## **Chéridanh TSIELA**

# **BTS SIO - SISR**

## **Epreuve E5**

# Projet Réseau : Mise en place d'un réseau Wifi

# Partie A : Configuration Access Point (AP) sur MikroTik

#### I – Contexte

Dans le cadre de l'amélioration de ses infrastructures informatiques, la Maison des Ligues (M2L) a entrepris la mise en place d'un réseau sans fil (Wi-Fi) pour répondre aux besoins croissants de connectivité de ses utilisateurs. Ce réseau sans fil est conçu pour connecter plusieurs VLANs distincts, chacun dédié à un groupe spécifique d'utilisateurs ou à des services particuliers.

#### II – Prérequis

- Routeur hAP Lite MikroTik
- Logiciel WinBox

#### II – Configuration du routeur AP

Pour connecter un appareil sans fil avec MikroTik Wifi AP, les appareils sans fil doivent fournir une clé de sécurité (mot de passe). MikroTik sans fil prend en charge les types d'authentification WPA PSK et WPA2 PSK. Les étapes suivantes montreront comment créer un mot de passe pour MikroTik Wifi AP avec profil de sécurité.

Depuis WinBox, cliquez sur le menu « Wireless ». La fenêtre Tables sans fil apparaîtra.

**AP MikroTik** 

- Cliquez sur l'onglet « Security Profiles », puis cliquez sur SIGNE PLUS (+). La fenêtre Nouveau profil de sécurité apparaîtra.
- Mettez un nom de profil significatif (profil Wifi) dans le champ de saisie « Name ».
- Choisissez « dynamic keys » dans le menu déroulant Mode.
- Cochez les cases « WPA PSK et WPA2 PSK » dans le panneau Types d'authentification.
- Fournissez maintenant un mot de passe fort dans la zone « WPA Pre-Shared Key » et « WPA2 Pre-Shared Key ».
- Puis cliquez sur le bouton « OK »

New Secu	rity Profile			
General	RADIUS	EAP	Static Keys	OK
		Name:	M2L-Security	Cancel
		Mode:	dynamic keys 🛛 🔻	Apply
Au	thentication	Types:	WPA PSK WPA2 PSK	Comment
	Unicast	Cinhers:		Сору
	Group	Ciphers:	✓ aes ccm □ tkip	Remove
W	PA Pre-Shar	red Key:	•••••	
WP	A2 Pre-Shar	red Key:	•••••	
	Supplicant	Identity:		
	Group Key	Update:	00:05:00	
Mana	agement Pro	tection:	disabled 🛛 🔻	
Managem	ent Protecti	ion Key:		
			Disable PMKID	

Après avoir créé le profil de sécurité, nous allons maintenant définir le mode sans fil et créer un SSID (Service Set Identifier) afin que les appareils sans fil puissent trouver notre point d'accès MikroTik avec le SSID créé.

Cliquez sur l'onglet **« Wifi Interfaces »** et vous trouverez ici l'interface WLAN (par défaut : wlan1). Il peut être désactivé la première fois.

Donc, si vous trouvez désactivé, cliquez dessus avec le bouton droit de la souris, puis cliquez sur l'option « **Enable** » pour activer l'interface Wifi.

Wireless Tables													Г	
WiFi Interfaces	W60G Stat	ion Nstreme Du	al Access List	Registration	Connect List	t Security Pro	files Chanr	nels Int	terworking P	rofiles			E	
+ 🗸	× 🗆	CAP	WPS Client	Setup Repeater	Scanner	Freq. Usage	Alignmen	t Wire	eless Sniffer	Wireless	Snooper	Align	Find	
Name	1	Туре	Actual	MTU MAC Ad	dress	ARP Mod	Band	Chann.	Frequen	SSID	Tx		Rx	-
gy was	selected	Show Category Detail Mode Inline Comme Show Column Find Find Next Select All Add Remove Enable Comment Torch Reset Traffic C	ounters	Ctrl+F Ctrl+G Ctrl+A > DEL Ctrl+E Ctrl+D Ctrl+M					2112					•

- Double-cliquez sur l'interface Wifi disponible et activée. La fenêtre d'interface apparaîtra.
- Dans l'onglet Général, vous pouvez définir le nom de l'interface Wifi dans la zone de saisie « **Name** » ou vous pouvez le conserver par défaut (wlan1).

