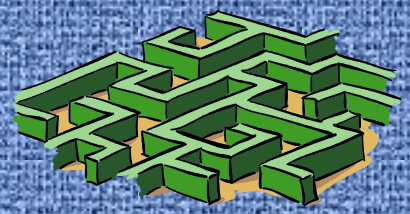
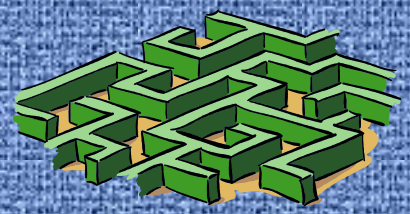
WISP Hotspot: Redes Malladas Metropolitanas

Alessio Garavano
ISPARG S.A.
Soluciones IP Profesionales
www.isparg.com.ar
info@isparg.com.ar



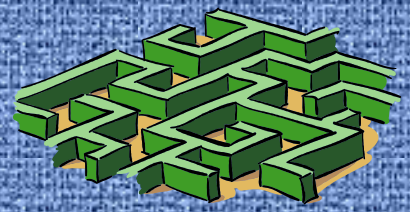
HOTSPOT

Hotspots son comunmente conocidos como lugares publicos(hoteles, aeropuertos, barcos, etc) que ofrecen acceso inalambrico libre a internet para ser accedido por dispositivos móviles como notebooks, celulares, PDAs, consolas, etc



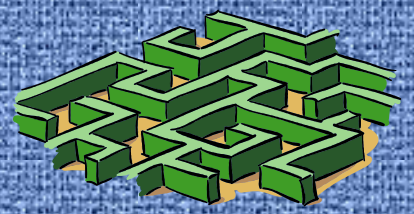
HOTSPOT

Hoy en dia, gracias a la funcionalidad y capacidad que nos ofrece el Servidor Hotspot de Mikrotik, podemos utilizar la solucion en diversos ambientes en los que parecian imposible de hacerlo...



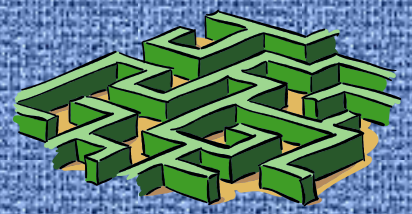
Wireless ISP HotSpot

- **Así es! miles de ISPs en el mundo lo recomiendan como la solución mas flexible y fácil de implementar y/o migrar a una red mucho mas dinámica, controlada y segura**



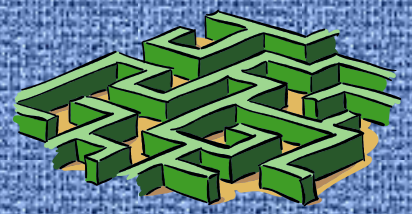
WiFi: Wireless Fidelity

- **Las comunicaciones por radio existen desde hace 150 años, y ahora tan sólo hemos unido la tecnología IP con los sistemas de radio y gracias a las ventajas y posibilidades que nos ofrece Mikrotik en Wireless, ¿El resultado es? "Explosivo!"**



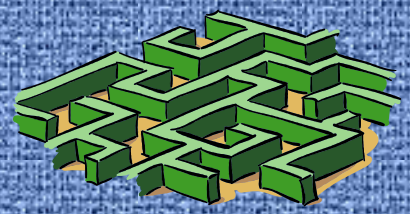
WiFi Mesh

- La tecnología de redes malladas (mesh) es una variante del WiFi tradicional, en la que las clásicas celdas WiFi basadas en cableado Ethernet hasta el switch se sustituyen por una red mallada, donde los nodos se comunican entre sí sin cables, estableciendo una macro-burbuja de cobertura que puede cubrir desde un área controlada hasta un municipio completo



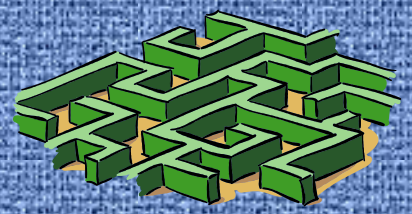
WiFi Mesh

- Cualquier ciudad puede tener su Red Inalámbrica Municipal o Metropolitana.
- Para usos privados, publicos o para ambos.
- No hay que dudar demasiado al pensar en realizar estas inversiones, la tecnología no tiene mucho tiempo de vida, pero está ampliamente probada y aprobada.



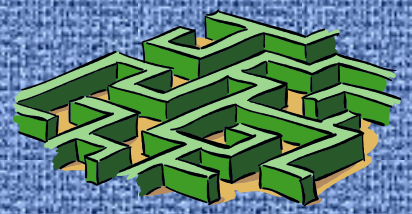
Mikrotik
WiFi Mesh & HotSpot ISP

- **Fusionando todo el potencial de una Red WiFi Mesh con la poderosa solución Hotspot de Mikrotik, obtenemos resultados sorprendentes a la hora entregar servicios de Internet de Banda Ancha y Telefonía IP en una ciudad**

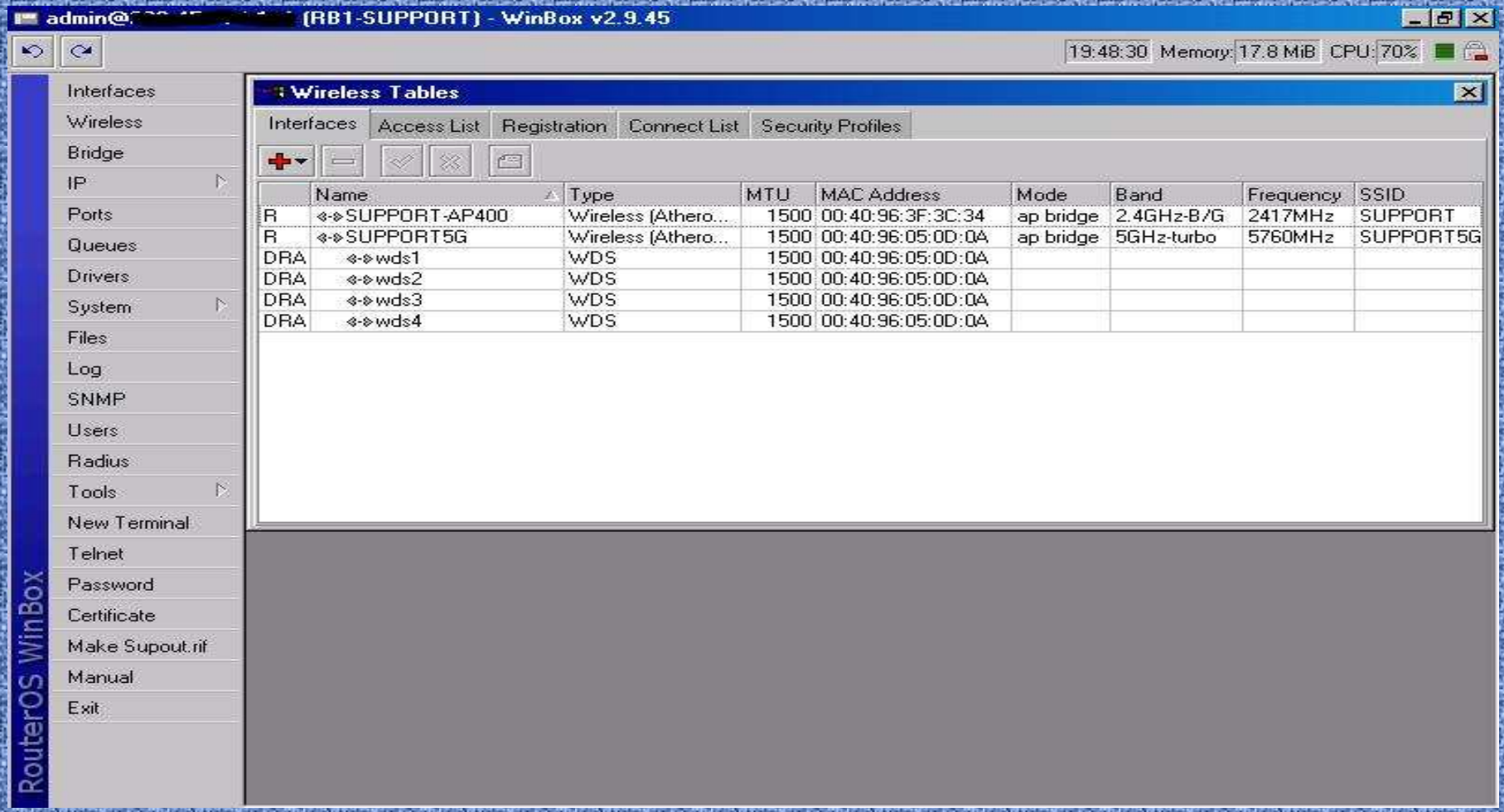


Implementando Mikrotik en un Wireless & Wired ISP

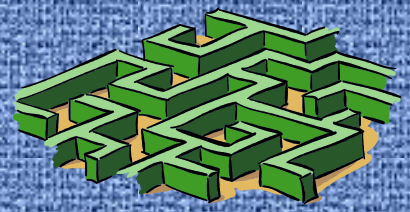
- Wireless Mesh Dual Band: Distribución del Servicio
- HotSpot Server: Autenticación y Control de Usuarios
- User Manager: Administración simple. Accesos unificados y Servicios Prepagos
- Web-Proxy Cache: Aceleración Web y ahorro de Ancho de Banda
- Wireless: Tipos de Accesos y Seguridad
- Bridge: Control y Seguridad a nivel de capa 2
- QoS: Calidad y Ecualización de Servicios
- Tips de Seguridad Avanzada para ISPs



