گروه انفورماتیک
توسعه شبکه پایدار

آموزش میکروتیک
MTCNA

NAT
Mangle
PPP Server
EOIP Tunnel
DHCP Server
Web Proxy
Hotspot Gateway
Queue – Traffic Shaping

نویسنده:
احسان سونی

فهرست

فصل اول : آشنایی با روتر میکروتیک و نصب سیستم عامل میکروتیک

معرفی میکروتیک

میکروتیک نام تجاری شرکت تولید کننده تجهیزاتی است که معمولا به همین نام خوانده می شود.شرکت میکروتیک در کشور Latvia (شرق اروپا) فعالیت می کند.این شرکت در سال ۱۹۹۵ توسط دو دانشجوی MIT آمریکا به وسیله ی نگارش سیستم عامل میکروتیک به این نام گذاشته شد.همزمان با شکل گیری استانداردهای ۸۰۲,۱۱ و توسعه سخت افزاری این سیستم قابلیت وایرلس نیز به آن افزوده شد و به دلیل استقبال کاربران ، این شرکت سیستم عاملی مبتنی بر کرنل لینوکس (Linux 2.6) بنام Mikrotik Router OS را ارائه داد.

ویژگی های Mikrotik Router OS

از ویژگی های Mikrotik ارایه سرویس هایی مانند Routing,Wireless,Hotspot,BandWidth Manager,Tunnels and Vpn,... بر روی لایه ۳ می باشد که دیگر نیازی به لایه های بالاتر ندارد و این ویژگی در بالا بردن کیفیت و Performance سیستم تاثیر دارد.
یکی دیگر از ویژگی های میکروتیک پایداری آن است.میکروتیک همانند یک روتر قوی از سرعت بوت بالا و عملکرد خودکار بدون نیاز به هیچگونه Login یا استارت کردن هر نوع سرویس برخوردار است.
سیستم عامل میکروتیک دارای چندین سطح مجوز یا License Level می باشد.هر سطح مجوز ویژگی های بیشتری نسبت به سطوح قبلی دارد ویژگی هایی مانند : امکان مدیریت کاربران بیشتر،رفع مشکلات مجوزهای قبلی،اضافه شدن امکانات جدید و ... امروزه مجوزهای سطح ۳و۴و۵و۶ برای میکروتیک قابل ارائه می باشد چرا که سطح صفر به عنوان نسخه Demo و سطح یک آن نسخه ی انتقالی از نسخه قدیمی ۲,۸ (Free) به بعد بود.به منظور ارتقای عملکرد این سیستم باید لایسنس هر ویژگی را دریافت کرد تفاوت این سطوح را در جدول زیر میتوان مشاهده کرد :

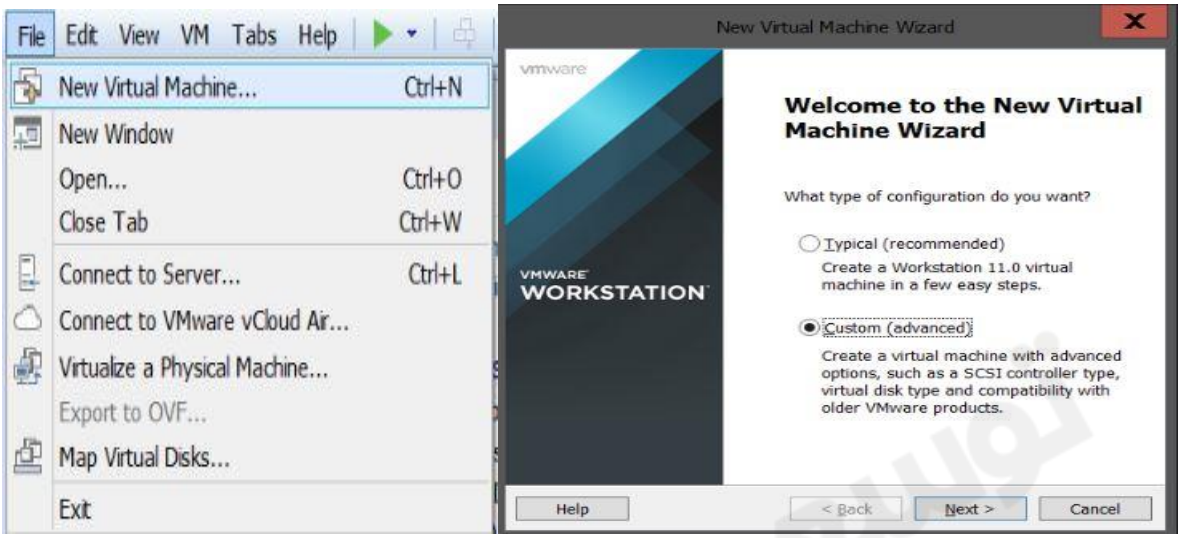
Level number	0 (Demo mode)	1 (Free)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	volume only	$45	$95	$250
Upgradable To	-	no upgrades	ROS v6.x	ROS v6.x	ROS v7.x	ROS v7.x
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited

نقطه ی قوت دیگر میکروتیک به صرفه بودن آن نسبت به نمونه های مشابه است در ضمن برروی تمامی روتربردهای آن نسخه ای از Router OS نصب می باشد.
تجهیزات شرکت میکروتیک به دو دسته نرم افزاری بنام Router OS و سخت افزاری بنام Routerboard تقسیم میشوند.
Router OS میکروتیک برروی یک کامپیوتر پنتیوم ۳ نیز قابل نصب می باشد و میتوان اعمالی مانند NAT,Firewall,Filtering را روی آن کامپیوتر انجام دهیم.

نصب سیستم عامل میکروتیک بر روی VmWare Workstation

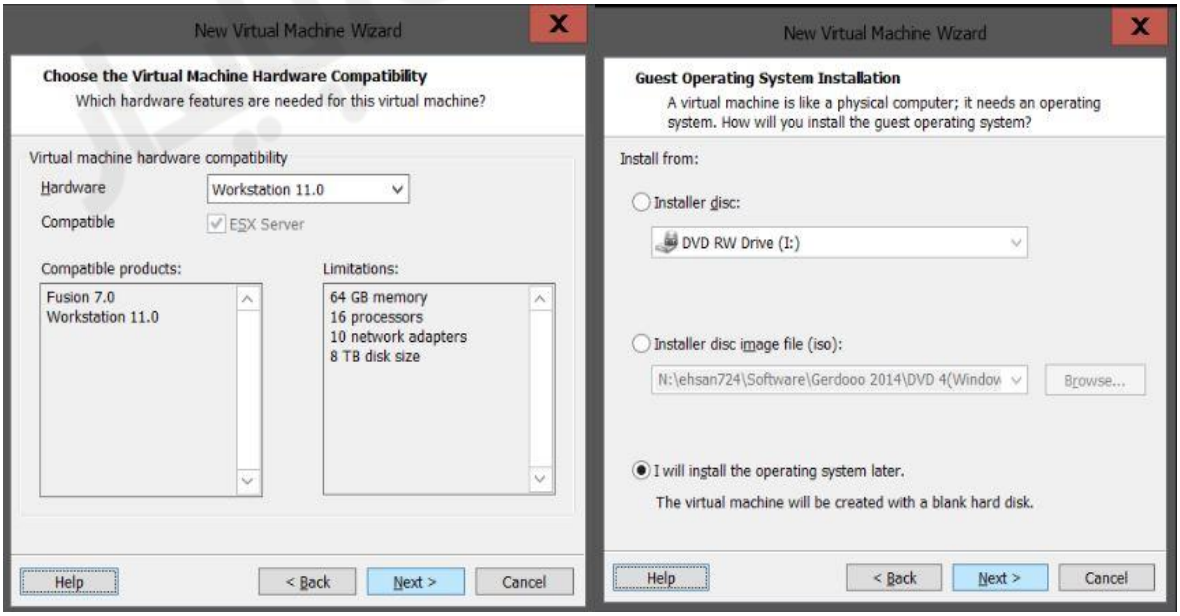
نحوه ایجاد ماشین مجازی:

از منوی **File** گزینه **New Virtual Machine...** را انتخاب میکنیم و در صفحه ی بعد برای اینکه مشخصات ماشین مجازی را طبق نیاز تغییر دهیم گزینه ی **Custom** را انتخاب میکنیم.



در این مرحله دستگاهی که حاوی نصب سیستم عامل مورد نظر می باشد را انتخاب میکنیم.

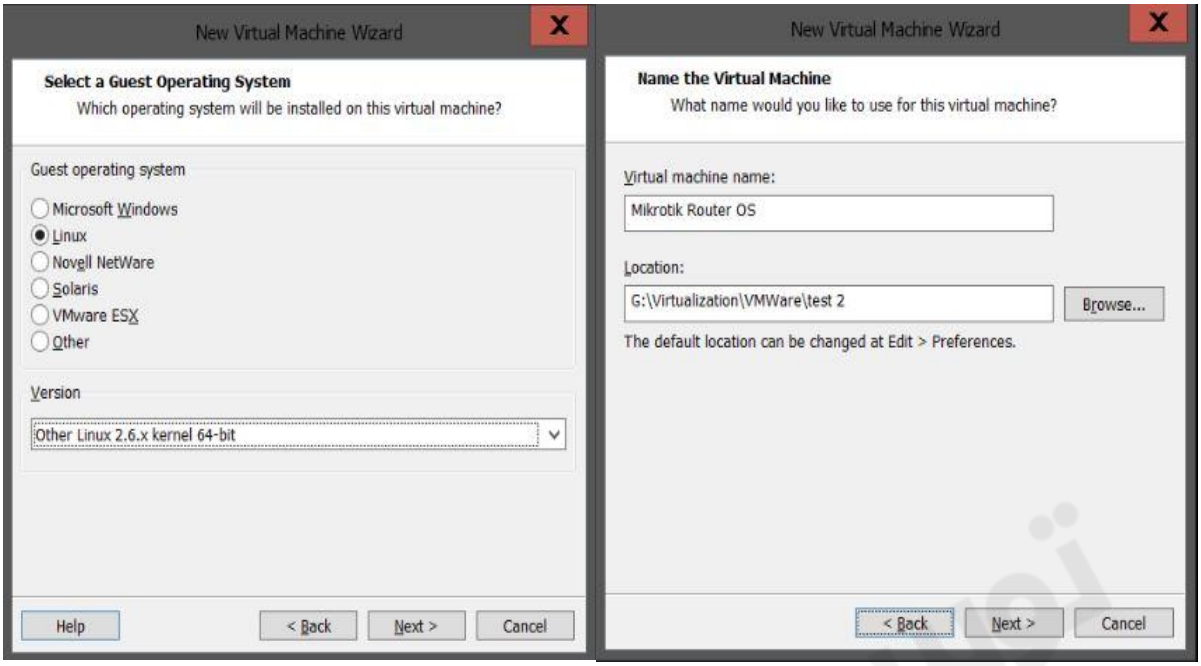
- چنانچه سیستم عامل بر روی **DVD** باشد گزینه اول را انتخاب میکنیم.
- چنانچه سیستم عامل به صورت فایل **iso** گزینه دوم را انتخاب میکنیم.
- چنانچه بخواهیم بعد از آماده سازی ماشین مجازی دستگاه را مشخص کنیم گزینه سوم را انتخاب میکنیم.



در این مرحله نوع سیستم عاملی که بر روی این ماشین قرار است نصب شود و نسخه ی آن را انتخاب میکنیم.

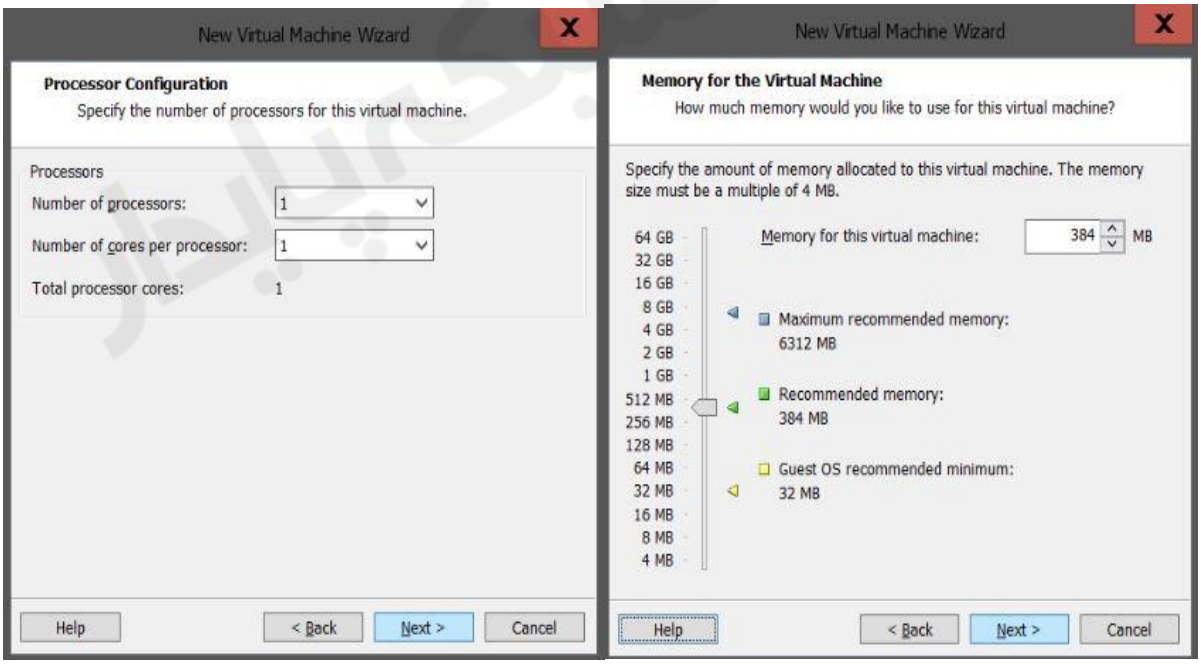
نکته : برای نصب میکروتیک سیستم عاملی از نوع **Linux** انتخاب میکنیم.

در مرحله بعد یک نام برای ماشین مجازی در نظر گرفته می شود و در قسمت **Location** مسیر نصب فایل های مورد نیاز را مشخص میکنیم.



میزان پردازنده ای که می خواهیم به ماشین مجازی اختصاص دهیم را مشخص می کنیم.

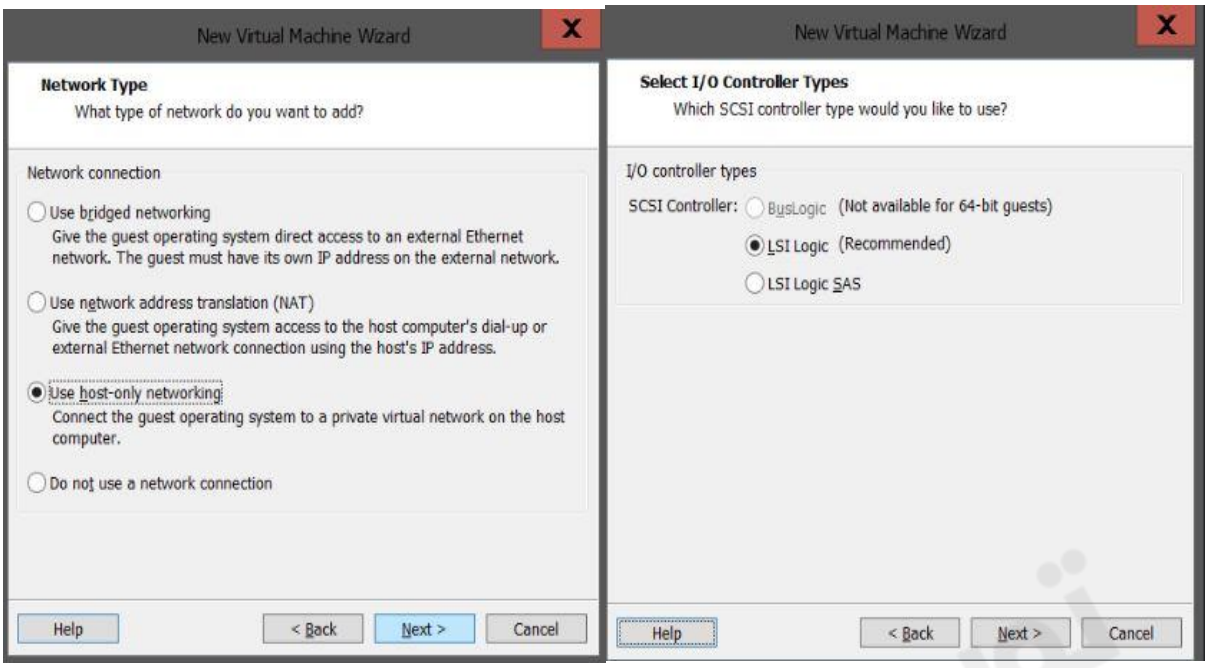
در مرحله بعد میزان **RAM** مورد نیاز برای ماشین مجازی را مشخص می کنیم.



نوع کارت شبکه را مشخص میکنیم.

نوع کارت شبکه را **Host Olny** قرار میدهیم تا بتوانیم از طریق سیستم عامل اصلی خودمان به **Router OS** دسترسی پیدا کینم.

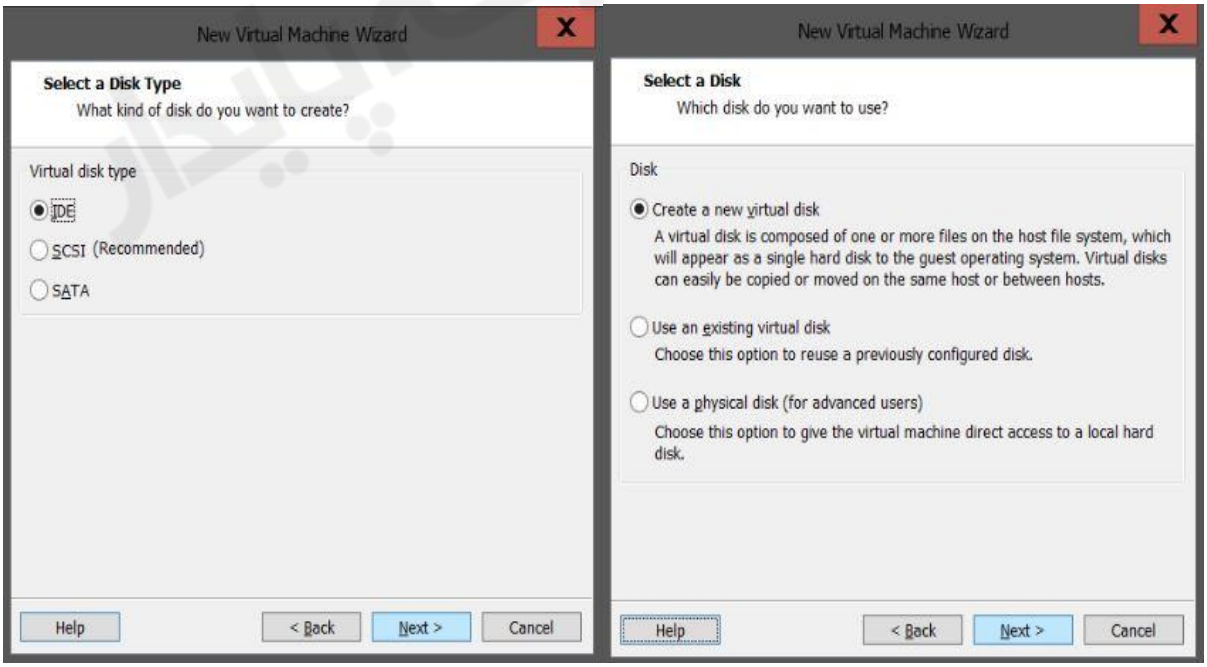
در مرحله بعد نوع کنترلر ماشین را تعیین کرده ، تنظیمات پیش فرض را انتخاب میکنیم.



برای ایجاد یک دیسک مجازی جدید برروی این سیستم گزینه اول را انتخاب میکنیم و چنانچه بخواهیم از فایل های دیسک های مجازی که از قبل ایجاد شده باشد استفاده کنیم گزینه دوم را انتخاب میکنیم.

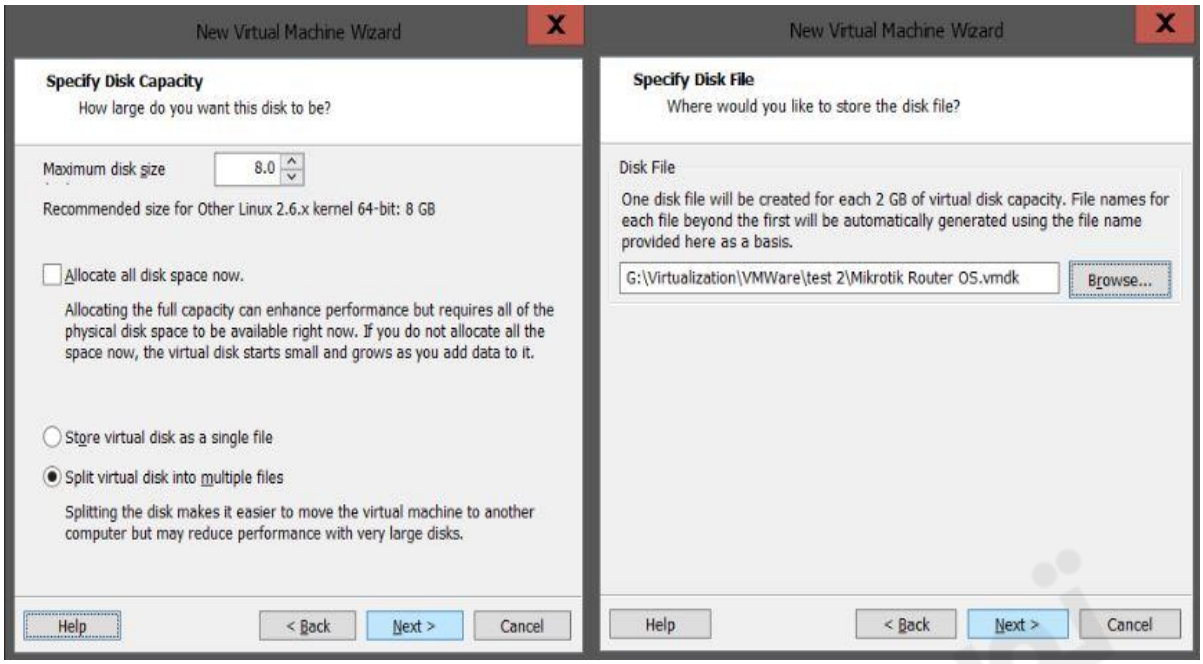
در مرحله ی بعد دیسک مجازی را انتخاب میکنیم.برای نصب میکروتیک از دیسک IDE باید استفاده شود.

نکته : Mikrotik OS های قدیمی با هاردهای Sata,Iscasi مشکل داشت و فقط با IDE کار میکرد اما این مشکل در Mikrotik OS های جدید رفع شده است.



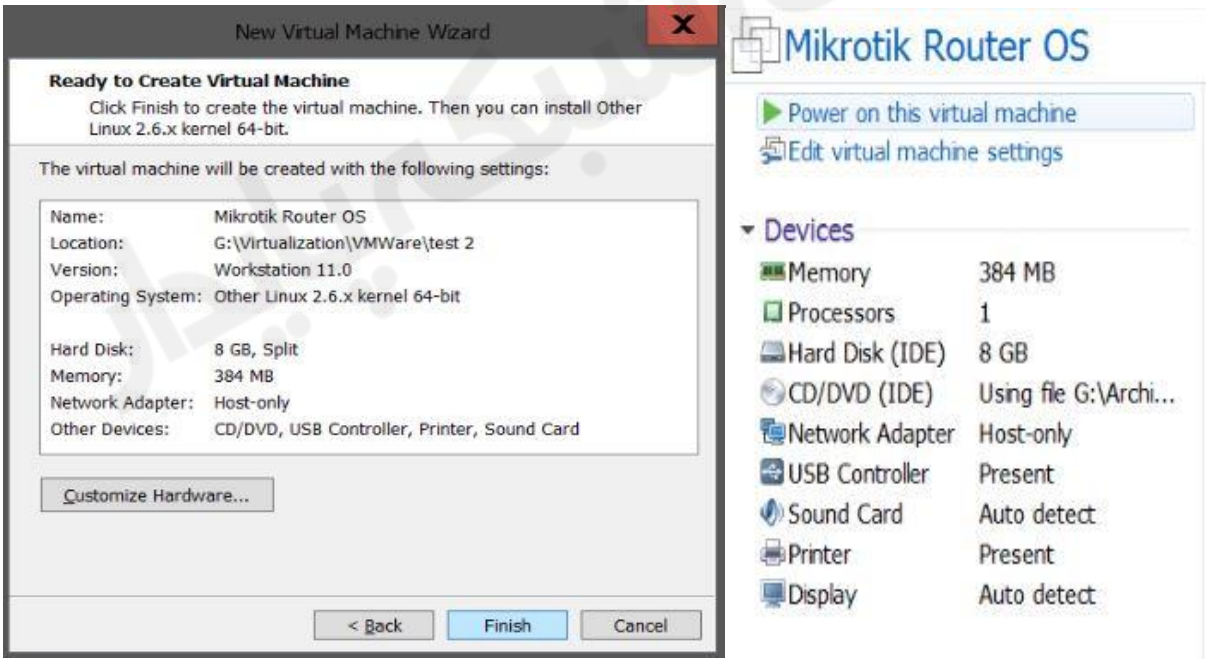
میزان فضای دیسک مجازی را انتخاب میکنیم.چنانچه گزینه Allocate all Disk Space را به حالت انتخاب در بیاورید تمام فضای مشخص شده را از روی سیستم اصلی برای فایل های نصب میکروتیک رزرو می کند.

در مرحله بعد یک نام برای فایل نصب میکروتیک در نظر گرفته و به مرحله بعد میرویم.



در این مرحله خلاصه ای از تنظیمات انجام شده نمایش داده می شود

در مرحله بعد بر روی گزینه **Power on this virtual machine** کلیک میکنیم تا مراحل نصب سیستم عامل میکروتیک آغاز شود.



نصب Mikrotik OS بر روی VmWare

در ابتدای نصب سیستم عامل میکروتیک بر روی سیستم صفحه ای مشابه شکل زیر نشان داده می شود :

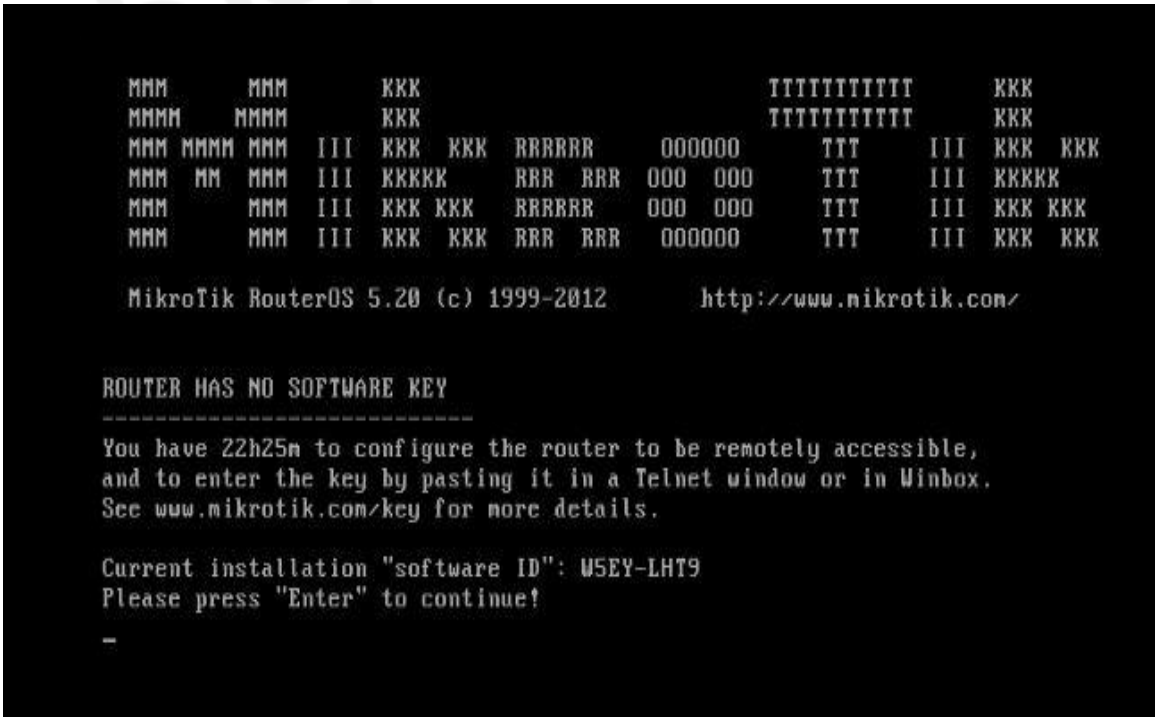
- برای انتخاب تمام **Package** های میکروتیک باید کلید **A** را فشار دهید.
- چنانچه بخواهید موردی از **Package** را انتخاب کنید از کلید **Space** استفاده کنید.
- با استفاده از کلید **I** موارد مشخص شده از **Package** میکروتیک را میتوان نصب کرد.

در مراحل بعد سوالی مبنی بر حفظ تنظیمات قبلی پرسیده می شود و با استفاده از کلید y به این سوال پاسخ مثبت می دهیم.

در ادامه پیغامی مبنی بر پاک شدن تمام داده های روی دیسک نشان داده می شود که با استفاده از کلید y این مورد را نیز می پذیریم و مراحل نصب را ادامه می دهیم.

بعد از طی شدن فرایند نصب تمام Package نیاز است که سیستم یک بار ریستارت شود.

بعد از لود شدن کامل سیستم عامل میکروتیک با استفاده از نام کاربری admin بدون اینکه رمزی را وارد کنیم به میکروتیک وارد میشویم.



روش های دسترسی به Mikrotik

جهت دسترسی به میکروتیک و اعمال تنظیمات برروی آن چند روش می توان استفاده کرد :

۱-اتصال از طریق کابل کنسول (Console)

۲-اتصال از راه دور(Remotly)

۲,۱-رابط متنی Command Line Interface(CLI)

- ✓ Telnet
- ✓ SSH
- ✓ Winbox Terminal

۲,۲-رابط گرافیکی Graphical User Interface(GUI)

- ✓ Winbox
- ✓ Webfig

۳-اتصال از طریق نرم افزارهای جانبی(Application Interface)

اتصال از طریق کنسول

زمانی که امکان دسترسی مستقیم به میکروتیک وجود داشته باشد بهترین حالت ، استفاده از کنسول آن است.

برای این کار چنانچه از Router OS میکروتیک استفاده می کنید بر روی سیستمی که Router OS روی آن نصب است Login کرده و تنظیمات مورد نظرتان را اعمال کنید و چنانچه از Routerborad میکروتیک استفاده میکنید باید کابل کنسول دستگاه را به کامپیوتر متصل کنید و از این طریق تنظیمات را بر روی میکروتیک اعمال کنید.

برای این کار سوکت RG-45 از کابل کنسول را به پورت کنسول از Routerborad را متصل کرده و از سمت دیگر پورت سریال کابل کنسول را به پورت سریال کامپیوتر متصل میکنیم.

نکته : چنانچه کامپیوتری پورت سریال نداشته باشد از مبدل سریال به USB استفاده میکنیم.

نمونه ای از یک دستگاه Mikrotik RouterBorad

نمونه ای از یک کابل کنسول

اتصال از راه دور(Remotly)

بطور کلی همیشه امکان دسترسی مستقیم به میکروتیک وجود ندارد و گاهی نیاز است که از راه دور برای اعمال تنظیمات بر روی میکروتیک اقدام شود.

دو روش برای اتصال از راه دور برای میکروتیک وجود دارد :

۱-از طریق رابط دستوری (Command Line Interface)

۲-از طریق محیط گرافیکی (Graphical User Interface)

از طریق رابط دستوری

برای اتصال از طریق رابط دستوری در میکروتیک چند روش وجود دارد :

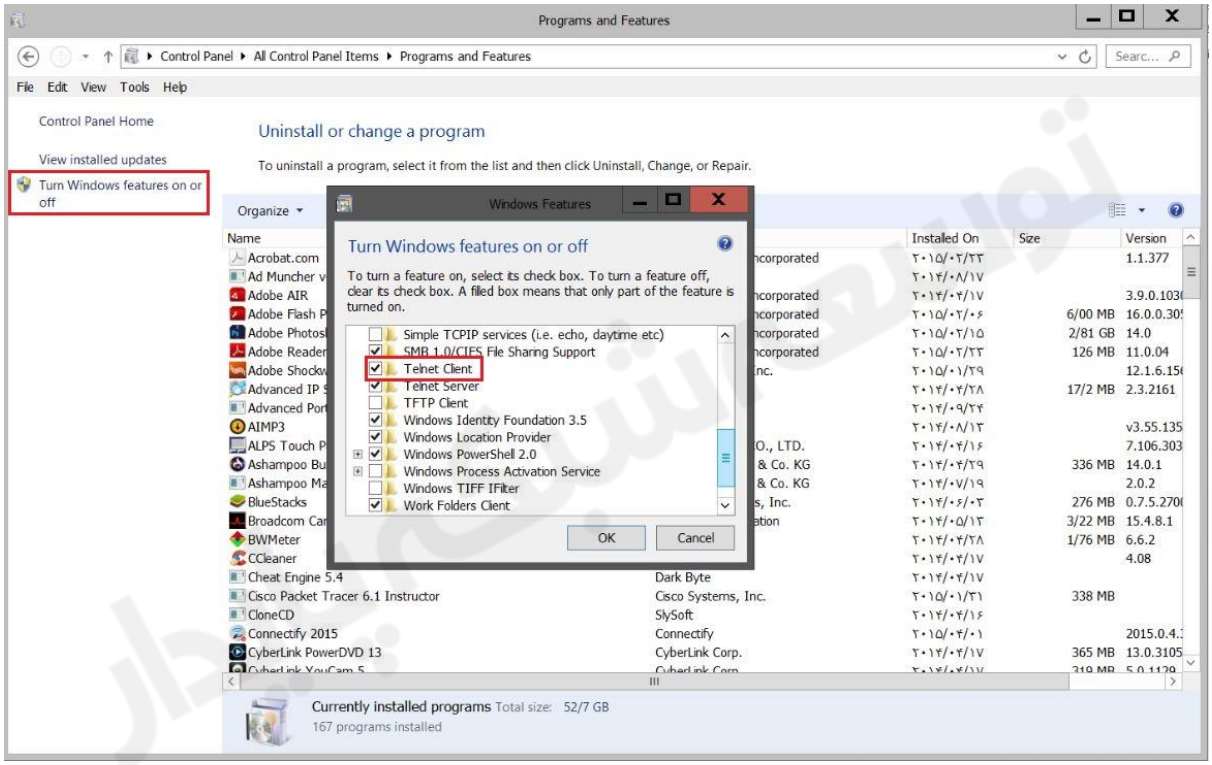
Telnet-۱

پروتکل Telnet برای برقراری ارتباط متنی بین دو سیستم در شبکه مورد استفاده قرار میگیرد.این پروتکل از پورت TCP/23 استفاده میکند.

برای برقراری ارتباط با میکروتیک از طریق Telnet باید بر روی سیستم کلاینت ویژگی مربوط به Telnet را از مسیر زیر فعال میکنیم :

Control Panel/Program And Features/Turn Windows Features On or Off

بعد از این مراحل سرویس مربوط به Telnet Client را فعال میکنیم.



در قدم بعد برای اتصال به سیستم میکروتیک از طریق Telnet در پنجره ی CMD دستور زیر را وارد میکنیم :

در واقع بعد از دستور Telnet آدرس IP سیسام میکروتیکی که قصد وارد شدن به آن را داریم را وارد میکنیم.
نکته : به صورت پیش فرض آدرس IP در میکروتیک ۱۹۲,۱۶۸,۸۸,۱ می باشد.
بعد از این مرحله زمانی که کلاینت به میکروتیک متصل شد باید یوزرنیم و پسورد معتبری که در میکروتیک تعریف شده است را وارد میکنیم.

نکته : بصورت پیش فرض یوزرنیم در میکروتیک **admin** و بدون پسورد می باشد.

در نهایت محیط **CLI** مربوط به میکروتیک نشان داده خواهد شد و از این طریق می توان تنظیمات مورد نظر را اعمال کرد.

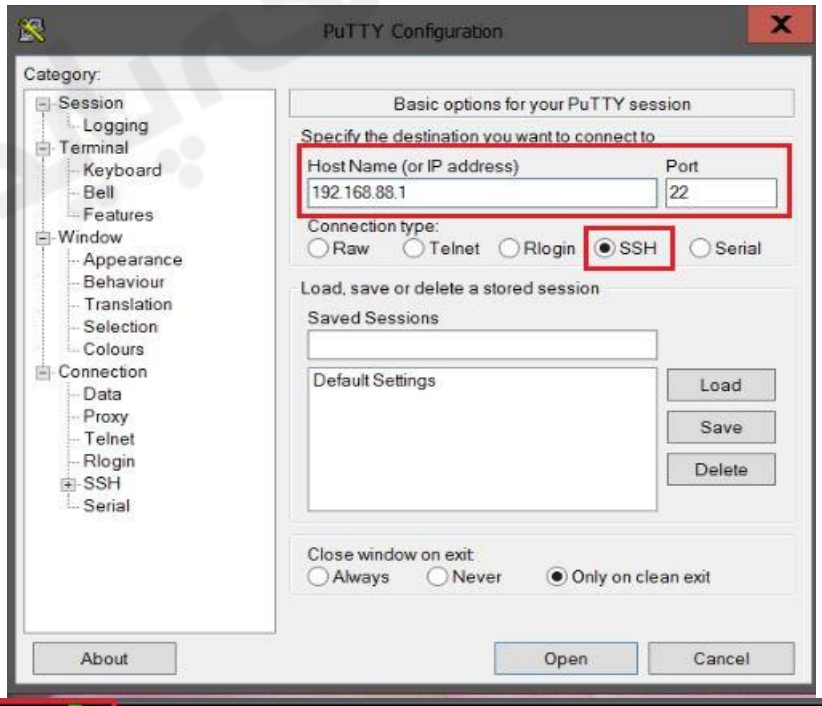
نکته : با استفاده از دستور **quit** می توان از این محیط خارج شد.

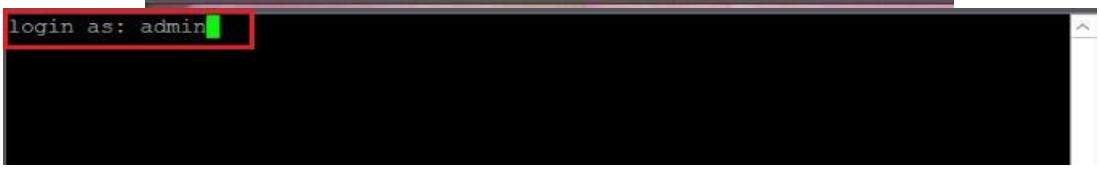
Secure Shell(SSH)-۲

برای اتصال به میکروتیک از طریق **SSH** از یک نرم افزار جانبی مانند **Putty** استفاده شود.

برای این کار بعد از اجرای نرم افزار :

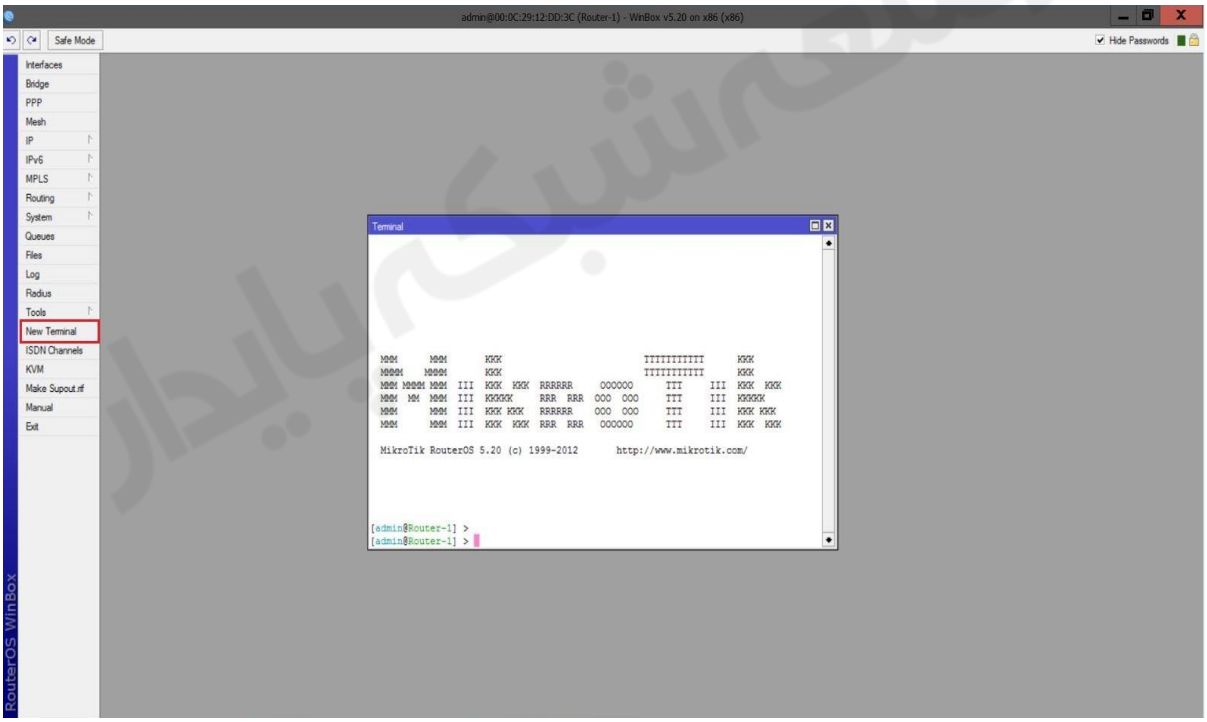
۱. در قسمت **Host Name(or Ip Address)** نام سیستم میکروتیک و یا **IP** آن را وارد میکنیم.
۲. در قسمت **Connection Type** نوع **SSH** را انتخاب میکنیم.
۳. بعد از برقراری ارتباط نام کاربری و پسورد معتبری که میتوانیم با آن میکروتیک به آن متصل شویم را وارد میکنیم.





Winbox Terminal-۳

از طریق نرم افزار Winbox نیز می توانیم به محیط Command Line دسترسی داشته باشید.برای استفاده از این قابلیت در نرم افزار Winbox از منوی اصلی گزینه New Terminal را انتخاب کرده تا اینکه پنجره Terminal باز شود.



از طریق محیط گرافیکی

Winbox-۱

نرم افزار گرافیکی برای مدیریت RouterBorad و Router OS میکروتیک می باشد.این نرم افزار کم حجم توسط شرکت میکروتیک ارائه شده است.این نرم افزار را میتوانید از سایت رسمی میکروتیک دانلود کنید.آدرس سایت میکروتیک www.Mikrotik.com

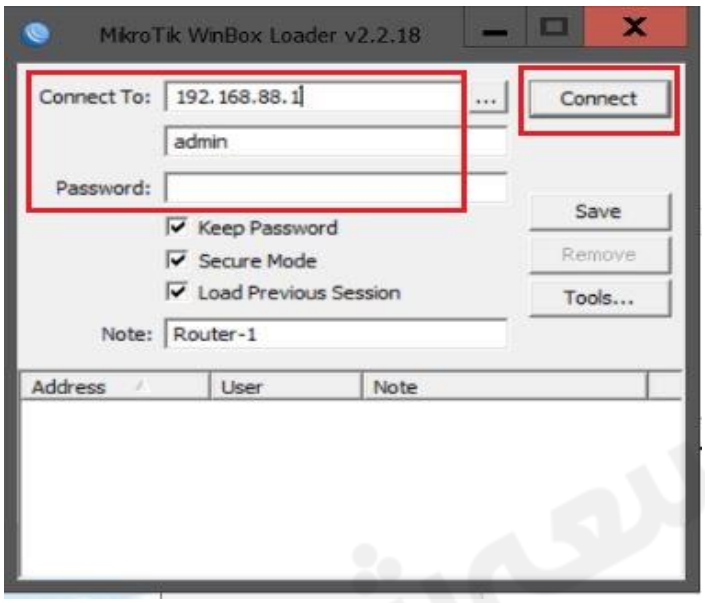
با استفاده از نرم افزار Winbox به دو روش می توان به دستگاه های میکروتیک متصل شد :

- ✓ **IP-Address**
- ✓ **Mac-Address**

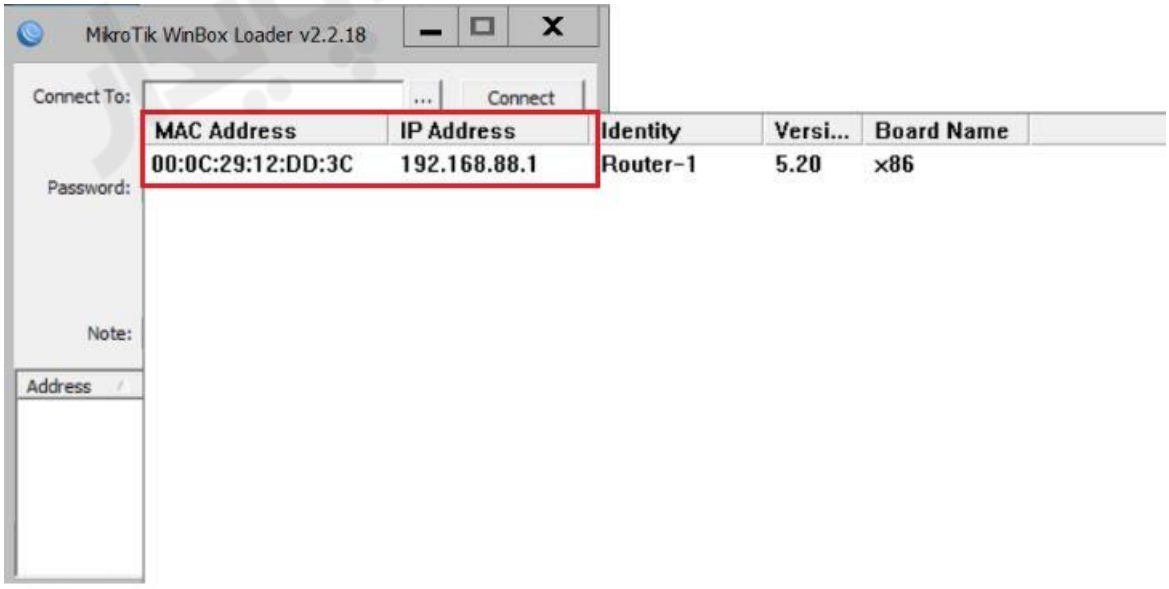
نکته : برای اتصال به میکروتیک از طریق **Mac-Address** تنها زمانی که میکروتیک در **Broadcast Domain** شما باشد امکان پذیر است و با توجه به اینکه **Mac** در لایه ۲ کار میکند بنابراین برای ارتباط با روتر میکروتیک نیازی به تنظیم **IP** بر روی آن نمی باشد بنابراین اتصال میکروتیک از طریق **Mac-Address** در اینترنت به هیچ عنوان امکان پذیر نیست.

چنانچه دستگاه میکروتیک در **Broadcast Domain** شما نباشد برای اتصال به آن **IP** دستگاه مورد نظر را در قسمت **Connect TO** وارد کرده و نام کاربری و رمز عبور تعریف شده در دستگاه را وارد کرده و برروی **connect** کیک میکنیم.

بصورت پیش فرض نام کاربری **admin** و بدون رمز عبور می باشد.



چنانچه دستگاه های میکروتیک در **Broadcast Domain** شما باشد برای اتصال به میکروتیک از طریق **Winbox** بعد از اجرای این نرم افزار بر روی علامت ... کلیک می کنیم در پنجره باز شده **Mac-Address** و **IP-Address** میکروتیک هایی که شناسایی می شوند لیست شده است.

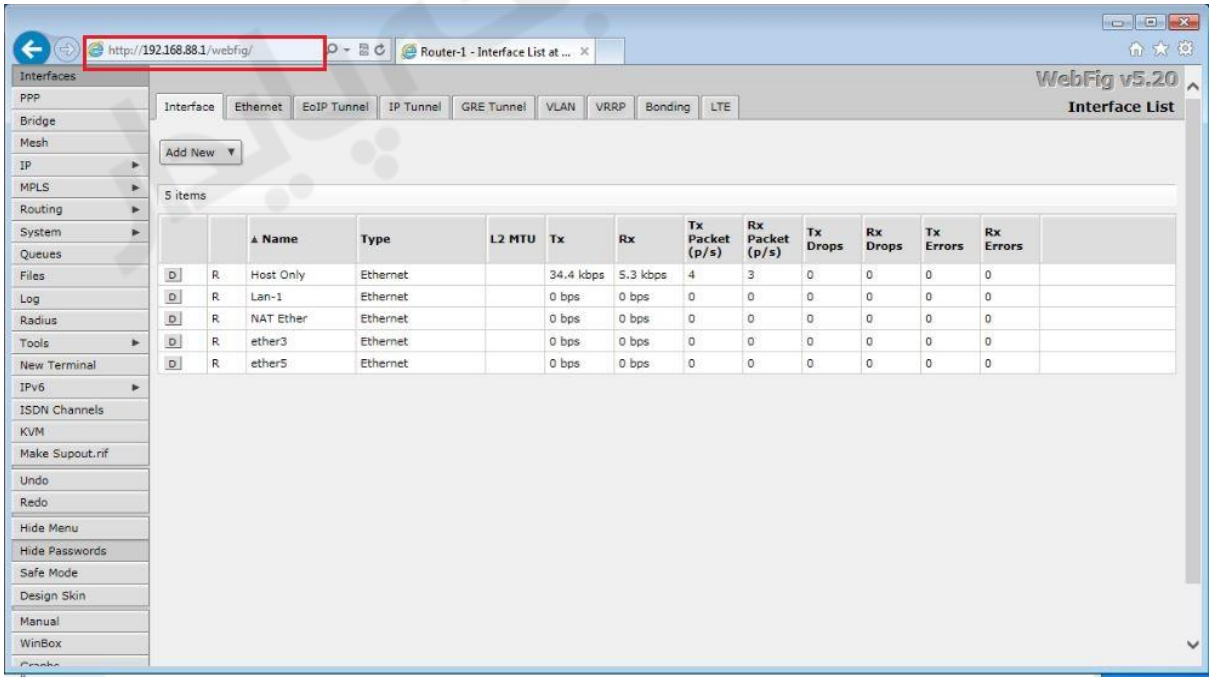


Webfig-۲

یک رابط کاربری وب برای نظارت ، مدیریت و عیب یابی میکروتیک می باشد.

برای استفاده از Webfig نیازی به نصب هیچ برنامه ای نیست و تنها وجود یک مرورگر روی سیستم کفایت می کند.این روش برای اتصال به میکروتیک به صورت WebBased می باشد.

برای این کار در پنجره مرورگر خود IP مربوط به میکروتیک را وارد کرده و بعد از وارد کردن نام کاربری و رمز عبور بر روی Login کلیک کرده، وارد صفحه Webfig می شویم و رابط گرافیکی میکروتیک برای شما نمایش داده می شود.



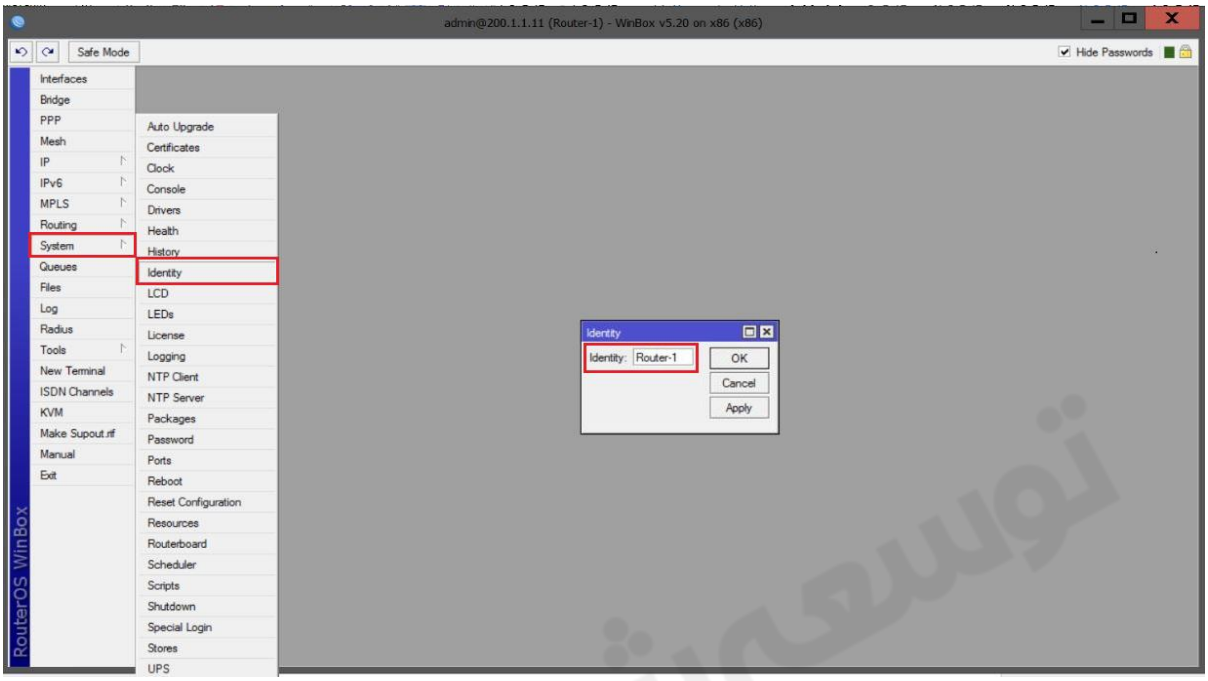
۳-اتصال از طریق Application Interface

حالت خاصی از روش های اتصالی به میکروتیک از طریق نرم افزارهای جانبی است این نرم افزارها می توانند پورتی را بر روی میکروتیک باز کنند و از طریق این پورت می توان دستگاه میکروتیک را مدیریت کرد.

فصل دوم : تنظیمات اولیه روتر میکروتیک

۱)تغییر نام سیستم میکروتیک

از طریق Winbox

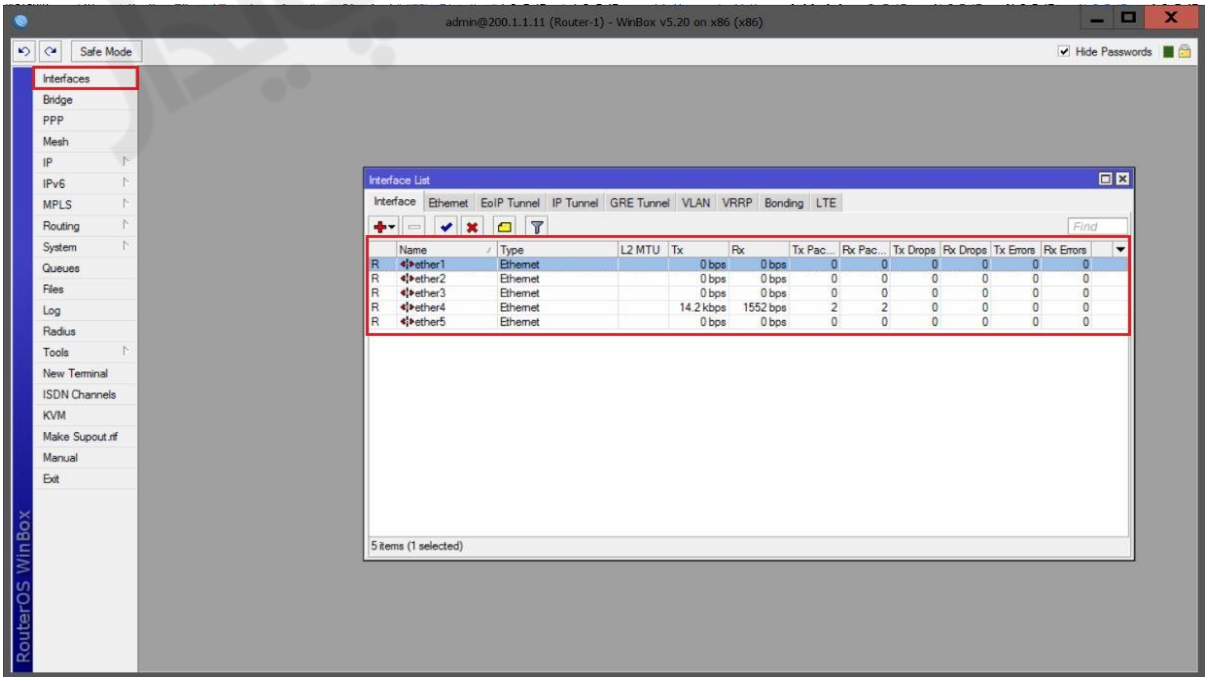


از طریق New Terminal

[admin@Router-1] > system identity set name=Router-1

۲)نمایش کارت شبکه های موجود در روتر میکروتیک

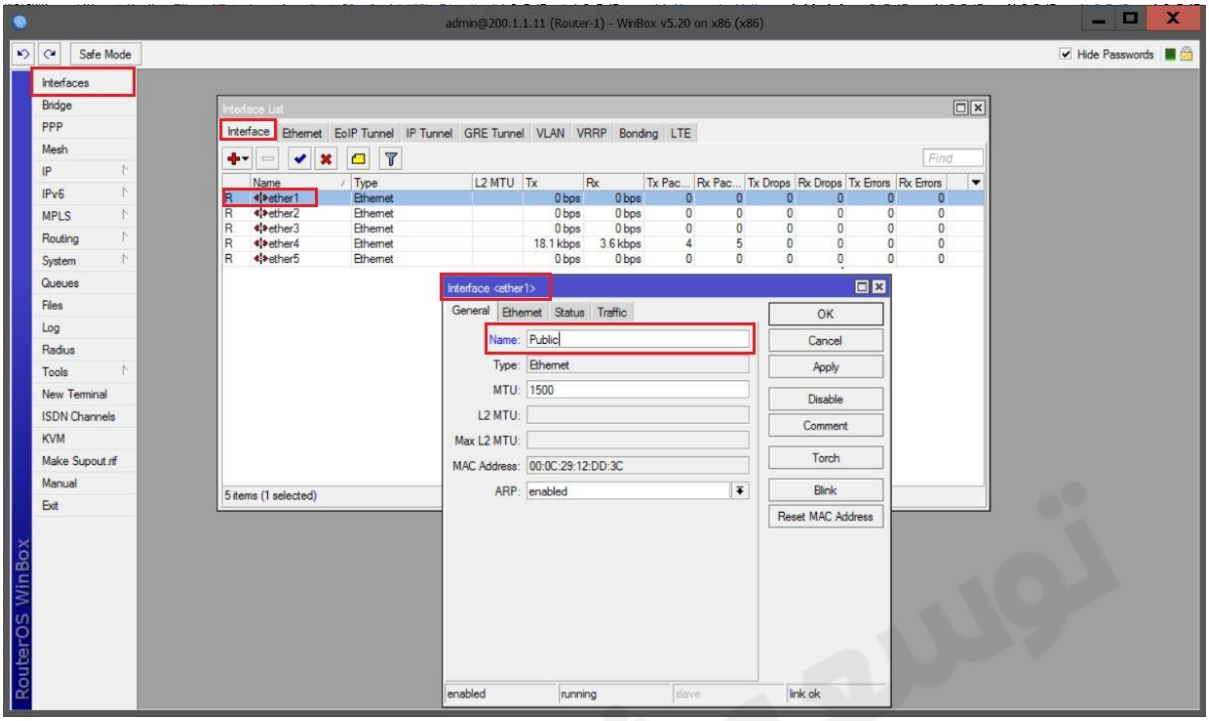
برای نمایش کارت شبکه از منوی اصلی Interface را انتخاب کرده و از پنجره Interface List می توانیم کارت شبکه ها را مشاهده کنیم.



[admin@Router-1] > interface ethernet print

۳)تغییر نام کارت شبکه

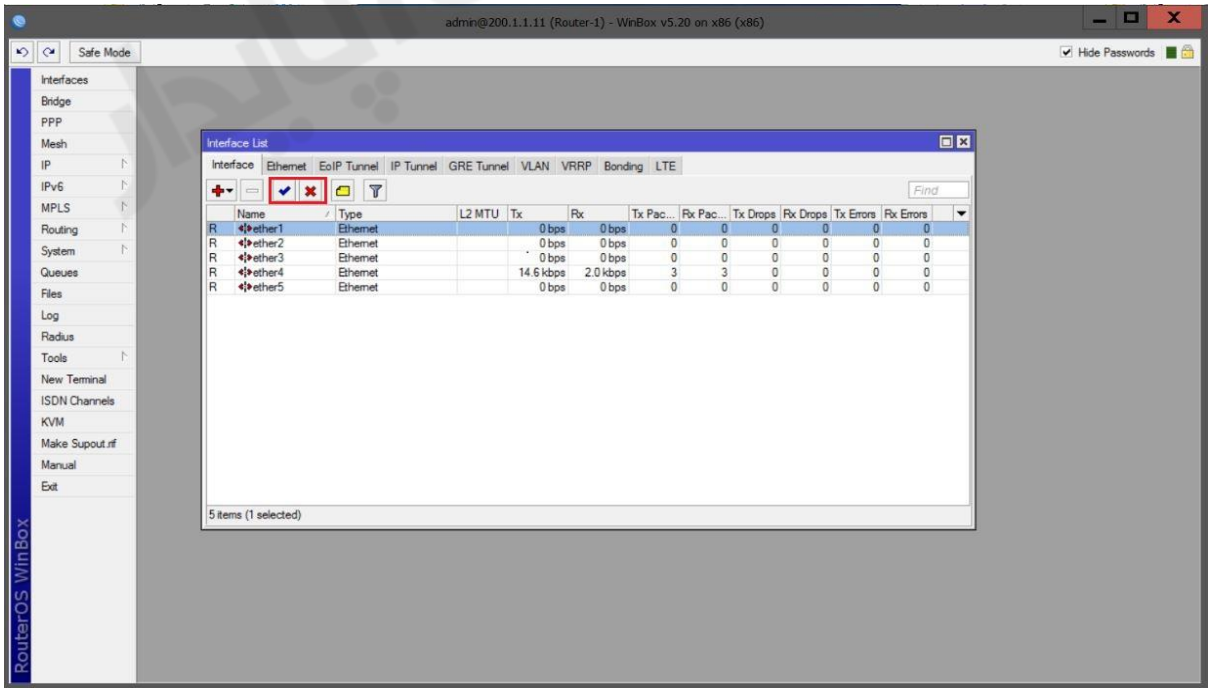
برای تغییر نام کارت شبکه از منوی اصلی گزینه Interface را انتخاب کرده و در پنجره Interface List بر روی کارت شبکه مورد نظر دوبار کلیک میکنیم در پنجره <Interface<ether در قسمت Name نام مورد نظر را وارد می کنیم.



[admin@Router-1] > interface ethernet set ether1 name=Public

۴)فعال و غیر فعال کردن کارت شبکه

برای این کار از منوی اصلی Interface را انتخاب کرده واز پنجره Interface List کارت شبکه مورد نظر را انتخاب و با علامت  **آن را غیرفعال(Disable) و با علامت**  **آن را فعال (Enable) می کنیم.**



[admin@Router-1] > interface ethernet disable ether1
[admin@Router-1] > interface ethernet enable ether1

۵)انتساب IP به کارت های شبکه میکروتیک

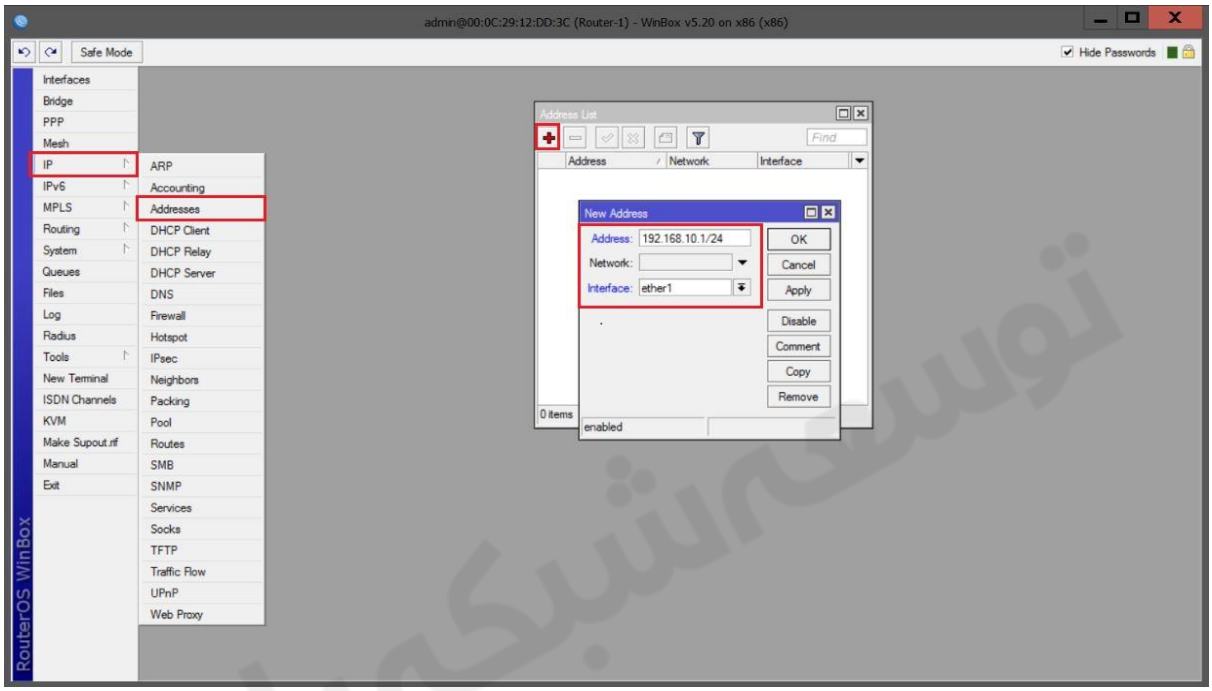
برای انتساب IP به کارت های شبکه میکروتیک به دو صورت می توان عمل کرد :

- ✓ Dynamic IP
- ✓ Static IP

در روش Dynamic سیستم به صورت خودکار تنظیمات را از سروری بنام DHCP دریافت می کند.نحوه ی دریافت تنظیمات شبکه از DHCP در فصل های بعد توضیح داده می شود.

در روش Static مدیر شبکه به صورت دستی آدرس IP را به کارت شبکه میکروتیک اختصاص میدهد.

برای دادن IP بصورت دستی از منوی اصلی گزینه IP و از زیرمنو باز شده Addresses را انتخاب می کنیم و در پنجره Address List برای اضافه کردن IP بر روی علامت ADD کلیک می کنیم.



در پنجره New Address باید سه Option مشخص شده در شکل مقدار دهی شود.

- ✓ Address : آدرس IP مورد نظر را وارد می کنیم.
- ✓ Network : SubnetMask مورد نظر برای آدرس IP را مشخص می کنیم.
- ✓ Interface : کارت شبکه ای را که می خواهیم این IP به آن اختصاص داده شود را مشخص می کنیم.

[admin@Router-1] > ip address add address=192.168.10.1/24 interface=ether1

۵-۱)برای نمایش IP هایی که بر روی کارت شبکه تنظیم شده است از دستور زیر استفاده می کنیم :

[admin@Router-1] > ip address print

خروجی دستور بالا :

```
[admin@Router-1] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS            NETWORK         INTERFACE
0   192.168.10.1/24    192.168.10.0    ether1
```

۵-۲)غیر فعال کردن IP Address :

[admin@Router-1] > ip address disable numbers=0

۵-۳)فعال کردن IP Address :

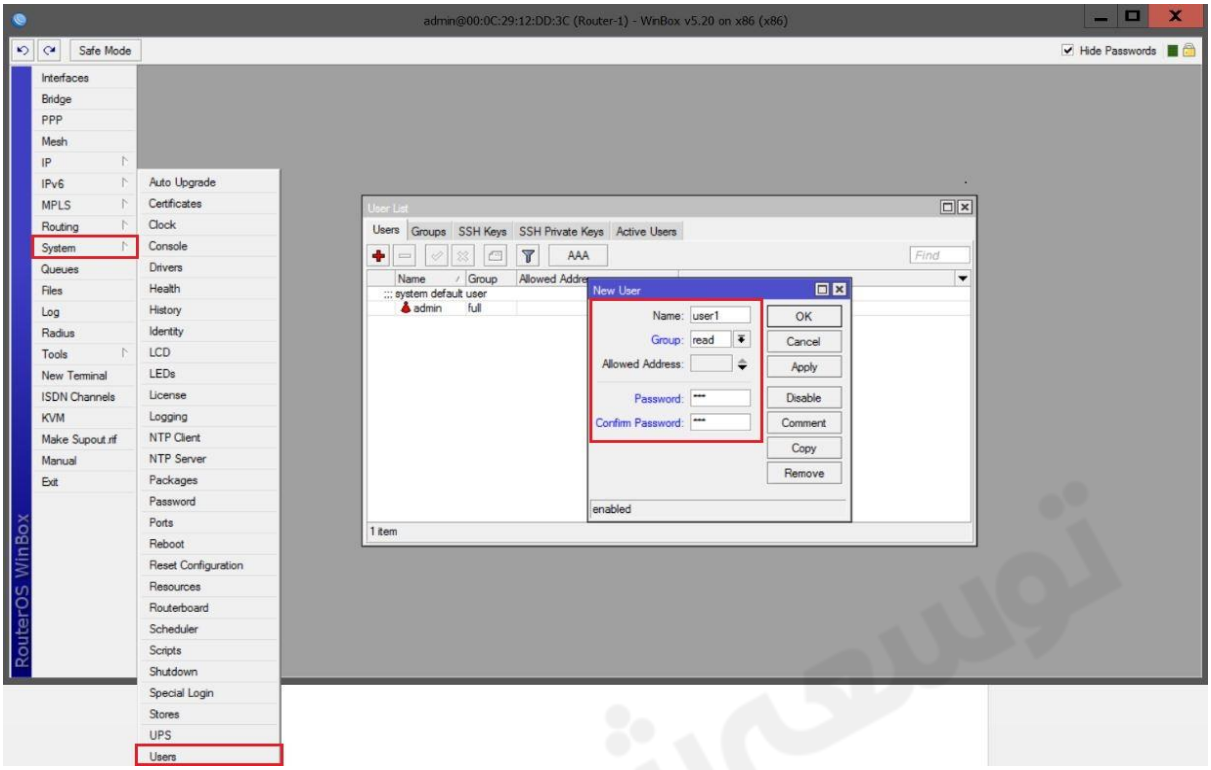
[admin@Router-1] > ip address enable numbers=0

۵-۴)حذف IP Address :

[admin@Router-1] > ip address remove numbers=0

۶)ایجاد یک کاربر جدید :

از منوی اصلی گزینه **System** و از زیر منوی باز شده گزینه **Users** را انتخاب می کنیم.در پنجره **User List** بر روی علامت **ADD** کلیک کرده و از صفحه **New User** مشخصات جدید را وارد می کنیم.



Name : نامی را برای کاربر مورد نظر انتخاب می کنیم.

Password : رمز عبور مورد نظر را برای کاربر مشخص می کنیم.

Group : سطح دسترسی کاربر را مشخص می کنیم.بصورت پیش فرض ۳ گروه با دسترسی های مختلف در میکروتیک وجود دارد که عبارت اند از :

- ✓ **Read** : اعضای این گروه فقط توانایی مشاهده تنظیمات را دارند.
- ✓ **Write** : اعضای این گروه علاوه بر مشاهده تنظیمات توانایی تغییر و اضافه کردن تنظیمات جدید را نیز دارند.
- ✓ **Full** : اعضای این گروه توانایی اعمال تنظیمات و پیکربندی روتر میکروتیک را دارند.

Address :چنانچه بخواهیم مشخص کنیم که کاربری صرفا از طریق سیستم خاص به میکروتیک متصل شود آدرس **IP** سیستم مورد نظر را در این قسمت وارد می کنیم.

[admin@Router-1] > user add name=user1 password=123 group= read address=10.10.10.1

۶-۱)نمایش کاربران تعریف شده :

[admin@Router-1] > user print

خروجی دستور بالا :

```
[admin@Router-1] > user print
Flags: X - disabled
 #   NAME                GROUP                ADDRESS
 0   ;;; system default user
     admin               full
 1   user1               read                 10.10.10.10/32
```

۶-۲)غیرفعال کردن یک کاربر :

برای غیر فعال کردن کاربر هم از طریق نام کاربر و هم از طریق شماره خط می توان آن کار را انجام داد

[admin@Router-1] > user disable user1
[admin@Router-1] > user disable numbers=1

۳-۶)فعال کردن یک کاربر :

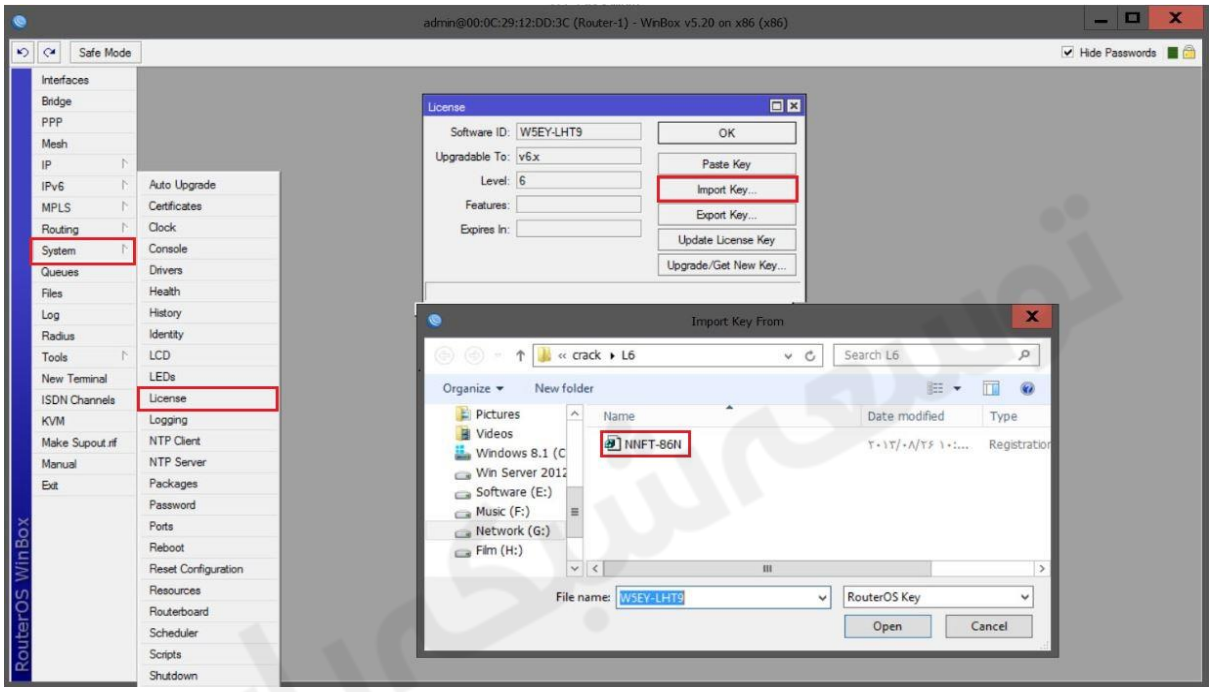
[admin@Router-1] > user enable user1
[admin@Router-1] > user enable numbers=1

۴-۶)حذف یک کاربر

[admin@Router-1] > user remove user1
[admin@Router-1] > user remove numbers=1

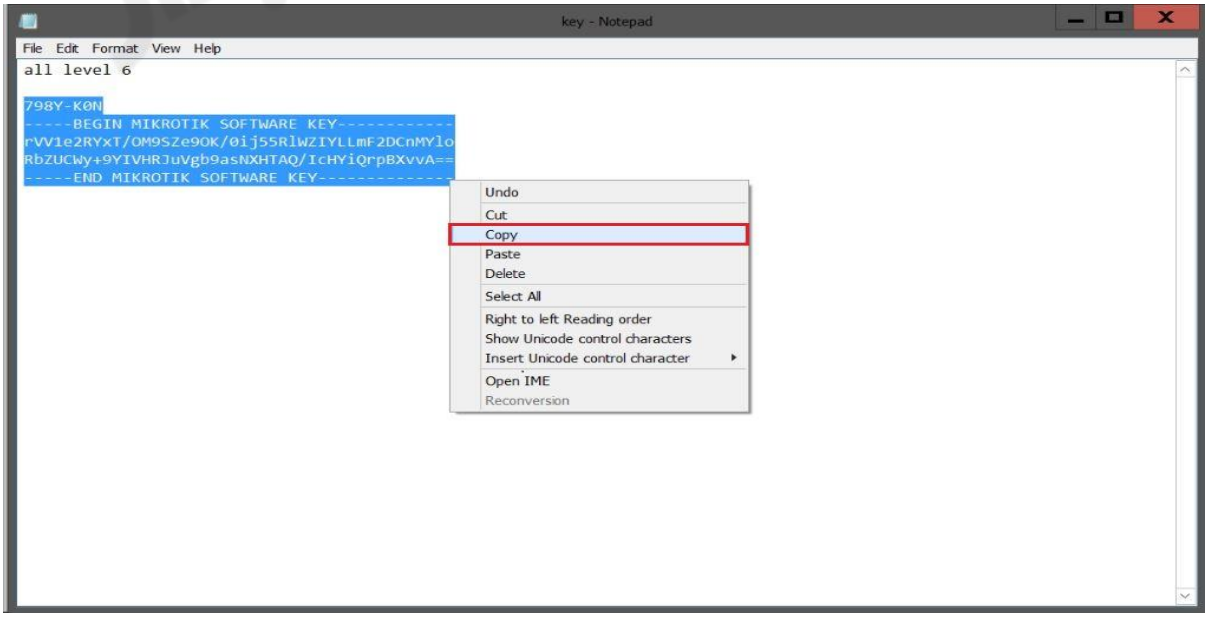
۷)نحوه لایسنس کردن میکروتیک :

- **اگر فایل بصورت Key. باشد آن را از زیر Import می کنیم :**

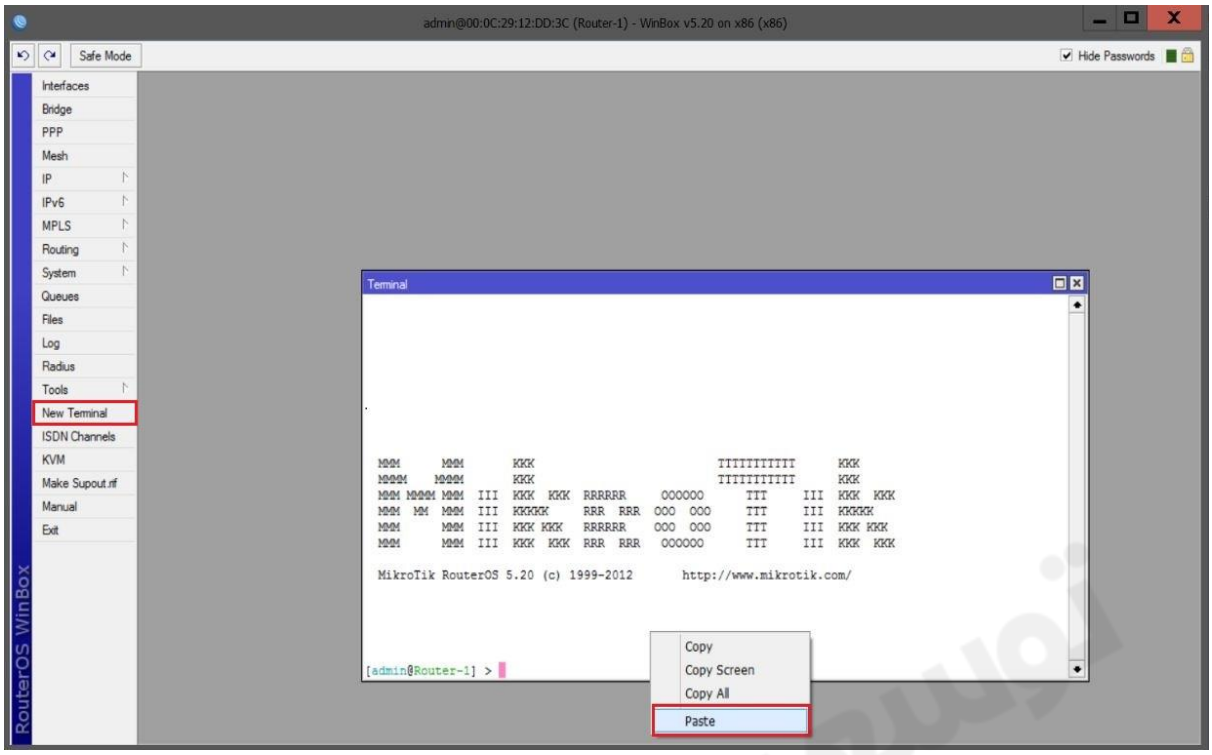


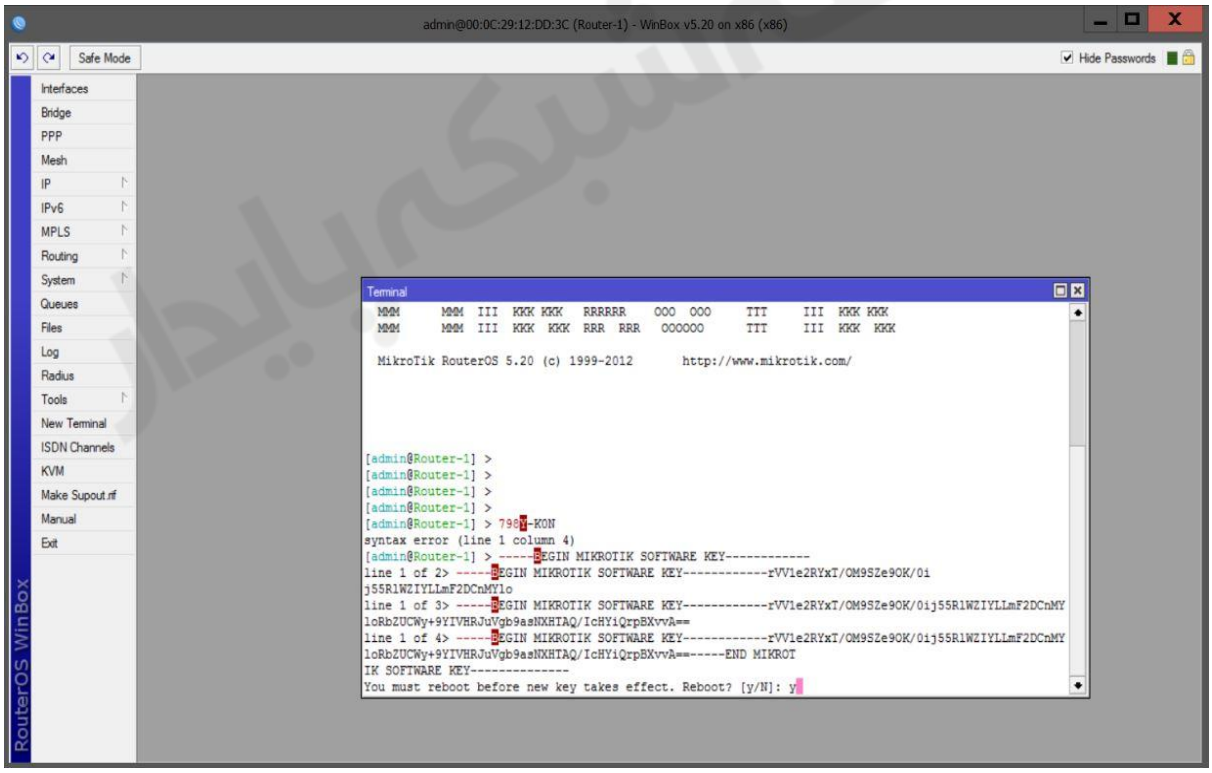
- **اگر بصورت فایل متنی باشد از مسیر زیر آن را ADD می کنیم :**

ابتدا کد را کپی میکنیم



سپس کد کپی شده را در میکروتیک **Paste** کنید.



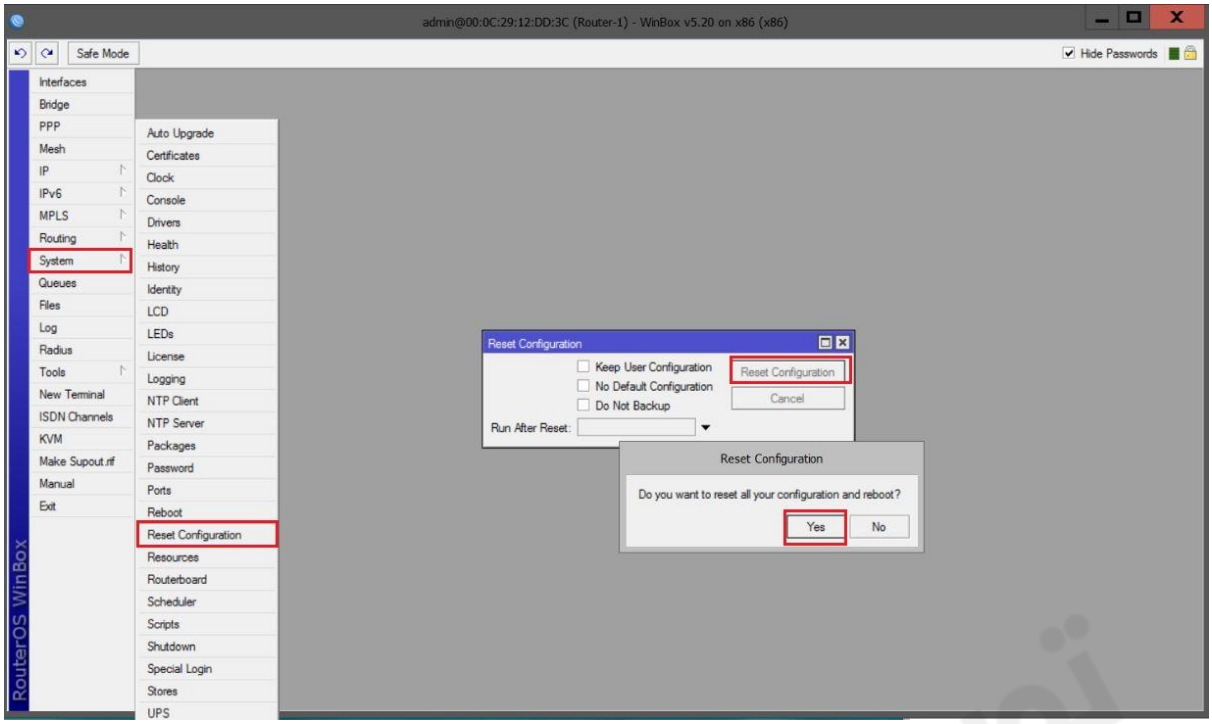


در آخر سیستم را ریستارت می کنیم.

۸)برگرداندن تنظیمات دستگاه به تنظیمات کارخانه :

برای این کار از منوی اصلی گزینه **System** و از زیرمنوی باز شده **Reset Configuration** را انتخاب می کنیم.

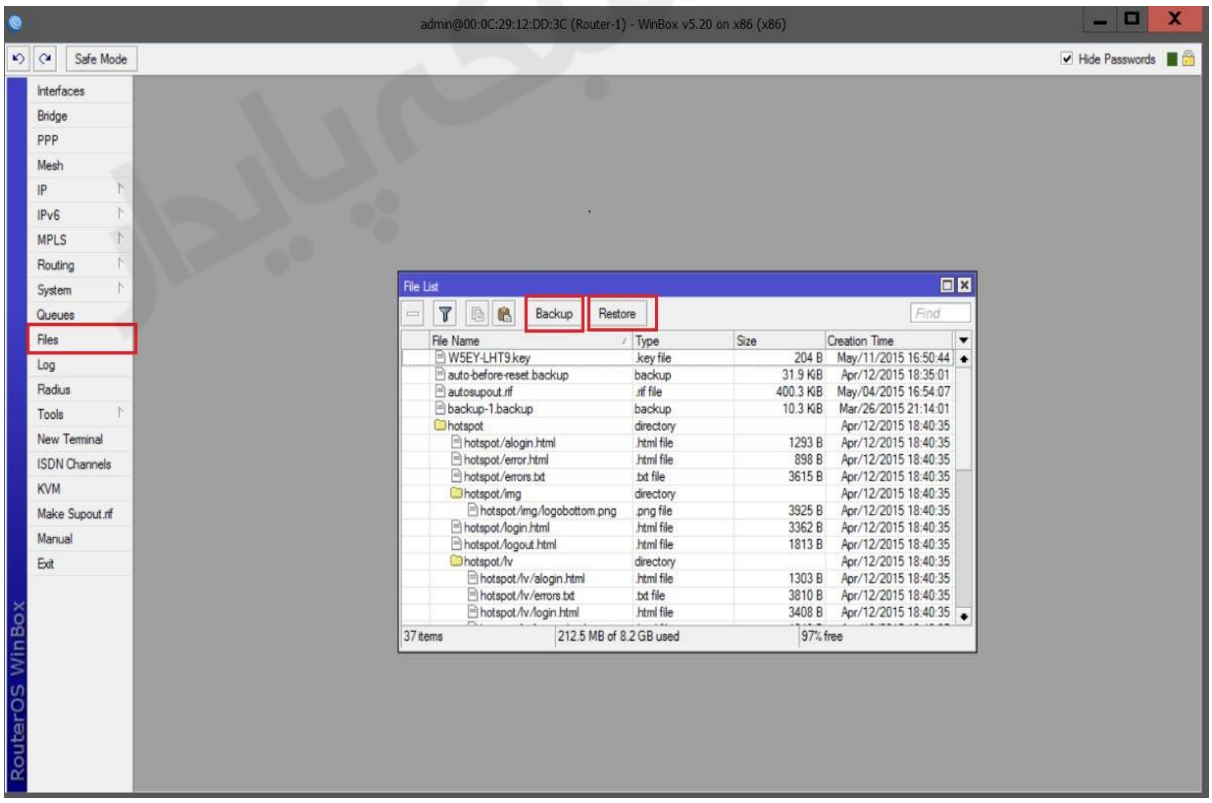
[admin@Router-1] > system reset-configuration



۹) Backup گرفتن و Restore کردن

برای این کار از منوی اصلی گزینه File را انتخاب میکنیم و از پنجره File List دکمه Backup یا Restore را انتخاب میکنیم.

نکته : اگر بخواهیم فایلی که Backup گرفته شده را بر روی هارد دیسک خودمان داشته باشیم فایل Backup گرفته شده را برروی هارد دیسک Drag یا کپی میکنیم.



[admin@Router-1] > system backup save name=backup-10
[admin@Router-1] > system backup load name=backup-10.backup

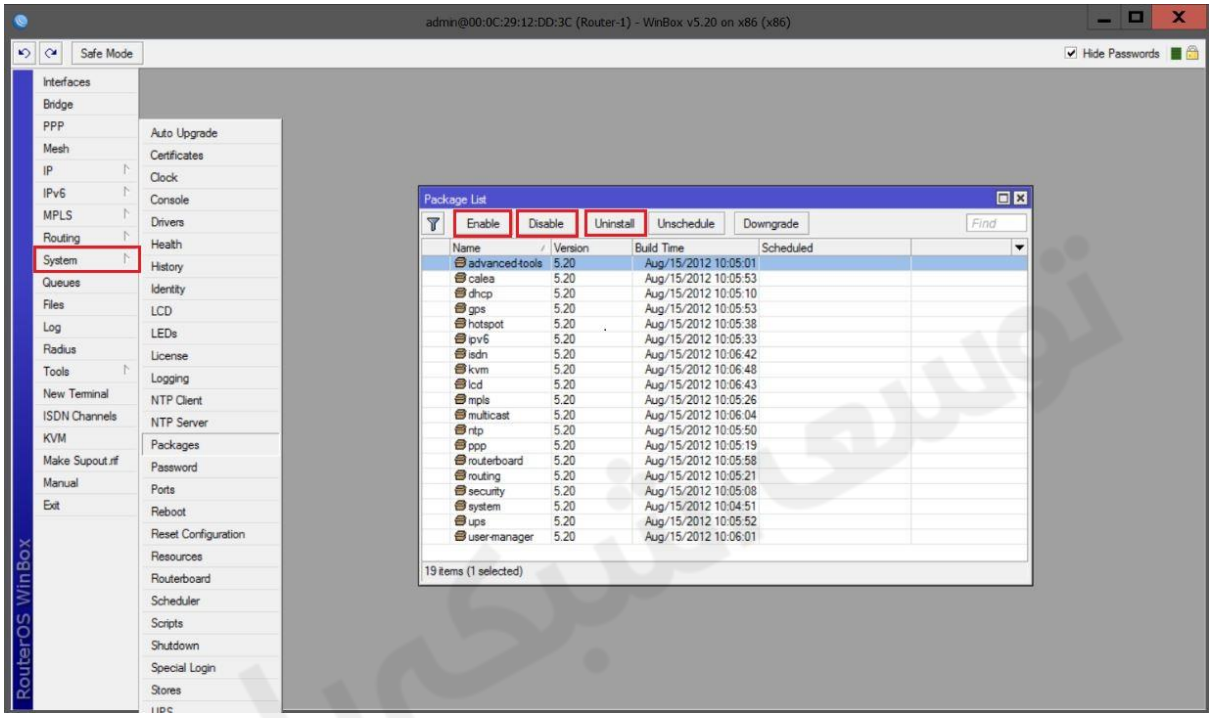
۱۰)**Export** گرفتن از تنظیمات و **Import** کردن آن بر روی روتر دیگر

```
[admin@Router-1] > export file=config-11
[admin@Router-1] > import file-name=config-11.rsc
```

۱۱)نصب و **Upgrade** کردن **Package** :

Package ها را از سایت میکروتیک دانلود می کنیم و از منو اصلی **File** را انتخاب کرده و **Package** ها را در این قسمت کپی می کنیم بعد از این کار از منوی اصلی گزینه **System** و از زیر منوی باز شده **Reboot** را انتخاب میکنیم تا سیستم ریستارت شود.

برای دیدن **package** هایی که نصب کردیم از منوی اصلی گزینه **System** و از زیر منو باز شده **Package** را انتخاب میکنیم.در این قسمت ما می توانیم **Package** ی را **Enable** یا **Disable** و یا **Uninstall** کنیم.



فصل سوم : مفاهیم مسیریابی در میکروتیک

آشنایی با مفهوم Routing

مسیریابی یا **Routing** یکی از مهمترین ویژگی های مورد نیاز در یک شبکه به منظور ارتباط با سایر شبکه ها است.در صورتی که امکان مسیریابی پروتکل ها وجود نداشته باشد کامپیوترها قادر به مبادله داده نخواهند بود.

تعریف **Routing** : از **Routing** به منظور دریافت یک بسته ی اطلاعاتی(**Packet**) از یک دستگاه و ارسال آن از طریق شبکه برای دستگاهی دیگر و بر روی شبکه ای متفاوت استفاده می گردد.در صورتی که شبکه شما دارای روتر نباشد امکان مسیریابی داده بین شبکه شما و سایر شبکه ها را نخواهد داشت.

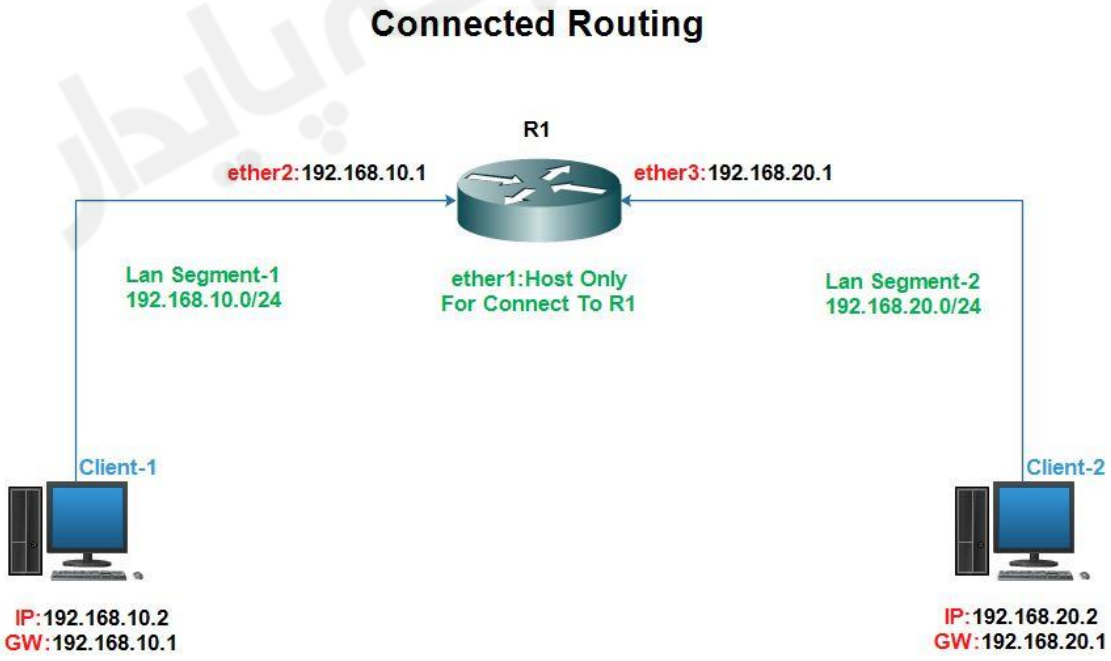
به طور کلی دو روش مسیریابی وجود دارد :

- ✓ **Static Route**
- ✓ **Dynamic Route**

در مسیریابی **Static** یا ایستا بسته های اطلاعاتی فقط از همان مسیری که توسط مدیر شبکه تعریف شده اند راهشان برای رسیدن به مقصد را پیدا می کنند و راه دیگری را نمی توانند پیدا کنند.

در مسیریابی **Dynamic** یا پویا بسته اطلاعاتی ما همیشه از یک مسیر مشخص برای رسیدن به مقصد استفاده نمی کنند بعضا براساس پروتکل های مورد استفاده در آنها بهترین مسیر برای رسیدن به مقصد پیدا می شود و کانال مربوطه برای رسیدن بسته ی اطلاعاتی به مقصد نیز باز می شود.در ساده ترین تعریف ، اگر روترهای موجود در میسر مبدا به مقصد تشخیص دهند که مسیر بهترین برای رسیدن بسته اطلاعاتی به مقصد وجود دارد قطعا بسته اطلاعاتی خود را از این مسیر عبور می دهند ،معمولا این فرایند با پیدا کردن کوتاه ترین مسیر بین مبدا و مقصد انجام می شود.فرایند پیدا کردن بهترین مسیر در پروتکل های مسیریابی مختلف بصورت متفاوتی انجام می شود برخی از آنها از ملاک **Hop Count** برای پیدا کردن این مسیر استفاده می کنند و برخی فقط سریعترین مسیر را پیدا می کنند.روترهایی که در یک شبکه وجود دارند و از یک پروتکل مسیریابی **Dynamic** استفاده می کنند اطلاعات موجود در **Routing Table** های خود را با همدیگر به اشتراک می گذارند تا همیشه بروز باقی بمانند.

سناریو ۱ : هدف این سناریو برقراری ارتباط بین دو شبکه با **Subnet** های متفاوت می باشد.

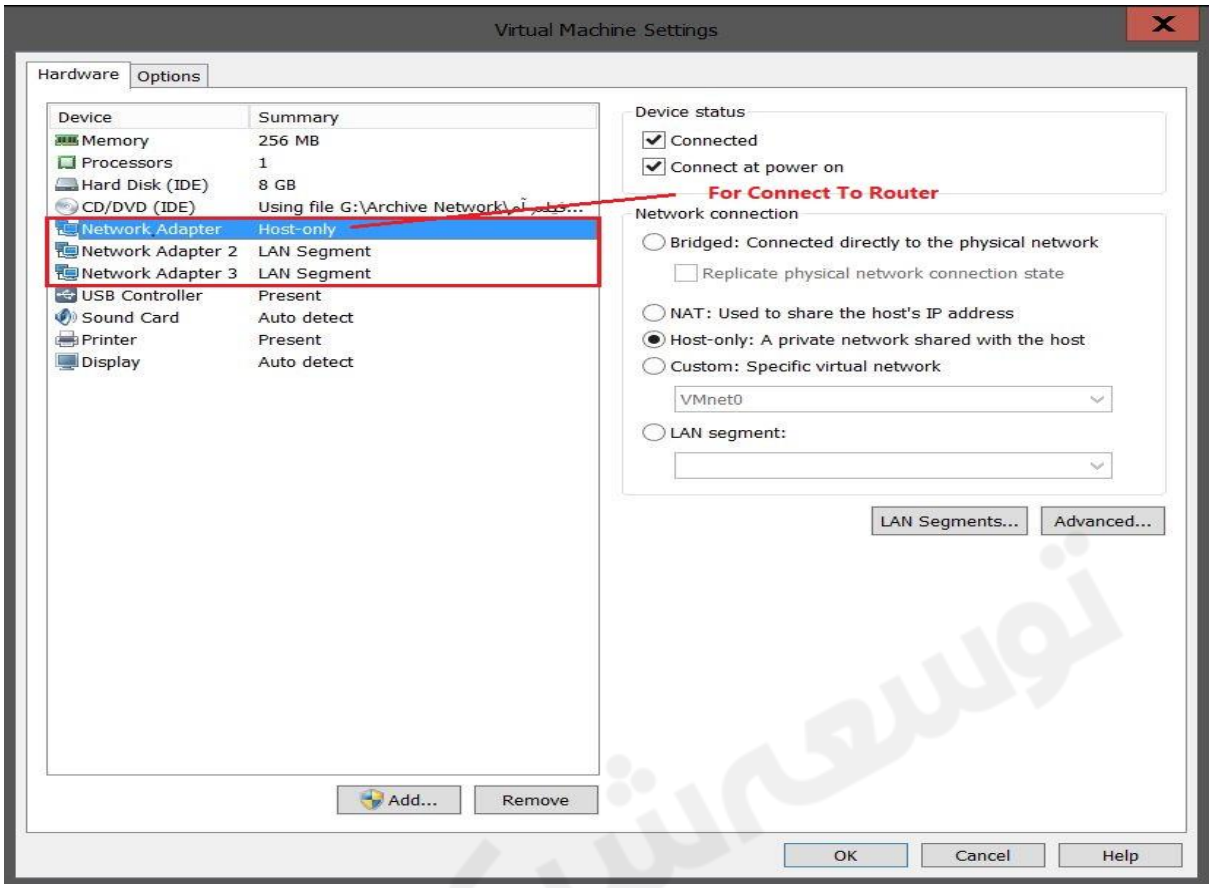


برای پیاده سازی این سناریو :

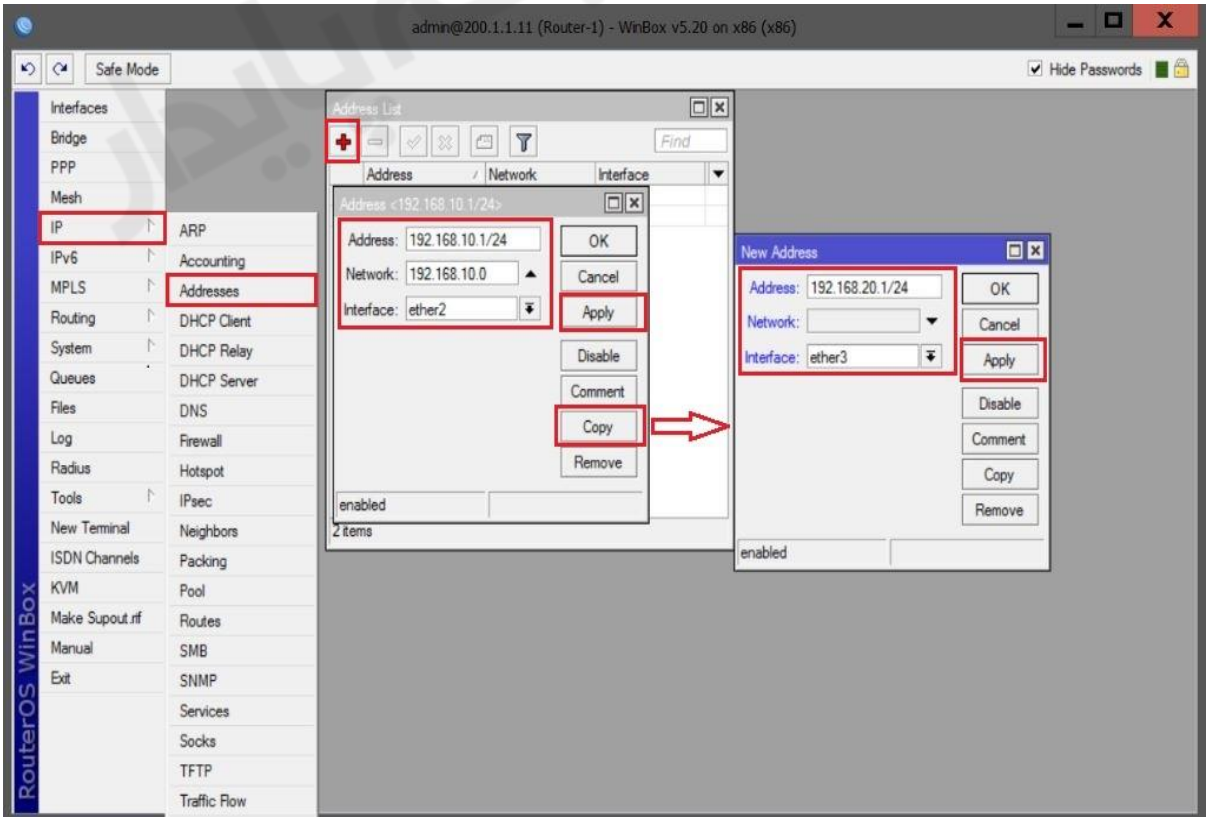
- ➢ یک روتر میکروتیک به عنوان مسیریاب در نظر گرفته شده است.
- ➢ دو سیستم کلاینت به عنوان کلاینت های موجود در هر شبکه راه اندازی می کنیم.

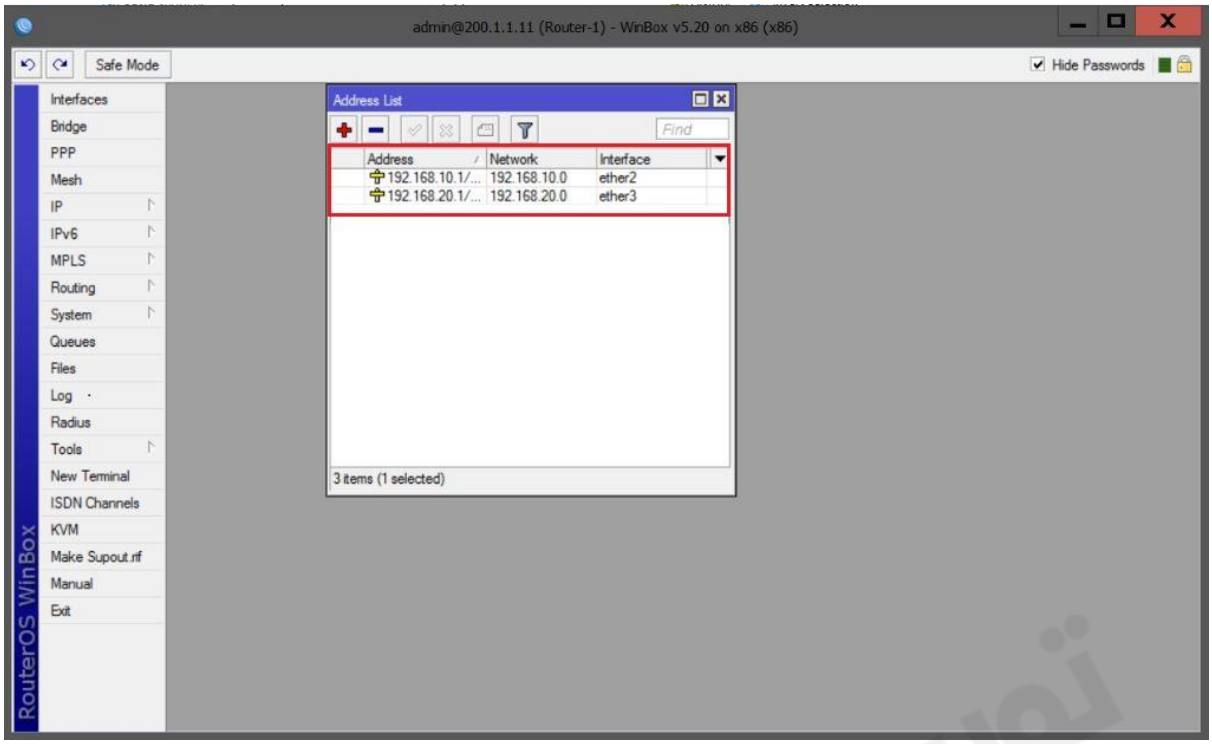
تنظیمات در روتر میکروتیک(R1):

اضافه کردن کارت شبکه به روتر در VmaWare و قرار دادن آنها در Lan Segment های مختلف



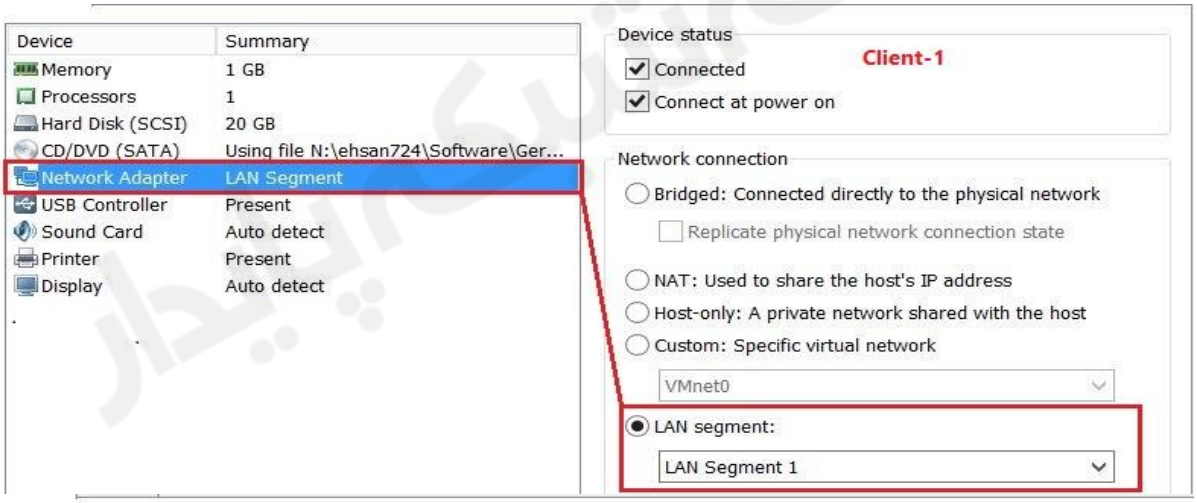
انتساب IP برای کارت های شبکه روتر R1 :

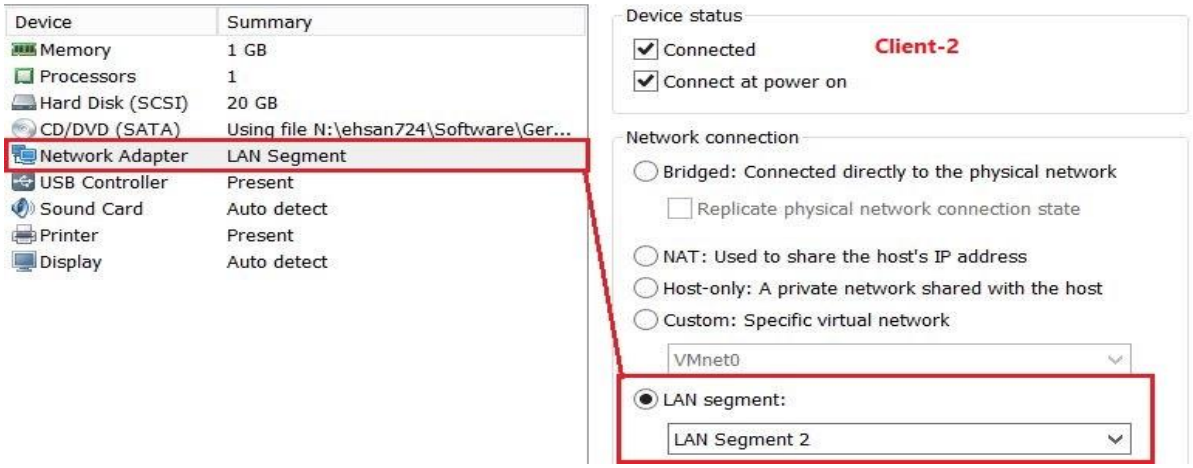




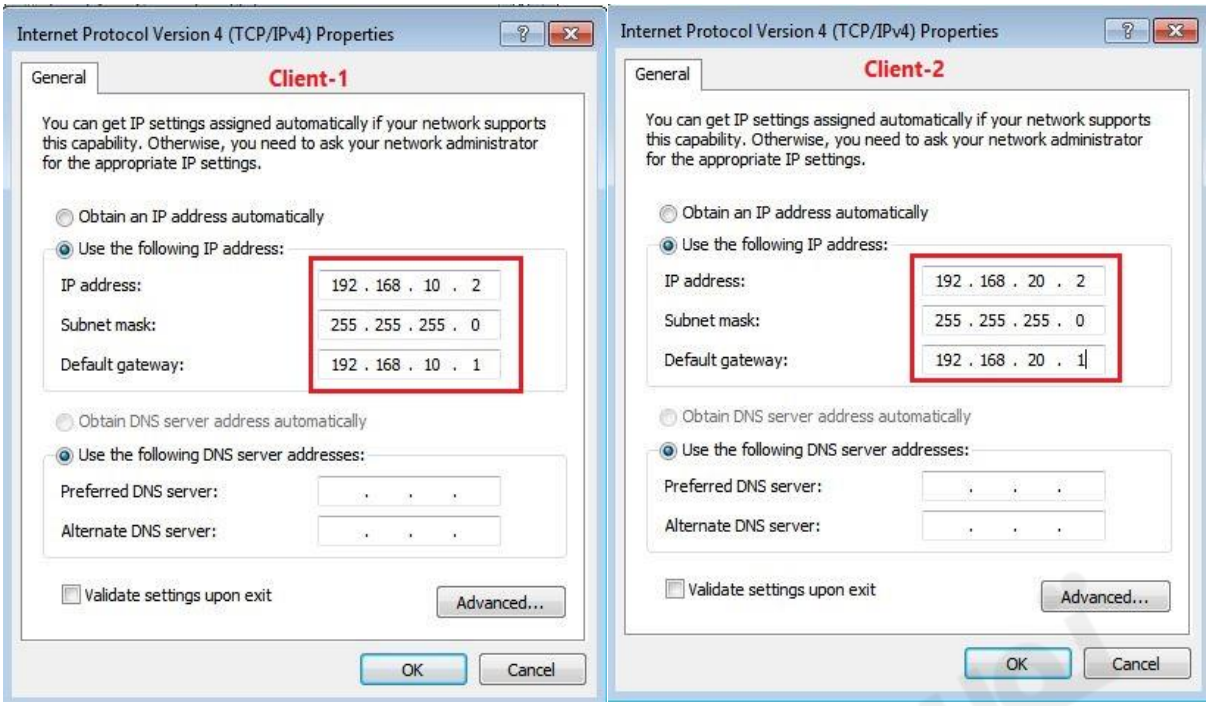
تنظیمات در سیستم های کلاینت :

کلاینت ۱ را در Lan Segment-1 و کلاینت ۲ را در Lan Segment-2 قرار میدهیم.سپس طبق سناریو برای آنها IP تنظیم میکنیم.





تنظیم **IP** برای کلاینت ها :



با این تنظیمات باید ارتباط بین کلاینت ها برقرار باشد برای تست اینکه ارتباط برقرار است از کلاینت ها به یکدیگر **Ping** میزنیم

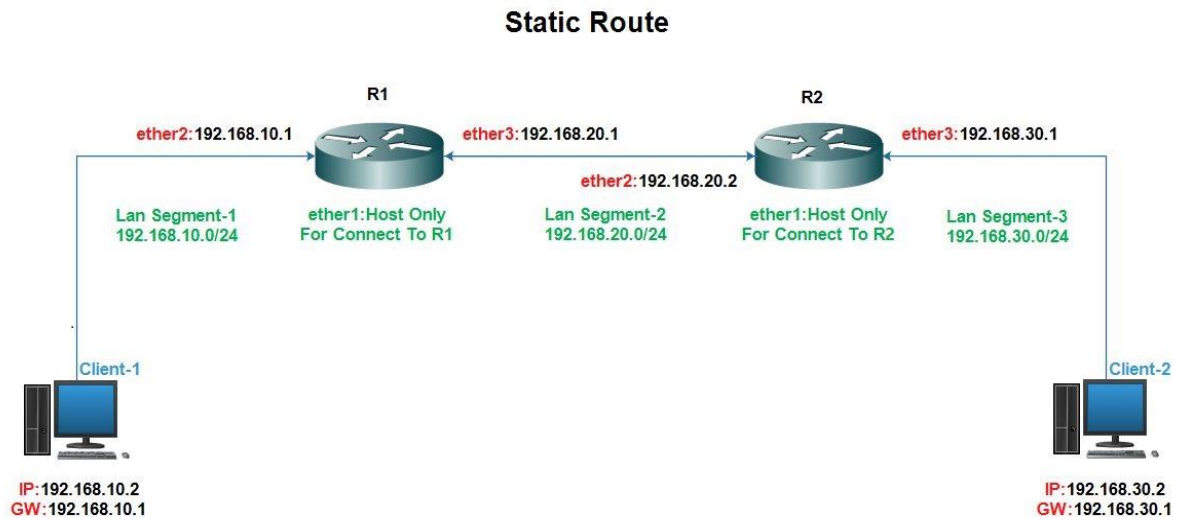
کلاینت ۱ به کلاینت ۲:

```
C:\Users\LanSegmet1>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:
Reply from 192.168.20.2: bytes=32 time=1ms TTL=127
Reply from 192.168.20.2: bytes=32 time=1ms TTL=127
Reply from 192.168.20.2: bytes=32 time=5ms TTL=127
Reply from 192.168.20.2: bytes=32 time=1ms TTL=127
```

کلاینت ۲ به کلاینت ۱:

```
C:\Users\LanSegment>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
```

سناریو ۲ : هدف این سناریو برقراری ارتباط بین دو شبکه با **Subnet** های متفاوت با استفاده از **Static Route** می باشد.

