

سیستم مدیریت مرکزی وایرلس ها CapsMan

مدیریت و پیکربندی تعداد زیادی Access Point کاری بس دشوار و زمانبر است مخصوصا زمانی که نیاز به اعمال تغییرات جزئی پس از پیکربندی اولیه رادیوها باشد، زیرا همیشه نیاز به اعمال تغییرات و ارتقای وضعیت رادیوها می باشد. در نتیجه یک سیستم مدیریت تغییرات Change Management ویژه ی رادیوها ضروری می باشد.

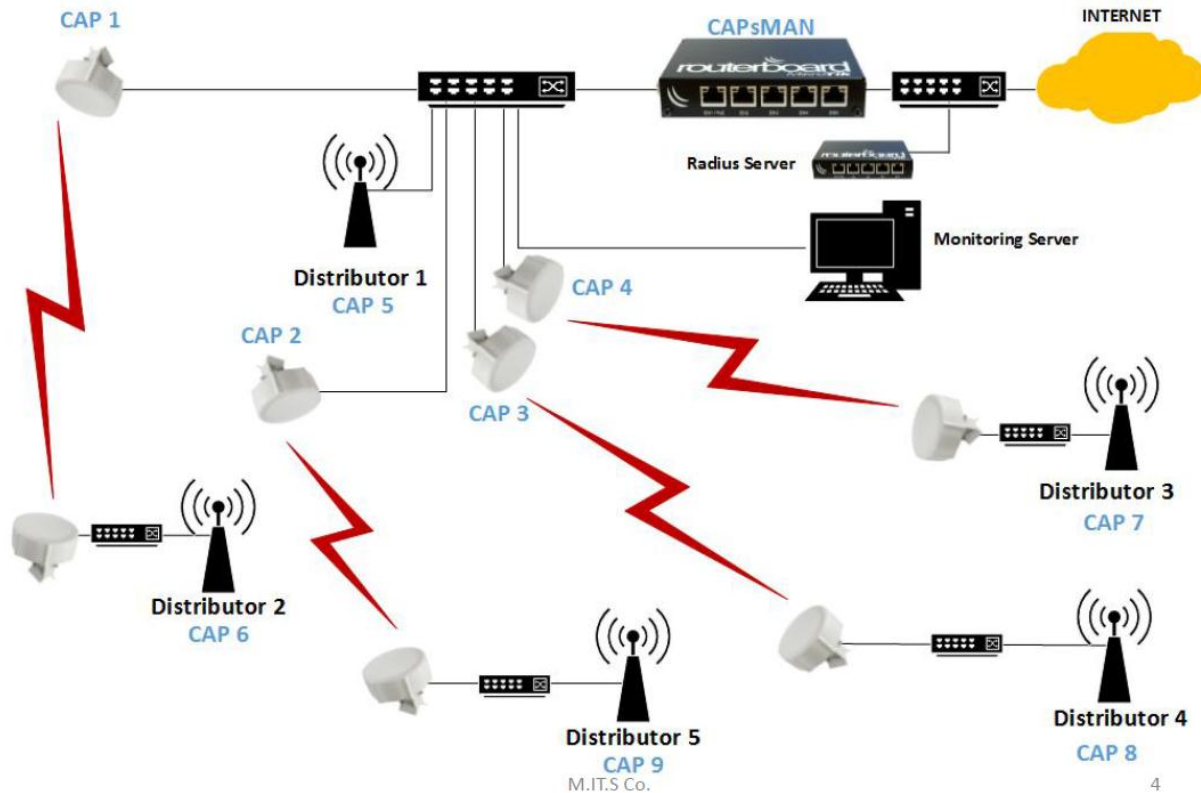
از آنجا که تجهیزات سخت افزاری شرکت میکروتیک نسبتا ارزان بوده و نیز کارایی قابل قبولی دارند لذا در شبکه های با اندازه کوچک و متوسط از آن ها بسیار استفاده می گردد. این شرکت بنا به نیاز عنوان شده در خصوص مدیریت رادیوها اقدام به ارائه سیستم مدیریت تغییرات به نام CapsMan نموده است. نسخه نخست آن بر روی پکیج های ۶,۱۱ به بعد قابل استفاده است و نیز نسخه ۲ آن از پکیج ۶,۲۲ به بعد قابل دسترسی است. همچنین حداقل لایسنس مورد نیاز برای سیستم عامل های روتر، سطح ۴ می باشد.

برای درک بهتر مطلب به شکل زیر توجه فرمایید:

در اینجا مشاهده می نمایید که یک روتربرد میکروتیک نقش CapsMan را بازی کرده و رادیوها به عنوان Cap ها بدان متصل می گردند تا زین پس تمامی تغییرات و حتی روتینگ اطلاعات و مسیر ارتباطات به صورت مرکزی و از طریق CapsMan انجام پذیرند.

