

Seguretat Informàtica: Seguretat Física. Tècniques d'atacs Hacker



Xavier Tartera

La principal premissa que cal presentar davant un atac és l'ANONIMAT, i això no vol dir que no diguis el teu nom....

La funció que té l'ús de tècniques d'anonimat per un atacant té dos aspectes fonamentals:

- Ocultar la seva identitat.
- Esborrar el seu rastre

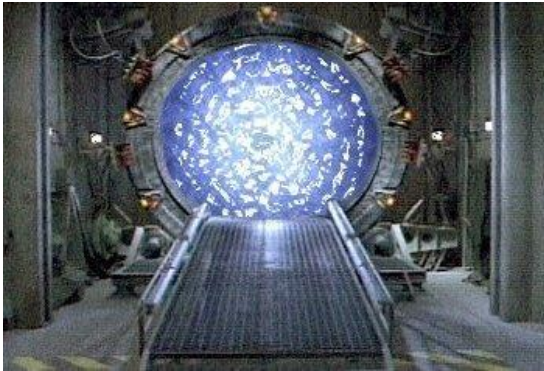
S'usen tres tècniques principalment:

- Anonimat Físic: Cibercafè, wifi's obertes, etc...
- Anonimat per ús de "bouncer"
- Anonimat per ús de proxy

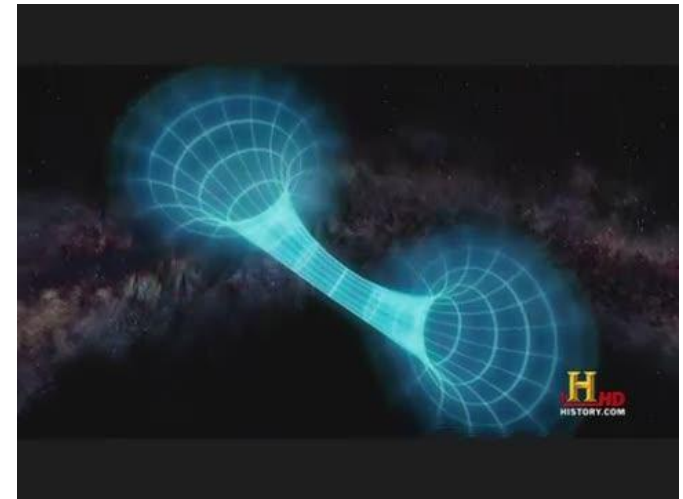


Anonimat per ús de “bouncer”

Les tècniques més freqüents utilitzen un sistema que es converteixi amb l'inici d'un portal del sistema atacant, que cerca finalitzar el seu recorregut en el sistema víctima.



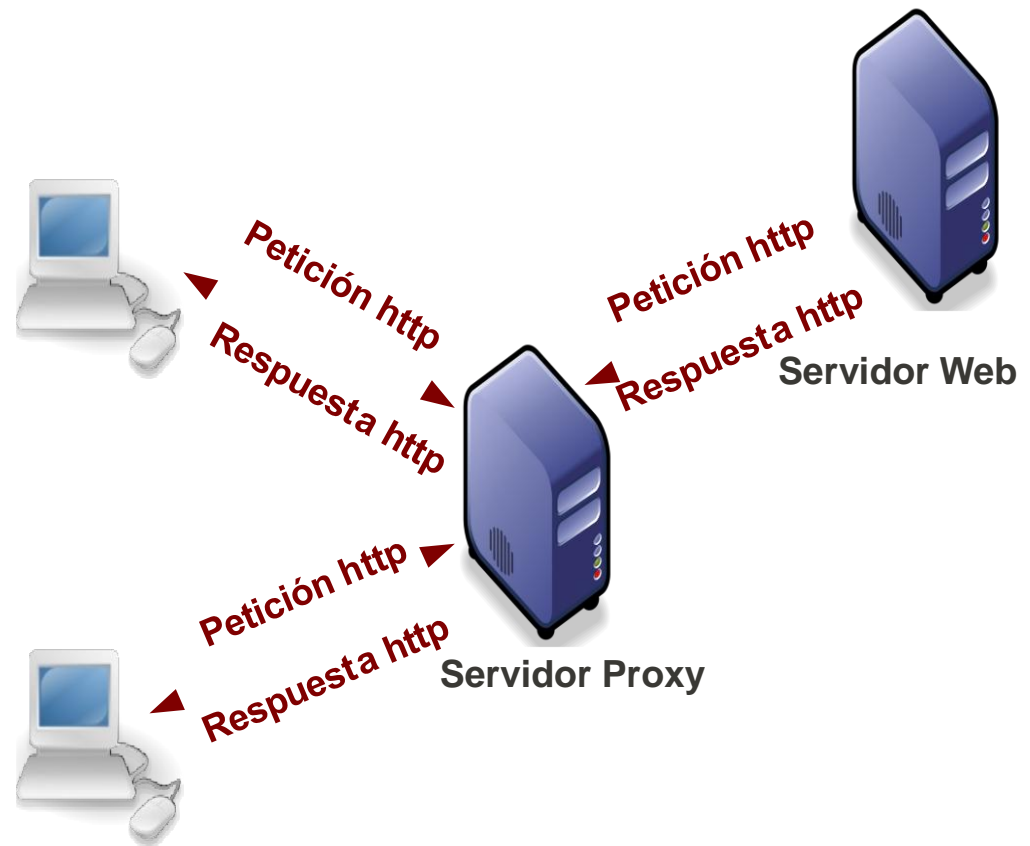
Un “bouncer” és un sistema sobre el que l'atacant hi té drets totals.



Per convertir a una víctima en un “bouncer” és necessari aprofitar les vulnerabilitats del seu sistema amb l'ús de algun exploit o injecció de algun troià.

Anonimat per ús de proxy's

- Un proxy és un intermediari entre un client i un servidor.
- Actúa a la vegada com a client i servidor.
- Normalment un proxy, ho és de varis clients i té una caché associada per augmentar la velocitat en futures peticions http.



Anonimat per ús de proxy's

Un servidor proxy és un equip servidor que es troba entre els usuaris i els servidors als que necessiten tenir accés. Quan l'usuari sol·licita un determinat recurs remot mitjançant una adreça URL, el servidor proxy rep aquesta sol·licitud i obté els recursos per complir-la.

- Aquest procés permet al servidor proxy d'emmagatzemar el contingut sol·licitat en la memòria cau.
- Tota nova sol·licitud que demana informació ja en la memòria cau ja no necessita manteniment per anar a buscar des del servidor remot.
- En canvi, la nova sol·licitud compta amb els serveis de les dades emmagatzemades a la memòria cau.
- L'objectiu propòsit d'un proxy és recuperar el recurs sol·licitat des del servidor remot, o de la memòria cau en els discos locals tornar a l'usuari sol·licitant la informació desitjada.

Anonimat per ús de proxy's

Hi ha alguns tipus (nivells) d'anonimat en alguns servidor proxy.

- Proxy anònim (Anonymous proxy) o d'emascarament
- Proxy d'alt-anonimat (high-anonymous proxy) (elite) o anònim.
- Proxy transparent (transparent proxy) o obert.

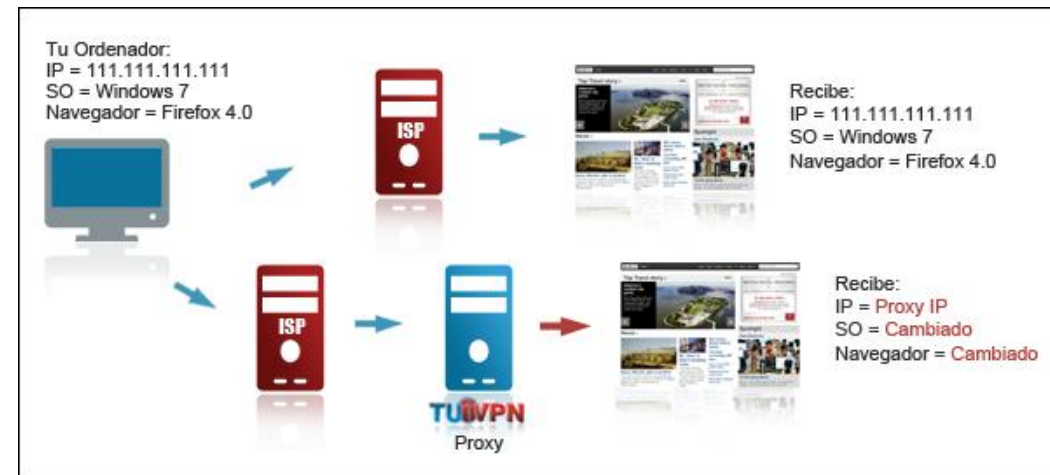
Anonymous Proxy mostra que és proxy. En resum, un host remot pot detectar proxy anònim com a proxy, però sense cap tipus d'informació sobre una IP de la persona que es troba darrere d'aquest proxy.