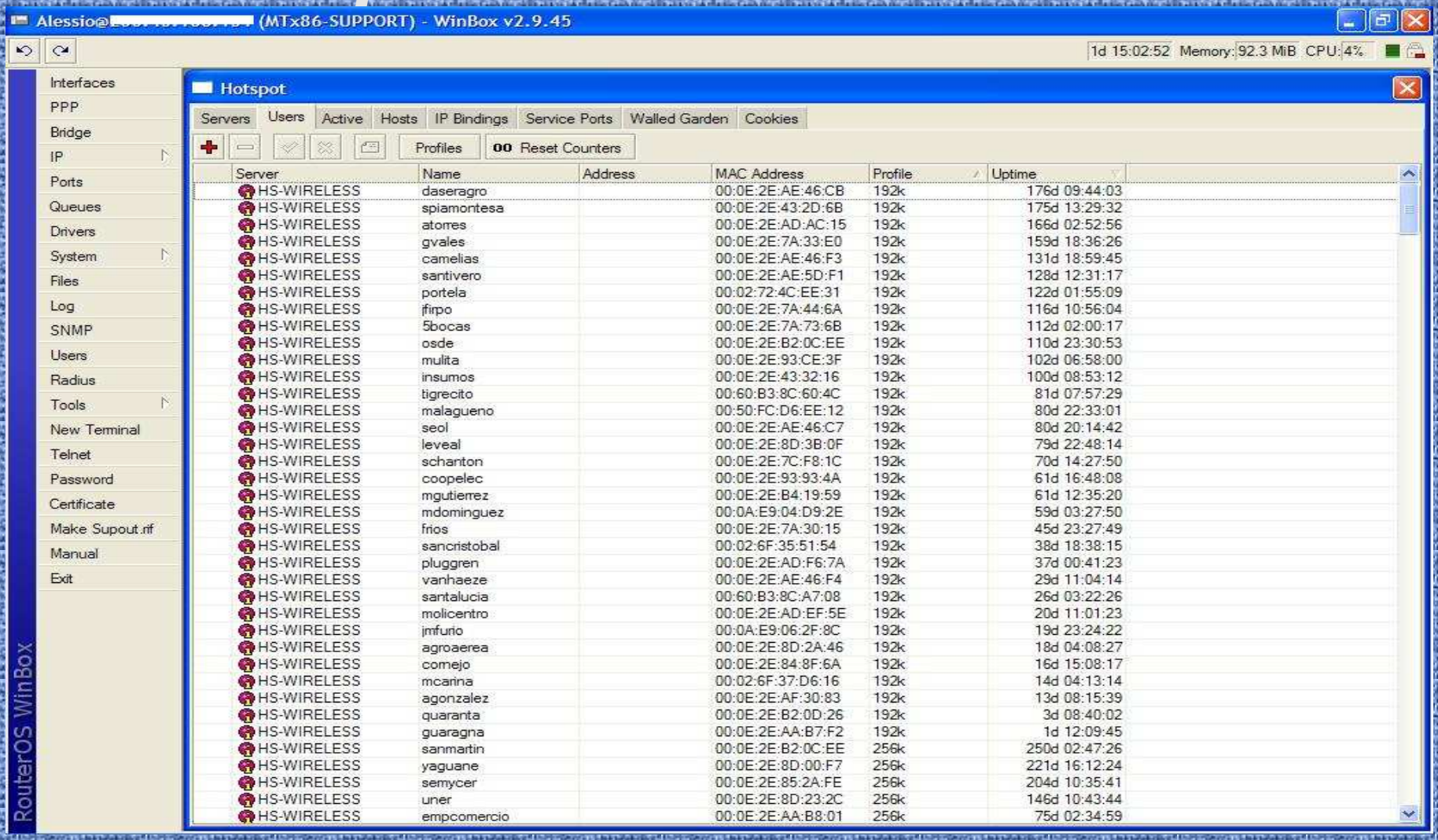
Wireless Mesh Dual Band



- Es la manera mas eficiente y economica de distribuir Internet en un municipio.
- En un mismo RB, se integra una red WDS bridgeada con RSTP en 5Ghz-Turbo y Nstreme, para la interconexiòn entre nodos y al backbone
- Y una red 2.4Ghz como AP para el acceso de los clientes con un mismo SSID en todos los nodos y diferentes canales si es necesario.

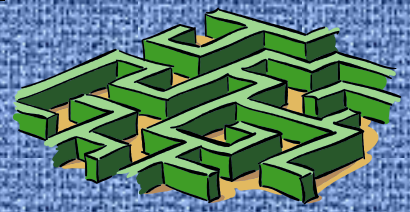


HotSpot: Control de Acceso

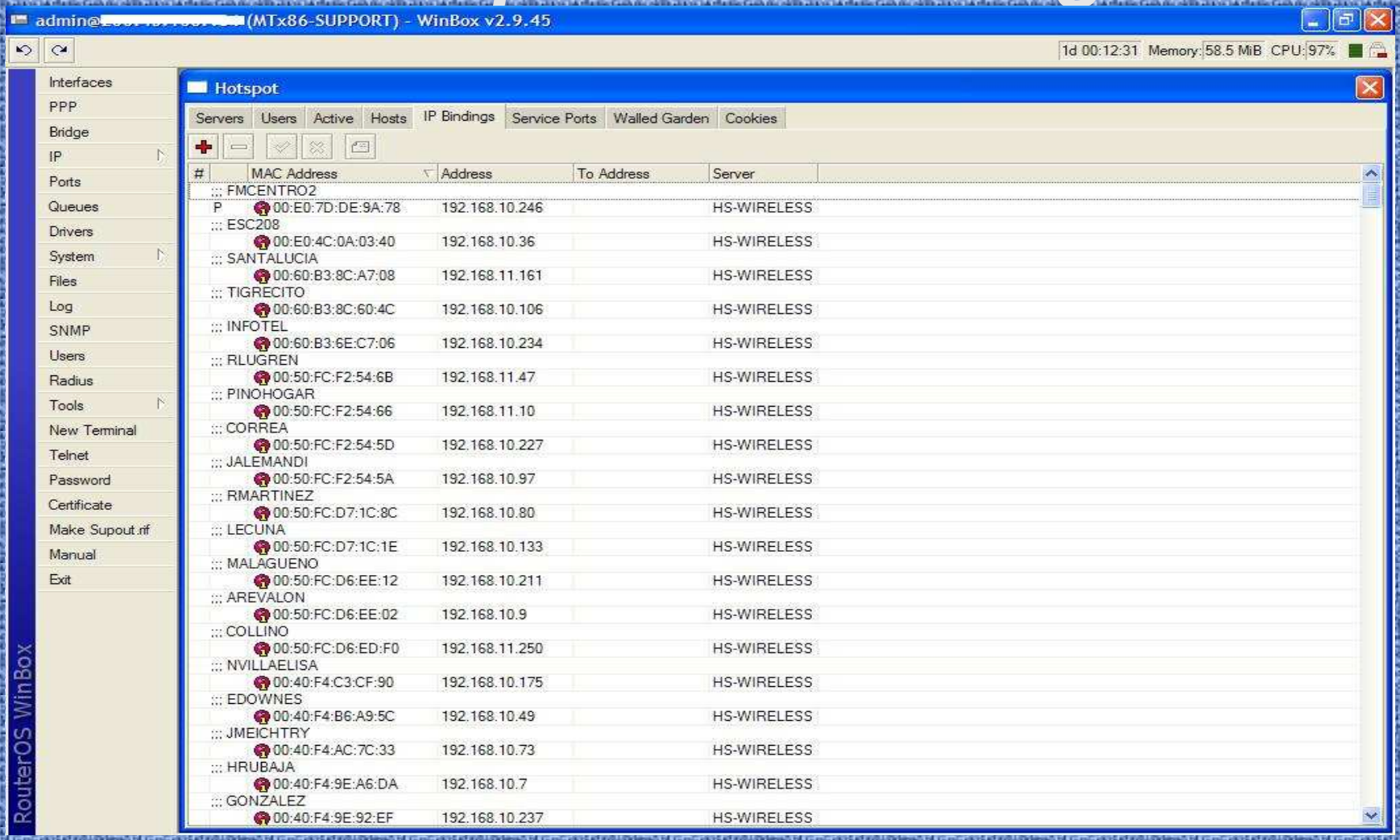


Server	Name	Address	MAC Address	Profile	Uptime
HS-WIRELESS	daseragro		00:0E:2E:AE:46:CB	192k	176d 09:44:03
HS-WIRELESS	spiamontesa		00:0E:2E:43:2D:6B	192k	175d 13:29:32
HS-WIRELESS	atorres		00:0E:2E:AD:AC:15	192k	166d 02:52:56
HS-WIRELESS	gvales		00:0E:2E:7A:33:E0	192k	159d 18:36:26
HS-WIRELESS	camelias		00:0E:2E:AE:46:F3	192k	131d 18:59:45
HS-WIRELESS	santivero		00:0E:2E:AE:5D:F1	192k	128d 12:31:17
HS-WIRELESS	portela		00:02:72:4C:EE:31	192k	122d 01:55:09
HS-WIRELESS	jfirpo		00:0E:2E:7A:44:6A	192k	116d 10:56:04
HS-WIRELESS	5bocas		00:0E:2E:7A:73:6B	192k	112d 02:00:17
HS-WIRELESS	osde		00:0E:2E:B2:0C:EE	192k	110d 23:30:53
HS-WIRELESS	mulita		00:0E:2E:93:CE:3F	192k	102d 06:58:00
HS-WIRELESS	insumos		00:0E:2E:43:32:16	192k	100d 08:53:12
HS-WIRELESS	tigrecito		00:60:B3:8C:60:4C	192k	81d 07:57:29
HS-WIRELESS	malagueno		00:50:FC:D6:EE:12	192k	80d 22:33:01
HS-WIRELESS	seol		00:0E:2E:AE:46:C7	192k	80d 20:14:42
HS-WIRELESS	leveal		00:0E:2E:8D:3B:0F	192k	79d 22:48:14
HS-WIRELESS	schanton		00:0E:2E:7C:F8:1C	192k	70d 14:27:50
HS-WIRELESS	coopelec		00:0E:2E:93:93:4A	192k	61d 16:48:08
HS-WIRELESS	mgutierrez		00:0E:2E:B4:19:59	192k	61d 12:35:20
HS-WIRELESS	mdominguez		00:0A:E9:04:D9:2E	192k	59d 03:27:50
HS-WIRELESS	frios		00:0E:2E:7A:30:15	192k	45d 23:27:49
HS-WIRELESS	sancristobal		00:02:6F:35:51:54	192k	38d 18:38:15
HS-WIRELESS	pluggren		00:0E:2E:AD:F6:7A	192k	37d 00:41:23
HS-WIRELESS	vanhaeze		00:0E:2E:AE:46:F4	192k	29d 11:04:14
HS-WIRELESS	santalucia		00:60:B3:8C:A7:08	192k	26d 03:22:26
HS-WIRELESS	molicentro		00:0E:2E:AD:EF:5E	192k	20d 11:01:23
HS-WIRELESS	jmfurio		00:0A:E9:06:2F:8C	192k	19d 23:24:22
HS-WIRELESS	agroaerea		00:0E:2E:8D:2A:46	192k	18d 04:08:27
HS-WIRELESS	comejo		00:0E:2E:84:8F:6A	192k	16d 15:08:17
HS-WIRELESS	mcarina		00:02:6F:37:D6:16	192k	14d 04:13:14
HS-WIRELESS	agonzalez		00:0E:2E:AF:30:83	192k	13d 08:15:39
HS-WIRELESS	quaranta		00:0E:2E:B2:0D:26	192k	3d 08:40:02
HS-WIRELESS	guaragna		00:0E:2E:AA:B7:F2	192k	1d 12:09:45
HS-WIRELESS	sanmartin		00:0E:2E:B2:0C:EE	256k	250d 02:47:26
HS-WIRELESS	yaguane		00:0E:2E:8D:00:F7	256k	221d 16:12:24
HS-WIRELESS	semycer		00:0E:2E:85:2A:FE	256k	204d 10:35:41
HS-WIRELESS	uner		00:0E:2E:8D:23:2C	256k	146d 10:43:44
HS-WIRELESS	empcomercio		00:0E:2E:AA:B8:01	256k	75d 02:34:59

