

The MikroTik logo is displayed in a stylized font. The word "Mikro" is in a regular weight, and "Tik" is in a bold weight. A small, curved line above the "i" in "Mikro" suggests motion or a signal. The logo is centered within a white rectangular area with rounded corners, which is part of a larger blue badge.

MTCRE

Mikrotik Certified Routing Engineer

Instagram.com/vaseghi.it
youtube.com/shahin vaseghi
github.com/shahinvaseghi

گردآورندگان : شاهین وانقی
ویراستار: علیرضا کهن ترابی

همانطور که میدانید روتر به تعداد پورت هایش بروادکست دامین دارد یعنی هر پورت آن در برادکست دامین یا رنج متفاوتی است پس نمیتوان به دو پورت در روتر آدرس همرنج داد؛ این قابلیت در روتر ها به ما توانایی مسیریابی را می دهد یعنی شبکه های مختلفی که به صورت لایه ۲ از هم مجزا هستند (برای مثال به سویچ های متفاوتی متصل اند یا در Vlan های مختلفی هستند) با استفاده از روتر به صورت مدیریت شده به هم متصل می شوند .

در روتر Forwarding method یا روشی که برای ارسال بسته ها تصمیم گیری می کند بر اساس Routing Table است . Routing Table به ۲ روش خودکار و دستی به اشکال مختلفی تکمیل می شود . برای مثال تنظیم یک آدرس بر روی هر کدام از پورت ها، باعث ایجاد یک Connected Route در جدول می شود و یا تنظیم یک DHCP Client میتواند بنا بر تنظیم شما باعث ایجاد یک Connected Route و یک Default Route شود . از طرفی پروتکل های مسیریابی نیز می توانند مسیر هایی را به جدول اضافه کنند. در آخر مسیر های دستی است که ادمین وارد می کند .

یکی از مهمترین وظایف لایه ۳ و تجهیزات لایه ۳ مثل روتر، مسیریابی یا Routing است . به طور کلی ۳ نوع مسیر در روتر وجود دارد :

۱. Connected Route : مسیرهای متصل، مسیر هایی هستند که خود روتر بر روی یکی از پورت هایش یک آدرس از آن رنج دارد، برای مثال اگر آدرس Ether 2 روتر ما 172.16.1.1/24 باشد در جدول مسیریابی روتر ما، یک مسیر به شکل زیر وجود دارد .

۲. Static Route : مسیری که ادمین به صورت دستی اضافه کرده است.

۳. Default Route : یک نوع مسیر که نقش Default Gateway را در روتر بازی می کند.

۴. Dynamic Route : انواع مسیری که به صورت خودکار در جدول ایجاد میشود مانند Connected Route ها یا مسیر هایی که پروتکل های مسیریابی ایجاد می کنند.

Address List			
Find			
Address	Network	Interface	
172.16.1.1/24	172.16.1.0	ether2	
192.168.1.1/24	192.168.1.0	ether1	
2 items			

Route List		
Find all		
Dst. Address	Gateway	
0.0.0.0/0	192.168.1.1	
172.16.1.0/24	bridge1	
192.168.1.0/24	ether1	
192.168.100.0/24	ether2	
4 items out of 11		

در جداول مسیریابی Flag ها نوع مسیر و روش ایجاد شدن این مسیر را به ما نشان میدهند. لیستی از Flag های جدول مسیریابی که مورد استفاده در میکروتیک است در زیر درج شده است:

	Dst. Address	Gateway
DAd	0.0.0.0/0	192.168.1.1
AS	172.16.1.0/24	192.168.1.1
DAC	192.168.1.0/24	ether1

۱. (X) disable: مسیر غیرفعال، این مسیر روی مسیرهای دیگر تاثیری ندارد.

۲. (A) active: مسیری که برای مسیریابی استفاده می شود.

۳. (D) dynamic: مسیرهایی که توسط برنامه ها و پروتکل ها ایجاد می شوند و قابل ویرایش نیستند.

۴. (C) connect: مسیرهای متصل، مسیرهایی که جهت کل رنج یک آدرس تنظیم شده بر روی یک پورت میباشد.

۵. (S) static: مسیرهایی که به صورت دستی توسط ادمین ایجاد شده اند.

۶. (r) rip: مسیر هایی که پروتکل rip ایجاد کرده است.

۷. (b) bgp: مسیر هایی که پروتکل bgp ایجاد کرده است.

۸. (o) ospf: مسیر هایی که پروتکل ospf ایجاد کرده است.

۹. (m) mme: مسیر هایی که پروتکل mme ایجاد کرده است.

۱۰. (B) blackhole: بسته های ارسال شده توسط این مسیر بی صدا از بین می روند.

۱۱. (U) unreachable: بسته های ارسال شده توسط این مسیر از بین می روند و به فرستنده

یک پیام ICMP Host Unreachable ارسال می شود

۱۲. (P) porhabit: بسته های ارسال شده توسط این مسیر از بین می روند و برای فرستنده یک

پیام ICMP communication administratively prohibited ارسال می شود

disabled (X)

active (A)

dynamic (D)

connect (C)

static (S)

rip (r)

bgp (b)

ospf (o)

mme (m)

blackhole (B)

unreachable (U)

prohibit (P)

هر بسته ای که به دست روتر می رسد به ترتیب بر اساس ترتیبی که روتر ایجاد میکند جدول مسیریابی را طی میکند تا با یکی از مسیرها منطبق شود و ارسال انجام شود.

