

Segurança na camada 2

MUM – Brasil – Novembro de 2009

Eng. Wardner Maia

Introdução

Nome: Wardner Maia

- Engenheiro Eletricista modalidade Eletrotécnica/Eletrônica/Telecomunicações
- Provedor de Internet desde 1995, utilizando rádio frequência para provimento de acesso desde 2000
- Ministra treinamentos em rádio frequência desde 2002 e em Mikrotik desde 2006
- Certificações Mikrotik:
 - Trainer (2007) – Riga, Latvia
 - MTCWE, MTCRE (2008) – Krakow, Poland
 - MTCUME, MTCTE (2009) – Praga, Czech Republik

Introdução

MD Brasil – TI & Telecom

- Operadora de Serviços de Comunicação Multimídia e Serviços de Valor Adicionado
- Distribuidora oficial de Hardware e Software Mikrotik
- Integradora e fabricante de equipamentos com produtos homologados na Anatel.
- Parceira da Mikrotik em treinamentos

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



Público alvo e objetivos da Apresentação

Público alvo:

→ Redes de pequenos/médios provedores de serviço de acesso à Internet e Telecomunicações Wireless ou Cabeados.

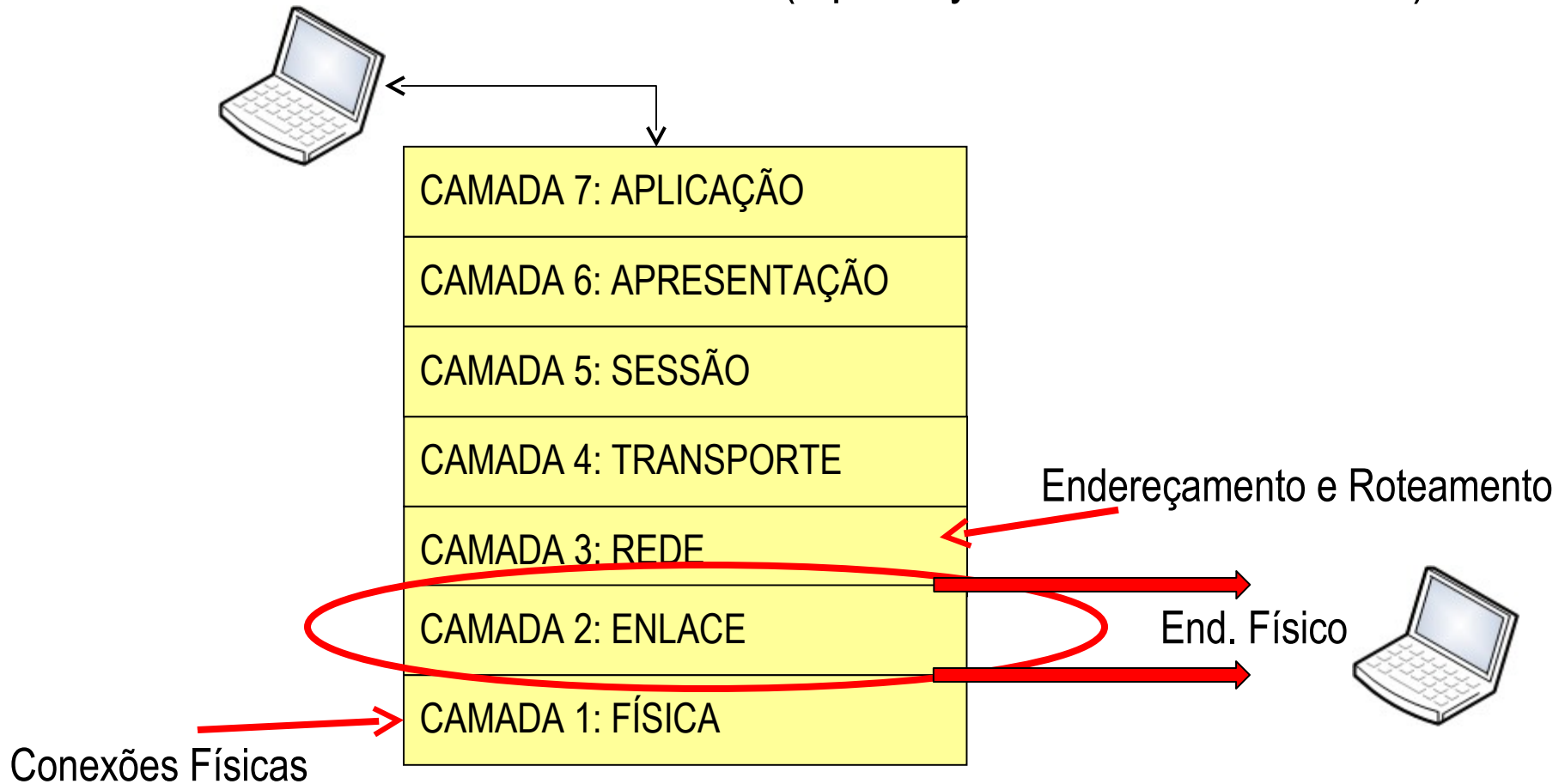
Objetivos:

→ Discutir as topologias de redes mais comuns utilizadas por esses operadores e suas particularidades do ponto de vista de segurança de acesso e disponibilidade da rede.

→ Entender conceitualmente as ameaças existentes na camada 2 vendo na prática demonstrações de suas graves consequências.

→ Discutir e implementar as contramedidas possíveis existentes no Mikrotik RouterOS propondo um conjunto de “melhores práticas” para assegurar a melhor segurança possível nesse nível.

O Modelo OSI (Open Systems Interconnection)





Porque o foco na camada II ?

→ Segurança é uma questão ampla que deve ser analisada sob vários contextos e perspectivas. Do ponto de vista de acesso à rede deve-se garantir a segurança mútua de acesso à rede, tanto do ponto de vista do cliente terminal como do backbone

→ Tendo como referencia o modelo OSI, pode-se dizer que a segurança das camadas superiores sempre depende das camadas inferiores. Uma rede segura precisa garantir além de outras coisas informações coerentes entre a camada 2 (enlace) e a camada 3 (rede)

→ Além dos problemas de segurança de acesso existem inúmeros ofensores a disponibilidade da rede por ataques de negação de serviço que exploram vulnerabilidades inerentes a camada II

→ Medidas de controle efetuadas na camada II ajudam a melhorar o desempenho da rede por filtrar tráfego inútil/indesejado.

AGENDA

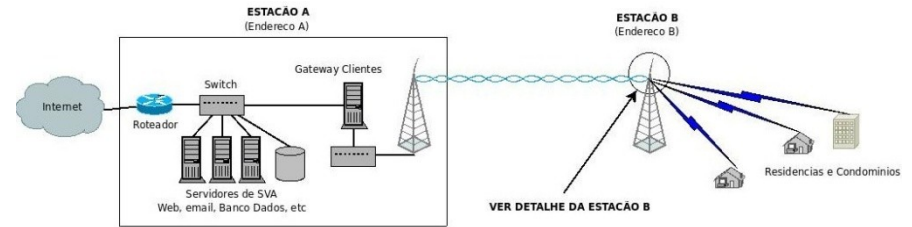


Topologias usuais de redes IP, Bridging, Switching e Firewalls de Camada II

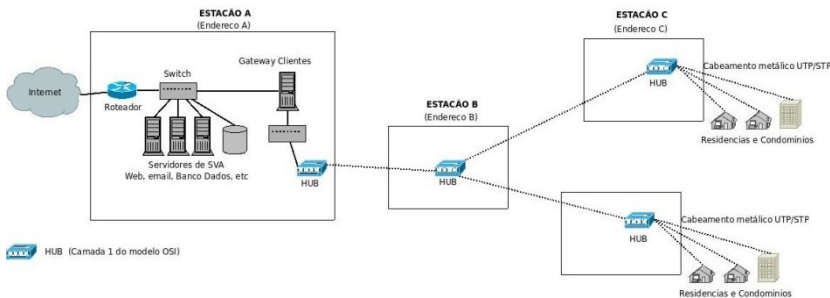
Vulnerabilidades e ataques típicos à camada II:

- Inundação da tabela de Hosts / Tabela CAM e exploração de protocolos de descoberta de vizinhança
- Explorando VLAN's e o Protocolo Spanning Tree
- “Matando de fome” uma rede com DHCP
- Ataques de envenenamento de ARP – Homem do meio
- Atacando usuários e provedores de Hotspot e PPPoE
- Ataques de desautenticação de usuários Wireless

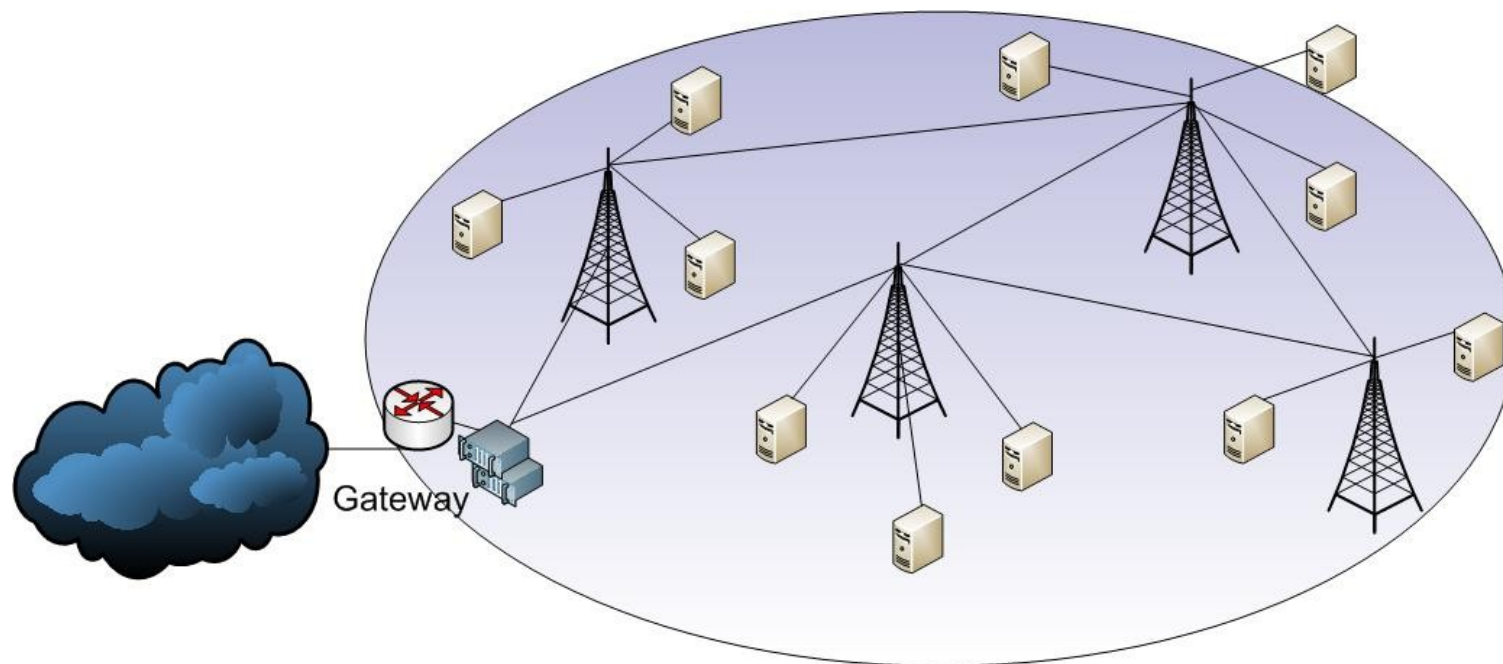
Contra-medidas, melhores práticas e demonstrações em tempo real



Topologias usuais de redes IP, Bridging, Switching e Firewalls de camada II (Filtros de Bridge)



Típica Rede em Camada 2

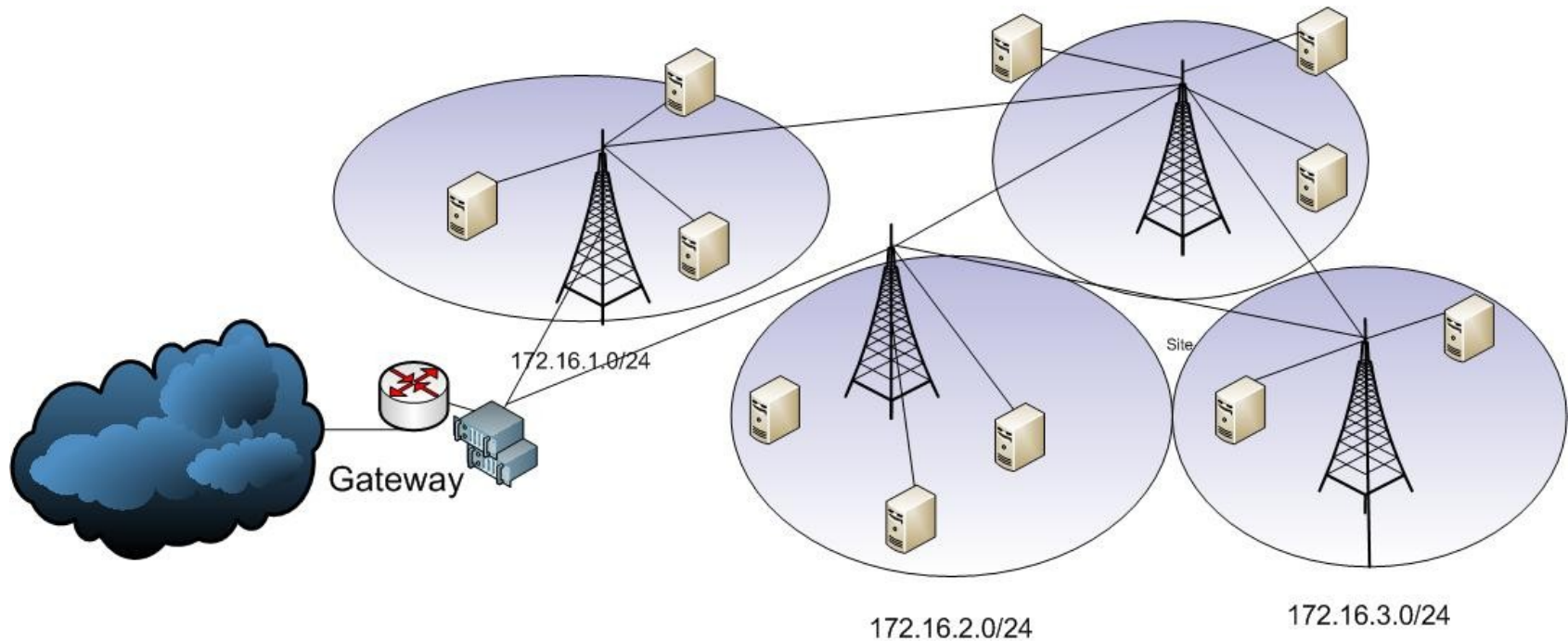


Site

Gateway dos clientes é o Gateway da borda

Somente um domínio de Broadcast

Típica Rede Roteada

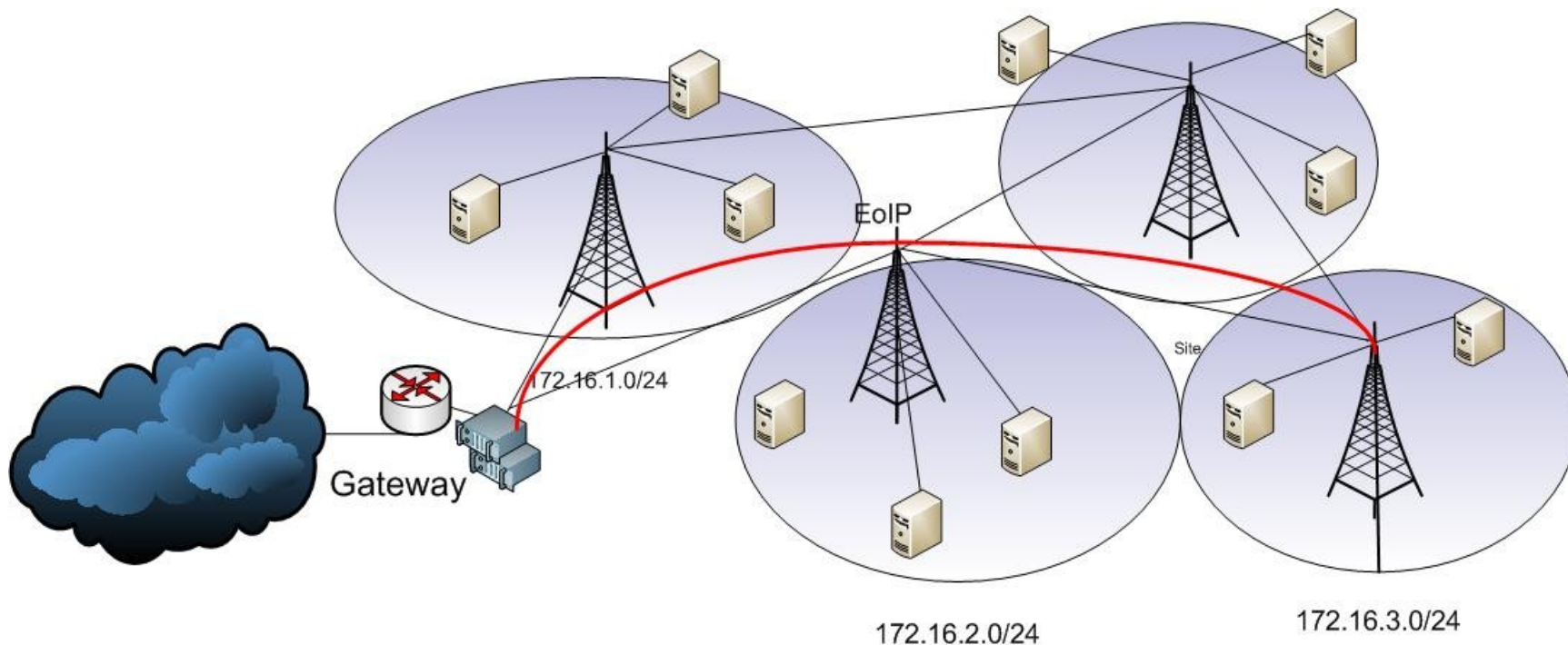


Gateway dos clientes é distribuído e próximo aos clientes

Domínios de broadcast segregados

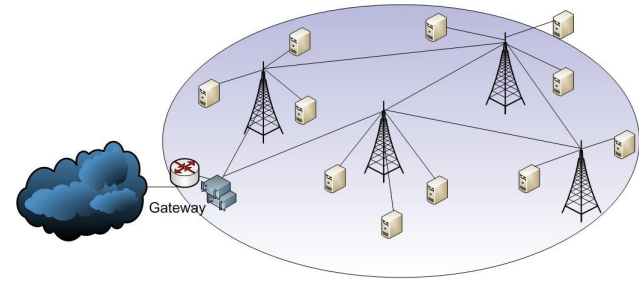
→ Mesmo nas redes roteadas podem haver segmentos em camada 2

Rede Roteada com Concentrador PPPoE “Bridge over Routing”



Uso de protocolo de roteamento dinámico, porém com Túneis transparentes até o concentrador.

