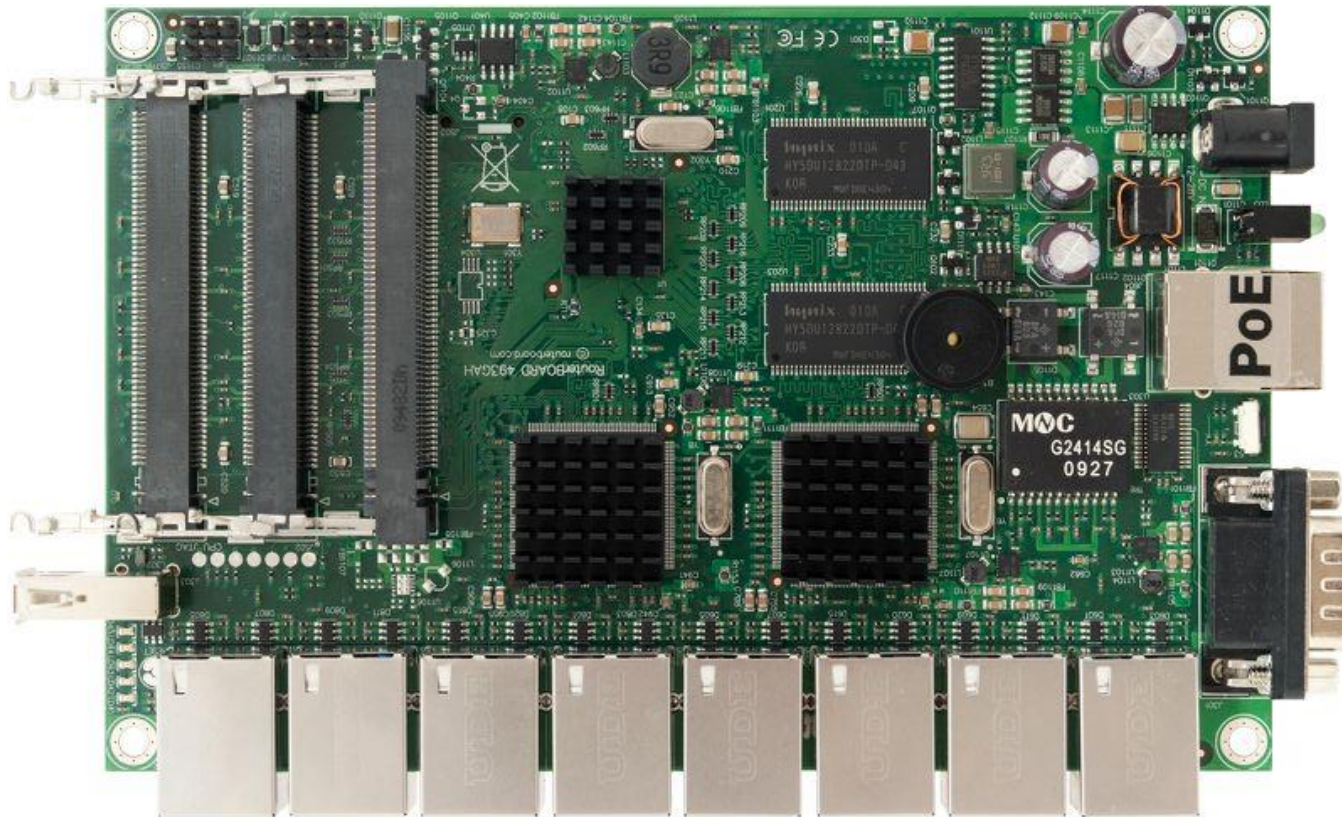


MÓDULO 3 | GESTIÓN DE RED



ARP

- Iniciales de “Address Resolution Protocol”
- Es un mecanismo que enlaza las direcciones IPs de capa 3 y las direcciones MAC de capa 2.
- Normalmente se usa como un proceso dinámico, pero puede ser configurado de forma estática en ciertas situaciones donde la seguridad lo garantice.

Modos ARP

- “ARP modes” le indica al RouterOS como debe comportarse ARP
 - Los modos se configuran “por interface”
- Los “modos” son:
 - **Enabled:** Modo por defecto. ARP las peticiones de ARP son contestadas y la tabla ARP se rellena automáticamente
 - **Disabled:** El interfaz no enviará o contestará peticiones ARP. Hay que indicar al resto de equipos la MAC del router
 - **Proxy ARP:** El router contesta peticiones ARP dirigidas a su red directamente conectada (independientemente del origen)
 - **Reply only:** El router constesta peticiones ARP. La tabla ARP del router se tiene que llenar de forma estática

Configurar ARP

- En menú interfaces elegir interfaz
 - En la pestaña General escoger listado ARP.

Interface <ether1>

General | Ethernet | Loop Protect | Status | Traffic

Name: ether1

Type: Ethernet

MTU: 1500

Actual MTU: 1500

L2 MTU: 1526

MAC Address: 00:0C:42:C8:41:67

ARP: enabled

ARP Timeout: enabled

OK

Cancel

Apply

Disable

Comment

Torch

Cable Test

Blink

Reset MAC Address

Reset Counters

running slave no link

Interface List

Interface | Interface List | Ethernet | EoIP Tunnel | IP Tunnel | GRE Tunnel | VLAN | VRRP | Bonding | LTE

