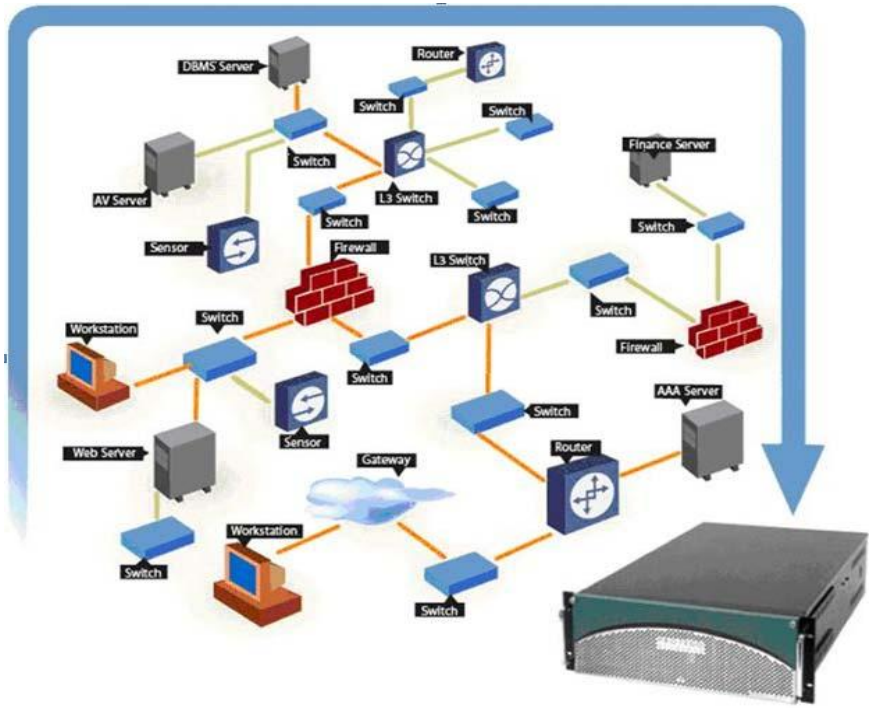
[MikrotikBrasil]
Routers & Wireless Systems



Seguridad en la capa 2

MUM – Argentina – Noviembre de 2009

Eng. Wardner Maia

Introducción

Nome: Wardner Maia

→ Ingeniero Electricista modalidad Eletrotécnica/Electrônica/Telecomunicaciones

→ Proveedor de Internet desde 1995, utilizando radio frecuencia para proveer aceso desde 2000

→Suministra entrenamientos en radio frecuencia desde 2002 y en Mikrotik desde 2006

→Posee las Certificaciones Mikrotik:
-- Trainer (2007) – Riga, Latvia
-- MTCWE, MTCRE (2008) – Krakow, Poland
-- MTCUME, MTCTE (2009) – Praga, Czech Republik

Introducción

MD Brasil – TI & Telecom

→ Operadora de Servicios de Comunicacción Multimedios y Servicios de Valor Añadido

→ Distribuidor mayorista de productos de Hardware e Software Mikrotik

→ Integradora y fabricante de equipos.

→ Socio de Mikrotik en entrenamientos

www.mdbrasil.com.br / www.mikrotikbrasil.com.br

Objetivos de la Presentación

Publico objetivo principal:

→ Pequeños y medianos proveedores de servicio de acceso a Internet y Telecomunicaciones que operan Redes Iñalambricas y Alambradas.

Objetivos:

→ Discutir las distintas topologias de redes más comunes empleadas por estos operadores con respecto a la seguridad y disponibilidad de la Red.

→ Entender conceptualmente los riesgos y amenazas existentes con demonstraciones practicas de los ataques.

→ Discutir la implementación de contramedidas posibles con Mikrotik RouterOS, proponiendo un conjunto de “mejores practicas” con respecto a las debilidades de la capa 2.

Modelo OSI
(Open Systems Interconnection)

CAPA 7: APLICACIÓN

CAPA 6: PRESENTACIÓN

CAPA 5: SESIÓN

CAPA 4: TRANSPORTE

CAPA 3: RED

CAPA 2: ENLACE

CAPA1: FÍSICA

Enderezamiento y enrutamiento

End. Físico

Conexiones físicas

¿Por qué el foco en la capa II ?

→ Seguridad es un proceso continuo y los administradores deben tener en cuenta muchos aspectos desde la capa fisica hasta la capa de aplicaciones. Del punto de vista del acceso a la Red no es suficiente garantizar que la red no sea invadida para que los clientes tengan seguridad en sus datos.

→ Teniendo como referencia el modelo OSI, se puede decir que la seguridad de las capas superiores siempre depende de las capas inferiores. Una red segura necesita garantizar, además de otras cosas, las informaciones coherentes entra la capa 2 (enlace) e la capa 3 (red)

→Además de los problemas de seguridad de acceso existen inúmeros ofensores a la disponibilidad de la red por ataques de negación de servicio que explotan vulnerabilidades inherentes a la capa II

→Medidas de controle hechas en la capa II ayudan a mejorar el desarrollo de la red por filtrar tráfego inútil/indeseado.

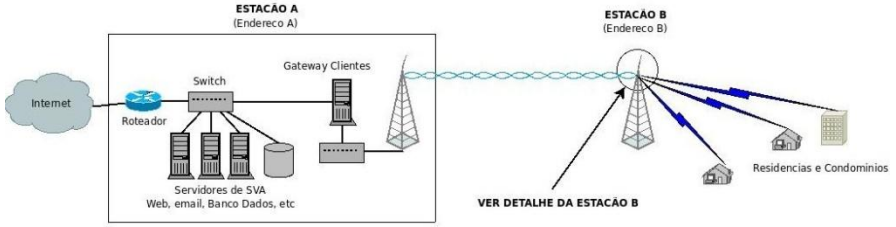
AGENDA

Topologias usuales de redes IP, Bridging, Switching y Firewalls de la Capa II

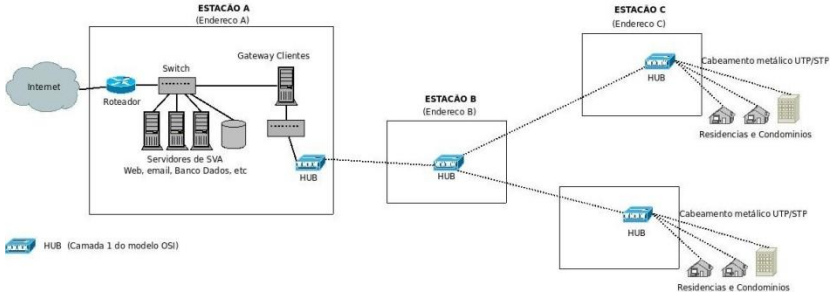
Vulnerabilidades y ataques típicos a la capa II:

- → Inundación de la tabla de Hosts / Tabela CAM y explotación de protocolos de descubierta del vecindario
- → Explotando VLAN´s y el Protocolo Spanning Tree
- → "Inanición" en una red con DHCP
- → Ataques de envenenamiento de ARP – Hombre del medio
- → Atacando usuários y proveedores de Hotspot y PPPoE
- → Ataques de desautenticación de usuarios Wireless

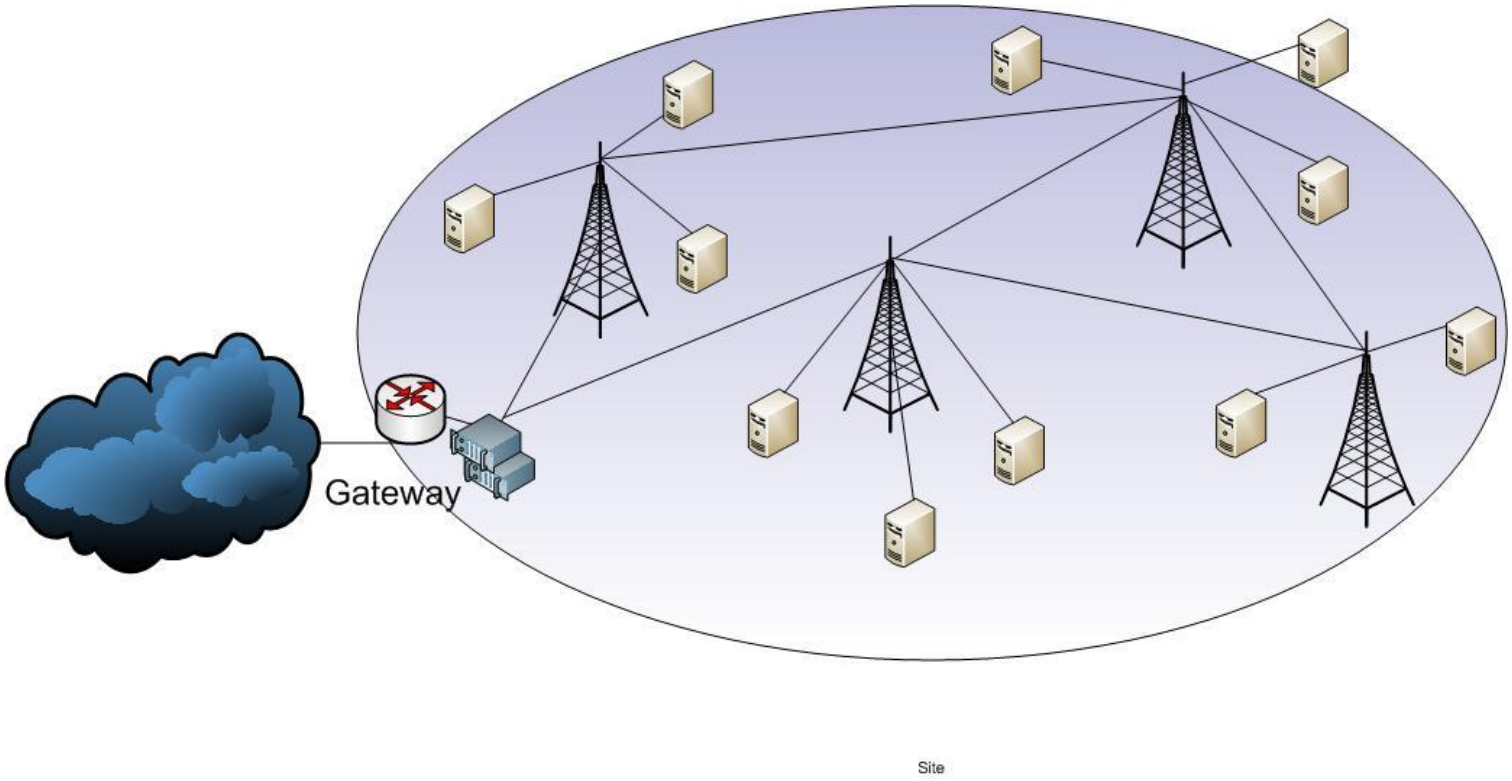
Contramedidas, mejores prácticas y demostraciones en tiempo real



Topologias usuales de redes IP, Bridging, Switching y Firewalls de capa II (Filtros de Bridge)



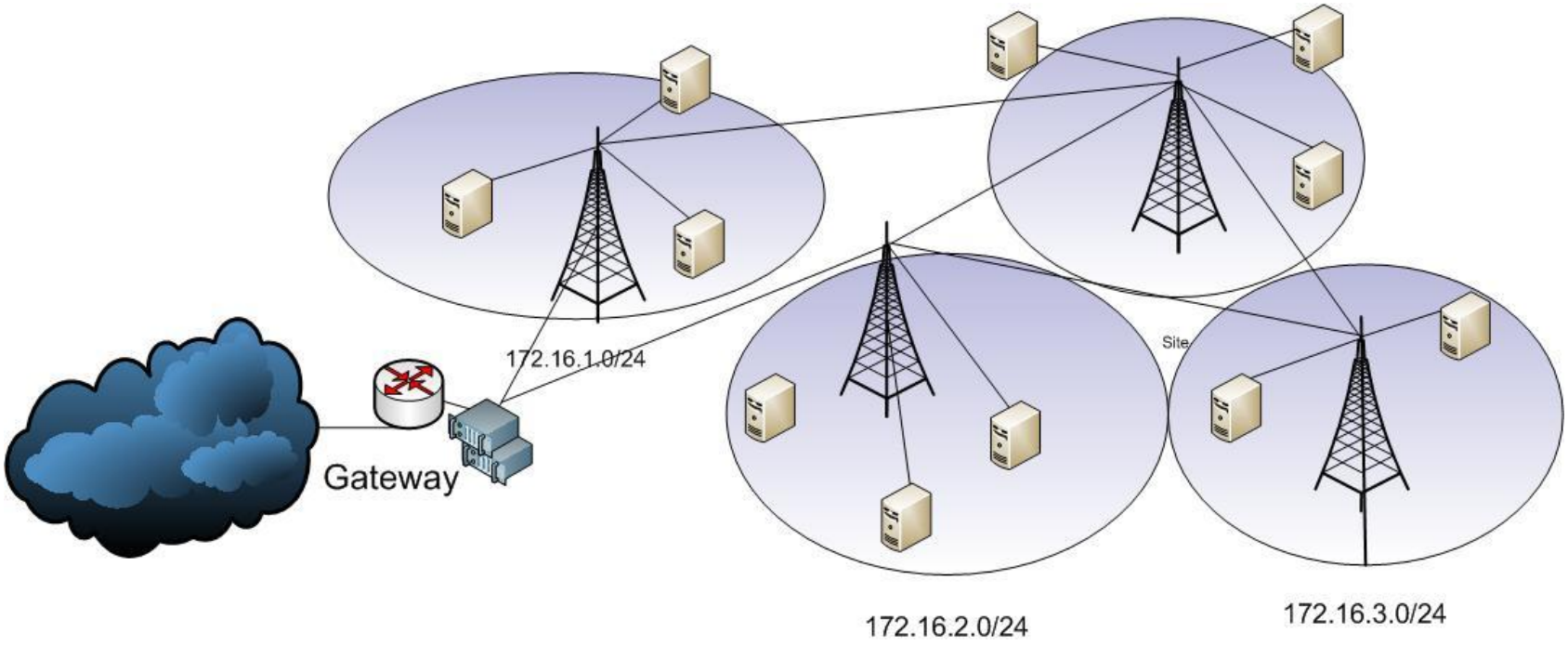
Típica Red en Capa 2



Gateway de los clientes es el Gateway de borde

Solamente un domínio de Broadcast

Típica Red Enrutada

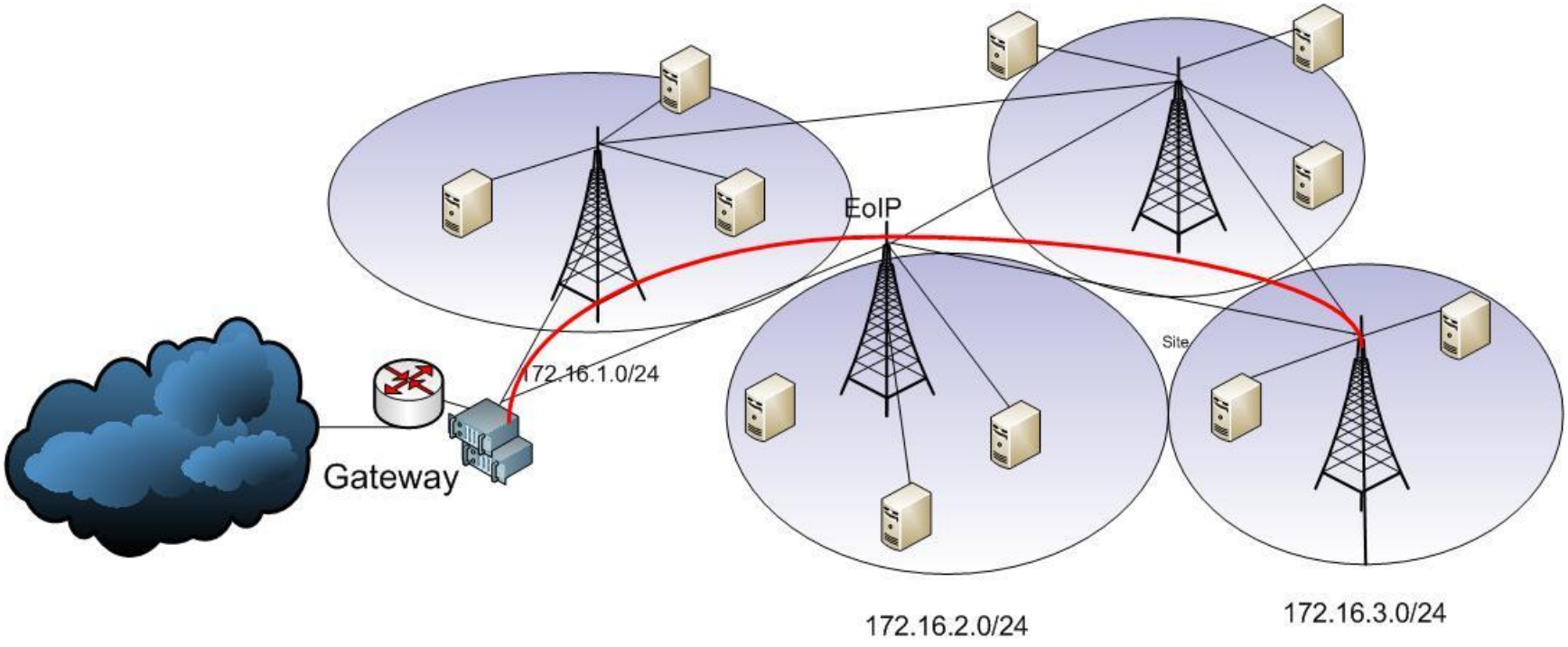


Gateway de los clientes es distribuído y cerca de los clientes

Domínios de broadcast segregados

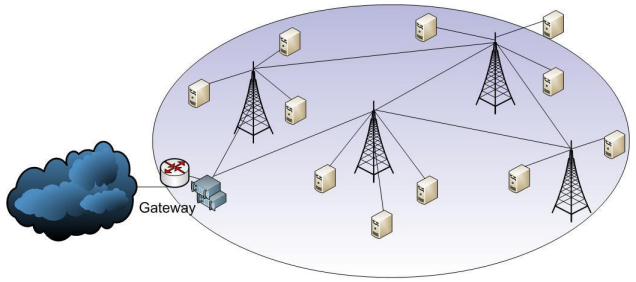
→ Incluso en las redes roteadas pueden haber segmentos en capa 2

Red Enrutada con Concentrador PPPoE
"Bridge over Routing"



Uso de protocolo de enrutamiento dinámico, pero con Túneles transparentes hasta el concentrador.

Redes en capa 2



Redes en ATM, Frame Relay, MPLS (capa “2.5”), etc

Vamos a abordar

- Redes IP en Bridge:
  - → Redes con IP fijo
  - → DHCP
  - → Hotspot
  - → Mezcladas con Bridge sobre enrutamiento
- Redes completamente en capa 2 con PPPoE

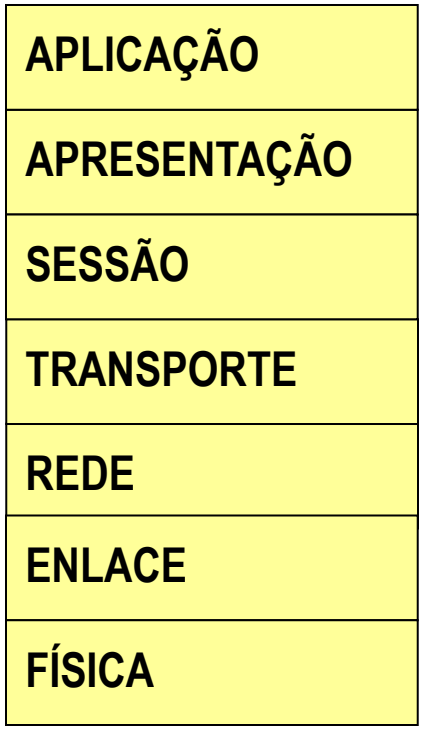
Bridging x Switching

Bridging x Switching

→ Bridging e Switching ocorrem na camada II, porém em níveis distintos.

