

México 2019



SEGURIDAD EN UNA RED CON HOTSPOT (Hardening)



MikroTik

PONENTE

EMPRESA

INTRODUCCIÓN

Miguel Ángel Félix García

Los Mochis, Sinaloa.



**Certificaciones: MTCNA, MTCWE, MTCTCE, MTCIPv6E,
MTCUME, MTCRE, MTCINE.**



Presentación Anterior: "The dude"

<https://mum.mikrotik.com/2018/MX/agenda/es#0DMDN105c9>

Ocupación



- WISP local con más de 1000 suscriptores (cpe).
- Consultor MikroTik.
- Asesoría en redes y enlaces Inalámbricos.
- Soluciones Llave En Mano.
- Soporte mensual o eventual a otros WISP.



Empresa

Mercado Wisp México



**Creada en el año 2015 con la finalidad
de ofrecer servicios y equipos
principalmente para implementaciones
de Redes Wisp.**



Empresa

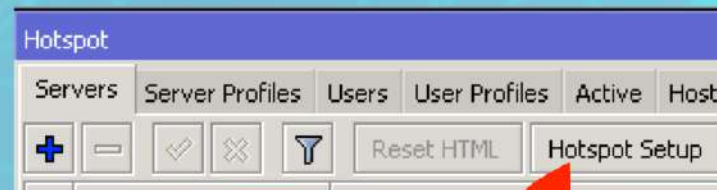
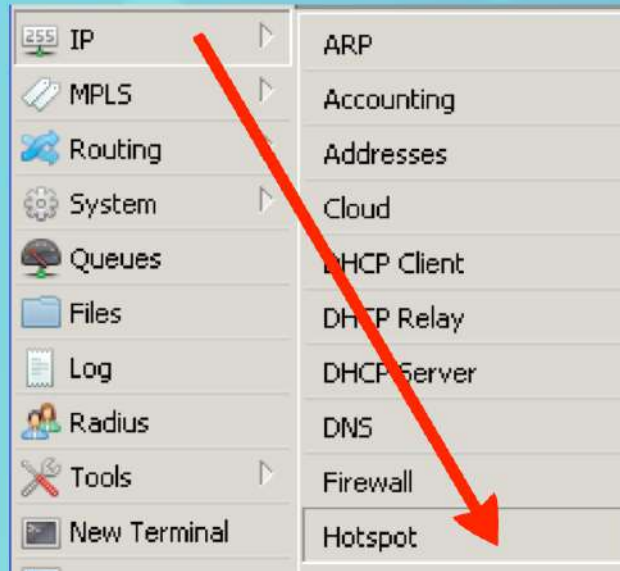
Mercado Wisp México



- Grupo en Facebook con mas de 15 mil usuarios.
- Grupos de Whatsapp donde se comparten ideas y conocimiento.
- Somos partner de Ecatel México y ofrece cursos oficiales para certificaciones en MikroTik.



Qué es Hotspot?



/ip hotspot setup



Resumen



En México existe un mercado muy grande para usar el servicio de hotspot y credenciales prepago (voucher) como forma de administrar una red y dar el servicio para acceso a internet.



Problema



Se construyen redes con hotspot de gran tamaño para poder llevar el servicio hasta los usuarios.

Se diseñan para operar con un unico dominio de broadcast exponiendo la integridad completa de la red y el servicio que se maneje (Hotspot).



Objetivo



- Trabajar con topologías de red seguras administradas con hotspot.
- Evitar ataques y fallas continuas de capa 2 dentro de este tipo de implementaciones.
- Lograr que mi hotspot **NO** sea el motivo de una mala calidad en el servicio que llega a los dispositivos finales.



Objetivo



mercadowispMexico@ [REDACTED] ADMINISTRADOR) - WinBox v6.4

Session: [REDACTED]

Hotspot

User Profiles Active Hosts IP Bindings Service Ports Walled Garden ...

Find

Server	User	Address	Uptime	Session Ti...	Rx ...	Tx R...
R	hs-vla...	cxq...	172.31.5...	00:06:44	2d 22:55:12	351.6 ...
R	hs-vla...	v1rajp	172.31.19...	23:58:11	1d 19:53:43	204.1 ...
R	hs-vla...	7uz...	172.31.55...	00:10:47	08:31:09	97.3 k...
R	hs-vla...	oliob0	172.31.53...	03:53:10	20d 05:53...	156.5 ...
R	hs-vla...	yrfimi	172.31.5...	00:42:14	3d 19:55:59	67.3 k...
R	hs-vla...	ygd...	172.31.58...	02:04:48	02:19:21	61.6 k...
R	hs-vla...	F8:...	172.31.33...	00:11:10		63.2 k...
R	hs-vla...	4pu...	172.31.61...	01:03:29	00:55:50	76.0 k...
R	hs-vla...	5q5rkl	172.31.60...	04:32:55	10d 20:22...	20.5 k...
R	hs-vla...	fcgvaz	172.31.6...	08:20:11	01:42:06	26.9 k...
R	hs-vla...	umj...	172.31.21...	00:43:46	3d 01:47:30	73.2 k...
R	hs-vla...	lqyrkt	172.31.5.97	00:15:37	16d 20:33...	36.5 k...
R	hs-vla...	rmxh7l	172.31.49...	04:31:08	13:06:12	110.1 ...
R	hs-vla...	ede...	172.31.7.79	01:38:39	2d 22:52:59	85.4 k...
R	hs-vla...	amo...	172.31.60...	05:18:19	18d 16:24...	28.6 k...
R	hs-vla...	E8:...	172.31.62...	00:45:53		17.2 k...
R	hs-vla...	srmioi	172.31.21...	00:42:32	21d 00:00...	16.5 k...
R	hs-vla...	1uiepq	172.31.67...	00:16:49	1d 23:31:54	48.7 k...
R	hs-vla...	fpk5yz	172.31.48...	08:01:20	8d 17:35:43	26.6 k...
R	hs-vla...	pgb...	172.31.72...	21:54:22	28d 15:37...	53.9 k...

791 items out of 790 (1 selected)

Resources

Uptime: 3d 11:34:26

Free Memory: 3289.9 MiB

Total Memory: 3968.0 MiB

CPU: tilegx

CPU Count: 36

CPU Frequency: 1200 MHz

CPU Load: 5 %

Free HDD Space: 775.2 MiB

Total HDD Size: 1024.0 MiB

Architecture Name: tile

Board Name: CCR1036-12G-4S

Version: 6.43.4 (stable)

Build Time: Oct/17/2018 06:37:48

Factory Software:

Objetivo



mercadowisp_mexico@

Session:

Hotspot

User Profiles Active Hosts IP Bindings Service Ports Walled Garden ...