Interface <wlan< th=""><th>1&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></wlan<>	1>										
General Wir	eless	HT	WDS	Nstreme	NV2	Advance	d Status				ОК
Name:	wlan1									(	Cancel
Туре:	Wirel	ess (At	heros Al	R9300)							Apply
MTU:	1500									[	Disable
Actual MTU:	1500									C	omment
	1600									Adva	nced Mode
MAC Address:	DC:20	C:6E:E ed	A:F0:2A								Torch
ARP Timeout:								•		Reset T	raffic Counters
										WP	S Accept
										W	PS Client
										Setup	o Repeater
											Scan
										Freq	. Usage
											Align
											Sniff
										Sr	nooper
										Reset (	Configuration
enabled			runr	ning	slave		passthrou	gh s	sea	rching	

AP MikroTik

- Cliquez sur l'onglet « Wireless » et choisissez « ap bridge » dans le menu déroulant Mode.
- Mettez le nom SSID dans la zone de saisie « SSID ».
- Cliquez maintenant sur le bouton Mode avancé et choisissez votre profil de sécurité créé dans le menu déroulant Profil de sécurité.
- Assurez-vous que les cases Authentification par défaut et Transfert par défaut sont cochées. Sinon, les appareils ne seront pas connectés jusqu'à l'authentification MAC.

Interface <wlan1></wlan1>							
General Wireless	HT WDS	8 Nstreme	NV2	Status	Traffic		ОК
Mode	ap bridge					₹	Cancel
Band	: 2GHz-B/G	ì				₹	Apply
Channel Width:	20MHz					₹	Disable
Frequency	: 2412	1.				<b>∓</b> MHz	Comment
Socurity Profile	Maison de	es Ligues					Advanced Mode
WPS Mode:	: push butto	nity				▼	Torch
Frequency Mode	: regulatory	domain				Ŧ	Reset Traffic Counters
Country	etsi					₹	WPS Accept
Installation	any					₹	WPS Client
Default AP Tx Limit	:					▼ bps	Setup Repeater
Default Client Tx Limit:	:					▼ bps	Sean
	<ul> <li>Default</li> </ul>	Authenticate	e				Freq Usage
	✓ Default	Forward					Alian
	Hide S	SID					Sniff
							Spooper
							Reset Configuration
enabled	ru	nning	slave		passthro	ugh s	earching

Le SSID désormais créé sera trouvé dans les appareils sans fil et l'appareil sans fil peut être connecté en fournissant un mot de passe.

A présent que notre premier SSID est créé, nous allons créer d'autres **SSID virtuel** pour chaque réseau de notre entreprise en taguant des VLAN correspondant à chaque réseau.

Avant la création des SSID, nous allons d'abord configurer les profils de sécurité de SSID virtuel dans l'onglet « Security Profiles » dans le menu « Wireless »