→O processo de Switching é normalmente mais rápido (“wire speed”)

→ A partir da v4.0 o Mikrotik RouterOS suporta switching para vários equipamentos,



Bridge

Switch

Switching

→ El switch mantiene una tabla con los MAC's conectados a ella, relacionándolos con la puerta donde fueron "aprendidos".

→ Cuando un MAC no existe en la tabla, él es buscado en todas las puertas, y la switch se porta como um HUB.

→ El espacio (Host table o CAM table) es limitado y cuando totalmente lleno hace con que la switch se porte como un HUB !

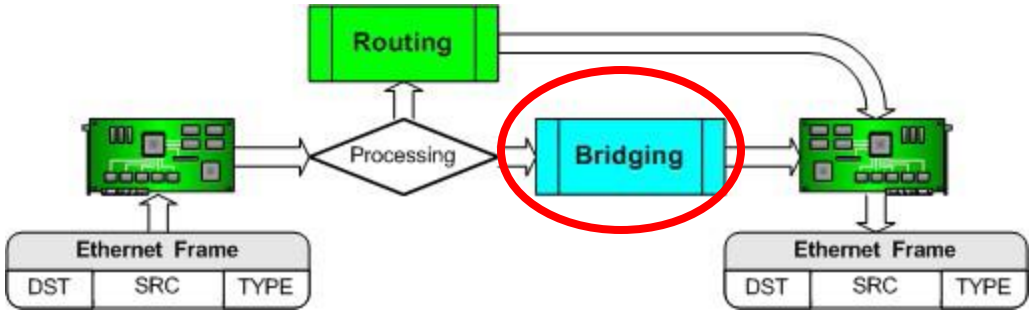
Feature	Atheros8316	Atheros7240	ICPlus175D	Other
Port Switching	yes	yes	yes	yes
Port Mirroring	yes	yes	yes	no
Host table	2k entries	2k entries	no	no
Vlan table	4096 entries	16 entries	no	no
Rule table	32 rules	no	no	no
	(RB450G)	(RB750)	(RB450)	

Bridging

→ Como en las Switches, la Bridge mantiene una tabla con los MAC's conectados a ella, relacionándolos con la puerta donde fueron "aprendidos". Esos MAC's son repasados para otras bridges conectadas en el mismo segmento de red.

→ El número de entradas no tiene propriamente un límite pero depende del hardware pues consume recursos de memória que son finitos.

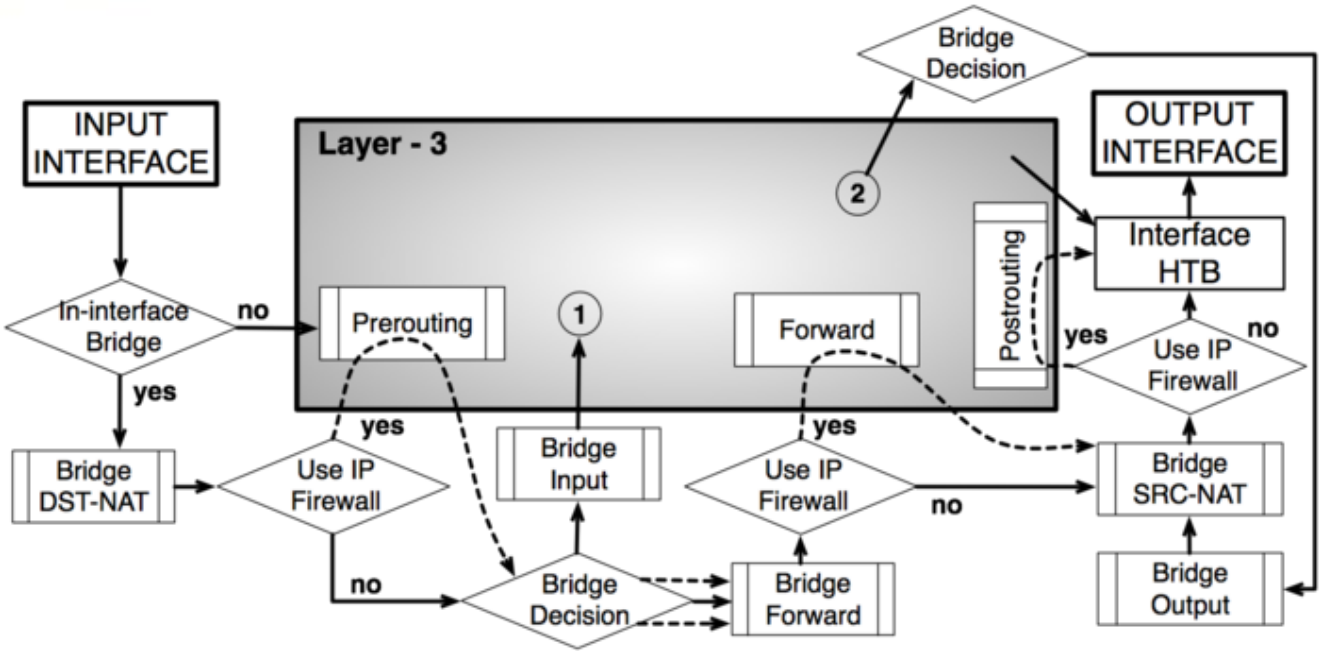
→ En las bridges es posible inspecionar los frames ethernet en capa 2 y se les puede aplicar filtros, marcaciones, etc

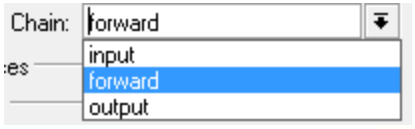


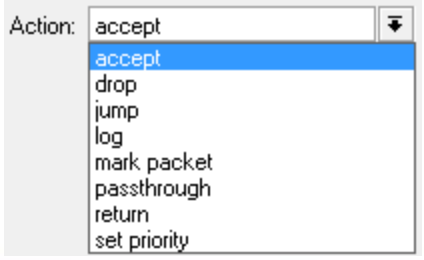
Bridge | Ports | Filters | NAT | Hosts

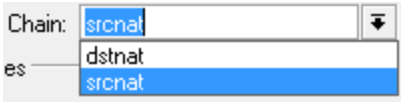
	MAC Address	On I...	Age	Bridge
	00:0C:42:5A:89:A1	ether2	00:00:05	bridge1
L	00:0C:42:5A:89:B0	ether2	00:00:11	bridge1
	00:0C:42:5A:89:9D	ether3	00:00:07	bridge1
L	00:0C:42:5A:89:B1	ether3	00:00:11	bridge1
	00:0C:42:36:C8:1C	ether5	00:00:10	bridge1
	00:0C:42:42:42:42	ether5	00:00:11	bridge1
L	00:0C:42:5A:89:B3	ether5	00:00:11	bridge1

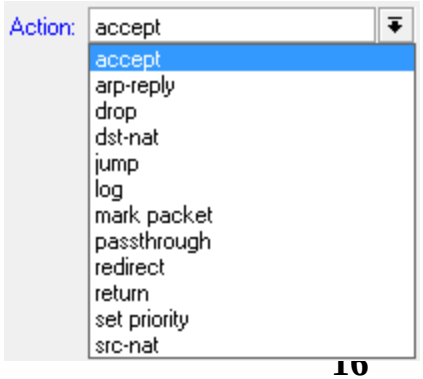
Filtros de capa 2









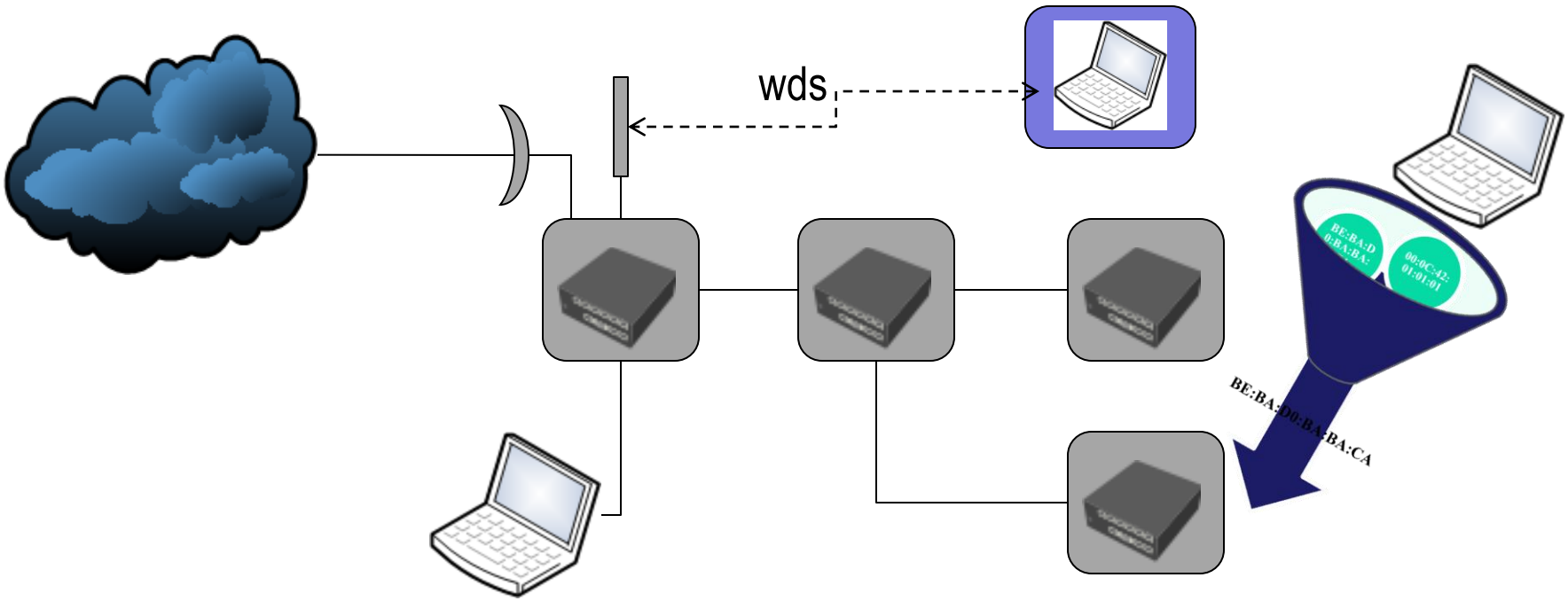


Atacando la capa 2

Inundación de la Tabla de Hosts (MAC Flooding)

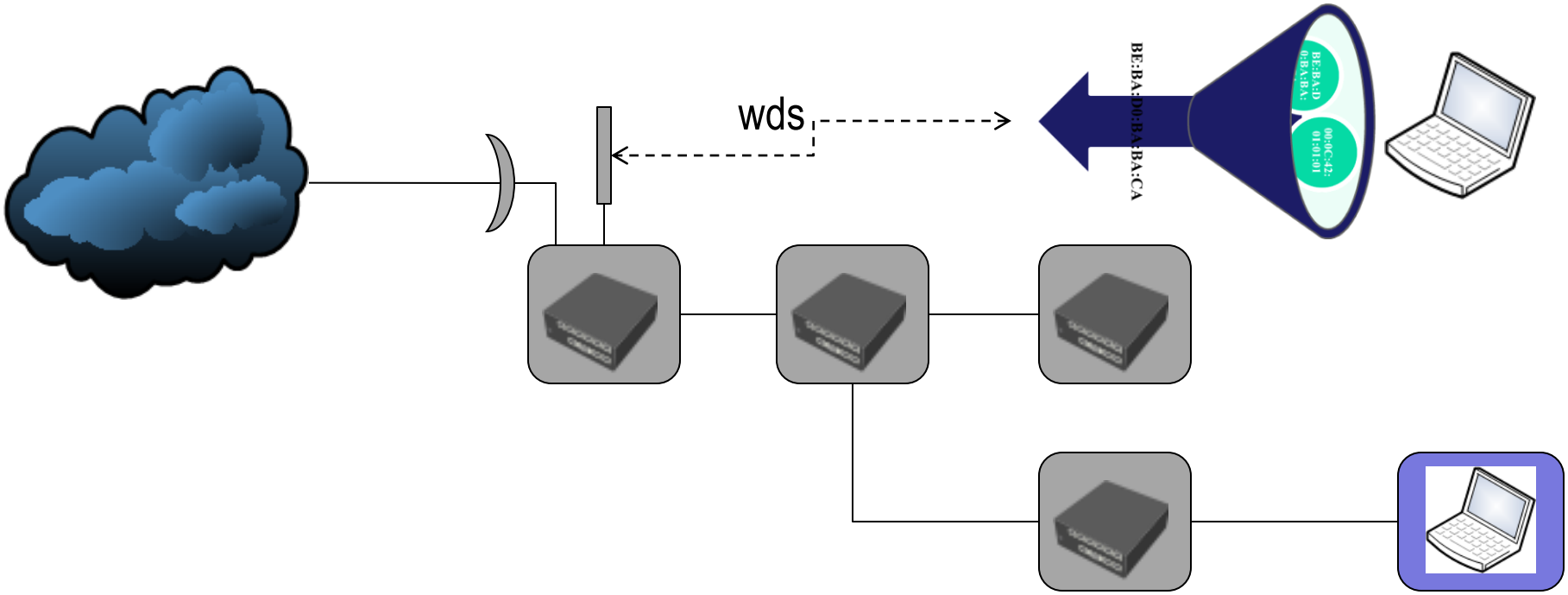
Ataques a switches y bridges
Inundación de la tabla de hosts

Existen herramientas de instalación extremadamente sencillas, desarrolladas para programas para “auditoria de seguridad de redes” que ejecutan el flood de MAC’s en redes en bridge.

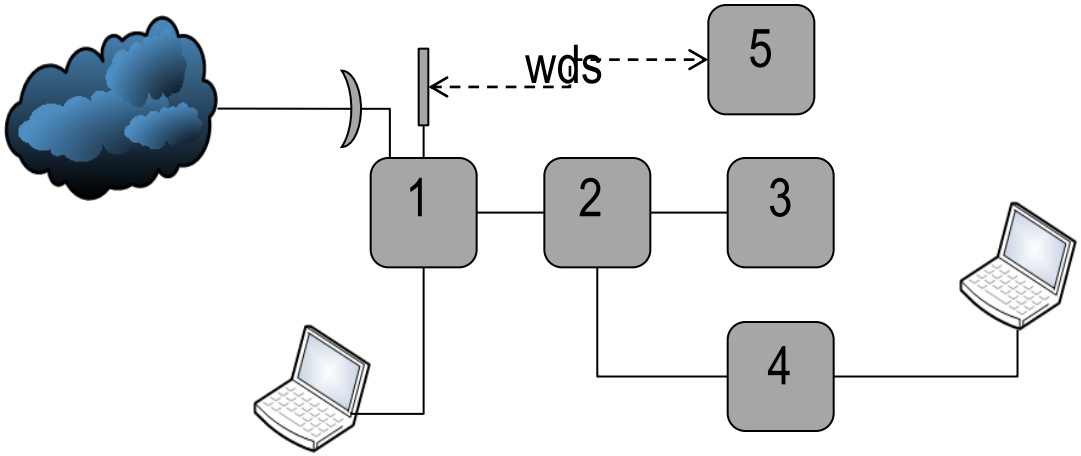


Ataques a switches y bridges
Inundación de la tabla de hosts

El flood puede ser hecho en qualquer puerta de las bridges, incluso en las intefaces iñalambricas donde corra una WDS



Inundación de la Tabla de Hosts (Mac Flooding) DEMO



- Disparando el ataque a partir de 4
- Averiguando el efecto en todos los otros
- Protegiendo solamente 4
- Protegiendo 4 y los otros

Ataques a switches y bridges
Contramedidas

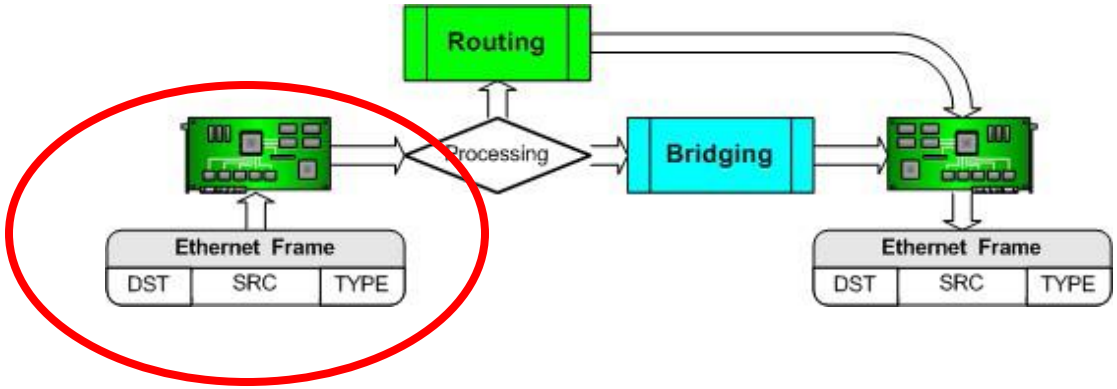
Switches:

→El ataque no causa DoS, pero una vez llena la CAM table, la Switch se porta como HUB

→ Cuando utilizadas como switches, no hay qué hacer para prevenir esos ataques sino dar acceso en capa 2 a los possibles atacantes.

→Una feature como “port security” existente en las switches Cisco sería deseable para el Mikrotik RouterOS.

Ataques a switches y bridges
Contramedidas



Bridge | Ports | Filters | NAT | Hosts

	MAC Address	On I...	Age	Bridge
	00:0C:42:5A:89:A1	ether2	00:00:05	bridge1
L	00:0C:42:5A:89:B0	ether2	00:00:11	bridge1
	00:0C:42:5A:89:9D	ether3	00:00:07	bridge1
L	00:0C:42:5A:89:B1	ether3	00:00:11	bridge1
	00:0C:42:36:C8:1C	ether5	00:00:10	bridge1
	00:0C:42:42:42:42	ether5	00:00:11	bridge1
L	00:0C:42:5A:89:B3	ether5	00:00:11	bridge1

→ Antes de pasar por los filtros, los MAC´s deben ser “aprendidos” por la Bridge

→ Debido a eso, los filtros son inútiles para la protección de esa Bridge en específico.

→ El ataque tendrá éxito y causará DoS en el equipo.

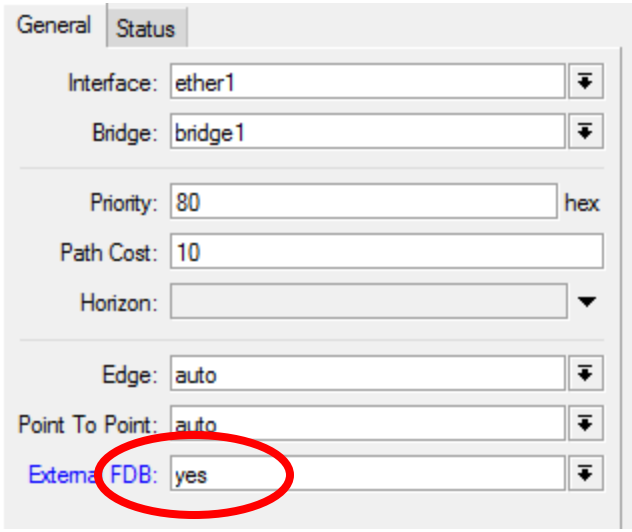
Ataques a switches y bridges
Contramedidas

Bridges:

→ Configurando la(s) puerta(s) para External FDB (Forwarding DataBase) la tabla de hosts no será cargada (para la(s) puerta(s) configuradas.

→ Esa medida evita el DoS en el equipo en cuestión pero no en las otras bridges a él conectados. El flood será hecho para todas las puertas.

→ Felizmente una vez aceptos los MAC's atacantes, es possible filtrar la propagación de ellos.