Redes em camada 2



Redes em ATM, Frame Relay, MPLS (camada “2.5”), etc

Vamos abordar

Redes IP em Bridge:

→ Redes com IP fixo

→ DHCP

→ Hotspot

→ Mistas com Bridge sobre roteamento

Redes Inteiramente em camada 2 com 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,

APLICAÇÃO
APRESENTAÇÃO
SESSÃO
TRANSPORTE
REDE
ENLACE
FÍSICA

Bridge
Switch

Switching

→ O switch mantém uma tabela com os MAC's conectados a ela, relacionando-os com a porta que foram "aprendidos".

→ Quando um MAC não existe na tabela, ele é procurado em todas as portas, comportando-se a switch como um HUB.

→ O espaço (Host table ou CAM table) é limitado e quando preenchido totalmente faz com que a switch comporte-se como um HUB !

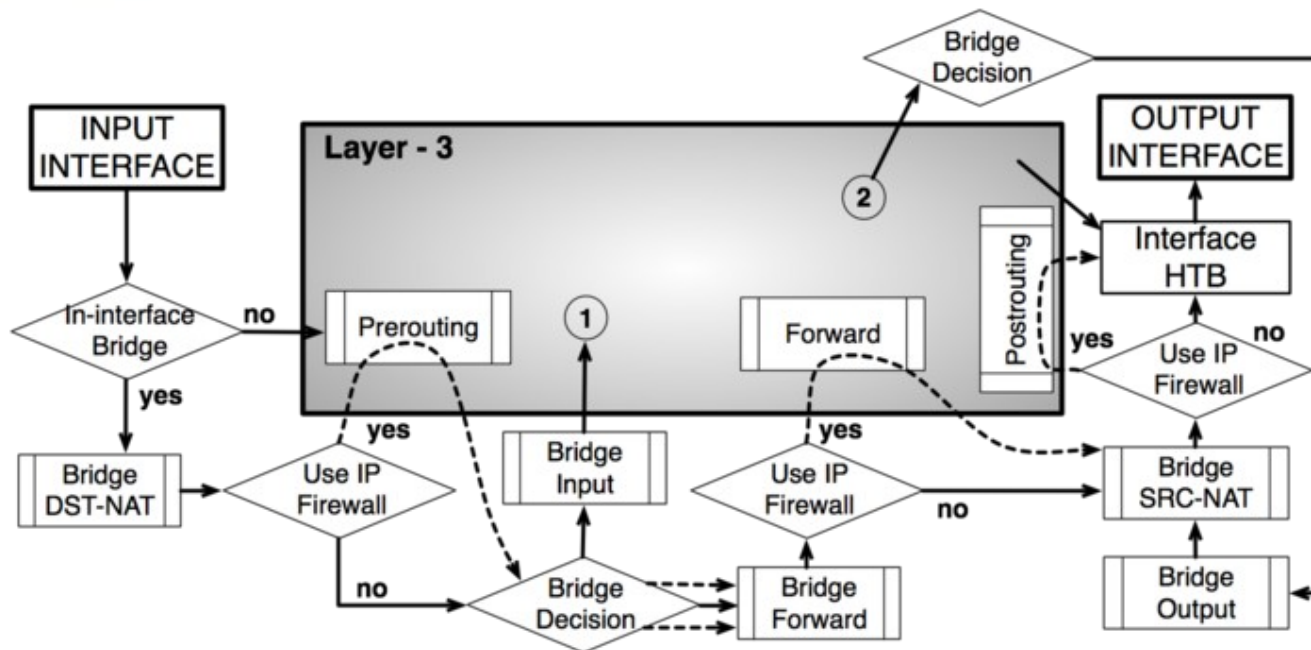
Feature	Atheros8316	Atheros7240	ICPlus175D	Other
Port Switching	yes	yes	yes	yes
Port Mirroring	yes	yes	yes	no
Host table	2k entries	2k entries	no	no
Vlan table	4096 entries	16 entries	no	no
Rule table	32 rules	no	no	no

(RB450G)

(RB750)

(RB450)

Filtros de camada 2



Chain: forward

Chain: input

Chain: forward

Chain: output

Action: accept

Action: accept

Action: drop

Action: jump

Action: log

Action: mark packet

Action: passthrough

Action: return

Action: set priority

Chain: srcnat

Chain: dstnat

Chain: srcnat

Action: accept

Action: accept

Action: arp-reply

Action: drop

Action: dst-nat

Action: jump

Action: log

Action: mark packet

Action: passthrough

Action: redirect

Action: return

Action: set priority

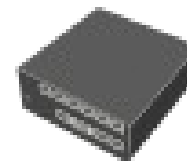
Action: src-nat

Atacando a camada 2

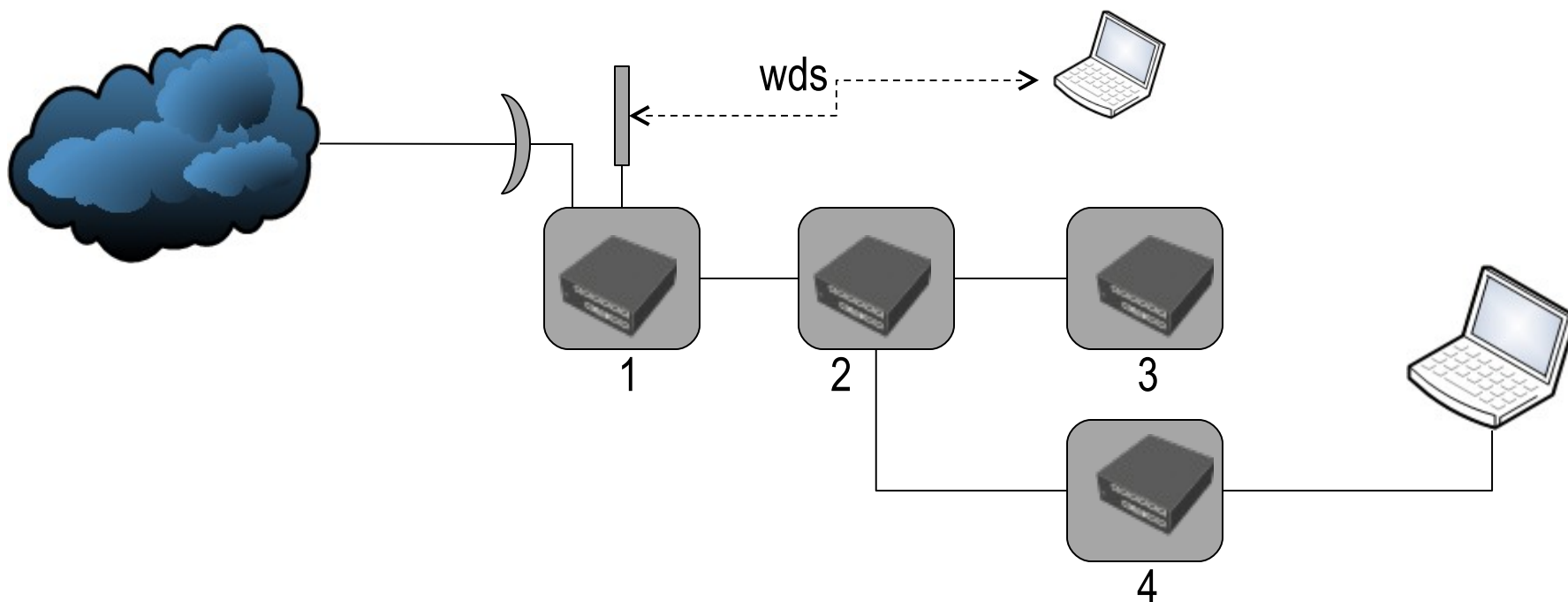
Inundação da Tabela de Hosts (MAC Flooding)



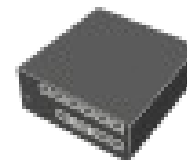
Ataques a switches e bridges Inundação da tabela de hosts



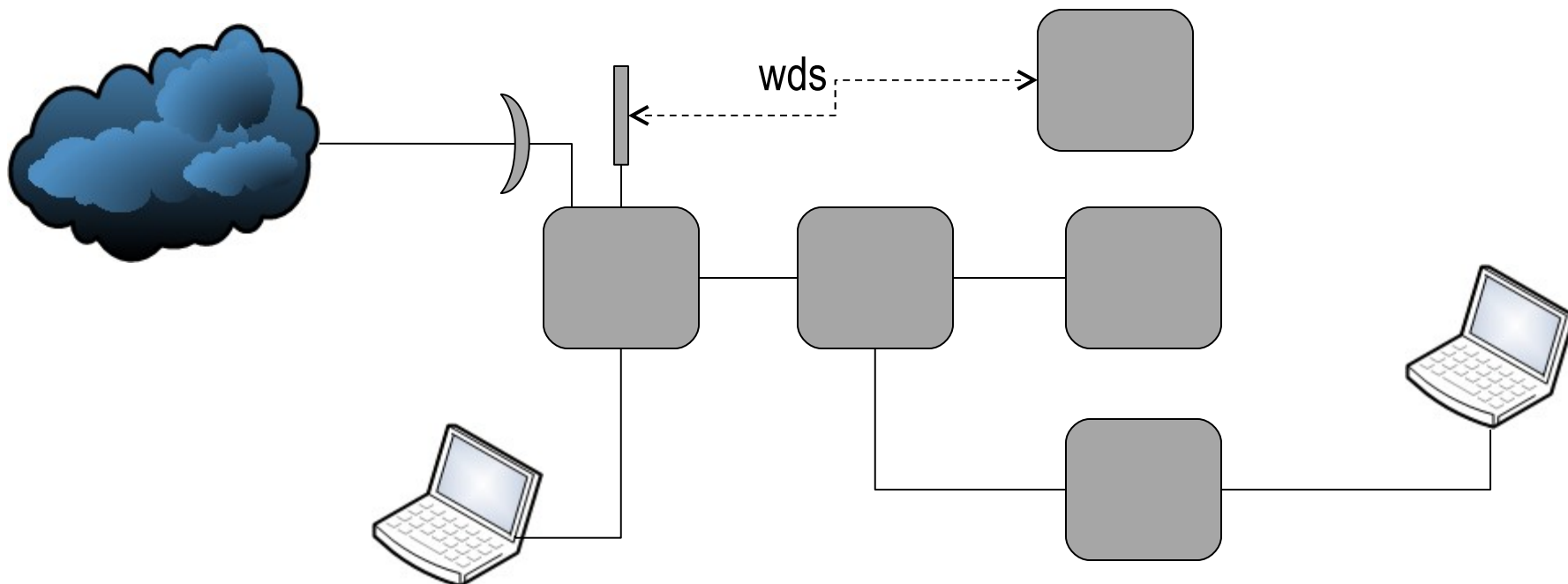
Existem ferramentas de extrema simplicidade de instalação desenvolvidas para programas para “auditoria de segurança de redes” que executam o flood de MAC’s em redes em bridge.



Ataques a switches e bridges Inundação da tabela de hosts

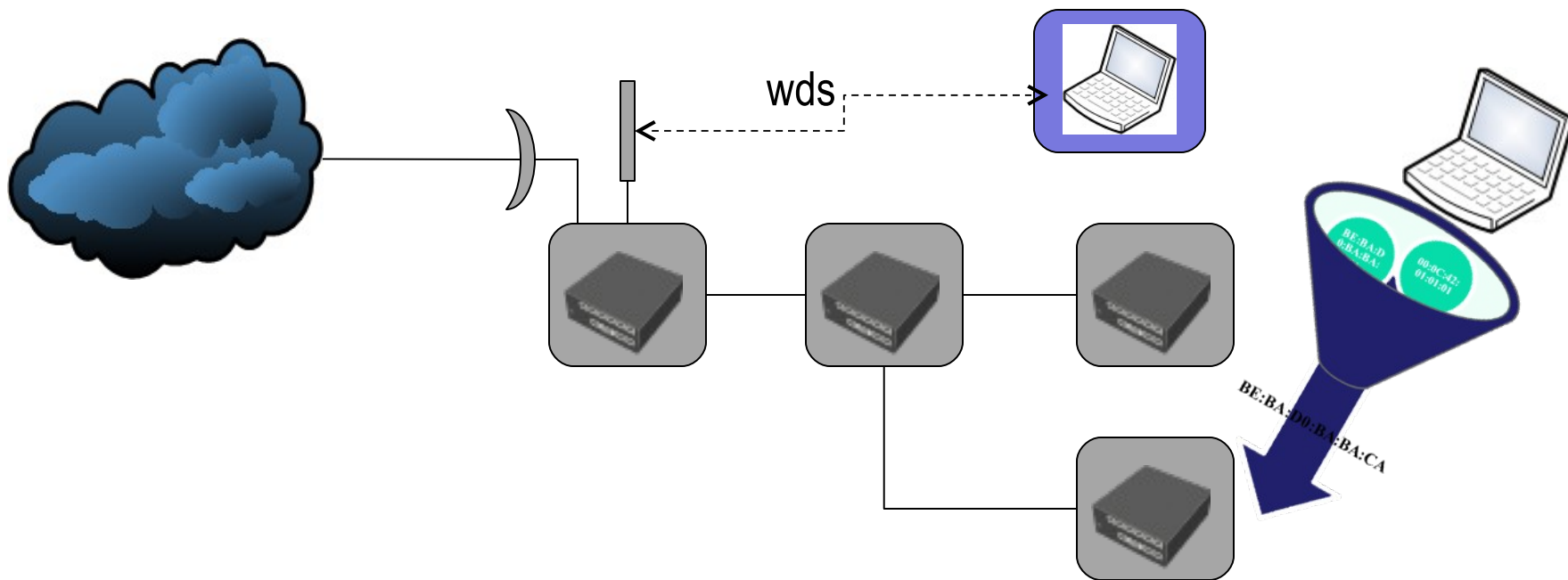


Existem ferramentas de extrema simplicidade de instalação desenvolvidas para programas para “auditoria de segurança de redes” que executam o flood de MAC’s em redes em bridge.



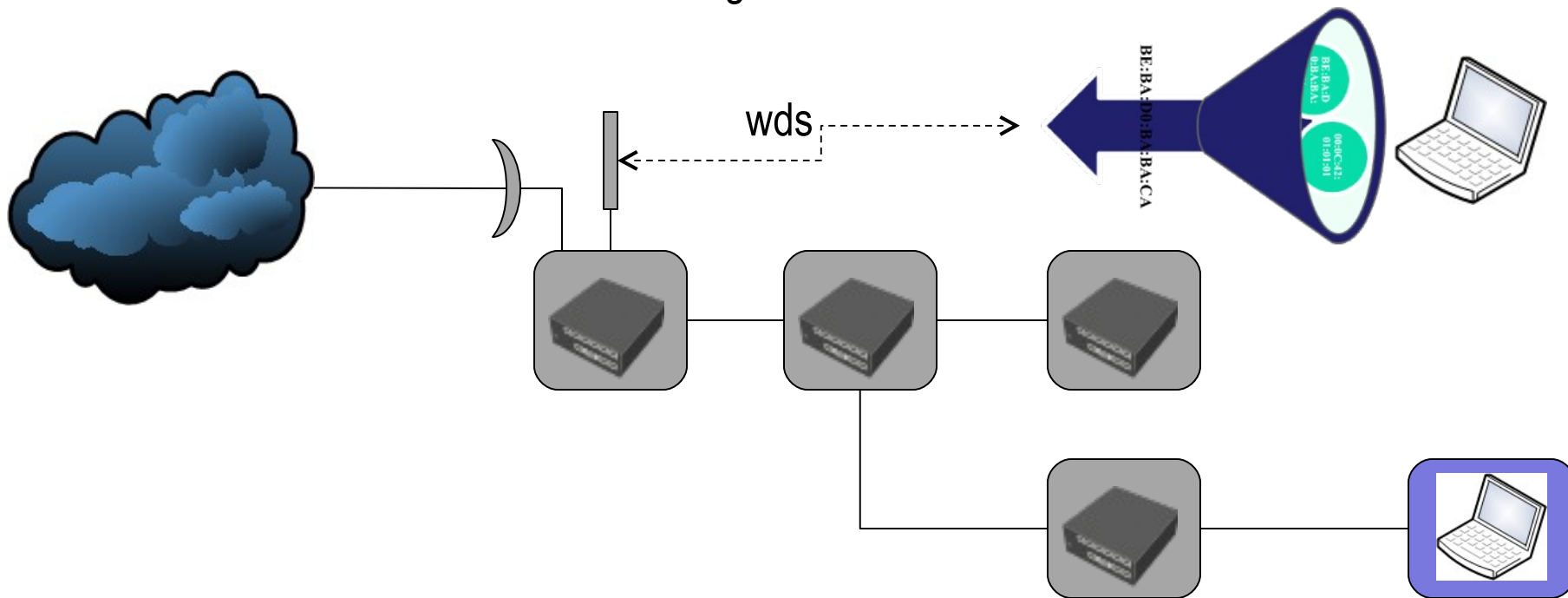
Ataques a switches e bridges Inundação da tabela de hosts

Existem ferramentas de extrema simplicidade de instalação desenvolvidas para programas para “auditoria de segurança de redes” que executam o flood de MAC’s em redes em bridge.