El proxy d'alt anonimat (high-anonymous proxy) no demostra que es tracti de poder en absolut d'ocultació d'IP, però sí que ho fa en gran mesura.

El proxy transparent canvia una adreça IP, però al mateix temps mostra IP real de l'usuari.

Anonimat per ús de proxy's

- D'aquesta manera s'esta aconseguint cert anonimat, al quedar registrada el el servidor accedit la direcció IP del Proxy i no la del atacant.
- Tot i així, els proxy's guarden registre de les comunicacions que han gestionant
- També és possible trobar un proxy que no requereixen validació i que doni suport al servei que volem utilitzar.

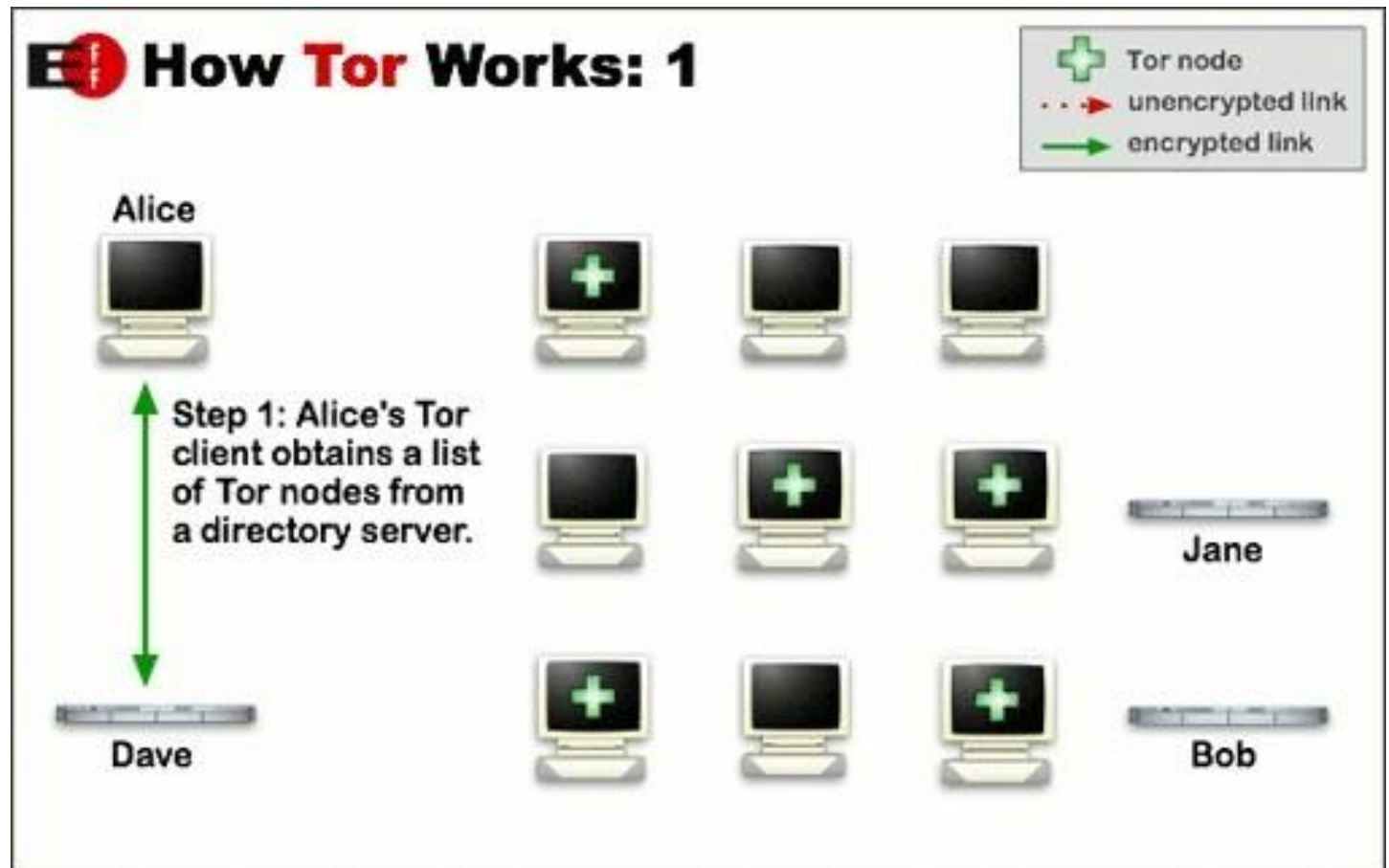
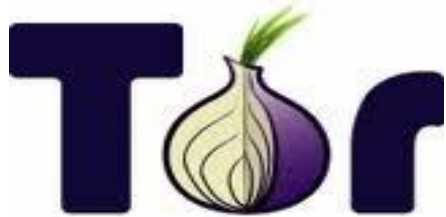


Enllaços interessants...

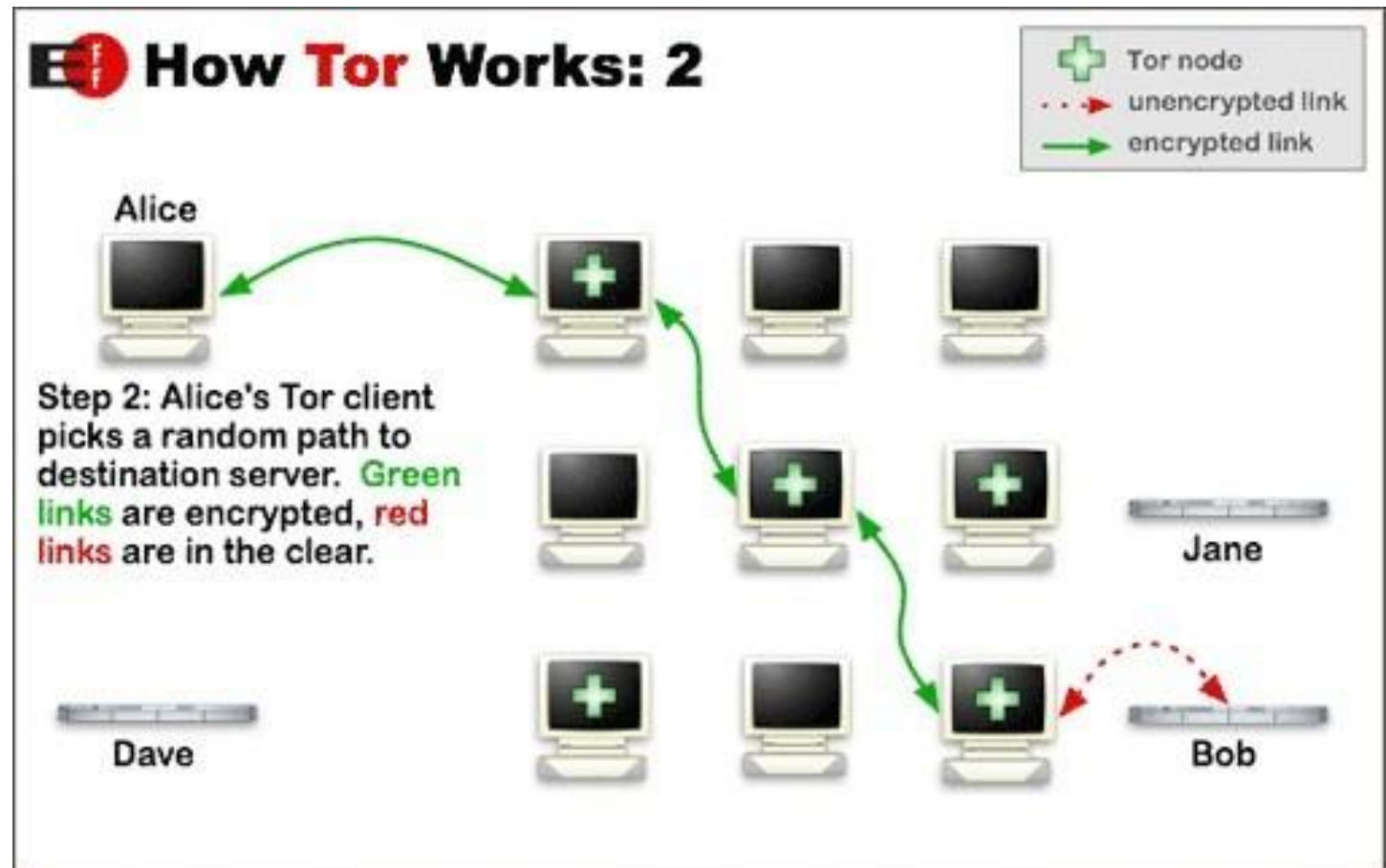
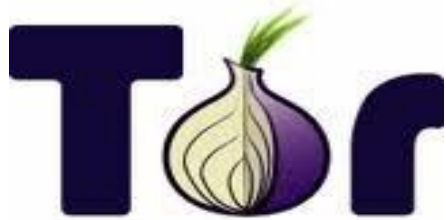
<http://www.tipsgeek.org/proxys-anonimos-gratis/122>

