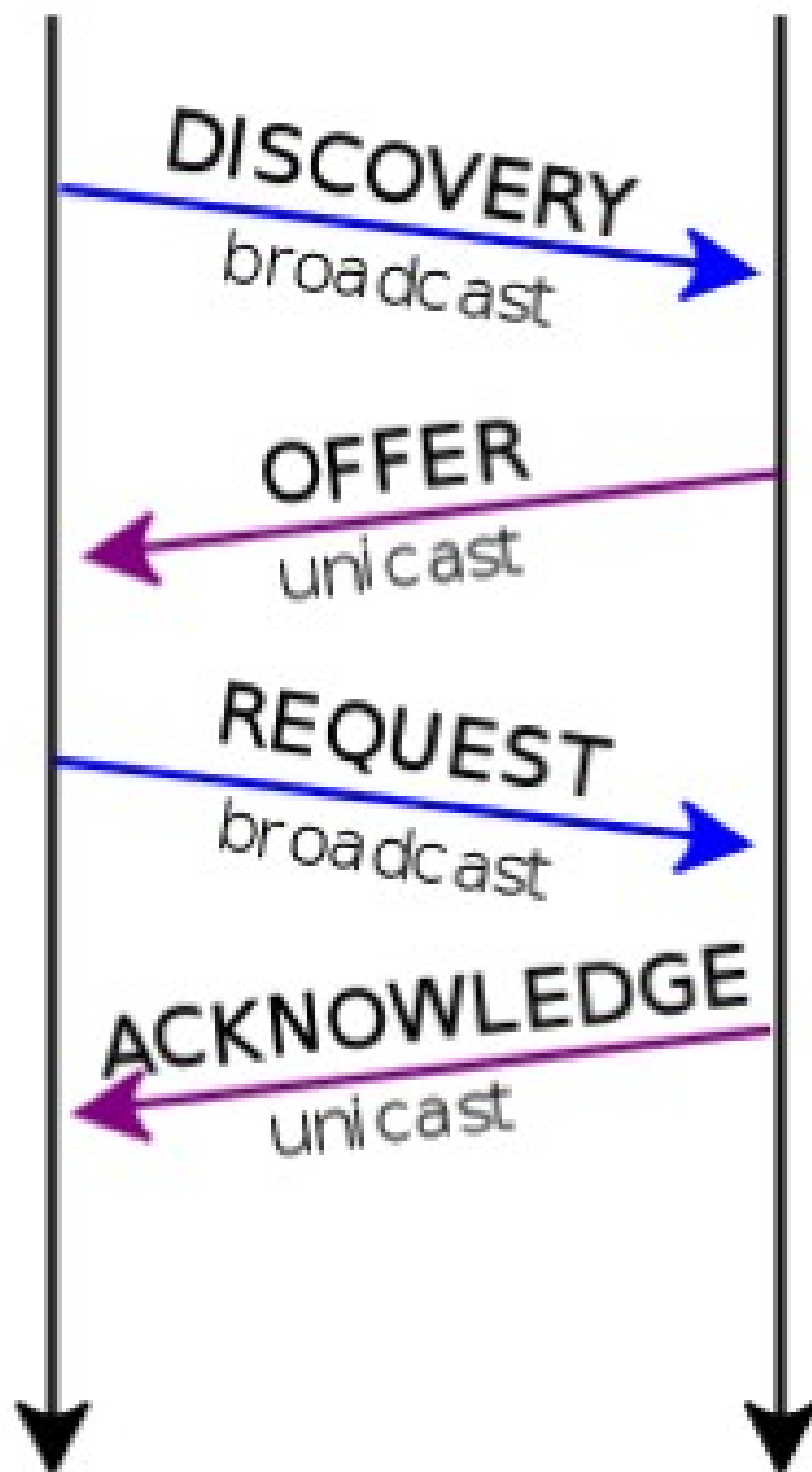
- En Octubre de 1993 DHCP se definió por primera vez como un protocolo de seguimiento estático de las normas en el RFC 1531.
- En 1997 muchos trabajadores mejoraron el protocolo ,ya que gano popularidad y se publico el RFC 2131.
- En la actualidad se mantiene como el estándar para redes Ipv4.
- El protocolo BOOTP a su vez fue definido por primera vez en el RFC 951 como un reemplazo para el protocolo RARP (del inglés "Reverse Address Resolution Protocol"), o resolución de direcciones inversa.

Operaciones

- DHCP discovery (para ubicar servidores de DHCP disponibles).
- DHCP offer (repuesta del servidor a un paquete DHCP discover, que contiene los parametros iniciales).
- DHCP request (solicitudes varias de clientes. Ejemplo: Para extender su conexión)
- DHCP acknowledgement ()
- DHCP information (El cliente solicita parámetros locales, ya tiene su dirección IP)
- DHCP releasing (el cliente libera su dirección IP)

client

server



time —→

DHCP discovery

UDP Src=0.0.0.0 sPort=68 Dest=255.255.255.255 dPort=67							
OP		HTYPE		HLEN		HOPS	
0x01		0x01		0x06		0x00	
XID							
0x3903F326							
SECS				FLAGS			
0x0000				0x0000			
CIADDR (Client IP address)							
0x00000000							
YIADDR (Your IP address)							
0x00000000							
SIADDR (Server IP address)							
0x00000000							
GIADDR (Gateway IP address)							
0x00000000							
CHADDR (Client hardware address)							
0x00053C04							
0x8D590000							
0x00000000							
0x00000000							
192 octets of 0s, or overflow space for additional options. BOOTP legacy							
Magic cookie							
0x63825363							
DHCP Options							
DHCP option 53: DHCP Discover							
DHCP option 50: 192.168.1.100 requested							
DHCP option 55: Parameter Request List:							
Request Subnet Mask (1), Router (3), Domain Name (15), Domain Name Server (6)							