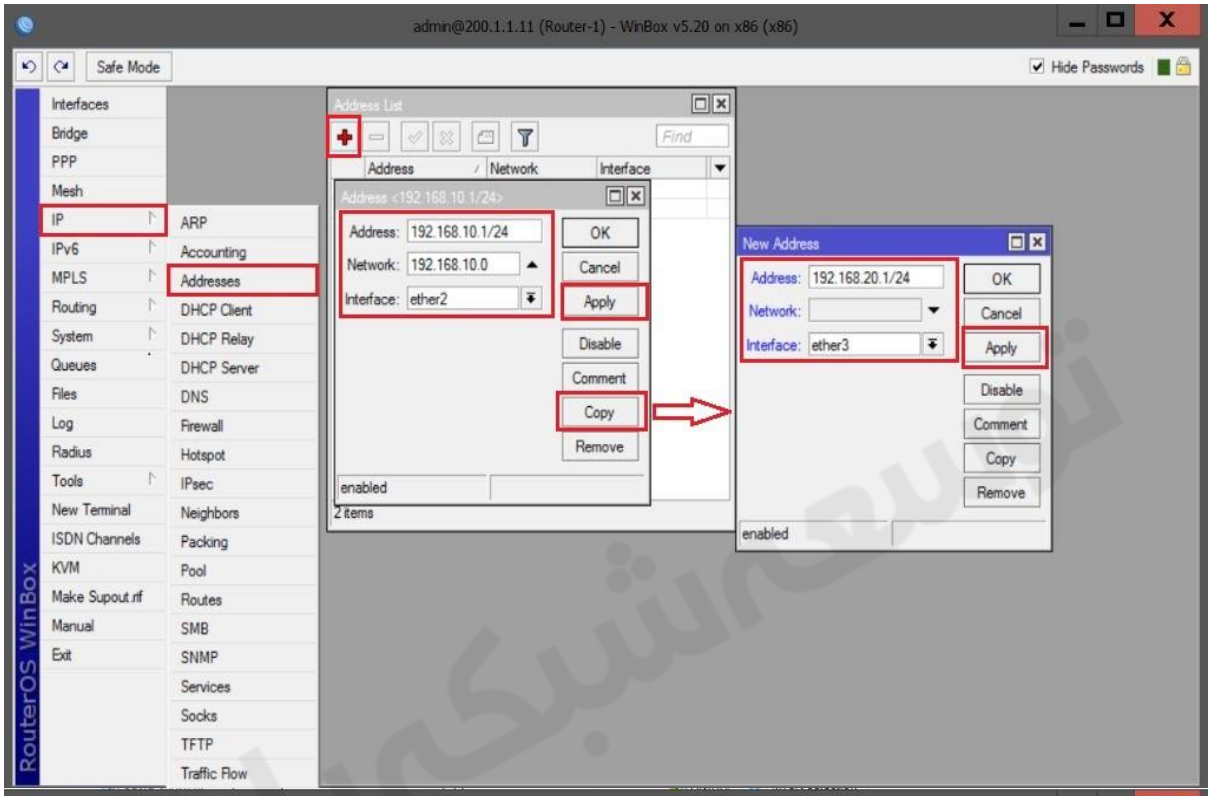


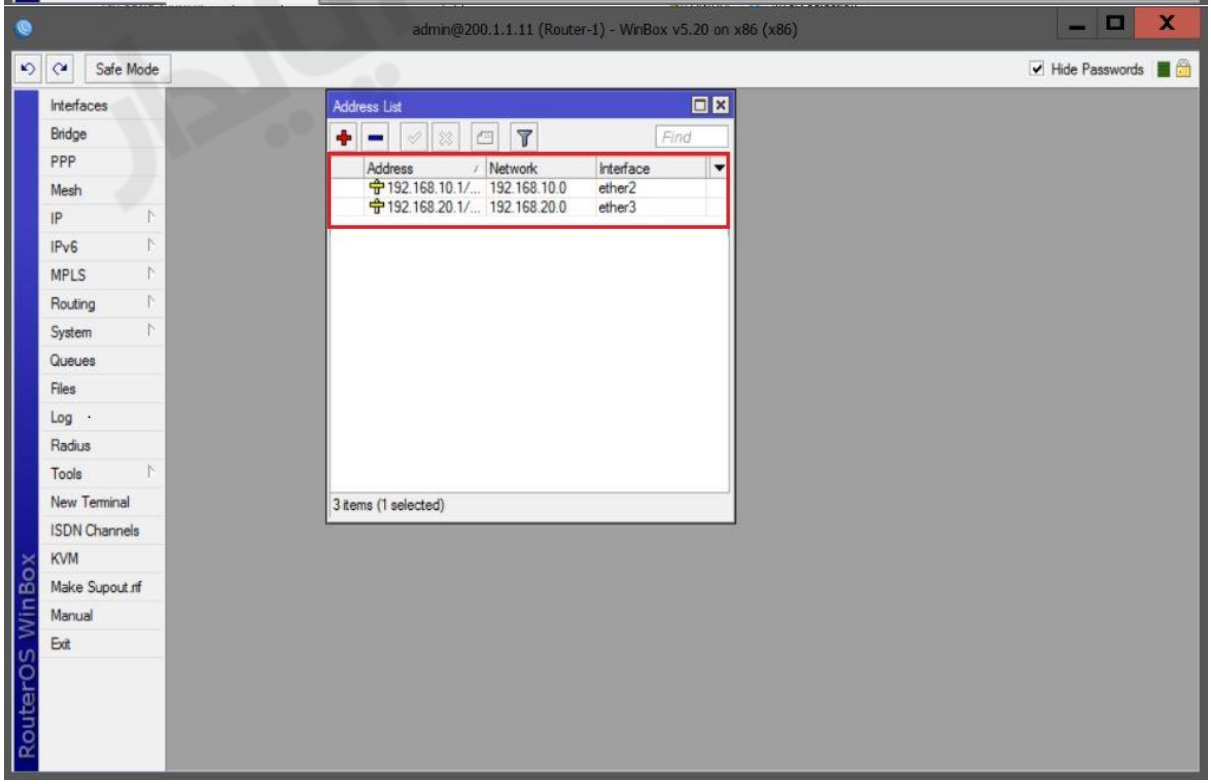
برای پیاده سازی این سناریو :

- **دو روتر میکروتیک به عنوان مسیریاب در نظر گرفته شده است.**
- **دو سیستم کلاینت به عنوان کلاینت های موجود در هر شبکه راه اندازی می کنیم.**

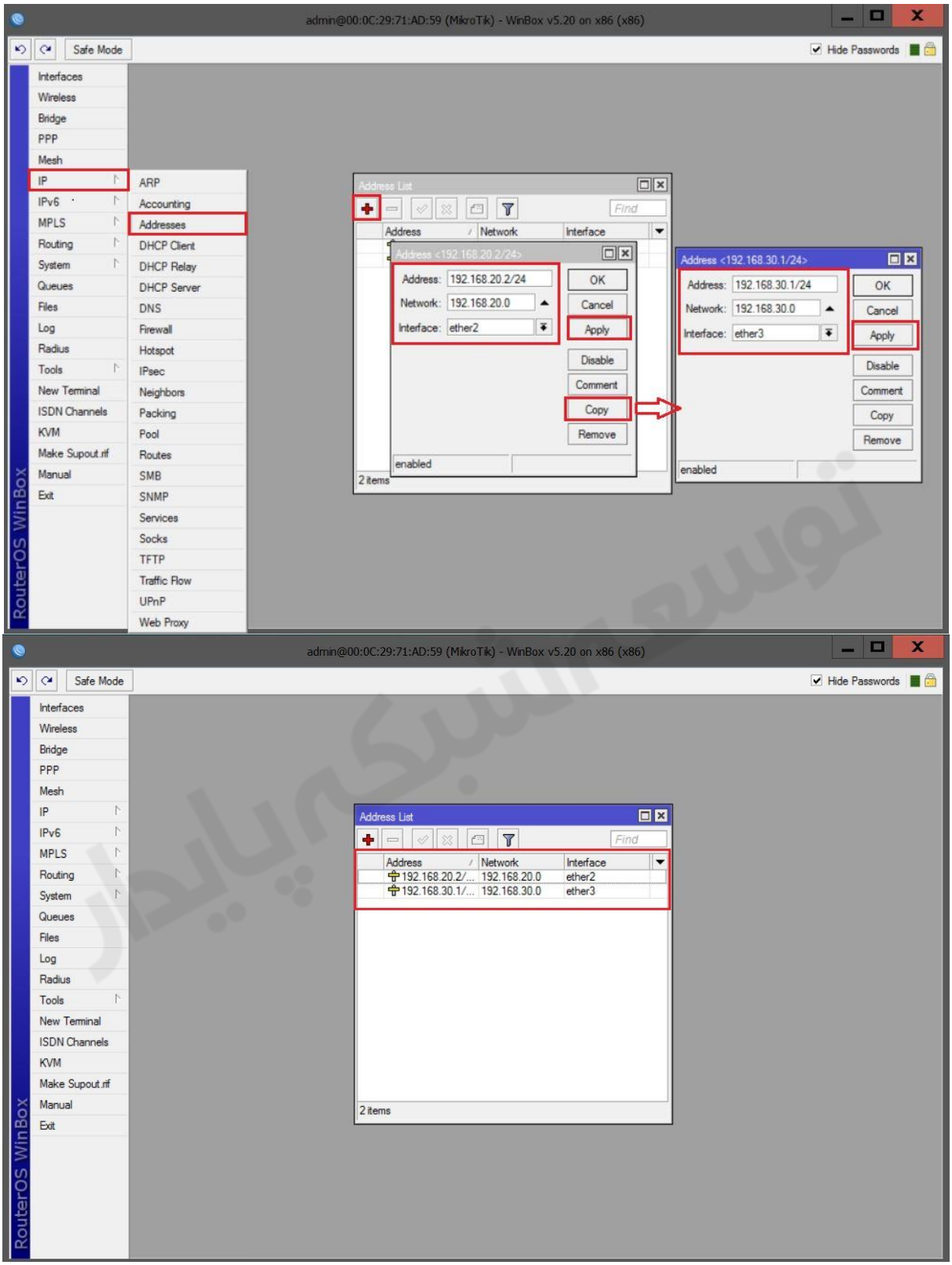
برای پیاده سازی این سناریو طبق شکل بالا روترها و کلاینت ها را بر روی VmWare راه اندازی می کنیم و کارت شبکه های آنها را در Lan Segment های گفته شده قرار می دهیم و طبق شکل بالا به هرکدام از دستگاه ها IP هایی که مشخص کردیم را برای آنها تنظیم می کنیم.

انتساب IP برای کارت های شبکه روتر R1 :





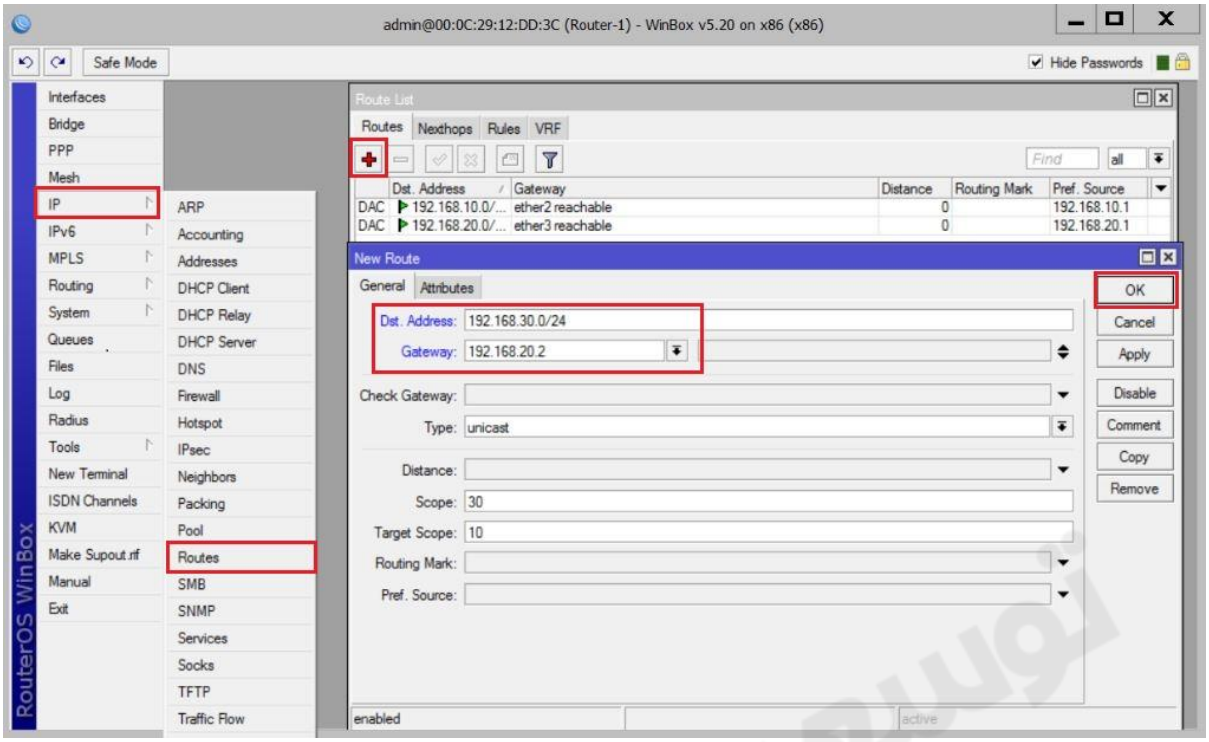
انتساب IP برای کارت های شبکه روتر R2 :



تا اینجای کار ارتباط بین دو روتر برقرار است برای تست برقرار بودن این ارتباط می توانید از منوی اصلی گزینه **Tools** و از زیر منوی باز شده **Ping** را انتخاب کنید و **IP** روتر مقابل را وارد می کنید.برای اینکه ارتباط بین دو شبکه **Lan** را برقرار کنید باید بر روی روترها **Static Route** و یا **Dynamic Route** ایجاد کنید.ما در این سناریو از **Static Route** استفاده می کنیم و در ادامه به بررسی **Dynamic Route** نیز خواهیم پرداخت.

ایجاد Static Route بر روی روتر R1 :

برای این کار از منوی اصلی گزینه IP و از زیر منوی باز شده Routes را انتخاب می کنیم.

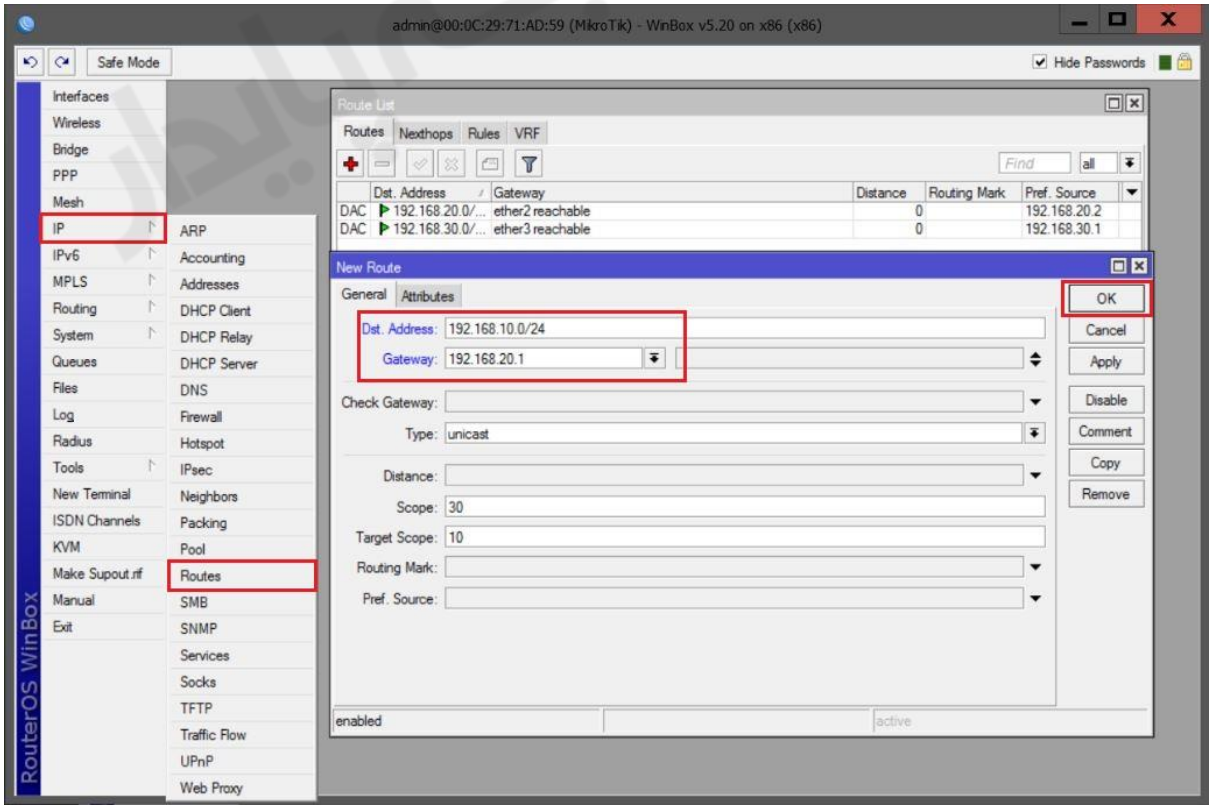


Dst. Address : در این قسمت IP زیر شبکه ایی که قصد Route به آن را دارید وارد می کنید.

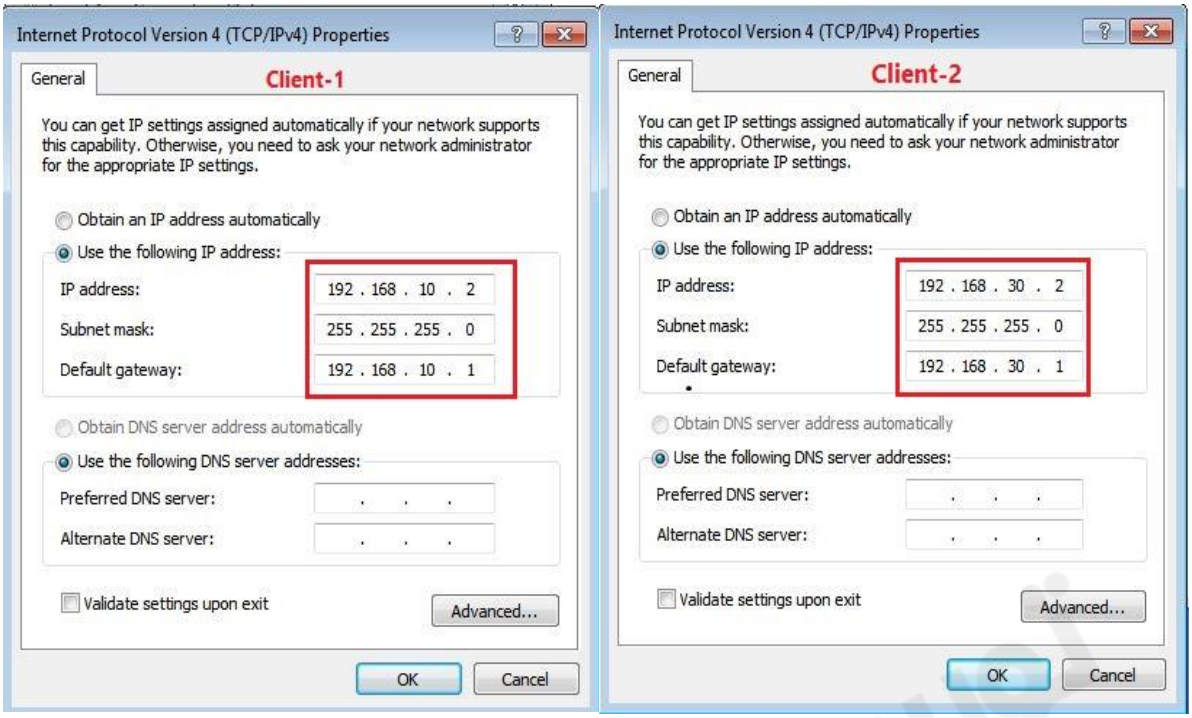
Gateway : در این قسمت مقصد بعدی که بسته ها به آنجا ارسال خواهند شد را می نویسیم.

نکته : چنانچه زیر شبکه مورد نظر شما با چندین روتر در ارتباط باشد تنها IP روتر مجاور را در Gateway وارد می کنیم.

ایجاد Static Route بر روی روتر R1 :



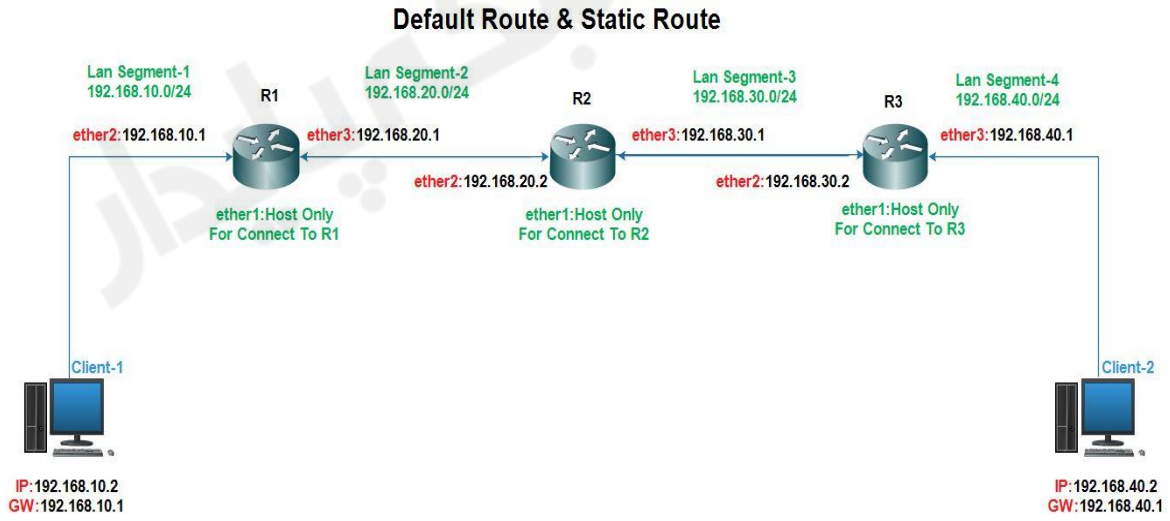
تنظیم **IP** برای کلاینت ها :



با این تنظیمات باید ارتباط بین کلاینت ها برقرار باشد برای تست اینکه ارتباط برقرار است از کلاینت ها به یکدیگر **Ping** میزنیم.

سناریو ۳ :

هدف این سناریو برقراری ارتباط بین دو شبکه با **Subnet** های متفاوت با استفاده از **Default Route & Static Route** می باشد.

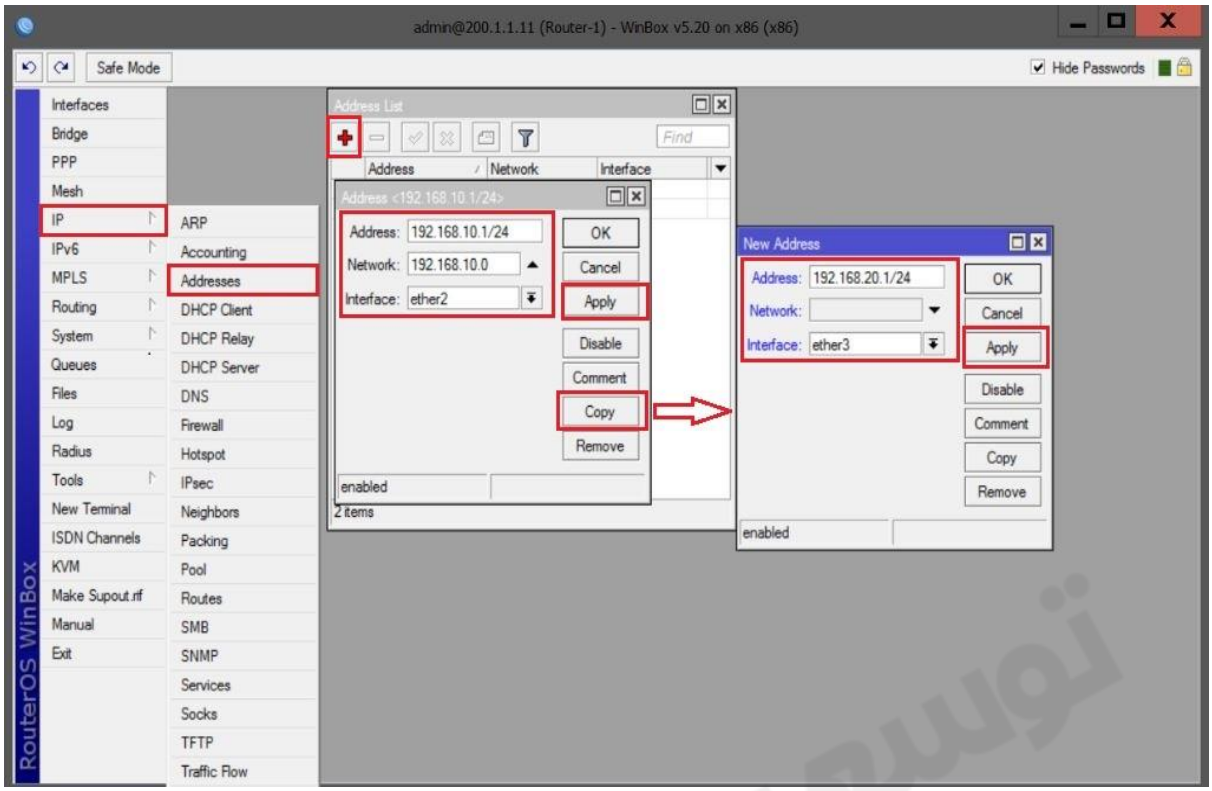


برای پیاده سازی این سناریو :

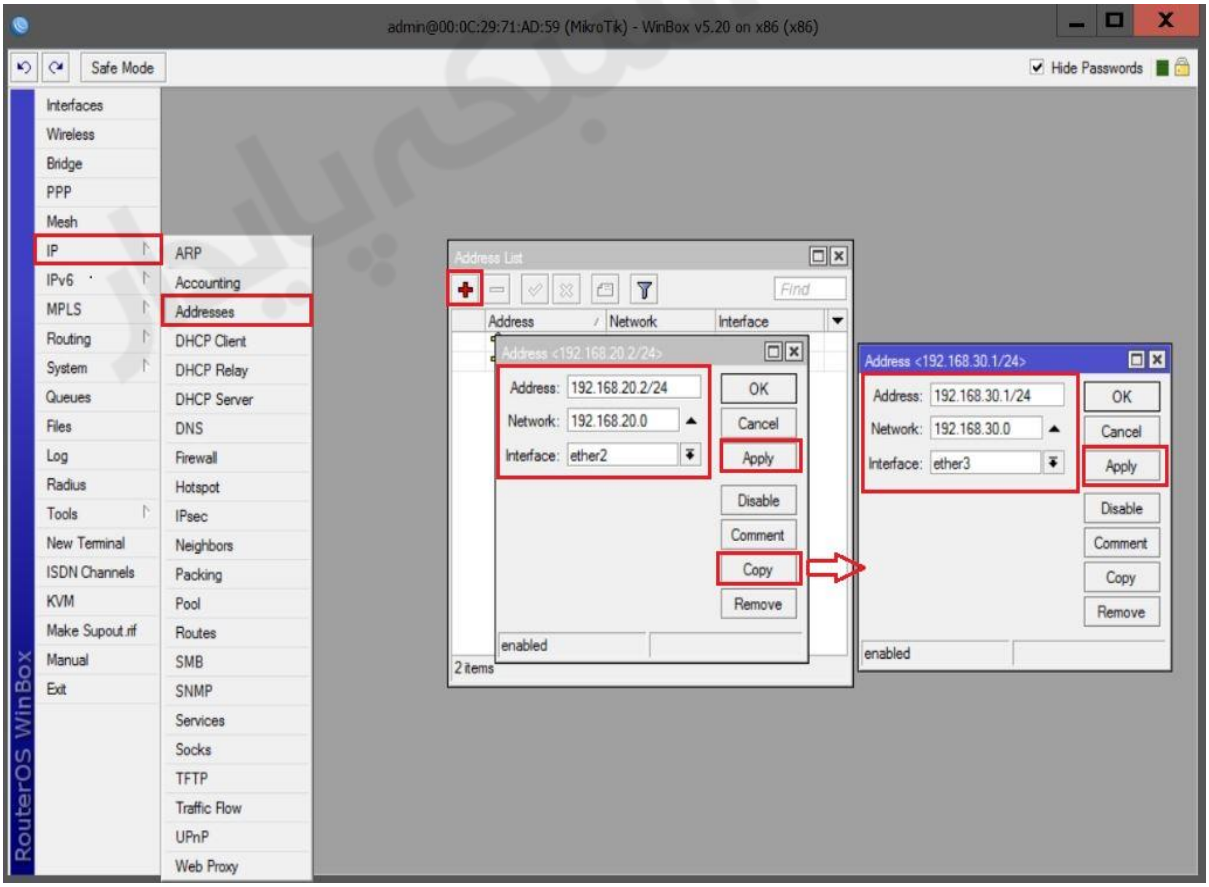
- سه روتر میکروتیک به عنوان مسیریاب در نظر گرفته شده است.
- دو سیستم کلاینت به عنوان کلاینت های موجود در هر شبکه راه اندازی می کنیم.

برای پیاده سازی این سناریو طبق شکل بالا روترها و کلاینت ها را بر روی **VmWare** راه اندازی می کنیم و کارت شبکه های آنها را در **Lan Segment** های گفته شده قرار می دهیم و طبق شکل بالا به هرکدام از دستگاه ها **IP** هایی که مشخص کردیم را برای آنها تنظیم می کنیم.

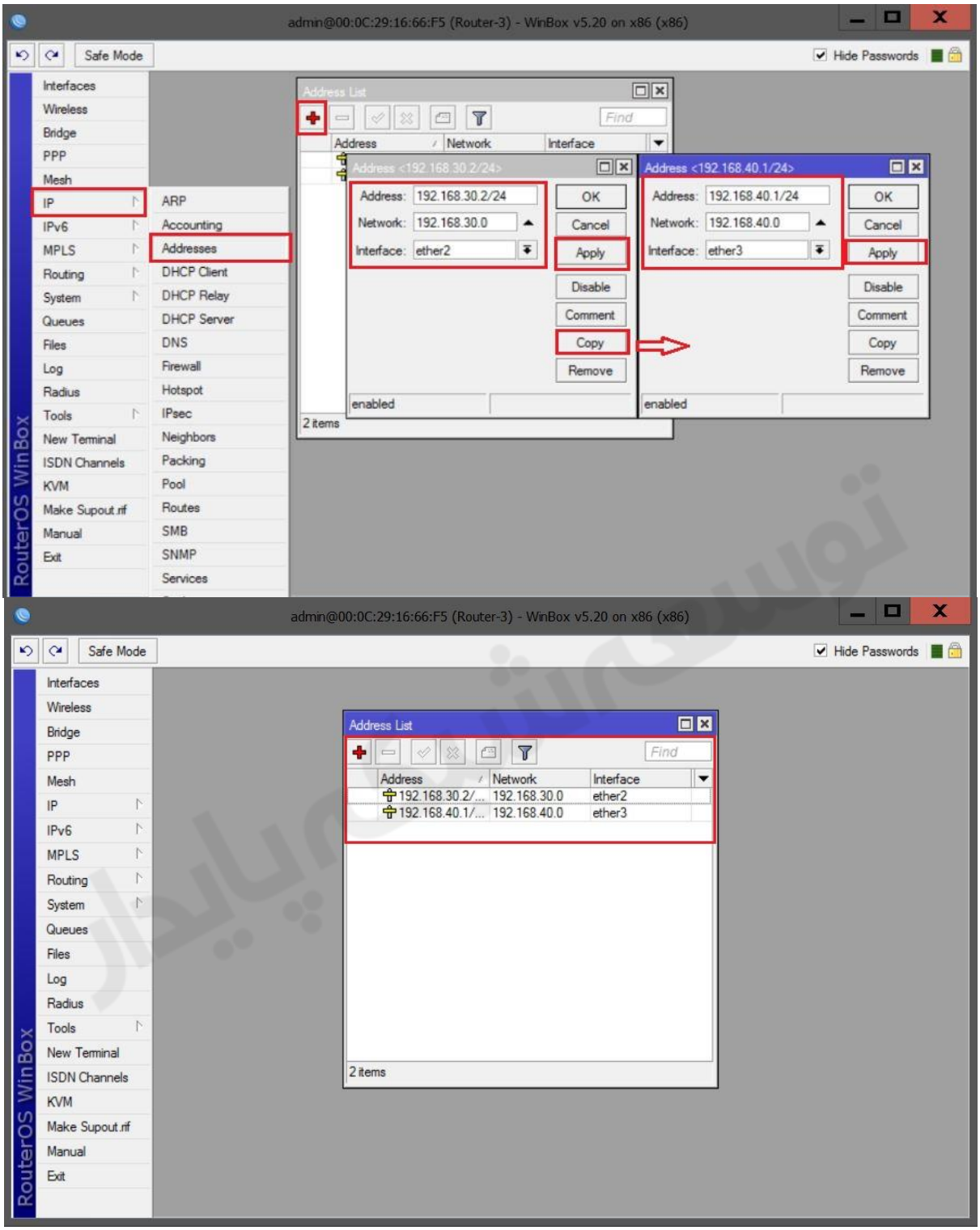
انتساب IP برای کارت های شبکه روتر R1 :



انتساب IP برای کارت های شبکه روتر R2 :



انتساب IP برای کارت های شبکه روتر R3 :

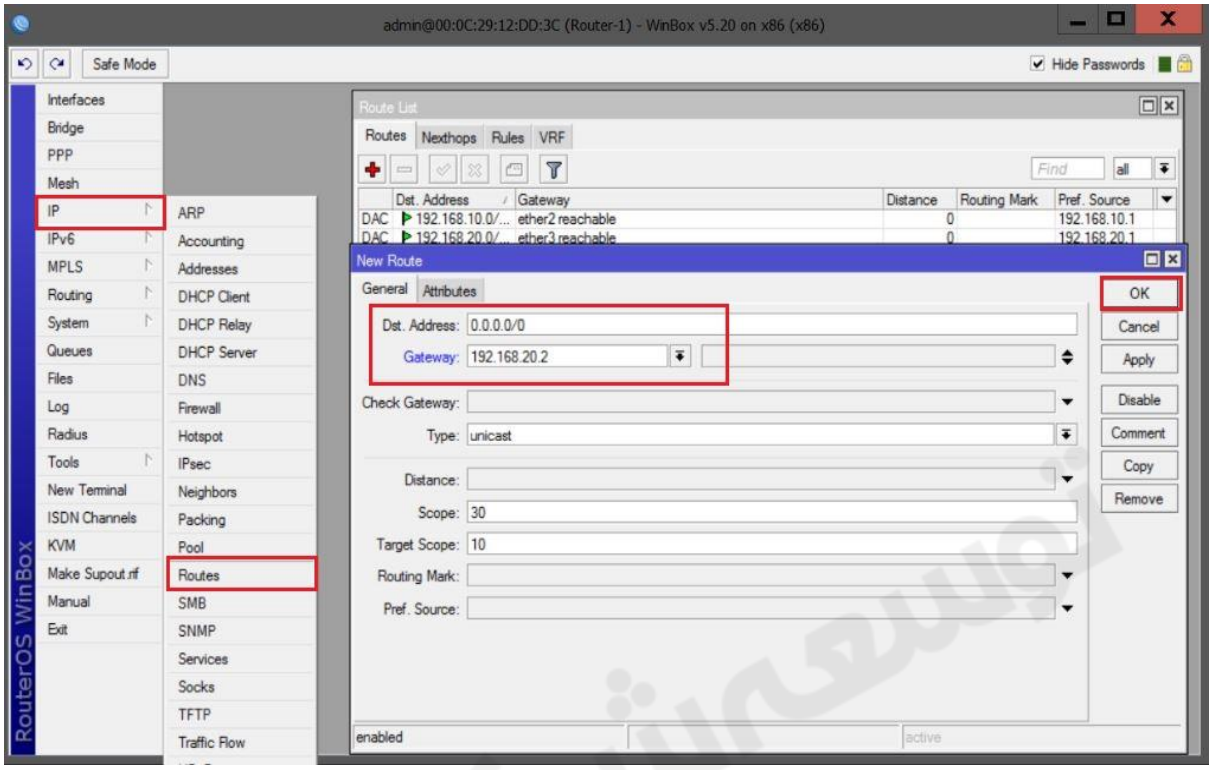


- تا اینجای کار با این تنظیمات ارتباط روتر **R2** با دو روتر دیگر برقرار است چون به صورت مستقیم به دو روتر دیگر وصل است ولی با دو شبکه **Lan** ارتباطی ندارد.
- روتر **R1** با شبکه ای که کلاینت ۱ در آن است و با روتر **R2** ارتباطاتش برقرار است.
- روتر **R3** با شبکه ای که کلاینت **2** در آن است و با روتر **R2** ارتباطاتش برقرار است.

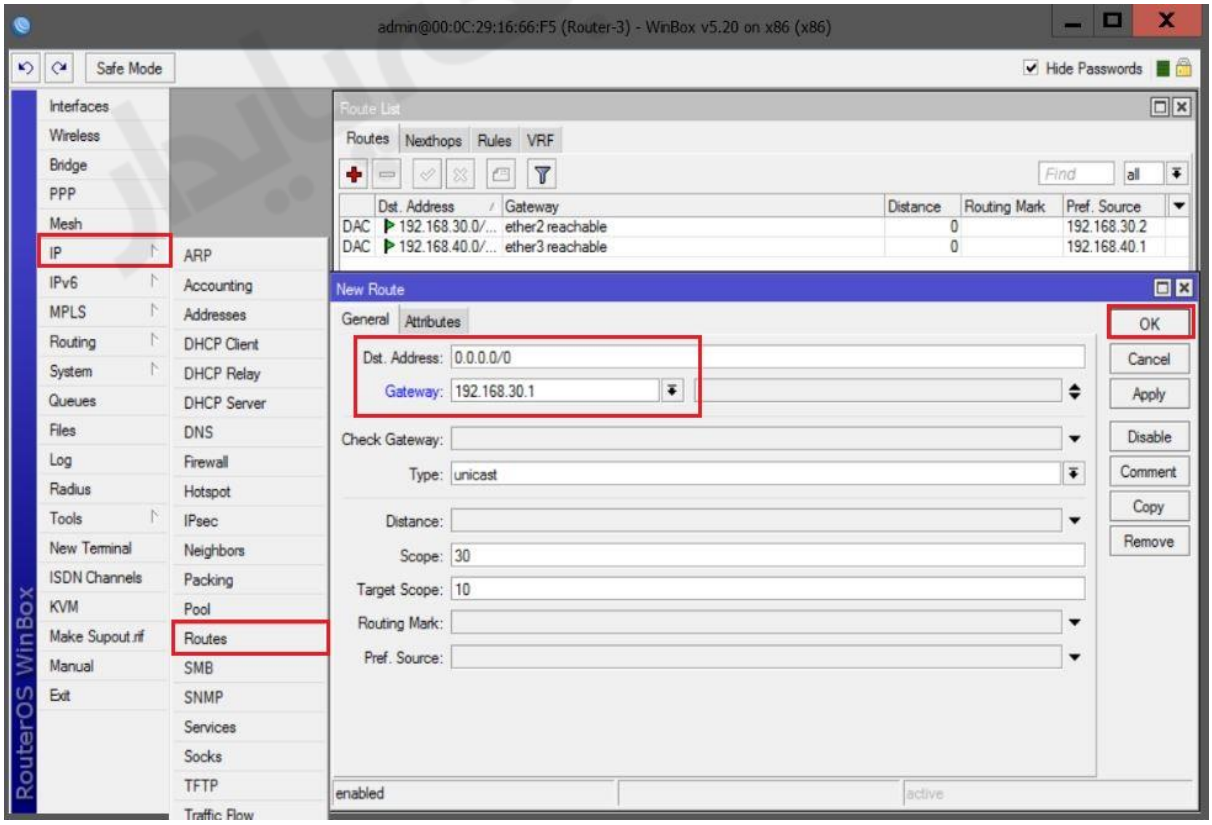
برای اینکه تمامی ارتباطات برقرار باشد باید تنظیمات زیر را بر روی روتر انجام دهیم :

تعریف Default Route در روتر R1 :

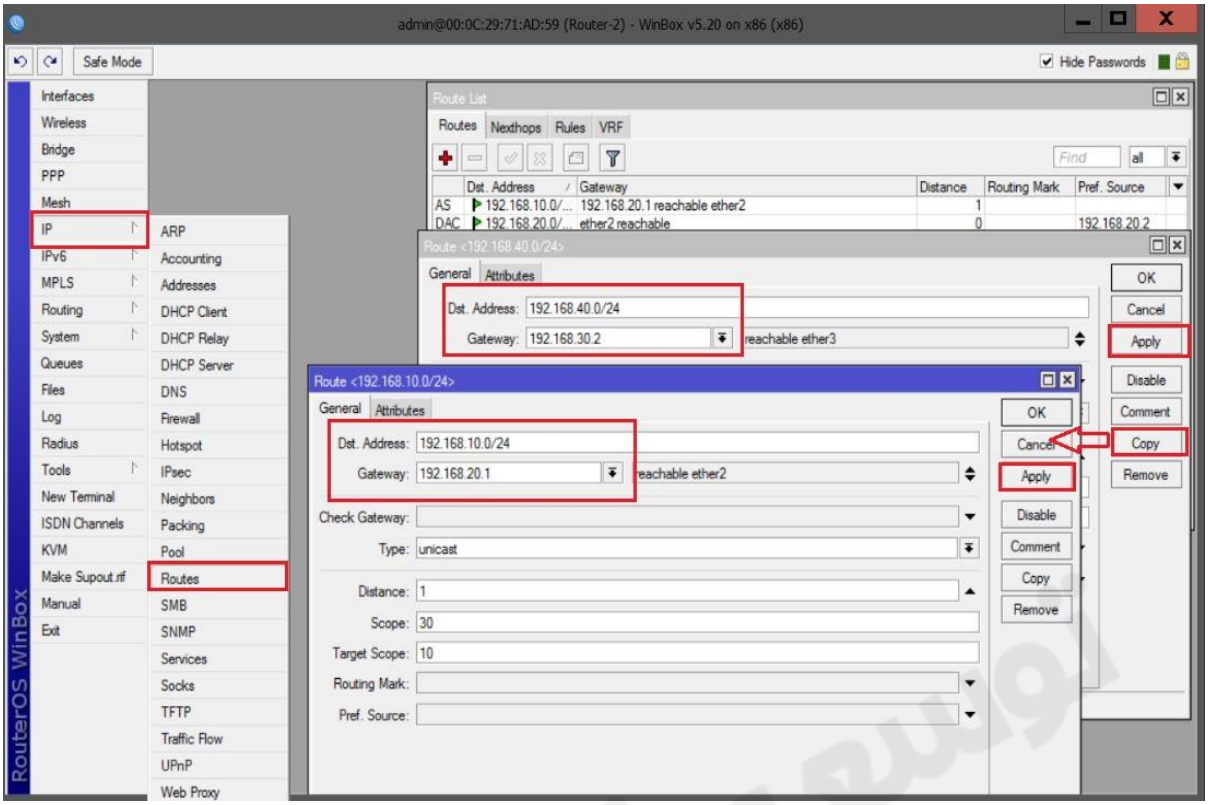
Default Route یا مسیر پیش فرض همان اصطلاح چهار صفر میباشد (0.0.0.0/0) که یک نوع خاص از مسیریابی پویا می باشد.در مسیر پیش فرض یک مسیر را برای روتر مشخص می کنید تا زمانی که یک مقصد را شناسایی نکرد در خواست مورد نظر را به مسیر پیش فرض که برایش تعریف شده ارسال کند.



تعریف Default Route در روتر R3 :

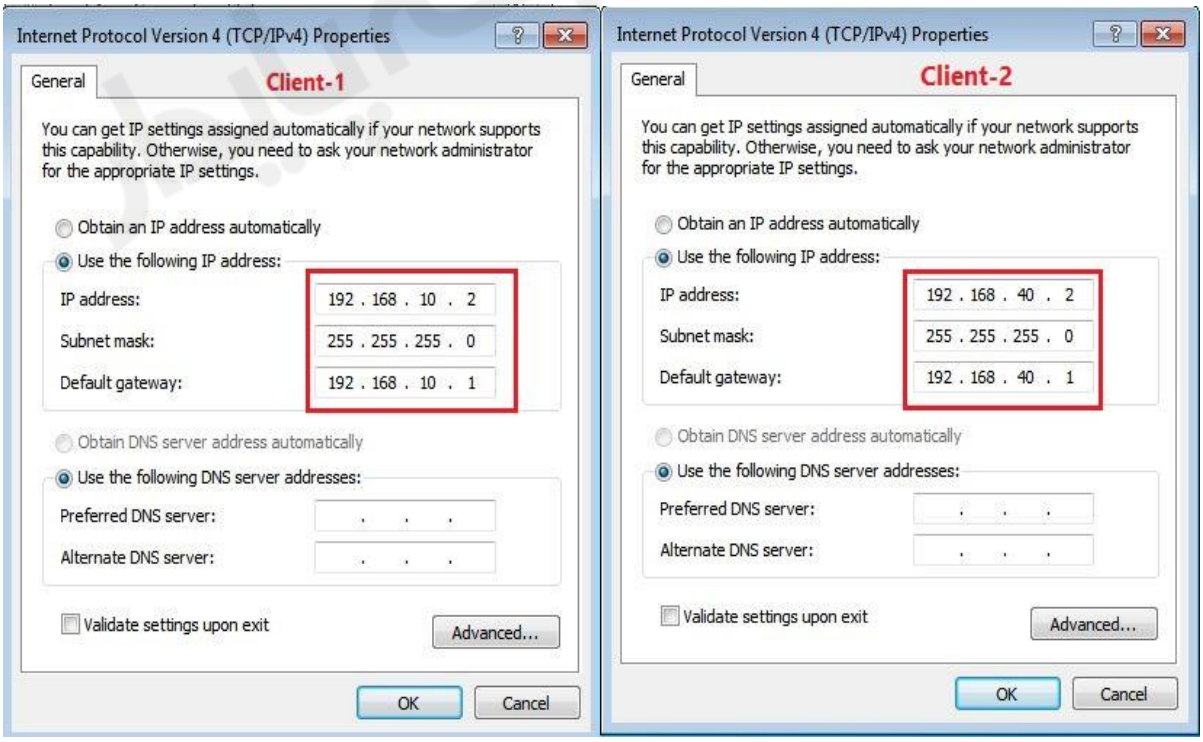


ایجاد **Static Route** بر روی روتر **R2** :



نکته : دلیل اینکه برای روتر **R2** ، **Static Route** تعریف کردیم این بود که **Packet** های ارسالی از سمت دو روتر مختلف بود و امکان داشت هر دفعه **Packet** به یکی از روترها تحویل داده می شد.

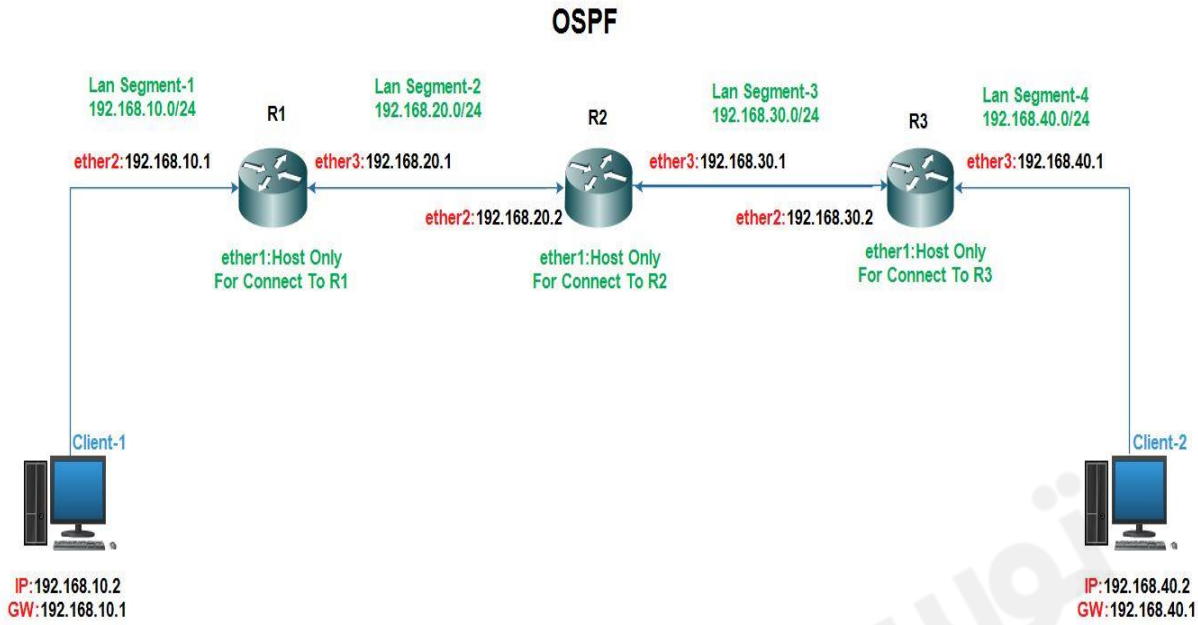
تنظیمات **IP** در کلاینت :



با این تنظیمات باید ارتباط بین کلاینت ها برقرار باشد برای تست اینکه ارتباط برقرار است از کلاینت ها به یکدیگر **Ping** میزنیم.

سناریو ۴ :

هدف این سناریو برقراری ارتباط بین دو شبکه با **Subnet** های متفاوت با استفاده از **Dynamic Route** و پروتکل **OSPF** می باشد.

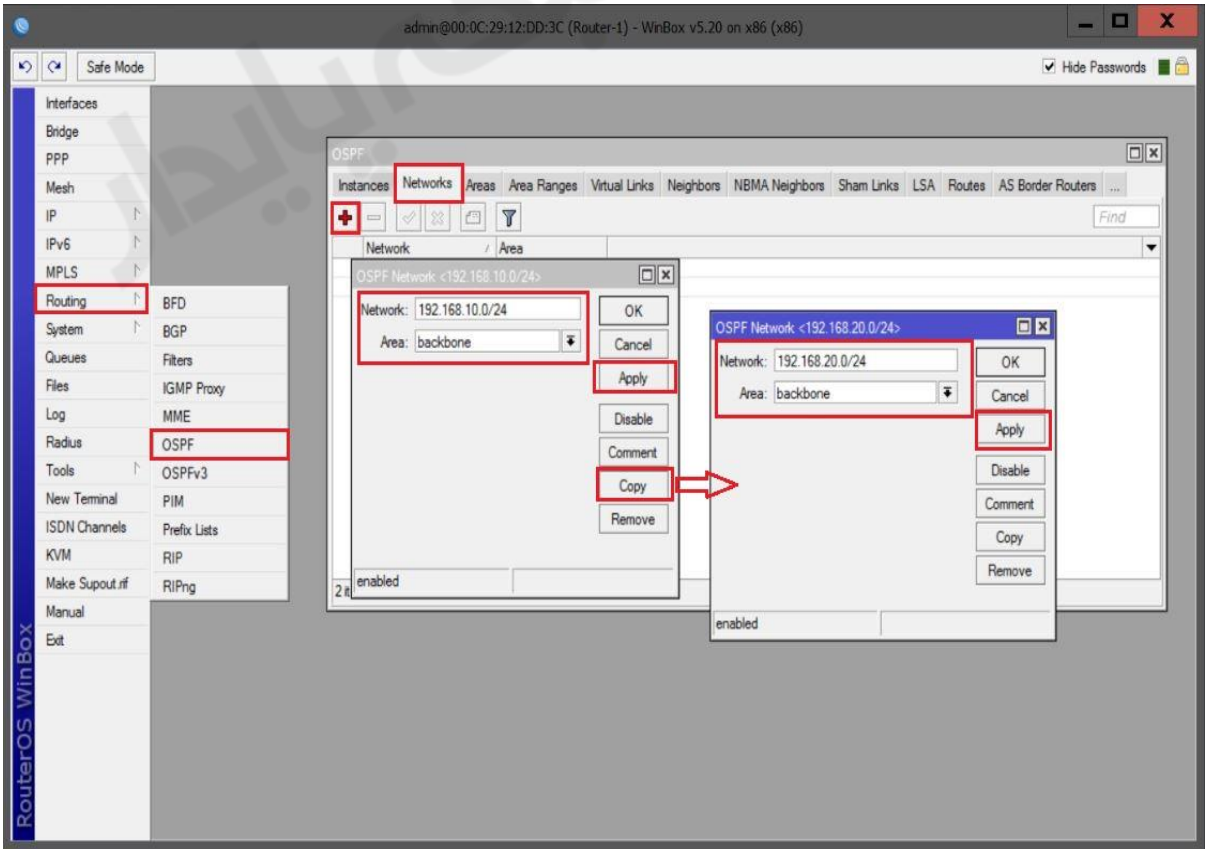


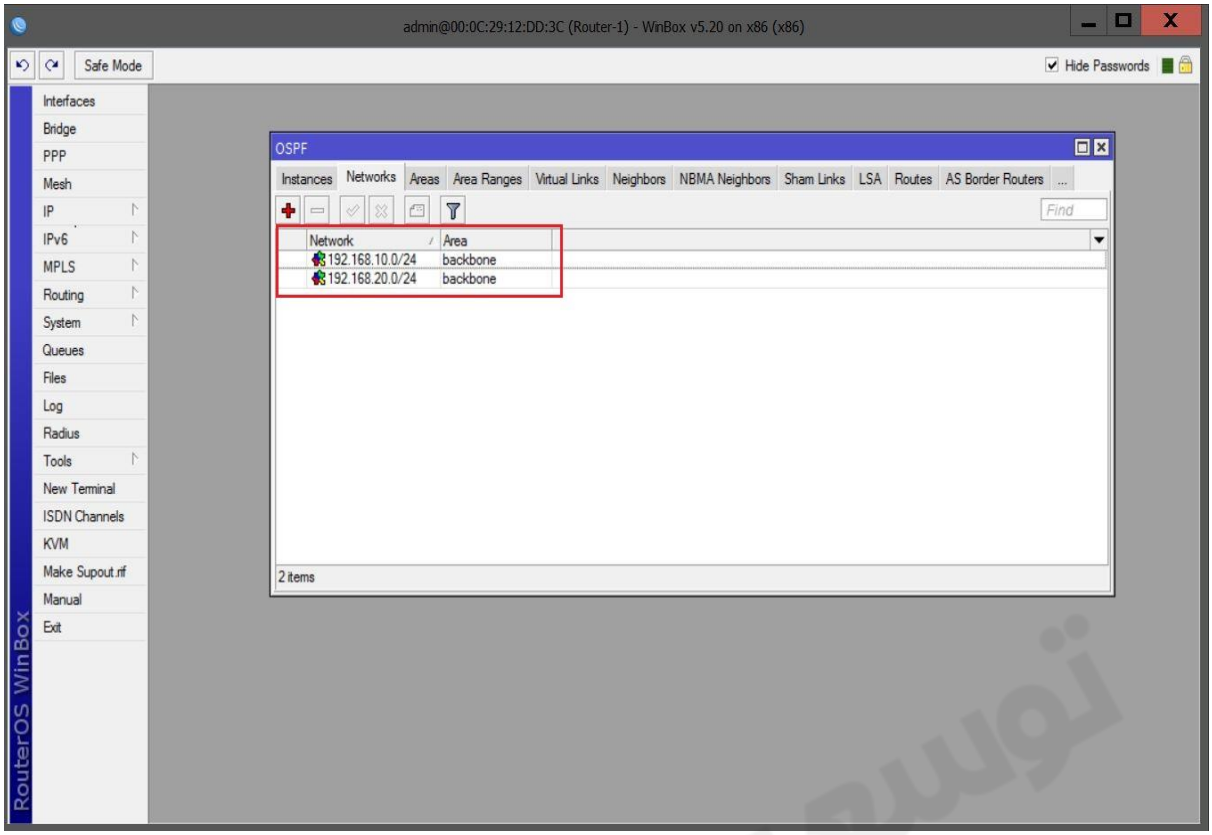
این سناریو مثل سناریو ۳ می باشد با این تفاوت که این سناریو بصورت **Dynamic** و با استفاده از پروتکل **OSPF** مسیریابی می شود.

همانند سناریو قبل برای کارت های شبکه روترها **IP** تنظیم می کنیم سپس به مسیریابی روترها می پردازیم.

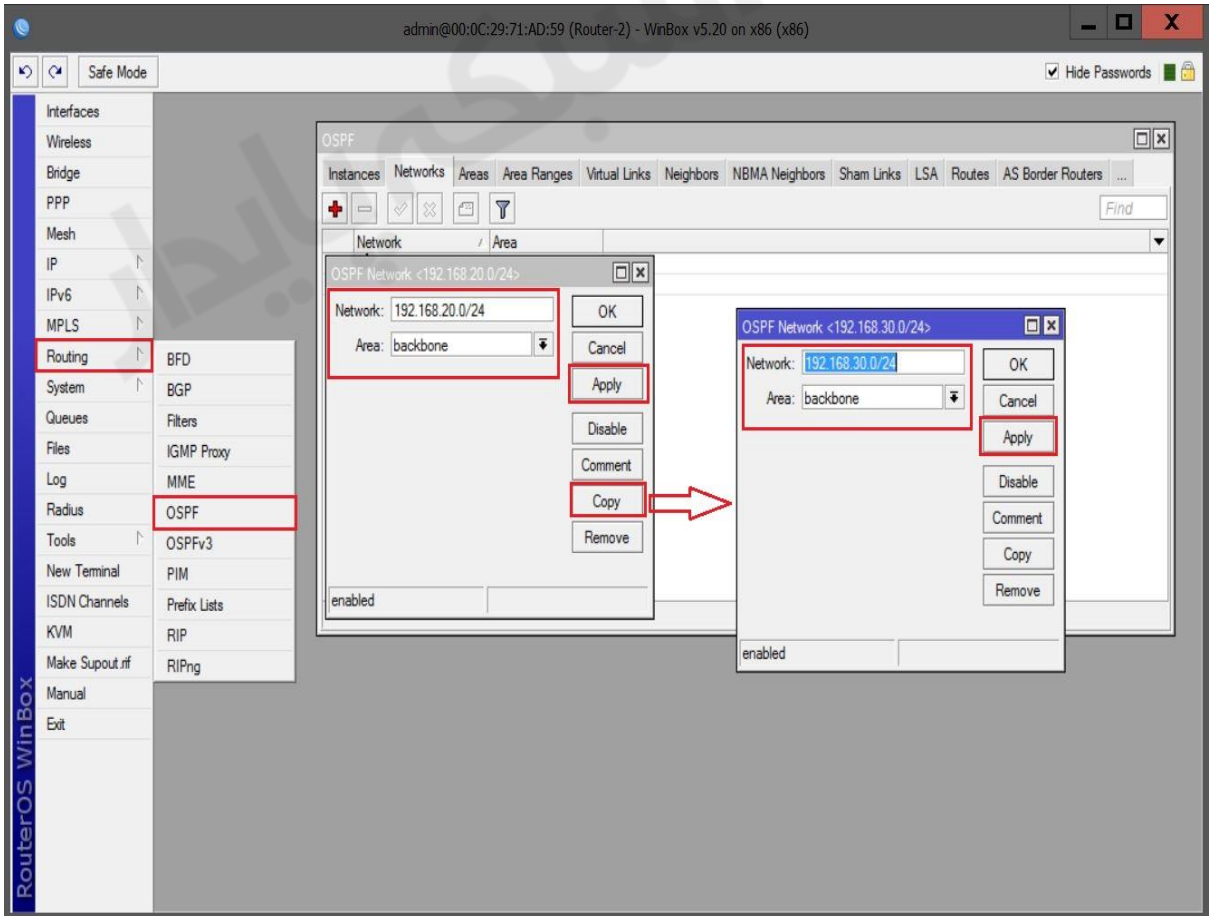
راه اندازی پروتکل **OSPF** در روتر **R1** :

برای اینکار از منوی اصلی گزینه **Routing** و از زیر منوی باز شده **OSPF** را انتخاب میکنیم و از پنجره ی بازشده به تب **Network** میرویم و **Network** هایی که بر روی روتر وجود دارد را **ADD** می کنیم.

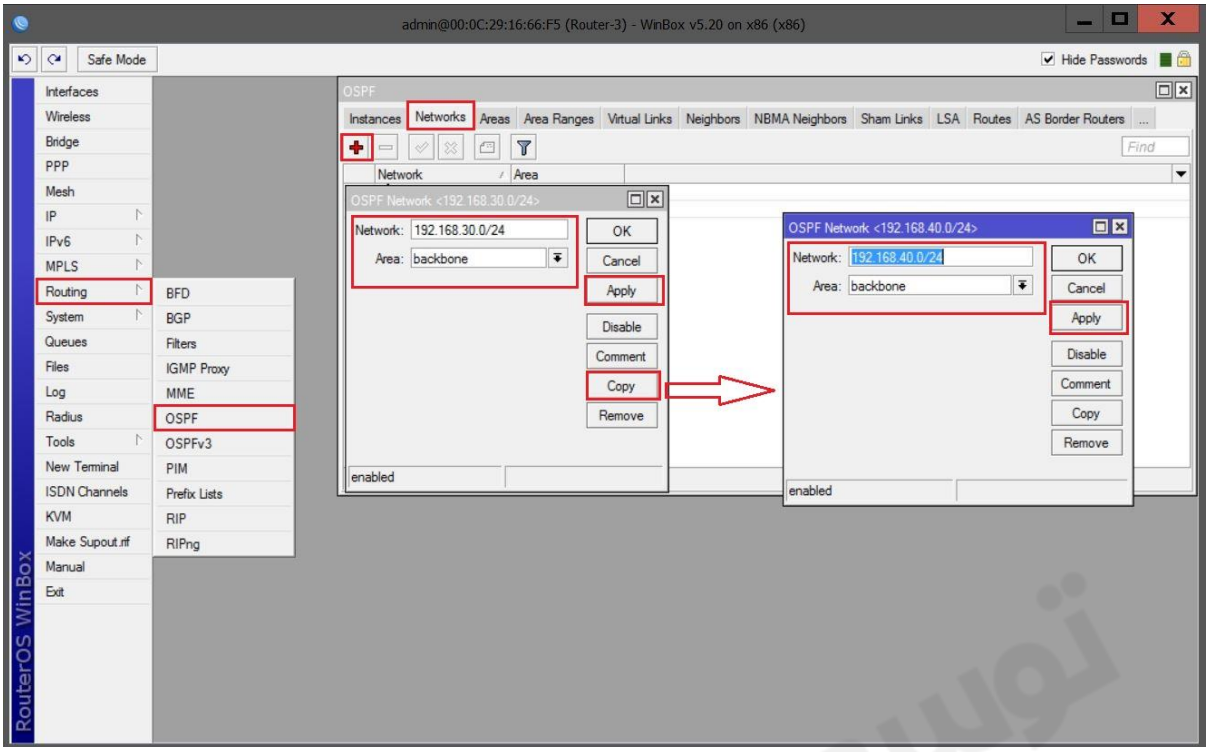




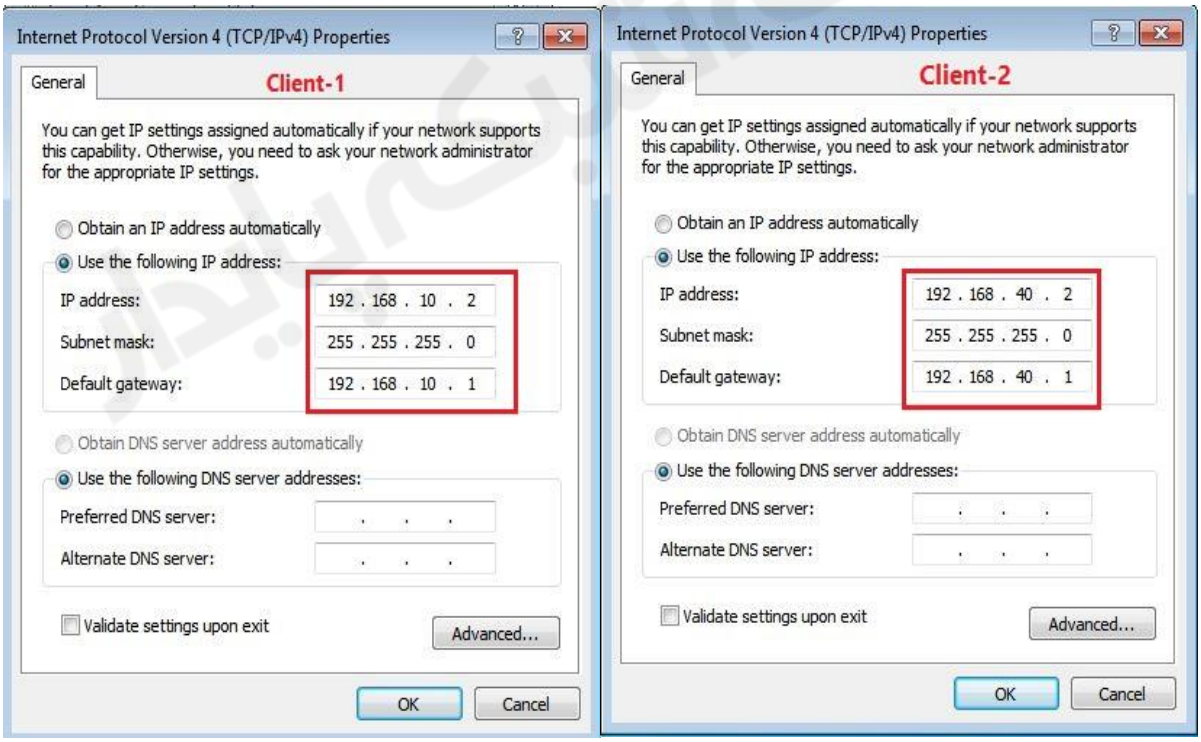
راه اندازی پروتکل OSPF در روتر R2 :



راه اندازی پروتکل **OSPF** در روتر **R3** :



تنظیمات **IP** در کلاینت :



با این تنظیمات باید ارتباط بین کلاینت ها از طریق پروتکل OSPF برقرار باشد برای تست اینکه ارتباط برقرار است از کلاینت ها به یکدیگر Ping میزنیم.

فصل چهارم : NAT(Network Address Translation)

Firewall :

فایروال در لغت به معنی دیواره آتش می باشد که در کاربرد نیز همین مفهوم را دارد.زمانی که دو شبکه را به یکدیگر متصل می کنیم احتیاج به حافظت از هر یک نسبت به دیگری داریم که اکثر فایروال های امروزی برای حفاظت از یک شبکه در مقابل اینترنت استفاده میشوند.میکروتیک را می توان به عنوان یک فایروال قوی استفاده کرد.از قابلیت های فایروال میکروتیک ایجاد **NAT** و **Filtering** میتوان نام برد.

در شبکه معمولا فایروال را بر روی **Gateway** نصب می کنند که کار حفاظتی شبکه داخلی را از حملات خارجی را به عهده دارد.فایروال ها ممکن است استراتژی های مختلفی داشته باشند که بسته به توع شبکه و سطوح امنیت آنها دارد.

در این فصل ما قابلیت **NAT** در میکروتیک را بررسی میکنیم و در فصل های بعد به بررسی **Filtering** و **Mangle** که از قابلیت های فایروال میکروتیک می باشد خواهیم پرداخت.

NAT :

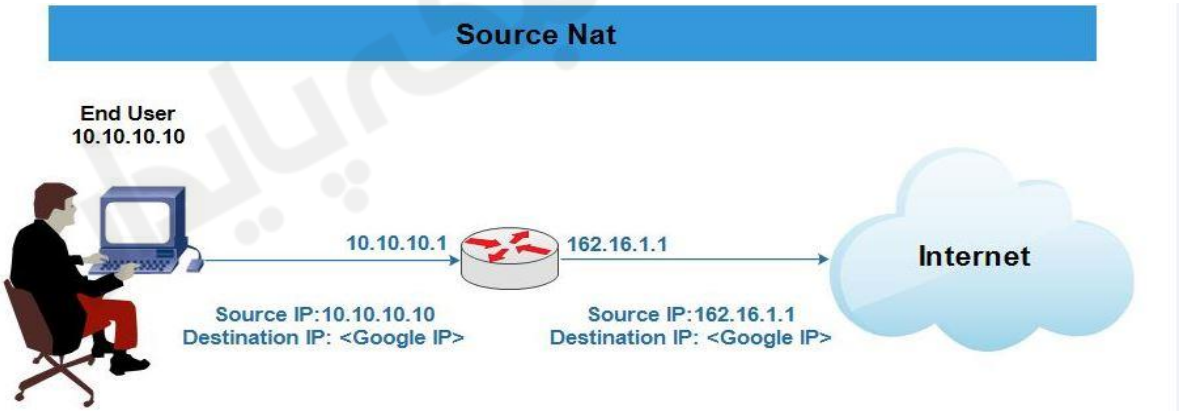
Nat مخفف **Network Address Translation** می باشد فراین تغییر در هدرهای یک بسته اطلاعاتی است و این تغییرات انواع مختلفی از **Nat** را ایجاد می کند.

ما برای شبکه ای داخلی از **IP** های **Private** استفاده می کنیم این **IP** ها در شبکه های محلی استفاده می شود و در دنیای **Wan** (اینترنت) قابل مسیریابی نیستند به همین خاطر یک سرویس ب نام **Nat** به وجود آمد که آن را روی روتر راه اندازی می کنیم و با تنظیم این سرویس کامپیوترهای **Private** می توانند با کمک این سرویس **IP** آدرس **Private** را به **IP** آدرس **Public** ترجمه کنند و با کمک این **IP** به دنیای اینترنت ارتباط برقرار کنند.

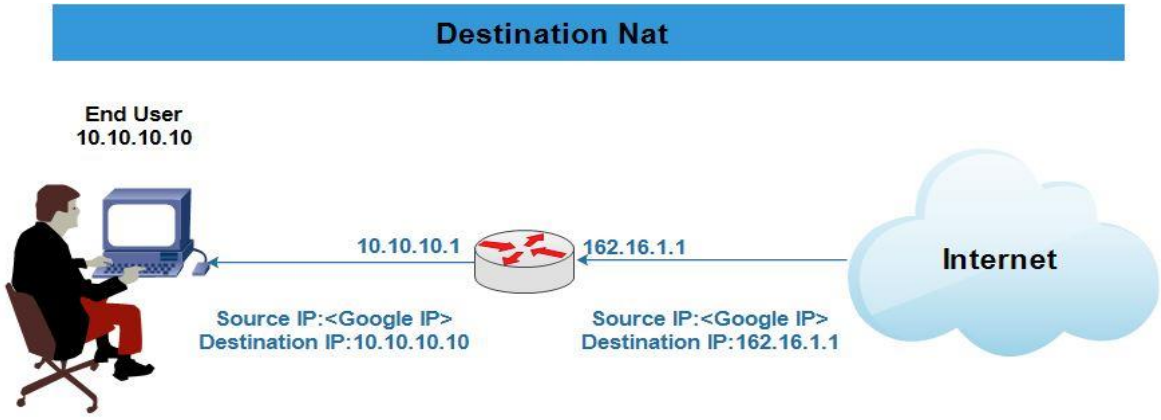
انواع Nat :

بطور کلی ما دو روش برای اجرای **Nat** وجود دارد :

۱. **Source Nat=Src Nat** : در این روش آدرس **IP** مبدا تغییر می کند (**Nat** می شود)



۲. **Destination Nat=Dst Nat** : در این روش آدرس **IP** مقصد تغییر می کند (**Nat** می شود)



قاعده کلی برای تمام روش های Nat بصورت زیر می باشد :

هر بسته ای که روی کارت شبکه محلی روتر دریافت می شود عملیات جایگزینی (NAT) آدرس مبدا با آدرس اینترنتی (IP Valid) روتر انجام می شود سپس بسته به مقصد ارسال می شود(Source Nat)
بعد از آن پاسخ این بسته از سمت سیستم گیرنده به روتر فرستاده می شود.روتر آدرس مقصد که آدرس اینترنتی روتر است را به آدرس محلی سیستم فرستنده تغییر می دهد و در نهایت روتر بسته را به سیستم اصلی تحویل می دهد(Destination Nat)

تنظیمات Source Nat در روتر :

```
[admin@Router-1]>ip firewall nat add chain=[srcnat/dstnat] out-interface=etherX src-address=[source ip address] dst-address=[destination ip address] action=[masquerade/src-nat] to address=[ip range]
```

۱)chain : برای مشخص کردن نوع Nat استفاده می شود.

۲)out-interface : اسم کارت شبکه روتر که می خواهیم بسته ها از آن خارج شوند را مشخص می کنیم.

۳)src-address : از این پارامتر برای مشخص محدوده ی شبکه مبدا استفاده می شود

مثال هایی برای Src-Address :

۳-۱)اعمال عملیات nat بر روی یک سیستم خاص :

Src-address = 192.168.10.2

۳-۲)اعمال عملیات nat بر روی تمامی کلاینت های یک شبکه :

Src-address = 192.168.10.0/24

۳-۳)اعمال عملیات nat بر روی تعدادی از سیستم های یک شبکه :

در ادامه بصورت عملی این عملیات را پیاده سازی خواهیم کرد.

نکته : چنانچه بخواهیم تمامی کلاینت ها موجود در شبکه مبدا بتوانند بسته های خود را به سمت روتر ارسال کنند در src-address چیزی نمی نویسیم.

۴)dst-address : برای اعمال عملیات nat بر روی سیستم هایی که مقصد آنها سیستم مشخصی است استفاده می شود.

نکته : چنانچه بخواهیم تمام بسته هایی که از روتر خارج می شوند بدون توجه به مقصد ، آنها را nat کنیم پارامتر Dst-address را خالی می گذاریم.بنابراین تمامی بسته ها از روتر عبور می کنند.

۵)Action : عملیاتی که بر روی بسته ها انجام می شود توسط این پارامتر انجام می شود.

۵-۱)Masquerade : در این روش IP روتر جایگزین فیلد Source IP در بسته ارسالی از سمت کلاینت می شود.در این حالت ارتباط به سمت شبکه خارجی توسط خود روتر برقرار می شود.چرا که آدرس IP روتر در فیلد Source IP جایگزین آدرس IP کلاینت می شود.

۵-۲)Src-nat : در این روش یک یا چند IP خاص جایگزین Source IP در بسته ارسالی می شود بنابراین امنیت و کنترل بیشتری روی شبکه های محلی خود خواهید داشت.

۶)To Address : در این پارامتر تعدادی IP در نظر گرفته می شود و عملیات nat برای هر سیستم با استفاده از یکی از این IP ها صورت میگیرد.در حقیقت برای انتساب آدرس IP به کلاینت ها Pooling تعریف می شود.

منطق Pooling به این صورت می باشد که هر Request که به سمت Nat Router فرستاده می شود یک IP انتساب داده می شود.زمانی که تمامی IP ها مورد استفاده قرار گرفت Request بعدی نمی تواند ارتباط برقرار کند و به حالت Wating وارد می شودتا زمانی که یکی از Request های قبلی ارتباط را قطع کند.

حالت های مختلف Pooling :

۶-۱)در پارامتر To Address می توان برای اعمال Nat بر روی بسته ها تنها یک IP را مشخص کرد.در مثال زیر مشخص کردیم تمامی سیستم هایی که می خواهند از روتر عبور کنند به آدرس ۱۹۲,۱۶۸,۱۰,۱ Nat شوند.

To Address : 192.168.10.1

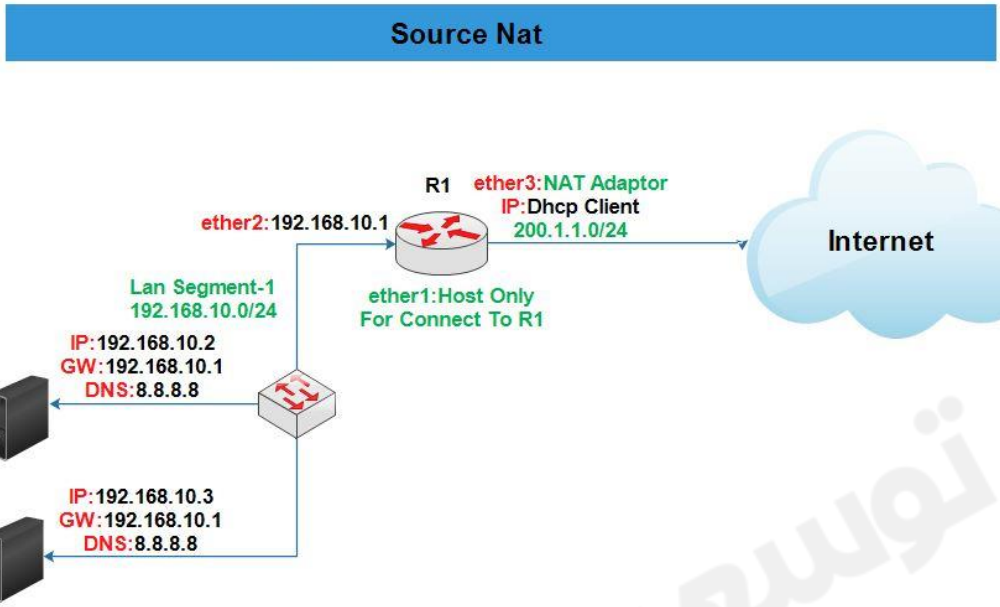
۶-۲)در پارامتر To Address می توان برای اعمال Nat بر روی بسته ها یک محدوده کامل از IP ها را مشخص کرد.

To Address : 192.168.10.0/24

۳-۶)تعیین کردن یک محدوده ی مشخص از IP ها :

To Address : 192.168.10.1-192.168.10.25

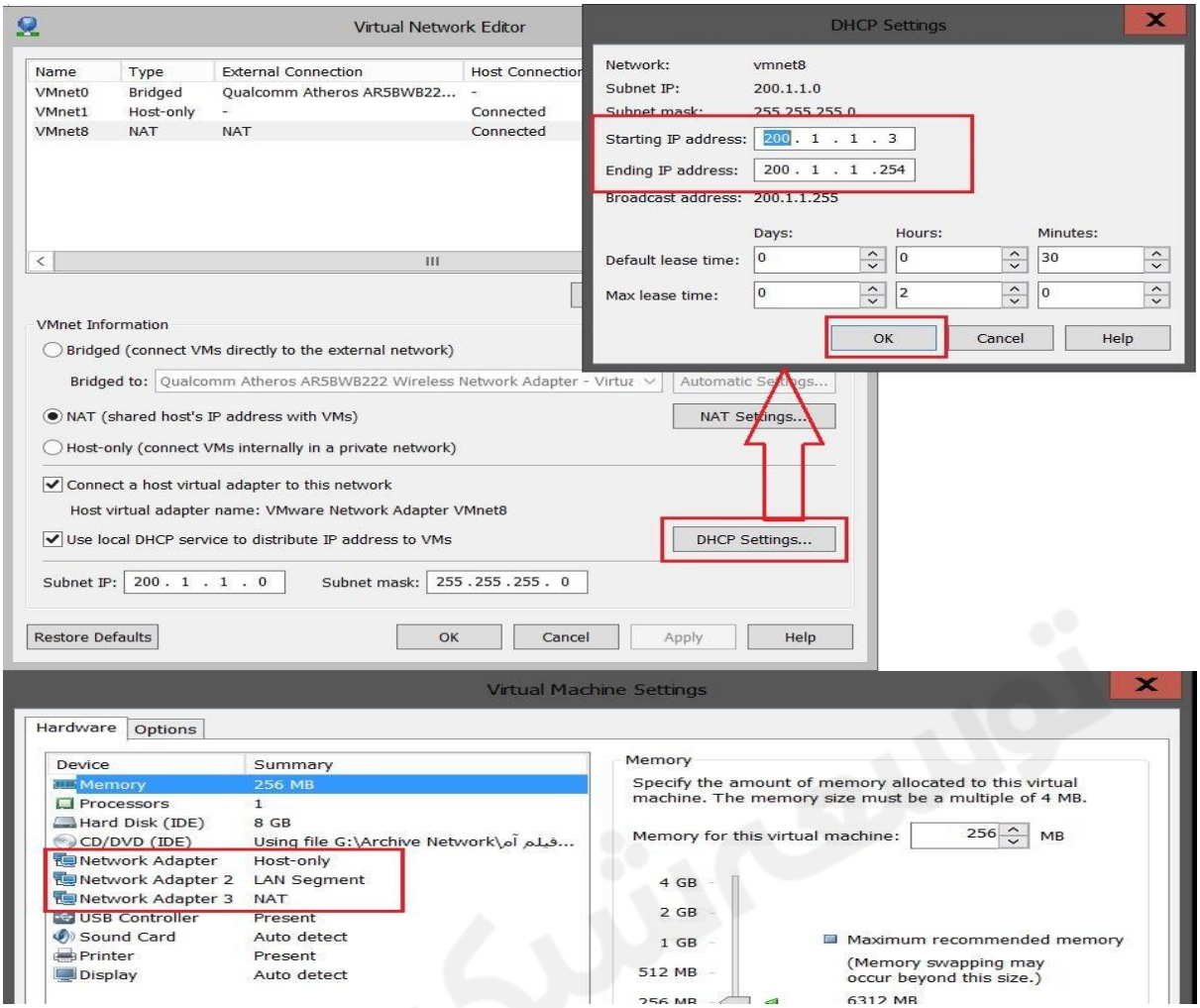
سناریو ۱ : هدف از انجام این سناریو بررسی Source Nat در روتر می باشد.



در این سناریو روتر را به گونه ایی پیکربندی می کنیم که کلاینتی که IP آن 192.168.10.2 است بتواند به اینترنت دسترسی پیدا کنند در حالتی که آدرس IP آن به 200.1.1.5 (IP ی که از DHCP Client دریافت میکند)Nat بشود.

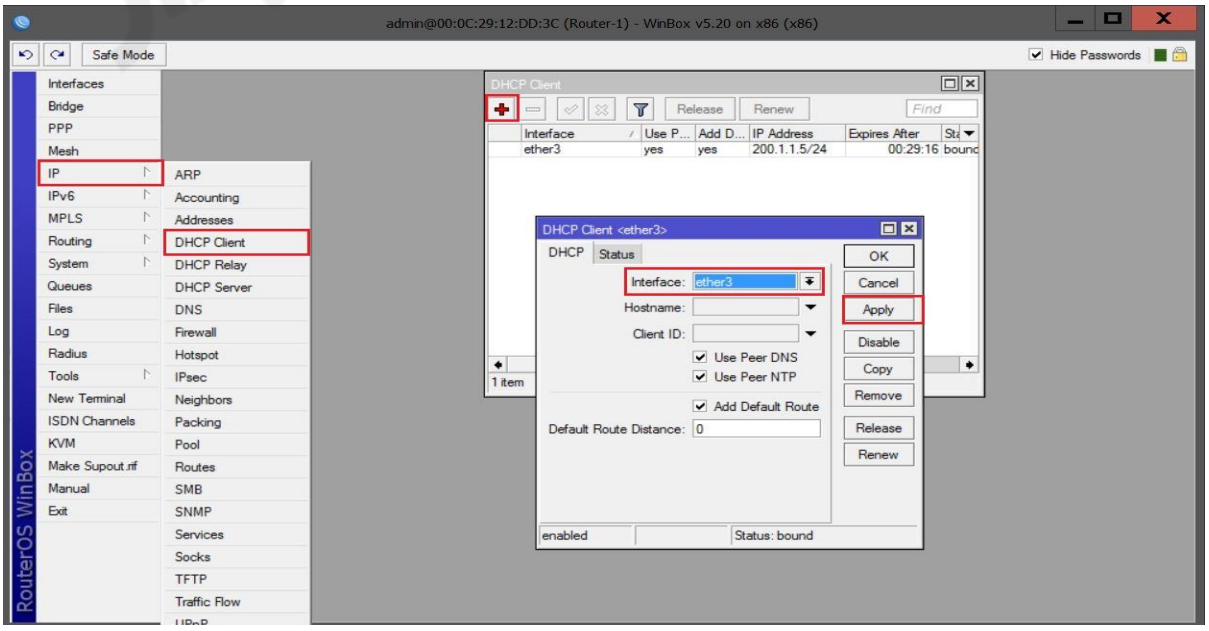
تنظیمات کارت شبکه در VmWare :

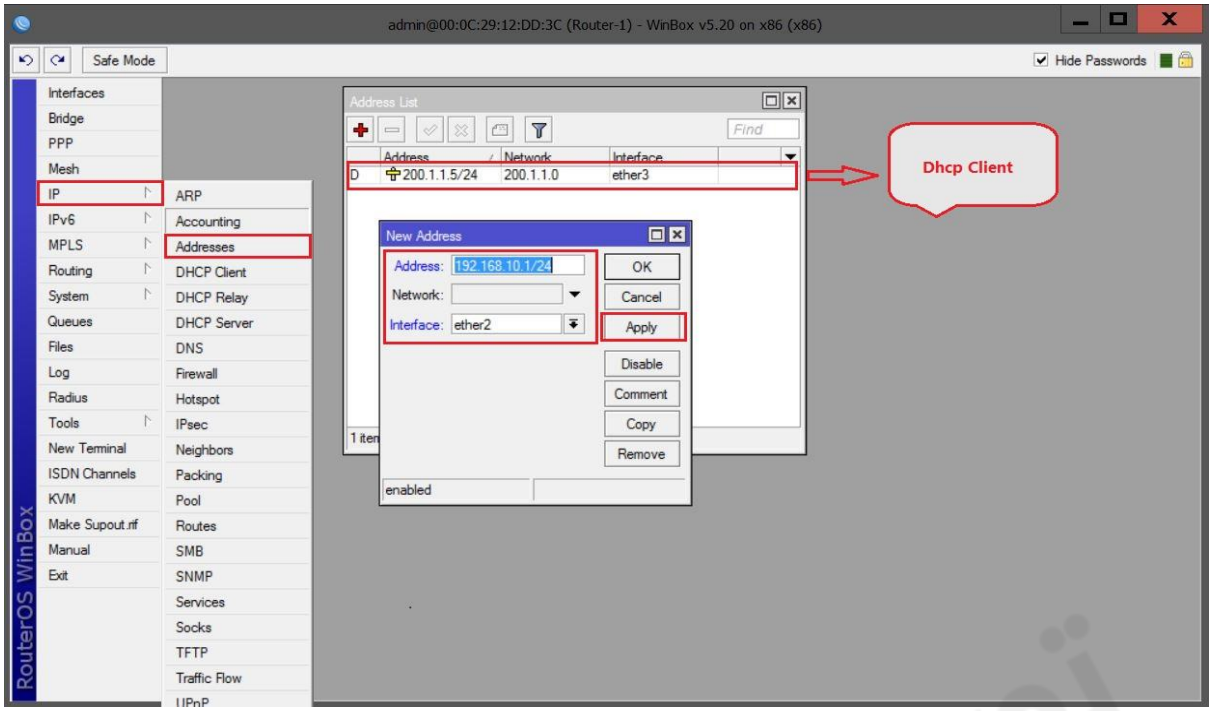
نکته ایی که باید توجه داشته باشید این است که ما میخواهیم کارت شبکه ether3 از Dhcp Client آدرس IP بگیرد ما در این سناریو رنج IP را 200.1.1.0/24 در نظر گرفتیم در ادامه مسیر این تنظیمات را نشان خواهیم داد و همچنین ما می خواهیم از طریق همین کارت شبکه به اینترنت دسترسی داشته باشیم که برای این کار ما از قبل سیستم اصلی خودمان را به اینترنت وصل می کنیم و کارت شبکه ether3 را در حالت Nat قرار می دهیم.



انتساب IP به کارت های شبکه روتر R1 :

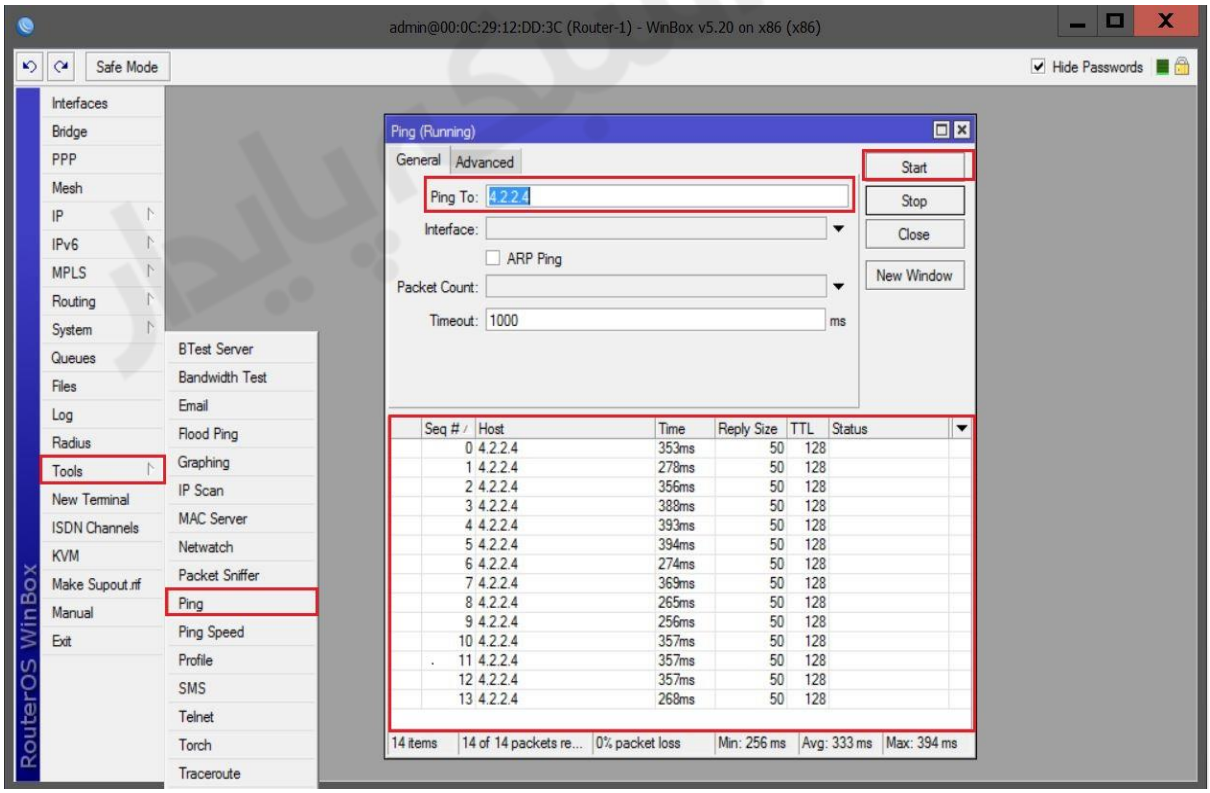
همان طور که در سناریو مشخص کردیم Ether3 باید از Dhcp Client (Vmware) آدرسIP دریافت کند.برای این کار از منوی اصلی گزینه IP و از زیر منوی باز شده Dhcp Client را انتخاب میکنیم.در پنجره باز شده بر روی Add کلیک و از تب Dhcp اینترفیس مورد نظر را انتخاب و ok را میزینم.





تا اینجای کار و با این تنظیمات باید روتر R1 به اینترنت دسترسی داشته باشد برای تست این کار به یک آدرس DNS Public در دنیای اینترنت Ping میزنیم تا از برقرای ارتباط به اینترنت مطمئن شویم.

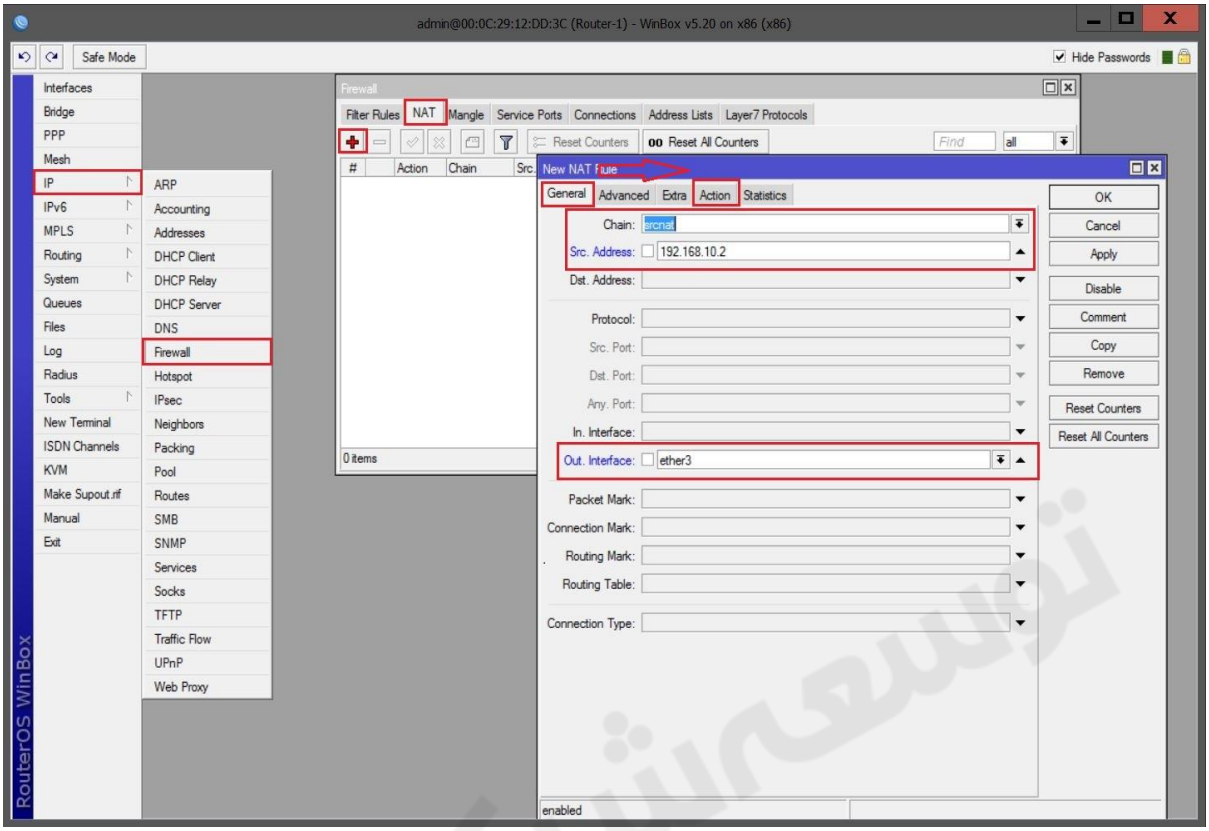
برای Ping کردن از منوی اصلی گزینه Tools و از زیر منوی باز شده Ping را انتخاب می کنیم.

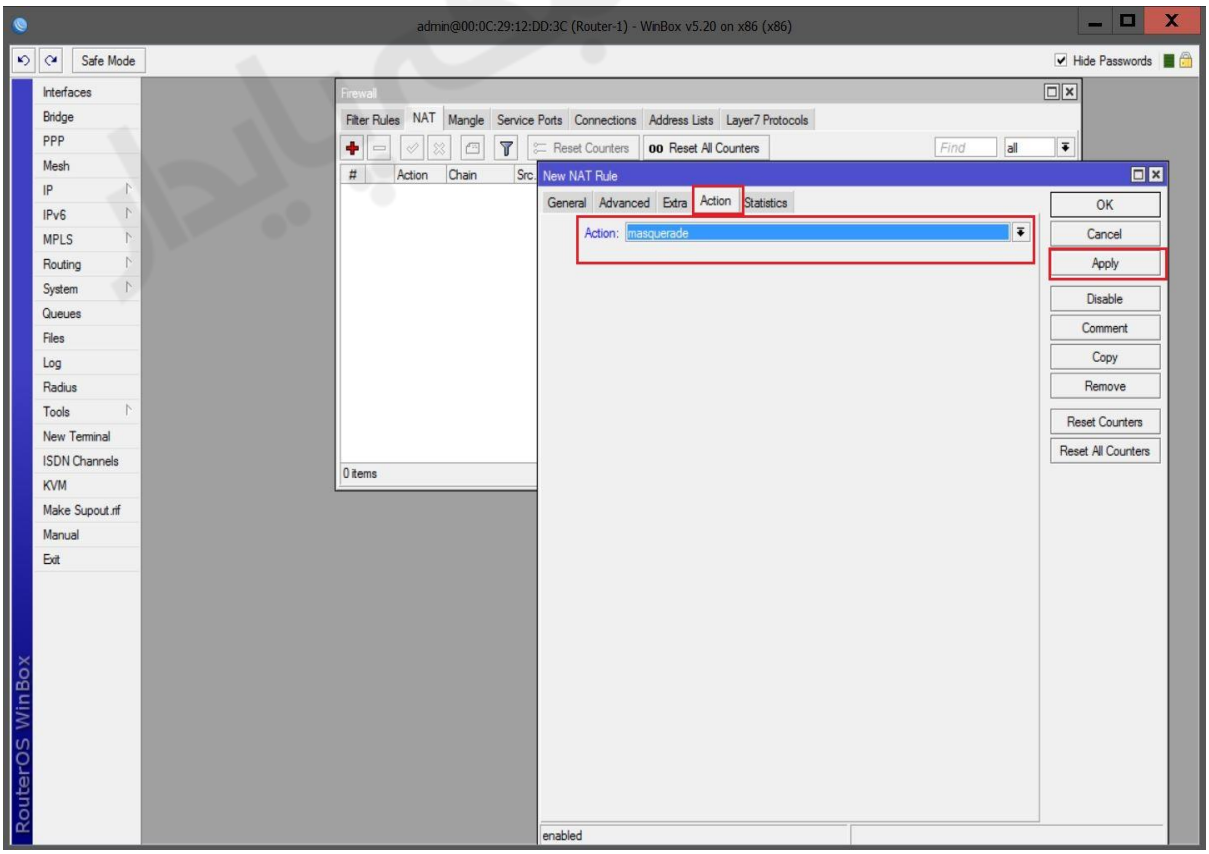


همان طور که در تصویر بالا مشاهده می کنید روتر R1 ما به اینترنت دسترسی دارد.اگر به سیستم کلاینت بروید می بینید که هنوز کلاینت به اینترنت دسترسی ندارد برای این کار ما باید Nat ایجاد کنیم.

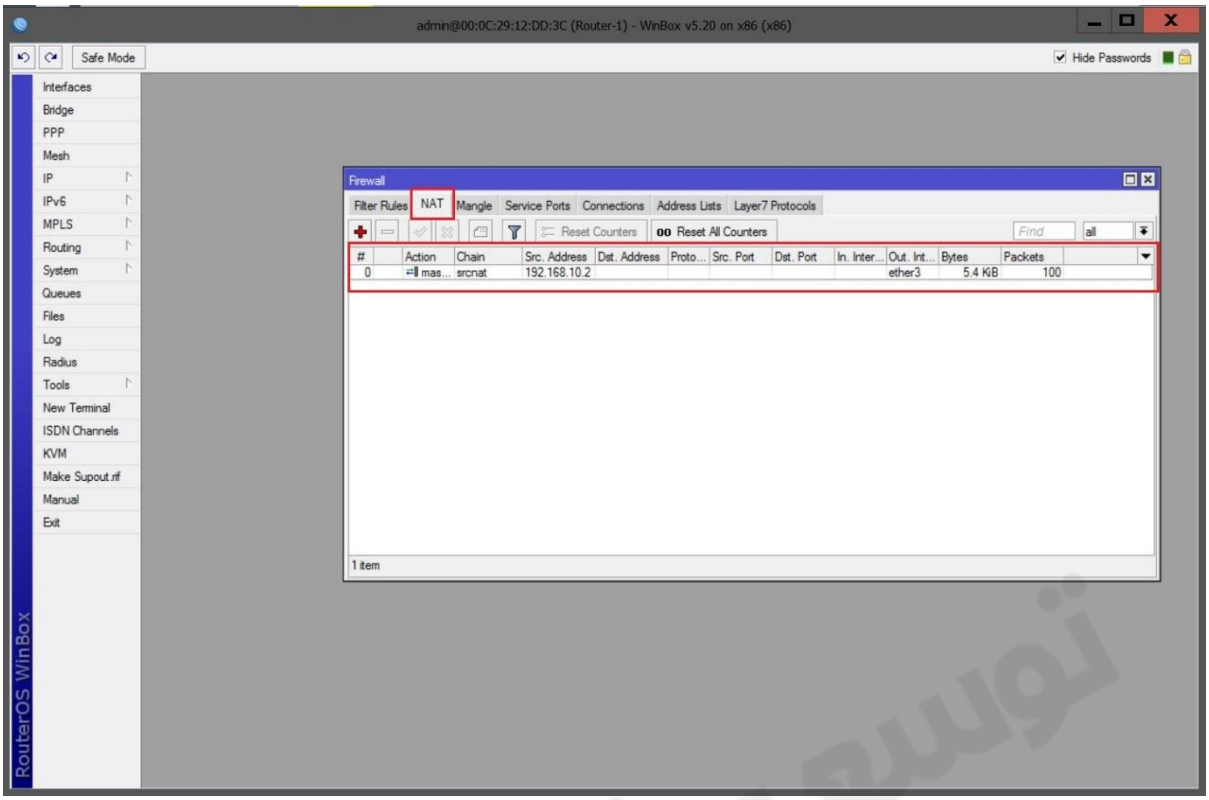
ایجاد NAT برای دسترسی کلاینت به اینترنت :

برای این کار از منوی اصلی گزینه IP و از زیر منوی باز شده Firewall را انتخاب میکنیم.در پنجره باز شده به تب NAT میرویم و بر روی ADD کلیک می کنیم.تنظیمات را مثل زیر انجام می دهیم.

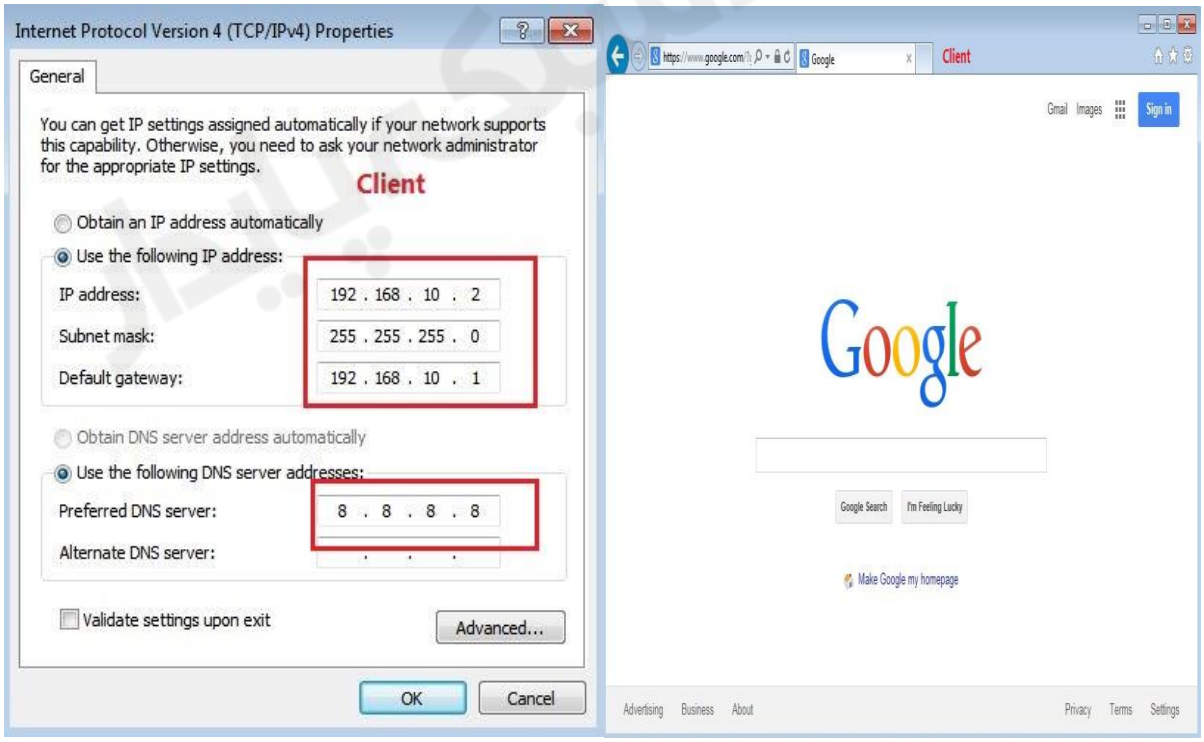




نتیجه **NAT** ی که ایجاد کردیم را در تصویر زیر مشاهده می کنید.



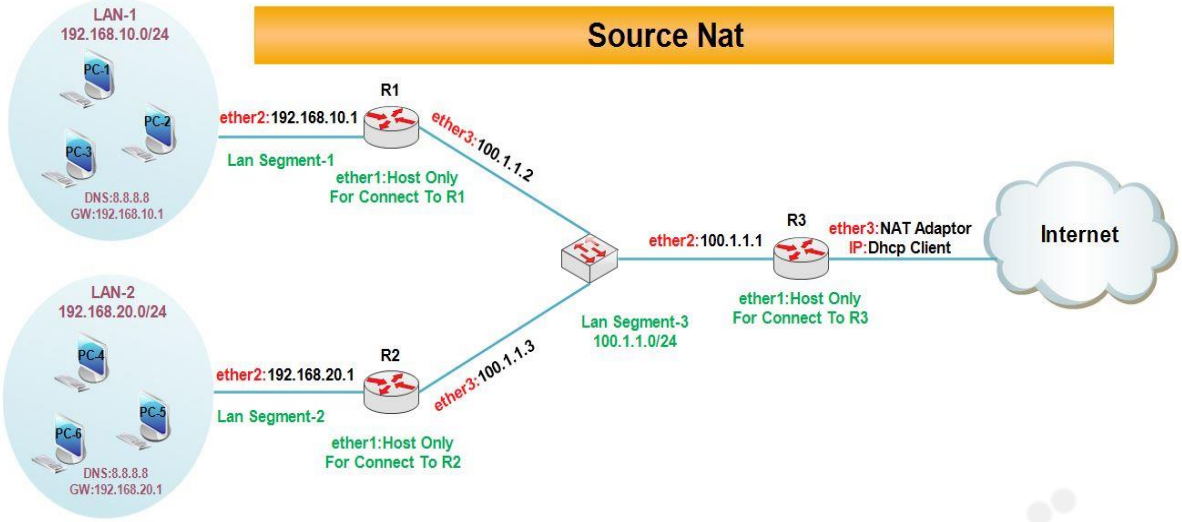
تنظیمات **IP** در کلاینت :



همان طور که در تصویر بالا مشاهده می کنید کلاینت ما به اینترنت دسترسی پیدا کرده است.

نکته:با تنظیماتی که در روتر انجام دادیم فقط همین کلاینت به اینترنت دسترسی دارد و مابقی کلاینت ها به اینترنت دسترسی ندارند.در سناریو بعد با تنظیماتی که انجام می دهیم تمامی کلاینت های یک شبکه محلی به اینترنت دسترسی خواهند داشت.

سناریو ۲ : هدف از انجام این سناریو بررسی **Source Nat** در روتر می باشد.



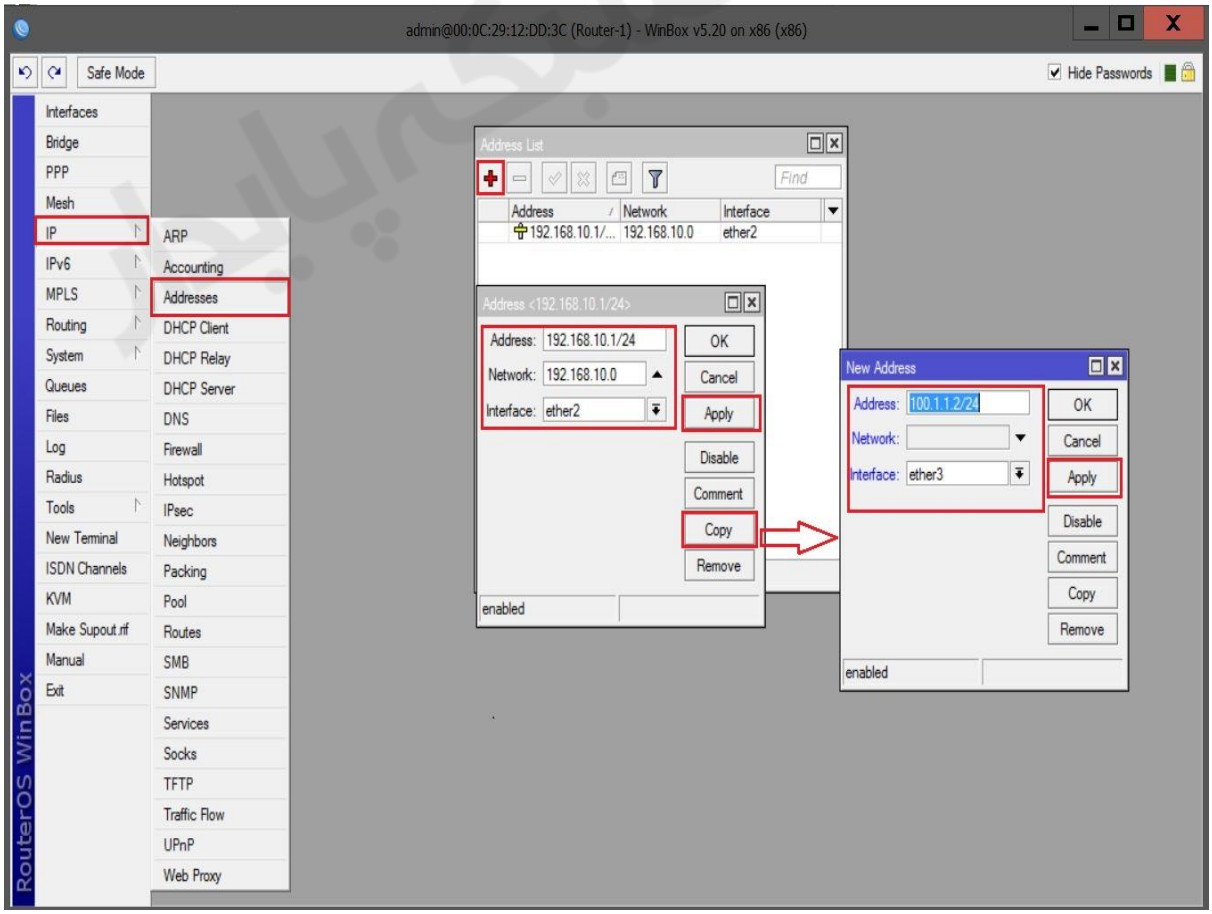
در این سناریو روترها را به گونه ای پیکربندی می کنیم که امکان دسترسی شبکه های محلی به اینترنت وجود داشته باشد.

برای پیاده سازی این سناریو :

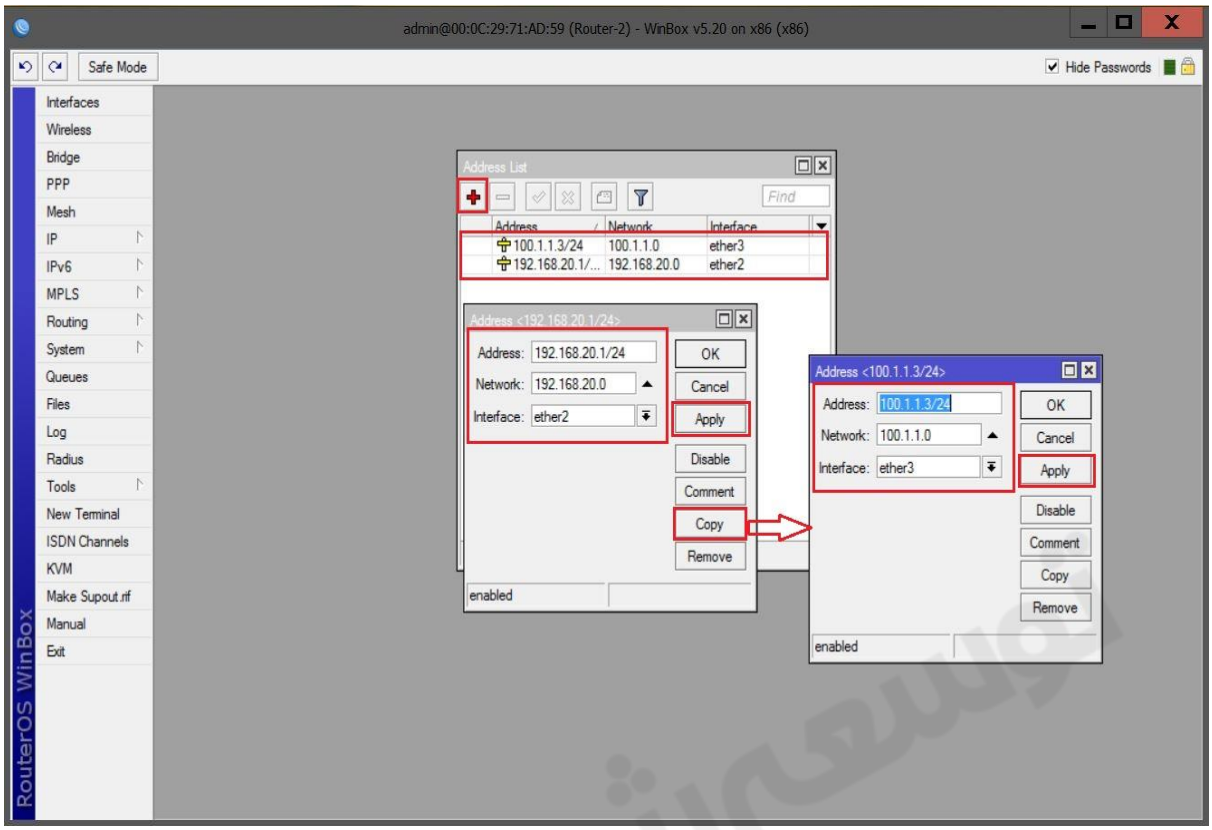
- سه روتر به عنوان مسیریاب های موجود در نظر گرفته شده است.روتر **R3** به اینترنت دسترسی دارد.
- سه سیستم به عنوان کلاینت های موجود در هر شبکه راه اندازی می کنیم.به کلاینت ها طبق سناریو **IP** میدهیم.

انتساب **IP** به کارت های شبکه روترها :

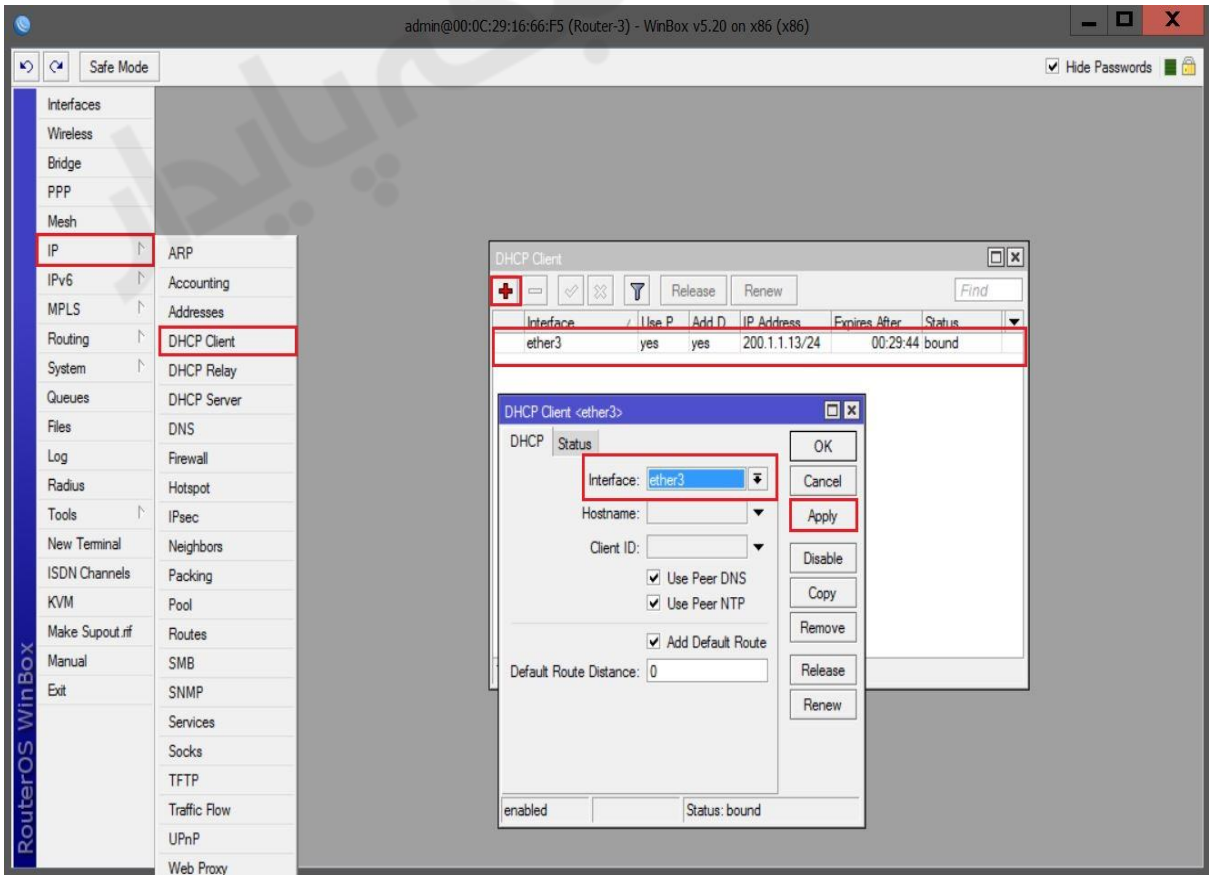
روتر **R1** :

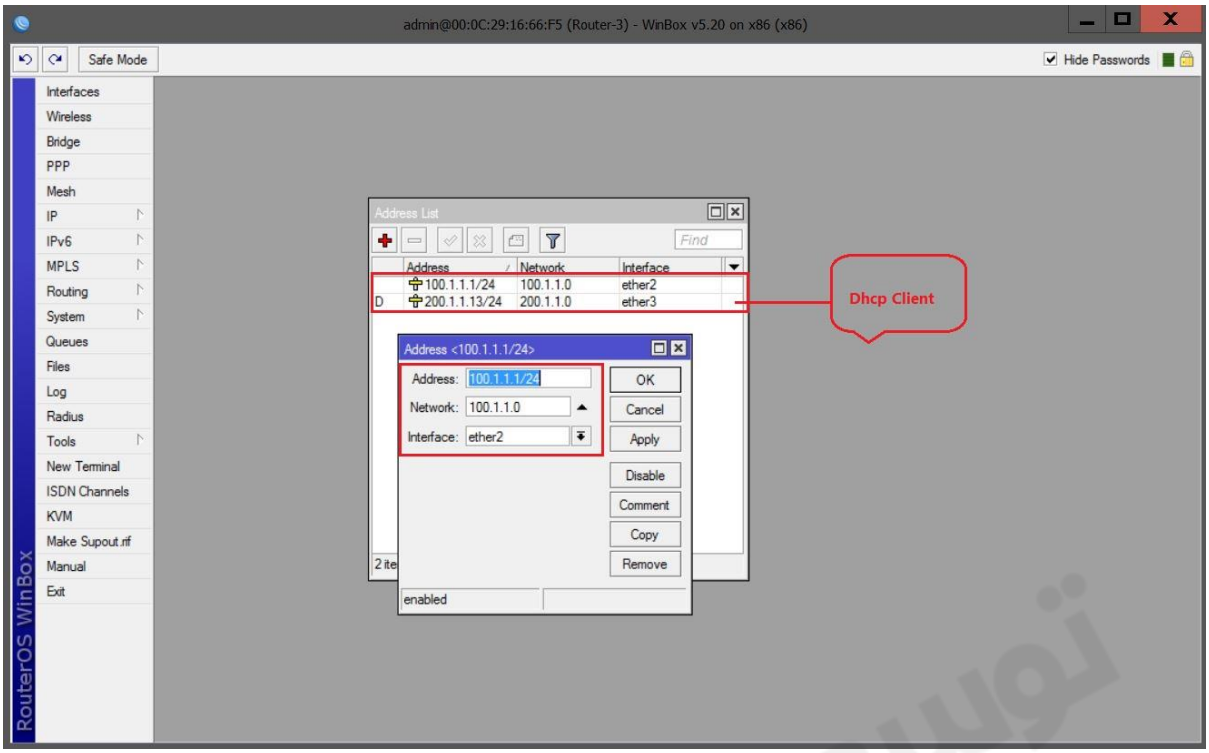


روتر **R2**:



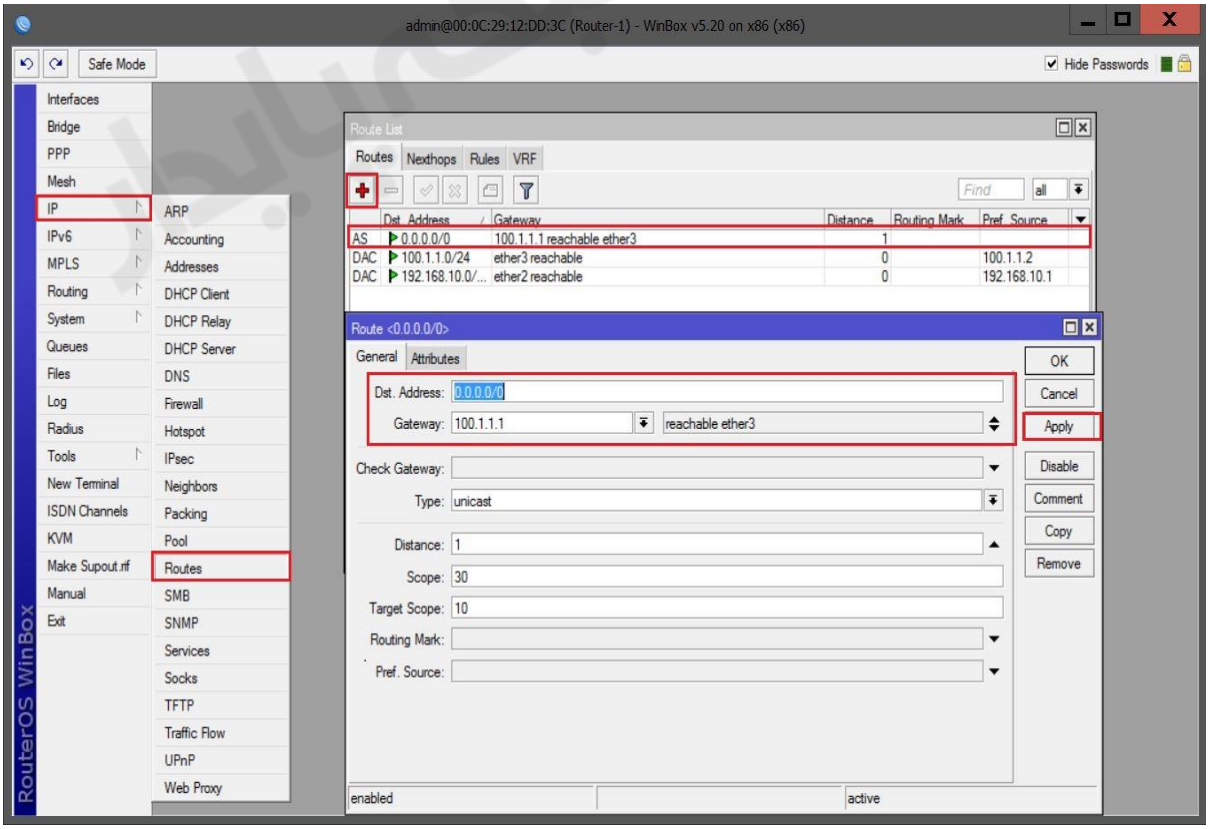
روتر **R3**:



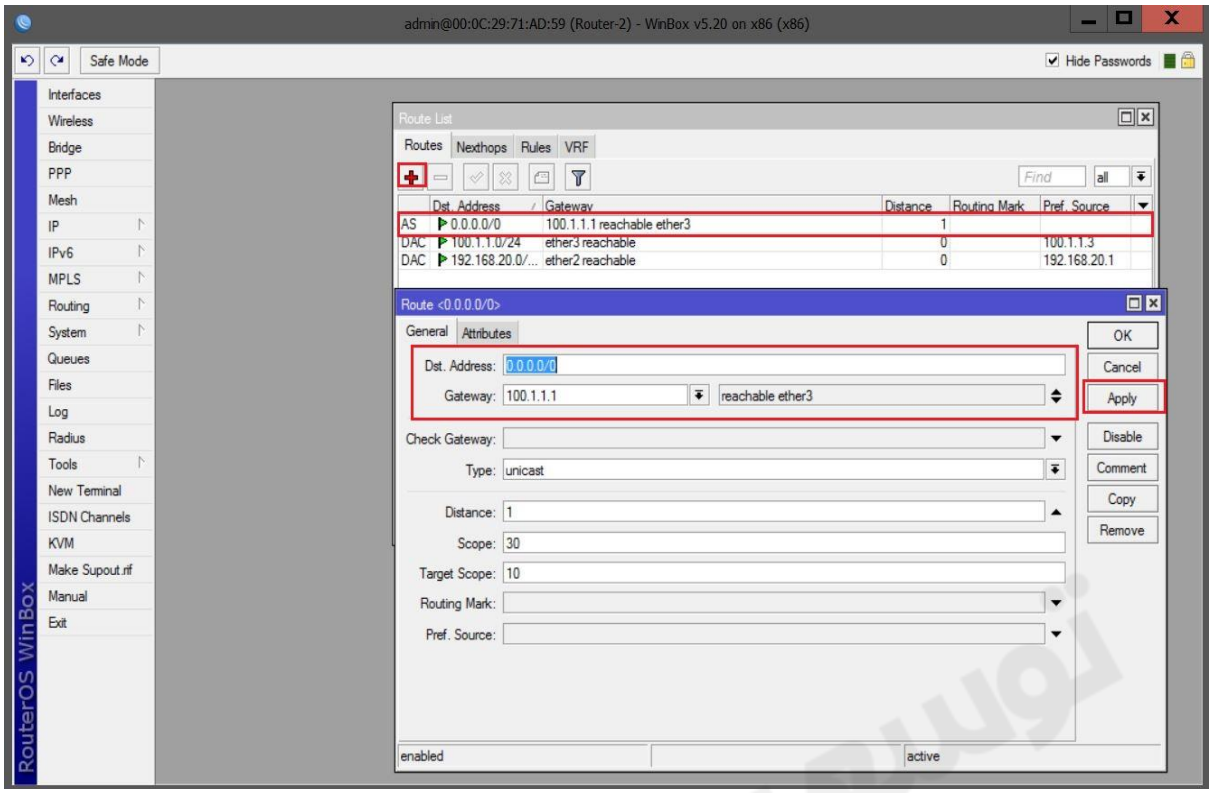


تا اینجای کار ارتباط بین روترها برقرار است ولی کلاینت ها فقط با روتر سر راه خود ارتباط دارند برای اینکه کلاینت ها بتوانند به اینترنت دسترسی داشته باشند باید بتوانند به روتر R3 دسترسی پیدا کنند برای این کار ابتدا در روتر R1 و R2 یک Default Route تعریف می کنیم.