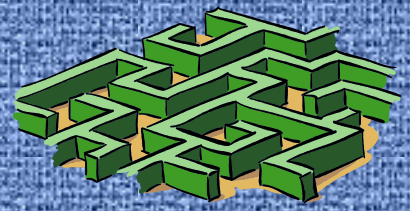
- Manteniendo una buena gestión en la carga de Usuarios y sus MACs, se establece una excelente seguridad en el acceso de los mismos.



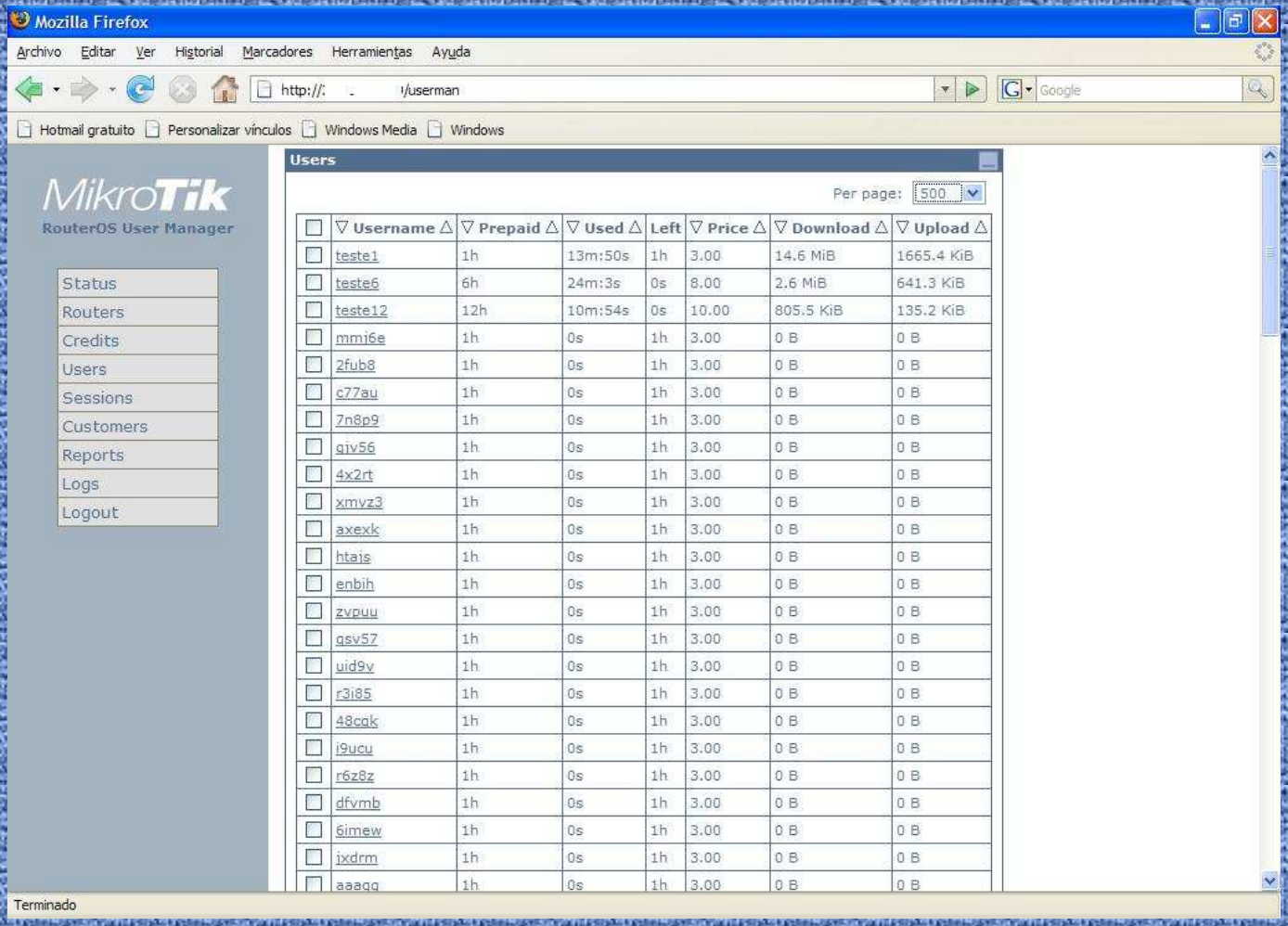
HotSpot: IP-Bindings



- En IP-Bindings es importante mantener actualizadas y unidas las MACs e IPs de los clientes, para aumentar el nivel de seguridad y control de acceso.
- Tambien es útil para permitir a algunos hosts o subredes pasar de largo al servicio Hotspot o bloquear su acceso a la red definitivamente.