DHCP offer

UDP Src=192.168.1.1 sPort=67 Dest=255.255.255.255 dPort=68			
OP	HTYPE	HLEN	HOPS
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SECS		FLAGS	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0xC0A80164			
SIADDR (Server IP address)			
0xC0A80101			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s. BOOTP legacy			
Magic cookie			
0x63825363			
DHCP Options			
DHCP option 53: DHCP Offer			
DHCP option 1: 255.255.255.0 subnet mask			
DHCP option 3: 192.168.1.1 router			
DHCP option 51: 86400s (1 day) IP address lease time			
DHCP option 54: 192.168.1.1 DHCP server			
DHCP option 6: DNS servers 9.7.10.15, 9.7.10.16, 9.7.10.18			

DHCP request

UDP Src=0.0.0.0 sPort=68 Dest=255.255.255.255 ^[a] dPort=67			
OP	HTYPE	HLEN	HOPS
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SECS		FLAGS	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0x00000000			
SIADDR (Server IP address)			
0xC0A80101			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s. BOOTP legacy			
Magic cookie			
0x63825363			
DHCP Options			
DHCP option 53: DHCP Request			
DHCP option 50: 192.168.1.100 requested			
DHCP option 54: 192.168.1.1 DHCP server.			

DHCP acknowledgement

UDP Src=192.168.1.1 sPort=67 Dest=255.255.255.255 dPort=68			
OP	HTYPE	HLEN	HOPS
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SECS		FLAGS	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0xC0A80164			
SIADDR (Server IP address)			
0xC0A80101			
GIADDR (Gateway IP address switched by relay)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s. BOOTP legacy			
Magic cookie			
0x63825363			
DHCP Options			
DHCP option 53: DHCP ACK (value=5) or DHCP NAK (value=6)			
DHCP option 1: 255.255.255.0 subnet mask			
DHCP option 3: 192.168.1.1 router			
DHCP option 51: 86400s (1 day) IP address lease time			
DHCP option 54: 192.168.1.1 DHCP server			
DHCP option 6: DNS servers 9.7.10.15, 9.7.10.16, 9.7.10.18			

DHCP information

Un cliente DHCP puede solicitar más información que el servidor envía con el DHCPOFFER originales. El cliente también puede solicitar datos de repetición para una aplicación particular. Por ejemplo, los navegadores utilizan DHCP Inform para obtener la configuración de proxy web a través de WPAD.

DHCP releasing

El cliente envía una solicitud al servidor DHCP para liberar la información de DHCP y el cliente desactiva su dirección IP. Como los dispositivos de cliente por lo general no saben cuando los usuarios pueden desactivarlos de la red, el protocolo no exige el envío de DHCP Release.

Parametros de configuración del cliente

Un servidor DHCP puede proveer de una configuración opcional al dispositivo cliente. Dichas opciones están definidas en RFC 2132 (Inglés) Lista de opciones configurables:

Rango de IP a asignar

Dirección del servidor DNS

Nombre DNS

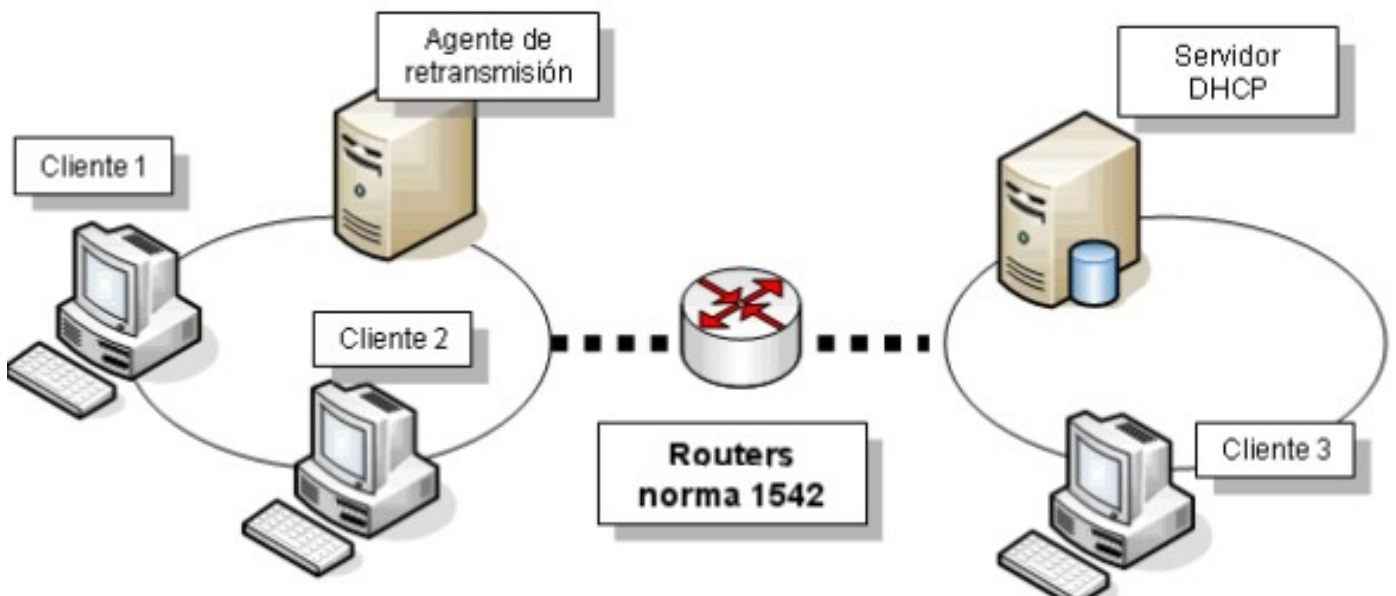
Puerta de enlace de la dirección IP

Máscara de subred

Servidor TFTP

DHCP relaying

En redes pequeñas, donde se logró sólo una subred IP, los clientes DHCP se comunican directamente con los servidores DHCP. Sin embargo, los servidores DHCP también pueden proporcionar direcciones IP para múltiples subredes.