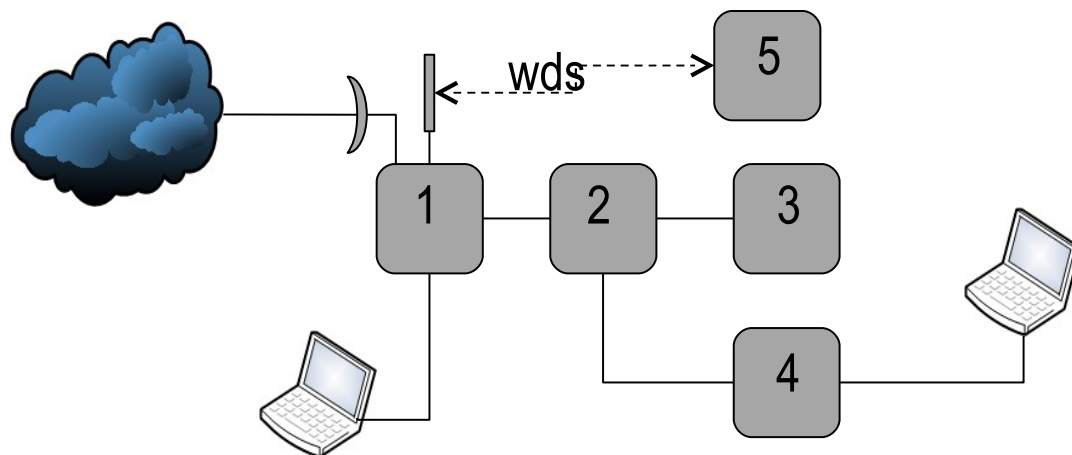
Ataques a switches e bridges Inundação da tabela de hosts

Existem ferramentas de extrema simplicidade de instalação desenvolvidas para programas para “auditoria de segurança de redes” que executam o flood de MAC’s em redes em bridge.



Inundação da Tabela de Hosts (Mac Flooding)

DEMO



- Disparando o ataque a partir de 4
- Verificando o efeito em todos os outros
- Protegendo somente 4
- Protegendo 4 e os outros

Ataques a switches e bridges Contra medidas

Switches:

→ O ataque não causa DoS, mas uma vez lotada a CAM table a Switch comporta-se como HUB

→ Quando utilizadas como switches, não há o que se fazer para prevenir esses ataques a não ser não dar acesso em camada 2 aos possíveis atacantes.

→ Uma feature como “port security” existente nas switches Cisco seria desejável para o Mikrotik RouterOS.

Ataques a switches e bridges Contra medidas

Bridges:

→ Setando a(s) porta(s) para External FDB (Forwarding DataBase) a tabela de hosts não será carregada (para a(s) porta(s) setadas).

→ Essa medida evita o DoS no equipamento em questão mas não nas outras bridges a ele ligados. O flood será feito para todas as portas.

→ Felizmente uma vez aceitos os MAC's atacantes, é possível filtrar a propagação dos mesmos.

General | Status

Interface: ether1

Bridge: bridge1

Priority: 80 hex

Path Cost: 10

Horizon: [dropdown]

Edge: auto

Point To Point: auto

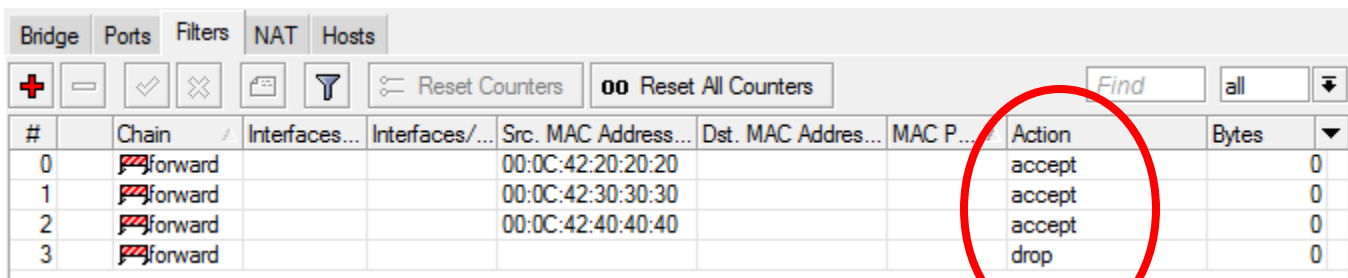
External FDB: yes

Ataques a switches e bridges Contra medidas

Mas quais filtros executar ?

→ O ideal seria somente aceitar os MAC's realmente conhecidos e que fazem parte da rede.

→ Como isso nem sempre é possível, pode-se escrever um script para ativa-los "on the fly" quando e se a tabela de hosts crescer de forma anômala..



#	Chain	Interfaces...	Interfaces/...	Src. MAC Address...	Dst. MAC Address...	MAC P...	Action	Bytes
0	forward			00:0C:42:20:20:20			accept	0
1	forward			00:0C:42:30:30:30			accept	0
2	forward			00:0C:42:40:40:40			accept	0
3	forward						drop	0

Atacando a camada 2

Explorando Protocolos de
“Descoberta de Vizinhança”

"Lo peor es que
el empeoramiento
empieza a empeorar"

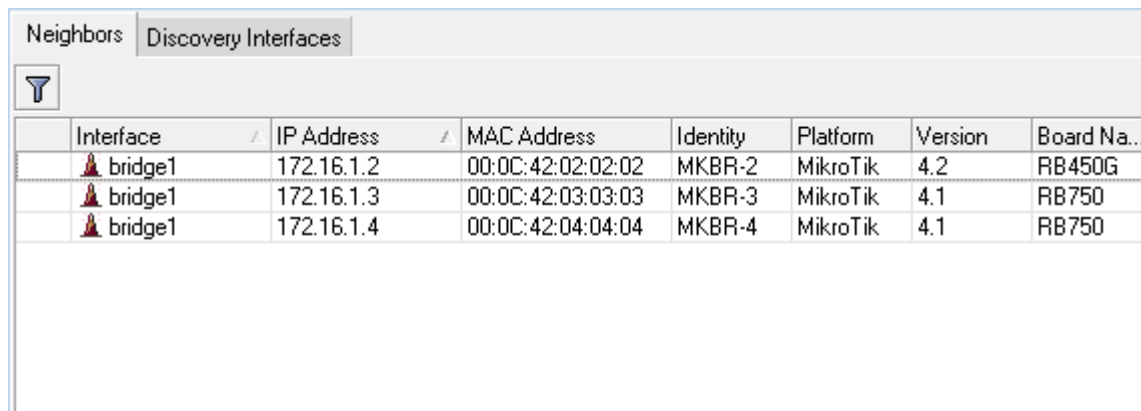


Explorando protocolos de “Descoberta de vizinhança”

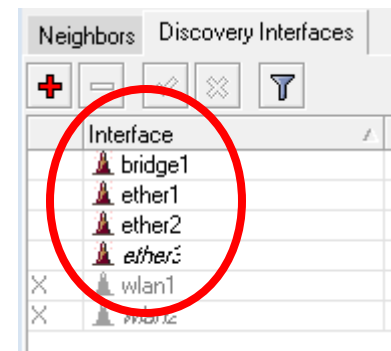
→ Protocolos de descoberta de vizinhança auxiliam nas tarefas administrativas e de controle de rede.

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

→ Utiliza protocolo UDP, porta 5678 que é divulgada por broadcast a cada 60 segundos em cada interface.



Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...
bridge1	172.16.1.2	00:0C:42:02:02:02	MKBR-2	MikroTik	4.2	RB450G
bridge1	172.16.1.3	00:0C:42:03:03:03	MKBR-3	MikroTik	4.1	RB750
bridge1	172.16.1.4	00:0C:42:04:04:04	MKBR-4	MikroTik	4.1	RB750



Interface
bridge1
ether1
ether2
ether3
wlan1
wlan2

Explorando protocolos de “Descoberta de vizinhança”

Memory: 93.6 MB CPU: 100% Hide Passwords

Neighbor List

Neighbors Discovery Interfaces

Interface	IP Address	MAC Address	Identity
bridge1	0.9.158.115	10:23:7A:1D:07:0E	3YC8P4Y
bridge1	0.10.151.122	68:43:3D:48:9C:D0	ROMIZDD
bridge1	0.14.242.30	A2:9F:CC:06:32:90	K3FBS7D
bridge1	0.15.98.50	86:44:43:24:AC:14	5A7J2XA
bridge1	0.23.35.92	C8:38:A0:5F:C9:2B	3GXTB7K
bridge1	0.52.49.11	E2:55:60:65:1D:A4	B7K3XBT
bridge1	0.55.26.46	46:78:4A:76:F8:7D	QLZ4CQ9
bridge1	0.58.197.86	CE:24:40:26:15:F4	C9PL7GC
bridge1	0.70.85.0	F2:56:12:21:F3:FD	RONI1V0
bridge1	0.86.80.73	B6:4A:20:10:6D:D1	4HCU94
bridge1	0.98.36.92	AC:25:24:5E:E5:8E	FASQ2XS
bridge1	0.98.177.28	BC:C4:04:05:9D:19	4YCUP4L
bridge1	0.101.225.40	30:F5:F2:59:0B:1C	TB7K3XB
bridge1	0.104.50.31	00:BE:C8:21:6E:51	GUQ8LHh
bridge1	0.109.219.41	78:05:E7:5F:05:15	KGUB83G
bridge1	0.141.51.66	7C:E0:D8:14:70:AE	RM11DR0
bridge1	0.151.57.10	18:1E:85:31:3C:DE	IEW061I
bridge1	0.179.179.88	9E:96:A5:1D:58:C5	LGUB83G
bridge1	0.242.252.88	A6:C6:9F:0F:26:59	9MHZC9C
bridge1	1.16.84.120	98:EC:5A:64:2A:87	3FXTA7F
bridge1	1.21.2.2	1C:F9:16:1F:C5:71	05M1VDF
bridge1	1.35.238.28	C2:6C:D6:77:E5:F3	NIWE0NJ
bridge1	1.38.251.107	52:5A:10:17:B5:E2	CQL4HCL
bridge1	1.72.30.90	0E:D1:C3:4F:B5:57	MZHDQ9I

4539 items

→ Ferramentas de ataque disponíveis na Internet atacam tanto Mikrotik RouterOS como Cisco CDP

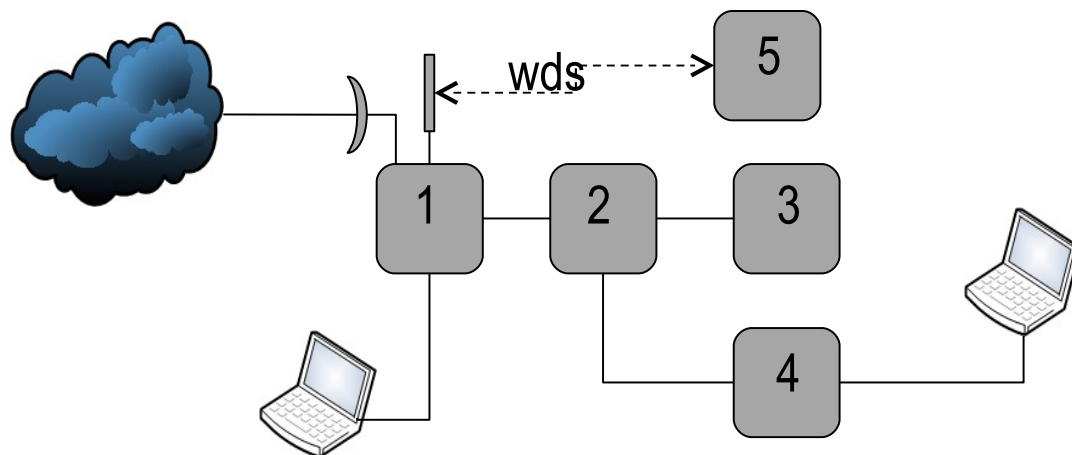
→ Essas ferramentas podem ser usadas somente para obter informações da rede e equipamentos ou causa DoS.

→ O ataque pode ser disparado de qualquer porta da bridge contaminando todos os equipamentos da rede.

15 segundos de ataque em uma RB433AH

Exploração de Protocolos de Descoberta de Vizinhança

DEMO



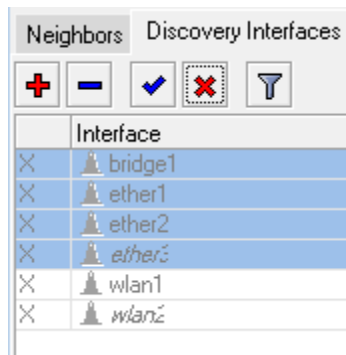
- Disparando o ataque a partir do equipamento 4
- Verificando o efeito em 1
- Tomando as medidas preventivas em 1
- Fazendo os filtros em 4

Contra medidas para ataques baseados em protocolos de “Descoberta de vizinhança”

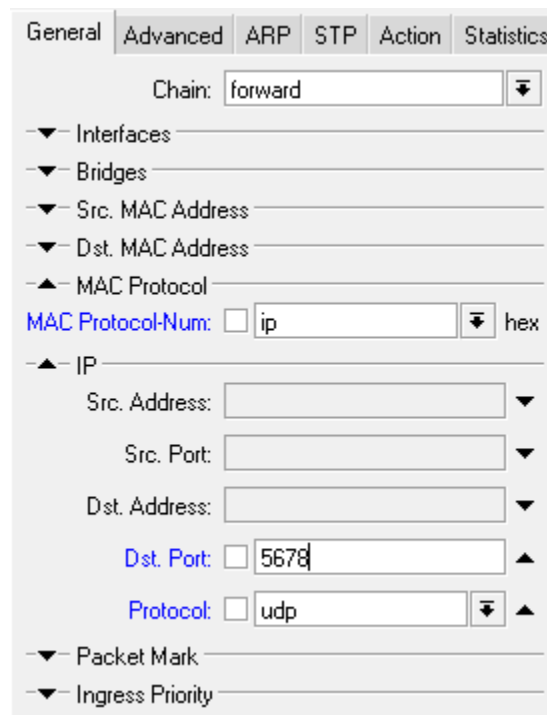
→ Desabilitar o MNDP em todas as interfaces

→ Mesmo como o MNDP bloqueado, o tráfego gerado por tentativas desse tipo de ataque existirá. Bloquear a porta UDP 5678 em todos os filtros de bridge pode ajudar a evitar esse tráfego

→ Lembrar que toda Interface ethernet-like (EoIP, IPIP, PpPp estática, etc) tem por default o MNDP habilitado.



Neighbors		Discovery Interfaces	
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



General Advanced ARP STP Action Statistics

Chain: forward

Interfaces

Bridges

Src. MAC Address

Dst. MAC Address

MAC Protocol

MAC Protocol Num: ip hex

IP

Src. Address:

Src. Port:

Dst. Address:

Dst. Port: 5678

Protocol: udp

Packet Mark

Ingress Priority

Atacando a camada 2

Matando “de fome” Redes com DHCP
(DHCP Starvation)



Fundamentos do DHCP

O protocolo DHCP é executado em 4 fases:

1) O Cliente procura em seu barramento físico um 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) O Servidor de DHCP oferece (e reserva durante um tempo) um IP ao 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 do DHCP

3) O cliente requisita (aceita) o IP oferecido

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) O Servidor confirma a atribuição do 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

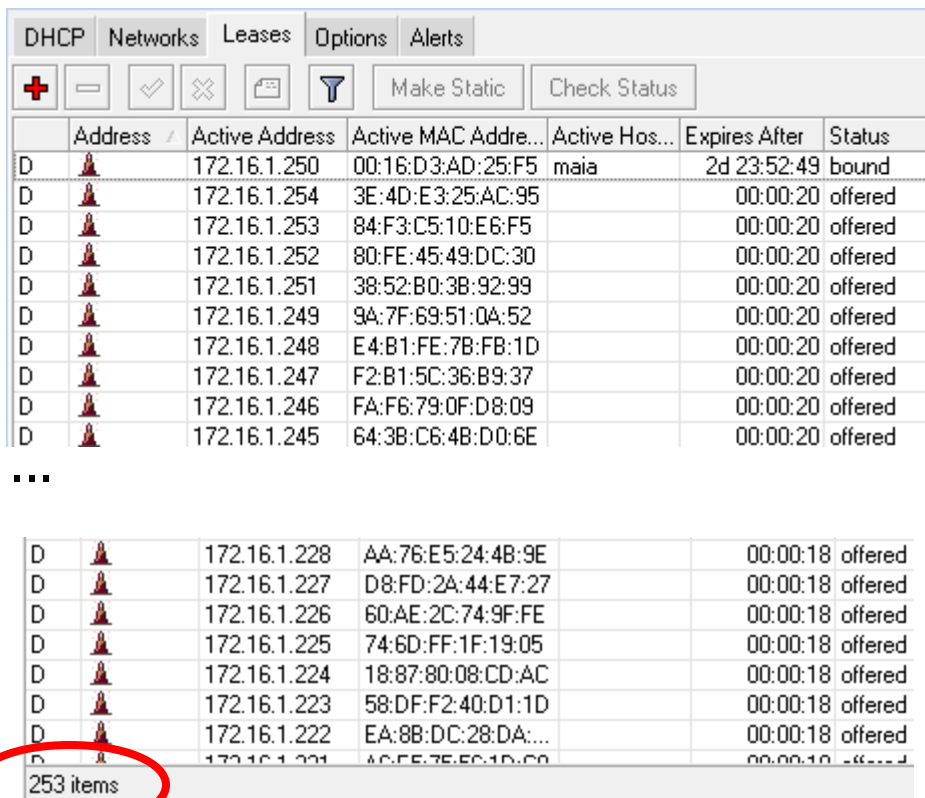
Ataques contra o DHCP

Existem dois tipos de ataques de “Starvation” do DHCP conhecidos:

- 1) O atacante gera inúmeros pedidos de DHCP e cumpre todas as fases do processo até obter os IP's
- 2) O atacante gera inúmeros pedidos de DHCP mas não os confirma

Tanto um como outro ataque utilizam MAC's gerados aleatoriamente e causam a negação do serviço pelo esgotamento dos IP's disponíveis. O ataque de tipo 1 é mais lento e mais persistente e do tipo 2 é mais rápido e tem de ser feito continuamente visto que o tempo de “offer” é pequeno.

