

ROMON

Francisco J. Montilla - fco.j.montilla@gmail.com

MUM MADRID

Octubre 2015

I

FRANCISCO J. MONTILLA

- Administrador de Sistemas desde 1998
- Freelance
- Primer contacto RouterOS en 2007
- MTCNA, MTCWE, MTCTCE, MTCRE

RoMON

- Qué es, y qué nos aporta
- Configuración Básica y Securización
- Demo
- Estrategia de Despliegue
- Resumen
- Preguntas

RoMON

ROUTER MANAGEMENT OVERLAY NETWORK

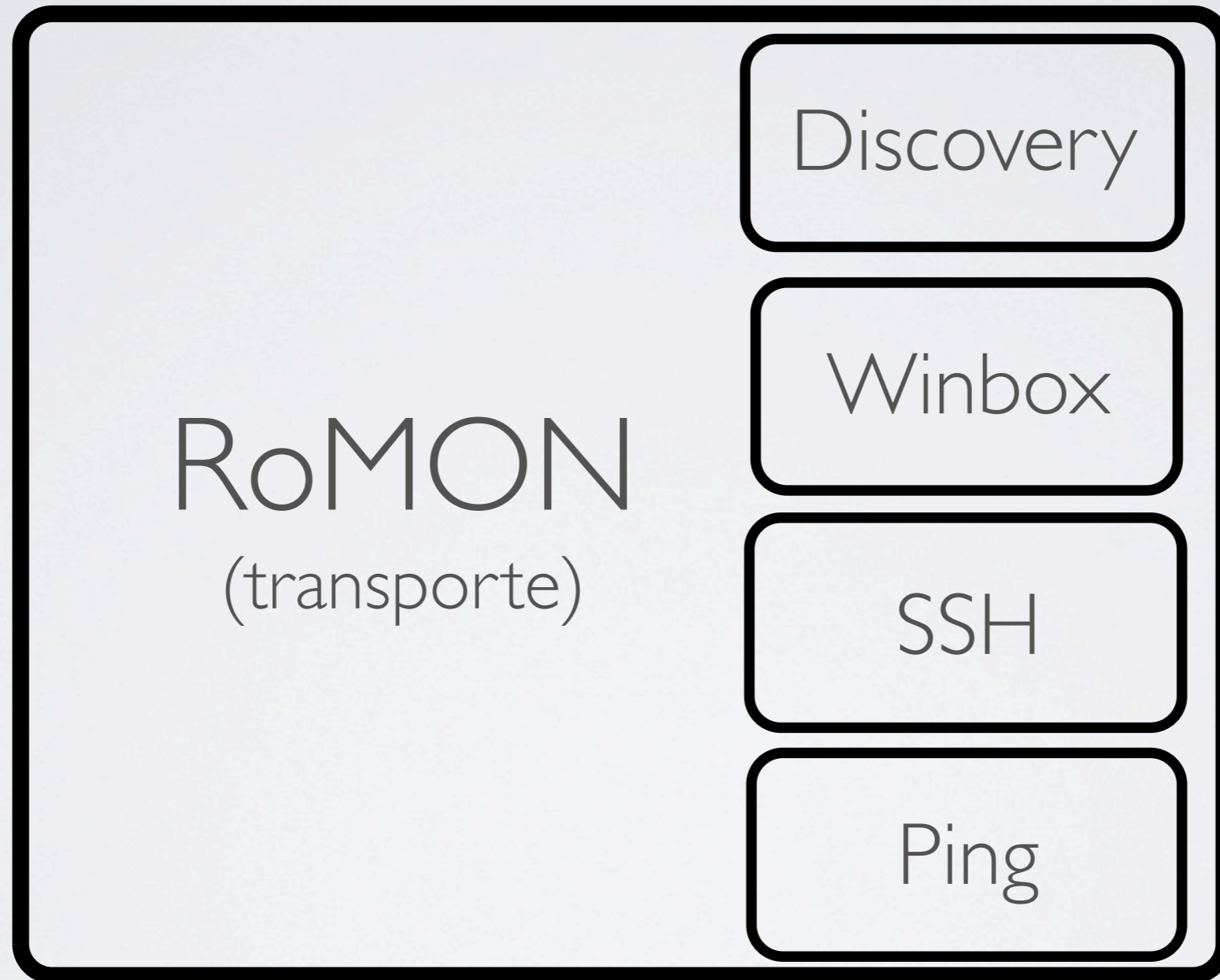
- Nuevo Protocolo Propietario de Mikrotik
- *Independiente* de transporte (Capa 2 o Capa 3)
- Aplicaciones: Discovery, Winbox, Ping y SSH