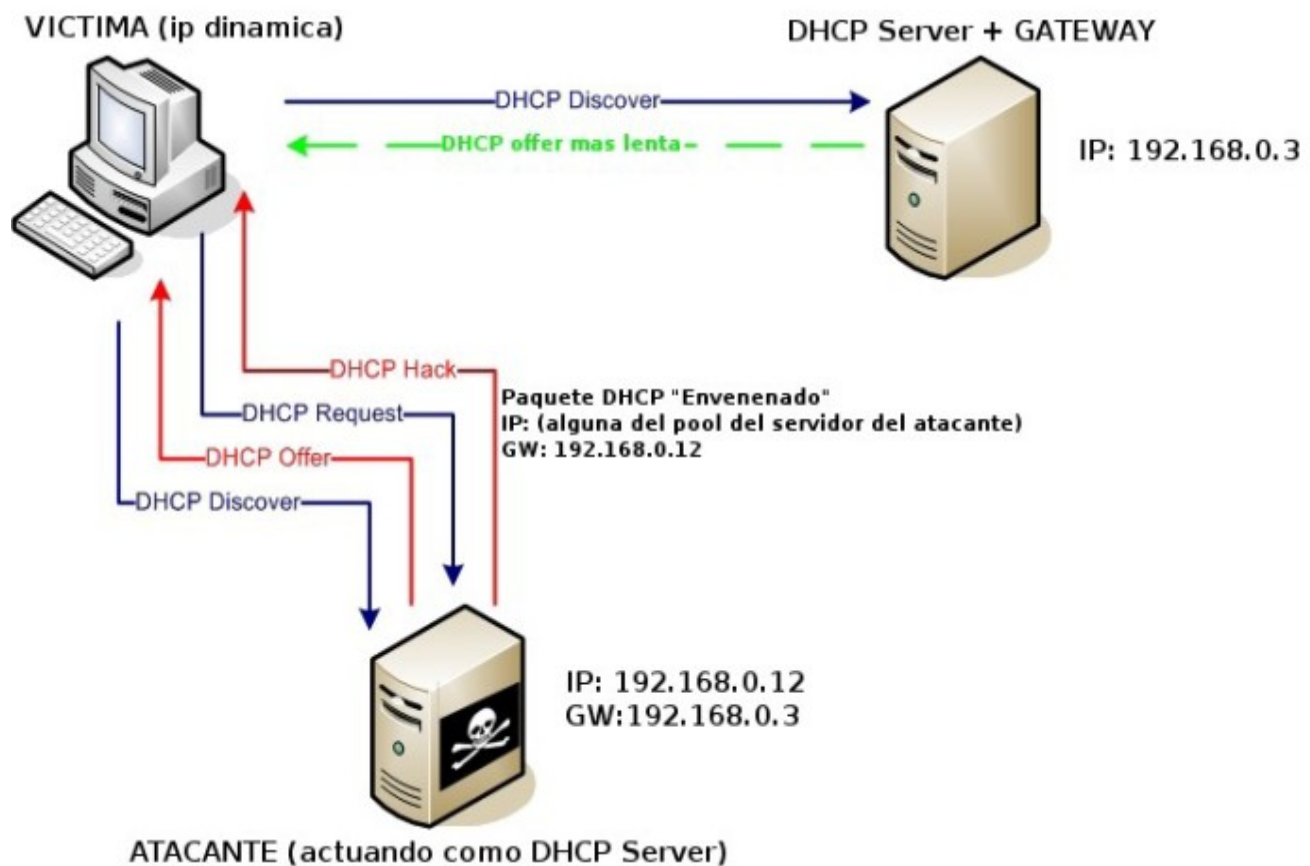


Seguridad

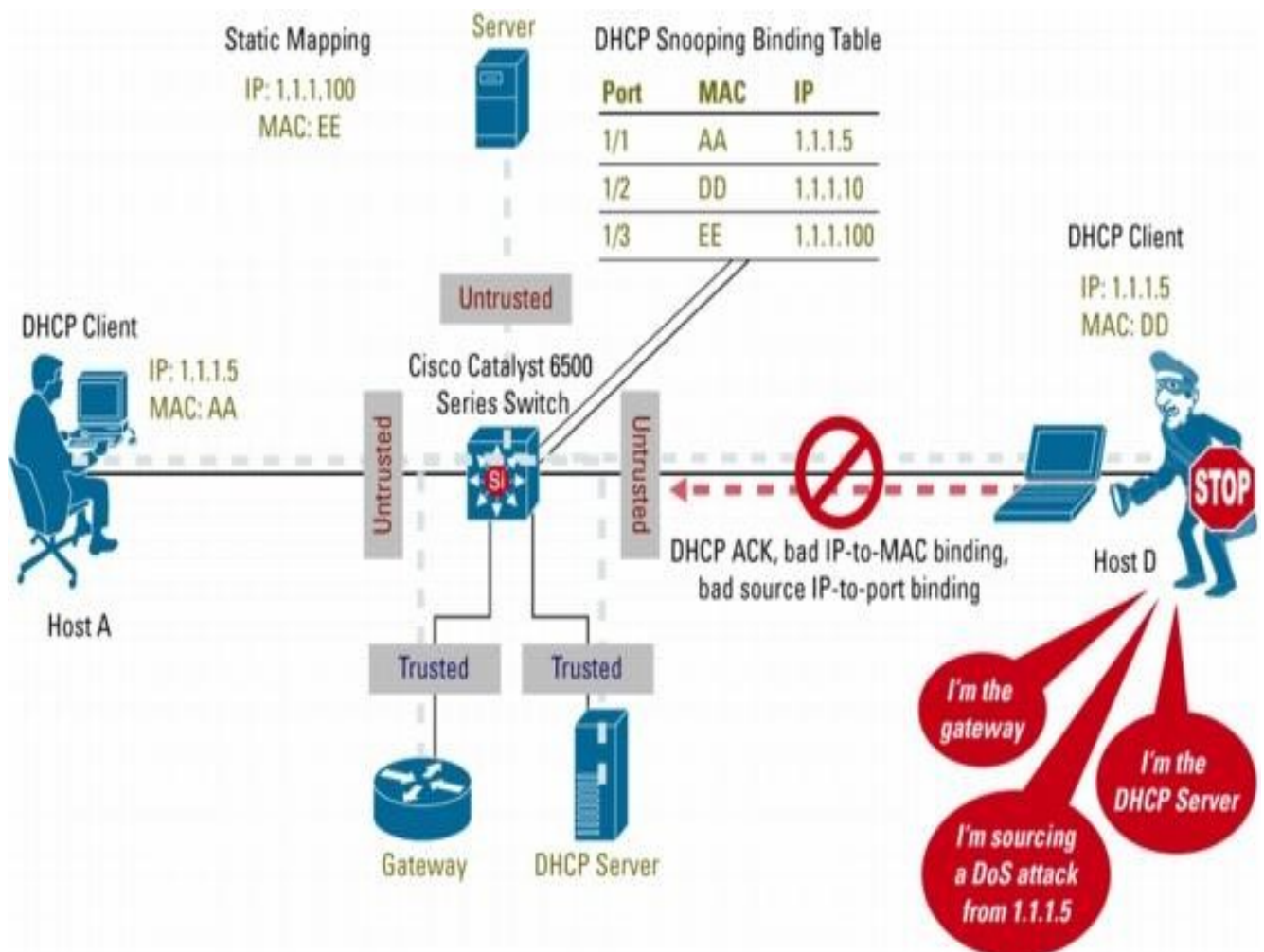


El protocolo DHCP base no incluye ningún mecanismo para la autenticación. Debido a esto, es vulnerable a una variedad de ataques. Estos ataques se dividen en tres categorías principales:

* Servidores DHCP no autorizados que proporcionan información falsa a los clientes:



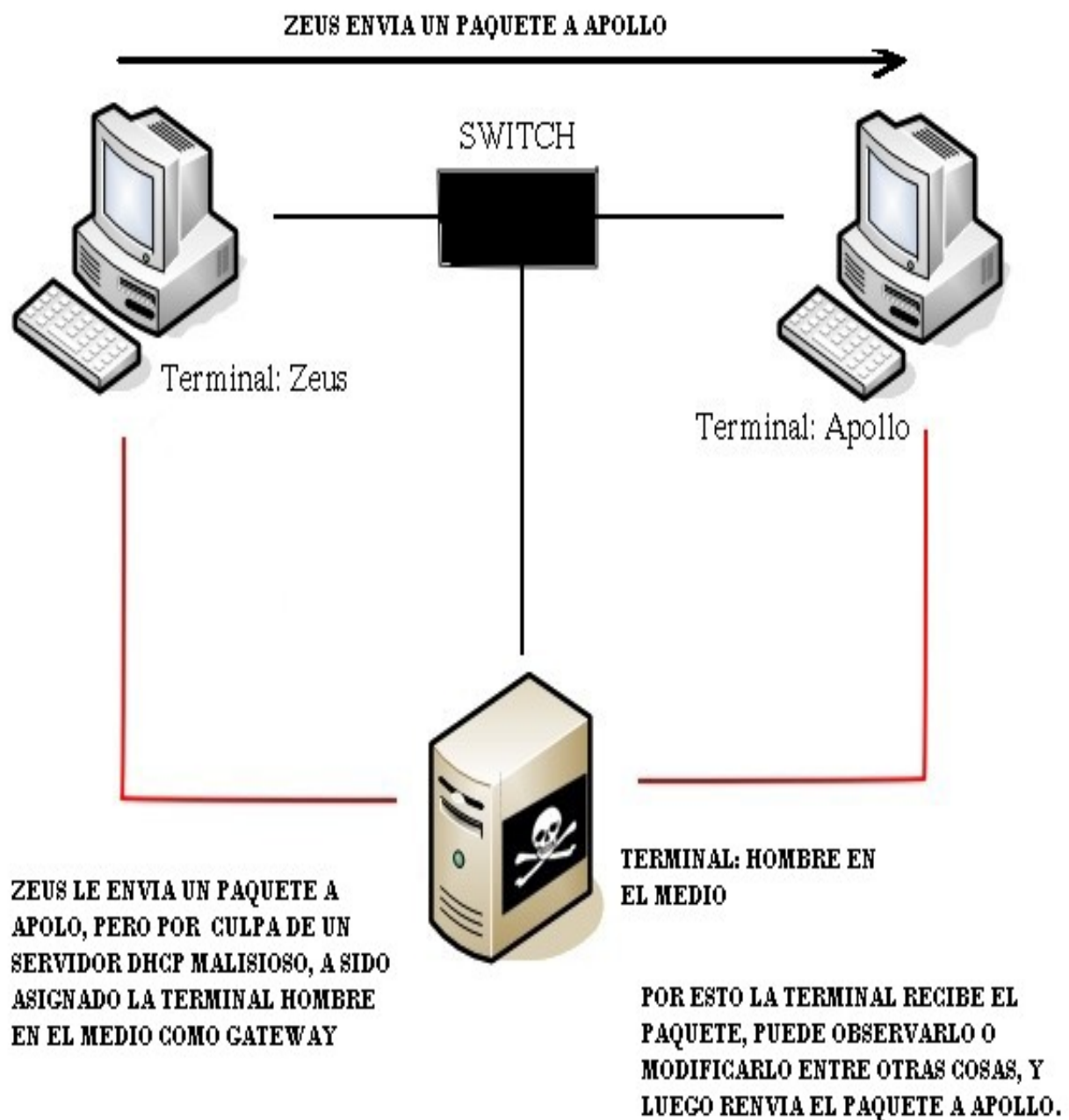
- * Clientes no autorizados tengan acceso a los recursos.
- * Ataques de agotamiento de recursos provenientes de clientes DHCP maliciosos.