+ - ✓ ✗

Detect Internet

Find

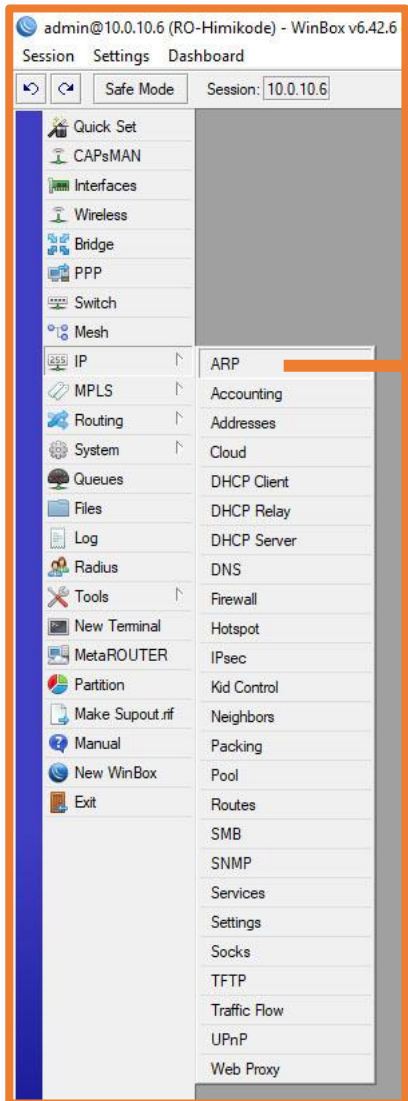
	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
R	br-LAN	Bridge	1500	1522	21.1 kbps	2.2 kbps	6	4	0 bps	0 bps	0	0
R	vlan2225_inv	VLAN	1500	1518	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R	vlan2226	VLAN	1500	1518	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R	eoip-WAN	EoIP Tunnel	1408	65535	105.5 kbps	25.9 kbps	12	12	0 bps	0 bps	0	0
R	ether1	Ethernet	1500	1526	0 bps	0 bps	0	0	0 bps	0 bps	0	0
RS	ether2	Ethernet	1500	1522	21.4 kbps	2.6 kbps	6	4	0 bps	0 bps	0	0
S	ether3	Ethernet	1500	1522	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether4	Ethernet	1500	1522	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether5	Ethernet	1500	1522	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether6	Ethernet	1500	1522	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether7	Ethernet	1500	1522	0 bps	0 bps	0	0	0 bps	0 bps	0	0
RS	ether8	Ethernet	1500	1522	480 bps	0 bps	1	0	0 bps	0 bps	0	0
R	ether9-WAN	Ethernet	1500	1522	105.1 kbps	34.1 kbps	12	12	0 bps	0 bps	0	0
XS	wlan2.4	Wireless (Atheros AR9...	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0
XS	wlan5	Wireless (Atheros AR9...	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0

15 items (1 selected)

Tabla ARP

- La tabla ARP muestra todas las entradas y el interfaz por el que se han aprendido.
- La tabla ARP proporciona:
 - La dirección IP de los dispositivos conocidos
 - La dirección MAC asociada con la dirección IP
 - El interfaz por el que han sido aprendidas
- Se pueden agregar entradas estáticas a la tabla ARP para securizar la red
 - Evitamos ARP poisoning / ARP spoofing
 - Requiere muuuucho trabajo y planificación

TABLA ARP



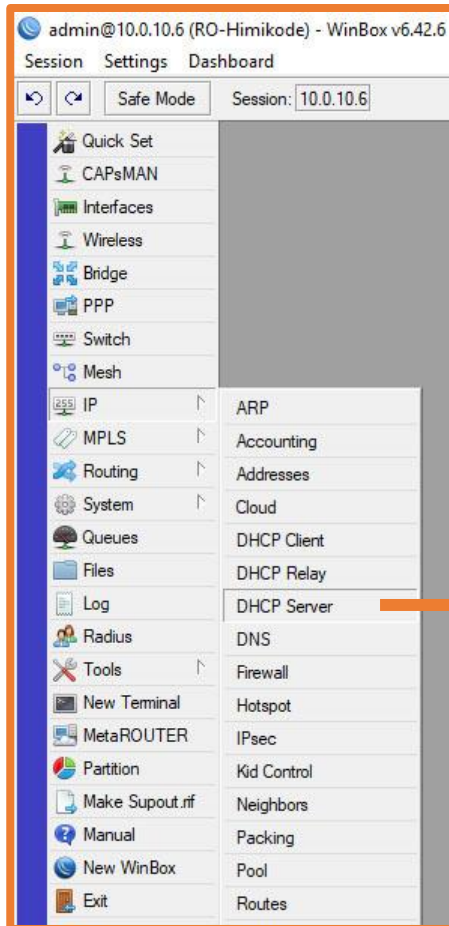
ARP List

	IP Address	MAC Address	Interface
DC	10.0.10.1	64:D1:54:D4:CB:39	ether9-WAN
DC	10.0.10.5	02:19:E3:1E:06:DF	eoip-WAN
DC	192.168.30.78	04:69:F8:EC:6C:A4	br-LAN
DC	192.168.30.79	78:88:6D:57:27:BF	br-LAN
D	192.168.30.87	6C:40:08:B6:ED:EE	br-LAN
D	192.168.30.89	A8:5C:2C:5F:1B:ED	br-LAN
D	192.168.30.90	B0:E2:35:8E:B9:4C	br-LAN
DC	192.168.30.91	00:0B:82:B6:82:5F	br-LAN
D	192.168.30.93	00:26:4A:16:3C:04	br-LAN
DC	192.168.30.99	F0:9F:C2:2C:0B:90	br-LAN
DC	192.168.99.109	74:D2:1D:FF:18:08	vlan2225_inv