RoMON

REQUISITOS

- RouterOS \geq 6.28
- Sólo interfaces ethernet y wireless
- No activado por defecto: activar y verificar ID (mac)
- Winbox 3rc

RED DE GESTIÓN DE ROUTERS SUPERPUESTA (ROUTER MANAGEMENT OVERLAY NETWORK)



RoMON

LOCALIZACIÓN (DISCOVERY)

- Protocolo Independiente de Capa3 o Capa2
- Multisalto
- Los routers con RoMON activo forman una “malla” de discovery o localización

RoMON: APLICACIONES

Winbox

Discovery

File Tools

Connect To: 58.140.2.31

Login: admin

Password: *****

Session: <own> Browse...

Note: CCR PE

Group: WISP:press

RoMON Agent:

Add/Set

Connect To RoMON

Connect

Keep Password

Secure Mode

Autosave Session

Open In New Window

Discovery (Running)

Address	Cost	Hops	Path	L2MTU	Identity	Version
4C:5E:0C:B8:FD:F2	200	1	4C:5E:0C:B8:FD:F2	1500	R2	6.30.4
4C:5E:0C:4F:AB:5E	400	2	4C:5E:0C:B8:FD:F2, 4C:...	1500	R3	6.30.4

2 items

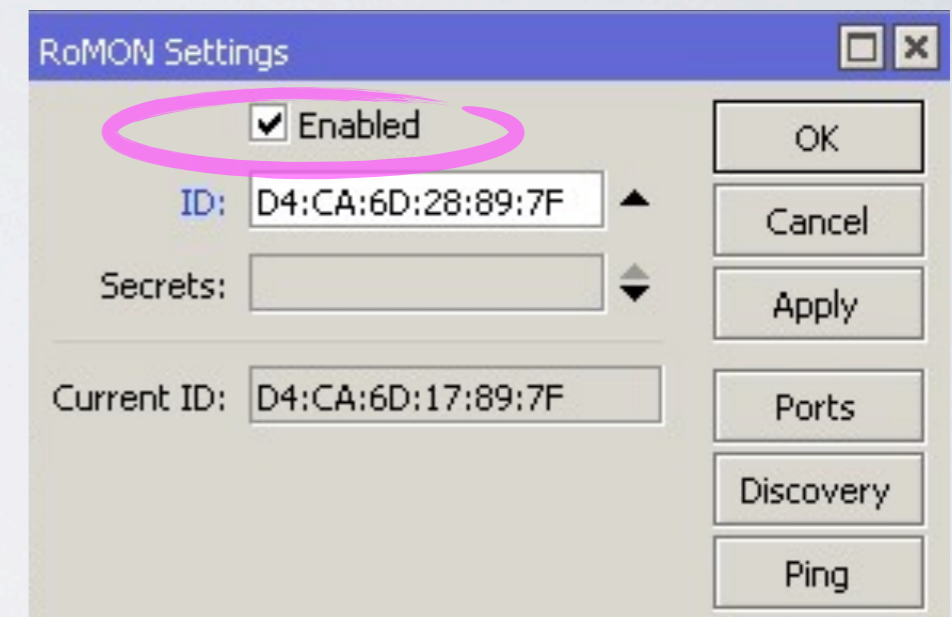
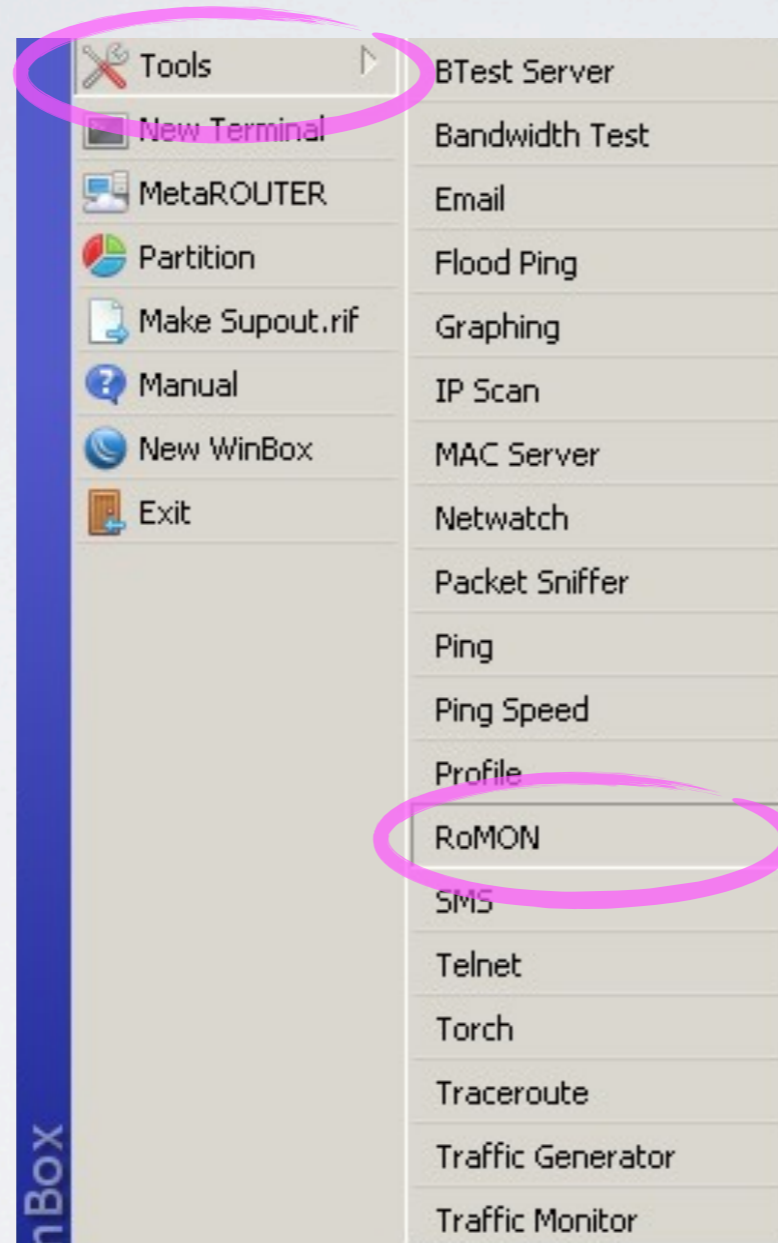
SSH

Ping

```
[admin@Mikrotik] /tool romon> ssh address=D4:CA:6D:57:7B:F3
password:
Welcome back!
```

```
[admin@Mikrotik] /tool romon> ping D4:CA:6D:57:7B:F3
SEQ HOST TIME STATUS
0 D4:CA:6D:57:7B:F3 timeout
1 D4:CA:6D:57:7B:F3 15ms
2 D4:CA:6D:57:7B:F3 6ms
3 D4:CA:6D:57:7B:F3 8ms
4 D4:CA:6D:57:7B:F3 16ms
sent=5 received=4 packet-loss=20% min-rtt=6ms avg-rtt=11ms max-rtt=16ms
```