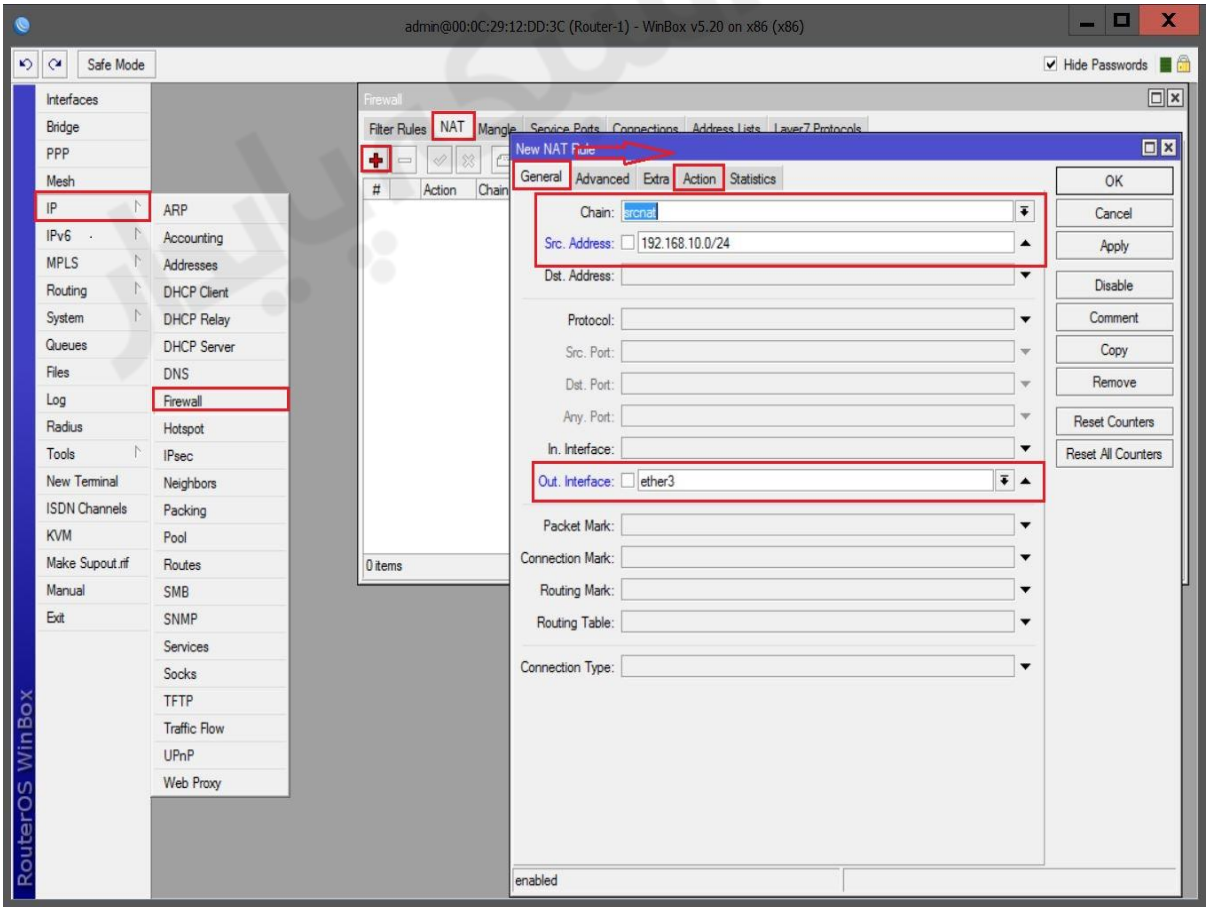
ایجاد Default Route در روتر R1 :

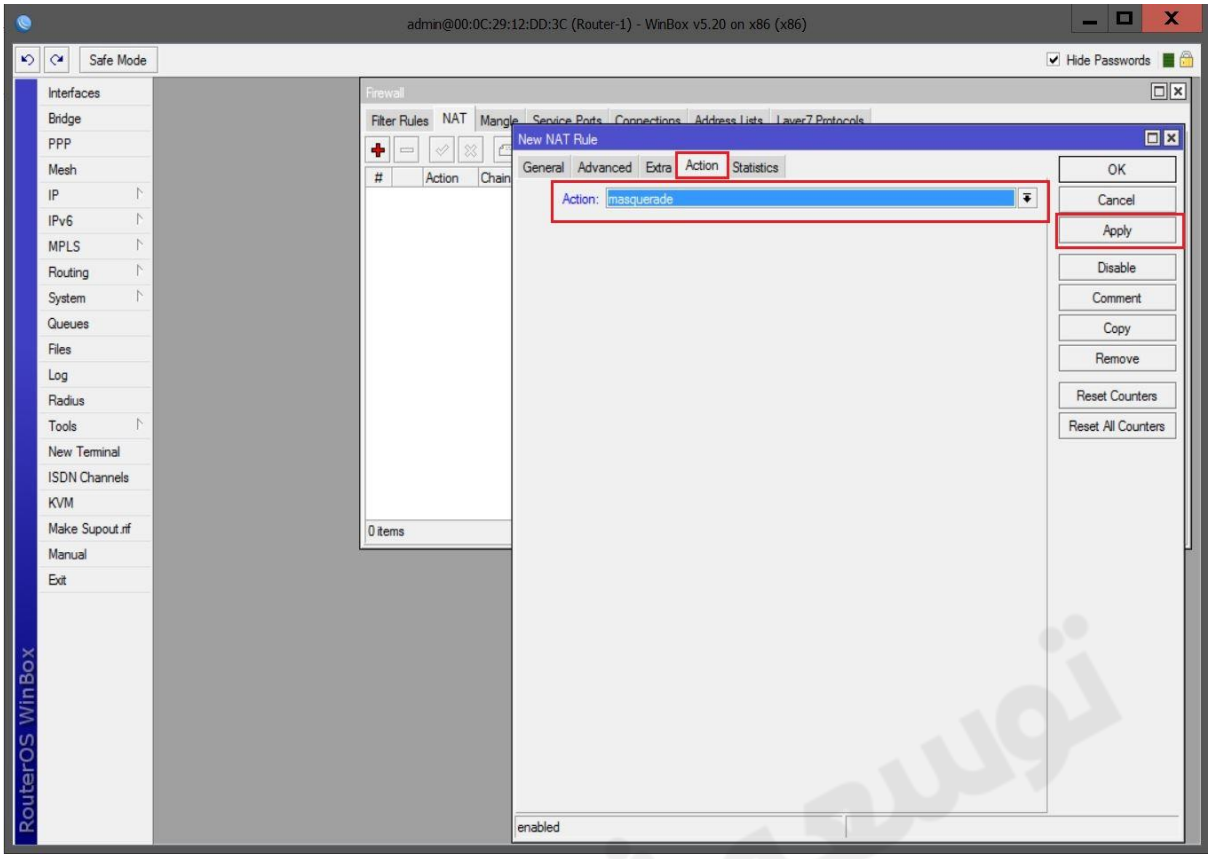


ایجاد **Default Route** در روتر **R2** :

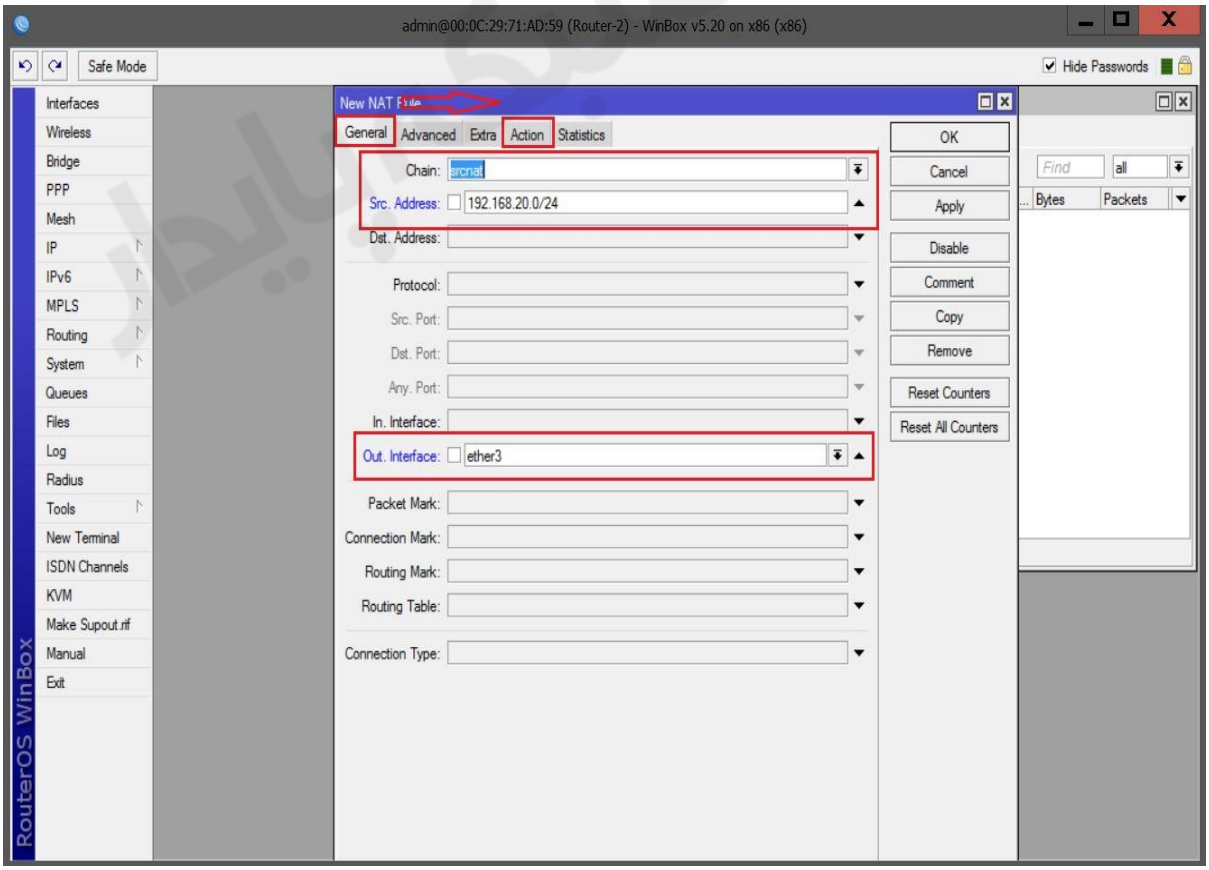


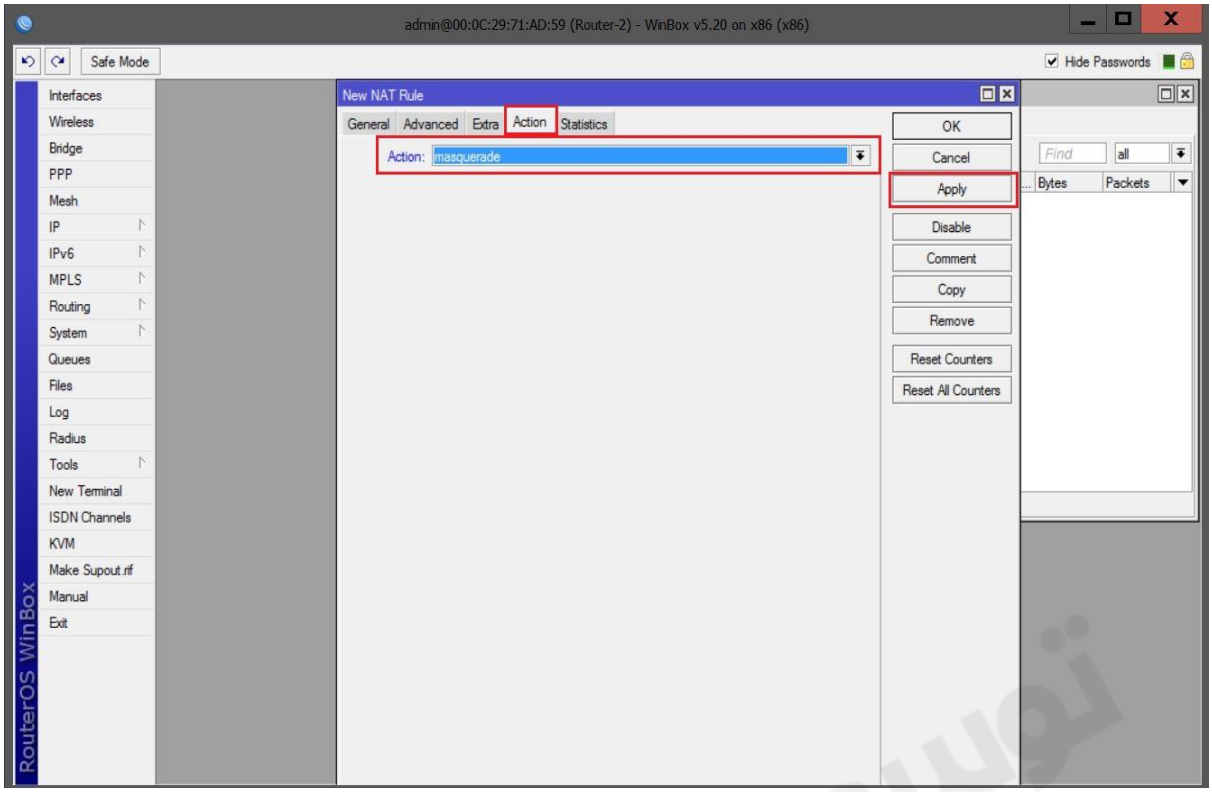
اعمال عملیات **Nat** بر روی بسته هایی که به سمت روتر **R1** می آیند :



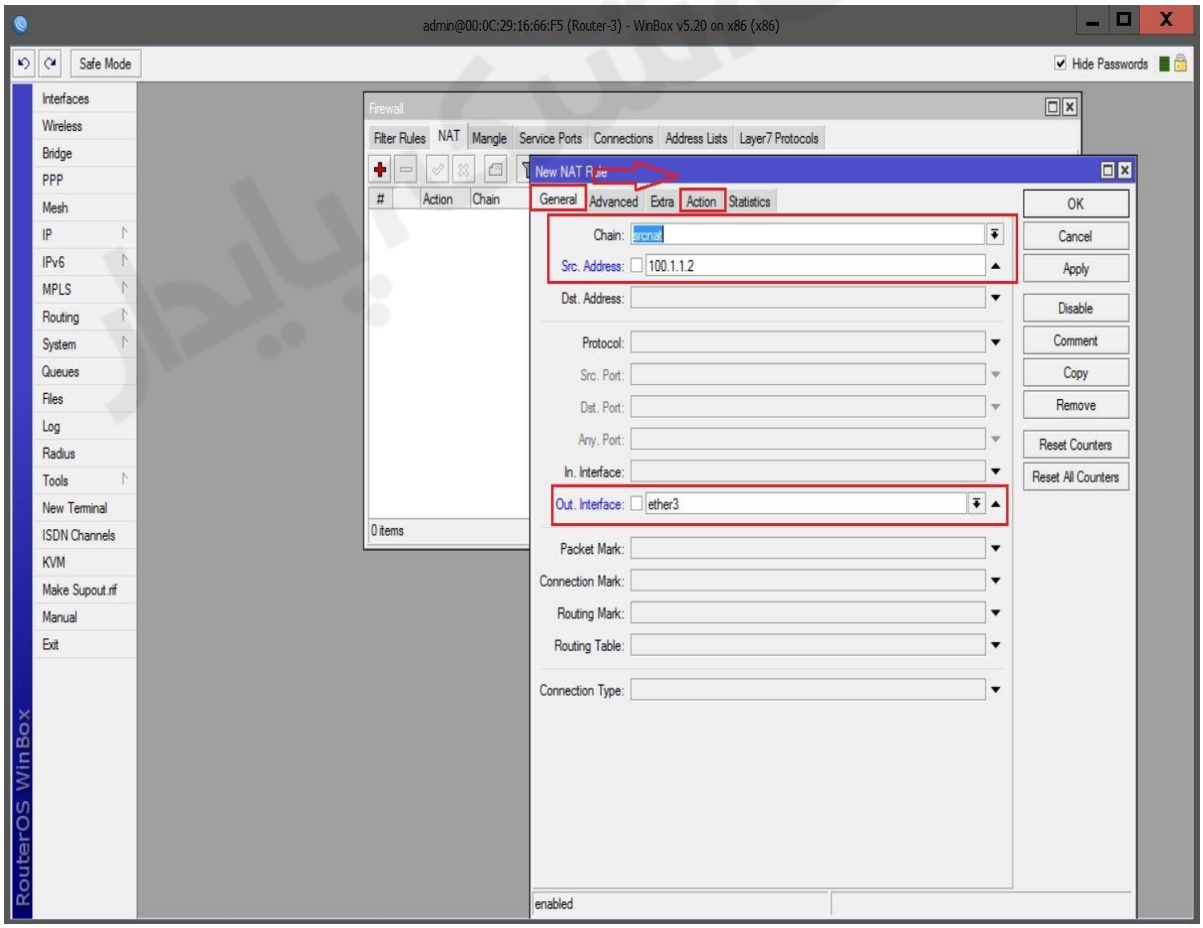


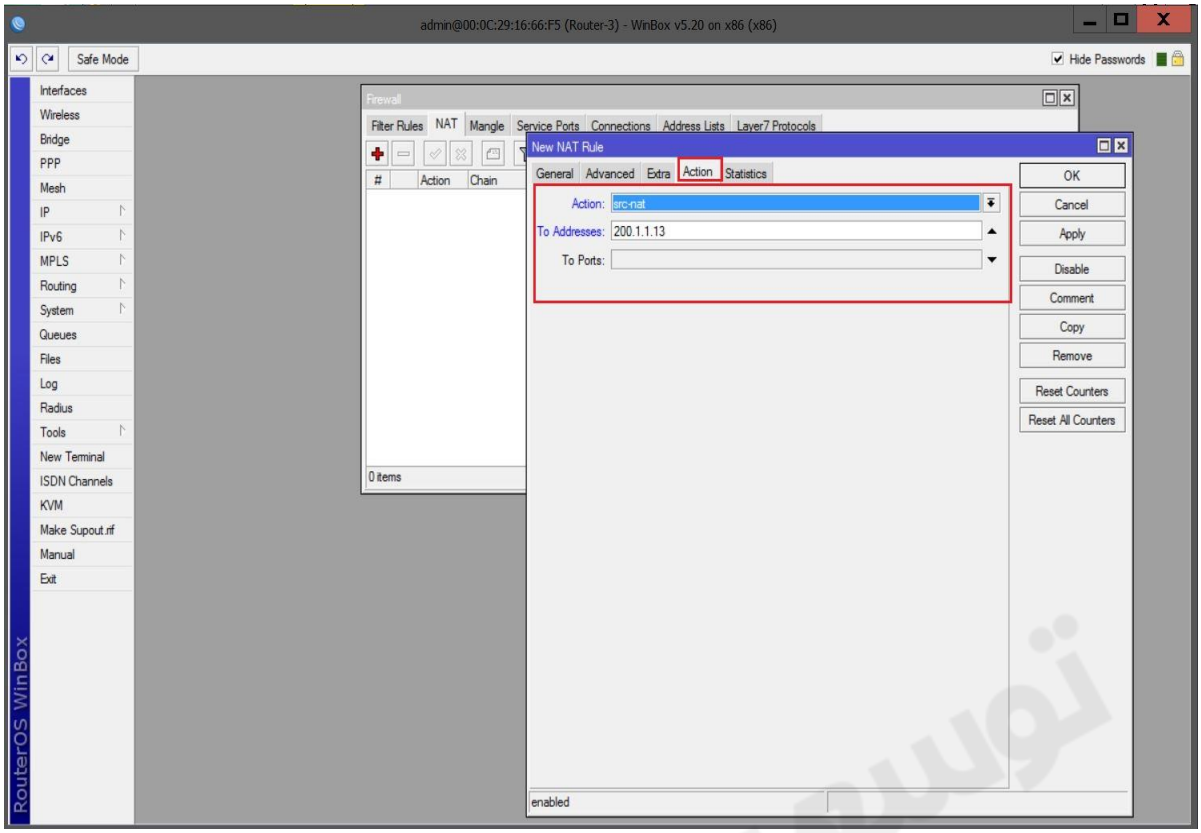
اعمال عملیات Nat بر روی بسته هایی که به سمت روتر R2 می آیند :



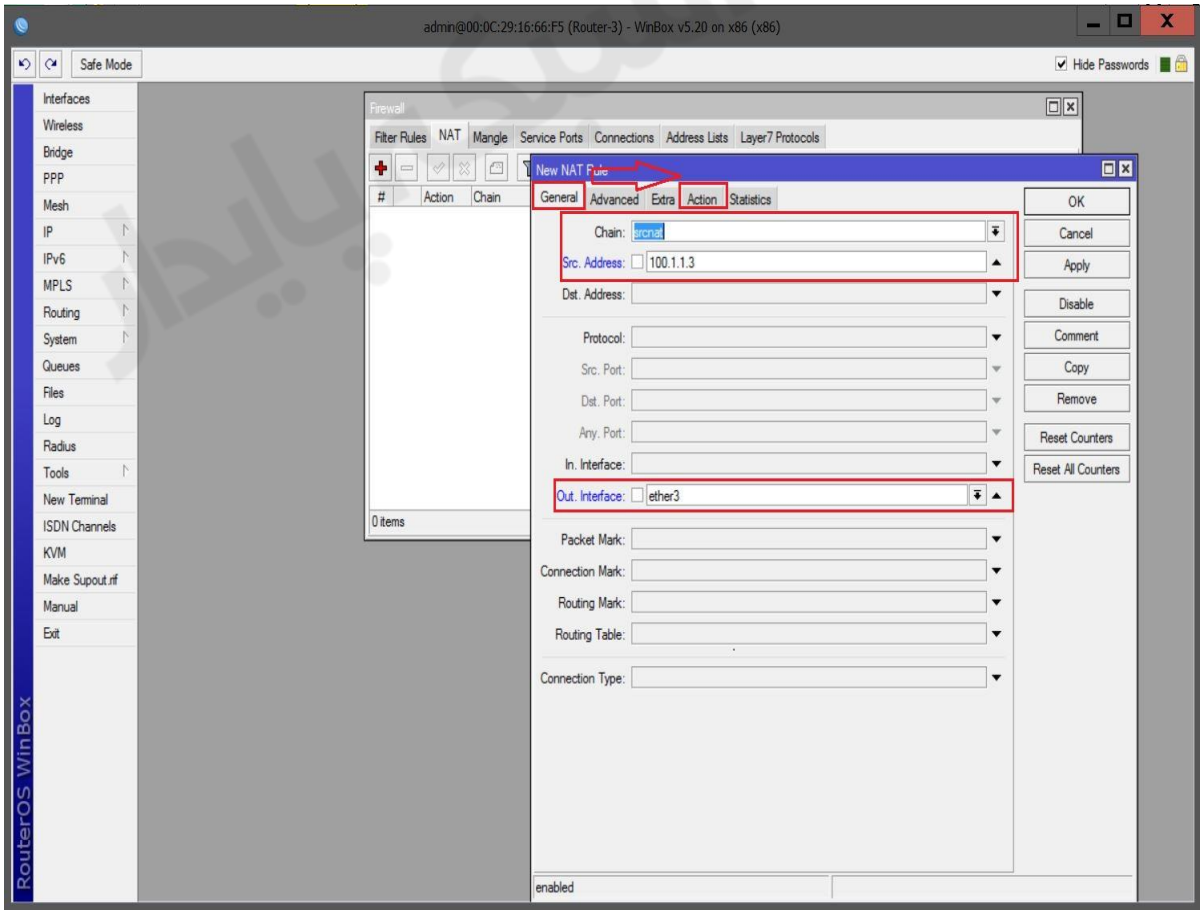


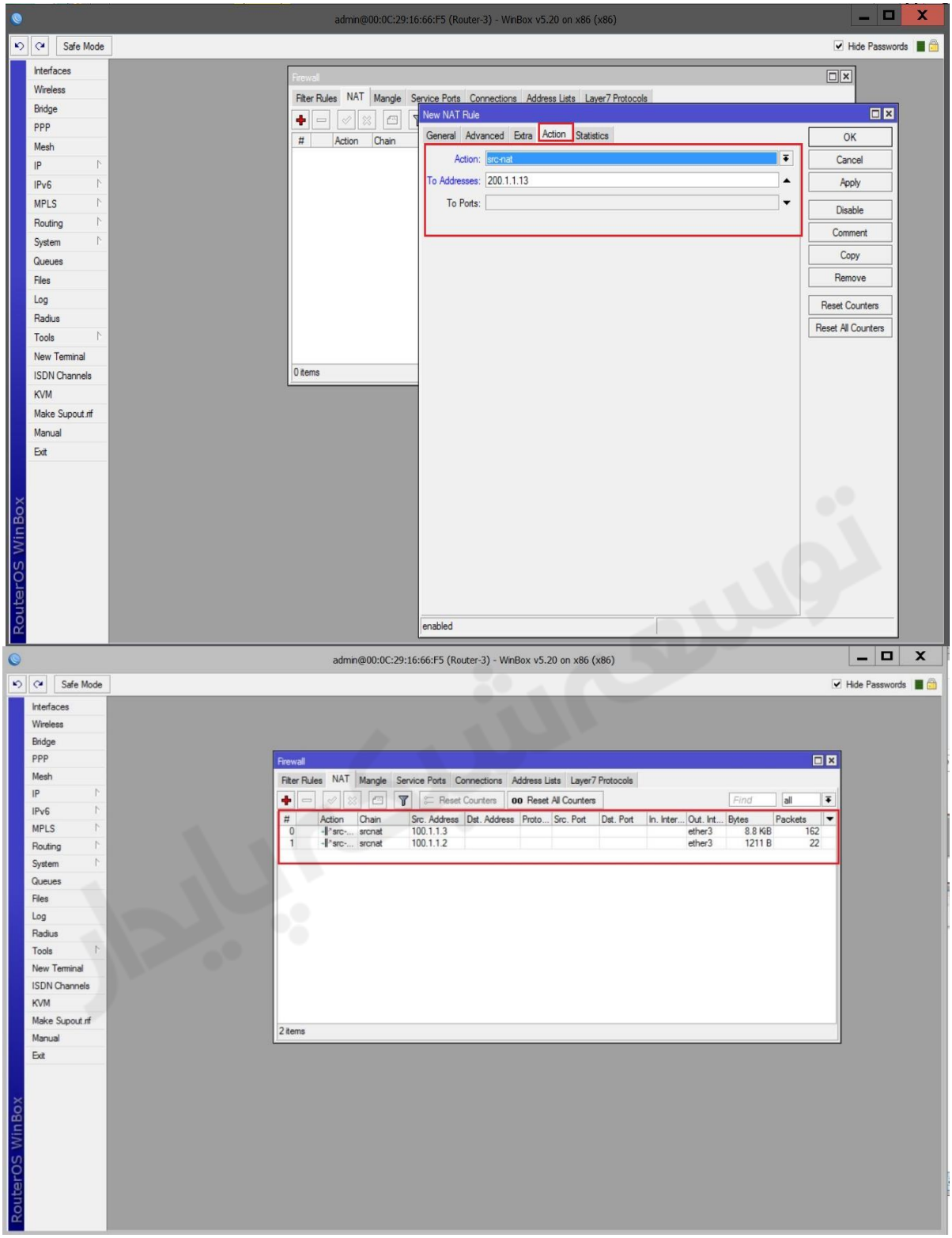
اعمال عملیات Nat برای بسته هایی که از طرف روتر R1 به سمت روتر نهایی R3 می آیند :





اعمال عملیات Nat برای بسته هایی که از طرف روتر R2 به سمت روتر نهایی R3 می آیند :





با این تنظیمات تمامی سیستم های موجود در Lan-1 و Lan-2 به اینترنت دسترسی پیدا می کنند.

نکته : می توانیم در روتر R3 بجای اینکه دوتا Nat ایجاد کنیم یک Natایجاد کنیم و در قسمت Src-Address آدرس IP:100.1.1.0/24 را وارد کنیم.

نکته : دلیل اینکه ما در روتر R3 آدرس شبکه 100.1.1.2 را وارد کردیم به این دلیل است که کلاینت های موجود در شبکه Lan موقع عبور از روتر R1 آدرس IP آنها Nat می شود.در روتر R2 نیز به همین شکل می باشد.

Destination Nat :

در این روش در صورتی که فیلد **Destination-IP** در بسته های اطلاعتی شامل آدرس **IP** مربوط روتر باشد آدرس **IP** مربوط به روتر در این بسته ها تغییر نمی کند به عبارتی چنانچه بخواهیم از یک شبکه **Public** بطور مثال اینترنت به یک شبکه **Private** بطور مثال شبکه **Lan** دسترسی داشته باشیم از این روش استفاده می کنیم.
در این عملیات آدرس **IP** معتبر (**Valid IP**) روتر در بسته های اطلاعاتی را به آدرس **IP** نامعتبر (**Invalid IP**) **Nat** میکنیم(تغییر می دهیم).

تظیمات Destination Nat در روتر :

```
[admin@Router-1]>ip firewall nat add chain=[dstnat] dst-address=[destination ip address] to address=[ip For nat]  protocol=[tcp/udp] dst-port=[router.destination port] to-port=[destination port]
```

۱) **Dst Address** : در این پارامتر آدرس همان کارت شبکه ای از روتر که می خواهیم در صورت رسیدن بسته درخواست به آن ، بسته به سمت وب سرور داخلی شبکه تغییر مسیر دهد را مشخص می کنیم.

۲) **To Address** : در این پارامتر مقصد بسته را مشخص می کنیم.

۳) **Dst port,To Port,Protocol** : چنانچه بخواهیم مشخص کنیم که بسته هایی که به سمت کدام پورت روتر می رسند **Nat** شوند از این پارامترها استفاده می کنیم :

۳-۱) **Dst Port** : پورتی در روتر که بسته ها را دریافت می کند.

۳-۲) **To Port** : پورتی در سیستم مقصد که با استفاده از فرایند **Dst-nat** بسته ها به سمت آن هدایت می شوند.

۳-۳) **Protocol** : در این پارامتر **Tcp** و یا **Udp** بودن پروتکل را مشخص می کنیم.

نکته : چنانچه پارامترهای **Dst Port,To Port,Protocol** را خالی بگذاریم به عبارتی پورت ها را **Full Port** در نظر گرفته ایم و محدودیتی برای پورت ها اعمال نکرده ایم

نکته : اگر بخواهیم پورت ها را به صورت ترکیبی مشخص کنیم پارامتر **To Port** را بصورت زیر بکار می بریم :

- تفکیک پورت ها بصورت تکی :

To Port : 23,22

- تفکیک پورت ها بصورت محدوده ای از پورت ها :

To Port : 1-5

- تفکیک بصورت تکی و محدوده ای از پورت ها :

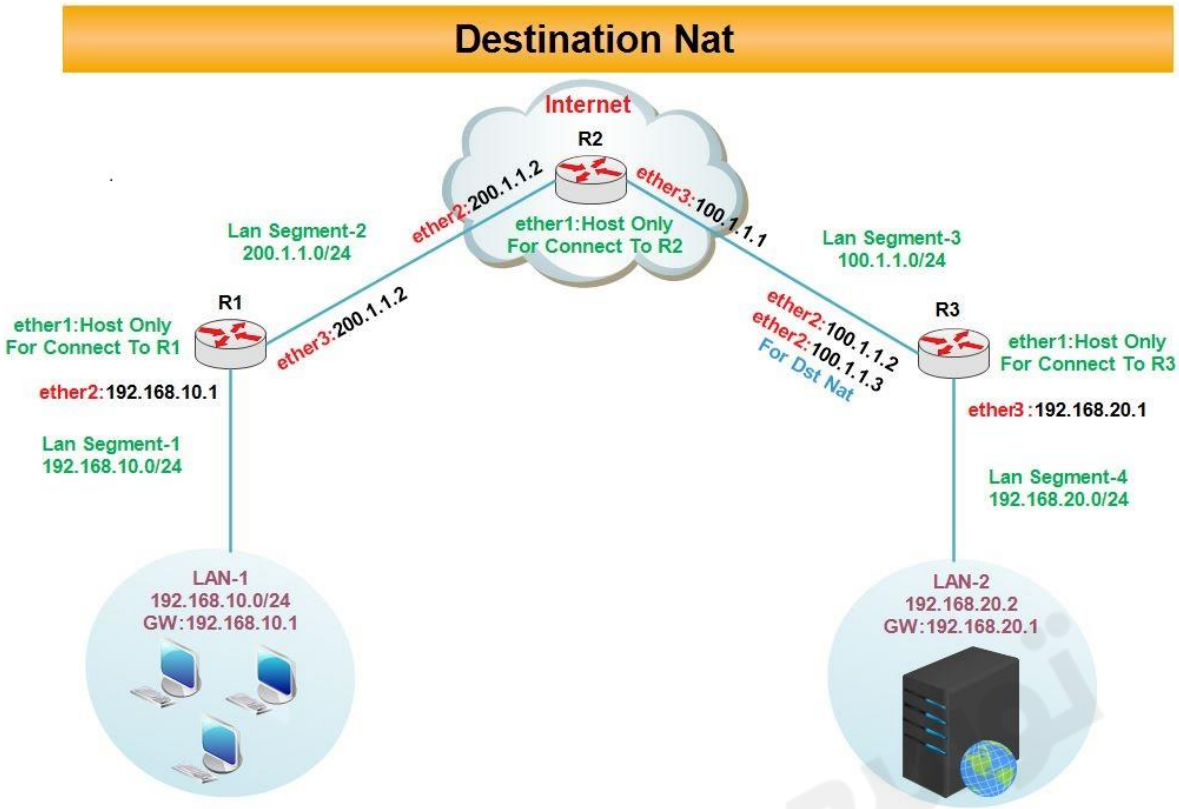
To Port : 23,22,1-5

سناریو ۳ : هدف از انجام این سناریو پیاده سازی عملیات **Destination Nat** بر روی روتر می باشد.

در این سناریو در شبکه داخلی (**Lan-2**) یک وب سرور وجود دارد.برای اینکه این سرور از طریق اینترنت قابل دسترس باشد نیاز است که یک آدرس **IP**معتبر بر روی سرور وجود داشته باشد.چنانچه سرور با یک آدرس **IP**نامعتبر به روتر متصل باشد عملا در اینترنت دیده نمی شود.بنابراین باید در روتر مشخص شود که هر بسته ایی که به سمت روتر فرستاده می شود به سمت وب سرور موجود در شبکه داخلی هدایت شود.

عملیات Dst Nat به این صورت مطرح می شود :

بسته ی در خواست برای استفاده از وب سرور از سمت کلاینت در یک شبکه خارجی (در این سناریو شبکه **Lan-1**) به سمت روتر فرستاده می شود .زمانی که بسته در روتر دریافت می شود فیلد **Destination IP** با آدرس **IP** ای که در پارامتر **To Address** برای آن مشخص شده جایگزین می شود و به این ترتیب بسته به وب سرور موجود در شبکه محلی می رسد در صورتی که آدرس **IP** آن سرور نامعتبر(**Invalid**) می باشد.



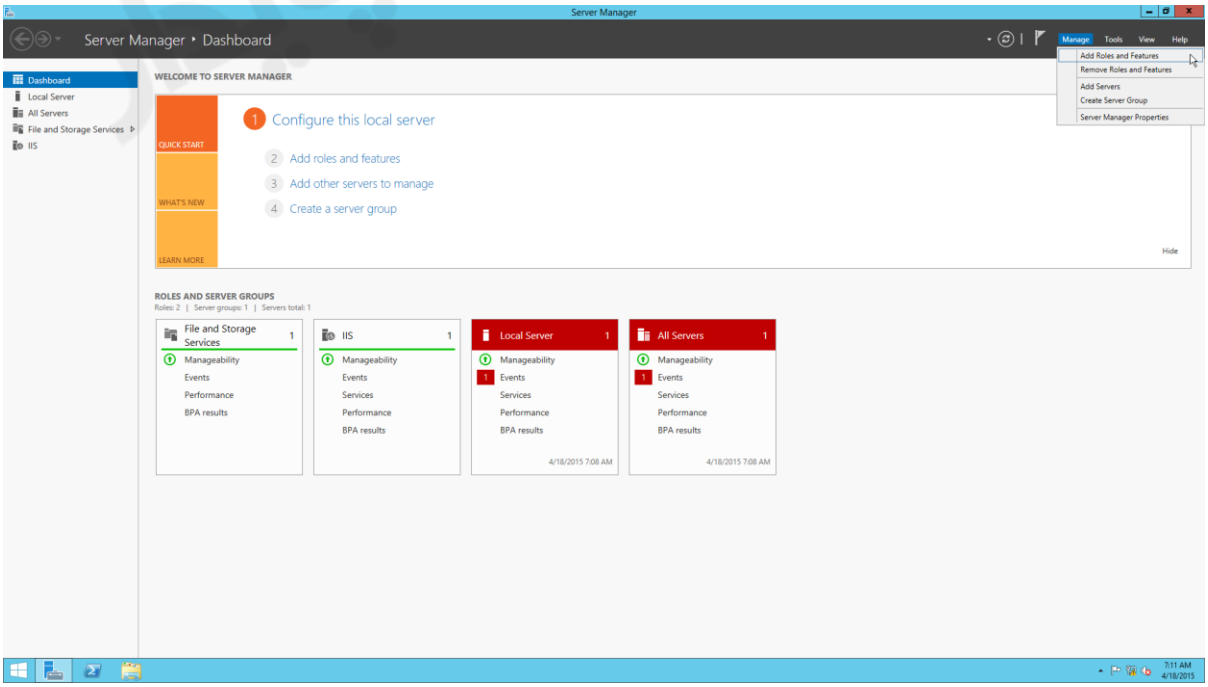
برای پیاده سازی این سناریو :

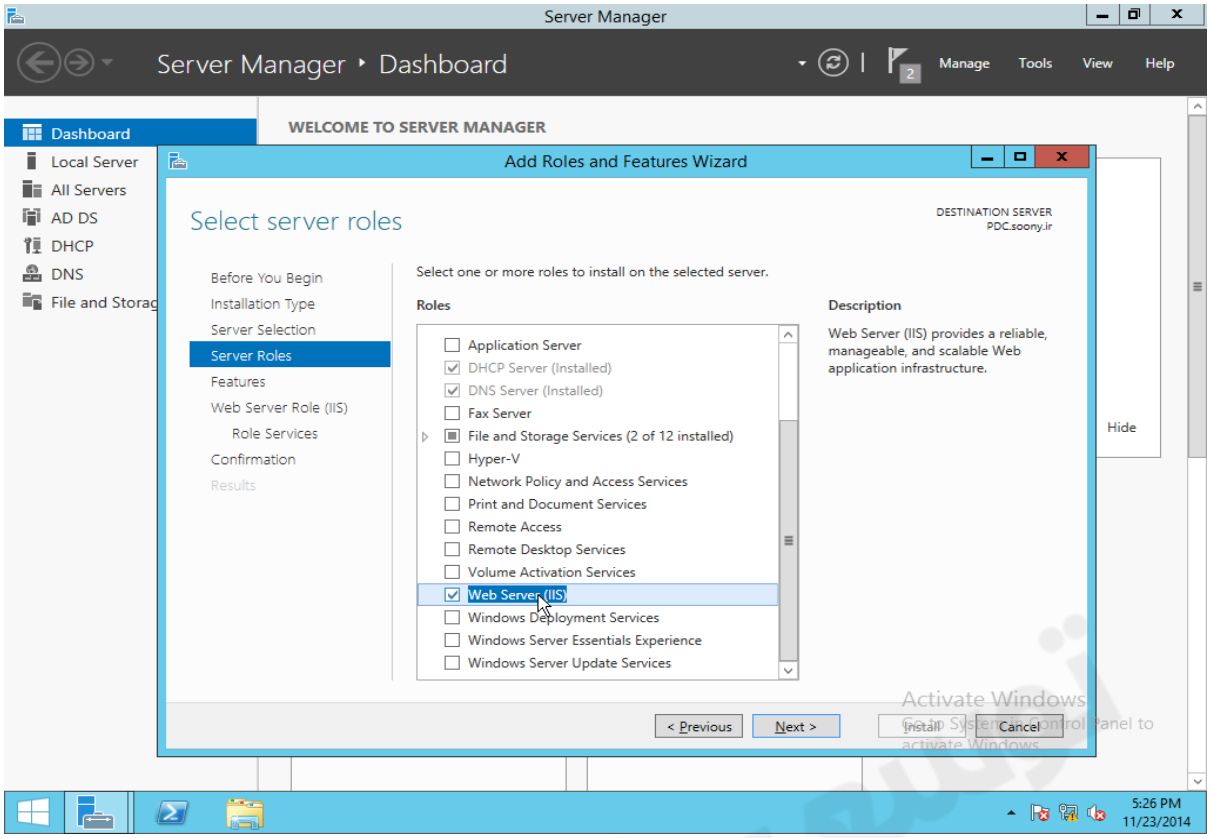
- سه روتر به عنوان مسیریاب های موجود در نظر گرفته شده است.روتر **R2** به عنوان روتر در دنیای اینترنت می باشد.
- یک سیستم به عنوان کلاینت در **Lan-1** در نظر گرفته شده است.
- یک ویندوز سرور۲۰۱۲ به عنوان وب سرور در شبکه **Lan-2** در نظر گرفته شده است.

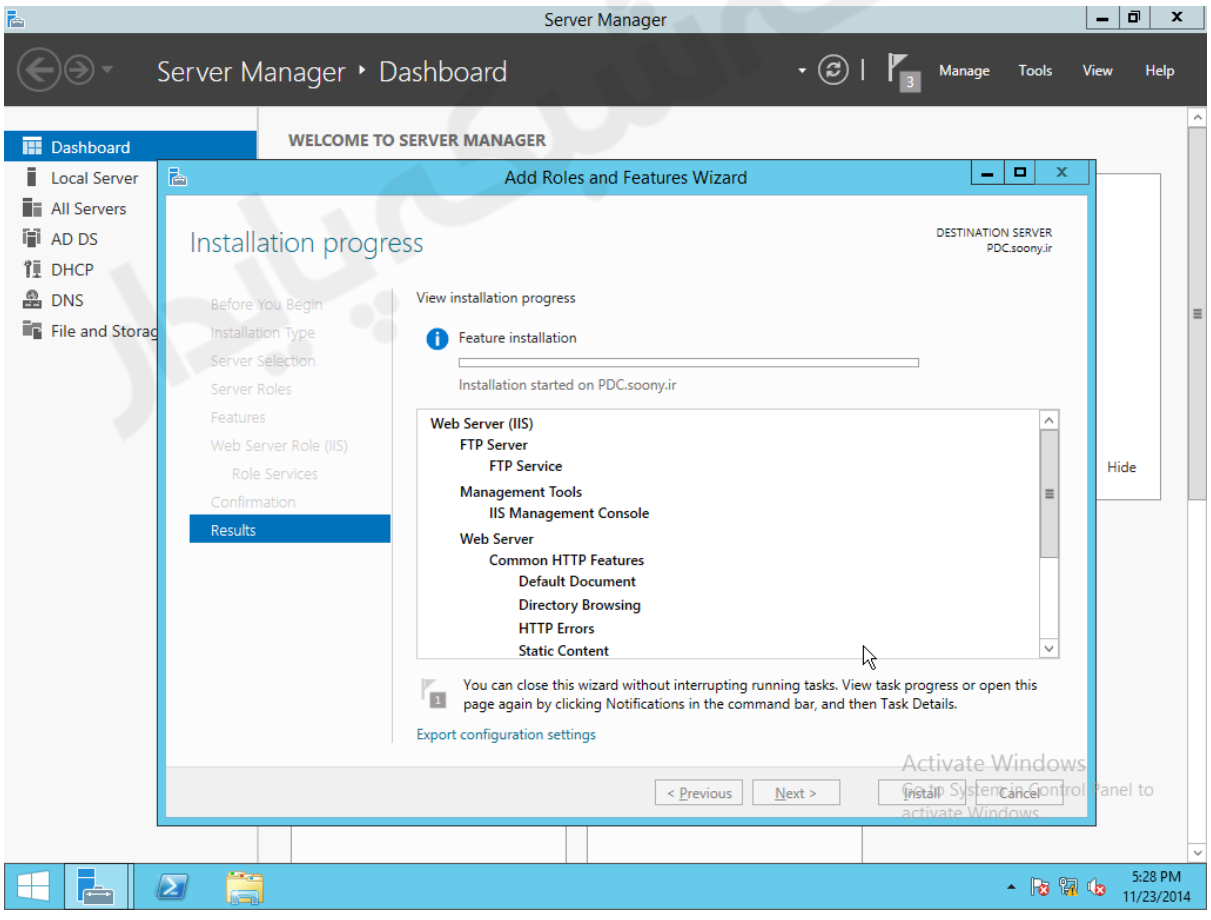
برای پیاده سازی این سناریو در ابتدا وب سرور را بروی ویندوز سرور ۲۰۱۲ نصب و راه اندازی می کنیم.

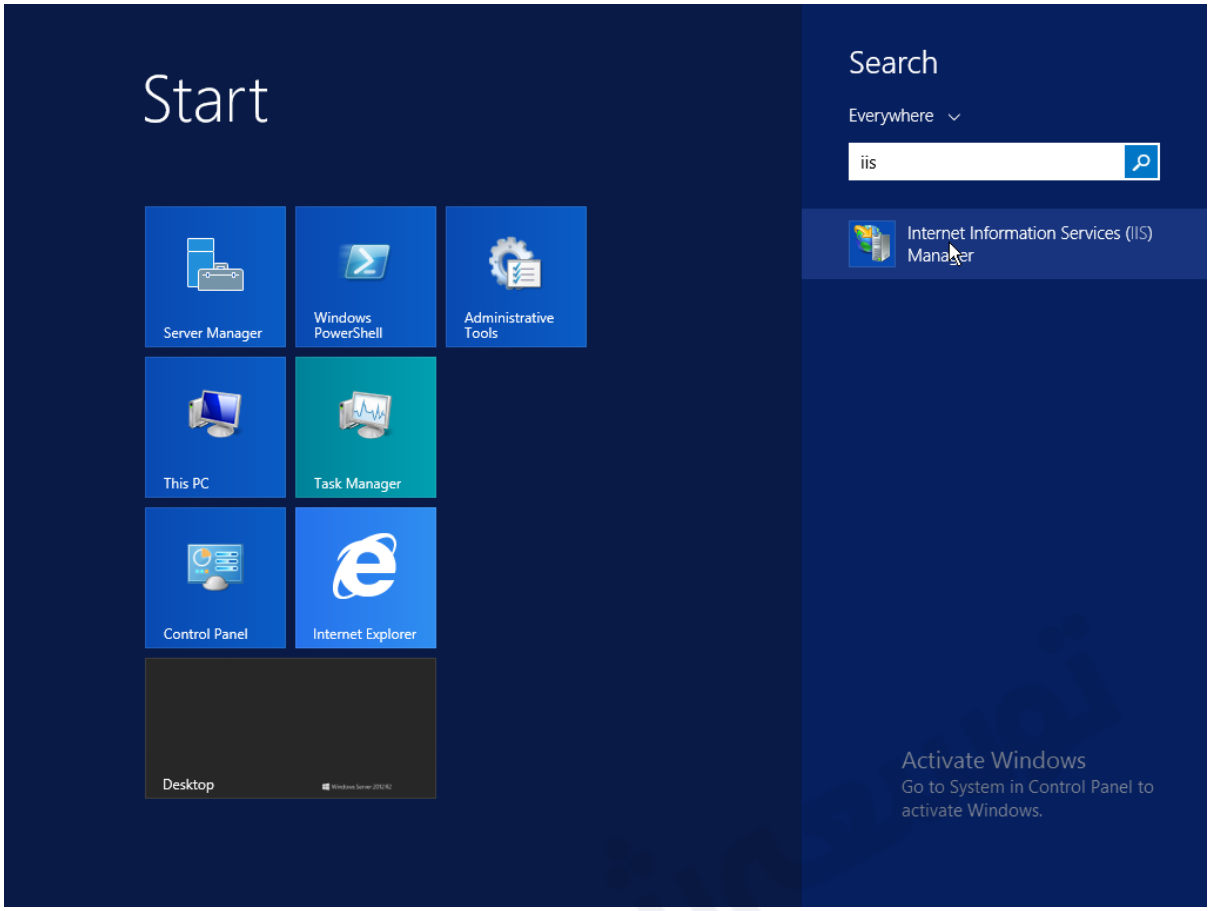
مراحل نصب و راه اندازی وب سرور :

Server Manager > Add Role & Features > Server Roles And Role Services

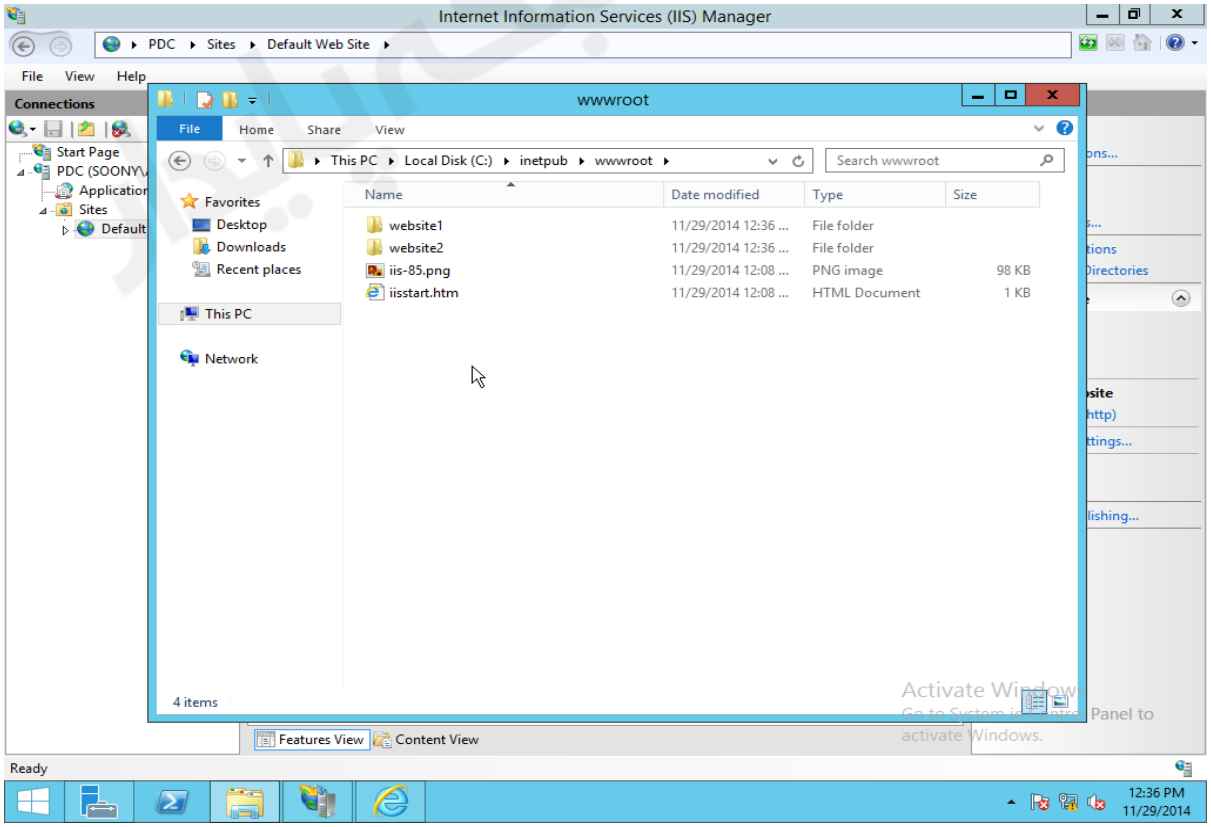



Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storag
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
PDC.soony.ir
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Application Server
DHCP Server (Installed)
DNS Server (Installed)
Fax Server
File and Storage Services (2 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Essentials Experience
Windows Server Update Services
Description
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
< Previous
Next >
Install
Cancel
Hide
Activate Windows
5:26 PM
11/23/2014

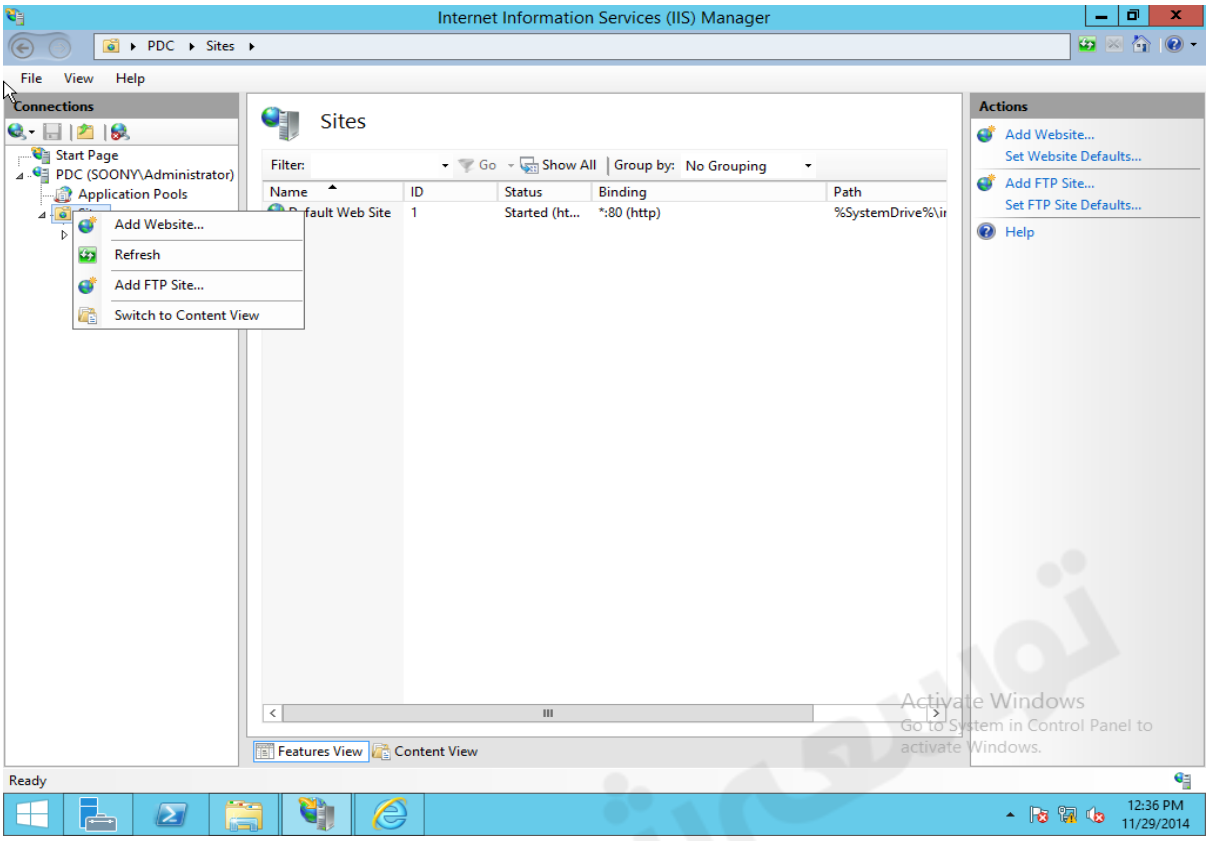

Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storag
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
PDC.soony.ir
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation started on PDC.soony.ir
Web Server (IIS)
FTP Server
FTP Service
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Install
Cancel
Hide
Activate Windows
5:28 PM
11/23/2014

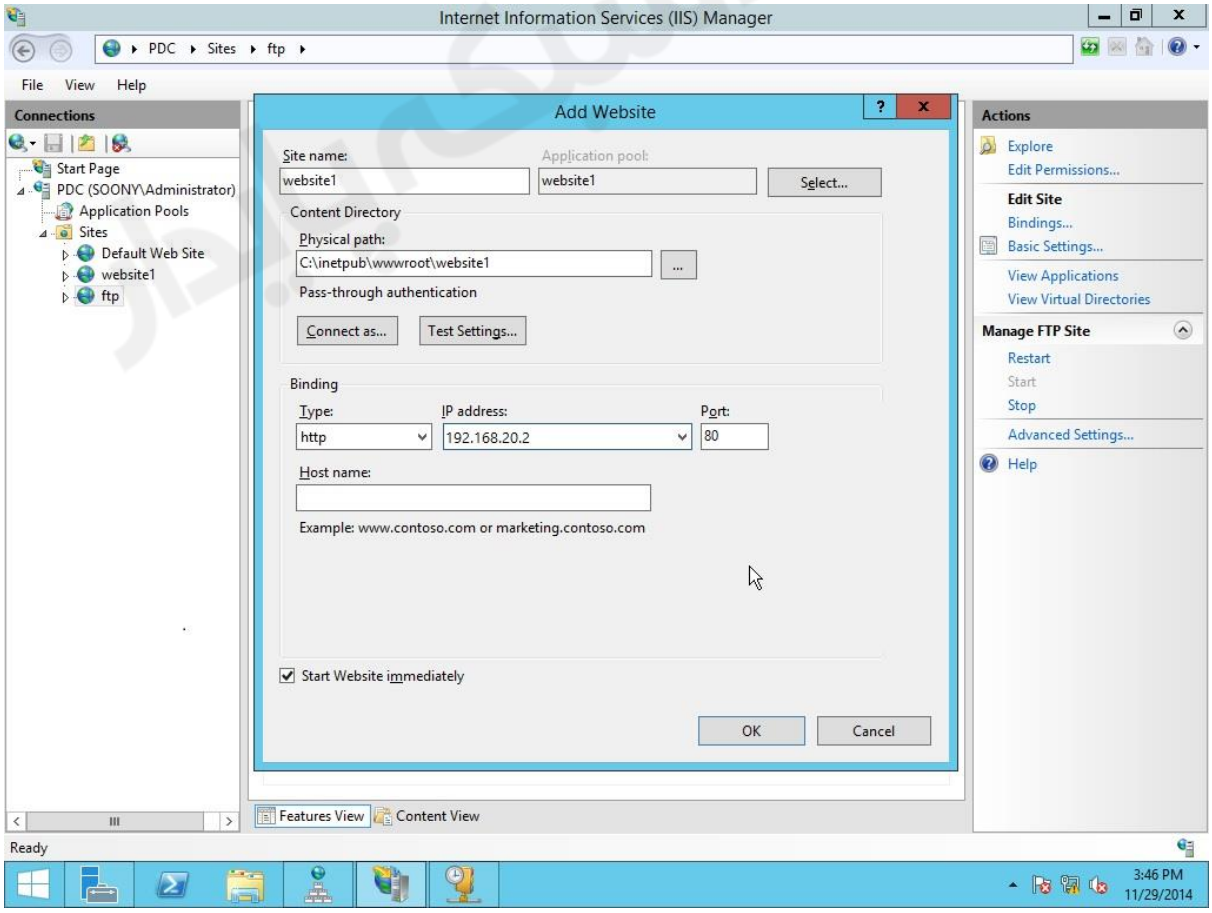


در یک درایو یک وب سایت ایجاد میکنیم.



نصب وب سایت : برروی **Site** کلیک راست و **...Add Website** را انتخاب میکنیم.





Site Name : اسم وب سایت است.

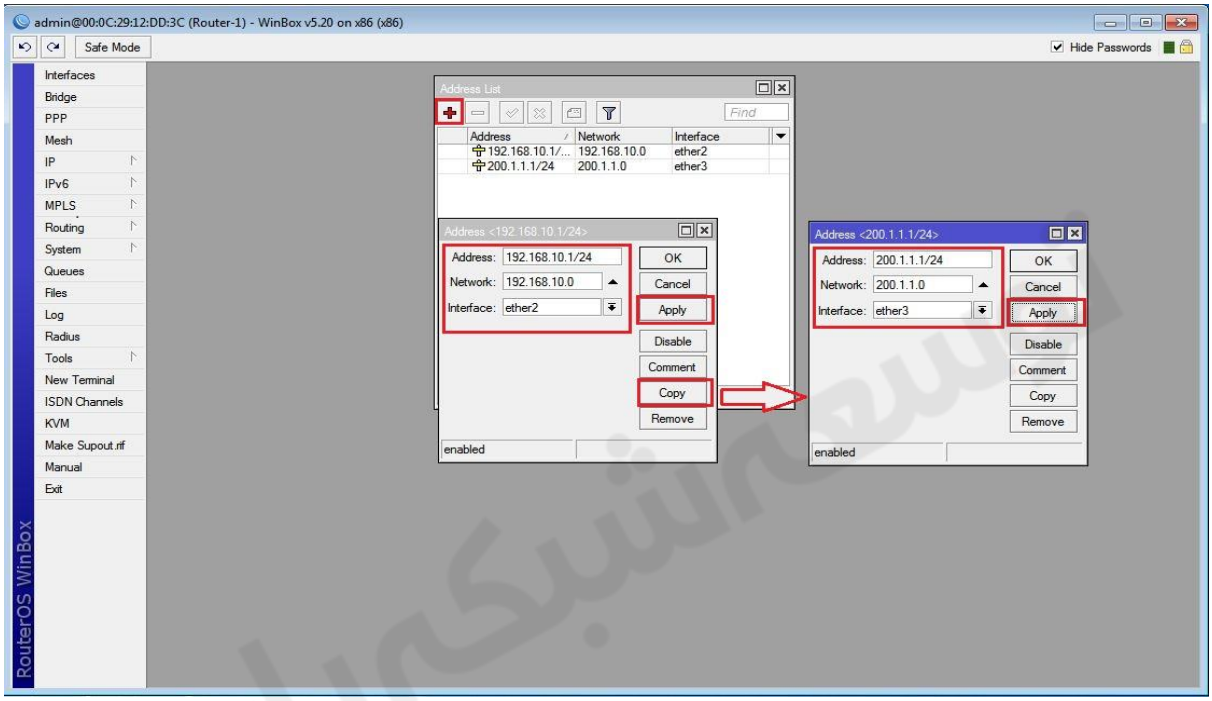
Physical Path : مسیر فیزیکی قرار گرفتن فایل های مربوط به وب سایت را مشخص می کند.

IP Address : از لیست باز شونده آدرس **IP** مورد نظر خودتان برای وب سایت را تعیین کنید و در صورتیکه مطمئن نیستید گزینه **All Unassigned**را بزنید تا تنظیمات پیشفرض ملاک قرار بگیرند.

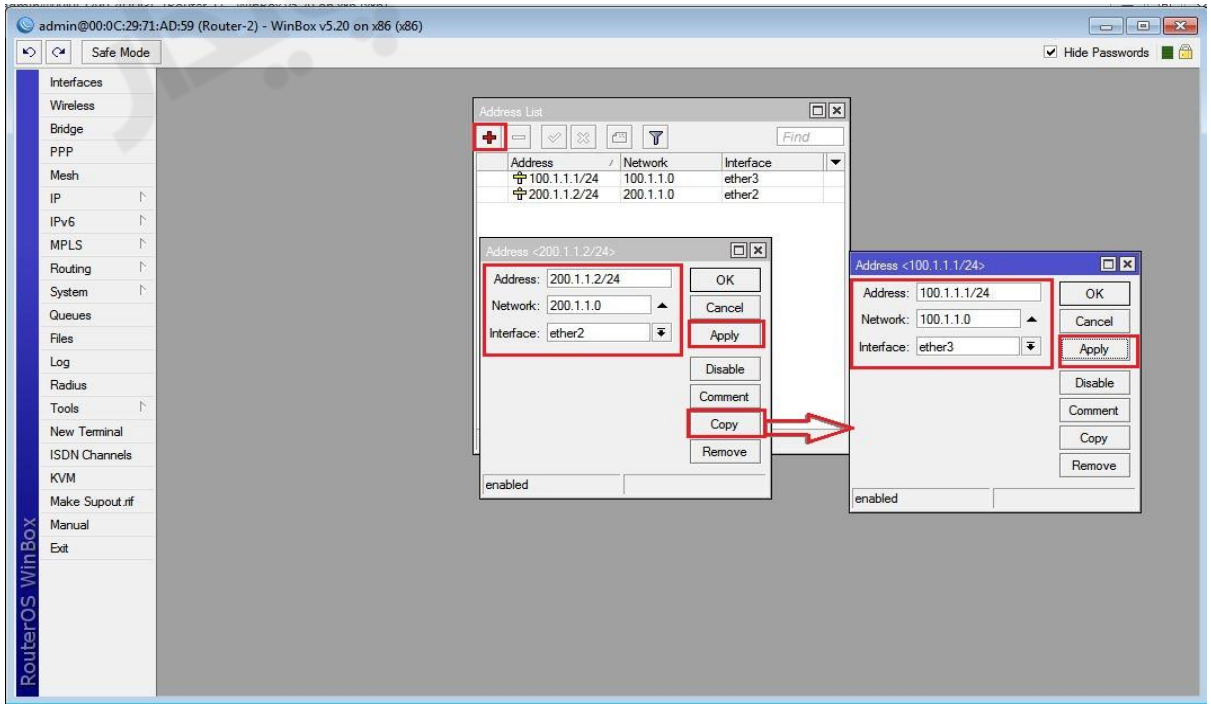
وب سرور اماده فعالیت است و کافیست که فایل های مربوط به وب سایت خود را در قسمتی که در **Physical Path** تعیین شده قرار داده و فایل اصلی را با عنوان **index.html** در آن قرار دهید و براحتی می توانید با استفاده از آدرس **IP** تخصیص داده شده به آن دسترسی داشته باشد.

انتساب **IP** به کارت های شبکه روترها :

روتر **R1** :

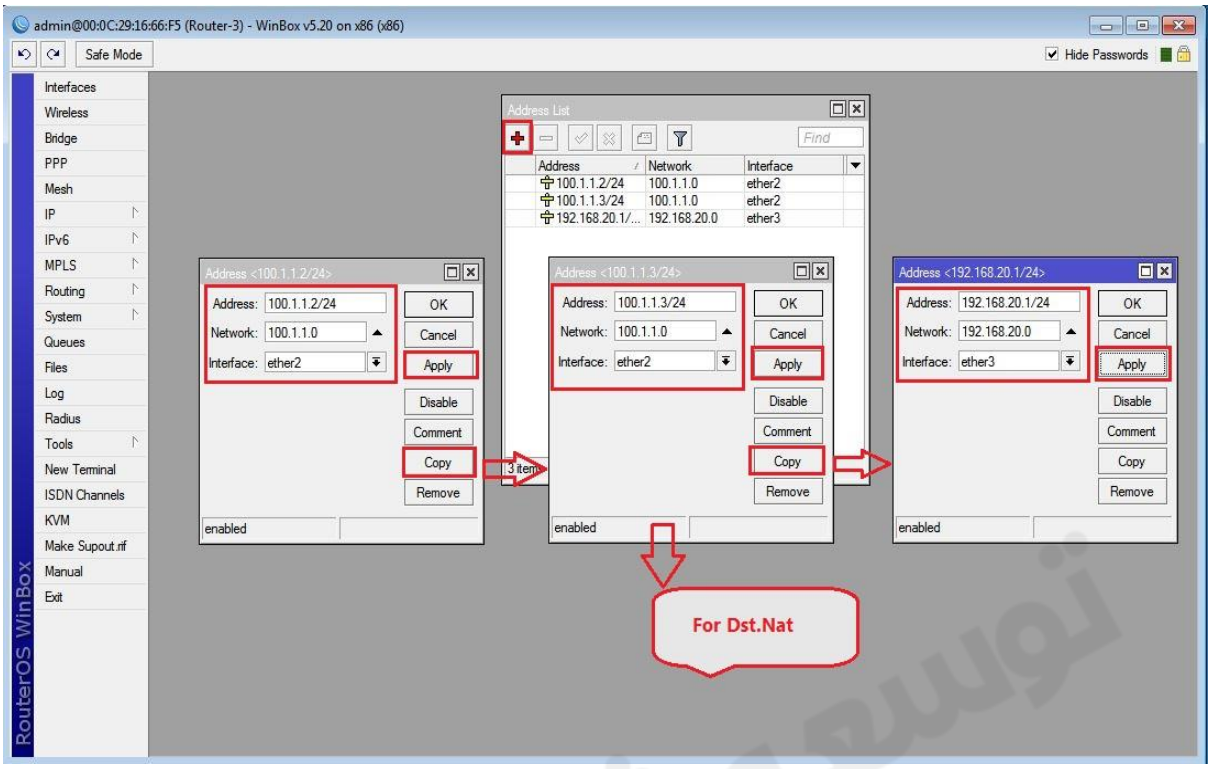


روتر **R2** :



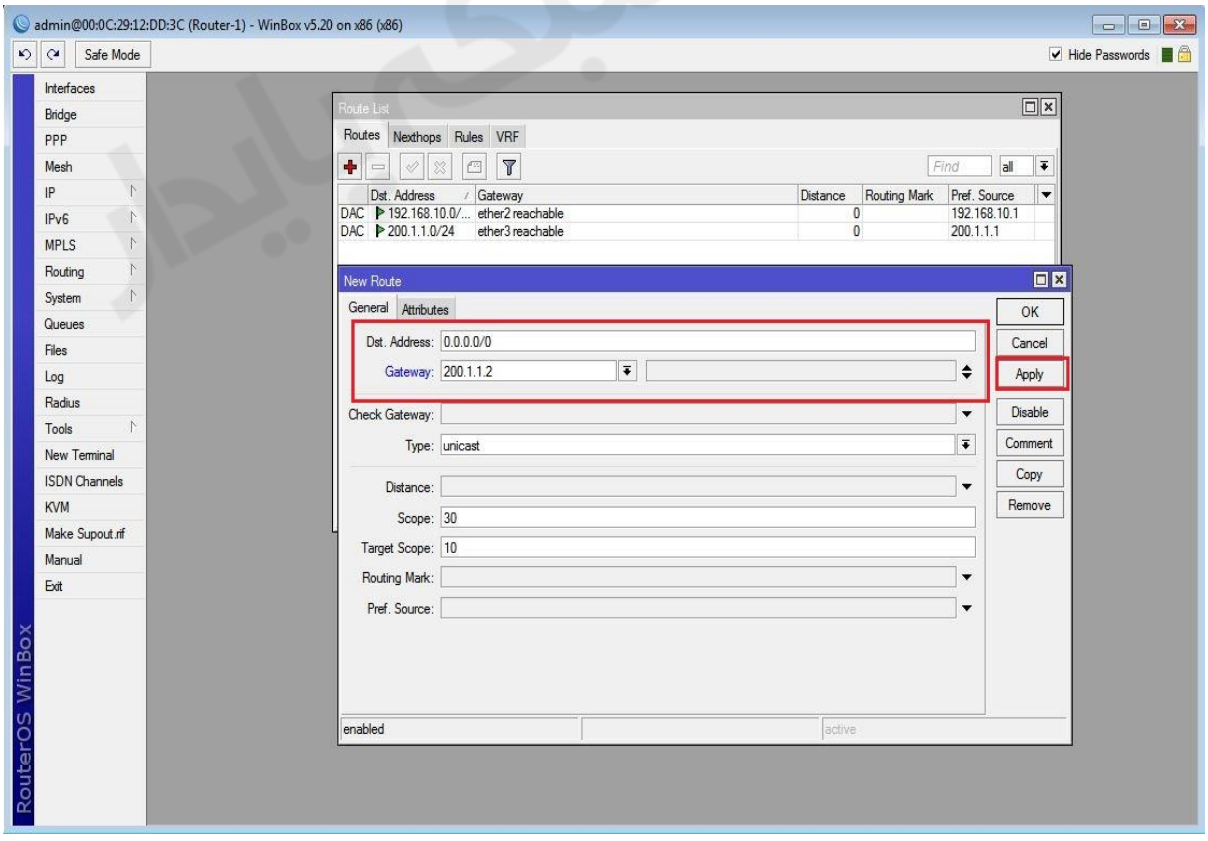
روتر **R3** :

دلیل اینکه در این روتر برای **Ether2** دوتا آدرس **IP** تنظیم کردیم این است که یکی **IP** ها را می خواهیم برای **Dst.Nat** استفاده کنیم.

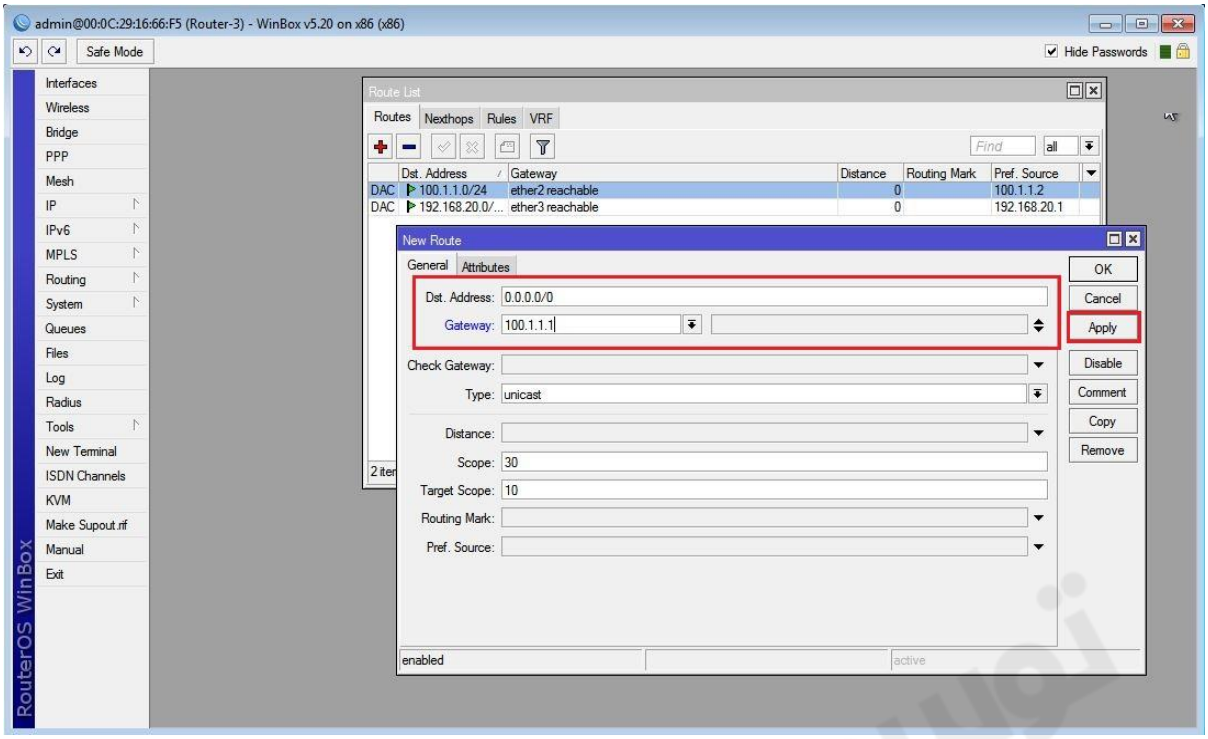


تا اینجا ارتباط بین روتر **R1** و **R3** برقرار نیست برای برقراری این ارتباط در هر دو روتر **Default Route** تعریف می کنیم

تعریف **Default Route** در روتر **R1** :

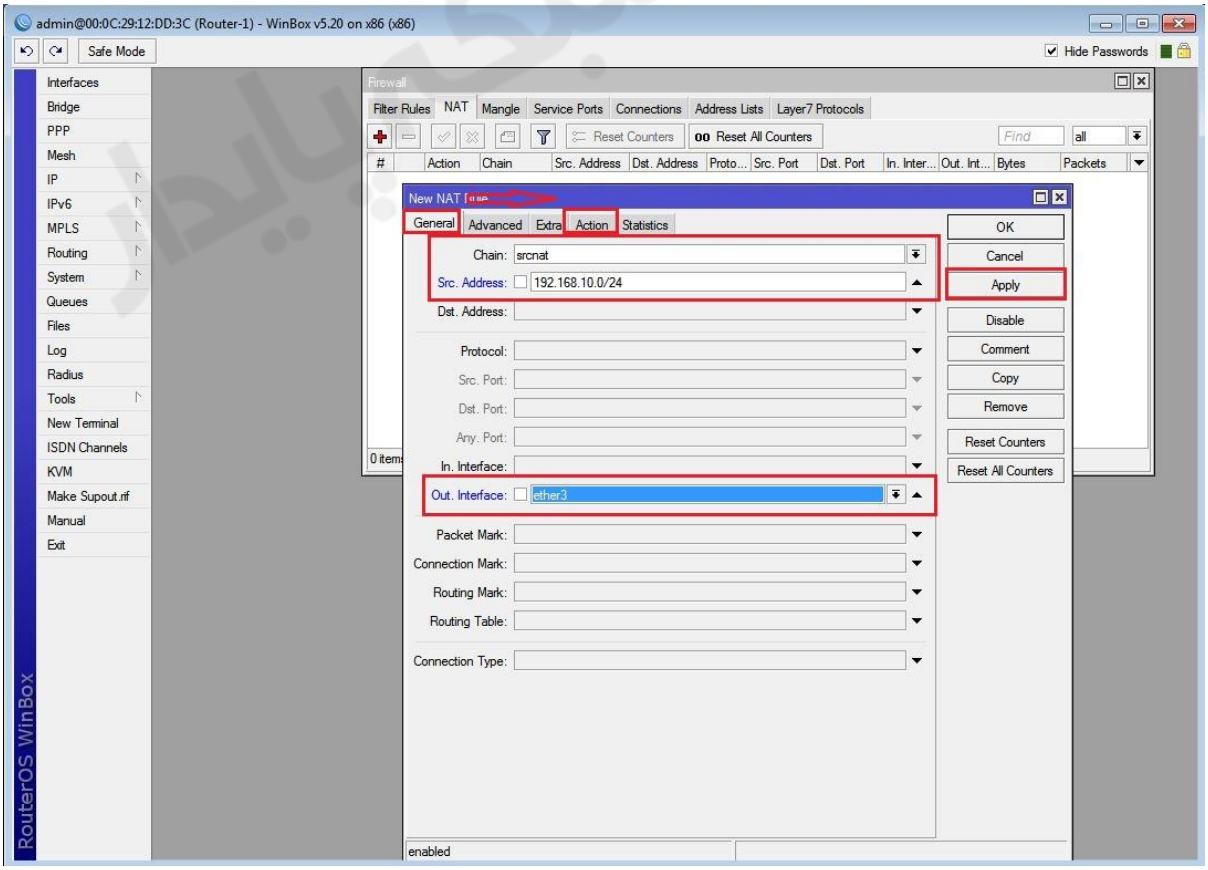


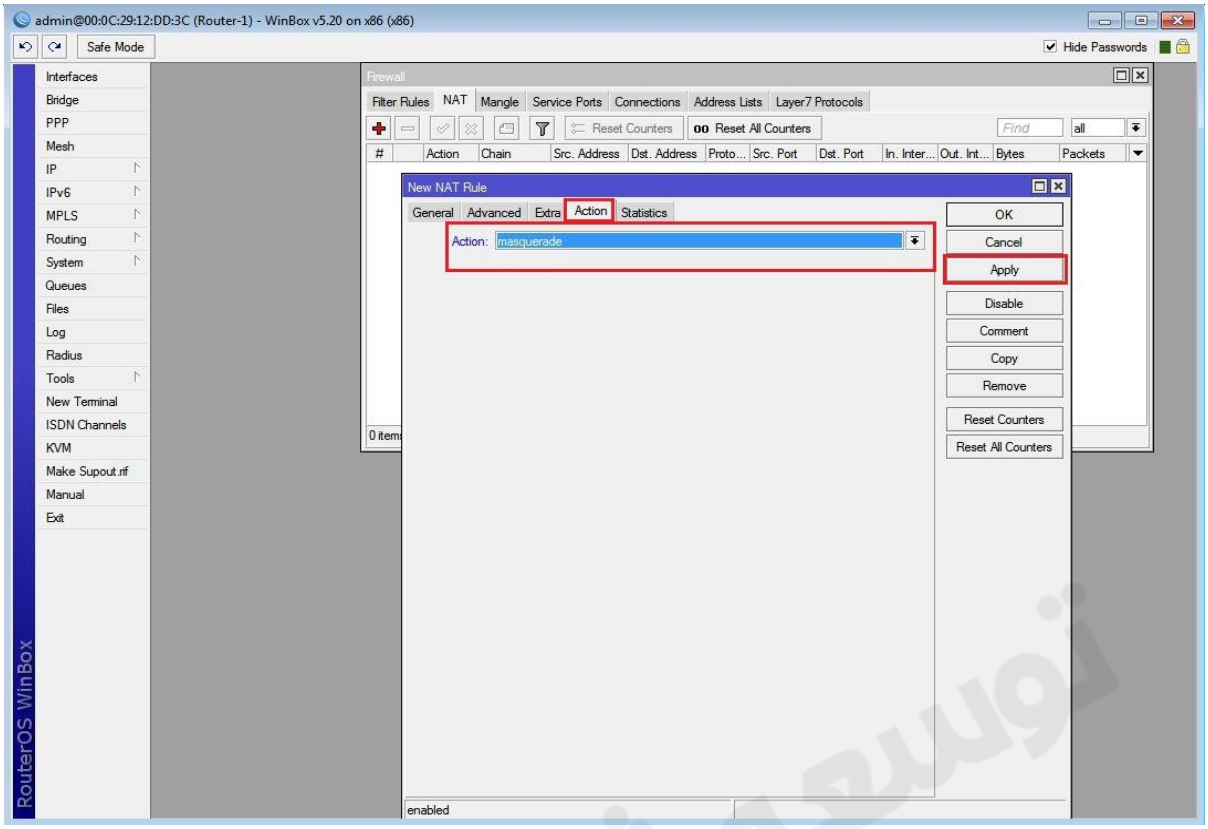
تعریف **Default Route** در روتر **R3** :



تا اینجای کار ارتباط بین روترها برقرار است اما کلاینت های موجود در شبکه Lan-1 به اینترنت دسترسی ندارند(در این سناریو روتر R2 به عنوان اینترنت در نظر گرفته شده است) برای اینکه کلاینت های Lan-1 به اینترنت دسترسی داشته باشند باید Nat اینجاد کنیم.

اعمال عملیات Nat برای بسته هایی که از طرف روتر R1 به سمت روتر R2 می آیند :

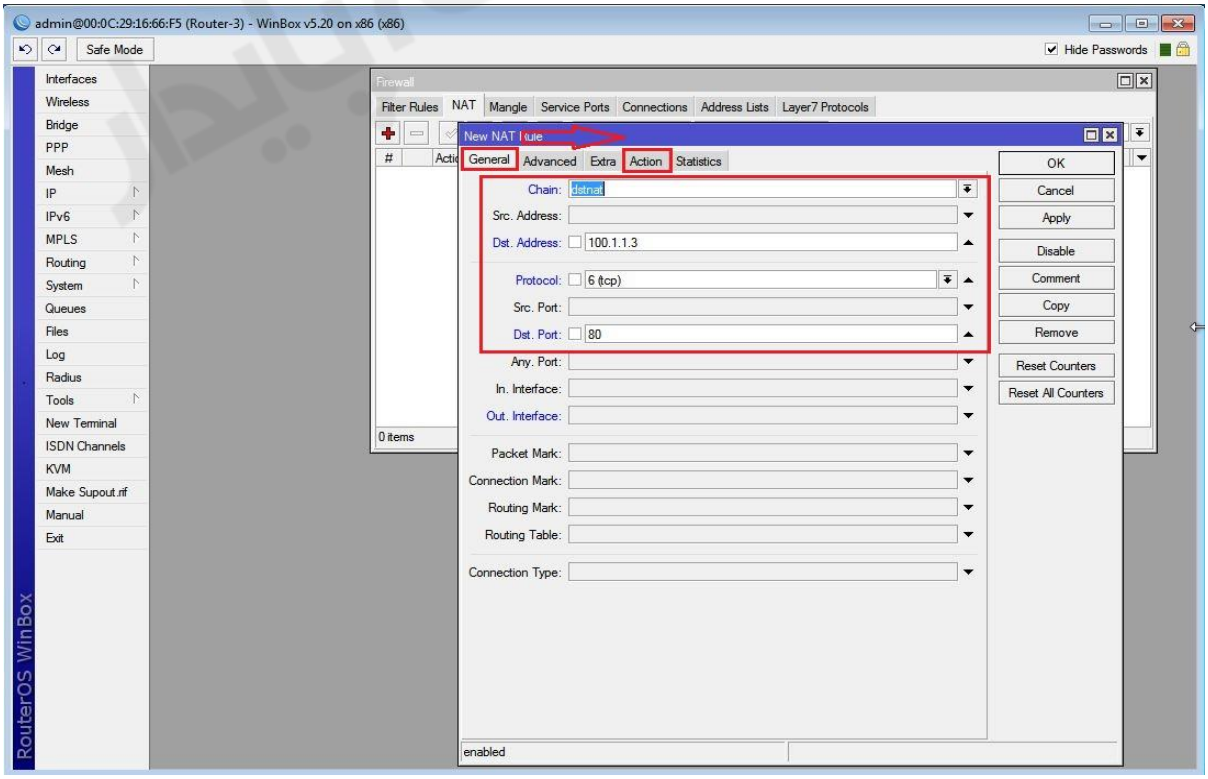


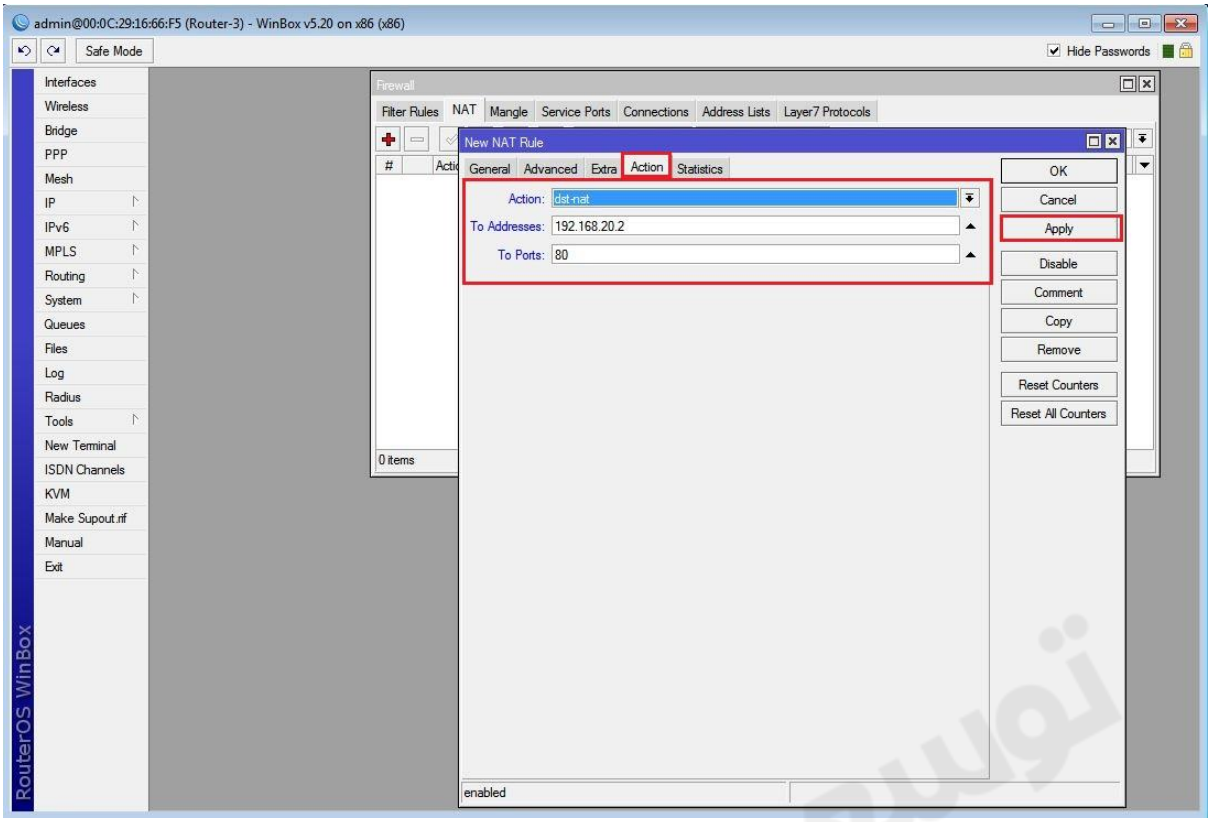


با این تنظیمات کلاینت های موجود در شبکه Lan-1 به اینترنت دسترسی پیدا می کند یعنی می تواند به روتر R2 و روتر R3 دسترسی داشته باشد.با این تنظیمات زمانی که کلاینت IP:100.1.1.3 را در مرورگر خود وارد می کند به صفحه Webfig روتر R3 دسترسی پیدا می کند در این سناریو هدف ما این بود که زمانی کلاینتی این IP را وارد کرد به وب سرور موجود در شبکه Lan-2 دسترسی پیدا کند.

برای اینکار باید یک Nat با تنظیمات زیر انجام دهیم.

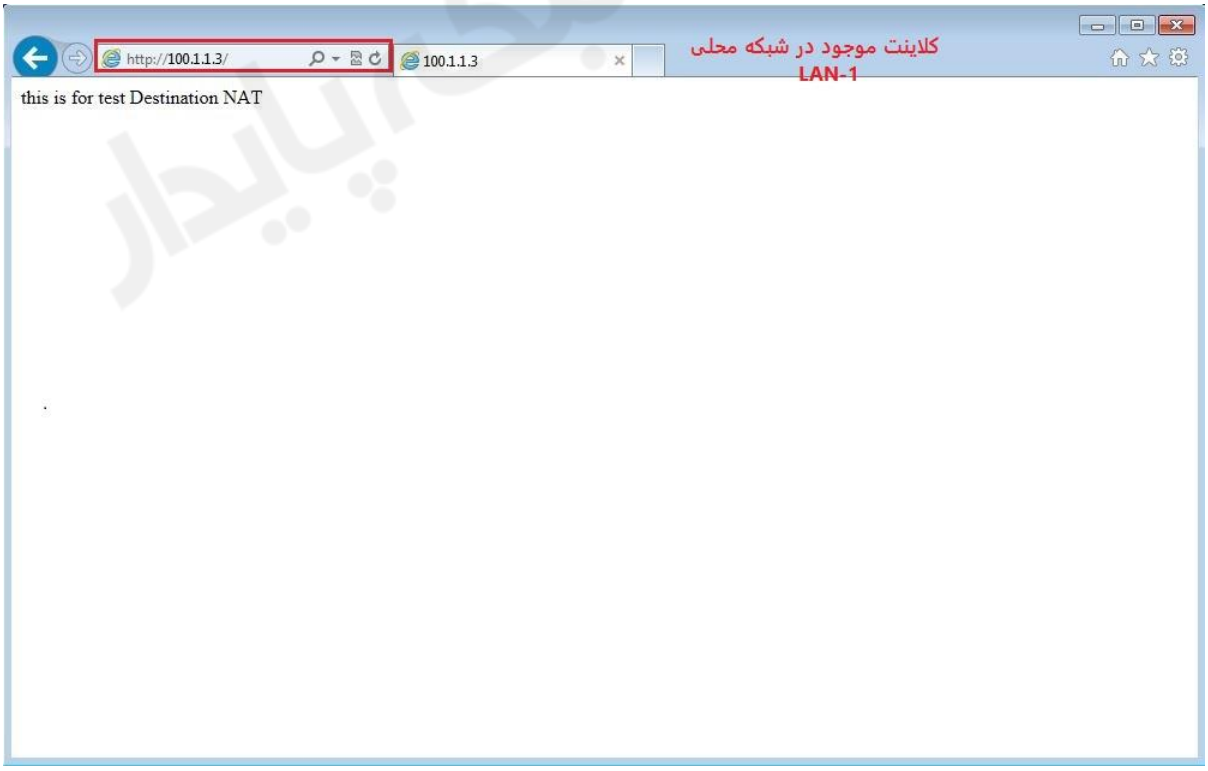
اعمال عملیات Nat کردن بسته هایی که از طرف اینترنت به سمت روترR3 می آیند :





تنظیمات IP کلاینت را همانند سناریو انجام می دهیم .

با تنظیمات IP در کلاینت و با تنظیماتی که بر روی روترها انجام دادیم زمانی که در سیستم کلاینت IP:100.1.1.3 را وارد کنیم به وب سرور دسترسی پیدا می کنیم.



فصل پنجم : فیلترینگ

Filtering :

یکی دیگر از قابلیت های فایروال ایجاد فیلترینگ است.در فیلترینگ پکت هایی که از روتر عبور می کنند تحت کنترل قرار می گیرند و براساس قوانینی که به آنها **Rule** گفته می شود فیلتر می شوند.

قاعده کلی فیلترینگ :

فایروال بر پایه ی رول های آن بنا شده است یعنی فایروال و روتر کاری را انجام می دهد که رول ها بگویند.

هر رول از دو قسمت تشکیل شده است :

- قسمت اول : ترافیک بسته ها را مشخص می کند(ترافیک ورودی و یا خروجی از میکروتیک).
- قسمت دوم : عملیاتی است که بر روی بسته ها انجام می شود.

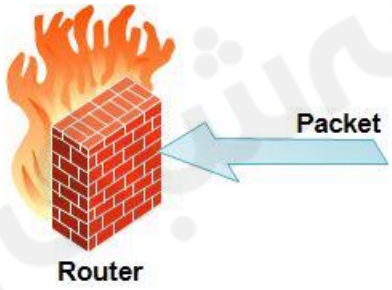
تنظیمات فیلترینگ در روتر :

```
[admin@Router-1]>ip firewall filter add chain=[input / output / forward] src-address=[source ip address]
action=[drop / accept / reject] dst-port=[destination port] protocol=[protocol]
```

پارامترهای مورد استفاده در **Rule** های فیلترینگ :

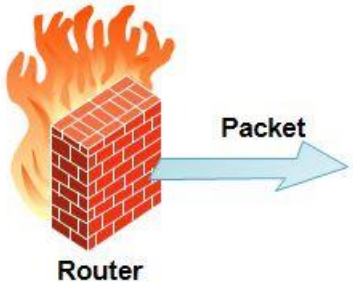
۱) **chain** : در این پارامتر ، مسیر ترافیک بسته های مورد نظر را مشخص می کنیم این پارامتر می تواند سه حالت را در بر گیرد :

۱-۱) **Input** : این حالت مربوط به پکت هایی است که مقصدشان خود دستگاه میکروتیک است.



بطور مثال : ارسال بسته های **ICMP** برای **Ping** کردن روتر میکروتیک و یا زمانی که شما با ساتفاده از **WinBox** و **SSH** و ... ممکن است به میکروتیک متصل شوید بنابراین **Chain=Input** قرار م دهیم.

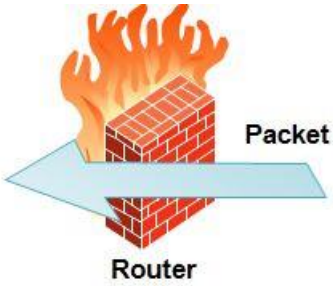
۱-۲) **Output** : این حالت مربوط به بسته هایی است که از روتر میکروتیک خارج می شوند.



بطور مثال : بسته هایی که از داخل روتر سعی در **Telnet** زدن به سیستم یا دستگاهی را داشته باشند و یا روتر سعی در اتصال به سرویس دهنده های **DNS** و **NTP** و ... را داشته باشد.

۱-۳) **Forward** : این حالت مربوط به ترافیکی است که از روتر شما عبور می کند.

فرایند ارسال بسته از یک کارت شبکه روتر به کارت شبکه دیگر آن را **Forward** می گویند.



بطور مثال : یک سیستم داخلی درخواست سایتی را از اینترنت داشته باشد و چنانچه روتر شما نقش **Gateway** در شبکه را داشته باشد روتر بسته درخواست را از کارت شبکه ایی که به شبکه داخلی مرتبط باشد دریافت می کند و به کارت شبکه ایی که به **WAN** مرتبط است ارسال می کند.

۲)**Action** :در این پارامتر عملیاتی که بر روی **Packet**ها اعمال می شود را تعیین می کنیم.

۲-۱)**Accept** : در این حالت به بسته ها اجازه عبور داده می شود.

۲-۲)**Drop** : در این حالت به بسته اجازه عبور داده نمی شود.به عبارتی بسته ها متوقف می شوند و هیچ جوابی به فرستنده بسته ها داده نمی شود.

۲-۳)**Reject** : همانند **Drop** است با این تفاوت که پیامی با استفاده از بسته **ICMP** نیز به کاربر نشان می دهد.

۲-۴)**add-dst-to-address-list** : **IP** مقصد را ذخیره می کند.

۲-۵)**add-dst-to-address-list** : **IP** مبدا را ذخیره می کند.

قبل از اینکه به رفتار این دو به پردازیم بهتر است با **Address List** ها آشنا بشیم.**Address List**ها زمانی به کار می آیند که شما بخواهید برای تعداد زیادی **IP** که از یک محدوده یا رنج نیستند تصمیم بگیرید.مثلا می خواهیم سه **IP** جدا را از دسترسی به وب محروم کنیم بدون استفاده از **Address List**ها باید سه رول متفاوت را بنویسیم.اگر این تعداد **IP**ها ۱۰۰ تا بود چه اتفاقی می افتاد ؟ برای راحتی اینگونه موارد از آدرس لیست ها استفاده می شود.به این معنی که آدرس های مورد نظر را در یک لیست قرار داده و به ازای آن لیست یک رول را می نویسیم.

در صورتی که خواسته باشید بعضی از **IP**های ورودی رو **Log** کنید مثلا کسانی که سعی می کنند از طریق **Winbox** به روتر وصل شوند می توان به کمک دو **Action** بالا یک لیست آدرس از آنها تهیه کنید.

۲-۶)**Log** : تقریبا شبیه دو مورد بالا می باشد اما با چند تفاوت مهم . **Log** یک سری اطلاعات را برای ما ذخیره می کند که این اطلاعات از طریق منوی اصلی گزینه **Log** قابل دسترس می باشد این اطلاعات شامل موارد زیر می باشد :

In-interface,out-interface,src-mac,protocol,src-port

اولین تفاوت همین اطلاعات بالا می باشد که با اطلاعات ذخیره شده قبل متفاوت می باشد و دوم اینکه شما از لیست آدرس ها در رول های بعدی می توانید استفاده کنید اما **Log** صرفا جهت اطلاع می باشد.

۲-۷)**Jump** : پرش به زنجیره **Chain** مشخص شده است.

۲-۸)**Return** : برگرداندن کنترل به زنجیره در جایی که پرش صورت گرفته است

۲-۹)**Trapit** : ضبط و نگهداری ارتباط **Tcp** (کاربرد در کم کردن اثر حملات **Dos**).این **Action** بسته های **Tcp** را نگه میدارد و به آنها جواب مناسبی می دهد.

۲-۱۰)**Passthrough** :این **Action** کار خاصی انجام نمی دهد صرفا از رول خارج می شود یا صرف نظر می کند.در نظر نگرفتن قانون و رفتن به قانون بعدی(کاربرد : بیشتر برای آمار گیری)

۳)**Src-Address** : برای مشخص کردن آدرس فرستنده یک بسته ، از این پارامتر استفاده می کنیم.

بطور مثال : چنانچه بخواهیم بسته هایی که فقط از سمت یک سیستم خاص به روتر می رسند را فیلتر کنیم آدرس **IP** سیستم فرستنده را در این پارامتر مشخص می کنیم.

نکته : چنانچه بخواهیم بسته های مربوط به تمامی کلاینت های موجود در شبکه مبدا را فیلتر کنیم پارامتر **Src-Address** را خالی می گذاریم.

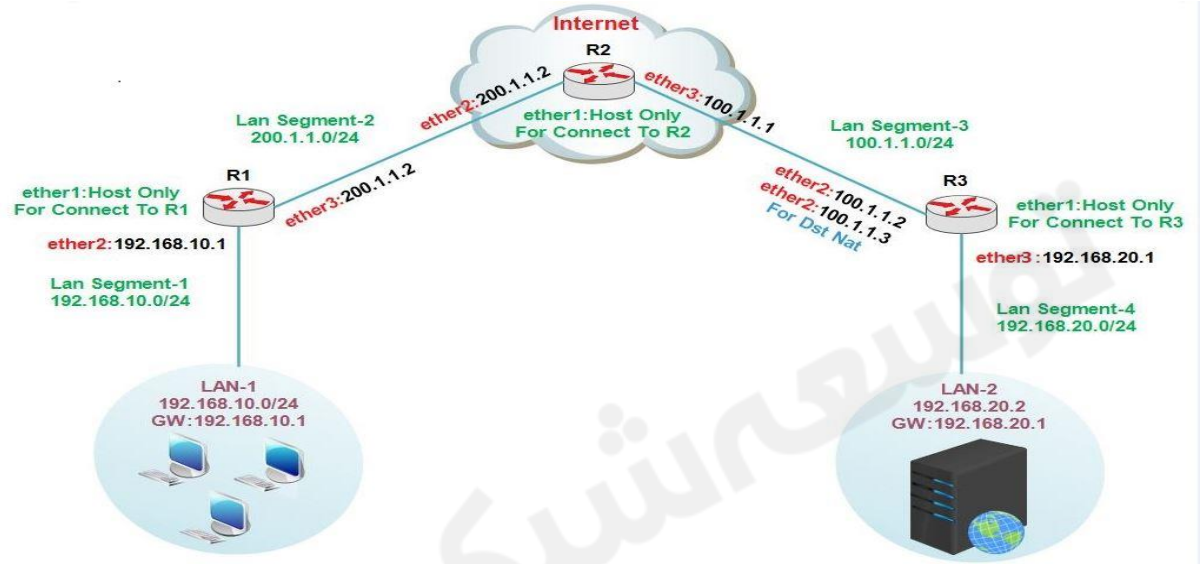
۴) **Dst-Port** : برای اعمال فیلترینگ بر روی بسته هایی که مقصد آنها پورت خاصی باشد از این پارمتر استفاده می شود.

نکته : چنانچه در دستور فیلترینگ این پارامتر را ذکر نکنیم کل پورت ها را در نظر میگیرد.

۵) **Protocol** : برای اعمال فیلترینگ بر روی بسته هایی که مقصد آنها پروتکل خاصی باشد از این پارامتر استفاده می شود.

بطور مثال : بسته های مربوط به پروتکل **ICMP** برای **Ping** کردن

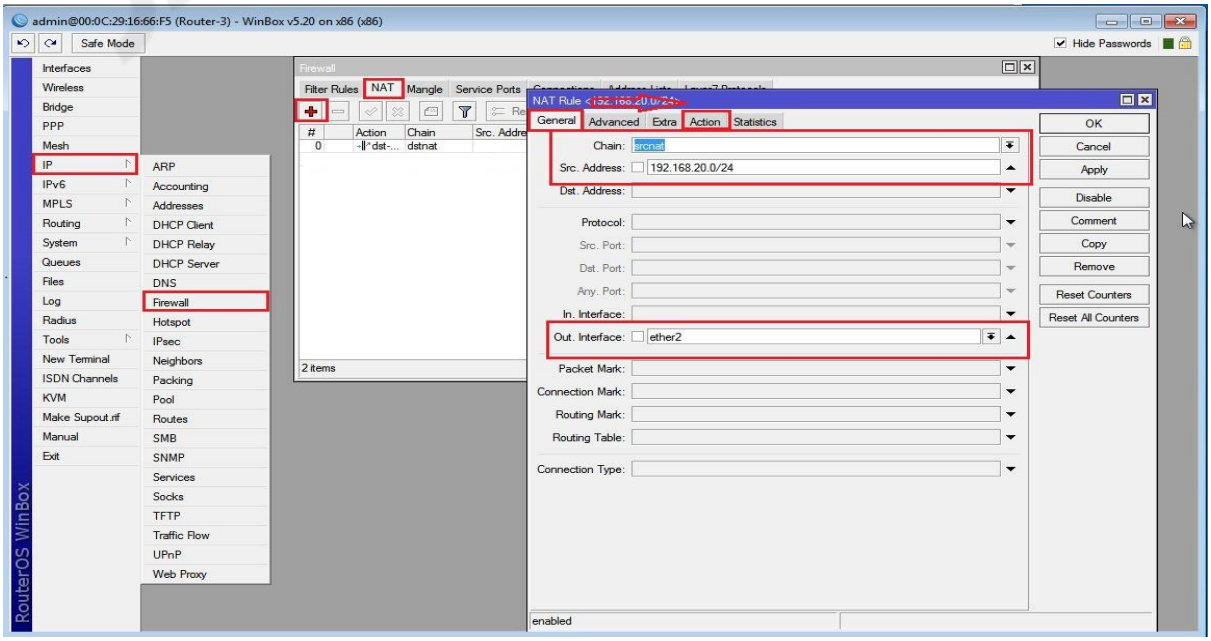
سناریو ۱ : هدف از انجام این سناریو بررسی مثال هایی از تنظیمات **Filtering** می باشد.

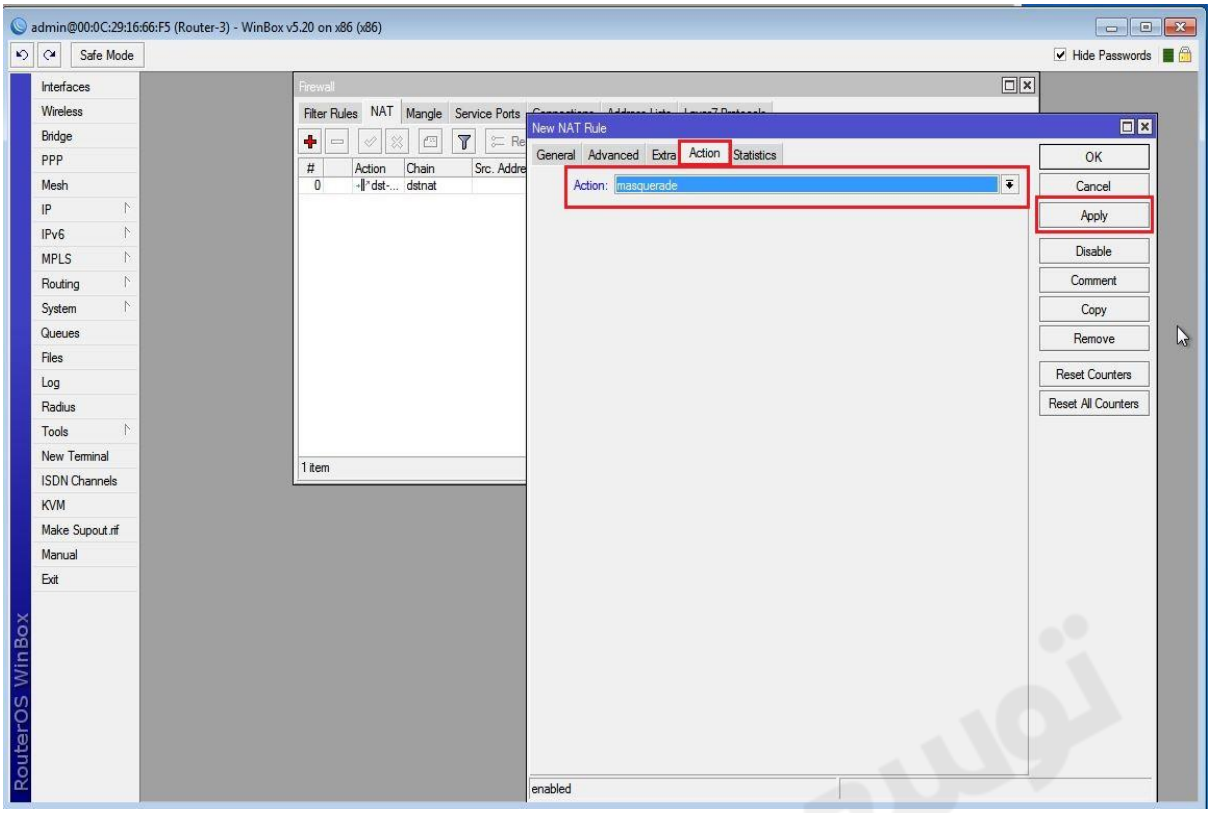


این سناریو همان سناریو **Destination Nat** می باشد و تمامی تنظیمات همان تنظیمات قبل می باشد فقط در سناریو **Destination Nat** شبکه محلی **Lan-2** به اینترنت دسترسی نداشت که در این سناریو بروی روتر **R3** ، **Nat** ایجاد می کنیم تا **Lan-2** نیز به اینترنت دسترسی داشته باشد.

نکته : توجه داشته باشید در این سناریو روتر **R2** به عنوان اینترنت در نظر گرفته شده است.

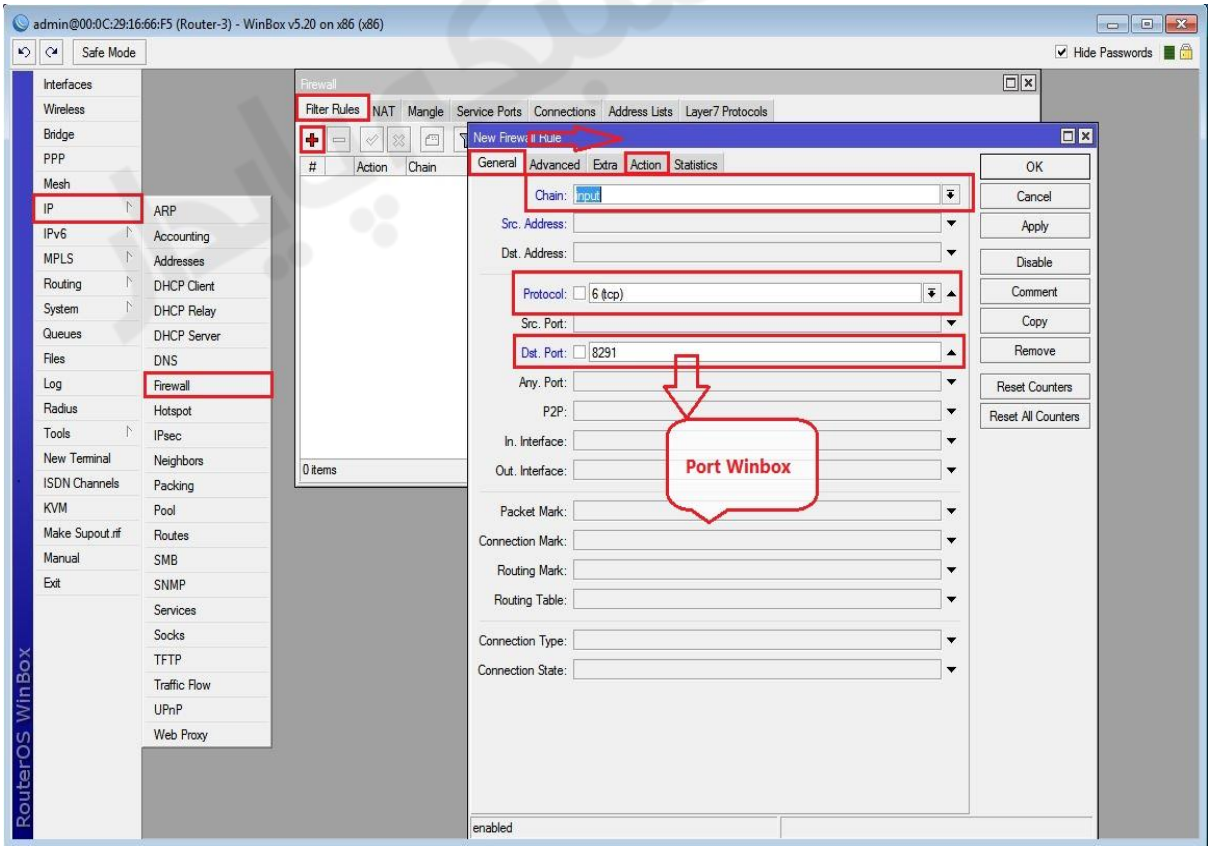
اعمال عملیات **Nat** بر روی بسته هایی که به سمت روتر **R3** می آیند :

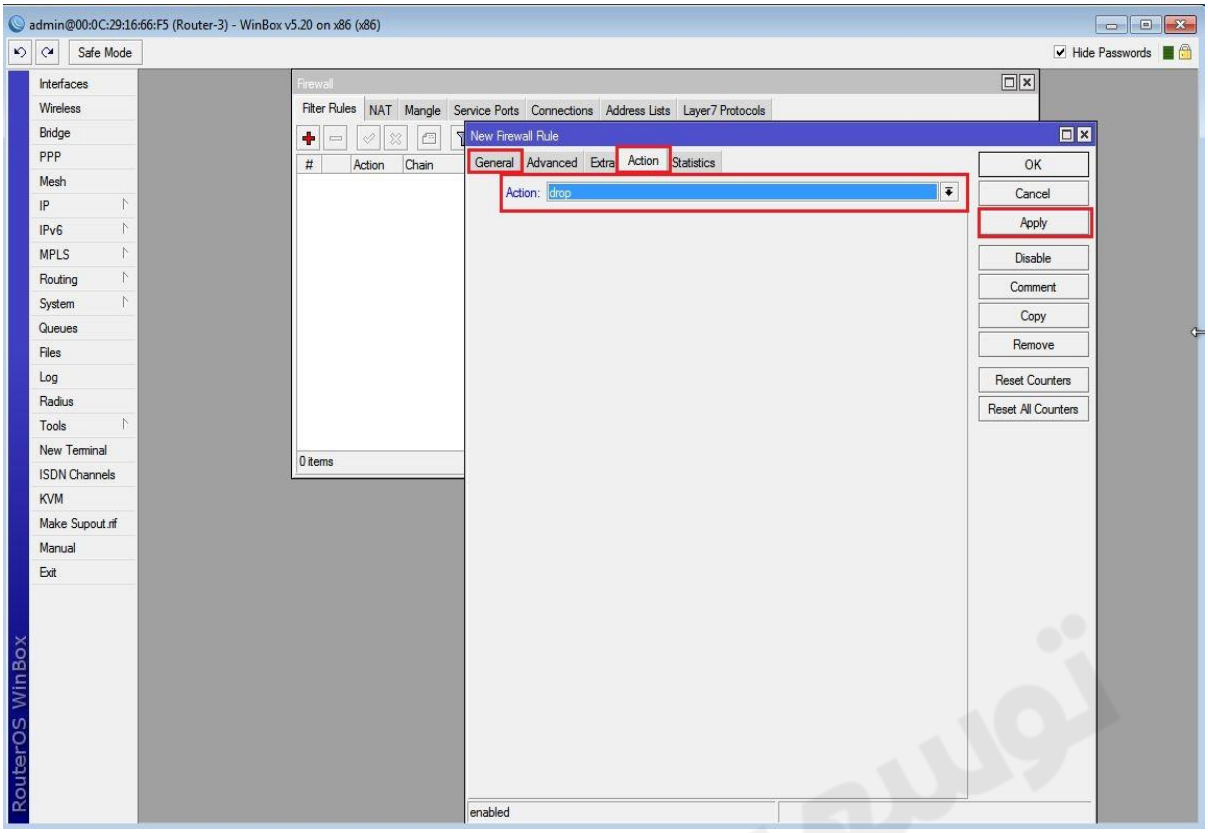




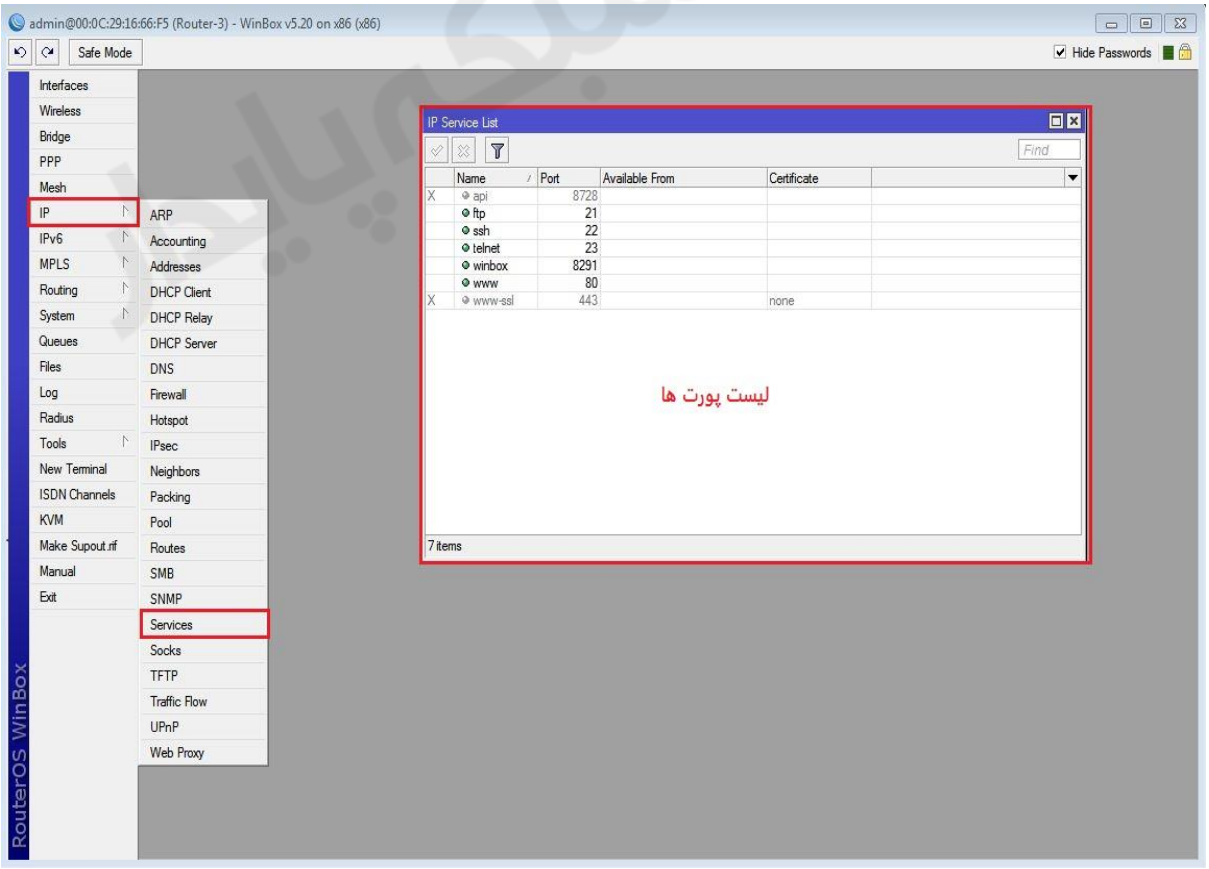
مثال ۱)هیچ سیستمی نتوانند از طریق Winbox به روتر R3 متصل شوند :

برای ایجاد فیلترینگ از منوی اصلی گزینه IP و از زیرمنوی باز شده Firewall را انتخاب می کنیم در پنجره باز شده به بخش Filter Rule رفته و برروی ADD کلیک می کنیم در پنجره باز شده فیلتر مورد نظر را ایجاد می کنیم.