Server	User	Address	MAC Address	Uptime	Rx ...	Tx Rat
hs-bri...	332k...	192.168.1...	CC:FD:17:AA:...	01:55:11	29.0 k...	1067.3
hs-vla...	334u...	172.16.11...	FC:2D:5E:ED:...	14:56:16	58.1 k...	1064.8
hs-vla...	887t...	172.16.10...	D4:C9:4B:1E:...	03:40:00	35.8 k...	1037.9
hs-bri...	6643...	192.168.1...	A8:51:5B:E0:...	04:35:41	35.7 k...	1029.2
hs-bri...	4432...	192.168.1...	A8:51:5B:D6:...	1d 04:44:33	12.0 k...	1027.9
hs-bri...	554j...	192.168.1...	A0:91:69:C1:...	01:23:37	38.7 k...	1026.9
hs-bri...	554b...	192.168.1...	9C:E3:3F:D7:...	00:09:29	47.6 k...	1025.7
hs-vla...	226d...	172.16.70...	A8:A1:98:F0:...	15:29:55	27.3 k...	1025.6
hs-vla...	3342i...	172.16.23...	04:1B:6D:CC:...	22:15:36	44.0 k...	1024.1
hs-vla...	4456...	172.16.14...	84:9F:85:7A:...	20:46:45	29.3 k...	1013.2
hs-bri...	332b...	192.168.1...	B4:BF:F6:CD:...	00:11:03	31.7 k...	1012.8
hs-vla...	6643	172.16.90	50:8C:96:FD:	1d 04:43:28	21.0 k...	1004.0

2340 items

Resources

Uptime: 1d 04:46:13

Free Memory: 1501.7 MiB

Total Memory: 1939.2 MiB

CPU: tilegx

CPU Count: 16

CPU Frequency: 1200 MHz

CPU Load: 9 %

Free HDD Space: 330.1 MiB

Total HDD Size: 512.0 MiB

Architecture Name: tile

Board Name: CCR1016-12G

Qué es Hardening?



En pocas palabras para este tema es incrementar la seguridad en nuestra red con hotspot.

Qué es Firewall?



Es el encargado de la seguridad del flujo de datos de la red y del propio router.

México 2019





AGENDA



Qué es Hotspot?



Qué es Hardening?

Problemas en un hotspot "por qué?"

Solución

Demostración

Problemas en un Hotspot



Por qué?

Qué necesito saber



Problemas en un Hotspot



Por qué

Cómo funciona un hotspot

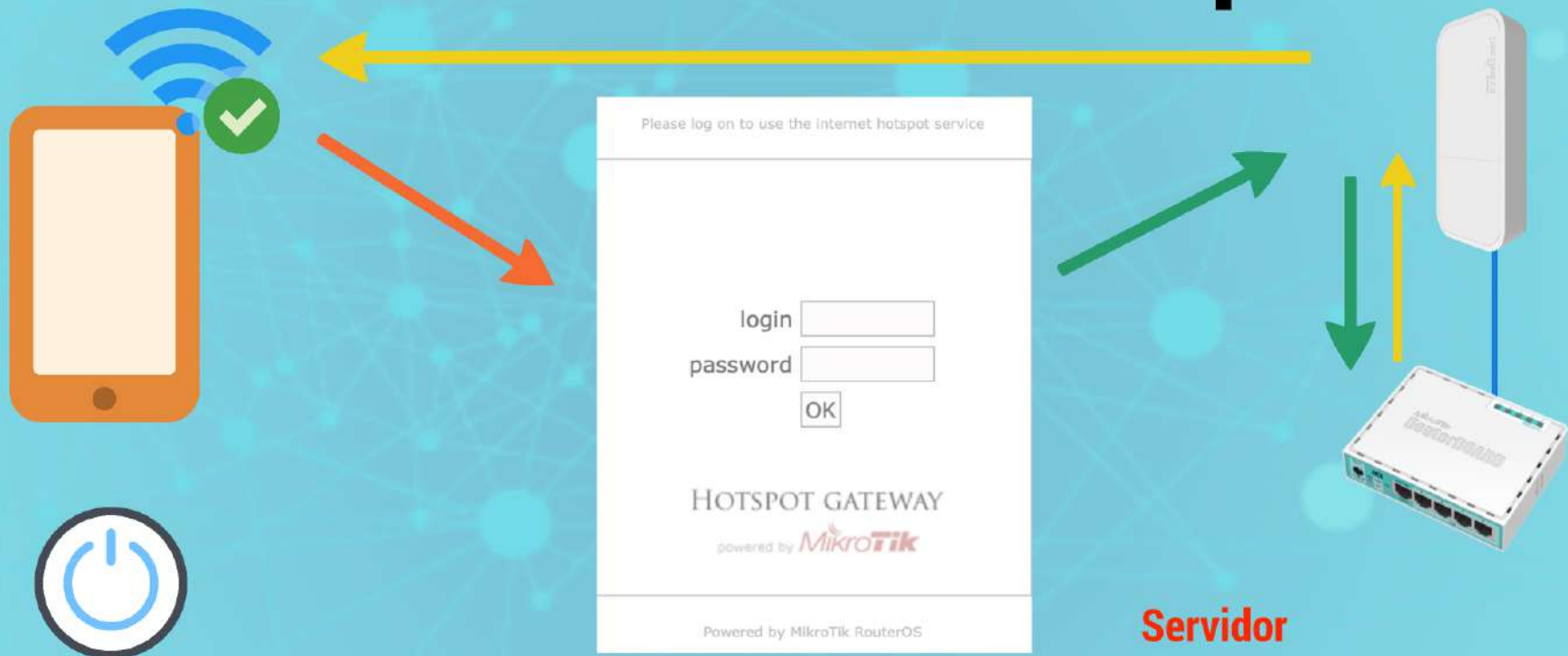


Cómo funciona un Hotspot?



Servidor

Cómo funciona un Hotspot?



Cómo funciona un Hotspot?





Qué hace un Servidor DHCP?

Es el encargado de entregar direcciones ip dinamicas y otros parametros a los equipos en la red para ello hace uso de un pool o rango de direcciones

Qué es DHCP?

Cómo funciona?



D
O
R
A

Qué es DHCP?

Cómo funciona?



Discover

Offer

Request

Ack

Qué es DHCP?

Cómo funciona?