11 items

SERVIDOR DHCP

- Iniciales de Dynamic Host Configuration Protocol
- Se usa para asignar automáticamente direcciones IP, mascara, puertas de enlace, y opcionalmente, otros parametros que pidan los clientes



DHCP Server

DHCP Networks Leases Options Option Sets Alerts

+ - ✓ ✗ Filter DHCP Config DHCP Setup Find

Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp-LAN	br-LAN		00:10:00	LAN_pool	no
dhcp-inv	vlan2225_inv		00:10:00	inv_pool	no
dhcp1	vlan2226		00:10:00	dhcp_pool2	no

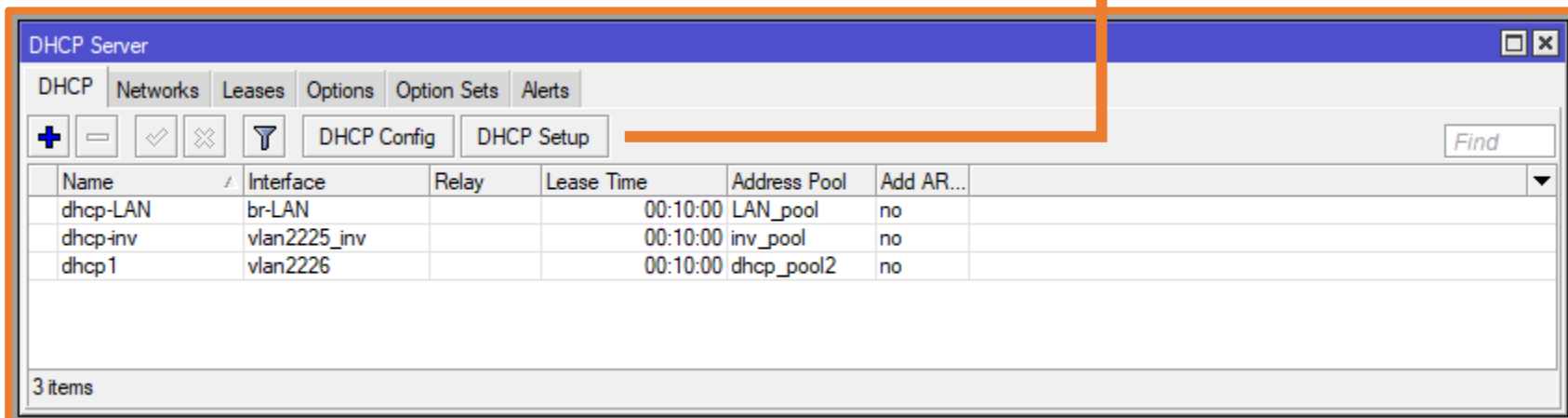
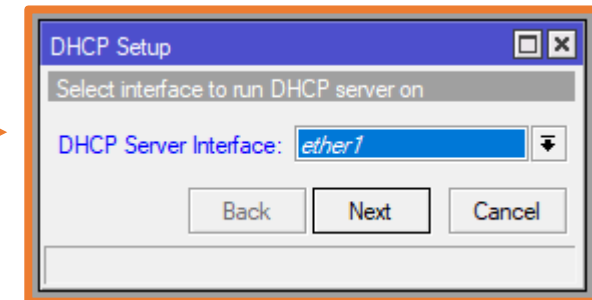
3 items

Configuración del Servidor de DHCP

- El interfaz que soportará el servidor de DHCP debe tener su propia dirección ip, la cual no estará incluida en el « address pool »
 - Un pool es un rango de direcciones IP que están disponibles para los clientes de enlace, y opcionalmente, otros parámetros que pidan los clientes
- En la ventana de DHCP-server, únicamente hay que pulsar el botón de “DHCP Setup” y contestar a las preguntas.
 - Interfaz del servidor DHCP
 - Espacio de direcciones del servidor DHCP
 - Gateway para la red DHCP
 - Direcciones para los clientes
 - Servidores de DNS (se pueden especificar varios)
 - Tiempo de concesión

LAB DHCP Server

- Crear un servidor DHCP en una interfaz
 - Recuerda, el primer paso es asignar una ip válida a la interfaz.
 - Crea un pool de Ips
 - Nombre y parametros (como la interfaz)

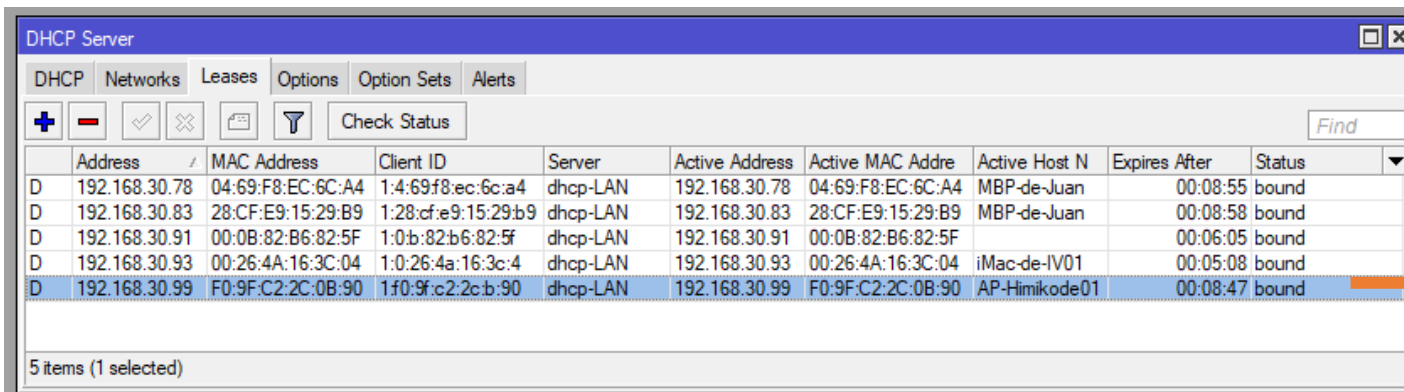


Otras Configuraciones DHCP

- El DHCP se puede utilizar para establecer opciones como
 - 42 : NTP Servers
 - 70 : POP3-Server
 - Visita <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml> para obtener mas opciones DHCP
- Importante
 - Si tienes un entorno con bridge, el servidor DHCP debe configurarse en el interfaz de bridge. Si se configura en uno de los puertos del bridge, el servidor de DHCP no funcionará.