انتخاب ترتیب و بهترین مسیر توسط جدول روتینگ بر اساس ۲ شرط انجام می شود.

۱. **Longest Prefix** : از نظر روتر، ترتیب بررسی مسیرها بر اساس Subnet mask شبکه های مقصد یا Prefix آنها انجام می شود. هرچه سابنت بزرگتر باشد، روتر این مسیر را زودتر بررسی میکند. یعنی برای مثال، مسیر 192.168.1.0/30 زودتر از مسیر 192.168.2.0/24 بررسی می شود چون Prefix بزرگتری دارد.

۲. **Distance** : فاصله اولویت بندی بین دو مسیر برای یک مقصد است؛ Distance مقداری بین ۰ تا ۲۵۵ است. تمامی مسیرهای Connected دارای فاصله ۰ هستند، Distance در مسیرهای دستی بین ۱ تا ۲۵۵ می باشد. مسیرهایی که توسط پروتکل های مسیریابی ایجاد شوند همگی دارای Distance یکسان می باشند.

برای ایجاد static route باید موارد زیر را تنظیم کنید:

Dst.Address : آدرس سیستم یا شبکه مقصد

Gateway : آدرس روتری که از طریق آن می توانیم به شبکه مقصد دسترسی پیدا کنیم که آدرس پورت متصل به ما در روتر بعدی یا Next Hop است

Check Gateway : با فعال کردن این گزینه و قرار دادن آن روی حالت Ping روتر به صورت مداوم Ping آدرس Gateway این مسیر را میگیرد و در صورت عدم دریافت جواب، این مسیر را غیر فعال می کند.

Distance : فاصله یا اولویت بین مسیر هایی که برای مقصد های یکسان است

Routing Table : جدول مسیریابی این مسیر

Pref. Source : برای فعال کردن این گزینه، باید یکی از آدرس های روتر را در اینجا بنویسید تا آدرس فرستنده این بسته ها یا همان Src.IP بسته هایی که با این مسیر ارسال می شوند با این آدرس عوض شود. (چیزی شبیه به NAT)

Scope: 30 ▲

Target Scope: 10 ▲

Scope	Route type	Target Scope
0		
10	Connected (running)	10
20	OSPF, RIP, MME	10
30	Static	10
40	eBGP	10
40	iBGP	30
200	Connected (not active)	

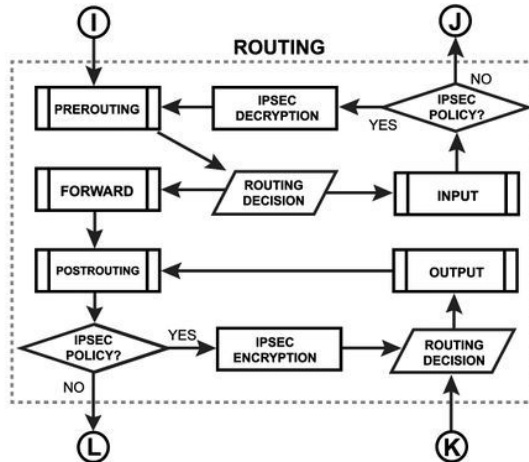
دو مفهوم دیگر در مسیرهای میکروتیک Scope و Target Scope هستند .

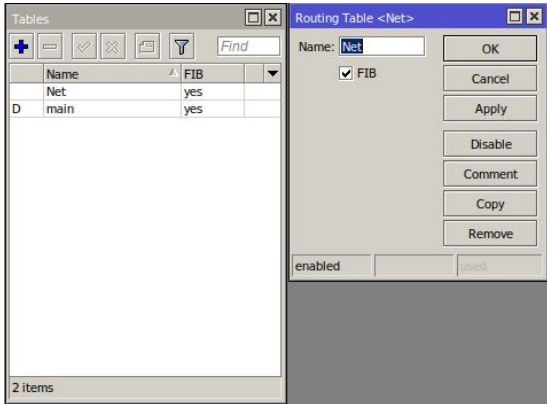
هر نوع مسیر در میکروتیک Scope خاص خود را دارد که در لیست روبرو مشاهده میکنید .
 Scope ها به طور مستقیم برای ما موثر نیستند بلکه Target Scope است که برای ما مهم است.
 Target Scope مسیرهایی هستند که روتر برای پیدا کردن Gateway یک مسیر بررسی می کند . ما از این کار برای نوشتن مسیر با Gateway از شبکه هایی که به ما متصل نیست استفاده می کنیم.

با استفاده از Routing Mark میتوانیم تعیین کنیم چه افرادی از این مسیر استفاده کنند . برای استفاده از این قابلیت باید ابتدا بسته ها از طریق IP > Firewall < Mangle برچسب گذاری بشن و بعد از طریق این گزینه این برچسب ها خوانده شود.

برچسب گذاری که توسط Mangle صورت میگیرد در Chain prerouting انجام می شود.

در Packet Flow میکروتیک در باکس Routing اولین مرحله فرایند prerouting می باشد.