http://windowspanol.about.com/od/RedesYDispositivos/ss/Configurar-Proxy_2.htm

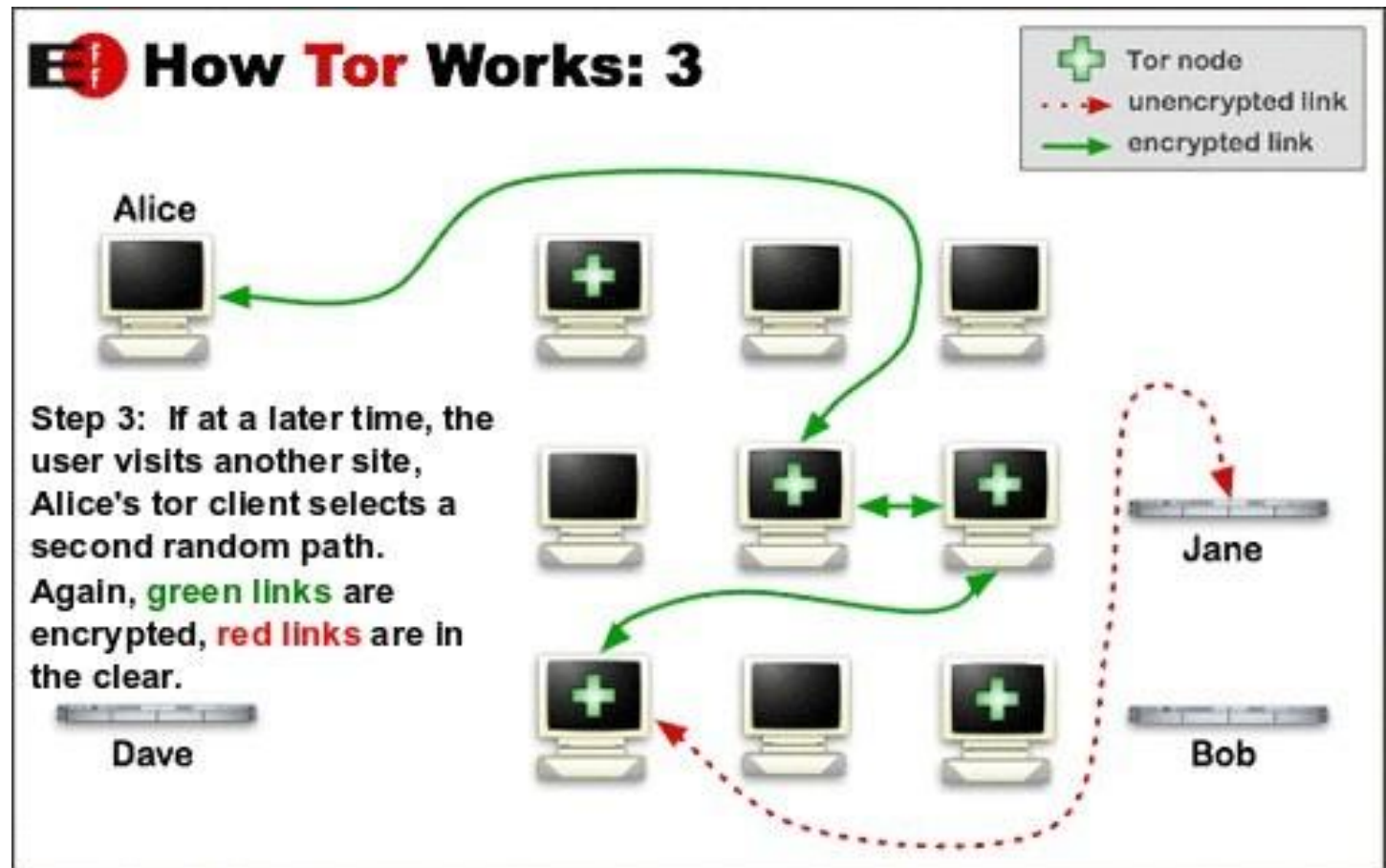
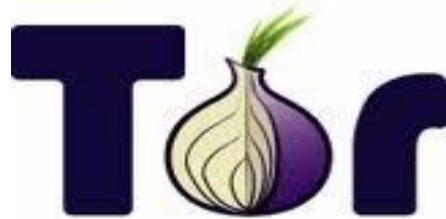
Anonimat per ús de proxy's



Anonimat per ús de proxy's




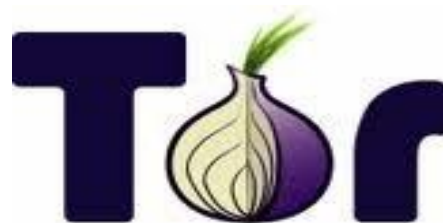
Anonimat per ús de proxy's




Anonimat per ús de proxy's

Live Demo Using IP2Location™ - December 2010

IP Address	: 81.38.17.227
Location	:  SPAIN, MADRID, MADRID
Latitude / Longitude	: 40.416691 LATITUDE, -3.700345 LONGITUDE
Connecting through	: TELEFONICA DE ESPANA SAU
Time Zone	: UTC +01:00
Net Speed	: DSL
IDD Code	: 34
Weather Station	: SPXX0050 - MADRID
MCC	: 214
MNC	: 05
Mobile Brand	: TME



Live Demo Using IP2Location™ - December 2010

IP Address	: 199.48.147.41
Location	:  UNITED STATES, CALIFORNIA, SAN FRANCISCO
Latitude / Longitude	: 37.77493 LATITUDE, -122.419416 LONGITUDE
Connecting through	: APPLIED OPERATIONS LLC
Time Zone	: UTC -08:00
Net Speed	: DSL
IDD Code	: 1
Area Code	: 415/650
Weather Station	: USCA0131 - BRISBANE

Spoofing

Spoofing o suplantació de identitat.

Objectius:

- Falsejar informació
- Enganyar
- Obtenir informació d'un usuari determinat
- Comprometre la seguretat d'uns sistema de xarxa.
- Crear confusió, fent aparentar coses que no són reals.
- ...



Tipus de Spoofing

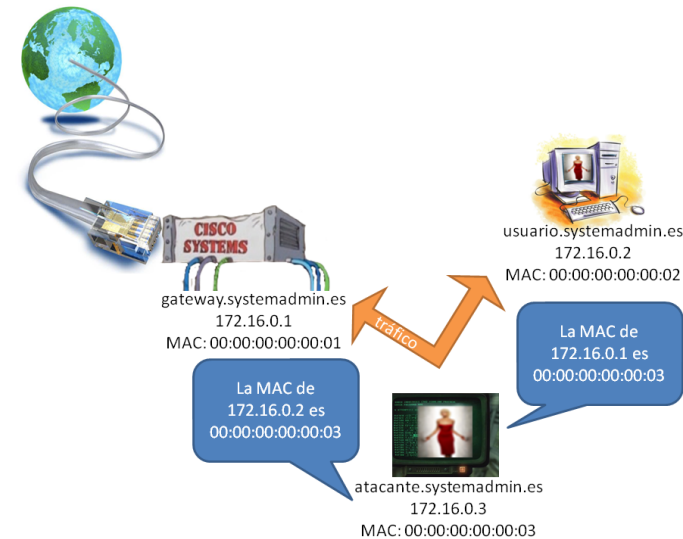
- ARP Spoofing
- IP Spoofing
- Mail Spoofing
- DNS Spoofing
- Web Spoofing
- Combinació amb altres tècniques : Sniffing i Hijacking

ARP Spoofing

Es tracta de suplantar la direcció MAC de un host, es realitza a nivell d'enllaç, pel qie són atacs a màquines connectades al mateix medi físic de LAN.