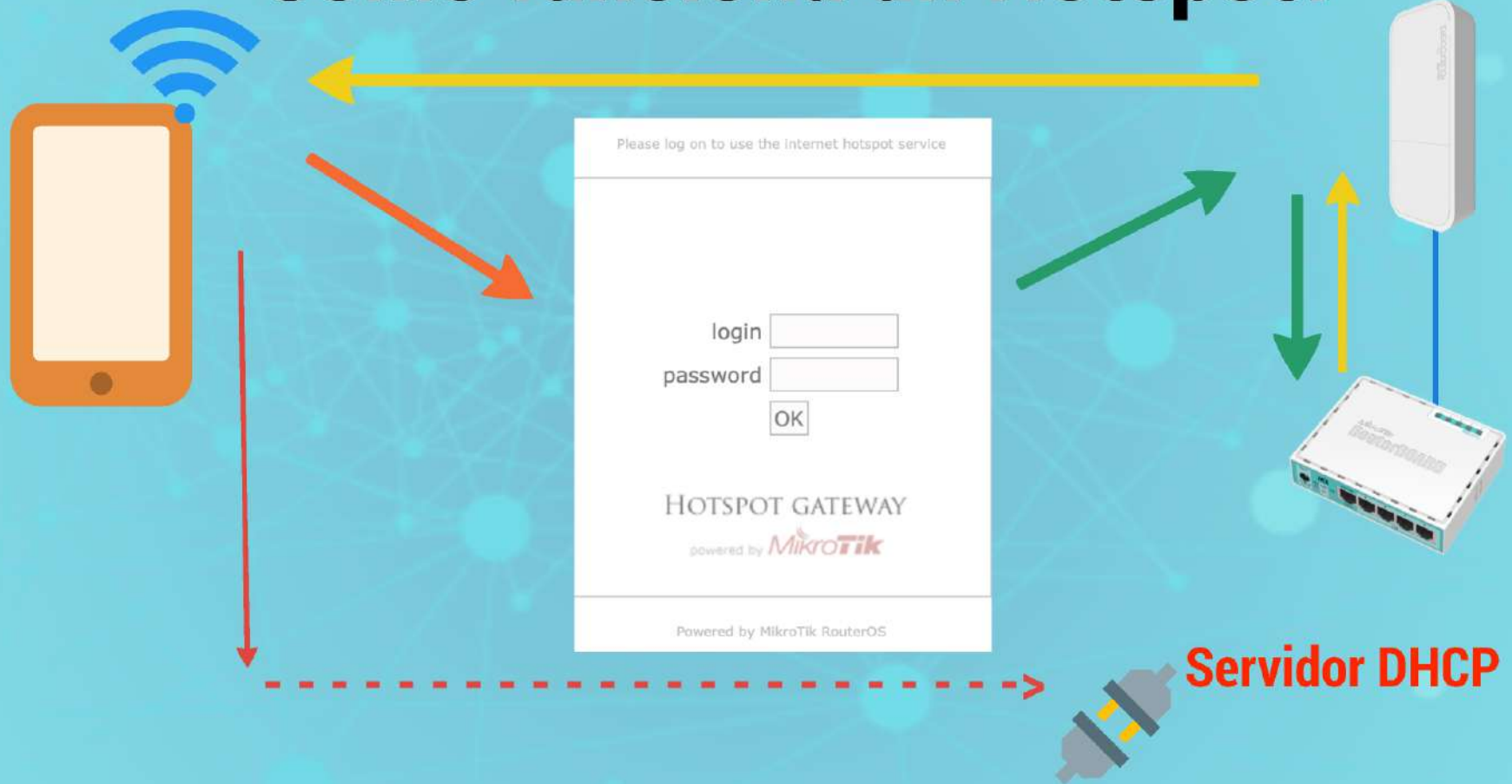
Discover **Cliente**

Offer **Servidor**

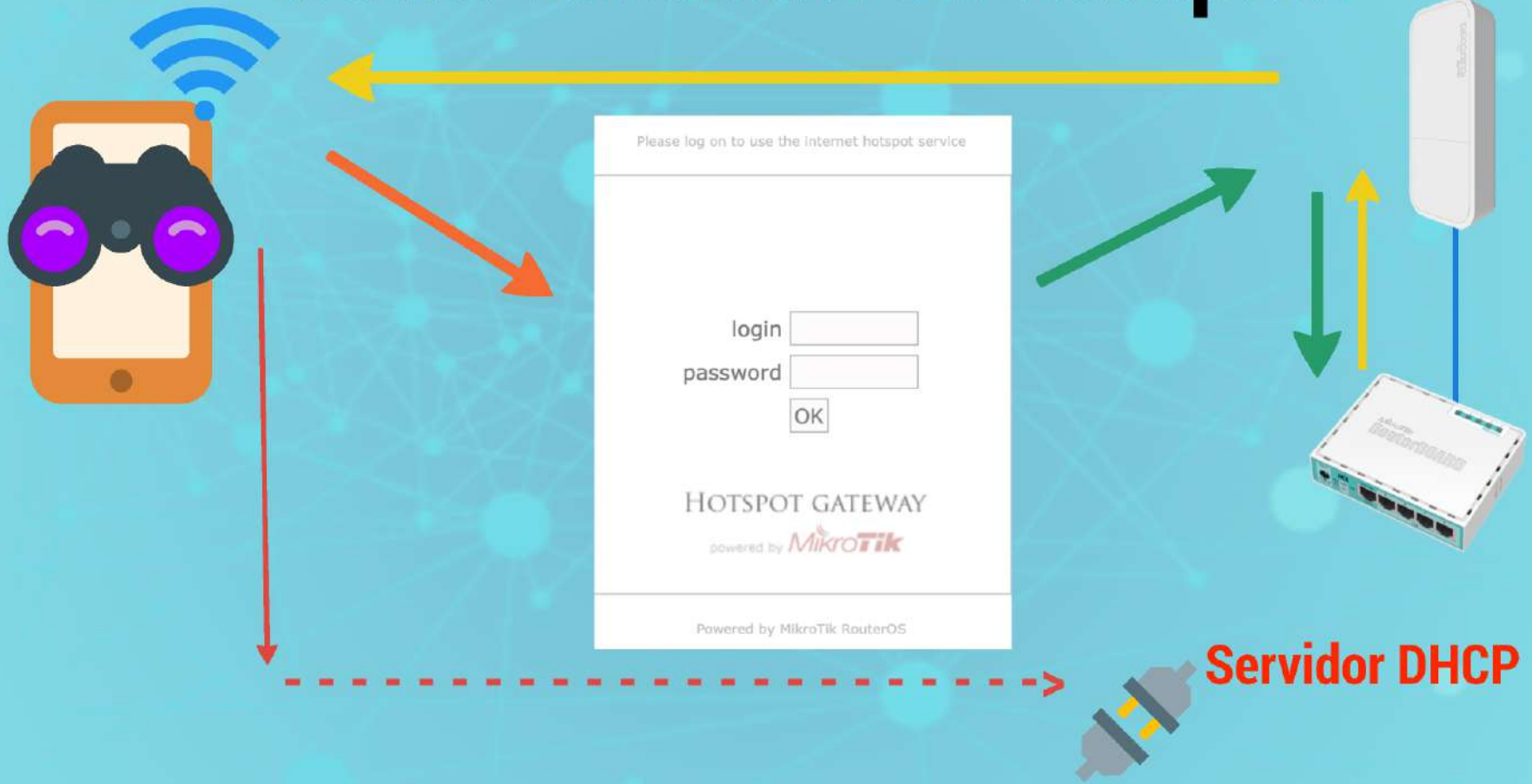
Request **Cliente**

Ack **Servidor**

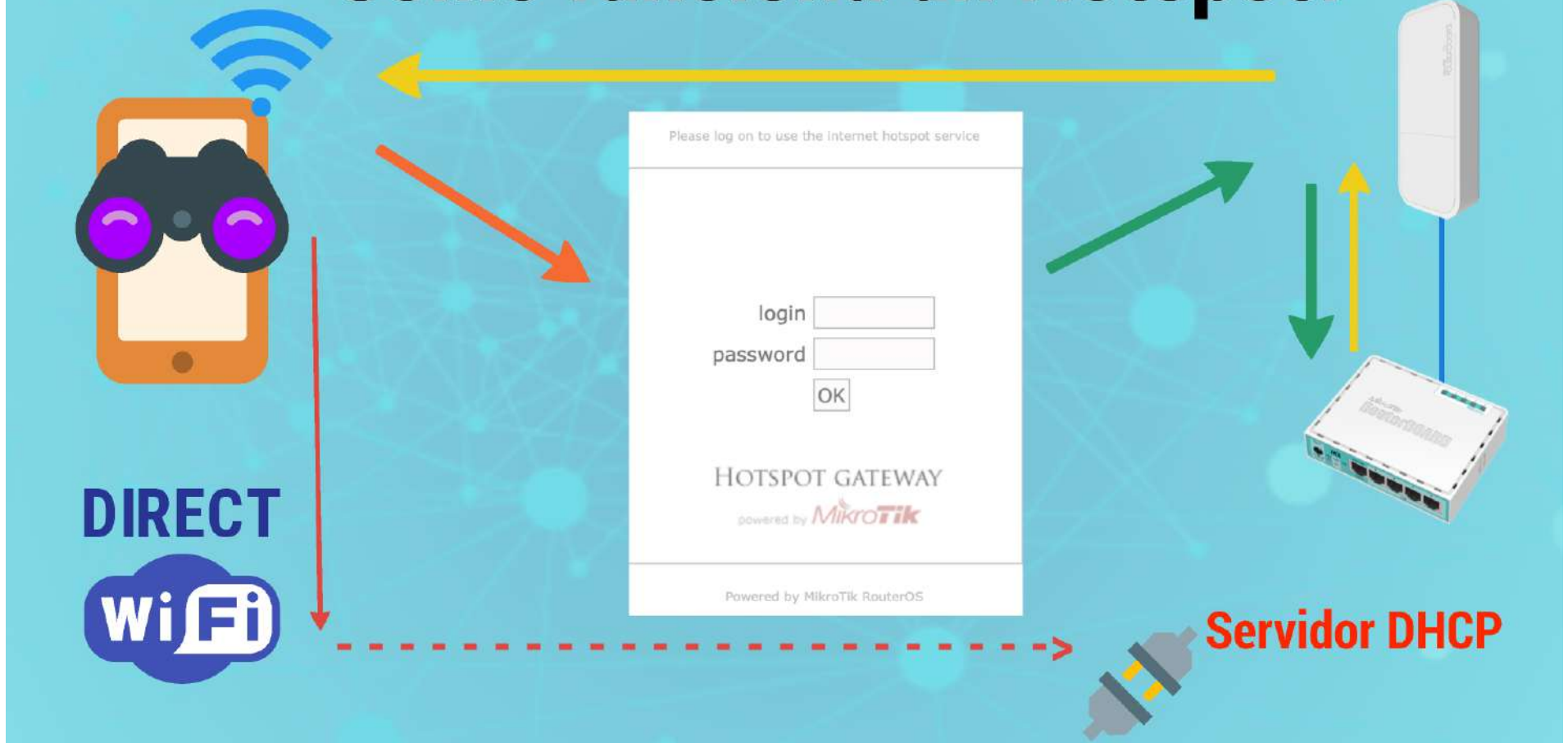
Cómo funciona un Hotspot?



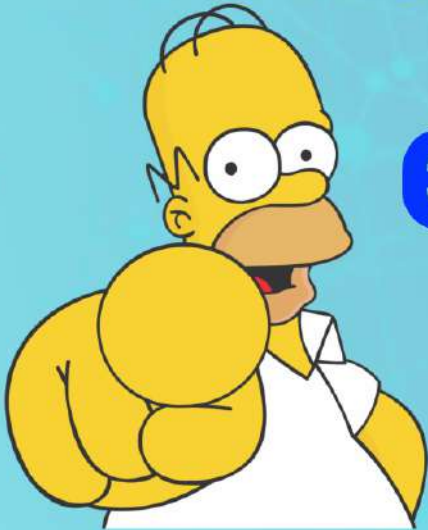
Cómo funciona un Hotspot?



Cómo funciona un Hotspot?

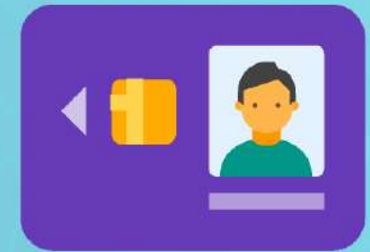


**Ahora sera mas facil
entender lo que pasa
en un Hotspot !!**





Identificación del problema

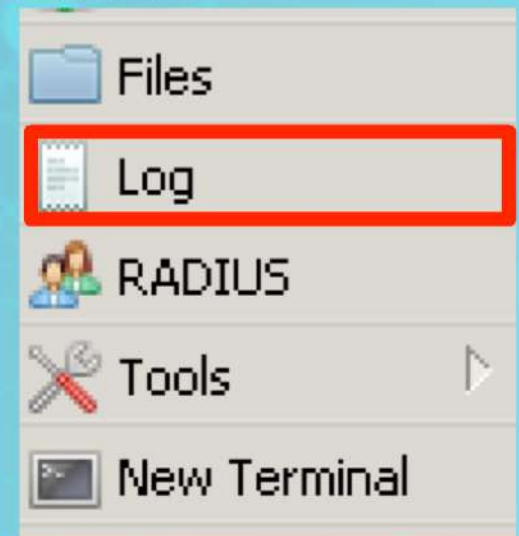


Puede suceder que sea mucho mas facil y rapido identificar y encontrar el problema, pero reconocer cual es el motivo no tanto.



Log

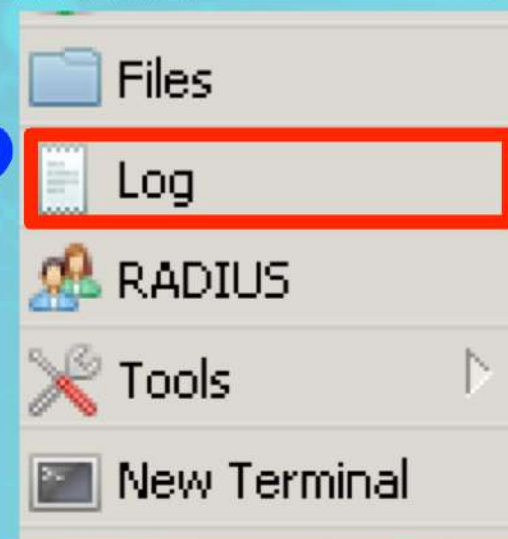
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success



Log

memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success

Recuerdan que dijo DORA?



Problema en ciclo dhcp "Offer"



dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success

Problema en ciclo dhcp "Offer"



dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success

Notaste la diferencia del ejemplo anterior?

Problema en ciclo dhcp "Offer"



dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success

Notaste la diferencia del ejemplo anterior?

memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success

Problema en ciclo dhcp "Offer"

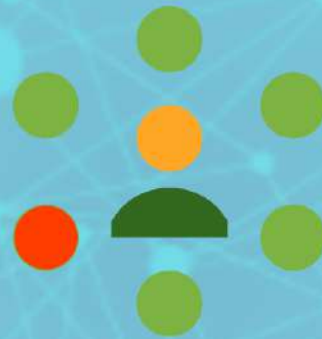


dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success
dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.148.40 for 34:8A:7B:71:5B:48 without success

Notaste la diferencia del ejemplo anterior?

memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.151.52 for 30:07:4D:74:3D:86 without success
memory	dhcp, warning	dhcp-HOTSPOT-TAYOLTITA offering lease 172.16.150.161 for 50:9E:A7:74:68:1F without success

Qué debo hacer?



Aislar el problema permitira tener un sistema robusto y de mayor disponibilidad.