برای استفاده از قابلیت Route Mark ابتدا باید یک جدول مسیریابی یا Routing Table تشکیل دهید تا بسته های برچسب دار مسیرهای متفاوتی در جدول های متفاوتی از جدول اصلی داشته باشند
برای این کار به منو Routing > Tables بروید. برای ایجاد منو جدید کافی است یک اسم انتخاب کنید و گزینه FIB را تیک بزنید.

برای برچسب زدن به بسته ها به منو IP > Firewall > Mangle رجوع کنید .

یک Mangle با Chain : prerouting ایجاد کنید . می توانید بسته هایی که مایل هستید از این جدول استفاده کنند را به روش های مختلفی انتخاب کنید .

۱. Src. Address : توسط آدرس مبدا، مانند وقتی که قصد دارید به افرادی خاص یا یک سرور اینترنت خاص بدهید.

۲. Dst. Address : توسط آدرس مقصد، مانند وقتی که میخواهید تمامی ترافیک یک آدرس خاص از یک پورت اختصاصی ارسال شود.

۳. Src. Address List : آدرس مبدا عضو یک لیست خاص باشد. مانند وقتی که قصد دارید به گروهی از آدرس ها یک اینترنت خاص بدهید

۴. Dst. Address List : آدرس مقصد عضو یک آدرس لیست خاص باشد. مانند وقتی که قصد دارید تمامی ترافیک هایی که به سمت سرورها می روند از مسیر خاصی استفاده کنند.

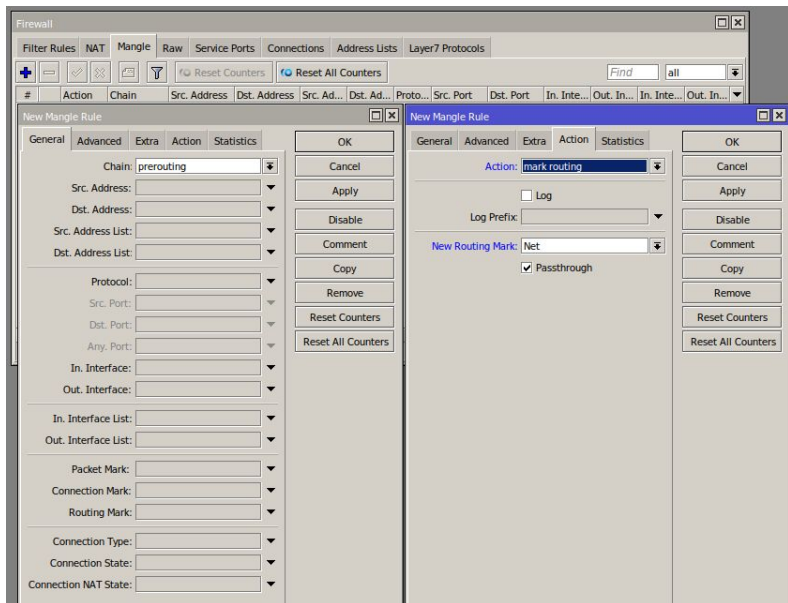
۵. Protocol : پروتکل محتویات بسته ۶. Src.Port : فیلد پورت فرستنده در هدر لایه ۴ بسته ۷. Dst.Port : فیلد پورت گیرنده در هدر لایه ۴ بسته

۸. Any.Port : مقدار این قسمت برای هر دو فیلد فرستنده و گیرنده چک می شود.
۹. In.Interface : پورت ورودی

۱۰. Out.Interface : پورت خروجی ۱۱. In.Interface List : لیست پورت های ورودی

۱۲. Out.Interface List : لیست پورت های خروجی ۱۳. PacketMark : برچسب بسته ۱۴. Connection Mark : برچسب ارتباط

۱۵. Routing Mark : برچسب مسیر ۱۶. Routing Table : جدول مسیریابی



در بخش Mangle، در قسمت Action، گزینه mark routing را انتخاب کنید و جدول مورد نظرتان را انتخاب کنید.
حالا می توانید Route ها را در جدول های مختلف ایجاد کنید و بسته ها برای مقاصد مشابه مسیر های متفاوتی داشته باشند.

The image shows two side-by-side screenshots of the 'New Address' dialog box in Mikrotik WinBox. Both dialogs have a title bar with a close button. The left dialog has a blue title bar and contains the following fields: 'Address' with the value '192.168.1.1/32', 'Network' with the value '172.16.1.1', and 'Interface' with the value 'ether1'. Below these fields are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. At the bottom left is a checkbox labeled 'enabled'. The right dialog has a grey title bar and contains the following fields: 'Address' with the value '172.16.1.1/32', 'Network' with the value '192.168.1.1', and 'Interface' with the value 'ether1'. Below these fields are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. At the bottom left is a checkbox labeled 'enabled'.

برای استفاده از Point-to-Point Addressing کافی است به روش زیر عمل کنید:

آدرس روتر اول را در **Address** وارد کنید و **Prefix /32** بدهید. به عنوان **Network** آدرس روتر مقابل را وارد کنید ؛ اینکار باعث می شود که **Gateway** آین آدرس تعیین شود.

و دقیقا در روتر روبرو برعکس اینکار را انجام دهید . با انجام این کار تعداد بسیار کمتری آدرس استفاده می کنید .