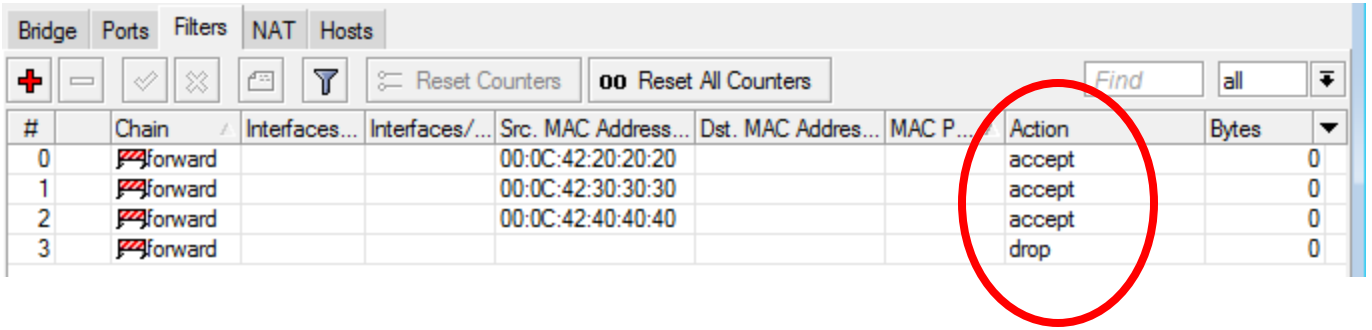


Ataques a switches y bridges
Contramedidas

¿Pero cuáles filtros ejecutar?

→El ideal sería solamente aceptar los MAC's realmente conocidos y que hacen parte de la red.

→ Como eso ni siempre es possible, se puede escribir un script para activarlos "on the fly" cuando y si la tabla de hosts aumenta de forma anómala..



Atacando la capa 2

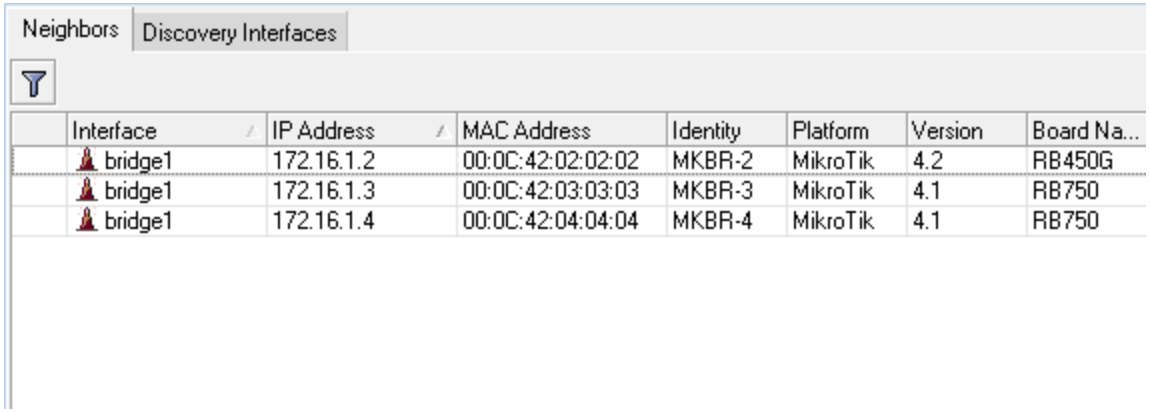
Explotando Protocolos de
“Descubierta de Vecindario”

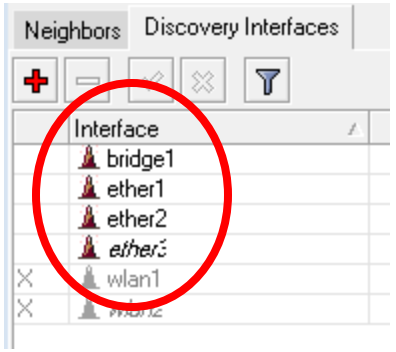
Explotando protocolos de "Descubierta de vecindario"

→ Protocolos de descubierta de vecindario ayudan en las tareas administrativas y de control de red.

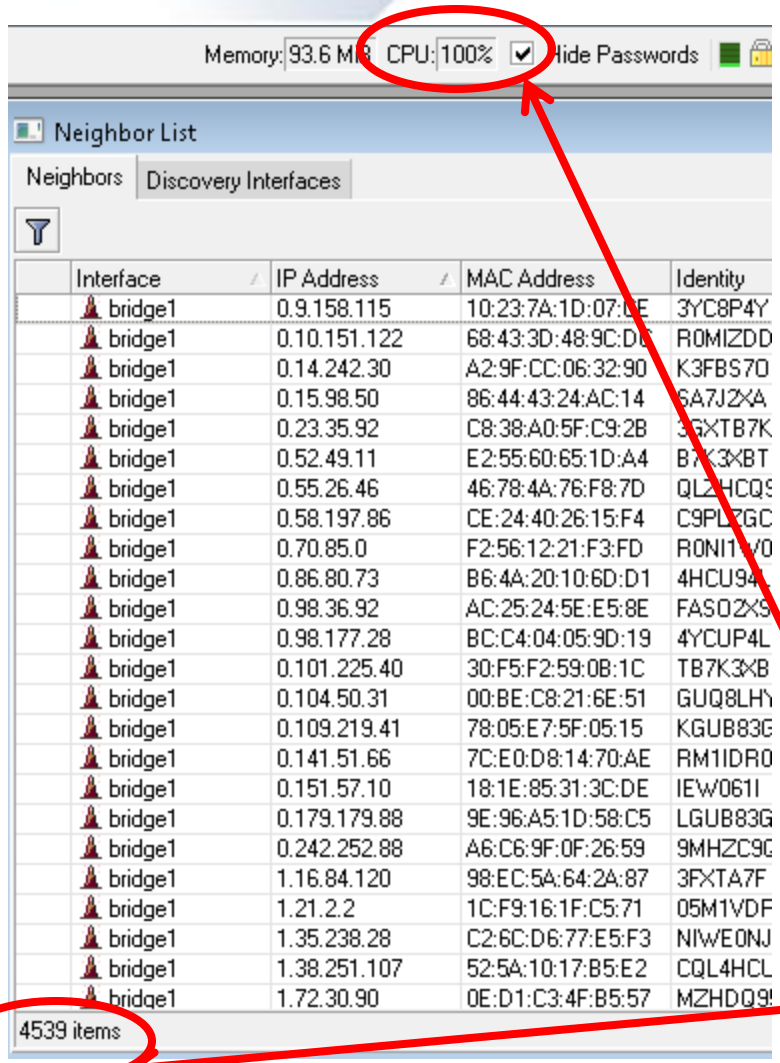
→ Mikrotik RouterOS utiliza MNDP - Mikrotik Neighbor Discovery Protocol. (Cisco utiliza protocolo semejante - CDP).

→ MNDP trabaja com protocolo UDP, puerta 5678 que es divulgada por broadcast a cada 60 segundos en cada interface.





Explotando protocolos de "Descubierta de vecindario"



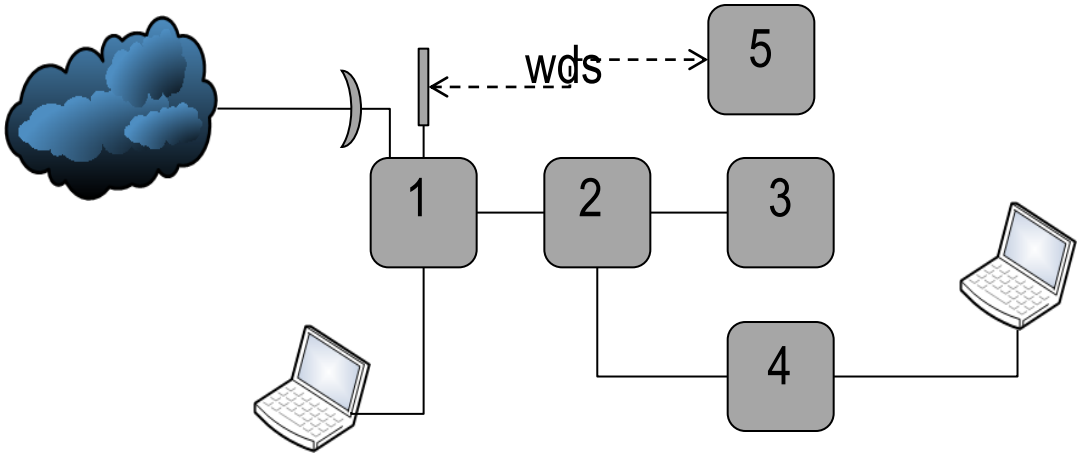
→ Herramientas de ataque desarolladas para Cisco y disponibles en la Internet atacan tanto Mikrotik RouterOS como Cisco CDP

→ Esas herramientas pueden ser utilizadas solamente para obtener informaciones de la red y equipos o causa DoS.

→ El ataque puede ser disparado de cualquier puerta de la bridge contaminando todos los equipos de la rede.

15 segundos de ataque en una RB433AH

Explotando de Protocolos de Descubierta de Vecindario DEMO



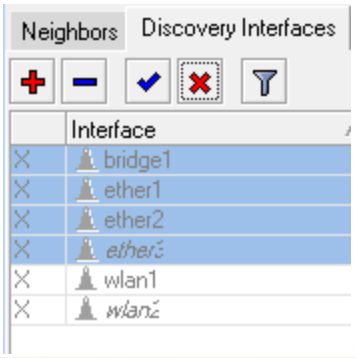
- Disparando el ataque a partir del equipo 4
- Averiguando el efecto en 1
- Tomando las medidas preventivas en 1
- Haciendo los filtros en 4

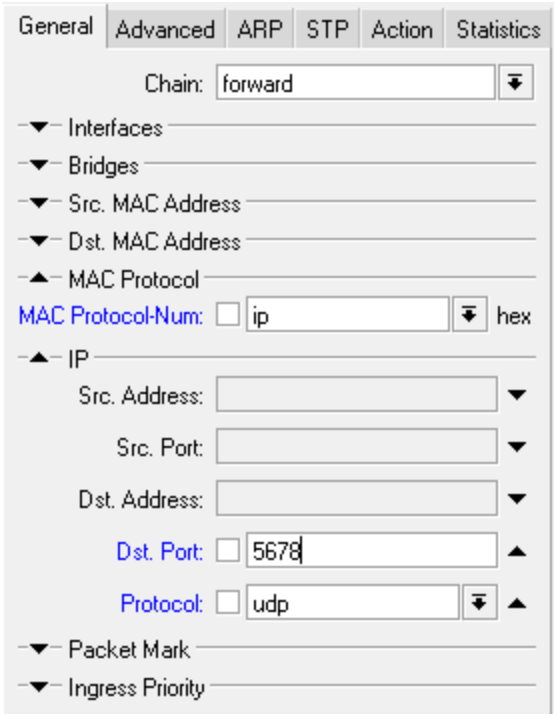
Contramedidas para ataques basados en protocolos de “Descubierta de vecindario”

→ Desabilitar el MNDP en todas las interfaces

→Aunque el MNDP esté bloqueado, el tráfego generado por tentativas de ese tipo de ataque existirá. Bloquear la puerta UDP 5678 en todos los filtros de bridge puede ayudar a evitar ese tráfego

→ Acordarse que toda Interfaz ethernet-like (EoIP, IPIP, PPtP estática, etc) tiene por default el MNDP habilitado.





Atacando la capa 2

Inanición de Redes con DHCP
(DHCP Starvation)

Fundamentos do DHCP

El protocolo DHCP es ejecutado en 4 fases:

1) El Cliente busca en su barramiento físico un servidor de DHCP

DHCP Discovery

Src-mac=<mac_do_cliente>, dst-mac=<broadcast>, protocolo=udp, src-ip=0.0.0.0:68, dst-ip=255.255.255.255:67

2) El Servidor de DHCP oferece (y reserva durante un rato) un IP al solicitante

DHCP Offer

Src-mac=<mac_do_DHCP-server>, dst-mac=<broadcast>, protocolo=udp, src-ip=<ip_do_DHCP-server>:68, dst-ip=255.255.255.255:67

Fundamentos de DHCP

3) El cliente requisita (acepta) el IP ofrecido

DHCP Request

Src-mac=<mac_do_cliente>, dst-mac=<broadcast>, protocolo=udp, src-ip=0.0.0.0:68, dst-ip=255.255.255.255:67

4) El Servidor confirma la atribución del IP

DHCP Acknowledgment

Src-mac=<mac_do_DHCP-server>, dst-mac=<broadcast>, protocolo=udp, src-ip=<ip_do_DHCP-server>:68, dst-ip=255.255.255.255:67

Ataques contra el DHCP

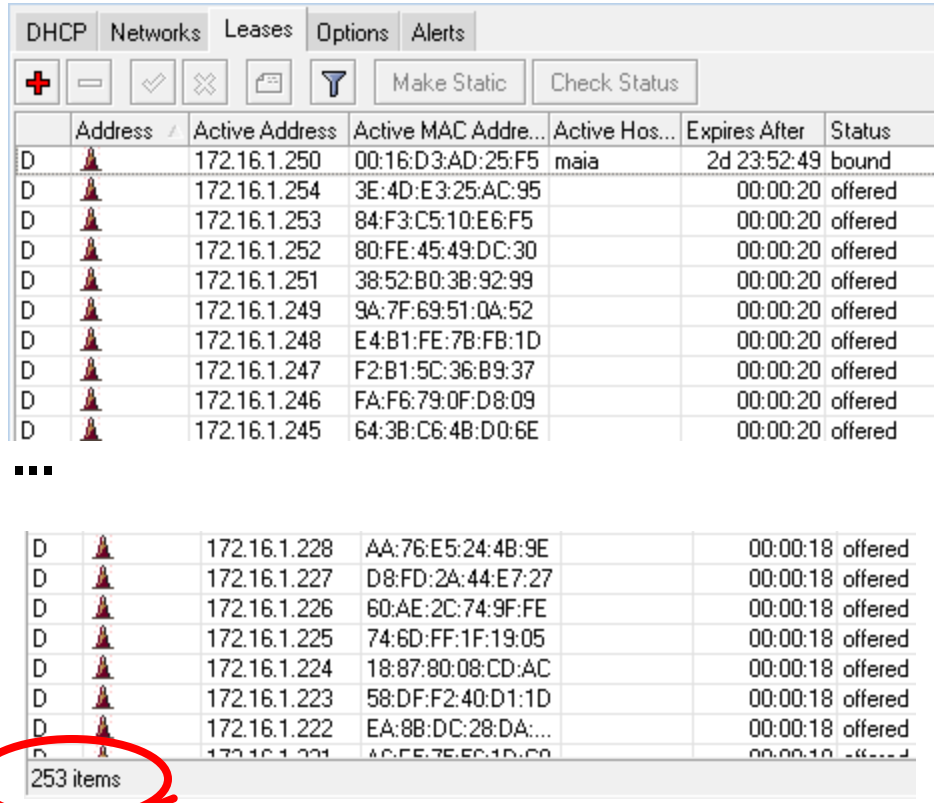
Existen dos tipos de ataques de “Starvation” del DHCP conocidos:

1) El atacante genera inúmeros pedidos de DHCP y cumple todas las fases del proceso hasta obtener los IP´s

2) El atacante genera inúmeros pedidos de DHCP pero no los confirma

Tanto uno como otro ataque utilizan MAC´s generados aleatoriamente y causan la negación del servicio por el agotamiento de los IP´s disponibles. El ataque de tipo 1 es más lento y más persistente y del tipo 2 es más rápido y tiene que ser hecho continuamente, pues el tiempo de “offer” es pequeño.

Inanición de redes con DHCP (DHCP starvation)



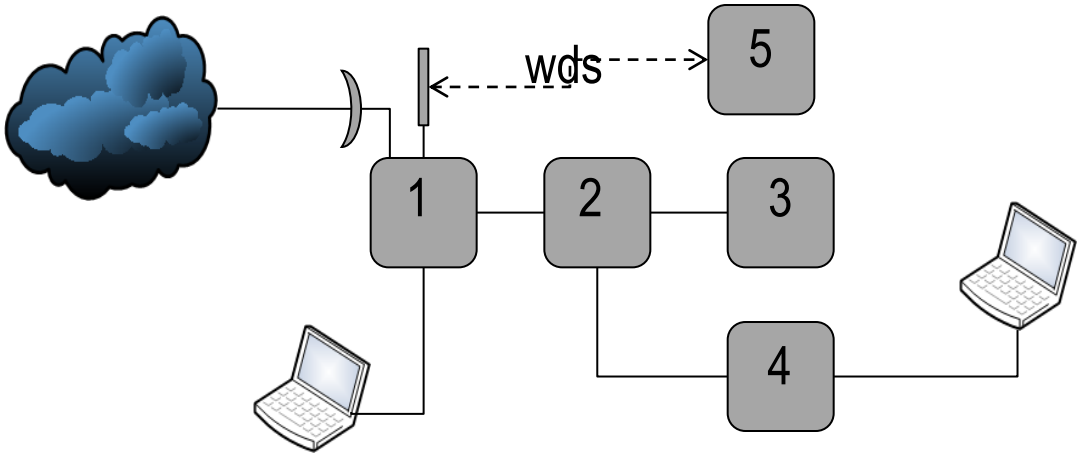
→ El ataque se basa en enviar paquetes de dhcp discovery para todos los hosts de la red, haciendo con que el DHCP los ofrezca.

→ En ese momento se puede poner en la red um DHCP falso atribuyendo otros IP´s, gateways, DNS´s, etc.

→ Alternativamente se puede aceptar los IP´s manteniendo el DHCP sin más IP´s para entrega

Menos de 5 segundos de ataque agota una classe C !

Inanición de Redes con DHCP"
(DHCP Starvation)
DEMO



- Disparando los ataques de tipo 1 e 2 a partir del host 4
- Observando el efecto en 1 (Servidor de DHCP)

DHCP Starvation
Contramedidas

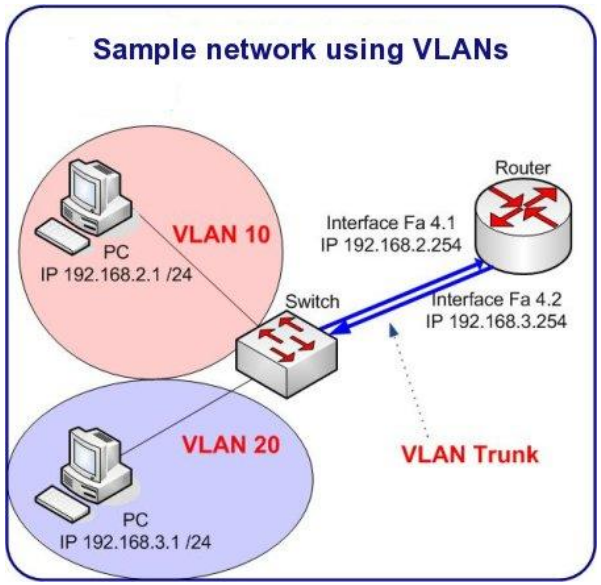
→Filtros permitiendo pasar solamente los MAC´s conocidos

→ Leases estáticos en el DHCP

→ Considerar la posibilidade de utilizar Radius o User Manager

Atacando la capa 2

Explotando Vlan´s



VLAN´s

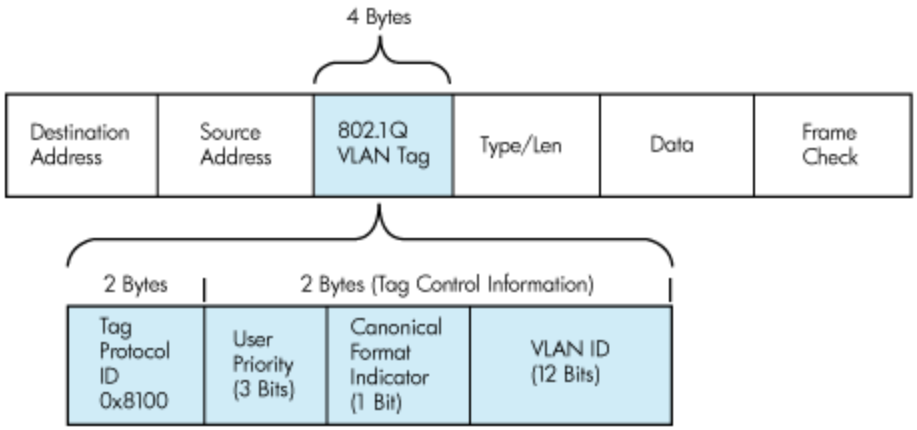
Una Vlan es un grupo de hosts que se comunican entre si como si estuvieran el el mismo domínio de broadcast independiente de la ubicación física. Pueden ser utilizadas para muchas funciones en una red, como:

→ Creación de várias redes de capa 3 sobre un dispositivo de capa 2

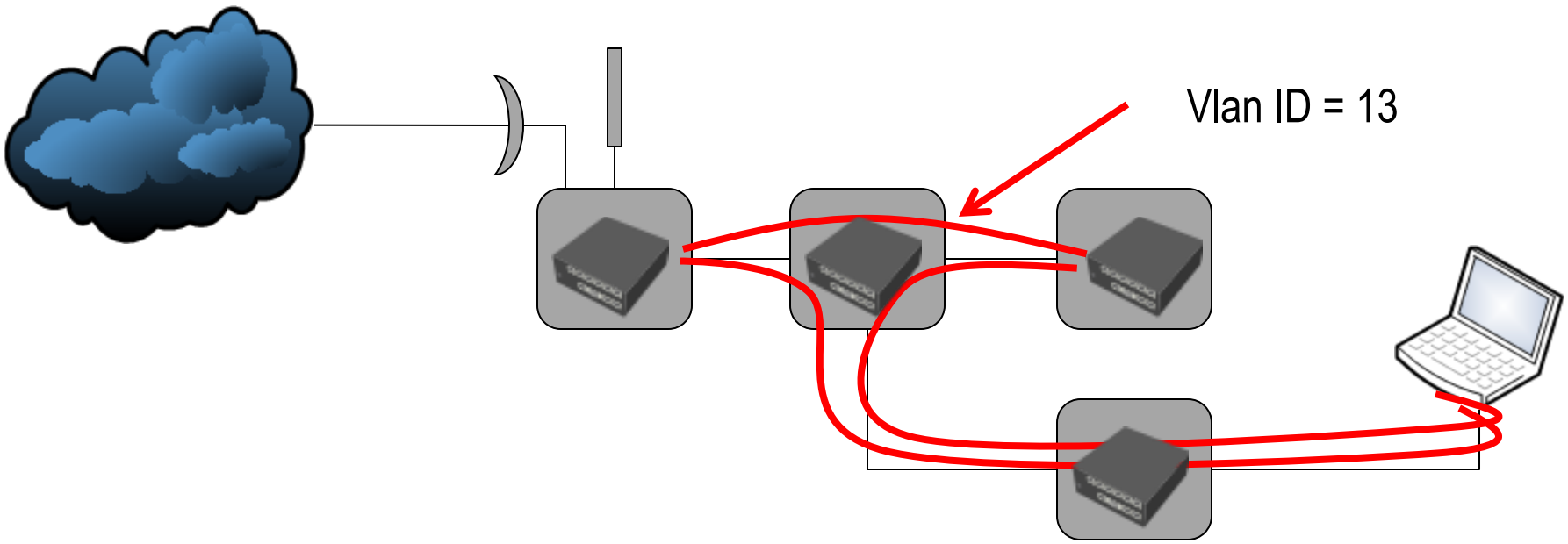
→ Segmentación de tráfego y limitación de domínios de Broadcasts

→ Possibilidad de aplicar reglas de QoS individuales

→ ¿Seguridad?