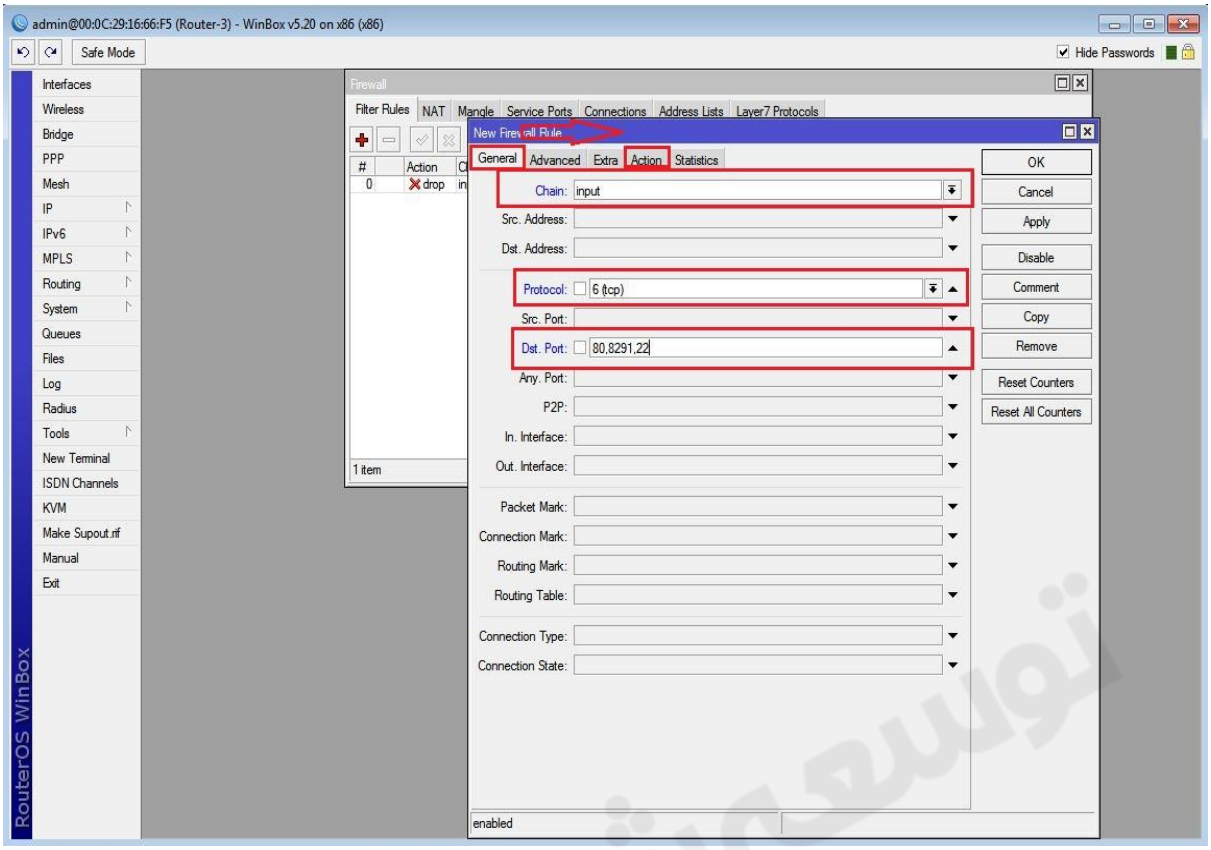


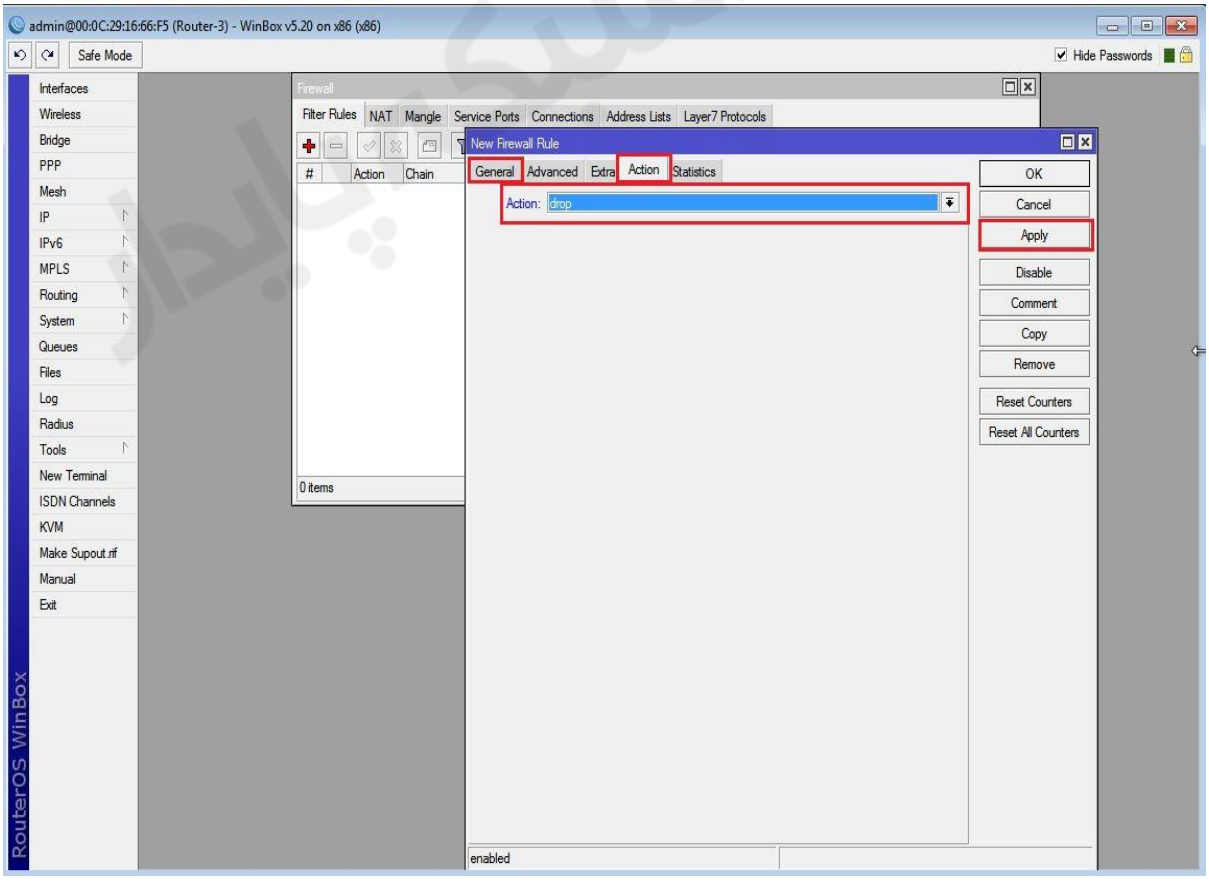


برای دیدن لیست پورت ها می توانیم از منوی اصلی گزینه IP و از زیرمنوی بازشده Services را انتخاب کنیم در پنجره باز شده لیست پورت ها را مشاهده می کنید.



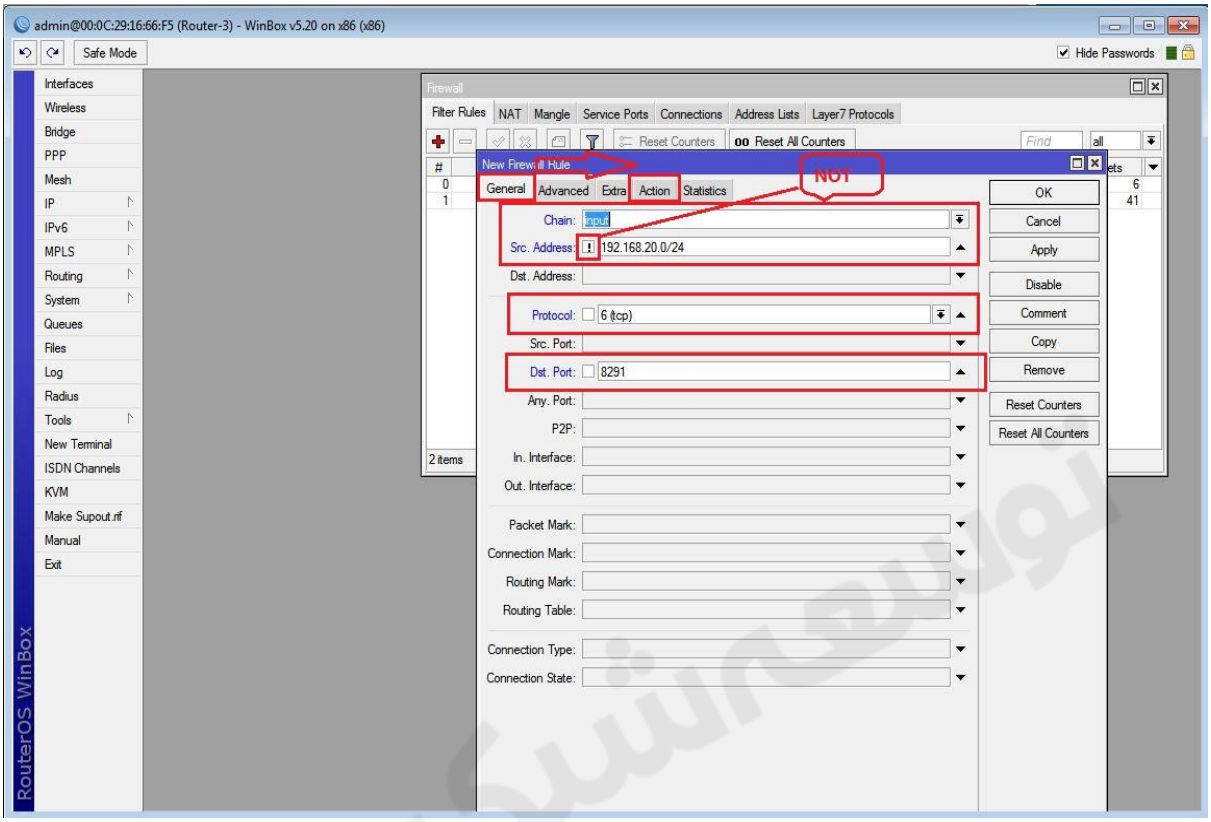
مثال ۲)هیچ شبکه ایی نتواند به روتر R3 دسترسی داشته باشد(Webfig و SSH و Winbox)

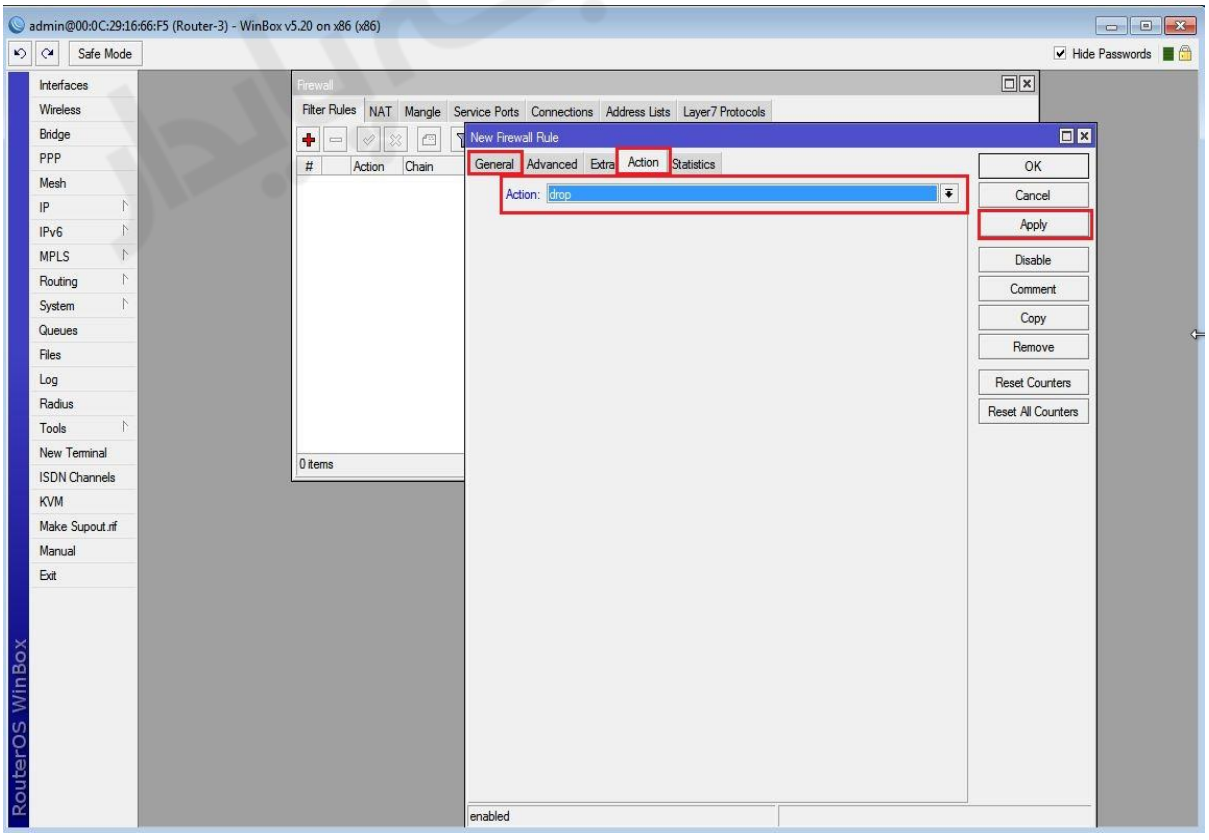




مثال ۳)شبکه ایی که مستقیم به روتر **R3** در ارتباط است(یعنی **Lan-2**) بتواند با **Winbox** به روتر **R3** دسترسی داشته باشد اما بقیه شبکه ها نتوانند دسترسی داشته باشند.

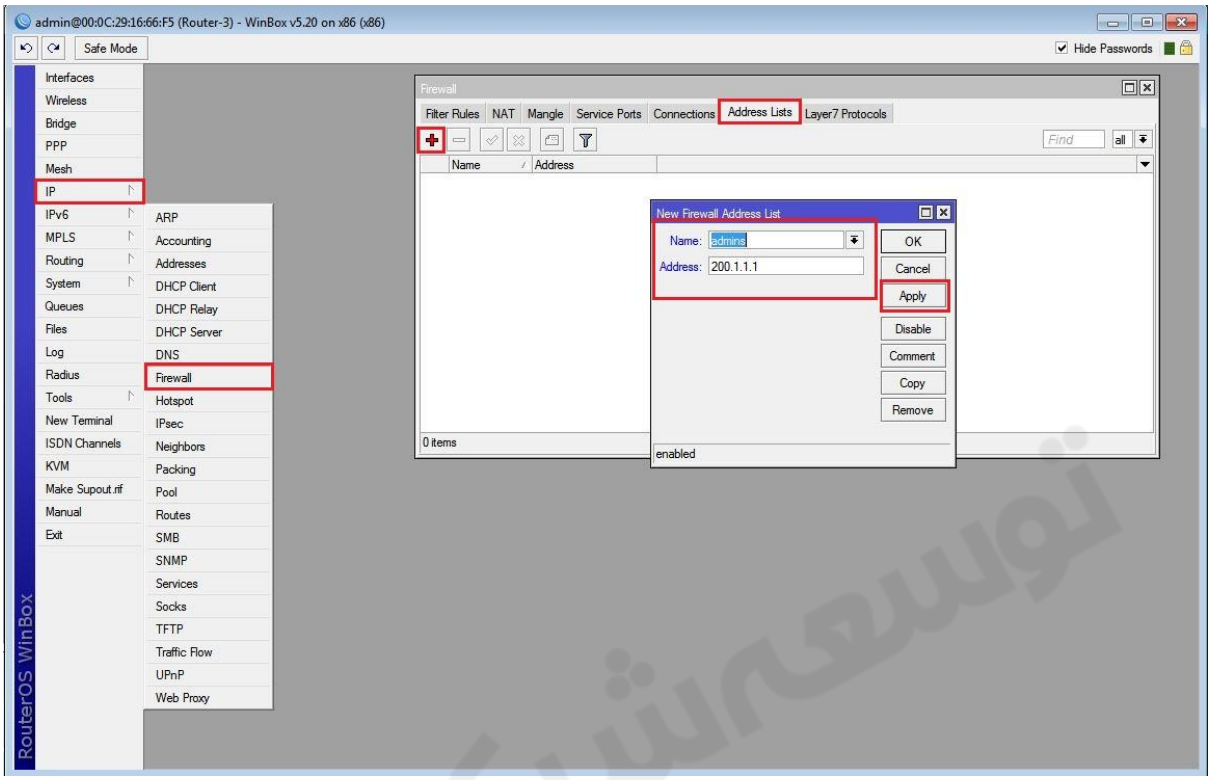
نکته : در این مثال چون **Not** را انتخاب کردیم یعنی همه ی شبکه ها بجز شبکه ایی که در **Src-address** وارد کردیم نتوانند از طریق **Winbox** به روتر دسترسی داشته باشند.



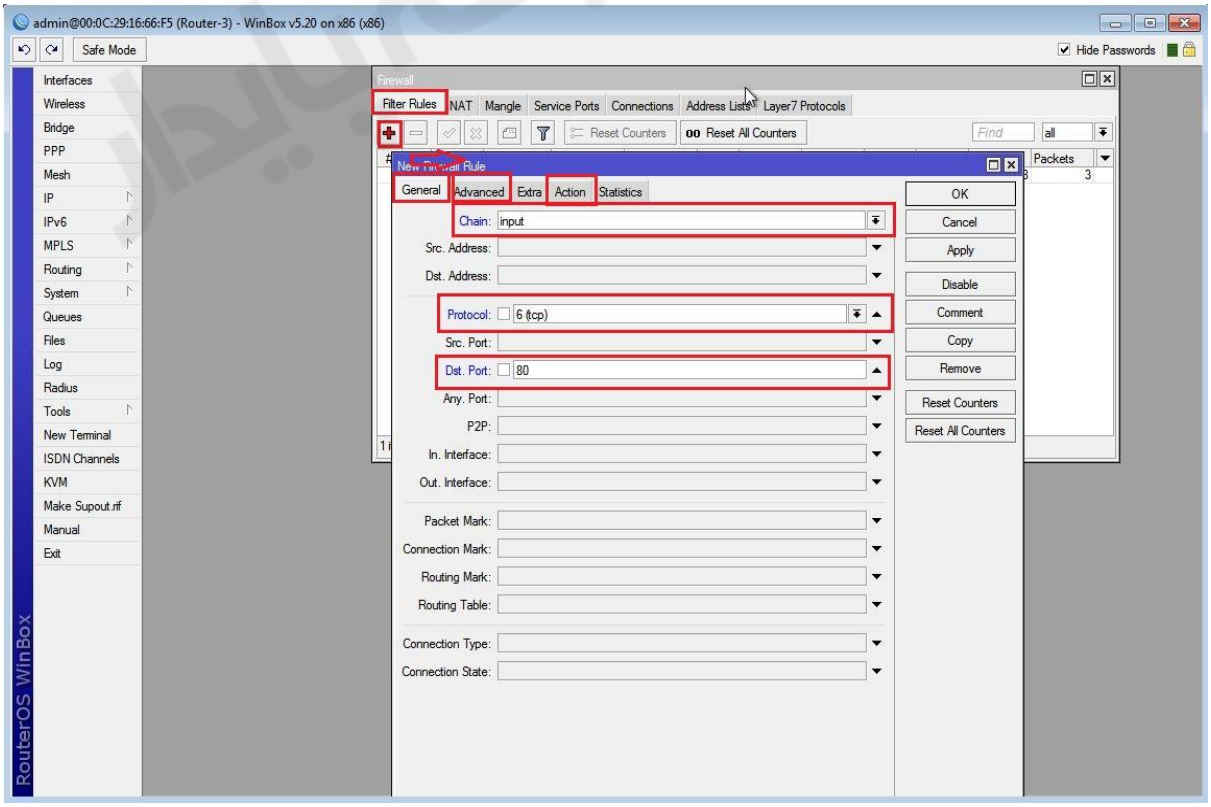


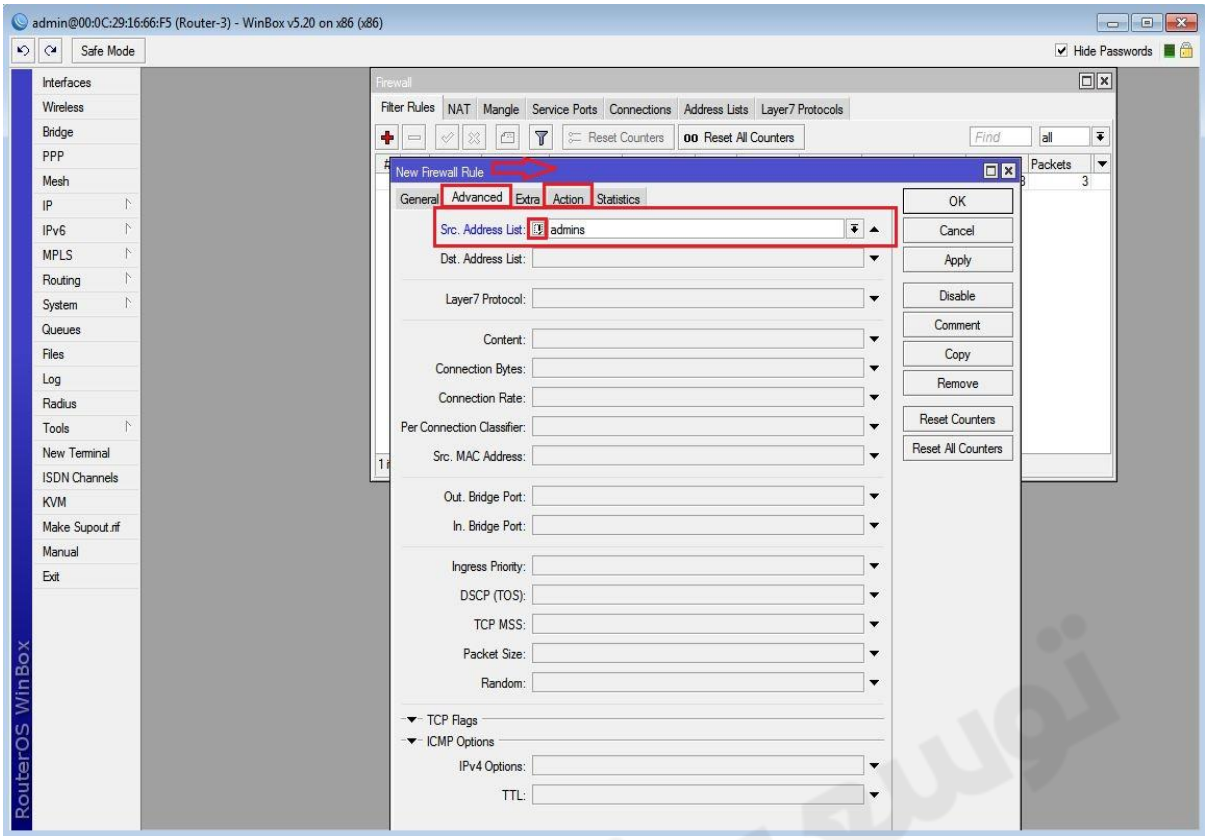
مثال ۴) فقط یک سری کاربران بتوانند به کمک Webfig به روتر R3 دسترسی داشته باشند.

ابتدا یک آدرس لیست از کاربرانی که می خواهیم دسترسی به آنها بدهیم اجاد می کنیم سپس فیلترینگ اعمال می کنیم.
برای ایجاد کردن آدرس لیست از منوی اصلی گزینه IP و از زیرمنوی باز شده Firewall را انتخاب میکنیم و از پنجره بازشده به بخش Address List رفته و بر روی ADD کلیک می کنیم.در پنجره باز شده هر چند کاربر که مورد نیاز باشد را تعریف میکنیم.(براساس IP)

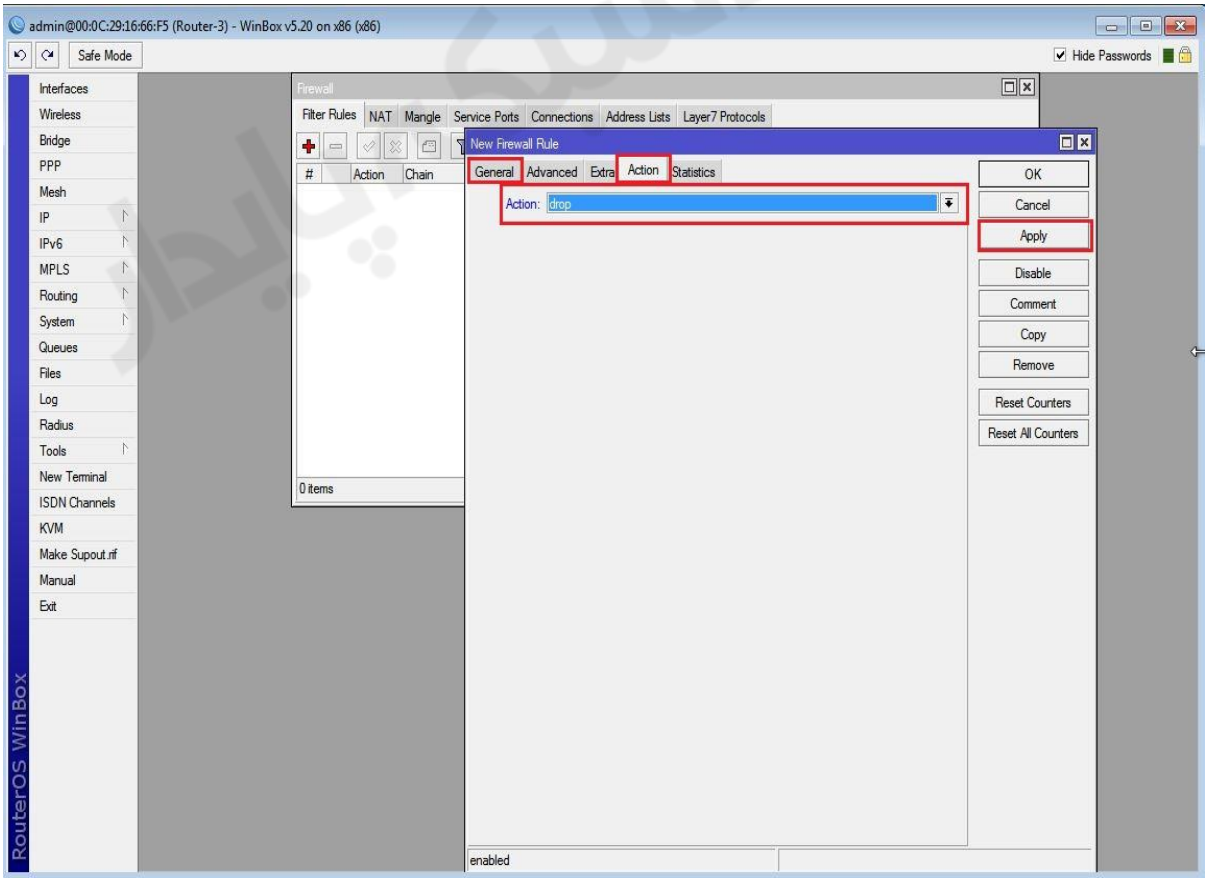


دلیل اینکه در قسمت Address : 192.168.10.2 را وارد نکردیم این بود که این IP از طریق روتر R1 ، Nat می شود به همین خاطر IP:200.1.1.1 را وارد کردیم در صورت نوشتن IP:192.168.10.2 به جواب نخواهیم رسید.

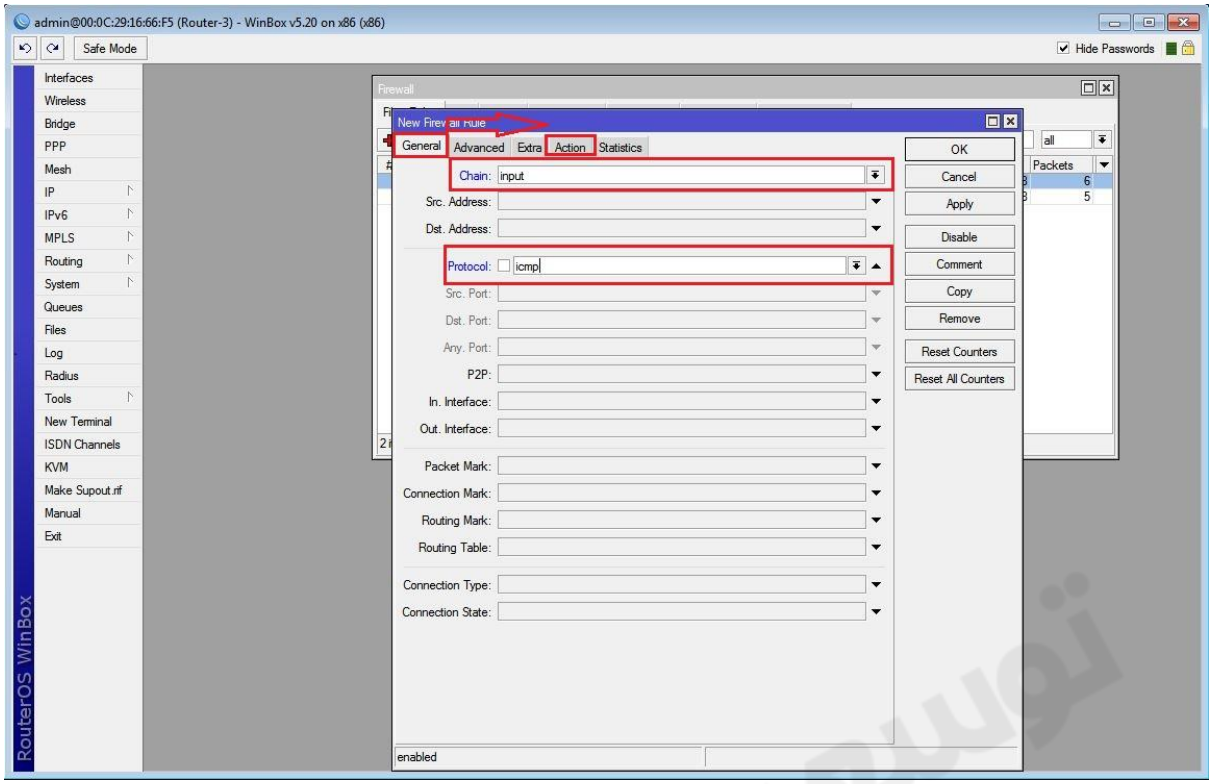


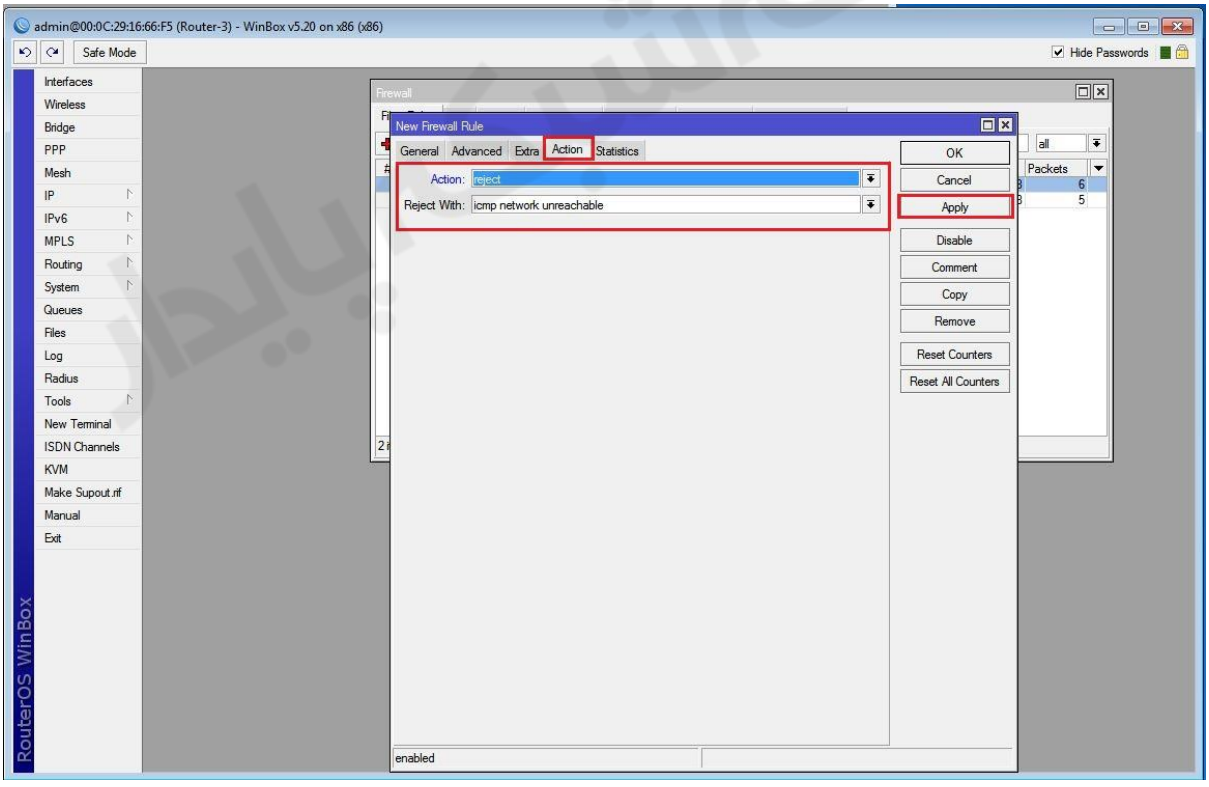


در Src-Address List آدرس لیستی که خودمان ایجاد کردیم را انتخاب می کنیم و گزینه Not را نیز فعال می کنیم تا فقط کاربرانی که خودمان انتخاب کردیم بتوانند به Webfig روتر R3 دسترسی داشته باشند.

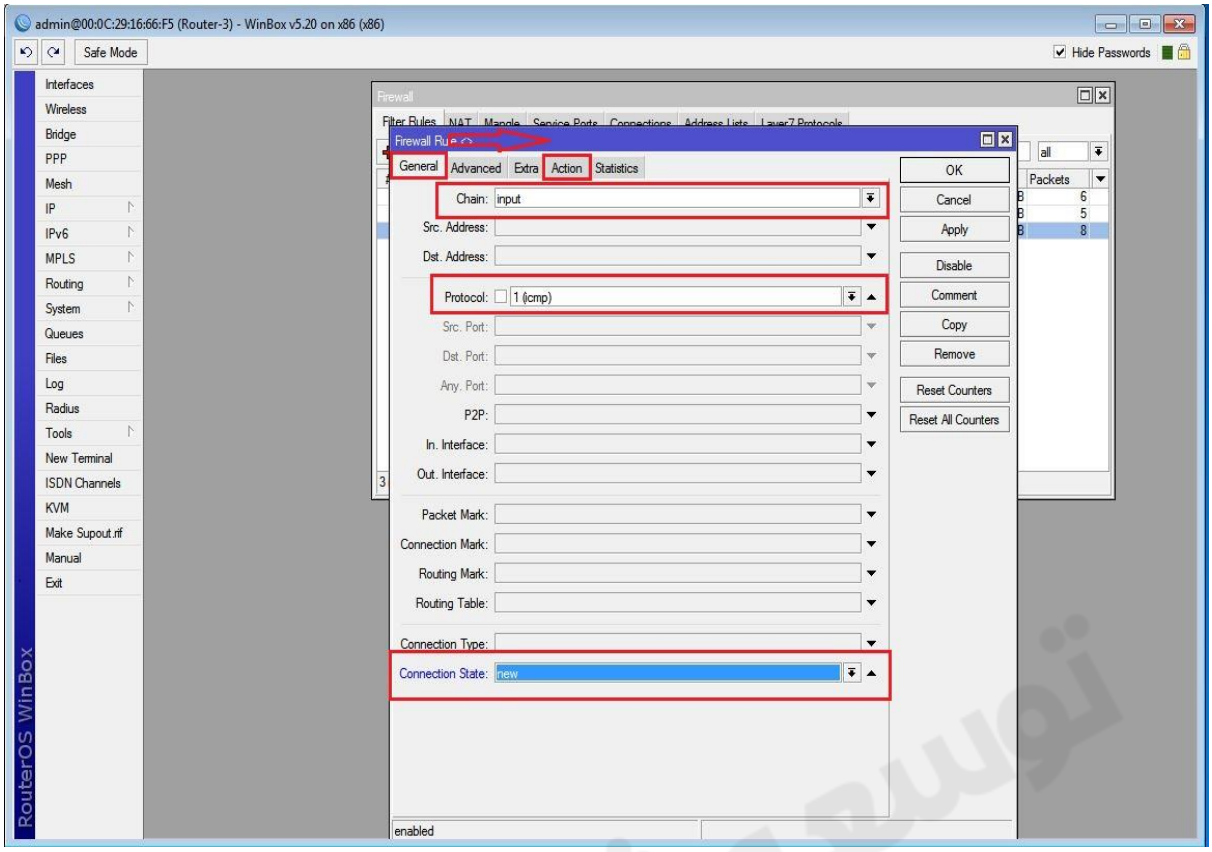


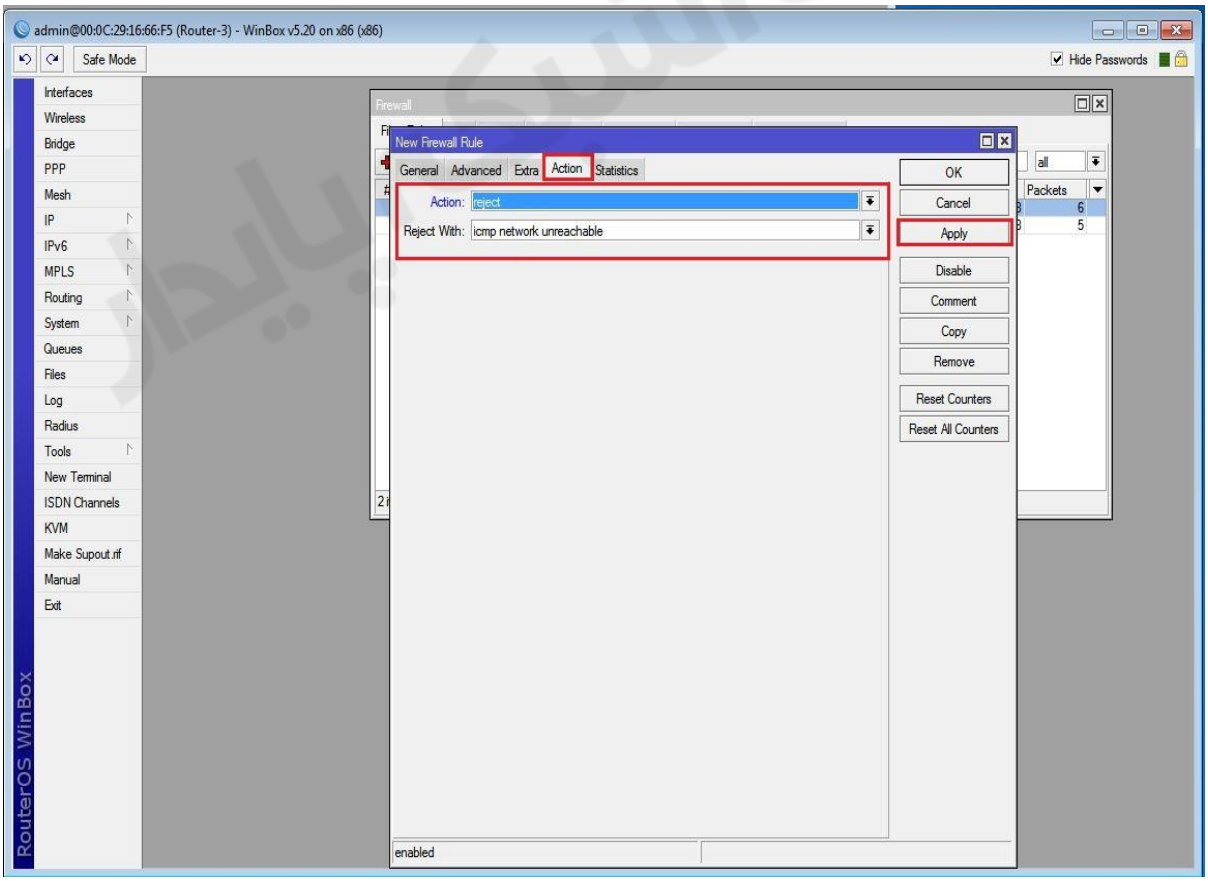
مثال ۵) میخواهیم رولی ایجاد کنیم که هیچ سیستمی نتواند روتر R3 را Ping کند.





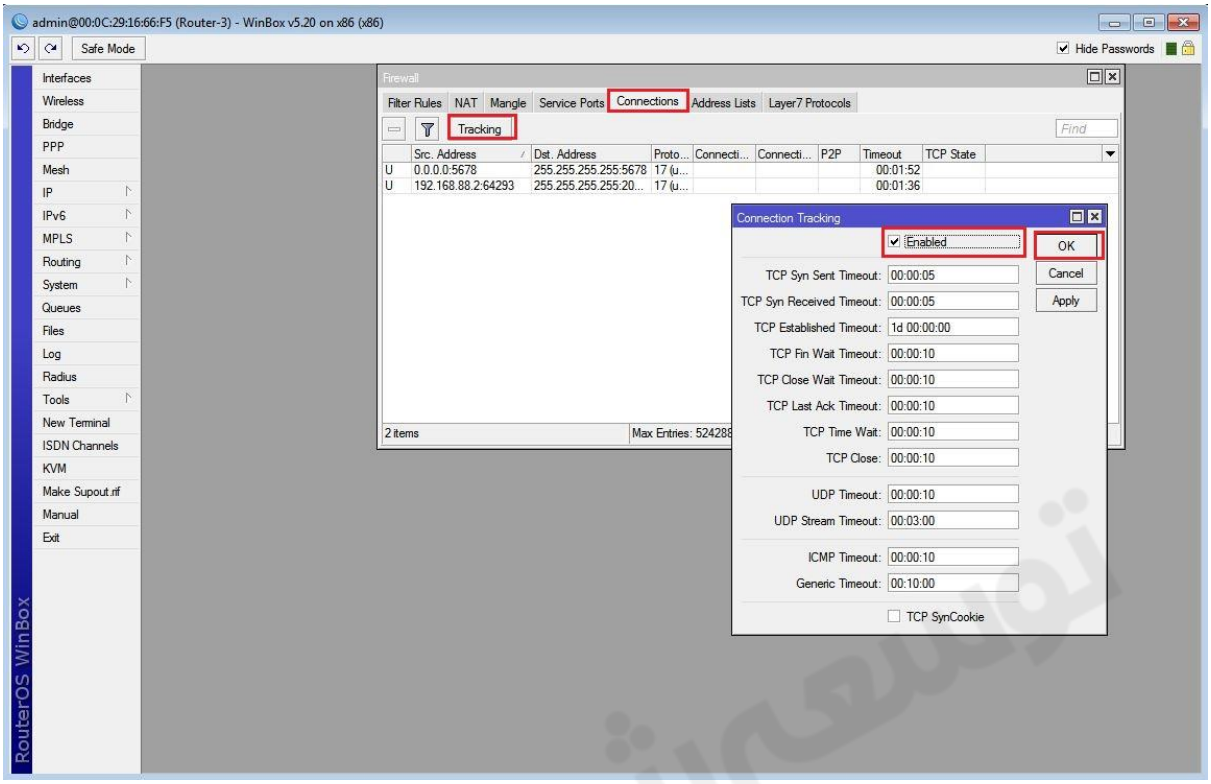
با تنظیم این فیلترینگ بسته هایی که به روتر R3 وارد می شود ping داده نمی شود.در قسمت Reject With پیامی که خودمان مشخص کردیم نشان داده می شود.اگر از داخل روتر به یک شبکه دیگر Ping بدیم پیام Timeout داده می شود چون ICMP یک پیام دو طرفس که دارای Send و Recive می باشد.ما می خواهیم یک استثنا قائل شویم تا اگر از داخل روتر Ping زدیم باز باشد ولی از هر شبکه ایی خواستن روتر را Ping کنند بسته باشد.



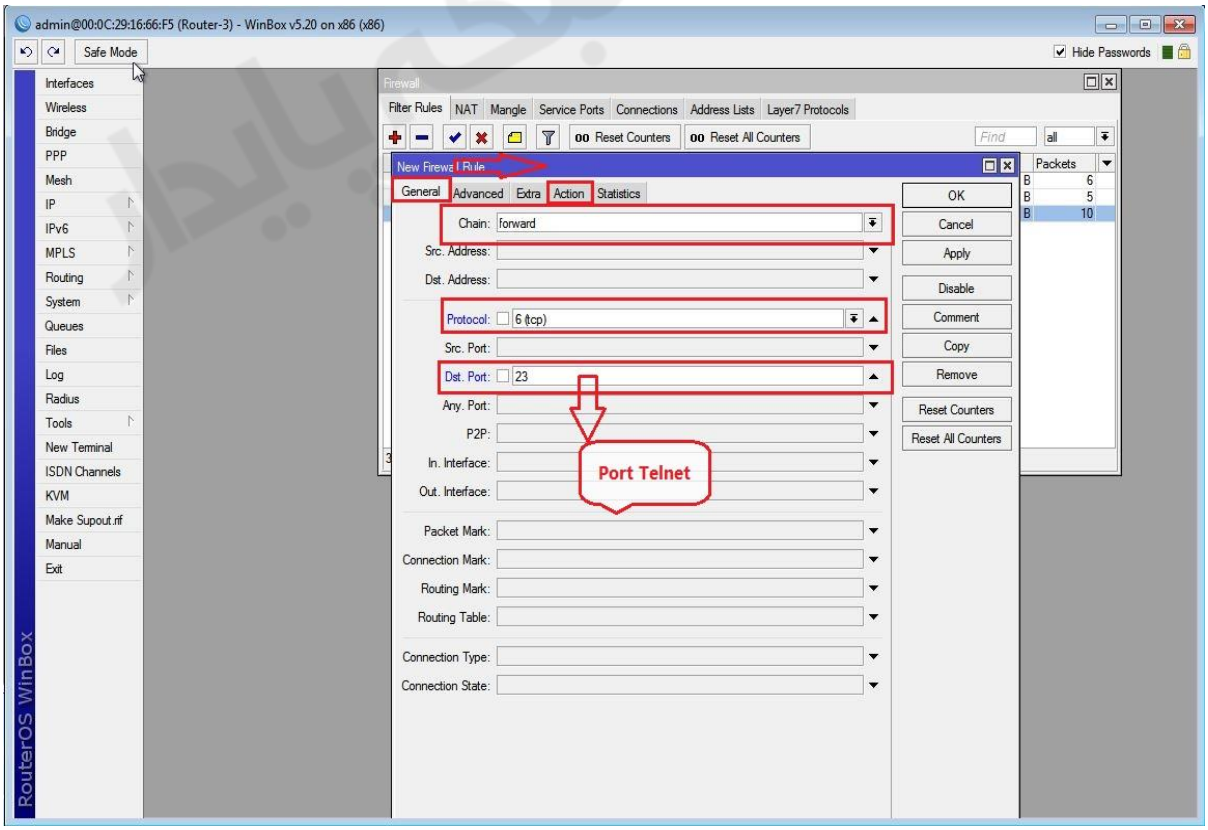


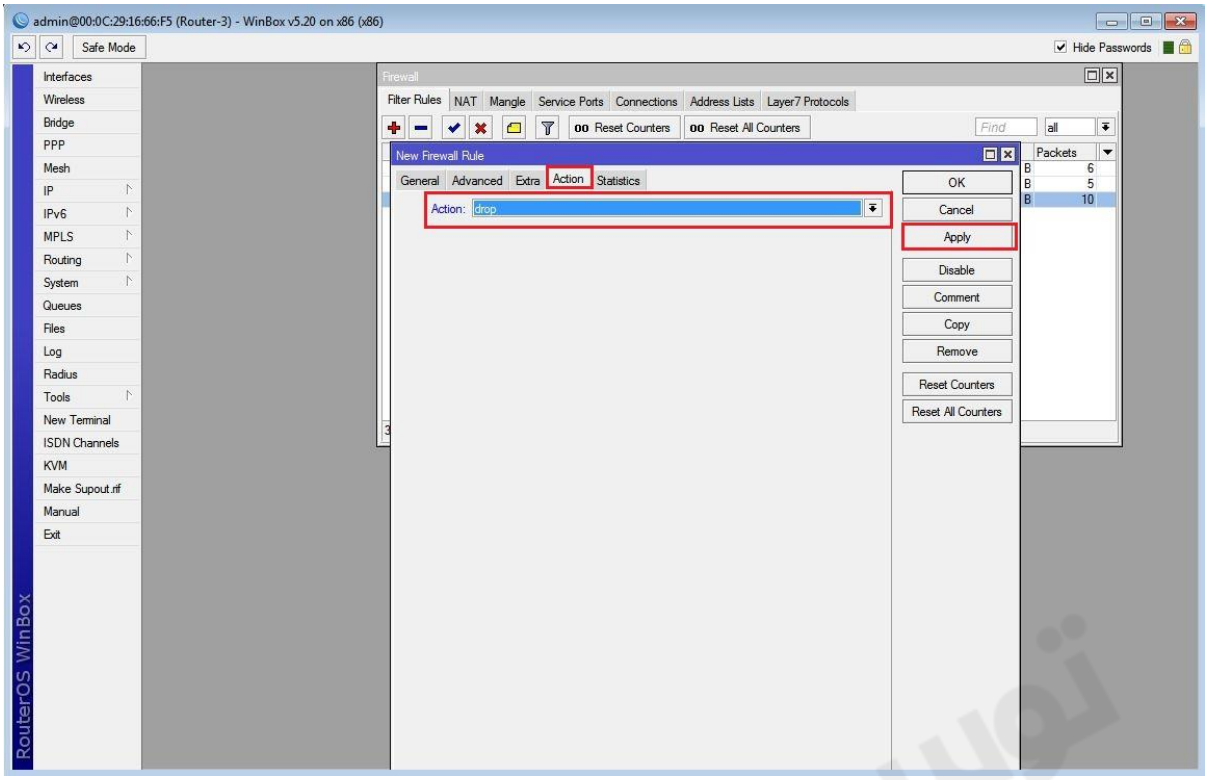
با این تنظیمات زمانی که از داخل روتر به هر شبکه ایی Ping بزنیم بسته ICMP فیلتر نمی باشد.

نکته : در صورتی که هنوز نمی توانستید از داخل روتر Ping کنید از پنجره Firewall به بخش Connections رفته و بر روی Traking کلیک کرده و از پنجره بازشده یکبار تیک گزینه Enable را برداشته Ok میزنیم و سپس مجددا آن تیک را قرار می دهیم.در خیلی از موارد که ما با فایروال کار می کنیم و به جواب نمیرسیم با این کار مشکل ما حل می شود.(براساس تجربه)



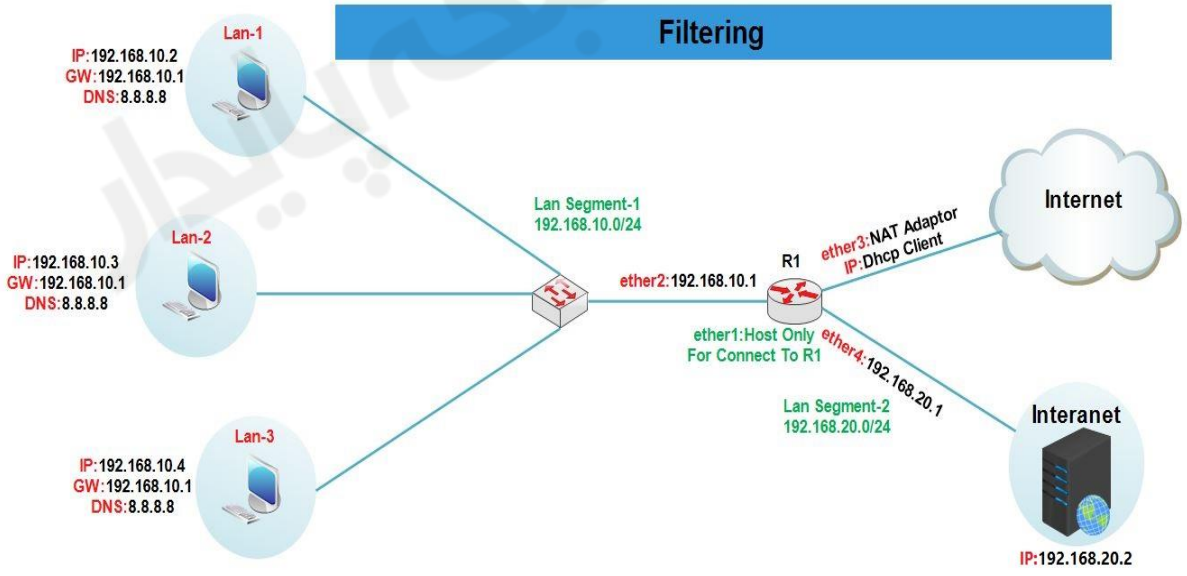
مثال ۶) هیچ سیستمی اجازه ارتباط از طریق Telnet به هیچ مقصدی را نداشته باشد.





با این تنظیم چنانچه سیستمی بخواهد به خود روتر **Telnet** بزند مشکلی وجود ندارد اما چنانچه بخواهید این رول را طوری تنظیم کنید که کلاینت ها نتوانند به روتر **Telnet** بزنند باید **Chain=input** قرار دهید.

سناریو ۲ : هدف از انجام این سناریو بررسی عملیات **Filtering** می باشد.

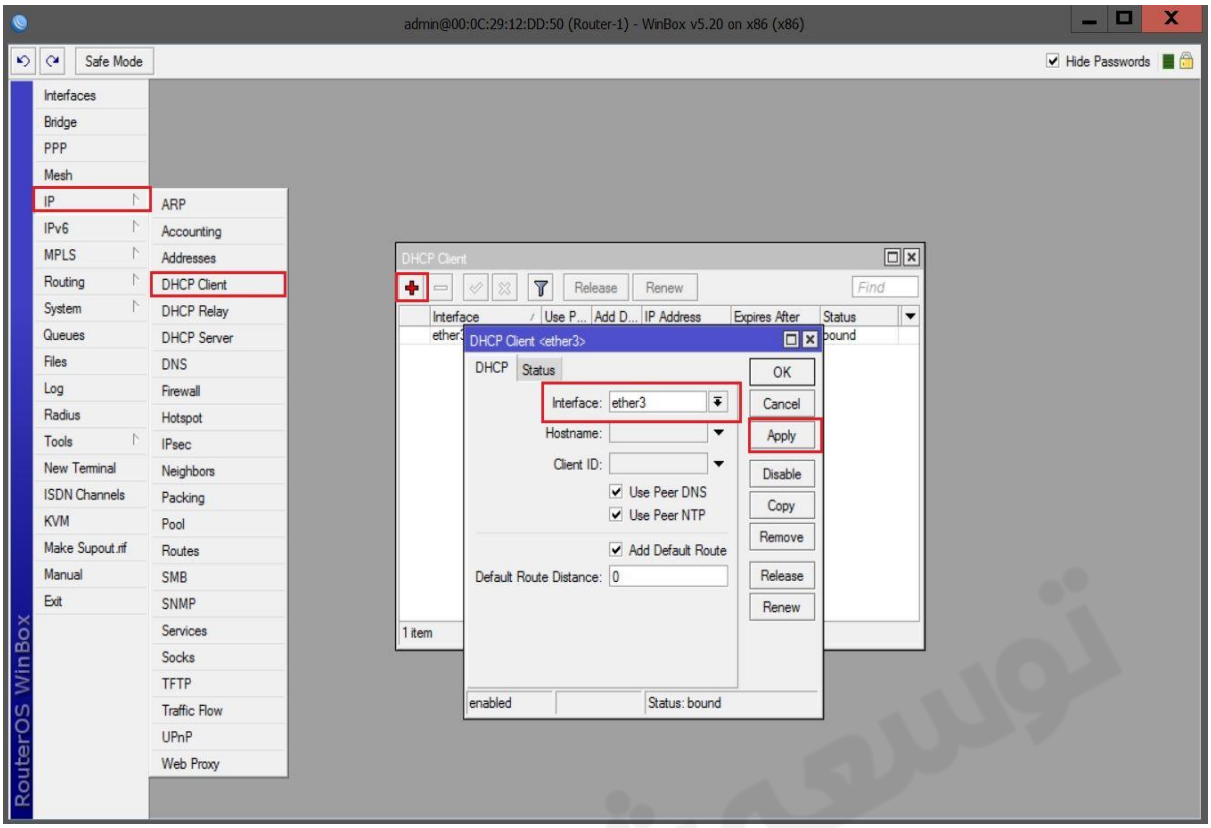


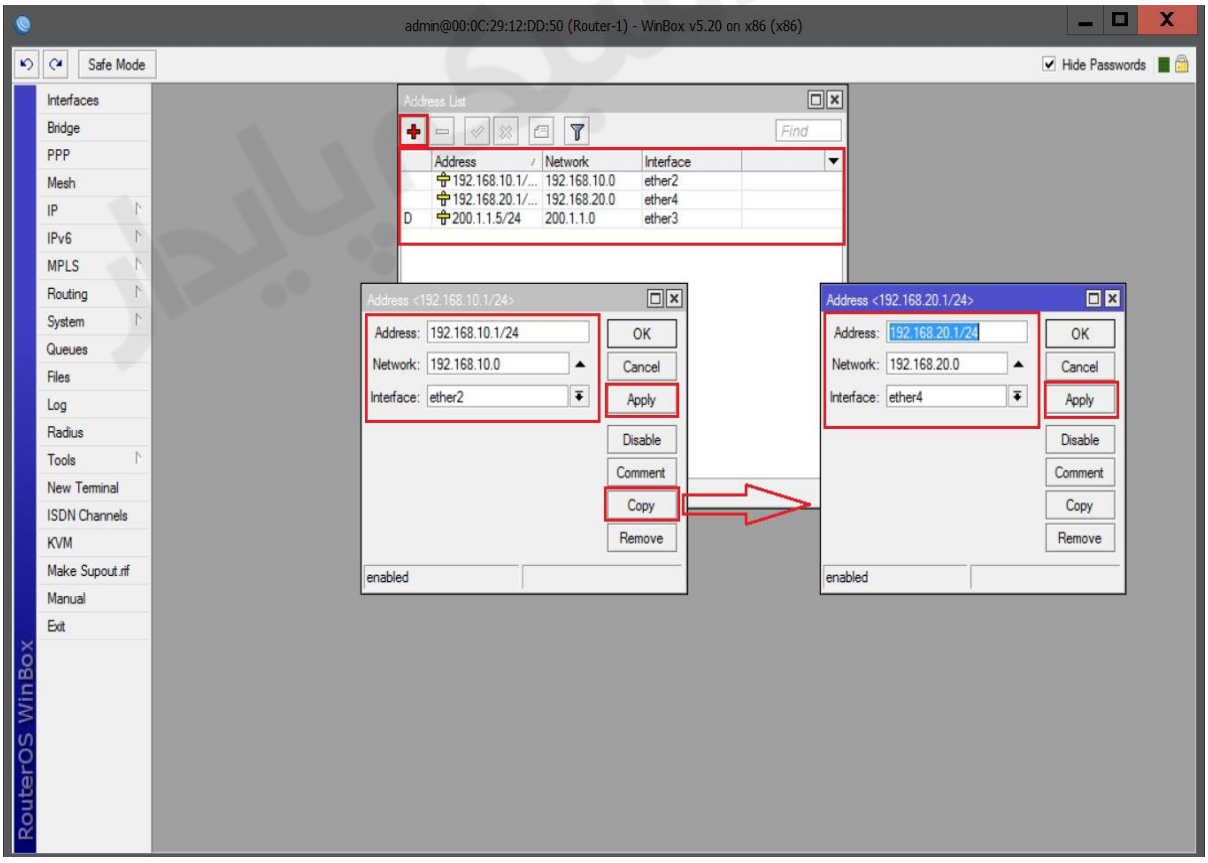
در این سناریو روتر **R1** را به گونه ایی تنظیم می کنیم که **Lan-1** تنها به وب سرور موجود در شبکه اینترانت ، **Lan-2** تنها به اینترنت و **Lan-3** هم به اینترنت و هم به اینترانت دسترسی داشته باشند.

برای پیاده سازی این سناریو :

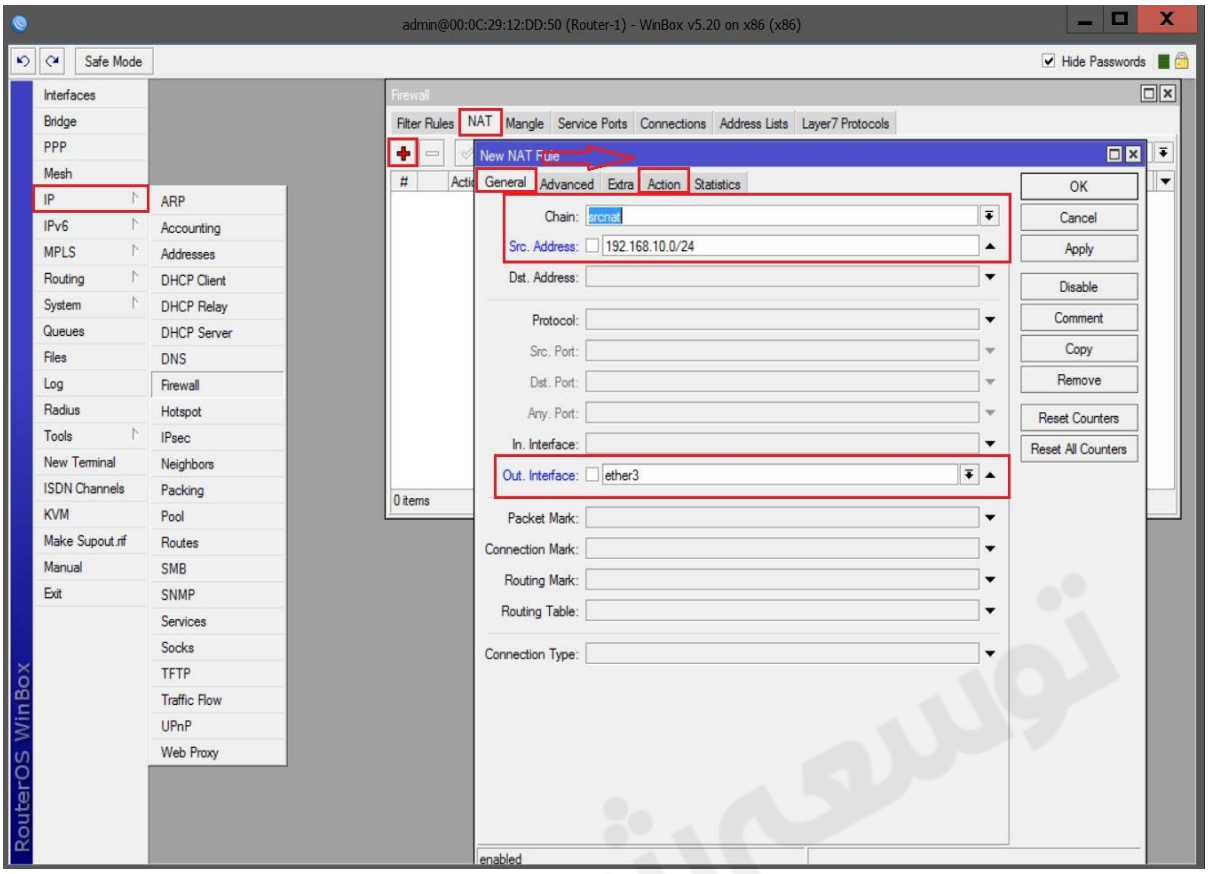
- سه سیستم جهت شبیه سازی کلاینت های موجود در هر **Lan**.
- یک روتر به عنوان **Firewall**(این روتر از طریق کارت شبکه **ether3** به اینترنت دسترسی دارد).
- یک سرور ۲۰۱۲ جهت شبیه سازی شبکه اینترانت که بر روی آن وب سرور راه اندازی شده است.

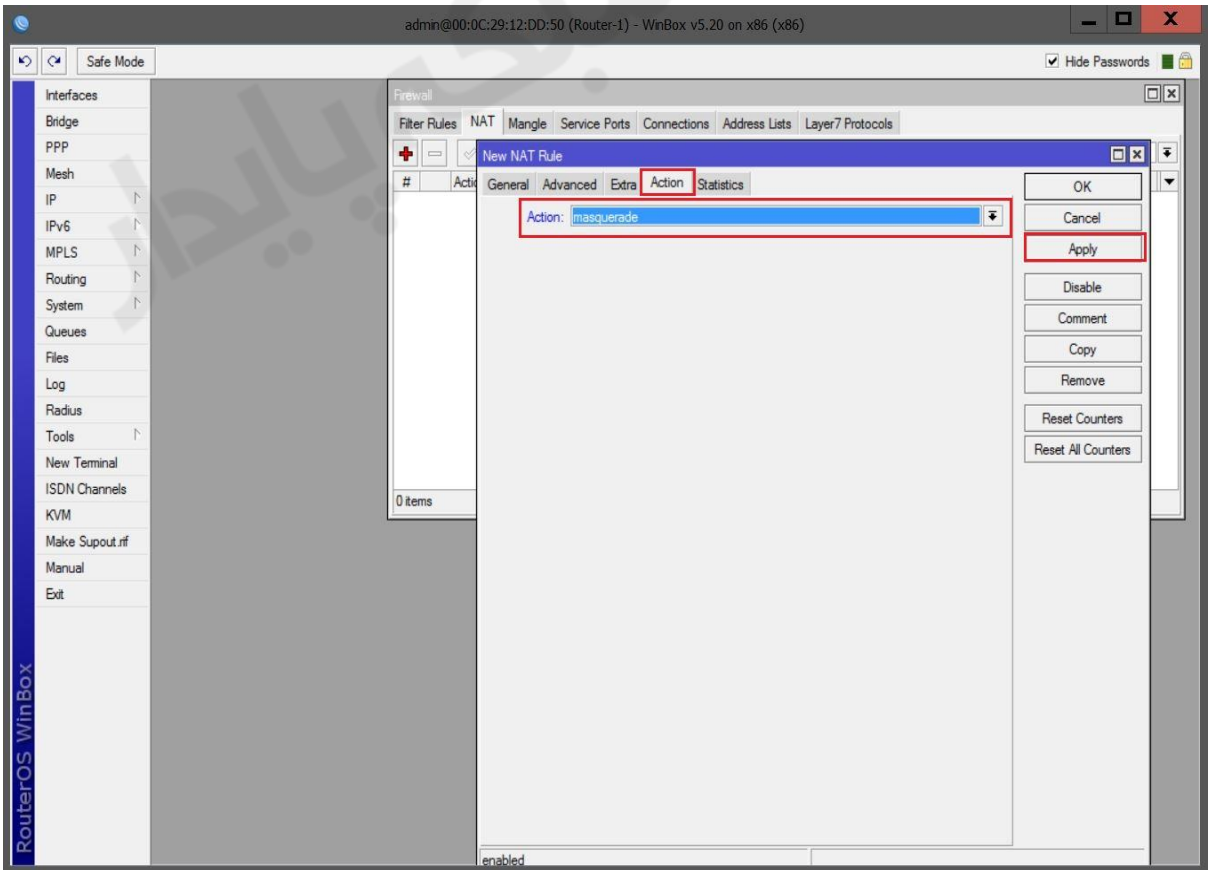
انتساب IP برای کارت های شبکه روتر R1 :



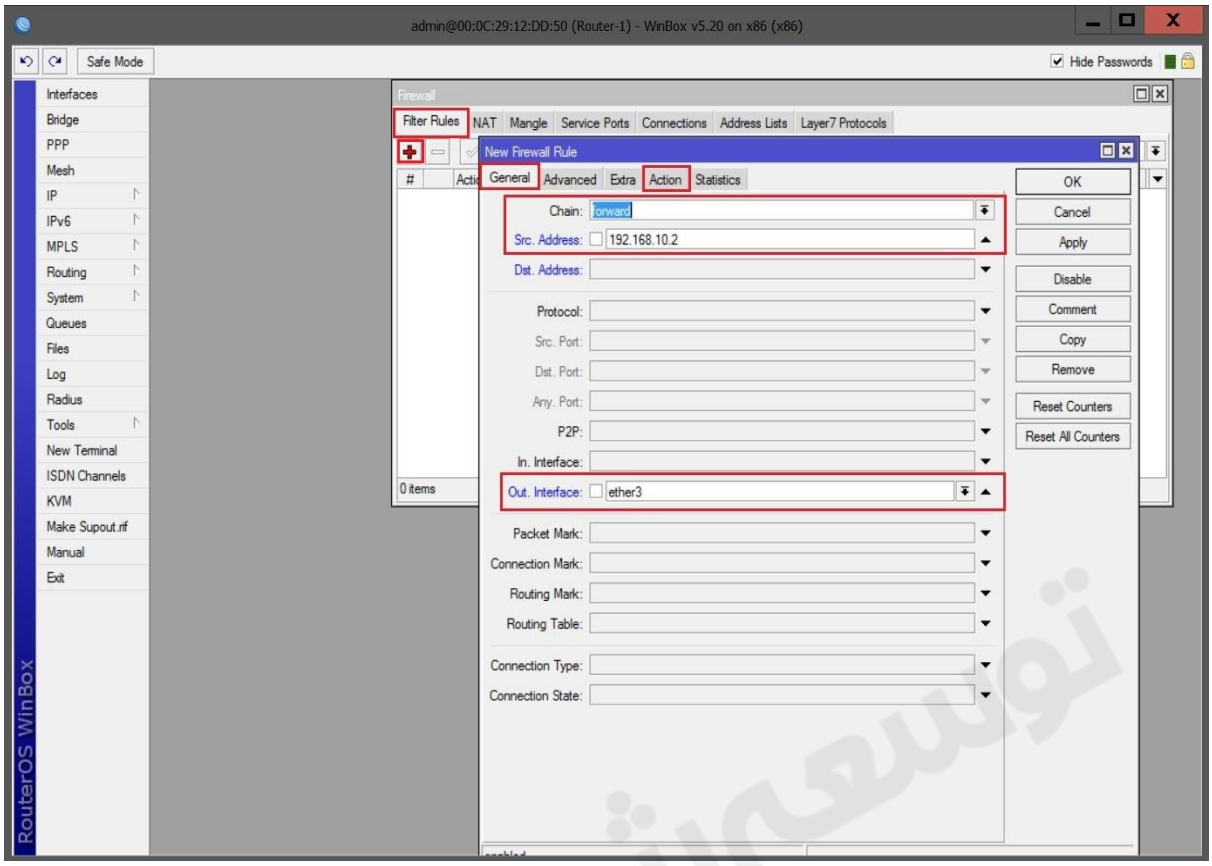


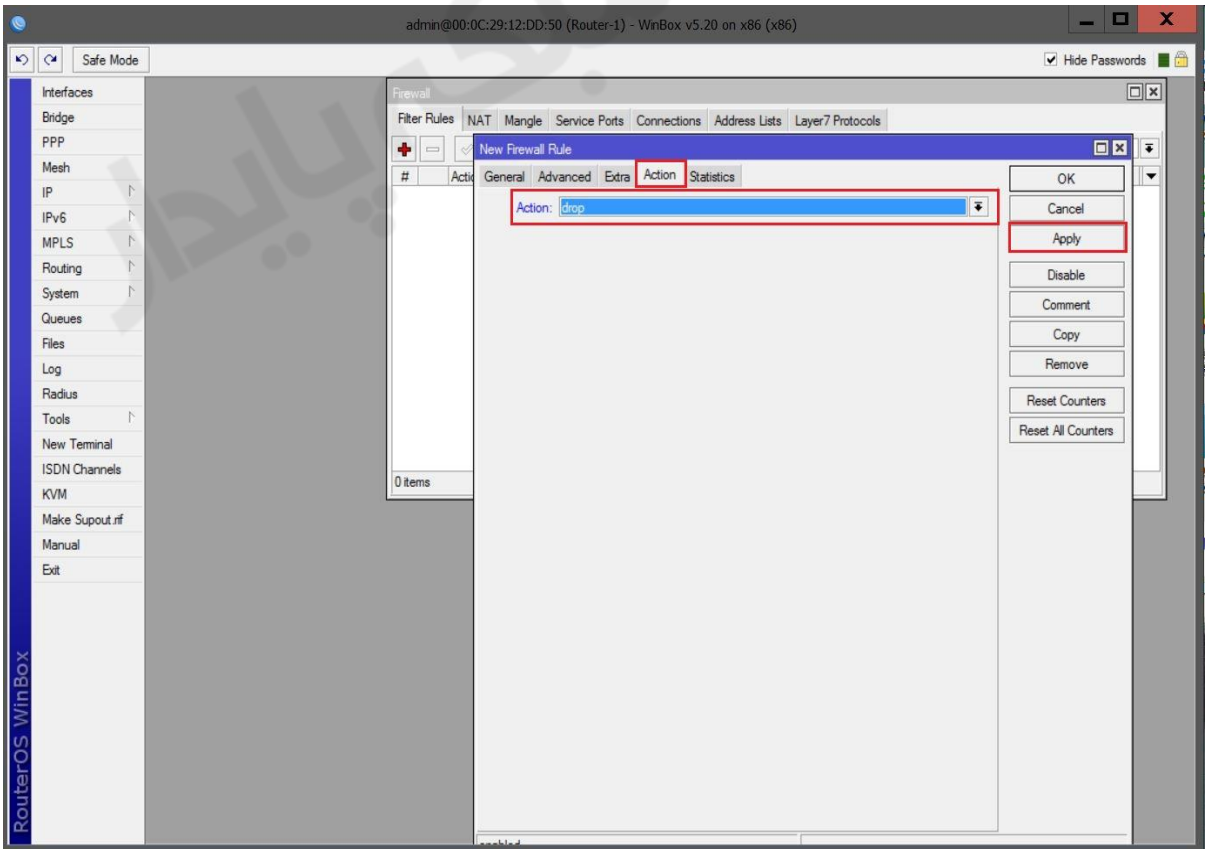
اعمال عملیات Nat بر روی بسته هایی که به سمت روتر R1 می آیند :



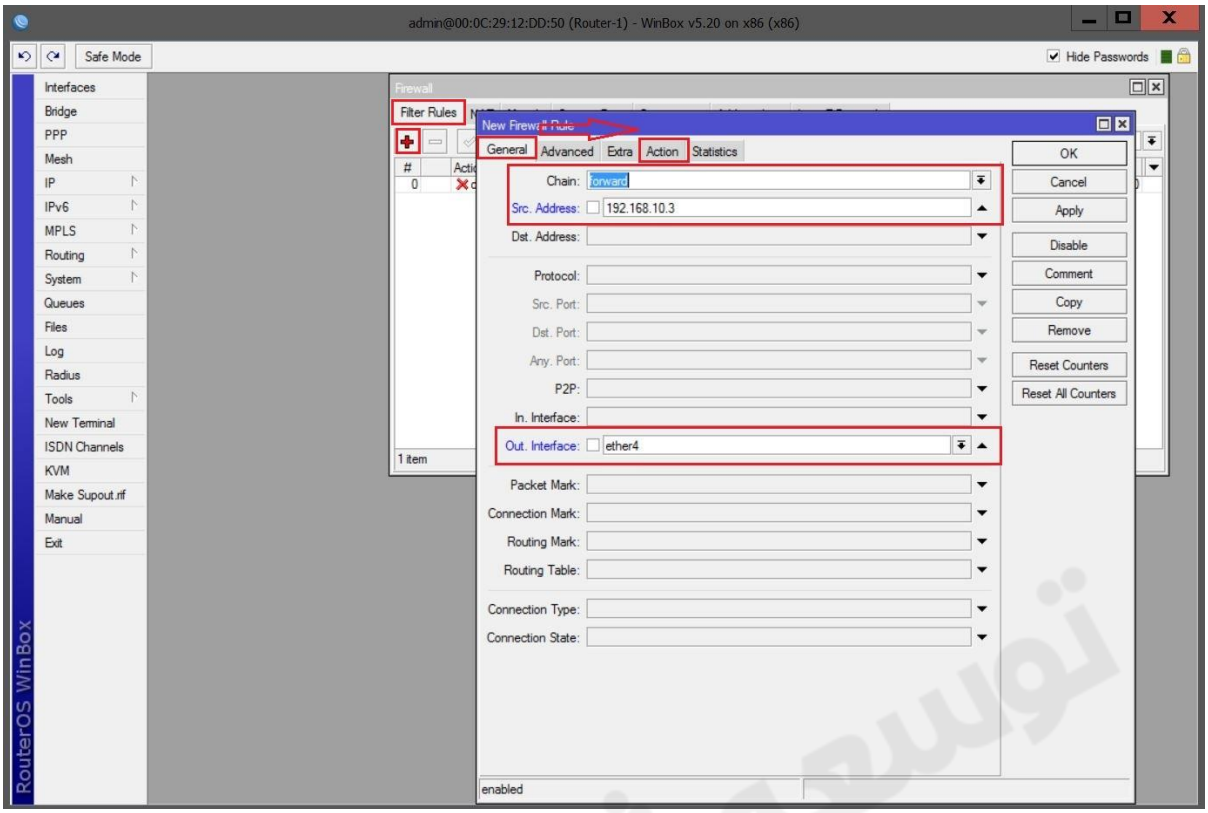


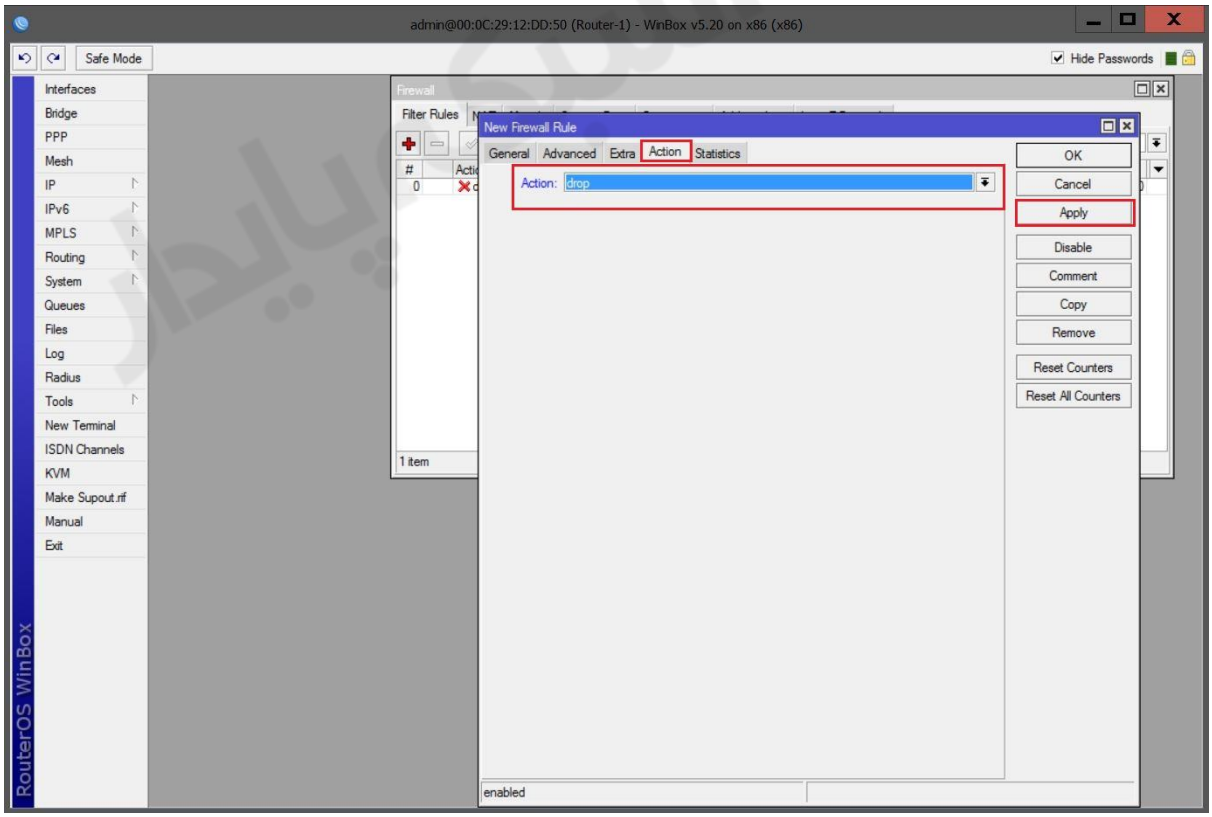
تنظیمات جهت عدم دسترسی کلاینت موجود در Lan-1 به اینترنت :





تنظیمات جهت عدم دسترسی کلاینت موجود در **Lan-2** به اینترانت :





تنظیمات جهت دسترسی کلاینت موجود در **Lan-3** به اینترنت و اینترانت :

طبق قانون گفته شده از آنجا که محدودیتی برای ترافیک بسته های Lan-3 وجود ندارد هیچ فیلتری برای این نوع ترافیک ها در نظر گرفته می شود.

فصل ششم : Mangle

Mangle یکی از بهترین قسمت های زیر شاخه فایروال میکروتیک می باشد که در بستر شبکه های بزرگ استفاده می شود.کاربرد این سرویس میکروتیک را می توان در کنترل ترافیک فهمید.وقتی که شبکه شما دارای رنج ها و **IP Gateway** های متعددی باشد برای اینکه بتوانید هر سرویس شبکه را فقط بر روی بعضی از **Gateway**ها هدایت کنید تا از ترافیک زیاد و بار بالا بر روی یک پورت روتر جلوگیری بعمل بیاید.یکی از مهمترین قابلیت های **Mangle** مبحث **Marking** می باشد این قابلیت در واقع با نشانه دار کردن بسته های ارسالی ترافیک شما را دسته بندی می کند که این دسته بندی می تواند براساس پورت و پروتکل ویا **IP** باشد و پس از دسته بندی قابلیت این را دارد که شما انتخاب کنید که از کدوم گذرگاه عبور داده شود.از این قابلیت میکروتیک هم میتوان در مدیریت پهنای باند یا همان **Queue Tree** و هم در تجمیع پهنای باند اینترنت و همچنین فیلترینگ و مسیریابی استفاده نمود.

پارامترهای مورد استفاده در **Mangle** :

۱)**Prorouting** : یعنی قبل از اینکه عملیات مسیریابی انجام شود.

۲)**Postrouting** : زمانی که بسته می خواهد روتر را ترک کند و به سمت بیرون برود(یعنی زمانی که می خواهد مسیریابی انجام شود).

۳)**TOS(Type of Service)** : ما با استفاده از این قابلیت می توانیم بسته ها را روی یک روتر مارک کنیم و در یک روتر دیگر برای آن بسته ها فیلترینگ تعریف کنیم.برای اینکار ما از قابلیت **DSCP(TOS)** استفاده می کنیم.

۴)**TTL(Time To Live)** : از طریق **Mangle** می توان هدر بسته را تغییر داد.فیلد **TTL** برای این منظور است که بسته های سرگردان بعد از مدتی از بین بروند، بدین ترتیب که بسته از هر روتر (**Hop**) که عبور می کند یکی از مقادیر **TTL** کم می شود تا نهایتا مقدار آن به صفر برسد.

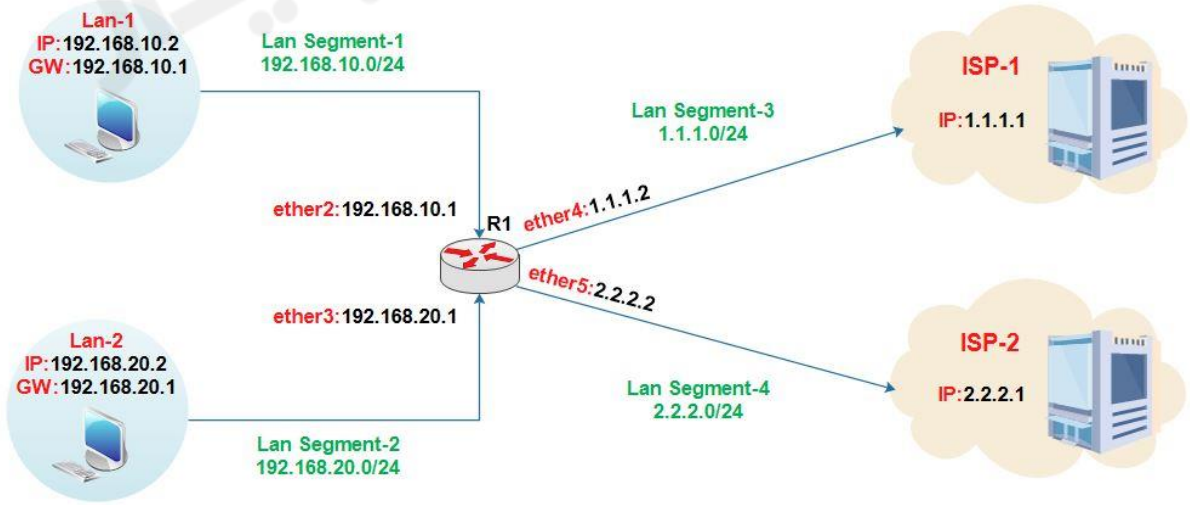
یکی از کاربردهای **TTL** این است که با دستکاری کردن آن می توان یک سری از **Hop Count** ها را از دید کاربر مخفی کرد.

۵)**Mark Connection** : نشانه گذاری ارتباط

۶)**Mark Packet** : نشانه گذاری بسته(کاربرد در کنترل پهنای باند)

۷)**Mark Routing** : نشانه گذاری مسیر (کاربرد در عملیات مسیریابی پیشرفته)

سناریو ۱ : هدف از انجام این سناریو بررسی کاربردهای **Mangle** می باشد.



این سناریو را با دو سوال مورد بررسی قرار میدهیم.

نکته ای که باید به آن توجه داشته باشید این است که برای انجام این سناریو ما به دو خط اینترنت مجزا از دو **ISP** نیاز داریم ولی بدلیل اینکه ما همچین چیزی برایمان امکان پذیر نیست فقط آنها را بصورت مجازی کانفیگ می کنیم.

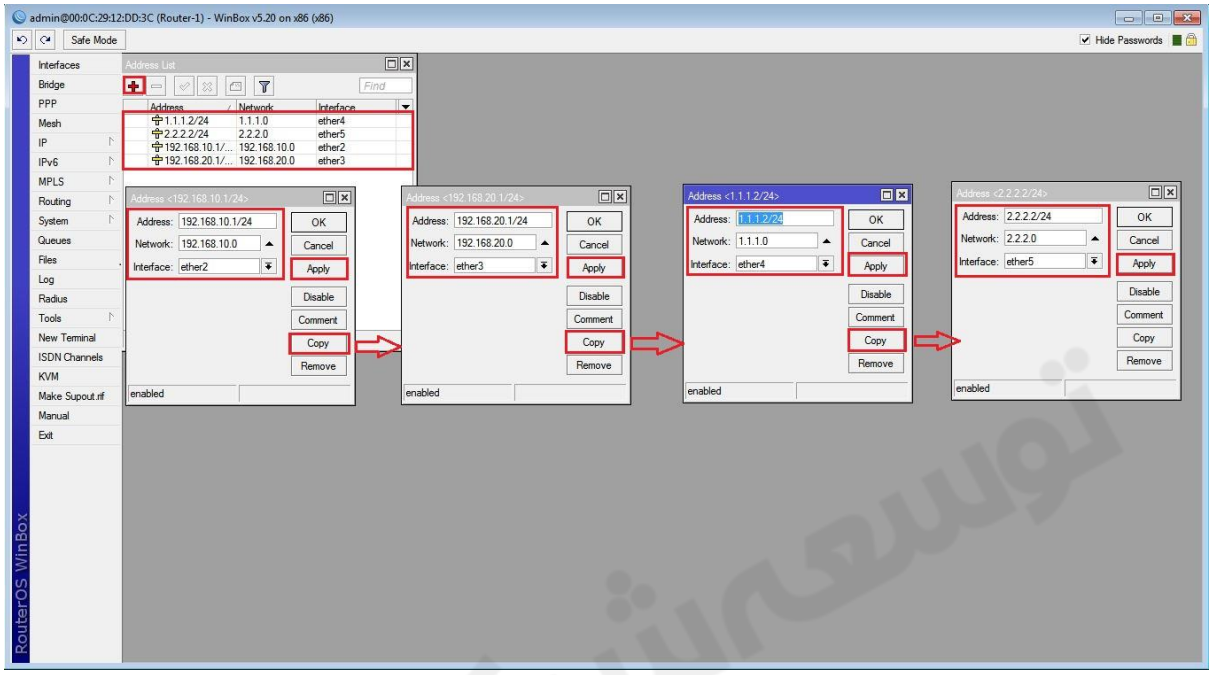
سوال ۱) بسته هایی که از سمت **Lan-1** به سمت **Lan-2** حرکت می کنند **Drop** شوند.

سوال ۲) **Lan-1** از طریق **ISP-1** و **Lan-2** از **ISP-2** به اینترنت دسترسی پیدا کنند.

جواب سوال ۱ :

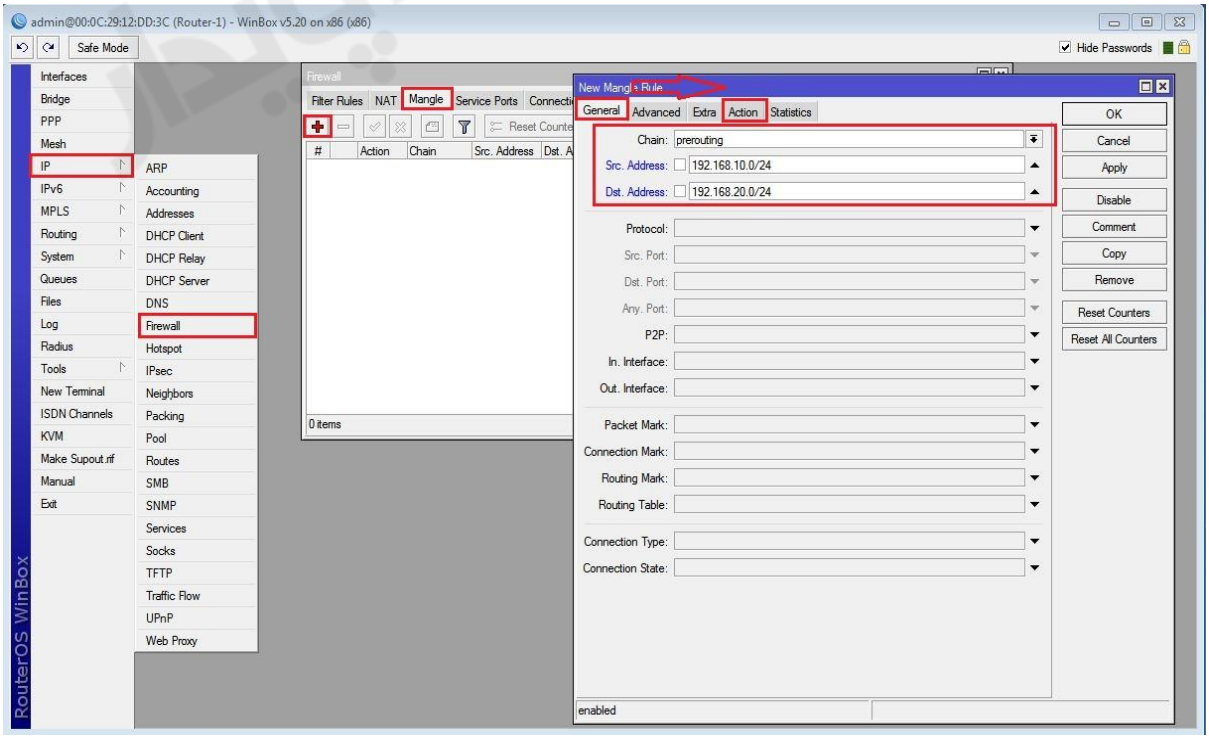
اولین کاری که ما انجام میدهیم این است که برای کارت های شبکه روتر (R1) IP تنظیم میکنیم.بعد از این کار بسته های Lan-1 را مارک می کنیم و بعد از مارک کردن این بسته ها، آنها را فیلتر می کنیم.

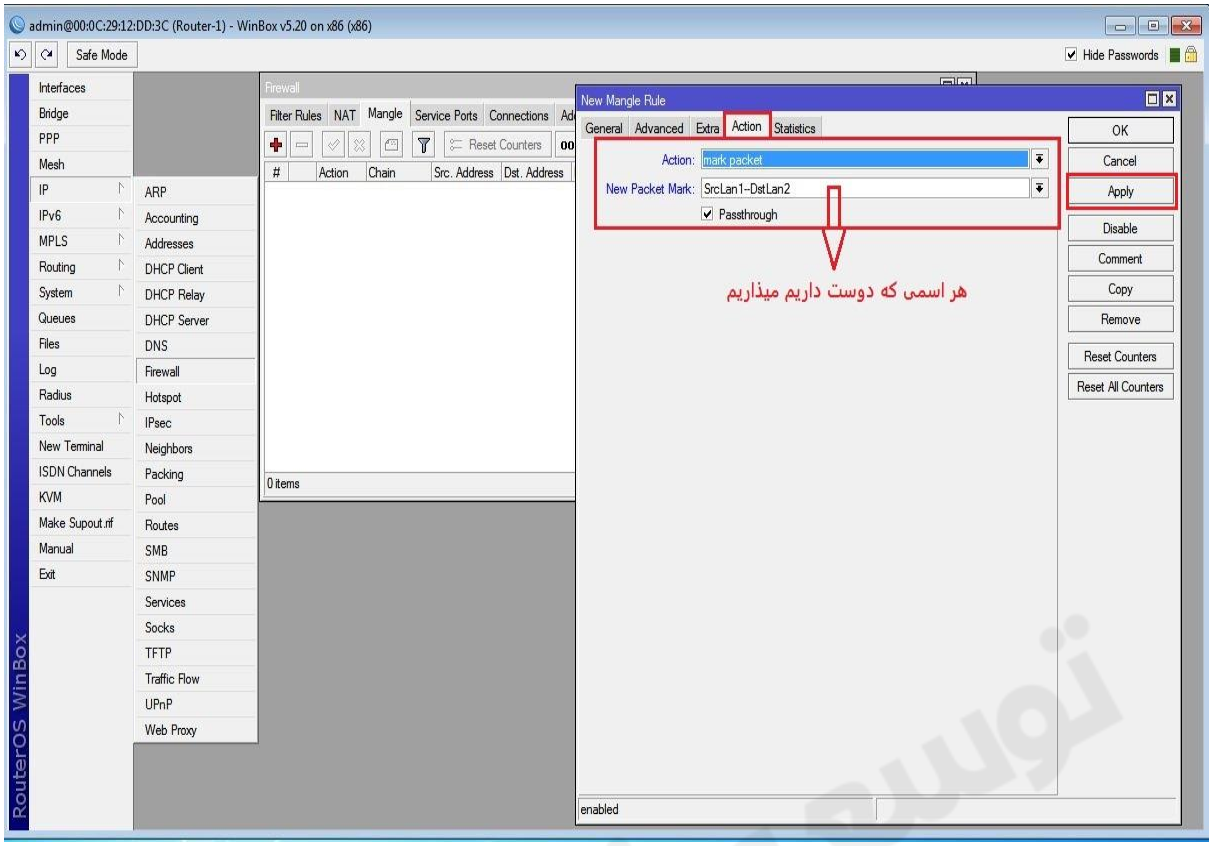
انتساب IP برای کارت های شبکه روتر R1 :



مارک کردن بسته هایی که از سمت شبکه Lan-1 به سمت شبکه Lan-2 حرکت می کنند :

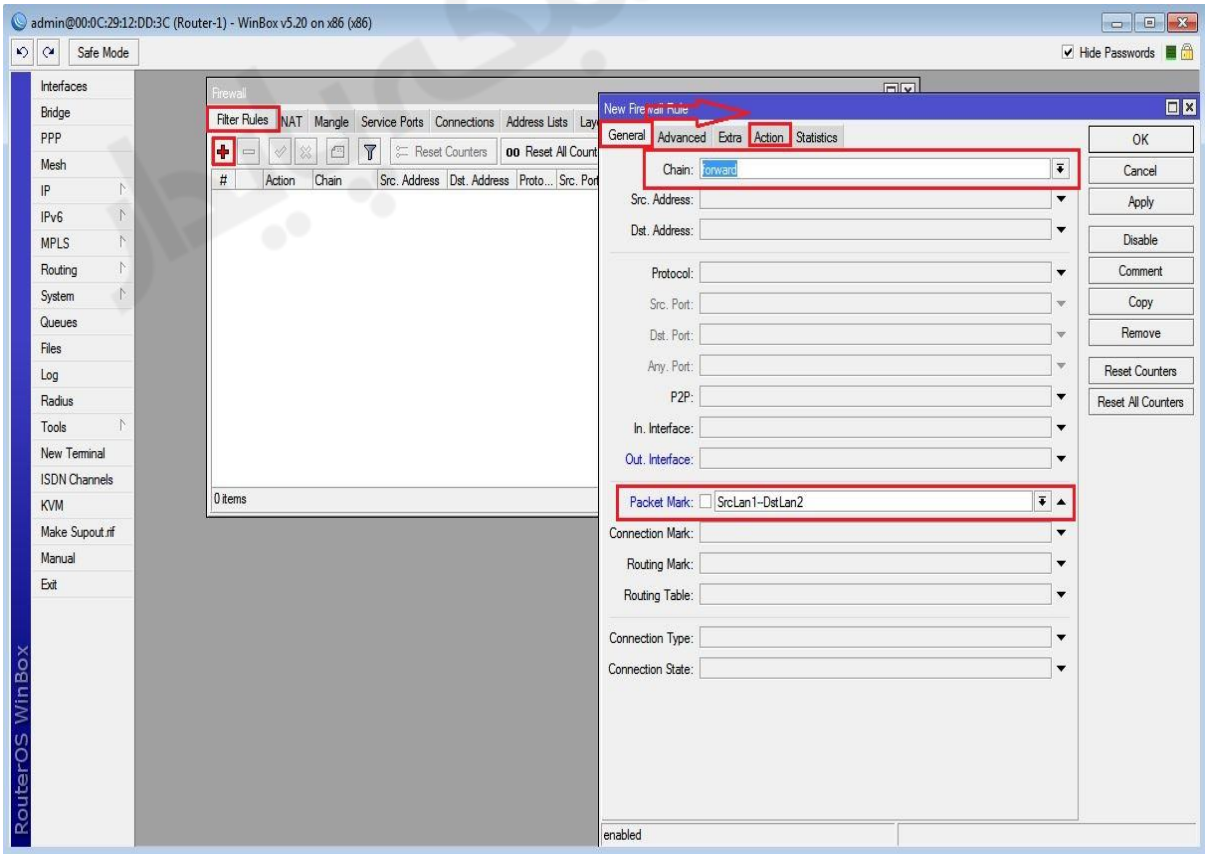
برای اینکار از منوی اصلی گزینه IP و از زیر منوی باز شده Firewall را انتخاب کرده و از پنجره ی باز شده به بخش Mangle رفته و تنظیمات را طبق مراحل زیر انجام می دهیم.

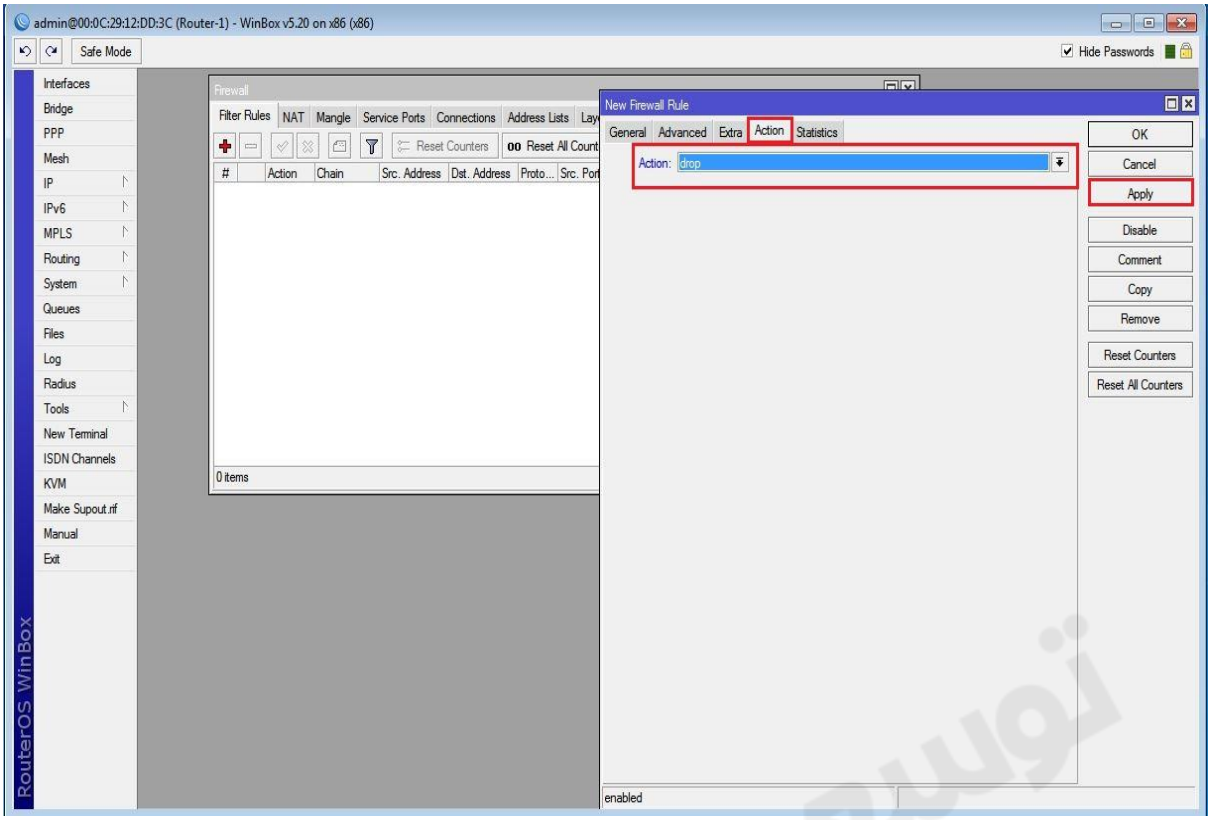




Drop کردن بسته هایی که در مرحله قبل مارک کردیم :

برای این کار به بخش Filter Rule رفته و تنظیمات را طبق مراحل زیر انجام می دهیم.

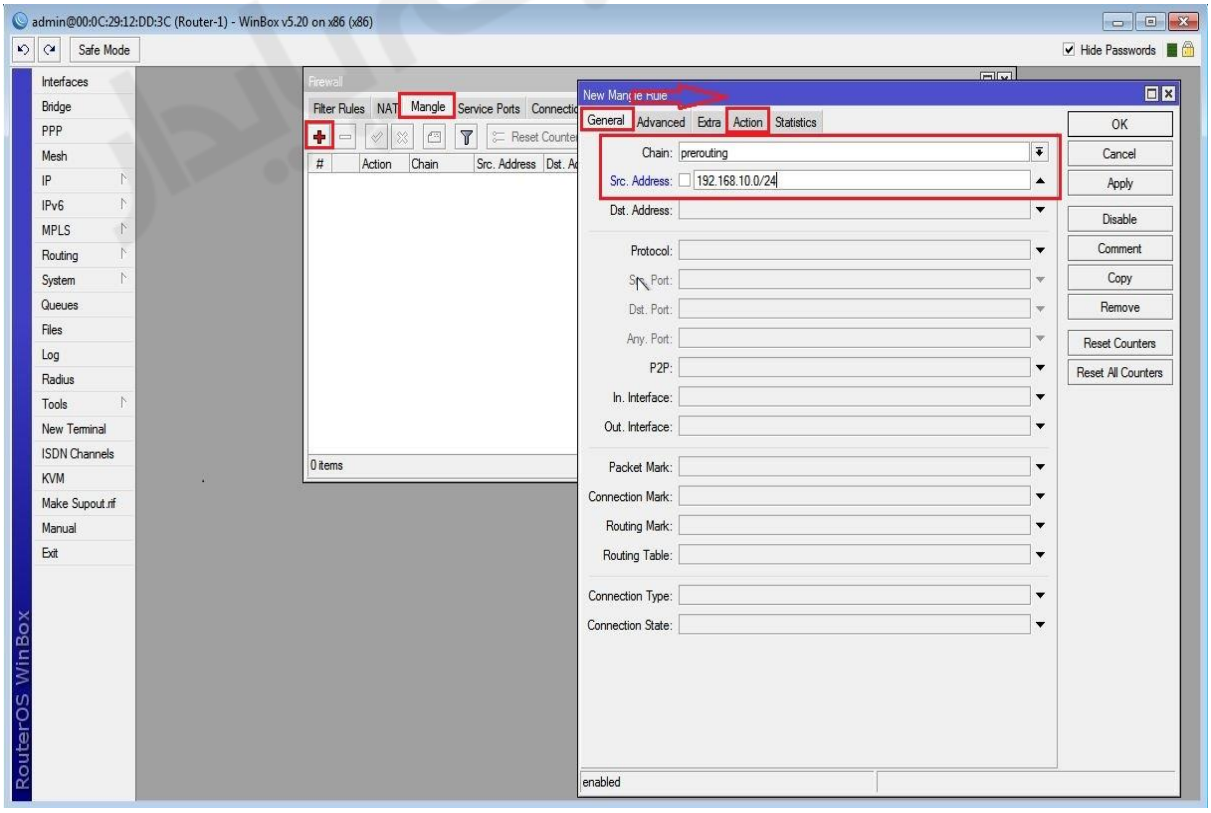


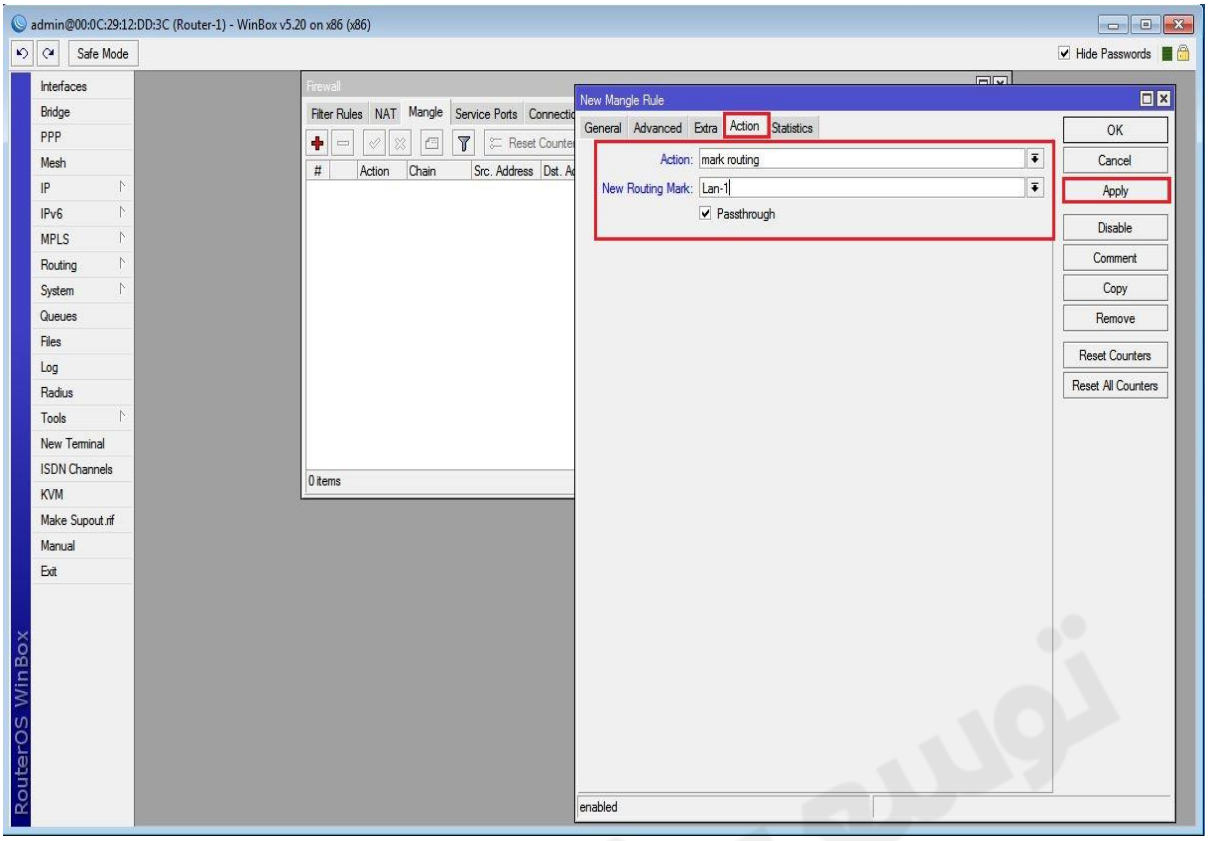


با این تنظیمات شبکه Lan-1 به شبکه Lan-2 دسترسی نخواهد داشت.

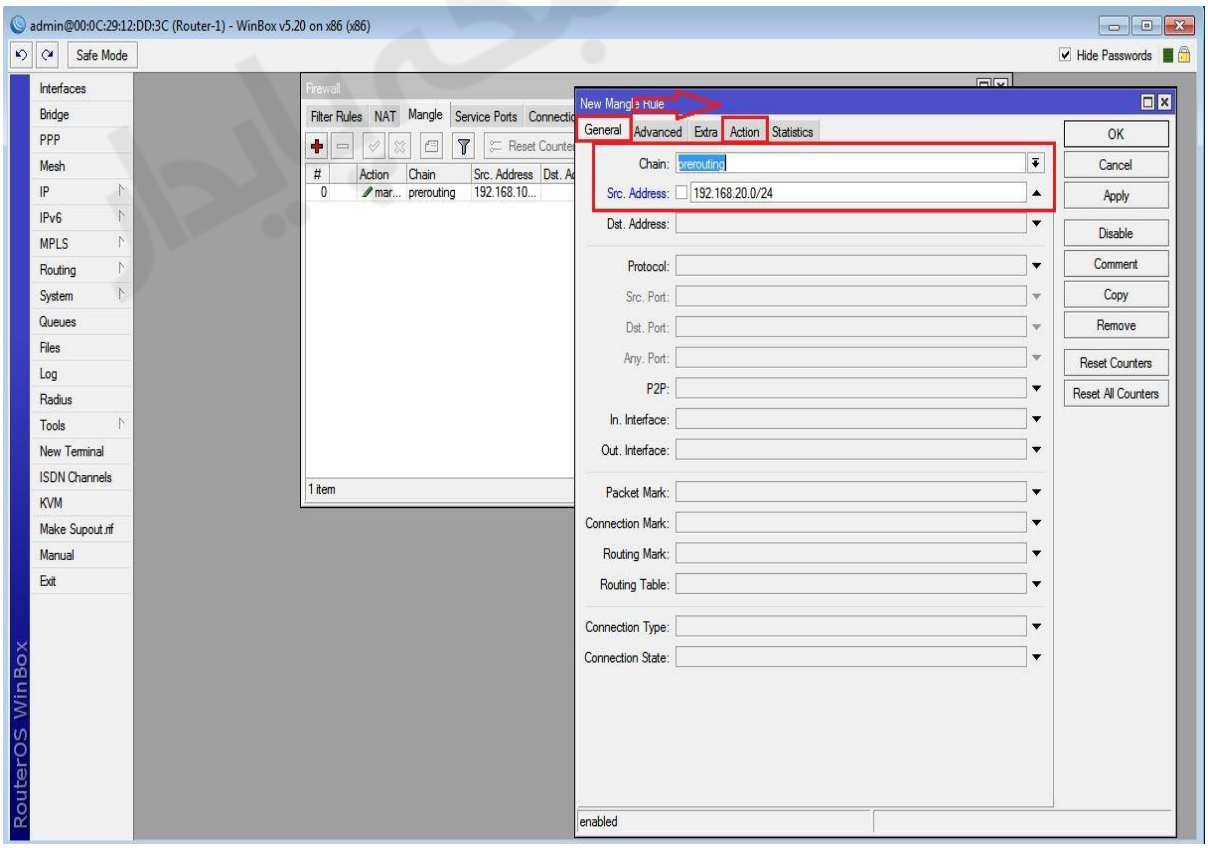
جواب سوال ۲ :

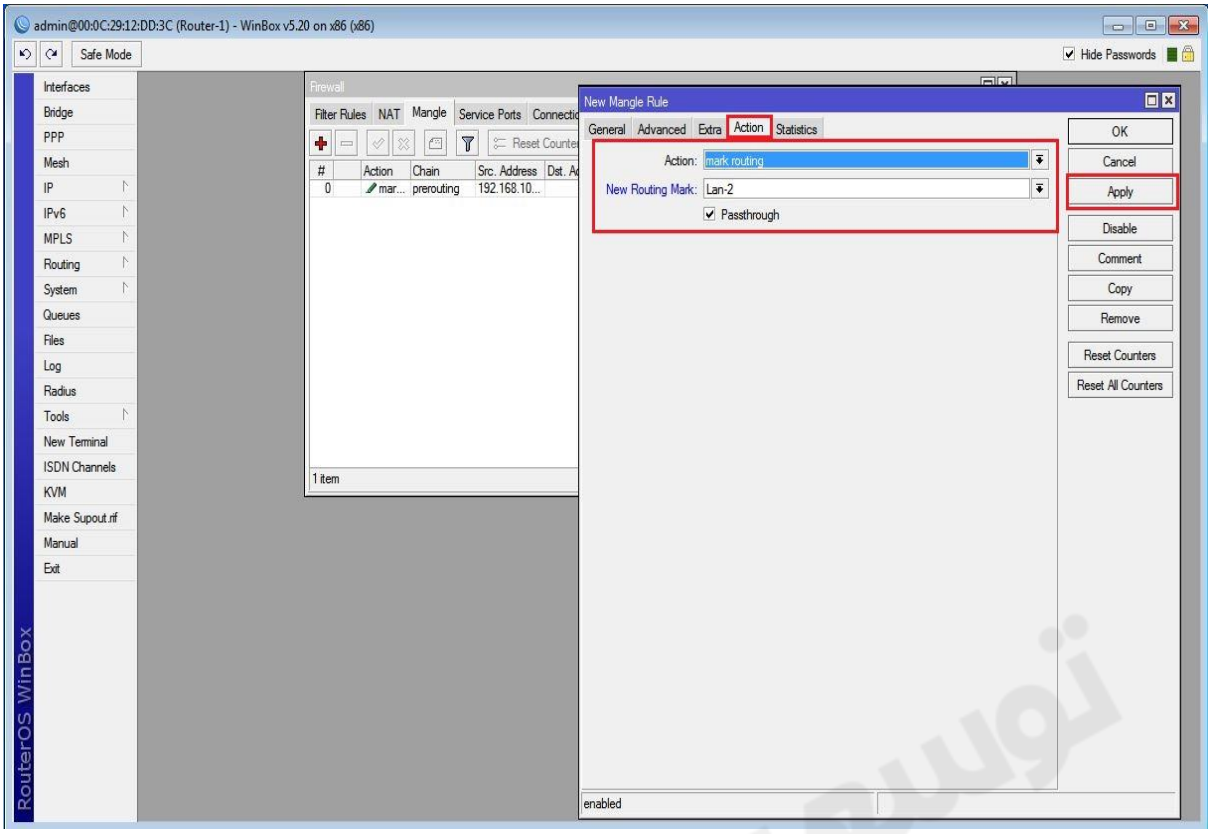
مارک کردن بسته هایی که از سمت شبکه Lan-1 به سمت روتر حرکت میکنند:



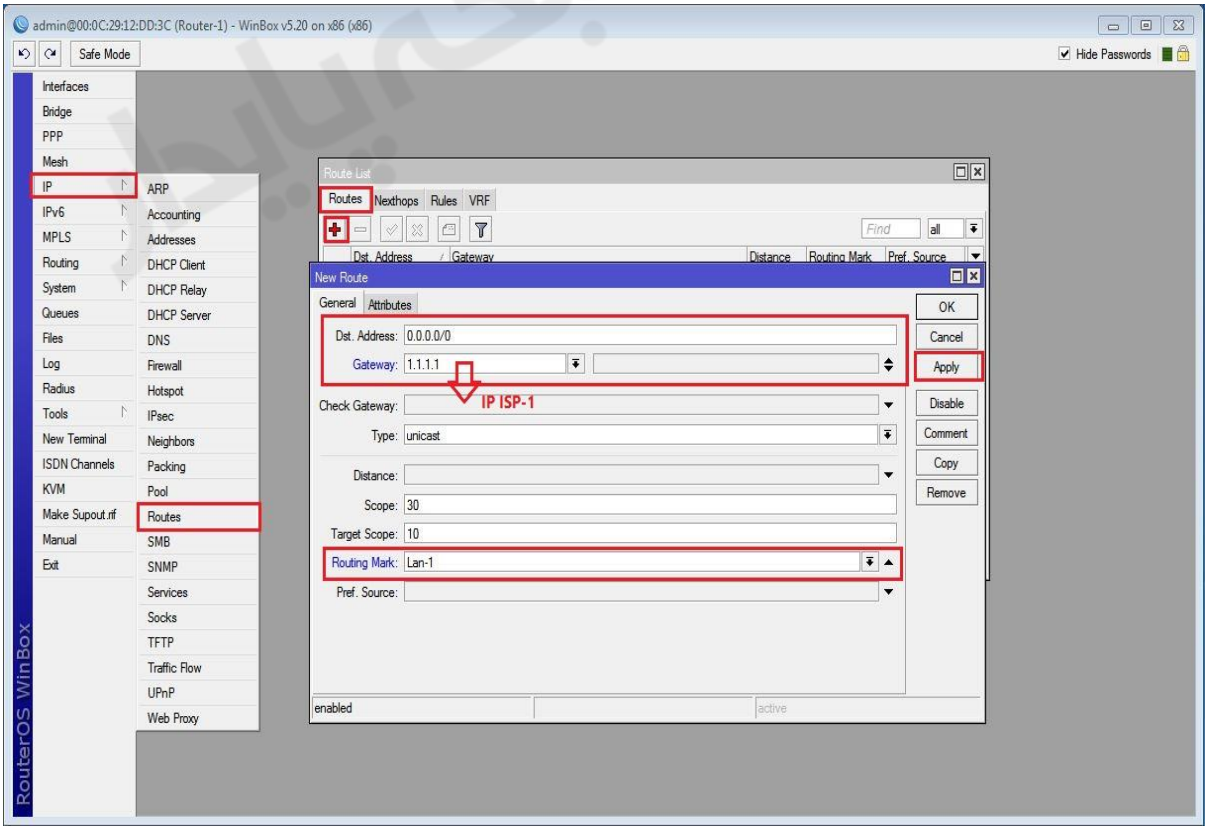


مارک کردن بسته هایی که از سمت شبکه Lan-2 به سمت روتر حرکت میکنند :

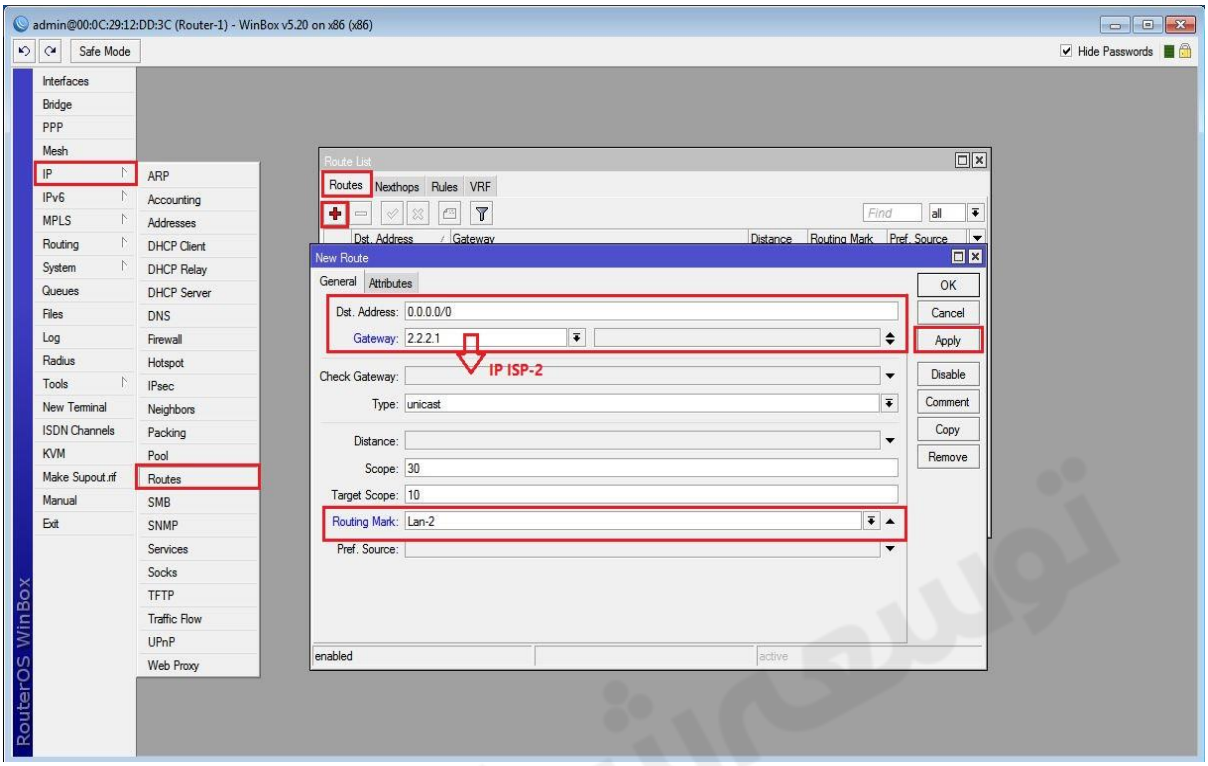


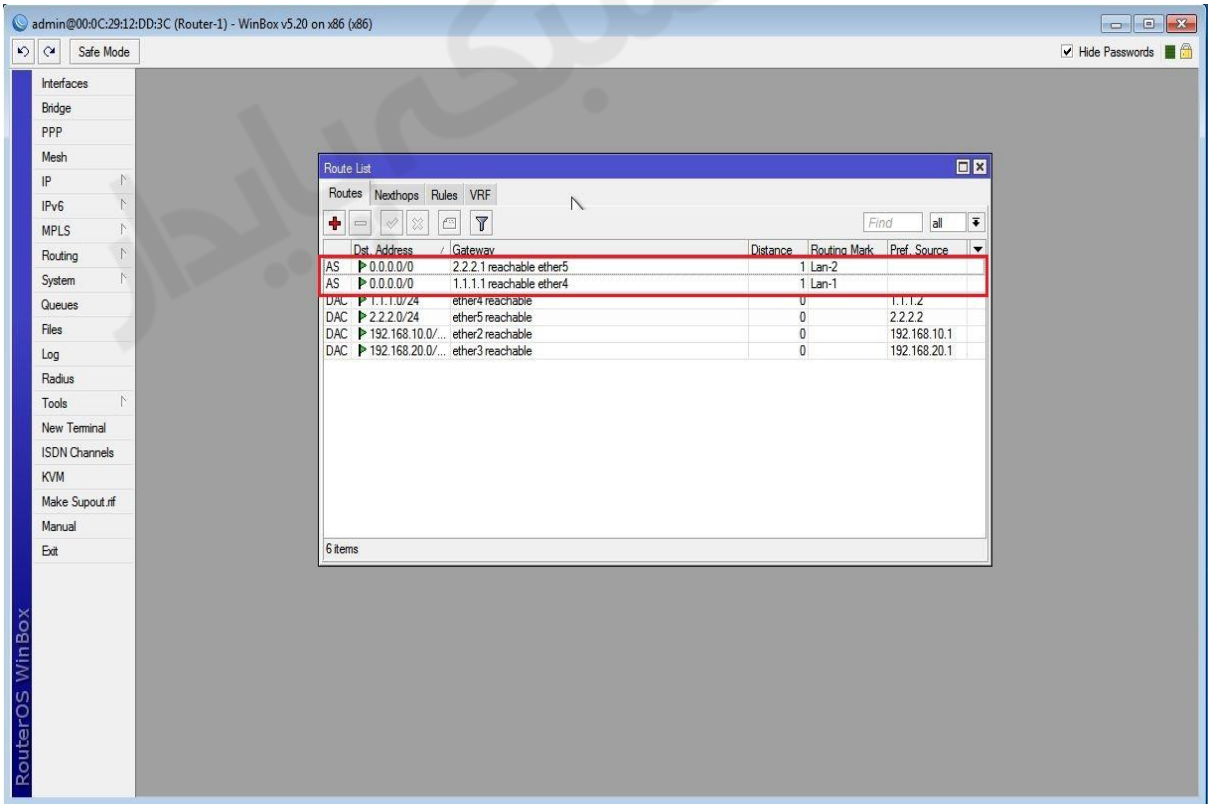


ایجاد **Route** برای اینکه کلاینت های شبکه **Lan-1** از **ISP-1** به اینترنت دسترسی پیدا کنند.در مرحله قبل ما بسته هایی که از شبکه **Lan-1** به سمت روتر حرکت کردند را قبل از مسیر یابی مارک کردیم و اسم آن را **Lan-1** قرار دادیم در این مرحله باید موقع ایجاد **Route** گذرگاه یا همان **GateWay** را برای شبکه **Lan-1** آدرس **IP** ، **ISP-1** وارد کنیم و در قسمت **Routing Mark=Lan-1** را انتخاب کنیم.