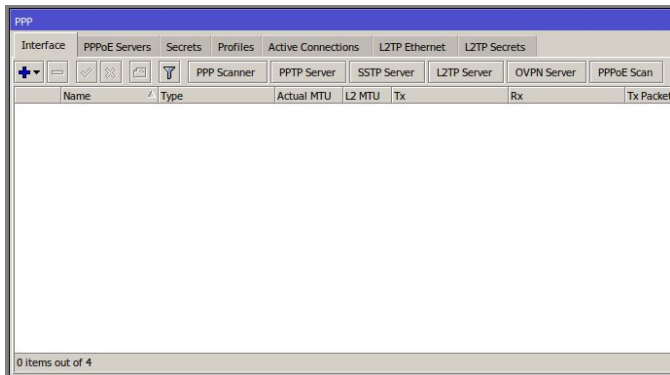
Site To Site (Router to Router)	Client to Site (Endpoint to Router)
1- Tunneling IPsec GRE 4/6 EoIP VxLAN IPsec	VPN PPTP L2TP SSTP OpenVPN WireGuard
2- VPN PPTP L2TP SSTP OpenVPN WireGuard	

برای ارتباط از راه دور در روتر ها ۲ روش Tunneling و VPN وجود دارد. از تانل ها برای ارتباط بین روتر ها استفاده می کنیم و از VPN ها برای ارتباط کاربران با شبکه . هنگام استفاده از تانل، روتر ها باید در هر دو سمت آدرس ثابت داشته باشند و قادر باشند Ping یکدیگر را بگیرند.

هنگام استفاده از VPN ها تنها کافی است یکی از طرفین که نقش Server را ایفا می کند آدرس ثابت داشته باشد . تنظیمات مربوط به VPN ها در منو PPP قرار دارد و تنظیمات مربوط به تانل ها در منو Interface

۱. VPN : برای راه اندازی وی پی ان باید یکی از پروتکل های موجود را انتخاب و آن را تنظیم کنید اما ابتدا چند اقدام است که بین تمامی آنها مشترک است .

۱.۱ IP > Pool : با استفاده از این منو باید یک ظرف آدرس برای کاربرانی که متصل میشوند ایجاد کنید .



۱.۲ PPP > Profile : ایجاد یک پروفایل:

Name : اسم این پروفایل

Local Address : آدرسی که روتر بر روی اینترفیس VPN خود قرار می دهد که میتواند تک آدرس باشد یا یک Pool IP

Remote Address : آدرسی است که به کاربر می دهیم؛ این آدرس می تواند یک آدرس باشد یا یک Pool IP

DNS Server : آدرس DNS Server برای کاربرها

در تب Protocol گزینه Use Encryption را فعال کنید.

در قسمت limit میتوانید بر روی ارتباطاتی که از طریق این پروفایل متصل شده اند محدودیت قرار دهید :

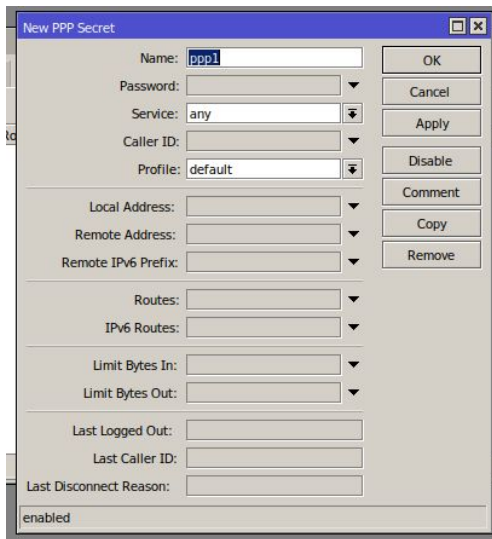
Only One : در آن واحد، تنها یک کاربر از طریق این پروفایل می تواند متصل شود

Session Timeout : بعد از مدت زمان مشخص از وصل شدن قطع شود :

Idle Timeout : بعد از یک مدت مشخص که ارسال و دریافت نداشت قطع شود :

Rate Limit : محدودیت حجمی که به صورت آپلود / دانلود مشخص می شود برای مثل :

«10G/5G : 10G Download / 5G Upload»



برای ایجاد بوزرنیم و پسورد برای کاربر های VPN به منو PPP > Secret مراجعه کنید و یک سکرت جدید ایجاد کنید .

Name : همان Username کاربر می باشد **Password :** رمز کاربر

Service : پروتکل هایی که با رمز کاربر میتوان به آنها متصل شد

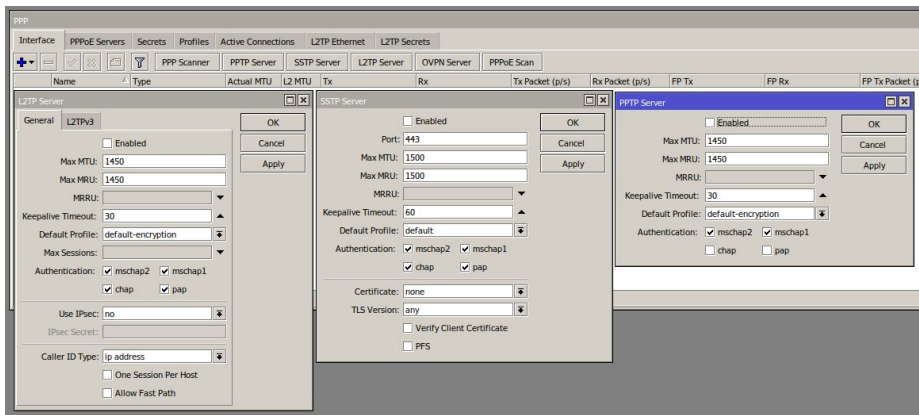
Caller ID : آدرس دستگاه هایی که کاربر فقط می تواند با آن به سرور متصل شود. در کانکشن های PPPoE میتوانید در این قسمت مک آدرس وارد کنید.