Security Pr	ofile <m2l-s< th=""><th>Security</th><th>-Admin&gt;</th><th></th><th></th><th>[</th><th>×</th><th> </th></m2l-s<>	Security	-Admin>			[	×	
General	RADIUS	EAP	Static Keys	Γ		ОК		
		Name:	M2L-Security-Admin		(	Cancel		
		Mode:	dynamic keys ₹			Apply		
Au	thentication	Types:	WPA PSK WPA2 PSK		C	omment	:	
	Universit (	·	WPA EAP WPA2 EAP			Сору		
	Group (	Ciphers: Ciphers:	v aes ccm tkip		R	lemove		
WP	PA Pre-Shar A2 Pre-Shar Supplicant Group Key I agement Pro	ed Key: ed Key: ldentity: Update: tection:	00:05:00      disabled     ₹					
Managem	ent Protecti	on Key:	Disable PMKID					
Vireless Tab <u>les</u>								
WiFi Interfaces	W60G Station	Nstreme [	Dual Access List Registration Connect List Secur	urity Pr	ofiles	Channels	Interwor	king Profiles
Name M2L-Security	A Mode	nic keys	Authentication Types Unicast Ciphers Group Cipher WPA PSK WPA2 PSK aes ccm aes ccm	hers	WPA P	re-Shared H	Key	WPA2 Pre-Share
M2L-Security-	Admin dunan	nic kove	MPA PSK WPA2 PSK are com are com		•••••			•••••

aes ccm

aes ccm

Nous allons trois profils de sécurités : Admin, Direction et Compta

Une fois les profils de sécurités créés, nous allons maintenant créés les interfaces wifi virtuelles pour chaque réseau.

aes ccm

aes ccm

•••••

.....

•••••

.....

Rendez-vous dans le menu « Wireless » puis « SIGNE PLUS (+) » puis cliquez sur « Virtuel »



AP MikroTik

M2L-Security-Compta

default

5 items

M2L-Security-Direction

dynamic keys

dynamic keys

none

WPA PSK WPA2 PSK

WPA PSK WPA2 PSK

https://cheridanh/projects

Nous allons créer les trois SSID en mettant un nom, en choisissant le profil de sécurité qui correspond et à chaque interface virtuelle, on va lui attribuer un « VLAN ID »

Interface <wlan2></wlan2>		
General Wireless W[	OS Status Traffic	ОК
Mode	ap bridge 🛛 🔻	Cancel
Secondary Channel	\$	Apply
SSID	M2L Admin	Disable
Master Interface	wlan1 ▼	Comment
Security Profile	M2L-Security-Admin	Сору
WPS Mode	: disabled	Remove
VLAN Mode	: use tag	Advanced Mode
VLAN ID	: 100	Torch
Default AP Tx Rate	. ▼ bps	Reset Traffic Counters
Default Client Tx Rate	∵ bps	
	<ul> <li>Default Authenticate</li> </ul>	
	Default Forward	
	Hide SSID	
enabled	running slave passthrough	running ap

### VLAN ID : 100 pour l'interface virtuel Admin

### VLAN ID : 120 pour l'interface virtuel Direction

Interface <wlan3></wlan3>				
General Wireless W[	S Status T	raffic		ОК
Mode	ap bridge		₹	Cancel
Secondary Channel	:		\$	Apply
SSID	M2L Direction	1		Disable
Master Interface	: wlan 1		₹	Comment
Security Profile	M2L-Security-	Direction	<b></b>	Сору
Interworking Profile			· · ·	Remove
VLAN Mode	use tag		₹	Advanced Mode
VLAN ID	120			Torch
Default AP Tx Rate	:		▼ bps	Reset Traffic Counters
Default Client Tx Rate	:		▼ bps	
	<ul> <li>Default Aut</li> </ul>	thenticate		
	✓ Default For	ward		
	Hide SSID			
enabled	running	slave	passthrough	running ap

AP MikroTik

Interface <wlan4></wlan4>			
General Wireless W[	S Status Traffic		ОК
Mode	ap bridge	₹	Cancel
Secondary Channel		\$	Apply
SSID	M2L Compta		Disable
Master Interface	wlan1	<b>.</b>	Comment
Security Profile	M2L-Security-Compta	3₹	Сору
Interworking Profile	disabled	•	Remove
WFS Mode	disabled		
VLAN Mode	use tag		Advanced Mode
VLAN ID	121		Torch
Default AP Tx Rate		▼ bps	Reset Traffic Counters
Default Client Tx Rate		▼ bps	
	<ul> <li>Default Authentica</li> </ul>	ate	
	<ul> <li>Default Forward</li> </ul>		
	Hide SSID		
enabled	running slave	passthrough	running ap