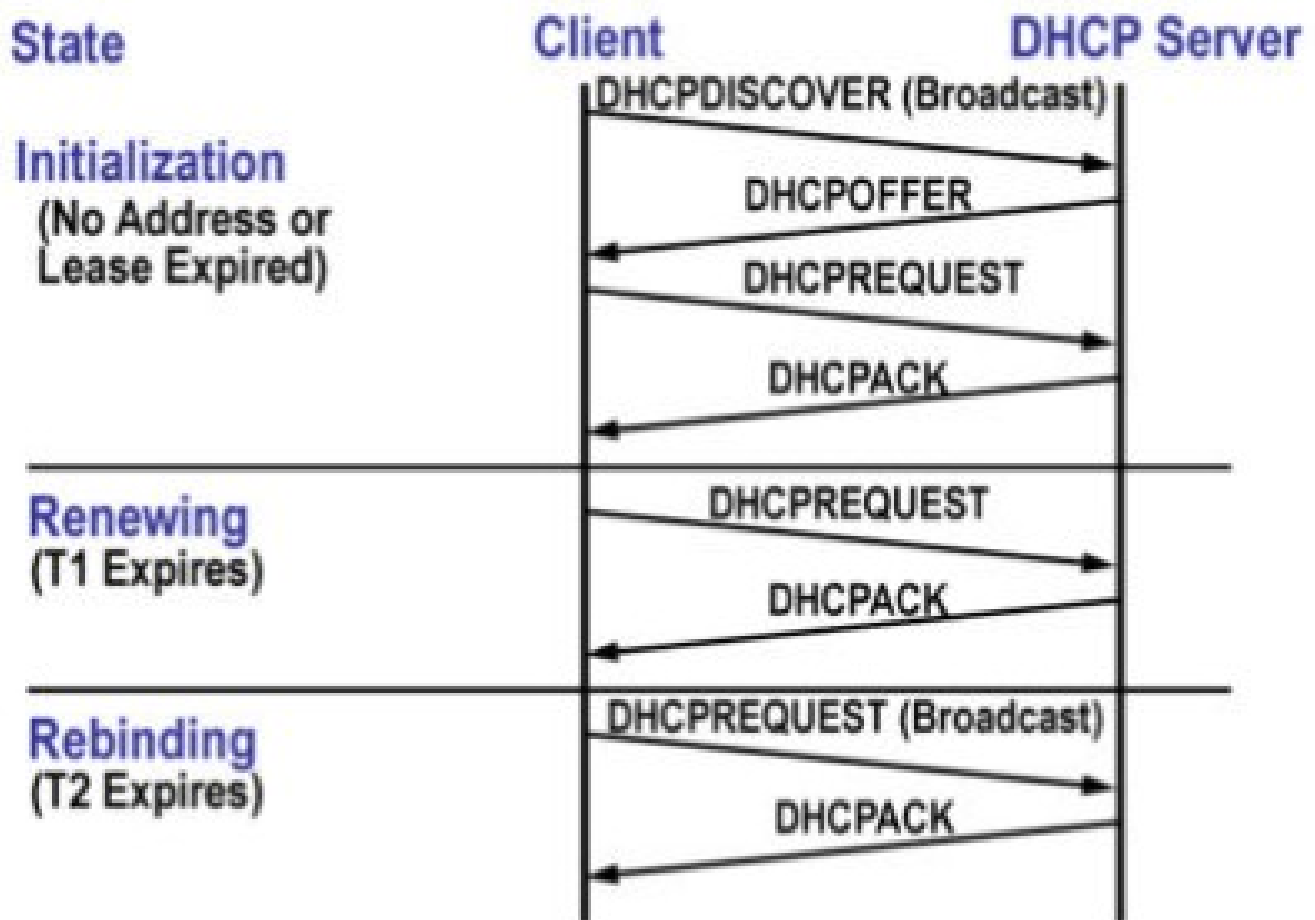
Ataque de negacion de servicios:



Ejemplo de man-in-the-middle-attack (hombre en el medio):



Reliability



IETF standards documents (RFCs)

- RFC 2131, Dynamic Host Configuration Protocol.
- RFC 2132, DHCP Options and BOOTP Vendor Extensions.
- RFC 3046, DHCP Relay Agent Information Option.
- RFC 3942, Reclassifying Dynamic Host Configuration Protocol Version Four (DHCPv4) Options.
- RFC 4242, Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6.
- RFC 4361, Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4).
- RFC 4436, Detecting Network Attachment in IPv4 (DNaV4).