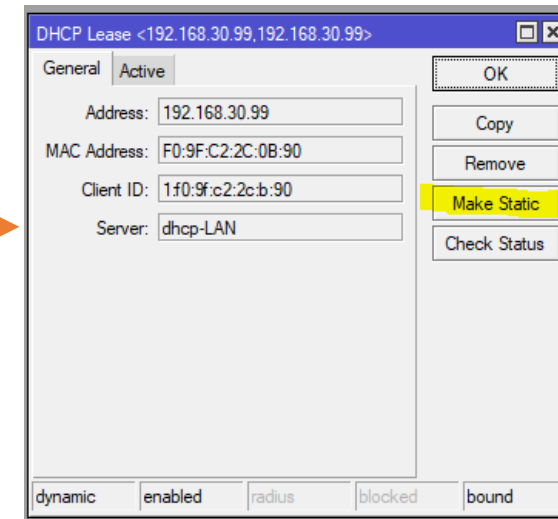
Gestión de la concesión DHCP Server

- La sección "/ip dhcp-server lease" proporciona información acerca de los clientes DHCP y las concesiones
- Muestra las concesiones estáticas y dinámicas.
- Puede convertir una concesión dinámica en estática
 - Es bastante útil cuando un cliente necesita mantener la misma dirección IP
 - ¡Ojo! Si se cambia la tarjeta de red de cliente, obtendrá una nueva dirección IP.



	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host N	Expires After	Status
D	192.168.30.78	04:69:F8:EC:6C:A4	1:4:69f8:ec:6c:a4	dhcp-LAN	192.168.30.78	04:69:F8:EC:6C:A4	MBP-de-Juan	00:08:55	bound
D	192.168.30.83	28:CF:E9:15:29:B9	1:28:cf:e9:15:29:b9	dhcp-LAN	192.168.30.83	28:CF:E9:15:29:B9	MBP-de-Juan	00:08:58	bound
D	192.168.30.91	00:0B:82:B6:82:5F	1:0:b:82b6:82:5f	dhcp-LAN	192.168.30.91	00:0B:82:B6:82:5F		00:06:05	bound
D	192.168.30.93	00:26:4A:16:3C:04	1:0:26:4a:16:3c:4	dhcp-LAN	192.168.30.93	00:26:4A:16:3C:04	iMac-de-IV01	00:05:08	bound
D	192.168.30.99	F0:9F:C2:2C:0B:90	1f0:9f:c2:2c:b:90	dhcp-LAN	192.168.30.99	F0:9F:C2:2C:0B:90	AP-Himikode01	00:08:47	bound

5 items (1 selected)