Matando “de fome” redes com DHCP (DHCP starvation)



	Address	Active Address	Active MAC Address	Active Host	Expires After	Status
D	172.16.1.250	00:16:D3:AD:25:F5	maia		2d 23:52:49	bound
D	172.16.1.254	3E:4D:E3:25:AC:95			00:00:20	offered
D	172.16.1.253	84:F3:C5:10:E6:F5			00:00:20	offered
D	172.16.1.252	80:FE:45:49:DC:30			00:00:20	offered
D	172.16.1.251	38:52:B0:3B:92:99			00:00:20	offered
D	172.16.1.249	9A:7F:69:51:0A:52			00:00:20	offered
D	172.16.1.248	E4:B1:FE:7B:FB:1D			00:00:20	offered
D	172.16.1.247	F2:B1:5C:36:B9:37			00:00:20	offered
D	172.16.1.246	FA:F6:79:0F:D8:09			00:00:20	offered
D	172.16.1.245	64:3B:C6:4B:D0:6E			00:00:20	offered
...						
D	172.16.1.228	AA:76:E5:24:4B:9E			00:00:18	offered
D	172.16.1.227	D8:FD:2A:44:E7:27			00:00:18	offered
D	172.16.1.226	60:AE:2C:74:9F:FE			00:00:18	offered
D	172.16.1.225	74:6D:FF:1F:19:05			00:00:18	offered
D	172.16.1.224	18:87:80:08:CD:AC			00:00:18	offered
D	172.16.1.223	58:DF:F2:40:D1:1D			00:00:18	offered
D	172.16.1.222	EA:8B:DC:28:DA:...			00:00:18	offered
D	172.16.1.221	AC:55:75:5C:1D:00			00:00:18	offered
253 items						

→ O ataque baseia-se em mandar pacotes de dhcp discovery para todos os hosts da rede, fazendo com que o DHCP ofereça os mesmos.

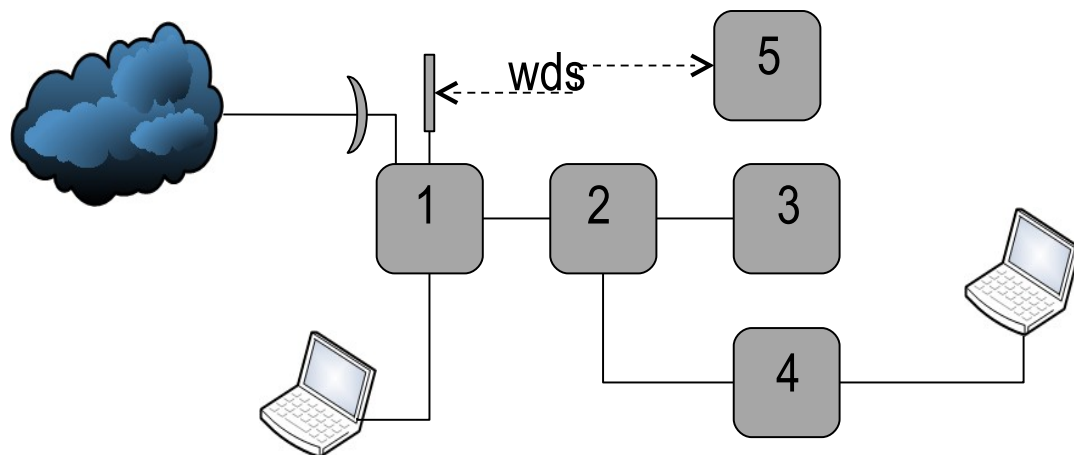
→ Nesse momento pode-se levantar um DHCP falso atribuindo outros IP's, gateways, DNS's, etc.

→ Alternativamente pode-se aceitar os IP's mantendo o DHCP sem mais IP's para entrega

Menos de 5 segundos de ataque esgota uma classe C !

“Matando de fome” Redes com DHCP” (DHCP Starvation)

DEMO



- Disparando os ataques de tipo 1 e 2 a partir do host 4
- Observando o efeito em 1 (Servidor de DHCP)

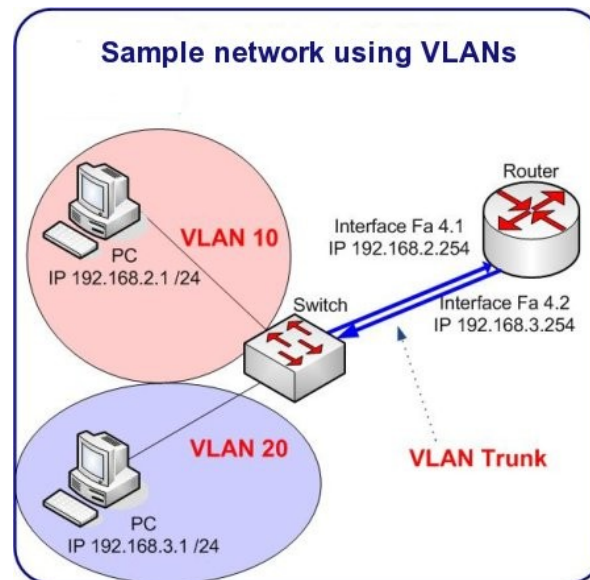
DHCP Starvation Contra medidas

- Filtros permitindo passar somente os MAC's conhecidos
- Leases estáticos no DHCP
- Considerar a possibilidade de utilizar DHCP ou User Manager



Atacando a camada 2

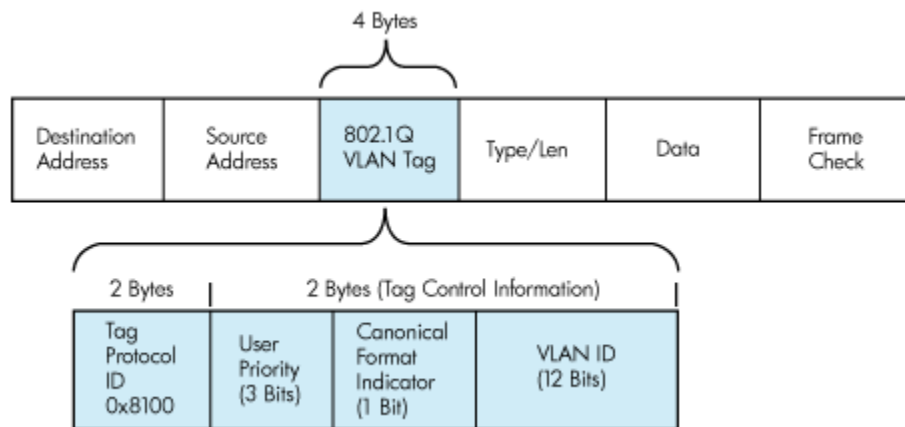
Explorando Vlan's



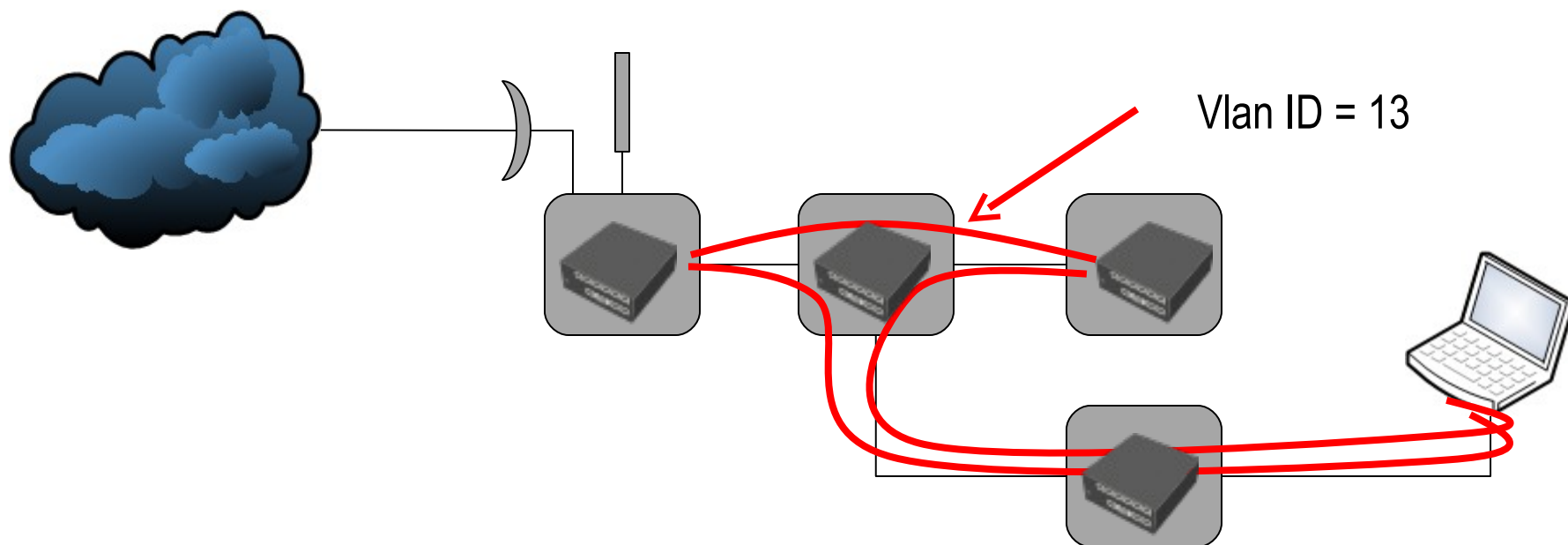
VLAN's

Uma Vlan é um grupo de hosts que comunicam-se entre si como se estivessem no mesmo domínio de broadcast independente da localização física. Podem ser utilizadas para muitas funções em uma rede, como:

- Criação de várias redes de camada 3 sobre um dispositivo de camada 2
- Segmentação de tráfego e limitação de domínios de Broadcasts
- Possibilidade de aplicar regras de QoS individualizadas
- Manutenção remota sem interferir na rede ativa
- Segurança ?



Explorando as VLAN's

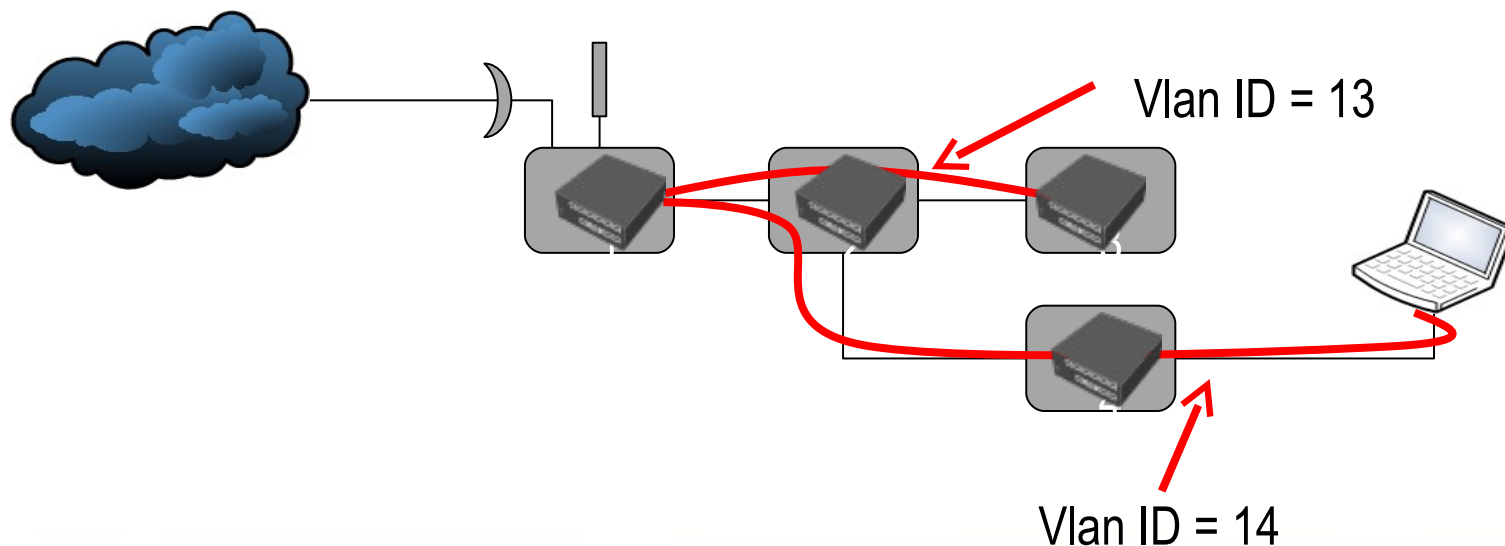


→ A primeira fragilidade é óbvia pois não havendo qualquer cuidado para filtrar, qualquer host que tenha a mesma Vlan Tag ID pode fazer parte da Vlan

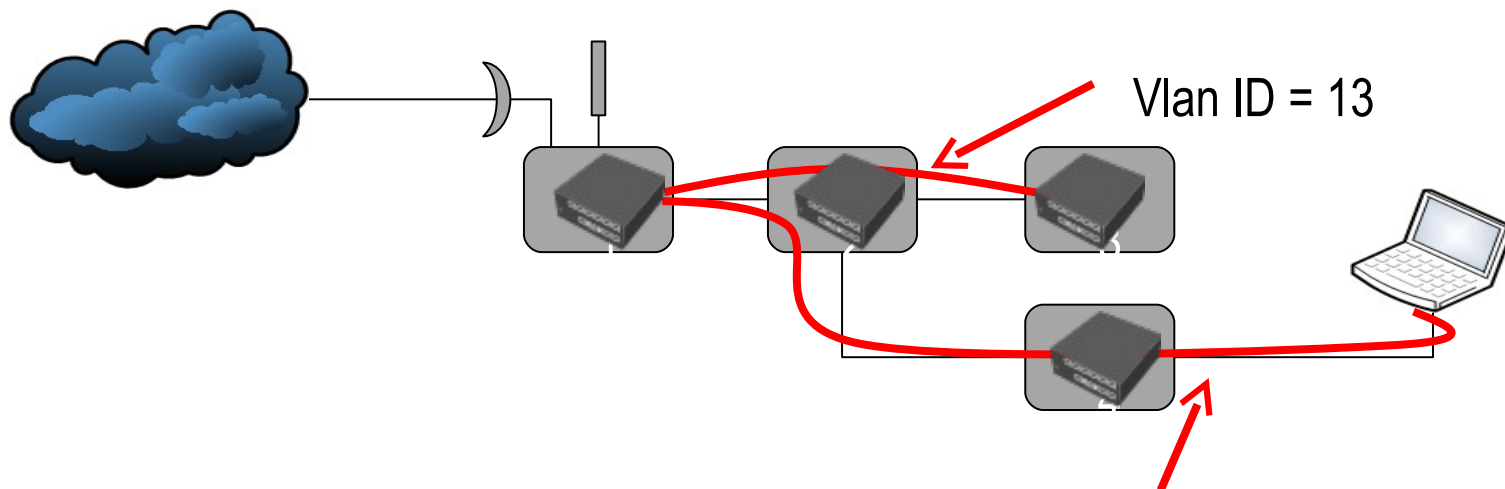
Explorando as VLAN's

→ Ataque de “rótulo duplo” (double tagging) em Vlan's

- O atacante forma um pacote com a Vlan Tag ID = 13 (Vlan a qual ele não pertence), encapsulado com a Vlan Tag ID = 14 (a qual ele pertence)
- A switch (bridge) retira a Tag 14 mandando o pacote para a Vlan 13
- O ataque é também unidirecional.



Ataques a Vlan's DEMO



- Restringindo a participação em uma Vlan
- Ataque unidirecional de rótulo duplo

Explorando VLAN's Contra medidas

General Advanced ARP STP Action Statistics

Chain:

▼ Interfaces

▼ Bridges

▼ Src. MAC Address

▼ Dst. MAC Address

▲ MAC Protocol

MAC Protocol-Num:

▼ IP

▼ Packet Mark

▼ Ingress Priority

→ Sendo o VLAN ID o único parametro a ser configurado em uma VLAN, a única medida é bloquear o MAC Protocolo 8100 – Vlan's em todas as portas de entrada da rede;

→ O bloqueio de ataques de proxy de Vlan's só podem ser controlados através de listas de acesso de MAC's.