Referencias

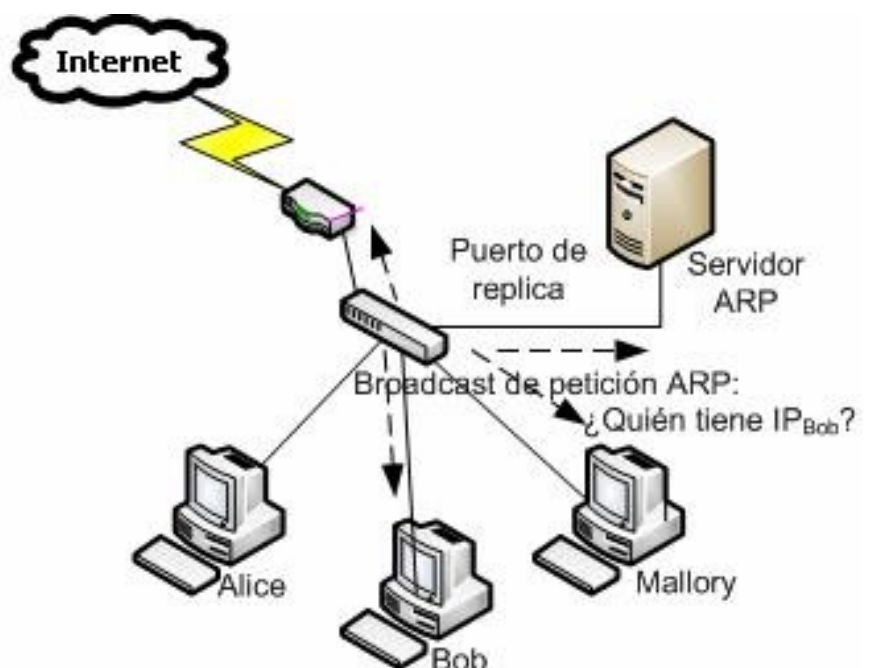
- http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol





FUNCIONAMIENTO DEL **PROTOCOLO ARP**

El protocolo ARP se publicó en Noviembre de 1982 como RFC 826 por David C. Plumier. Como la seguridad en las tecnologías de la información no era un factor importante en aquella época, el objetivo era simplemente proporcionar funcionalidad. ARP transforma direcciones IP a direcciones MAC.



IP



MAC

ARP REQUEST

OPCODE =

SENDER MAX =

SENDER IP =

TARGET MAX =

TARGET IP =

ARP REPLY

OPCODE =

SENDER MAC =

TARGET MAX=

TARGET IP =

Estructura del Paquete

0	8	16	24	31
TIPO DE HARDWARE		TIPO DE PROTOCOLO		
HLEN	PLEN	OPERACION		
SENDER HA (octeto 0 - 3)				
SENDER HA (OCTETO 4 - 5)		SENDER IP (OCTETO 0 - 1)		
SENDER IP (OCTETO 2 - 3)		TARGET HA (OCTETO 0 - 1)		
TARGET HA (octeto 2 - 5)				
TARGET IP (octeto 0 - 3)				

El ARP utiliza un formato simple de mensaje que contiene una petición de resolución de dirección o respuesta.

El ARP utiliza un formato simple de mensaje que contiene una petición de resolución de dirección o respuesta.

El tamaño del mensaje ARP depende de la capa superior y tamaños de direcciones de capa inferior, que se da por el tipo de protocolo de red (por lo general IPv4) en uso y el tipo de hardware o capa de enlace virtual que el protocolo de capa superior que se está ejecutando. El encabezado del mensaje especifica estos tipos, así como el tamaño de las direcciones de cada uno. El encabezado del mensaje se completa con el código de operación para la solicitud y la respuesta. El contenido del paquete principalmente consta de cuatro direcciones, la dirección de hardware y la dirección IP de los host emisores y de los host receptores.

IP



MAC



La estructura principal del paquete ARP seria de la siguiente manera:

- Tipo de Hardware (HTYPE):Este campo especifica el tipo de protocolo de red. Ejemplo: Ethernet es 1.
- Tipo de protocolo (PTYPE):Este campo especifica el protocolo de interconexión de redes para las que se destina la petición ARP.Para IPv4, esto tiene el valor 0x0800.
- Longitud de hardware (HLEN):Longitud (en octetos) de una dirección de hardware (MAC). Direcciones Ethernet tamaño es 6.
- Longitud de protocolo (PLEN):Longitud (en octetos) de direcciones utilizadas en el protocolo de capa superior. (El protocolo de capa superior se especifica en PTYPE.) Tamaño de la dirección IPv4 es 4.
- Operación:Especifica la operación que el emisor está realizando: 1 para la petición, 2 para la respuesta.
- Dirección de hardware del remitente (SHA):En una solicitud ARP este campo se utiliza para indicar la dirección del host que envía la solicitud.
- Dirección de protocolo del remitente (SPA):Dirección de red interna del remitente.
- Dirección hardware de destino (THA):En una solicitud de ARP se ignora este campo. En una respuesta ARP este campo se utiliza para indicar la dirección del host que originó la petición ARP.
- Dirección de protocolo de destino (TPA):Dirección de red interna del receptor previsto.

