

Common weaknesses in public wi-fi hotspots

pof

`pof@eslack.org`

Octubre 2004

Disclaimer

Esta presentación pretende introducir al oyente a los diferentes mecanismos de seguridad utilizados en hotspots públicos y sus posibles deficiencias. El autor no pretende promover el uso indebido de estas prácticas sino potenciar el uso de mecanismos de autenticación seguros y crear una mayor conciencia de seguridad entre los usuarios. El autor en ningún caso se hace responsable del uso que haga cada uno con la información contenida en esta presentación.

Índice

1. **Introducción**
2. **HotSpot Setup Tradicional**
 - **Access Point Controller**
 - **Standard Web Access Method**
 - **Ataque Rogue AP**
3. **Dynamic Address Translation**
 - **Deficiencias en Dynamic Address Translation**
4. **Multi-provider Roaming**
 - **Deficiencias en Multi-provider Roaming**
5. **Layer 2 user isolation**
 - **Deficiencias en Layer 2 user isolation**
6. **Gnivirdraw: Wardriving Inverso**

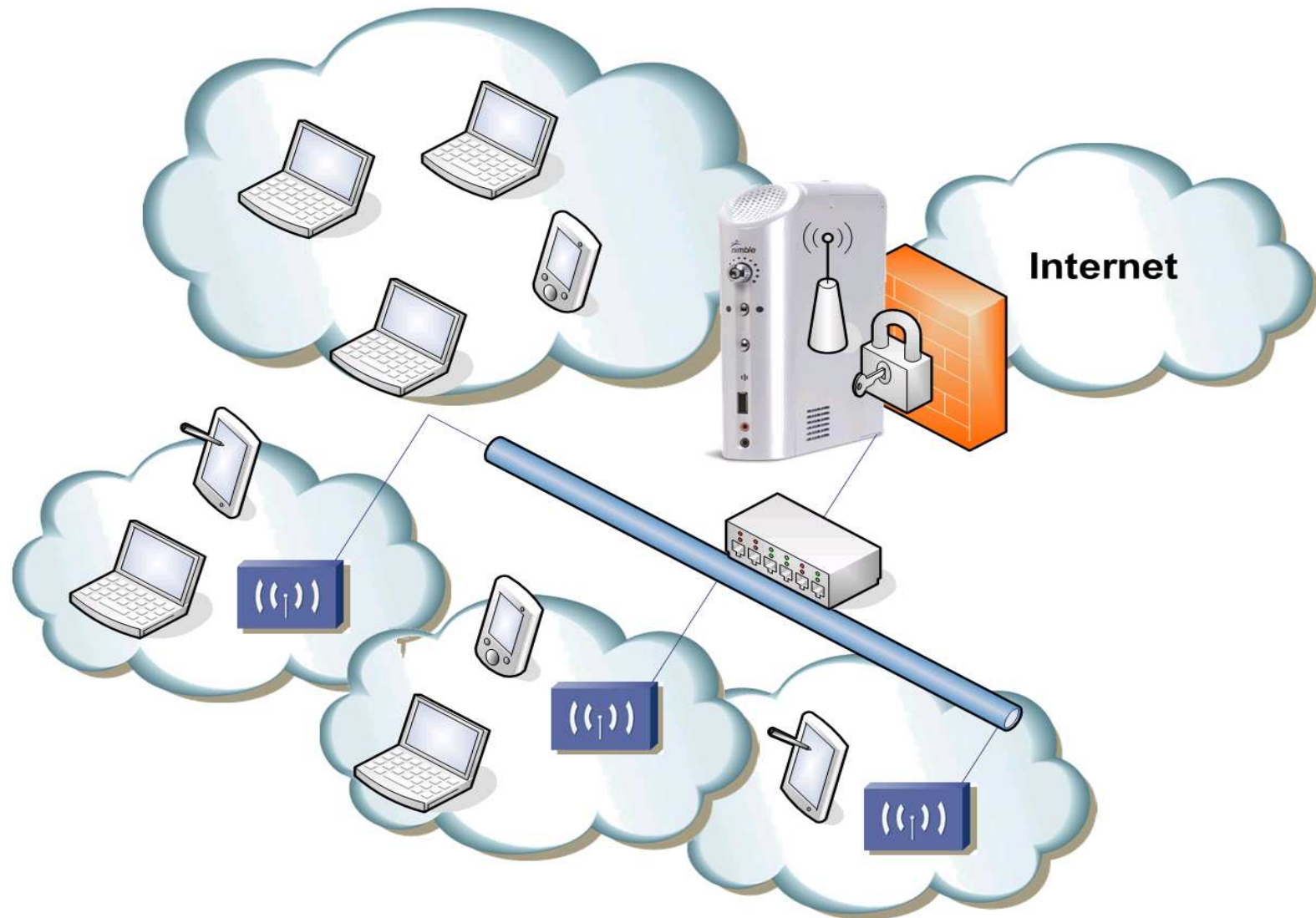
1. Introducción

- **Hotspot:** Lugar público o semi-público que dispone de conexión a Internet a través de tecnología *wireless*