General Advanced ARP STP Action Statistics

Action:

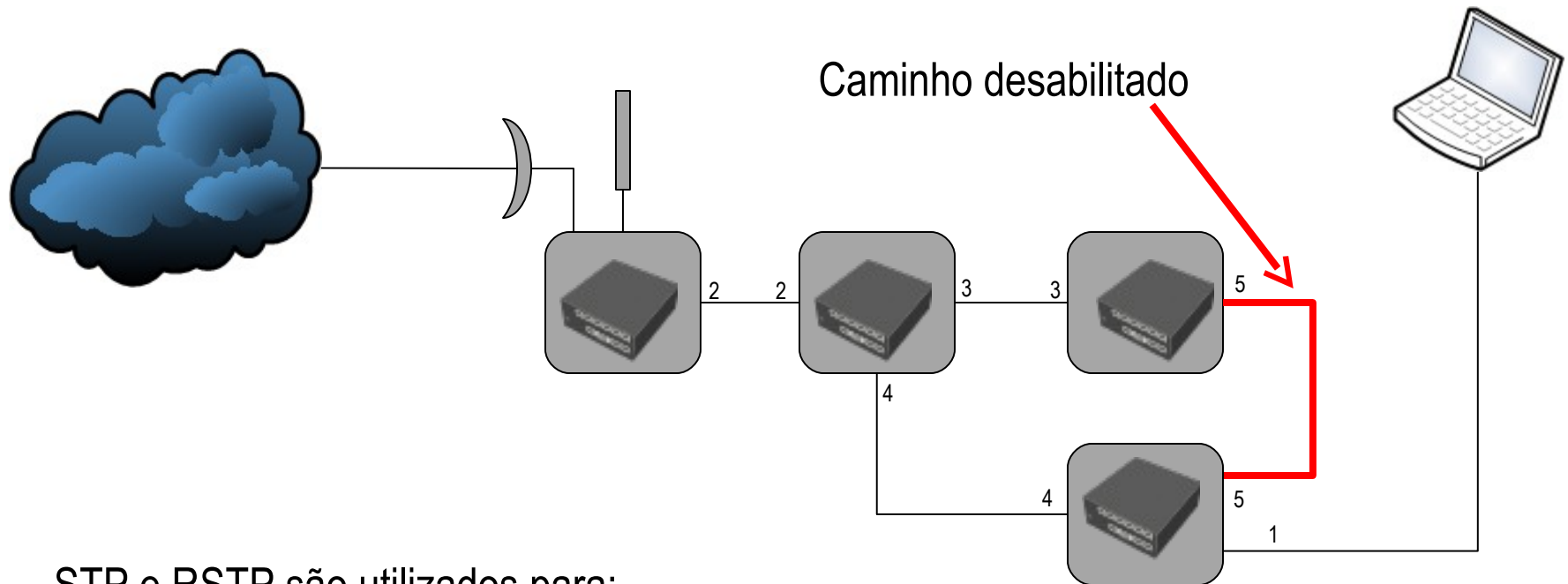
→ O Bloqueio de ataques de rótulo duplo podem ser controlados através de lista de acesso de MAC's e poderiam ser pelo exame do conteúdo dos pacotes IP na camada 3

Atacando a camada 2

Explorando o Spanning Tree



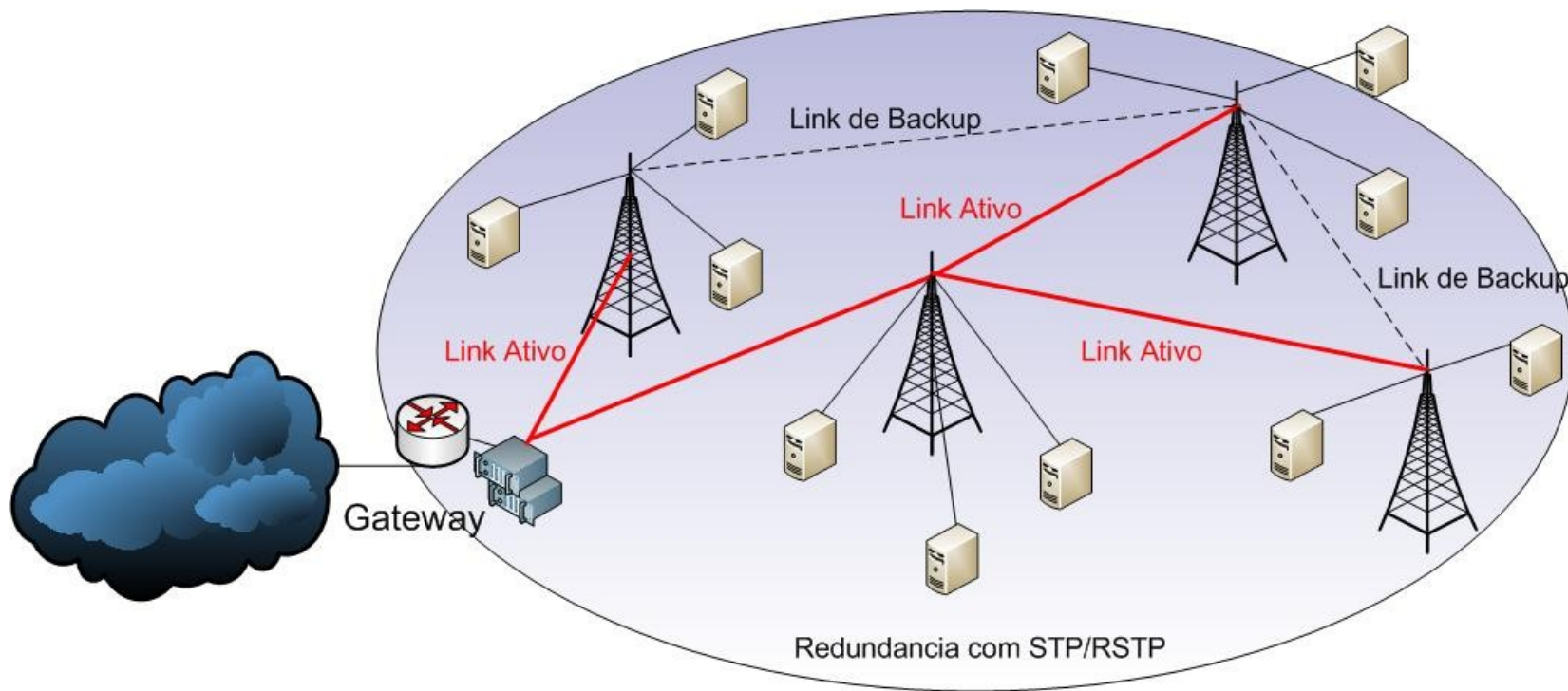
Aplicações do Spanning Tree



STP e RSTP são utilizados para:

- Evitar a formação de loops em redes em Bridge
- Possibilitar topologias com redundancia de caminhos

Aplicações do Spanning Tree



Princípios de funcionamento do STP

- As bridges participantes do Spanning Tree elegem entre si uma bridge root (normalmente a de menor Bridge ID)
- Cada dispositivo calcula o menor caminho a partir de si para a bridge root
- Para cada bridge é eleita uma porta root, que tem o menor caminho para a bridge root
- Os dispositivos trocam entre si mensagens de BPDU (Bridge Protocol Data Unit)



←

{ Protocol ID
Version
BDOU Type
Flags

Port ID
Message Age
Hello Time
Forw Delay

→

Princípios de funcionamento do STP

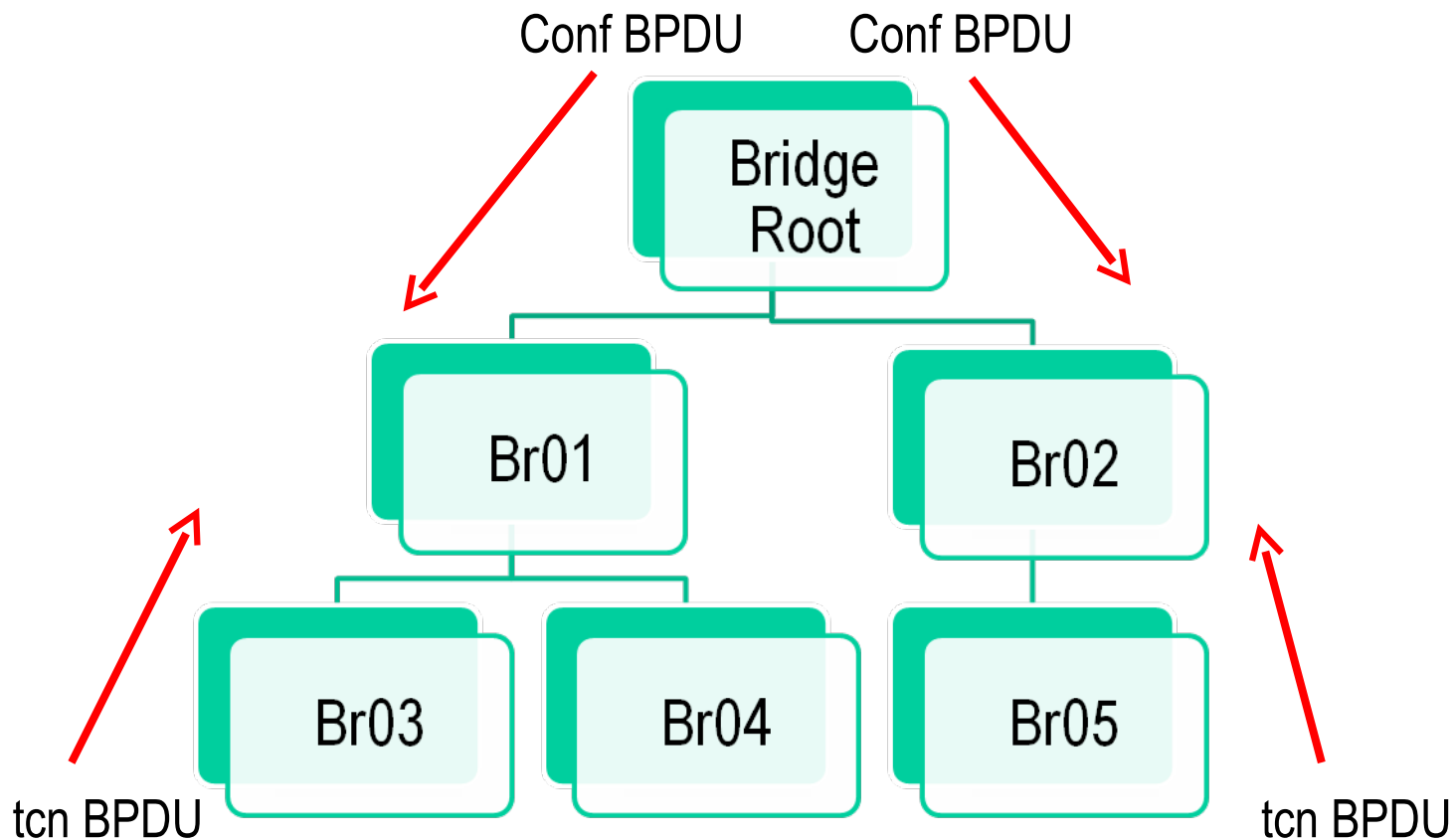
→ Uma vez eleita a Bridge Root, esta passa a anunciar periodicamente mensagens de configuração que são repassadas pelas bridges participantes do STP com seu próprio MAC como MAC de origem. (conf BPDU)

→ Quando ocorre uma mudança na topologia em qualquer segmento da rede, a bridge responsável por esse segmento envia mensagens comunicando essa mudança (tcn BPDU – Topology Change Notification BPDU)

				Root ID	Root Path Cost	Bridge ID					
--	--	--	--	---------	----------------	-----------	--	--	--	--	--

Protocol ID	Version	Mes. Type
-------------	---------	-----------

Princípios de funcionamento do STP



Spanning Tree x Rapid Spanning Tree (RSTP)

- RSTP foi proposto pelo IEEE 802.1w para fazer frente a uma necessidade de mais velocidade de resposta a adaptação de mudanças de topologia

- RSTP trabalha com o conceito de estados das portas. Uma porta pode estar:
 - Desconhecida (quando o estado ainda não foi determinado)
 - Alternativa (não faz parte da topologia ativa no momento – backup)
 - Designada (quando a porta está designada para uma lan a ela conectada)
 - Root (caminho para a bridge root)

- As mensagens de BPDU no RSTP incorporam o estado das portas e uma série de modificações em relação ao STP que tornam o protocolo bem mais rápido. No entanto RSTP é compatível com STP.

Segurança com STP e RSTP

Tanto STP como RSTP tem características que proporcionam a possibilidade de ataques diversos, sendo que a raiz do problema é a inexistência de autenticação nas mensagens de BPDU

Assim é possível praticar ataques diversos tanto de DoS como de MiTM, fazendo:

- Flooding de mensagens de conf BPDU
- Flooding de mensagens de tcn BPDU
- Flooding de mensagens BPDU assumindo o papel de bridge root
- Ataque de homem do meio quando se tem acesso a duas bridges da topologia.

Atacando o Spanning Tree

→ Atacante mandando uma mensagem 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 uma mensagem 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 baseado em muitas mensagens 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 baseado em muitas mensagens 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 o Spanning Tree

→ Atacante assumindo o 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
```

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

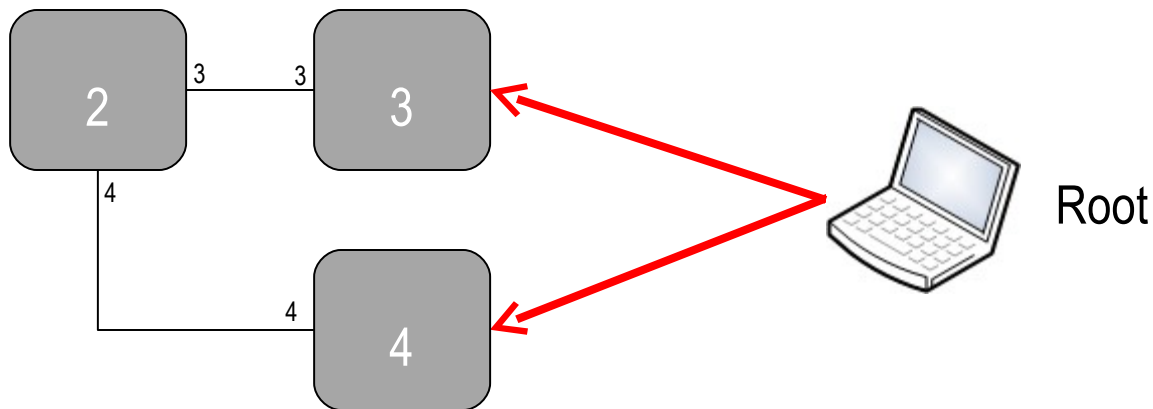
Interface	Bridge	Priority (h...)	Path Cost	Horizon	Role	Root Pat...
ether1	bridge1	80	10		root port	20
ether2	bridge1	80	10		disabled port	
ether3	bridge1	80	10		disabled port	
ether4	bridge1	80	10		designated port	
ether5	bridge1	80	10		disabled port	

Atacando o Spanning Tree

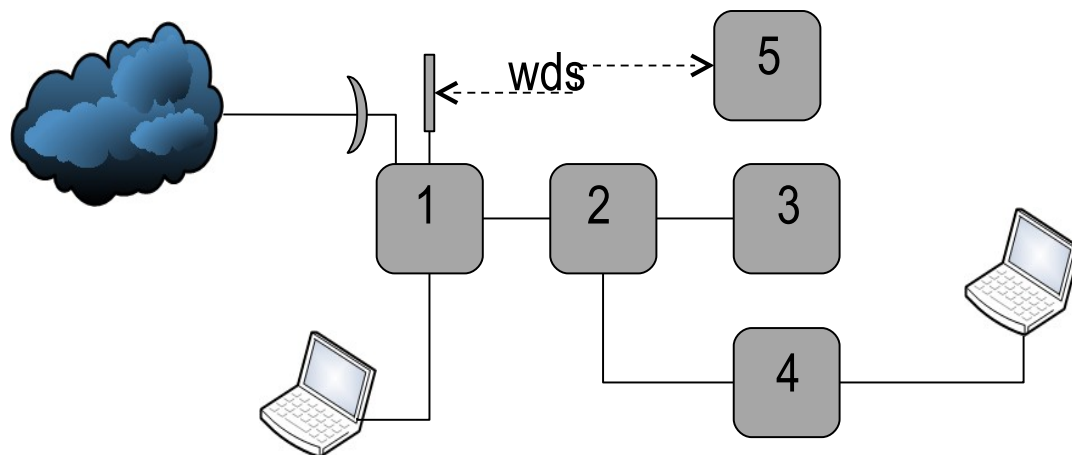
→ Atacante assumindo o papel de uma bridge comum

```
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 assumindo o papel de root + Homem do Meio



Ataques ao Spanning Tree DEMO

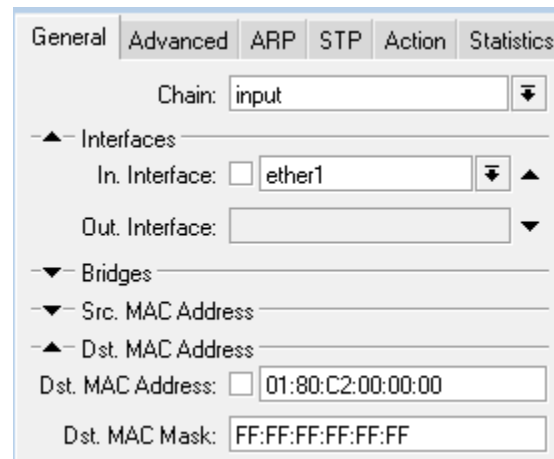


- Mandando mensagens de conf ou tcn BPDU para causar DoS
- Transformando-se em uma Bridge participante do STP
- Transformando-se em porta Root no RSTP

Atacando o Spanning Tree Contra medidas

Mensagens de Spanning Tree são enviadas por padrão para o endereço MAC **01:80:C2:00:00:00** .

→ Filtrar as portas de borda da rede para esse endereço é solução para que o atacante não logre sucesso em se tornar root.

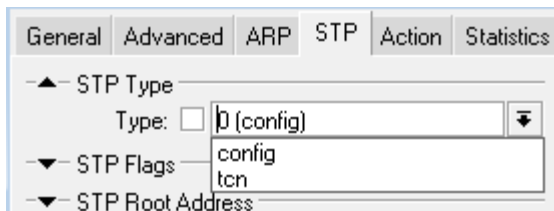


→ No entanto isso não evita os ataques de DoS ao STP/RSTP ☹

Atacando o Spanning Tree Contra medidas

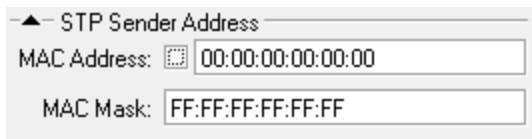
É possível também filtrar seletivamente as mensagens de STP pelos classificadores:

→ Tipo de mensagem conf BPDU ou tcn BPDU



The screenshot shows the Mikrotik WinBox configuration interface for STP. The 'STP' tab is selected. Under 'STP Type', the 'Type' dropdown is set to '0 (config)'. The 'STP Flags' dropdown is expanded, showing 'config' and 'tcn' options. The 'STP Root Address' section is partially visible below.