پس می توان دریافت که علاوه بر مدیریت تغییرات، قابلیت مهم دیگری وجود دارد تا ضمن پردازش دیتای رادیوها و عبور ترافیک دریافتی توسط این رادیوها از یک نقطه مرکزی (CAPsMAN) امکان رومینگ اطلاعات را فراهم آورد. به بیان ساده تر با پیاده سازی چنین ساختاری امکان جابجایی و رومینگ اطلاعات کاربران بین رادیوهای مختلف فراهم می شود.

CAP to CAPsMAN Network Diagram



Cap (Controlled Access Point)

ارتباط سیستم مدیریت مرکزی CapsMan با رادیوها یا همان Cap ها به روش صورت می پذیرد:

۱- ارتباط مبتنی بر لایه ۲ و بر پایه Mac Address

۲- ارتباط مبتنی بر لایه ۳ و بر پایه IP Address

• جهت برقراری ارتباط مبتنی بر Mac نکات ذیل حایز اهمیت می باشند:

(۱) ضرورتی برای تنظیم IP بر روی Cap ها وجود ندارد.

(۲) CapsMan و Cap ها می بایست در یک بخش Segment یا به اصطلاح vLan قرار گیرند.

۳) ارتباط می تواند بر روی تونل لایه ۲ ای نیز باشد.

- جهت برقراری ارتباط مبتنی بر IP که از نوع UDP است، نکات ذیل قابل توجه است:

۱) ارتباط از پشت NAT نیز قابل برقراری است.

۲) آدرس IP ها باید یکدیگر را ببینند یا به قولی ping کنند.

۳) اگر در یک بخش یا segment نباشند، به شرط ارتباط بین IP ها مشکلی وجود ندارد.

مراحل اصلی پیاده سازی به صورت تیتروار:

۱- فعال سازی قابلیت CAPsMAN

۲- ساخت یک اینترفیس Bridge

۳- اختصاص آدرس IP به اینترفیس Bridge ساخته شده

۴- ایجاد یک تمپلیت برای پیکربندی رادیوهای شبکه

۵- تعریف مکانیزم تشخیص رادیوها

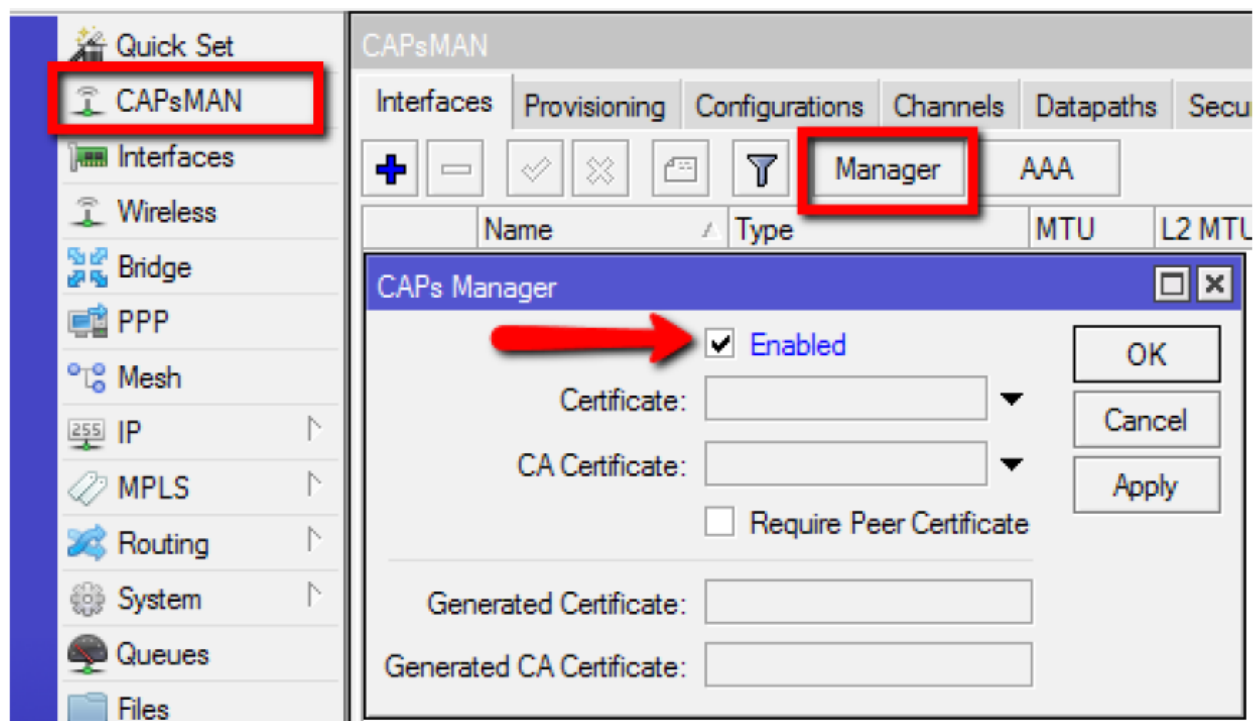
۶- فعال سازی قابلیت CAP بر روی رادیوها

مرحله اول:

ابتدا می بایست بسته ی نرم افزاری Wireless-fp را بر روی روتر CAPsMAN و رادیوهای Cap نصب کنید. پیشنهاد می شود از

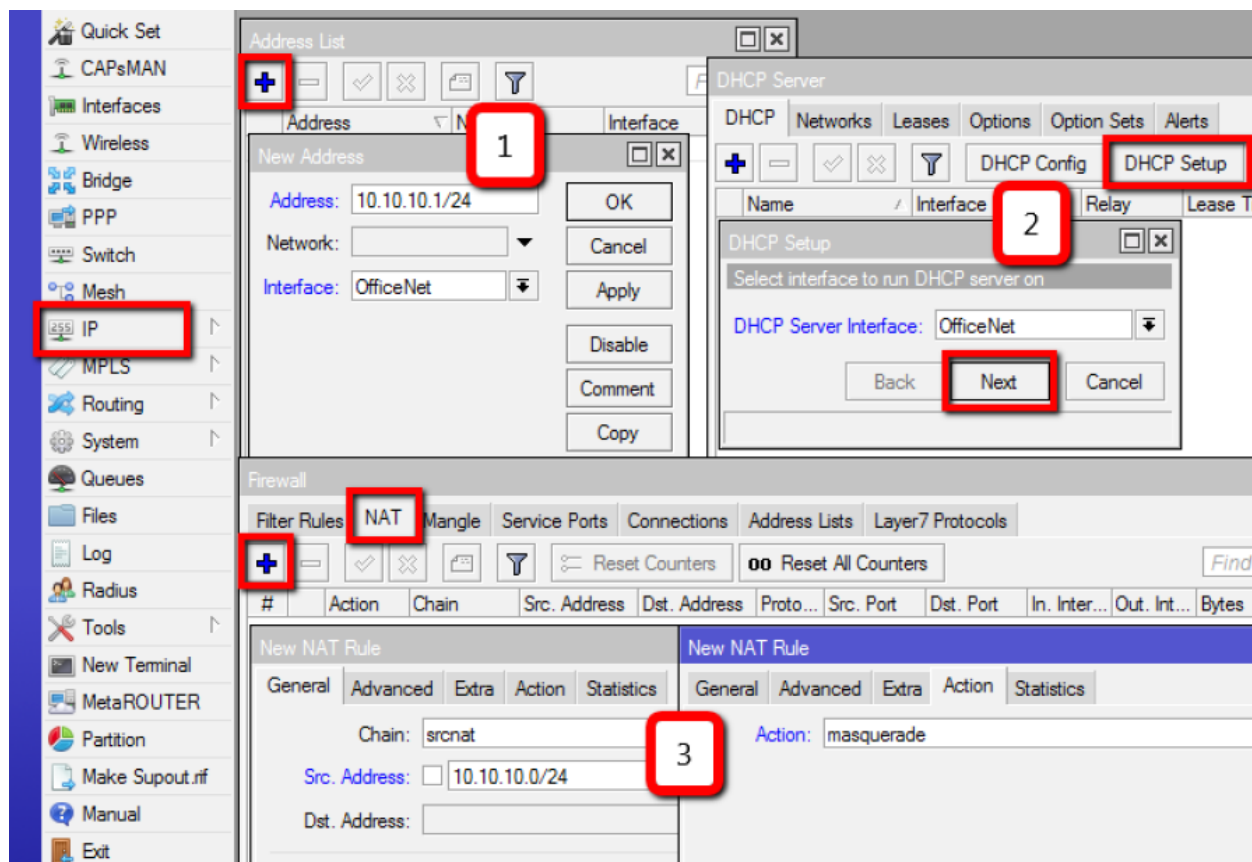
نسخه RouterOS کاملی که در سایت میکروتیک گذارده شده، استفاده نمایید.

سپس قابلیت CAPsMAN را روی روتر اصلی فعال می کنیم:



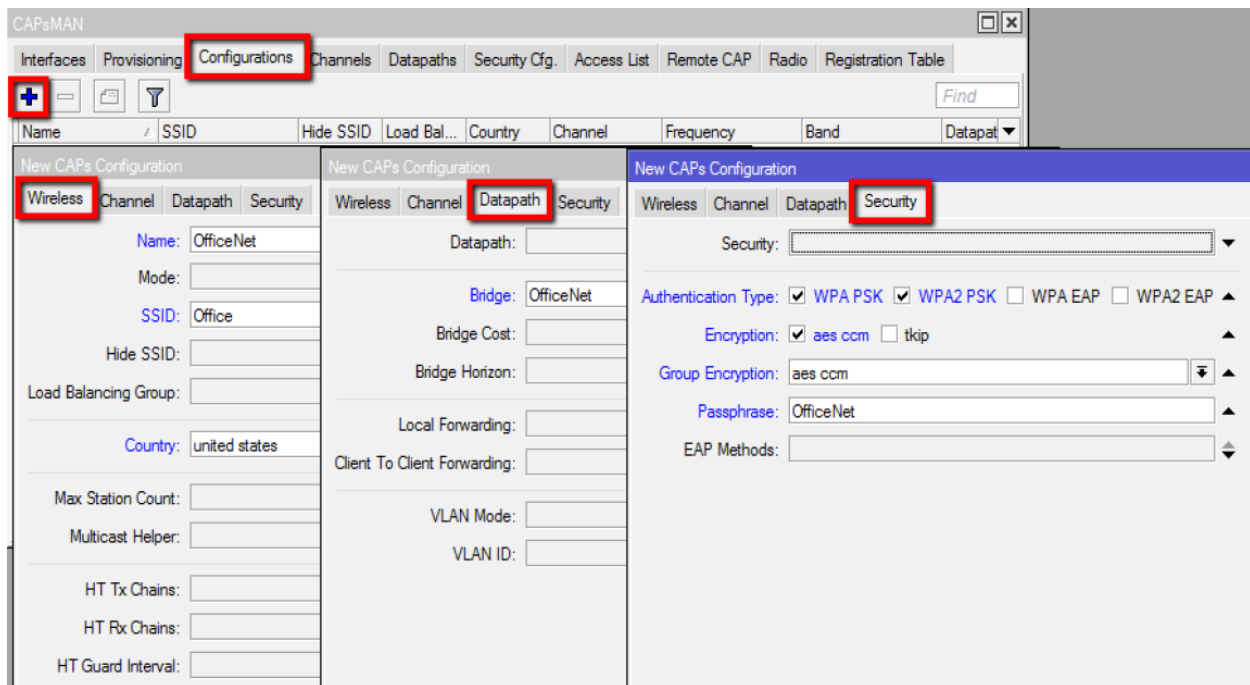
مرحله دوم:

حال می توانید تنظیمات عمومی مورد نظرتان را روی روتر اعمال نمایید. تنظیماتی از قبیل اختصاص آدرس IP، پیکربندی DHCP،
پیاده سازی NAT، ساخت Bridge و ...



مرحله سوم:

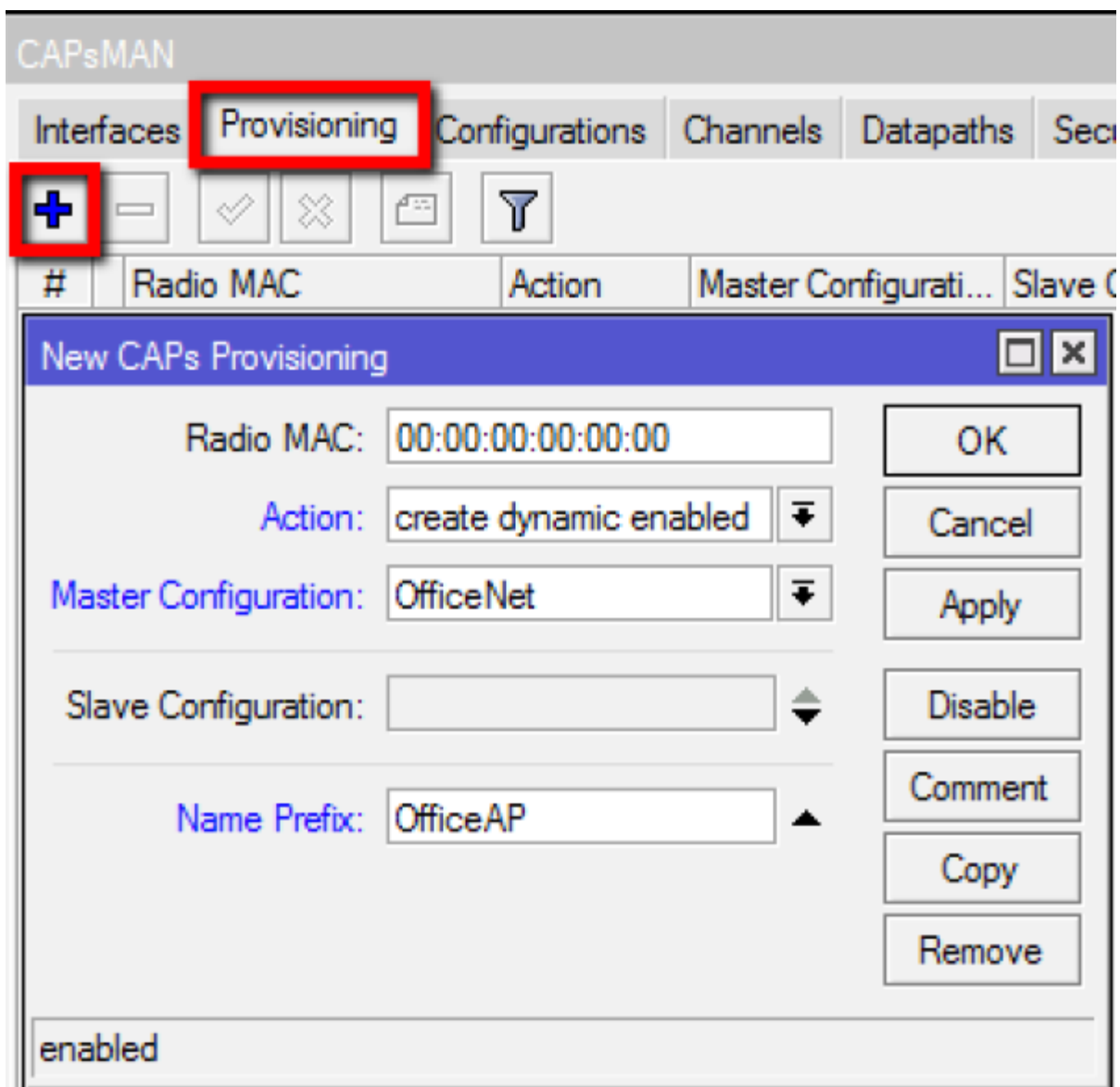
تنظیمات مورد نظری که می خواهید بر روی رادیوها اعمال کنید را انتخاب و تعریف نمایید.