VLAN ID : 121 pour l'interface virtuel Compta

Ce qui nous donne le résultat suivant :

Wireless 7	<b>Fables</b>																[	□×
WiFi Inte	erfaces	W60G Station	Nstreme	Dual Ac	ccess List	Registration	Con	nect List	Sec	urity Profile	s Channel	ls Interv	working Pr	rofiles				
<b>+</b> -	- 🖉	× 🖻 🍸	CAP	WPSC	Client S	etup Repeater	Sc	anner	Freq.	Usage	Alignment	Wireles	ss Sniffer	Wireless	s Snooper	Align	Find	
	Name		Туре			Actual M 🔽	MAC	Address		ARP	Mode	Band	Chann	Frequen	SSID		Tx	•
S	😝 wlan	1	Wireless (	Atheros A	(R9300)	1500	DC:20	C:6E:EA:F	0:2A	enabled	ap bridge	2GHz	20MHz	2412	Maison des	Ligues		
	<=> W	lan2	Virtual			1500	DE:20	C:6E:EA:F	0:2A	enabled	ap bridge				M2L Admin	1		
	<=> W	lan3	Virtual			1500	DE:20	C:6E:EA:F	0:2B	enabled	ap bridge				M2L Directi	ion		
	<=> W	lan4	Virtual			1500	DE:20	C:6E:EA:F	0:2C	enabled	ap bridge				M2L Compt	ta		
•												·		· 			•	•
4 items ou	t of 11																	

Les SSID désormais créés seront trouvés dans les appareils sans fil et l'appareil sans fil peut être connecté en fournissant un mot de passe que nous avions saisis dans le profil de sécurité.

Mais la connexion ne suffit pas pour accéder à Internet. L'adresse IP, la passerelle par défaut et d'autres paramètres réseau doivent être fournis pour accéder à Internet aux appareils connectés. Nous allons donc maintenant configurer le serveur DHCP pour attribuer automatiquement l'adresse IP, la passerelle par défaut et d'autres paramètres réseau.

Nous allons maintenant créer une interface bridge et ajouter les interfaces wifi virtuelles, y compris le port physique sur lequel nous voulions connecter au switch à ce pont.

**AP MikroTik** 

- Cliquez sur le menu « Bridge ». L'interface du bridge apparaîtra.
- Dans l'onglet « **Bridge** », cliquez sur **SIGNE PLUS (+)**. La fenêtre Nouvelle interface apparaîtra.
- Mettez le nom de l'interface du bridge dans le champ de saisie « Name ».

Interface <bridge-wlan1-ether1></bridge-wlan1-ether1>	
General STP VLAN Status Traffic	ОК
Name: Bridge-ether2-vitrualWLAN	Cancel
Type: Bridge	Apply
MTU:	Disable
Actual MTU: 1500	Comment
L2 MTU: 1598	Сору
ARP: enabled	Remove
ARP Timeout:	Torch
Admin. MAC Address:	Reset Traffic Counters
Ageing Time: 00:05:00	
· · · · · · · · · · · · · · · · · · ·	
enabled running slave	passthrough

- Cliquez maintenant sur l'onglet « **Ports** » et cliquez sur **SIGNE PLUS (+)**. La fenêtre Nouveau bridge de pont apparaîtra.
- Choisissez l'interface « ether2 » dans le menu déroulant Interface.
- Choisissez l'interface de bridge créée dans le menu déroulant Bridge.
- Cliquez sur « OK » faîtes de même pour les interfaces virtuelles « wlan2, wlan3, wlan4 ».