ARP probe

- Un ARP Probe es una petición ARP construido con una dirección ip de remitente totalmente en cero. El término se utiliza en la especificación de direcciones IPv4 detección de conflictos (RFC 5227). Antes de comenzar a utilizar una dirección IPv4 (si recibió una configuración manual, DHCP, o algún otro medio), el host implementa esta especificación para probar si la dirección ya está en uso, por medio de paquetes ARP Probe en broadcast.

ARP spoofing

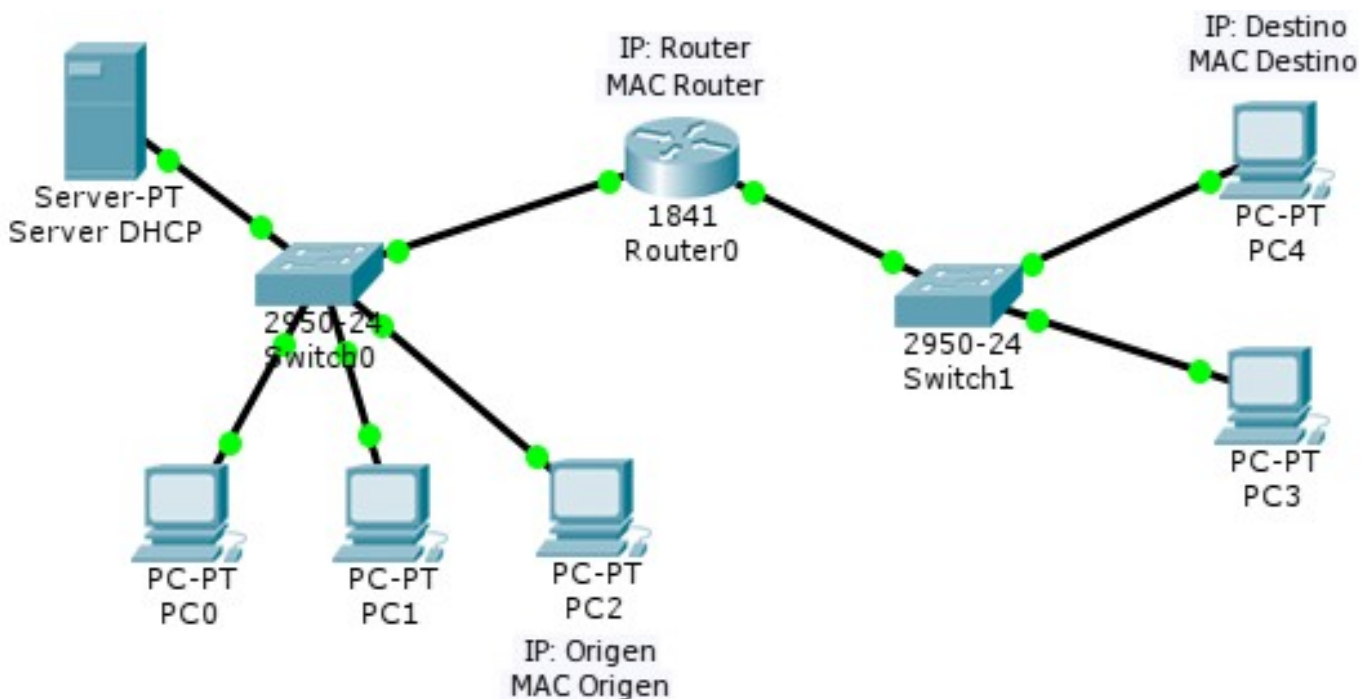
El principio básico detrás de ARP spoofing es explotar las vulnerabilidades en el protocolo ARP mediante el envío de mensajes ARP imitando a la LAN. Los ataques de suplantación ARP se pueden ejecutar desde un host comprometido en la LAN o de la máquina de un atacante que está conectado directamente a la LAN.

Existen algunos mecanismos de defensa para estos ataques:

- Entradas ARP estáticas: Asignar manualmente las entradas IP-Mac de la tabla cache arp de los host manualmente.
- Software de detección de suplantación de identidad ARP: Software que detecta ARP Spoofing en general se basa en algún tipo de certificación o verificación cruzada de respuestas ARP.
- seguridad del sistema operativo:
- Los sistemas operativos reaccionan de manera diferente, por ejemplo, Linux ignora respuestas no solicitadas, pero por otra parte utiliza las peticiones de otras máquinas para actualizar su caché.