Objectius:

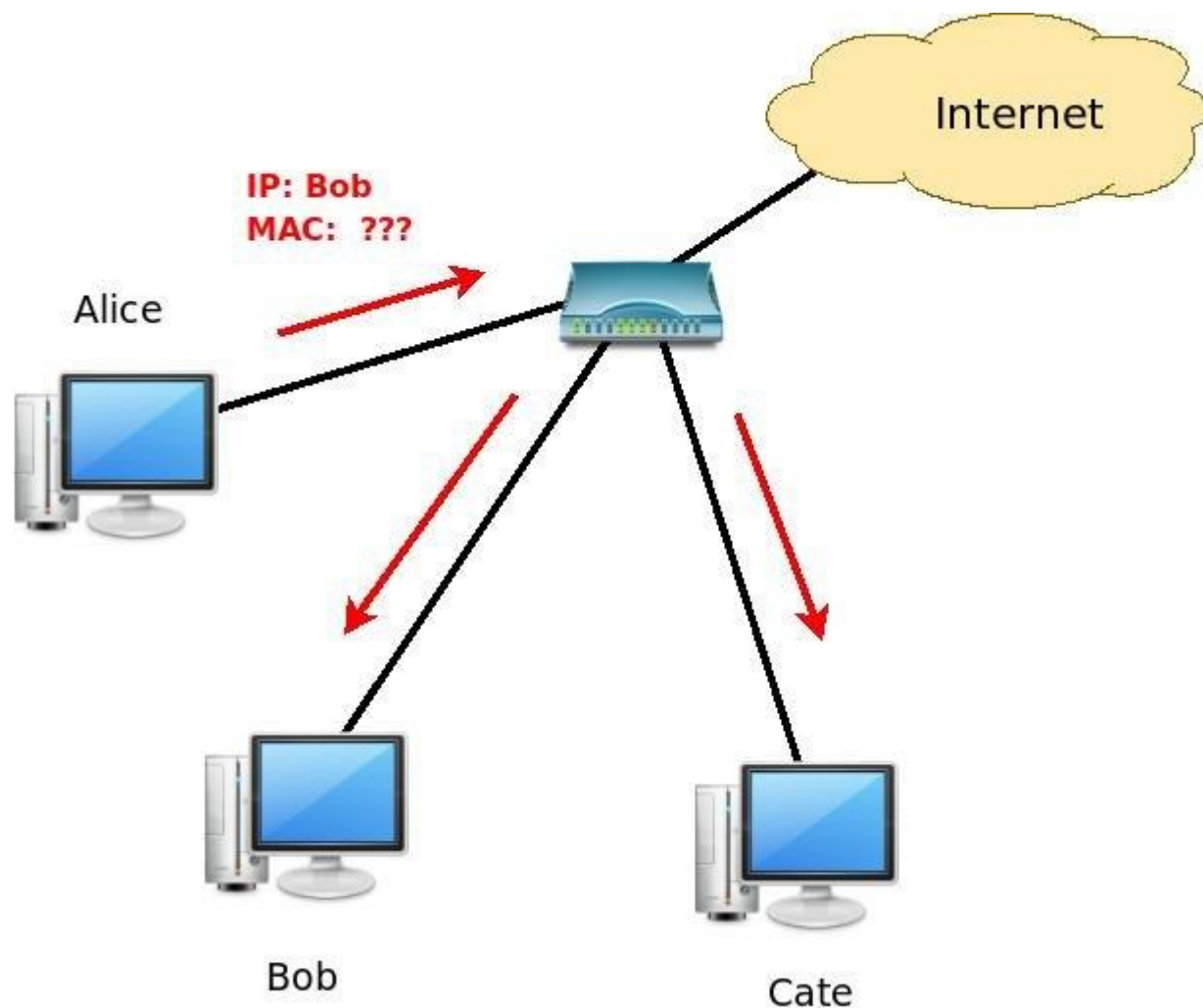
- Suplantar identitats físiques: MAC
- Reconduir una comunicació Física
- Atacar comunicacions locals
- Robatori de comunicacions.



El protocol ARP (Address Resolution Protocol) és l'encarregat de convertir les adreces IP a adreces MAC per tal de que el paquet arribi correctament al següent salt de la mateixa subxarxa.

ARP Spoofing (exemple I)

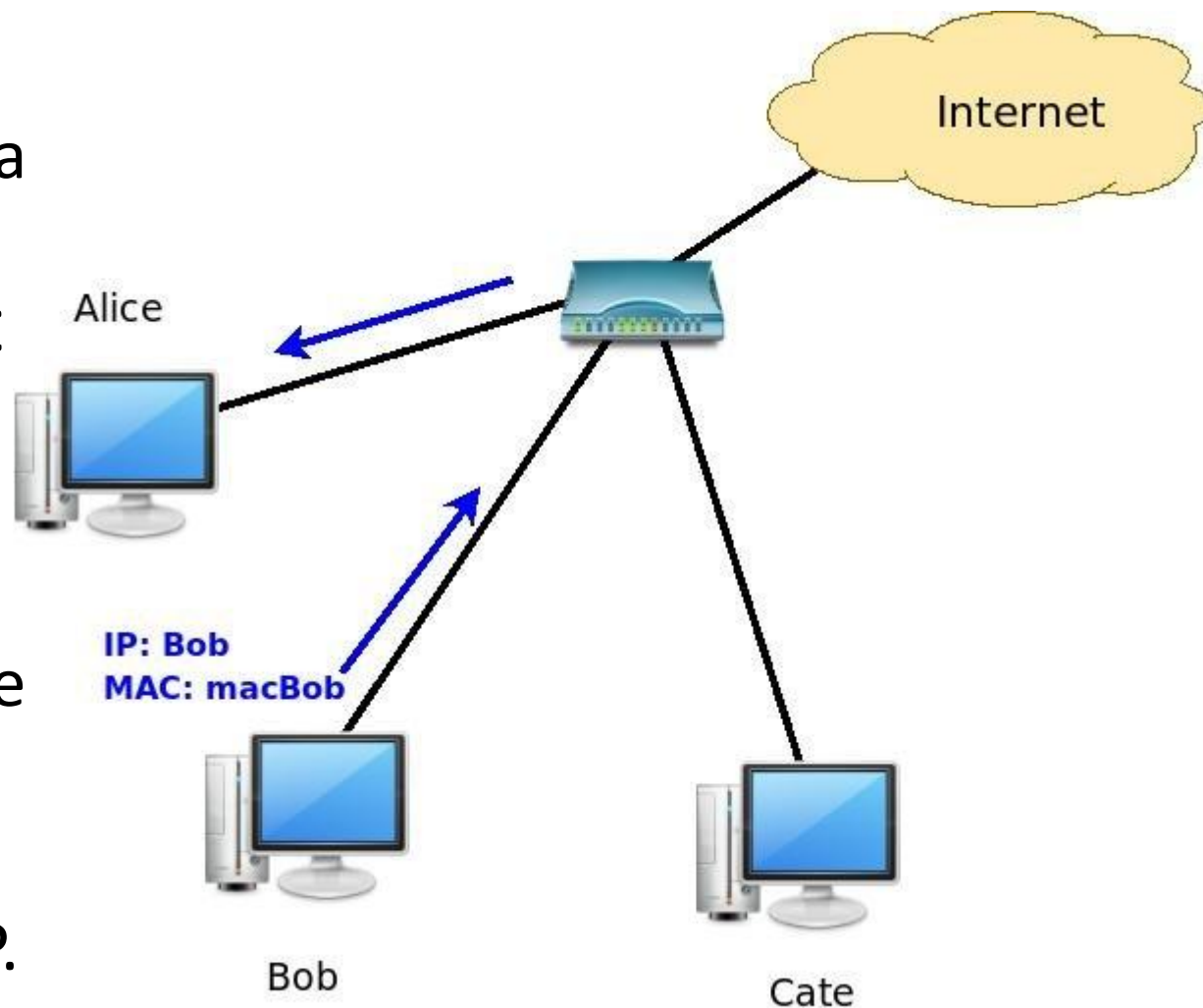
Alice vol enviar un paquet al Bob, però com no sap quina MAC té en Bob, primer envia una ARP request.