ایجاد **Route** برای اینکه کلاینت های شبکه **Lan-2** از **ISP-2** به اینترنت دسترسی پیدا کنند.در مراحل قبل ما بسته هایی که از شبکه **Lan-2** به سمت روتر حرکت کردند را قبل از مسیر یابی مارک کردیم و اسم آن را **Lan-2** قرار دادیم در این مرحله باید موقع ایجاد **Route** گذرگاه یا همان **GateWay** را برای شبکه **Lan-2** آدرس **IP** ، **ISP-2** وارد کنیم و در قسمت **Routing Mark=Lan-2** را انتخاب کنیم.





با این تنظیمات شبکه **Lan-1** از **ISP-1** به اینترنت دسترسی پیدا می کند و همچنین به شبکه **Lan-2** دسترسی ندارد و شبکه **Lan-2** از طریق **ISP-2** به اینترنت دسترسی پیدا می کند.

فصل هفتم : DHCP Server

DHCP مخفف کلمه **Dynamic Host Configuration Protocol** می باشد.این پروتکل برای انتساب تنظیمات شبکه (بطور مثال **IP** و ...) به صورت خودکار به دستگاه های لایه سه موجود در شبکه به کار می رود.
دستگاه های لایه سه شامل : کامپیوتر ، موبایل ، دوربین و ... که **IP** میگیرند می باشد.

بصورت کلی به دو روش می توان به کلاینت ها **IP** اختصاص داد :

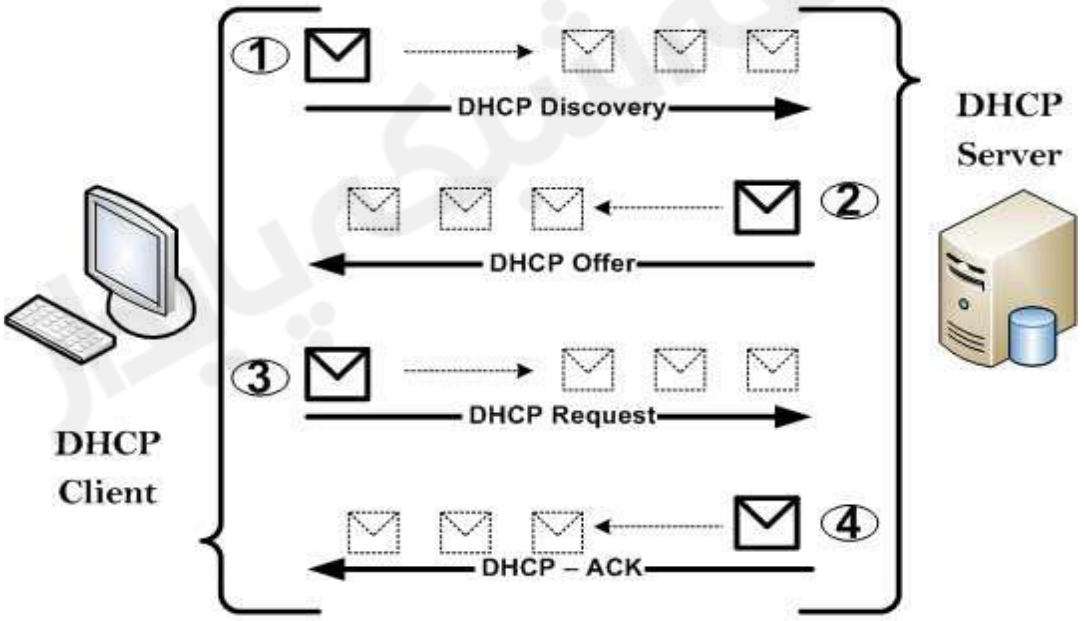
۱. **Static IP**
۲. **Dynamic IP**

Static : در این روش مدیر شبکه به صورت دستی به کارت شبکه **IP** مورد نظر را انتساب می دهد.

Dynamic : در این روش یک سرور به عنوان **Dhcp Server** در شبکه قرار می گیرد تا اینکه بصورت اتوماتیک به سیستم های موجود ، تنظیمات شبکه را اختصاص دهد.

Dhcp بصورت **Client-Server** ساخته شده است.به این معنی که کلاینت ، یک بسته (**Request**) مبنی بر گرفتن تنظیمات شبکه را ارسال می کند و سرور در پاسخ (**Reply**) تنظیمات را برای کلاینت ارسال می کند.

بطور کلی مراحل دریافت تنظیمات از **Dhcp Server** در شکل زیر شرح داده شده است :



۱)زمانی که کامپیوتری در شبکه قرار میگیرد یک بسته به اسم **Dhcp Discover** که برای پیدا کردن **Dhcp Server** است را در کل شبکه **Broadcast** می کند.

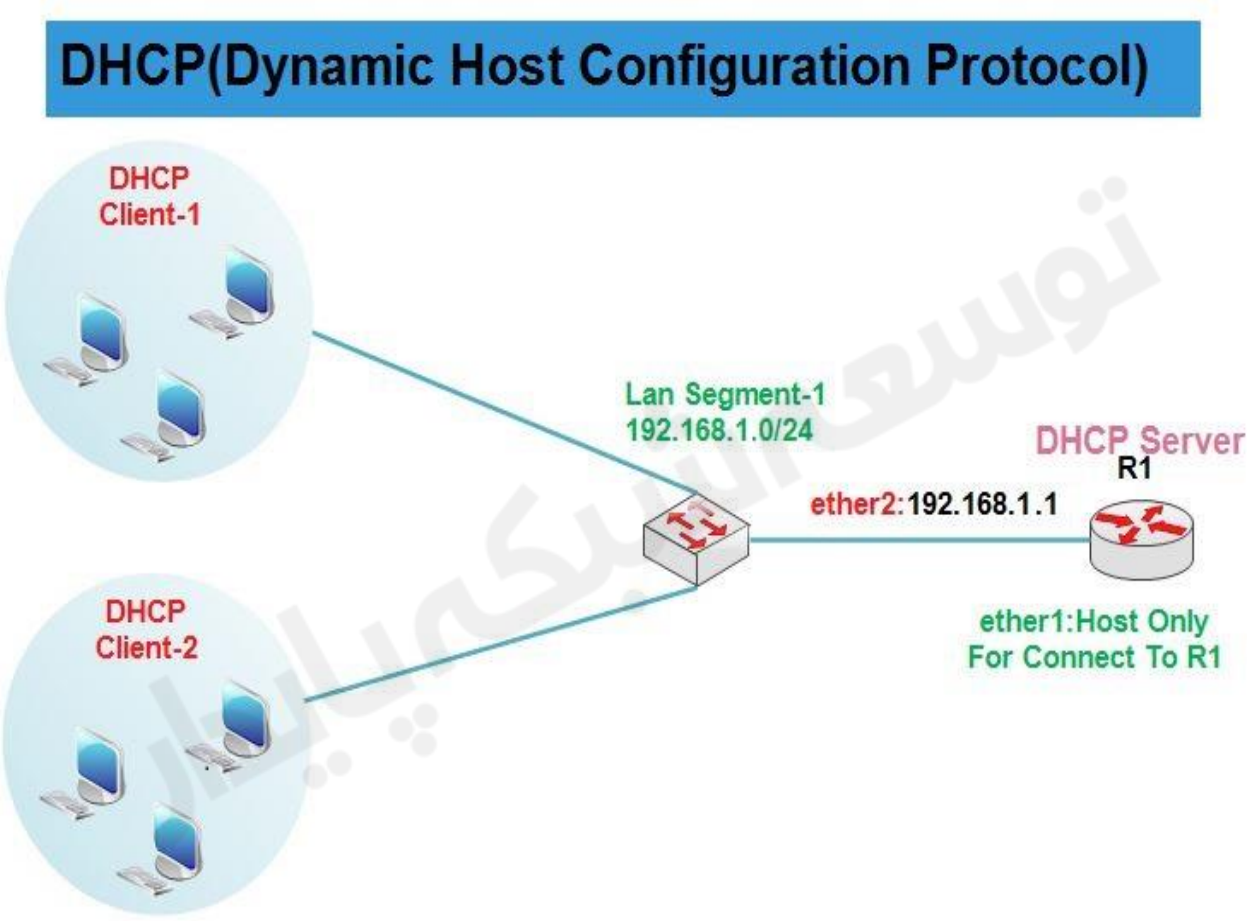
۲)**Dhcp Server** های موجود درشبکه (در صورتی که چندین **Dhcp Server** وجود داشته باشد) تنظیمات شبکه را در قالب بسته ای به اسم **Dhcp Offer** به کلاینت ها پیشنهاد می دهند.

۳)کلاینت اولین بسته ی **Dhcp Offer** که به سمت آن آمده است را قبول می کند و بسته **Dhcp Request** که شامل درخواست تنظیمات شبکه از همان **Dhcp Server** می باشد را در کل شبکه **Broadcast** می کند.

۴)تمامی **Dhcp Server** ها بسته **Request** را دریافت می کنند ، اما تنها آن سروری که کلاینت بسته **Offer** آن را پذیرفته است ، تنظیمات را در قالب بسته ایی به نام **Dhcp-Ack** برای کلاینت ارسال می کند و از این رو سرور مورد نظر تایید می کند که **IP** پیشنهادی را به کلاینت اختصاص داده است.چنانچه به هر دلیلی این **IP** به کلاینت اختصاص داده نشود یک بسته با عنوان **Dhcp-NAck** به کلاینت برگشت داده می شود.

میکروتیک را می توان هم به عنوان یک **Dhcp Server** هم به عنوان یک **Dhcp Client** در شبکه به کار برد.

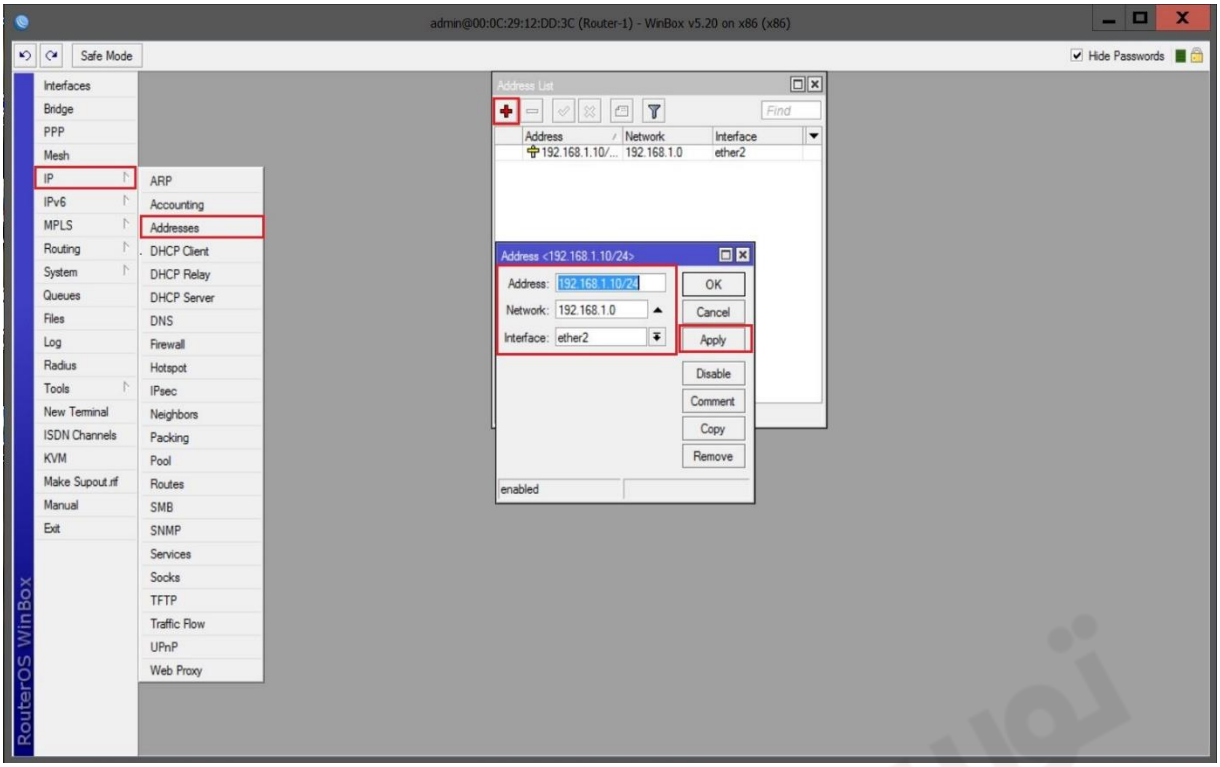
سناریو ۱ : برای پیاده سازی سرویس **DHCP** بر روی دستگاه میکروتیک سناریو زیر را بررسی می کنیم :



در این سناریو یک روتر میکروتیک به عنوان **Dhcp Server** و یک کلاینت در نظر گرفته شده است که بصورت اتومات از **Dhcp** سرور **IP** دریافت کند.

*نکته ایی که باید توجه داشته باشد در این سناریو ما فقط **Dhcp** سرور را ، راه اندازی می کنیم و شما می توانید برای اینکه کلاینت ها از **Dhcp** سرور **IP** گرفته و به اینترنت دسترسی داشته باشند را با استفاده از سناریو های قبل انجام دهید.

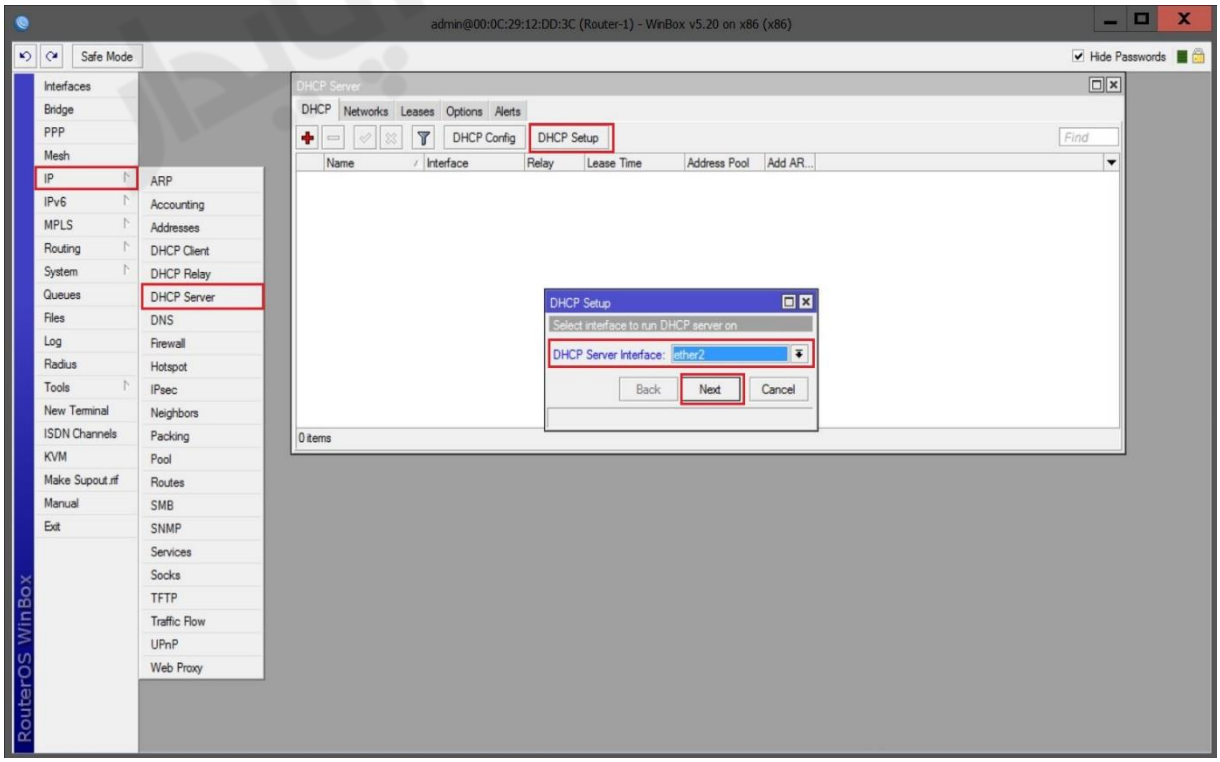
طبق سناریو اولین کاری که انجام می دهیم این است که به کارت شبکه روتر **R1** آدرس **IP** اختصاص می دهیم.



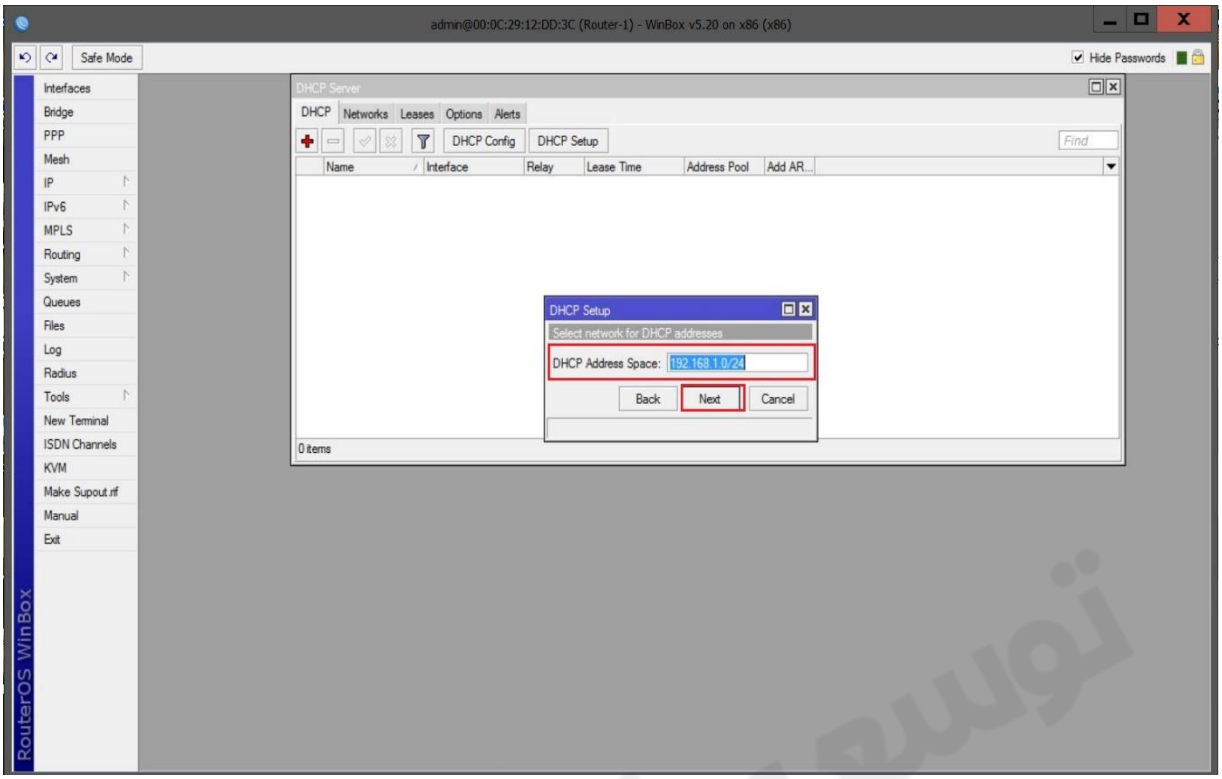
نصب و راه اندازی DHCP سرور :

برای این کار از منوی اصلی گزینه IP را انتخاب و از زیر منوی باز شده DHCP Server را انتخاب می کنیم.از پنچره باز شده و از بخش DHCP گزینه DHCP Setup را انتخاب می کنیم .

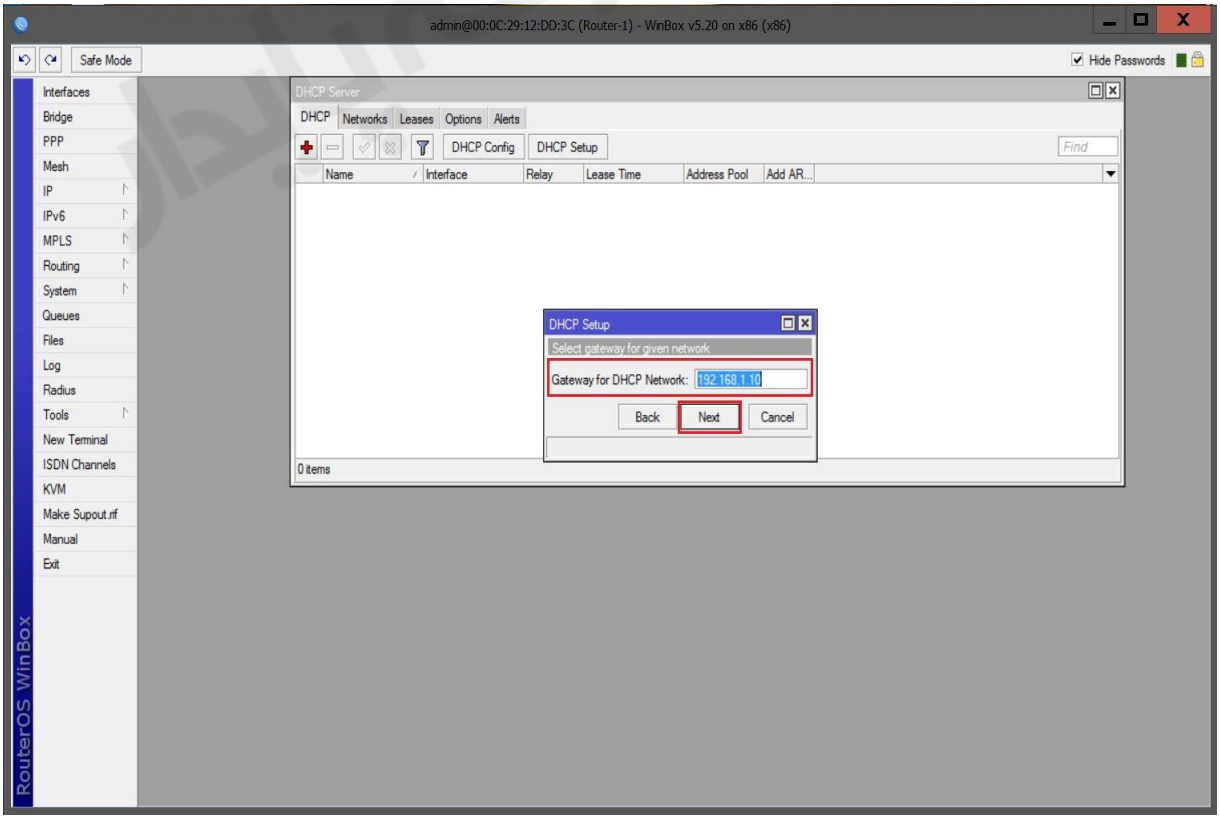
در این مرحله باید کارت شبکه مورد نظر که می خواهیم از طریق آن سرویس DHCP به کلاینت ها IP دهد را انتخاب کنیم.



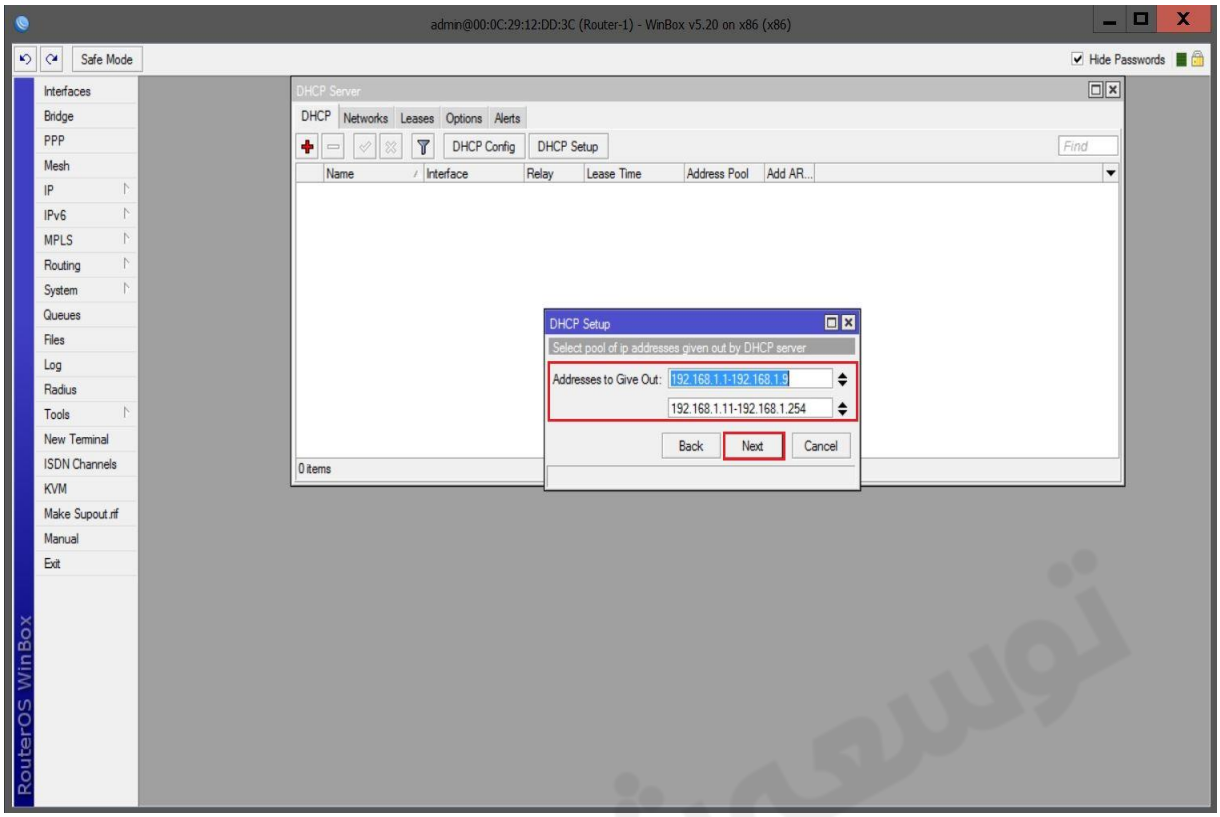
در این مرحله محدوده **IP** مربوط به شبکه ایی که می خواهیم **DHCP** در آن فعال باشد را انتخاب می کنیم.



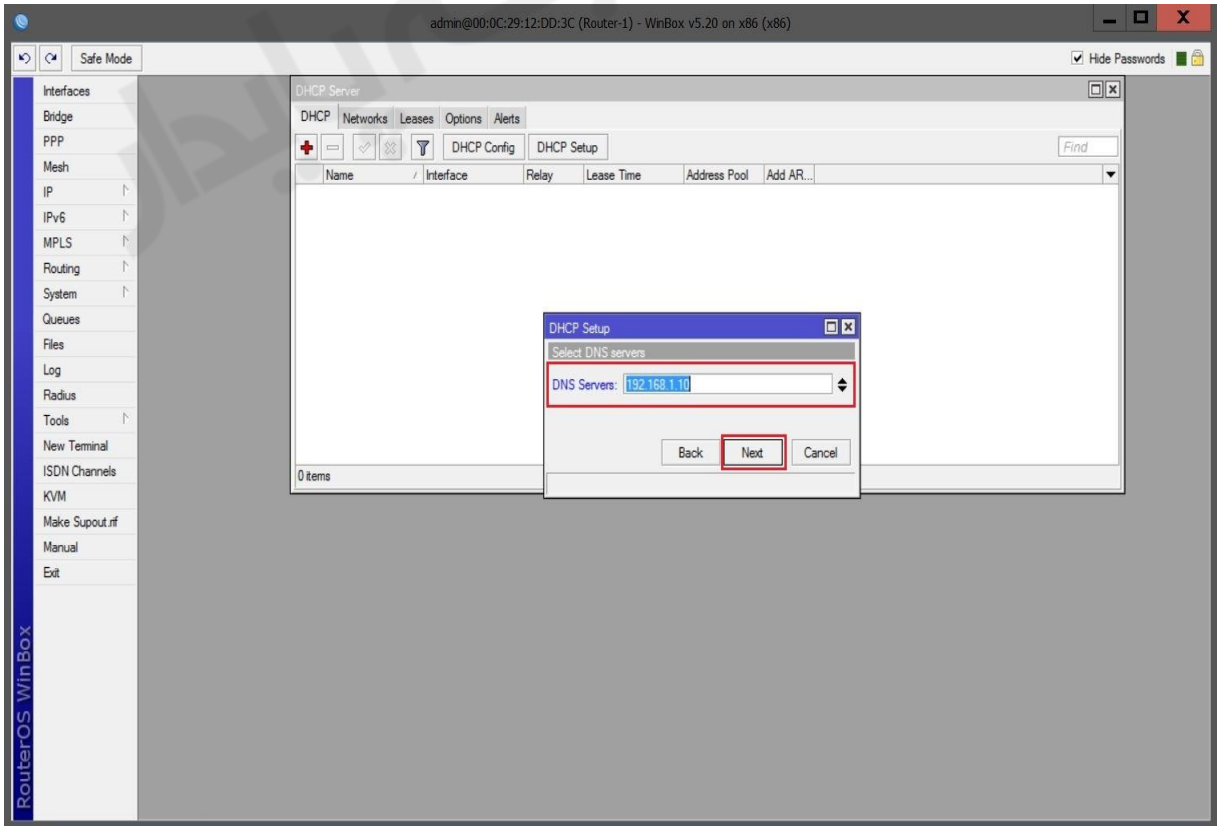
در این قسمت **Gateway** (دروازه) مورد نظر که می خواهیم برای کلاینت ها را **Set** کنیم را وارد میکنیم.این **Option** در حقیقت **IP** مربوط به روتر در شبکه می باشد.



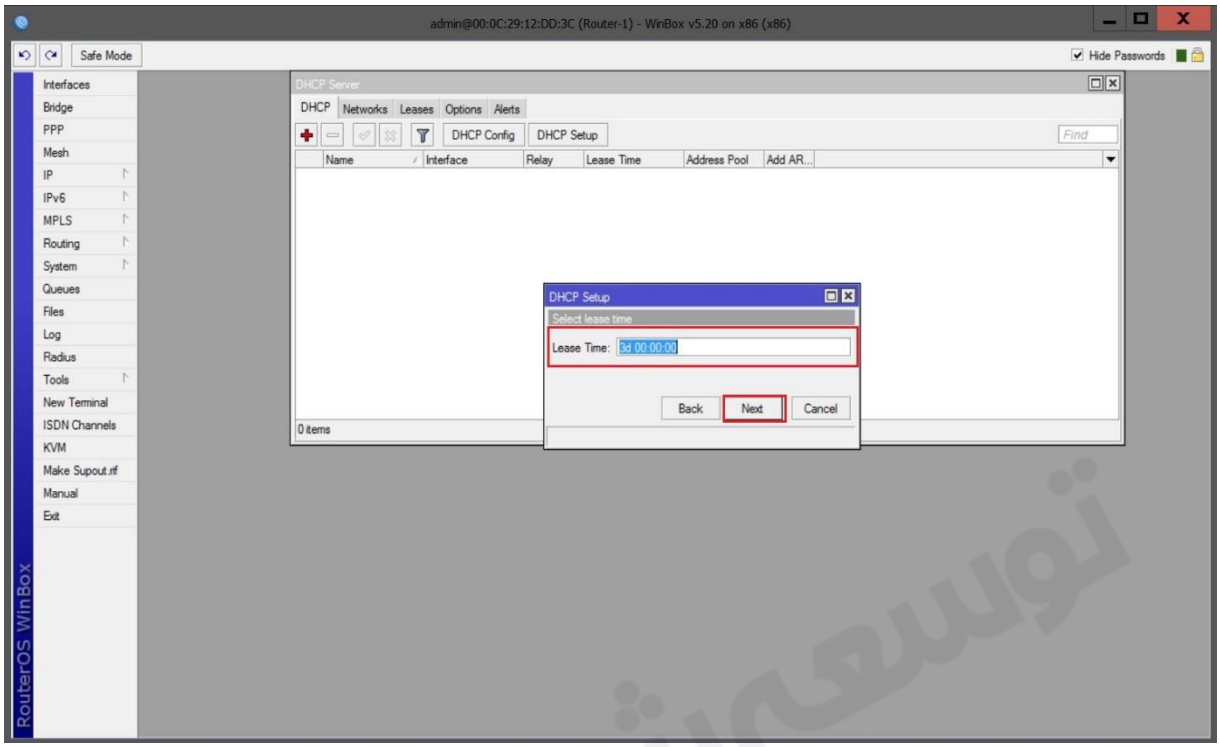
در این قسمت **Pool** یا محدوده ایی از **IP**ها را که می خواهیم **DHCP** برای کلاینت ها شبکه در نظر بگیرد را انتخاب می کنیم.



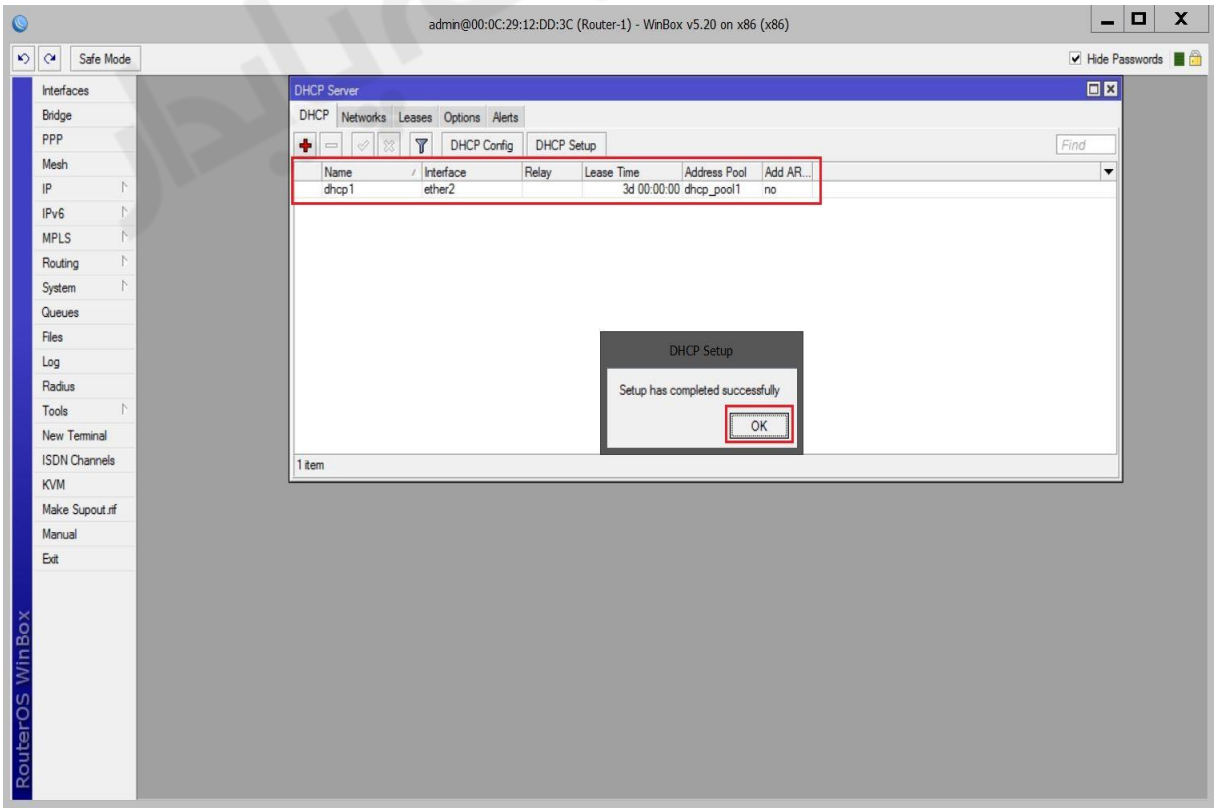
آدرس مربوط به **DNS** سرور موجود در شبکه را وارد میکنیم.



در این قسمت مدت زمانی که IP به کلاینت تخصیص داده می شود را انتخاب می کنیم.بصورت پیش فرض ۳ روز این IP به کلاینت اختصاص داده می شود و بعد از این مدت IP از کلاینت گرفته می شود و چنانچه درخواست برای IP از سیستم دیگری زودتر به DHCP Server برسد این IP به کلاینت دیگر اختصاص داده می شود.

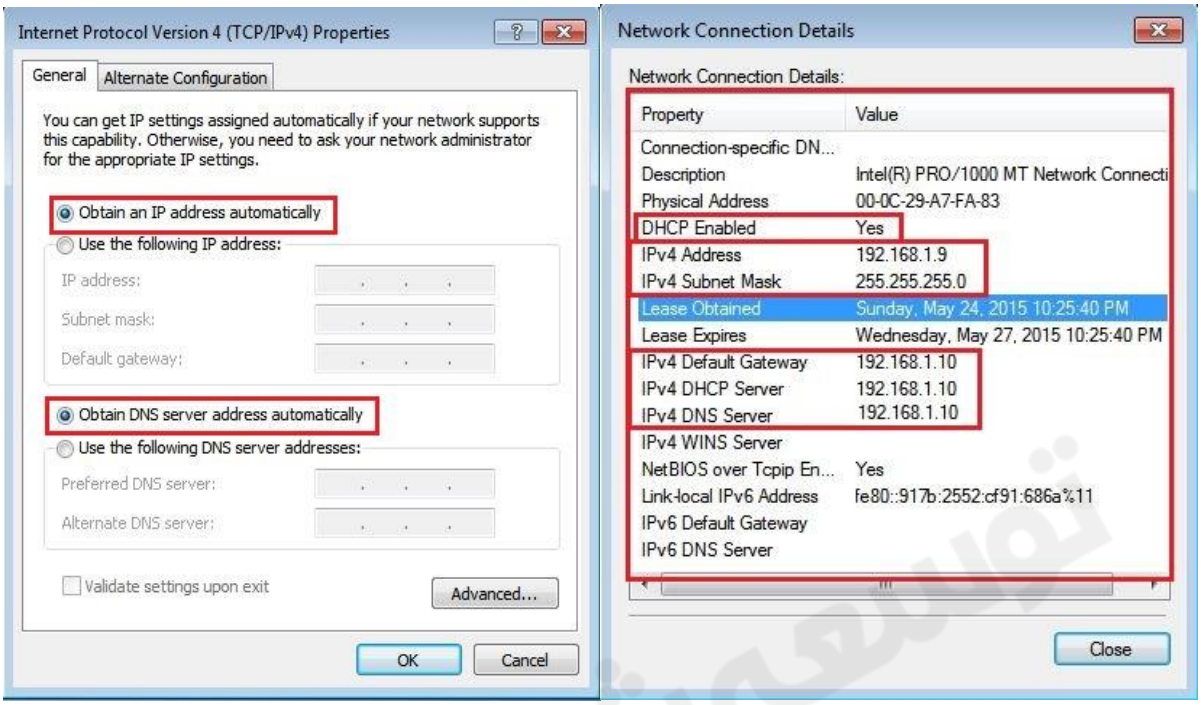


و در نهایت پس از این مرحله DHCP راه اندازی شده و شما با پیغام زیر رو به رو خواهید شد :

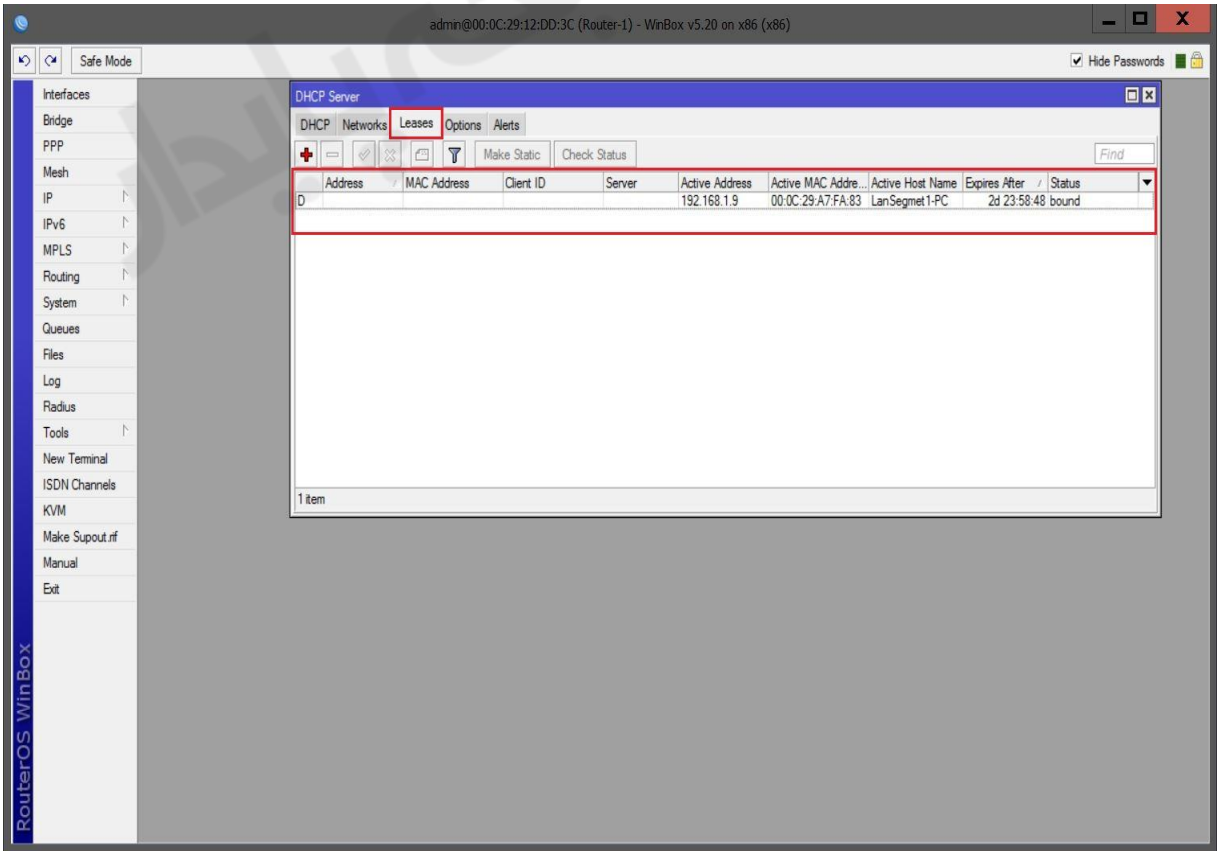


تنظیم کردن کلاینت و دریافت IP از DHCP سرور :

برای این کار کافی است به جای اینکه بصورت دستی برای کلاینت IP تعریف کنید گزینه زیر که در عکس ملاحضه می کنید را انتخاب کنید. با این کار کلاینت از DHCP که بر روی روتر میکروتیک راه اندازی کردید IP دریافت خواهد کرد.



همچنین در روتر میکروتیکی که DHCP راه اندازی کردید می توانید مشخصات کلاینت هایی که از DHCP سرور IP دریافت کرده اند را ببینید.



نکته : در خیلی از **Dhcp** سرورها(ویندوز و سیسکو و ...) چنانچه **Scope** و یا **Pool** ی که تعریف کرده ایم در محدوده ی کارت شبکه **Dhcp** سرور نباشد به کلاینت ها **IP** داده نمی شود اما در میکروتیک **Pool** تعریف شده می تواند از محدوده **IP** کارت شبکه نباشد.

بطور مثال چنانچه **IP** مربوط به کارت شبکه **Dhcp-Server** از محدوده **10.10.10.0** باشد اما **Pool** تعریف شده از محدوده **192.168.1.0/24** باشد کلاینت ها از محدوده **192.168.1.X** آدرس**IP** میگیرند.

نصب و راه اندازی **DHCP** سرور از طریق دستور :

با وارد کردن دستور **ip dhcp-server setup** مواردی بصورت محاوره ایی پرسیده می شود که در زیر مشاهده می کنید :

[admin@Router-1] > ip dhcp-server setup

Select interface to run DHCP server on

dhcp server interface: ether2

Select network for DHCP addresses

dhcp address space: 192.168.1.0/24

Select gateway for given network

gateway for dhcp network: 192.168.1.10

Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.1.1-192.168.1.9,192.168.1.11-192.168.1.254

Select DNS servers

dns servers: 192.168.1.10

Select lease time

lease time: 3d 00:00:00

نشان دادن تنظیمات مربوط به **DHCP** :

[admin@Router-1] > ip dhcp-server print

با استفاده از این دستور تنظیمات مربوط به شبکه ایی که **Dhcp** سرور در آن قرار دارد را مشاهده می کنید :

[admin@Router-1] > ip dhcp-server network print

نشان دادن تنظیمات مربوط به **Pool** :

[admin@Router-1] > ip pool print

رزرو کردن یک **IP** برای یک سیستم خاص :

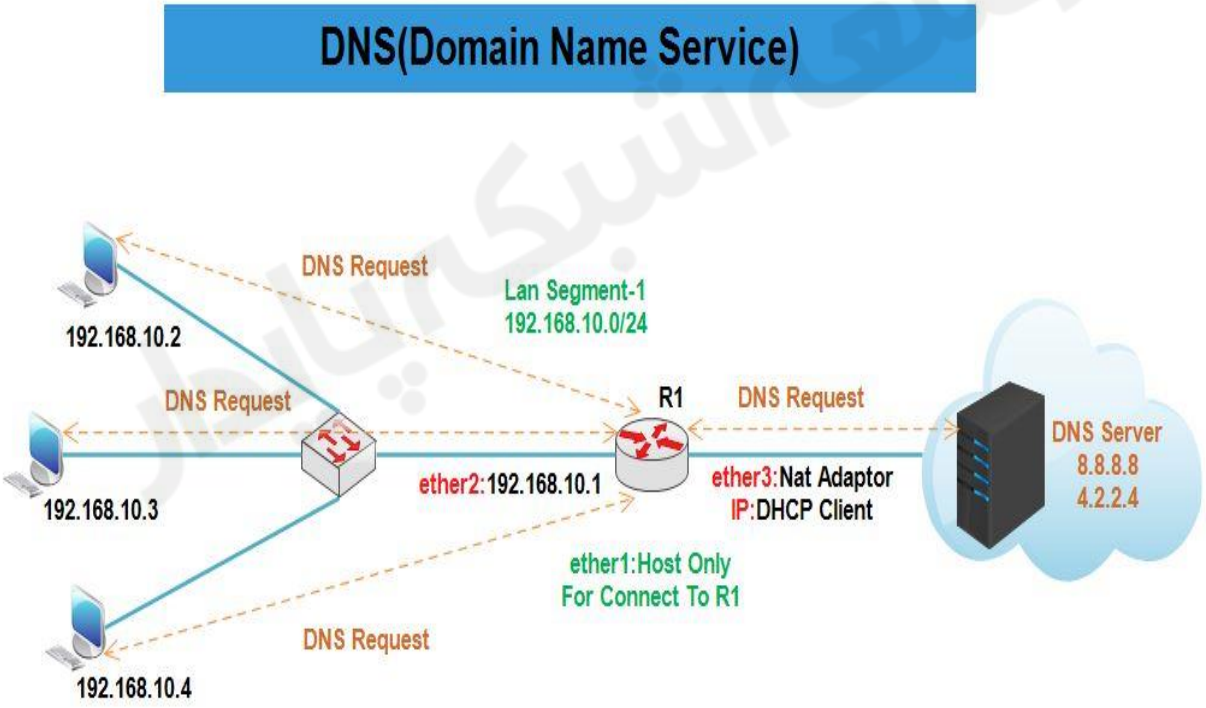
[admin@Router-1] >ip dhcp-server lease add mac-address=<Mac Address> address=192.168.1.100

فصل هشتم : DNS

DNS مخفف **Domain Name Service** است و سرویسی برای تبدیل نام دامنه به **IP** ، یا **IP** به اسم ، در شبکه های **Lan** ، اینترنت و ... می باشد. عملکرد سرویس **DNS** به این صورت است که وقتی کاربری در **URL** خود ، نام سایتی را وارد می کند این درخواست به سرور **DNS** ارسال می شود بر روی **DNS** سرور به ازای هر نام یک آدرس **IP** نیز برای آن تنظیم شده است ، بنابراین سرور فوق ، آدرس **IP** برای **URL** درخواست شده را برمیگرداند و از این پس درخواست های صفحات وب براساس **IP** مسیریابی می شود.

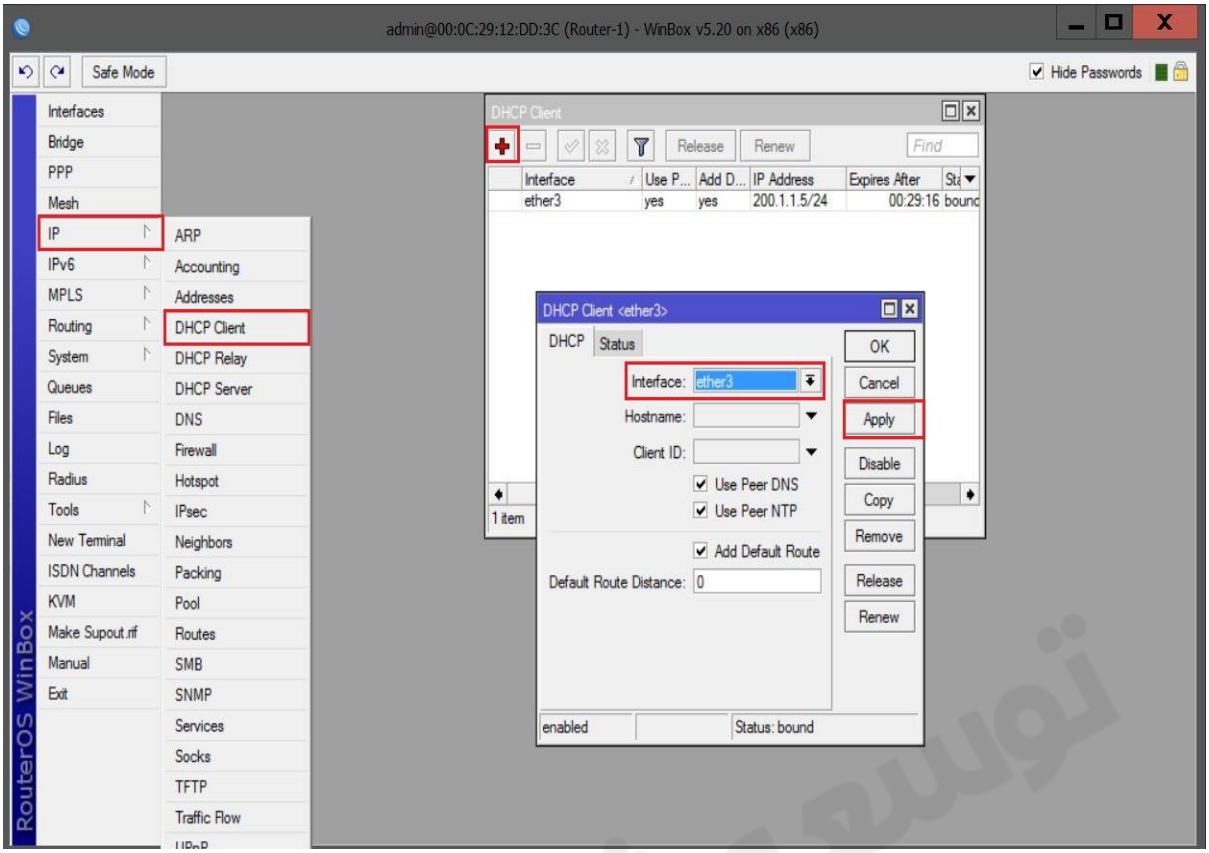
در بسیاری از مواقع ، کاربران به علت عدم آگاهی لازم از مفاهیم شبکه ، در هنگام تنظیم **IP** بر روی سیستم خود و یا تغییر آن به هر علتی ، تنظیمات **DNS** آن را به درستی انجام نمی دهند. بنابراین در هنگام باز کردن صفحه مورد نظر خود برروی مروگر ، چون درخواست به سرور **DNS** ارسال نمی شود بنابراین هیچ **IP** آدرسی جهت مسیریابی بازگردانده نشده و در نهایت صفحه درخواست شده ، برروی مرورگر باز نمی شود. عیب یابی و حل این موضوع ، سبب اتلاف وقت کابران و مدیران شبکه می شود. در نتیجه اگر تمام درخواست های **DNS** از طریق روتر پاسخ داده شوند دیگر با چنین مشکلاتی روبه رو نخواهید شد.

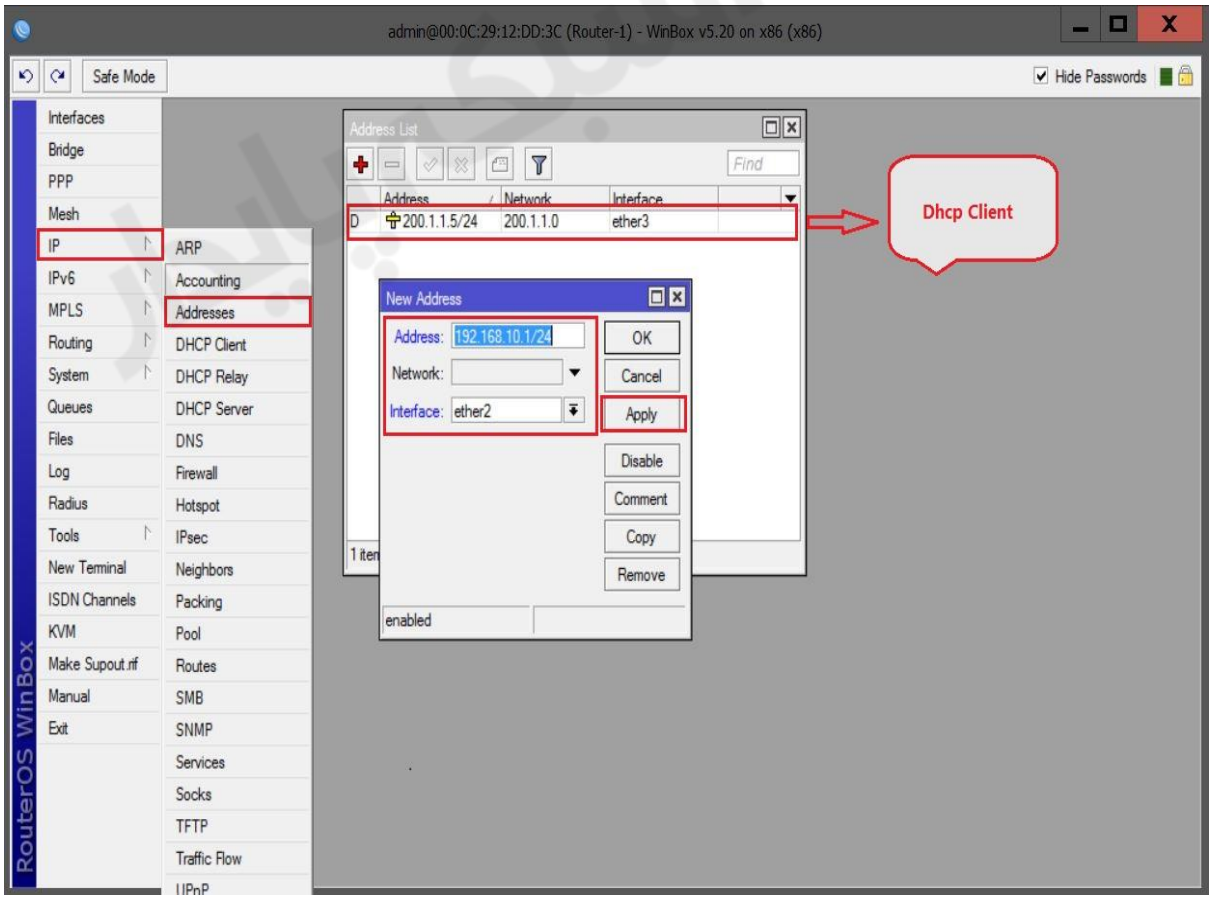
سناریو ۱ : در این سناریو نحوه تنظیم پاسخگویی به در خواست های **DNS**ای را ، بگونه ای که فقط از طریق روتر انجان پذیرند را آموزش می دهیم.در این حالت در صورتی که کاربر بر روی تنظیمات کارت شبکه خود ، آدرس **DNS** را اشتباها تنظیم کرده باشد و یا از هر آدرس دیگری برای **DNS** استفاده کند ، تنظیمات **DNS** ای کاربر بدون اهمیت بوده و میکروتیک مستقیما به درخواست های **DNS**ای پاسخ خواهد داد.



انتساب **IP** به کارت های شبکه روتر **R1** :

همان طور که در سناریو مشخص کردیم **Ether3** باید از **Dhcp Client** (**Vmware**) آدرس**IP** دریافت کند.برای این کار از منوی اصلی گزینه **IP** و از زیر منوی باز شده **Dhcp Client** را انتخاب میکنیم.در پنجره باز شده بر روی **Add** کلیک و از تب **Dhcp** اینترفیس مورد نظر را انتخاب و **ok** را میزنیم.

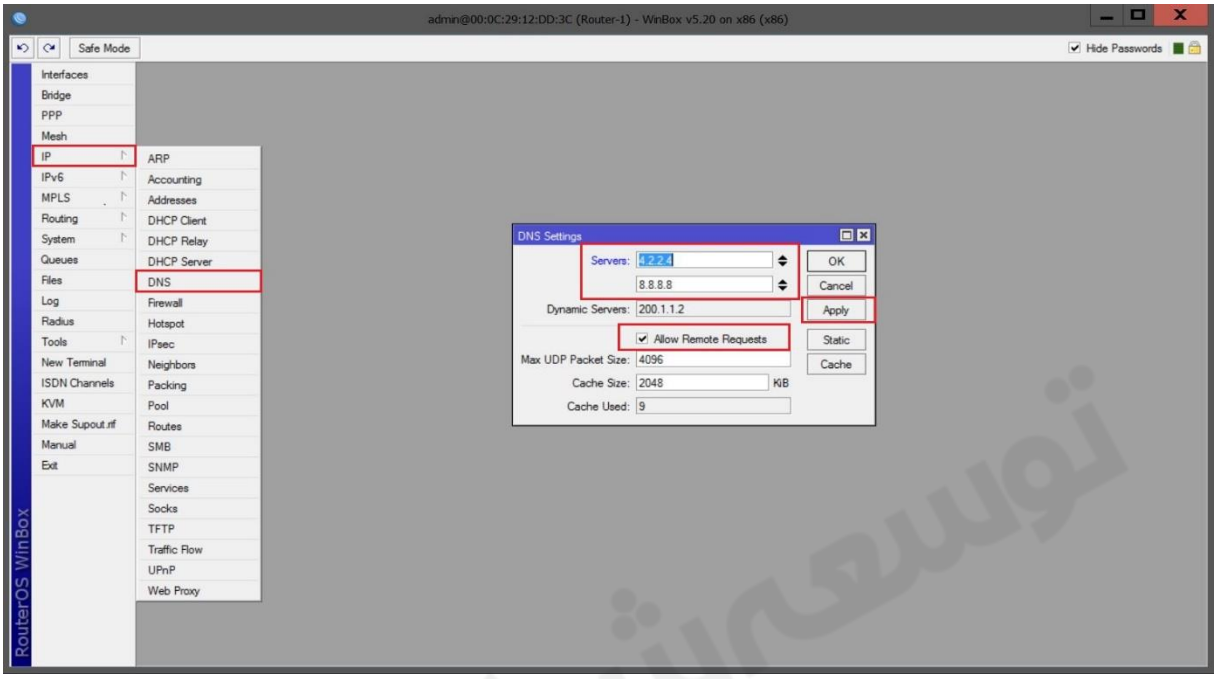

admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
RouterOS WinBox
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Socks
TFTP
Traffic Flow
DHCP Client
Release
Renew
Find
Interface
Use P...
Add D...
IP Address
Expires After
ether3
yes
yes
200.1.1.5/24
00:29:16
1 item
DHCP Client <ether3>
DHCP
Status
Interface: ether3
Hostname:
Client ID:
Use Peer DNS
Use Peer NTP
Add Default Route
Default Route Distance: 0
OK
Cancel
Apply
Disable
Copy
Remove
Release
Renew
enabled
Status: bound


admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
RouterOS WinBox
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Socks
TFTP
Traffic Flow
Address List
Find
Address
Network
Interface
D
200.1.1.5/24
200.1.1.0
ether3
Dhcp Client
New Address
Address: 192.168.10.1/24
Network:
Interface: ether2
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled

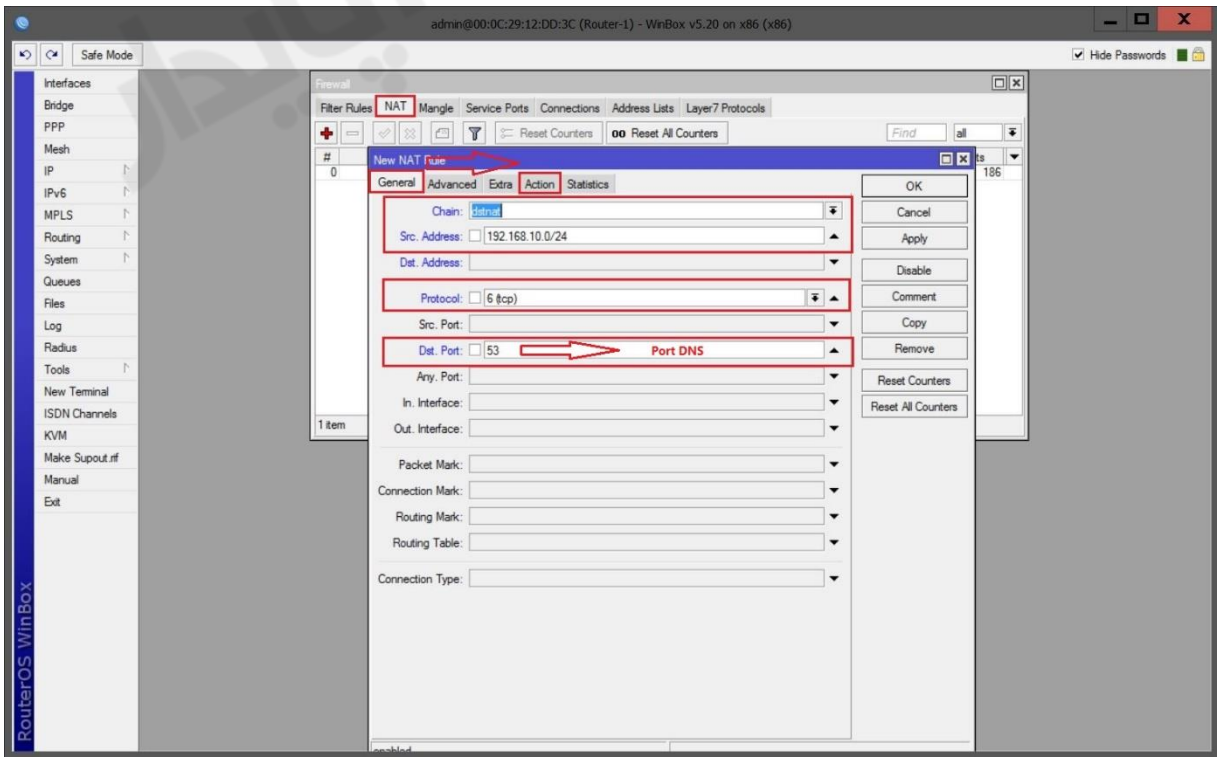
نصب و راه اندازی DNS :

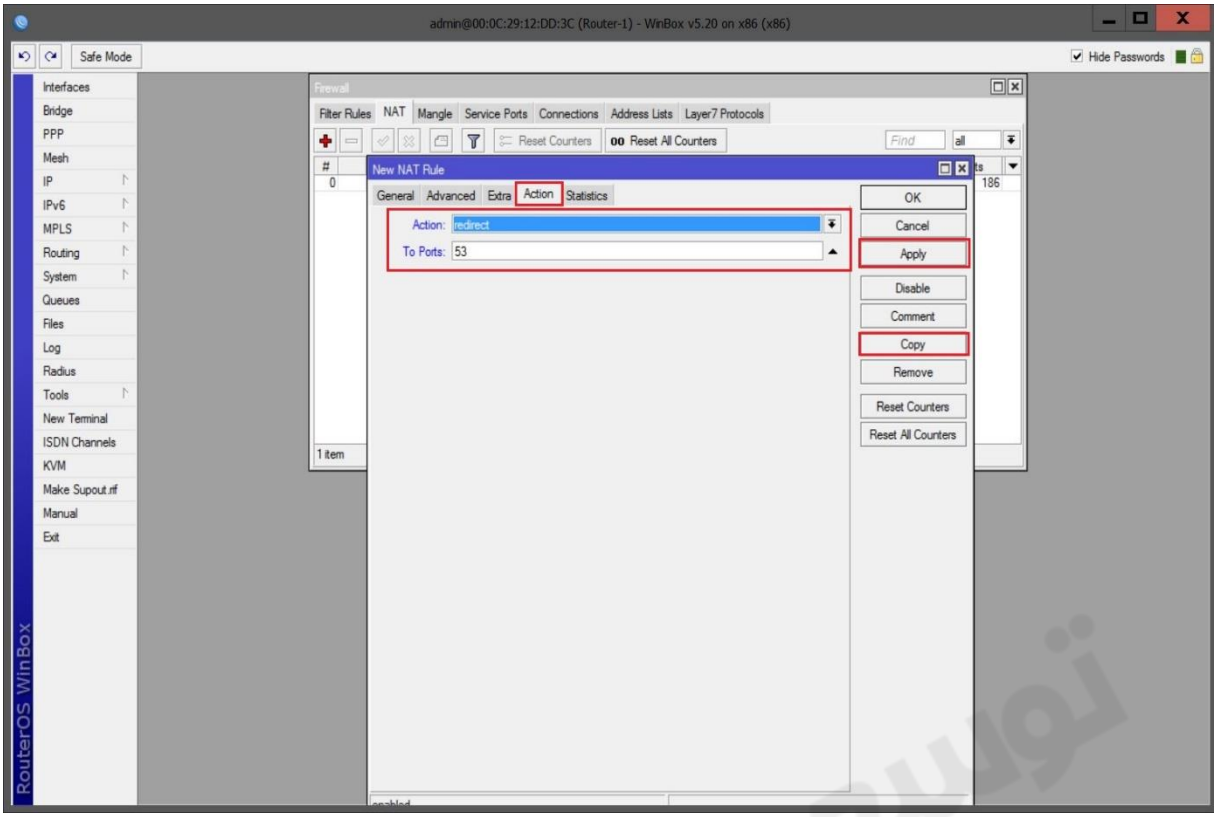
برای این کار از مسیر اصلی گزینه IP را انتخاب و از زیر منوی باز شده بر روی DNS کلیک می کنیم.از پنجره باز شده تنظیمات را طبق عکس زیر انجام می دهیم.

به این نکته توجه داشته باشد در صورتی که تیک گزینه Allow Remote Request فعال شود روتر شما به عنوان DNS سرور شناخته شده و ممکن است در معرض حملات و آسیب های DNSای از طریق اینترنت قرار گیرد.

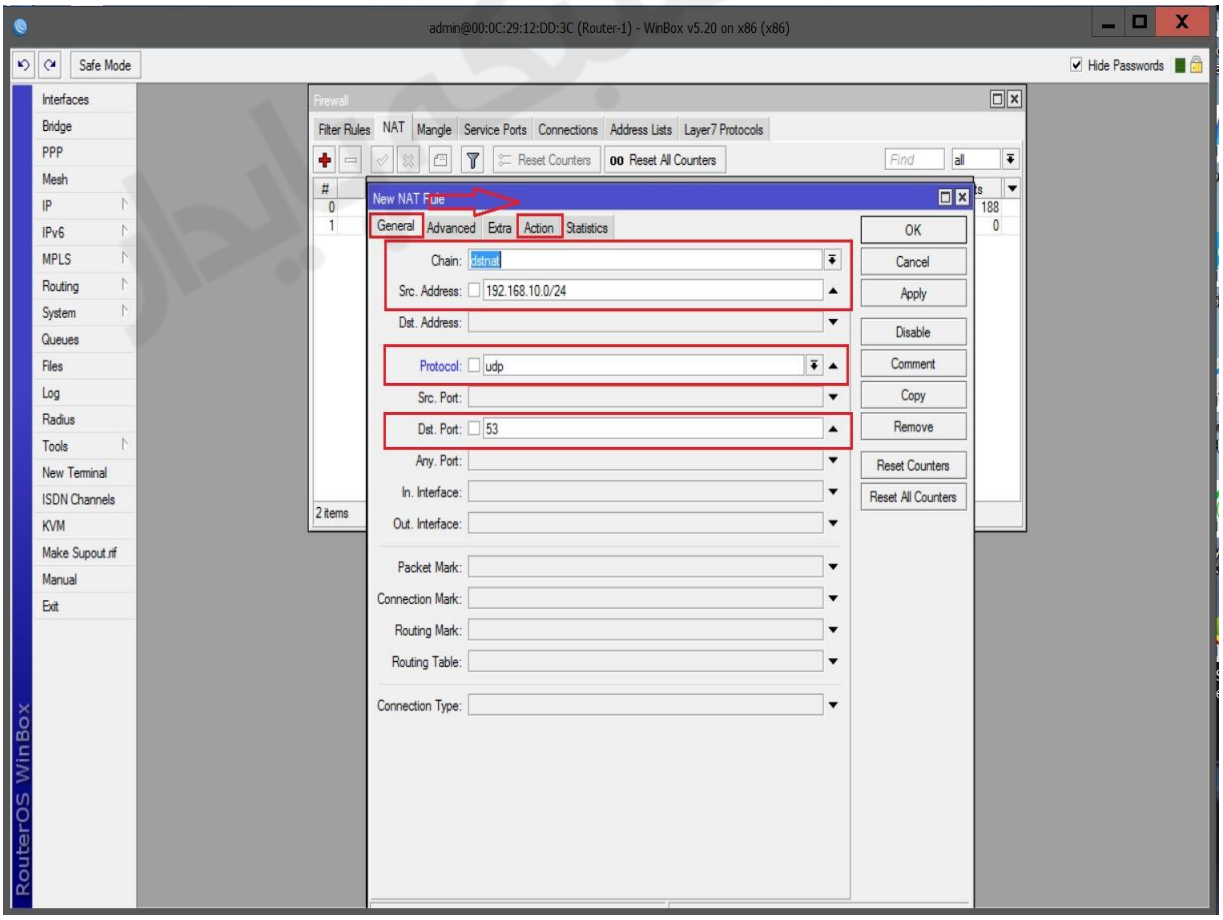


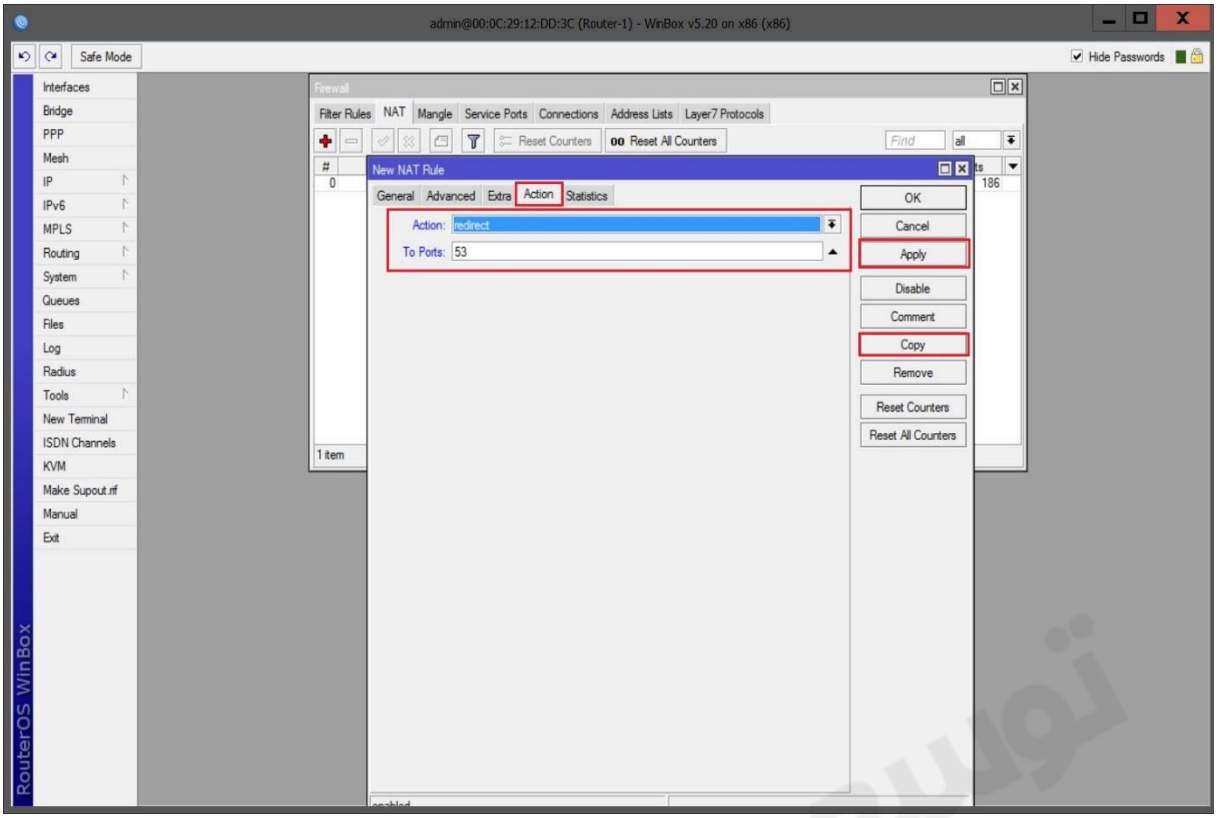
با این تنظیمات پروسه Resolve(تبدیل اسم به IP و یا IP به اسم) انجام میشود اما در صورتی که کاربر به هر علتی IP آدرس DNS را بصورت دستی و اشتباه وارد کند پروسه Resolve اتفاق نمی افتد برای جلوگیری از این مشکل به مسیر زیر رفته و کارها را طبق تنظیماتی که در عکس های زیر مشاهده می کنید انجام میدهیم :





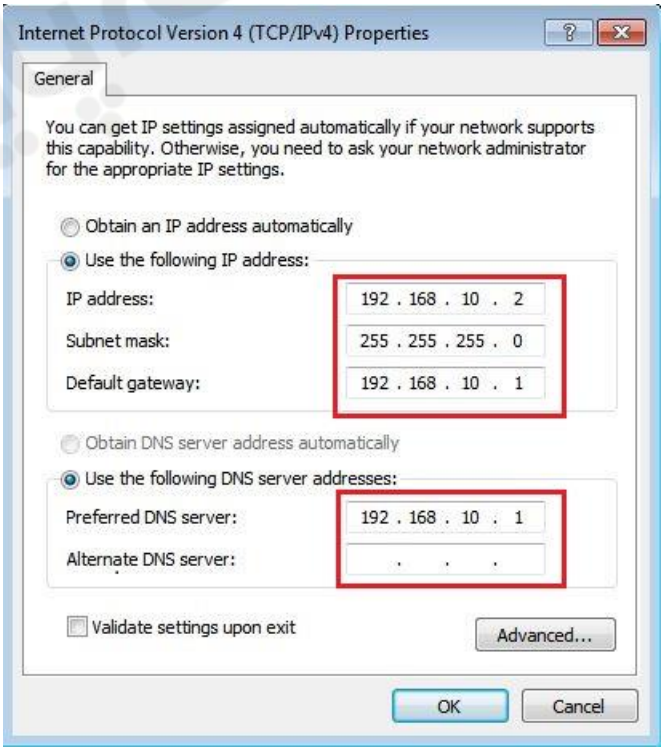
نکته : چون DNS هم از TCP و هم از UDP پشتیبانی می کند به همین د لیل هر دو آن را تعریف می کنیم و 53 نیز پورت پیش فرض DNS می باشد.



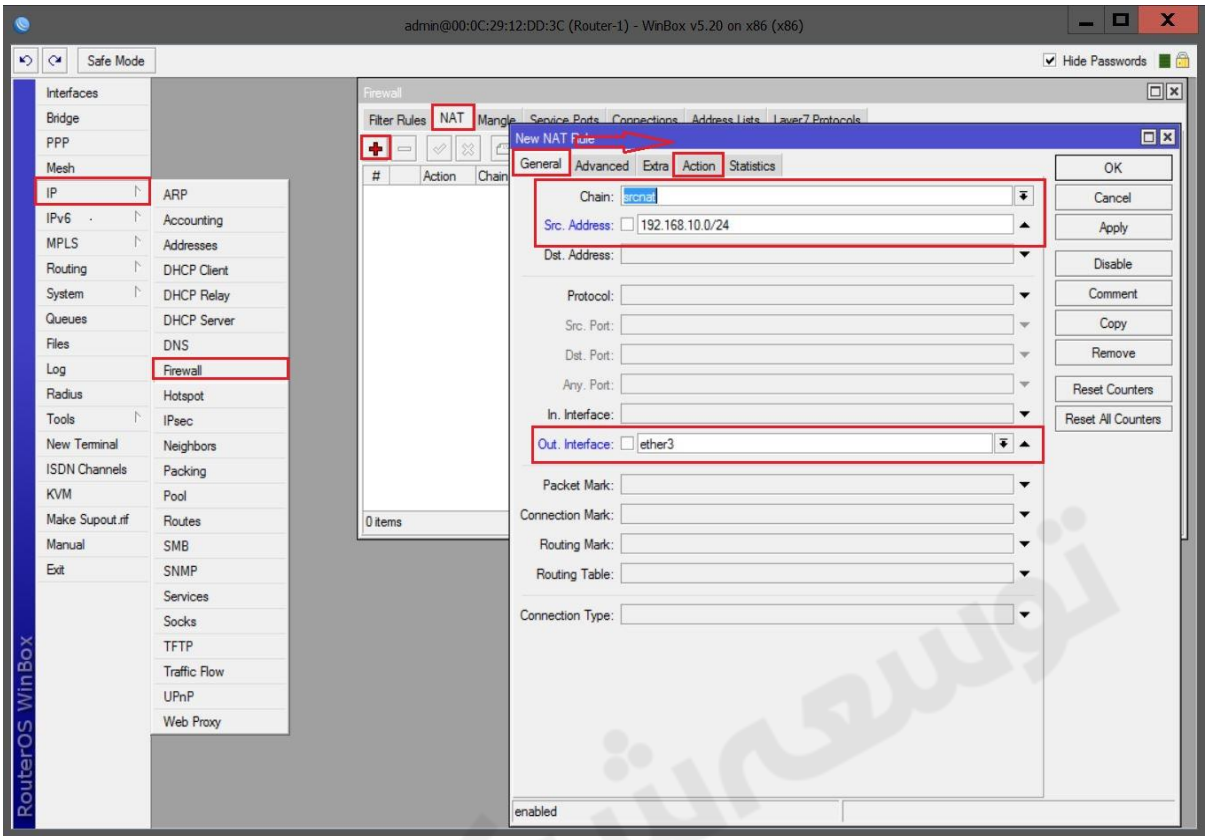


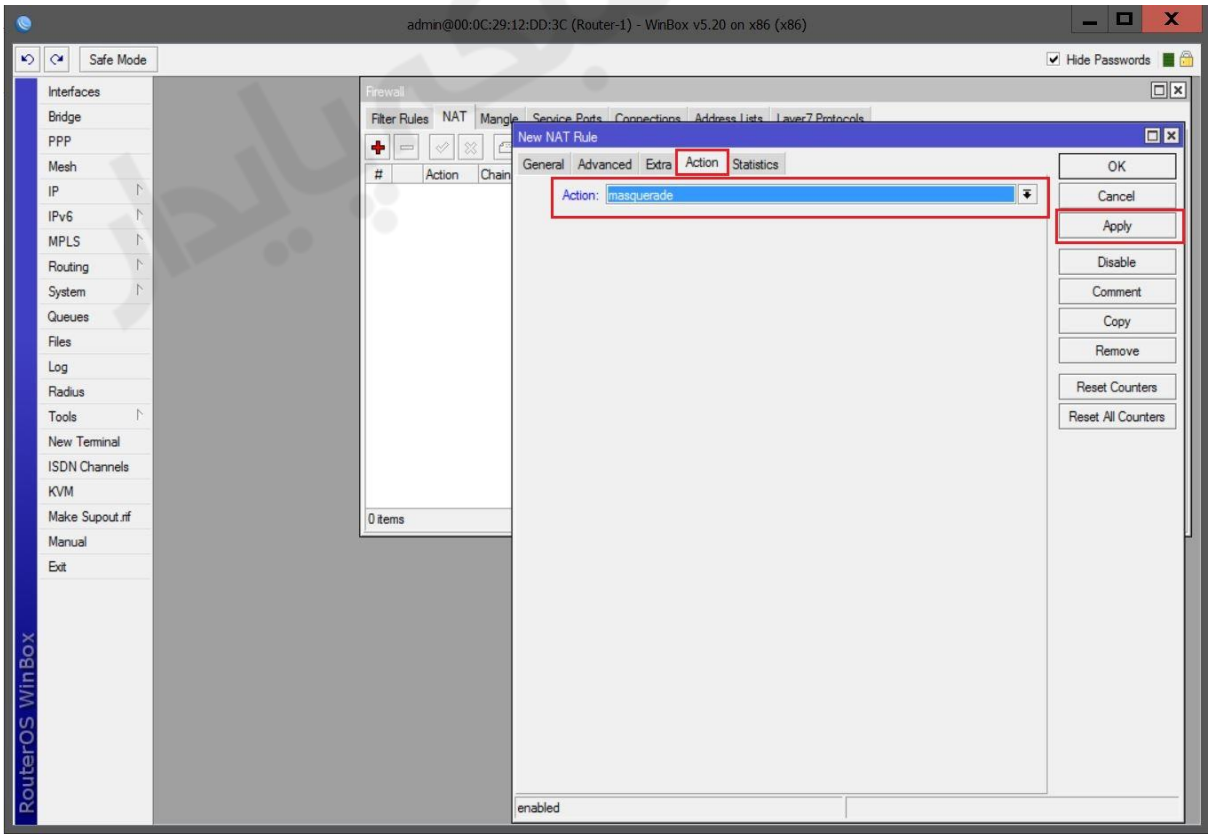
به این ترتیب با این تظیمات درخواست های **DNS** ای بر روی پورت **DNS** میکروتیک **Redirect** می شود.حال اگر کاربر به هر علتی در تنظیمات **DNS** سیستم خود هر آدرسی را وارد کند حتی اگر آدرس وارد شده اشتباه بود یا یک **IP** آدرس نامتعارف بود ، چون تمامی درخواست های **DNS** ای بر روی پورت **DNS** میکروتیک ارسال می شوند ، پروسه **Resolve** درخواست ها با موفقیت انجام می پذیرند.

تنظیمات کلاینت :



ایجاد NAT برای دسترسی کلاینت به اینترنت :





با این تنظیمات کلاینت به اینترنت نیز دسترسی پیدا خواهد کرد.

فصل نهم : Web Proxy

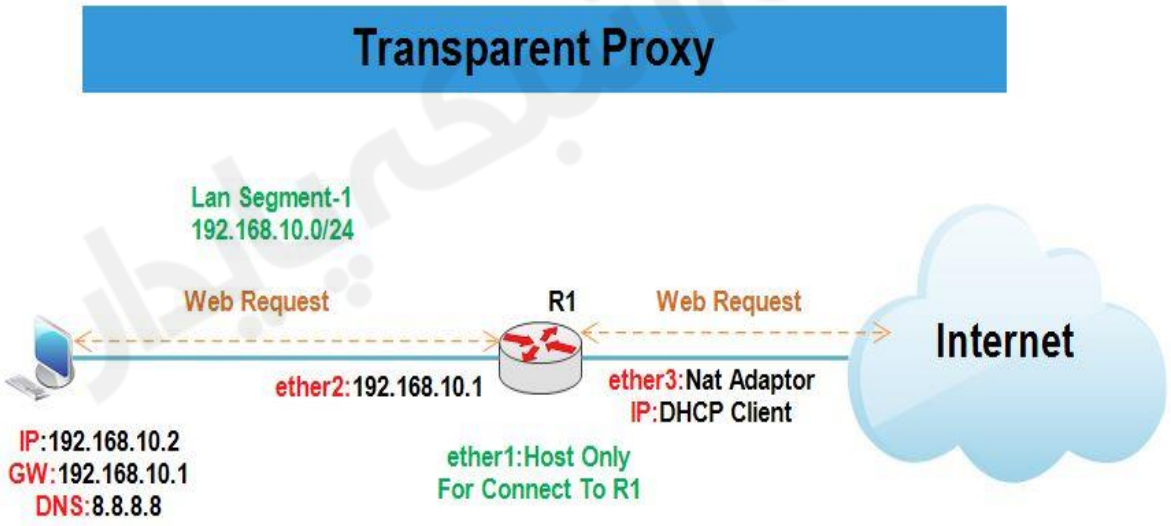
پروکسی سرور کامپیوتر یا روتری است که بین یک مرورگر و اینترنت قرار می گیرد. پروکسی سرورها به بهبود عملکرد صفحات وب در یک سازمان یا شرکت کمک می کند بطوری که با ذخیره یا کش کردن صفحات وب ، دسترسی به آنها سریع تر خواهد بود. همچنین از پروکسی سرور می توان برای فیلتر کردن برخی صفحات وب و یا جلوگیری از دانلود برخی پسوندهای خاص استفاده نمود. بطور کلی از پروکسی سرور جهت میریت صفحات وب استفاده می شود.

عملکرد وب پروکسی بدین شکل است وقتی کلاینت درخواست دسترسی به صفحات وب را به سمت روتر ارسال می کند روتر یک نسخه از آن را در کش خود ذخیره کرده و برای پاسخگویی به درخواست های مشابه بعدی نسخه کپی شده را برای کلاینت ها ارسال می کند.

قابلیت های پروکسی در میکروتیک :

- **Proxy** معمولی : در این حالت بر روی مرورگر تنظیمات پروکسی اعمال می شود.
- **Transparent Proxy** : در این حالت تنظیمات فقط بر روی روتر اعمال می شود و کلاینت متوجه هیچگونه تغییری در مرورگر خود احساس نخواهد کرد.
- **Access** : می توان صفحات وب را براساس آدرس مبدا یا مقصد ، **URL** ، پسوند فایل و ... فیلتر کرد.
- **Cache** : صفحات وب در حافظه روتر ذخیره می شود.

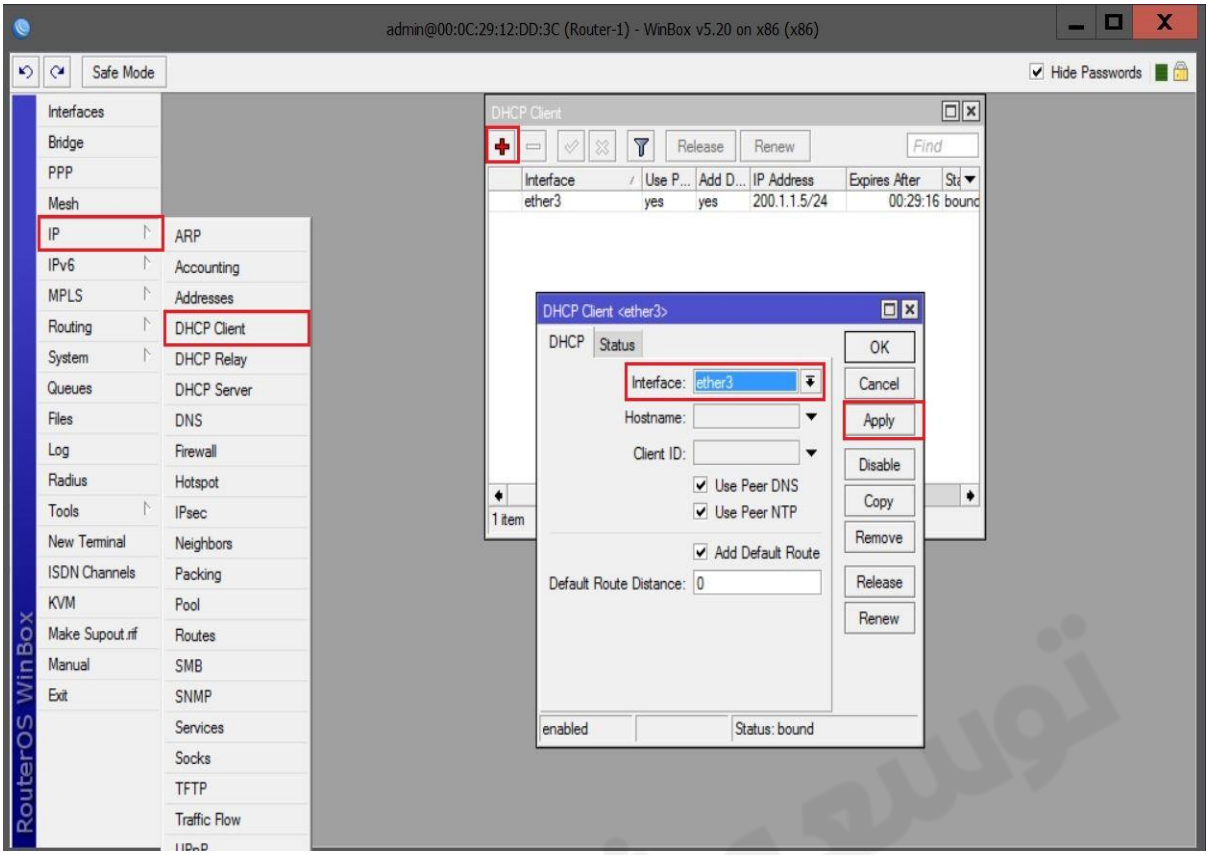
سناریو ۱ : راه اندازی Transparent Proxy

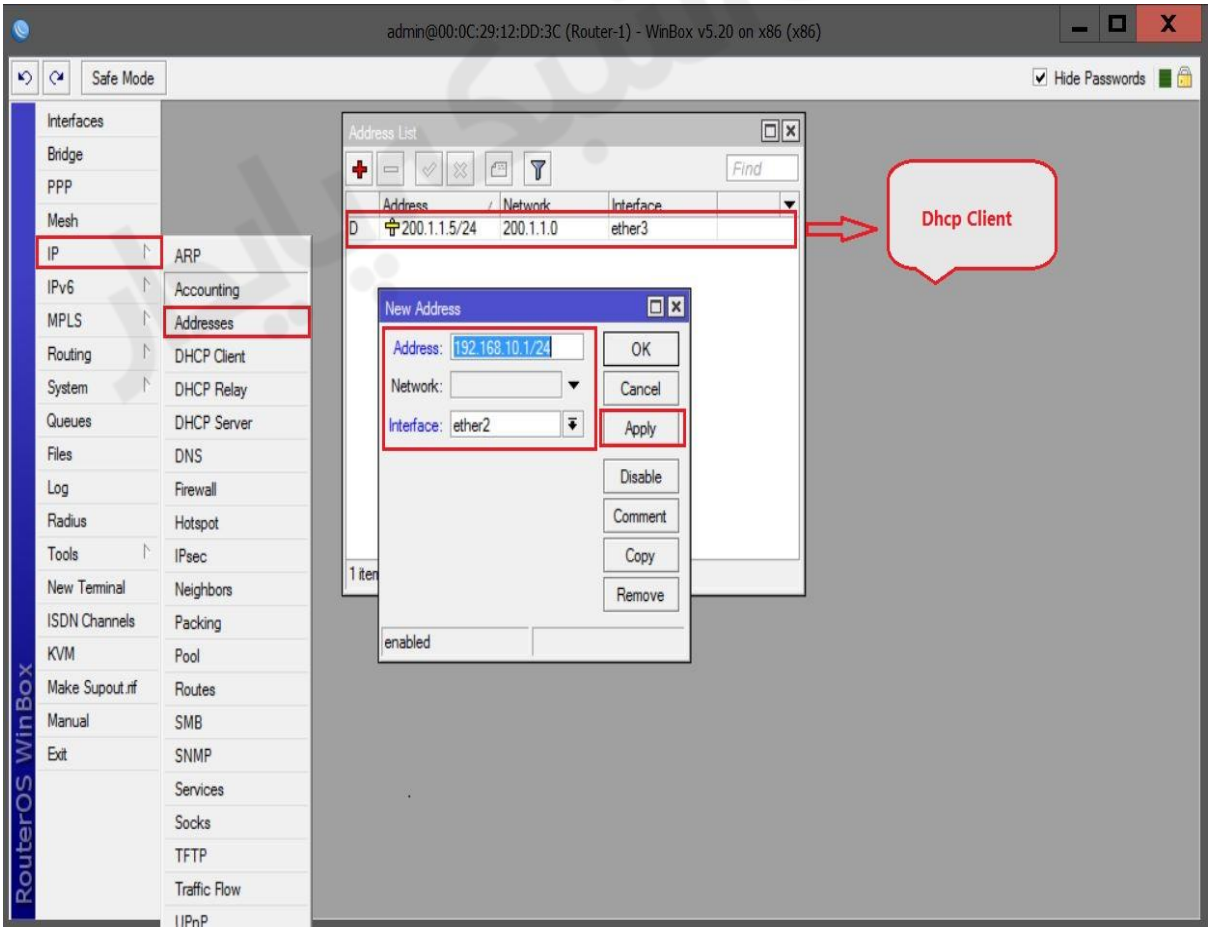


*نکته : قبل از راه اندازی وب پروکسی باید از طریق روتر کاربران را به اینترنت متصل کنید یا به عبارتی دسترسی آنها به اینترنت باید از طریق روتر صورت گیرد.

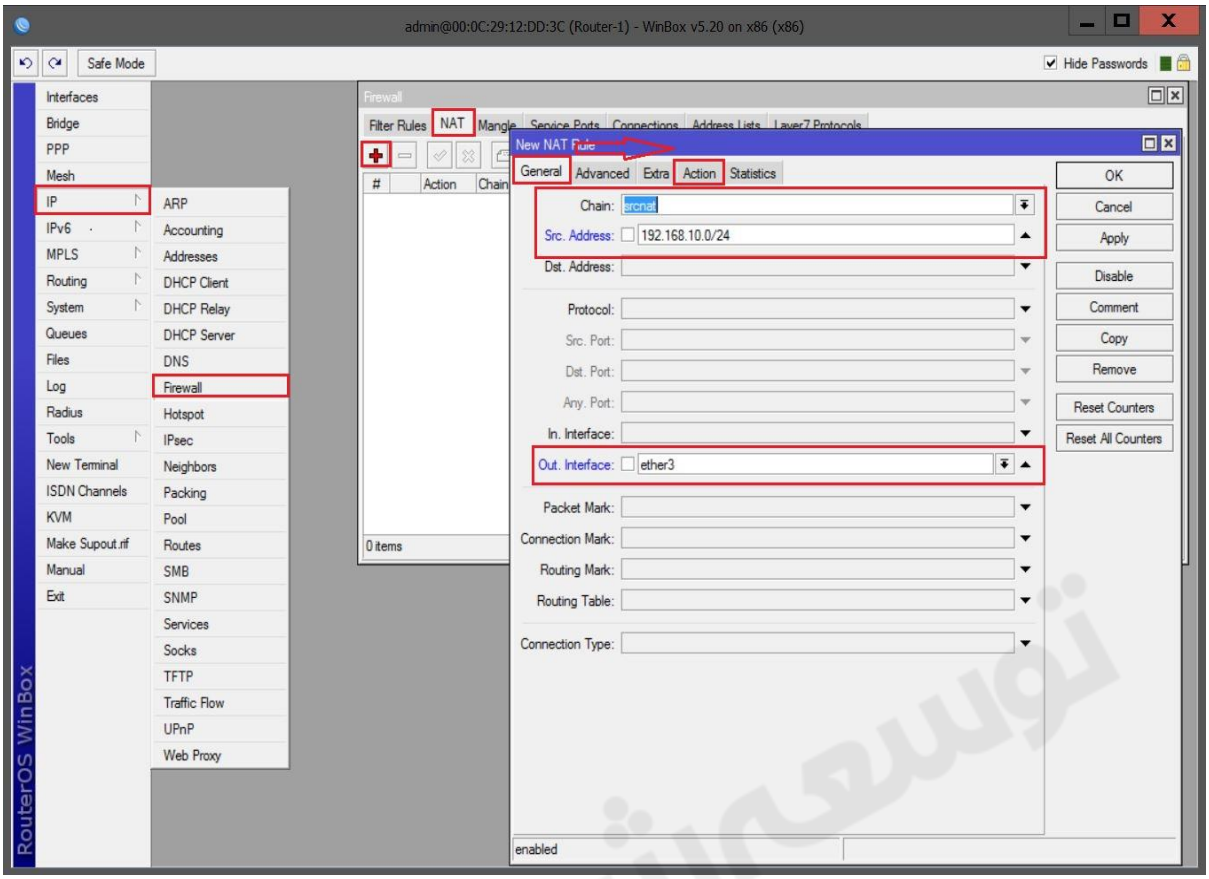
انتساب **IP** به کارت های شبکه روتر **R1** :

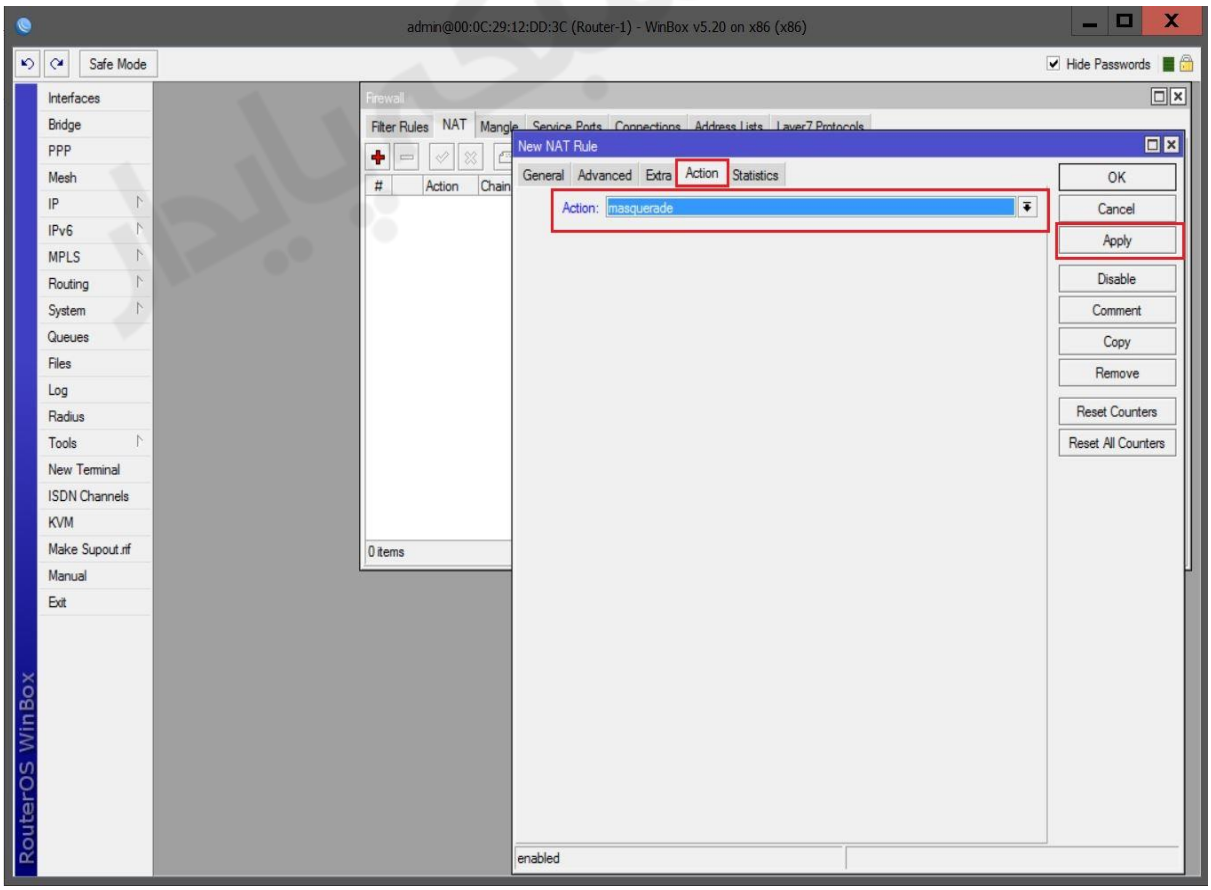
همان طور که در سناریو مشخص کردیم **Ether3** باید از **Dhcp Client** (**Vmware**) آدرس**IP** دریافت کند.برای این کار از منوی اصلی گزینه **IP** و از زیر منوی باز شده **Dhcp Client** را انتخاب میکنیم.در پنجره باز شده بر روی **Add** کلیک و از تب **Dhcp** اینترفیس مورد نظر را انتخاب و **ok** را میزنیم.


admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
RouterOS WinBox
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Socks
TFTP
Traffic Flow
DHCP Client
Release
Renew
Find
Interface
Use P...
Add D...
IP Address
Expires After
ether3
yes
yes
200.1.1.5/24
00:29:16
1 item
DHCP Client <ether3>
DHCP
Status
Interface: ether3
Hostname:
Client ID:
Use Peer DNS
Use Peer NTP
Add Default Route
Default Route Distance: 0
OK
Cancel
Apply
Disable
Copy
Remove
Release
Renew
enabled
Status: bound

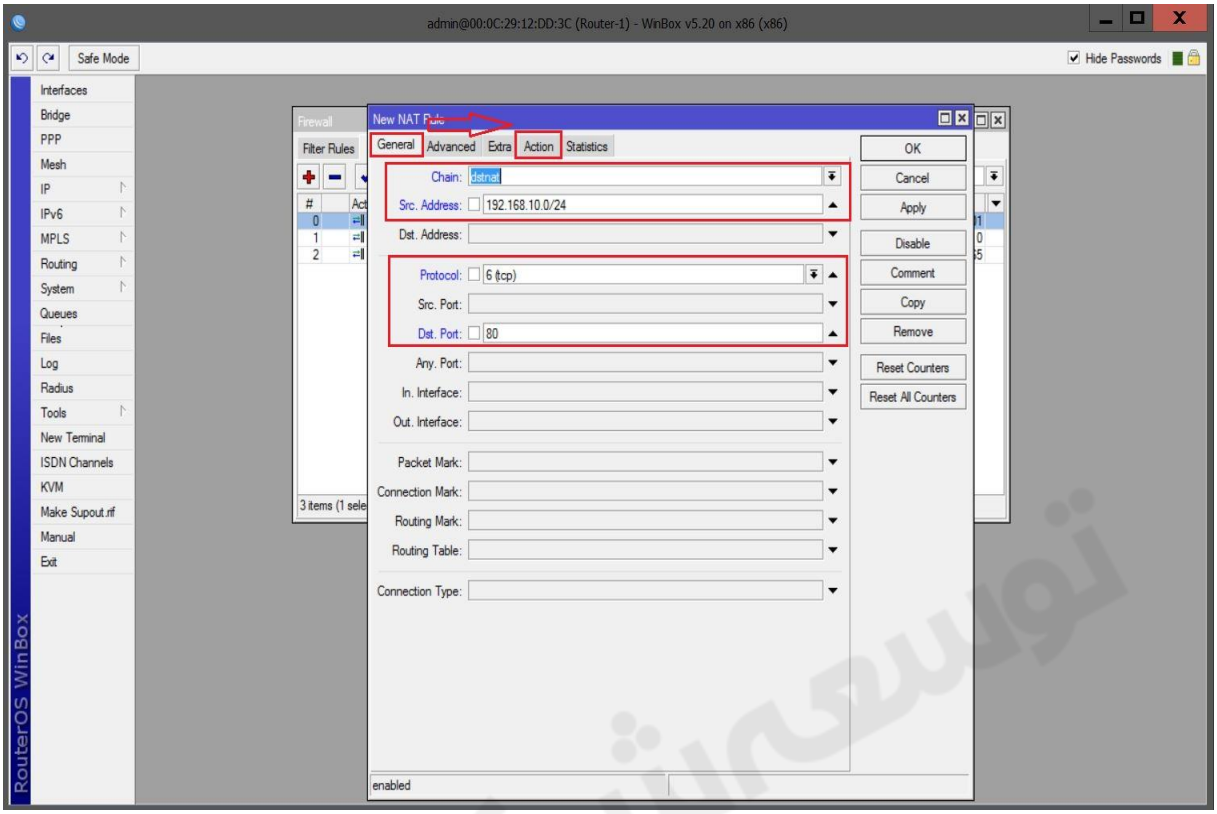

admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
RouterOS WinBox
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Socks
TFTP
Traffic Flow
Address List
Find
Address
Network
Interface
D
200.1.1.5/24
200.1.1.0
ether3
Dhcp Client
New Address
Address: 192.168.10.1/24
Network:
Interface: ether2
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled

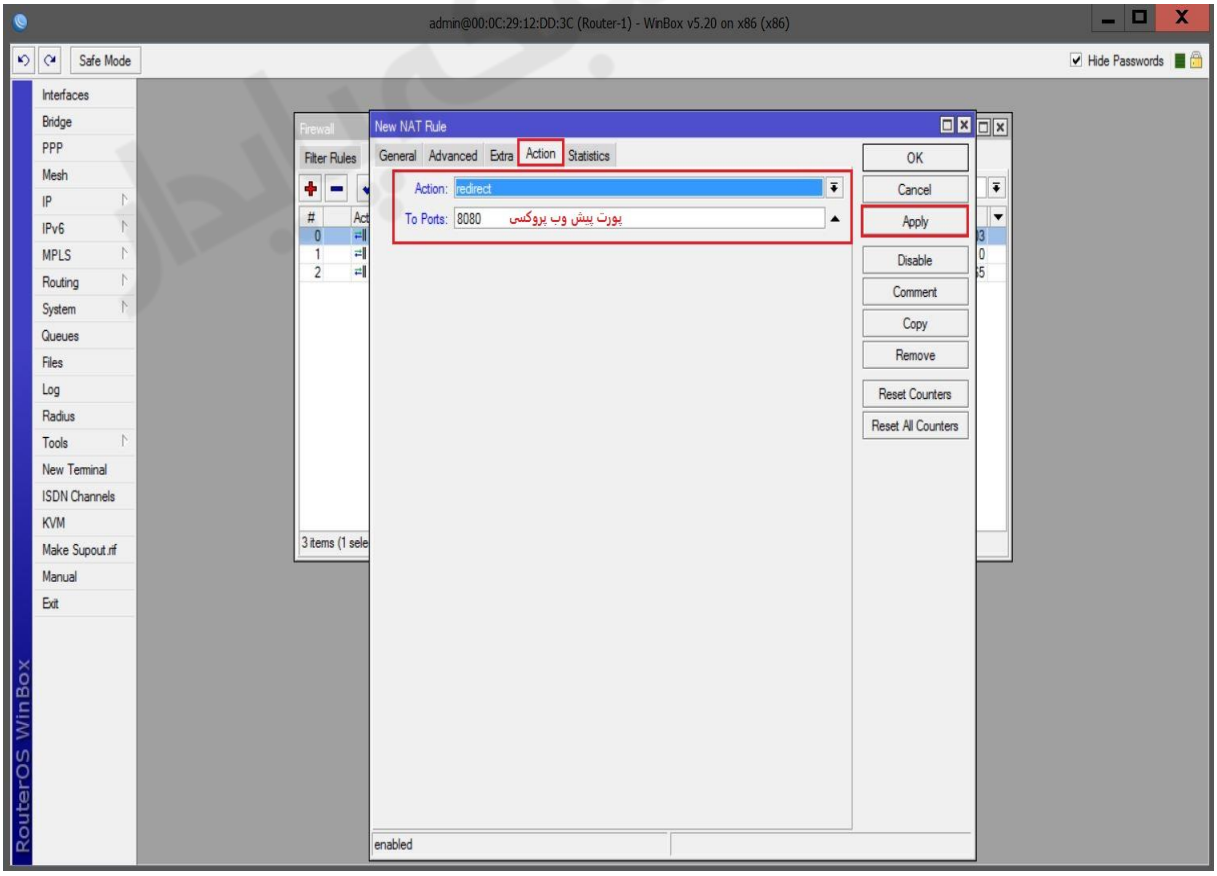
ایجاد NAT برای دسترسی کلاینت به اینترنت :





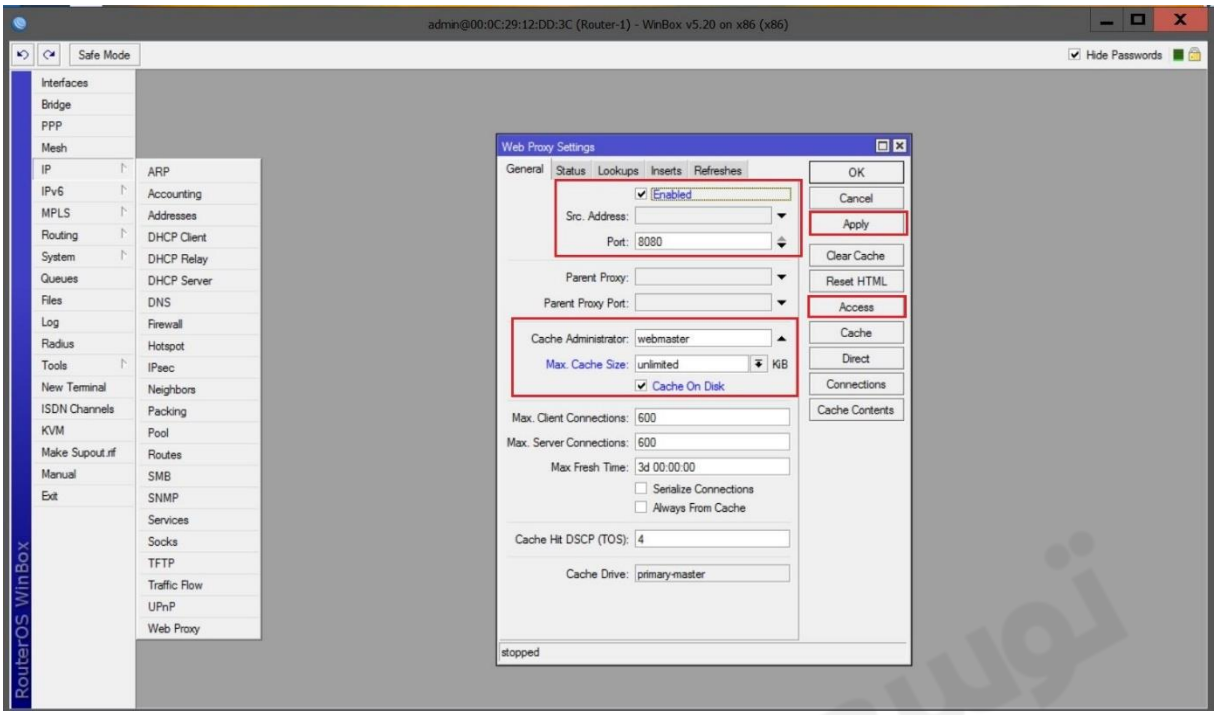
تا اینجای کار کلاینت ها مستقیم به اینترنت دسترسی دارند. برای اینکه از وب پروکسی به عنوان واسط بین کلاینت و اینترنت استفاده شود و بتوانیم از قابلیت های وب پروکسی استفاده کنیم باید یک **Nat** ایجاد کنیم تا کلاینت هایی که مقصد آنها اینترنت است به وب پروکسی **Redirect** شوند.





فعال کردن Web Proxy :

برای فعال کردن قابلیت Web Proxy از منوی اصلی گزینه IP و از زیرمنوی باز شده Web Proxy را انتخاب می کنیم.

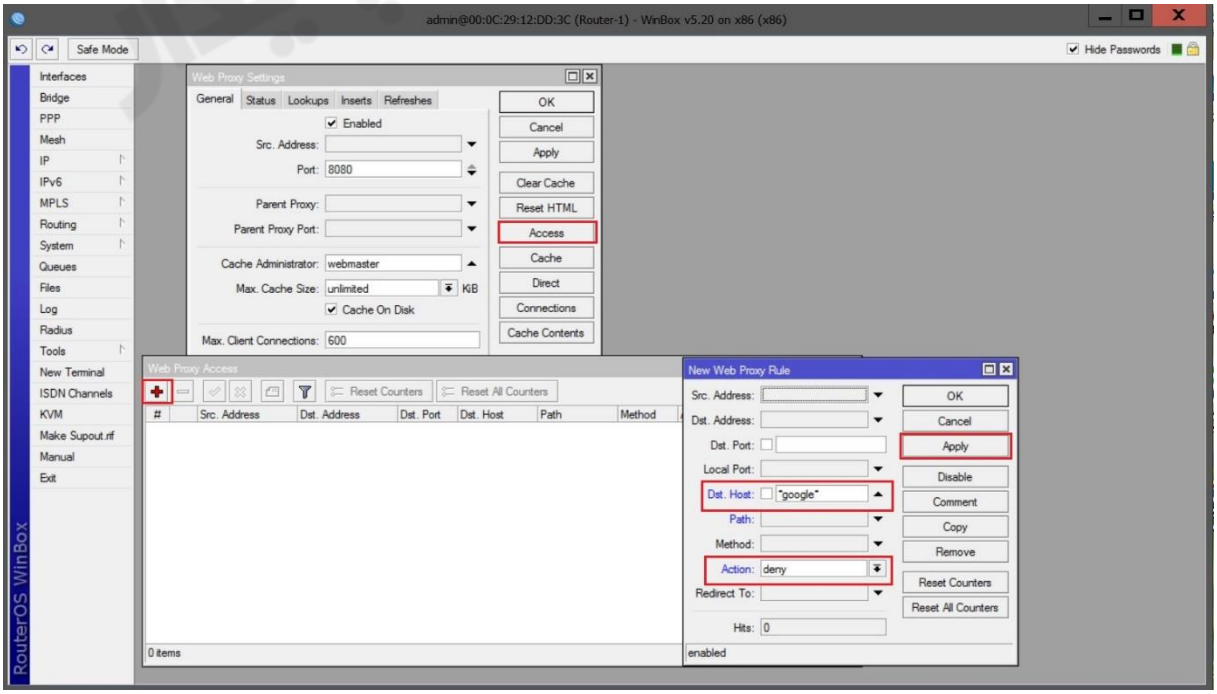


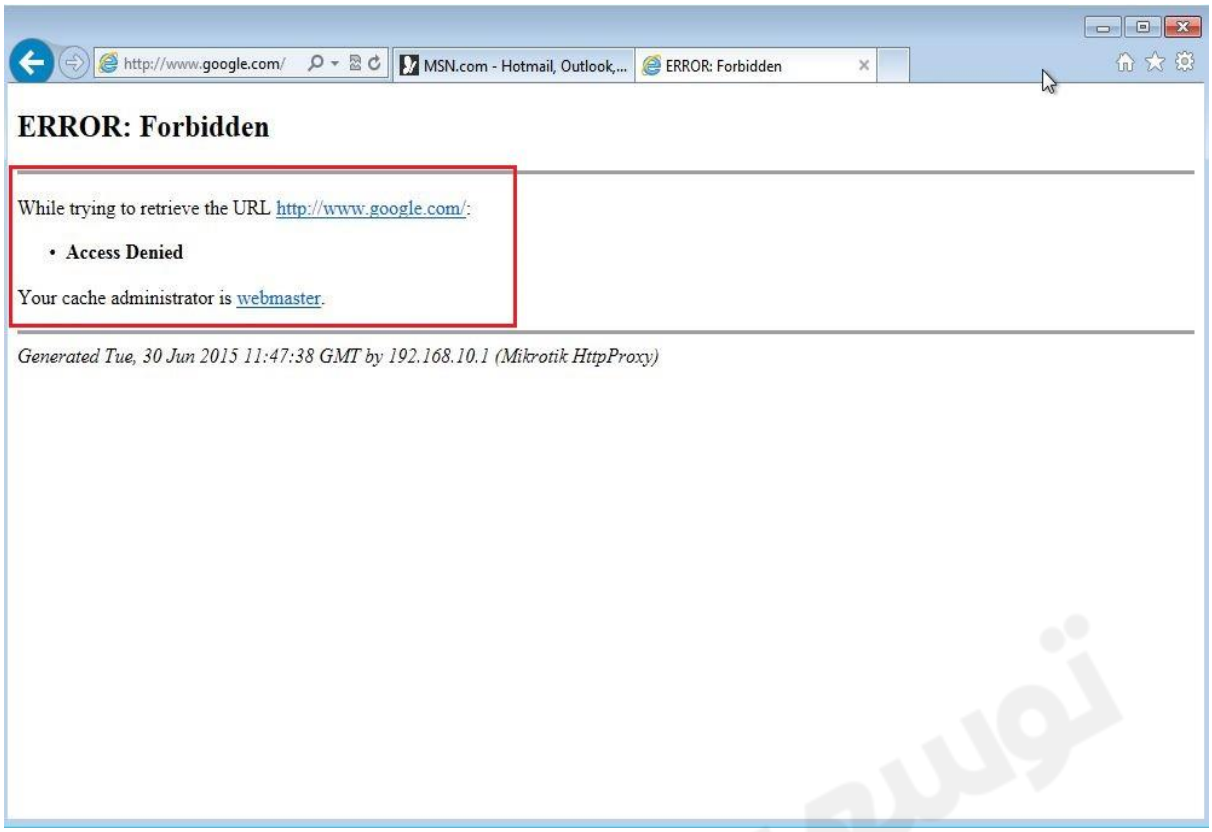
در پنجره Web Proxy Setting تیک Enable را فعال می کنیم و سپس در قسمت سرور آدرسی که می خواهیم پروکسی بر روی آن اعمال شود را وارد می کنیم در صورت خالی گذاشتن این فیلد پروکسی بر روی هر درخواستی اعمال می شود و یا می تواند آدرس یکی از پورت های روتر باشد در این حالت وب پروکسی فقط برروی همان پورت اعمال می شود. در فیلد Port شماره پورت دلخواه Web Proxy را وارد می کنیم.این شماره پورت بصورت پیش فرض 8080 می باشد. اگر می خواهیم سایتهایی که مدنظرمان هست را کش کنیم گزینه Cache On Disk را فعال می کنیم.