Bridge Port <ether.< th=""><th>2&gt;</th><th></th></ether.<>	2>	
General STP	VLAN Status	ОК
Interface:	ether2	Cancel
Bridge:	Bridge-ether2-vitrualWLAN	Apply
Horizon:	▼	Disable
Leam:	auto Ŧ	Comment
	<ul> <li>Unknown Unicast Flood</li> </ul>	Сору
	<ul> <li>Unknown Multicast Flood</li> </ul>	Bemove
	✓ Broadcast Flood	
	Trusted	
	✓ Hardware Offload	
Multicast Router:	Temporary Query F	
	Fast Leave	
enabled	inactive Hw. Offload	9

**AP MikroTik** 

Faites de même pour les interfaces virtuelles, ce qui donne :

Bridge															×
Bridge	Ports	Port Ext	ensions	VLANs	MSTIs	Port MST	Port MST Overrides MVRP			tes Filters NAT Hos			MDB		
+ -		× 🖻	7											Find	
#	#       Interface       Bridge       Horizon       Trusted       Priority (h       PVID       Role       Actual Pa       Root Pat       Internal R       ▼														
0 H	👗 et	ther2	Bridge-et	her2-vitrua	alWLAN		no	80	1	designa	ited port		200000		
11	👗 и	ilan2	Bridge-et	her2-vitrua	alWLAN		no	80	1						
21	👗 и	ilan3	Bridge-et	her2-vitrua	alWLAN		no	80	1						
31	👗 и	ilan4	Bridge-et	her2-vitrua	alWLAN		no	80	1						
4 items	4 items														

Configurons à présent les interfaces réseau. Pour se faire, nous allons mettre les adresses IP sur nos interfaces WAN et LAN (tous nos VLANs).

Pour l'interface WAN, rendez-vous dans le menu « IP => DHCP Client » et cliquez sur SIGNE PLUS (+). Choisissez l'interface « ether1 » puis faites « OK »

DHCP Client <ether1></ether1>	
DHCP Advanced Status	ОК
Interface: ether1	Cancel
Use Peer DNS	Apply
Use Peer NTP	Disable
Add Default Route: yes	Comment
	Сору
	Remove
	Release
	Renew
enabled Status: bound	

### Ce qui donne

DHCP Client							×
DHCP Client	DHCP Clie	ent Option	IS				
+ - •	× 🗅	7	Release	Renew		Find	
Interface	Δ	Use P	Add D	IP Address	Expires After	Status	┱
ether1		yes	yes	10.190.0.67/24	23:05:30	bound	
1 item (1 selecte	ed)						

AP MikroTik

Pour l'interface LAN, nous avions trois VLAN, nous allons donc créer des interfaces VLANs que nous mettrons des adresses IP par après.

- Rendez-vous dans le menu « Interfaces => VLANs » et cliquez sur SIGNE PLUS (+).
- Mettez le nom du VLAN
- Mettez un « VLAN ID » identique à celui que nous avions créés dans l'interface Wifi Virtuel
- Choisissez l'interface bridge que nous avions créés puis faites « OK »

Interface <vlan< th=""><th>V-Admin&gt;</th><th></th><th></th><th></th></vlan<>	V-Admin>			
General Loo	p Protect Status Tra	affic	. [	ОК
Name:	VLAN-Admin			Cancel
Туре:	VLAN			Apply
MTU:	1500			Disable
Actual MTU:	1500			Comment
L2 MTU:	1594			Comment
MAC Address:	DC:2C:6E:EA:F0:26			Сору
ARP:	enabled		₹	Remove
ARP Timeout:			▼ [	Torch
VLAN ID:	100			Reset Traffic Counters
Interface:	Bridge-ether2-vitrualWL	AN	₹	
	Use Service Tag			
	MVRP			
enabled		running	slave	passthrough

Faites de même pour les autres interfaces, ce qui donne :