→ Endereço do remetente



The screenshot shows the 'STP Sender Address' configuration section in Mikrotik WinBox. The 'MAC Address' field is set to '00:00:00:00:00:00' and the 'MAC Mask' field is set to 'FF:FF:FF:FF:FF:FF'.

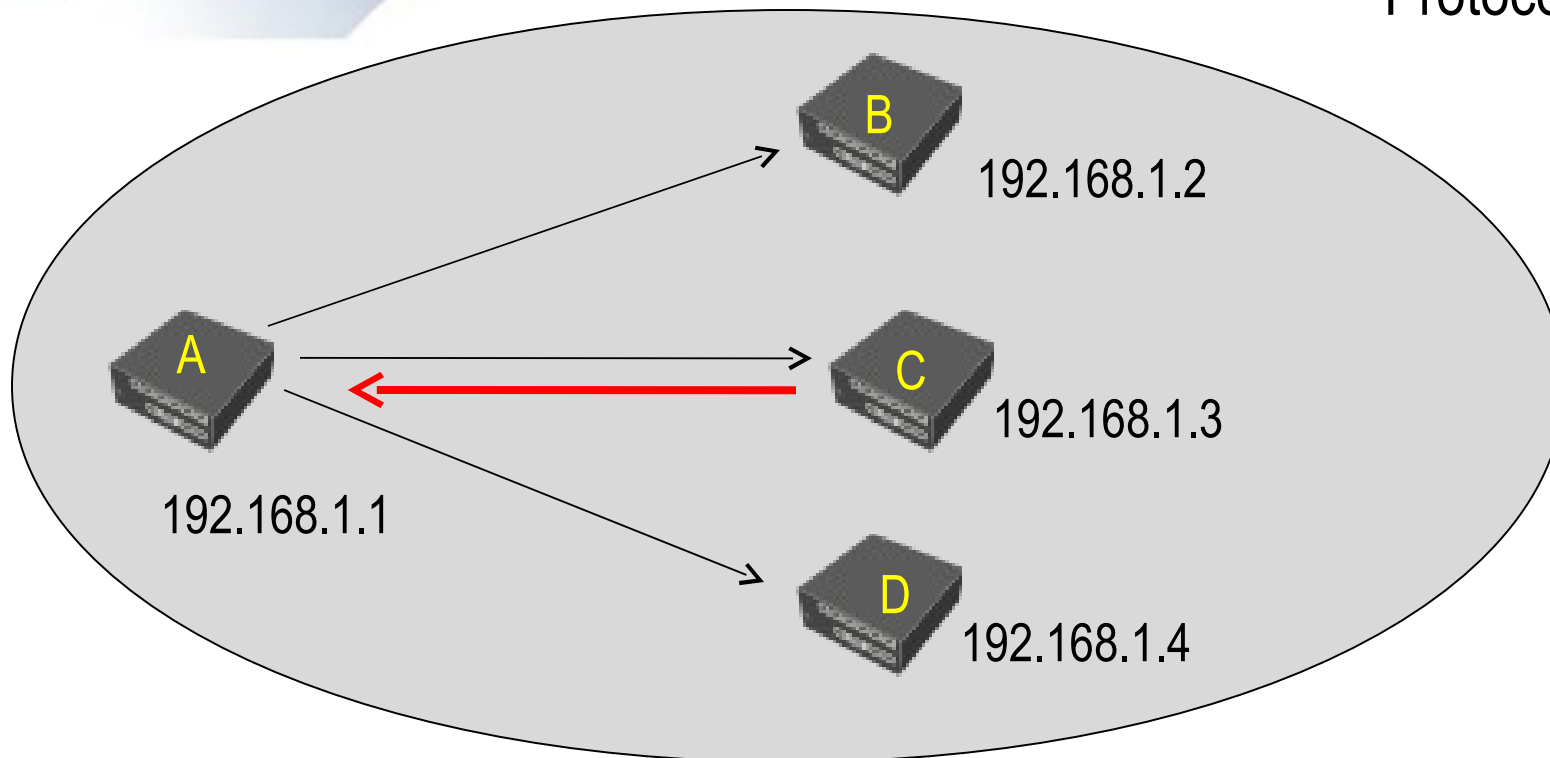
→ No entanto isso não evita os ataques de DoS ao STP/RSTP ☹

Atacando a camada 2

Envenenamento de ARP
(ARP Poisoning ou ARP Spoof)



Protocolo ARP



→ A pergunta para todos: “Quem tem o IP 192.168.1.3 ?”

→ C responde para A: “O IP 192.168.1.3 está no MAC XX:XX:XX:XX:XX:XX”

→ A registra em sua tabela arp o par: 192.168.1.3, MAC XX:XX:XX:XX:XX:XX

Envenenamento de ARP

Envenenamento de ARP

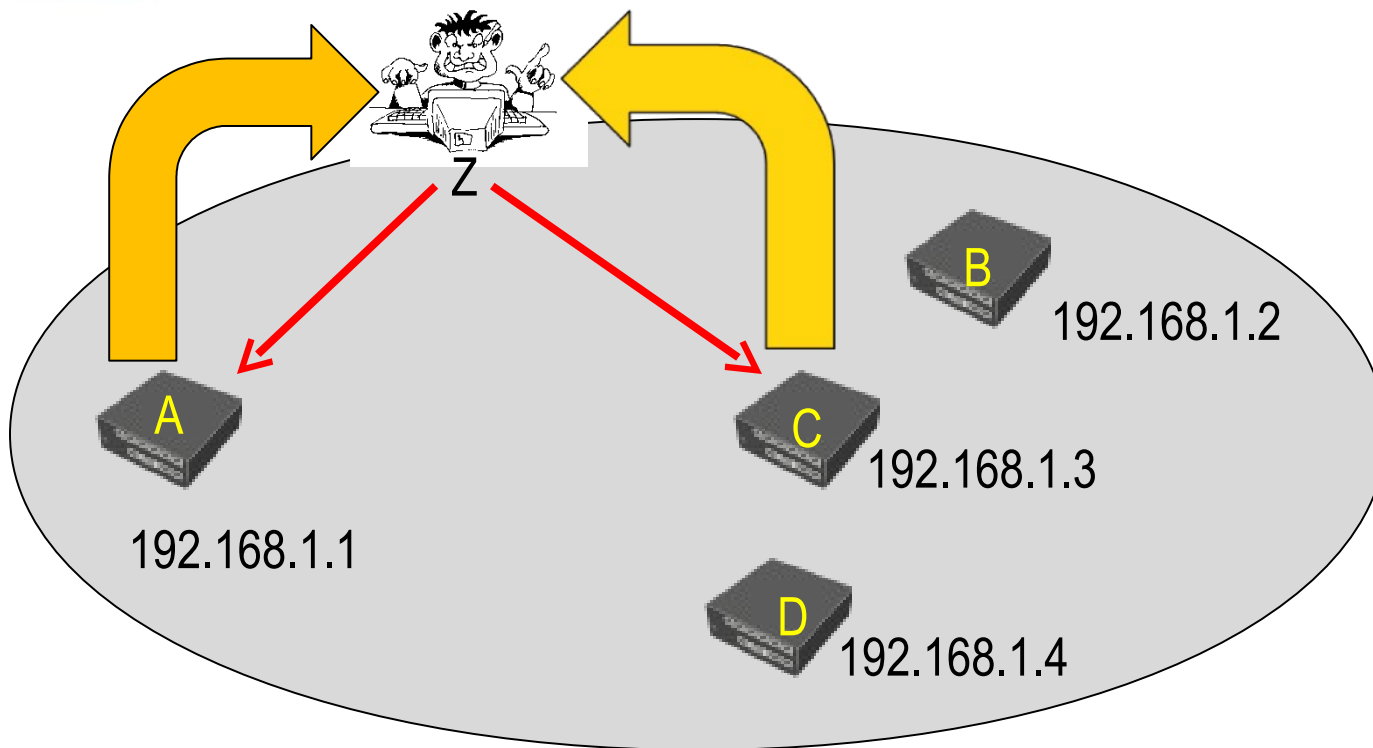
→ “Atacante” emite para um alvo específico (ou em broadcast), mensagens de ARP “gratuitas” anunciando que o seu MAC é o MAC de quem quer spoofar (normalmente o gateway)

→ “Atacado” tem suas tabelas ARP “envenenadas” e passam a mandar os pacotes para o Atacante

→ “Atacante” manda para o gateway mensagens de ARP “gratuitas” anunciando seu MAC com o IP do Atacado

→ Atacado fala com o Gateway através do Atacante – Homem do meio

“Envenenamento” de ARP

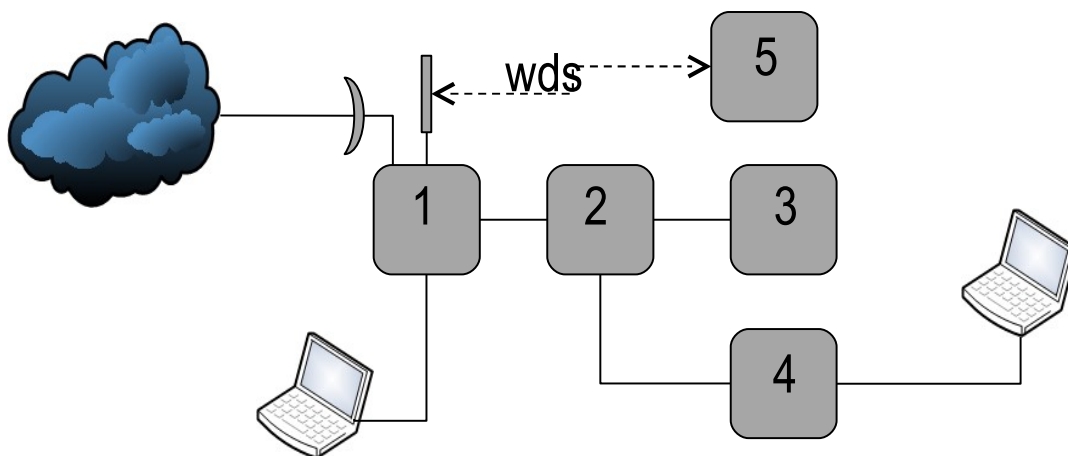


→ Z fala para A: “O IP 192.168.1.3 está no MAC ZZ:ZZ:ZZ:ZZ:ZZ:ZZ”

→ Z fala para C: “O IP 192.168.1.1 está no MAC ZZ:ZZ:ZZ:ZZ:ZZ:ZZ”

→ A passa a falar com C (e vice versa) através de Z (Homem do meio)

Spoof de ARP + Homem do meio DEMO



- Fazendo o arp-spoof a partir de 4
- Verificação nos outros hosts
- Filtrando o ARP

Defesas para Arp-Spoof

1) Mudança no comportamento do protocolo ARP

General STP Status Traffic

Name: bridge1

Type: Bridge

MTU: 1500

L2 MTU: 1522

MAC Address: 00:0C:42:01:01:01

ARP: enabled

Admin. MAC Address: enabled

enabled
disabled
proxy-arp
reply-only

ARP disabled → todos hosts tem que ter entradas estáticas.

ARP Reply-Only → Somente o concentrador tem entradas estáticas.

Inconvenientes:

- Arp estático em todos os hosts é muito difícil implementar na prática
- Reply-Only não protege o lado do cliente.

Defesas para Arp-Spoof

2) Segregação do tráfego (isolação de clientes)

Em uma rede típica voltada para provimento de acesso é desejável que os clientes na camada 2 somente “enxerguem” o gateway. Vamos chamar de segregação do tráfego às medidas que tem de ser tomadas para isolar todo tipo de tráfego entre clientes.

No caso de uma rede Wireless, com essas medidas tem que ser feitas em 2 níveis:

- Na Interface (Wireless)
- Em todas as “portas” da bridge.(Wireless e Wired)

Segregando o tráfego na camada 2 (1 Interface Wireless)

Interface <wlan1>

General Wireless WDS Nstreme Status Traffic

Mode: ap bridge

Band: 2.4GHz-B/G

Frequency: 2412 MHz

SSID: MKBR100-NG

Scan List:

Security Profile: default

Antenna Mode: antenna a

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

AP Access Rule <BE:BA:D0:BA:BA:CA>

MAC Address: BE:BA:D0:BA:BA:CA

Interface: all

Signal Strength Range: -120..120

AP Tx Limit:

Client Tx Limit:

Authentication

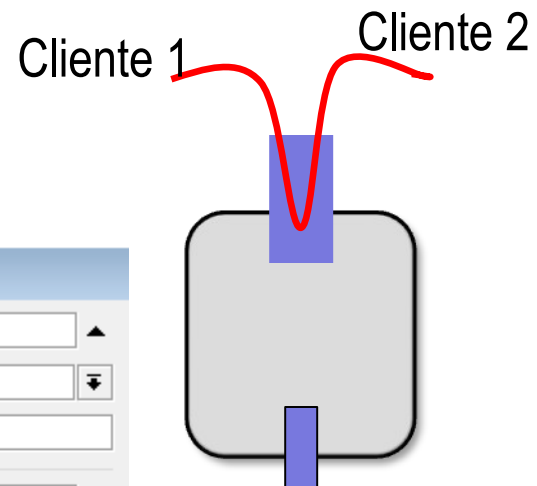
Forwarding

Private Key: none Qx

Private Pre Shared Key:

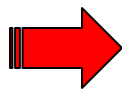
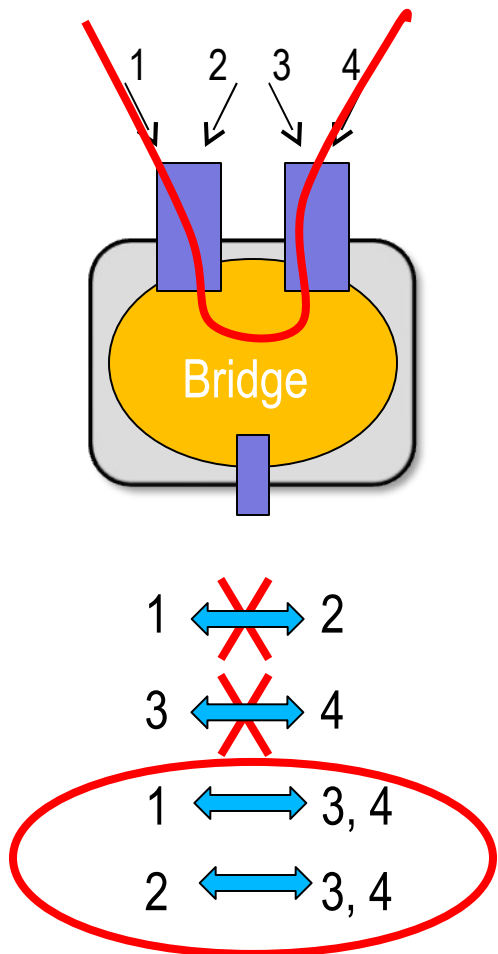
Time

disabled



Default forward desabilitado nas placas e nos access lists

Segregação de tráfego na camada II (2 interfaces em bridge)



General Advanced ARP STP Action Statistics

Chain: forward

Interfaces

In. Interface: wlan1

Out. Interface: wlan2

General Advanced ARP STP Action Statistics

Action: drop

General Advanced ARP STP Action Statistics

Chain: forward

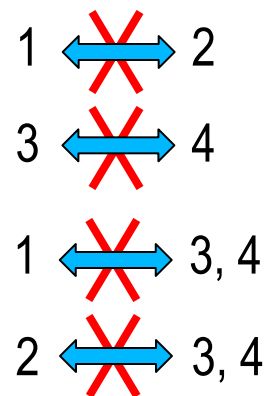
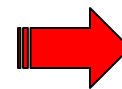
Interfaces

In. Interface: wlan2

Out. Interface: wlan1

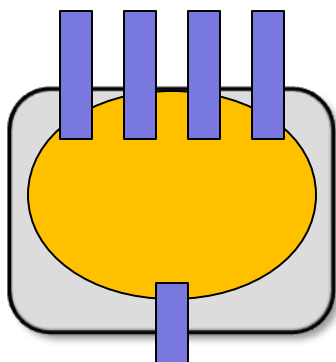
General Advanced ARP STP Action Statistics

Action: drop



2 Regras

Wlan1, 2, 3 e 4



ether1

Segregando o tráfego na camada II
4 Interfaces em Bridge

12 Regras ?

#	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 Regras

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

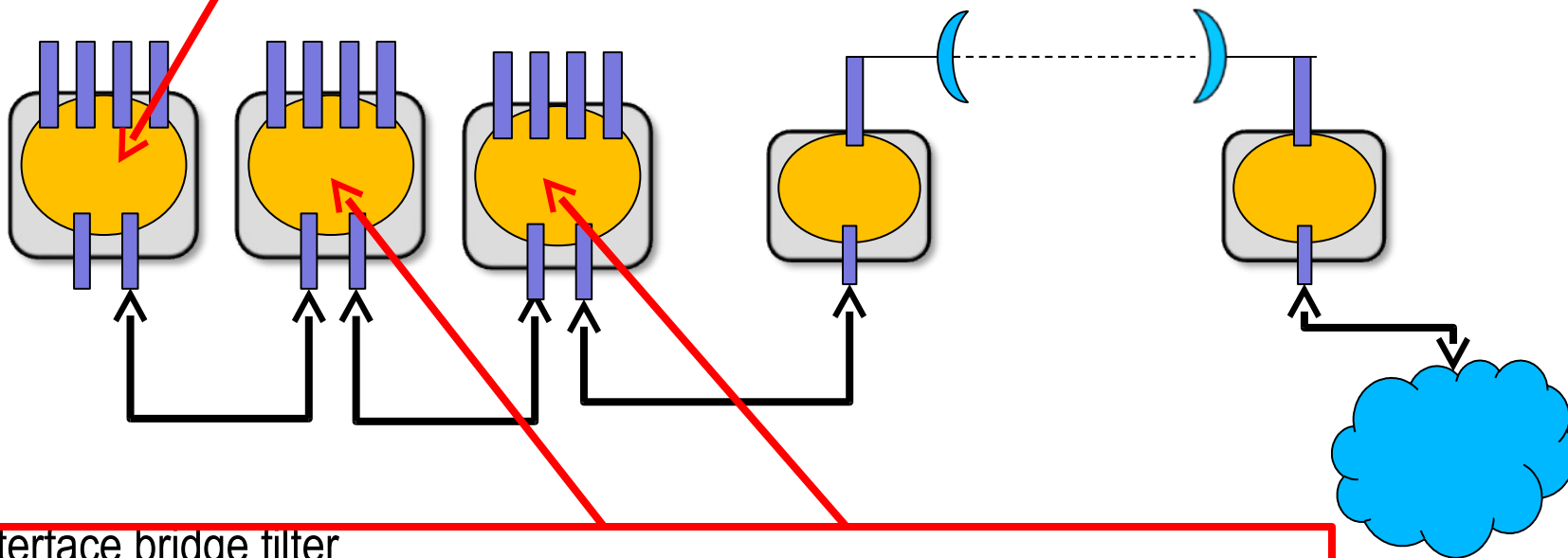
1 Regra !