فیلترینگ از طریق Web Proxy :

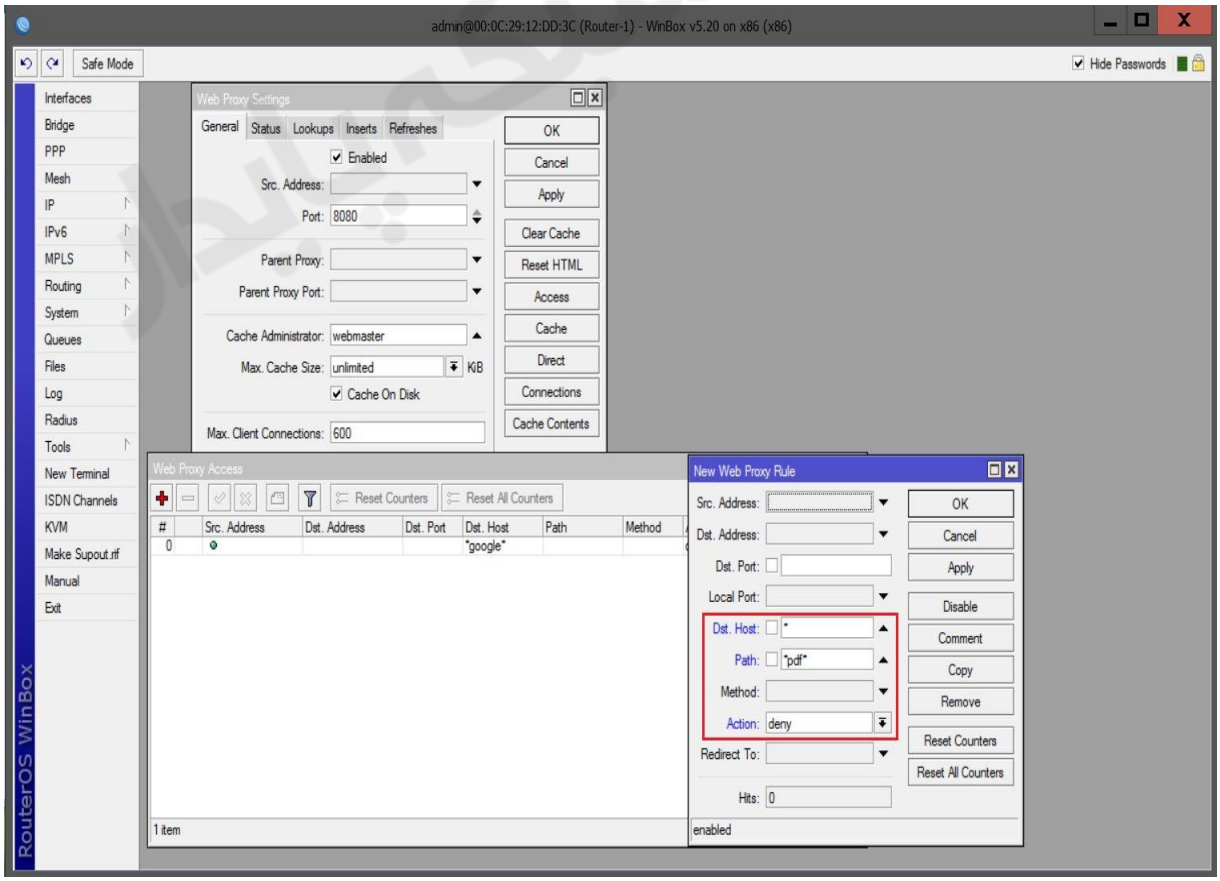
از پنجره Web Proxy Setting گزینه Access را انتخاب می کنیم.

مثال ۱)سایت Google برای هیچ کلاینتی باز نشود؟

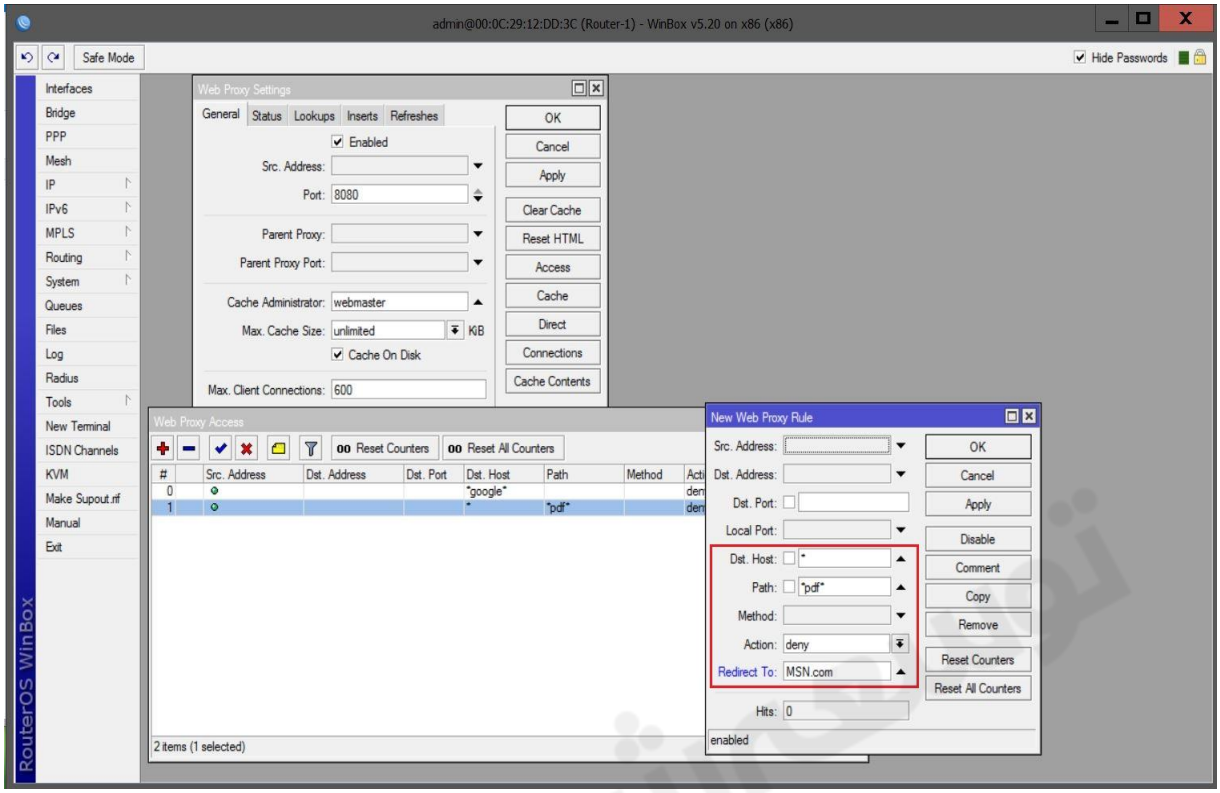




مثال ۲)کلاینت نتواند فایل های Pdf دانلود کند؟



مثال ۳)کلاینت نتواند فایل های Pdf را دانلود کند و بعد از کلیک بر روی لینک دانلود به یک سایت دیگر (مثلا MSN.com) Redirect شود ؟



فصل دهم : Queue – Traffic Shaping

در میکروتیک برای مدیریت پهنای باند و محدود کردن سرعت دسترسی کاربران می توان از ویژگی های **Queue** استفاده کرد.**Queue**ها به دو صورت ساده (**Simple Queue**) و درختی (**Queue Tree**) قابل پیاده سازی می باشند.توجه داشته باشید که با استفاده از **Queue**ها فقط می توان سرعت آپلود و دانلود کاربران را محدود کرد و در صورتی که بخواهیم بر روی حجم کاربران محدودیت اعمال نمایید لازم است از **User Manage** استفاده کنید(در فصل های بعد این امکان را آموزش خواهیم داد).

پارامترهای مورد استفاده در **Queue** :

۱) **Name** : یک نام بدلخواه انتخاب می کنیم.

۲) **Target** : در این قسمت باید آدرس **IP** یا محدوده ایی از آدرس **IP** را تعیین کنید این آدرس قرار است با محدودیت در پهنای باند مواجه شوند(آدرس **IP** کامپیوتر مورد نظر)

۳) **Target Upload** : حداکثر میزان مجاز آپلود

۴) **Target Downlad** : حداکثر میزان مجاز دانلود

*نکته : توجه داشته باشید که تعیین میزان آپلود یا دانلود بستگی به میزان پهنای باندی دارد که از **ISP** دریافت کرده اید. در صورتی که سرعت **dedicate** داشته باشید مطمئنا تقسیم آن راحت خواهد بود.

۵) **Max Limit** : ماکزیمم پهنای باند که روتر قرار است رد کند

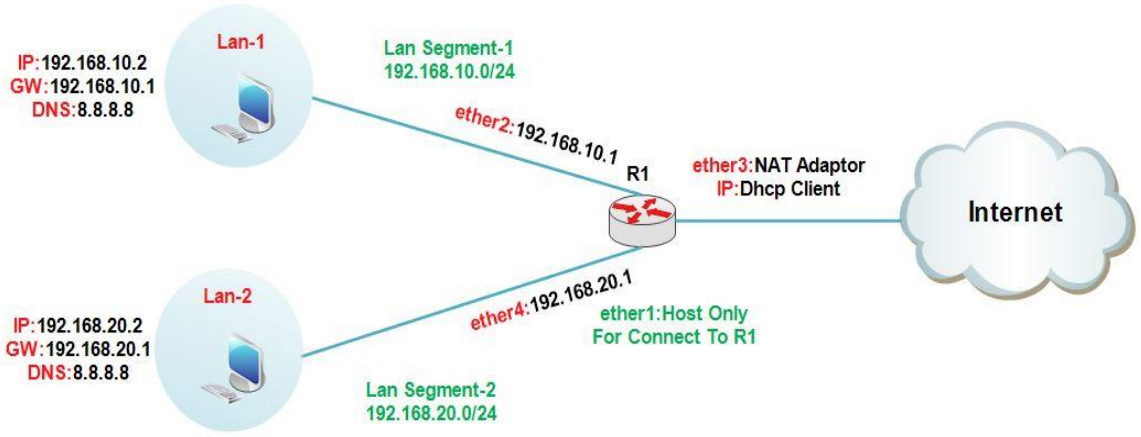
۶) **Time** : در قسمت **Time** می توانید ساعاتی از شبانه روز و روزهایی از هفته را که می خواهید محدودیت پهنای باند اعمال شود را تنظیم نمایید.

*نکته : برای این کار باید دو الگو بنویسید.در اولین الگو که بهتر است بالاتر باشد ، پهنای باندی که قرار است در روز و ساعات بیشتری اعمال شود را قرار دهید و در دومین الگو که خواهید نوشت می توانید زمان و ساعت را در زمانی که الگوی اول قرار ندارد را تعیین کنید.

۷) **Priority** : اولویت عدد بین ۱ الی ۸ می باشد.عدد کوچکتر اولویت بالاتر

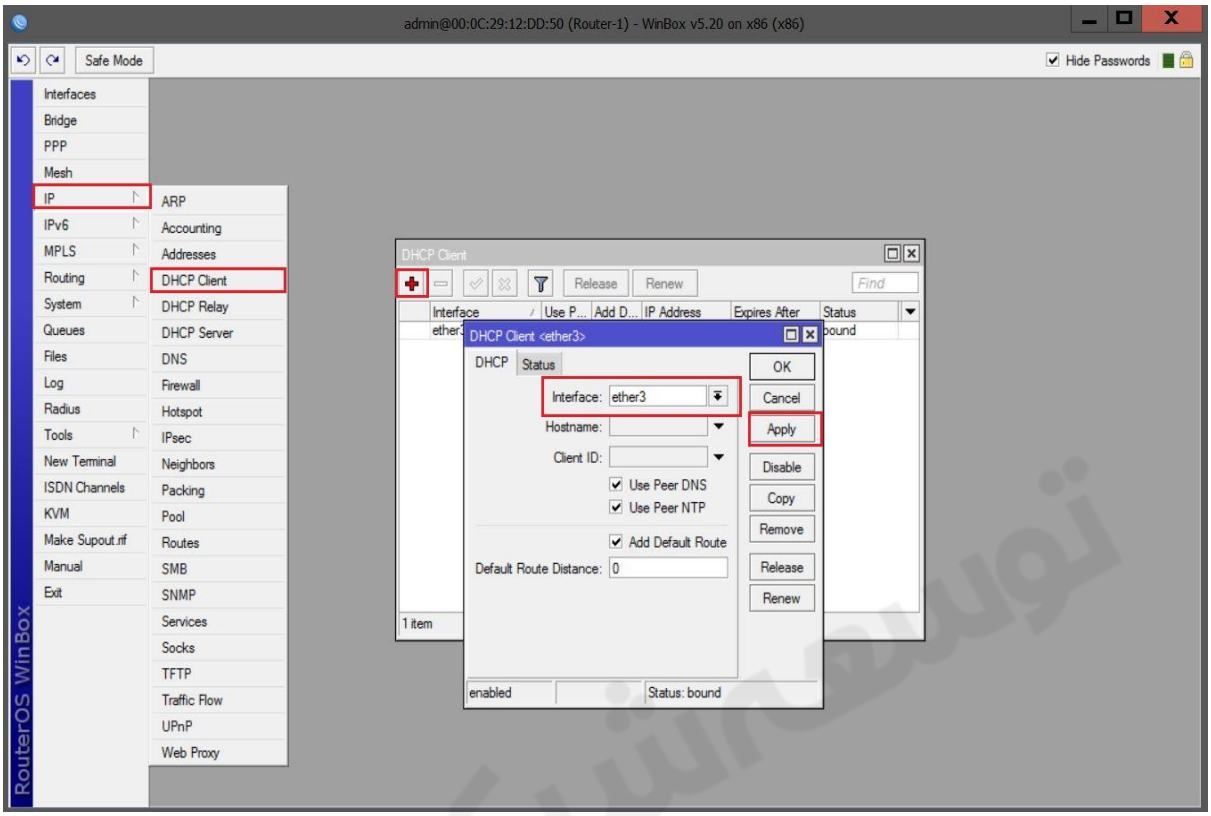
۸) **Limit At** : مقدار پهنای باند گارانتی شده ، یعنی مقداری که تحت هر شرایطی باید رد شود.

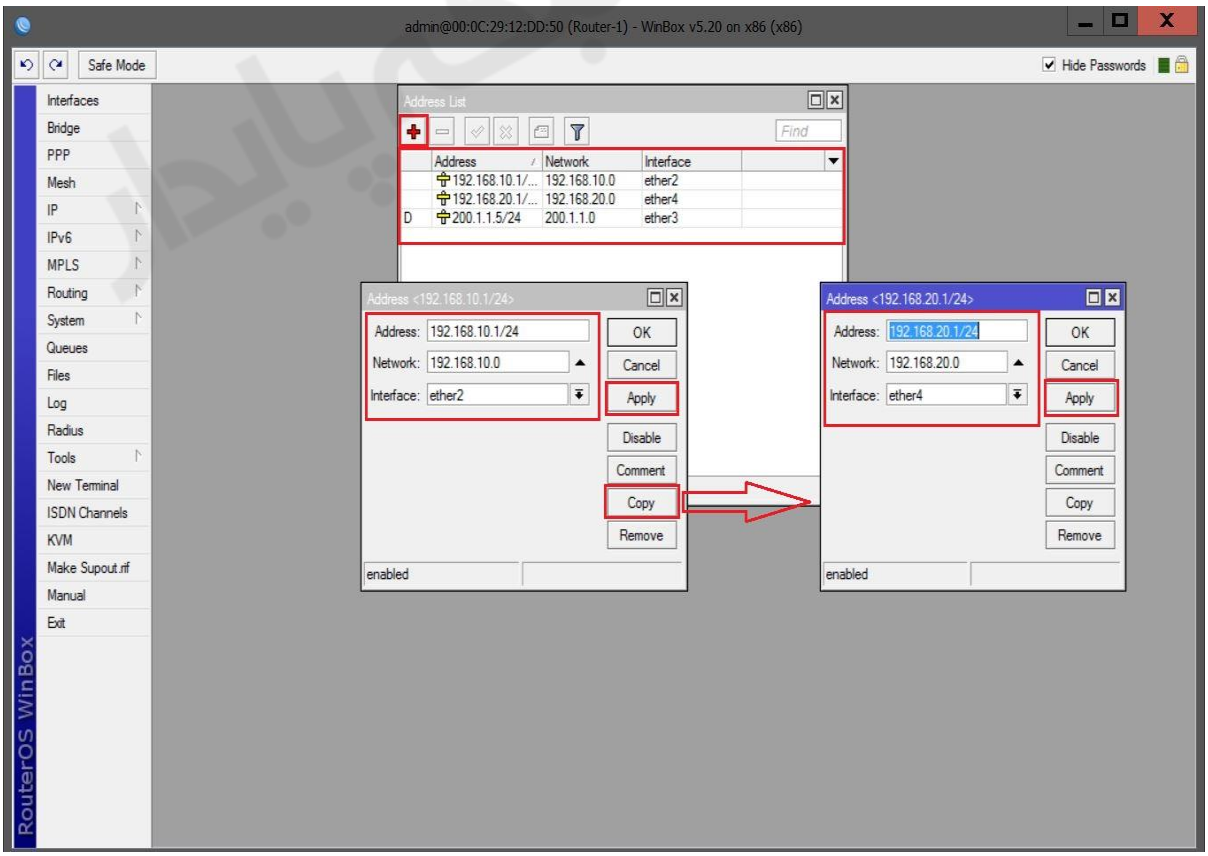
سناریو ۱ : بررسی قابلیت های **Queue** و ایجاد محدودیت پهنای باند برای کاربران



در این سناریو می خواهیم دسترسی کاربران Lan-1 و Lan-2 به اینترنت را محدود کنیم بصورتی که کاربران Lan-1 پهنای باند 128K و کاربران Land-2 پهنای باند 256K داشته باشند.

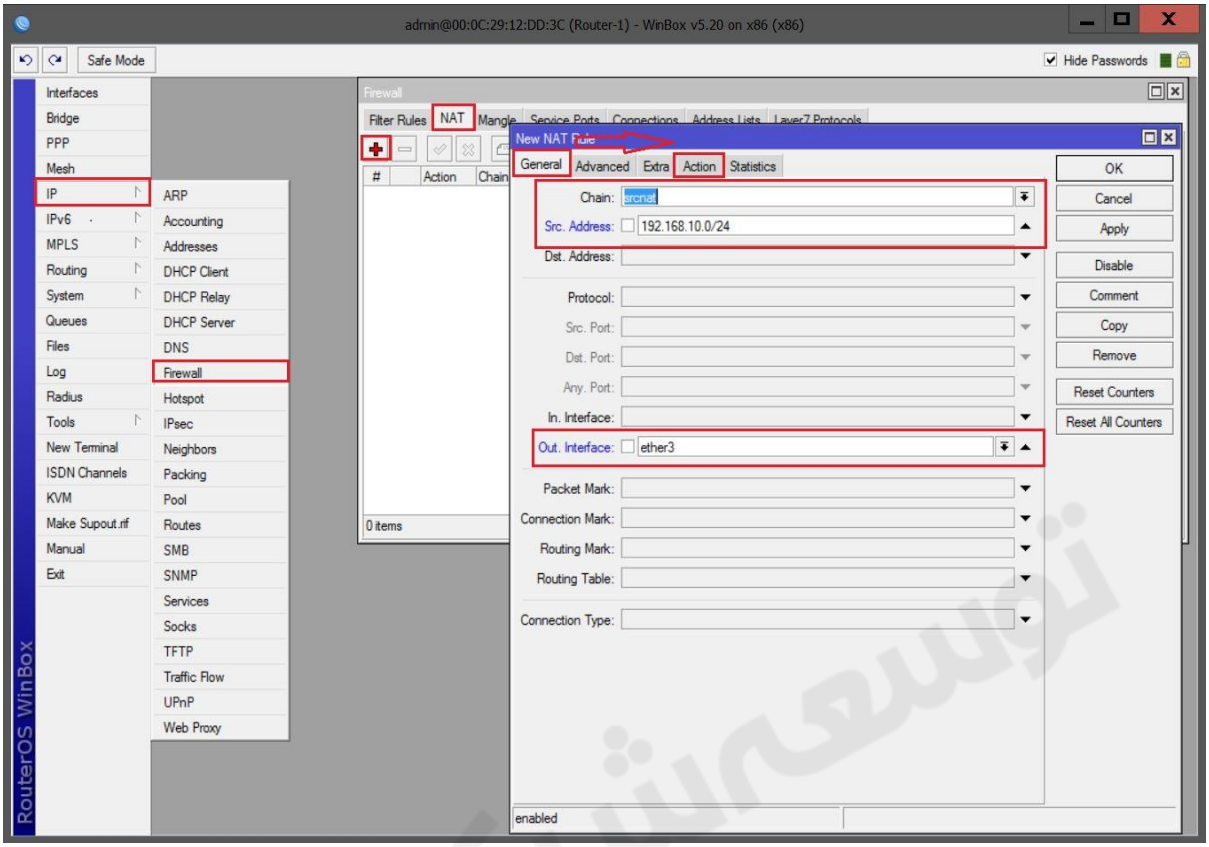
انتساب IP به کارت شبکه های روتر :

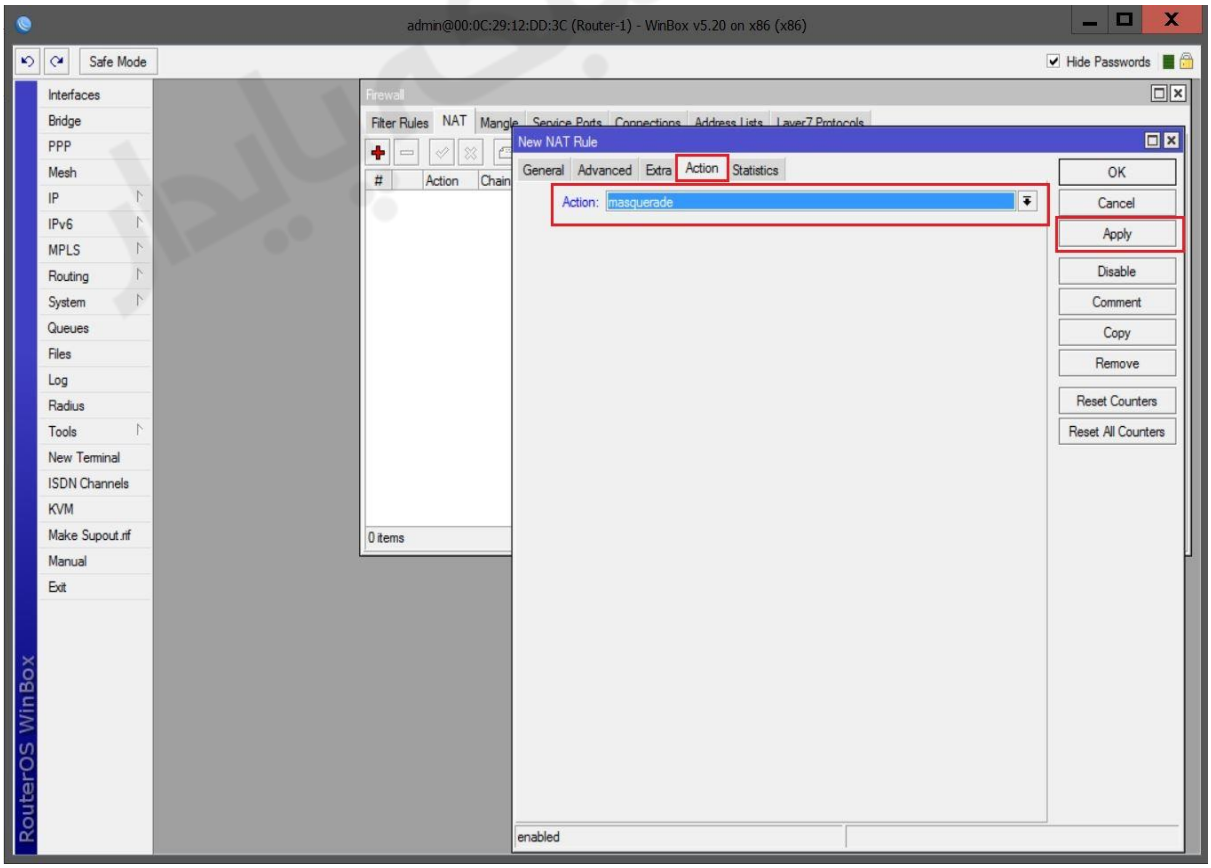




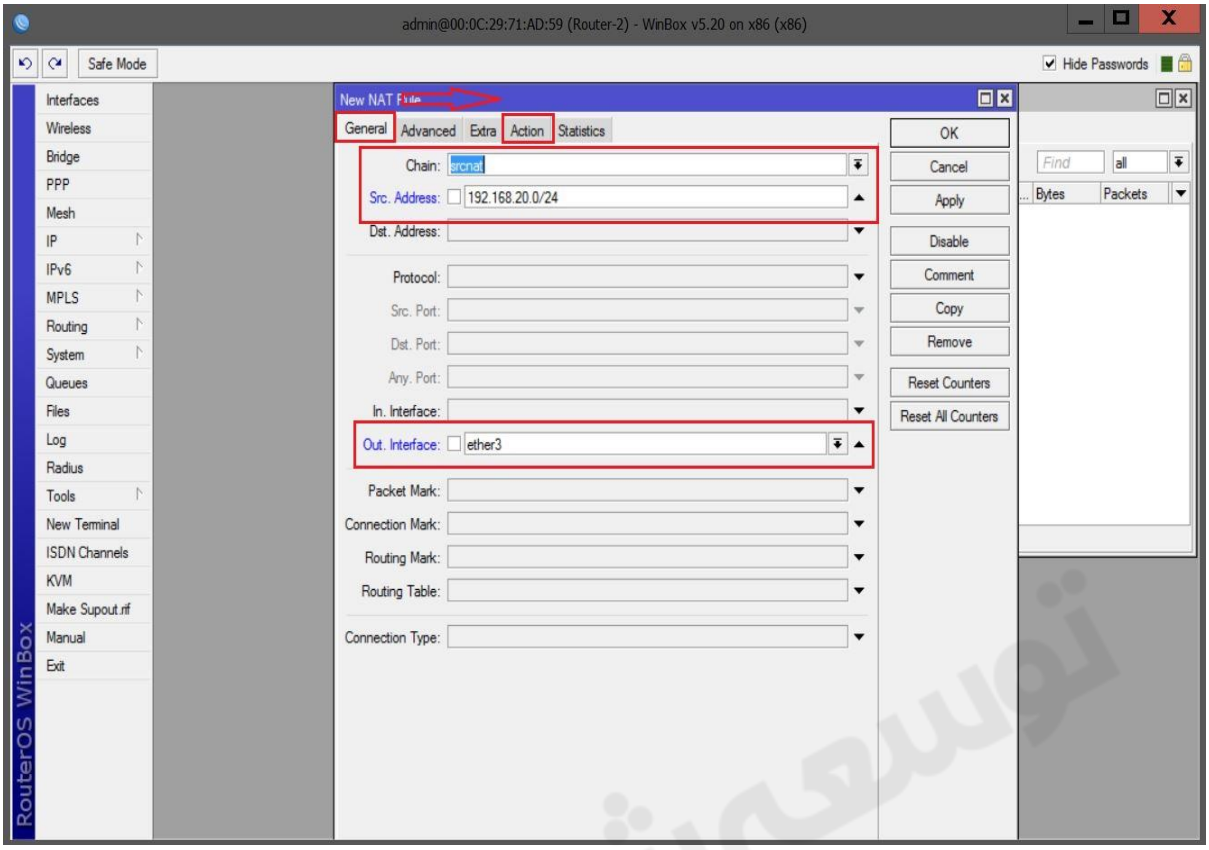
ایجاد Nat برای دسترسی کلاینت ها به اینترنت :

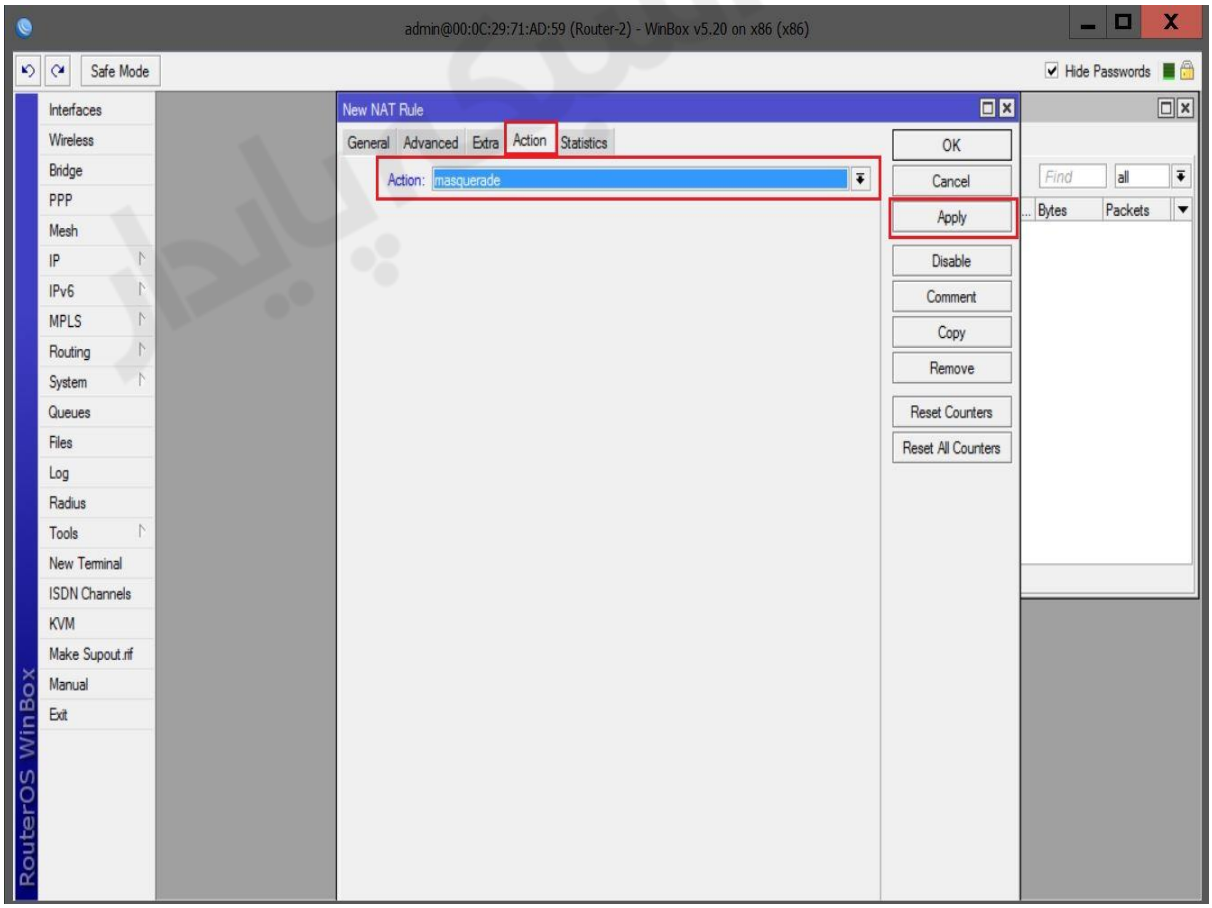
Lan-1 :





: **Lan-2**

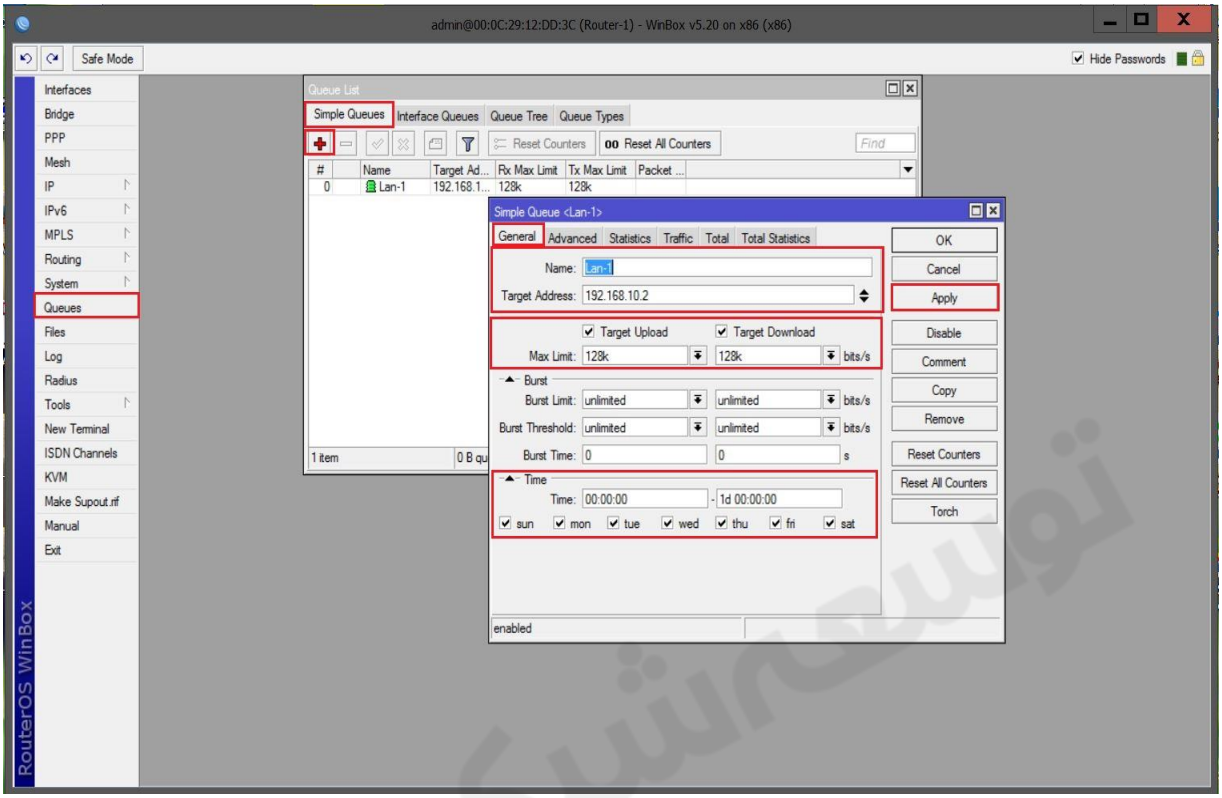

admin@00:0C:29:71:AD:59 (Router-2) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
RouterOS WinBox
New NAT Rule
General
Advanced
Extra
Action
Statistics
Chain: srcnat
Src. Address: 192.168.20.0/24
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface: ether3
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Find
all
Bytes
Packets


admin@00:0C:29:71:AD:59 (Router-2) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
RouterOS WinBox
New NAT Rule
General
Advanced
Extra
Action
Statistics
Action: masquerade
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Find
all
Bytes
Packets

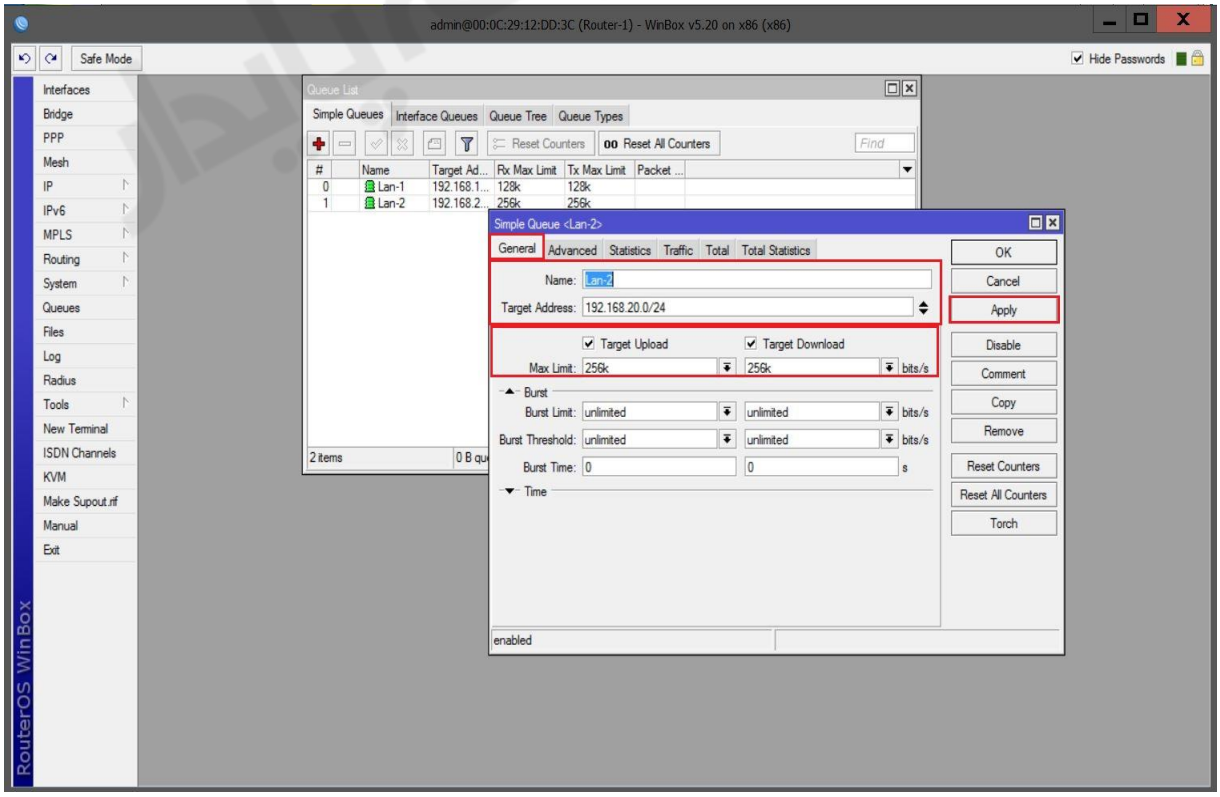
ایجاد محدودیت پهنای باند برای دسترسی کلاینت ها به اینترنت :

برای این کار از منوی اصلی Queues را انتخاب کرده و از پنجره ی باز شده از بخش Simple Queues برروی Add کلیک می کنیم و تنظیمات را اعمال می کنیم.

شبکه Lan-1 :

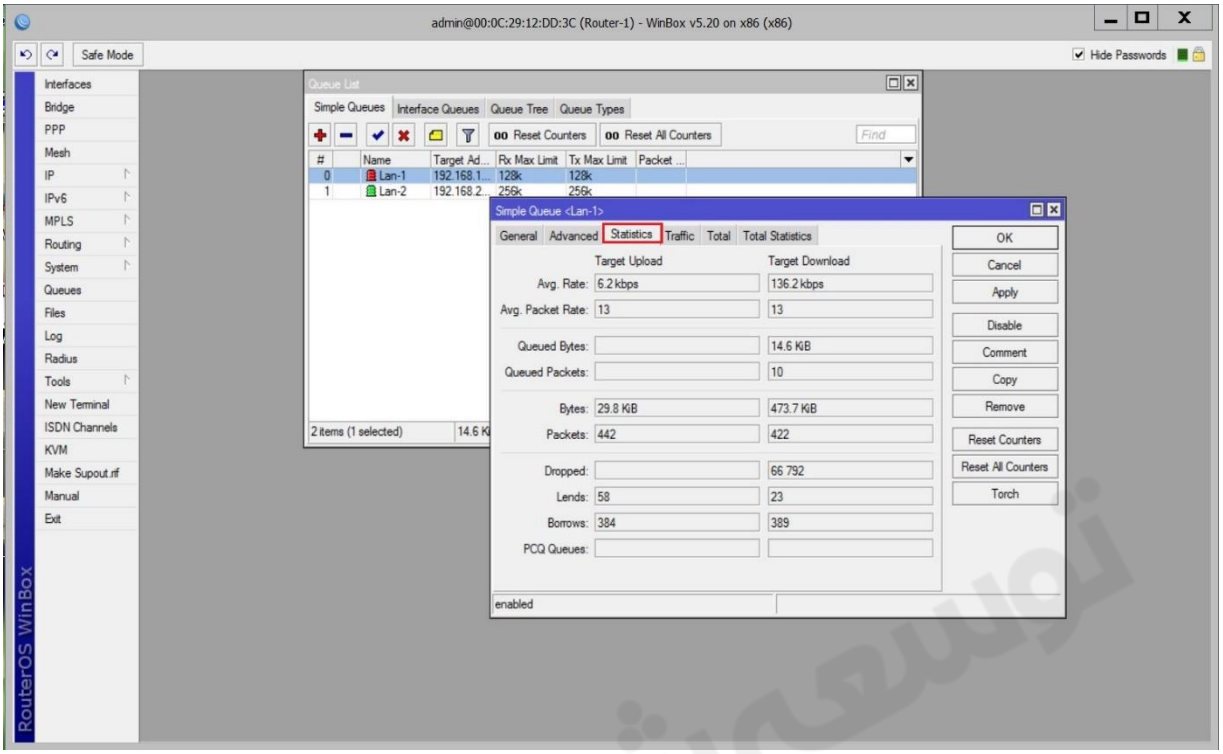


شبکه Lan-2 :



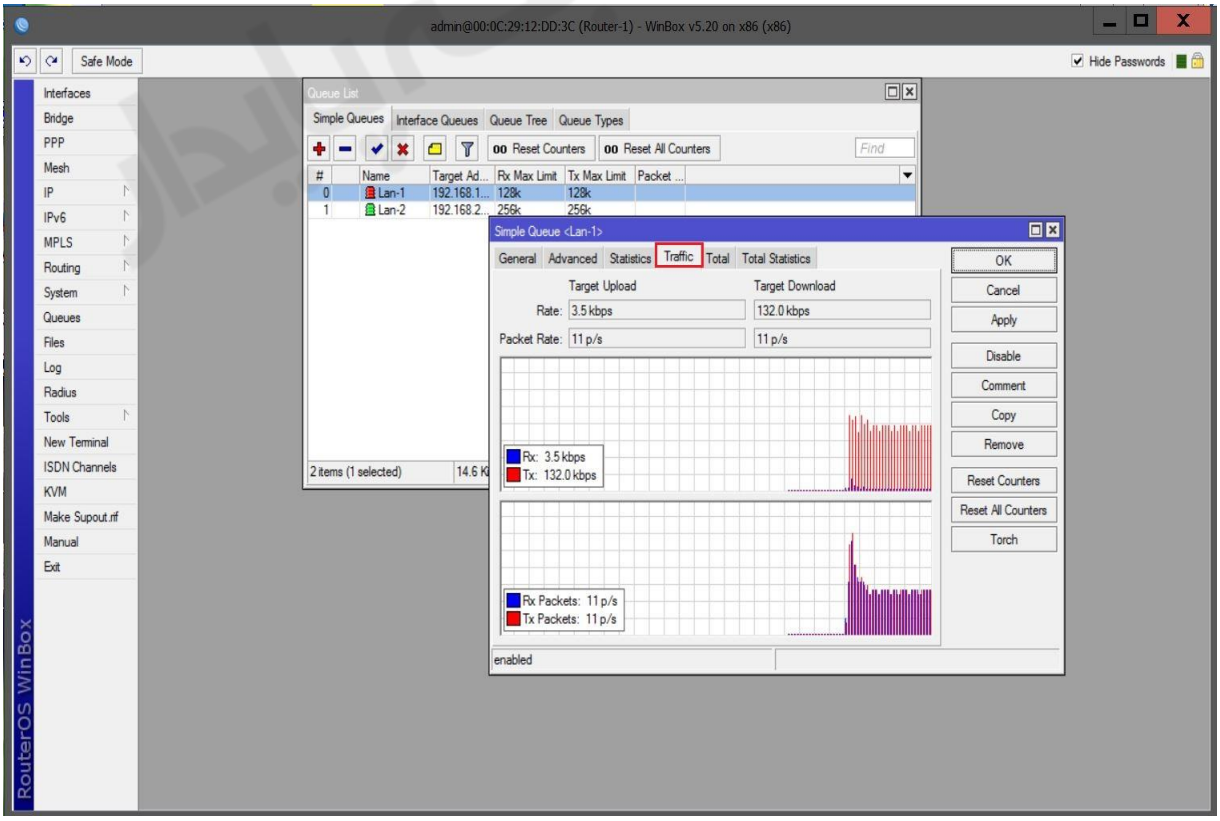
بررسی میزان مصرف پهنای باند :

برای مشاهده ی مصرف هر کاربر پس از کلیک بر روی نام Queue آن، به بخش Statistics میزان مصرف IP یا IP های مورد نظر و پارامترهایی از قبیل میزان ارسال Packet و ضریب ارسال و دریافت دیتا قابل مشاهده است.

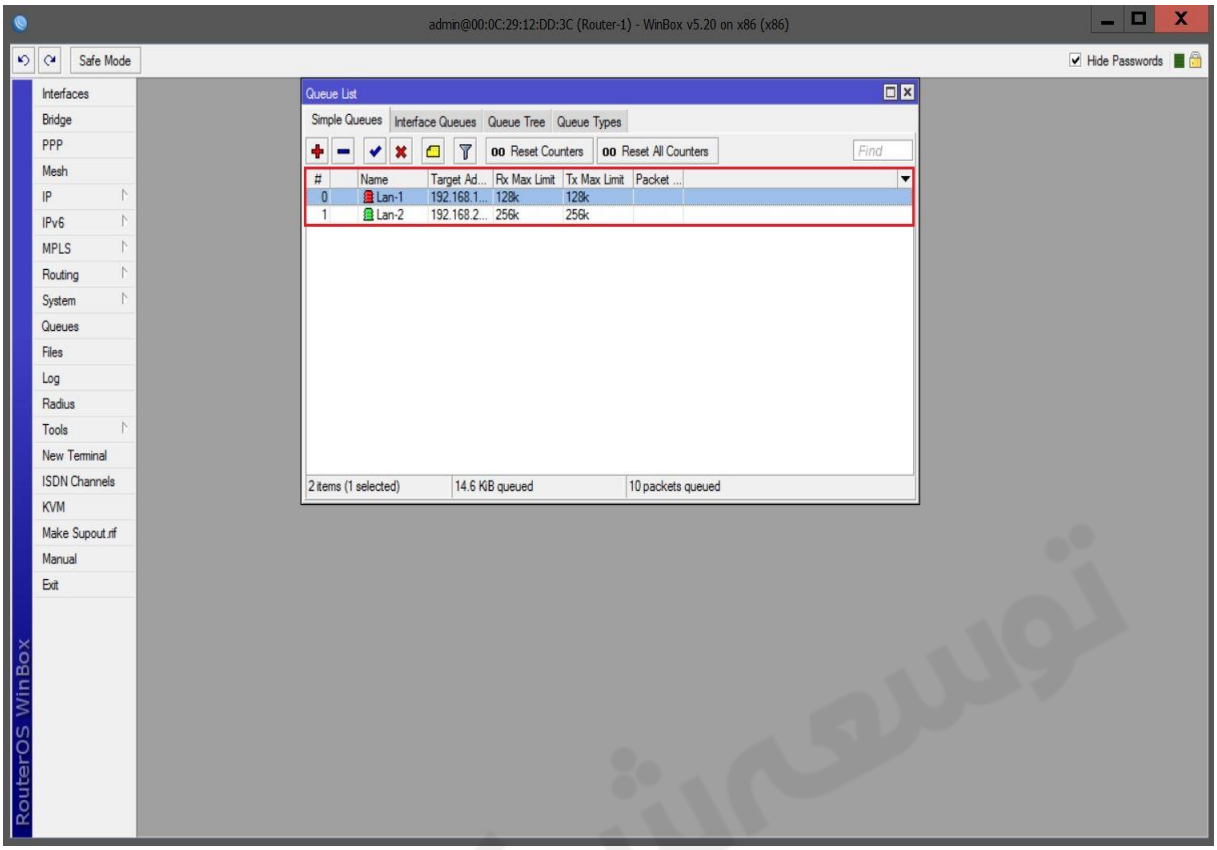


بررسی و مشاهده نمودار مصرف پهنای باند :

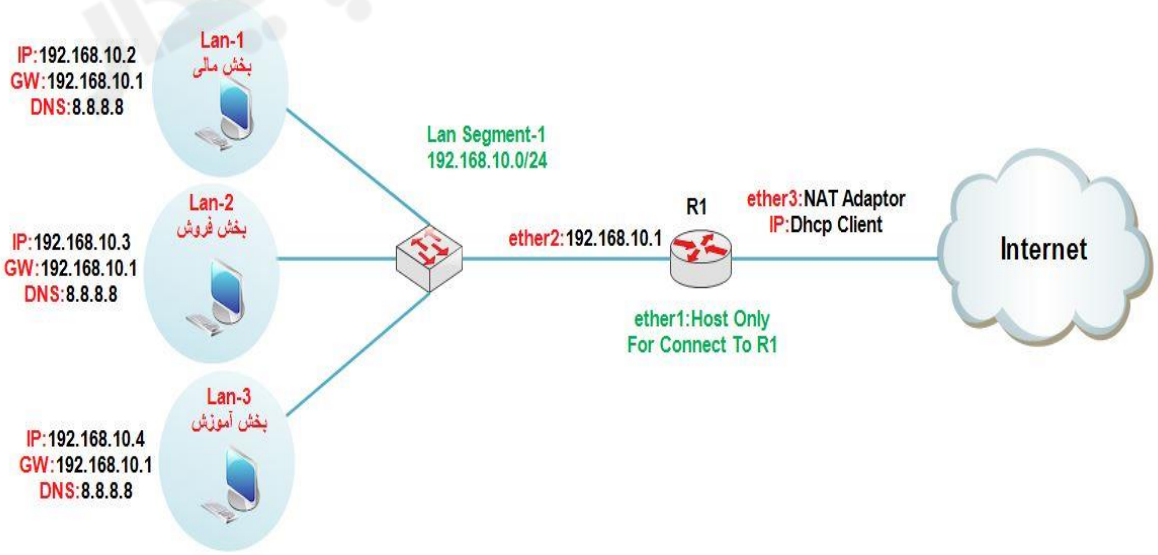
برای مشاهده نمودار مصرف پهنای باند که بصورت Live قابل مشاهده است باید به بخش Traffic مراجعه کنید :



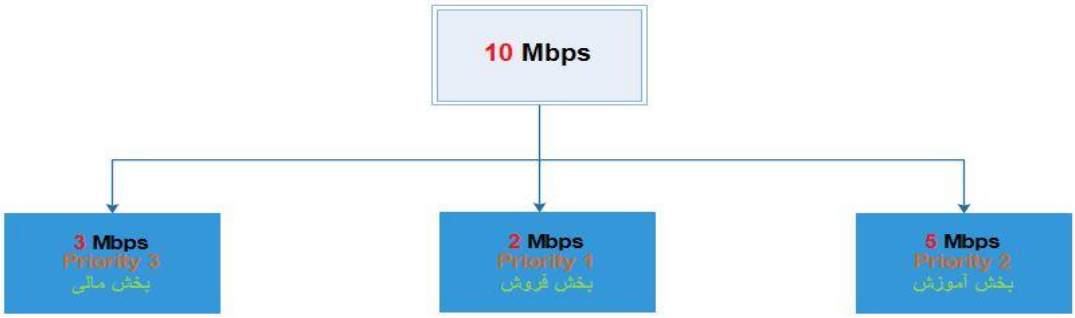
در صورتی که کلاینتی از تمام پهنای خود استفاده کند شکل سبز که در کنار نام آن قرار دارد به حالت قرمز در می آید.مثل عکس زیر :



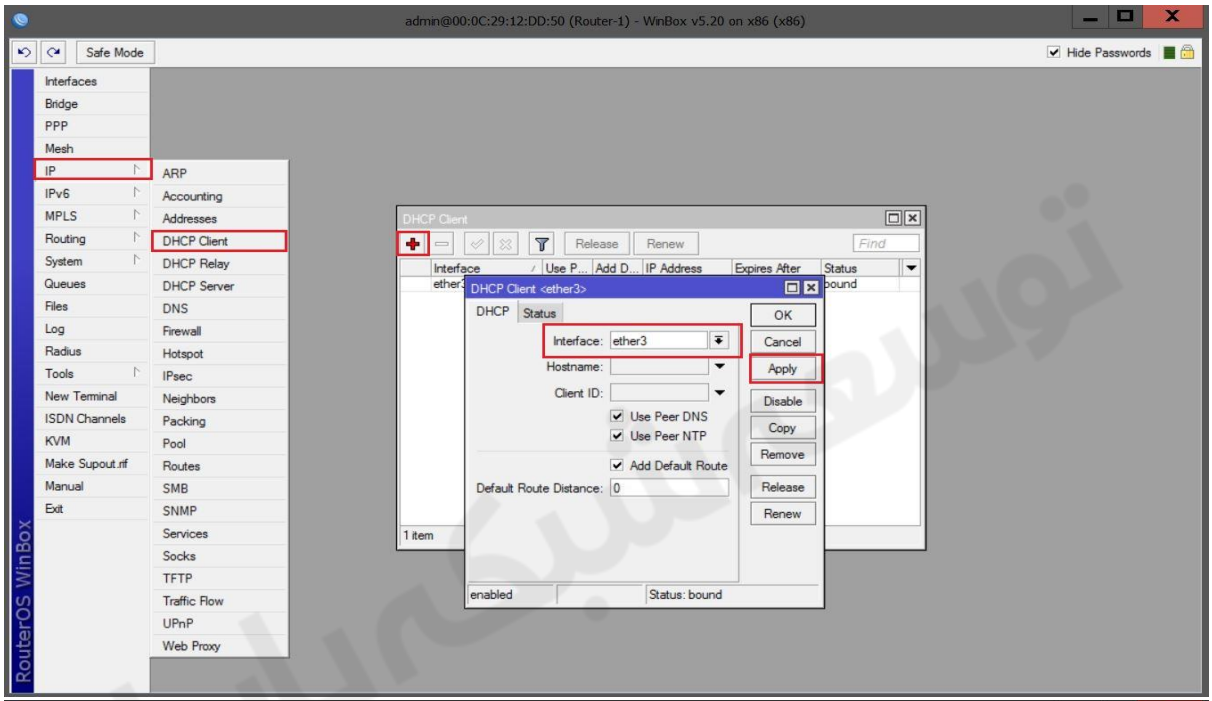
سناریو ۲ : در این سناریو ما **10Mbps** پهنای باند داریم که می خواهیم آنها را بین بخش های مختلف تقسیم کنیم.

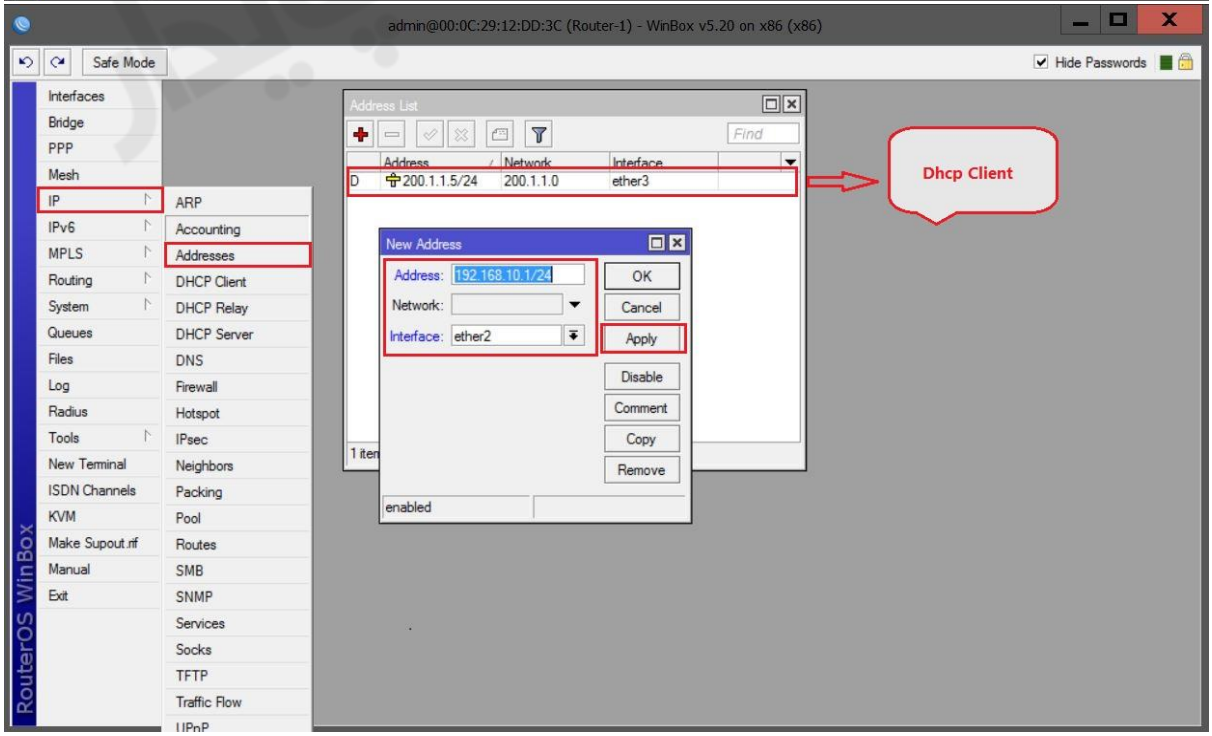


پهنای باند را طبق شکل زیر بین بخش های مختلفی که وجود دارد تقسیم می کنیم.

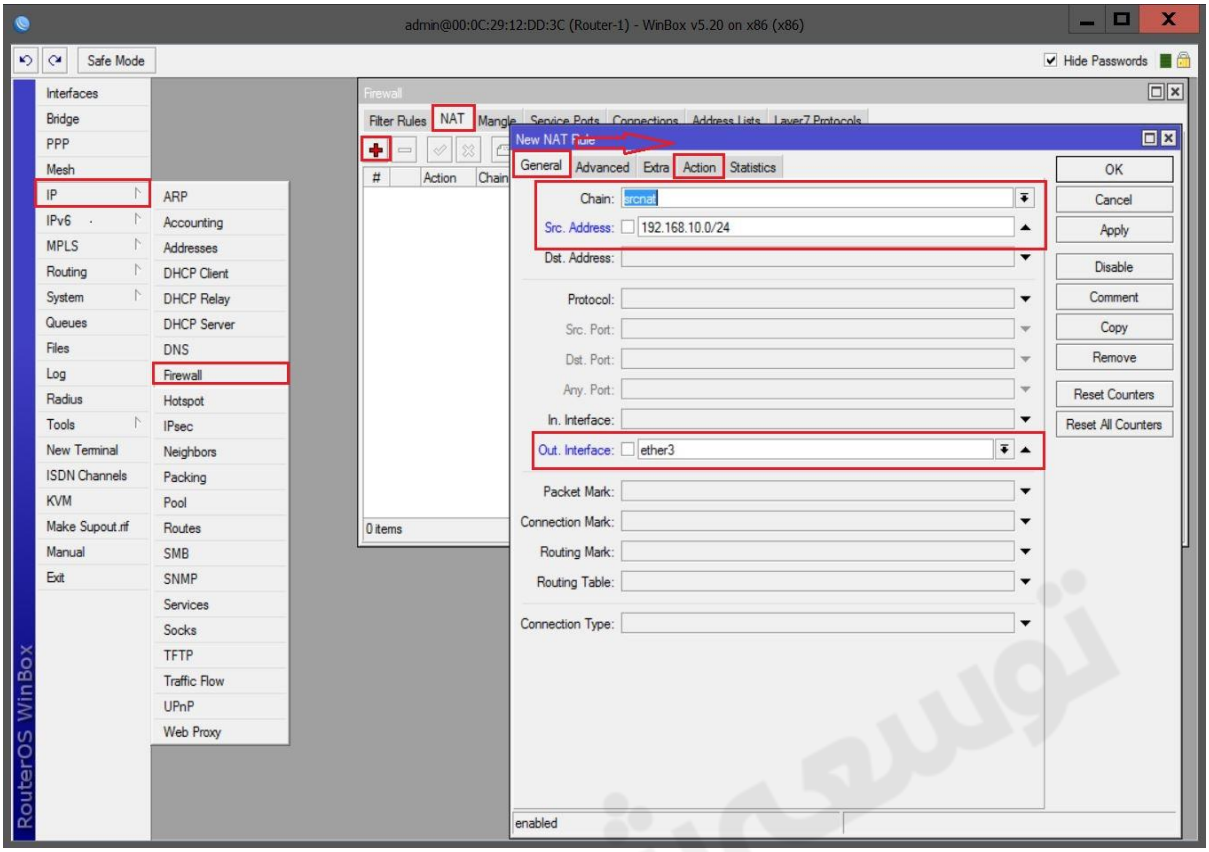


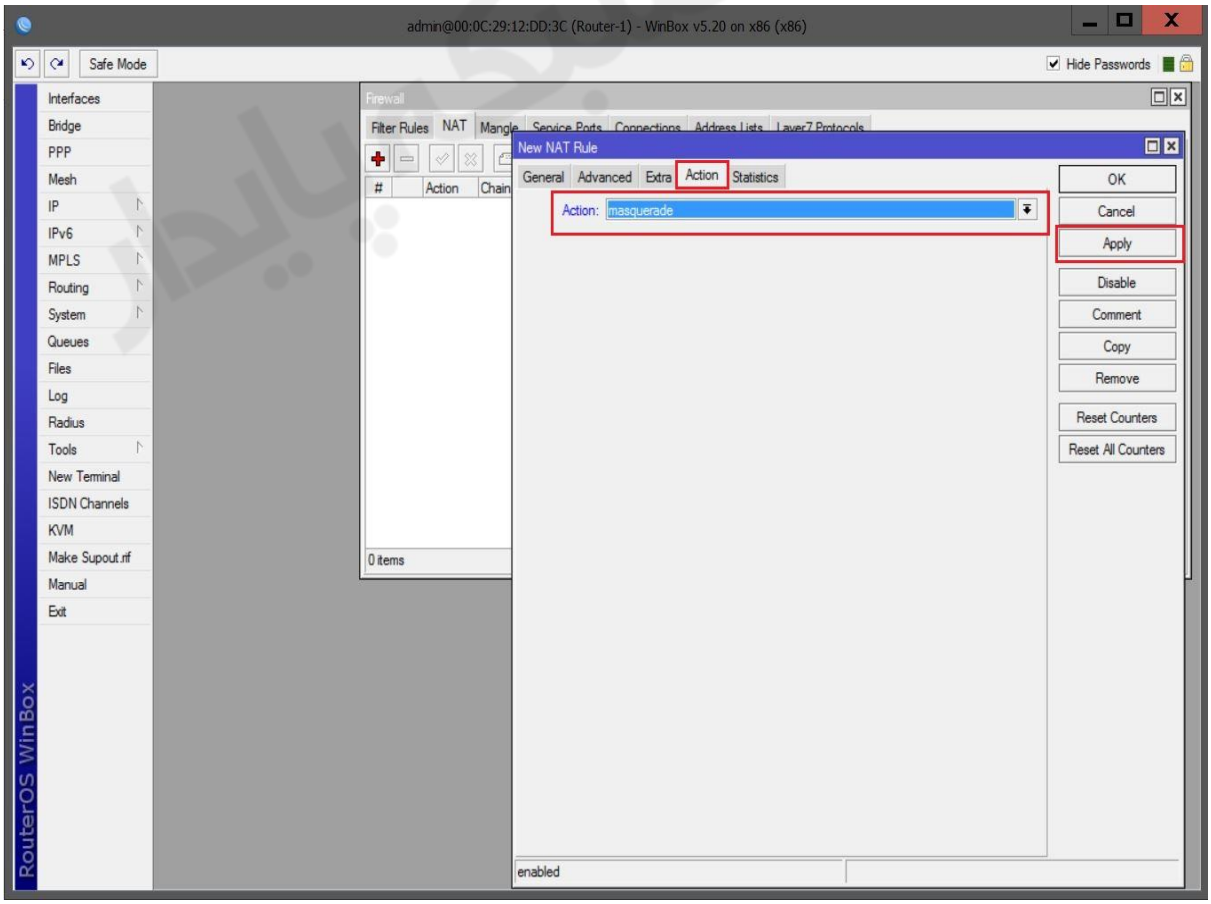
انتساب IP به کارت های شبکه روتر :





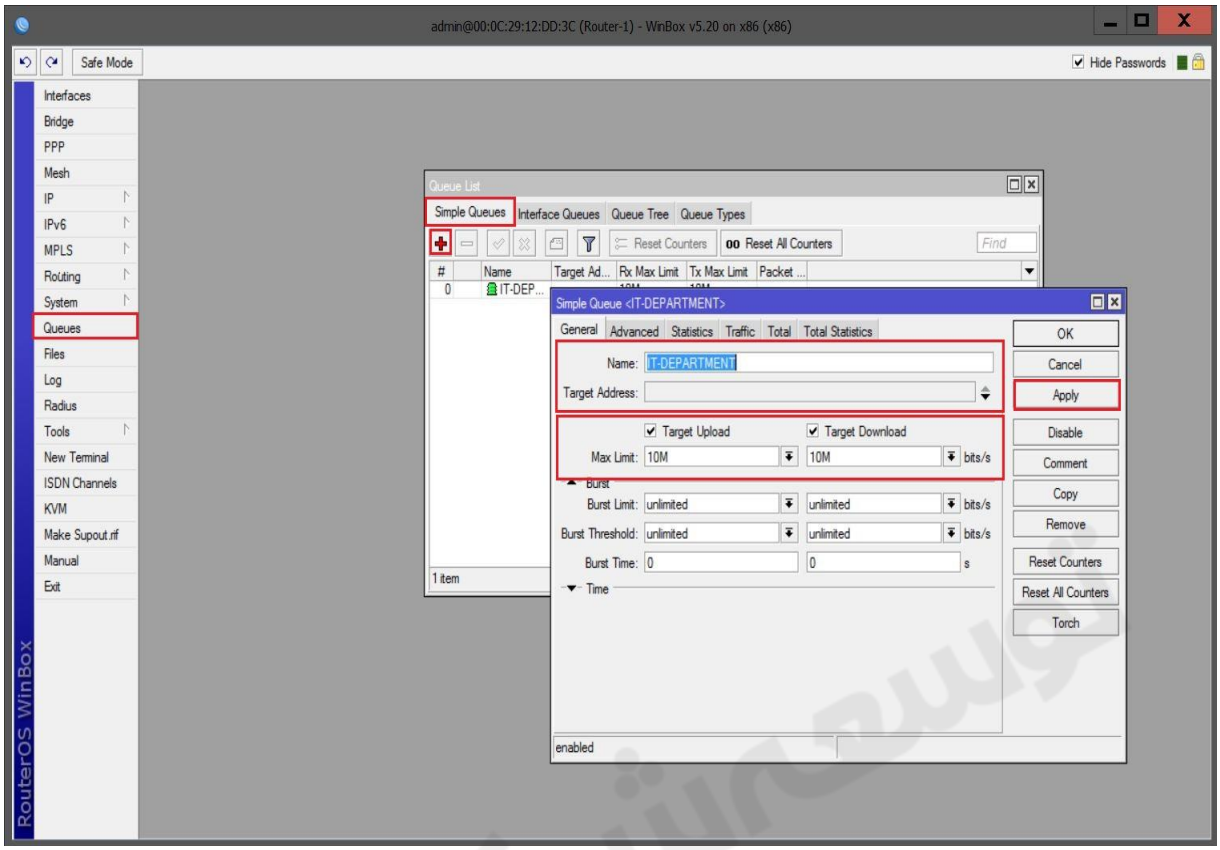
ایجاد Nat برای دسترسی کلاینت ها به اینترنت :



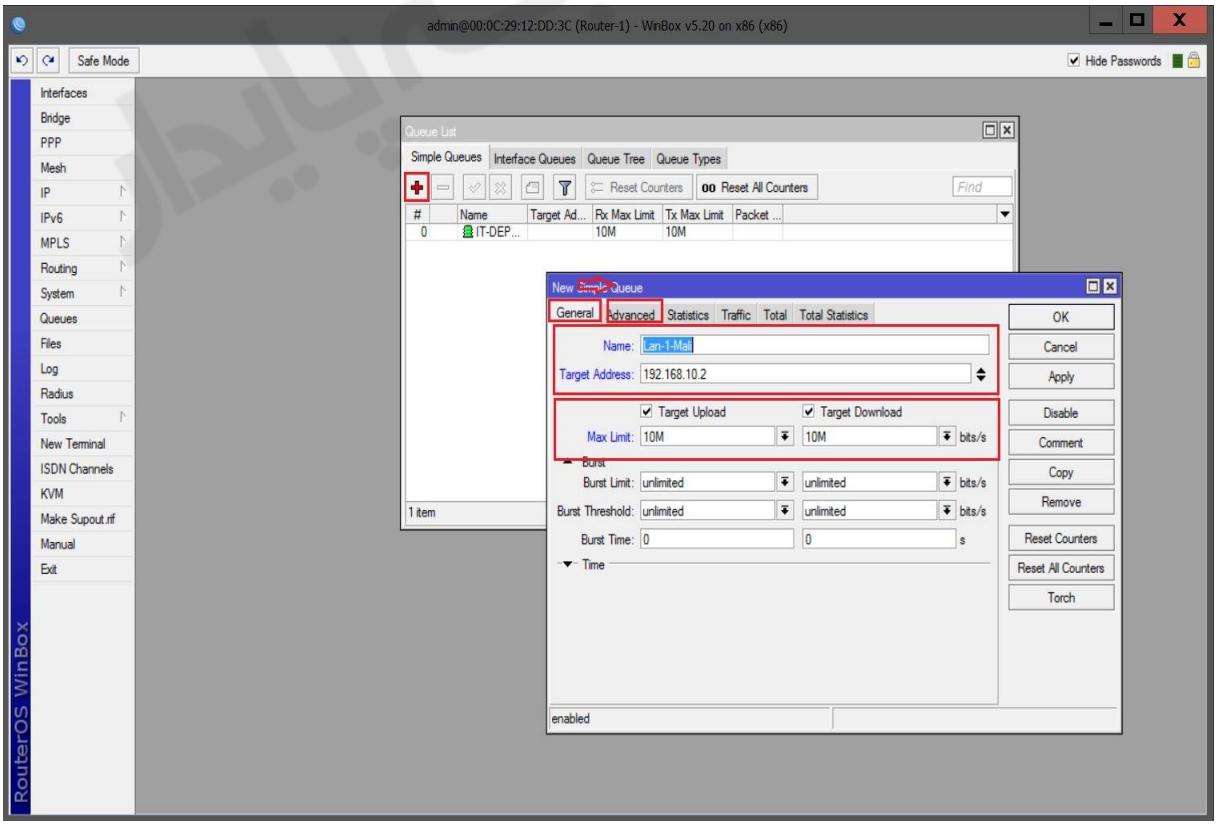


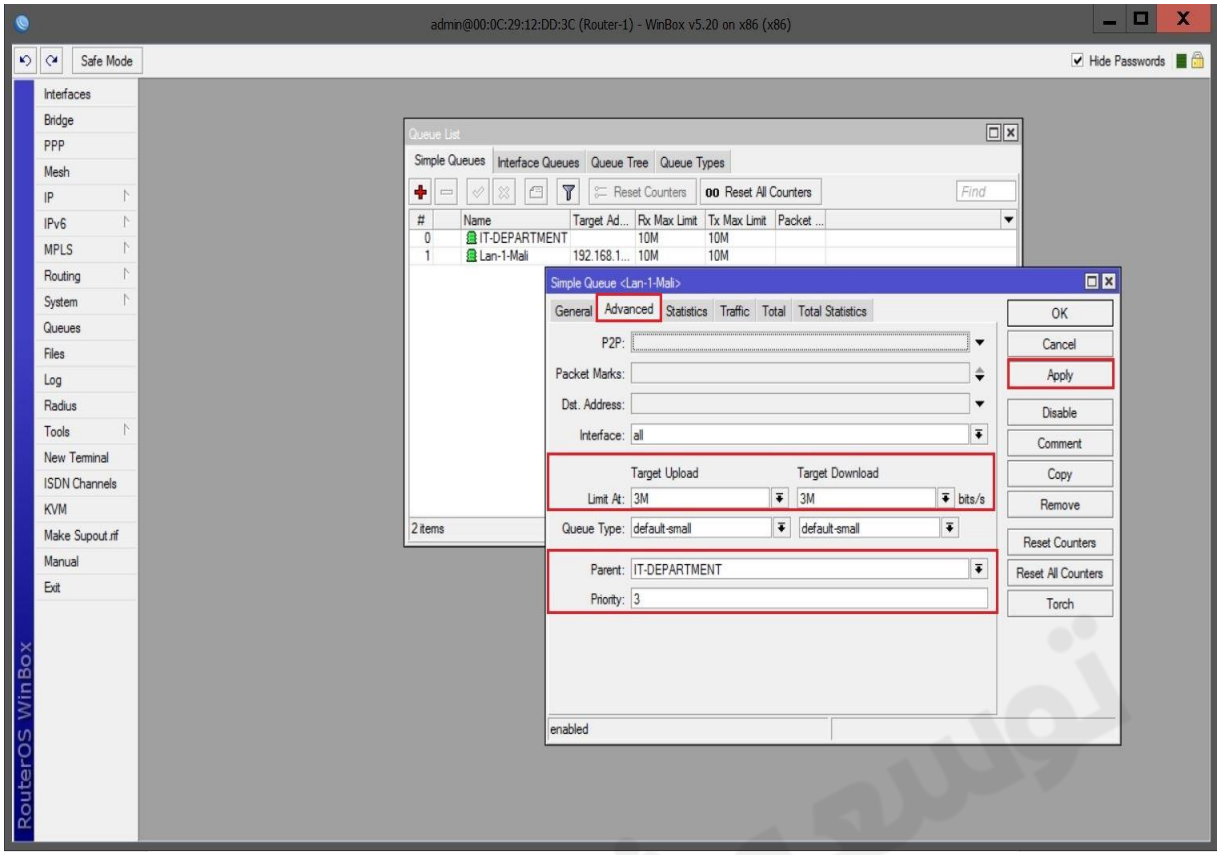
تقسیم پهنای باند بین بخش های مختلف :

برای این کار باید ابتدا یک Queue به عنوان Parent ایجاد کنیم سپس بخش های را به زیرمجموعه این Parent اضاف می کنیم.

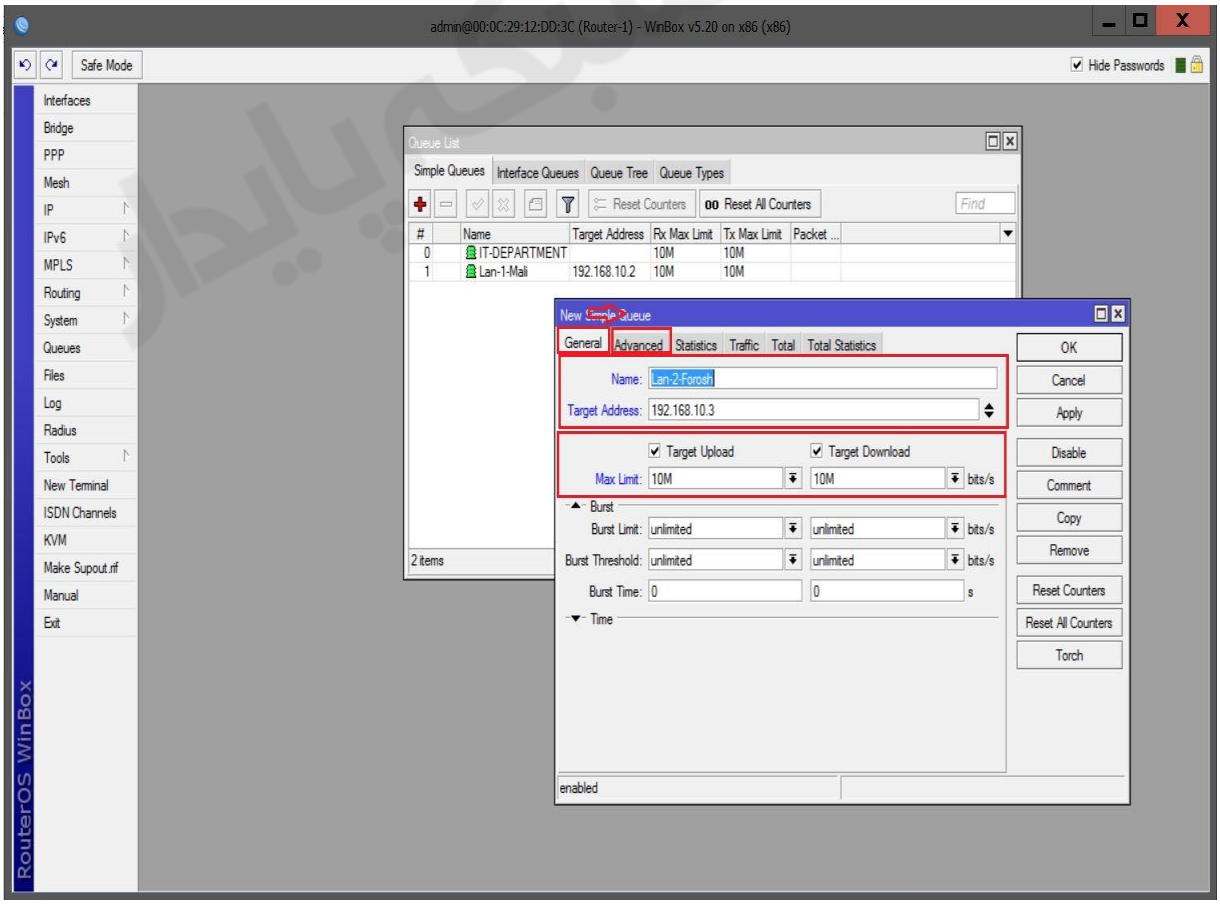


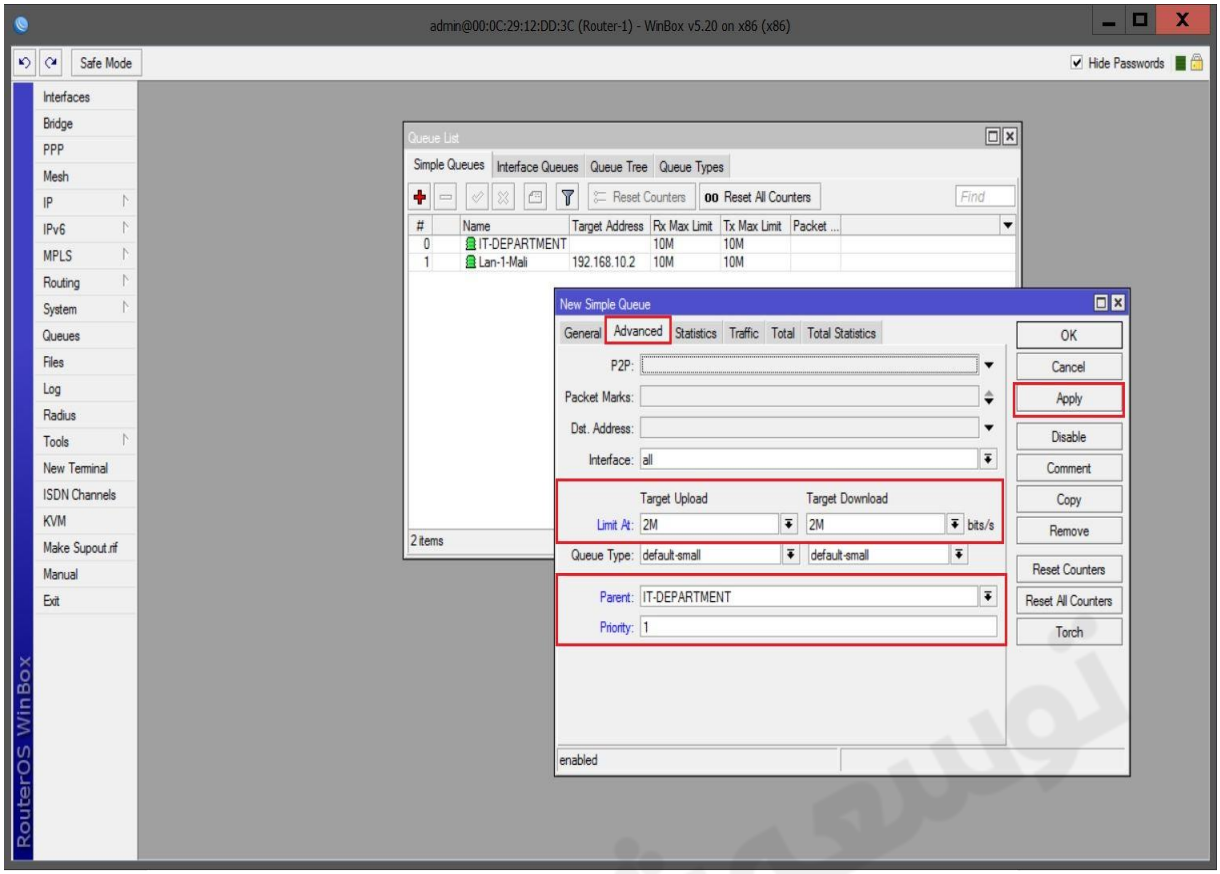
بخش مالی :



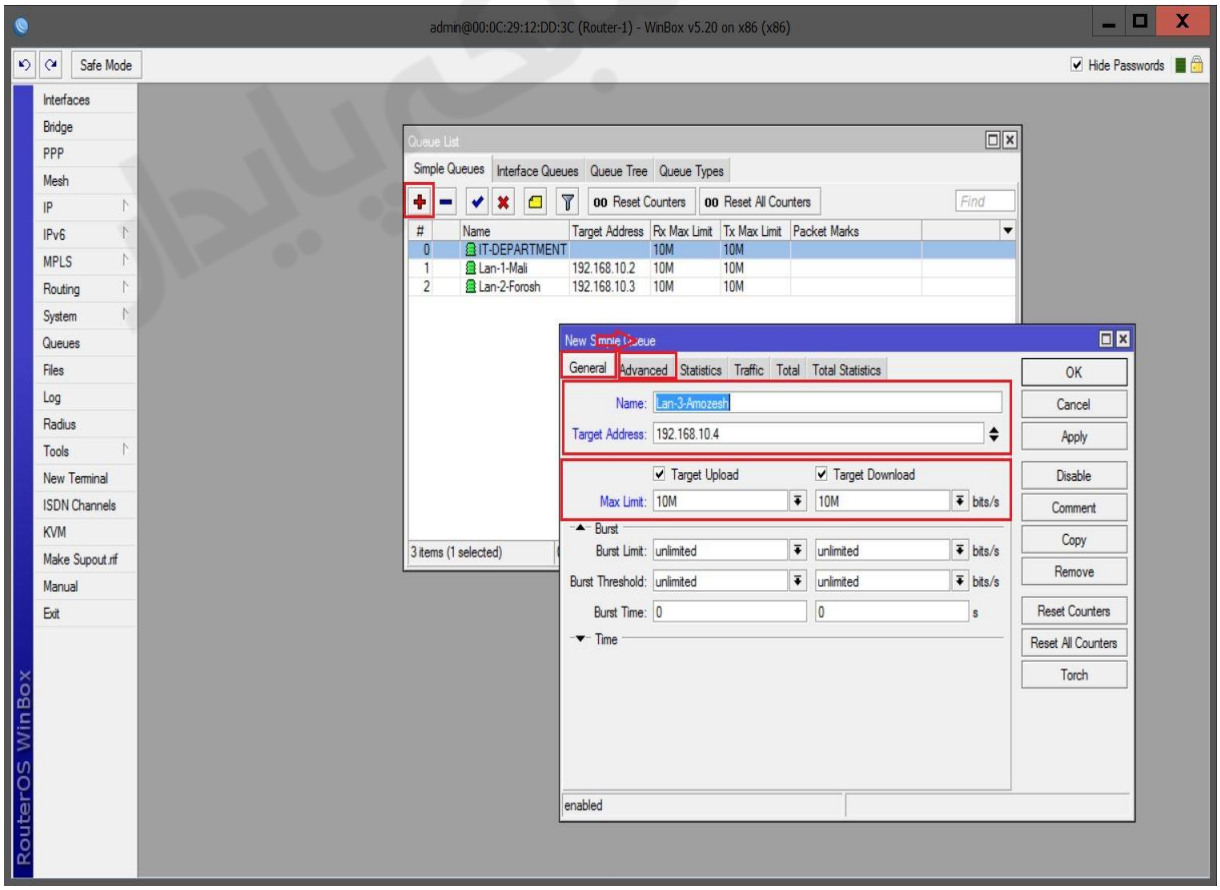

admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
RouterOS WinBox
Queue List
Simple Queues
Interface Queues
Queue Tree
Queue Types
Reset Counters
Reset All Counters
Find
Name Target Ad... Rx Max Limit Tx Max Limit Packet ...
0 IT-DEPARTMENT 10M 10M
1 Lan-1-Mali 192.168.1... 10M 10M
2 items
Simple Queue <Lan-1-Mali>
General
Advanced
Statistics
Traffic
Total
Total Statistics
P2P:
Packet Marks:
Dst. Address:
Interface: all
Target Upload
Target Download
Limit At: 3M 3M bits/s
Queue Type: default-small default-small
Parent: IT-DEPARTMENT
Priority: 3
enabled
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch

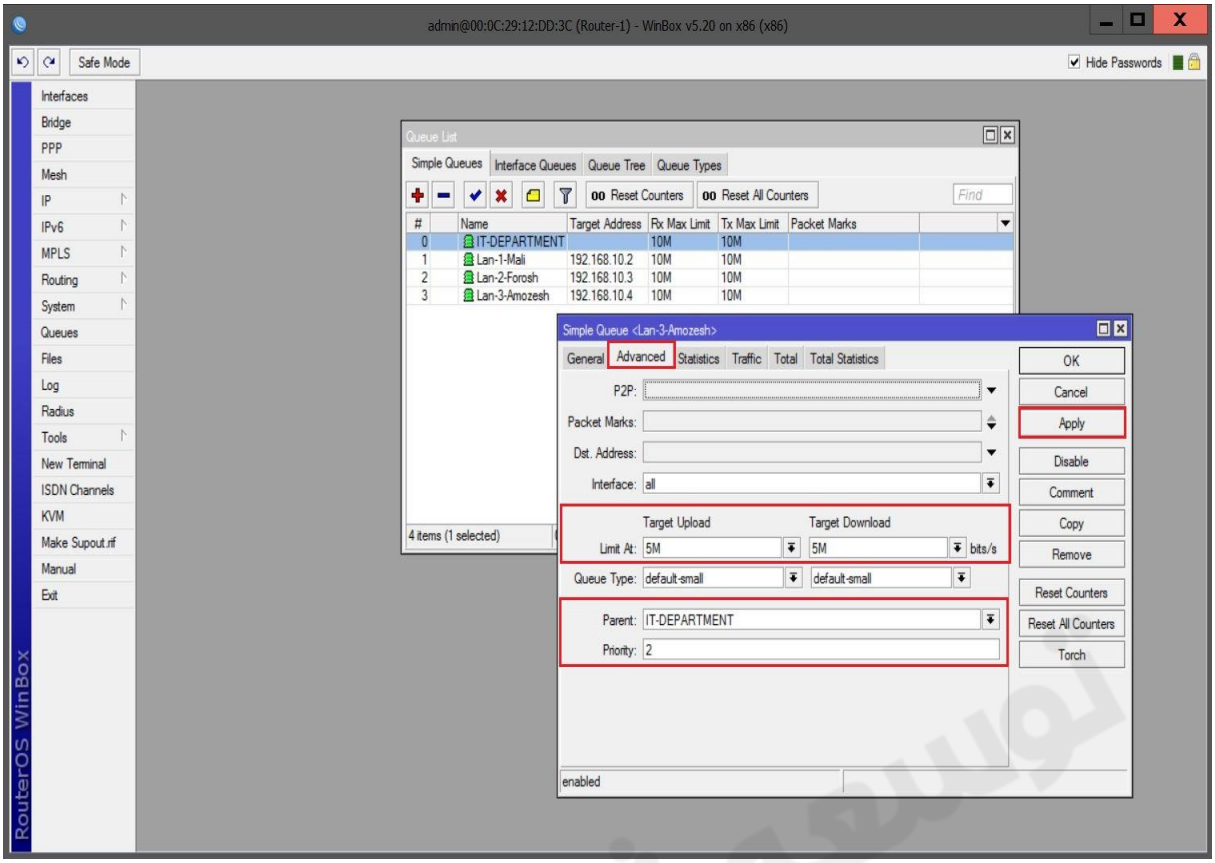
بخش فروش :


admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
RouterOS WinBox
Queue List
Simple Queues
Interface Queues
Queue Tree
Queue Types
Reset Counters
Reset All Counters
Find
Name Target Address Rx Max Limit Tx Max Limit Packet ...
0 IT-DEPARTMENT 10M 10M
1 Lan-1-Mali 192.168.10.2 10M 10M
2 items
New Simple Queue
General
Advanced
Statistics
Traffic
Total
Total Statistics
Name: Lan-2-Forosh
Target Address: 192.168.10.3
Target Upload
Target Download
Max Limit: 10M 10M bits/s
Burst
Burst Limit: unlimited unlimited bits/s
Burst Threshold: unlimited unlimited bits/s
Burst Time: 0 0 s
Time
enabled
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch


admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
RouterOS WinBox
Queue List
Simple Queues
Interface Queues
Queue Tree
Queue Types
Reset Counters
Reset All Counters
Find
Name Target Address Rx Max Limit Tx Max Limit Packet ...
0 IT-DEPARTMENT 10M 10M
1 Lan-1-Mali 192.168.10.2 10M 10M
2 items
New Simple Queue
General
Advanced
Statistics
Traffic
Total
Total Statistics
P2P:
Packet Marks:
Dst. Address:
Interface: all
Target Upload
Target Download
Limit At: 2M 2M bits/s
Queue Type: default-small default-small
Parent: IT-DEPARTMENT
Priority: 1
enabled
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch

بخش آموزش :


admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
RouterOS WinBox
Queue List
Simple Queues
Interface Queues
Queue Tree
Queue Types
Reset Counters
Reset All Counters
Find
Name Target Address Rx Max Limit Tx Max Limit Packet Marks
0 IT-DEPARTMENT 10M 10M
1 Lan-1-Mali 192.168.10.2 10M 10M
2 Lan-2-Forosh 192.168.10.3 10M 10M
3 items (1 selected)
General
Advanced
Statistics
Traffic
Total
Total Statistics
Name: Lan-3-Amozesh
Target Address: 192.168.10.4
Target Upload
Target Download
Max Limit: 10M 10M bits/s
Burst
Burst Limit: unlimited unlimited bits/s
Burst Threshold: unlimited unlimited bits/s
Burst Time: 0 0 s
Time
enabled
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch



در این سناریو با این کانفیگ برای مثال در صورتی که بخش مالی و فروش از پهنای باند خود استفاده نکنند بخش آموزش از تمام پهنای باند یعنی 10Mbps استفاده می کند اما در صورتی که فقط بخش مالی از پهنای باند خود استفاده نکند پهنای باند آن توسط بخش فروش مورد استفاده قرار می گیرد زیرا Priority آن کمتر است.

فصل یازدهم : PPPOE Server

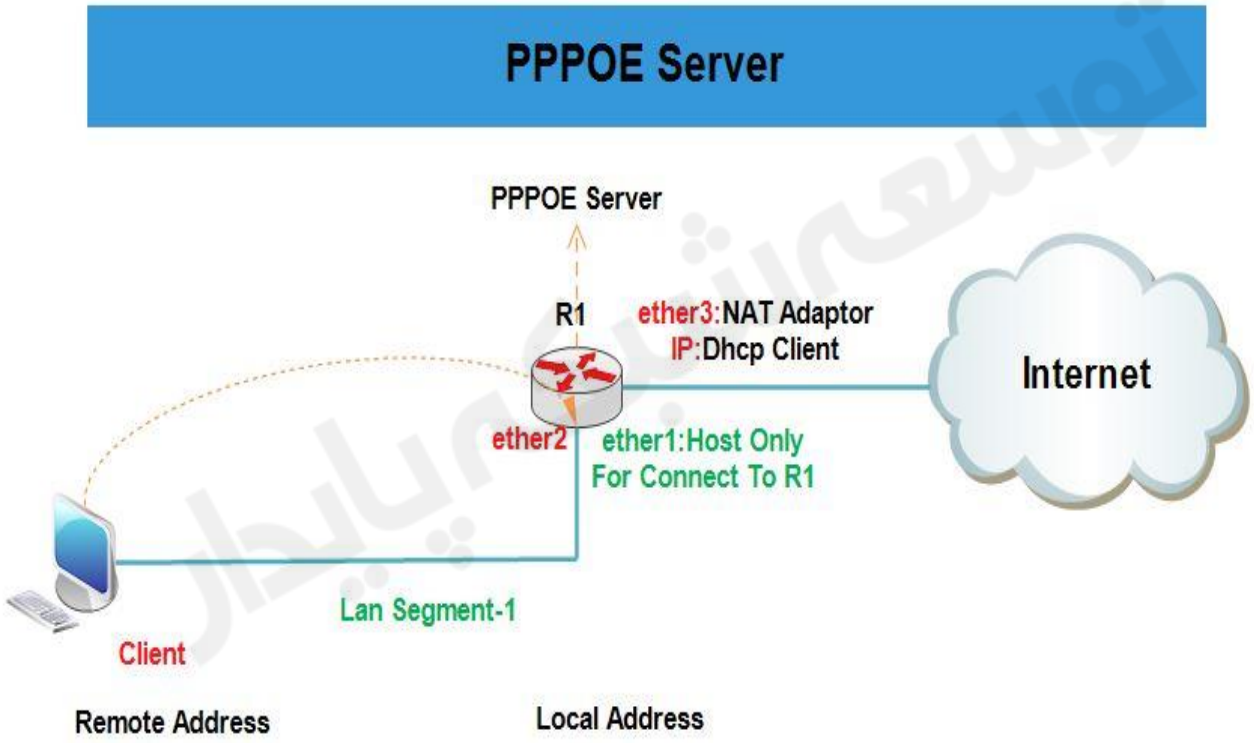
pppoe مختصر شده عبارت **Point To Ppint Over Ethernet** و یکی از پروتکل های شبکه می باشد که امکان تبادل داده بین دو شبکه و یا دو **Point** (نقطه) را برقرار می کند.

pppoe پروتکلی است که بصورت گسترده توسط **ISP** ها مورد استفاده قرار می گیرد جهت ارائه سرویس های اینترنتی پرسرعت **DSL** که معروف ترین آنها **ADSL** می باشد به کار میرود.

دلایل استفاده از **pppoe** ، حداقل وابستگی های ممکن برای برقراری یک کانکشن است که نیاز به تنظیم کردن **IP** و یا اطلاعات کاربر در خصوص آدرس های **IP** و تنظیم آن را دارا نمی باشد

pppoe یکی از ساده ترین پروتکل های **Tunneling** می باشد که روش های استاندارد **Encryption** (رمزنگاری)و **Authentication** (احراز هویت) و **Compressin** (فشرده سازی) که توسط **PPP** تعیین شده است استفاده می کند.

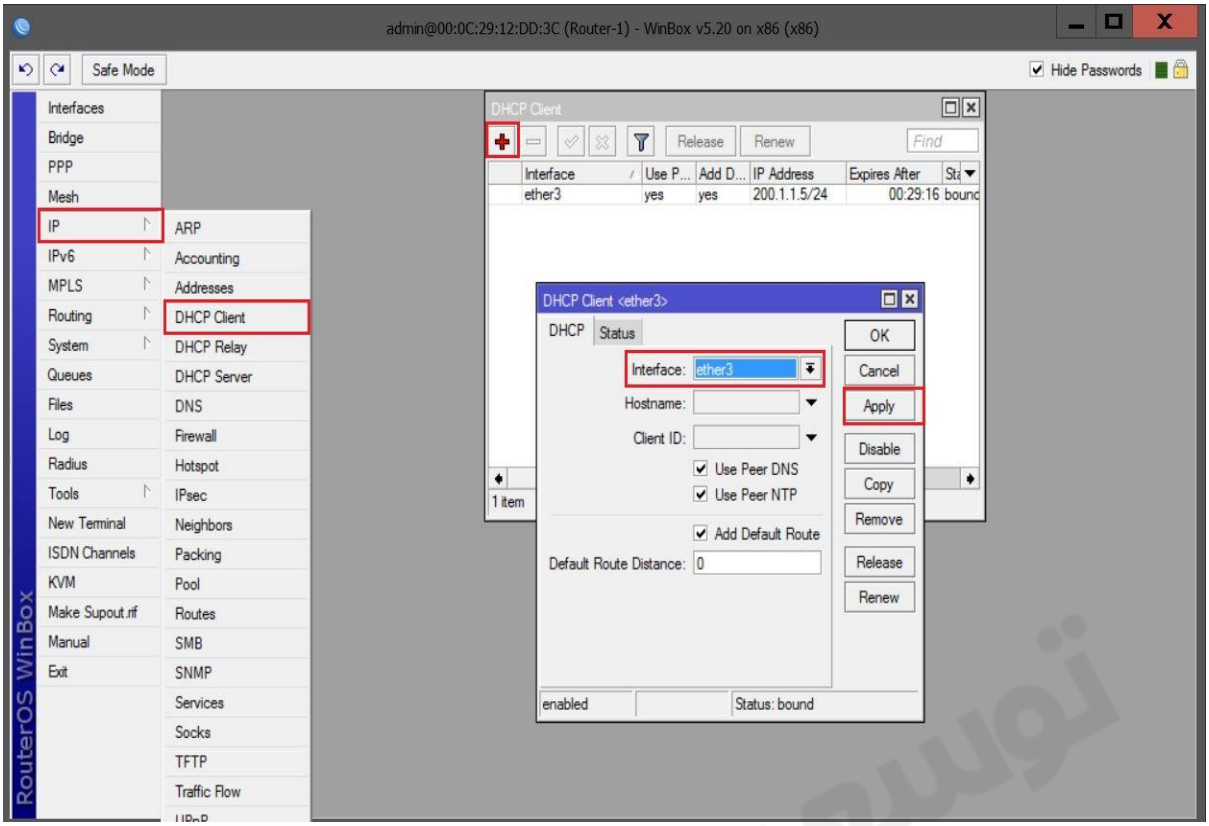
سناریو ۱ : راه اندازی PPPoE Server بر روی میکروتیک

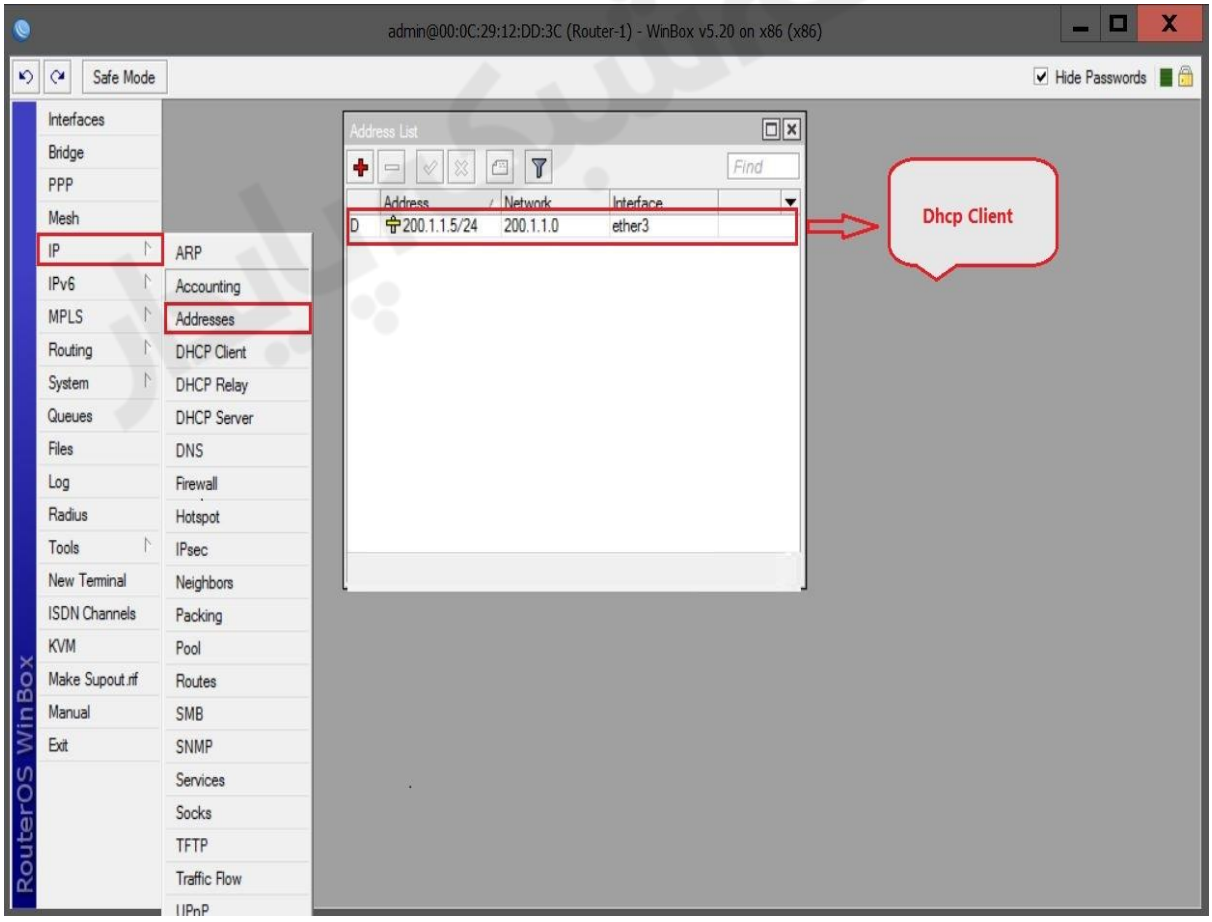


هدف این سناریو این است که با راه اندازی **PPPoE Server** بر روی میکروتیک ، کلاینت یا کلاینت ها بتوانند با ایجاد یک کانکشن به اینترنت دسترسی پیدا کنند.

انتساب **IP** به کارت های شبکه روتر **R1** :

همان طور که در سناریو مشخص کردیم **Ether3** باید از **Dhcp Client** (**Vmware**) آدرس**IP** دریافت کند.برای این کار از منوی اصلی گزینه **IP** و از زیر منوی باز شده **Dhcp Client** را انتخاب میکنیم.در پنجره باز شده بر روی **Add** کلیک و از تب **Dhcp** اینترفیس مورد نظر را انتخاب و **ok** را میزنیم.


admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
RouterOS WinBox
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Socks
TFTP
Traffic Flow
DHCP Client
Release
Renew
Find
Interface
Use P...
Add D...
IP Address
Expires After
ether3
yes
yes
200.1.1.5/24
00:29:16
1 item
DHCP Client <ether3>
DHCP
Status
Interface: ether3
Hostname:
Client ID:
Use Peer DNS
Use Peer NTP
Add Default Route
Default Route Distance: 0
OK
Cancel
Apply
Disable
Copy
Remove
Release
Renew
enabled
Status: bound

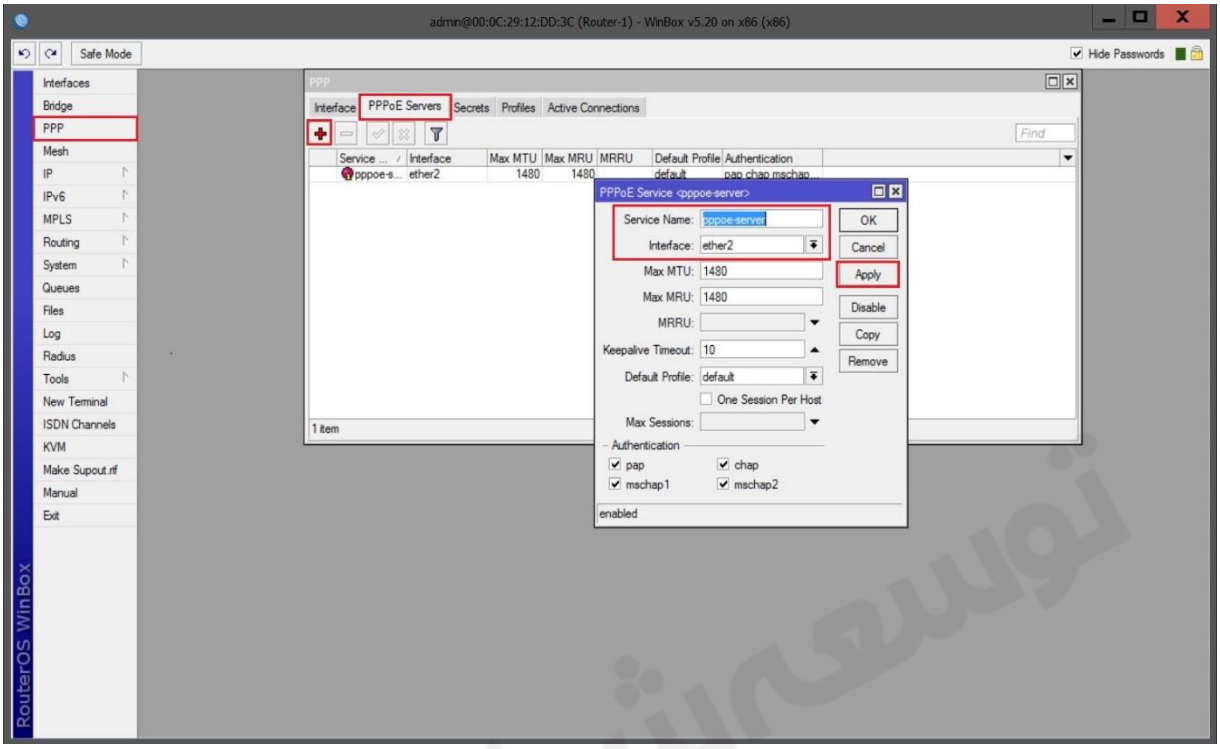

admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
RouterOS WinBox
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Socks
TFTP
Traffic Flow
Address List
Find
Address
Network
Interface
D
200.1.1.5/24
200.1.1.0
ether3
Dhcp Client

راه اندازی PPPoE Server :

برای اینکار از منوی اصلی گزینه PPP را انتخاب کرده و از پنجره باز شده به تب PPPoE Sever رفته و بروی Add کلیک میکنیم.

Service Name : یک نام به دلخواه انتخاب می کنیم.

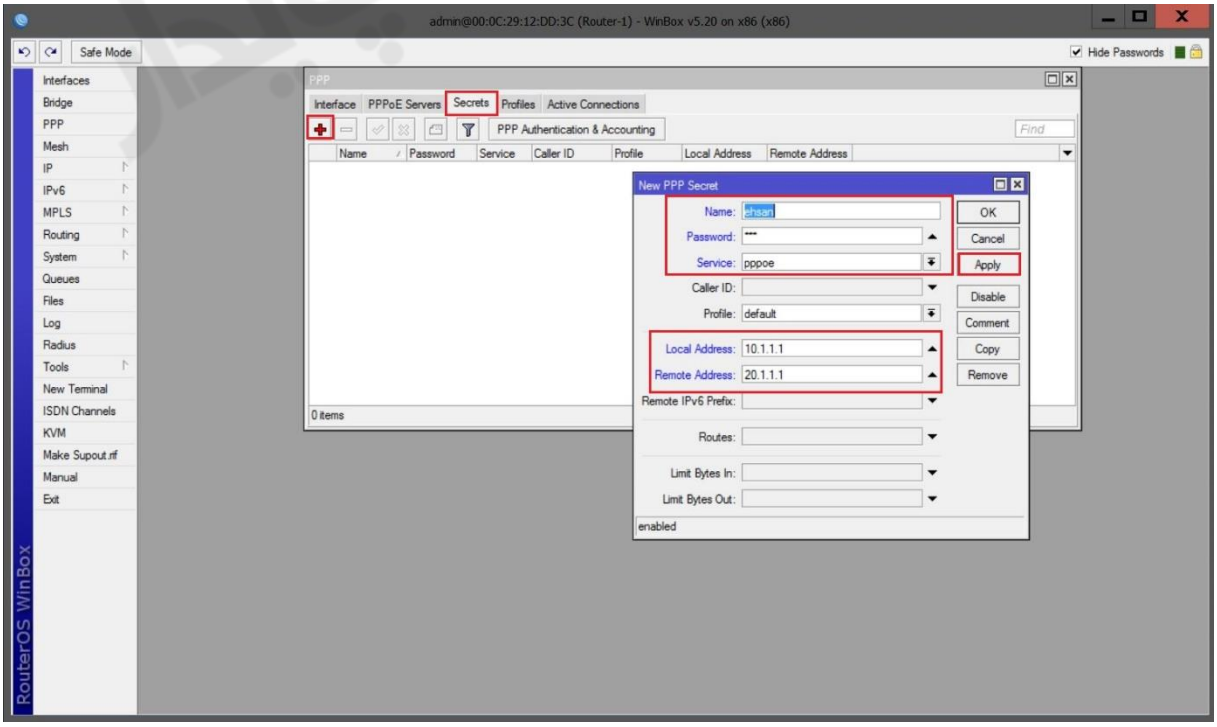
Interface :اینترفیسی که قصد راه اندازی PPPoE بر روی آن را دارید را انتخاب می کنید.



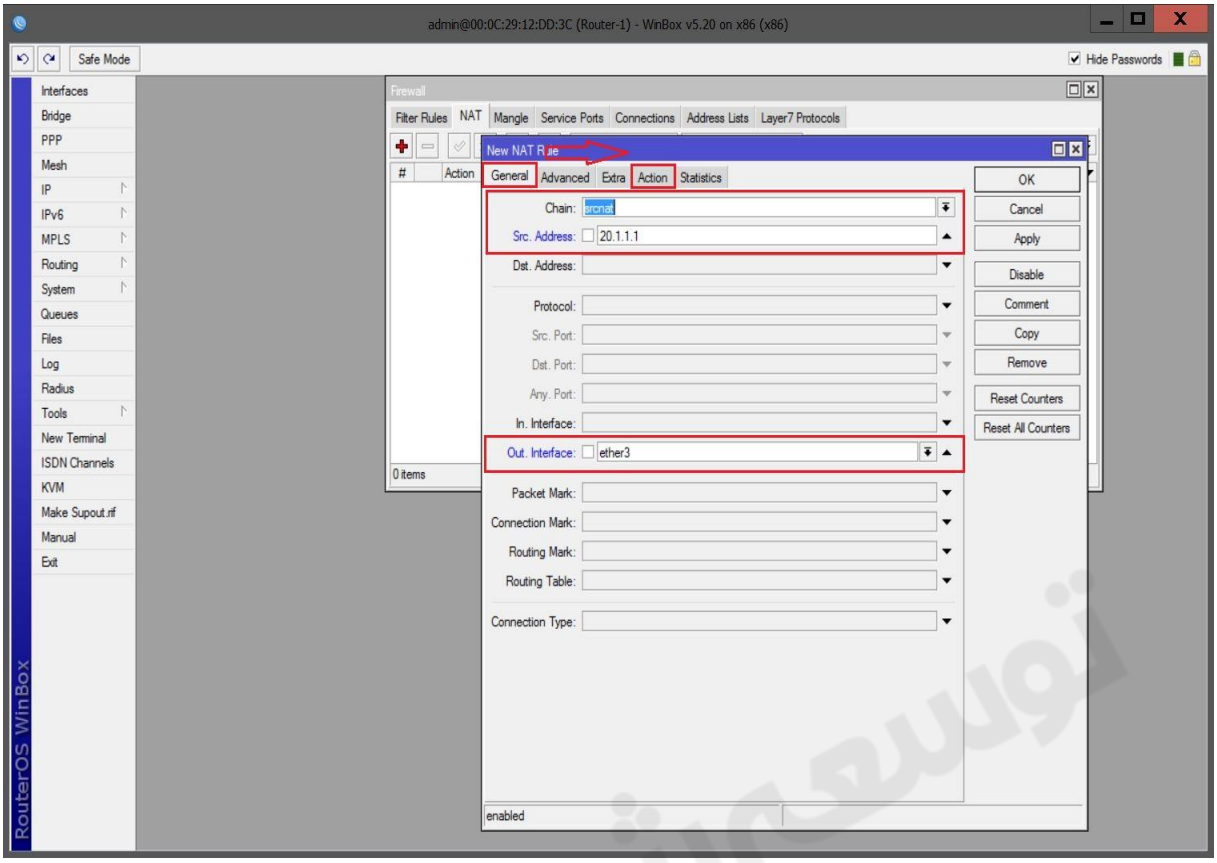
تعریف Accounting برای User ها :

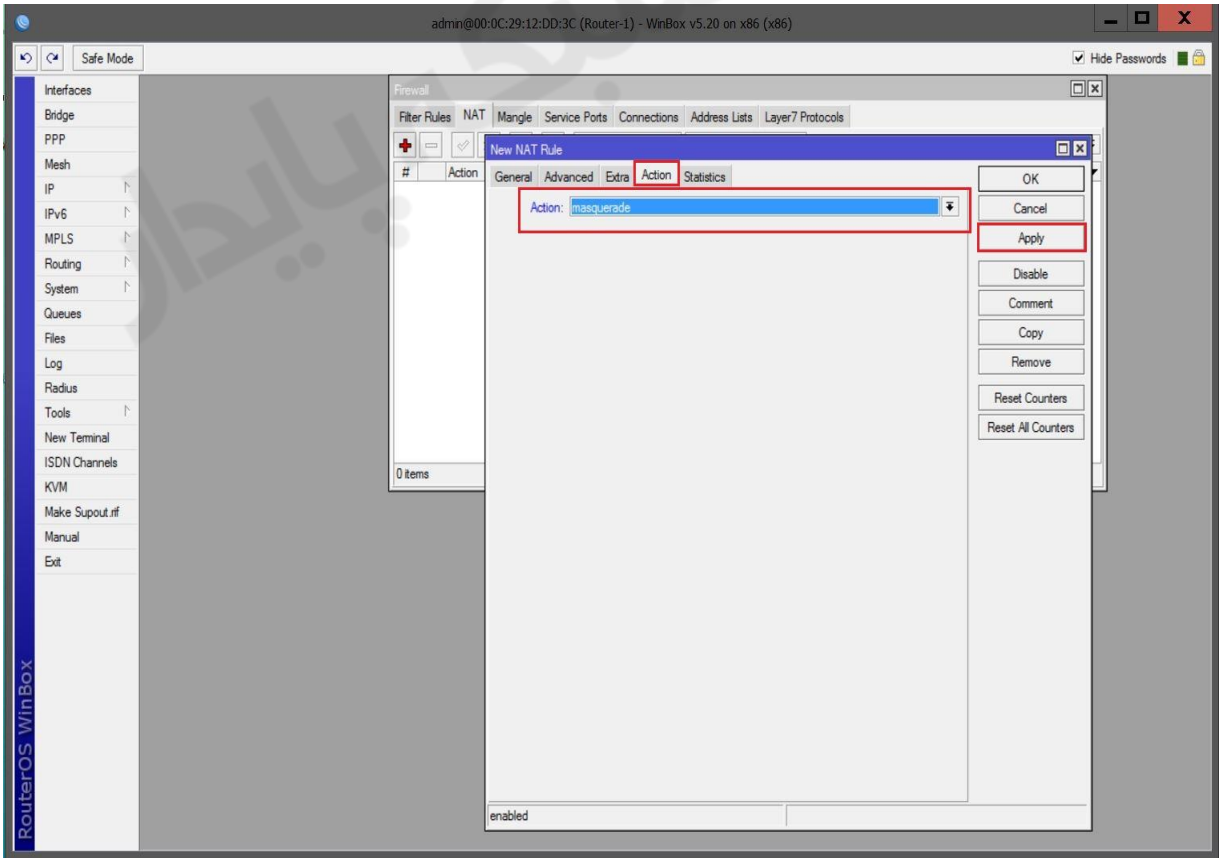
برای اینکار به تب Secret رفته و برروی Add کلیک می کنیم.

باید یک IP آدرس برای دو سر Tunnel تعریف کنیم که به سمت روتر اصطلاحا Local Address و به سمت کلاینت اصطلاحا Remote Address گفته می شود.



برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند باید یک **Nat** تعریف کنیم.