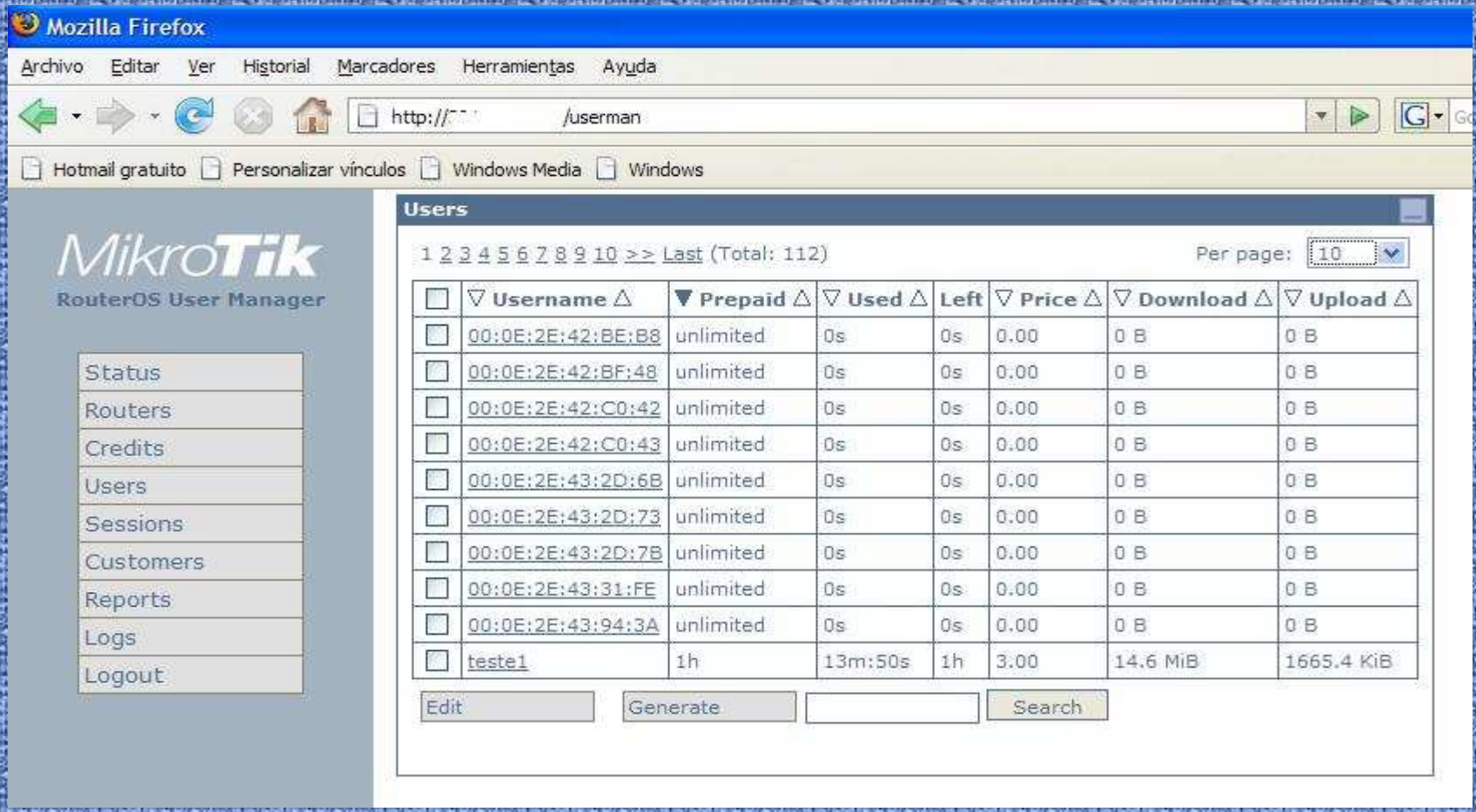
User Manager: Acceso Prepago



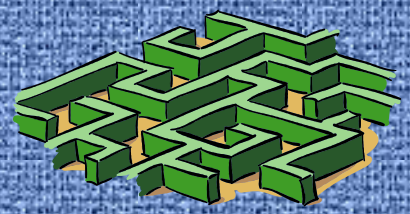
Username	Prepaid	Used	Left	Price	Download	Upload
teste1	1h	13m:50s	1h	3.00	14.6 MiB	1665.4 KiB
teste6	6h	24m:3s	0s	8.00	2.6 MiB	641.3 KiB
teste12	12h	10m:54s	0s	10.00	805.5 KiB	135.2 KiB
mmi6e	1h	0s	1h	3.00	0 B	0 B
2fub8	1h	0s	1h	3.00	0 B	0 B
c77au	1h	0s	1h	3.00	0 B	0 B
7n8p9	1h	0s	1h	3.00	0 B	0 B
qiv56	1h	0s	1h	3.00	0 B	0 B
4x2rt	1h	0s	1h	3.00	0 B	0 B
xmvz3	1h	0s	1h	3.00	0 B	0 B
axexk	1h	0s	1h	3.00	0 B	0 B
htais	1h	0s	1h	3.00	0 B	0 B
enbih	1h	0s	1h	3.00	0 B	0 B
zvpuu	1h	0s	1h	3.00	0 B	0 B
qsv57	1h	0s	1h	3.00	0 B	0 B
uid9v	1h	0s	1h	3.00	0 B	0 B
r3i85	1h	0s	1h	3.00	0 B	0 B
48cqk	1h	0s	1h	3.00	0 B	0 B
i9ucu	1h	0s	1h	3.00	0 B	0 B
r6z8z	1h	0s	1h	3.00	0 B	0 B
dfvmb	1h	0s	1h	3.00	0 B	0 B
6imew	1h	0s	1h	3.00	0 B	0 B
jxdrm	1h	0s	1h	3.00	0 B	0 B
aaaqq	1h	0s	1h	3.00	0 B	0 B

- Ahora con User Manager, Mikrotik incorporó la funcionalidad de Servidor RADIUS que tanta falta hacía en el sistema para centralizar la administración de nuestras redes.
- Podemos crear multiples cuentas en un solo click, vender tickets impresos, y permitir a los clientes ingresar a su cuenta vía Web para ver su estado, consumo, cambiar su contraseña y sus datos y tambien cargar crédito a su cuenta vía PayPal o Autorize.net

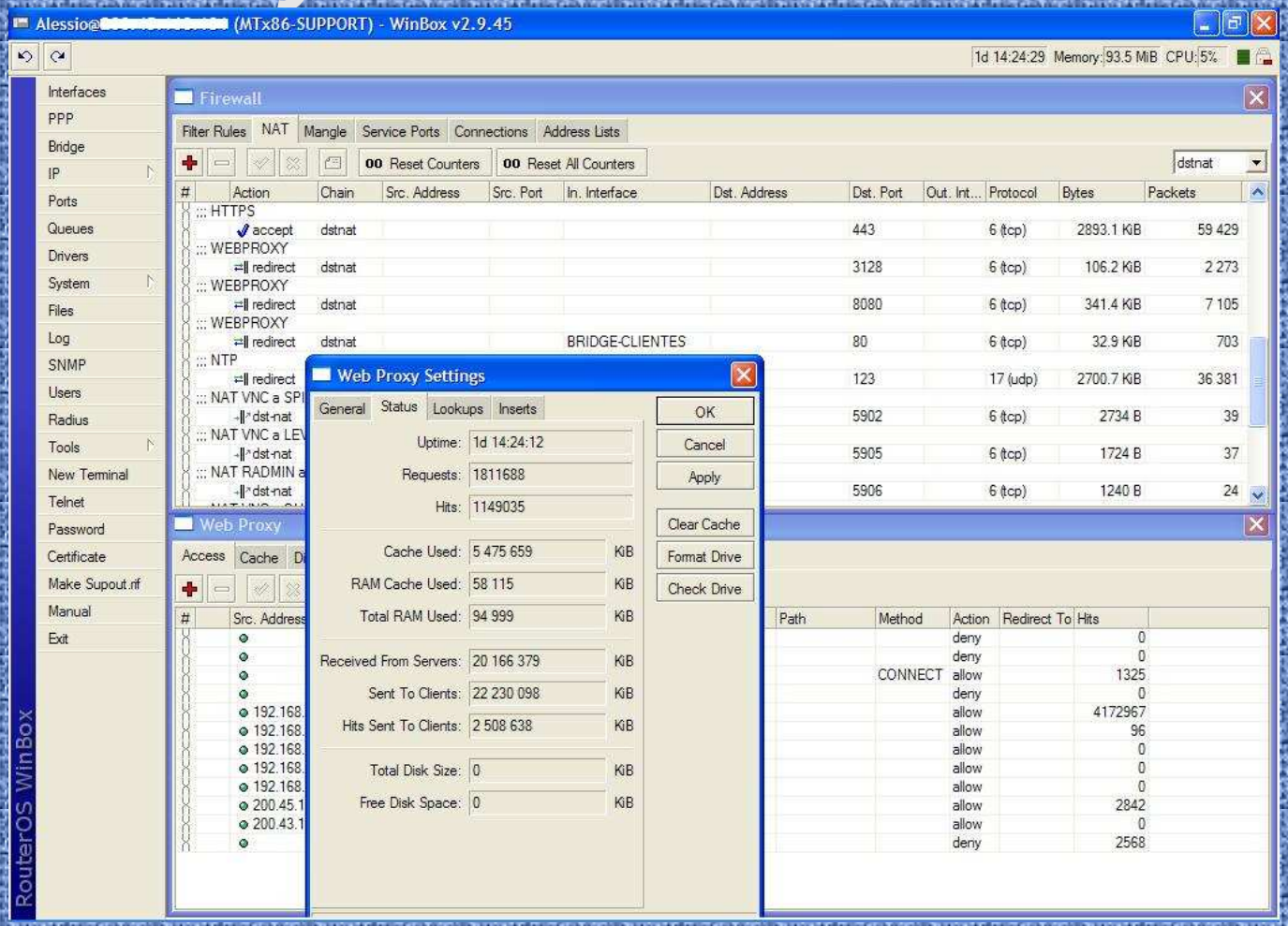
User Manager: Wireless MAC Control



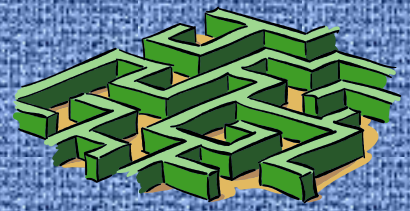
- Otra de las ventajas de User Manager, es la de permitirnos unificar la gestión de MAC de todos los CPEs que integran la red en único lugar.
- De esta manera, nos facilita la administración y permite a los clientes conectarse a cualquier nodo de la red (fail-over)



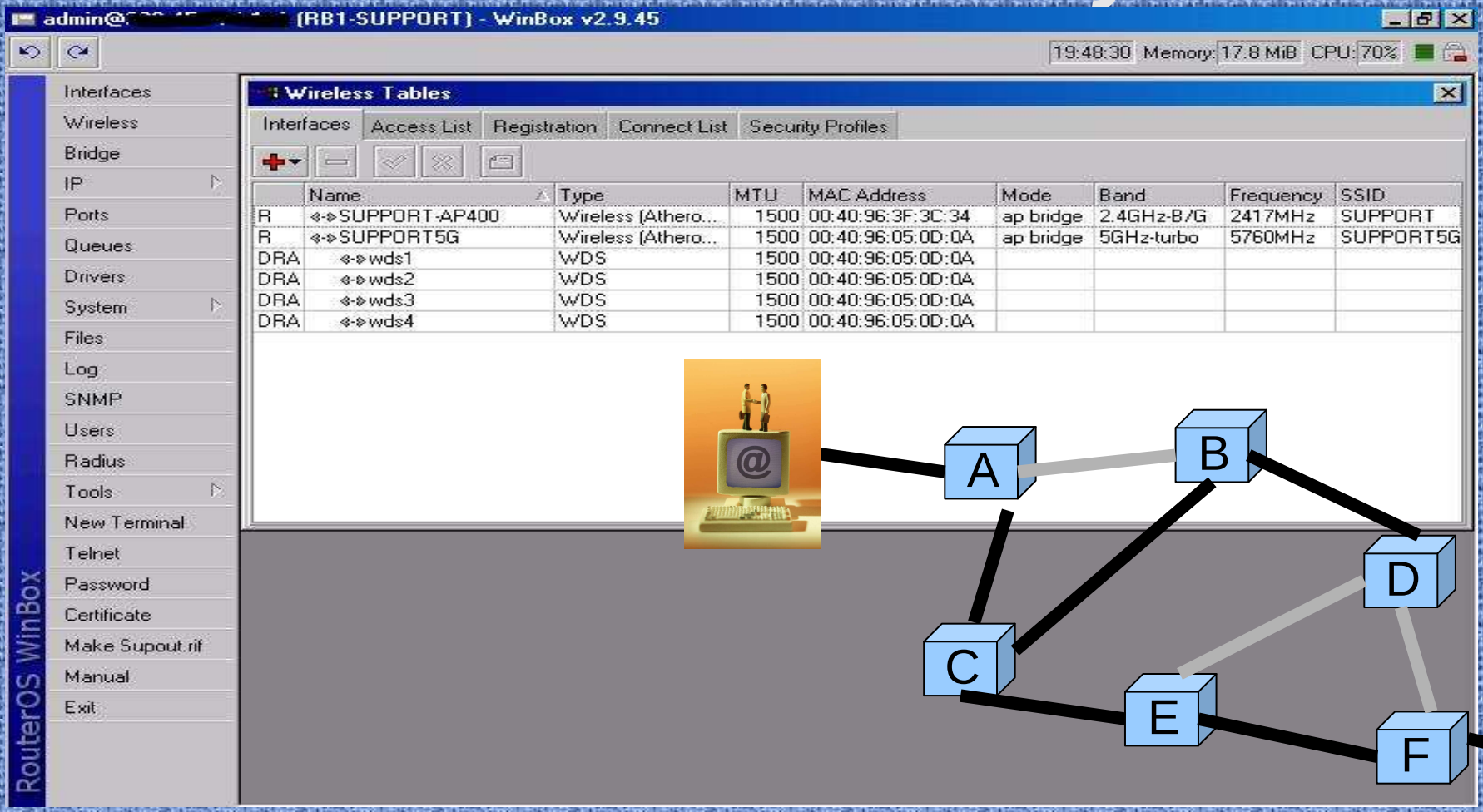
WebProxy Caché: Aceleración Web



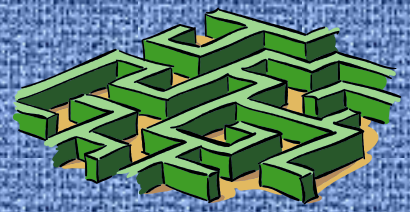
- WebProxy nos permite ahorrar ancho de banda (~40%) y acelerar la velocidad de navegación por Internet, ya que guarda las páginas visitadas anteriormente en su caché.
- Otra buena función es la de permitir realizar control de contenido mediante reglas de filtrado URL