Explotando las VLAN´s

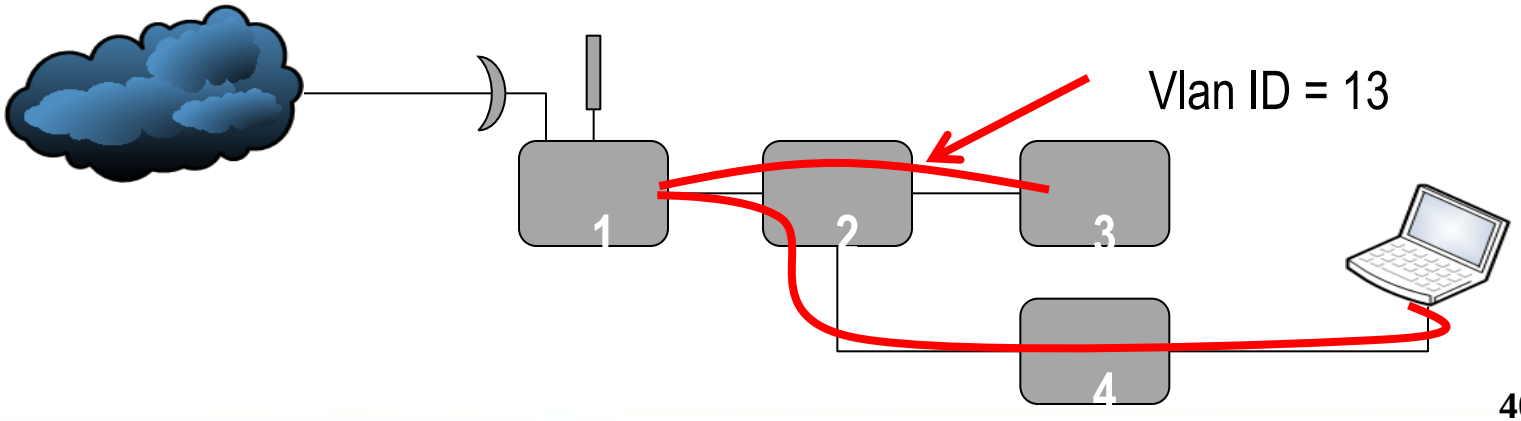


→ La primera fragilidad es obvia pues no habiendo cualquier cuidado para filtrar, cualquier host que tenga la misma Vlan Tag ID puede hacer parte de la Vlan

Explotando las VLAN´s

→ Ataque de “proxy” de Vlan´s

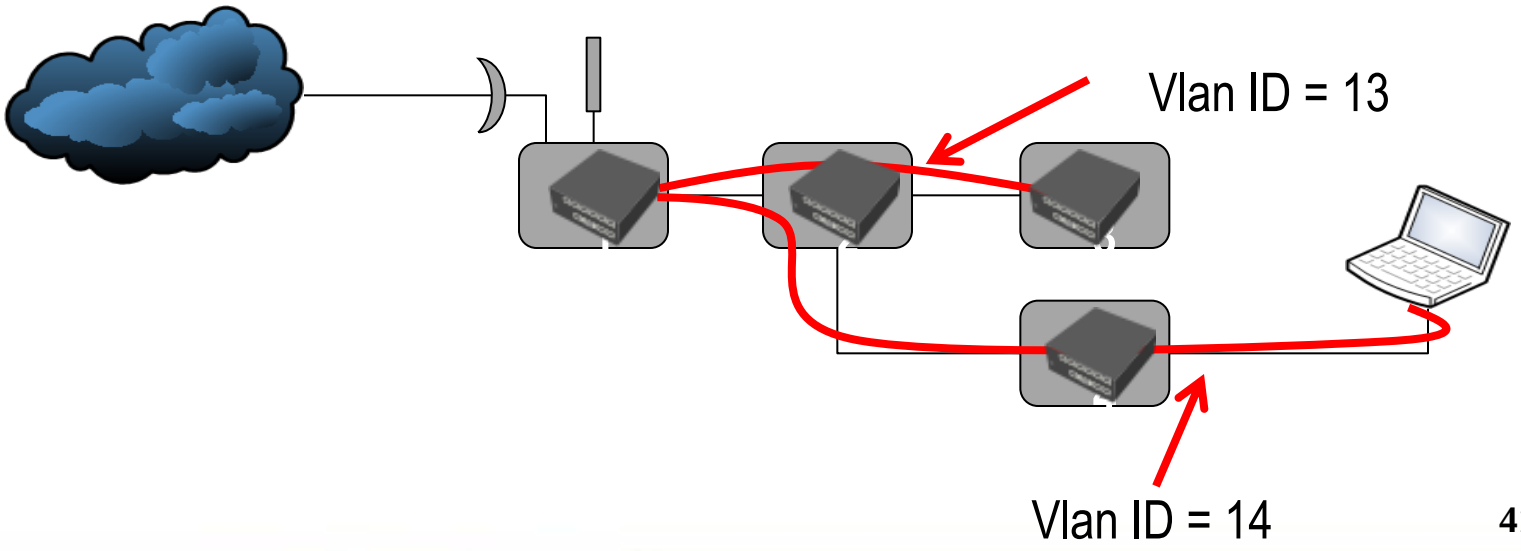
- El atacante manda un paquete con su dirección IP y MAC de origen (4), IP de destino del objeto (3) y MAC de destino el MAC del enrutador (1) que normalmente es la porta promíscua.
- El enrutador reescribe el MAC y manda el paquete para (3)
- El ataque es unidirecional pues la vuelta del pacote es desechada.



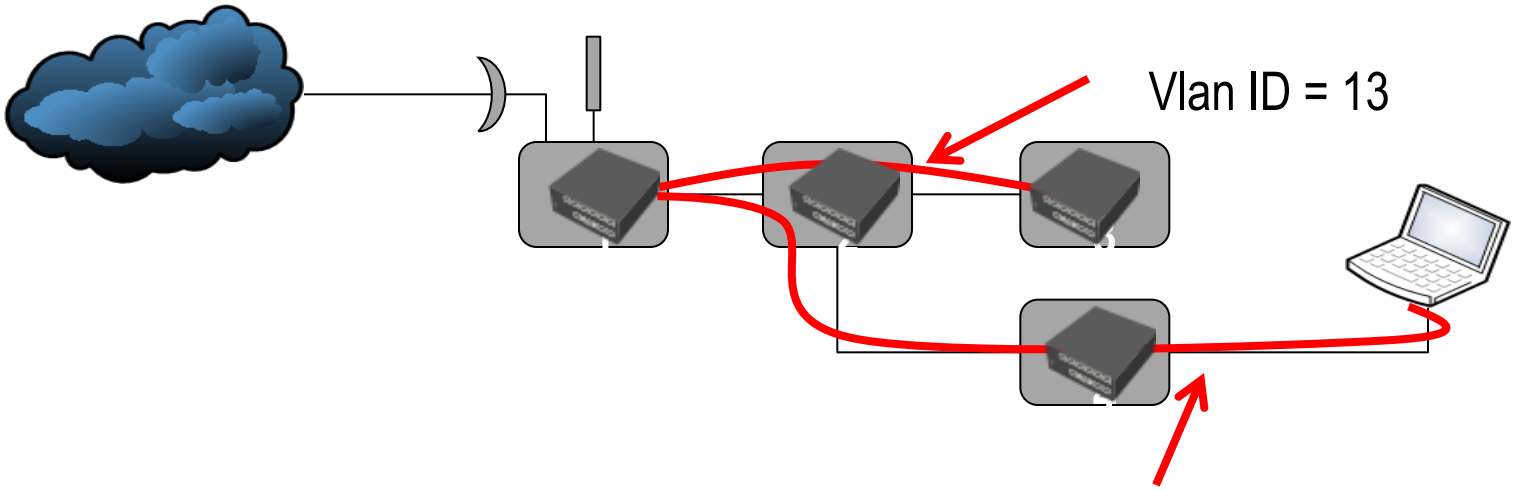
Explotando las VLAN´s

→ Ataque de “rótulo doble” (double tagging) en Vlan´s

- El atacante forma un paquete con la Vlan Tag ID = 13 (Vlan al que él no pertenece), encapsulado con la Vlan Tag ID = 14 (al que pertenece)
- La switch (bridge) saca la Tag 14 enviando el paquete para la Vlan 13
- El ataque es también unidirecional.

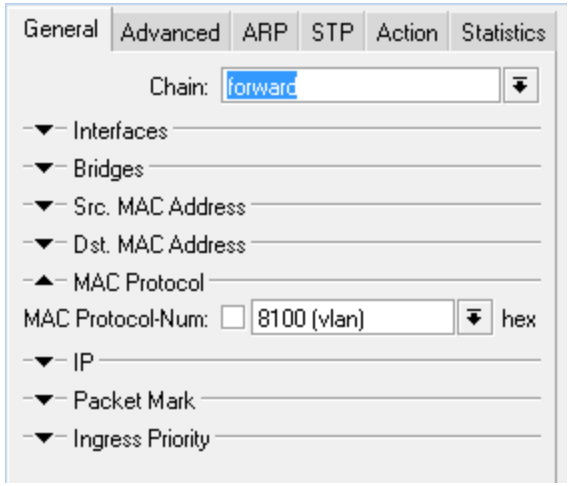


Ataques a Vlan´s
DEMO



- Restringiendo la participación en una Vlan
- Ataque unidirecional de rótulo doble

Explorando VLAN´s
Contramedidas



→ Siendo el VLAN ID el único parámetro a ser configurado en una VLAN, la única medida es bloquear el MAC Protocolo 8100 – Vlan´s en todas las puertas de entrada de la red;

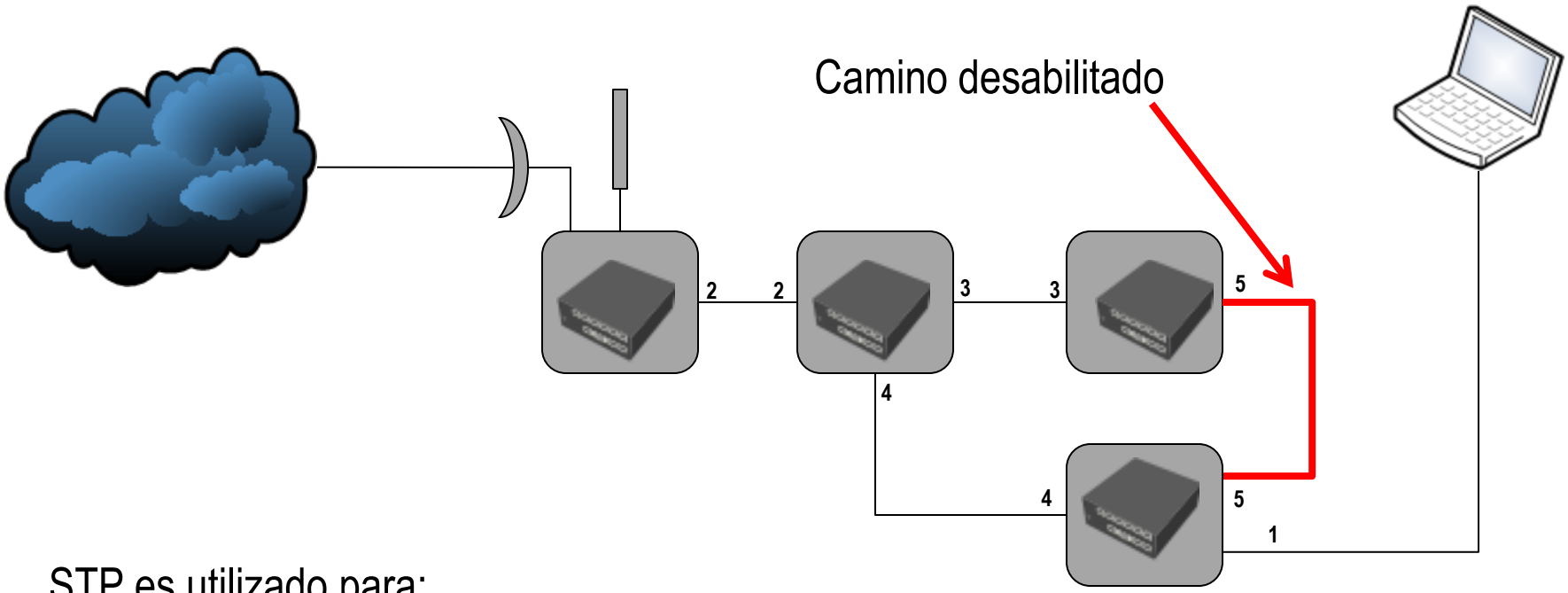
→El bloqueo de ataques de proxy de Vlan´s solamente pueden ser controlados a traves de listas de acceso de MAC´s.

→ El Bloqueo de ataques de rótulo doble pueden ser controlados a traves de lista de acceso de MAC´s y podrían ser por el exámen del contenido de los paquetes IP en la capa 3

Atacando la capa 2

Explotando el Spanning Tree

Aplicaciones del Spanning Tree

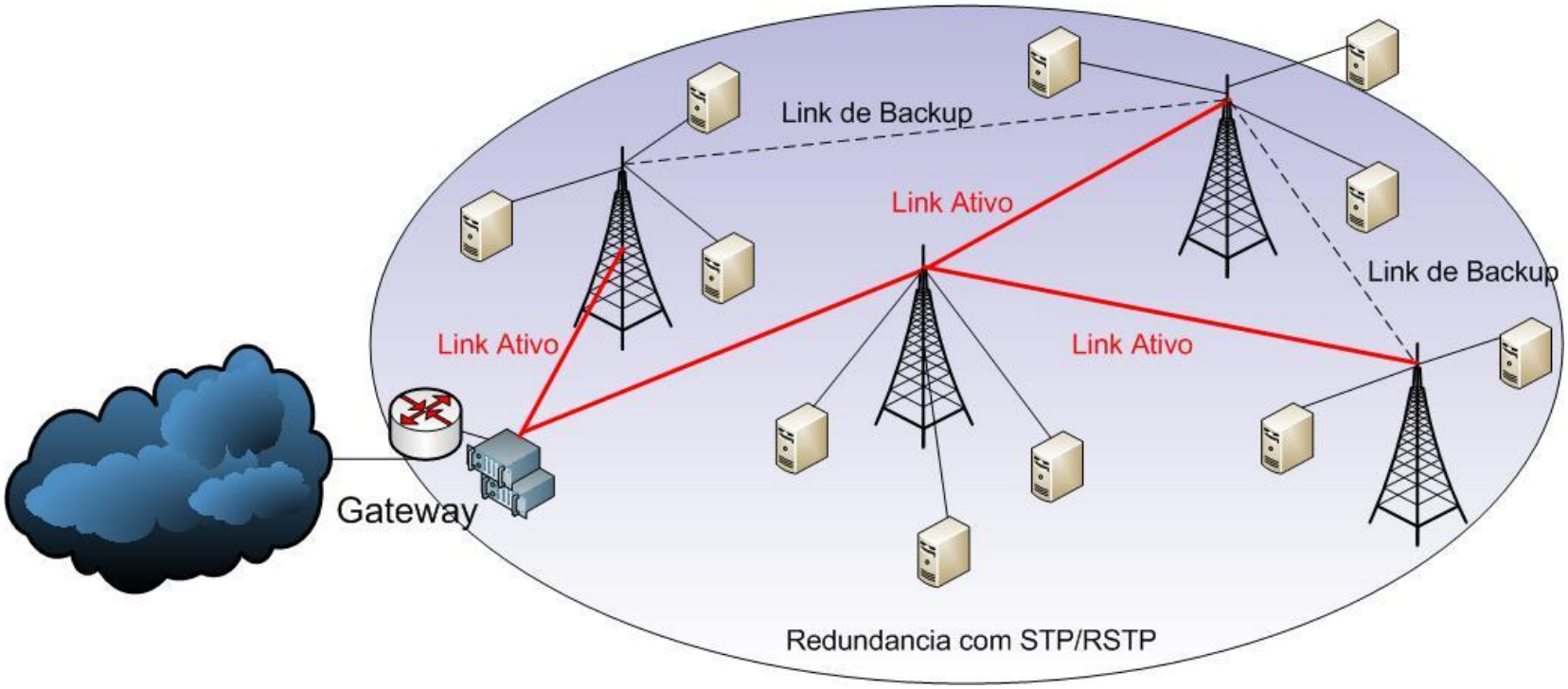


STP es utilizado para:

→ Evitar la formación de loops en redes en Bridge

→ Posibilitar topologías con redundancia de caminos

Aplicaciones del Spanning Tree



Spanning Tree x Rapid Spanning Tree (RSTP)

→RSTP fue propuesto por el IEEE 802.1w para hacer frente a una necesidad de más velocidad de respuesta a la adaptación de cambios de topologia.

→RSTP trabaja con el concepto de estados de las portas. Una puerta puede estar:

- → Desconocida (cuando el estado todavía no fue determinado)
- → Alternativa (no hace parte de la topología activa en el momento – backup)
- → Designada (cuando la porta está designada para uma lan a ella conectada)
- → Root (camino para la bridge root)

→ Los mensajes de BPDU en el RSTP incorporam el estado de las puertas y una série de cambios en relación al STP que hacen el protocolo mucho más rápido. Sin embargo, el RSTP es compatible con STP.