DHCP Lease <192.168.30.99,192.168.30.99>

General Active

Address: 192.168.30.99

MAC Address: F0:9F:C2:2C:0B:90

Client ID: 1f0:9f:c2:2c:b:90

Server: dhcp-LAN

Buttons: OK, Copy, Remove, **Make Static**, Check Status

dynamic enabled radius blocked bound

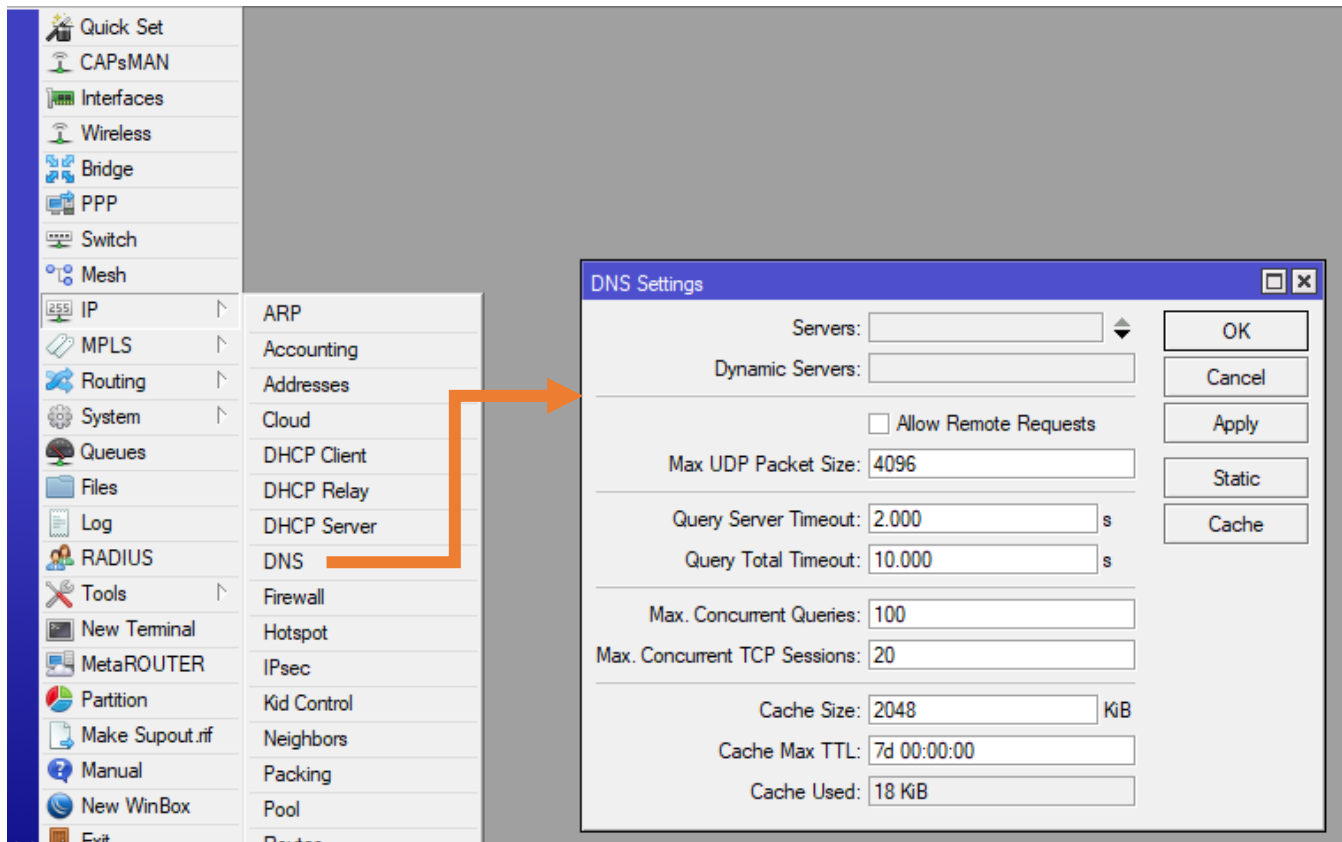
Gestión de la concesión DHCP Server

- El servidor de DHCP puede configurarse para trabajar únicamente con direcciones estáticas.
- Los clientes sólo recibirán la direcciones IP preconfiguradas.
- Evalua bien las necesidades antes de configurarlo de forma estática. Puede necesitar mucho trabajo y tiempo para redes grandes.

Cliente DHCP

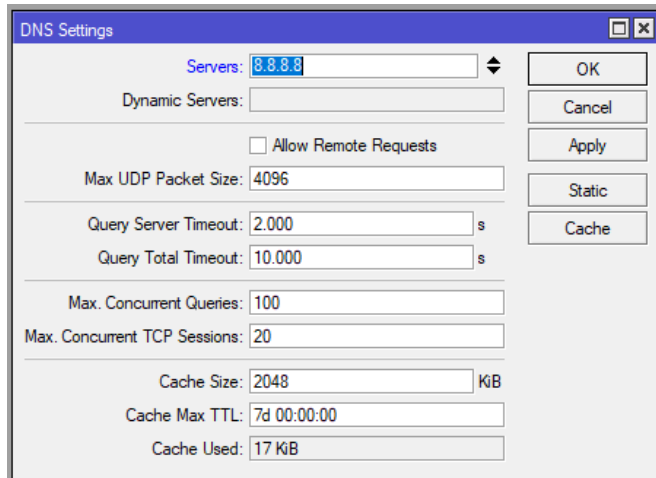
- Permite a los interfaces tipo ethernet solicitar una dirección IP.
 - El servidor DHCP remoto debe proporcionar:
 - Dirección
 - Máscara
 - Puerta de enlace
 - Dos servidores DNS (siempre que el servidor esté configurado)
 - El cliente DHCP debe proporcionar los datos:
 - Hostname
 - Clientid (en la forma de la dirección MAC)
- Se usa habitualmente en las interfaces conectadas a internet.

Domain Name Server



- Puerto 53 UDP (también puede utilizar TCP)
- Se encarga de resolver IP,s (difíciles de recordar por los humanos) por nombres de dominio.
- Si necesitamos resolver nombre de dominio desde nuestro Mikrotik deberemos configurar un servidor DNS

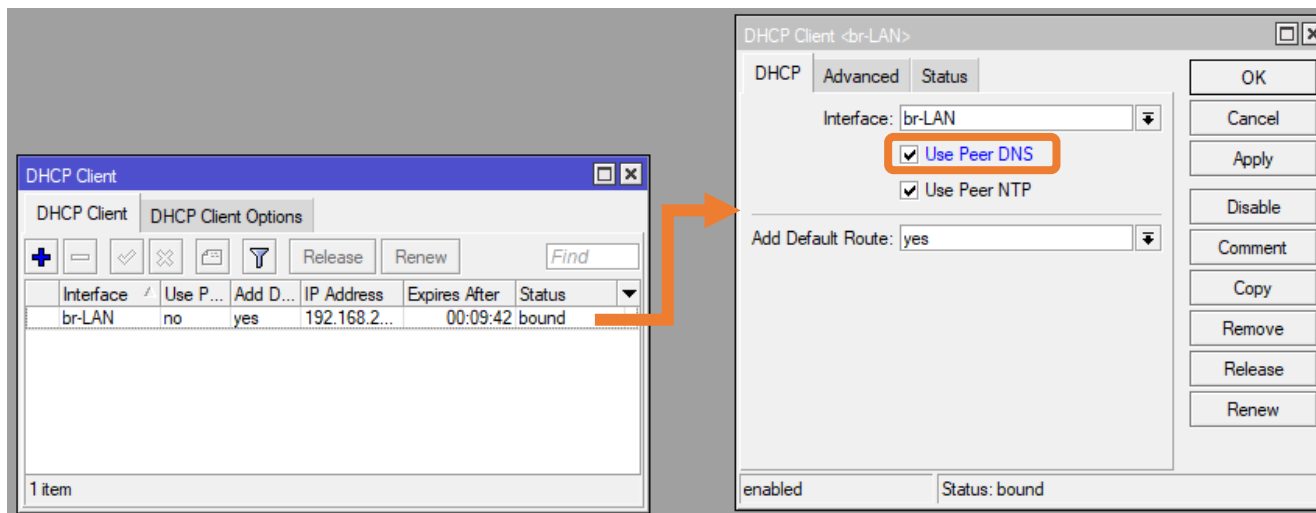
Domain Name Server



DNS Settings window showing configuration options:

- Servers: 8.8.8.8
- Dynamic Servers: (empty)
- ☐ Allow Remote Requests
- Max UDP Packet Size: 4096
- Query Server Timeout: 2.000 s
- Query Total Timeout: 10.000 s
- Max. Concurrent Queries: 100
- Max. Concurrent TCP Sessions: 20
- Cache Size: 2048 KB
- Cache Max TTL: 7d 00:00:00
- Cache Used: 17 KB

Buttons: OK, Cancel, Apply, Static, Cache



DHCP Client configuration window showing the DHCP Client Options tab:

Interface	Use P...	Add D...	IP Address	Expires After	Status
br-LAN	no	yes	192.168.2...	00:09:42	bound

Buttons: +, -, ✓, ✗, ⌂, ⌂, Release, Renew, Find

1 item

DHCP Client <br-LAN> window showing configuration options:

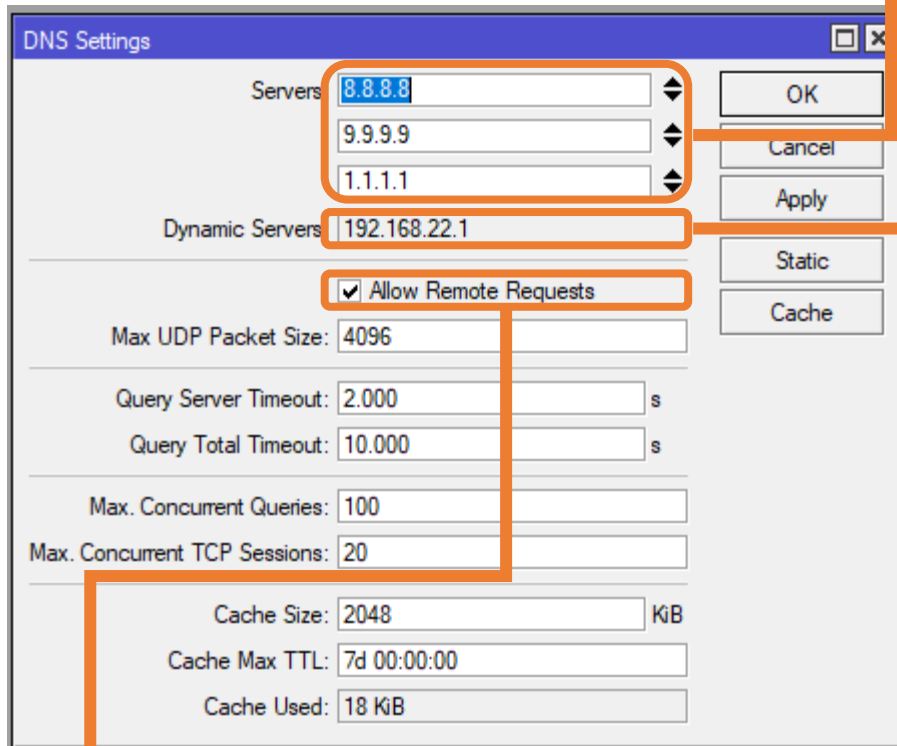
- Interface: br-LAN
- ☒ Use Peer DNS
- ☒ Use Peer NTP
- Add Default Route: yes

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Release, Renew

enabled Status: bound

- Podemos introducir una o varias IP,s de servidores DNS en DNS settings.
- Cuando configuramos un DHCP-Client en una interfaz podemos usar el servidor DNS que nos ofrezca el servidor DHCP junto con el resto de la configuración de red

Domain Name Server



DNS Settings

Servers: 8.8.8.8, 9.9.9.9, 1.1.1.1

Dynamic Servers: 192.168.22.1

☒ Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

Max. Concurrent Queries: 100

Max. Concurrent TCP Sessions: 20

Cache Size: 2048 KiB

Cache Max TTL: 7d 00:00:00

Cache Used: 18 KiB

- La petición intentará resolverla el primer servidor (en este caso el 8.8.8.8), si no puede resolver el nombre de dominio irá descendiendo al siguiente servidor
- Los servidores dinámicos (aprendidos por DHCP-Client) serán los últimos.

- Para que el propio router haga las funciones de resolver peticiones DNS, deberemos activar la casilla Allow Remote Request

- Herramienta de monitorización en tiempo real
- Se puede utilizar para monitorizar el flujos de paquetes a través de un interfaz
- Puede monitorizar el tráfico clasificado por:
 - Protocolo IP
 - Dirección origen y/o destino (IPv4 e IPv6)
 - Número de puerto
 - VLAN
 - Protocolo MAC
 - ...