Profile : پروفایلی که رمز کاربر به آن متصل می شود و کاربرانی که با این رمز به سرور متصل شوند از آن پروفایل آدرس دریافت می کنند .

Limit Byte In / Out : محدودیت حجم برای آپلود و دانلود

توجه کنید آدرس هایی که در **Secret** وارد می شوند نسبت به آدرس های **Profile** اولویت دارند

در قسمت **Routes** میتوانید یک روت به محض اتصال این یوزر در جدول مسیریابی ایجاد کنید



برای راه اندازی VPN Server در میکروتیک در **PPP > Interface** پروتکل مورد نظر را فعال می کنیم .

بهتر است برای امنیت، الگوریتم های **pap** و **chap** را غیر فعال کنیم .

در **L2tp** میتوانید **IPSec** را نیز فعال کنید.

SSTP بین دو دستگاه میکروتیک نیازی به سرتفیکیت ندارد اما اگر کاربر غیر میکروتیکی باشد به سرتفیکیت نیاز دارد.

کاربرانی که به **VPN Server** متصل شده اند را میتوانید از طریق تب **Active Connection** مشاهده کنید .

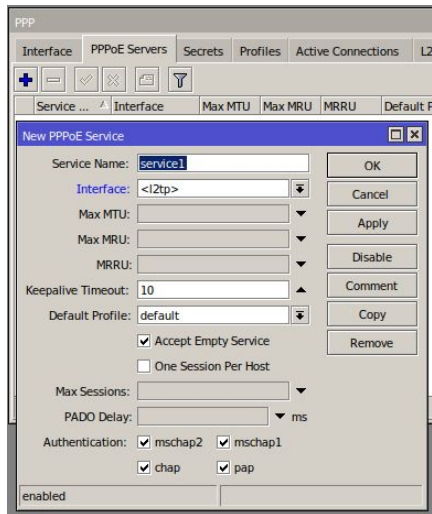
VPN هایی که در بالا مشاهده کردیم از نوع لایه ۳ ای هستند میکروتیک از VPN لایه ۲ ای نیز تحت پروتکل PPPoE پشتیبانی می کند.

برای راه اندازی PPPoE سرور به منو PPP > PPPoE Server بروید و یک گزینه اد کنید :
Service Name : اسم سرور Interface : پورت مورد نظری که سرویس را روی آن ارائه کنیم

برای ایجاد VPN Client در میکروتیک به Interface بروید و بر روی Add کلیک و پروتکل دلخواه را انتخاب کنید .

در PPPoE Client ابتدا در General پورتهای که سرویس را از آن دریافت می کنید انتخاب کنید سپس در Dial Out یوزرنیم و پسورد را انتخاب کنید

در بقیه پروتکل ها کافی است که در Dial Out آدرس سرور و یوزرنیم و پسورد را وارد کنید .
توجه داشته باشید که در پروتکل L2tp ممکن است لازم باشد IPSec را نیز وارد کنید.



برای راه اندازی PPPoE Client ابتدا باید در تب General پورت یا Interface ی که از طریق آن به سرور متصل هستید را انتخاب کنید.

سپس در تب Dial Out در قسمت Connect To آدرس VPN Server را وارد کنید .

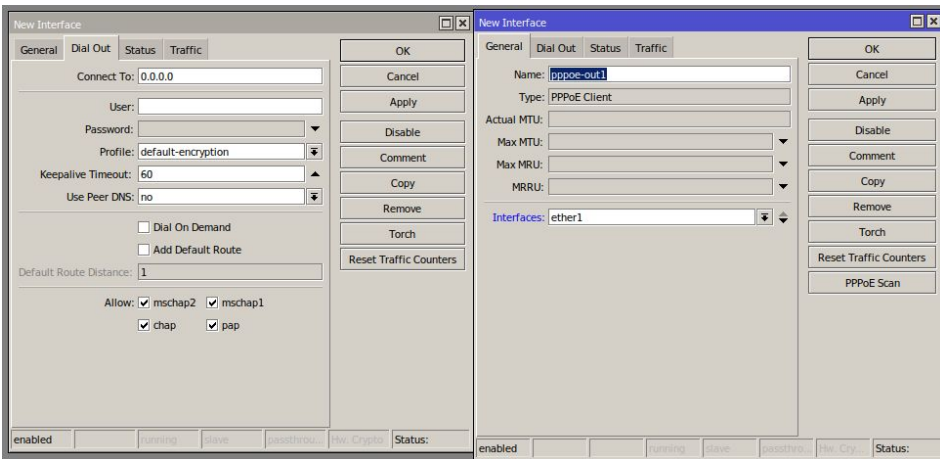
User : در این قسمت Username را وارد میکنید

Password : رمز را وارد کنید.