مرحله چهارم:

حال که تنظیمات اولیه برای اعمال روی رادیوها انتخاب و تعریف شد، نوبت به شناسایی و ارتباط با رادیوها می رسد. مکانیزم ارتباط و تشخیص رادیوها از یکدیگر بر مبنای گواهی Certificate های صادر شده است ولی اگر این گواهی ها وجود نداشته باشد می توان از آدرس Mac رادیوها استفاده کرد و آن ها را به اینترفیس مورد نظر روتر برای اعمال تغییرات روی رادیوها اختصاص داد. زیرا روتر برای اعمال تنظیمات از دو اینترفیس Master و Slave استفاده می کند. همچنین چگونگی اعمال تغییرات روی رادیوها را به دو صورت Static یا Dynamic مشخص نمود.

به این مکانیزم ارتباط و تشخیص رادیوها در اصطلاح Provisioning می گویند که به دو صورت داینامیک و ایستا قابل تعریف است.



۱- Master Interface : تغییرات مورد نظر را بر روی رادیوهای فیزیکی اعمال می کند.

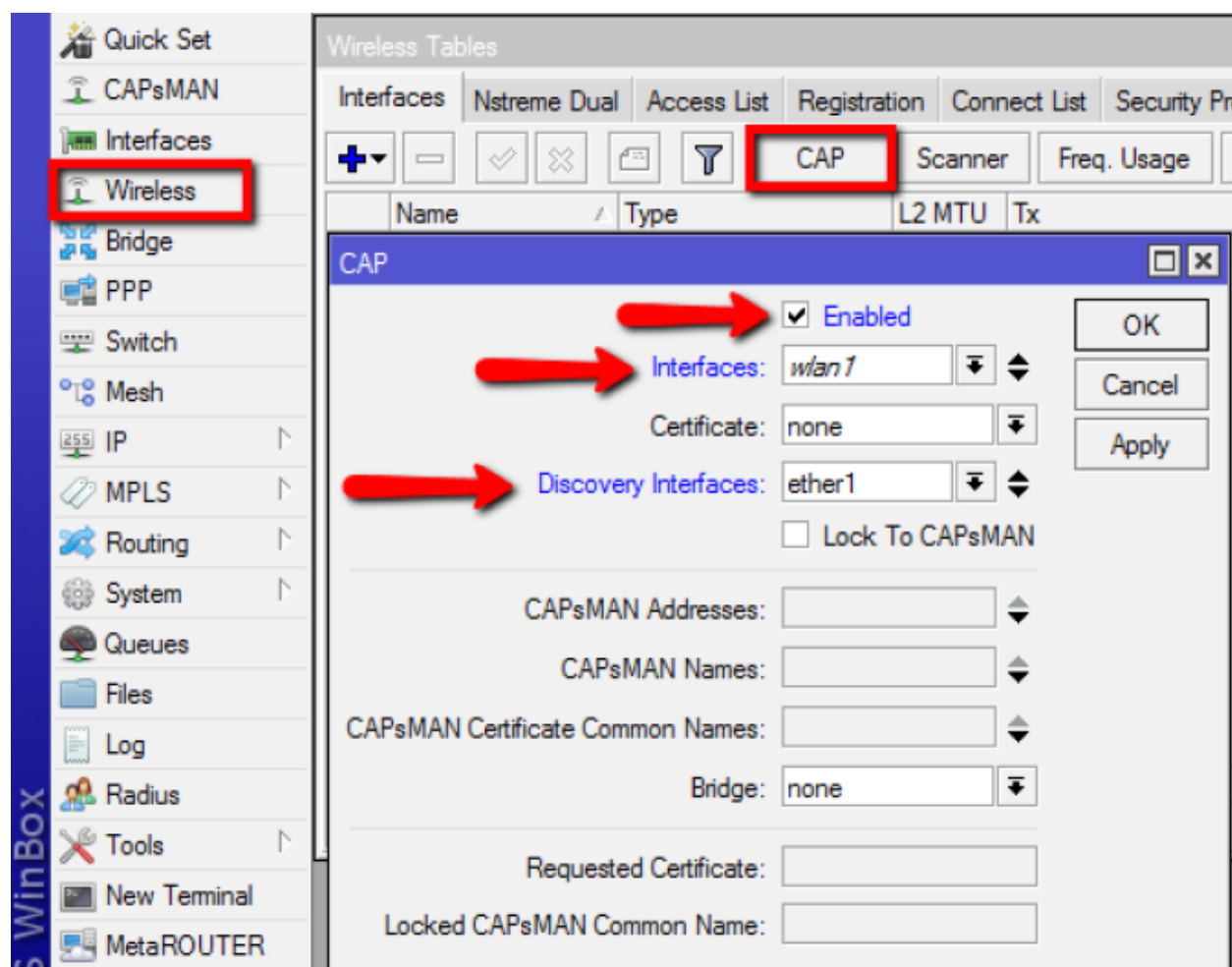
۲- Slave Interface : تغییرات را بر روی virtual AP اعمال می کند.