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

Obrigado Edson 😊

Segregando o tráfego na camada II Vários equipamentos em 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
```

Defesas para Arp-Spoof

Em redes onde existam outros equipamentos que não suportem a segregação de tráfego, a única medida que pode ser feita são filtros para controlar o protocolo ARP pelo menos nos trechos em que o tráfego passa pelo Mikrotik RouterOS. Exemplos:

1- Aceita requisições de ARP de qualquer host

General Advanced ARP STP Action Statistics
Action: **accept**

General Advanced ARP STP Action Statistics
-▲- ARP Opcode
ARP Opcode: 1 (request)

2- Aceita respostas de ARP oriundas do Gateway

General Advanced ARP STP Action Statistics
Action: **accept**

General Advanced ARP STP Action Statistics
-▲- ARP Opcode
ARP Opcode: 2 (reply)

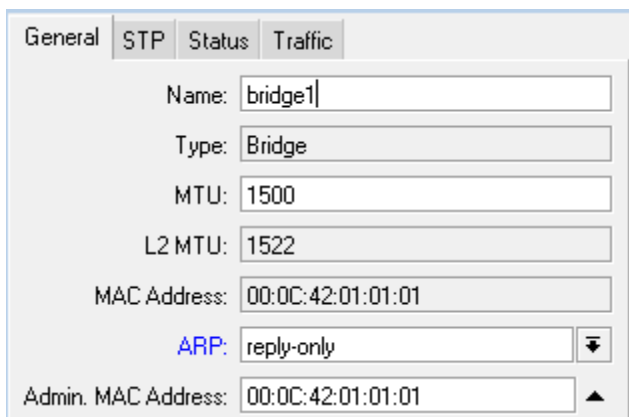
General Advanced ARP STP Action Statistics
Chain: **forward**
-▼- Interfaces
-▼- Bridges
-▼- Src. MAC Address
-▲- Dst. MAC Address

General Advanced ARP STP Action Statistics
Action: **accept**
MAC Protocol-Num: 806 (arp) hex

General Advanced ARP STP Action Statistics
Chain: **forward**
-▼- Interfaces
-▼- Bridges
-▲- Src. MAC Address
Src. MAC Address: 00:0C:42:01:01:01
Src. MAC Mask: FF:FF:FF:FF:FF:FF
-▼- Dst. MAC Address
-▲- MAC Protocol
MAC Protocol-Num: 806 (arp) hex

Defesas para Arp-Spoof

Em redes onde existam outros equipamentos que não suportem a segregação de tráfego, o que pode ser feito é combinar o ARP reply-only com alguns filtros e para evitar o envenenamento dos clientes pelo menos nos trechos em que o tráfego passa pelo Mikrotik RouterOS.



General | STP | Status | Traffic

Name:

Type:

MTU:

L2 MTU:

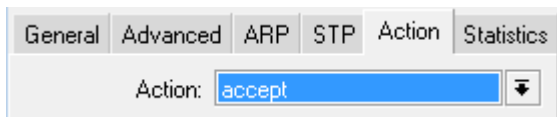
MAC Address:

ARP: ▼

Admin. MAC Address: ▲

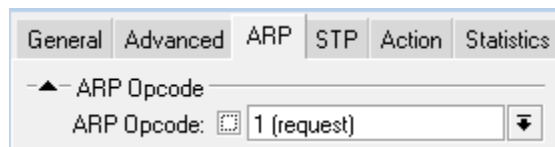
1 – Gateway em reply-only (tabelas estáticas)

2 - Aceita requisições de ARP de qualquer host



General | Advanced | ARP | STP | Action | Statistics

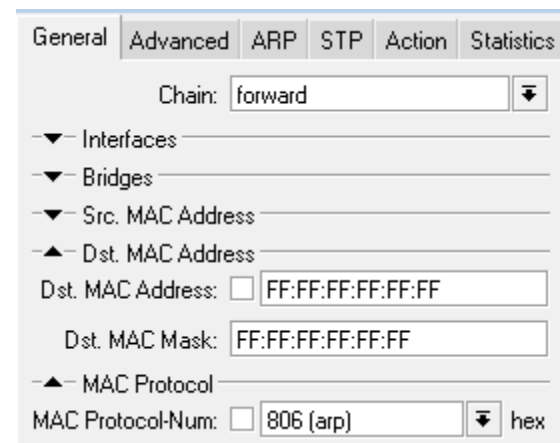
Action: ▼



General | Advanced | ARP | STP | Action | Statistics

▲ ARP Opcode

ARP Opcode: ▼



General | Advanced | ARP | STP | Action | Statistics

Chain: ▼

▼ Interfaces

▼ Bridges

▼ Src. MAC Address

▲ Dst. MAC Address

Dst. MAC Address:

Dst. MAC Mask:

▲ MAC Protocol

MAC Protocol-Num: ▼ hex

Defesas para Arp-Spoof

3 – Descarta qualquer resposta que não seja oriunda do Gateway

General Advanced ARP STP Action Statistics

Chain: forward

▼ Interfaces

▼ Bridges

▲ Src. MAC Address

Src. MAC Address: 00:0C:42:01:01:01

Src. MAC Mask: FF:FF:FF:FF:FF:FF

▼ Dst. MAC Address

▲ MAC Protocol

MAC Protocol-Num: 806 (arp) hex

General Advanced ARP STP Action Statistics

▲ ARP Opcode

ARP Opcode: 2 (reply)

General Advanced ARP STP Action Statistics

Action: drop

Protegendo o ARP (medidas complementares)

Pode-se ainda eliminar pacotes de ARP espúrios descartando ARP não ethernet e pacotes não IPV4

General Advanced **ARP** STP Action Statistics

Chain:

▼ Interfaces _____

▼ Bridges _____

▼ Src. MAC Address _____

▼ Dst. MAC Address _____

▲ MAC Protocol _____

MAC Protocol-Num:

▼ IP _____

▼ Packet Mark _____

▼ Ingress Priority _____

General Advanced **ARP** STP Action Statistics

Action:

General Advanced **ARP** STP Action Statistics

▼ ARP Opcode _____

▲ ARP Hardware Type _____

Hardware Type:

▼ ARP Packet Type _____

▼ ARP Addresses _____

▼ ARP Src. MAC Address _____

▼ ARP Dst. MAC Address _____

General Advanced **ARP** STP Action Statistics

▼ ARP Opcode _____

▼ ARP Hardware Type _____

▲ ARP Packet Type _____

Packet Type:

▼ ARP Addresses _____

▼ ARP Src. MAC Address _____

▼ ARP Dst. MAC Address _____

Medidas para controle de arp-poof em redes com PPPoE

→ Filtros de Bridge nas interfaces que “escutam” o PPPoE permitindo apenas PPPoE-discovery e PPPoE-session, são importantes e filtram totalmente o protocolo ARP. As interfaces podem inclusive ficar com o ARP desabilitado. Tais medidas são importantes não só para filtrar ARP mas também para outros tráfegos indesejados.

General | Advanced | ARP | STP | Action | Statistics

Chain: forward

▼ Interfaces

▼ Bridges

▼ Src. MAC Address

▼ Dst. MAC Address

▲ MAC Protocol

MAC Protocol-Num: 8863 (pppoe-discovery) hex

General | Advanced | ARP | STP | Action | Statistics

Chain: forward

▼ Interfaces

▼ Bridges

▼ Src. MAC Address

▼ Dst. MAC Address

▲ MAC Protocol

MAC Protocol-Num: pppoe-session hex

General | Advanced | ARP | STP | ...

Chain: forward

ARP | STP | Action | Statistics | ...

Action: drop

General | Advanced | ARP | STP | Action | Statistics

Action: accept

General | Advanced | ARP | STP | Action | Statistics

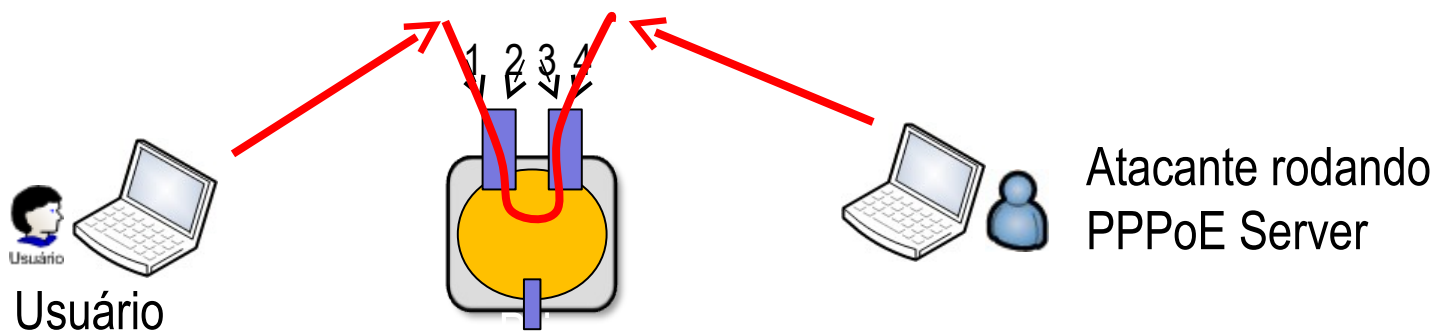
Action: accept

Uma rede que utiliza PPPoE está livre de ataques de arp-spoof por parte de seus clientes ?

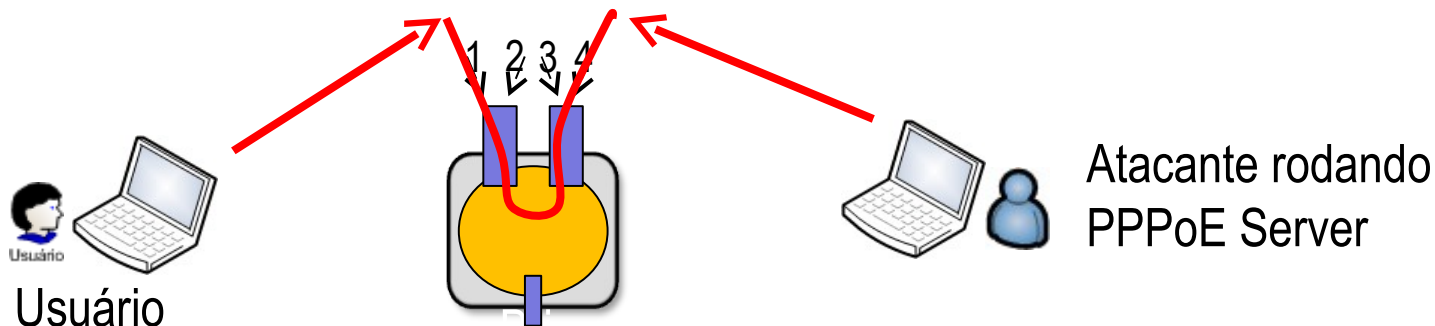
→ Se a rede utilizar somente PPPoE e não utilizar IP nas interfaces que “escutam” o PPPoE a resposta é obviamente sim.

→ No entanto não se pode descartar que tais redes estão sujeitas a todos os outros ataques abordados anteriormente e mais um:

→ Ataques entre clientes por servidor PPPoE Falso:



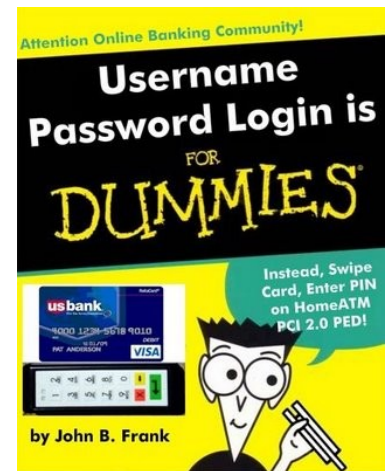
Solução para o problema anterior



- Desabilitar default forward nas interfaces e access lists
- Efetuar os filtros de Bridge entre interfaces **ANTES** de liberar o PPPoE.
- Efetuar os filtros de Bridge de PPPoE session e PPPoE discovery
- Descartar o restante

Atacando a camada 2

Atacando clientes e provedores de
PPPoE e Hotspot



Atacando Provedores e Clientes de Hotspot e PPPoE

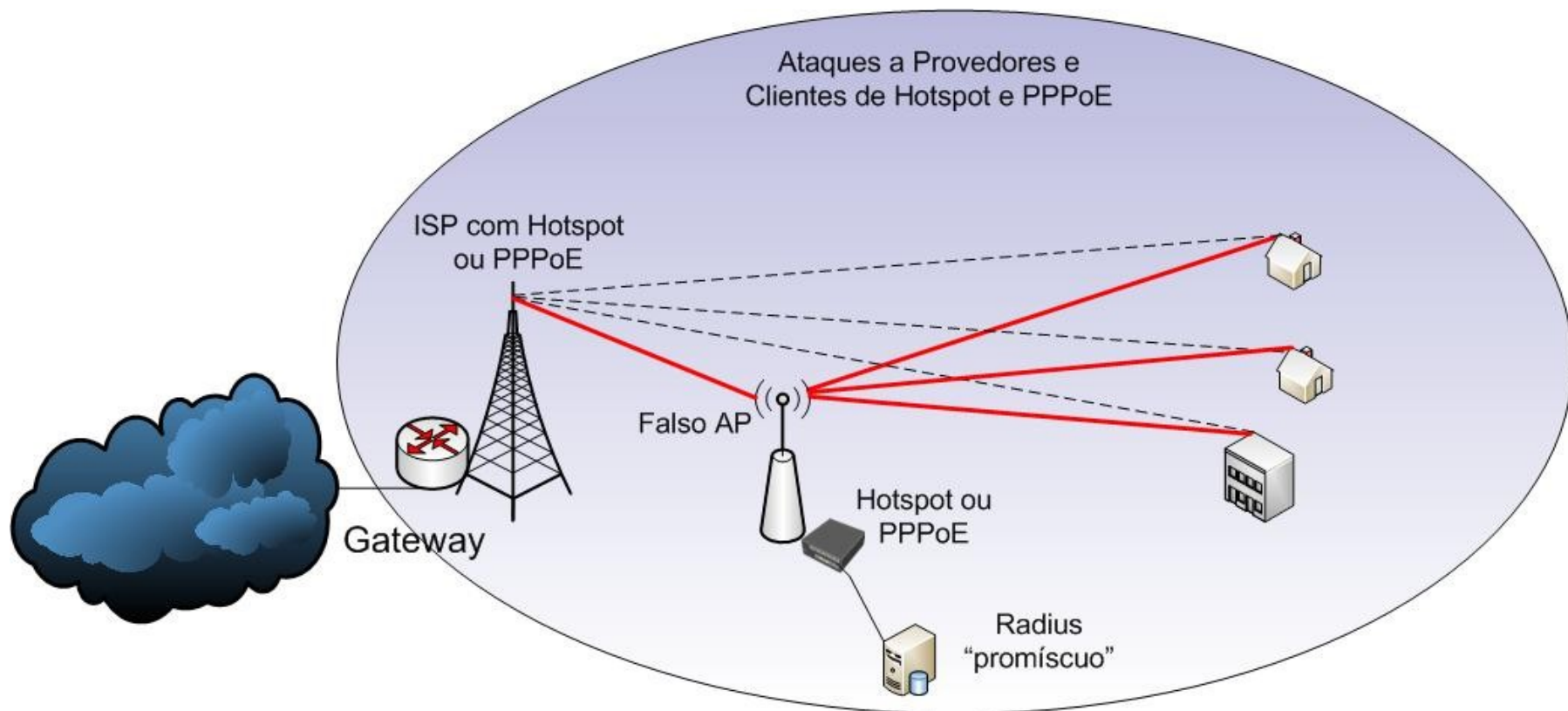
→ São ataques simples de camada 1 e 2 que consistem em colocar um AP com mesmo SSID e Banda de operação e executando o mesmo serviço (PPPoE ou Hotspot)

→ Dependendo da potencia do sinal e localização relativa do atacante em relação aos clientes não é necessário maiores medidas. Pode ser necessário fazer um ataque de DoS no provedor inicialmente.

→ O ataque pode ser feito para vários objetivos, como simples negação de serviço, descoberta de senhas de Hotspot e PPPoE, homem do meio, envenenamento de cache, etc.

→ Para descoberta de senhas pode-se utilizar um Radius em modo Promíscuo

Atacando Provedores e Clientes de Hotspot e PPPoE



Radius configurado para capturar usuários e 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
```