Interface L	ist											
Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VXLAN	VRRP	VETH	MACVLAN	Bonding	LTE
+ -	<ul><li>✓ X</li></ul>	7									Fir	d
	Name	∠ Type		MTU	Actual MTU	L2 MTU	VLAN ID	Interfac	е		Тх	-
R	😝 VLAN-Admin	VLAN		1500	1500	1594	100	Bridge-e	ther2-vitr	ualWLAN		336
R	😝 VLAN-Compta	VLAN		1500	1500	1594	121	Bridge-e	ther2-vitr	ualWLAN		0
R	😝 VLAN-Directior	n VLAN		1500	1500	1594	120	Bridge-e	ther2-vitr	ualWLAN		0
•	t of 14 (1 colocitod	<b>N</b>										•
5 items ou	t of 14 (1 selected,	)										

Pour adresser les interfaces des VLANs, rendez-vous dans le menu « IP => Adresses » et cliquez sur SIGNE PLUS (+). Choisissez l'interface VLAN correspondante, mettez l'adresse IP puis faites « OK »

**AP MikroTik** 

Address <172	2.16.100.1/24>		
Address: 17	72.16.100.1/24		ОК
Network: 17	72.16.100.0		Cancel
Interface: 🚺	(LAN-Admin	₹	Apply
			Disable
			Comment
			Сору
			Remove
enabled			

### Ce qui donne :

Address List		
+- * * #	T	Find
Address	Network	Interface 🔻
D 🛉 10.190.0.67/24	10.190.0.0	ether1
+ 172.16.100.1/24	172.16.100.0	VLAN-Admin
+ 172.16.120.1/24	172.16.120.0	VLAN-Direction
+ 172.16.121.1/24	172.16.121.0	VLAN-Compta
4.7		
4 items		

A présent rendez-vous dans le menu « Bridge »

- Cliquez maintenant sur l'onglet « VLANs » et cliquez sur SIGNE PLUS (+). La fenêtre Nouveau bridge de pont apparaîtra.
- Mettez l'ID du VLANs correspondant dans « VLAN IDs »
- Choisissez « ether2 » et l'interface wifi virtuel correspondant à chaque vlan
- Cliquez sur « **OK** » faîtes de même pour les autres VLANs.

Bridge VLAN <100>	,	
Bridge:	Bridge-ether2-vitrualWLAN	ОК
VLAN IDs:	100 🗢	Cancel
Tagged:	ether2 🗧 🗧	Apply
Untagged:	wlan2	Disable
MVRP Forbidden:	<b>≜</b>	Comment
	· · · · · · · · · · · · · · · · · · ·	Сору
Current Tagged:		Remove
Current Untagged:		
enabled		

AP MikroTik

Ce qui donne :

Bridge									
Bridge Ports Port Extensions	VLANs	MSTIs	Port MST Overrides	MVRP Attributes	Filters	NAT	Hosts	MDB	
<b>+ - * ×</b> 🗖 🏹	MVRP /	Attributes							Find
Bridge	VLAN I	Ds	Current Tagged		Cun	ent Unt	agged		
Bridge-ether2-vitrualWLAN	100								
Bridge-ether2-vitrualWLAN	120								
Bridge-ether2-vitrualWLAN	121								
3 items (1 selected)									

Nous allons maintenant configurer le serveur DHCP sur l'interface Bridge afin que les utilisateurs Wifi et les utilisateurs LAN puissent obtenir automatiquement l'adresse IP, la passerelle par défaut et d'autres paramètres réseau.

Rendez-vous dans le menu « IP => Pool » et cliquez sur SIGNE PLUS (+).

Mettez un nom à votre plage et saisissez une plage d'adresse IP d'adresses pour votre pool puis cliquez sur « **OK** ».