ARP Spoofing (exemple I)

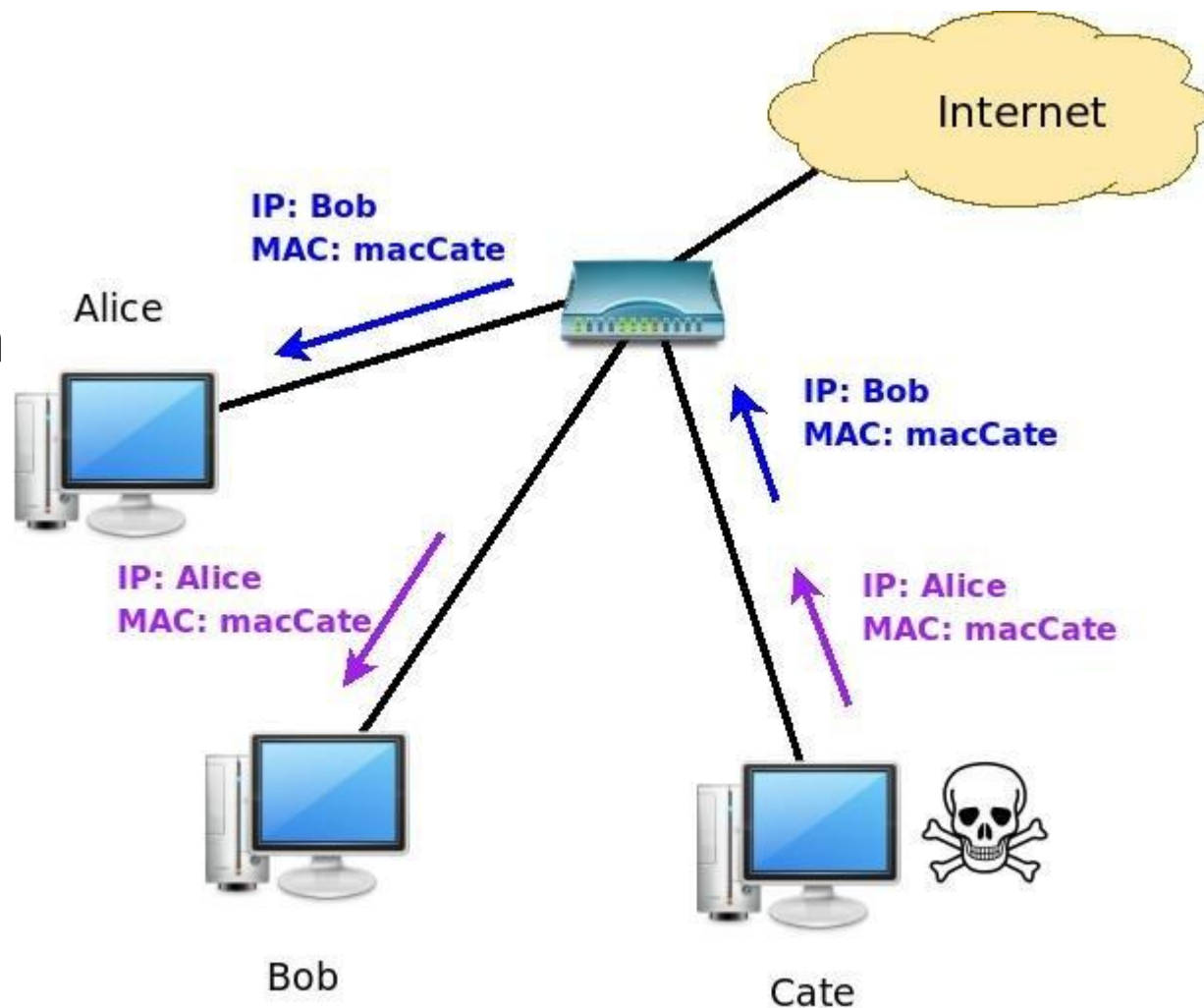
Llavors únicament en Bob contesta a la petició de l'Alice, enviant la seva adreça MAC.

Alice guardarà l'adreça MAC en una taula ARP, reemplaçant les antigues entrades en cas que n'hi hagi, i només falta que l'Alice envii el paquet amb la informació que ha obtingut del Bob a les capçaleres ARP.



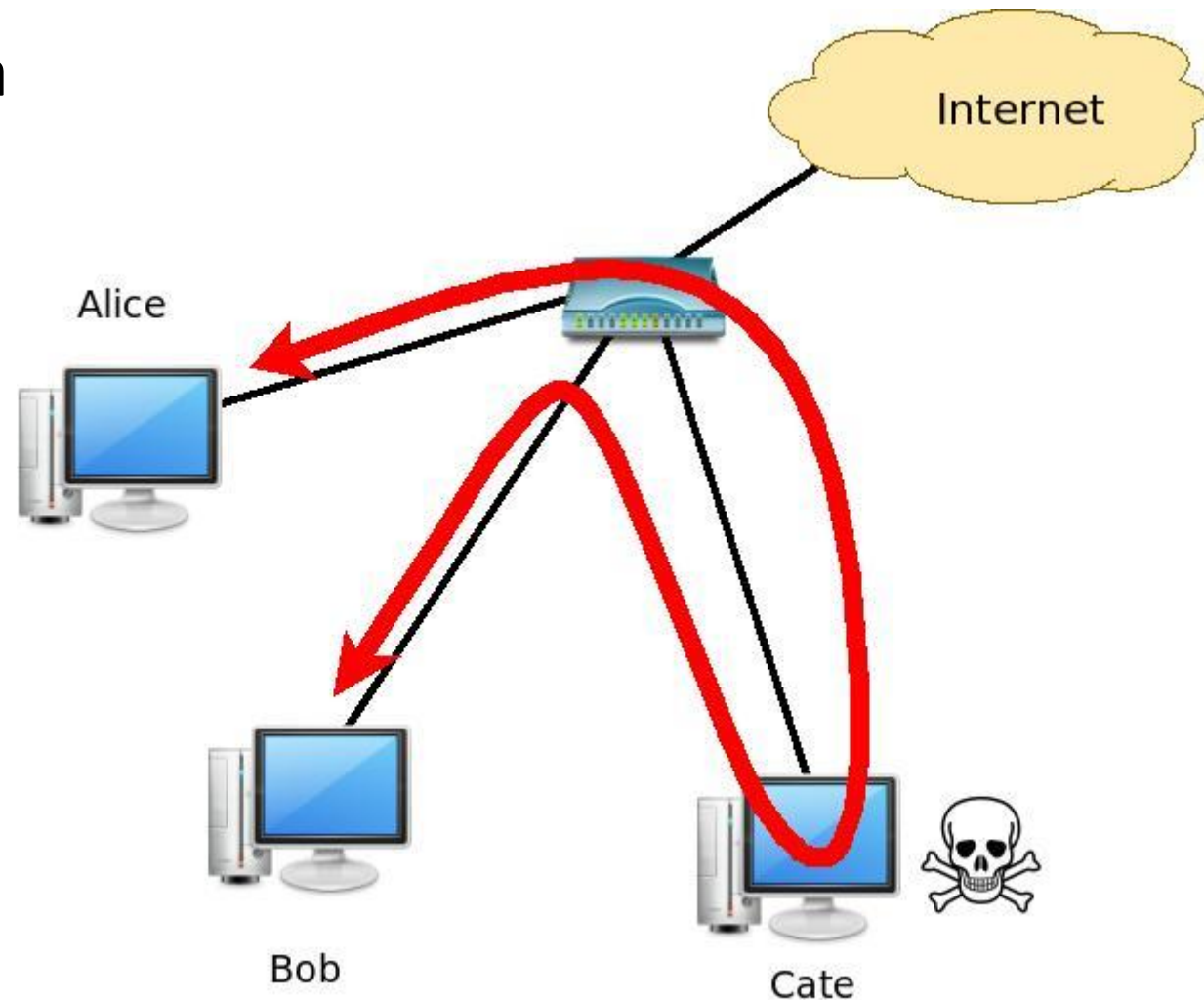
ARP Spoofing (exemple I)

La Cate vol capturar el tràfic generat entre Alice i Bob, pel que intentarà "enverinar" les taules ARP de tots dos. Per fer-ho envia un paquet ARP a Alice dient-li que a la IP del Bob li correspon la direcció MAC de la Cate i alhora envia un altre a Bob indicant que a la IP de l'Alice li correspon la direcció MAC de la Cate.



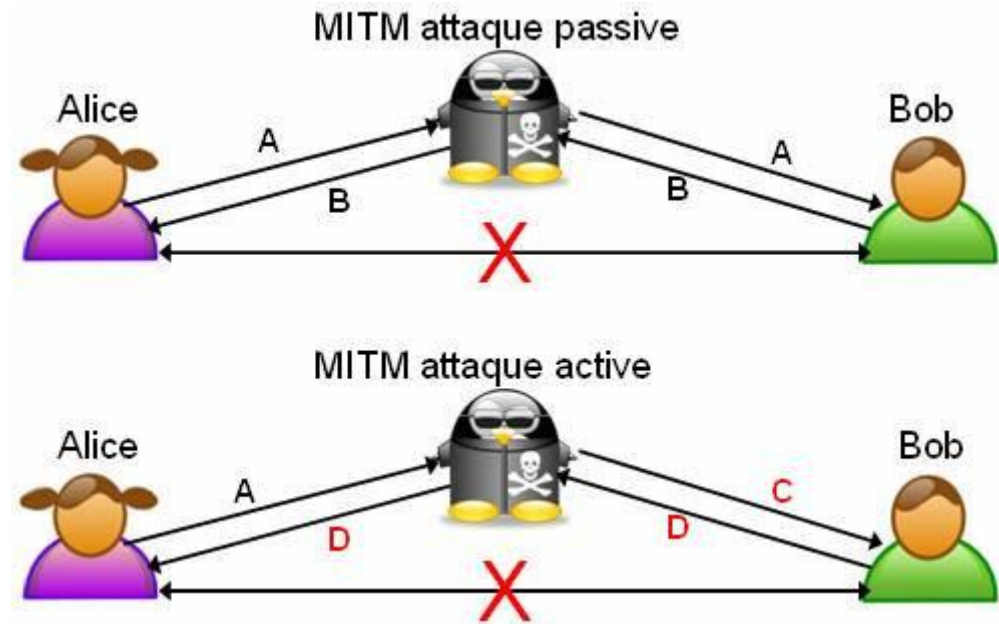
ARP Spoofing (exemple I)

Ara el trànsit generat entre l'Alice i el Bob passarà per la Cate, sempre que la Cate envii periòdicament els paquets maliciosos, ja que les taules es van actualitzant de forma periòdica.