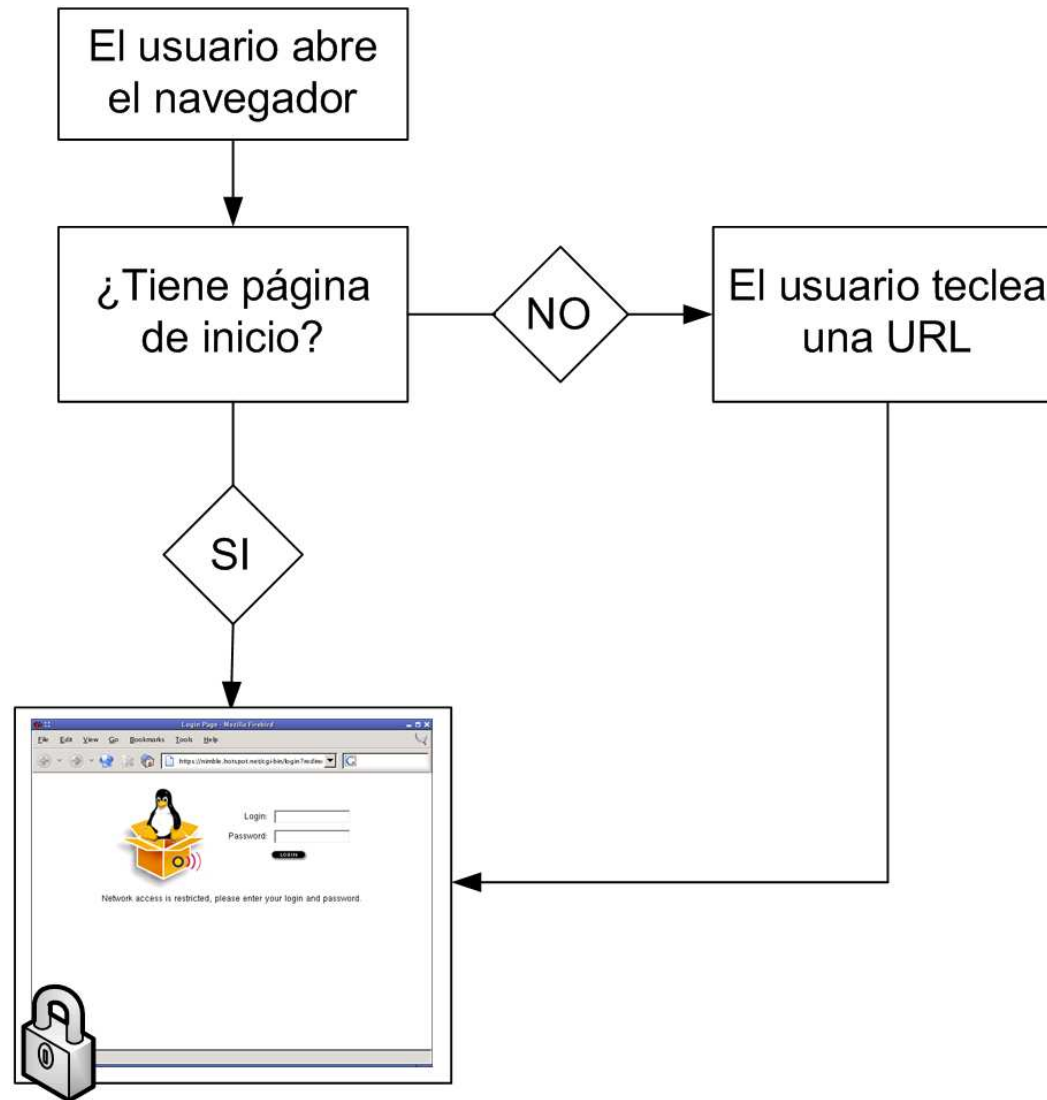


- Ejemplos: aeropuertos, cafeterías, hoteles, parques, salas de convenciones, recintos feriales, restaurantes, centros comerciales, bibliotecas...
- **WISP** (*Wireless Internet Service Provider*): Operadora que ofrece servicios de conexión a Internet inalámbricos en estos lugares