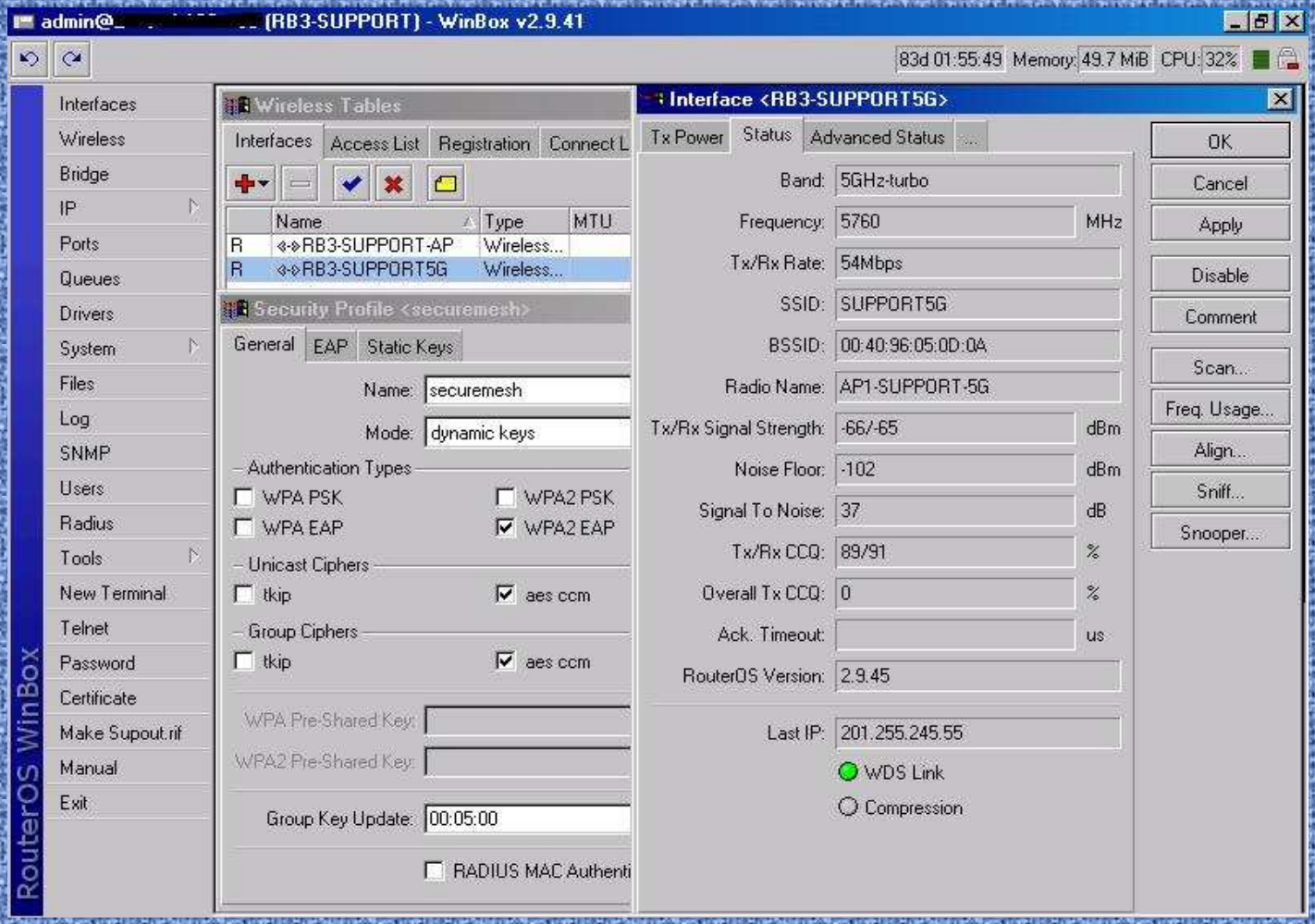
Wireless Mesh: WDS y RSTP



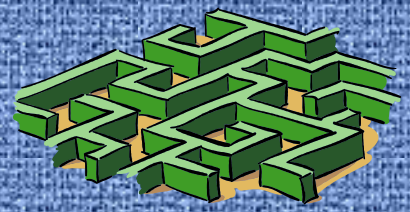
- En una red Wireless Mesh, para obtener alta disponibilidad, cada nodo debe interconectarse con al menos 2 o más nodos por enlaces WDS dinámicos.
- Para controlar la red, evitando loops y adicionando tolerancia a fallas, utilizaremos Bridge con Protocolo RSTP en toda la red.



Wireless Mesh: Características



- La interconexión entre nodos debe caracterizarse por ser de alto rendimiento, disponibilidad y seguridad, por lo que es recomendable realizarlo en modo 5Ghz-Turbo con Nstreme, WDS Dinámico y Seguridad WPA2-EAP con AES



Wireless Mesh: APs y Clientes

admin@ (RB1-SUPPORT) - WinBox v2.9.45

19:50:50 Memory: 18.0 MiB CPU: 79%

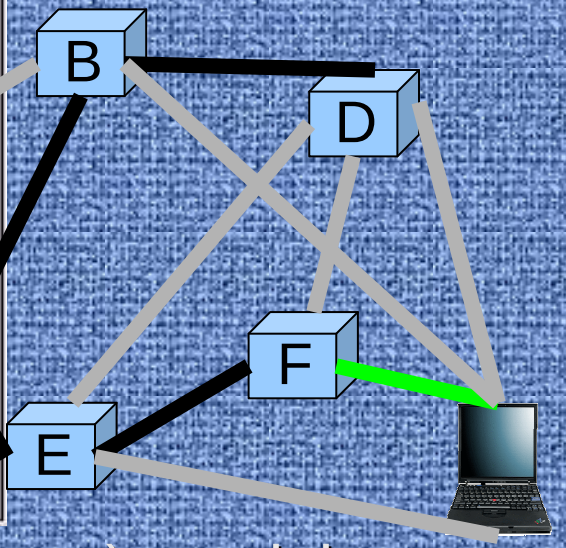
RouterOS WinBox

- Interfaces
- Wireless
- Bridge
- IP
- Ports
- Queues
- Drivers
- System
- Files
- Log
- SNMP
- Users
- Radius
- Tools
- New Terminal
- Telnet
- Password
- Certificate
- Make Supout.rif
- Manual
- Exit

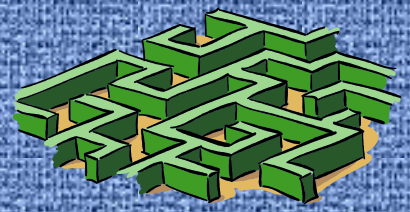
Scan <SUPPORT-AP400> (running)