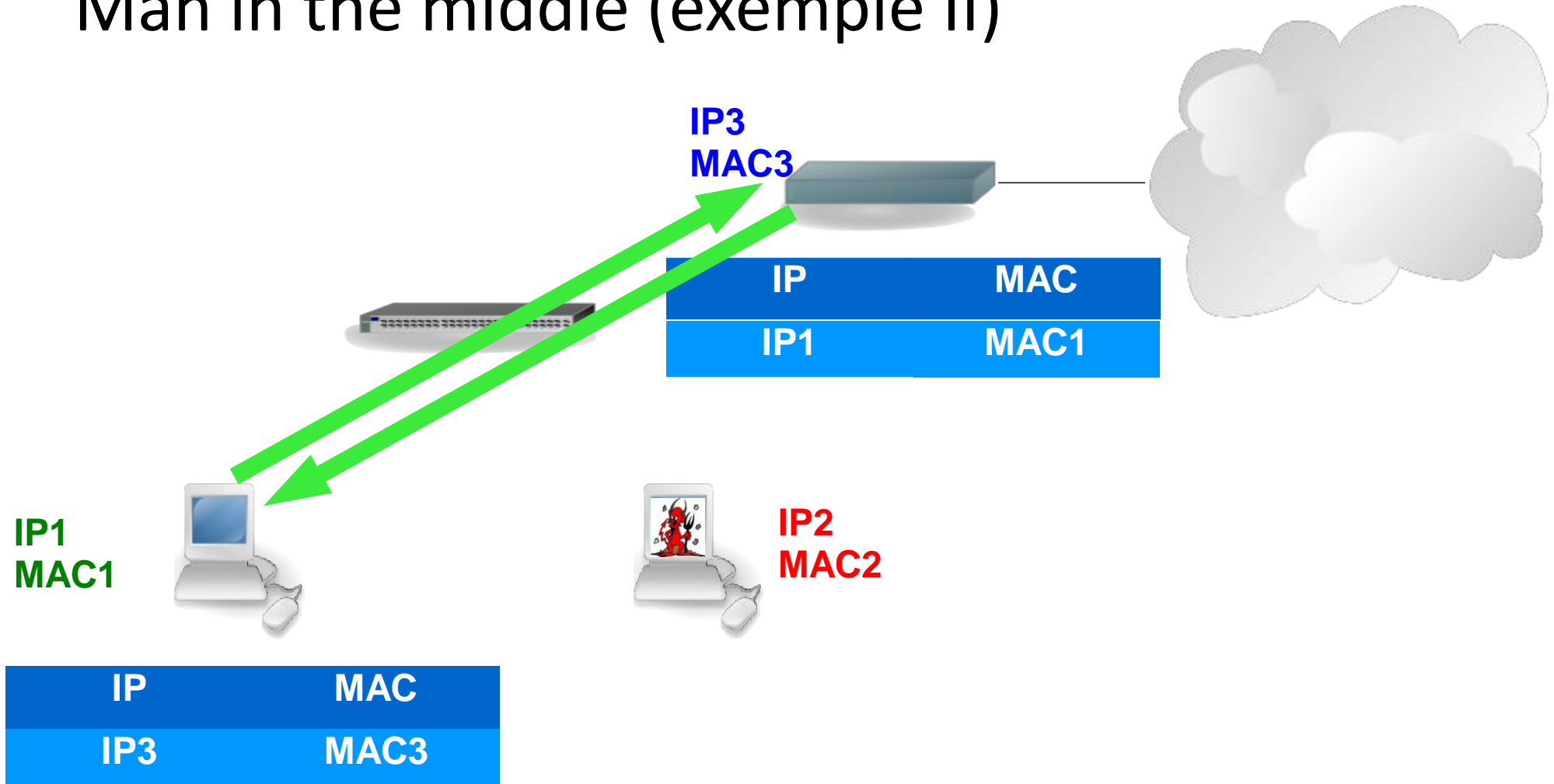


Man in the middle (exemple II)

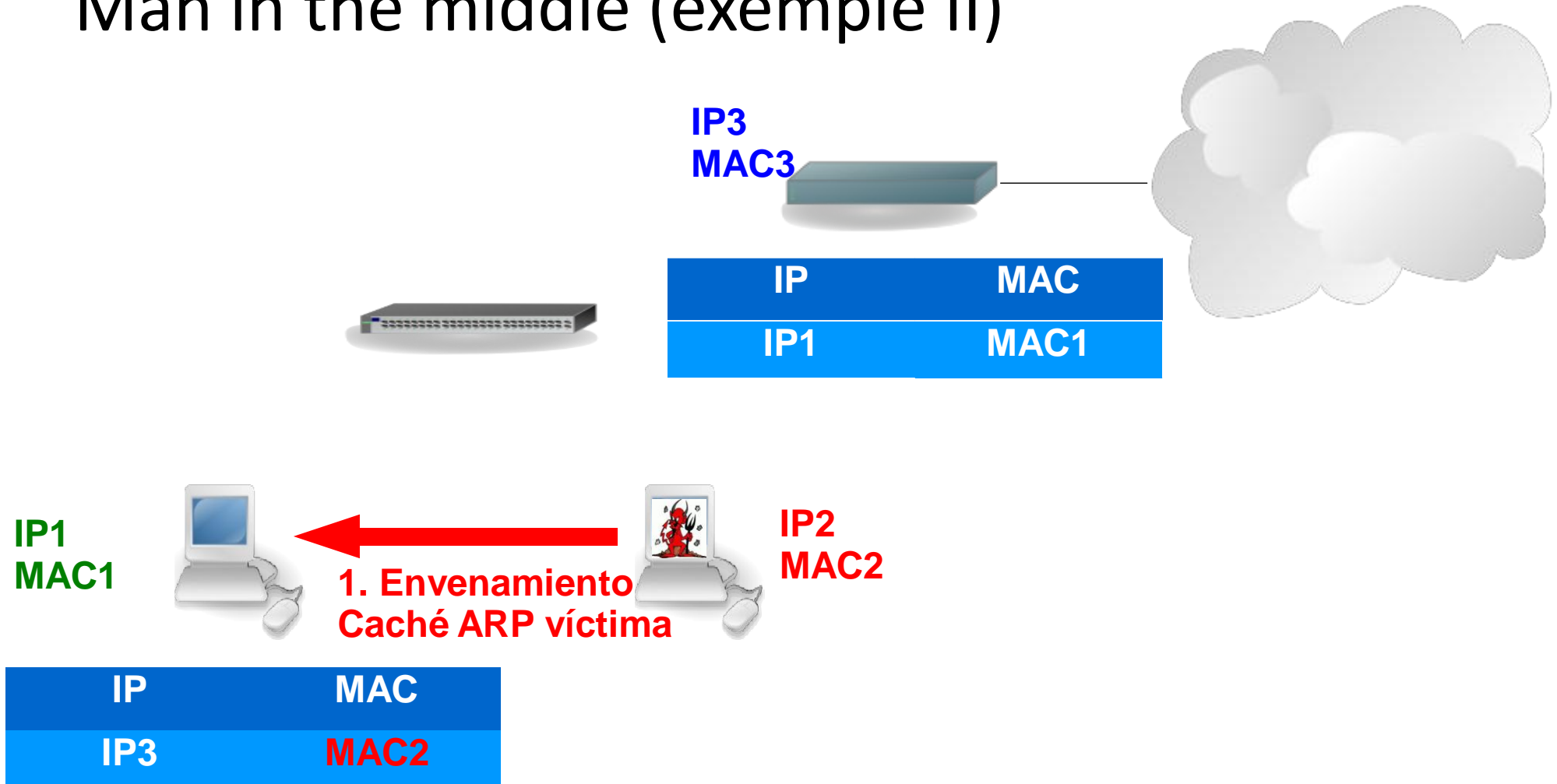
- La tècnica consisteix en interposar-se entre 2 sistemes realitzant enverinament de les cache de ARP.
- Serveix com Plataforma per altres atacs.
- Pot ser utilitzat pel robatori de sessions i/o contrasenyes.
- Serveix com a trampolí del sniffing en xarxes conmutades.