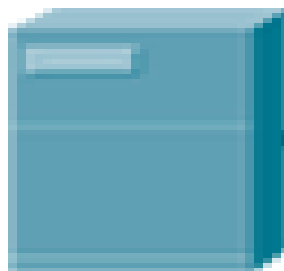
Proxy ARP

Unirse a una emisión
broadcast LAN con enlaces en
serie :

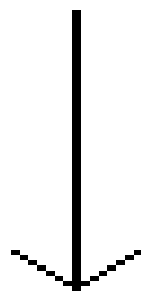


Tomando múltiples direcciones de una LAN:

Server

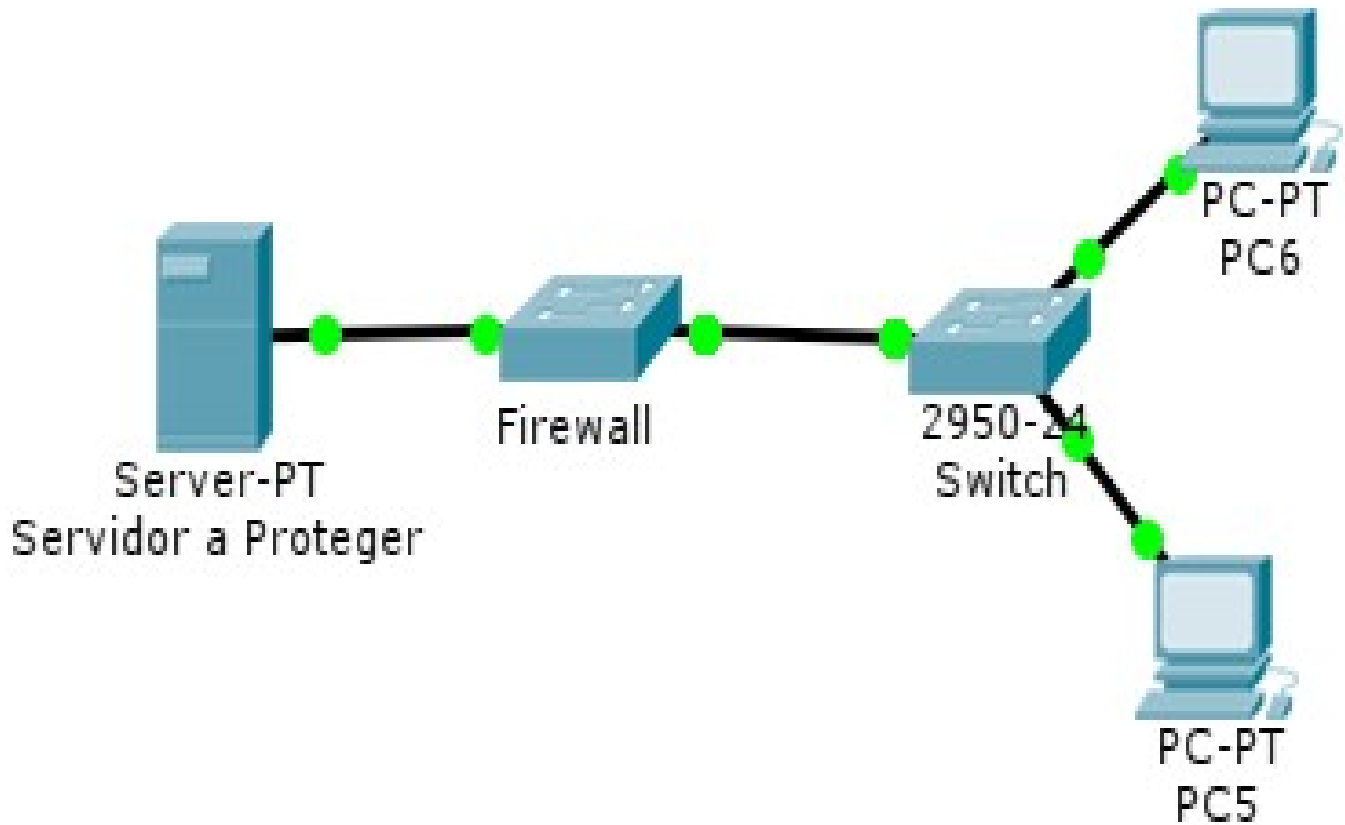


**Consulta de
Múltiples IP**



**IP : 192.168.1.10
IP : 192.168.1.11
IP : 192.168.1.12**

En un firewall:



* Mobile-IP:

En caso de Mobile-IP del Home Agent utiliza Proxy ARP para recibir mensajes en nombre del nodo móvil, de modo que pueda enviar el mensaje adecuado a la dirección del nodo móvil real (atención de la dirección).

- Transparent subnet gatewaying:
Una configuración que implica dos segmentos físicos que comparten la misma subred IP y conectados entre sí a través de un router. Este uso está documentado en el RFC 1027.

Ventajas:

La ventaja de Proxy ARP sobre otros esquemas de redes es la simplicidad. Una red puede ser extendido usando esta técnica sin el conocimiento del router.

Desventajas:

Las desventaja del Proxy ARP incluyen escalabilidad (se requiere una resolución ARP para cada dispositivo enrutado de esta manera) y fiabilidad (sin mecanismo de reserva presente). Las Técnicas de manipulación ARP, sin embargo, son la base de protocolos que proporcionan redundancia en redes de difusión (por ejemplo, Ethernet), más notablemente CARP y Virtual Router Redundancy Protocol.

IETF standards documents (RFCs)

- ★ RFC 826 - Ethernet Address Resolution Protocol, Internet Standard STD 37.
- ★ RFC 903 - Reverse Address Resolution Protocol, Internet Standard STD 38.
- ★ RFC 2390 - Inverse Address Resolution Protocol, draft standard
- ★ RFC 5227 - IPv4 Address Conflict Detection, proposed standard

Referencias

- ➔ http://en.wikipedia.org/wiki/Address_Resolution_Protocol
- ➔ http://en.wikipedia.org/wiki/ARP_spoofing
- ➔ http://en.wikipedia.org/wiki/Proxy_ARP