Start | Stop | Close | Connect

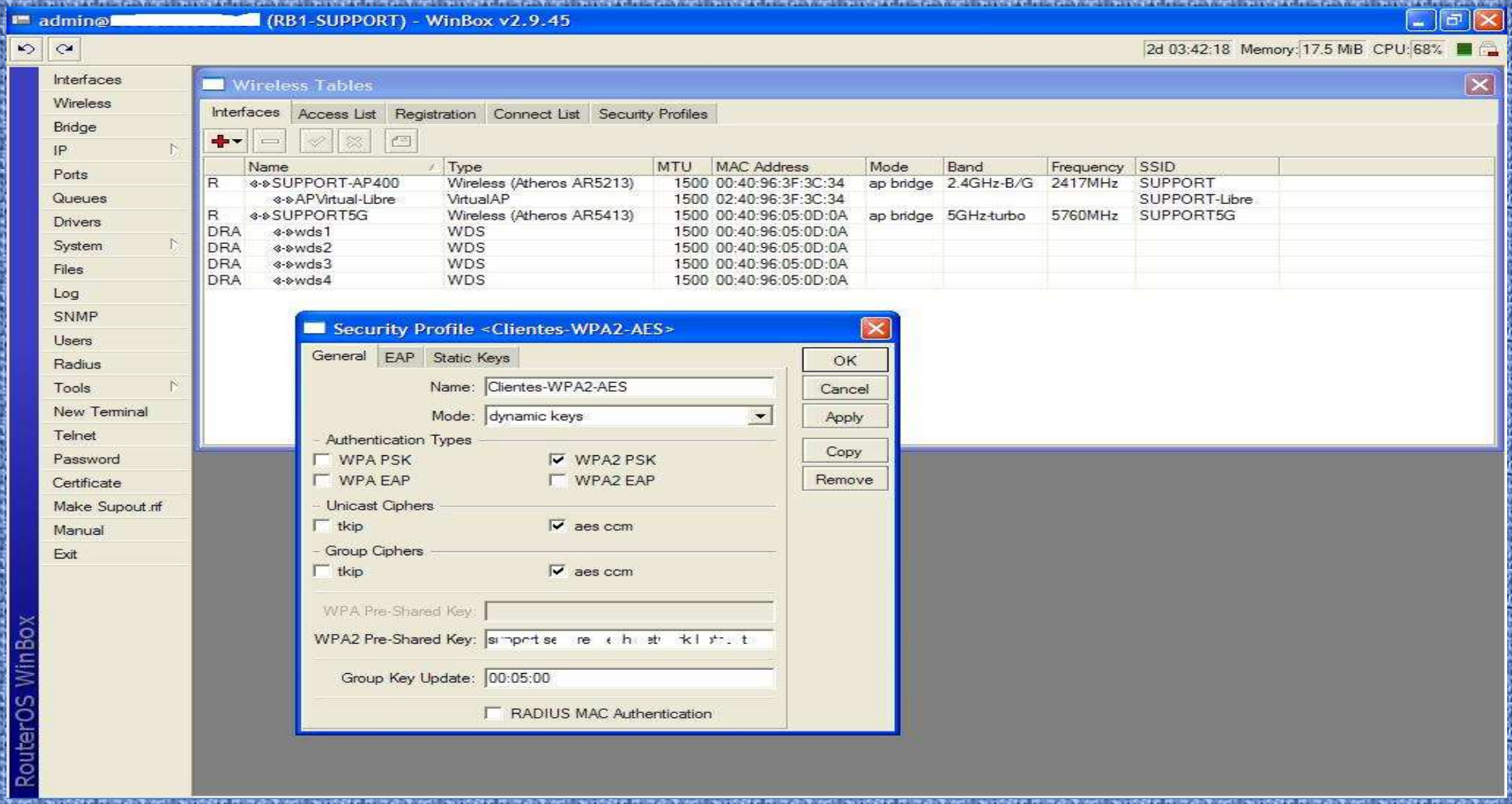
	Address	SSID	Band	Fre...	Signa...	Radio Name	RouterO...
BP	00:02:6F:21:CE:2F	CENTER	2.4GHz-G	2412	-92		
ABR	00:0C:42:0C:D8:A3	SUPPORT	2.4GHz-G	2412	-74	RB1-SUPPORT-AP2G	2.9.45
ABP	00:11:3B:02:02:30	default	2.4GHz-G	2412	-85		
AB	00:02:6F:44:8D:58	lan16	2.4GHz-G	2412	-82		
AB	00:02:6F:35:35:25	lan2	2.4GHz-G	2412	-83		
AB	00:19:E0:96:15:7C	▮▮▮▮	2.4GHz-G	2417	-76		
AB	00:02:6F:07:5F:4B	lan3	2.4GHz-G	2422	-83		
ABR	00:0A:E9:06:2E:BB	support2	2.4GHz-G	2422	-87	AP-RB$-SUPPORTCA	2.9.42
ABR	00:40:96:51:05:5A	SUPPORT	2.4GHz-G	2427	-77	SUPPORT-AP2	2.9.41
ABR	00:0C:42:0C:D8:9A	SUPPORT	2.4GHz-G	2437	-75	RB9-AP-SUPPORT	2.9.43
AB	00:02:2D:65:EE:0A	lan4	2.4GHz-G	2437	-88		
AB	00:02:6F:44:2E:D9	SUPPORT	2.4GHz-G	2447	-74		
AB	00:02:6F:44:8D:51	support2	2.4GHz-G	2447	-81		
AB	00:40:96:44:2E:CE	SUPPORT	2.4GHz-G	2462	-84		



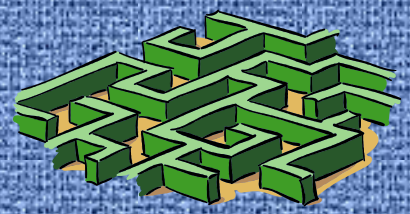
- Para brindar alta disponibilidad a los clientes (fail-over), se deben configurar todos los APs con un mismo SSID y la misma seguridad. No necesitan soportar WDS ni estar en la misma frecuencia.



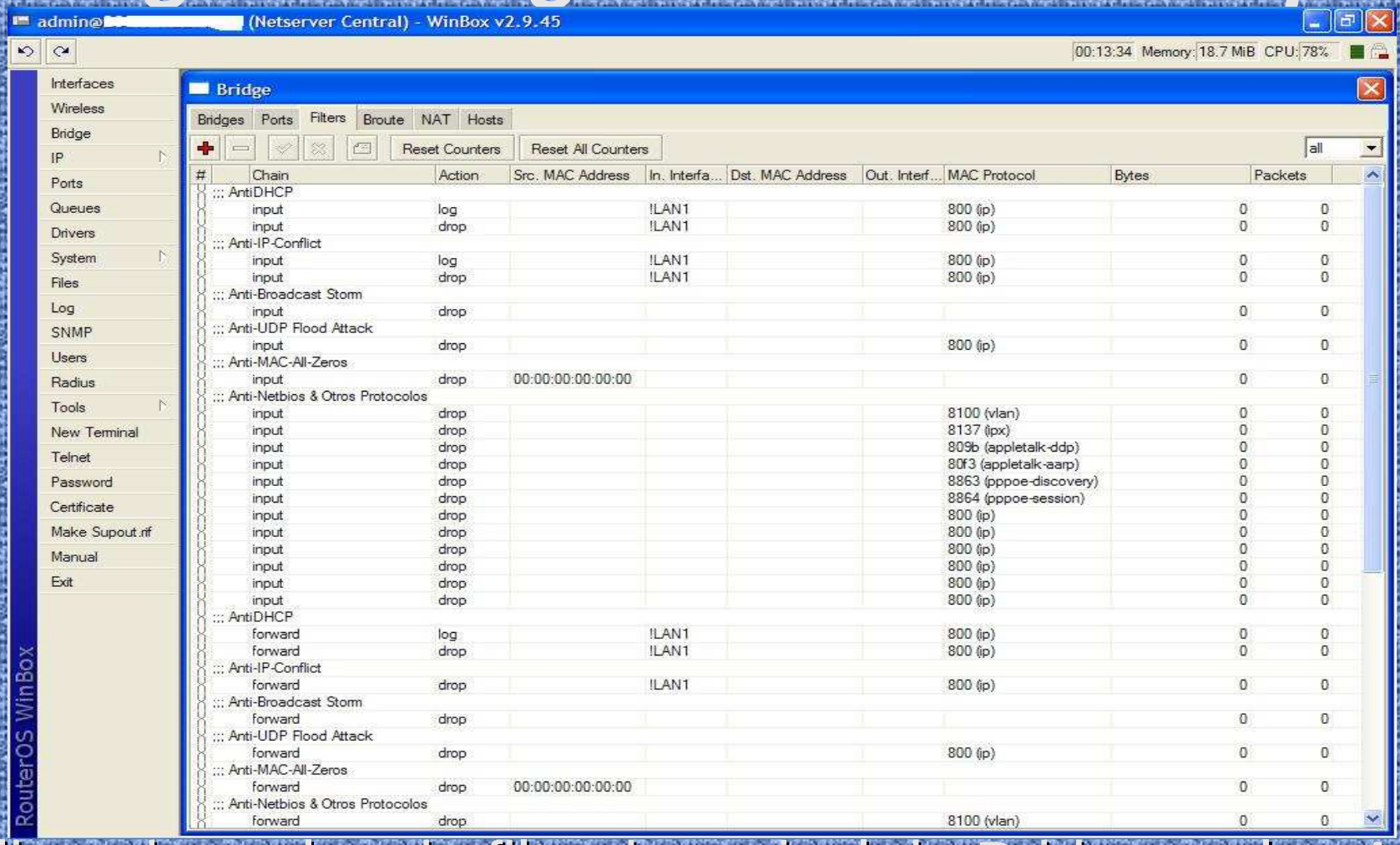
Wireless Mesh: Acceso Libre



- Por medio de APs Virtuales, se permite acceso libre a la red, para usuarios que quieren probar el sistema.
- Estos son atendidos por otro HotSpot Server en el mismo Servidor e invitados en la web de autenticación Hotspot a utilizar el servicio en forma limitada en la modalidad “Trial”

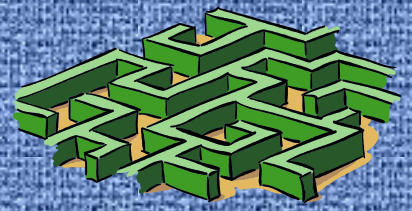


Bridge: Protegiendo APs en Capa 2



#	Chain	Action	Src. MAC Address	In. Interfa...	Dst. MAC Address	Out. Interf...	MAC Protocol	Bytes	Packets
	;;; AntiDHCP								
	input	log		!LAN1			800 (ip)	0	0
	input	drop		!LAN1			800 (ip)	0	0
	;;; Anti-IP-Conflict								
	input	log		!LAN1			800 (ip)	0	0
	input	drop		!LAN1			800 (ip)	0	0
	;;; Anti-Broadcast Storm								
	input	drop						0	0
	;;; Anti-UDP Flood Attack								
	input	drop					800 (ip)	0	0
	;;; Anti-MAC-All-Zeros								
	input	drop	00:00:00:00:00:00					0	0
	;;; Anti-Netbios & Otros Protocolos								
	input	drop					8100 (vlan)	0	0
	input	drop					8137 (ipx)	0	0
	input	drop					809b (appletalk-ddp)	0	0
	input	drop					80f3 (appletalk-aarp)	0	0
	input	drop					8863 (pppoe-discovery)	0	0
	input	drop					8864 (pppoe-session)	0	0
	input	drop					800 (ip)	0	0
	input	drop					800 (ip)	0	0
	input	drop					800 (ip)	0	0
	input	drop					800 (ip)	0	0
	input	drop					800 (ip)	0	0
	;;; AntiDHCP								
	forward	log		!LAN1			800 (ip)	0	0
	forward	drop		!LAN1			800 (ip)	0	0
	;;; Anti-IP-Conflict								
	forward	drop		!LAN1			800 (ip)	0	0
	;;; Anti-Broadcast Storm								
	forward	drop						0	0
	;;; Anti-UDP Flood Attack								
	forward	drop					800 (ip)	0	0
	;;; Anti-MAC-All-Zeros								
	forward	drop	00:00:00:00:00:00					0	0
	;;; Anti-Netbios & Otros Protocolos								
	forward	drop					8100 (vlan)	0	0

- Aplicando reglas de filtrado a nivel de Bridge en los APs, evitamos problemas de redes muy comunes que ocurren a diario, aveces intencionalmente por usuarios maliciosos



QoS: Ecualizando Servicios

admin@[redacted] (MTx86-NETSERVER) - WinBox v2.9.46

CPU: 40%

RouterOS WinBox

- Interfaces
- PPP
- Bridge
- IP
- Ports
- Queues
- Drivers
- System
- Files
- Log
- SNMP
- Users
- Radius
- Tools
- New Terminal
- Telnet
- Password
- Certificate
- Make Supout.rif
- Manual
- Exit