RoMON: CONFIGURACIÓN BÁSICA

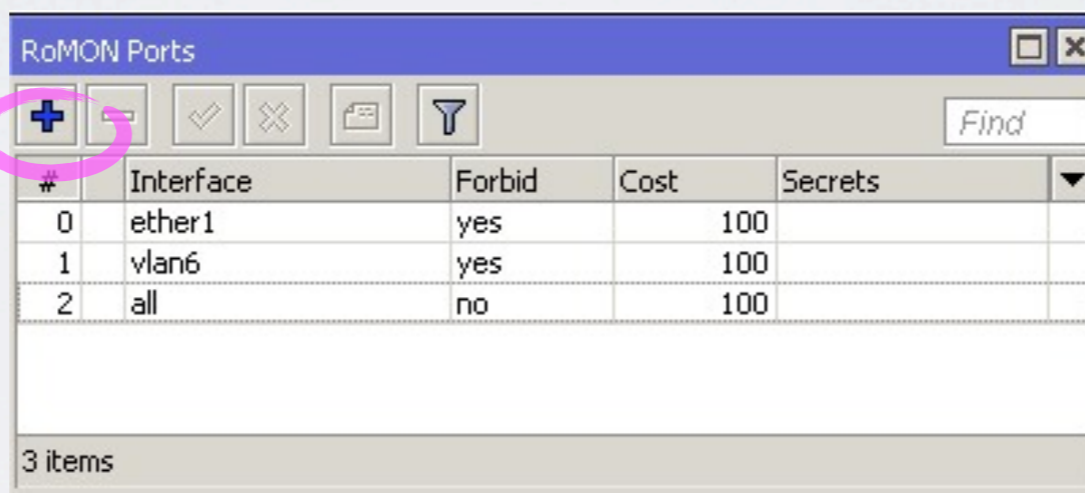
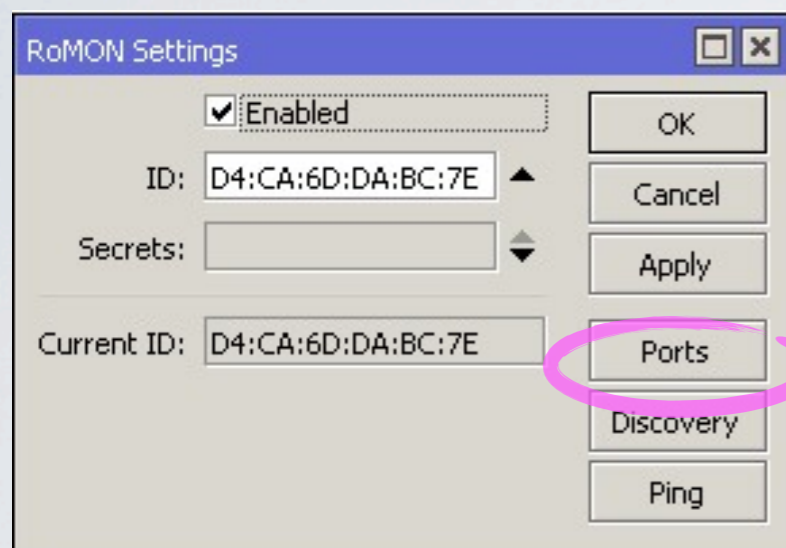


```
[admin@Mikrotik] > /tool romon
[admin@Mikrotik] /tool romon> set enabled=yes
[admin@Mikrotik] /tool romon> print
    enabled: yes
           id: 00:00:00:00:00:00
    secrets:
current-id: D4:CA:6D:DA:BC:7E
```

- Activar
- Comprobar ID

RoMON: SEGURIZACIÓN: PUERTOS

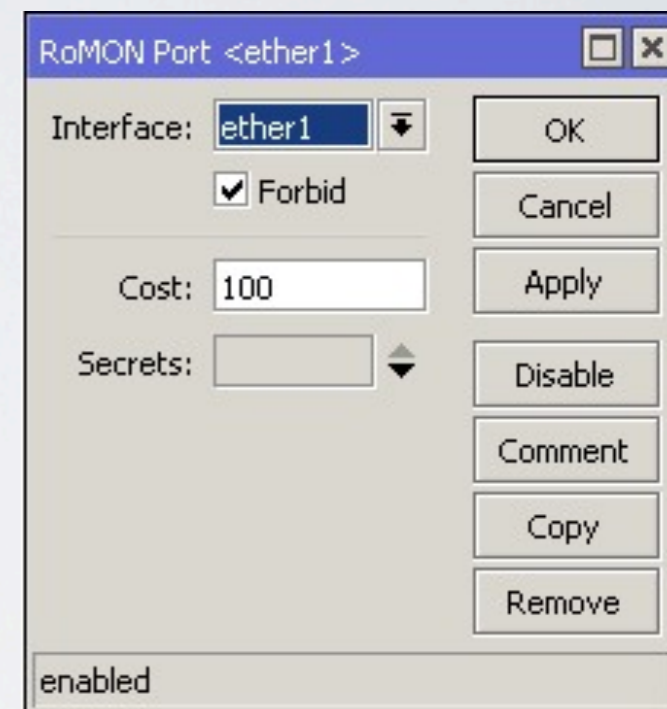
- Podemos definir qué puertos participan en RoMON