Pool vacio en el servidor DHCP



Problema !

memory	dhcp, error	dhcp-HOTSPOT-MACHOBAYO: failed to give out IP address: pool <hs-pool-HOTSPOT-MACHOBAYO> is empty
memory	dhcp, error	dhcp-HOTSPOT-MACHOBAYO: failed to give out IP address: pool <hs-pool-HOTSPOT-MACHOBAYO> is empty
memory	hotspot, error, info, ..	failed to get IP address for host 88:AE:07:7A:CD:2E/172.16.70.61: pool empty (6)



Pool vacio en el servidor DHCP



Problema !

memory	dhcp, error	dhcp-HOTSPOT-MACHOBAYO: failed to give out IP address: pool <hs-pool-HOTSPOT-MACHOBAYO> is empty
memory	dhcp, error	dhcp-HOTSPOT-MACHOBAYO: failed to give out IP address: pool <hs-pool-HOTSPOT-MACHOBAYO> is empty
memory	hotspot, error, info, ..	failed to get IP address for host 88:AE:07:7A:CD:2E/172.16.70.61: pool empty (6)



Recuerdas como funciona un Servidor DHCP?





Pool vacio en Servidor DHCP



El Servidor DHCP almacena las direcciones ip en una tabla (leases) por un tiempo definido durante la configuracion del servidor dhcp.

Asociandolas con las direcciones mac de los clientes que lo han solicitado .



/ip dhcp-server lease



Pool vacio en Servidor DHCP

Recomendacion

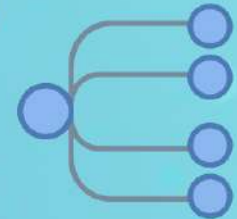


DHCP Server <dhcp-HOTSPOT-TAYOLTITA>

Name:	dhcp-HOTSPOT-TAYOLTITA	OK
Interface:	vlan-HOTSPOT-TAYOLTITA	Cancel
Relay:		Apply
Lease Time:	1d 00:00:00	Disable
Bootp Lease Time:	forever	Copy
Address Pool:	hs-pool-HOTSPOT-TAYOLTITA	Remove
Src. Address:		
Delay Threshold:		
Authoritative:	yes	
Bootp Support:	static	

Pool vacio en Servidor DHCP

Recomendacion



**Utilizar el tamaño de red adecuado
para los requerimientos de la red**





Problema en hotspot

Mala practica



Hotspot				
Servers Server Profiles Users User Profiles Active Hosts IP Bindings Service Po				
+ - ✓ ✗ 📁 🔍				
#		MAC Address	Address	To Address Server
34	P	🔑 CC:2D:E0:5F:87...		all
35	P	🔑 E4:8D:8C:4F:0E:74		all
36	P	🔑 68:72:51:40:F9:DE		all
37	P	🔑 E4:8D:8C:9D:A6...		all
38	P	🔑 64:D1:54:5F:6F:D7		all
39	P	🔑 64:D1:54:52:C5:...		all
40	P	🔑 44:D9:E7:BA:AD...		all
41	P	🔑 CC:2D:E0:00:24...		all
42	P	🔑 E4:8D:8C:50:EF:FF		all
43	P	🔑 E4:8D:8C:51:D5...		all
44	P	🔑 E4:8D:8C:51:D5...		all
45	P	🔑 E4:8D:8C:FA:19...		all
46	P	🔑 F4:8D:8C:B5:06:7B		all

742 items (1 selected)



Problema en hotspot

Mala practica



Hotspot

Servers Server Profiles Users User Profiles Active Hosts IP Bindings Service Profiles

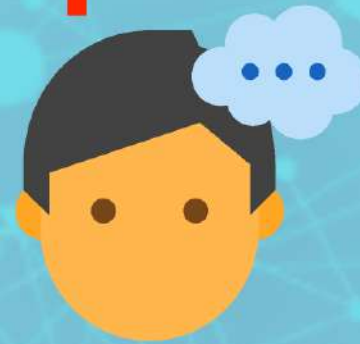
+ - ✓ ✗ 📁 🔍

#		MAC Address	Address	To Address	Server
34	P	CC:2D:E0:5F:87...			all
35	P	E4:8D:8C:4F:0E:74			all
36	P	68:72:51:40:F9:DE			all
37	P	E4:8D:8C:9D:A6...			all
38	P	64:D1:54:5F:6F:D7			all
39	P	64:D1:54:52:C5:...			all
40	P	44:D9:E7:BA:AD...			all
41	P	CC:2D:E0:00:24...			all
42	P	E4:8D:8C:50:EF:FF			all
43	P	E4:8D:8C:51:D5...			all
44	P	E4:8D:8C:51:D5...			all
45	P	E4:8D:8C:FA:19...			all
46	P	E4:8D:8C:B5:06:7B			all

742 items (1 selected)

Problema en hotspot

Ejemplo real !!!



Apr/08/2019 05:45:49	memory	wireless, info	C4:01:7C:E6:A8:E8@wlan1 established connection on 2442000, SSID Sevilla Premium
Apr/08/2019 05:45:52	memory	wireless, info	C4:01:7C:E6:A8:E8@wlan1: lost connection, received disassociation: unspecified (1)
Apr/08/2019 05:45:55	memory	wireless, info	C4:01:7C:E6:A8:E8@wlan1 established connection on 2442000, SSID Sevilla Premium
Apr/08/2019 05:45:59	memory	wireless, info	C4:01:7C:E6:A8:E8@wlan1: lost connection, received deauthentication: class 2 frame received (6)
Apr/08/2019 05:46:02	memory	wireless, info	C4:01:7C:E6:A8:E8@wlan1 established connection on 2442000, SSID Sevilla Premium
Apr/08/2019 05:46:22	memory	system, info, account	user admin logged out via local
Apr/08/2019 05:46:23	memory	wireless, info	C4:01:7C:E6:A8:E8@wlan1: lost connection, received deauthentication: class 2 frame received (6)
Apr/08/2019 05:46:26	memory	wireless, info	C4:01:7C:E6:A8:E8@wlan1 established connection on 2442000, SSID Sevilla Premium
Apr/08/2019 05:46:29	memory	wireless, info	C4:01:7C:E6:A8:E8@wlan1: lost connection, received deauthentication: class 2 frame received (6)
Apr/08/2019 05:46:32	memory	wireless, info	C4:01:7C:E6:A8:E8@wlan1 established connection on 2442000, SSID Sevilla Premium

Neighbor List

Discovery Settings

Find

Interface	IP Address	MAC Address	Ide...	Platform	Version	Board Name	IPv6	Age (s)	Uptime
wlan1	10.50.1.184	00:00:00:00:00:00					no	130	00:00:00
wlan1	10.50.3.184	74:4D:28:17:70:C8	Mikr...	MikroTik	6.40.9 (bugfix)	RB952Ui-5ac2nD	no	51	11:00:26
wlan1	10.50.0.131	E4:8D:8C:53:31:3B	Aul...	MikroTik	6.42.4 (stable)	RB962UGS-SHacT2HnT	no	49	18:07:14
wlan1	10.50.3.242	CC:2D:E0:4E:27:43	Mikr...	MikroTik	6.44.2 (stable)	RB931-2nD	no	4	20:19:14
wlan1	192.168.2.99	08:00:27:BF:9E:A5	Mikr...	MikroTik	6.42 (stable)	x86	no	38	00:02:08