Queue List

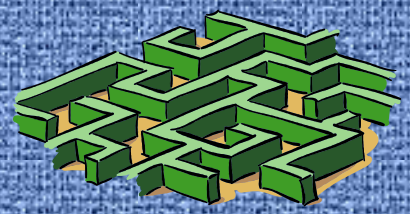
Simple Queues | Interface Queues | Queue Tree | Queue Types

Reset Counters | Reset All Counters

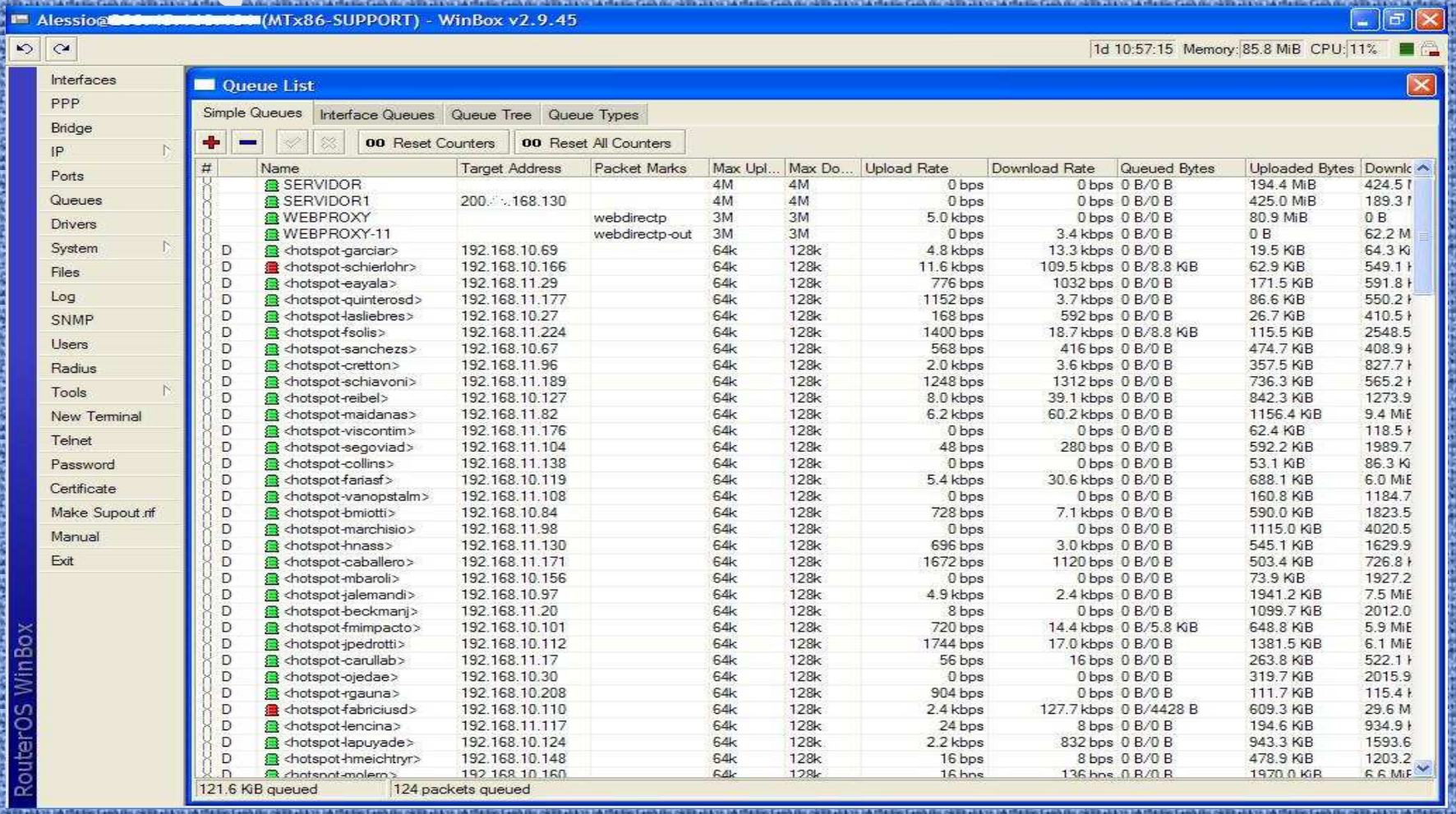
Name	Parent	Packet Mark	Limit At	Max Limit	Rate	Queued Bytes	Bytes	Packets
CLIENTES-IN	global-total		0	10M	5.6 Mbps	0 B	62922.9 MiB	154 814 743
DNS	CLIENTES-IN	dnsp	128k	256k	0 bps	0 B	0 B	0
FTP-In	CLIENTES-IN	ftpf	128k	256k	0 bps	0 B	37.5 MiB	74 260
ICMP	CLIENTES-IN	icmpp	320k	512k	4.6 kbps	0 B	82.0 MiB	1 116 428
MSN-In	CLIENTES-IN	msnf	500k	1M	65.9 kbps	0 B	632.1 MiB	3 278 644
Otros-In	CLIENTES-IN	other	0	2M	1072.6 kbps	0 B	14693.5 MiB	51 328 946
P2P-In	CLIENTES-IN	p2p	0	128k	110.3 kbps	0 B	3657.7 MiB	19 536 279
POP3-In	CLIENTES-IN	pop3f	5M	10M	0 bps	0 B	264.9 MiB	422 576
PPTP	CLIENTES-IN	pptp	512k	1M	72 bps	0 B	9.3 MiB	42 945
SMTP-In	CLIENTES-IN	smtpf	5M	10M	920 bps	0 B	142.8 MiB	266 921
VOIP-In	CLIENTES-IN	voip	512k	1M	37.7 kbps	0 B	1923.3 MiB	3 103 224
Web-In	CLIENTES-IN	webp	2M	4M	194.2 kbps	0 B	2343.2 MiB	17 711 916
WebDirect-IN	CLIENTES-IN	web-directp	1M	2M	6.4 kbps	0 B	885.4 MiB	1 959 489
WebProxy-IN	CLIENTES-IN	webproxyf	3M	4M	1959.8 kbps	0 B	17496.6 MiB	17 067 484
Webproxy-In	CLIENTES-IN	webproxyf-out	2M	4M	2.1 Mbps	0 B	20758.4 MiB	38 920 675
PUBLICA-OUT	WAN4-TELECOM		0	4M	556.8 kbps	0 B	7283.9 MiB	50 028 161
DNS-OUT	PUBLICA-OUT	dnsp	128k	256k	0 bps	0 B	0 B	0
FTP-Out	PUBLICA-OUT	ftpf	128k	256k	0 bps	0 B	5.9 MiB	35 125
ICMP-OUT	PUBLICA-OUT	icmpp	320k	512k	1808 bps	0 B	16.2 MiB	156 357
MSN-Out	PUBLICA-OUT	msnf	500k	1M	23.5 kbps	0 B	280.9 MiB	1 694 904
Otros-Out	PUBLICA-OUT	other	0	1M	286.9 kbps	0 B	3445.0 MiB	26 622 021
P2P-Out	PUBLICA-OUT	p2p	0	128k	0 bps	0 B	751.3 MiB	2 454 382
POP3-OUT	PUBLICA-OUT	pop3f	5M	10M	0 bps	0 B	8.2 MiB	151 832
PPTP-OUT	PUBLICA-OUT	pptp	512k	1M	32 bps	0 B	4551.0 KiB	22 280
SMTP-OUT	PUBLICA-OUT	smtpf	5M	10M	864 bps	0 B	137.9 MiB	140 055
VOIP-OUT	PUBLICA-OUT	voip	256k	512k	1592 bps	0 B	167.4 MiB	1 299 692
Web-Out	PUBLICA-OUT	webp	2M	4M	0 bps	0 B	1240.2 KiB	5 899
WebDirect-OUT	PUBLICA-OUT	web-directp	1M	2M	920 bps	0 B	43.0 MiB	605 711
WebProxy-OUT	PUBLICA-OUT	webproxyf-out	2M	4M	228.8 kbps	0 B	2294.5 MiB	16 535 705
Webproxy-out	PUBLICA-OUT	webproxyf	2M	4M	12.2 kbps	0 B	127.4 MiB	304 198

215.9 KiB queued | 196 packets queued

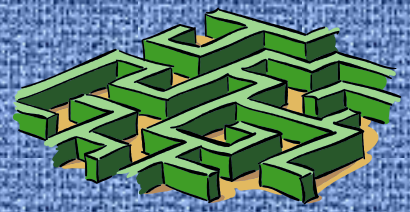
- Mikrotik nos ofrece una excelente posibilidad de detectar y marcar múltiples protocolos para luego en las Queues Tree realizar una ecualización de servicios, garantizando y priorizando ancho de banda acorde a las necesidades de cada uno.



QoS: Acelerando Servicios

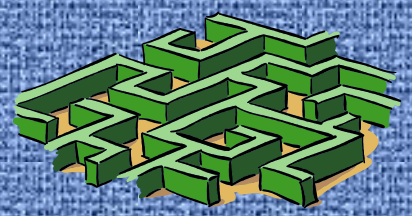


- Podemos permitir el acceso a los Servidores de Mail, Web y FTP locales y ciertas páginas importantes, a velocidades muy superiores a las contratadas por los usuarios; brindando de esta manera una Calidad de Servicio inigualable y muy perceptible.