MTCNA módulo 3 Torch

18



Torch (Running)

Basic

Interface:

Entry Timeout: s

Collect

☒ Src. Address ☐ Src. Address6

☒ Dst. Address ☐ Dst. Address6

☐ MAC Protocol ☒ Port

☒ Protocol ☐ VLAN Id

☐ DSCP

Filters

Src. Address:

Dst. Address:

Src. Address6:

Dst. Address6:

MAC Protocol:

Protocol:

Port:

VLAN Id:

DSCP:

Start

Stop

Close

New Window

Eth. Protocol ▲	Protocol	Src.	Dst.	Tx Rate ▼	Rx Rate	Tx Packet Rate	Rx Packet Rate ▼
800 (ip)	6 (tcp)	192.168.199.200:58658	159.148.147.196:443 (https)	757.3 kbps	54.9 kbps	68	52
800 (ip)	6 (tcp)	192.168.199.200:58656	159.148.147.196:443 (https)	303.5 kbps	51.1 kbps	28	27
800 (ip)	6 (tcp)	192.168.199.200:58659	159.148.147.196:443 (https)	296.5 kbps	40.9 kbps	29	26
800 (ip)	6 (tcp)	192.168.199.200:58655	159.148.147.196:443 (https)	171.4 kbps	54.0 kbps	22	23
800 (ip)	6 (tcp)	192.168.199.200:58661	159.148.147.196:443 (https)	63.2 kbps	22.5 kbps	6	8
800 (ip)	6 (tcp)	192.168.199.200:58662	159.148.147.196:443 (https)	47.7 kbps	22.4 kbps	6	8
800 (ip)	6 (tcp)	192.168.199.200:58657	159.148.147.196:443 (https)	0 bps	0 bps	0	0

7 items

Total Tx: 1639.8 kbps

Total Rx: 245.9 kbps

Total Tx Packet: 159

Total Rx Packet: 144

Ping

- Herramienta básica de conectividad que utiliza mensajes ICMP Echo para determinar la accesibilidad del equipo remoto.
- Una de las primeras herramientas a usar para determinar un problema. Si hace ping, el equipo está vivo (desde el punto de vista de la red).
- Hay que usarla en combinación con otras herramientas. Es un buen inicio, pero NO es la herramienta definitiva

Traceroute

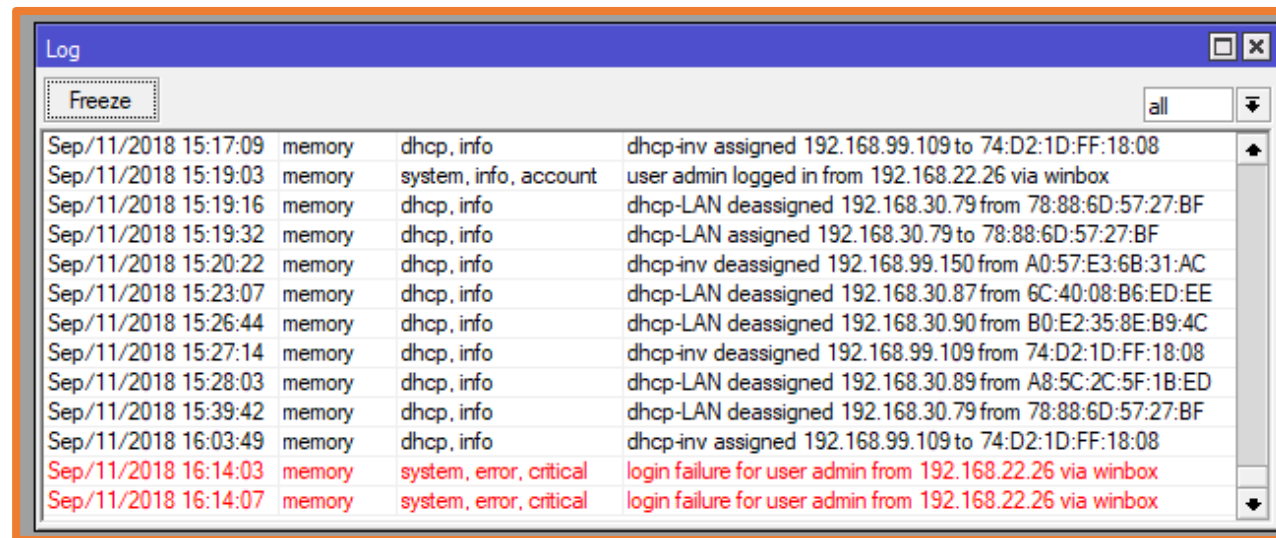
- Se usa para mostrar todos los routers que atravesamos hasta alcanzar nuestro destino.
- Indica el retardo en alcanzar cada router en el camino que seguimos hasta nuestro destino.
- Es efectivo en localizar un fallo o un router lento

System identity

- Es importante el establecer el nombre del sistema.
- Es imposible de gestionar 50 routers que todos se llamen « MikroTik ».Hace imposible la identificación del router problemático.
- Una vez asignado, hará que identifiquemos el router en el que estamos trabajando de una forma más simple.

Log del sistema y logs de debug

- El registro (permanent or not) es importante para asegurar la historia de los eventos del router
- La forma mas sencilla de ver los logs es a través del menú « log » en el Winbox.