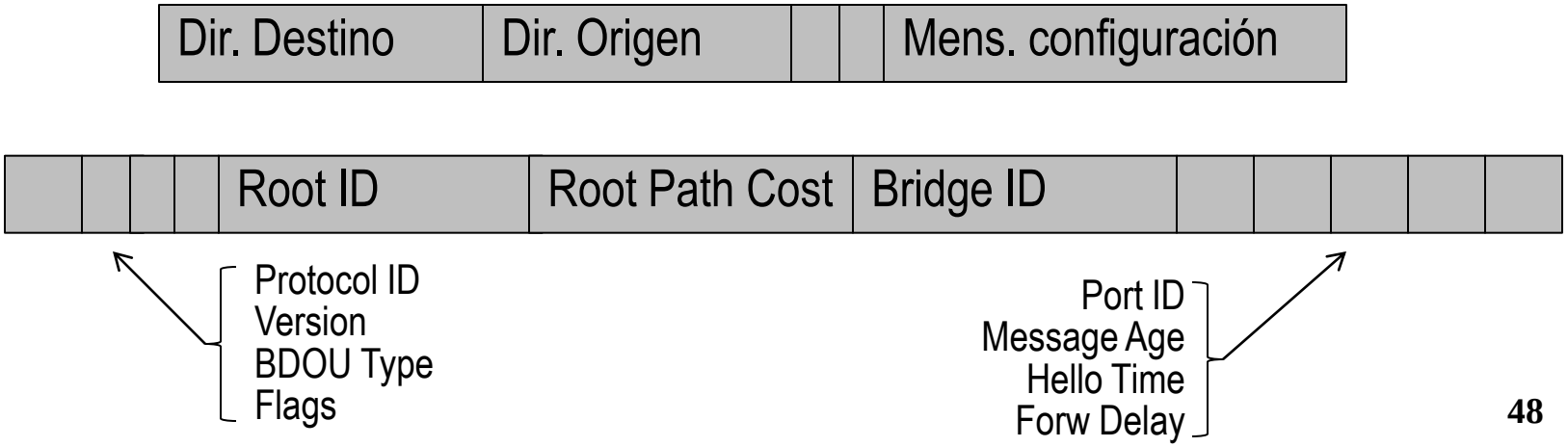
Princípios de funcionamiento del (R)STP

→La bridges participantes del Spanning Tree eligen entre si una bridge root (normalmente la de menor Bridge ID)

→ Cada dispositivo calcula el menor camino a partir de si para la bridge root

→ Para cada bridge es elegida una puerta root, que tiene el menor camino para la bridge root

→ Los dispositivos intercambian mensagens de BPDU (Bridge Protocol Data Unit)



Princípios de funcionamiento del (R)STP

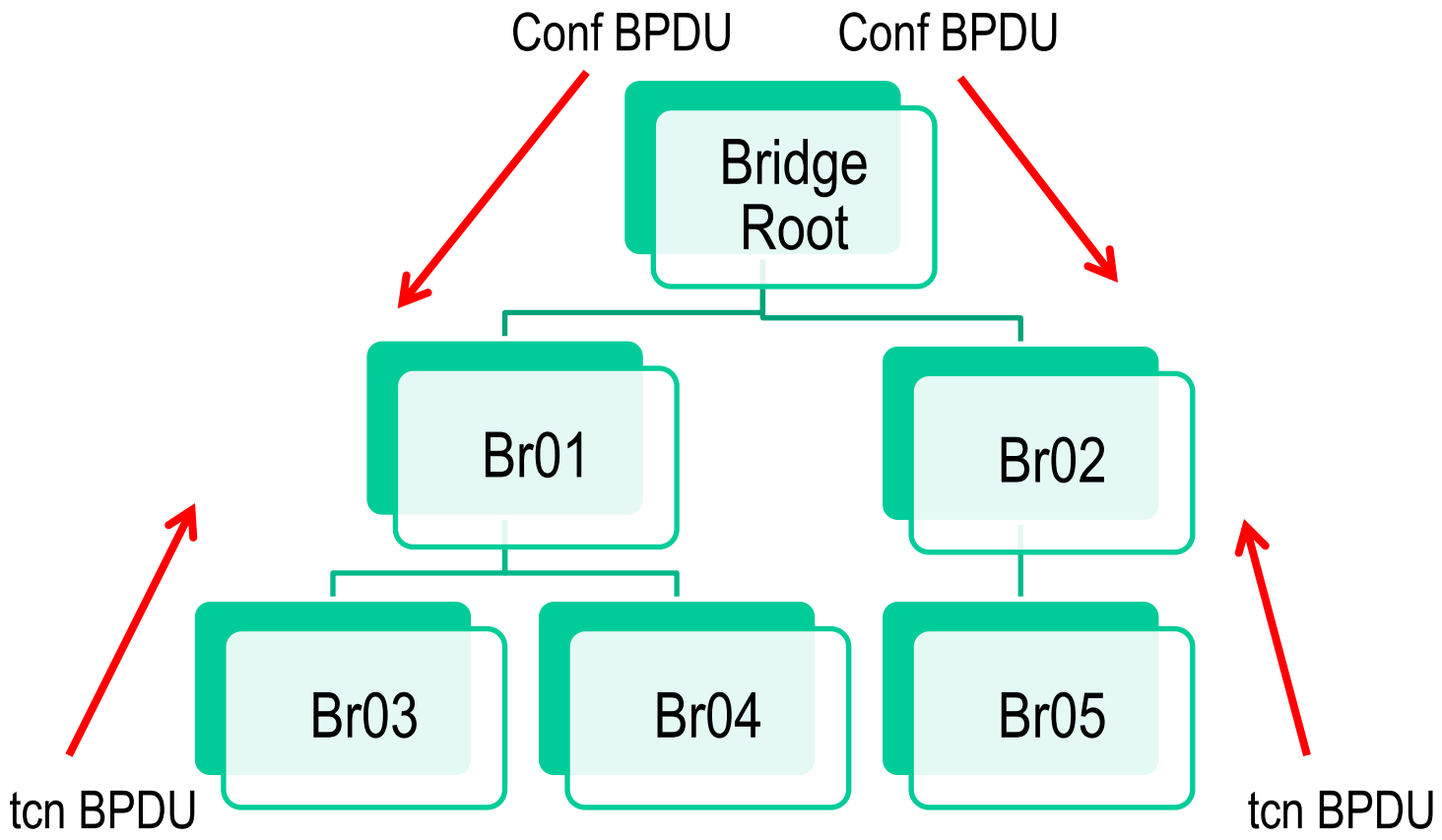
→ Una vez elegida la Bridge Root, ésta pasa a anunciar periódicamente mensajes de configuración que son repasadas por las bridges participantes del STP con su próprio MAC como MAC de origen. (conf BPDU)

→ Cuando ocurre un cambio en la topologia en qualquier segmento de la red, la bridge responsáble por ese segmento envía mensajes comunicando ese cambio (tcn BPDU – Topology Change Notification BPDU)

				Root ID	Root Path Cost	Bridge ID				

Protocol ID	Version	Mes. Type

Princípios de funcionamiento del (R)STP



Seguridad con STP y RSTP

Tanto STP como RSTP tienen caracteristicas que proporcionan la posibilidad de ataques diversos, pues la raíz del problema es la inexistencia de autenticación en las mensajes de BPDU

Así es posible practicar ataques diversos tanto de DoS como de MiTM, al hacer:

→ Flooding de mensajens de conf BPDU

→ Flooding de mensajens de tcn BPDU

→ Flooding de mensajens BPDU asumiendo el papel de bridge root

→ Ataque de hombre del medio cuando se tiene acceso a dos bridges de la topología.

Atacando el Spanning Tree

→ Atacante mandando un mensaje de conf BPDU

firewall info	input: in:ether1 out:(none), src-mac 04:08:20:12:a9:75, dst-mac 01:80:c2:00:00:00, eth-proto 0026

→ Atacante mandando un mensaje de tcn BPDU

firewall info	input: in:ether1 out:(none), src-mac 04:08:20:12:a9:75, dst-mac 01:80:c2:00:00:00, eth-proto 0007

→ Ataque de DoS basado en muchos mensajens de conf BPDU

firewall info	input: in:ether1 out:(none), src-mac 56:ea:a5:15:3e:6f, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac d2:50:ed:1e:48:31, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac 42:60:5b:79:2b:d4, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac 20:68:54:01:d9:1a, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac 18:f1:3a:59:72:0a, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac f6:89:e0:39:91:44, dst-mac 01:80:c2:00:00:00, eth-proto 0026

→ Ataque de DoS basado en muchos mensajens de tcn BPDU

firewall info	input: in:ether1 out:(none), src-mac 82:f0:19:5c:7b:1c, dst-mac 01:80:c2:00:00:00, eth-proto 0007
firewall info	input: in:ether1 out:(none), src-mac d6:d8:2a:50:1e:5c, dst-mac 01:80:c2:00:00:00, eth-proto 0007
firewall info	input: in:ether1 out:(none), src-mac 88:63:b3:6b:18:f1, dst-mac 01:80:c2:00:00:00, eth-proto 0007
firewall info	input: in:ether1 out:(none), src-mac f8:52:21:43:6d:dd, dst-mac 01:80:c2:00:00:00, eth-proto 0007
firewall info	input: in:ether1 out:(none), src-mac 7e:0c:00:23:a5:0f, dst-mac 01:80:c2:00:00:00, eth-proto 0007
firewall info	input: in:ether1 out:(none), src-mac 32:b5:28:36:70:27, dst-mac 01:80:c2:00:00:00, eth-proto 0007

Atacando el Spanning Tree

→ Atacante asumiendo el papel de root

firewall info	input: in:ether1 out:(none), src-mac 00:0c:42:03:04:04, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac 00:0c:42:03:04:04, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac 00:0c:42:03:04:04, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac 00:0c:42:03:04:04, dst-mac 01:80:c2:00:00:00, eth-proto 0026

Bridge | Ports | Filters | NAT | Hosts

Find

	Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root Pat...
	ether1	bridge1	80	10		designated port	
I	ether2	bridge1	80	10		disabled port	
I	ether3	bridge1	80	10		disabled port	
	ether4	bridge1	80	10		root port	10
I	ether5	bridge1	80	10		disabled port	

Bridge | Ports | Filters | NAT | Hosts

Find

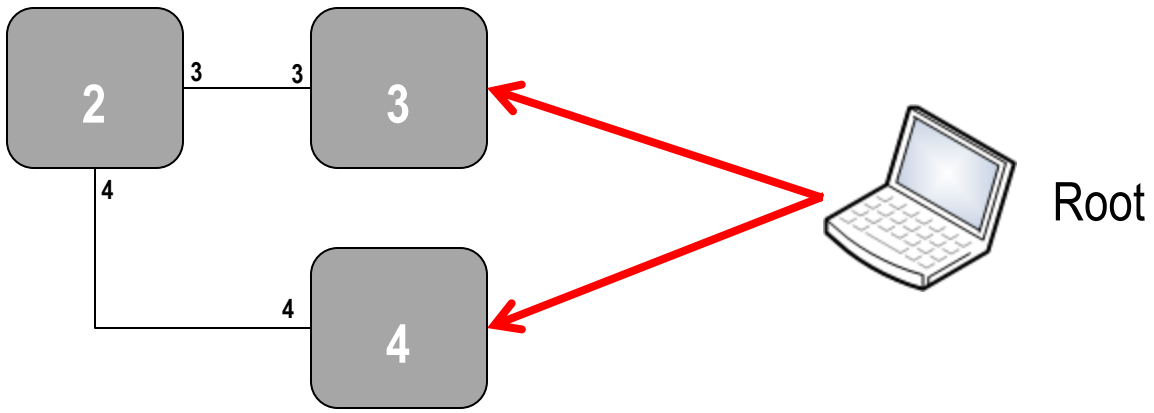
	Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root Pat...
	ether1	bridge1	80	10		root port	20
I	ether2	bridge1	80	10		disabled port	
I	ether3	bridge1	80	10		disabled port	
	ether4	bridge1	80	10		designated port	
I	ether5	bridge1	80	10		disabled port	

Atacando el Spanning Tree

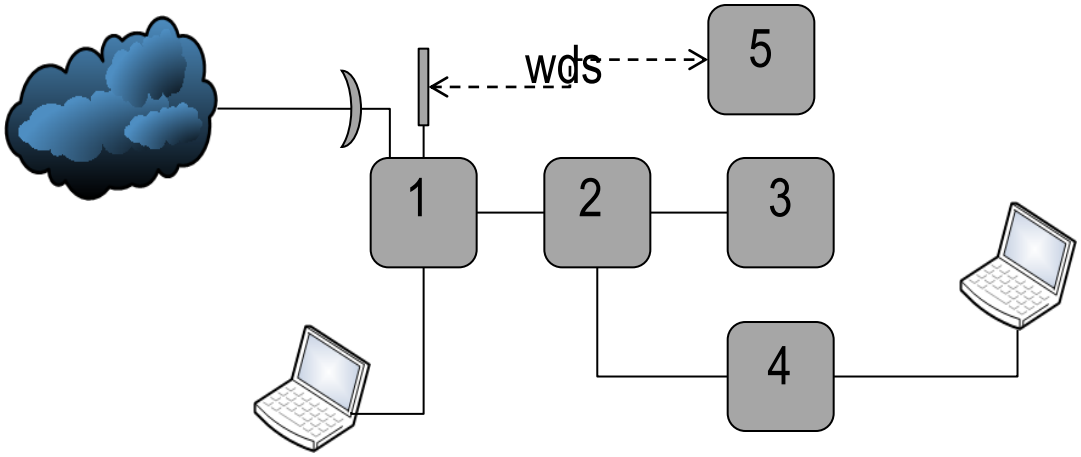
→ Atacante asumiendo el papel de una bridge común

firewall info	input: in:ether1 out:(none), src-mac 00:0c:42:05:04:04, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac 00:0c:42:05:04:04, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac 00:0c:42:05:04:04, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac 00:0c:42:05:04:04, dst-mac 01:80:c2:00:00:00, eth-proto 0026
firewall info	input: in:ether1 out:(none), src-mac 00:0c:42:05:04:04, dst-mac 01:80:c2:00:00:00, eth-proto 0026

→ Atacante asumiendo el papel de root + Hombre del Medio



Ataques al Spanning Tree
DEMO

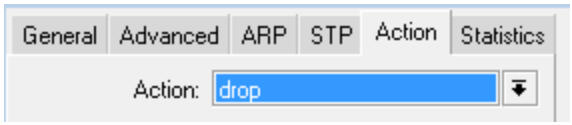


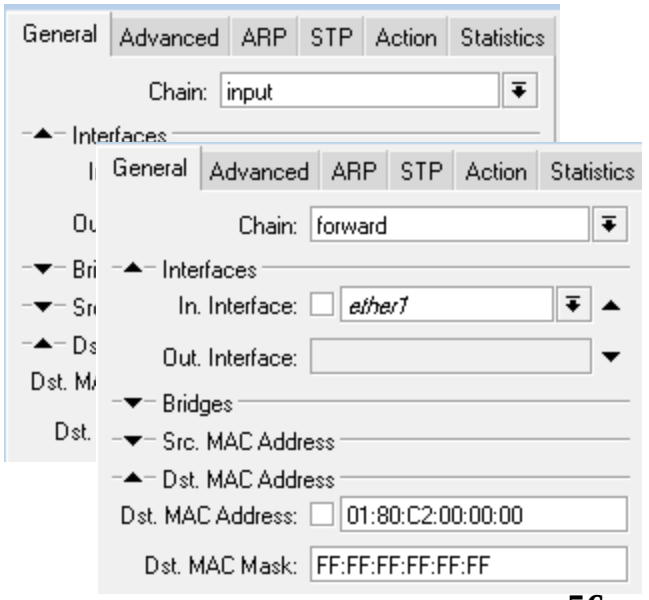
- Mandando mensajes de conf o tcn BPDU para causar DoS
- Convirtiéndose en una Bridge participante del STP
- Convirtiéndose en puerta Root en RSTP

Atacando el Spanning Tree
Contramedidas

Mensajes de Spanning Tree son enviadas por default para la dirección MAC **01:80:C2:00:00:00 .**

→ Filtrar las puertas de borde de la red para esa dirección es la solución para que el atacante no tenga éxito al convertirse en root.

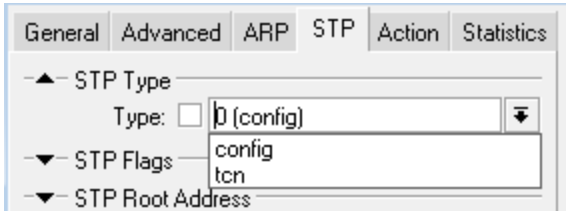




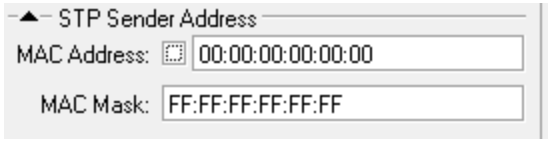
Atacando el Spanning Tree
Contramedidas

Es possible también filtrar selectivamente los mensajens de STP por los clasificadores:

→Tipo de mensaje conf BPDU o tcn BPDU



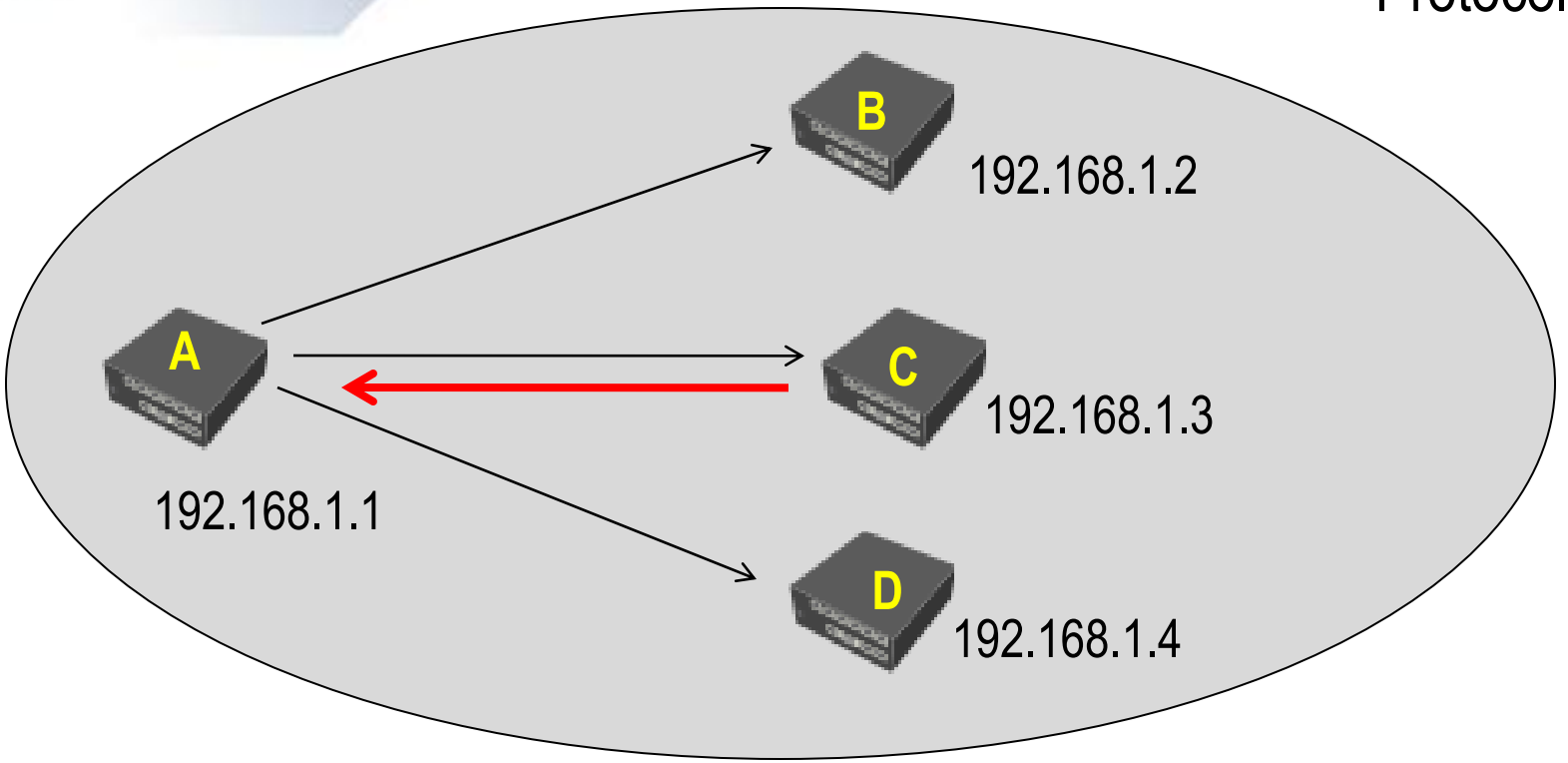
→ Dirección del remitente



Atacando la capa 2

Envenenamiento de ARP
(ARP Poisoning o ARP Spoof)

Protocolo ARP



→ **A pregunta para todos:** "¿Quién tiene el IP 192.168.1.3 ?"