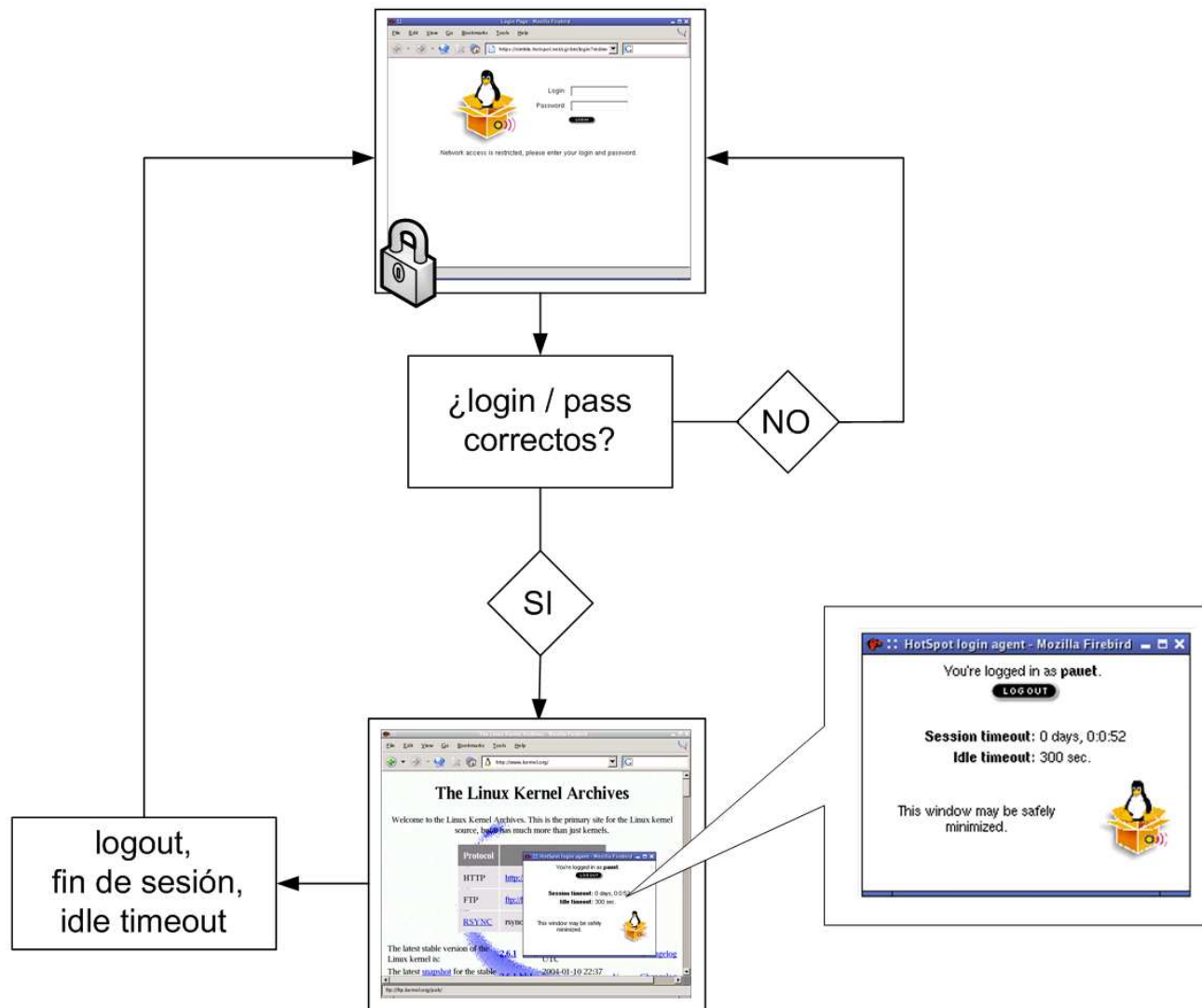
2.1 Access Point Controller



2.2 Standard Web Access Method (I)



2.2 Standard Web Access Method (II)



2.3 Ataque Rogue AP

- **Rogue AP:** Punto de acceso no autorizado, suplanta la identidad de un AP legítimo
- Vulnerabilidad en todos los hotspots públicos
- Más potencia que los APs normales
- Man-in-the-middle: airjack (<http://airjack.sf.net>)
- Nos hacemos pasar por el AP real (*AP clonning*) y mostramos el portal cautivo al usuario → capturamos sus credenciales (login / password)
- Implementación: hostap, httpd, dhcpd, iptables...
- Airstnarf (<http://airstnarf.shmoo.com>)
- Distinta repercusión según el tipo de account: Suscripción por minutos/tráfico, prepago con tiempo limitado...