5 items (1 selected)

```

[admin@MikroTik] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 192.168.220.254/24 192.168.220.0 ether1
1 D 10.50.1.168/20 10.50.0.0 wlan1
[admin@MikroTik] > /interface print detail
Flags: D - dynamic, X - disabled, R - running, S - slave
0 R name="ether1" default-name="ether1" type="ether" mtu=1500 actual-mtu=1500 l2mtu=1598 max-l2mtu=2028 mac-address=4C:5E:0C:14:8B:D5
last-link-up-time=jan/02/1970 00:00:42 link-downs=1

1 R name="wlan1" default-name="wlan1" type="wlan" mtu=1500 actual-mtu=1500 l2mtu=1600 max-l2mtu=2290 mac-address=4C:5E:0C:14:8B:D6
link-downs=0
[admin@MikroTik] > ping www.facebook.com
SEQ HOST SIZE TTL TIME STATUS
0 31.13.70.36 timeout
1 31.13.70.36 timeout
2 31.13.70.36 timeout
sent=3 received=0 packet-loss=100%

```

MERCADOWISPMEXICO



Interface List

Interface	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx
R ether1	Ethernet	1500	1598	51.8 kbps	11.3 kbps	12	15	51.8 kbps	
R wlan1	Wireless (Atheros AR...	1500	1600	1912 bps	20.9 kbps	3	20	1912 bps	

2 items (1 selected)

Neighbor List

Interface	IP Address	MAC Address	Id...	Platform	Version	Board Name	IPv6	Age (s)	Uptime
wlan1	10.50.3.184	74:4D:28:17:70:C8	Mikr...	MikroTik	6.40.9 (bugfix)	RB952U-Sac2nD	no	18	11:19:51
wlan1	10.50.0.131	E4:8D:8C:53:31:38	Aul...	MikroTik	6.42.4 (stable)	RB962UGS-SHacT2HnT	no	17	18:26:38

Terminal

```

0 R name="ether1" default-name="ether1" type="ether" mtu=1500 actual-mtu=1500 l2mtu=1598 max-l2mtu=2028 mac-address=4C:5E:0C:14:8B:D5
last-link-up-time=jan/02/1970 00:00:42 link-downs=1

1 R name="wlan1" default-name="wlan1" type="wlan" mtu=1500 actual-mtu=1500 l2mtu=1600 max-l2mtu=2290 mac-address=CC:2D:E0:4E:27:43
last-link-up-time=jan/02/1970 00:27:10 link-downs=29

admin@MikroTik] > ping 8.8.8.8

```

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	8.8.8.8	56	43	45ms	
1	8.8.8.8	56	43	169ms	
2	8.8.8.8	56	43	50ms	
3	8.8.8.8	56	43	79ms	
4	8.8.8.8	56	43	38ms	
5	8.8.8.8	56	43	121ms	
6	8.8.8.8	56	43	48ms	
7	8.8.8.8	56	43	90ms	
8	8.8.8.8	56	43	69ms	

```

sent=9 received=9 packet-loss=0% min-rtt=38ms avg-rtt=78ms max-rtt=169ms

admin@MikroTik] >

```

Qué debo hacer ?



Usar medidas de protección general contra todos los posibles problemas de un mismo origen sera lo mas efectivo en un hotspot





Manos a la obra!!!



 **MERCADOWISPMEXICO**

México 2019





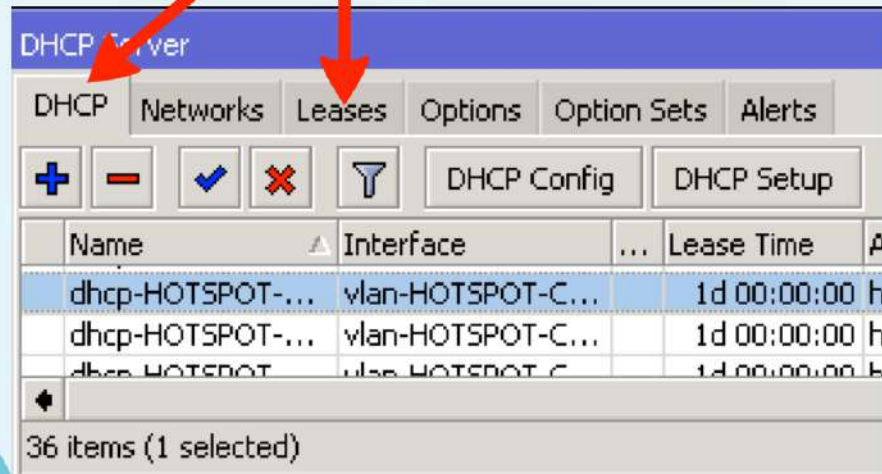
/ip dhcp-server

IP	ARP
MPLS	Accounting
Routing	Addresses
System	Cloud
Queues	DHCP Client
Files	DHCP Relay
Log	DHCP Server
Radius	DNS

NETWORK

DHCP

DHCP Server



`/ip dhcp-server set add-arp=yes [find]`



1

DHCP Server <dhcp1>

Name:	dhcp1	OK
Interface:	bridge-H5-CASA-BOSQUES	Cancel
Relay:		Apply
Lease Time:	01:00:00	Disable
Bootp Lease Time:	forever	Copy
Address Pool:	hs-pool-14	Remove
DHCP Option Set:		
Src. Address:		
Delay Threshold:		
Authoritative:	yes	
Bootp Support:	static	
	☐ Always Broadcast	
Insert Queue Before:	first	
	☒ Add ARP For Leases	

/ip dhcp-server lease print



DHCP Server

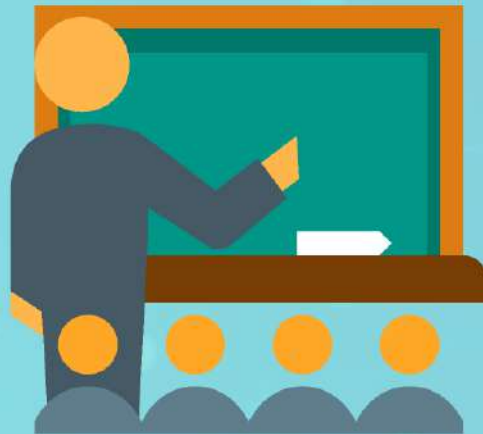
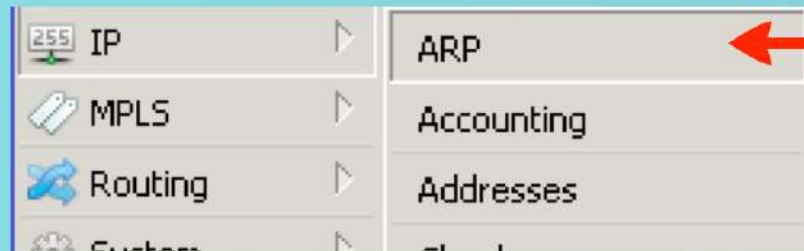
[DHCP](#)
[Networks](#)
[Leases](#)
[Options](#)
[Option Sets](#)
[Alerts](#)

[+](#)
[-](#)
[✓](#)
[✗](#)
[📄](#)
[🔍](#)
[Check Status](#)