→ **C contesta a A:** "El IP 192.168.1.3 está en el MAC XX:XX:XX:XX:XX:XX"

→ **A registra en su tabla arp el par:** 192.168.1.3, MAC XX:XX:XX:XX:XX:XX

Envenenamiento de ARP

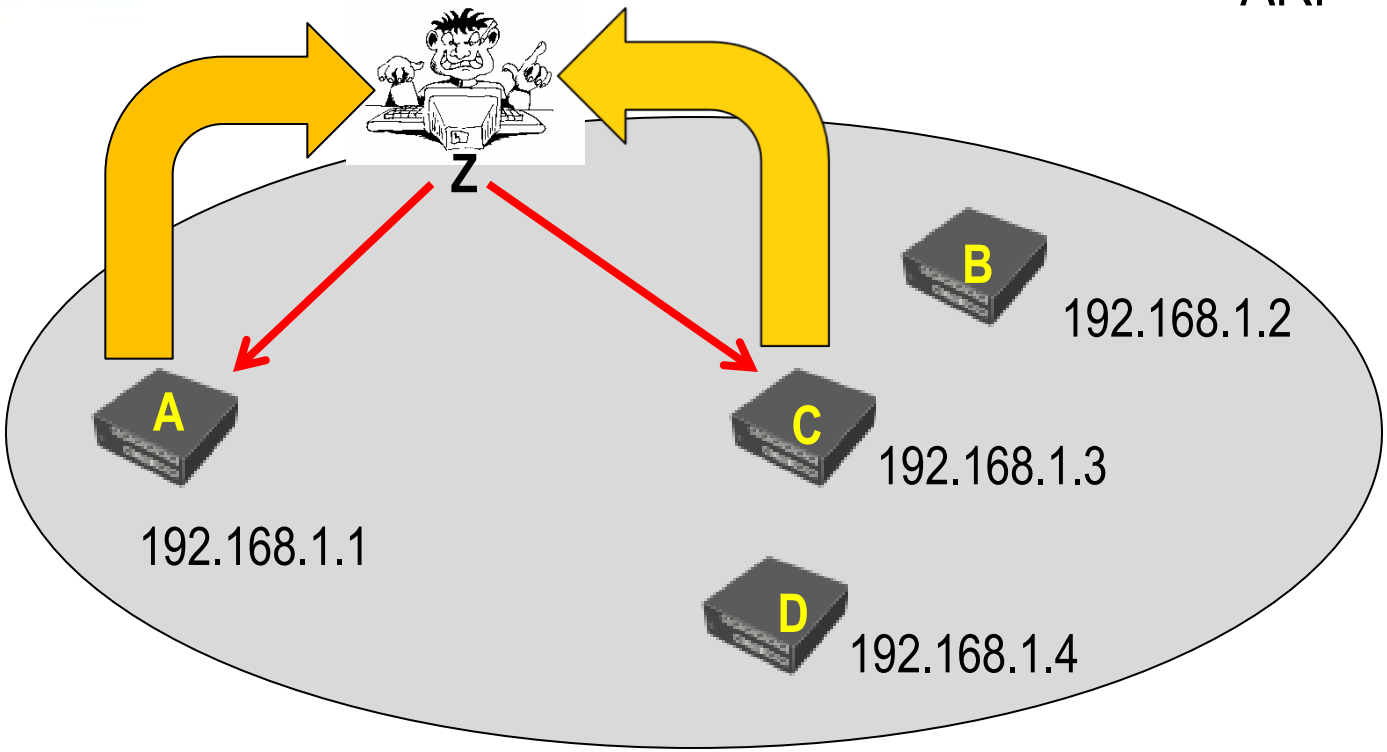
→ “Atacante” emite para um objeto específico (o en broadcast), mensajes de ARP “gratuitas” anunciando que su MAC es el MAC de quien quiere spoofar (normalmente el gateway)

→ “Atacado” tiene sus tablas ARP “envenenadas” y pasa a mandar los pacotes para el Atacante

→ “Atacante” manda para el gateway mensajes de ARP “grátis” anunciando su MAC con el IP del Atacado

→ Atacado se comunica con el Gateway a traves del Atacante – Hombre del medio

"Envenenamiento" de ARP

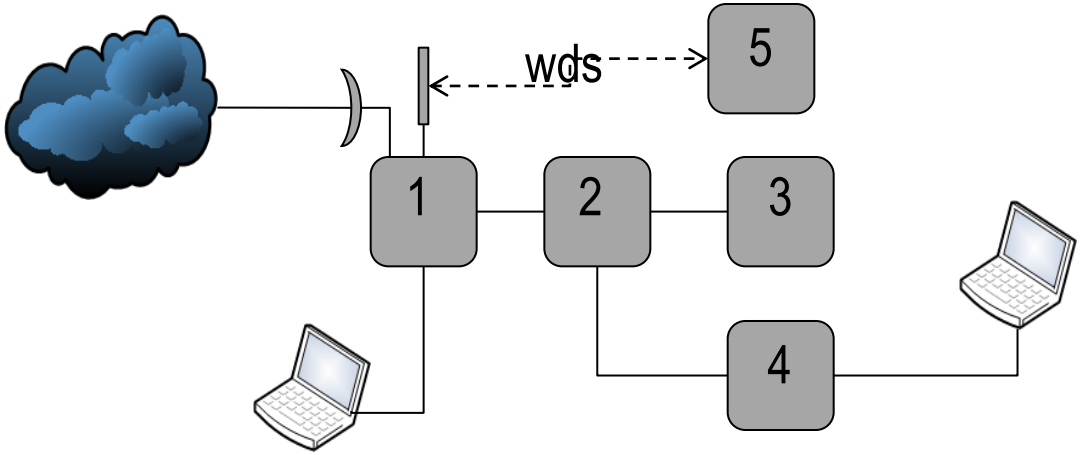


→ **Z dice a A:** "El IP 192.168.1.3 está nel MAC ZZ:ZZ:ZZ:ZZ:ZZ:ZZ"

→ **Z dice a C:** "El IP 192.168.1.1 está nel MAC ZZ:ZZ:ZZ:ZZ:ZZ:ZZ"

→ **A empieza a hablar con C (y vice versa) a traves de Z (Hombre del medio)**

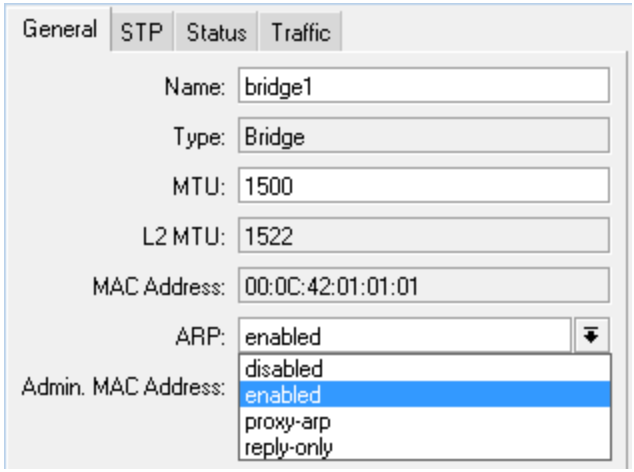
Spoof de ARP DEMO



- Haciendo el arp-spoof a partir de 4
- Averiguando en los otros hosts
- Filtrando el ARP

Defensas para Arp-Spoof

1) Cambio en el comportamiento del protocolo ARP



ARP disabled → todos los hosts deben tener entradas estáticas.

ARP Reply-Only → Solamente el concentrador tiene entradas estáticas.

Inconvenientes:

→ Arp estático en todos los hosts es muy difícil de implementar en la práctica

→ Reply-Only no protege el lado del cliente.

Defensas para Arp-Spoof

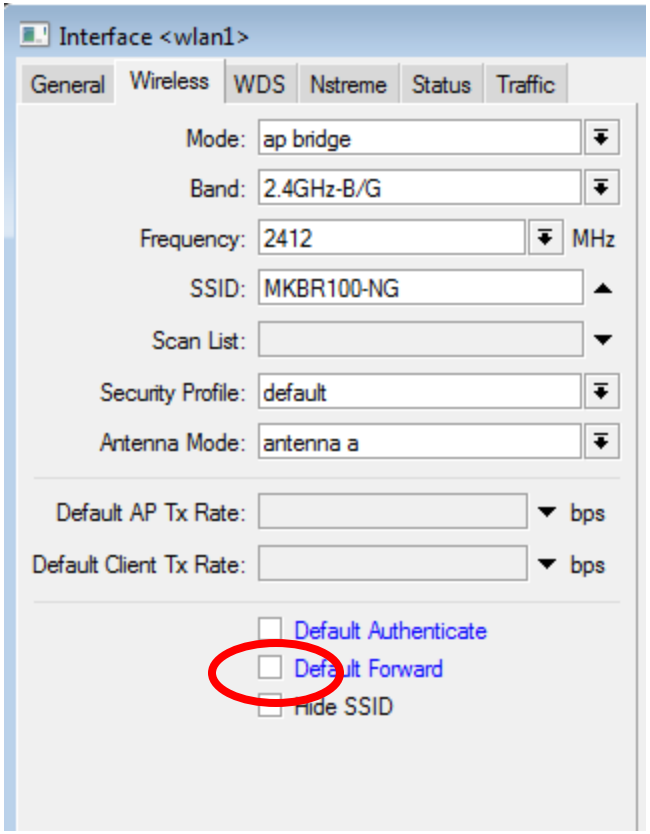
2) Segregación del tráfego (aislamiento de clientes)

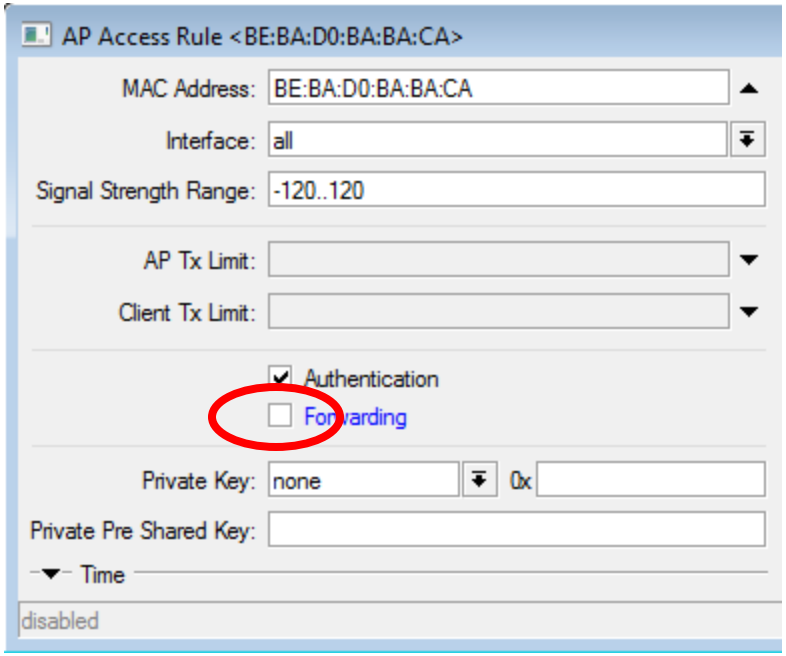
En una red típica volteada para proveer acceso es deseable que los clientes en la capa 2 apenas “vean”el gateway. Vamos a llamarles segregación de tráfego las medidas que deben ser tomadas para aislar todo tipo de tráfego entre los clientes.

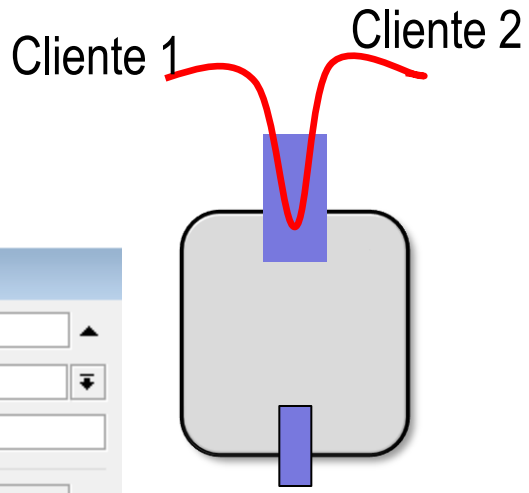
En el caso de una rede Iñalambrica, con esas medidas, deben ser hechas en 2 niveles:

- → En la Interfaz (Tarjeta Iñalambrica)
- → En todas las “puertas” de la bridge.(Iñalambricas y ethernet)

Segregando el tráfego en la capa 2 (1 Tarjeta Iñalambrica)

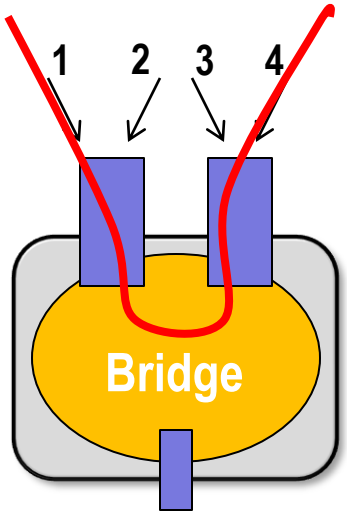


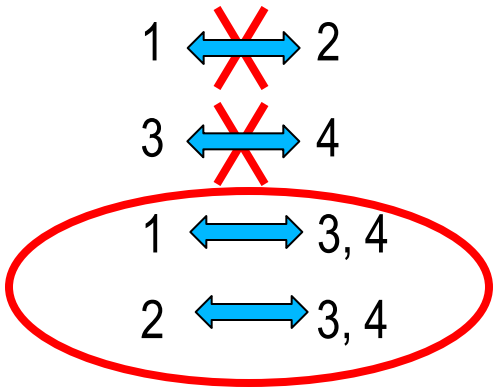


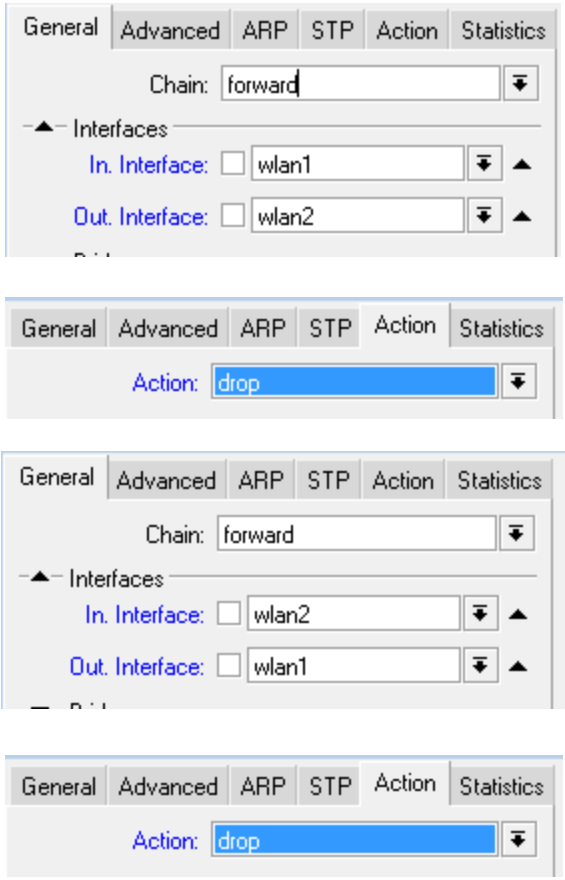


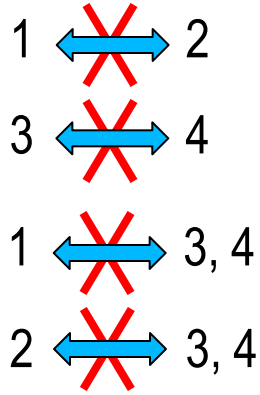
Default forward desabilitado en las interfaces y en los access lists

Segregación de tráfego en la capa II (2 tarjetas Iñalambricas en bridge)





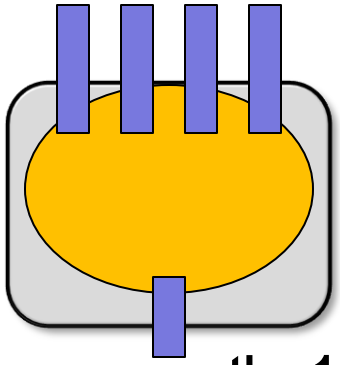




2 Reglas

Segregando el tráfego en la capa II
4 Interfaces en Bridge

Wlan1, 2, 3 y 4



ether1

¿12 Reglas?

Bridge | Ports | Filters | Broute | NAT | Hosts

oo Reset Co

#		Chain	Interfaces...	Interfaces...
0		forward	wlan1	wlan2
1		forward	wlan2	wlan1
2		forward	wlan1	wlan3
3		forward	wlan3	wlan1
4		forward	wlan1	wlan4
5		forward	wlan4	wlan1
6		forward	wlan2	wlan3
7		forward	wlan3	wlan2
8		forward	wlan2	wlan4
9		forward	wlan4	wlan2
10		forward	wlan3	wlan4
11		forward	wlan4	wlan3

4 Reglas

Bridge | Ports | Filters | Broute | NAT | Hosts

oo Reset

#		Chain	Interfaces...	Interfaces...
0		forward	wlan1	!ether1
1		forward	wlan2	!ether1
2		forward	wlan3	!ether1
3		forward	wlan4	!ether1

¡1 Regla !