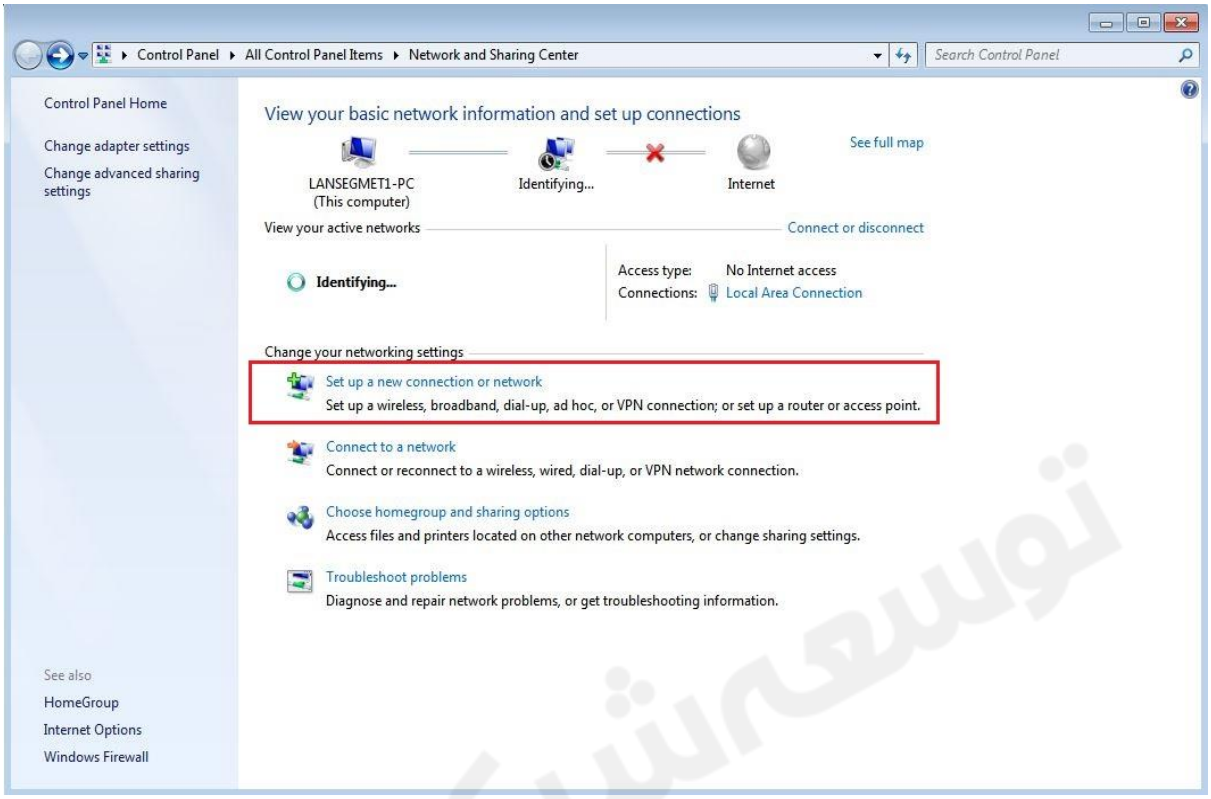


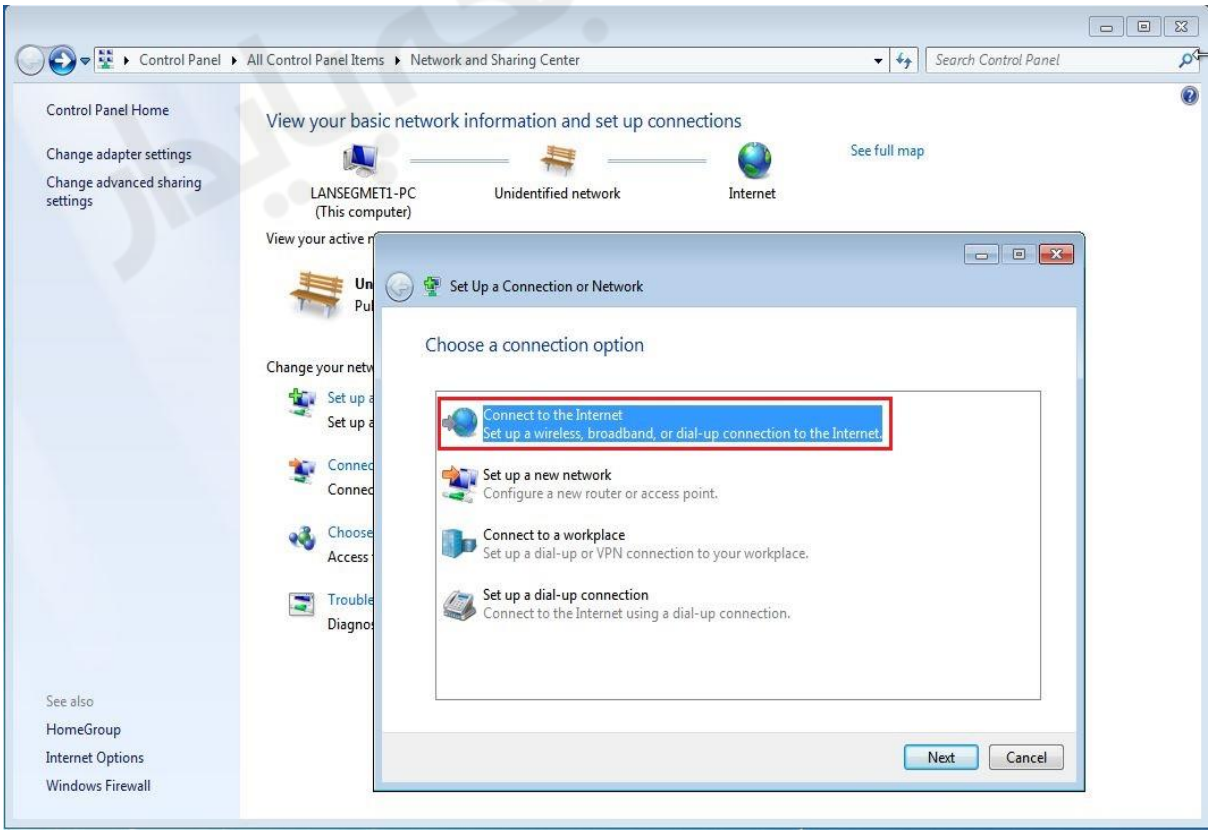
تنظیمات کلاینت :

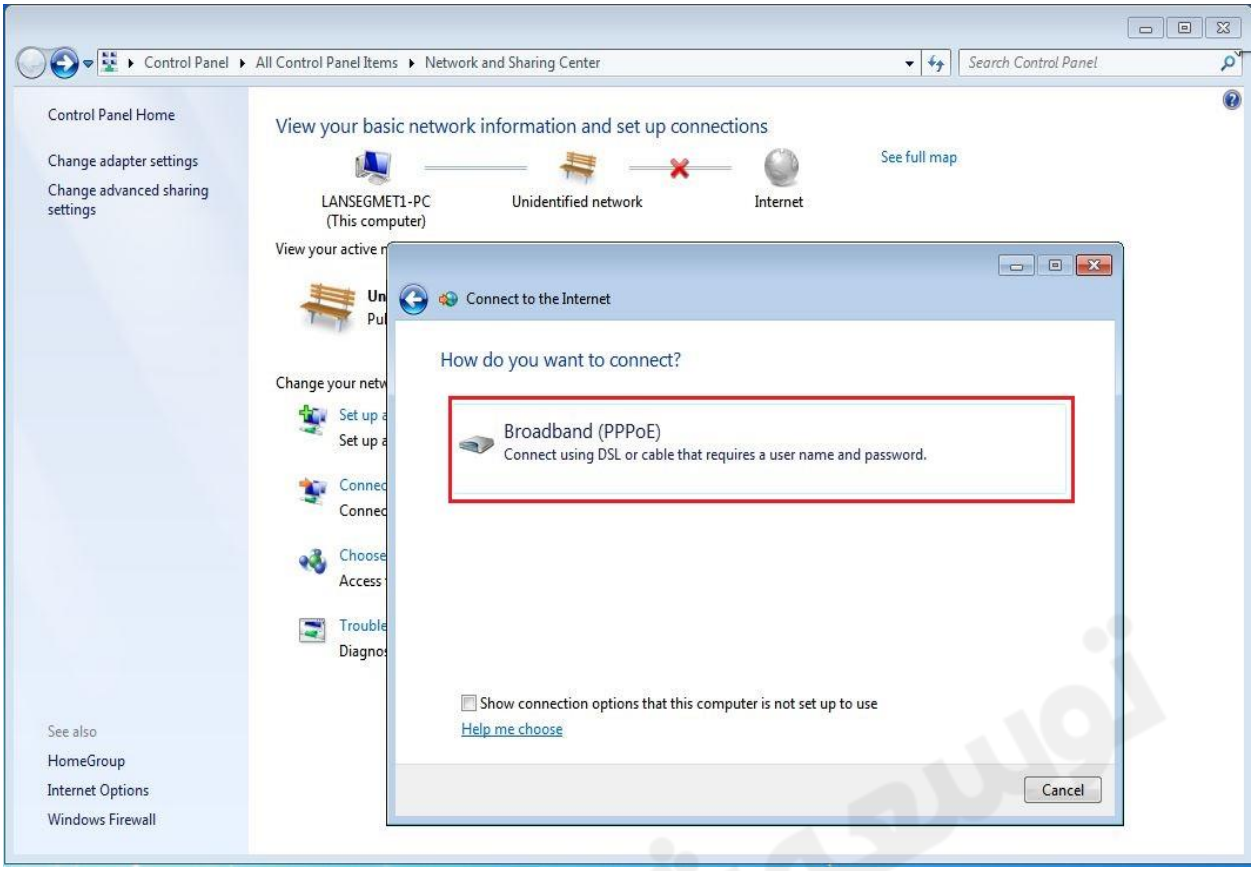
ایجاد کانکشن برای دسترسی به اینترنت :

برای این کار به مسیر زیر می رویم :

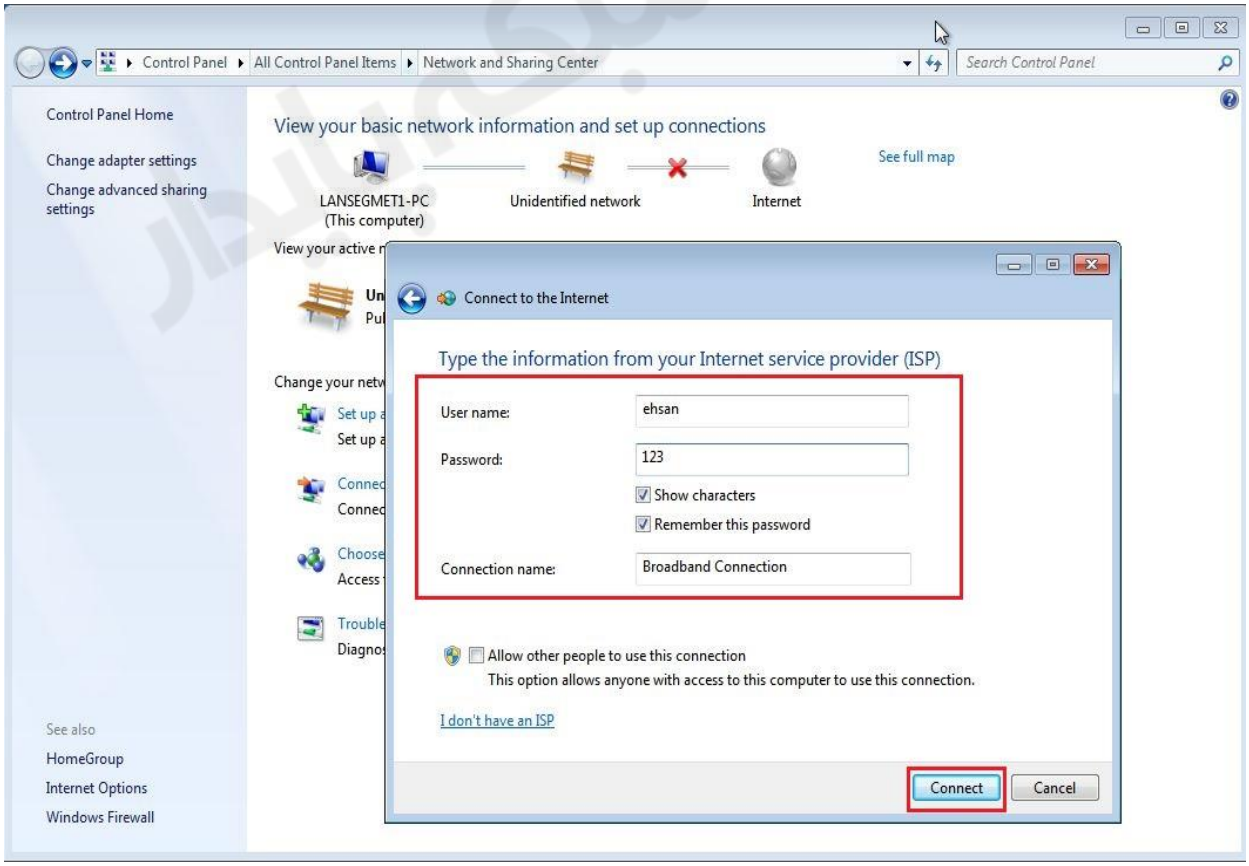
Control Panel > Network and Sharing > Setup new Connection or network

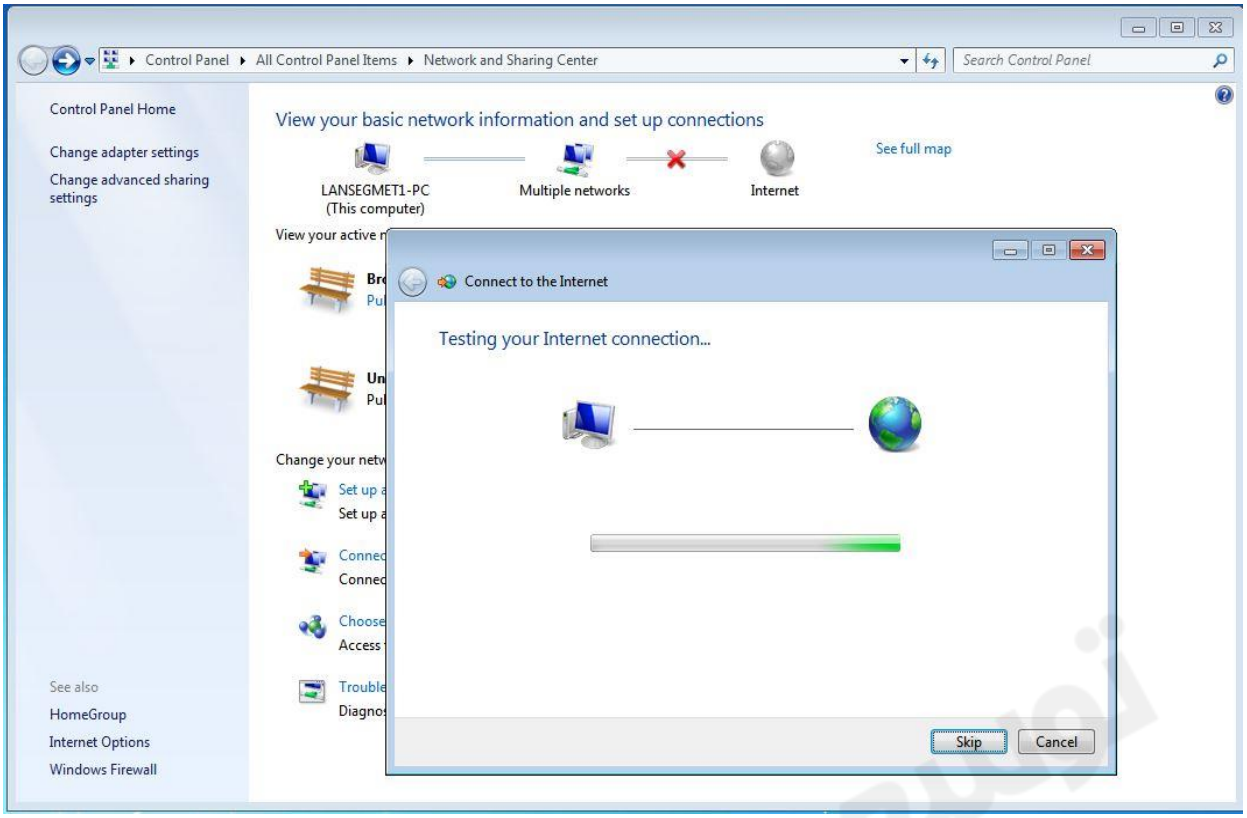




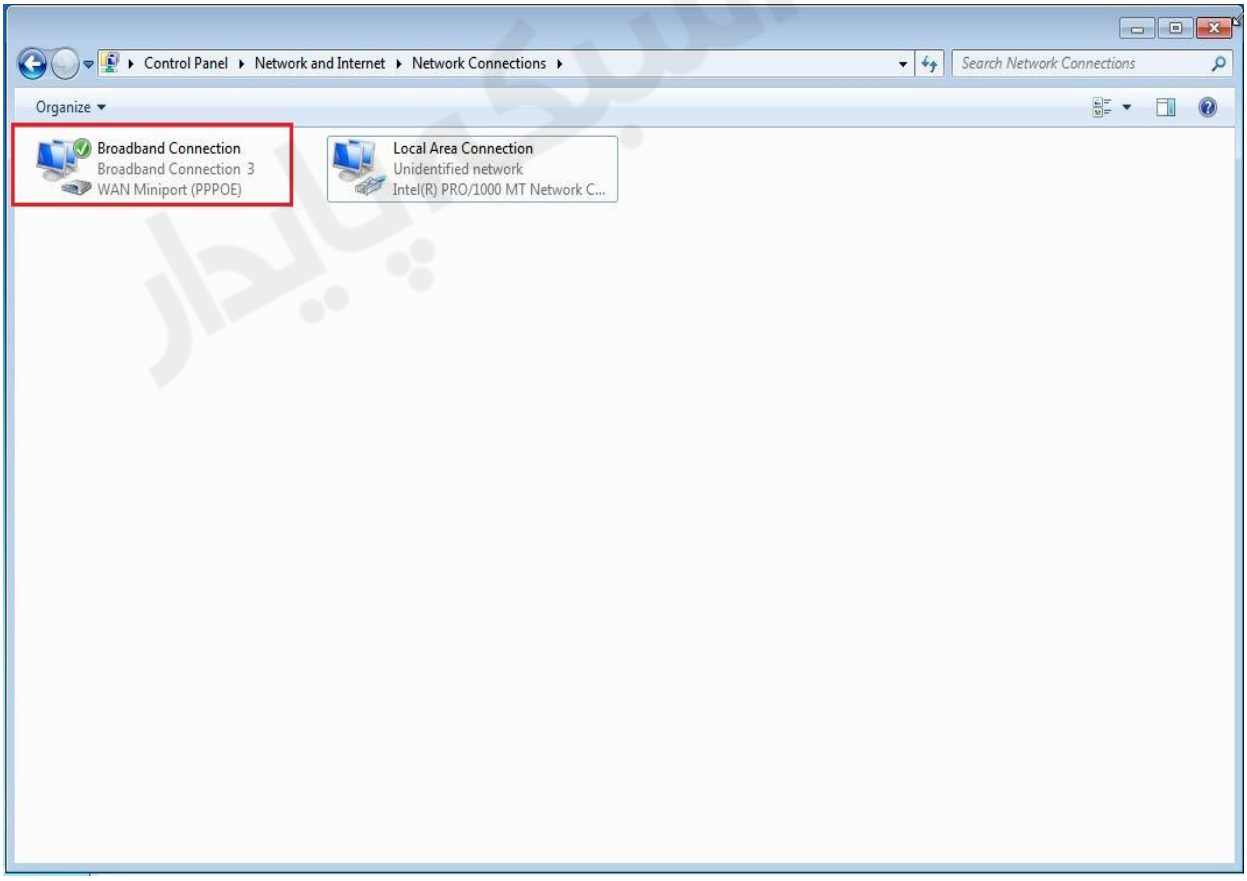


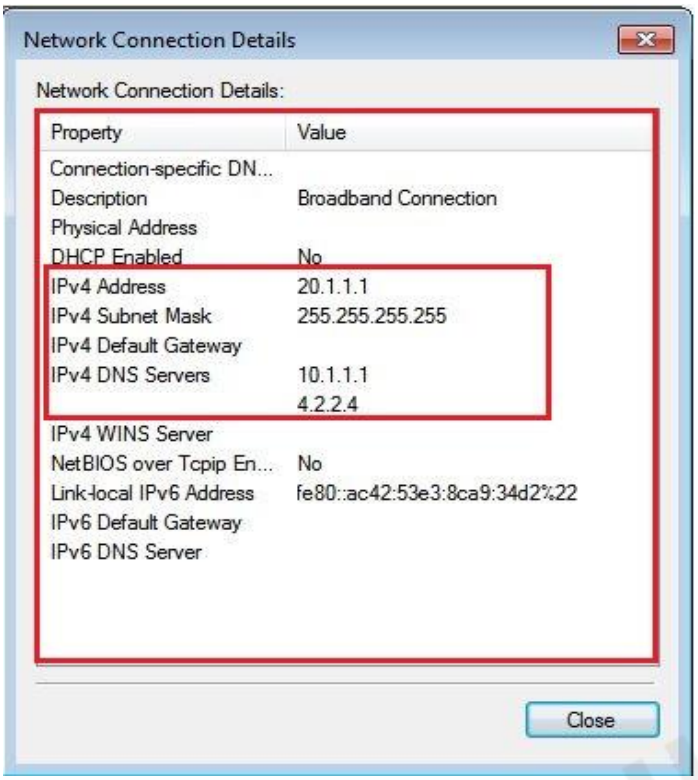
یوزرنیم و پسوردی که در روتر تعریف کردیم را وارد می کنیم.





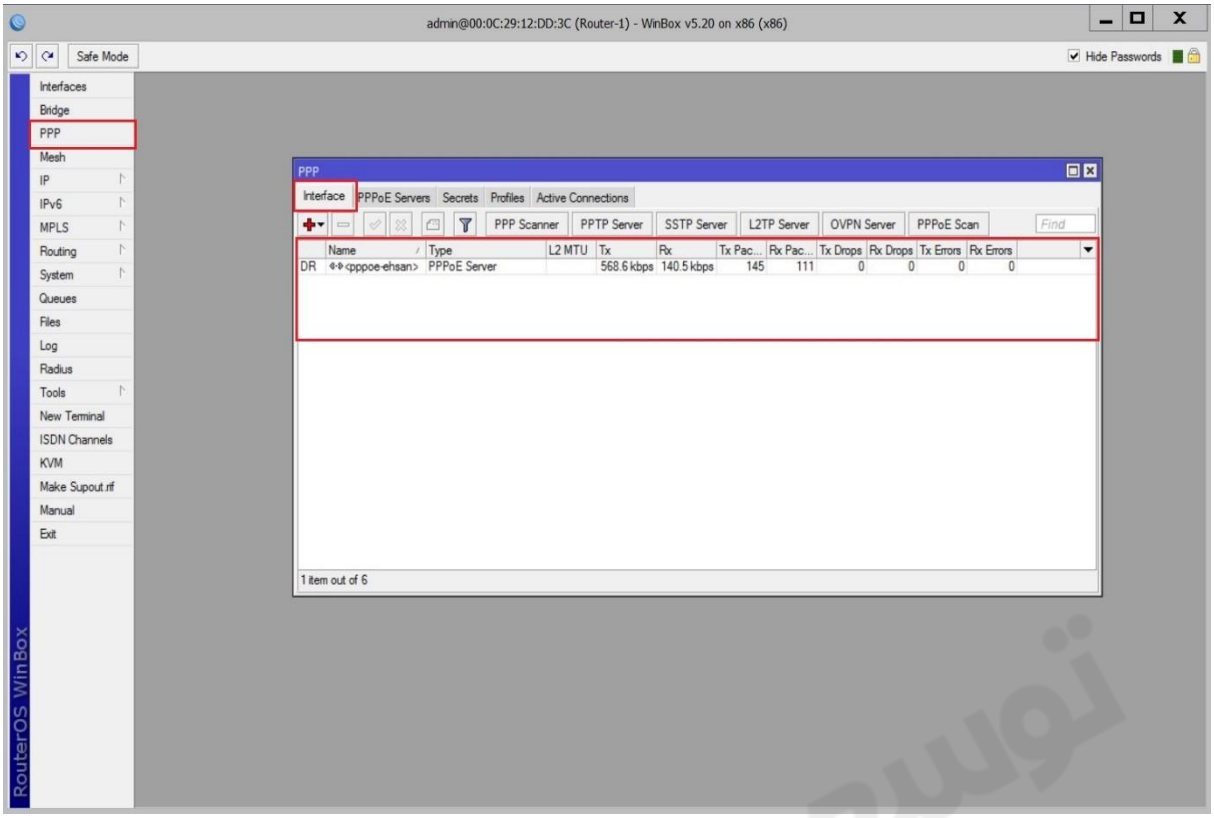
با این تنظیمات Connection ی که در عکس زیر مشاهده می کنید اضاف می شود.





کلاینت با **Remote Address** ی که در روتر تعریف کردیم به اینترنت دسترسی پیدا کرده است.

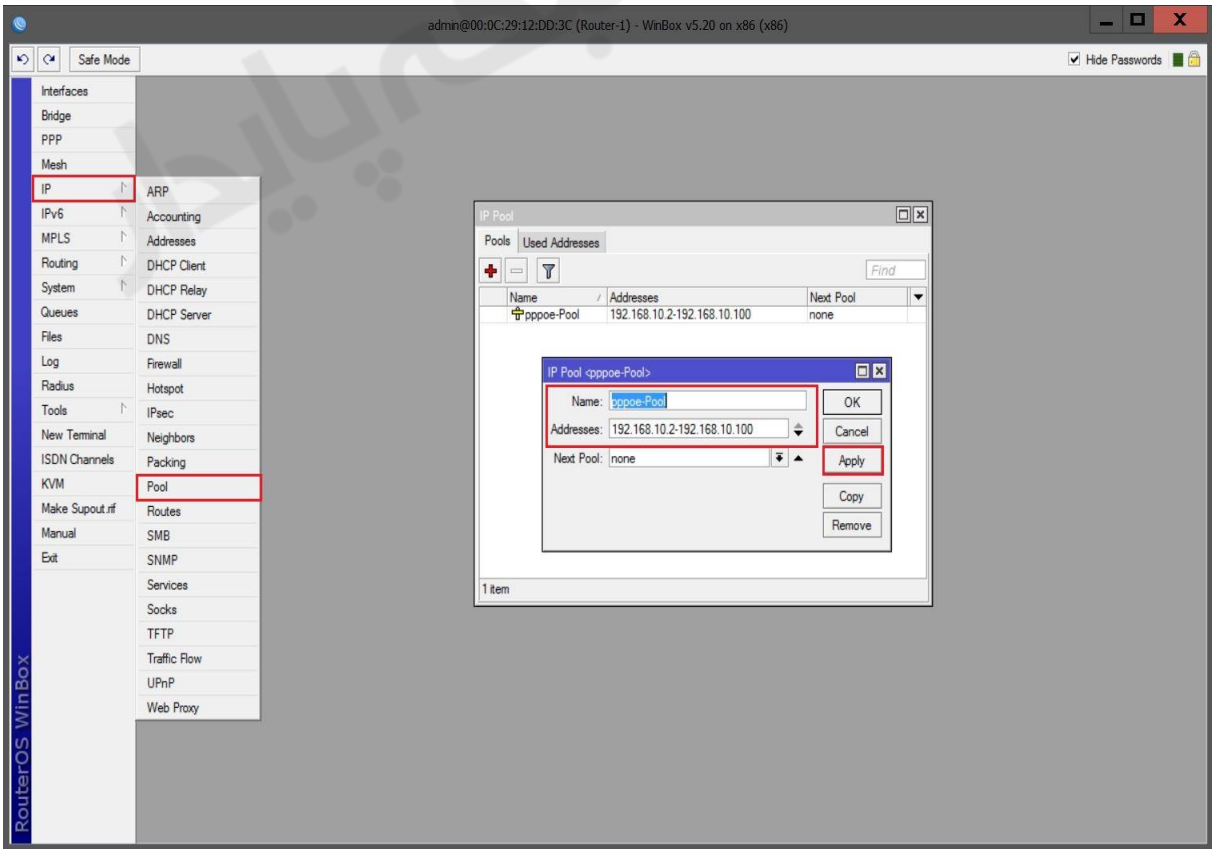
وقتی کاربر به روتر وصل می شود بر روی روتر یک اینترفیس ایجاد می شود و وقتی **disconnect** می شود این اینترفیس حذف می شود.



در این روش اگر تعداد کلاینت ها زیاد باشد کار وقت گیری است برای اینکار باید برای Remote Address یک Pool تعریف کنیم.

برای اینکار از منوی اصلی گزینه IP و از زیرمنوی باز شده Pool را انتخاب می کنیم.

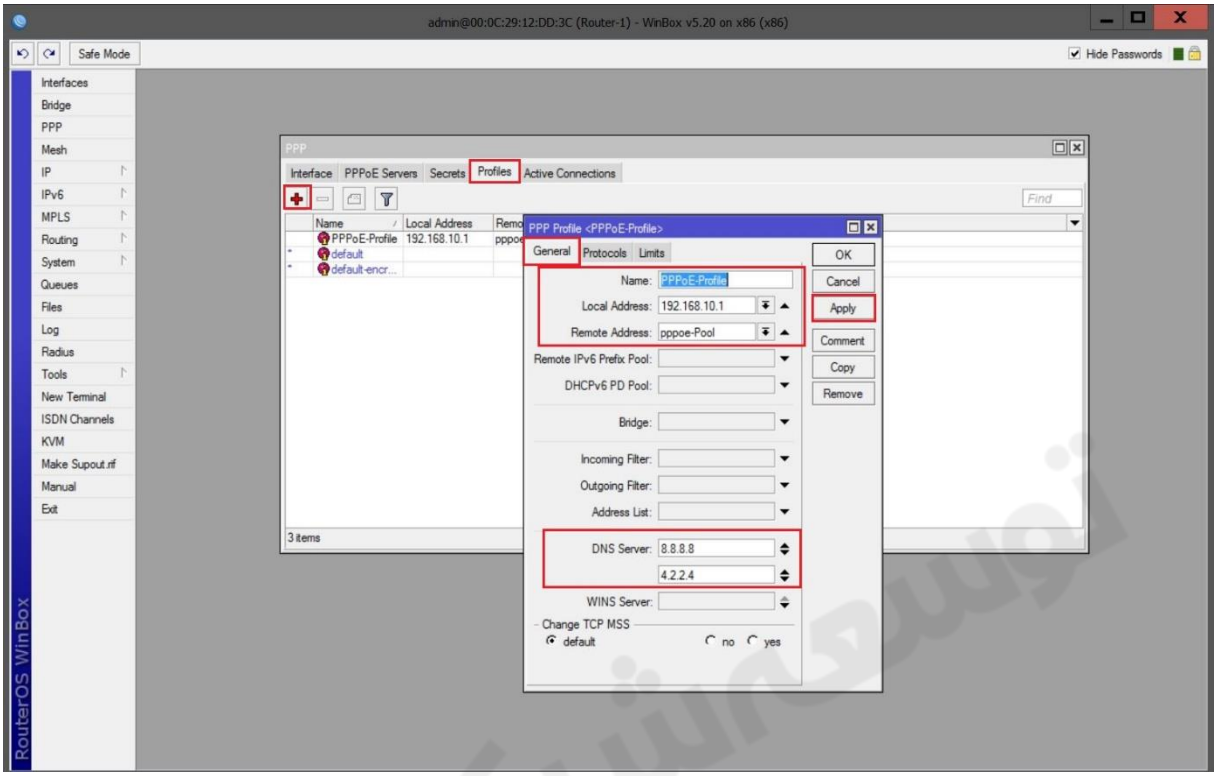
Address : رنج IP که می خواهیم به کلاینت ها داده شود را انتخاب می کنیم.



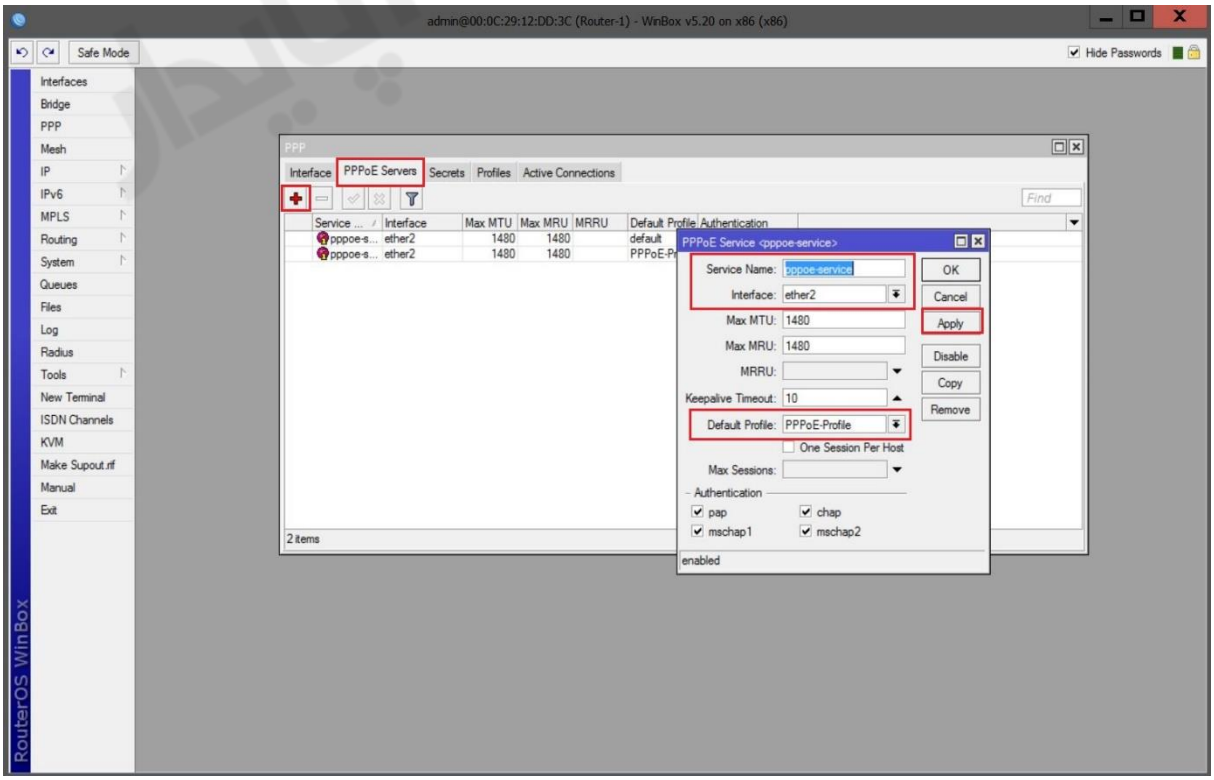
ایجاد Profile :

از تب Profiles برروی Add کلیک می کنیم.

در قسمت Remote Address باید Pool ی که تعریف کردیم را انتخاب کنیم.در صورتی که در شبکه DNS Server داشته باشیم آدرس IP آن را وارد میکنیم در غیر این صورت می توانیم از DNS سرورهای Public در دنیای اینترنت استفاده کنیم.

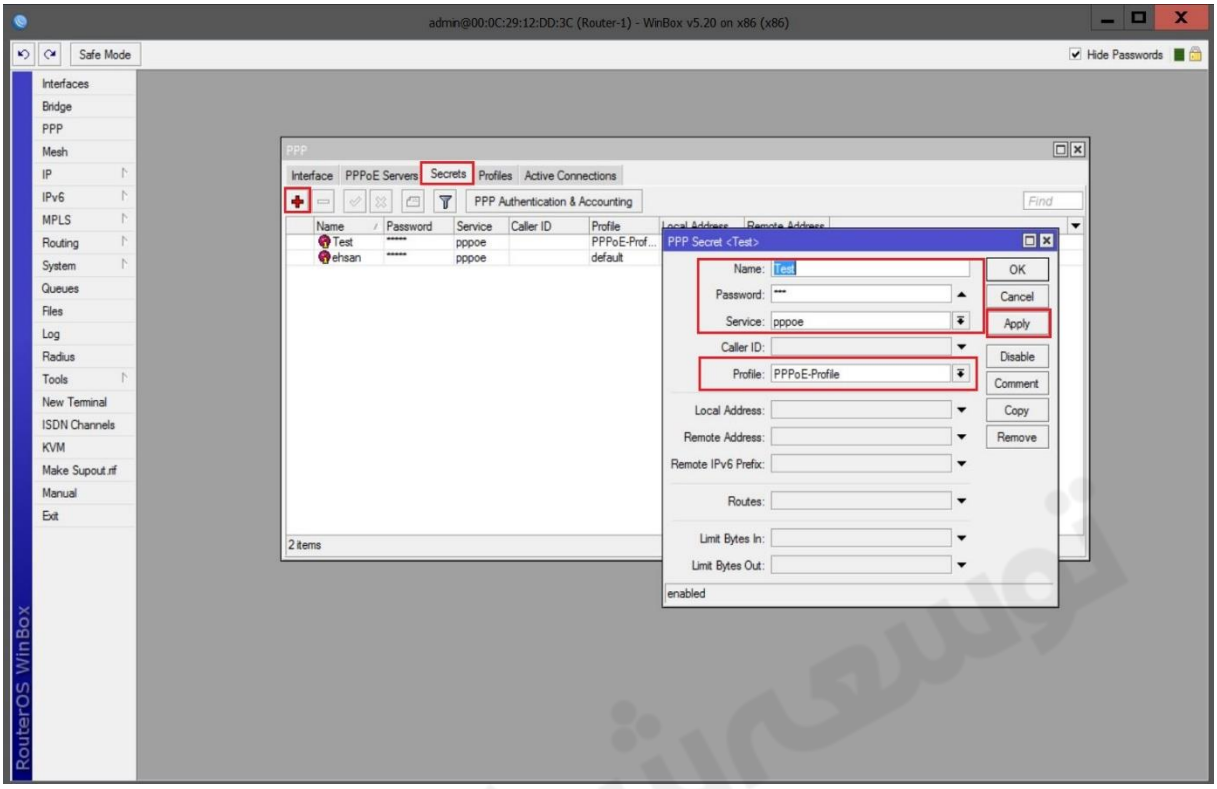


در مرحله بعد باید از بخش PPPoE Server برروی Add کلیک کرده و Default Profile را برابر با پروفایلی که در مرحله قبل ایجاد کردیم قرار دهیم.

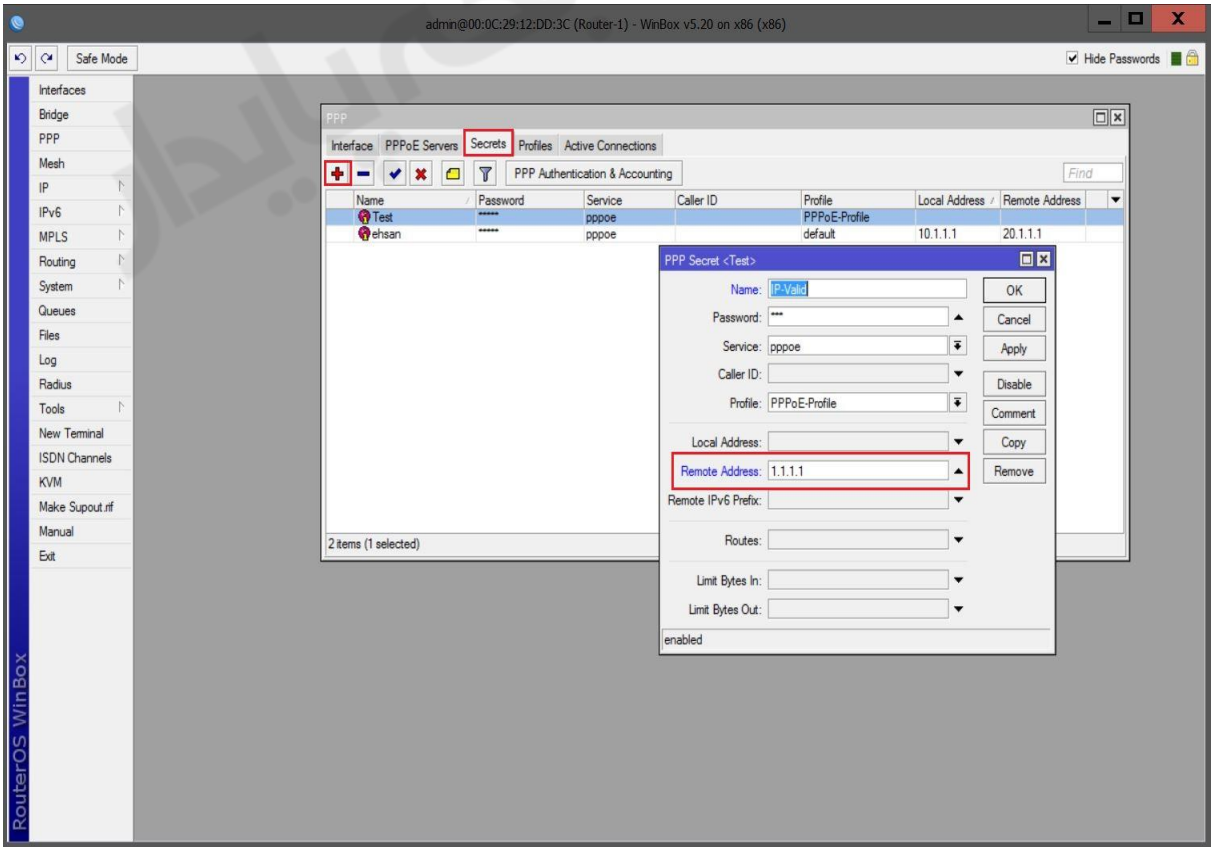


تعریف Acounting برای Userها :

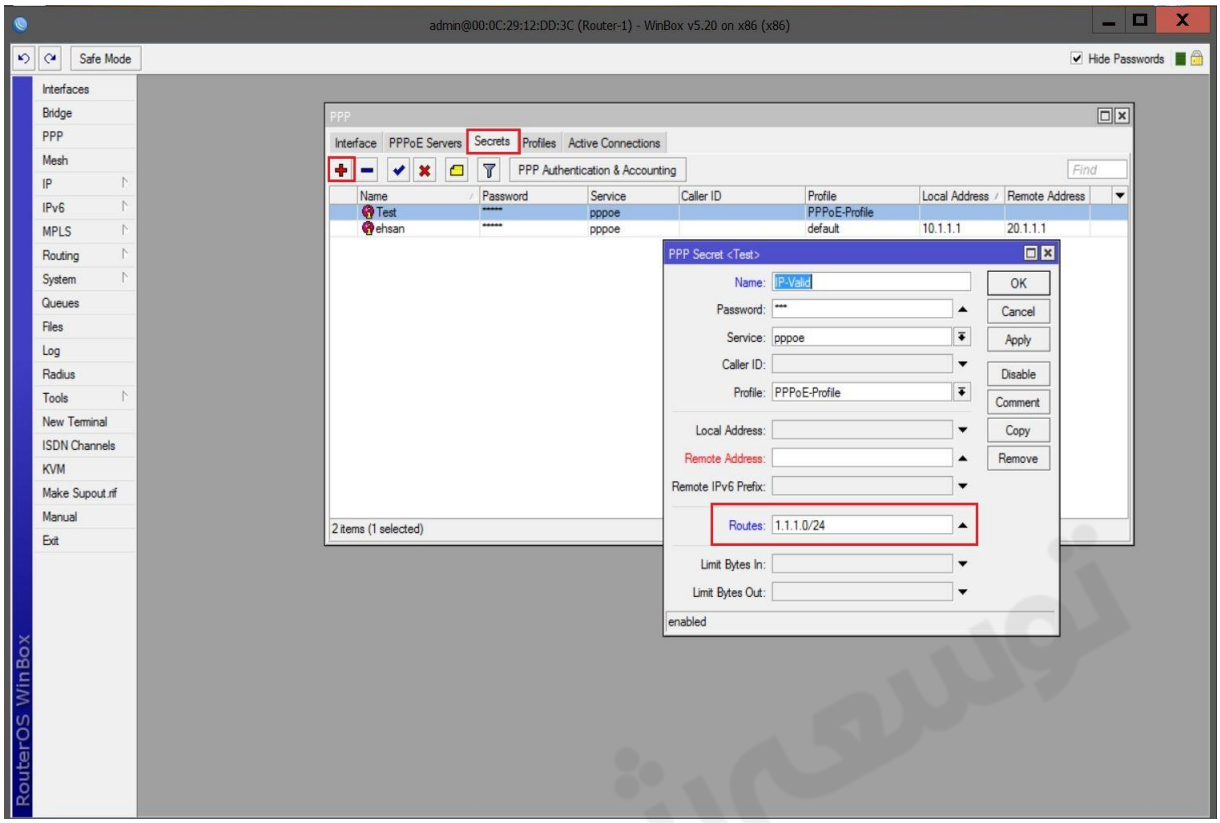
از تب Secrets بر روی Add کلیک کرده و از پنجره باز شده یوزرنیم و پسورد برای کاربرتعریف می کنیم و Profile را برابر با پروفایلی که از قبل ایجاد کردیم قرار میدهیم.



***نکته ۱ : اگر کاربری در خواست IP Valid داد این IP را در قسمت Remote Address وار د میکنیم :**

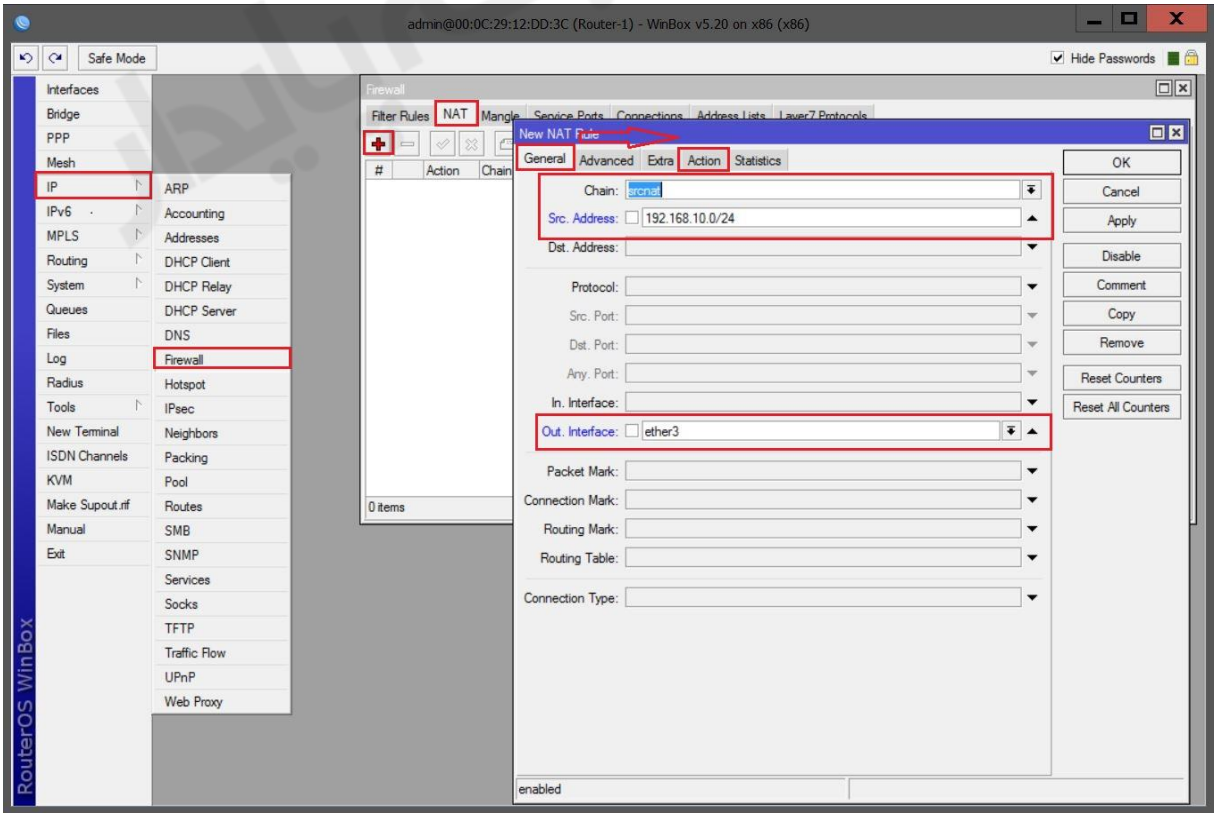


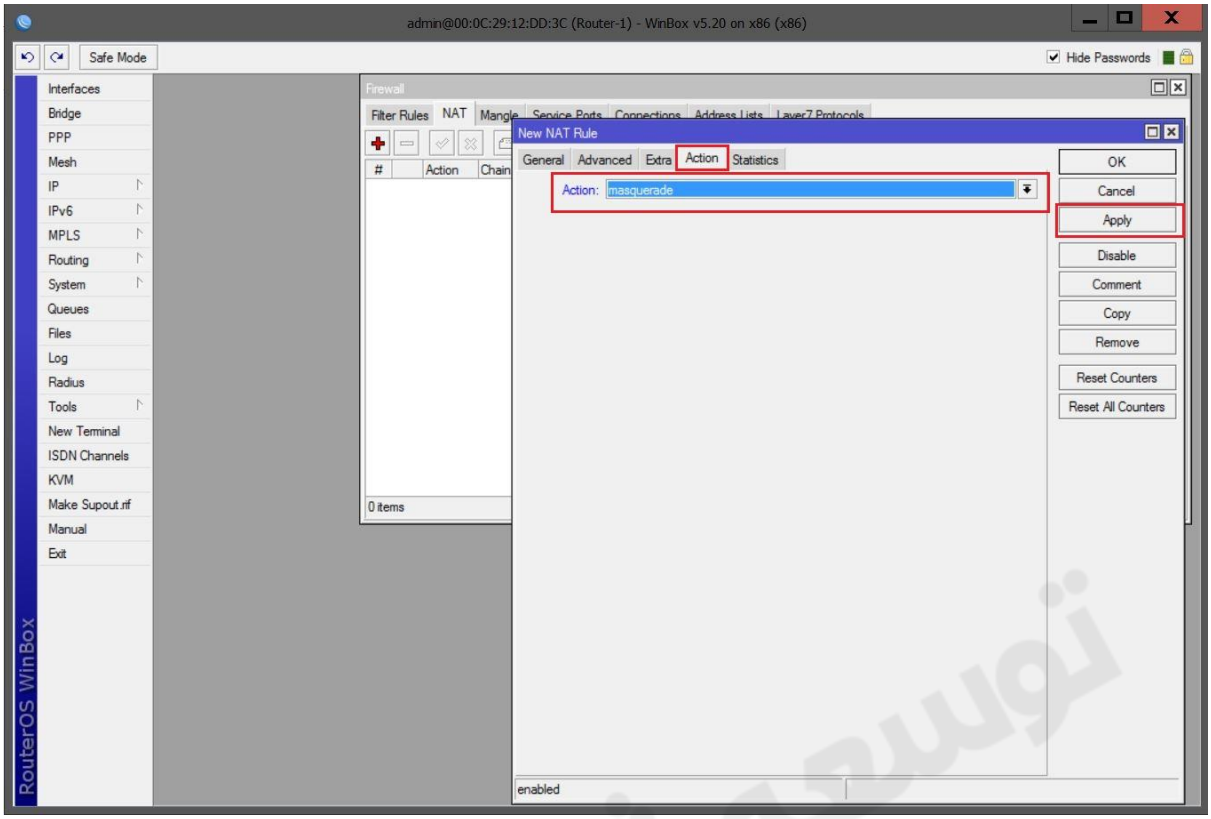
***نکته ۲ : اگر کاربر درخواست چندین IP Valid داشت و یا یک رنج IP درخواست داد دیگر نمی توانیم این IP ها را در قسمت Remote Address وارد کنیم و باید این رنج IP ها را در قسمت Routes وارد می کنیم.**



***نکته ۳ : Remote Address و Routes نسبت به Profile ارجعیت دارد.**

ایجاد Nat برای دسترسی کلاینت ها به اینترنت :





فصل دوازدهم : PPTP VPN Server

VPN(Virtual Private Network)

میکروتیک را می توان به عنوان یک **Vpn Server** در شبکه مورد استفاده قرار داد.

Vpn بطور کلی فرایندی است که توسط آن از **Vpn Client** به **Vpn Server** یک تانل امن (**Secure Tunnel**) برقرار می شود.این **Tunnel** مانند یک کابل شبکه مجازی از کلاینت به **Vpn Server** یک ارتباط امن را ایجاد می کند و از این به بعد داده ها از درون این **Connection** منتقل می شوند.

کلاینت می تواند از لحاظ جغرافیایی نزدیک **Vpn Server** باشد (در یک **Lan** باشد) و یا از **Vpn Server** دور باشد (بطور مثال در یک شهر و یا کشور دیگری باشد) که در این حالت برای برقراری ارتباط آنها بر روی بستر اینترنت **Connection** برقرار می شود.

شرکت ها از تکنولوژی **Vpn** برای این موضوع استفاده می کنند که شعبه های مختلف آنها بتوانند به منابع دیگری دسترسی داشته باشند.بطور مثال فرض کنید که در شعبه مرکزی یک شرکت ، یک سرور اتوماسیون اداری وجود داشته باشد ، حال شعبه های مختلف این شرکت از لحاظ جغرافیایی دورتر از شعبه مرکزی هستند می توانند با برقراری اتصال **Vpn** از این منابع استفاده کنند.

Tunnel در **Vpn** با استفاده از پروتکل های مختلفی پیاده سازی شود :

- **PPTP**
- **L2TP**
- **IPIP**
- **EOIP**
- **GRE**
- **و ...**

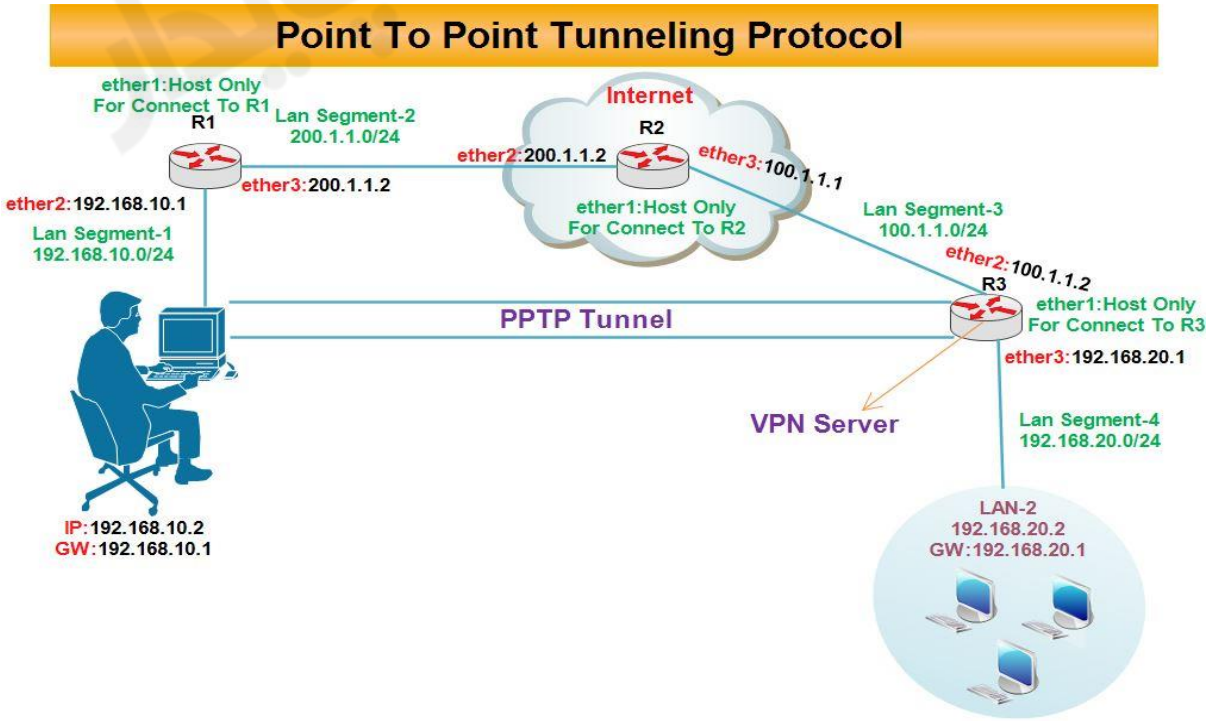
برای اینکه این **Connection** ها (ارتباط ها) برقرار شود ، کلاینت و سرور باید پروتکل **Tunneling** یکسانی مورد استفاده قرار دهند.

در ادامه به تفکیک ، این پروتکل ها را بررسی می کنیم.

PPTP (Point To Point Tunneling Protocol)

PPTP از پروتکل **PPP** (**Point to Point Protocol**) برای **Encapsulation** داده ها استفاده می کند.به عبارتی چنانچه **Tunnel** از نوع **PPP** (نقطه به نقطه یا نظیر به نظیر) باشد ، داده ها درون بسته **PPP** قرار می گیرد و فرستاده می شود.

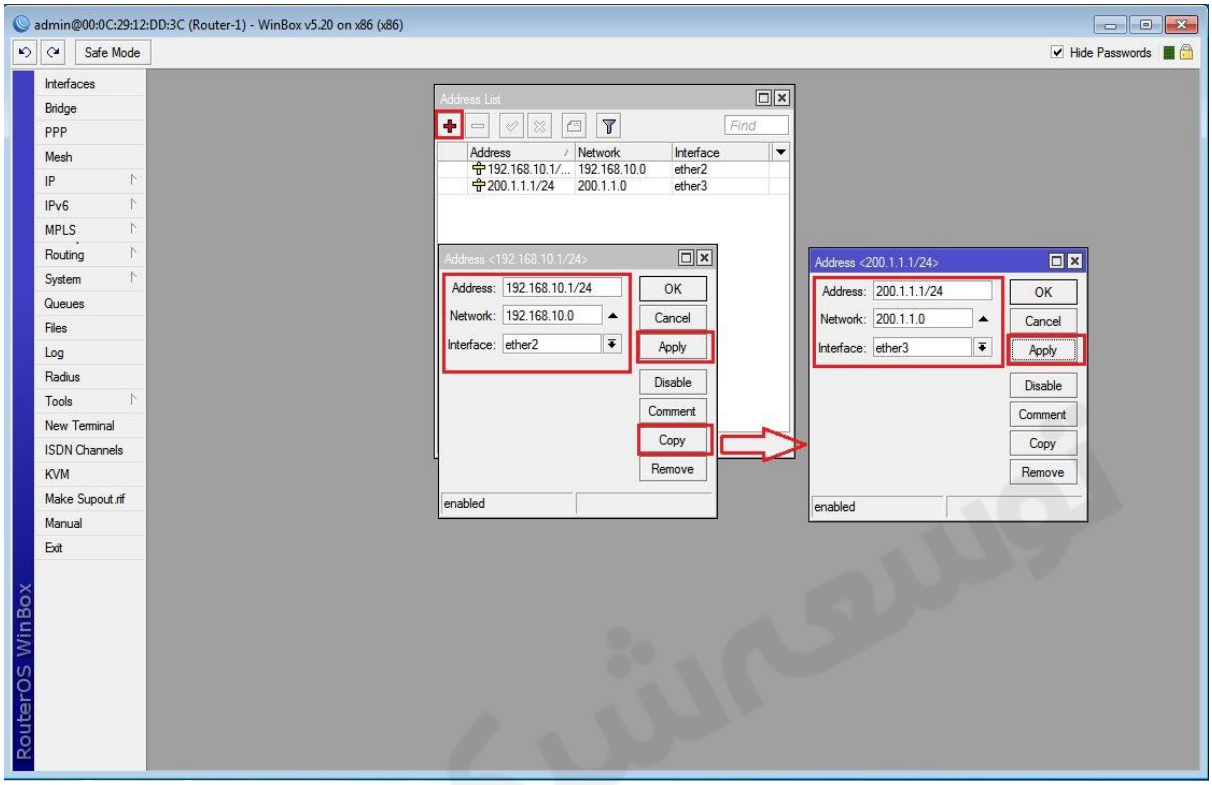
سناریو ۱ : هدف از این سناریو پیاده سازی پروتکل **PPTP** می باشد.



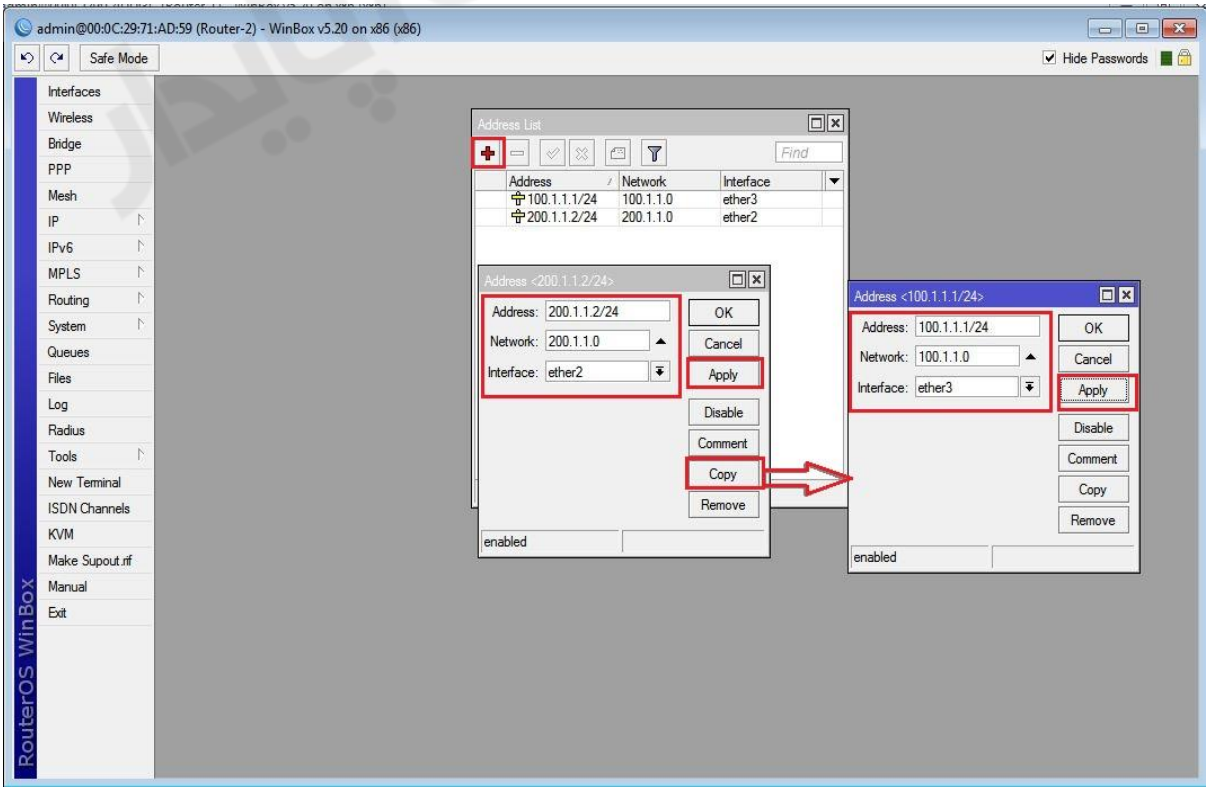
در این سناریو ، کاربر از طریق اینترنت یک کانال امن به بصورت نقطه به نقطه با استفاده از پروتکل **PPTP** به مسیریاب (روتر **R3**) موجود در شبکه دیگر برقرار می کند و از این طریق به شبکه محلی مقصد (**Lan-2**) دسترسی خواهد داشت.

انتساب IP به کارت های شبکه روترها :

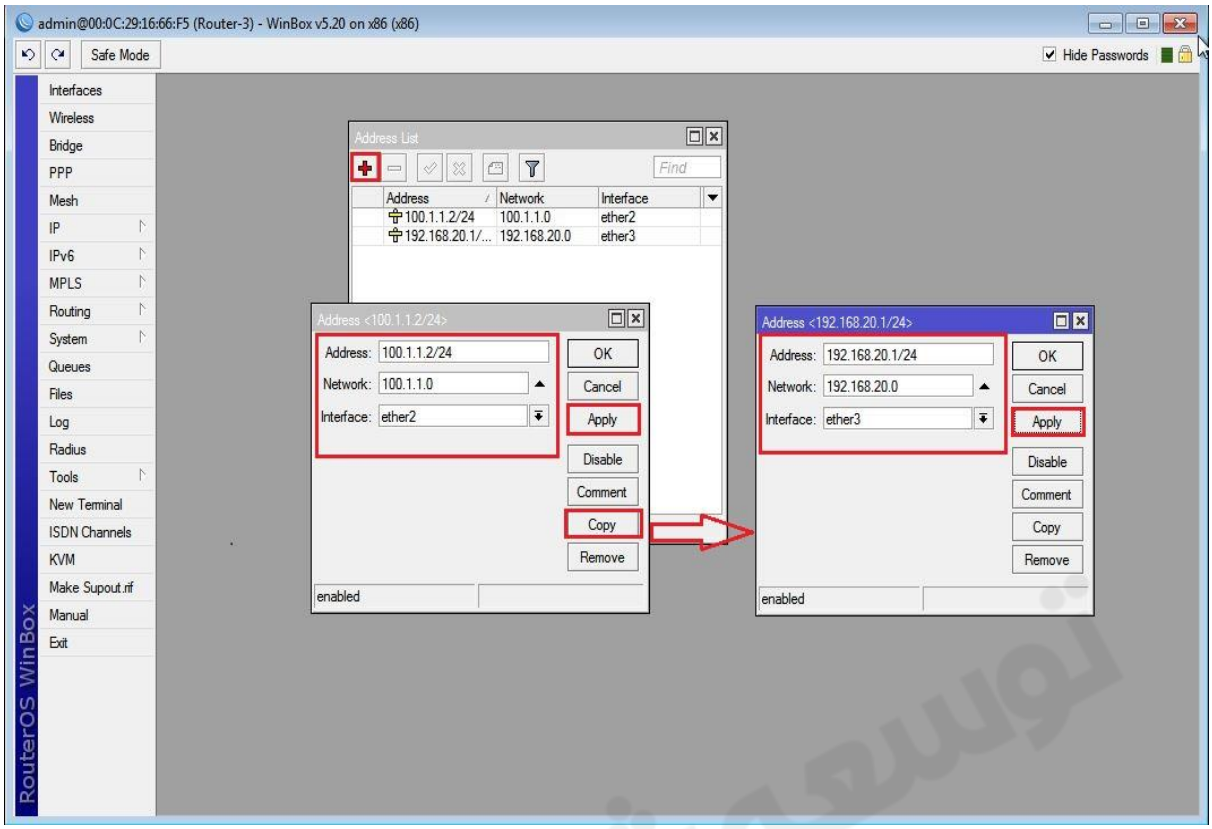
روتر R1 :



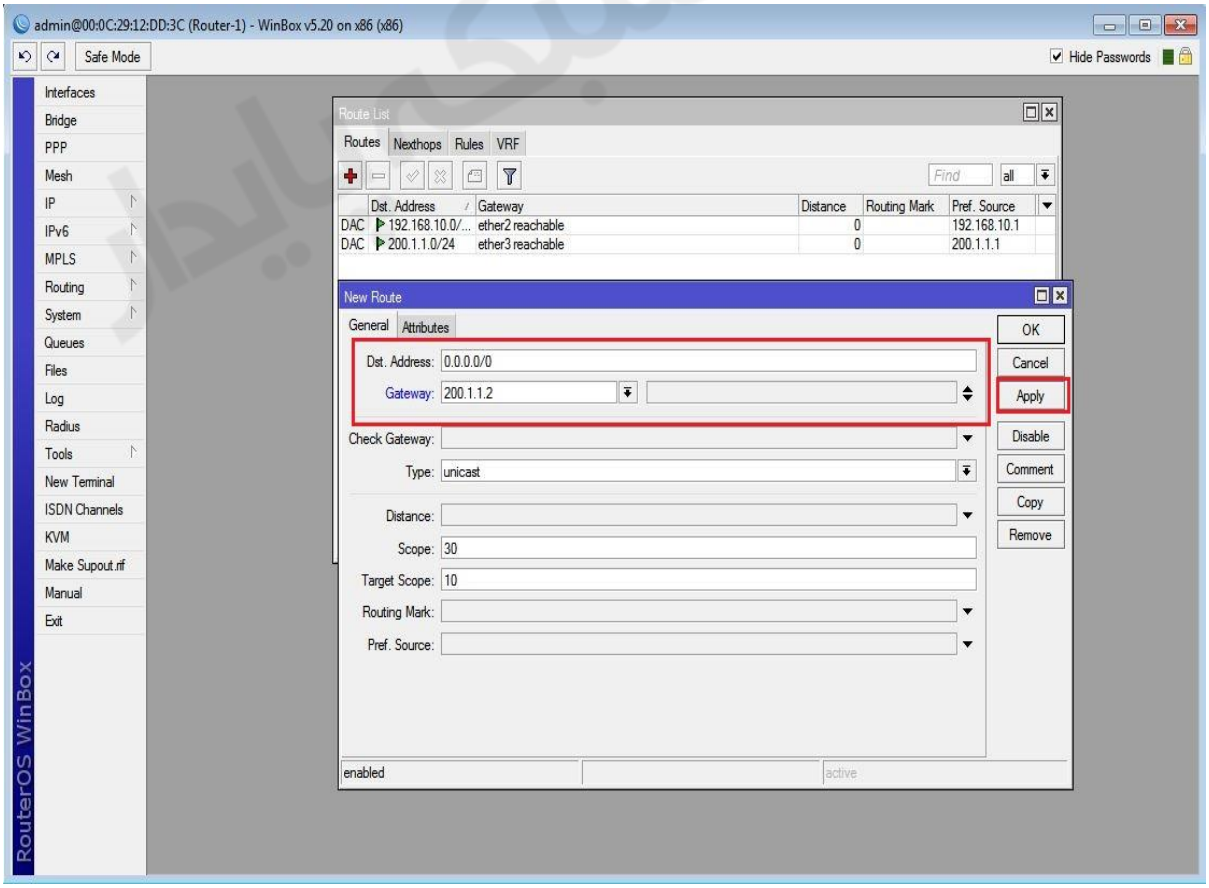
روتر R2 :



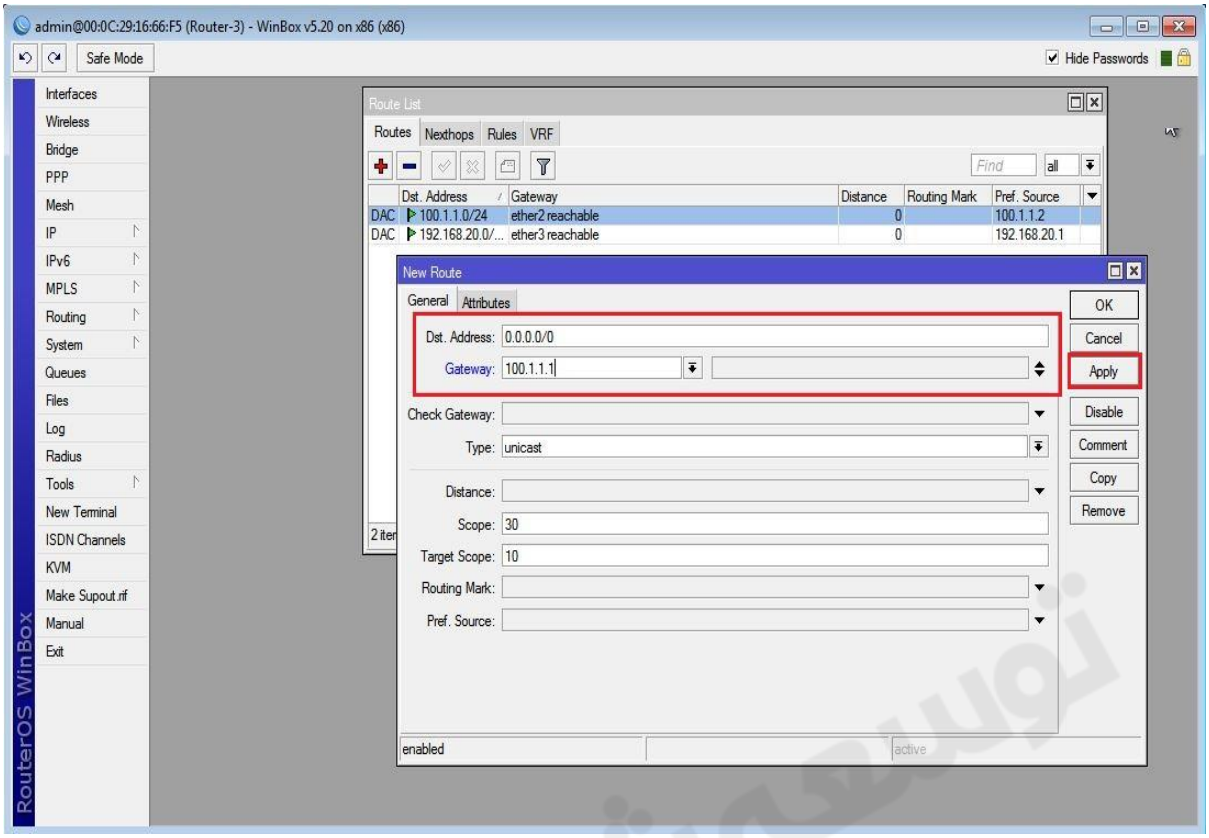
روتر **R3**:



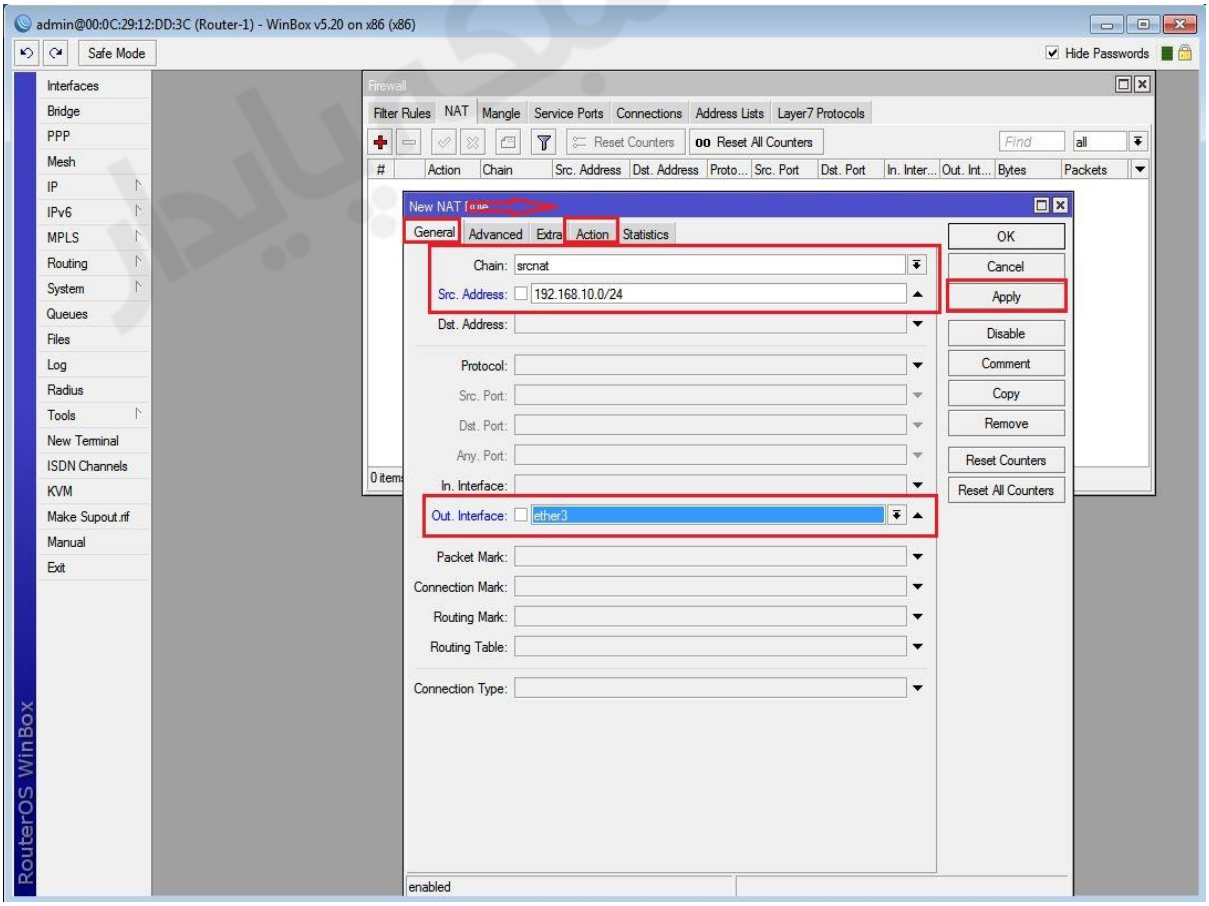
تعریف **Default Route** در روتر **R1**:

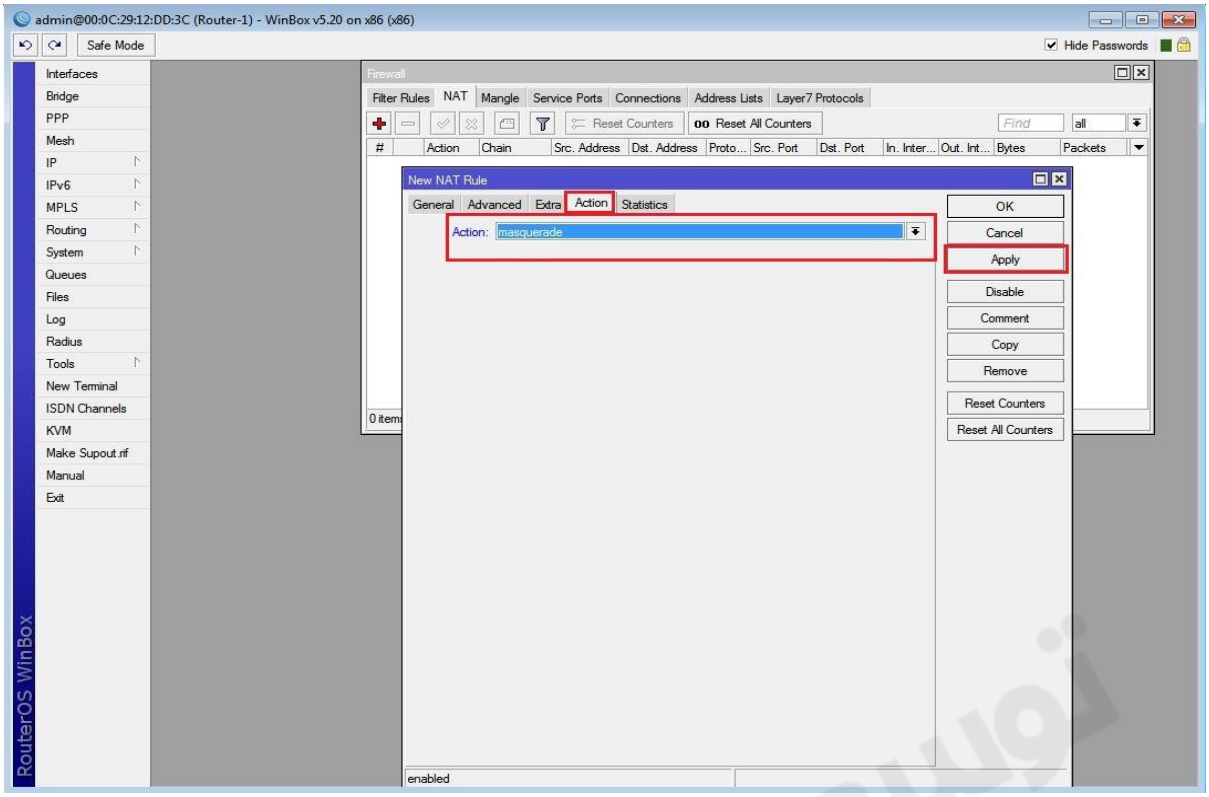


تعریف **Default Route** در **R3** :



ایجاد Nat در روتر R1 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.

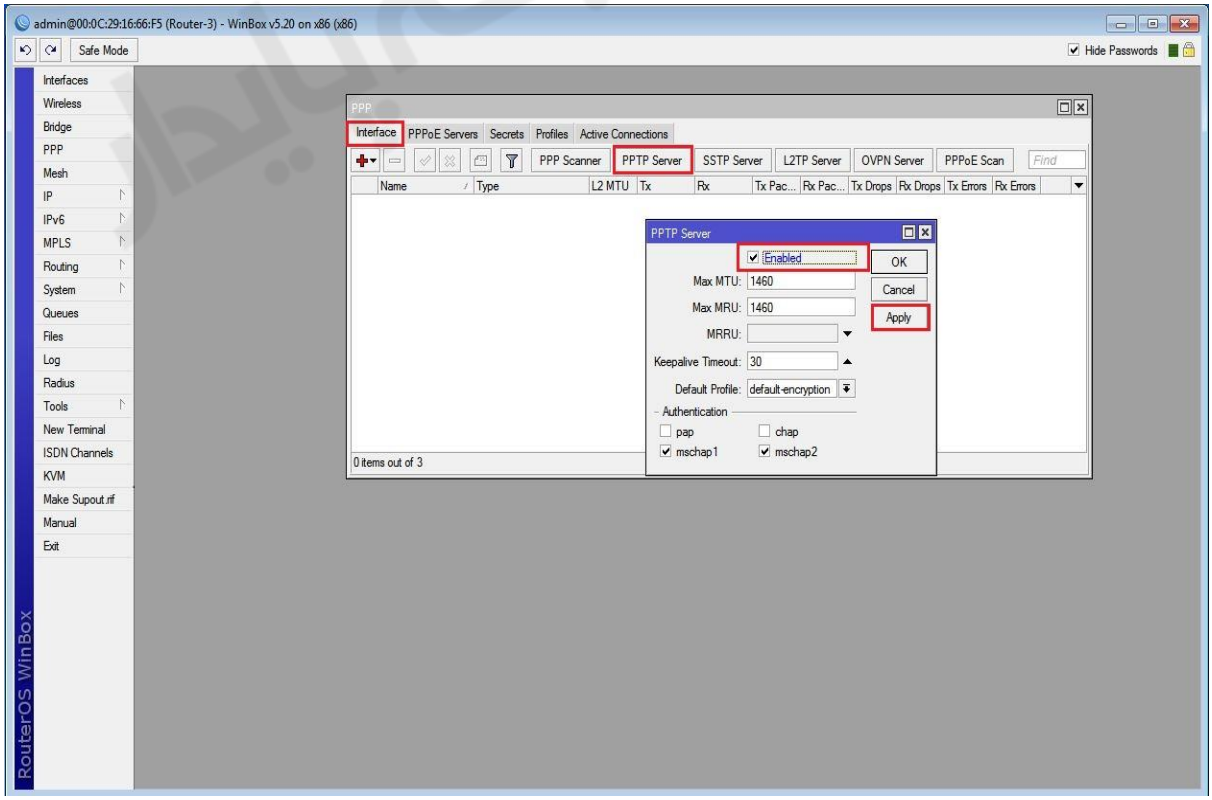




برای تبدیل میکروتیک به Vpn Server در قدم اول باید این قابلیت را برروی آن فعال کنیم و سپس تنظیمات مربوطه ، برای اتصال کاربران به این سرور را تعیین می کنیم.

فعال سازی سرویس PPTP :

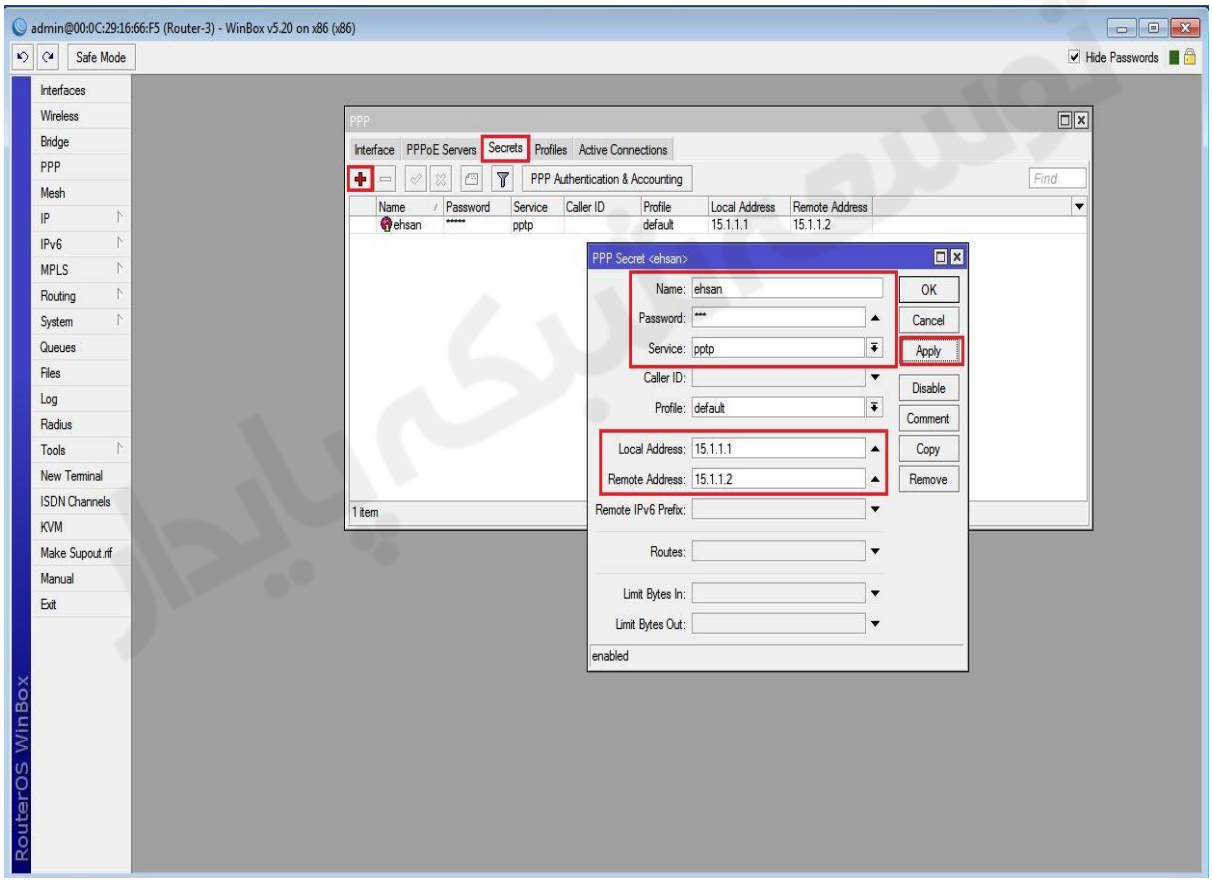
برای فعال سازی این سرویس از منوی اصلی PPP را انتخاب کرده در پنجره باز شده از تب Interface گزینه PPTP Server را انتخاب و تیک گزینه Enable را می زنیم.



برای پیاده سازی **tunnel** ابتدا سیستم کلاینت ، درخواست برقراری ارتباط را به سرویس ارائه می دهد ، سپس سرور معیارهای احراز هویت کلاینت ها که شامل نام کاربری و رمز عبور می باشد را بررسی می کند و در صورت تصدیق صحت این موارد ارتباط برقرار می شود.
بنابراین در مرحله بعد باید تنظیمات مربوط به سرور که شامل موارد زیر می باشد را انجام دهیم :
تعریف نام کاربری و رمز عبور معتبر ، پروتکل مورد استفاده ، **IP** معتبری که کلاینت از طریق آن می تواند به شبکه مقصد متصل شود و همچنین **IP**ای که بعد از اتصال کلاینت ، به آن اختصاص داده می شود.

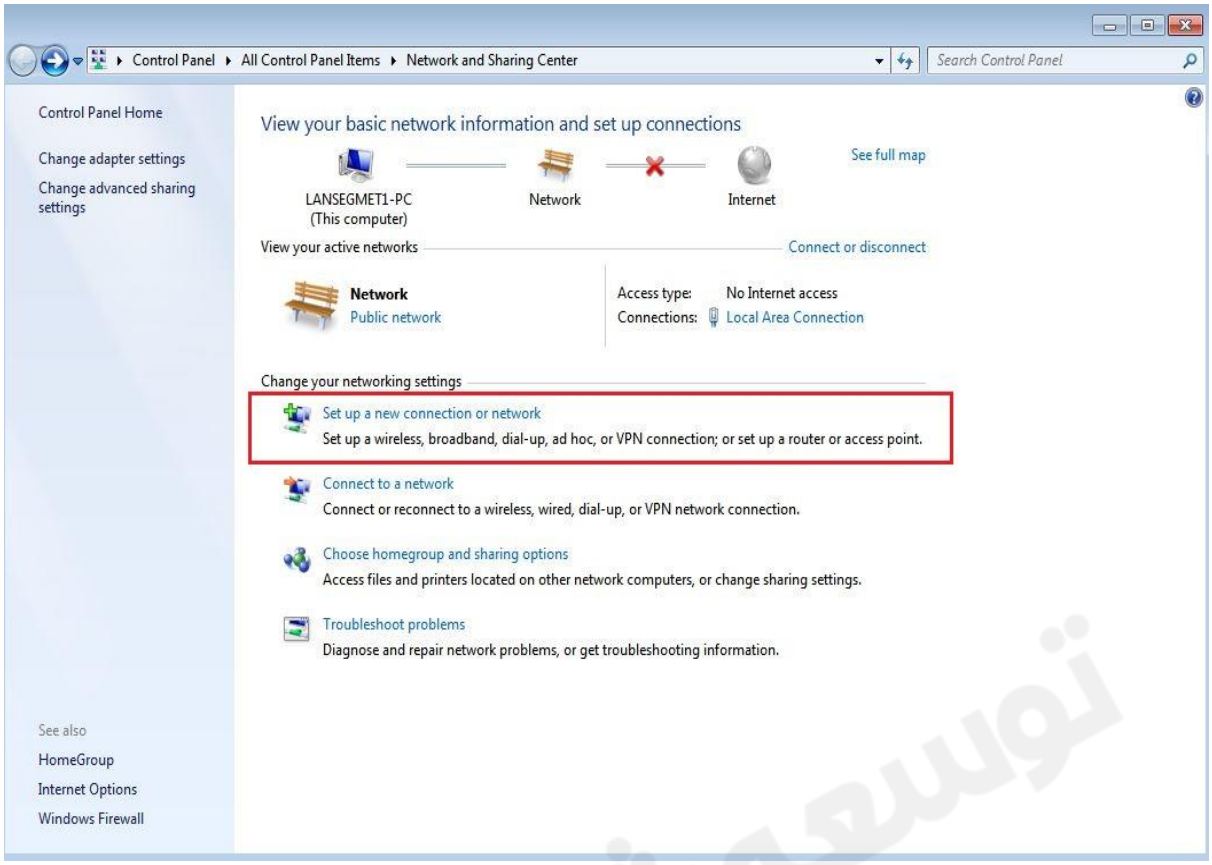
۱. **Name And Password** : نام کاربری و رمز عبور معتبری برای اتصال کاربران به **Vpn Server** را مشخص می کنیم.
۲. **Service** : پروتکلی که کلاینت ها می توانند توسط آن به **Vpn Server** متصل شوند را انتخاب می کنیم.
۳. **Local Address** : در این قسمت مشخص می کنیم که کلاینت ها از طریق کدام کارت شبکه مربوط به محدوده داخلی شبکه **Lan** دسترسی داشته باشد.به عبارتی **IP** کارت شبکه ای از میکروتیک را که می خواهیم بسته ها از طریق آن وارد **Lan** شوند.
۴. **Remote Address** : در این قسمت آدرس **IP**ای که به کلاینت بعد از اتصال به **Vpn Server** انتساب داده می شود را مشخص می کنیم.این **IP** هم می تواند از محدوده شبکه مقصد باشد و هم از محدوده ای غیر از شبکه مقصد.

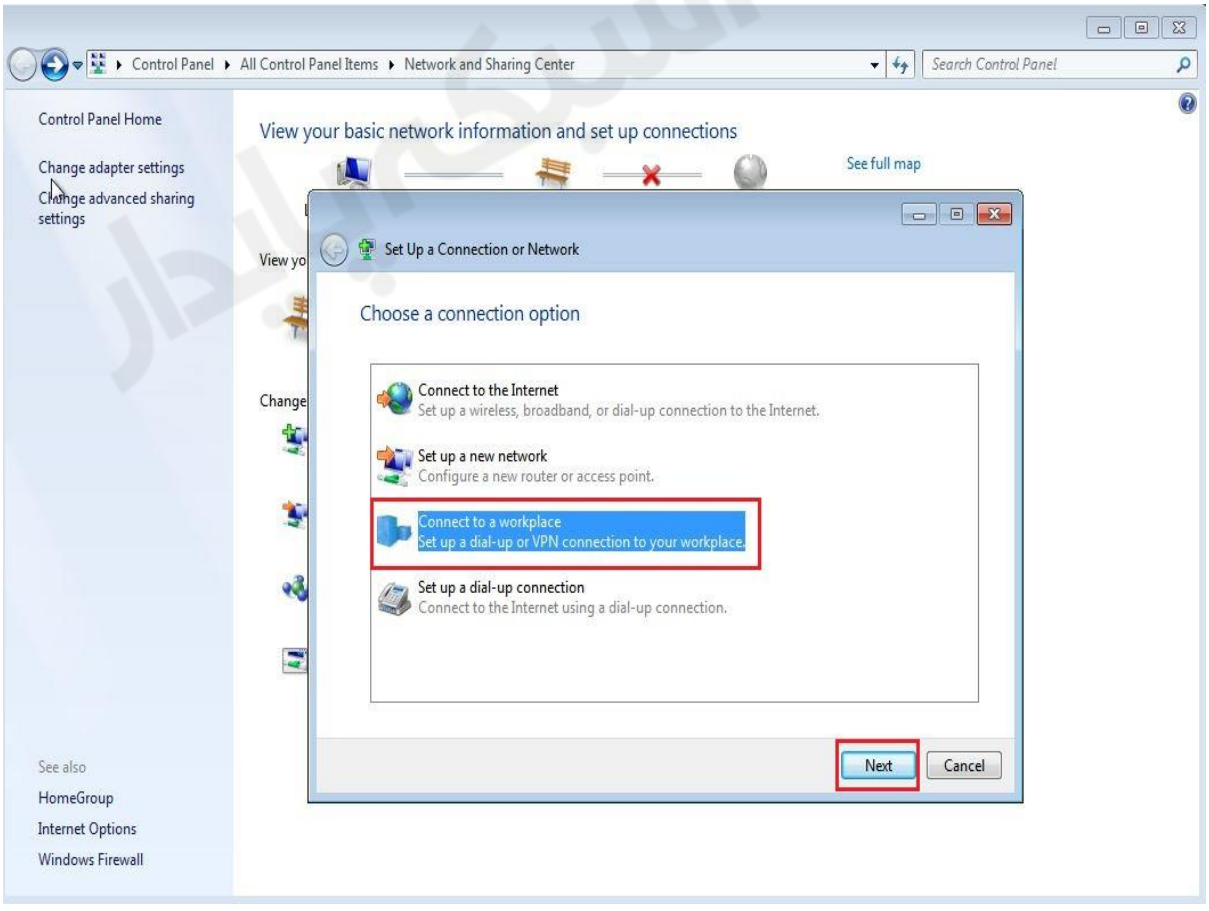
*نکته : در صورتی که این پارامتر را از محدوده **IP**های شبکه مقصد انتخاب شود مانند این است که کلاینت را درون شبکه مقصد آورده ایم.

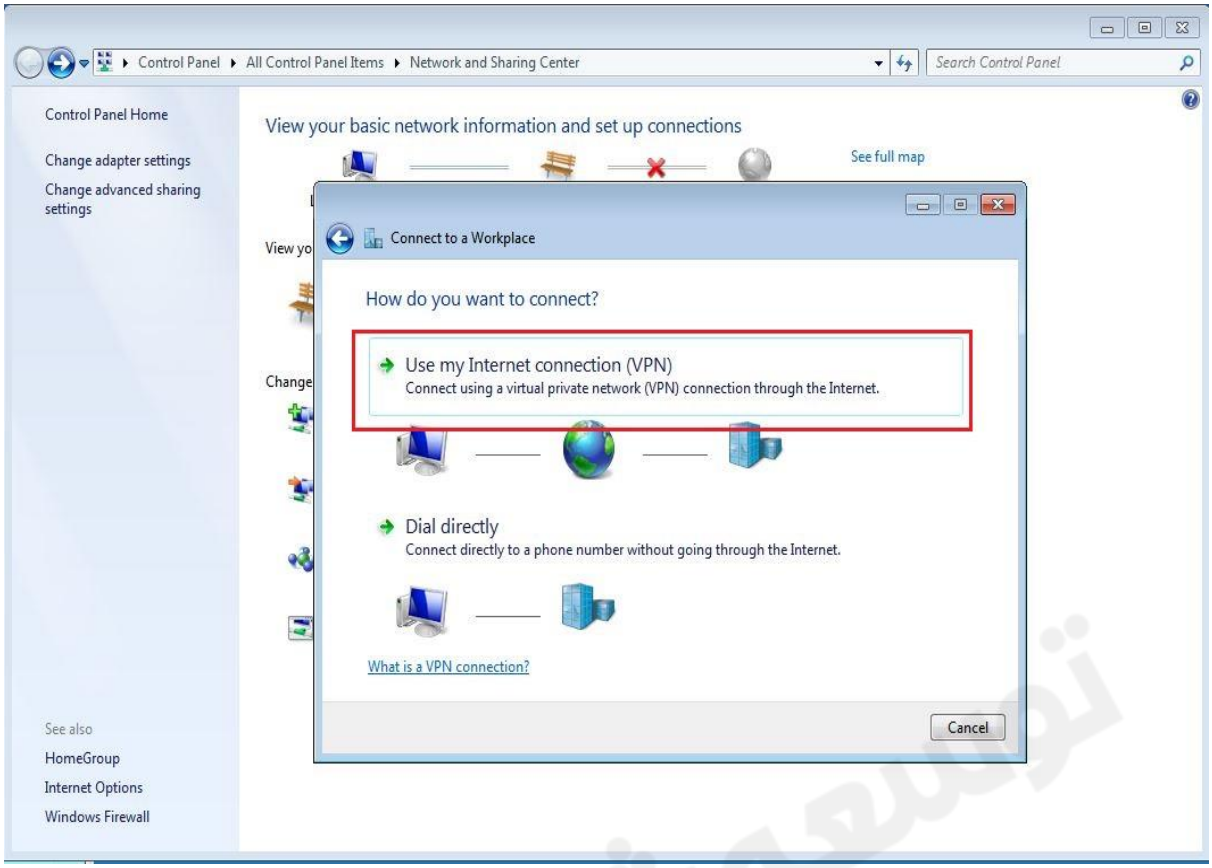


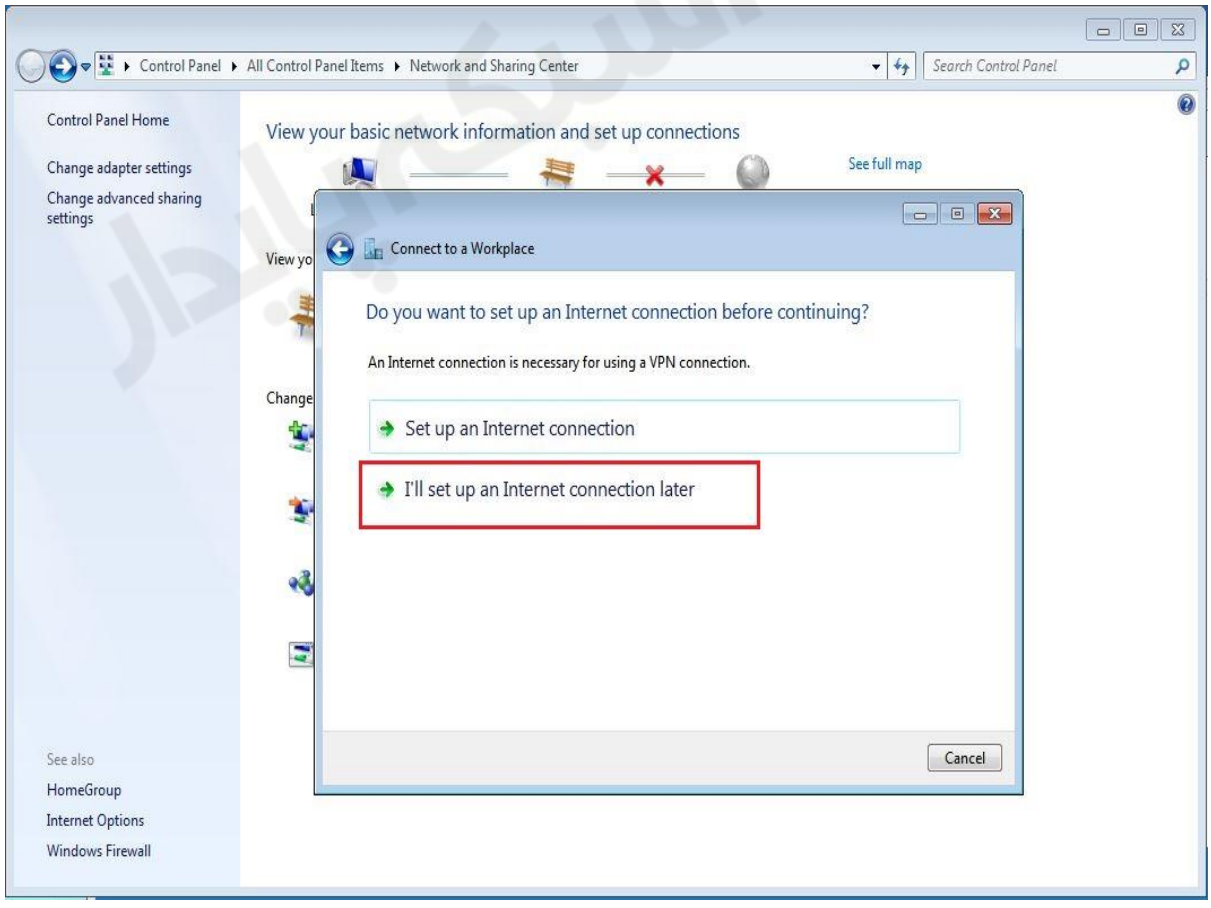
تنظیمات کلاینت :
طبق سناریو به کلاینت **IP** می دهیم.
تا اینجای کار با این تنظیمات هنوز ار تباط با شبکه **Lan-2** برقرار نیست.
در سیستم کلاینت باید یک **Vpn Connection** ایجاد کنیم برای اینکار به مسیر زیر فته :

Control Panel > Network and Sharing > Setup new Connection or network >

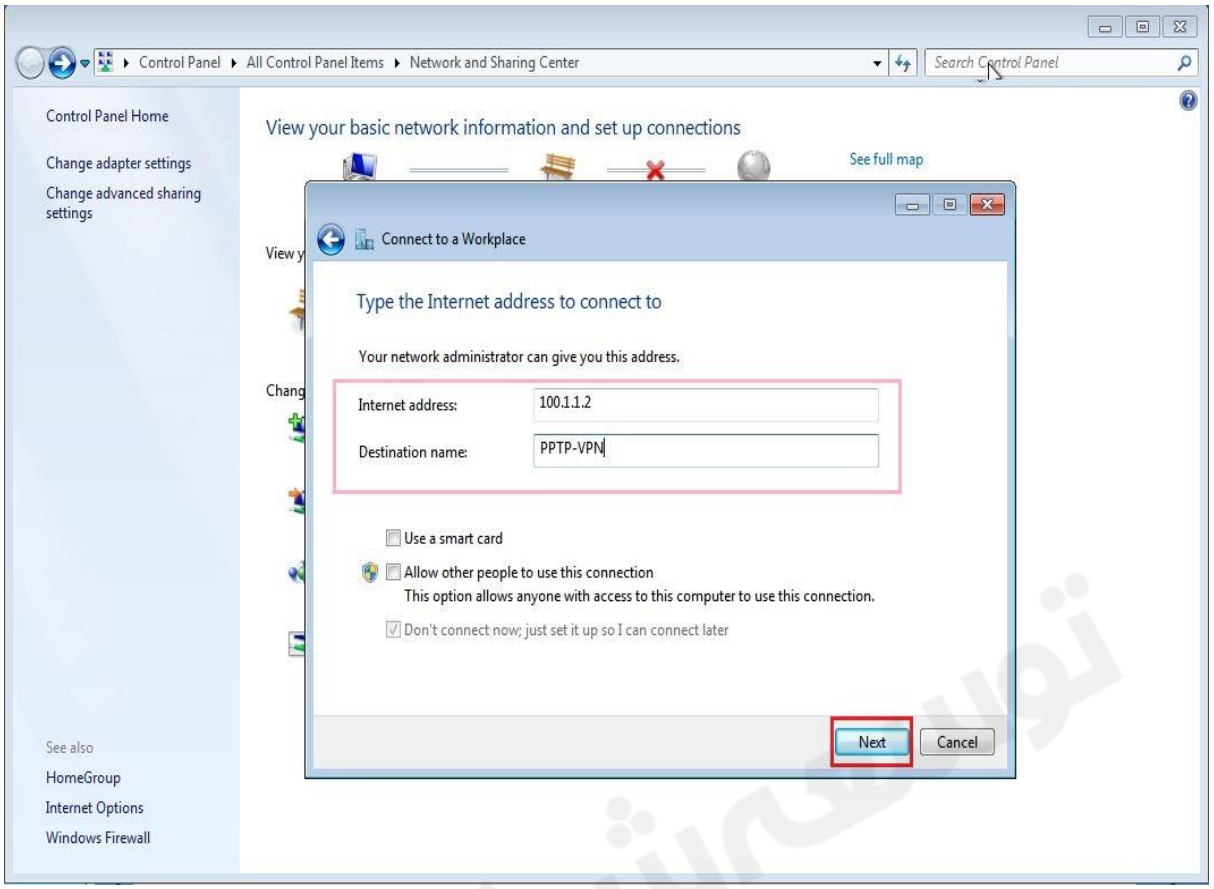

Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
LANSEGMET1-PC
(This computer)
Network
Internet
View your active networks
Connect or disconnect
Network
Public network
Access type: No Internet access
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
HomeGroup
Internet Options
Windows Firewall


Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a new network
Configure a new router or access point.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Set up a dial-up connection
Connect to the Internet using a dial-up connection.
Next
Cancel
See also
HomeGroup
Internet Options
Windows Firewall

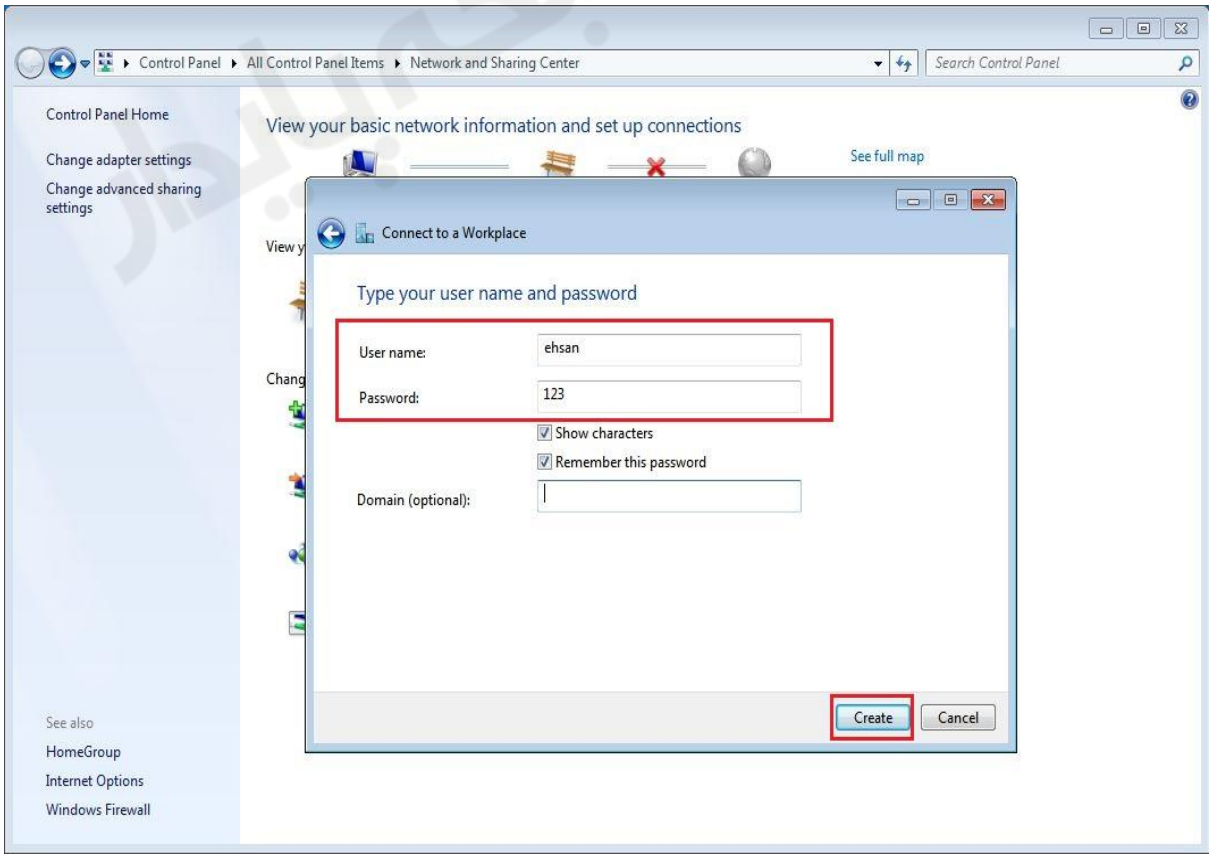

Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
Connect to a Workplace
How do you want to connect?
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.
Dial directly
Connect directly to a phone number without going through the Internet.
What is a VPN connection?
Cancel
See also
HomeGroup
Internet Options
Windows Firewall


Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
Connect to a Workplace
Do you want to set up an Internet connection before continuing?
An Internet connection is necessary for using a VPN connection.
Set up an Internet connection
I'll set up an Internet connection later
Cancel
See also
HomeGroup
Internet Options
Windows Firewall

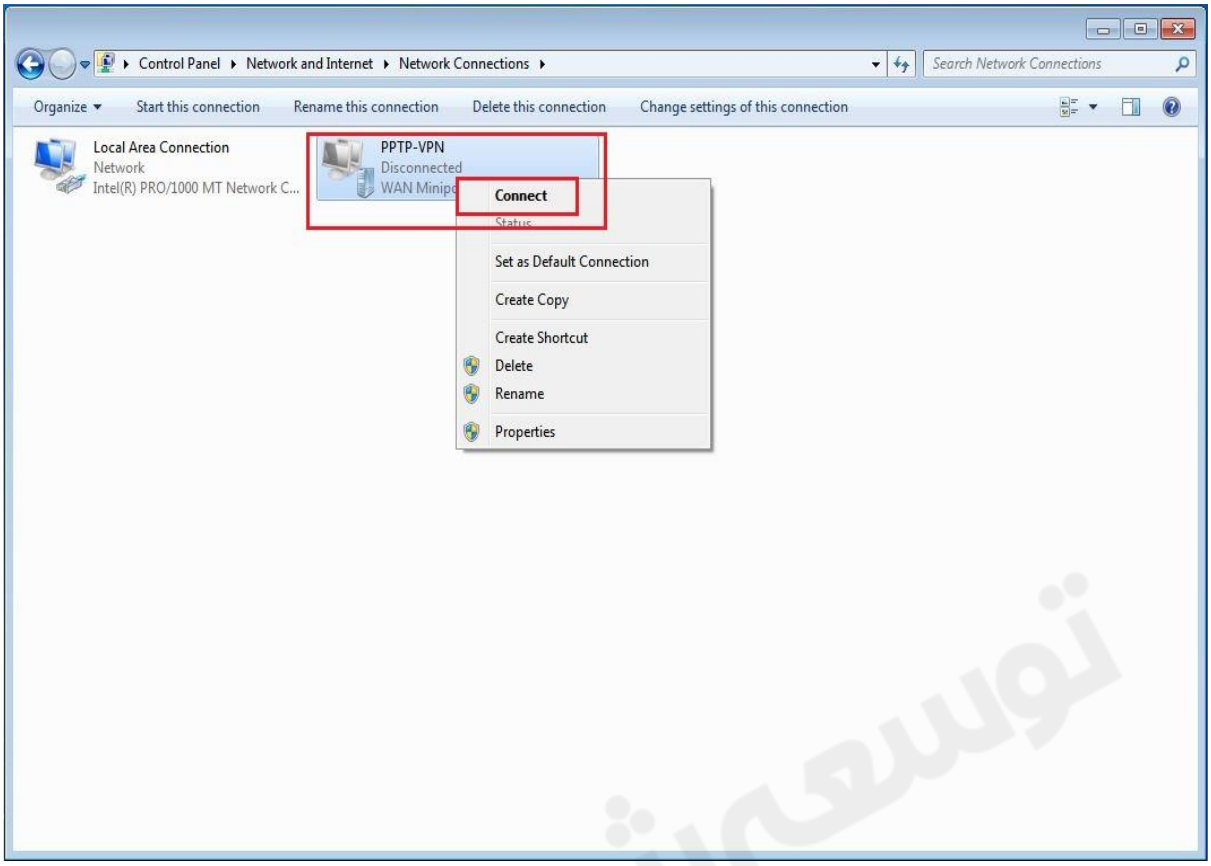
Internet Address : آدرس **IP** ، **Vpn Server** را وارد می کنیم.

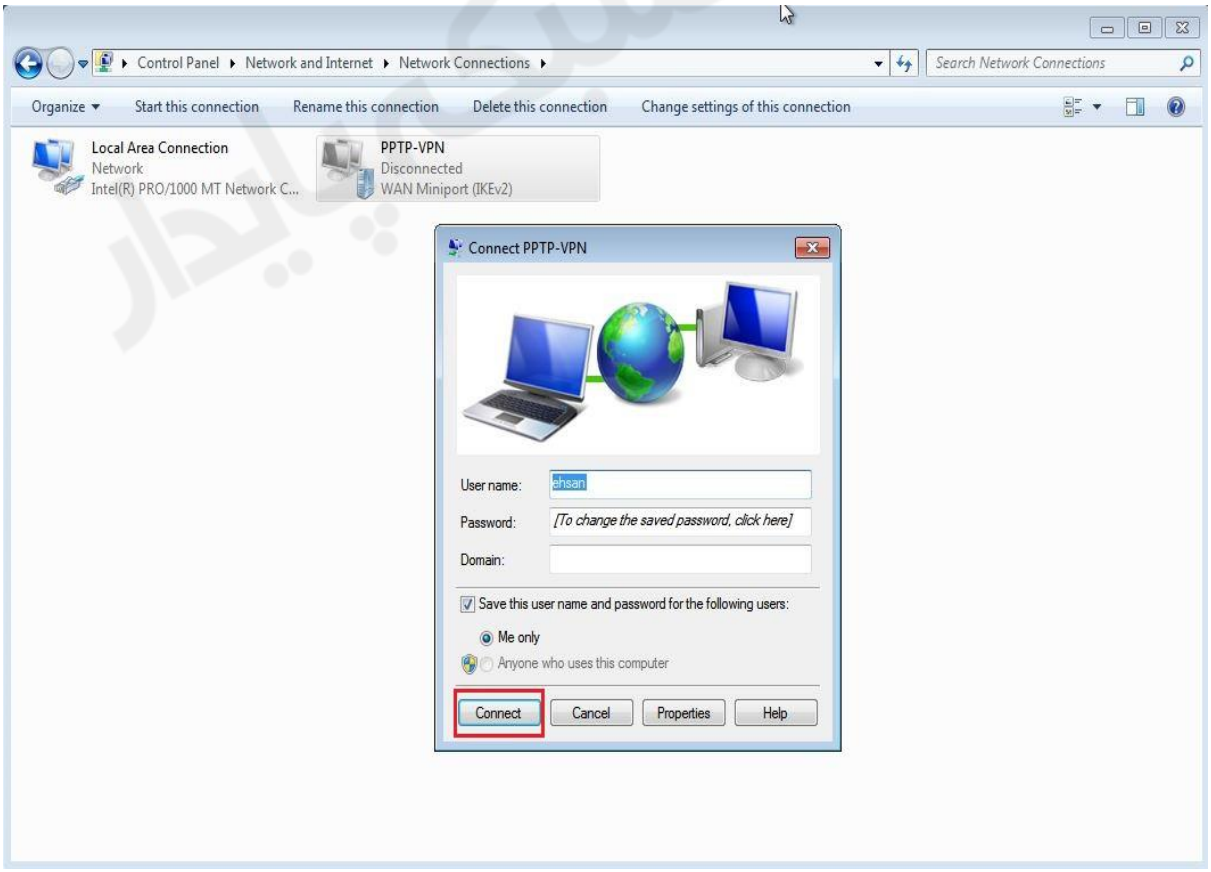


یوزرنیم و پسوردی که در روتر R3 ایجاد کردیم را وارد می کنیم.

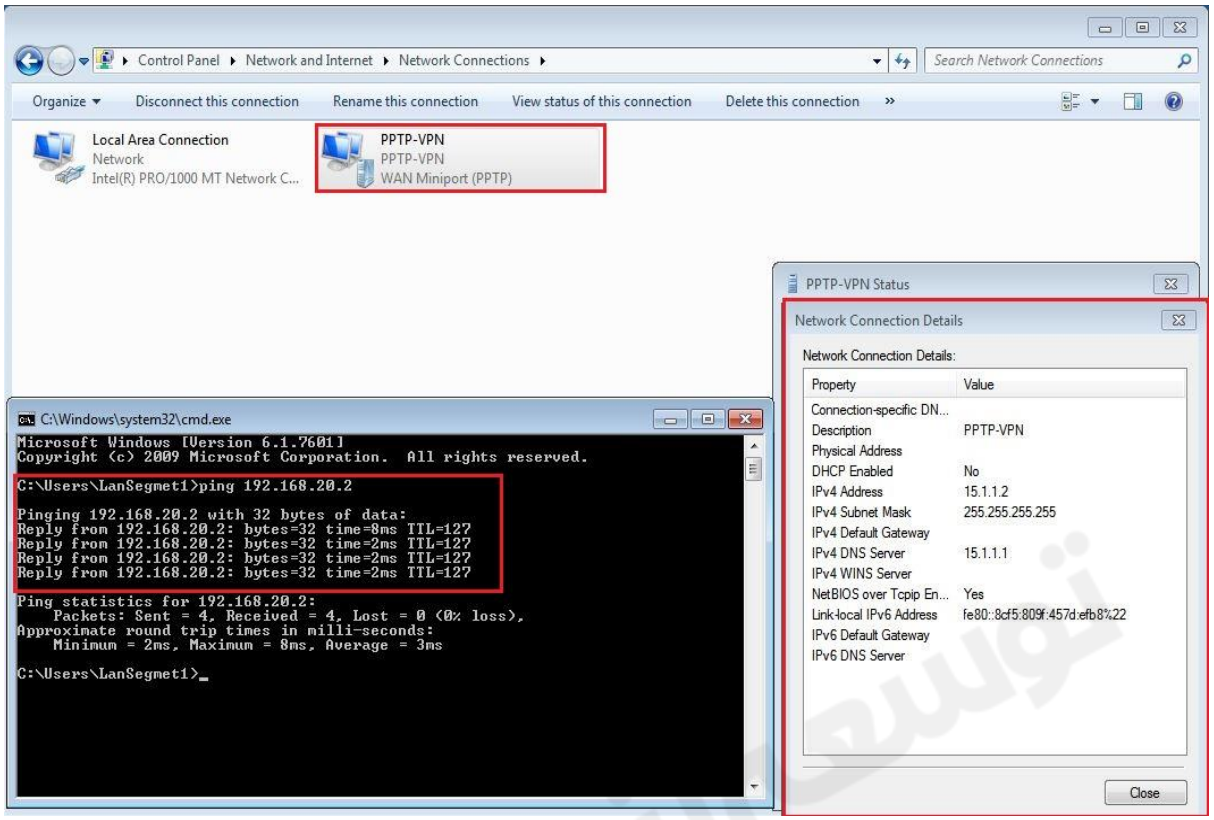


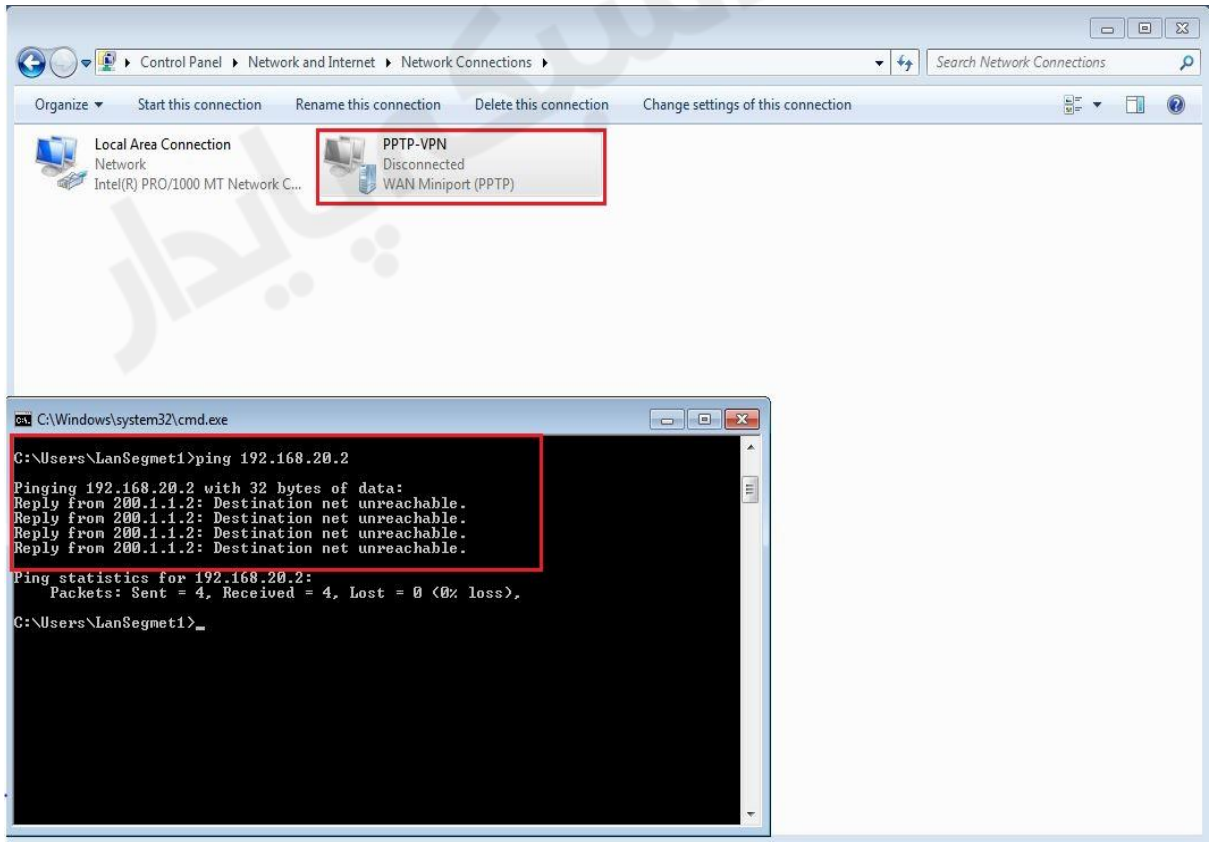
بر روی **Connection** ایجاد شده کلیک راست و بر روی **Connect** کلیک میکنیم.