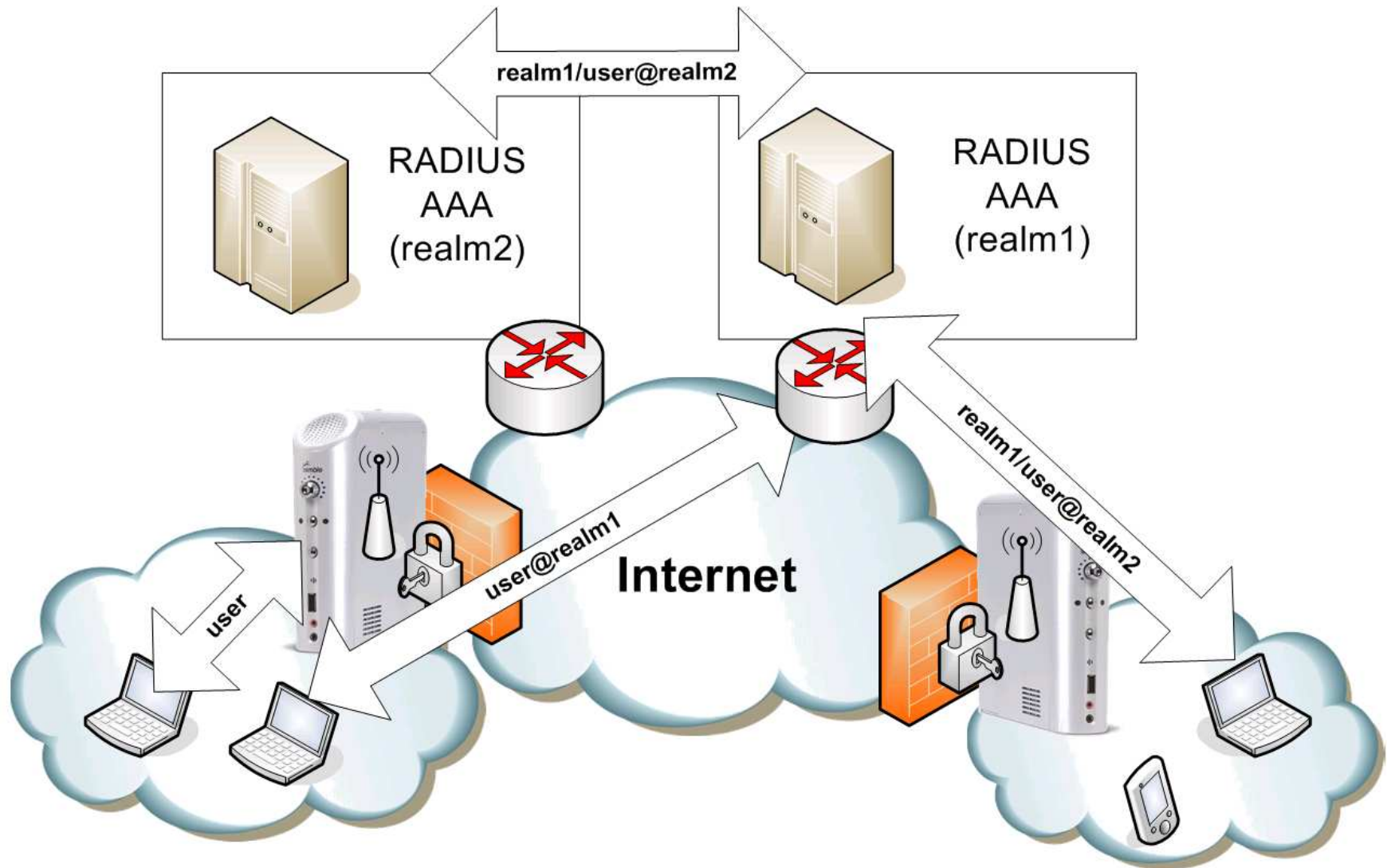
3. Dynamic Address Translation

- DAT: Captura cualquier *road-warrior* independientemente de su configuración de red (IP, DNS, PROXY...)
- Zero client configuration:
 - El gateway captura peticiones ARP request que no reciben reply
 - El gateway envia reply a estas peticiones, y hace *one-to-one NAT*
 - El gateway captura las peticiones a puertos de proxy y las reescribe
 - El gateway redirecciona al DNS local todas las peticiones