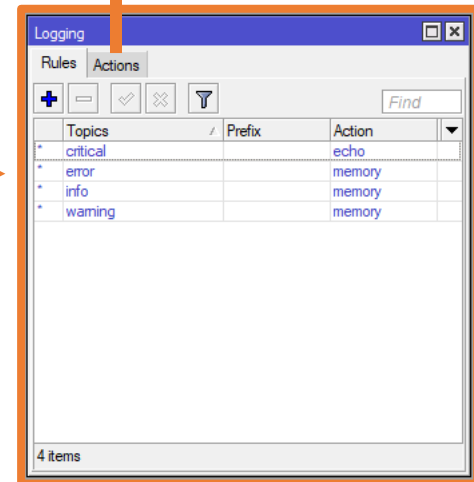
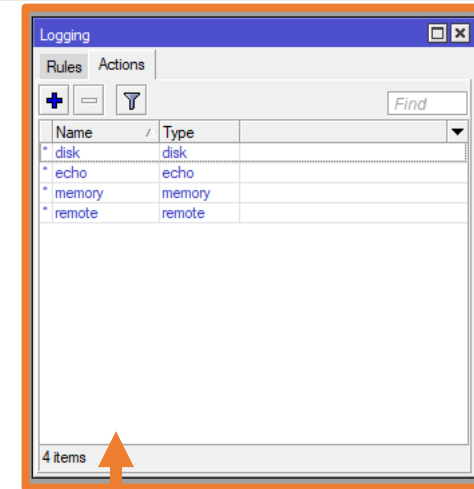
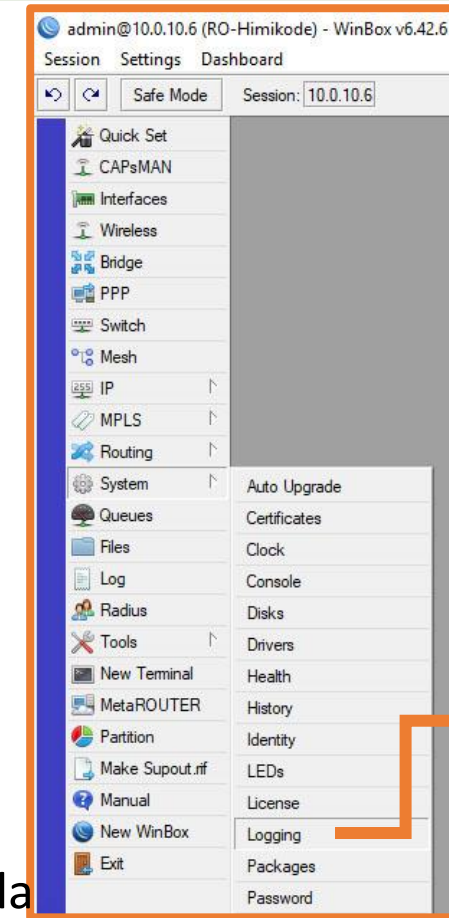


The screenshot shows the 'Log' window in Winbox. It has a 'Freeze' button and a dropdown menu set to 'all'. The log entries are as follows:

Time	Memory	System	Event
Sep/11/2018 15:17:09	memory	dhcp, info	dhcp-inv assigned 192.168.99.109 to 74:D2:1D:FF:18:08
Sep/11/2018 15:19:03	memory	system, info, account	user admin logged in from 192.168.22.26 via winbox
Sep/11/2018 15:19:16	memory	dhcp, info	dhcp-LAN deassigned 192.168.30.79 from 78:88:6D:57:27:BF
Sep/11/2018 15:19:32	memory	dhcp, info	dhcp-LAN assigned 192.168.30.79 to 78:88:6D:57:27:BF
Sep/11/2018 15:20:22	memory	dhcp, info	dhcp-inv deassigned 192.168.99.150 from A0:57:E3:6B:31:AC
Sep/11/2018 15:23:07	memory	dhcp, info	dhcp-LAN deassigned 192.168.30.87 from 6C:40:08:B6:ED:EE
Sep/11/2018 15:26:44	memory	dhcp, info	dhcp-LAN deassigned 192.168.30.90 from B0:E2:35:8E:B9:4C
Sep/11/2018 15:27:14	memory	dhcp, info	dhcp-inv deassigned 192.168.99.109 from 74:D2:1D:FF:18:08
Sep/11/2018 15:28:03	memory	dhcp, info	dhcp-LAN deassigned 192.168.30.89 from A8:5C:2C:5F:1B:ED
Sep/11/2018 15:39:42	memory	dhcp, info	dhcp-LAN deassigned 192.168.30.79 from 78:88:6D:57:27:BF
Sep/11/2018 16:03:49	memory	dhcp, info	dhcp-inv assigned 192.168.99.109 to 74:D2:1D:FF:18:08
Sep/11/2018 16:14:03	memory	system, error, critical	login failure for user admin from 192.168.22.26 via winbox
Sep/11/2018 16:14:07	memory	system, error, critical	login failure for user admin from 192.168.22.26 via winbox

Log del sistema

- **Actions:**
 - Tareas que el router realizará cada cierto intervalo de tiempo.
 - Las reglas le dicen al router que acción debe tomar.
 - Hay cinco tipos de acciones, así podemos tener un sistema de registro flexible.
- **Reglas**
 - Le indican al routerOS que acciones tomar según el evento acontecido (llamado en routerOS "topic")
 - Podemos tener mas de una regla para el mismo evento, cada regla puede llevar a cabo una acción diferente.
 - Podemos tener una regla con dos o mas eventos, ejecutando la misma acción
 - Agregar reglas es sencillo, elige uno o varios eventos, nombre de la regla y elige una acción. (Es aconsejable el crear primero las acciones)



Donde se envian los logs

- Como se indica en “actions”, los logs se puede encontrar en 5 lugares:
 - Disk : Un disco duro en el router
 - Echo : La consola del router (si la hay)
 - Email : una cuenta predefinida de correo
 - Memory : La memoria del router, tal y como se ve en la ventana de « log »
 - Remote : un servidor de syslog