۳- Static : تنظیمات بر روی RouterOS رادیوی مورد نظر ذخیره و در فرایند Reboot اعمال می گردند.

۴- Dynamic : تا زمانی که رادیو با CAPsMAN در ارتباط است، اعمال می شود.

مرحله پنجم:

قابلیت CAP را روی رادیوها و خود CAPsMAN می توان فعال نمود.



همانطور که در شکل پیداست، می توان CAPsMAN را با استفاده از آدرس IP یا اسم شناسایی نمود و یا از متد broadcast از طریق یک اینترفیس تعریف شده، استفاده کرد.



Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles CAP Scanner Freq. Usage Alignmer

Name Type L2 MTU Tx Rx

CAP

☒ Enabled

Interfaces: wlan1

Certificate: none

Discovery Interfaces: ether1

☐ Lock To CAPsMAN

CAPsMAN Addresses:

CAPsMAN Names: CAPsMAN1

CAPsMAN Certificate Common Names:

Bridge: bridgeLocal

Requested Certificate:

Locked CAPsMAN Common Name:

OK Cancel Apply

مرحله ششم : Optional

بررسی وضعیت Cap و CAPsMAN

CAPsMAN

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security

Manager AAA

Name	Type	MTU	L2 MTU
DSMB	OfficeAP1	1500	1600

Interface <OfficeAP1>

General Wireless Channel Datapath Security Status Traffic

Current State: running-ap

Current Channel: 2427/20-Ce/gn(30dBm)

Current Rate Set: CCK:1-11 OFDM:6-54 BW:1x-2x HT:0-7

Current Basic Rate Set: OFDM:6 BW:1x HT:0-7

CAP

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security

CAP Scanner Freq. Usage

Name	Type	L2 MTU	Tx
--- managed by CAPsMAN			
--- channel: 2427/20-Ce/gn(30dBm), SSID: Office, CAPsMAN forwarding			
X wlan1	Wireless (Atheros AR9...	1600	

در سربرگ Radio اطلاعاتی در مورد رادیوهای register شده نمایش داده می شود. Radio MAC نشان دهنده خود رادیوهای فیزیکی است در صورتی که Remote CAP Name نشان دهنده رادیوهای فیزیکی یا مجازی می باشد.

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio

Provision

Radio MAC	Remote CAP Name	Remote CAP Id...	Interface
4C:5E:0C:6C:63:28	[4C:5E:0C:6C:63:28]	Room4	
P 4C:5E:0C:6C:63:2B	[4C:5E:0C:6C:63:2B]	Room3	OfficeAP1
P 4C:5E:0C:6C:63:4C	[4C:5E:0C:6C:63:4C]	Room1	OfficeAP2
P 4C:5E:0C:6C:63:3A	[4C:5E:0C:6C:63:3A]	Room2	OfficeAP3

برای مشاهده اطلاعات بیشتر در مورد رادیوهای متصل شده می توانید به سربرگ Remote CAP مراجعه کنید:

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio Registration Table

Provision

Address	Name	Board	Serial	Version	Identity	Base MAC	State	Radios
4C:5E:0C:6C:63:26	[4C:5E:0C:6C:63:28]	RBmAP2n	52760434DCE4	6.19	Room4	4C:5E:0C:6C:63:28	Run	1
4C:5E:0C:6C:63:29	[4C:5E:0C:6C:63:2B]	RBmAP2n	5276046C9DA3	6.19	Room3	4C:5E:0C:6C:63:2B	Run	1
4C:5E:0C:6C:63:38	[4C:5E:0C:6C:63:3A]	RBmAP2n	527604845E6A	6.19	Room2	4C:5E:0C:6C:63:3A	Run	1
4C:5E:0C:6C:63:4A	[4C:5E:0C:6C:63:4C]	RBmAP2n	527604D1D5D4	6.19	Room1	4C:5E:0C:6C:63:4C	Run	1
::ffff:10.5.125.172	[D4:CA:6D:A2:85:60]	RBmAP2n	527602095F22	6.19	Room5	D4:CA:6D:A2:85:60	Run	1

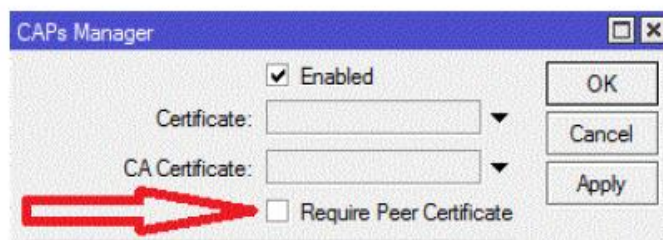
مرحله هفتم Optional :

برای دسترسی به CapsMan نیاز به احراز هویت داریم که به ۳ صورت زیر انجام پذیر می باشد:

۱- متد No Authentication که نیازی به احراز هویت ندارد.

۲- متد پیاده سازی احراز هویت تنها بر روی CapsMan

(require-peer-certificate=no on CAPsMAN)



۳- متد پیاده سازی احراز هویت بر روی Cap ها و CapsMan

(caps-man-certificate-common-names must specified on CAP)

(require-peer-certificate=yes on CAPsMAN)



13

حال می توان cap ها را مختص به یک CapsMan کرد یا به عبارتی بر روی آن قفل نمود که این کار با گزینه Lock to CAPsMAN قابل انجام است.

Cap های اضافه شده به لیست CAPsMan را می توان به عنوان یک اینترفیس مجازی بر روی کنسول مشاهده نمود.

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Rem

+ - ✓ ✗ [Icon] [Icon] Manager AAA

	Name	Type	MTU	L2 MTU	Tx
MI	cap1	Interfaces	1500	1600	0 bps
MI	cap2	Interfaces	1500		0 bps

Interface List

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

+ - ✓ ✗ [Icon] [Icon]

	Name	Type	L2 MTU	Tx	Rx
MI	cap1	Interfaces	1600	0 bps	
MI	cap2	Interfaces		0 bps	
R	ether1	Ethernet	1600	59.7 kbps	
	ether2	Ethernet	1598	0 bps	

مرحله هشتم:

در اینجا نوبت به انتخاب چگونگی انتقال اطلاعات می رسد به این منظور که دیتای دریافت شده توسط رادیوها از کاربران، از چه مسیری انتقال یابد. اگر از مد client to client Forwarding استفاده کنیم، دیتای دریافت شده توسط رادیوها اول به روتر CAPsMAN رفته سپس به مقصد ارسال می شود. ولی اگر از مد Local Forwarding استفاده کنیم، دیتا از خود رادیو یا همان CAP انتقال می یابد و CAPsMAN دیگر کنترلی روی اطلاعات ارسالی ندارد.

CAPs Datapath Configuration <datapath1>

Name:

Bridge: ▼ ▲

Bridge Cost: ▲

Bridge Horizon: ▲

Local Forwarding: ☐ ▲

Client To Client Forwarding: ☒ ▲

VLAN Mode: ▼

VLAN ID: ▼

OK

Cancel

Apply

Comment

Copy

Remove

مرحله نهم Optional :

اگر می خواهید CAP های متصل شده به CAPsMAN را به صورت استاتیک و دائمی درآورید، می توانید اطلاعات آن را توسط گزینه کپی و مطابق شکل زیر ثبت نمایید:

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio Registration Table

Find

Name	Type	MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	SSID	Hide SSID
DSMB	OfficeAP5	Interfaces	1500	1600	0 bps	0 bps	0	Office	

Interface <OfficeAP5>

General Wireless Channel Datapath Security Status Traffic

Name:

Type:

MTU:

L2 MTU:

MAC Address:

ARP: ▼

Radio MAC:

Master Interface: ▼

OK

Copy

Remove

Torch

New Interface

General Wireless Channel Datapath Security Status Traffic

Name:

Type:

MTU:

L2 MTU:

MAC Address:

ARP: ▼

Radio MAC:

Master Interface: ▼

OK

Cancel

Apply

Disable

Comment

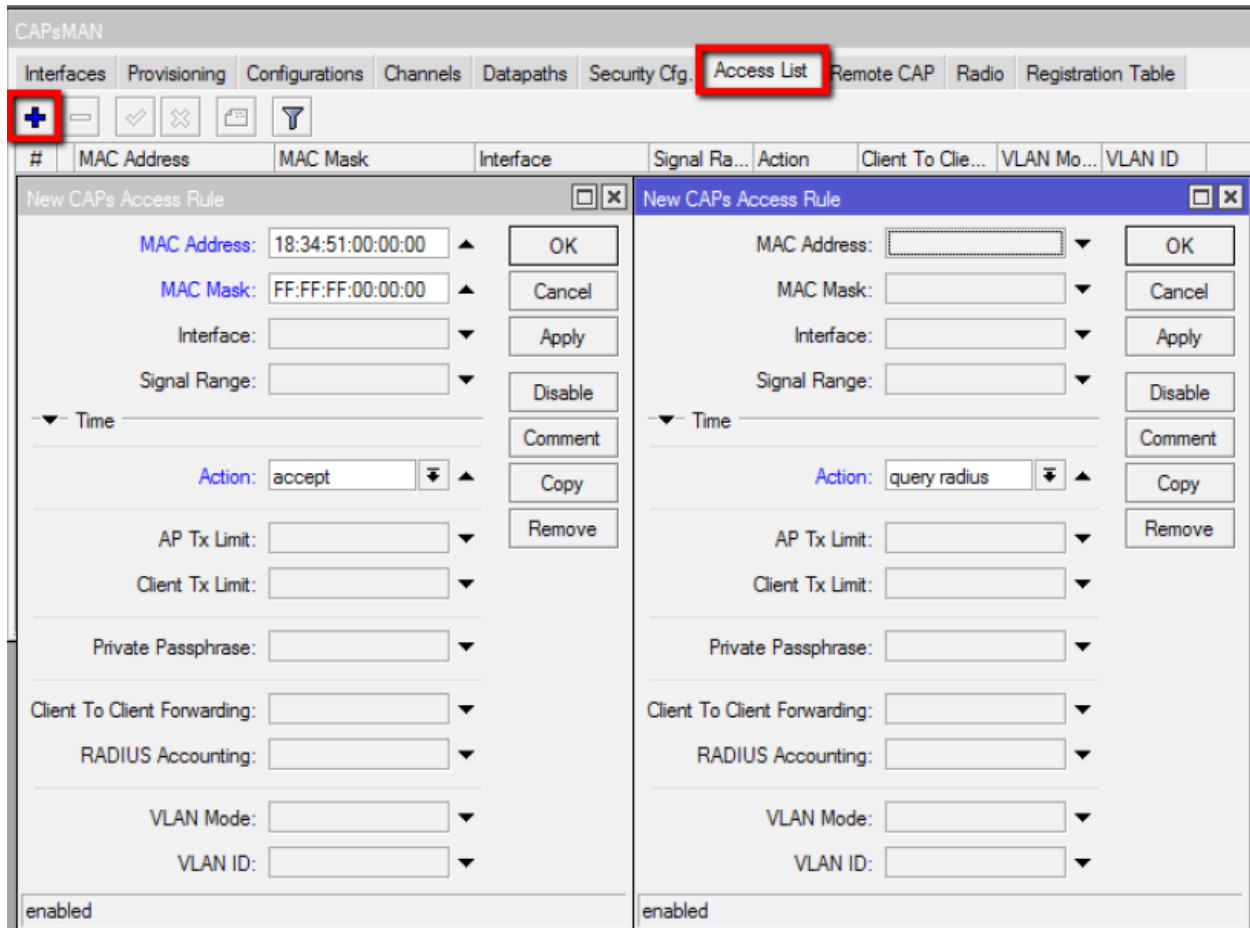
Copy

Remove

Torch

مرحله دهم Optional :

قابلیتی به نام Access List وجود دارد که امکاناتی از قبیل تعریف زمان، بازه ی سیگنال، احراز هویت با MAC، تعریف VLAN و نوع احراز هویت را در اختیار شما می گذارد تا مشخص نمایید چه تجهیزاتی قابل مدیریت و اتصال هستند.



اینترفیس های Cap ها می توانند با یکدیگر تشکیل یک گروه یا پروفایل دهند.

نکات:

برای داشتن ارتباطی امن بین Cap ها و CAPsMan می توان از IPSec یا Tunnel بهره برد.

نمونه تغییراتی که می توان بر روی Cap ها و از طریق CAPsMan انجام داد به قرار زیر می باشد:

۱- اطلاعات مربوط به کانال های رادیویی مانند تنظیمات فرکانس

۲- تعریف DataPath تا مشخص شود اطلاعات دریافتی از رادیوها می بایست از خود رادیو انتقال یابد یا اینکه ابتدا به

CAPsMan آمده و از آن جا route شود.

۳- تعریف Hotspot و تنظیمات مربوطه

۴- تنظیمات امنیتی مانند احراز هویت

۵- تنظیمات وایرلس مانند SSID

References :

Mikrotik.com

MITS-Co.com

Wiki.com