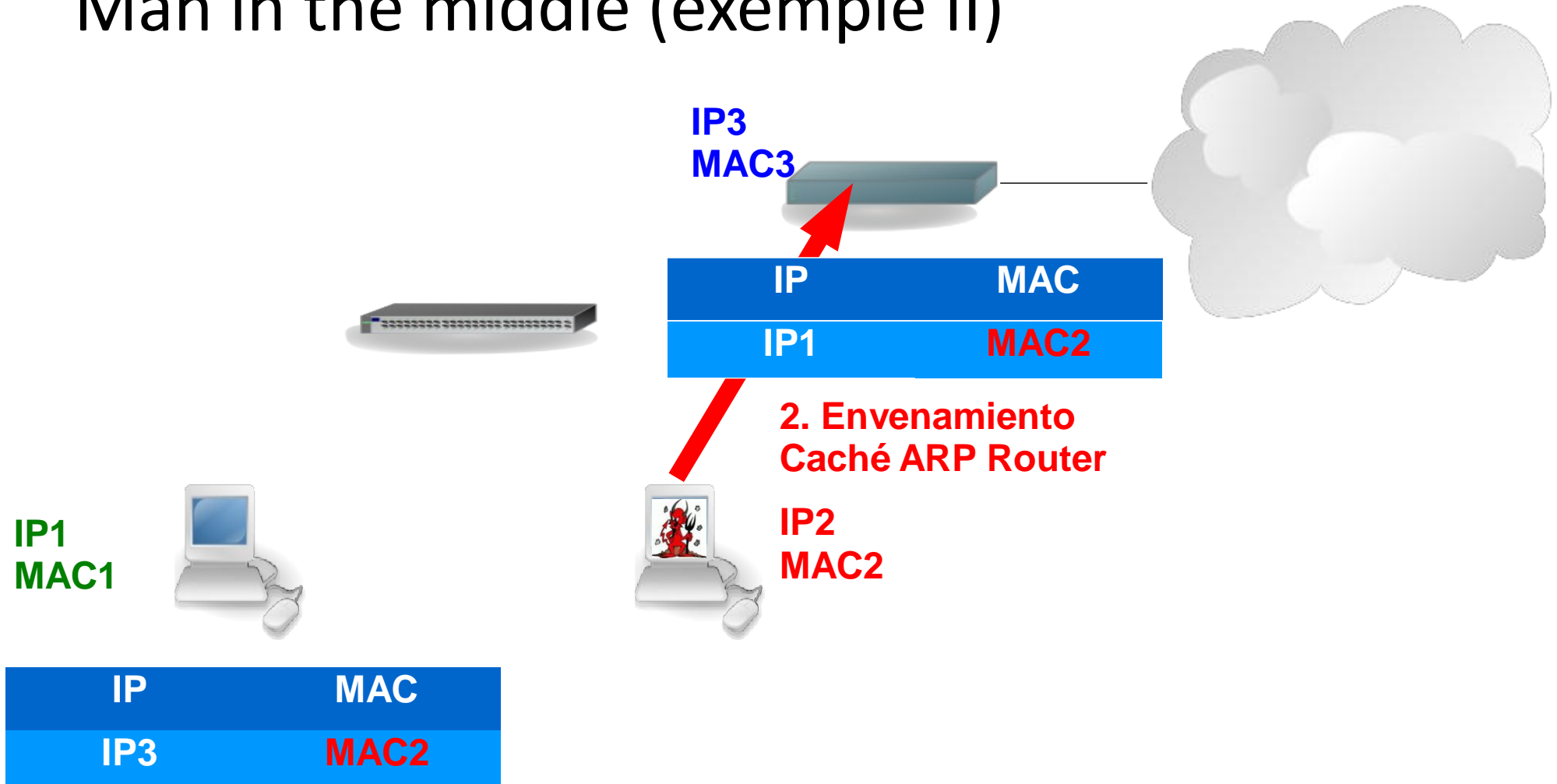
Man in the middle (exemple II)



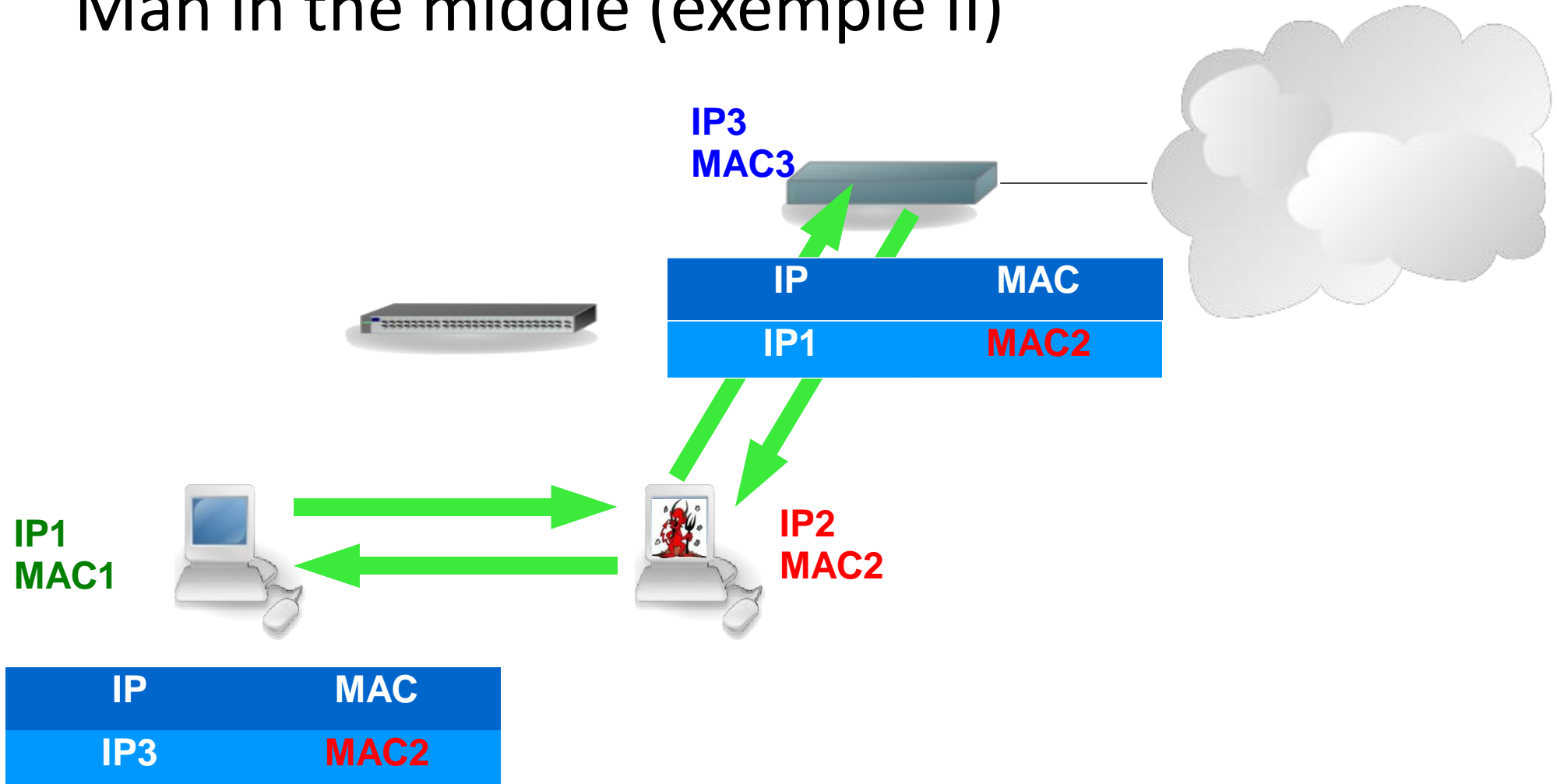
Man in the middle (exemple II)



Man in the middle (exemple II)