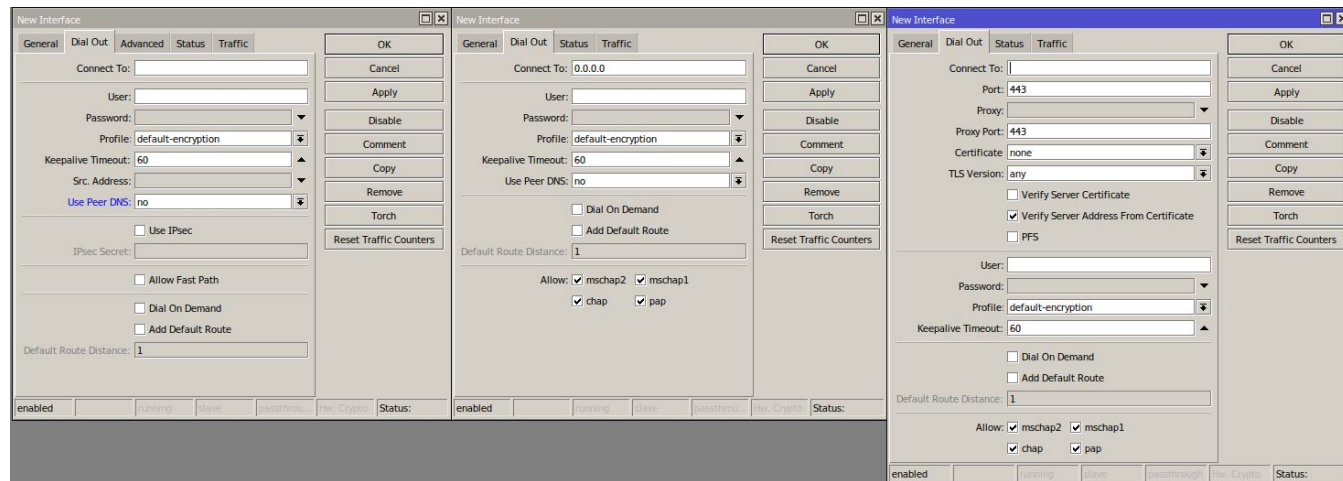
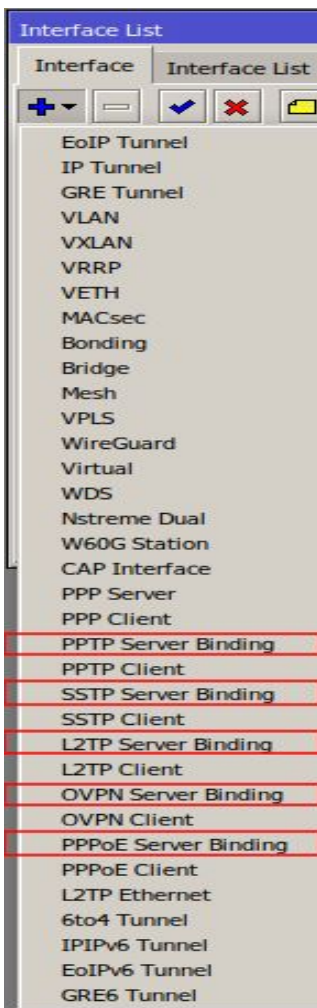
Add Default Route : با انتخاب این گزینه بعد از اتصال به سرور یک Default Route

به سمت سرور در جدول ایجاد می شود

قسمت Allow رمزنگاری بسته های ارسال شده توسط VPN انتخاب می شود که باید گزینه های mschap1 و mschap2 را انتخاب کنید زیرا الگوریتم های Chap و Pap شکسته شده اند



برای اینکه اینترفیس سرور های VPN با هر بار قطع و وصل شدن کاربر از بین نرود و همیشه وجود داشته باشد باید از گزینه های Server Binding در Interface یا PPP استفاده کنید.



برای راه اندازی VPN Client باید در تب Dial Out در قسمت Connect To آدرس VPN Server را وارد کنید .

User : در این قسمت Username را وارد میکنید

Password : رمز را وارد کنید.

Add Default Route : با انتخاب این گزینه بعد از اتصال به سرور یک Default Route به سمت سرور در جدول ایجاد می شود

در PPTP و SSTP قسمت Allow رمزنگاری بسته های ارسال شده توسط VPN انتخاب می شود که باید گزینه های mschap1 و

mschap2 را انتخاب کنید زیرا الگوریتم های Chap و Pap شکسته شده اند

در L2tp Client در صورتی که سرور از IPsec استفاده کند با فعال کردن گزینه Use IPsec رمز را وارد کنید.

برای راه اندازی تانل های مختلف ۲ مورد در تمامی آنها مشترک است؛ **Local Address** آدرس روتری است که در حال راه اندازی تانل در آن هستید و **Remote Address** که آدرس روتر روبرو است. توجه داشته باشید که تانل ها مانند VPN خودشان فرایند آدرس دهی را انجام نمی دهند بلکه باید خودتان بر روی **Interface** ها آدرس دهی انجام دهید.

توجه داشته باشید که تانل های **IPIP** و **GRE** از نوع لایه ۳ هستند اما پروتکل **EoIP** که انحصاری میکروتیک است به صورت لایه ۲ ای کار می کند.