The 'RoMON Ports' dialog box contains a table with the following data:

#	Interface	Forbid	Cost	Secrets
0	ether1	yes	100	
1	vlan6	yes	100	
2	all	no	100	

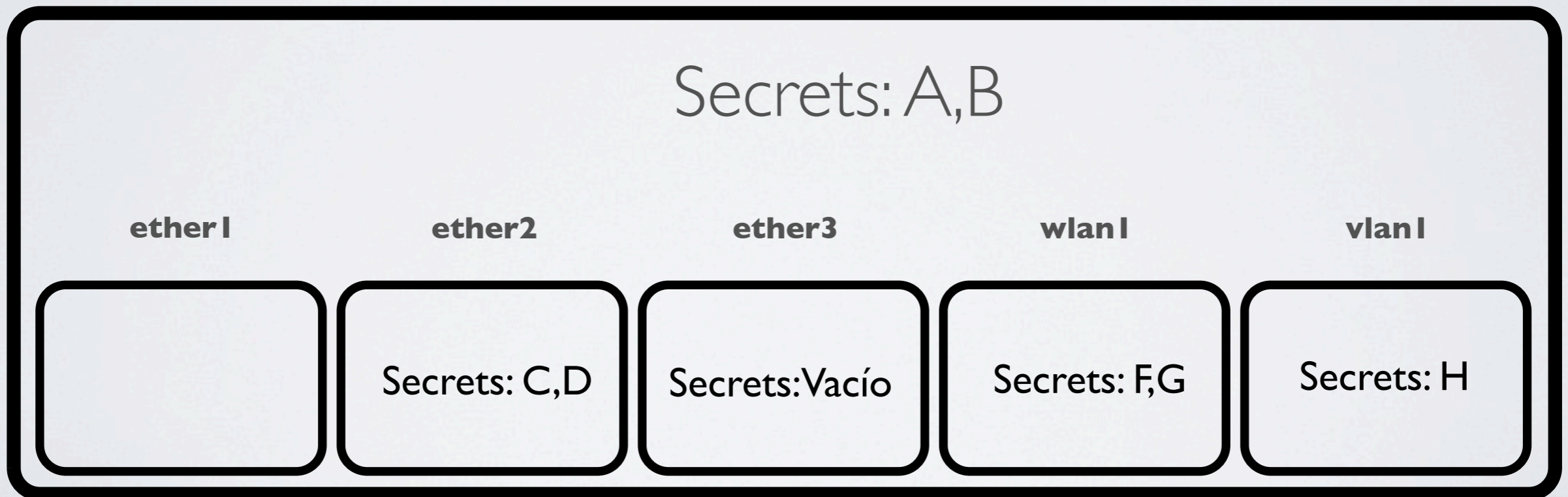
Additional elements: A toolbar with a '+' icon circled in pink, a 'Find' search box, and a status bar indicating '3 items'.



- Procesado como cortafuegos (solo aplica primera concordancia)