IP Pool <pool-m2l-admin></pool-m2l-admin>	
Name: Pool-M2L-Admin	ОК
Addresses: 172.16.100.100-172.16.100 🖨	Cancel
Next Pool: none ∓ 🔺	Apply
	Comment
	Сору
	Remove

#### Ce qui donne :

IP Pool		
Pools Used Address	es	
4 - 2 7		Find
Name 🛆	Addresses	Next Pool 🔻
中 Pool-M2L-Admin	172.16.100.100-172.16.100.200	none
💠 Pool-M2L-Compta	172.16.121.100-172.16.121.200	none
+ Pool-M2L-Direction	172.16.120.100-172.16.120.200	none
3 items (1 selected)		

AP MikroTik

Rendez-vous dans le menu « IP => DHCP Server » et cliquez sur SIGNE PLUS (+). Choisissez l'interface « VLAN » correspondante et le pool d'adresse correspondant que nous avions créé puis faites « OK ».

DHCP Server < DHC	P-Pool-Admin>	×
General Queues	Script	ОК
Name:	DHCP-Pool-Admin	Cancel
Interface:	VLAN-Admin F	Apply
Relay:	▼	Disable
Lease Time:	00:30:00	Comment
Bootp Lease Time:	forever F	Сору
Address Pool: DHCP Option Set:	Pool-M2L-Admin	Remove
Server Address:	▼	
Delay Threshold:	▼	
Authoritative:	yes 두	
Bootp Support:	static <b>=</b>	
Client MAC Limit:	▼	
Use RADIUS:	no Ŧ	
	Always Broadcast	
	Add ARP For Leases	
	✓ Use Framed As Classless	
	Conflict Detection	
enabled		

Faire de même pour les autres interfaces, ce qui donnent :

DHCP S	Server								
DHCP	Networks	Leases	Options	Option Set	s Option Ma	atcher Ale	rts		
+ -	← ●          ✓ ★ □          Ţ         DHCP Config         DHCP Setup          Find								
Na	me	△ Interfa	ice	Relay	Lease T	me	Address Pool	Add ARP For Leases	-
DH	CP-Pool-Admir	n VLAN	-Admin			00:30:00	Pool-M2L-Admin	no	
DH	CP-Pool-Comp	ta VLAN	-Compta			00:30:00	Pool-M2L-Compta	no	
DH	CP-Pool-Direct	t VLAN	-Direction			00:30:00	Pool-M2L-Direction	no	
							-		
3 items	(1 selected)								

Ensuite rendez-vous dans le menu « **Networks** » cliquez sur **SIGNE PLUS (+)** et spécifiez les options réseau propre à chaque VLAN

AP MikroTik

DHCP Network <172.16.1			
Address: 172.1	6.100.0/24		ОК
Gateway: 172.1	6.100.1	\$	Cancel
Netmask: 24		•	Apply
No 🗌 No	DNS		
DNS Servers: 172.1	6.100.1	\$	Comment
Domain:		•	Сору
WINS Servers:		\$	Remove
NTP Servers:		\$	
CAPS Managers:		<b>÷</b>	
Next Server:		•	
Boot File Name:		•	
DHCP Options:		\$	
DHCP Option Set:		•	

### Ce qui donne :

DHCP Se	rver									×
DHCP	Networks	Leases	Options	Option Sets	Option Match	er Alerts				
+ -	Find									
Address		△ Gatew	ay	DNS Serv	vers Dor	ain	WINS Servers	Next Server	•	•
172.16.1	00.0/24	172.1	5.100.1	172.16.10	00.1					
172.16.1	20.0/24	172.1	5.120.1	172.16.12	20.1					
172.16.1	21.0/24	172.1	6.121.1	172.16.12	21.1					
3 items										

Allez maintenant dans le menu « IP => DNS ». La fenêtre Paramètres DNS apparaîtra. Mettez l'adresse IP DNS fournie par votre FAI ou l'adresse IP DNS publique de Google 8.8.8.8 dans le champ de saisie « Servers » et cliquez surtout sur « Allow Remote Requests ».