مهمترین تفاوت **ipip** و **GRE** در **MTU** آنها است. $GRE\ MTU = 1476$ $IPIP\ MTU = 1480$ توجه داشته باشید که پروتکل **IPSEC** به دلیل رمزنگاری، ۵۰ واحد از **MTU** هر پروتکلی که به آن اضافه شود کم میکنند.

برای راه اندازی **IPSec** باید حتما گزینه **Allow Fast Path** را غیرفعال کنید.

برای راه اندازی **EoIP** باید در هر دو سمت **Tunnel ID** یکسان تنظیم کنید.

برای راه اندازی تانل ها در میکروتیک ابتدا باید یک پروتکل انتخاب کنید؛ در **Interface** منو های مختلفی برای پروتکل های مختلف وجود دارد. پروتکل های موجود در میکروتیک **GRE - ipip** و **EoIP** ... هستند.

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VXLAN	VRPP	VETH	MACSec	Bonding	LTE	VRF
R	bridge1 - Access	Bridge											
R	ether1	Ethernet											
R	ether2	Ethernet											
R	ether3	Ethernet											
S	vlan10	VLAN											
S	ether4	Ethernet											

Bridge

#	Interface	Bridge	Horizon	Trusted	Priority (h...)	Path Cost	PVID	Role	Root Pat...
0	ether4	bridge1 - Access Vlan10	no		80	10	1	disabled port	
1	vlan10	bridge1 - Access Vlan10	no		80	10	1	disabled port	

Bridge Port <ether4>

General STP VLAN Status

Interface: ether4

Bridge: bridge1 - Access Vlan10

Horizon:

Learn: auto

☒ Unknown Unicast Flood

☒ Unknown Multicast Flood

enabled inactive Hw. Offload

Bridge Port <vlan10>

General STP VLAN Status

Interface: vlan10

Bridge: bridge1 - Access Vlan10

Horizon:

Learn: auto

☒ Unknown Unicast Flood

☒ Unknown Multicast Flood

enabled inactive Hw. Offload

Interface <vlan10>

General Loop Protect Status Traffic

Name: Vlan10

Type: VLAN

MTU: 1500

Actual MTU: 1500

L2 MTU: 1594

MAC Address: 18:FD:74:0E:5D:04

ARP: enabled

ARP Timeout:

VLAN ID: 10

Interface: ether3

☐ Use Service Tag

enabled running slave passthrough

در فرایند Vlaning، در لایه ۲ پورت ها در ۲ وضعیت قرار دارند
۱. Access: یک پورت را عضو یک VLAN می کند ولی تغییری در بسته ایجاد نمیکند. تنها تغییرات در جداول مک آدرس ایجاد می شوند

۲. Trunk: این پورت می تواند ترافیک چند VLAN را همزمان جابجا کند که این کار را از طریق برچسب زدن به بسته ها انجام می دهد .

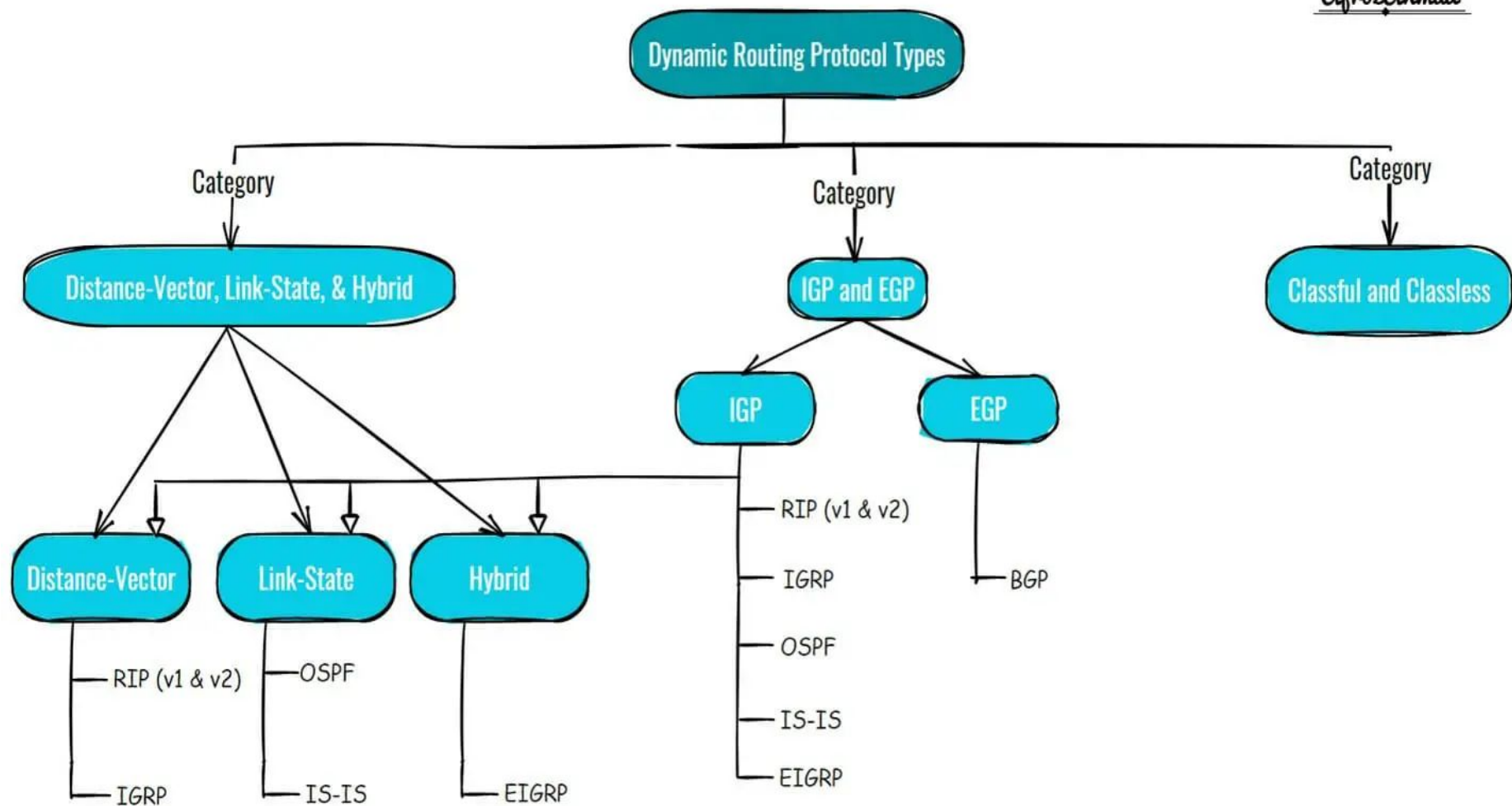
به بسته ها برچسب Dot1Q زده میشود و هر پورتی که قرار است این بسته ها را دریافت کند باید تنظیمات برچسب هایی مشابه با سمت مقابل داشته باشد .