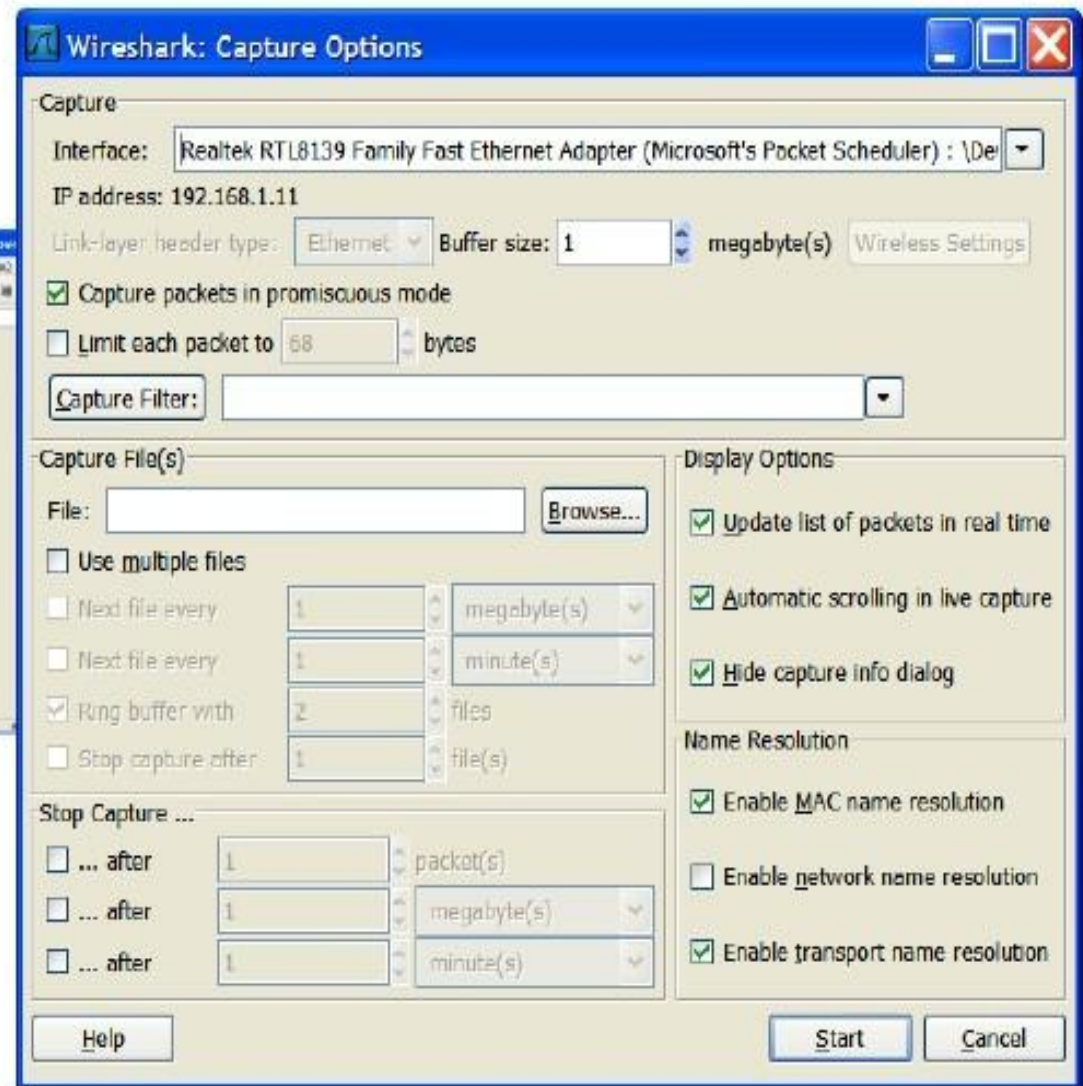
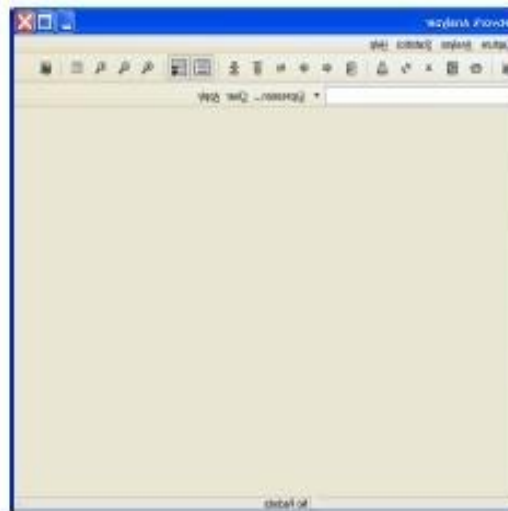
Man in the middle (exemple II)



Sniffing

- Escolta de la informació que no va dirigida a la màquina que està monitoritzant el trànsit de dades.
- S'utilitza com a metodologia per obtenir dades compromeses com contrasenyes.
- En un entorn de xarxa local conmutada necessita combinar-se amb altres tècniques (man in the middle).
- S'usen analitzadors de protocols (packet sniffers) que són programes que permeten monitoritzar i analitzar el trànsit d'una xarxa.

Wireshark

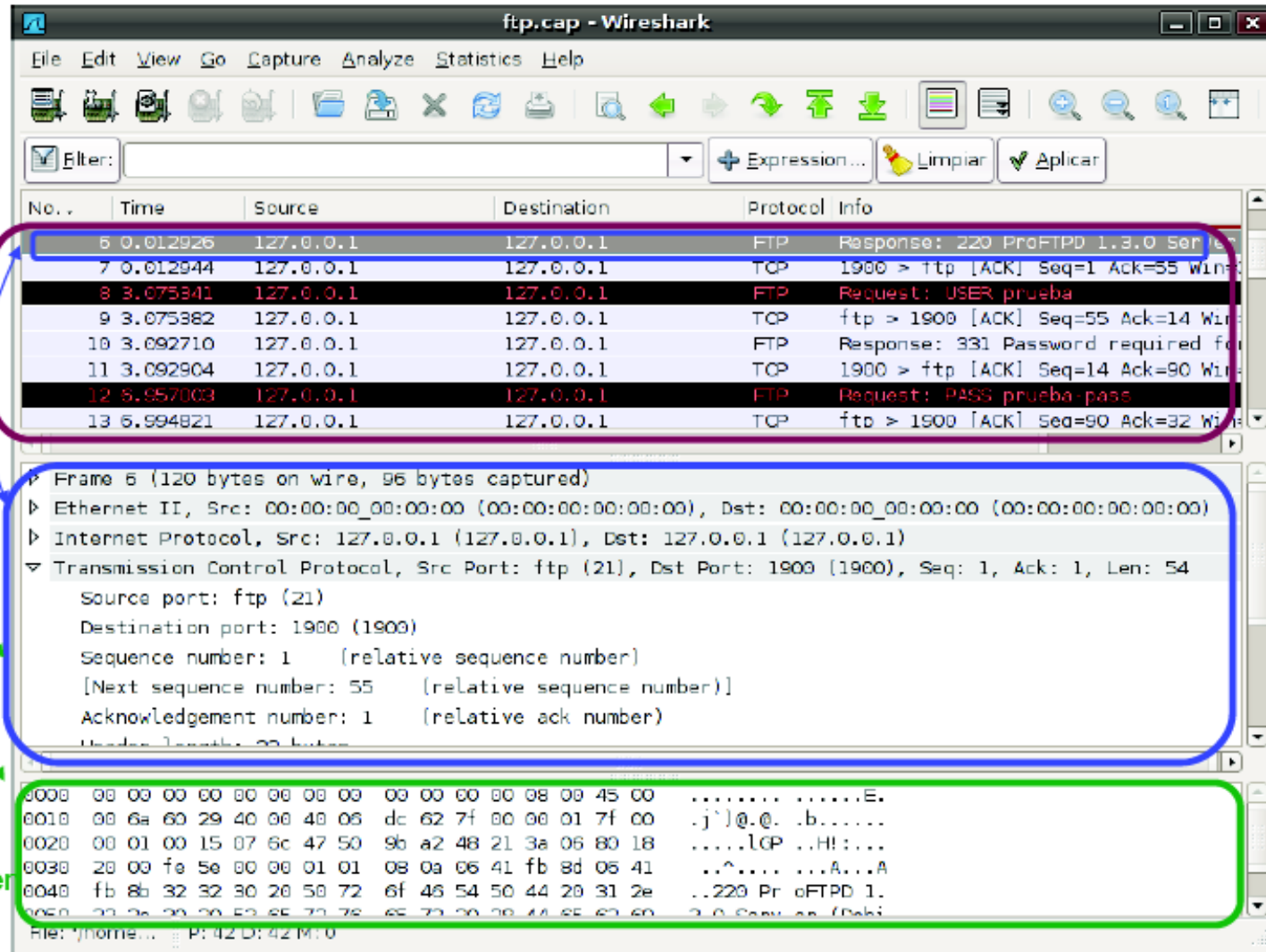


Wireshark

Resumen de los paquetes capturados

Detalle de las cabeceras del paquete seleccionado

Contenido del paquete seleccionado en hexadecimal y ASCII



Hijacking

Hijack vol dir “segrest”, i fa referència a tota tècnica il·legal que comporti apropiar-se o robar alguna cosa (normalment informació) per part d'un atacant.

Tipus:

- IP Hijacking
- Session Hijacking
- Browser Hijacking
- Modem Hijacking
- ...