	Address	MAC Address	Client	Server	Active Address	Active MAC Address	Active Hostname	Expires At	Status
D	172.16.20.200	4C:91:0C:1...		dhcp-HOTS...	172.16.20.200	4C:91:0C:1A:B3:F3	android-d...	18:31:35	bound
D	172.16.20.202	80:6C:1B:2A...		dhcp-HOTS...	172.16.20.202	80:6C:1B:2A:9D:...	android-2...	03:02:14	bound
D	172.16.20.203	BC:3D:85:84...		dhcp-HOTS...	172.16.20.203	BC:3D:85:84:D9:66	HUAWEI_...	14:48:46	bound
D	172.16.20.206	A0:39:F7:11...		dhcp-HOTS...	172.16.20.206	A0:39:F7:11:F1:42	android-2...	18:22:48	bound
D	172.16.20.209	5C:77:76:2D...		dhcp-HOTS...	172.16.20.209	5C:77:76:2D:1A:64	android-e...	21:06:34	bound
D	172.16.20.210	00:08:22:96...		dhcp-HOTS...	172.16.20.210	00:08:22:96:7C:EC	android-1...	23:28:31	bound
D	172.16.20.214	00:08:22:A5...		dhcp-HOTS...	172.16.20.214	00:08:22:A5:A8:F9	android-b...	21:00:36	bound

7018 items

/ip arp print



ARP List

	IP Address	MAC Address	Interface
DCH	172.16.20.26	3C:05:18:73:57:7C	vlan-HOTSPOT-
DCH	172.16.20.27	60:72:0B:8E:6C:B2	vlan-HOTSPOT-
DCH	172.16.20.28	40:4E:36:0E:3A:EC	vlan-HOTSPOT-
DCH	172.16.20.29	A0:57:E3:36:AE:74	vlan-HOTSPOT-
DCH	172.16.20.30	D0:04:01:FB:97:DD	vlan-HOTSPOT-
DCH	172.16.20.31	B8:53:AC:89:D1:3F	vlan-HOTSPOT-
DCH	172.16.20.32	CC:2D:E0:76:65:38	vlan-HOTSPOT-
DCH	172.16.20.33	38:80:DF:5C:4B:5A	vlan-HOTSPOT-
DCH	172.16.20.34	D0:04:01:7F:F0:37	vlan-HOTSPOT-
DCH	172.16.20.36	E8:93:09:2C:84:E8	vlan-HOTSPOT-
DCH	172.16.20.37	90:06:28:8C:45:45	vlan-HOTSPOT-
DCH	172.16.20.38	1C:23:2C:4E:ED:BF	vlan-HOTSPOT-
DCH	172.16.20.40	4C:91:0C:18:D0:71	vlan-HOTSPOT-
DCH	172.16.20.41	64:D1:54:52:59:84	vlan-HOTSPOT-
DCH	172.16.20.42	34:23:BA:EF:29:20	vlan-HOTSPOT-

7080 items



/interface print



/interface vlan set number="#INTERFACE" arp=reply-only

Interface List

Interface	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p
R	vlan-HOT...	VLAN	1500	1576	909.7 kbps	331.4 kbps	
R	vlan-HOT...	VLAN	1500	1576	15.4 Mbps	2.6 Mbps	
R	vlan-HOT...	VLAN	1500	1576	968 bps	0 bps	
R	vlan-HOT...	VLAN	1500	1576	257.9 kbps	39.0 kbps	
R	vlan-HOT...	VLAN	1500	1576	4.3 Mbps	774.1 kbps	
R	vlan-HOT...	VLAN	1500	1576	15.5 Mbps	1549.3 kbps	
R	vlan-HOT...	VLAN	1500	1576	13.1 Mbps	1714.3 kbps	
R	vlan-HOT...	VLAN	1500	1576	9.3 Mbps	1218.5 kbps	
R	vlan-HOT...	VLAN	1500	1576	3.5 Mbps	521.4 kbps	
R	vlan-HOT...	VLAN	1500	1576	14.1 Mbps	1438.4 kbps	
R	vlan-HOT...	VLAN	1500	1576	167.2 kbps	95.9 kbps	
R	vlan-HOT...	VLAN	1500	1576	440 bps	2.7 kbps	
R	vlan-HOT...	VLAN	1500	1576	6.3 Mbps	638.4 kbps	
R	vlan-HOT...	VLAN	1500	1576	5.4 Mbps	371.5 kbps	
R	vlan-HOT...	VLAN	1500	1576	6.5 Mbps	695.1 kbps	

53 items

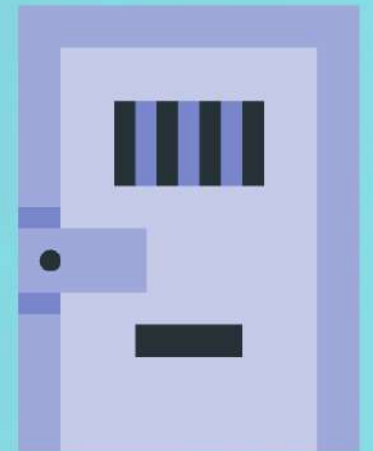
Interface <vlan-HOTSPOT-MUMMX19>

General	Loop Protect	Status	Traffic
Name:	vlan-HOTSPOT-MUMMX19		
Type:	VLAN		
MTU:	1500		
Actual MTU:	1500		
L2 MTU:	1576		
MAC Address:	E4:8D:8...4:72:2E		
ARP:	reply-only		
ARP Timeout:			

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch



Qué hicimos?

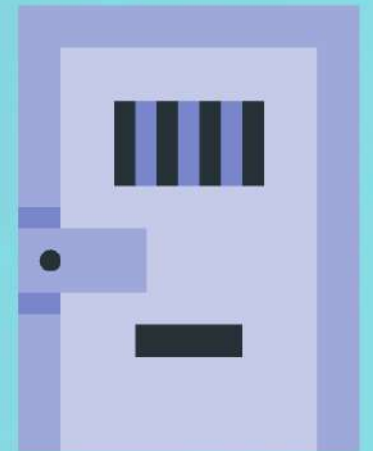




Qué hicimos?



DHCP + ARP

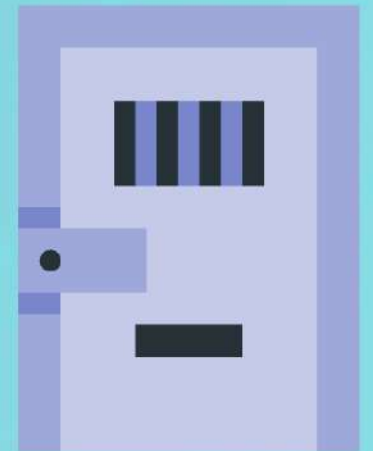




Qué hicimos?



DHCP + ARP

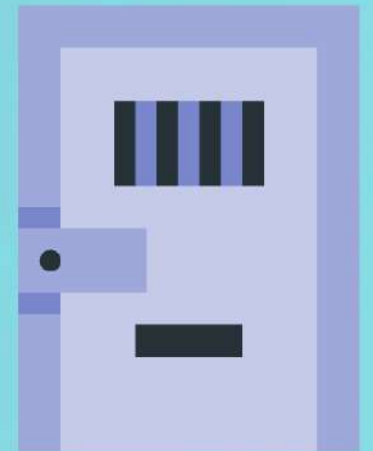




Qué hicimos?