3.1 Deficiencias en Dynamic Address Translation

- Según como esté hecha la implementación podríamos:
 - Arpfun: Llenarle la tabla de conexiones (NAT-ARP) trazadas. arping
(<http://freshmeat.net/projects/arping>)
 - Forzar NATs “inútiles” contra IPs de los APs, del mismo gateway o del servidor RADIUS...
 - Denegarle el servicio al gateway

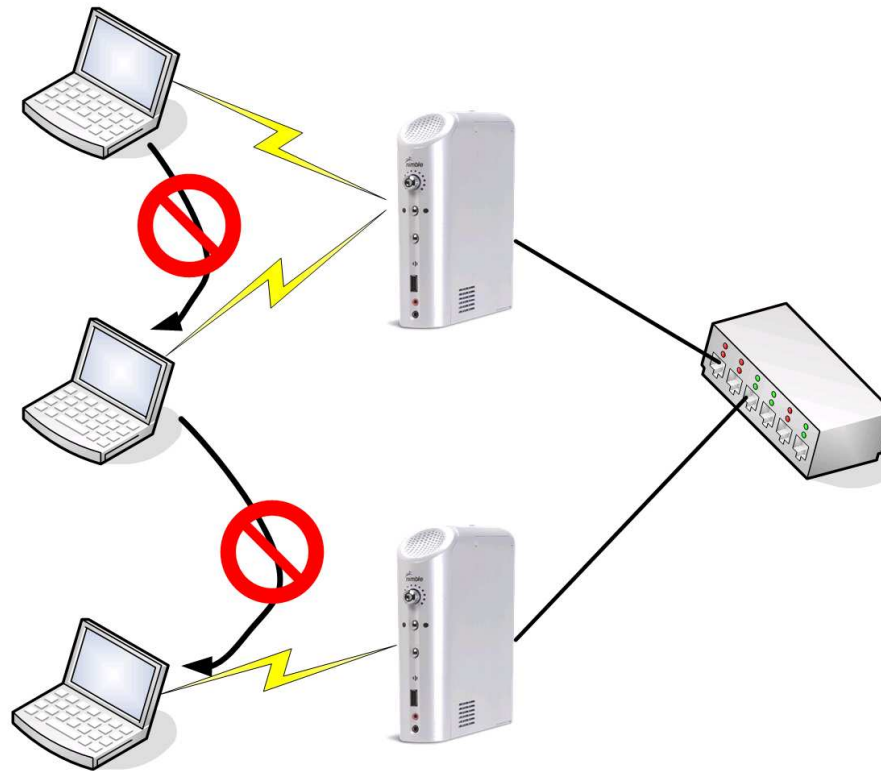
4. Multi-provider Roaming



4.1 Deficiencias en Multi-provider Roaming

- Si el gateway no llega al RADIUS se le da acceso gratuito al cliente para no dejarle sin servicio → Política usada por muchos WISPs
 - Podemos aprovechar deficiencias en DAT para provocar que el gateway no “vea” al RADIUS
 - Podemos suplantar la identidad del RADIUS
- Roamings mal configurados:
 - Ataques de fuerza bruta con **username@realm** probando distintos realms
 - Buscar realms con proxy a otros realms
 - Esperar RADIUS-TIMEOUT x RADIUS-RETRIES

5. Layer 2 user isolation



- Bloqueo de comunicación entre clientes:
 - Impide el acceso a unidades compartidas
 - Impide ataques

5.1 Deficiencias en Layer 2 user isolation

- Implementación de CISCO: PSPF (Public Secure Packet Forwarding)
 - Comportamiento distinto según versión de IOS del AP y del switch!!
- Si los APs no se pasan las tablas de usuarios asociados a través de LAN es posible acceder a un cliente conectado a otro AP
 - Soluciones: VLANs en el switch, port protected...
- Según como esté hecha la implementación podemos saltarnos la seguridad de capa 2 haciendo MAC-spoofing (usando MAC del AP / MAC de la víctima)

6. Gnivirdraw: Wardriving Inverso

- **Gnivirdraw:** Consiste en colocar un Rogue AP, esperando que alguien conecte.
- *wardrivers, wi-fi suckers*, clientes legítimos...
- Posibilidades:
 - Hackear al wardriver
 - Capturar contraseñas, correos, conversaciones de mensajería instantánea...
 - Suplantar identidad de AP en una oficina → espionaje corporativo, back-doors...

Preguntas?