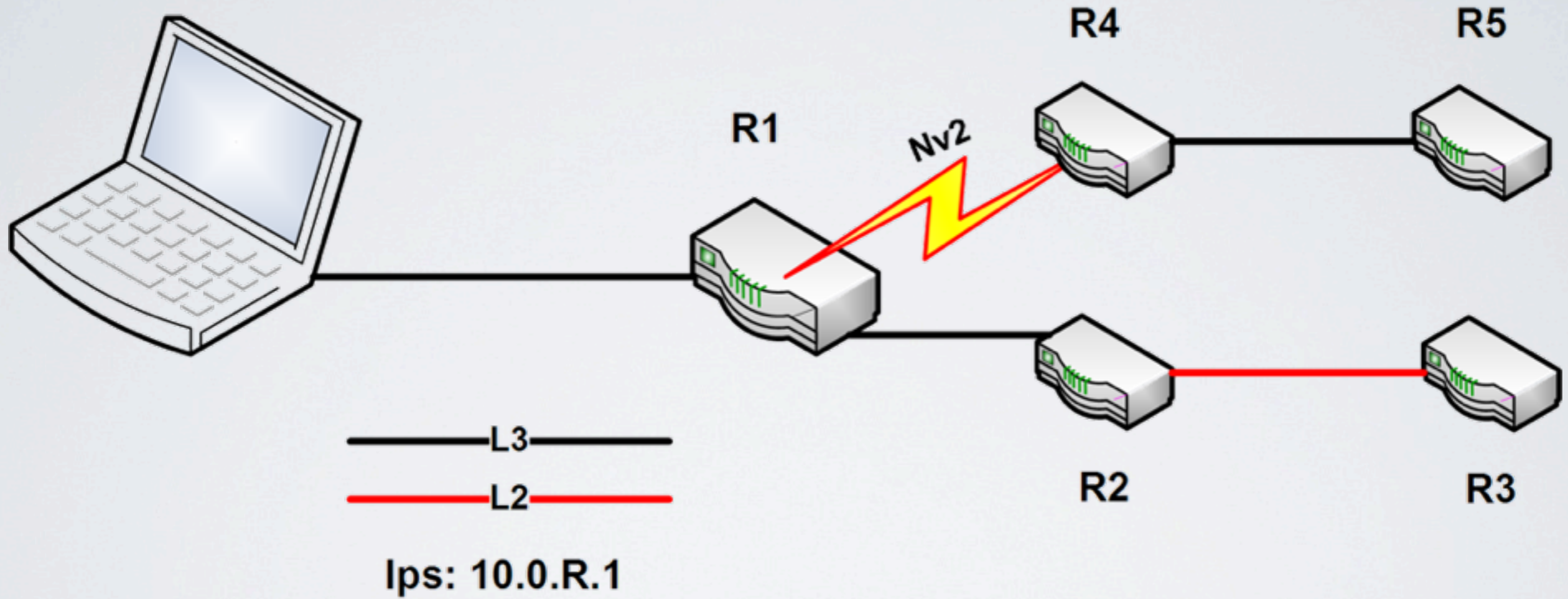
RoMON: SECURIZACIÓN: SECRETS

- Cifrado MD5 tramas {
 - Autenticación
 - Integridad
 - Prevención reinyección



||

RoMON: DEMO



RoMON: FUNCIONAMIENTO CON SECRETS

Cifrado/Descifrado MD5 de tramas...		
Salientes	Entrantes	
Primer Secret NO vacío	Cifrada MD5	Sin Cifrar
	Secret correcto (global/puerto)	Si entre Secrets hay uno vacío

RoMON: ESTRATEGIA DESPLIEGUE CON SECRETS

- Su diseño permite despliegue incremental/cambio de Secrets sin interrupción del funcionamiento de RoMON

1. Primera etapa: Añadir Secrets $\left\{ \begin{array}{l} 1. \text{ Vacío} \\ 2. \text{ MiSecReTo...} \end{array} \right.$
2. Segunda: Cambiar $\left\{ \begin{array}{l} 1. \text{ MiSecReTo...} \\ 2. \text{ Vacío} \end{array} \right.$
3. Tercera: dejar sólo *MiSecReTo...*

RoMON: EN RESUMEN

- RouterOS \geq 6.28, Winbox 3rc, No activado por defecto!
- Funcionamiento Independiente de Capa 2 o Capa 3
- Aplicaciones: Discovery, Winbox, Ping y SSH
- Posibilidad decidir qué puertos participan (Ether o Wlan)
- Securización: Secrets globales o por puerto
- Despliegue incremental o Cambio Secrets sin interrupción red
RoMON

ROMON: PREGUNTAS

- PDF Presentación: <https://goo.gl/nfuqOF>
- Ficheros .rsc Routers: <https://goo.gl/pw391c>
- email: fco.j.montilla@gmail.com
- nick: **pukkita**

¡Gracias!