DNS Settings			
Servers:		<b>\$</b>	OK
Dynamic Servers:	10.190.0.11		Cancel
	10.190.0.1		Apply
Use DoH Server:		•	Static
	Allow Remote Requests		Cache
VRF:	main	∓	Adlist
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:	80 KiB		

AP MikroTik

Accédez au menu « IP => Pare-feu ». La fenêtre du pare-feu apparaîtra.

Cliquez sur l'onglet « **NAT** » puis cliquez sur **SIGNE PLUS (+)**. La nouvelle fenêtre de règle NAT apparaîtra. Dans l'onglet Général, choisissez « **srcnat** » dans le menu déroulant Chaîne et placez le bloc LAN (172.16.100.0 / 24) dans « **Src** ».

NAT Rule <172.16.100.0/24>	
General Advanced Extra Action	ОК
Chain: srcnat	Cancel
Src. Address: 172.16.100.0/24	Apply
Dst. Address:	Disable
Src. Address List:	Comment
Dst. Address List:	Сору
Protocol:	Remove
Src. Port:	React Countern
Dst. Port:	Reset Counters
Any. Port:	Reset All Counters
In. Interface:	
Out. Interface:	
In. Interface List:	
Out. Interface List:	
Packet Mark:	
Connection Mark:	
Routing Mark:	
Connection Type:	
enabled	

Cliquez sur l'onglet « Action » et choisissez « mascarade » dans le menu déroulant, puis cliquez sur le bouton « OK ».

NAT Rule <172.16.100.0/24>	
Advanced Extra Action Statistics	ОК
Action: masquerade	Cancel
	Apply
Log Prefix:	Disable
To Ports:	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters
enabled	

AP MikroTik

Faites de même pour les autres réseaux, ce qui donne :

Firewall									
Filter Rul	es NAT Ma	ingle Raw	Service Ports	Conn	ections /	Address Lists	Layer7 F	Protocols	
+ -	+ - V X C Reset Counters Conters Find all F							₹	
#	Action	Chain	Src. Address	[	)st. Addres	s Src. Ad	Dst. Ad	Proto	Src. Por 🔻
0	asquerade 🗧	e srcnat	172.16.100.0	/24					
1	🔚 masquerade	e srcnat	172.16.120.0	/24					
2	asquerade	e srcnat	172.16.121.0	/24					
•									•
3 items (1	selected)								

A ce stade, tous les appareils sans fils peuvent se connecter sur le SSID de leur service en fournissant le mot de passe correspondant.

¶77.	M2L Admin Connecté, sécurisé				
	<u>Propriétés</u>				
		Déconnecter			
₽//。	ITIC Paris				
₩.	M2L Compta				
₹77.	Maison des Ligues				
Carte	dministrateur:C:\WINDOWS\ réseau sans fil Wi	system32\cmd.exe -Fi :	-		ľ
Su De Ad DH Co Ad Ba Ba Ba Pa Se IA DU Se Ne	ffixe DNS propre à scription resse physique CP activé nfiguration automat resse IPv6 de liais resse IPv4 sque de sous-réseau il obtenu il expirant sserelle par défaut rveur DHCP ID DHCPv6 ID DHCPv6 tBIOS sur Tcpip.	la connexion : : ique activée : : on locale : : 65319 : 65319	Intel(R) Dual Band Wireless-AC 8260 E4-B3-18-83-24-AD Dui Dui 5880::6098:924f:5d9a:9ce7%3(préféré) 172.16.100.199(préféré) 255.255.255.0 mercredi 12 juin 2024 13:46:32 mercredi 12 juin 2024 13:01:32 172.16.100.1 172.16.100.1 704 -01-00-01-2D-73-46-3D-C8-5B-76-1D-A8 172.16.100.1 Activé	- 30	

Liens utiles :

https://wiki.mikrotik.com/wiki/Manual:TOC https://help.mikrotik.com/docs/display/ROS/RouterOS https://help.mikrotik.com/docs/display/ROS/VLANs+on+Wireless

Chéridanh TSIELA

AP MikroTik