VLAN ها با شماره ای بین ۱ تا ۴۰۹۴ مشخص می شوند و مهمترین قسمت برچسب Dot1Q همین شماره است .

پورت های میکروتیک در وضعیت Trunk قرار دارند، برای اینکه یک VLAN را بر روی یک پورت تنظیم کنیم، در منو Interface VLAN یک گزینه اضافه کنید .

مهمترین قسمت این پنجره ۱. VLAN ID : شماره VLAN یا همان شماره برچسب Dot1q است. ۲. Interface: اینترفیسی که کابل ترانک به آن متصل است یا به هر صورت دیگری بسته های VLAN را دریافت می کند

برای اینکه یکی از پورت های میکروتیک را تبدیل به Access یکی از VLAN هایی بکنیم که از پورت دیگری دریافت کرده اید باید Interface آن VLAN را با آن پورتی که میخواهید Access کنید در یک Bridge قرار دهید.

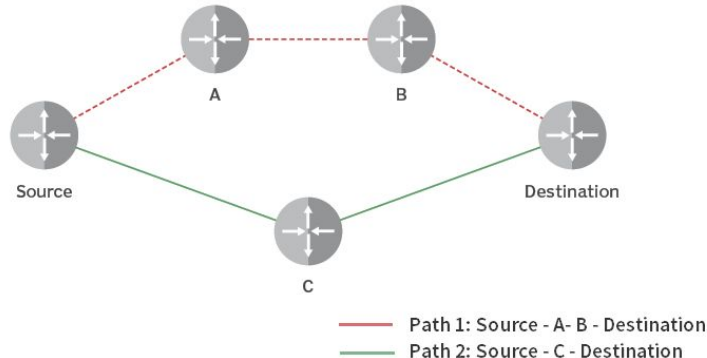


پروتکل های مسیریابی به دو روش تقسیم بندی می شوند، روش اول، از نظر داخلی یا خارجی بودن یا EGP و IGP. روش دوم، تقسیم بندی از نظر انتخاب بهترین مسیر است که Distance Vector نام دارد و یا پروتکل هایی که بر اساس تعداد روتر در مسیر یا Hop Count بهترین مسیر را انتخاب میکنند و یا Link state یا پروتکل هایی که بر اساس پایداری لینک بهترین مسیر را انتخاب میکنند و در آخر Hybrid ها که ترکیبی از اینها میباشد.

روش کار پروتکل های مسیریابی به اینصورت است که هر روتر Connected Route های خودش را برای باقی روتر های داخل شبکه پروتکل منتشر می کند و وقتی که همگی این کار را کردند تمامی روتر ها مسیرها را به سمت روتر های دیگر یاد میگیرند. در پروتکل های مسیریابی Distance Vector هر روتر جدول مسیریابی خودش را هر ۳۰ ثانیه منتشر می کند که بار زیادی ایجاد می شود اما در پروتکل های Link State جداول فقط در زمان تغییر منتشر می شوند.

Routing information protocol (RIP)

RIP uses the shortest number of hops to determine the best path to a remote network.



IGP ها در شبکه های Lan اجرا می شوند و EGP ها در شبکه های Wan.

یکی از پروتکل های دسته IGP که از نوع Distance Vector است Rip نام دارد که دو ورژن دارد.

ورژن ۱ به صورت Classfull کار می کند یعنی برای هر شبکه Subnet Mask بر اساس کلاس های IP هستند پس از شبکه 192.168.1.0/16 نمی شود استفاده کرد.

ورژن ۲ به صورت Classless کار می کند و هر شبکه ای که مدنظرتون باشد قابل استفاده است.

در شبکه ی RIP نهایتا ۱۶ عدد روتر می شود استفاده کرد.