Bridge | Ports | Filters | Broute | NAT | Hosts

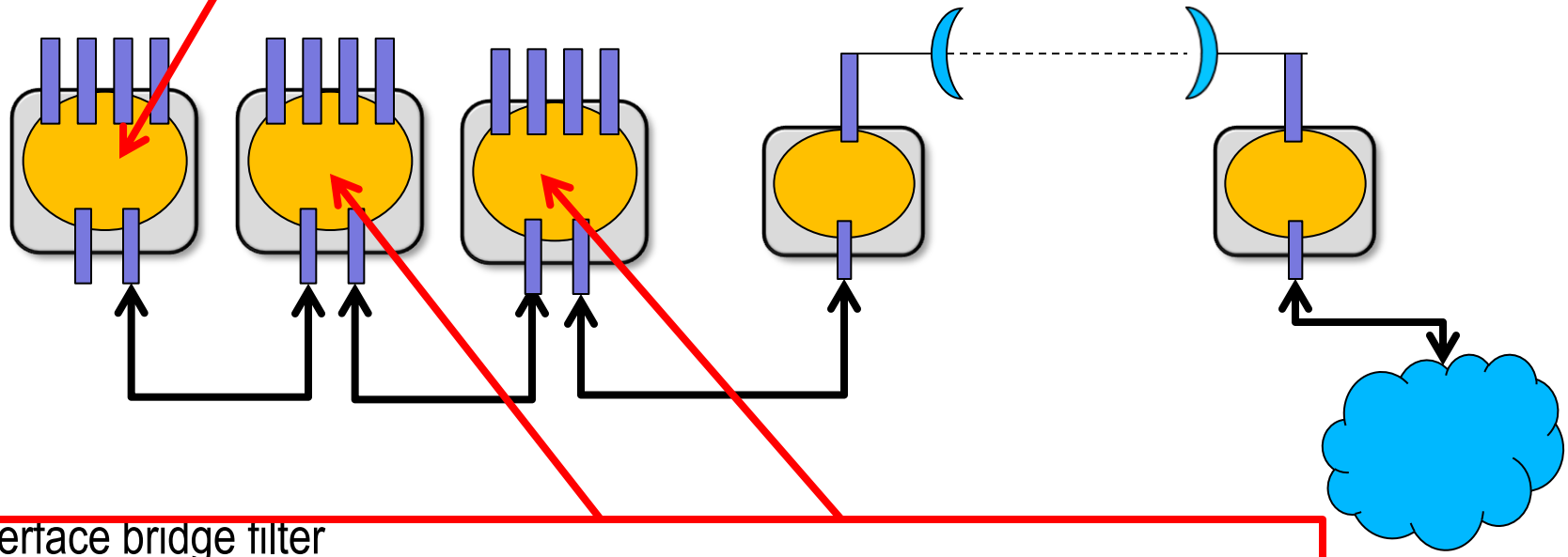
Reset

#		Chain	Interfaces...	Interfaces...
0		forward	!ether1	!ether1

Gracias, Edson ☺

Segregando el tráfego en la capa II
Varios equipos en Bridge

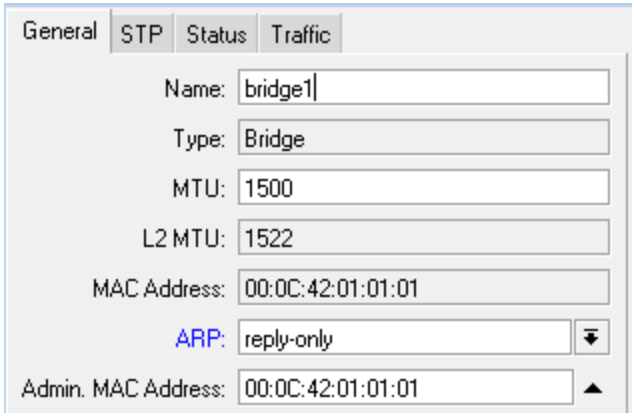
```
/interface bridge filter
add  chain=forward in-interface=!ether2
out-interface=!ether2  action=drop
```



```
/interface bridge filter
add  chain=forward in-interface=ether1  out-interface=ether2 action=accept
add  chain=forward in-interface=ether2  out-interface=ether1 action=accept
add  chain=forward in-interface=!ether2 out-interface=!ether2  action=drop
```

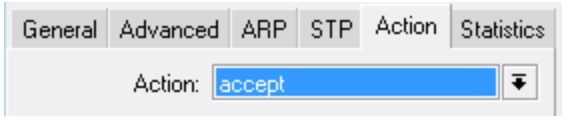
Defensas para Arp-Spoof

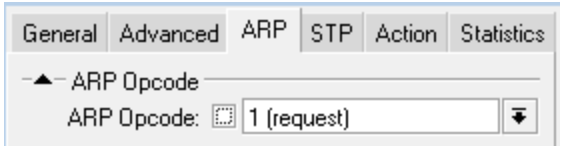
En redes donde hayan otros equipos que no acepten la segregación del tráfego, lo que puede ser hecho es juntar el ARP reply-only con algunos filtros e para evitar el envenenamiento de los clientes por lo menos en los trozos donde el tráfego pasa por el Mikrotik RouterOS.

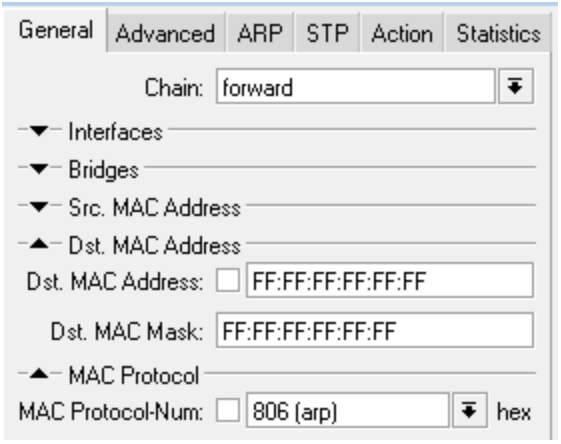


1 – Gateway em reply-only (tabelas estáticas)

2 - Acepta requisiciones de ARP de qualquier host

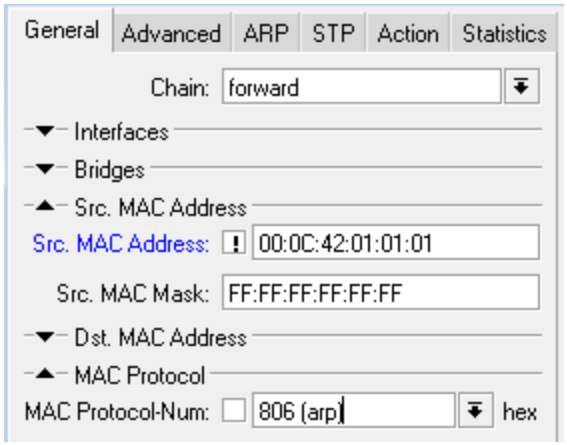


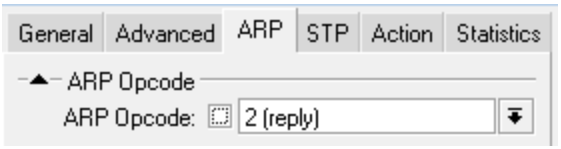




Defensas para Arp-Spoof

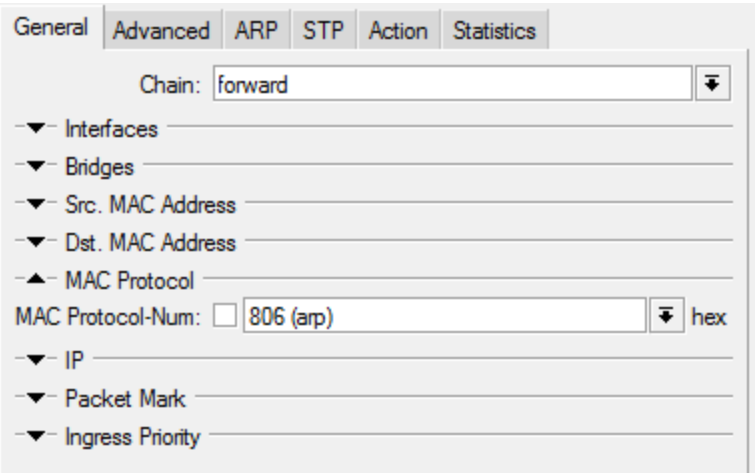
3 – Descarta cualquier respuesta que no sea originada del Gateway

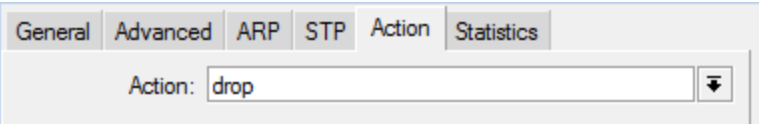


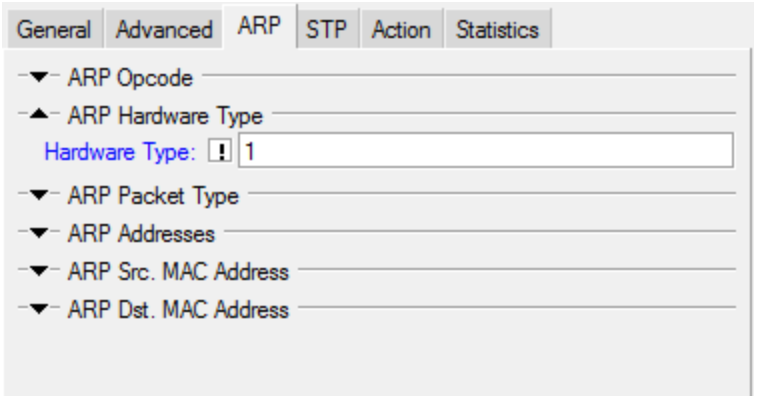


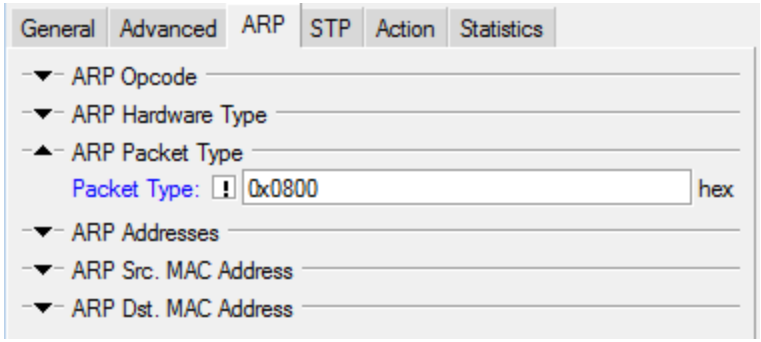
Protegiendo el ARP (medidas complementarias)

Se puede aun eliminar paquetes “inutiles” descartando tramas que no sean ethernet o IPV4



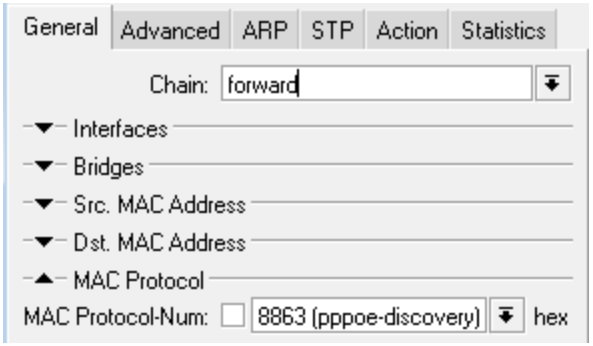


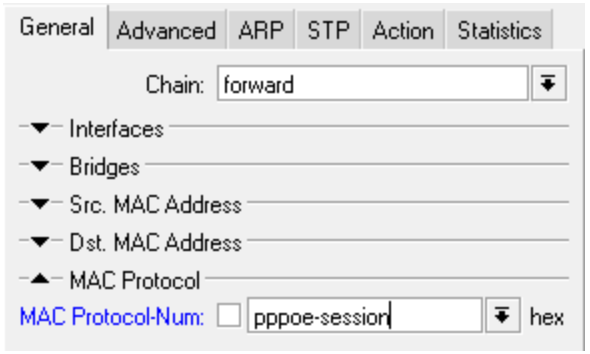




Medidas para control de arp-poof en redes con PPPoE

→ Filtros de Bridge en las interfaces que “escuchan” el PPPoE permitiendo solamente PPPoE-discovery y PPPoE-session, son importantes y filtran totalmente el protocolo ARP. Las interfaces pueden incluso tener el ARP desabilitado. Tales medidas son importantes no solo para filtrar ARP pero también para otros tráfegos indeseables.



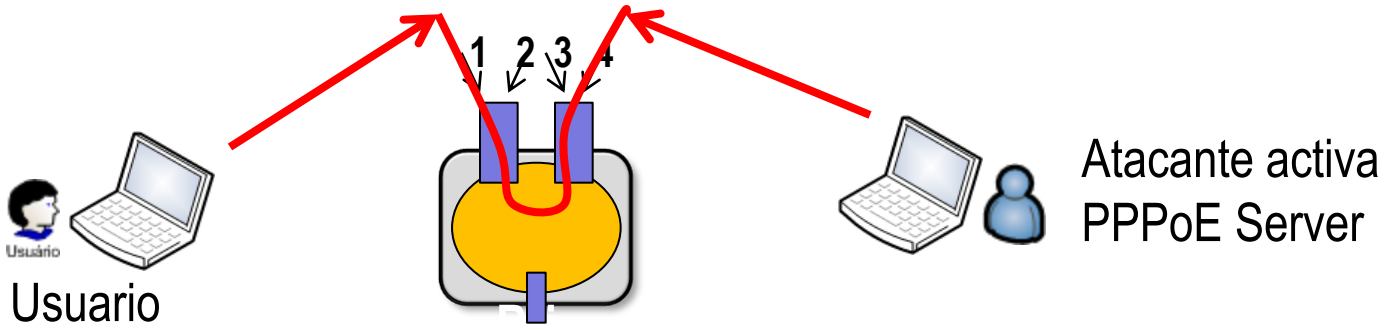


¿Una rede que utiliza PPPoE está libre de ataques de arp-spoof por parte de sus clientes?

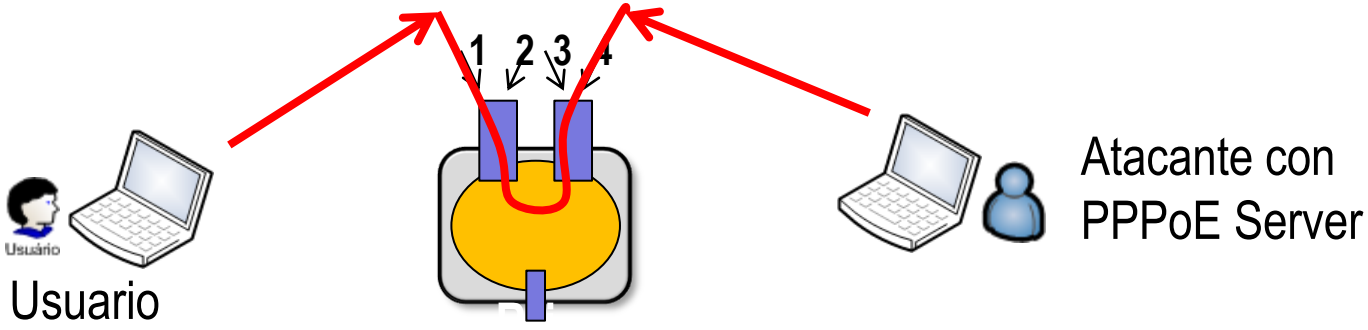
→ Si la red utiliza solamente PPPoE y no utiliza IP en las interfaces que “escuchan” el PPPoE la respuesta es claramente sí.

→Sin embargo no se puede ignorar que tales redes están sujetas a todos los otros ataques abordados previamente y uno más:

→ Ataques entre clientes por servidor PPPoE Falso:



Solución para el problema anterior



→Desabilitar default forward en las interfaces y access lists

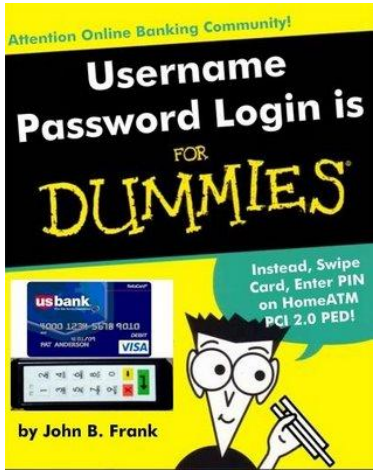
→ Efectuar los filtros de Bridge entre interfaces **ANTES** de liberar el PPPoE.

→ Aceptar los trafegos PPPoE session y PPPoE discovery

→Descartar el restante

Atacando la capa 2

Atacando clientes y proveedores de PPPoE y Hotspot



Atacando Proveedores y Clientes de Hotspot y PPPoE

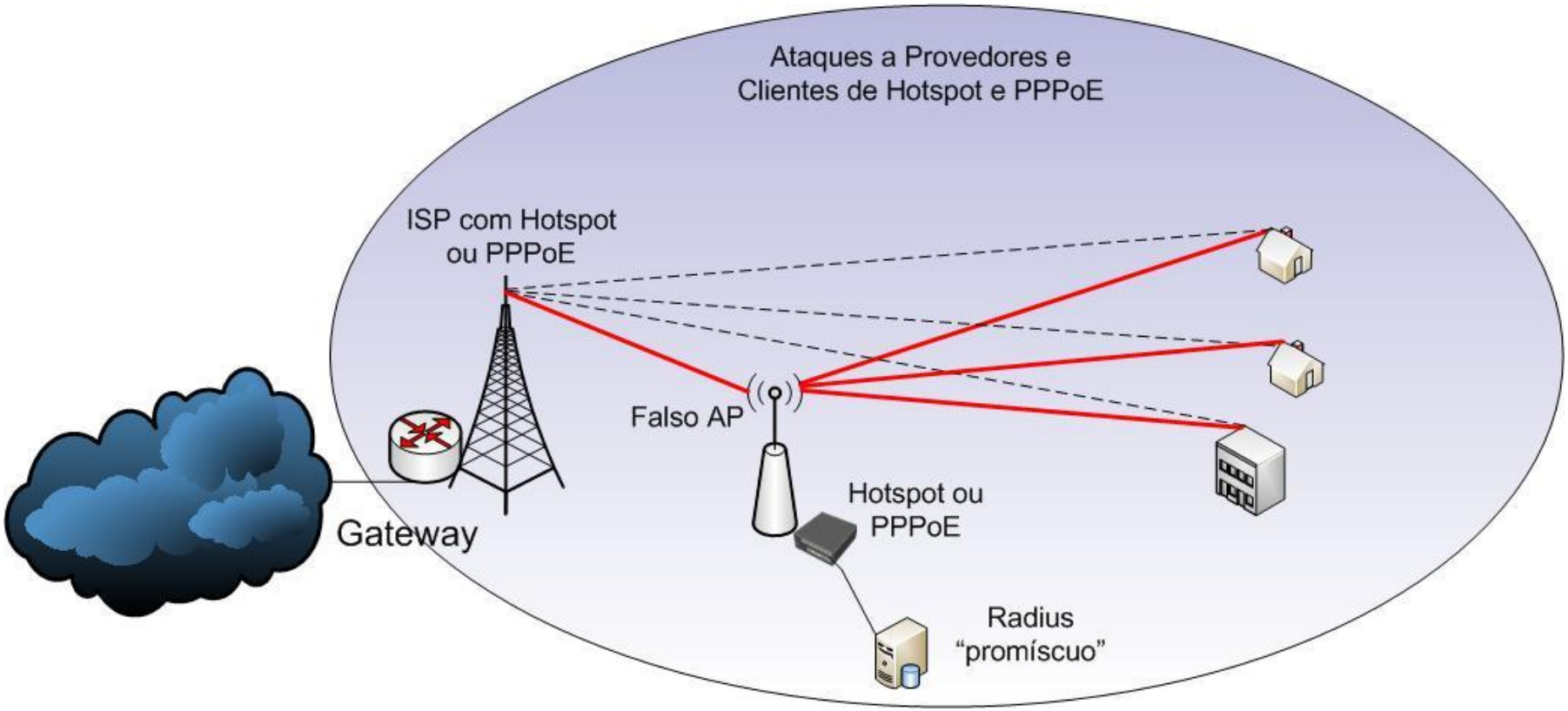
→ Son ataques sencillos de capa 1 y 2 que consisten en poner un AP con el mismo SSID y Banda de operación y ejecutar el mismo servicio (PPPoE o Hotspot)

→ Dependiendo de la potencia de la señal y ubicación relativa del atacante en relación a los clientes no es necesario mayores medidas. Puede ser necesario hacer un ataque de DoS en proveedor inicialmente.

→ El ataque puede ser hecho para varios objetivos, como simple negación de servicio, descubierta de contraseñas de Hotspot y PPPoE, hombre del medio, envenenamiento de cache, etc.