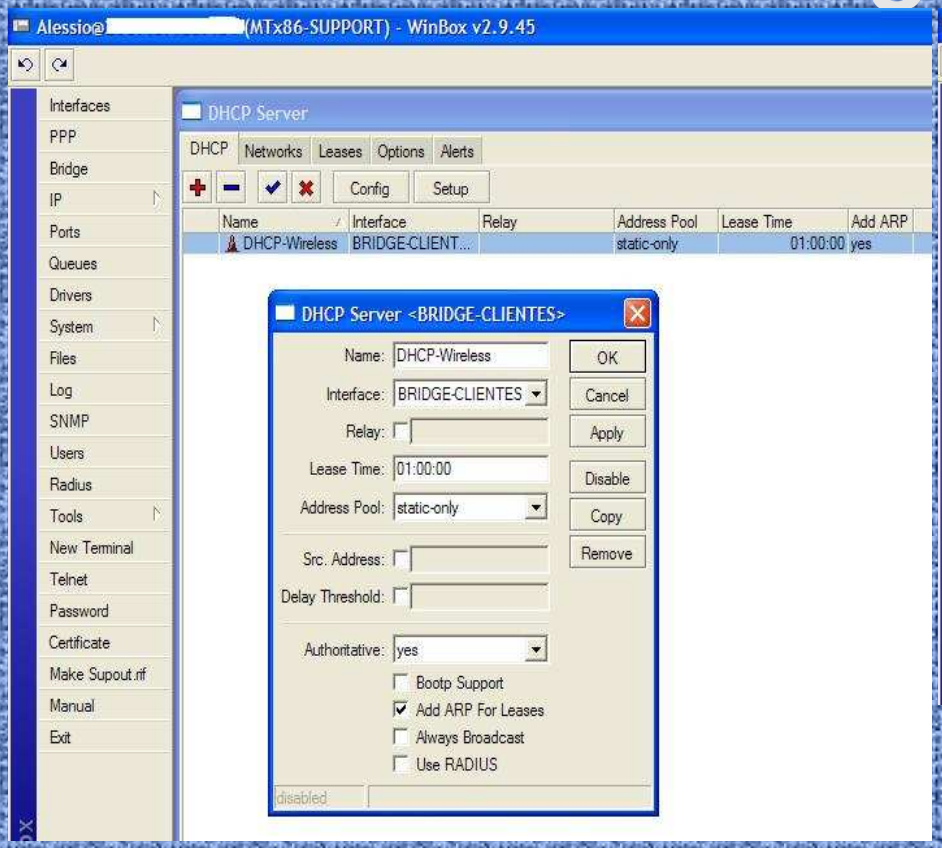


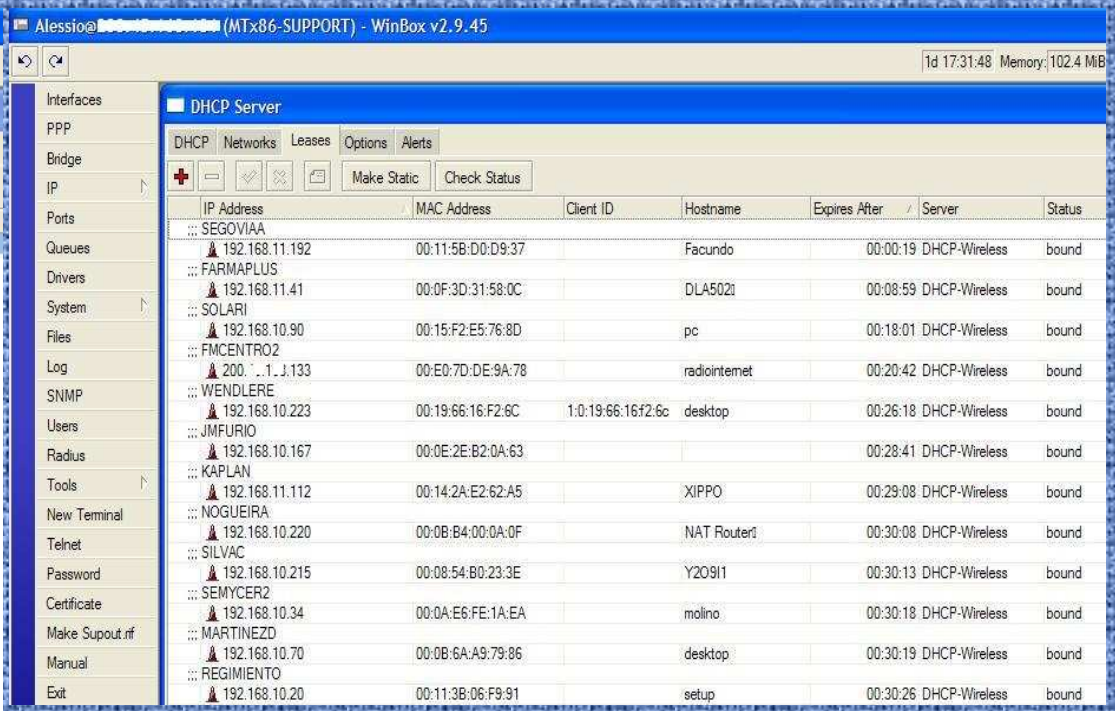
TIPs Adicionales de Seguridad

- Interfaces con ARP de sólo respuesta(reply-only)
- DHCP Leases Estáticos (con add ARP for Leases)
- Solución Anti-SPAM (para virus o spammers)

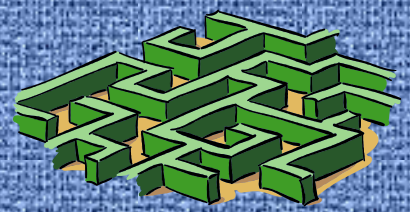


TIPs: Seguridad DHCP

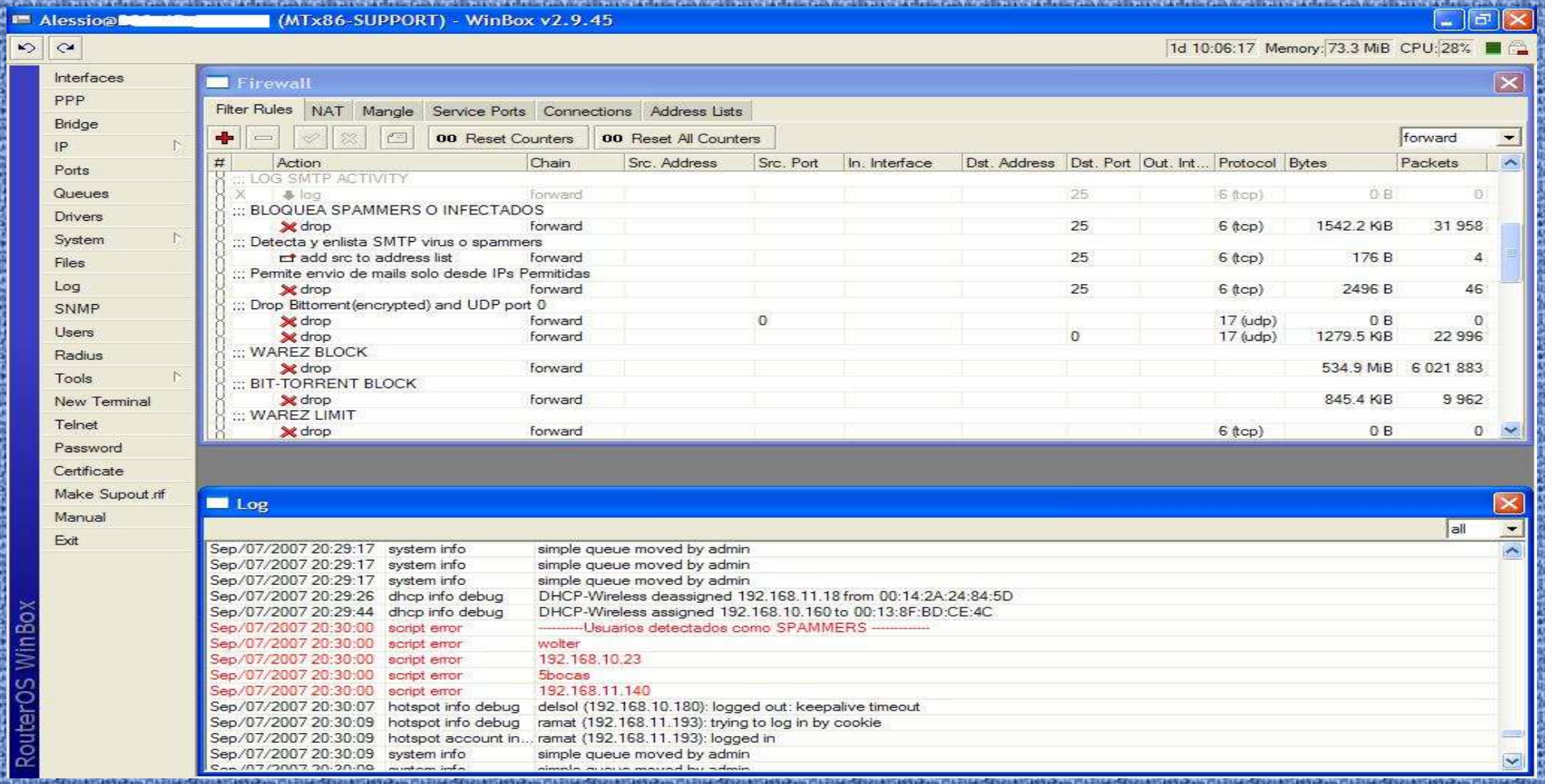




- Para adicionar mas de seguridad en la red, debemos configurar:
  - ARP=reply-only en la interfase por la que ingresan los clientes
  - DHCP-Server: Address-Pool=static-only y Add ARP For Leases=yes para que unicamente adicione en la tabla ARP a los hosts estáticos en Leases
  - DHCP-Server Leases: debemos hacer estáticos a todos los hosts que pertenecen a nuestra red (marcar todos y dar click en Make Static)

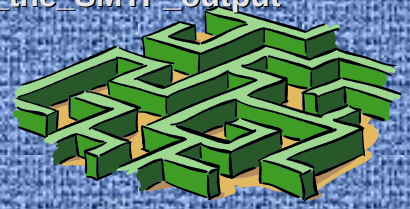


TIPs: Anti-SPAM



- Solución a los problemas de usuarios infectados por algun Virus Gusano (Worm) o a usuarios que quieren realizar actividades de envío masivo de correo electrónico (SPAM)
- Pueden encontrar mas info en el artículo publicado en el Wiki de Mikrotik.

http://wiki.mikrotik.com/wiki/How_to_autodetect_infected_or_spammer_users_and_temporary_block_the_SMTP_output



Muchas gracias por su atención!

Alessio Garavano
ISPARG S.A.
Soluciones IP Profesionales
www.isparg.com.ar
info@isparg.com.ar