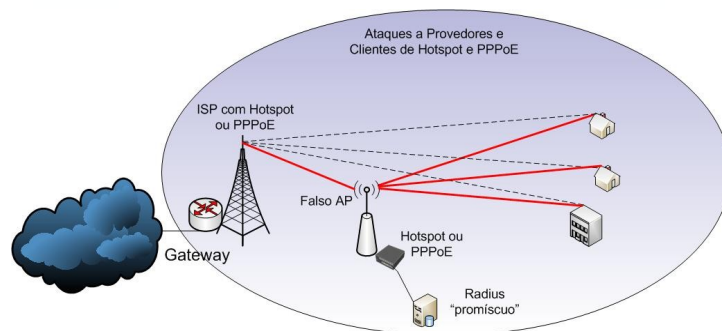
```
# allowed values: { no, yes }
```

```
log_auth_badpass = yes
```

```
log_auth_goodpass = yes
```

```
...
```

Ataques a Hotspot e PPPoE Contra medidas



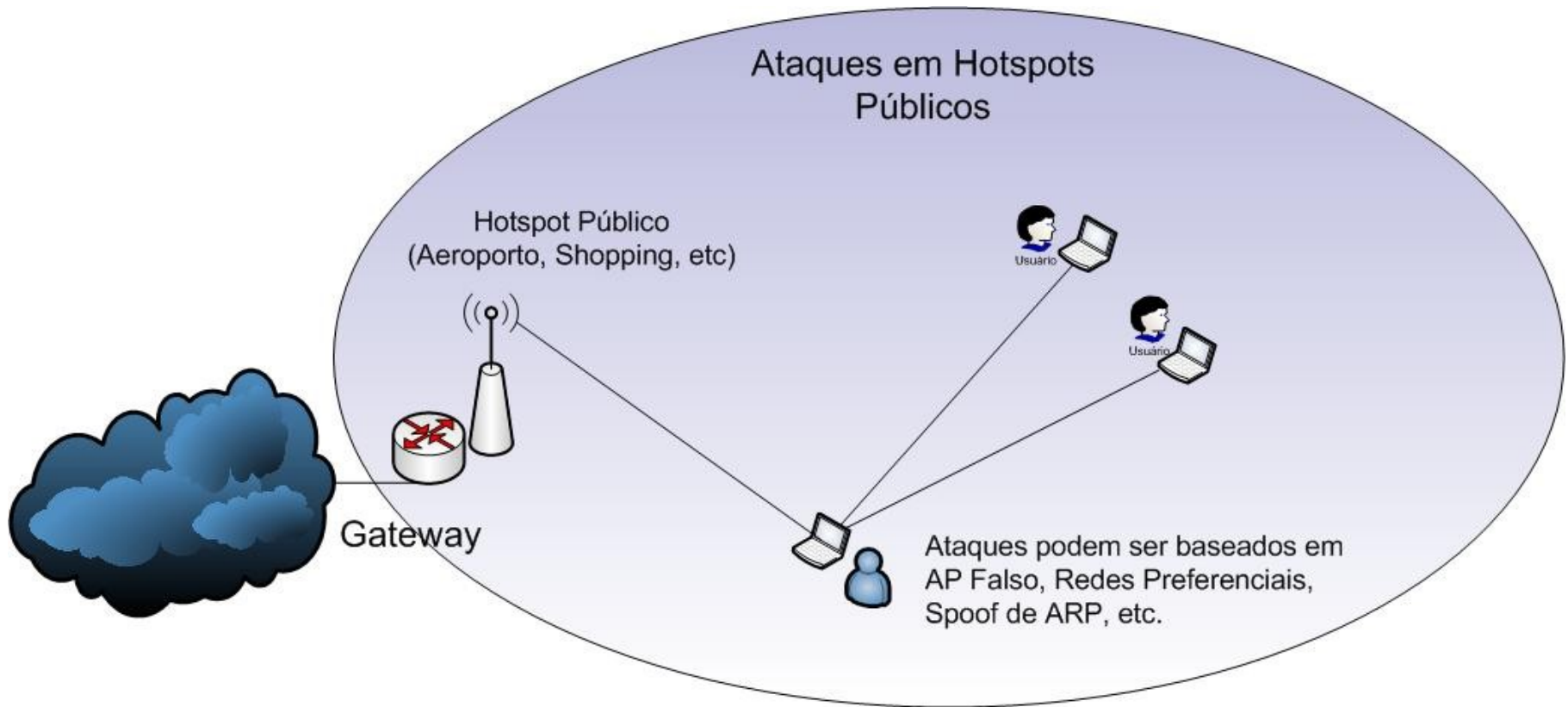
→ Somente criptografia bem implementada pode evitar esses ataques. É tolice pensar que uma rede Wireless está segura quando não usa criptografia.

→ A implementação de criptografia em uma rede pode ser feita de inúmeras maneiras, mais ou menos eficientes. A maneira mais segura seria com Certificados Digitais instalados em todos equipamentos (EAP-TLS) mas no entanto é na prática limitada pela ponta cliente que nem sempre tem o suporte adequado

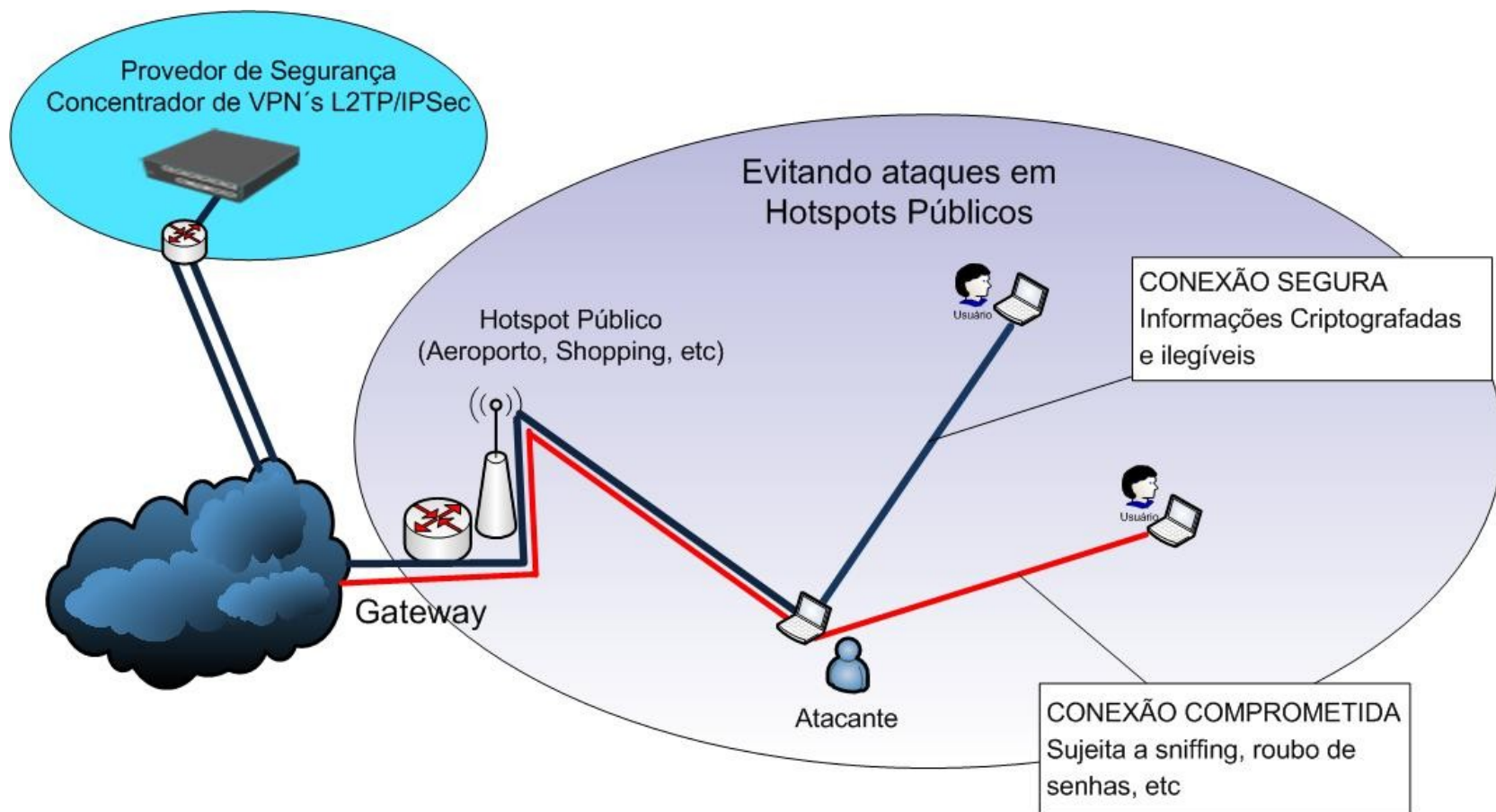
→ O Mikrotik tem uma solução intermediária muito interessante que é a distribuição de chaves PSK individuais por cliente com as chaves distribuídas por Radius.

Para detalhes dessa implementação ver <http://mum.mikrotik.com> – Brazil 2008

Ataques a Hotspots Públicos

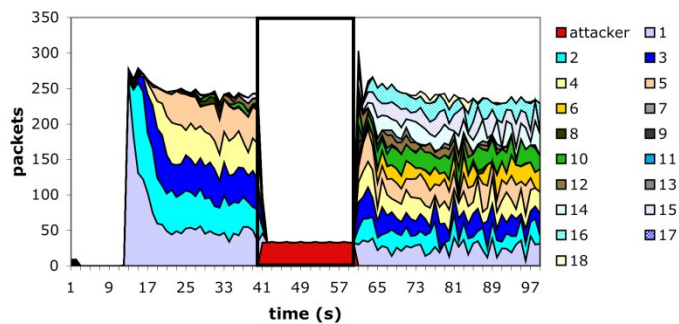


Acesso seguro em Hotspots Públicos



Atacando a camada 2

Ataques de Desautenticação (Deauth Attack)



Ataques de negação de serviço em Wireless

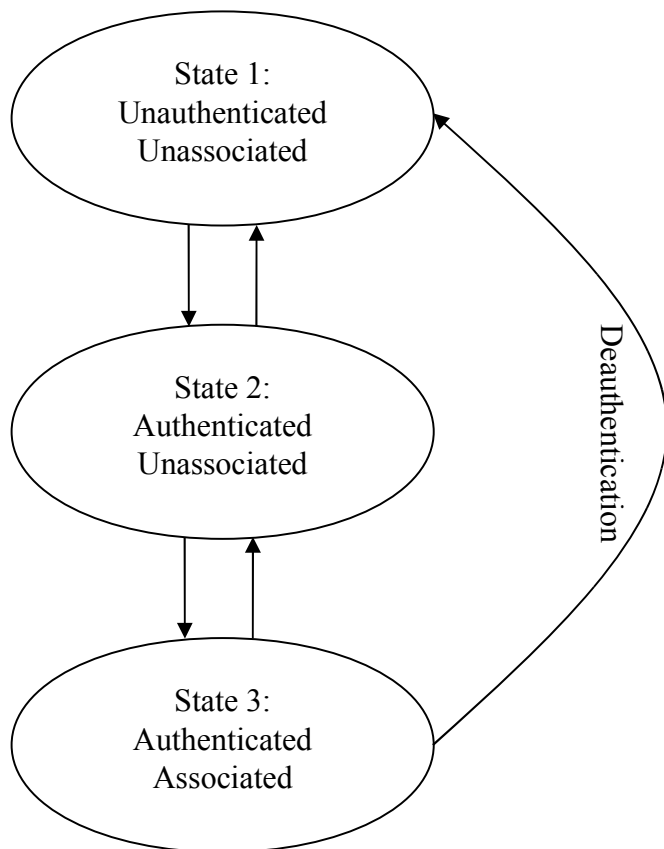
→ Ataques baseados em altas potencias de RF (Jamming) – Camada 1

Tendo em vista que estamos trabalhando com bandas não licenciadas, esse é um risco potencial e não há muito o que se fazer a não ser reclamar com a autoridade responsável pelo espectro. Um bom projeto de RF pode no entanto ajudar a termos uma menor exposição a esse tipo de ataque.

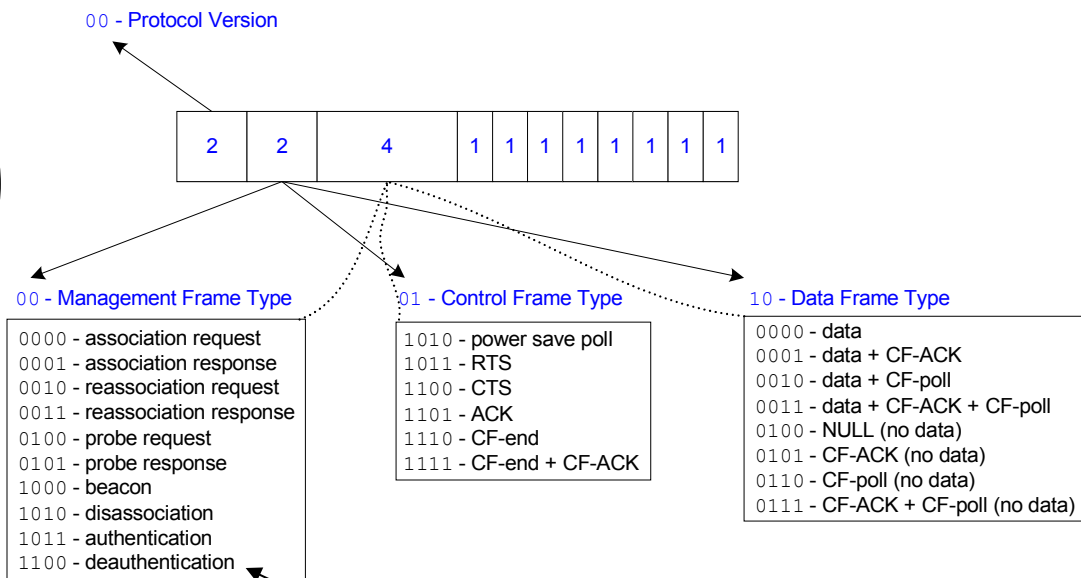
→ Ataques baseados no protocolo

Tem como base a exploração de vulnerabilidades nos frames de controle que existem graças a uma concepção fraca de segurança quando do desenvolvimento do protocolo 802.11 pois não houve preocupação quanto a autenticação desses frames.

Processo de Autenticação / Associação



802.11 Types and Subtypes



Ataque de Deauth

- 1 – O atacante utiliza qualquer ferramenta como airodump, kismet, wellenreiter, ou o próprio sniffer/snooper do Mikrotik RouterOS para descobrir :
 - MAC do AP
 - MAC do Cliente
 - Canal em uso
- 2 – Posta-se em qualquer posição em que o AP pode ouvir sua transmissão (mesmo um sinal fraco será suficiente desde que esteja alguns decibéis acima da sensibilidade do AP)
- 3 – Dispara o ataque solicitando ao AP que desautentique o cliente;

Esse ataque pode ser combinado com outros, levantando um AP falso e fazendo o homem do meio ou mesmo para facilitar a renovação da tabela ARP

Ataques de deauth - soluções

→ Depois de revelados os problemas com ataques de deauth e tendo estes tomado caráter real, algumas medidas foram propostas como a exposta no artigo abaixo:

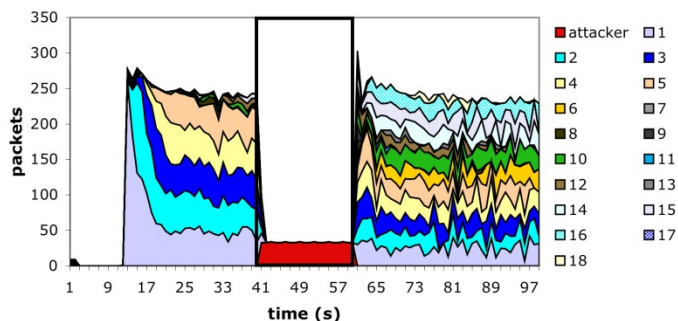
<http://sysnet.ucsd.edu/~bellardo/pubs/usenix-sec03-80211dos-slides.pdf>

→ Nos MUM's da Argentina em 2007 e da Polônia em 2009 foram apresentadas algumas soluções para fazer frente a esses ataques quando utilizando Mikrotik RouterOS. São soluções apenas paliativas que podiam até então serem 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 Desautenticação (Deauth Attack) Contra medidas



→ A partir da V4 o Mikrotik RouterOS incorpora a possibilidade de autenticação de frames de controle nos perfis de segurança

The screenshot shows the 'Security Profile <MKBR>' configuration window. The 'General' tab is selected. The 'Name' field is 'MKBR' and the 'Mode' is 'dynamic keys'. Under 'Authentication Types', 'WPA PSK' is checked. Under 'Unicast Ciphers', 'aes ccm' is checked. Under 'Group Ciphers', 'aes ccm' is checked. The 'WPA Pre-Shared Key' field is empty, and the 'WPA2 Pre-Shared Key' field contains 'xxxxxxxx'. The 'Group Key Update' is set to '00:05:00'. The 'Management Protection' dropdown is set to 'allowed' and is circled in red. The 'Management Protection Key' field contains 'xxxxxxx'.

Ataques à camada 2 e contramedidas Conclusões

- A exposição de qualquer rede a ataques de camada 2 é muito grande quando se tem acesso físico a mesma e os potenciais ataques de negação de serviço são na sua maioria avassaladores e de difícil controle
- Quando se necessita dar acesso em camada 2 a uma outra rede uma política rígida de controle de endereços físicos deve ser implementada, além de outros filtros.
- O Mikrotik RouterOS possui ferramentas que ajudam nesses controles, mas na medida do possível deve-se restringir ao máximo as portas de entrada para a rede que possam se utilizad dos potenciais ataques à camada 2

Obrigado ! ¡ Gracias !

Wardner Maia – maia@mikrotikbrasil.com.br