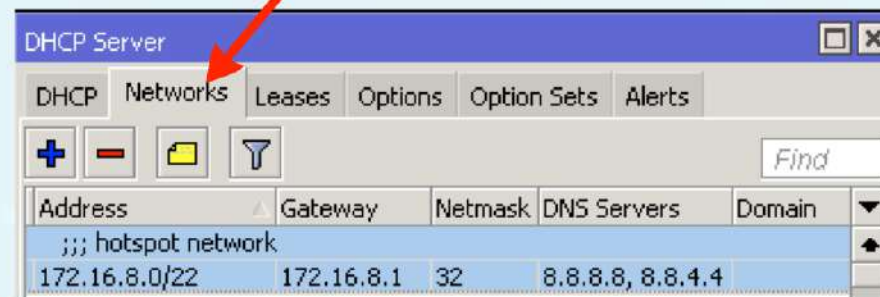


DHCP + ARP



NETWORK

/ip dhcp-server network



/ip dhcp-server network



DHCP Network <172.16.20.0/22>

Address:	172.16.20.0/22	OK
Gateway:	172.16.20.1	Cancel
Netmask:	32	Apply
DNS Servers:	8.8.8.8	Comment
	8.8.4.4	Copy



Si és posible hacer esto?



Calculadora IP

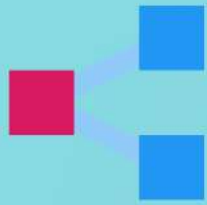
Address (Host or Network) Netmask (i.e. 24) Netmask for sub/supernet (optional)

172.16.20.1 / 32 move to:

Calcular [limpiar](#)

Address: 172.16.20.1 10101100.00010000.00010100.00000001
Netmask: 255.255.255.255 = 32 11111111.11111111.11111111.11111111
Wildcard: 0.0.0.0 00000000.00000000.00000000.00000000
=>
Hostroute: 172.16.20.1 10101100.00010000.00010100.00000001
Hosts/Net: 1 ← Class B, Private Internet

AprendaRedes.com, Versión: 0.38



DHCP vs PPPoE



Están en la misma dirección de red



+ - ✓ ✗ 📄 🔍			
Dynamic ▼ is ▼ yes			
	Address	Network	Interface
D	📶 172.19.1.252	172.19.1.1	<pppoe-ORLANDOL...
D	📶 172.19.1.252	172.19.1.2	<pppoe-SILVIABRO...
D	📶 172.19.1.252	172.19.1.3	<pppoe-MARTHAJ...
D	📶 172.19.1.252	172.19.1.4	<pppoe-JUANLOPEZ>
D	📶 172.19.1.252	172.19.1.5	<pppoe-CLAUDIAA...
D	📶 172.19.1.252	172.19.1.6	<pppoe-ANTONIAD...

Rutas con túneles PPP

Route List

Routes | Nexthops | Rules | VRF

Connected is yes

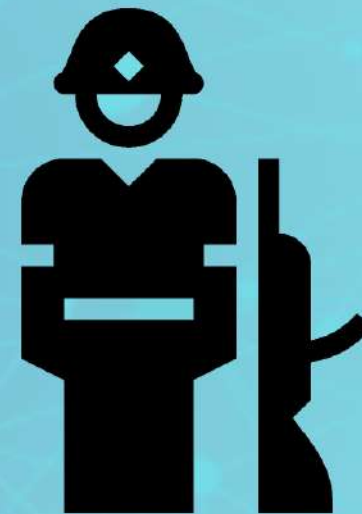
	Dst. Address	Gateway
DAC	▶ 172.19.1.1	<pppoe-ORLANDOL...
DAC	▶ 172.19.1.2	<pppoe-SILVIABRO...
DAC	▶ 172.19.1.3	<pppoe-MARTHAJO...
DAC	▶ 172.19.1.4	<pppoe-JUANLOPEZ...
DAC	▶ 172.19.1.5	<pppoe-CLAUDIAA...
DAC	▶ 172.19.1.6	<pppoe-ANTONIAD...
DAC	▶ 172.19.1.8	<pppoe-CRISTHIAN...

/32

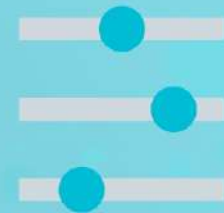


/ip firewall

255 IP	ARP
MPLS	Accounting
Routing	Addresses
System	Cloud
Queues	DHCP Client
Files	DHCP Relay
Log	DHCP Server
Radius	DNS
Tools	Firewall
New Terminal	Hotspot
LCD	IPsec



/ip firewall filter



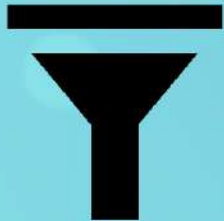
```
# SERIAL NUMBER = A20209270ED0
/ip firewall filter
add action=accept chain=input connection-state=established,related
add action=accept chain=input dst-port=179 protocol=tcp
add action=accept chain=input dst-port=8291 protocol=tcp
add action=drop chain=input connection-state=invalid
add action=drop chain=input in-interface-list=Internet
```

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

+ - [check] [X] [icon] 00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Int...	Out. I...	In. Int...	Out. I...	Src. A...	Dst. A...	Bytes	Packets
0	drop	prerouting			6 (tcp)		53			Internet				1740 B	39
1	drop	prerouting			17 (...)		53			Internet				1226.7 KiB	21 284
2	drop	prerouting								Internet		IREDE...		192 B	6





DNS

DNS Settings

Servers:	8.8.8.8	OK
	8.8.4.4	Cancel
Dynamic Servers:		Apply
	☐ Allow Remote Requests	Static
Max UDP Packet Size:	4096	Cache
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:	2048 KIB	

Conclusion

Conocer nuestra red es lo mas importante ante cualquier incidente!!!



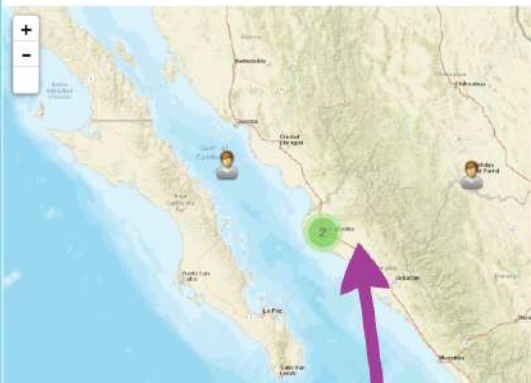
Contacto

Cel/WhatsApp: +521 6681055479

Web: <https://www.mercadowispmexico.com.mx>

Correo: soporte@mercadowispmexico.com

List of MikroTik Certified Consultants



<https://mikrotik.com/consultants/latinamerica/mexico>

MikroTik

Home About Buy Jobs Hardware Software Support Training Account

Support

General Forum Consultants RMA

North America +

Latin America -

- Argentina
- Bolivia
- Brazil
- Chile
- Colombia
- Costa Rica
- Dominican Republic
- Ecuador
- El Salvador
- Guatemala

Latin America

Miguel Angel Felix Garcia **MUM** **Presenter**

MTCRE, MTCWE, MTCTCE, MTCUME, MTCIPv6E, MTCINE
LOS MOCHIS, Mexico

Experience and successful cases: Network Design, Routing OSPF, BGP, MPLS, VRF, Traffic Engineering, VPN, Firewall, Load Balance, Failover, Tunnels, QoS, Wireless Solutions, CAPsMAN, Hotspot, Radius and Remote WISP Consulting.

5216681055479 www.mercadowispmexico.com.mx Email 5216681055479

<https://mikrotik.com/consultants/latinamerica/mexico>

México 2019