→ Para descubierta de contraseñas se puede utilizar un Radius en modo Promíscuo

Atacando Proveedores y Clientes de Hotspot y PPPoE



Radius configurado para descubrir usuarios y senhas

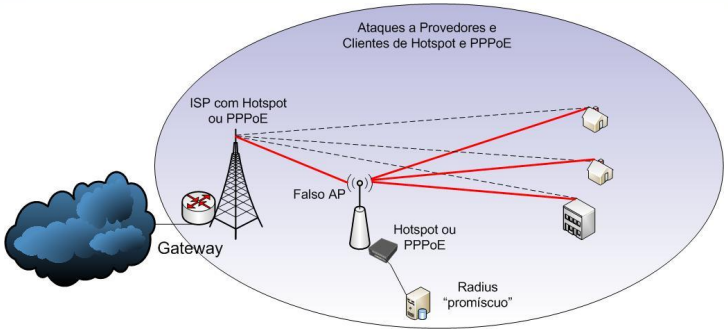
maia@maia-laptop:/etc/freeradius/radiusd.conf

…

# Log authentication requests to the log file
# allowed values: { no, yes }
log_auth = yes

# Log passwords with the authentication requests
# allowed values: { no, yes }
log_auth_badpass = yes
log_auth_goodpass = yes
…

Ataques a Hotspot y PPPoE
Contramedidas



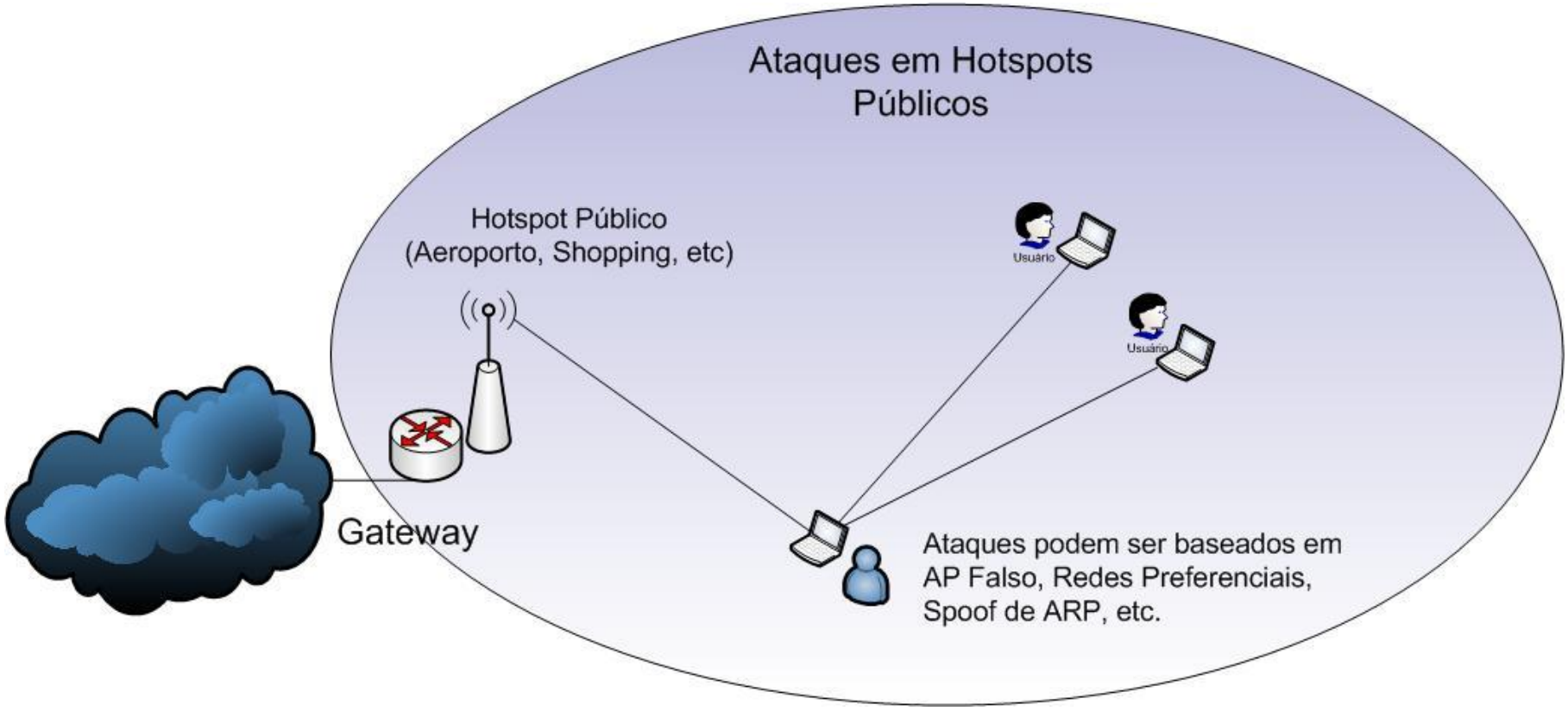
→ Solamente criptografía bien implementada puede evitar esos ataques. Es estúpido pensar que una red Wireless está segura cuando no usa criptografía.

→La implementación de la criptografía en una red puede ser hecha de inumeras maneras, más o menos eficientes. La manera más segura sería con Certificados Digitales instalados en todos los equipos (EAP-TLS) pero es en la práctica limitada por la punta cliente que ni siempre tiene el soporte adecuado.

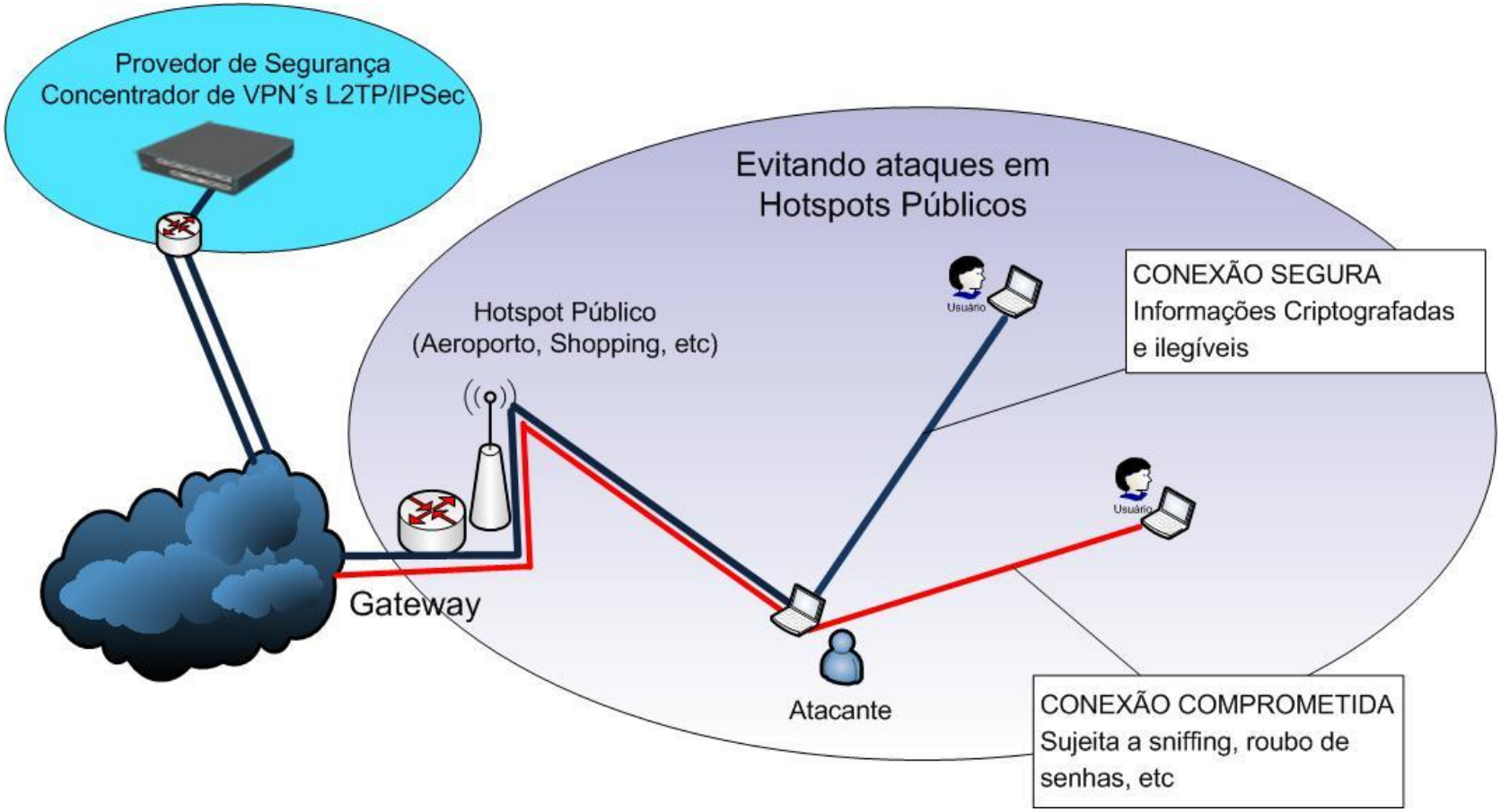
→El Mikrotik tiene una solución intermedia muy interesante que es la distribución de claves PSK individuales por cliente con las claves distribuídas por Radius.

Para detalles de esa implementación, véase http://mum.mikrotik.com – Brazil 2008

Ataques a Hotspots Públicos

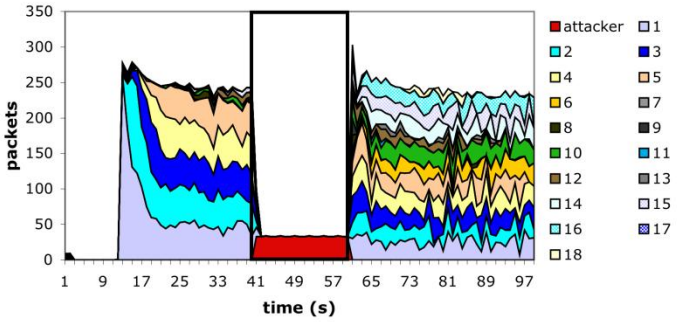


Acceso seguro en Hotspots Públicos



Atacando la capa 2

Ataques de Desautenticación
(Deauth Attack)



Ataques de negación de servicio en Redes Iñalambricas 802.11

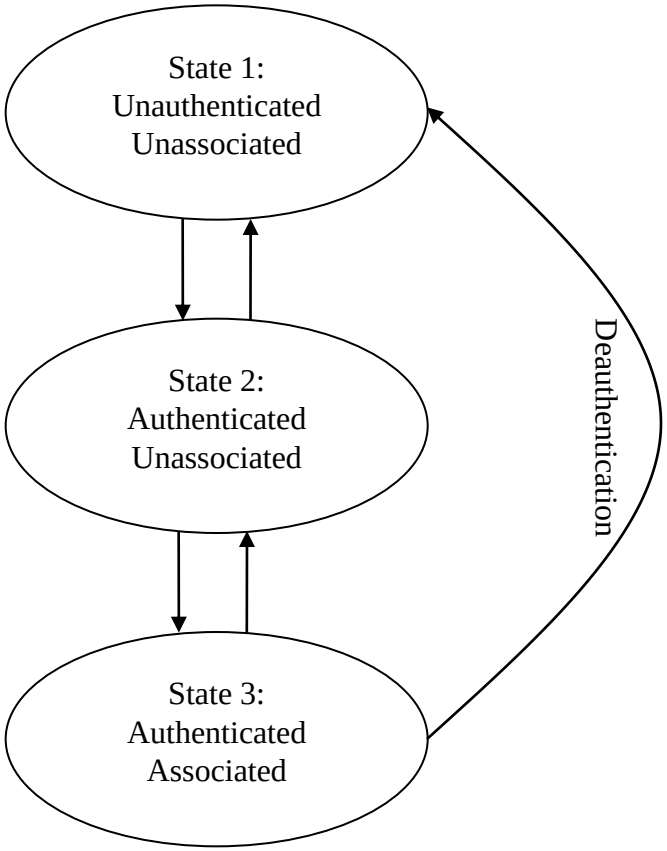
→ Ataques basados en altas potencias de RF (Jamming) – Capa 1

Teniendo en vista que estamos trabajando con bandas no licenciadas, ese es un risco potencial y no hay mucho qué hacer sino reclamar con la autoridad responsable por el espectro. Un buen proyecto de RF puede, sin embargo, ayudarnos a tener una exposición más pequeña a ese tipo de ataque.

→ Ataques basados en el protocolo

Tiene como base la exploración de vulnerabilidades en los frames de control que existen gracias a una concepción débil de seguridade en el desarrollo del protocolo 802.11 pues no hubo preocupación cuanto a la autenticación de esos frames.

Proceso de Autenticación / Asociación



802.11 Types and Subtypes

00 - Protocol Version

2	2	4	1	1	1	1	1	1	1	1

00 - Management Frame Type

0000 - association request
0001 - association response
0010 - reassociation request
0011 - reassociation response
0100 - probe request
0101 - probe response
1000 - beacon
1010 - disassociation
1011 - authentication
1100 - deauthentication

01 - Control Frame Type

1010 - power save poll
1011 - RTS
1100 - CTS
1101 - ACK
1110 - CF-end
1111 - CF-end + CF-ACK

10 - Data Frame Type

0000 - data
0001 - data + CF-ACK
0010 - data + CF-poll
0011 - data + CF-ACK + CF-poll
0100 - NULL (no data)
0101 - CF-ACK (no data)
0110 - CF-poll (no data)
0111 - CF-ACK + CF-poll (no data)

Ataque de Deauth

1 – El atacante utiliza cualquier herramienta como airodump, kismet, wellenreiter, o el própio sniffer/snooper de Mikrotik RouterOS para descubrir :

→ MAC del AP

→ MAC del Cliente

→ Canal en uso

2 – Se pone en cualquier posición en la que el AP puede oír su transmisión (incluso una señal débil será suficiente desde que esté algunos decibeles arriba de la sensibilidad del AP)

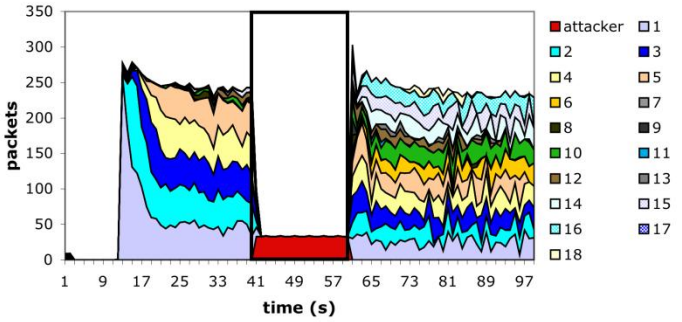
3 – Dispara el ataque solicitando al AP que desautentique el cliente;

Ese ataque puede ser combinado con otros, levantando un AP falso y haciendo el Hombre del medio o incluso para facilitar la renovación de la tabla ARP

Atacando la capa 2

Ataques de Desautenticación (Deauth Attack)

DEMO



Ataque de Deauth

maia@maia:~$ sudo my-l2-attacks –s 00:0C:42:AA:AA:AA –c 00:0C:42:CC:CC:CC
- - deauth=10 wlan0

09:54:01 Sending 64 direct DeAuth. STMAC: [00:0C:42:CC:CC:CC] [86|84 ACKs]
09:54:02 Sending 64 direct DeAuth. STMAC: [00:0C:42:CC:CC:CC] [111|99 ACKs]
09:54:03 Sending 64 direct DeAuth. STMAC: [00:0C:42:CC:CC:CC] [54|64 ACKs]
09:54:04 Sending 64 direct DeAuth. STMAC: [00:0C:42:CC:CC:CC] [138|130 ACKs]
09:54:07 Sending 64 direct DeAuth. STMAC: [00:0C:42:CC:CC:CC] [305|301 ACKs]
09:54:09 Sending 64 direct DeAuth. STMAC: [00:0C:42:CC:CC:CC] [318|311 ACKs]
09:54:12 Sending 64 direct DeAuth. STMAC: [00:0C:42:CC:CC:CC] [266|266 ACKs]
09:54:15 Sending 64 direct DeAuth. STMAC: [00:0C:42:CC:CC:CC] [322|316 ACKs]
09:54:17 Sending 64 direct DeAuth. STMAC: [00:0C:42:CC:CC:CC] [224|231 ACKs]
09:54:20 Sending 64 direct DeAuth. STMAC: [00:0C:42:CC:CC:CC] [346|344 ACKs]

Ataques de deauth - soluciones

→ Después de revelados los problemas con ataques de deauth e teniendo estos tomado caráter real, algunas medidas fueron propuestas como la expuesta en el artículo abajo:

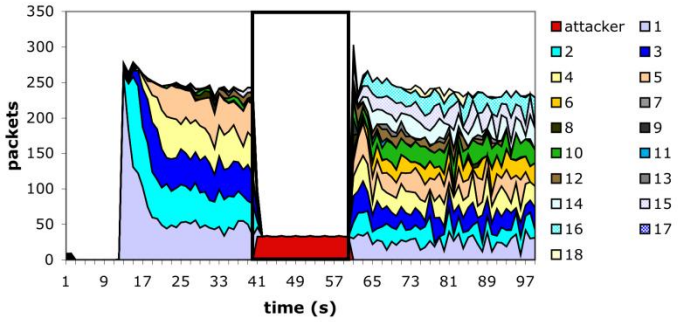
http://sysnet.ucsd.edu/~bellardo/pubs/usenix-sec03-80211dos-slides.pdf

→ Em los MUM´s de Argentina en 2007 y de Polonia en 2008 fueron presentadas algunas soluciones para hacer frente a esos ataques al utilizar Mikrotik RouterOS. Son soluciones meramente paliativas que podían hasta entonces ser adotadas.

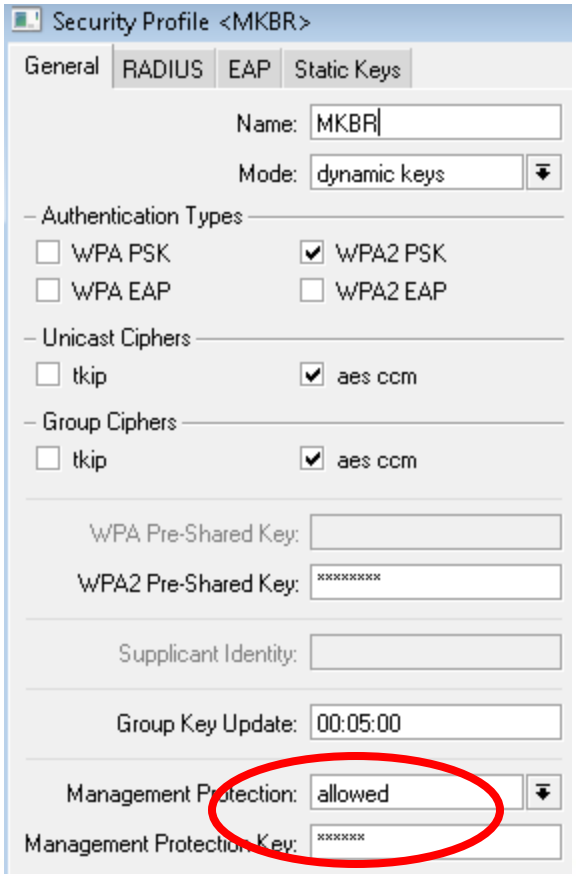
http://wiki.mikrotik.com/images/2/20/AR_2007_MB_Wireless_security_Argentina_Maia.pdf
http://mum.mikrotik.com/presentations/PL08/mdbrasil.pdf

Ataques de Desautenticación (Deauth Attack)

Contramedidas



→ A partir de la V4 el Mikrotik RouterOS incorpora la posibilidad de autenticación de frames de control en los perfiles de seguridad.



Ataques a la capa 2 y contramedidas
Conclusiones

→ La exposición de cualquer red a ataques de capa 2 es muy grande cuando se tiene acceso físico a ella y los potenciales ataques de negación de servicio son en su mayoría sobrepujantes y de difícil control.

→ Cuando se necesita dar acceso en capa 2 a una otra red, una política rígida de control de direcciones físicas deve ser implementada, además de otros filtros.

→ El Mikrotik RouterOS posee herramientas que ayudan en esos contolres, pero en la medida del posible, se debe restringir al máximo las puertas de entrada para la red que puedan ser utilizados de los potenciales ataques a la capa 2. Preferencialmente nunca permita aceso a la capa 2 por parte de clientes comunes.

→ Cambiar las Redes en capa 2 para Redes enrutadas en principio puede ser dificil, pero las ventajes son muchas. Cambiar de una Red enrutada para MPLS con Mikrotik es muy mas sencillo.

Referencias

→ Articulo de Cisco – Safe Layer 2 Security in depth – versión 2

→Seguridad en Capa 2 – Ing Gabriel Arellano

→ Layer 2 filtering and transparent frewalling – Cedric Blancher

→ Framework for Layer 2 attacks – Andres Berrueta / David Barroso

→ Messing up with WiFi public networks – Cedric Blancher

→ MUM Argentina 2007/ Poland 2008 / Brazil 2009 – Seguridad Iñalambrica

→ Mikrotik WIKI

¡ Gracias !

Wardner Maia – maia@mikrotikbrasil.com.br