همان طور که در عکس زیر مشهاده می کنید زمانی که بر روی **connect** کلیک کردید ارتباط کلاینت با شبکه **Lan-2** برقرار می شود و زمانی که **disconnect** کنید ارتباط با **Lan-2** قطع می شود.

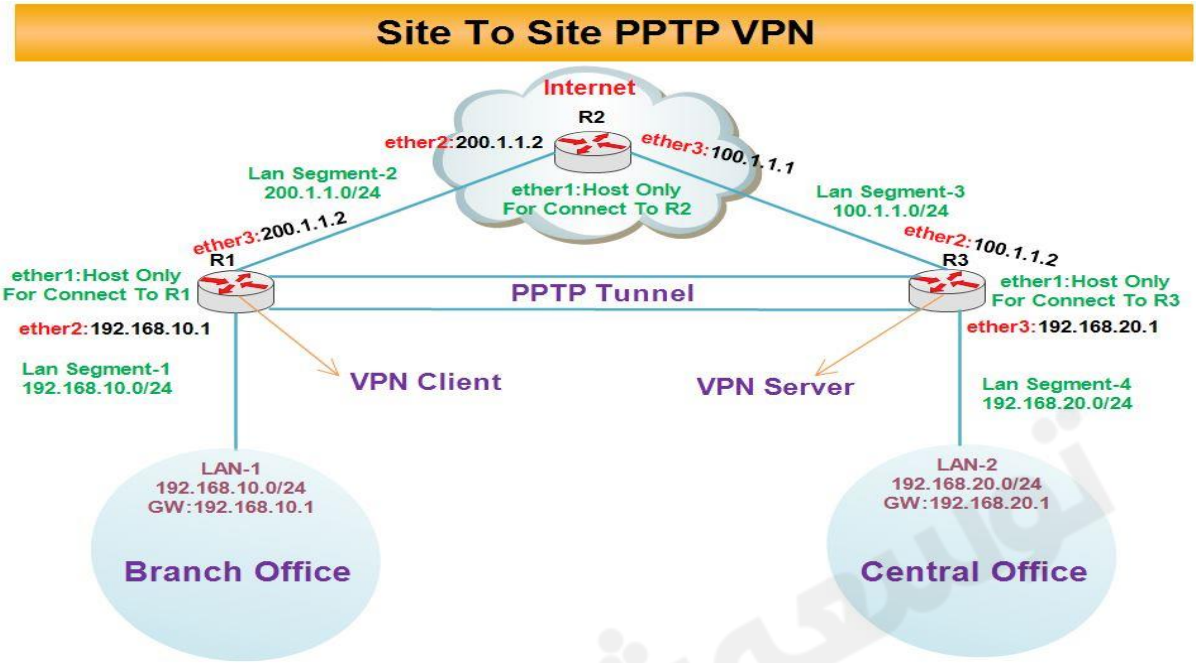




در این سناریو روش اتصال یک کلاینت به **Vpn Server** از طریق پروتکل **PPTP** را بررسی کردیم.

در ادامه روشی را مورد بررسی قرار می دهیم که با استفاده از پروتکل **PPTP** دو شبکه محلی بتوانند به یکدیگر متصل شوند.در این روش روترهای دو شبکه از طریق **Vpn** به یکدیگر متصل می شوند و ارتباط شبکه های داخلی آن با یکدیگر برقرار می شود.

سناریو ۲ : هدف از بررسی این سناریو پیاده سازی تکنیک **Site To Site** از طریق پروتکل **PPTP** می باشد.

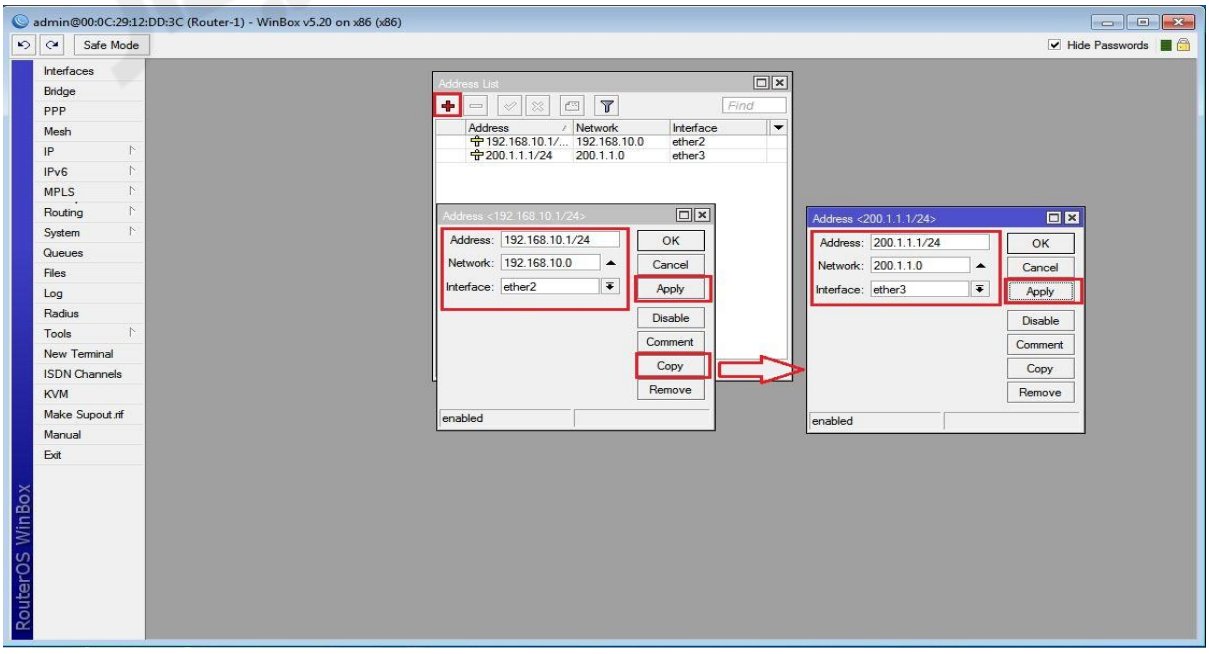


برای پیاده سازی **Site To Site** با استفاده از پروتکل **PPTP** سناریو زیر را بررسی می کنیم :

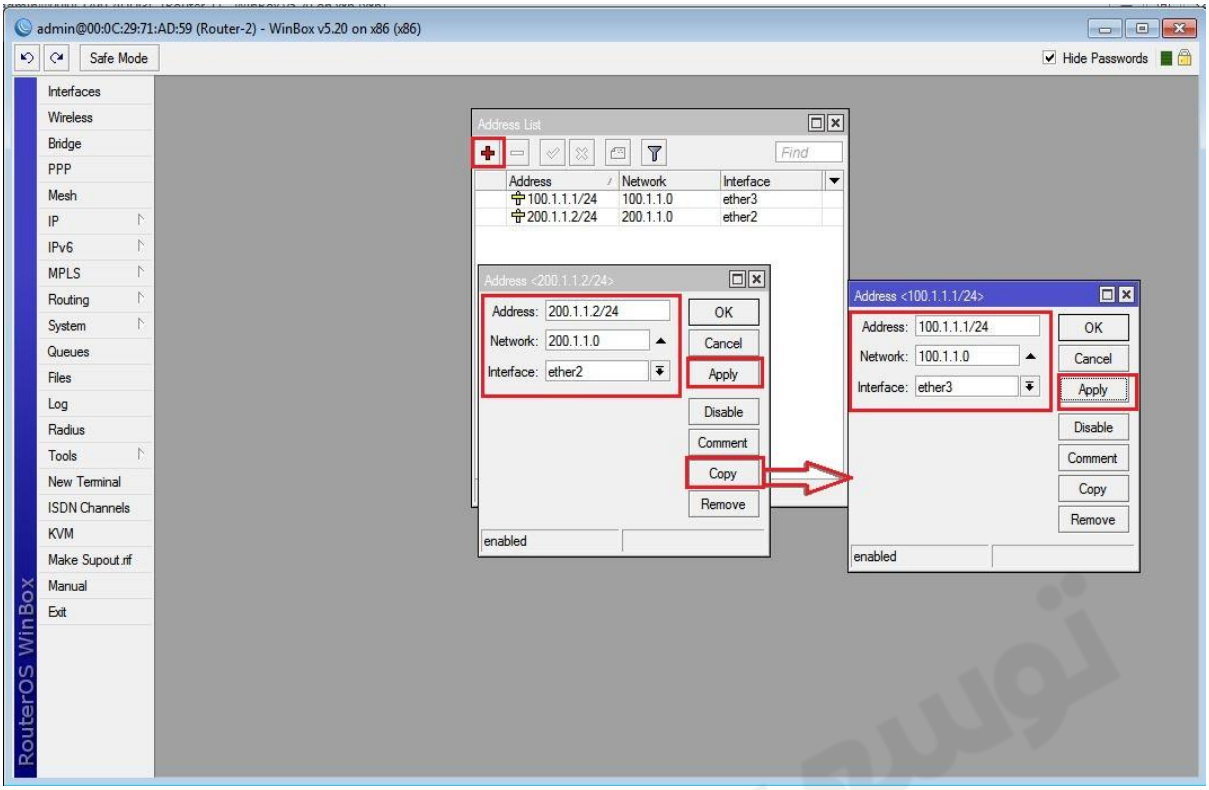
بطور مثال فرض کنید در شعبه مرکزی یک شرکت یک سرور اتوماسیون اداری وجود دارد این سرور یک **IP Valid** از محدود **IP**های شبکه داخلی دارد چنانچه بخواهیم کلاینت های موجود در بقیه شعبه های شرکت نیز بتوانند به این سرور متصل شوند(با استفاده از همان **Invalid IP**) از تکنیک **Site To Site** استفاده می کنیم.

انتساب **IP** به کارت های شبکه روترها :

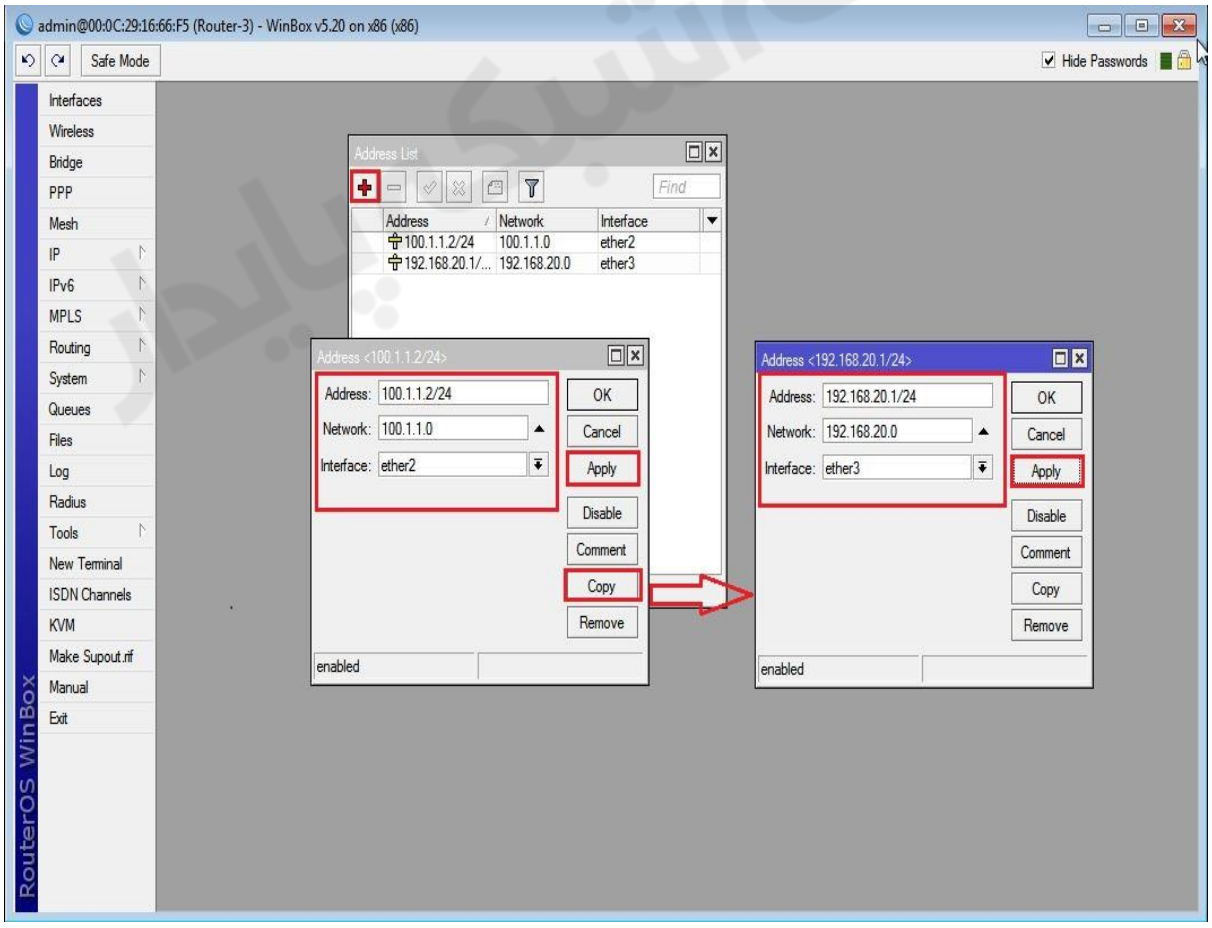
روتر **R1** :



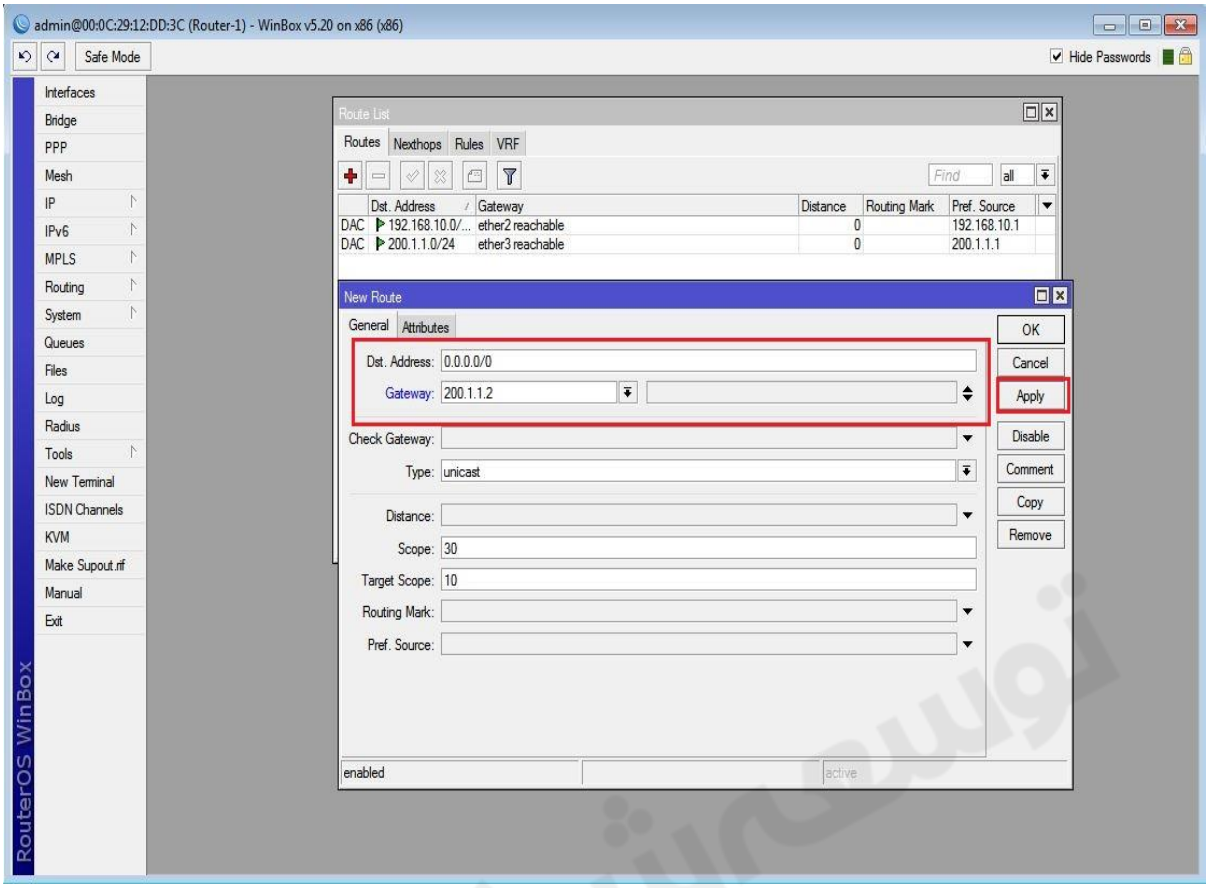
روتر **R2** :



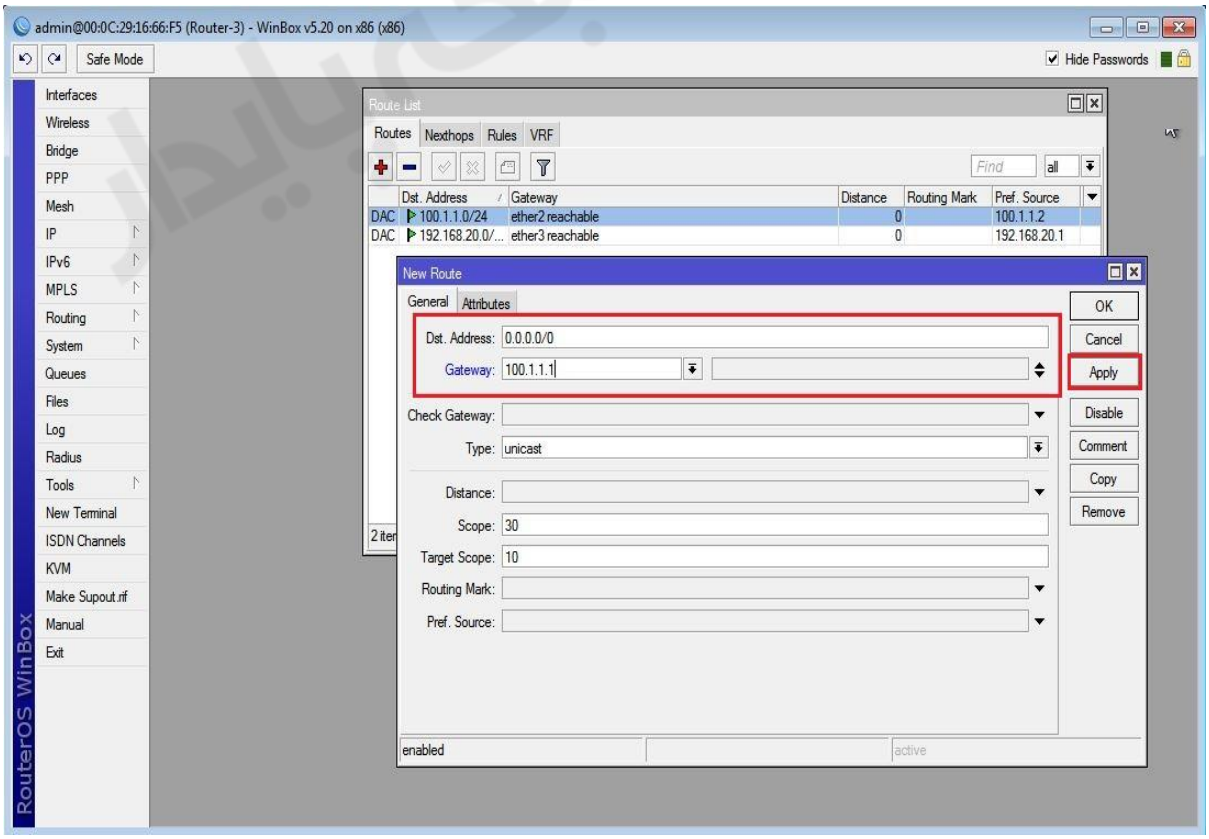
روتر **R3** :



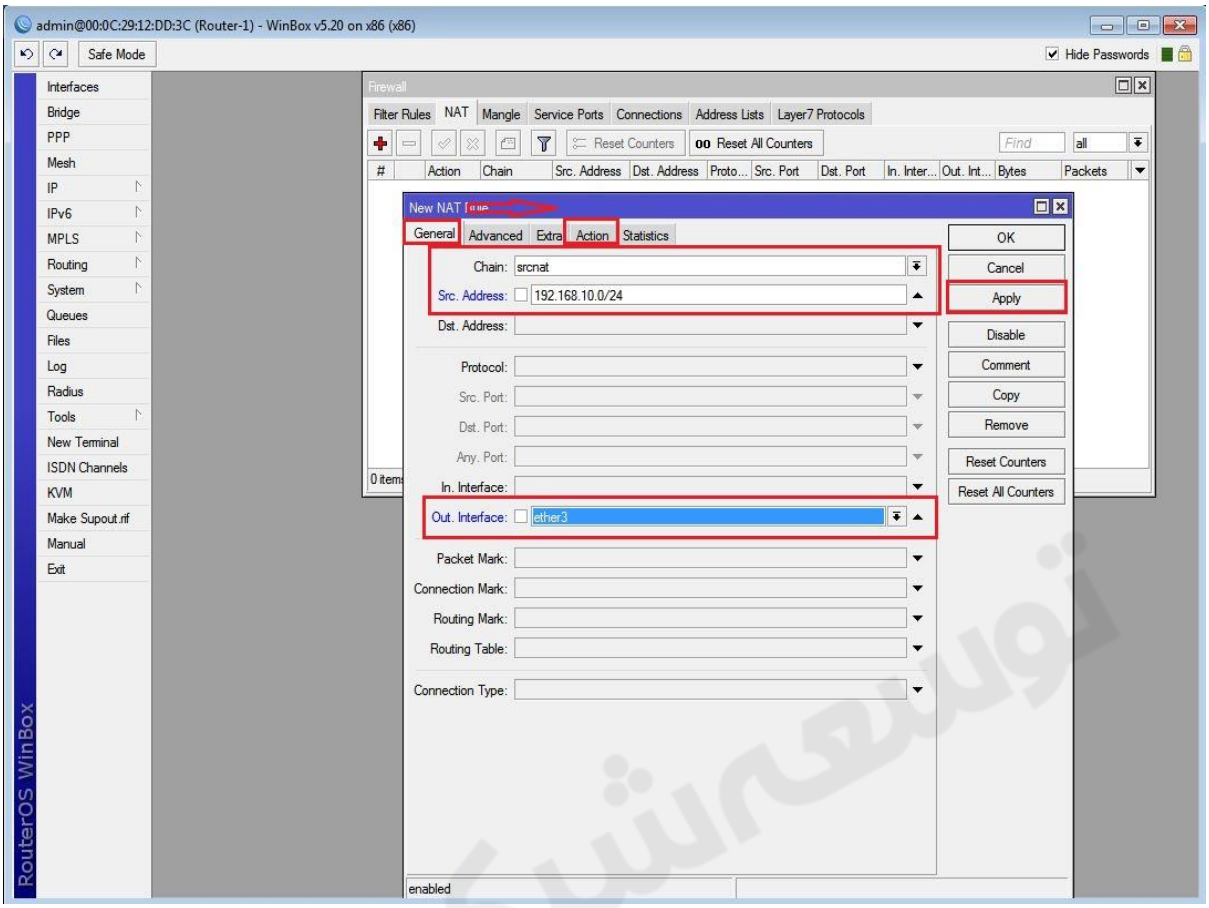
تعریف **Default Route** در روتر **R1** :

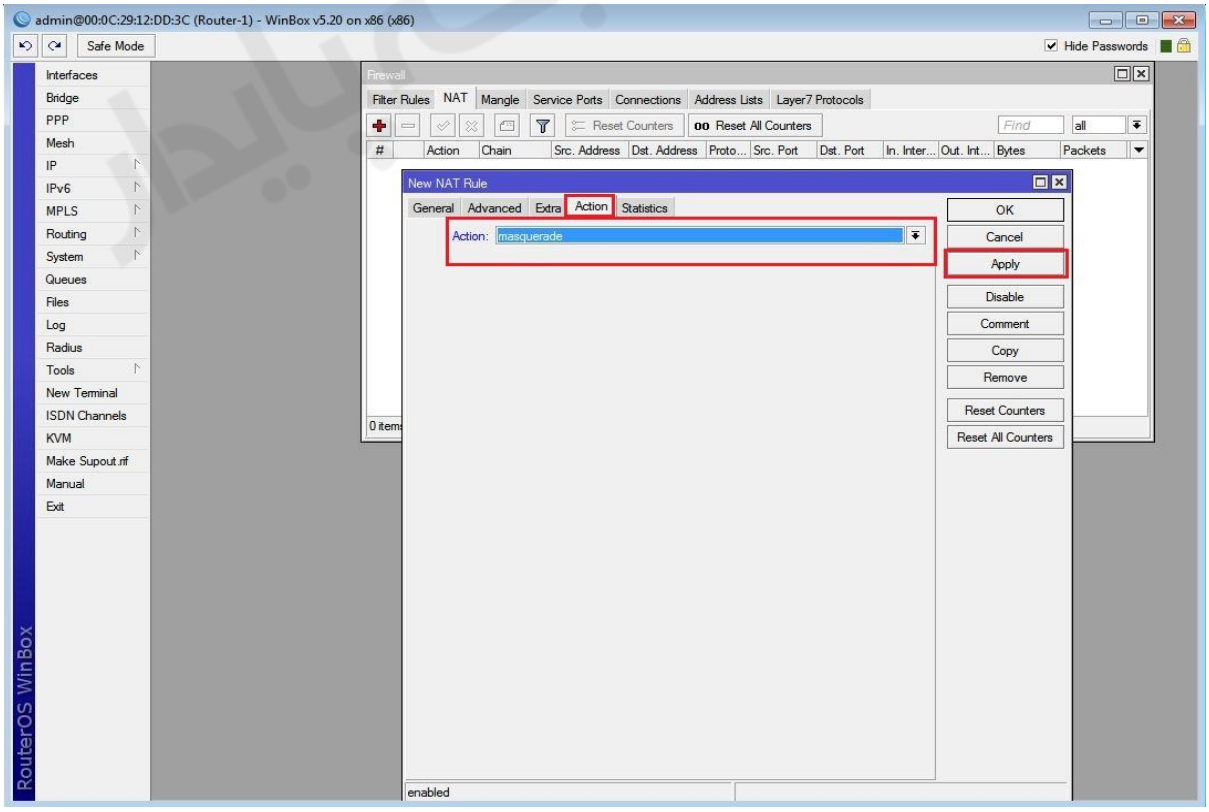


تعریف **Default Route** در **R3** :

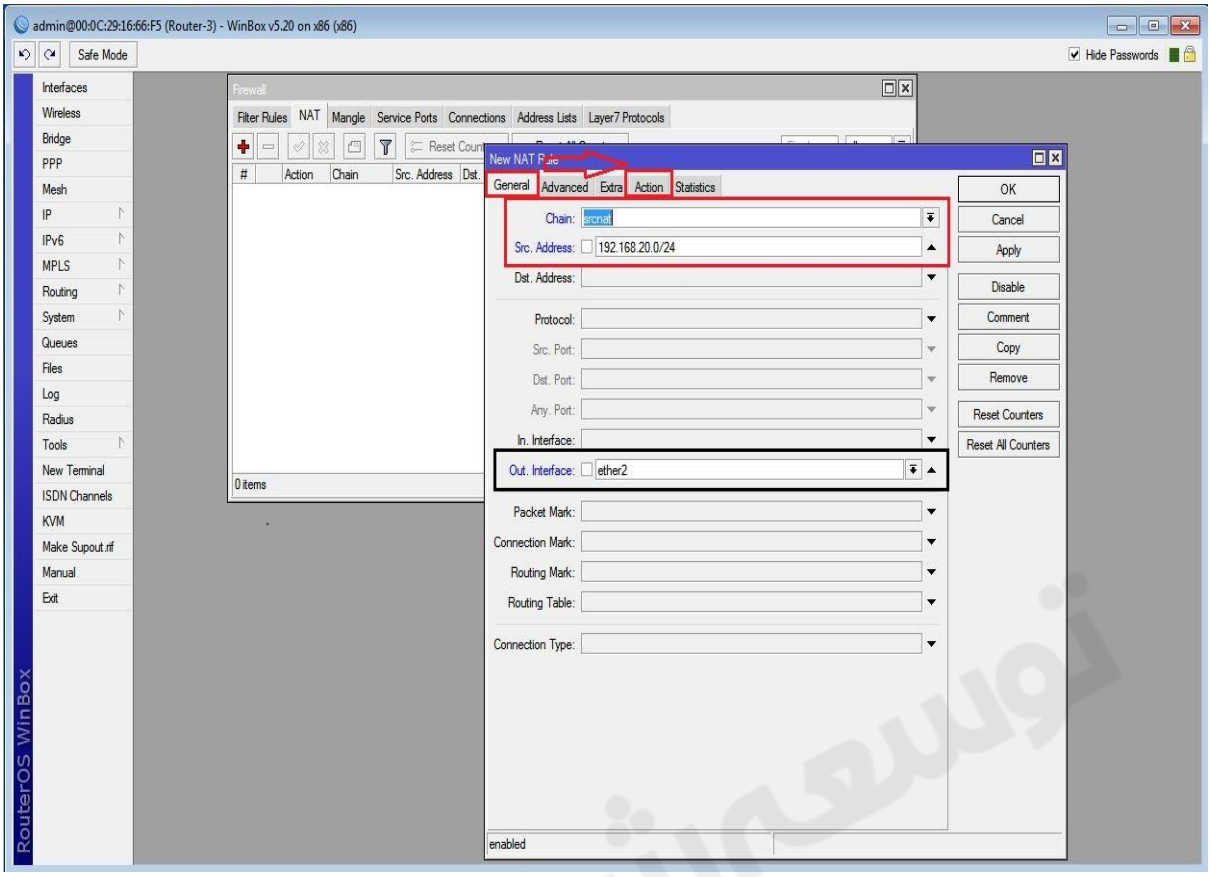


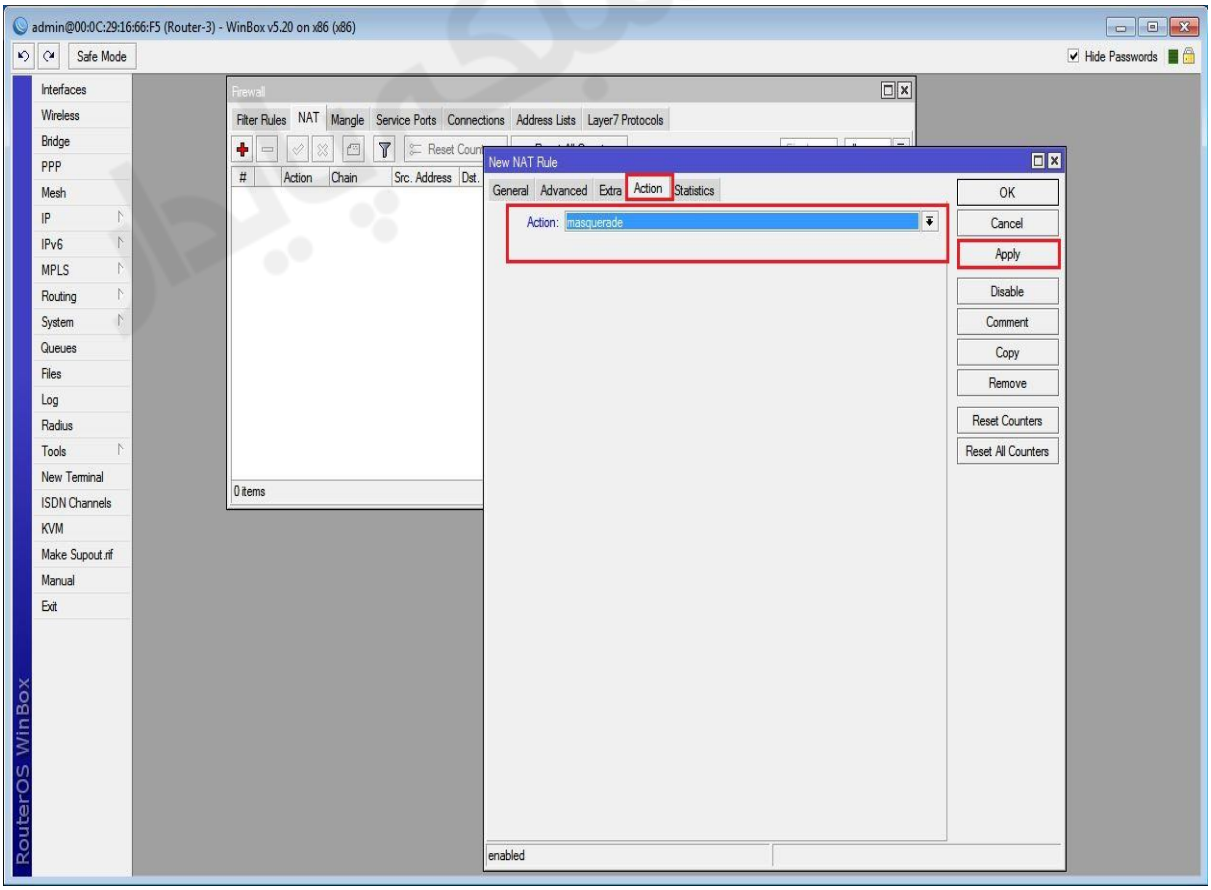
ایجاد Nat در روتر R1 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.



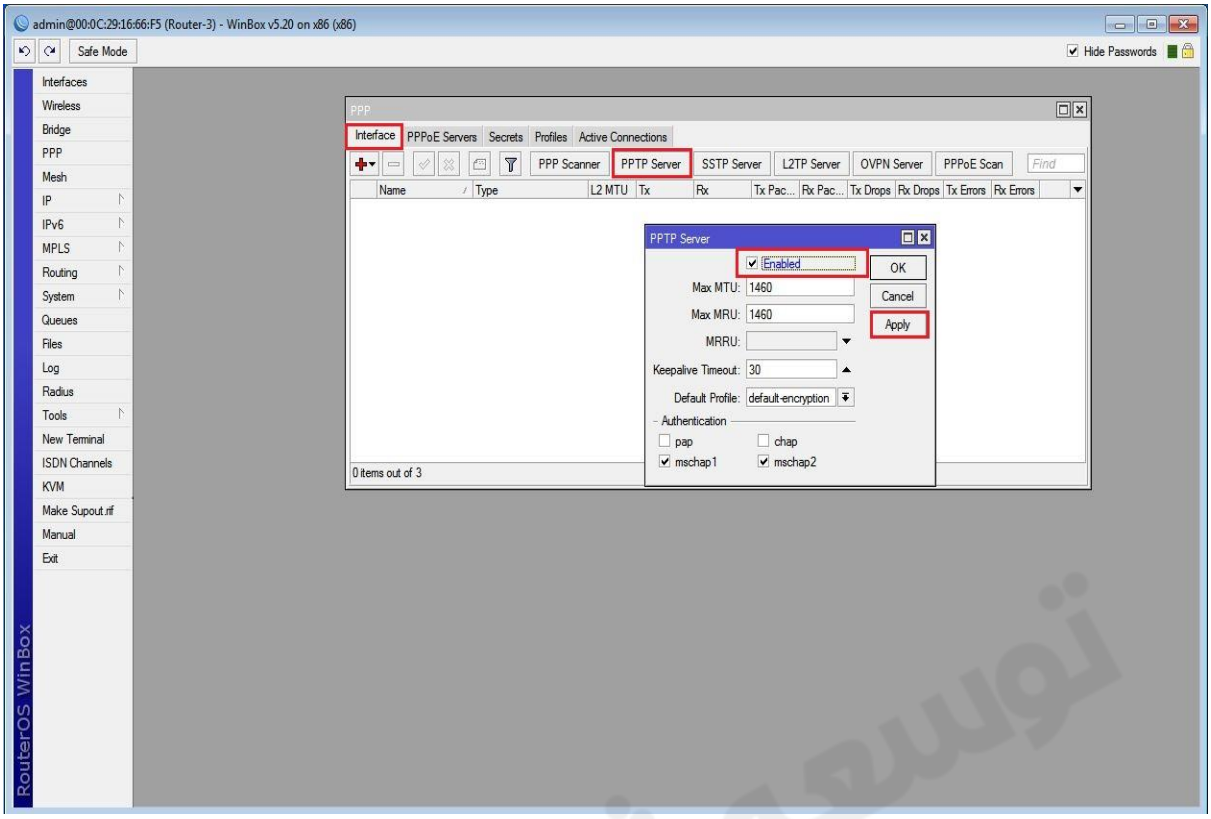


ایجاد Nat در روتر R3 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.

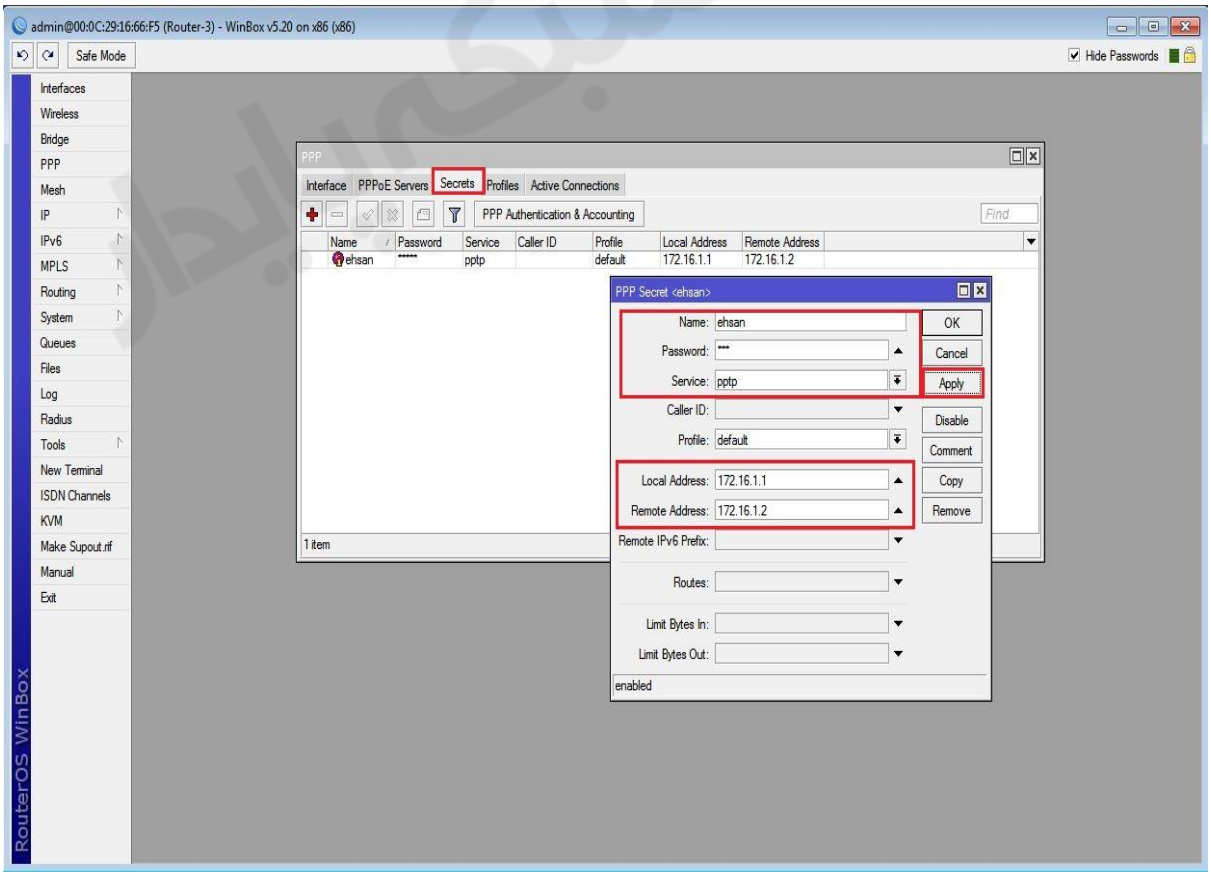




فعال سازی سرویس PPTP Server در روتر R3 :

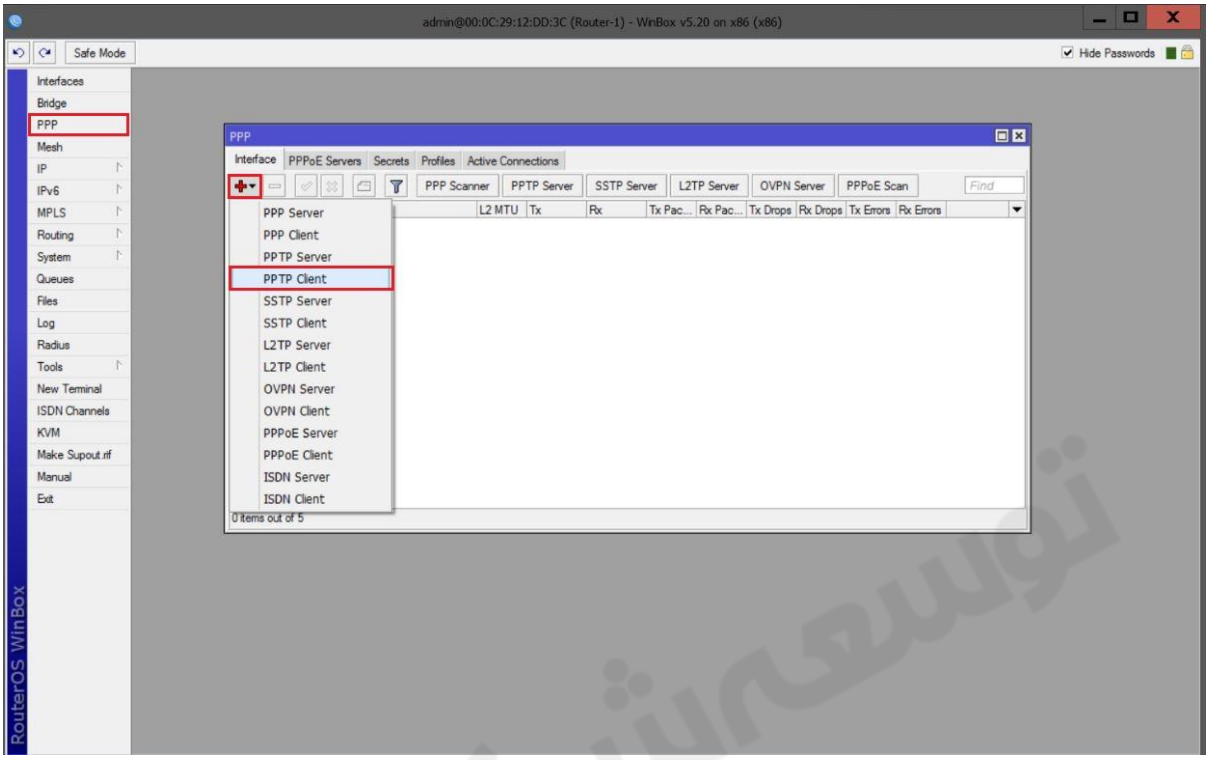


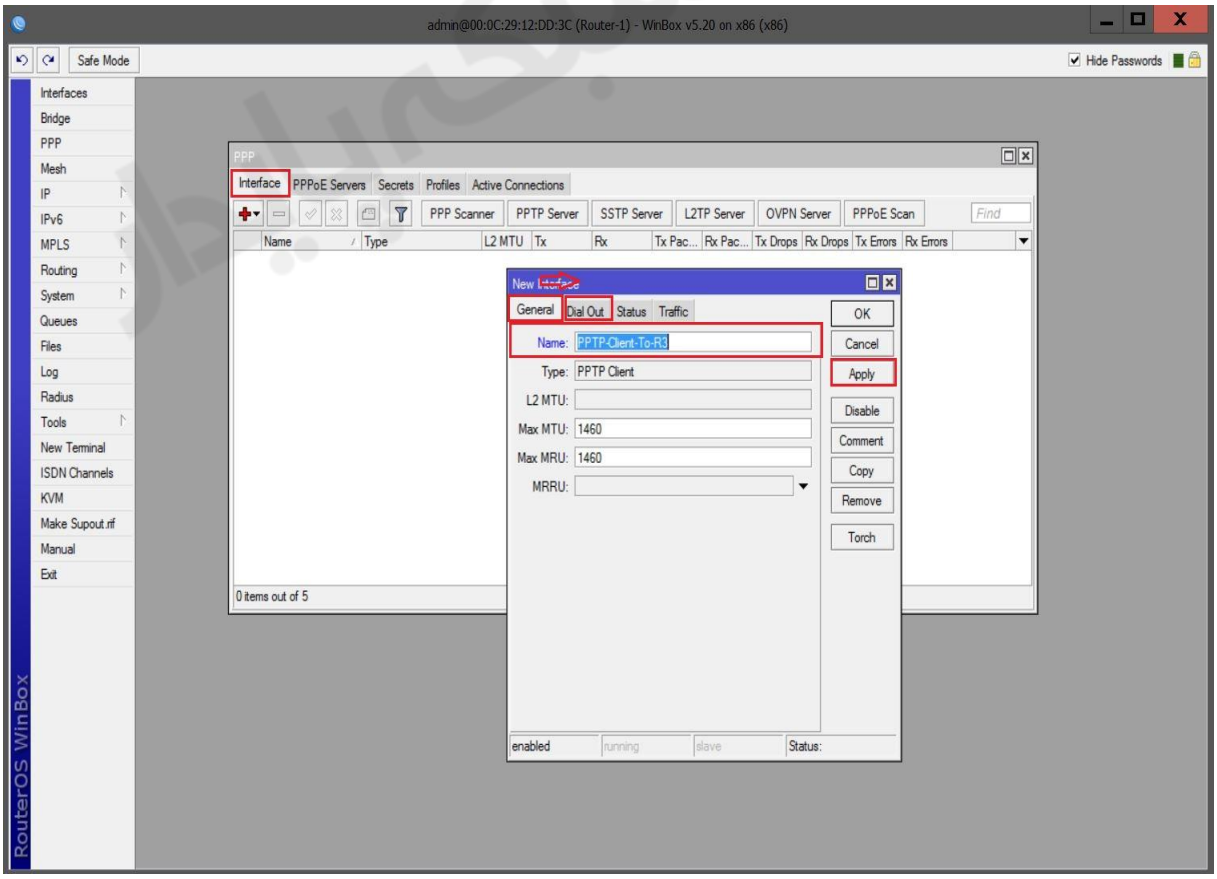
تنظیمات مربوط به سرور در روتر R3:



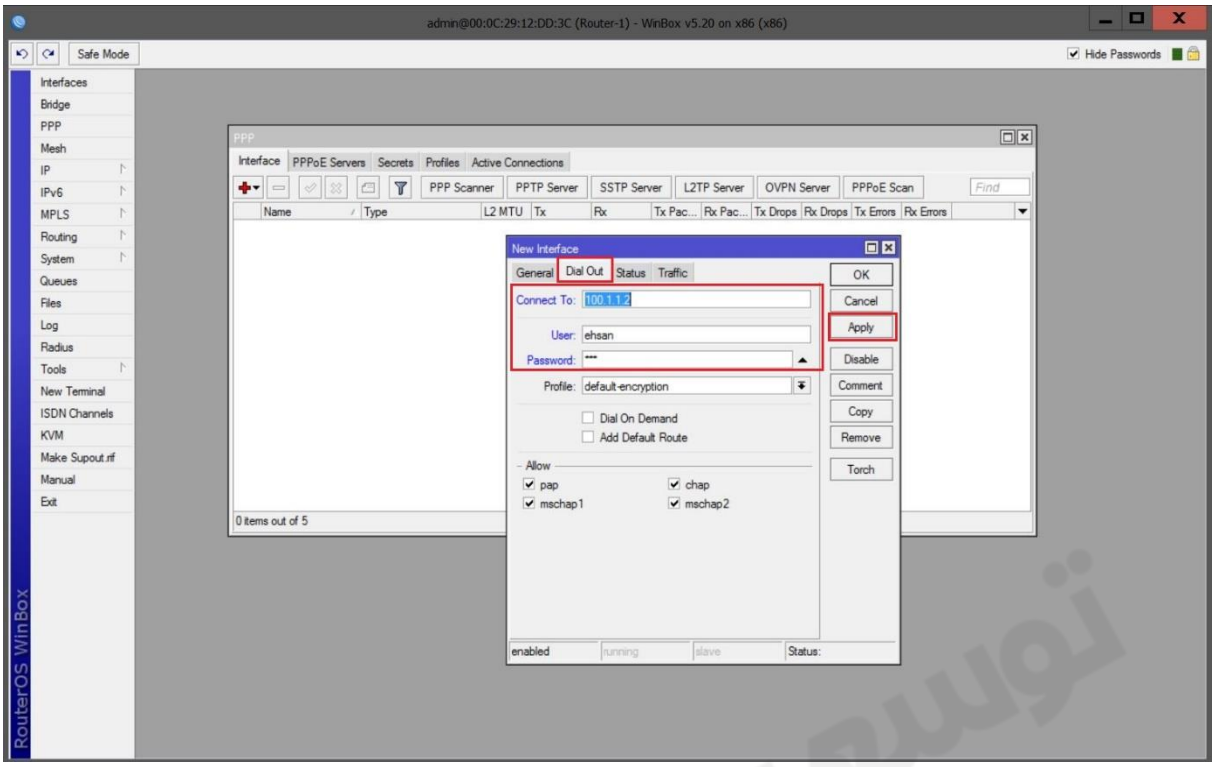
فعال سازی PPTP Client در روتر R1 :

از منوی اصلی PPP را انتخاب و از پنجره باز شده از تب Interface بر روی Add کلیک کرده و از زیر منوی باز شده PPTP Client را انتخاب می کنیم.





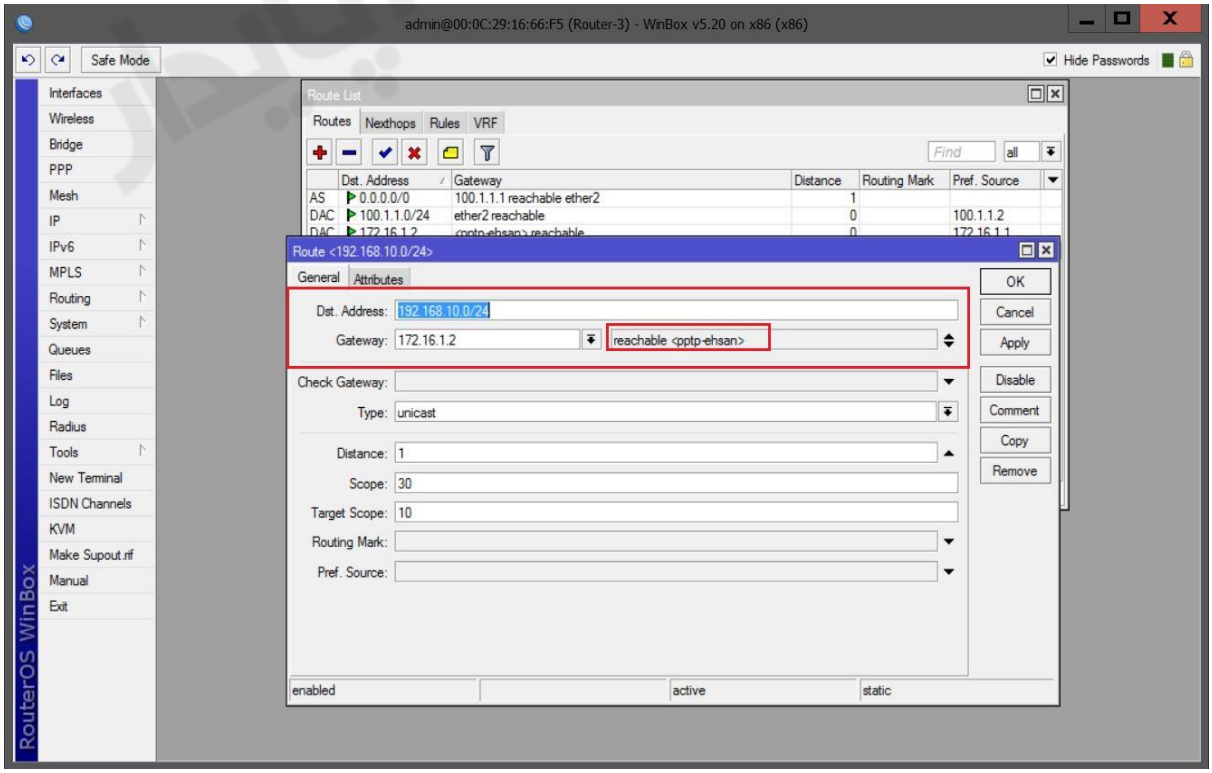
در تب **Dial Out** در قسمت **Connect To** آدرس **IP** ، **PPTP Server** و یوزرنیم و پسوردی که ساختیم را وارد می کنیم.



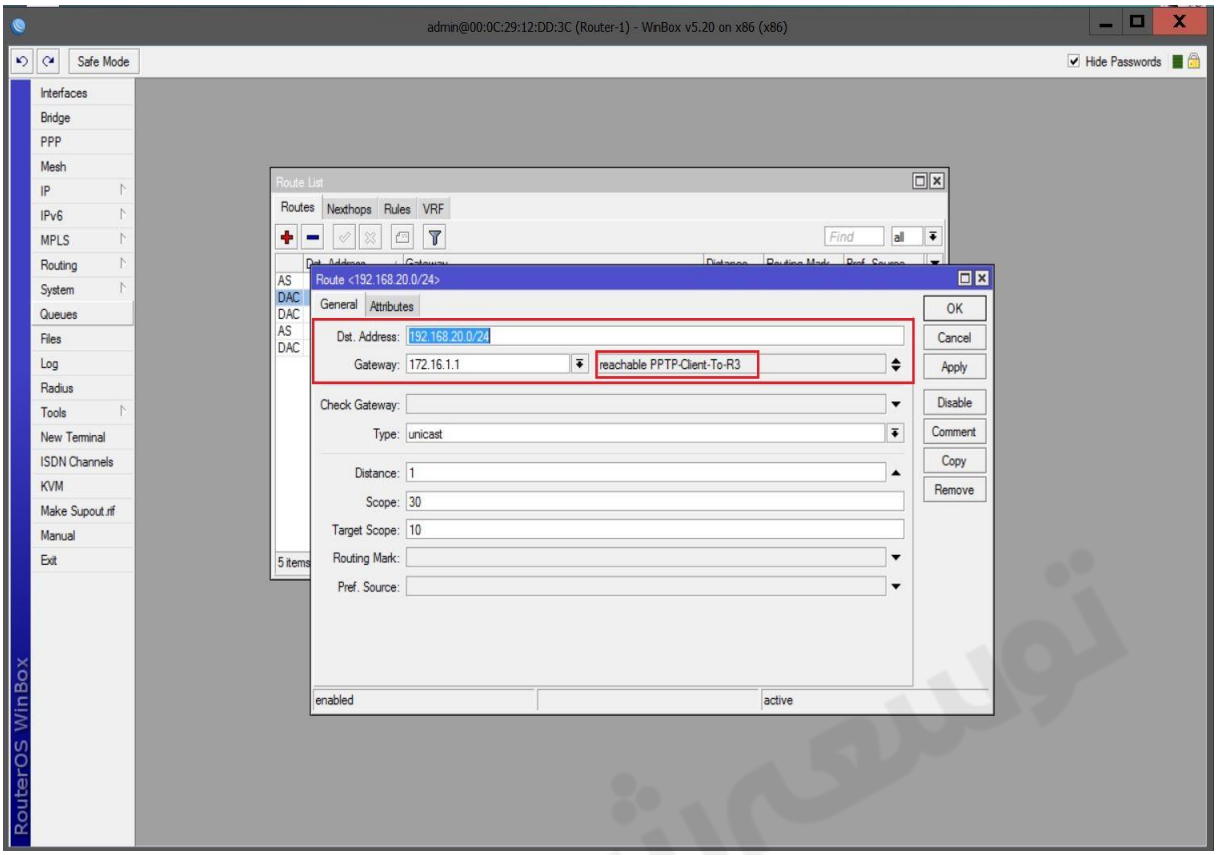
مسیریابی بسته ها در روتر R3 :

Dst.Address : در این قسمت آدرس شبکه مقصد را وارد می کنیم.

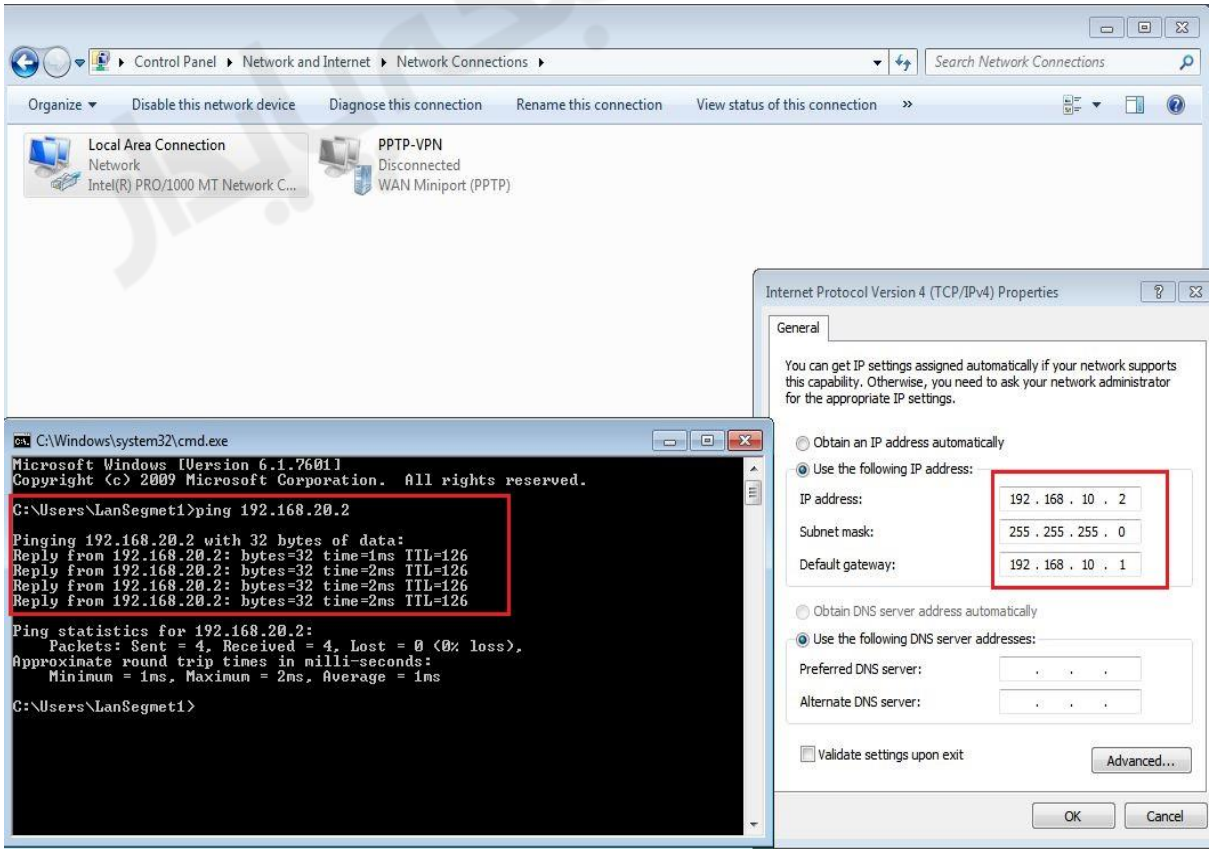
GateWay : در این قسمت آدرس کارت شبکه مجازی مربوط به به **Vpn Client** را وارد می کنیم.آدرسی که بصورت مجازی بعد از اتصال به **Vpn Server** به آن اختصاص داده می شود.

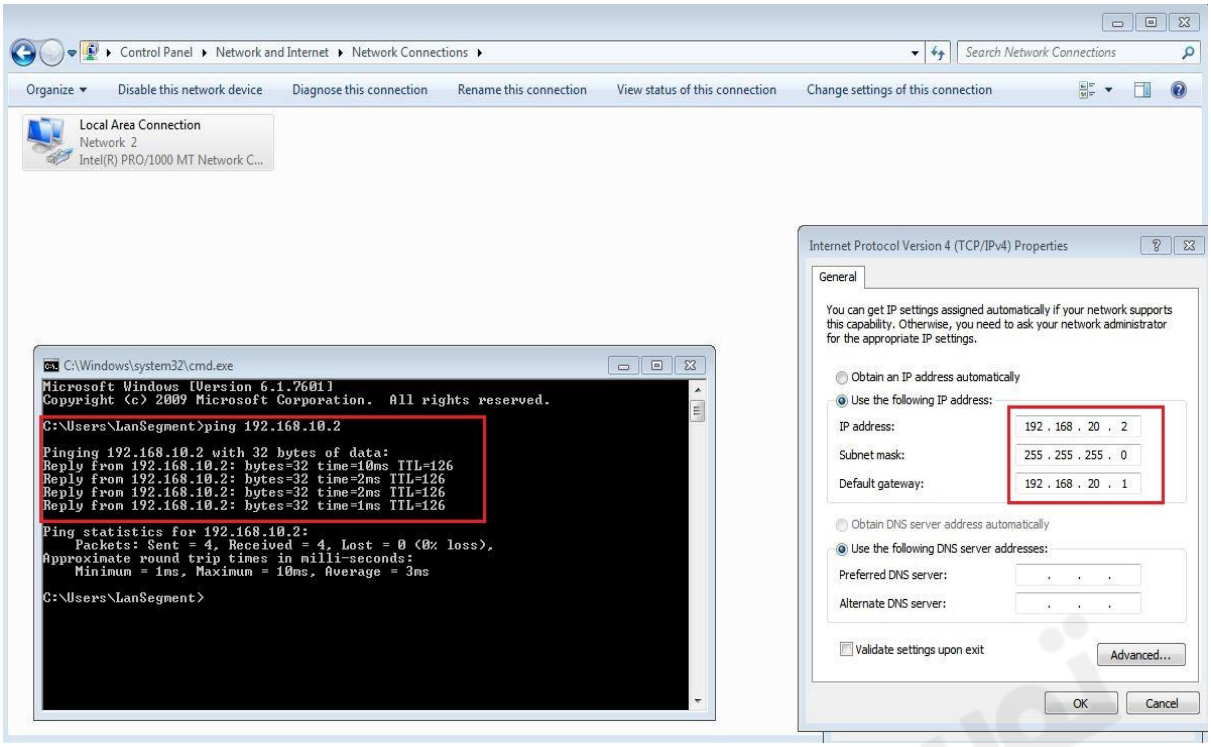


مسیریابی بسته ها در روتر R1 :



تنظیمات کلاینت :





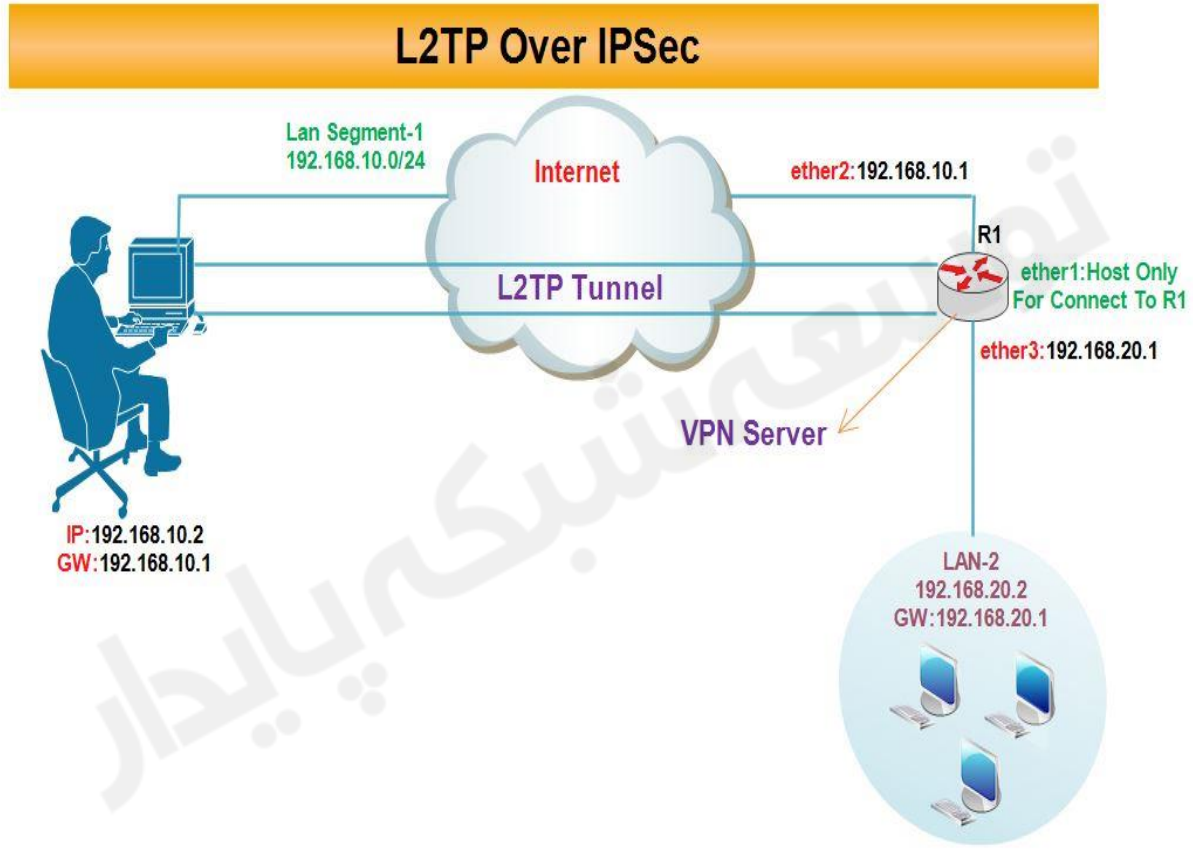
ارتباط بین دو شبکه بصورت Site To Site از طریق پروتکل PPTP برقرار شده است.

فصل سیزدهم : L2TP VPN Server

پروتکل تونلی ۲ لایه یا **Layer 2 Tunneling protocol** تحت عنوان **L2TP** شناخته می شود که حاصل عزم سیسکوو و ماکروسافت برای داشتن اتصالی ایمن تر می باشد.**L2TP** از ویژگی های امنیتی بیشتری نسبت به **PPTP** بهره می برد.به عنوان نمونه می توان به پروتکل **IPSec** که از الگوریتم های پیچیده تر رمزگذاری بهره می برد و در **L2TP** گنجانده شده است می توان اشاره کرد.همچنین **L2TP** از یک گواهی نامه از پیش به اشتراک گذاشته شده یا **Pre-Shared Certificate** هم بهره می برد.نرخ رمز گذاری این پروتکل ۱۶۸بیت و الگوریتم آن **3DES** است که تاییدیه دو مرحله ایی نیاز دارد.

L2TP نیز همانند **PPTP** از پروتکل **PPP** برای **Encapsulation** داده ها استفاده می شود.

سناریو ۱ : هدف از بررسی این سناریو نحوه ارتباط سیستم کلاینت به شبکه مقصد را با استفاده از پروتکل **L2TP** می باشد.

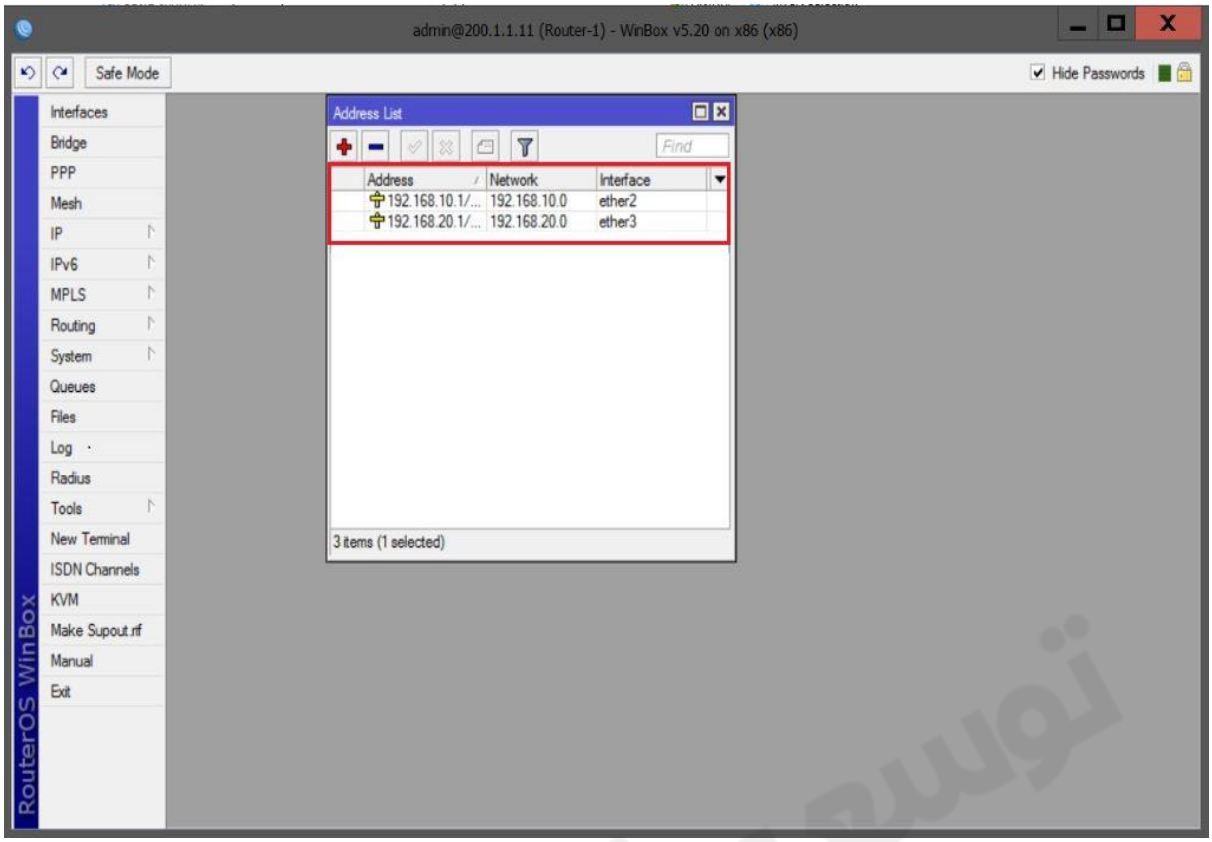


در سیستم عامل ویندوز ارتباط **L2TP** به صورت پیش فرض با پروتکل **IPSec** پیاده سازی می شود و به عنوان **L2TP Over IPSec** شناخته می شود.بنابراین چنانچه کلاینت سیستم عمل ویندوز داشته باشد ابتدا باید پروتکل **IPSec** پیاده سازی شود سپس پروتکل **L2TP** برروی بستر **IPSec** راه اندازی می شود.

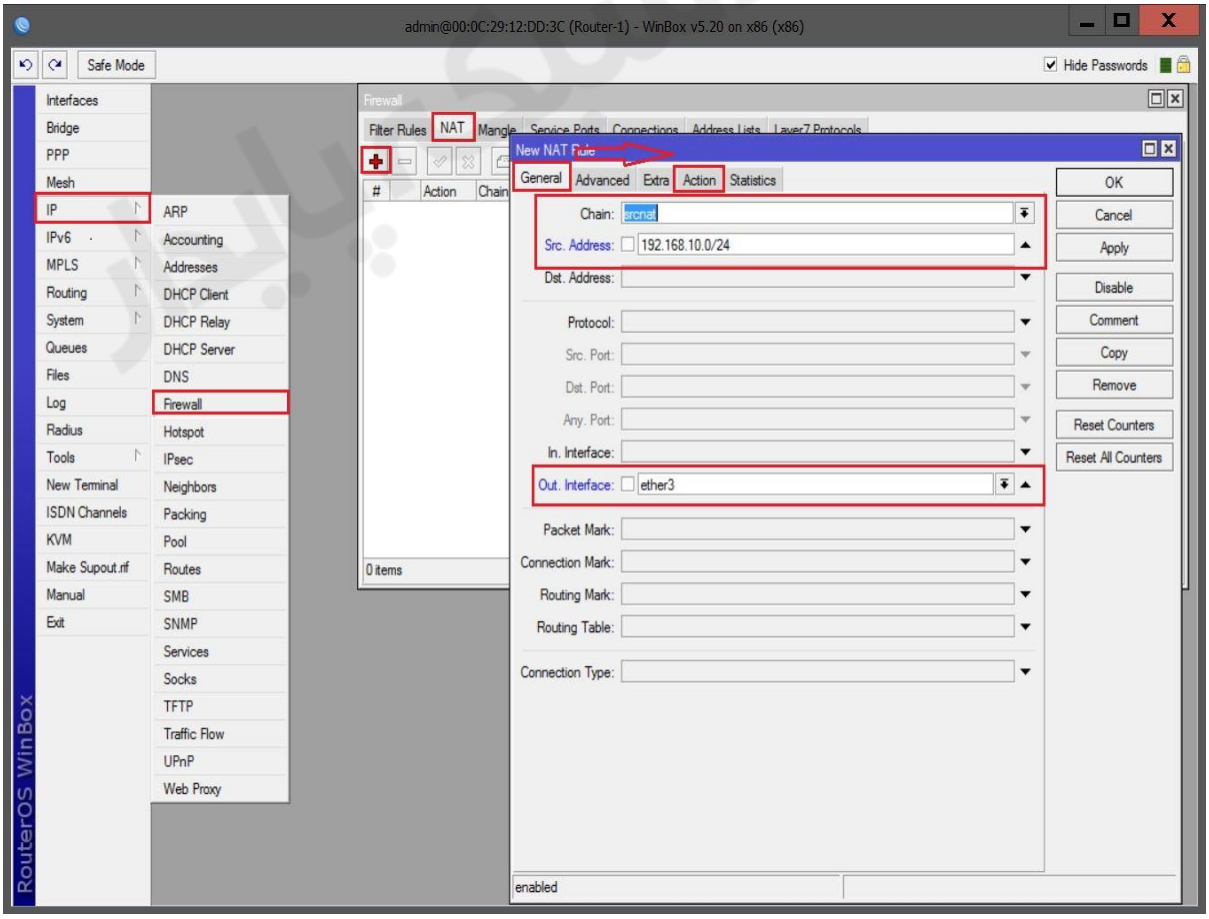
در این سناریو ، کاربر از طریق اینترنت یک کانال امن به با استفاده از پروتکل **L2TP** به مسیریاب موجود در شبکه دیگر برقرار می کند و از این طریق به شبکه محلی مقصد (**Lan-2**) دسترسی خواهد داشت.

انتساب **IP** به کارت های شبکه روترها :

روتر **R1** :

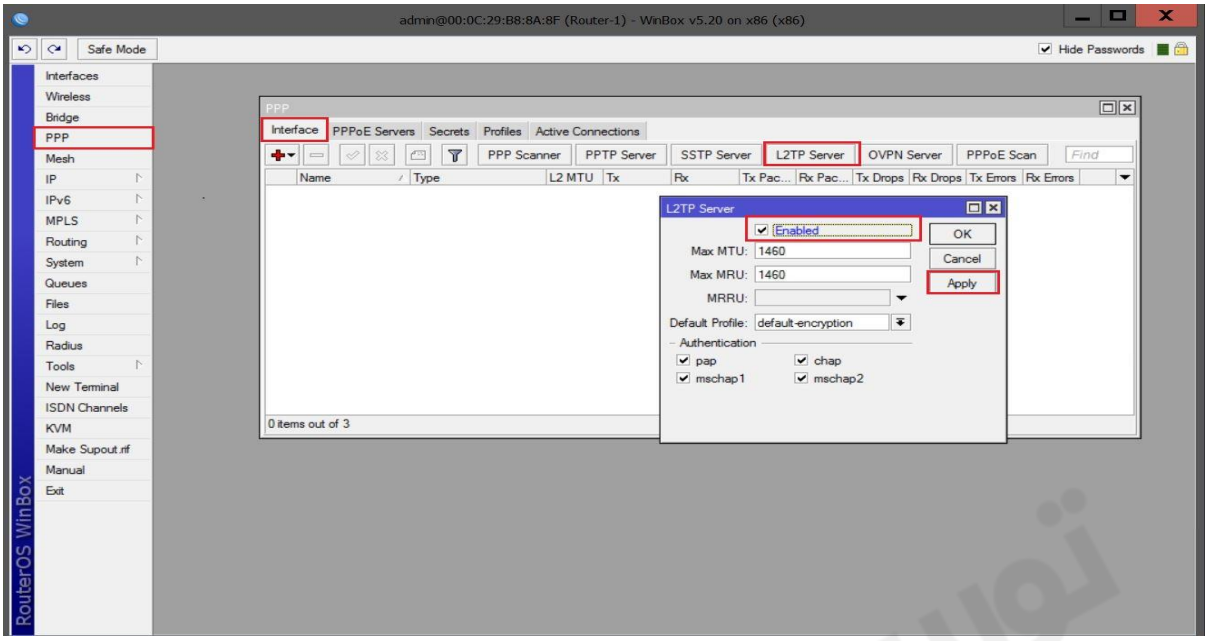


ایجاد Nat برای دسترسی کلاینت ها به اینترنت :



فعال سازی سرویس LT2P :

برای فعال سازی این سرویس از منوی اصلی PPP را انتخاب کرده در پنجره باز شده از تب Interface گزینه L2TP Server را انتخاب و تیک گزینه Enable را می زنیم.



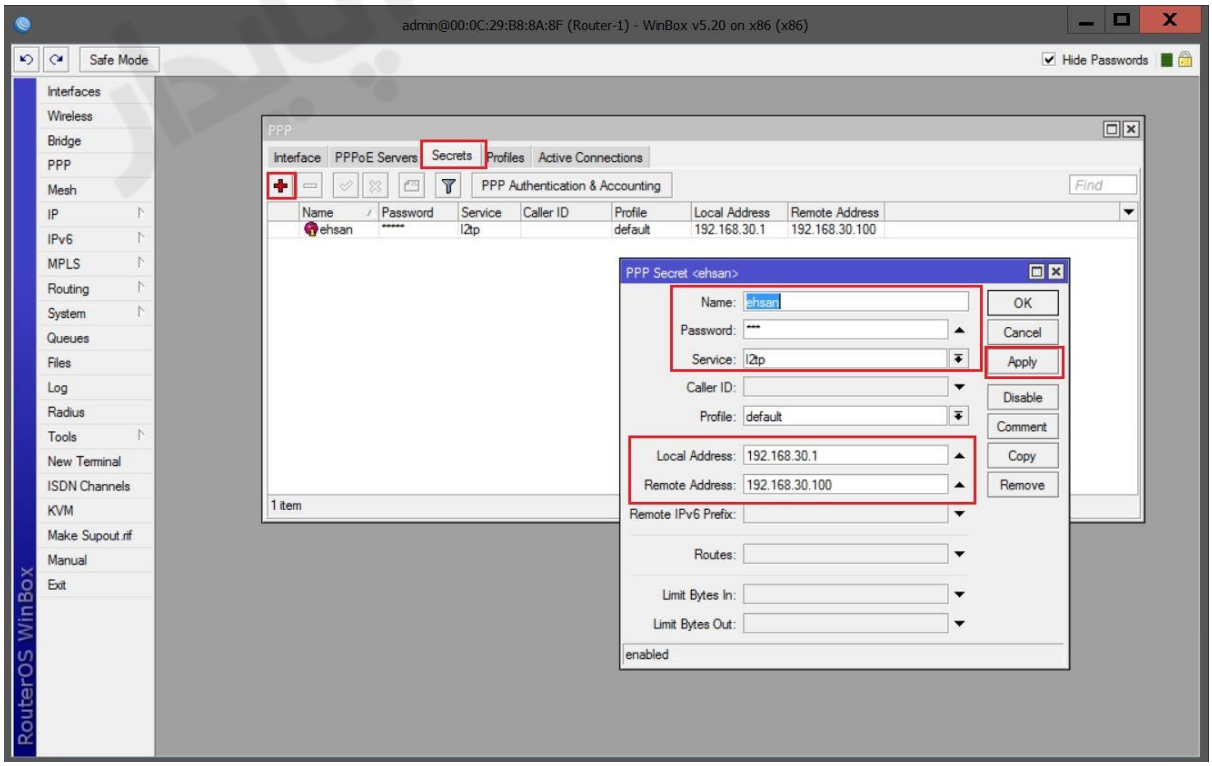
تنظیمات مربوط به سرور :

۵. **Name And Password** : نام کاربری و رمز عبور معتبری برای اتصال کاربران به **Vpn Server** را مشخص می کنیم.

۶. **Service** : پروتکلی که کلاینت ها می توانند توسط آن به **Vpn Server** متصل شوند را انتخاب می کنیم.

۷. **Local Address** : در این قسمت مشخص می کنیم که کلاینت ها از طریق کدام کارت شبکه مربوط به محدوده داخلی شبکه **Lan** دسترسی داشته باشد.به عبارتی **IP** کارت شبکه ای از میکروتیک را که می خواهیم بسته ها از طریق آن وارد **Lan** شوند.

۸. **Remote Address** : در این قسمت آدرس **IP**ای که به کلاینت بعد از اتصال به **Vpn Server** انتساب داده می شود را مشخص می کنیم.این **IP** هم می تواند از محدوده شبکه مقصد باشد و هم از محدوده ای غیر از شبکه مقصد.



ایجاد IPSec برای کلاینت های ویندوز :

برای اینکار از منوی اصلی IP را انتخاب و از زیر منوی باز شده IPSec را انتخاب میکنیم و پنجره باز شده به تب Peer می رویم و تنظیمات زیر را انجام می دهیم.

Address : در این پارامتر آدرس IP کلاینتی که اجازه اتصال به این Vpn Server را دارد را وارد می کنیم.

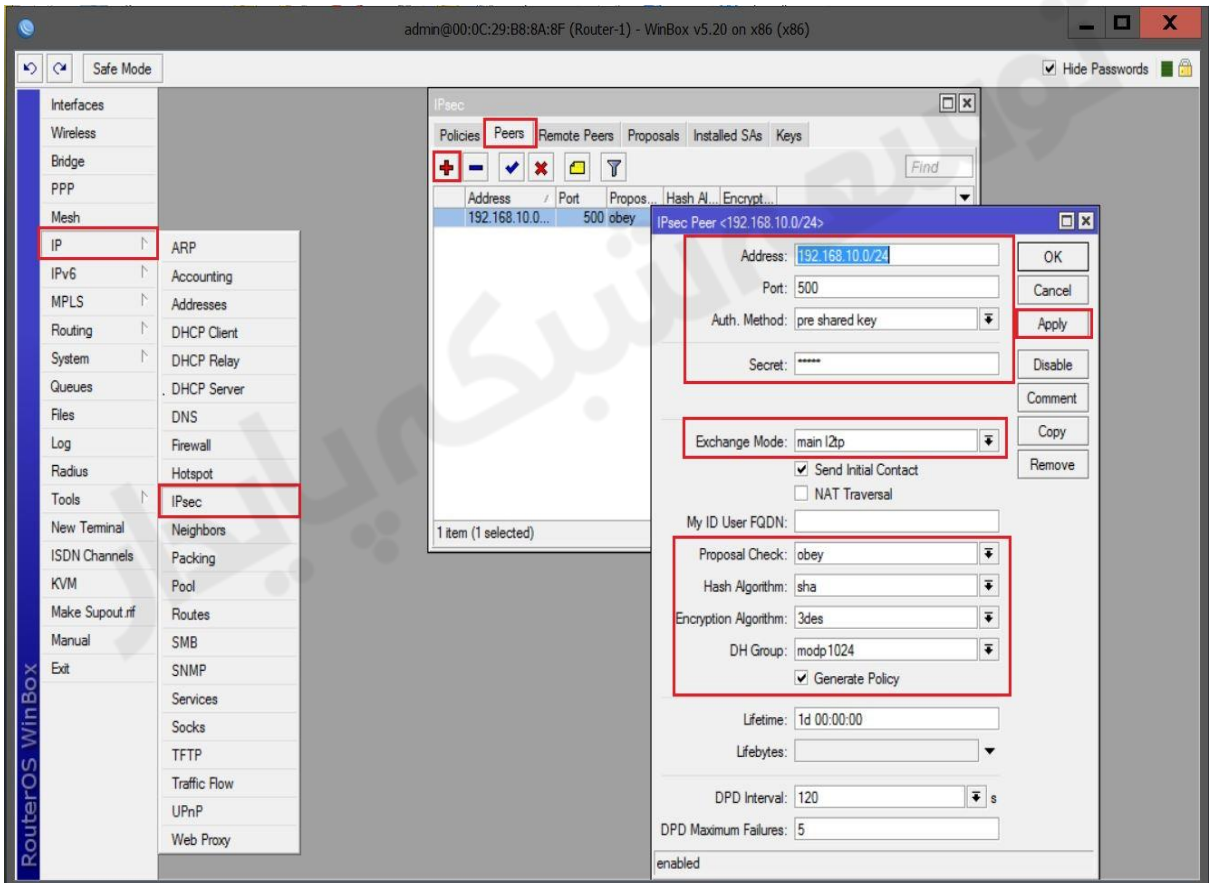
Auth-Method : در این قسمت روش احراز هویت کاربران یا Authentication Method را مشخص می کنیم این قسمت سه حالت دارد :

۱. **Pre-shared Key : کلیدی که بین مبدا و مقصد یکسان است.**
۲. **RSA-Key : اعمال رمز گذاری بر روی Pre-shared Key را انجام می دهد.**
۳. **RSA-Singature : اعمال رمز گذاری و امضای دیجیتالی بر روی Pre-shared Key را انجام می دهد.**

Secret : در این قسمت رمزی که بین سرور و کلاینت مشترک می باشد را وارد می کنیم.

Hash Algorithm : در این قسمت الگوریتم درهم سازی را مشخص می کنیم.

Enc-Algorithm : در این قسمت الگوریتم رمز گذاری داده ها را مشخص می کنیم.



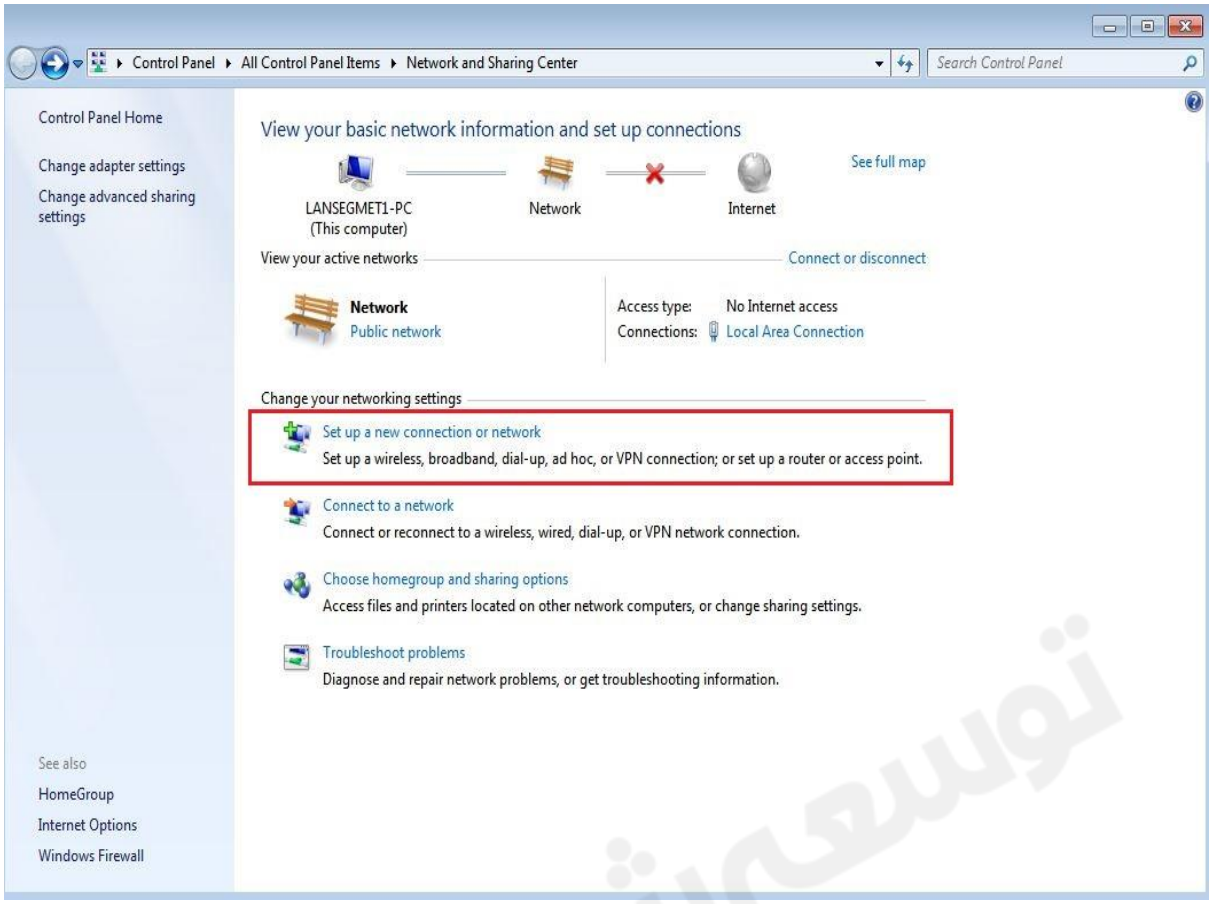
تنظیمات کلاینت :

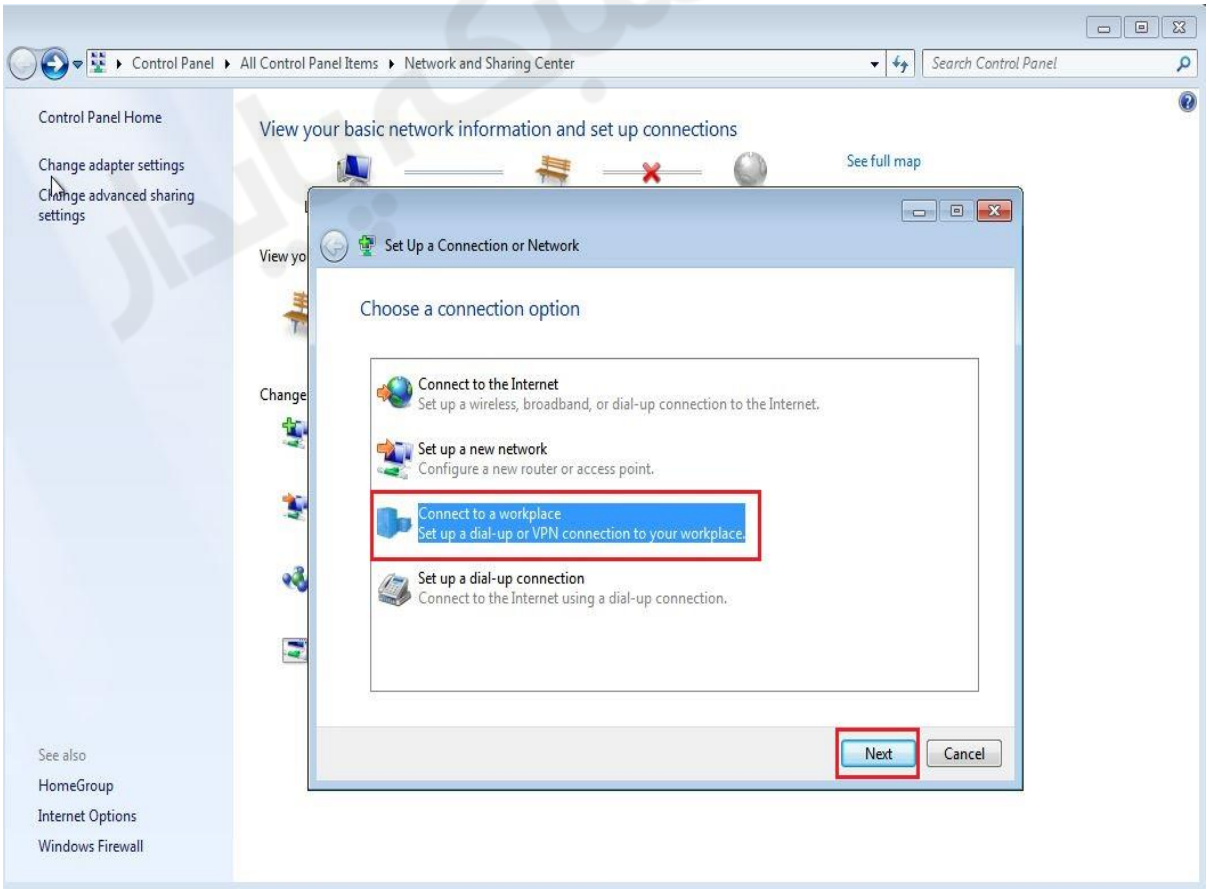
طبق سناریو به کلاینت IP می دهیم.

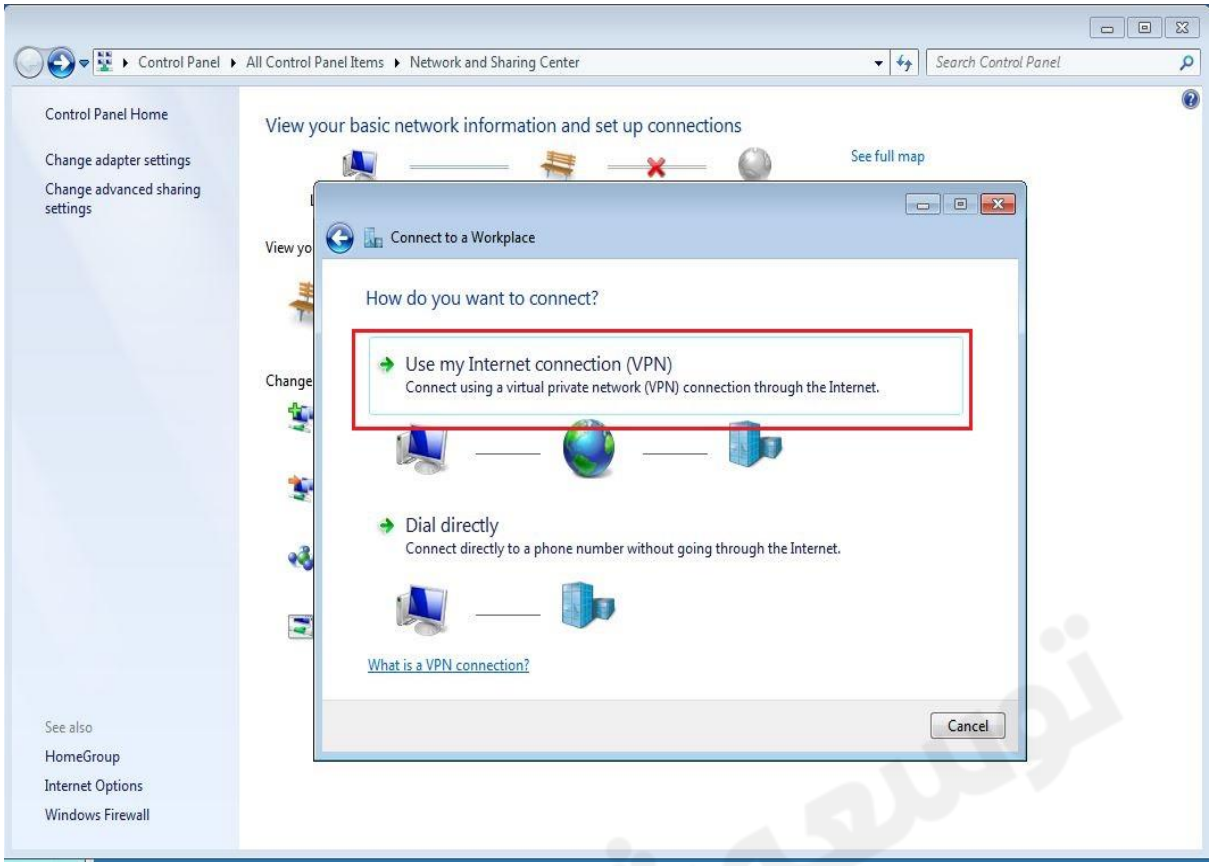
تا اینجای کار با این تنظیمات هنوز ار تباط با شبکه Lan-2 برقرار نیست.

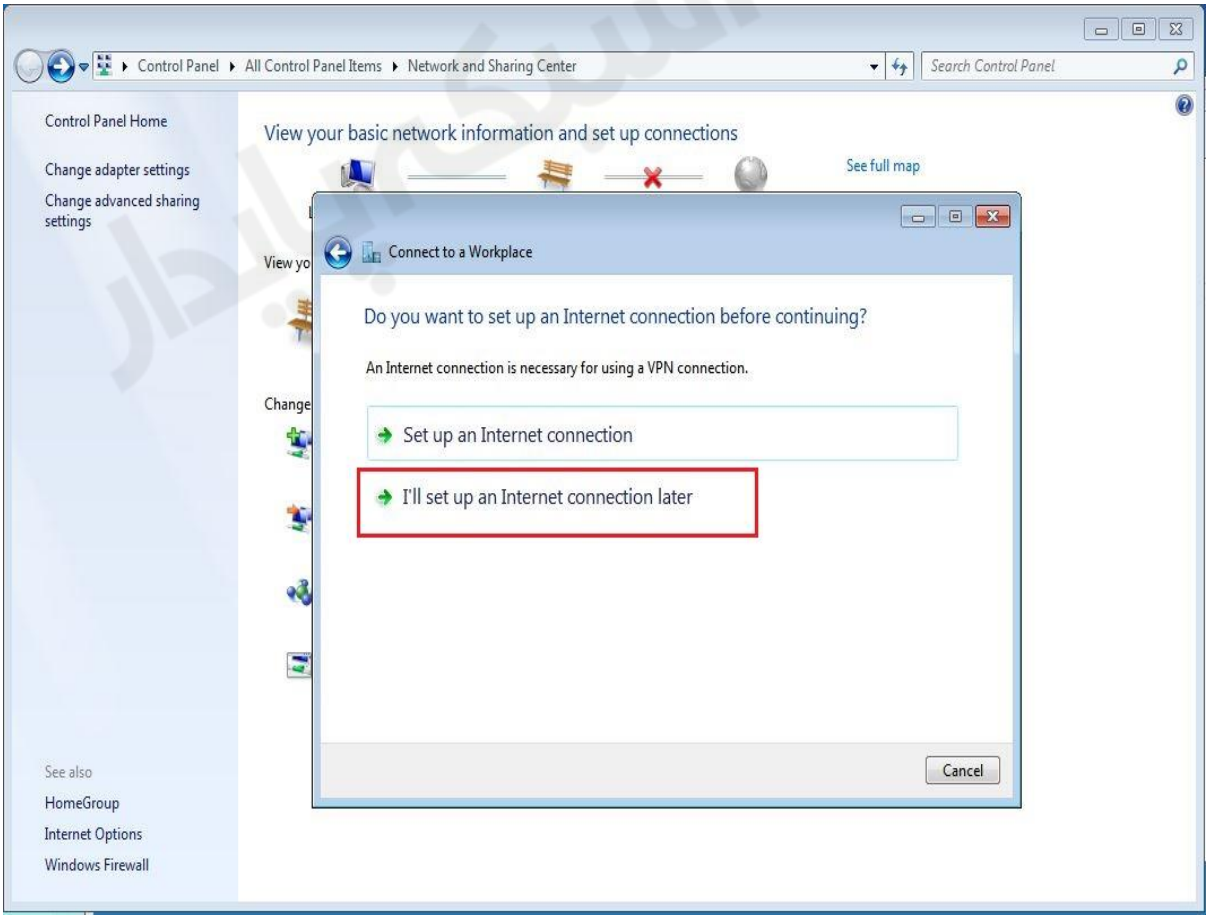
در سیستم کلاینت باید یک Vpn Connection ایجاد کنیم برای اینکار به مسیر زیر فته :

Control Panel > Network and Sharing > Setup new Connection or network >

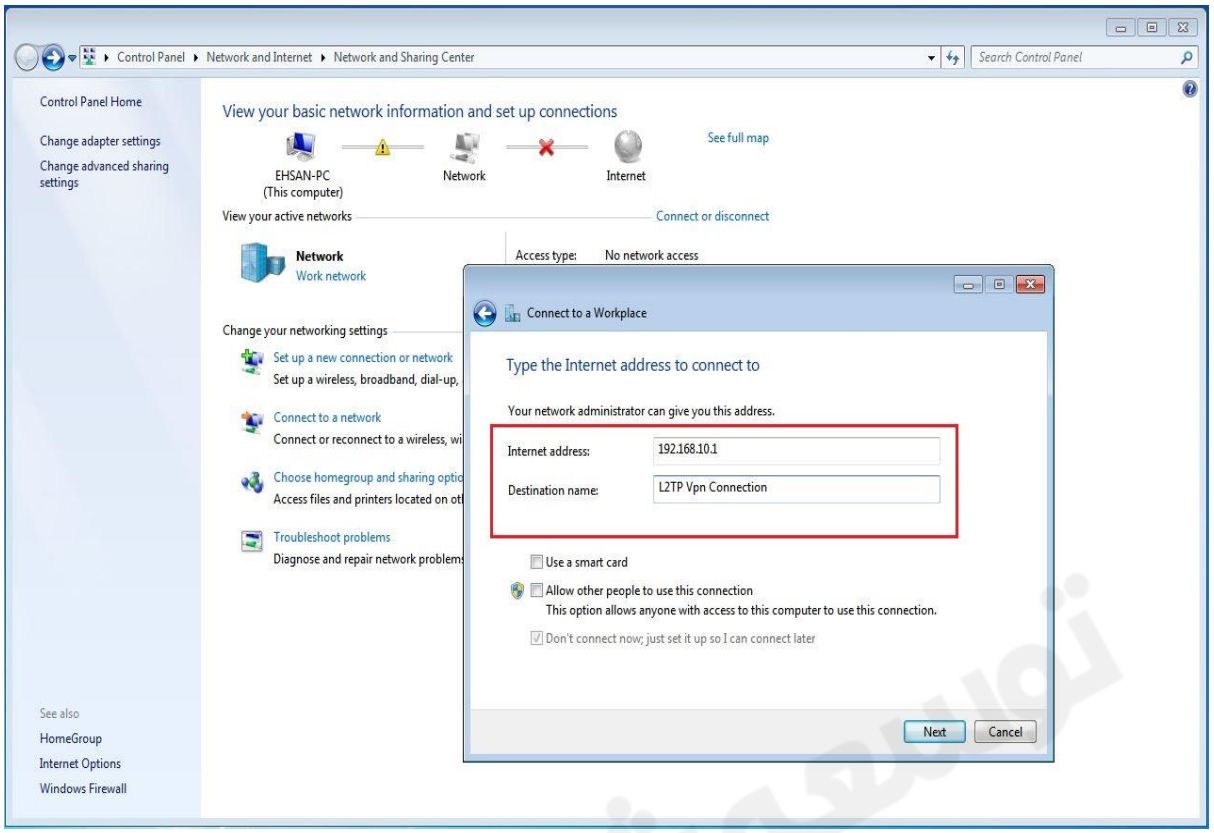

Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
LANSEGMET1-PC
(This computer)
Network
Internet
View your active networks
Connect or disconnect
Network
Public network
Access type: No Internet access
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
HomeGroup
Internet Options
Windows Firewall


Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a new network
Configure a new router or access point.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Set up a dial-up connection
Connect to the Internet using a dial-up connection.
Next
Cancel
See also
HomeGroup
Internet Options
Windows Firewall

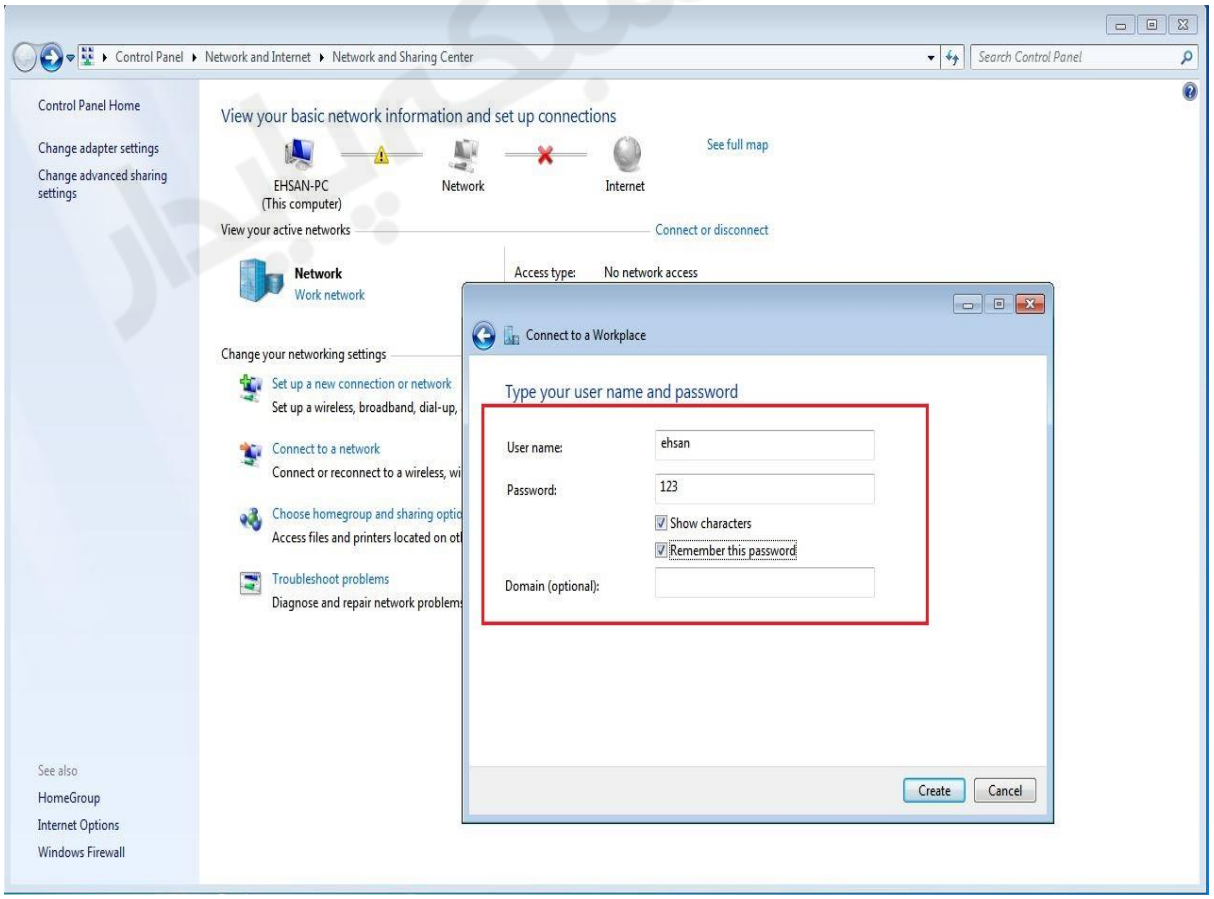

Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
Connect to a Workplace
How do you want to connect?
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.
Dial directly
Connect directly to a phone number without going through the Internet.
What is a VPN connection?
Cancel
See also
HomeGroup
Internet Options
Windows Firewall


Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
Connect to a Workplace
Do you want to set up an Internet connection before continuing?
An Internet connection is necessary for using a VPN connection.
Set up an Internet connection
I'll set up an Internet connection later
Cancel
See also
HomeGroup
Internet Options
Windows Firewall

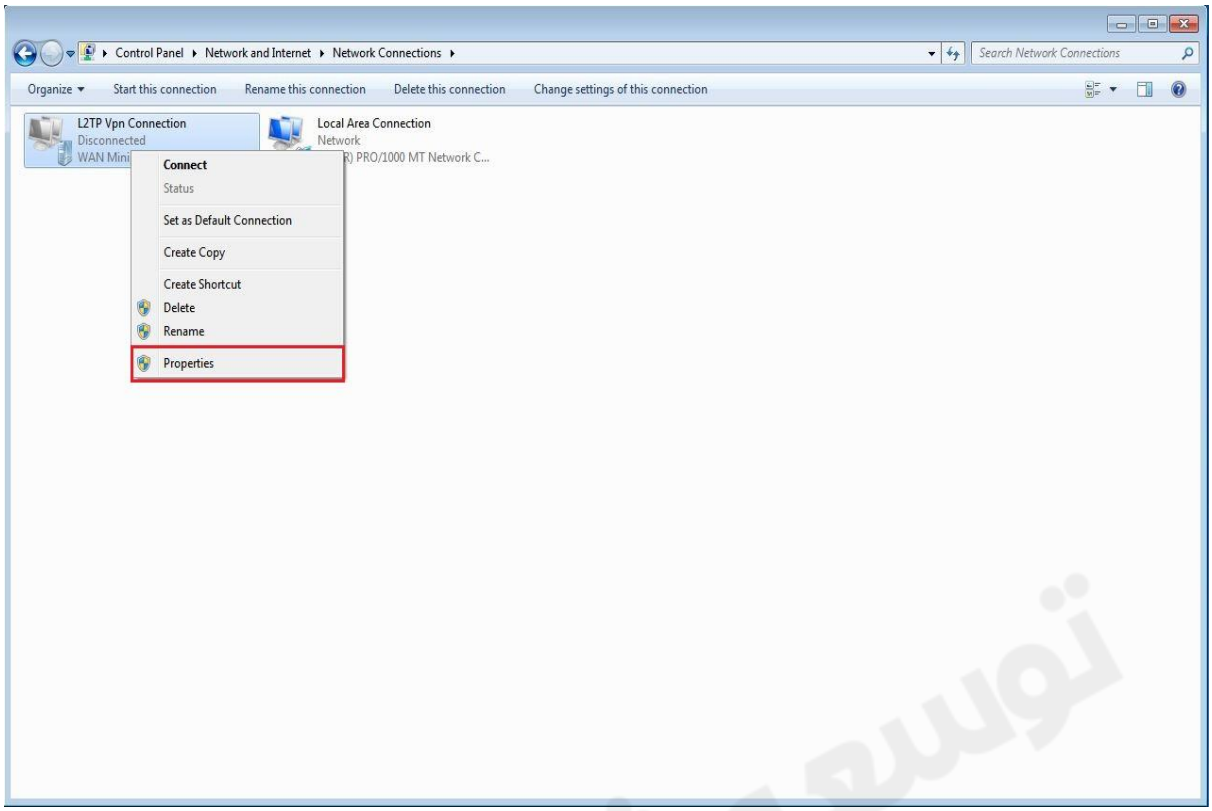
Internet Address : آدرس **IP** ، **Vpn Server** را وارد می کنیم.



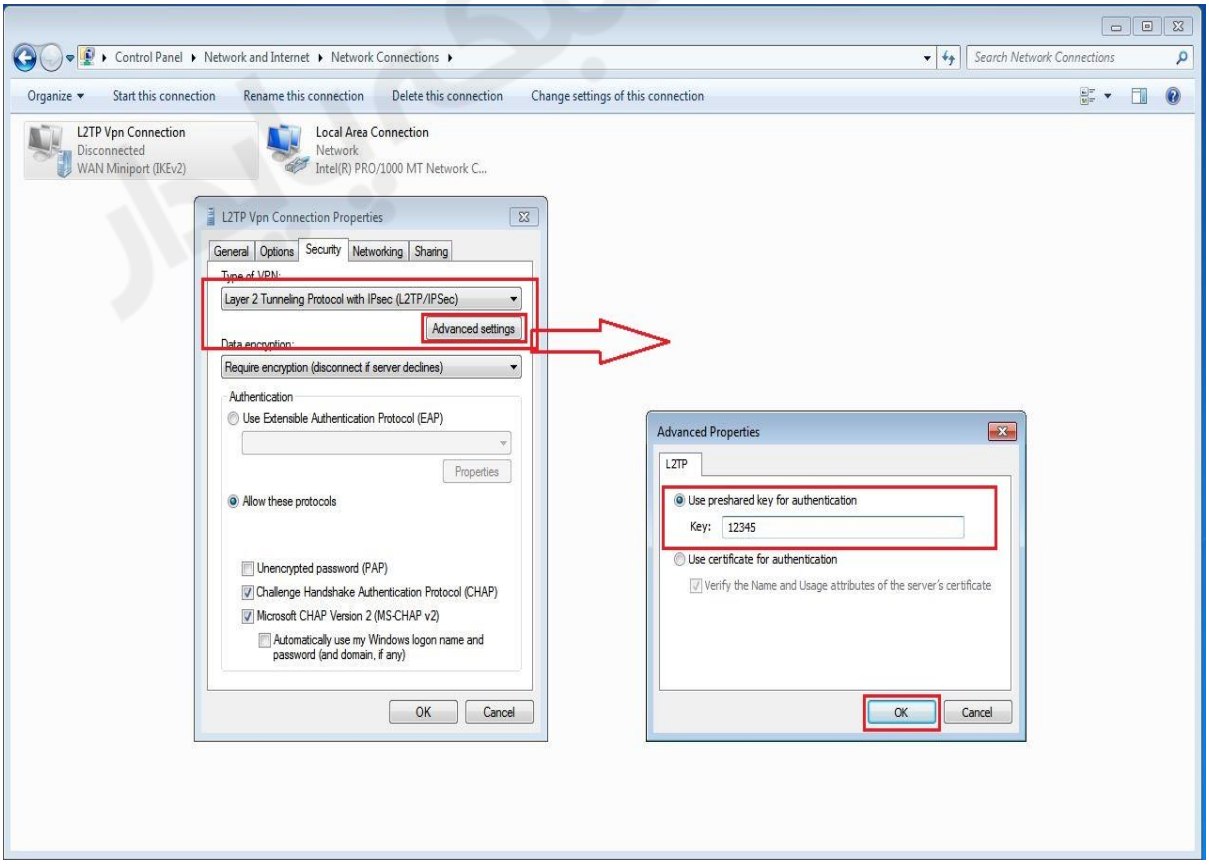
یوزرنیم و پسوردی که در روتر R3 ایجاد کردیم را وارد می کنیم.



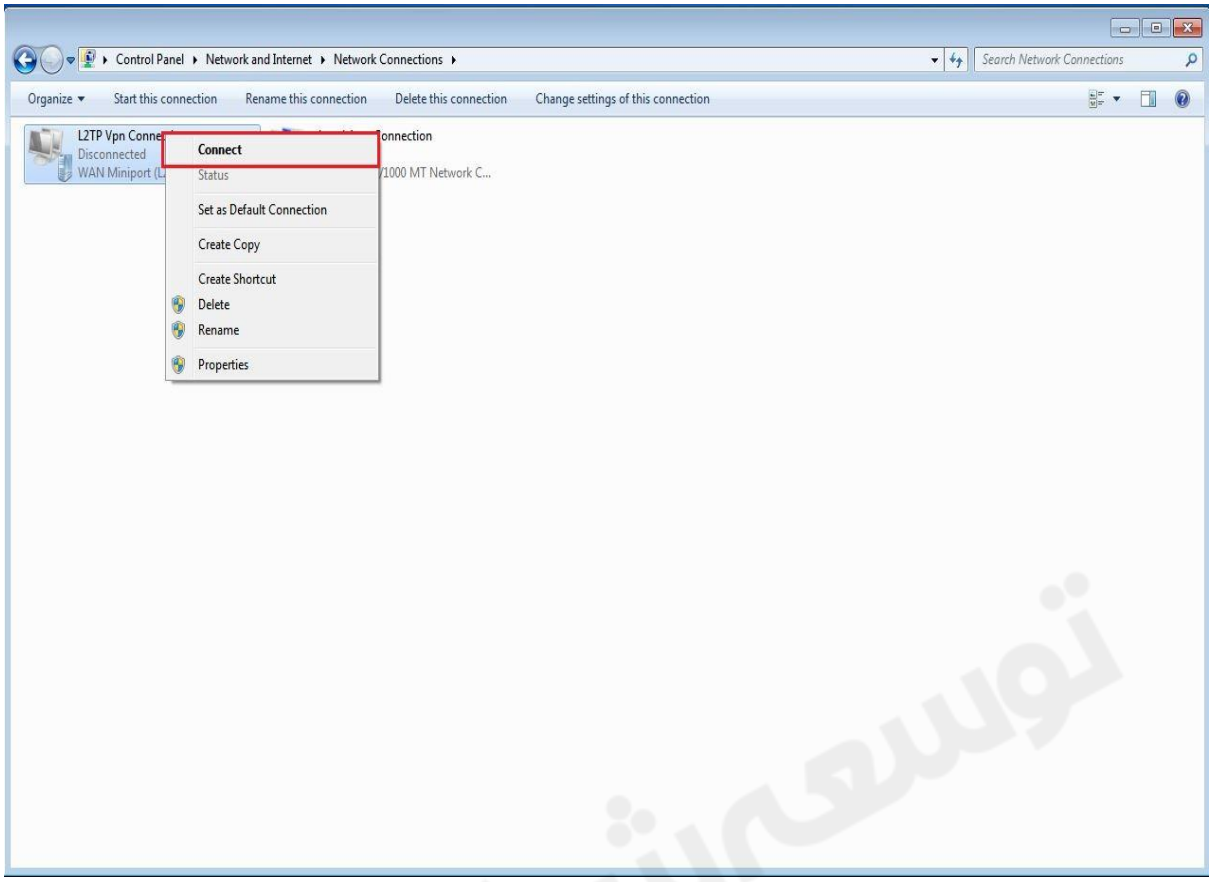
بر روی **Connection** ایجاد شده کلیک راست و **Properties** را انتخاب می کنیم.



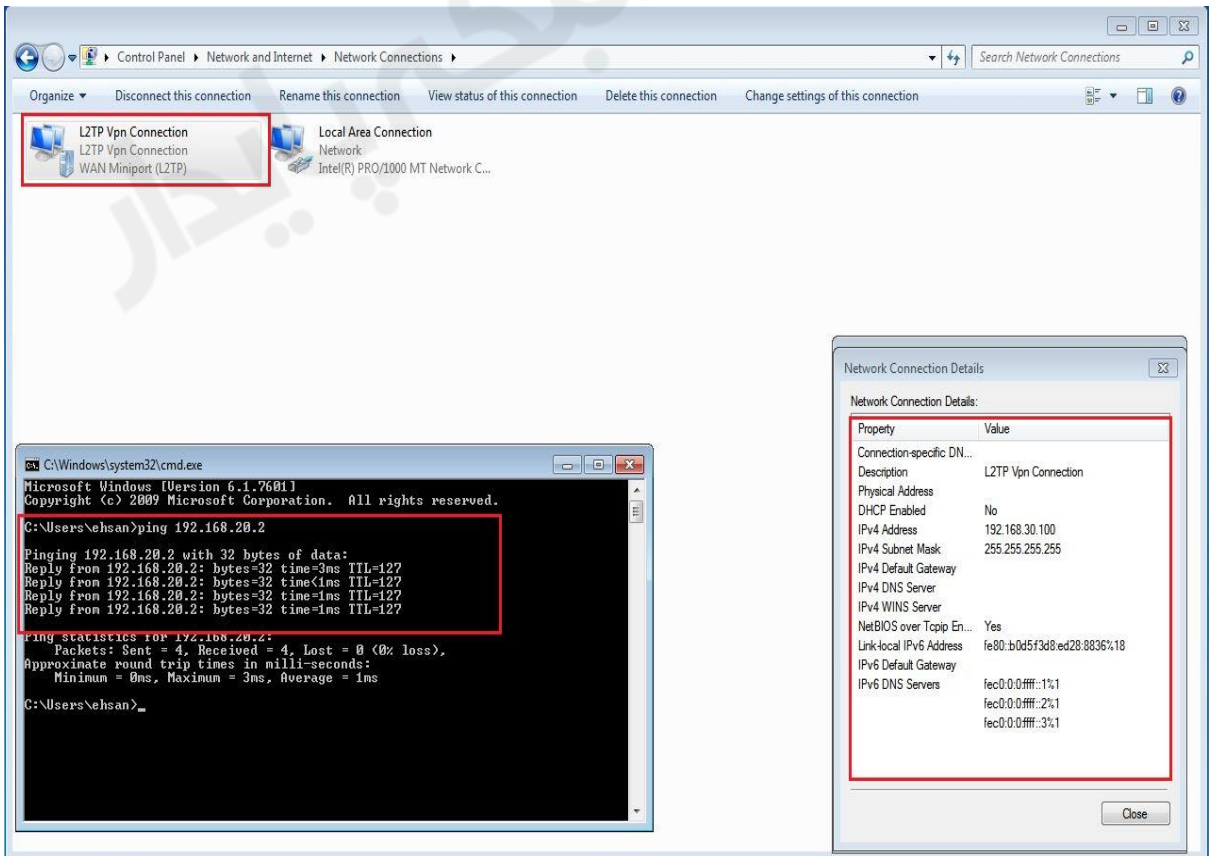
از پنجره باز شده به تب **Security** می رویم و **Type of Vpn** را برابر **L2TP** قرار می دهیم و بر روی **Advanced setting** کلیک میکنیم و از پنجره باز شده **Key** را برابر با **Secret** که در روتر تنظیم کردیم قرار می دهیم و **OK** می زنیم.



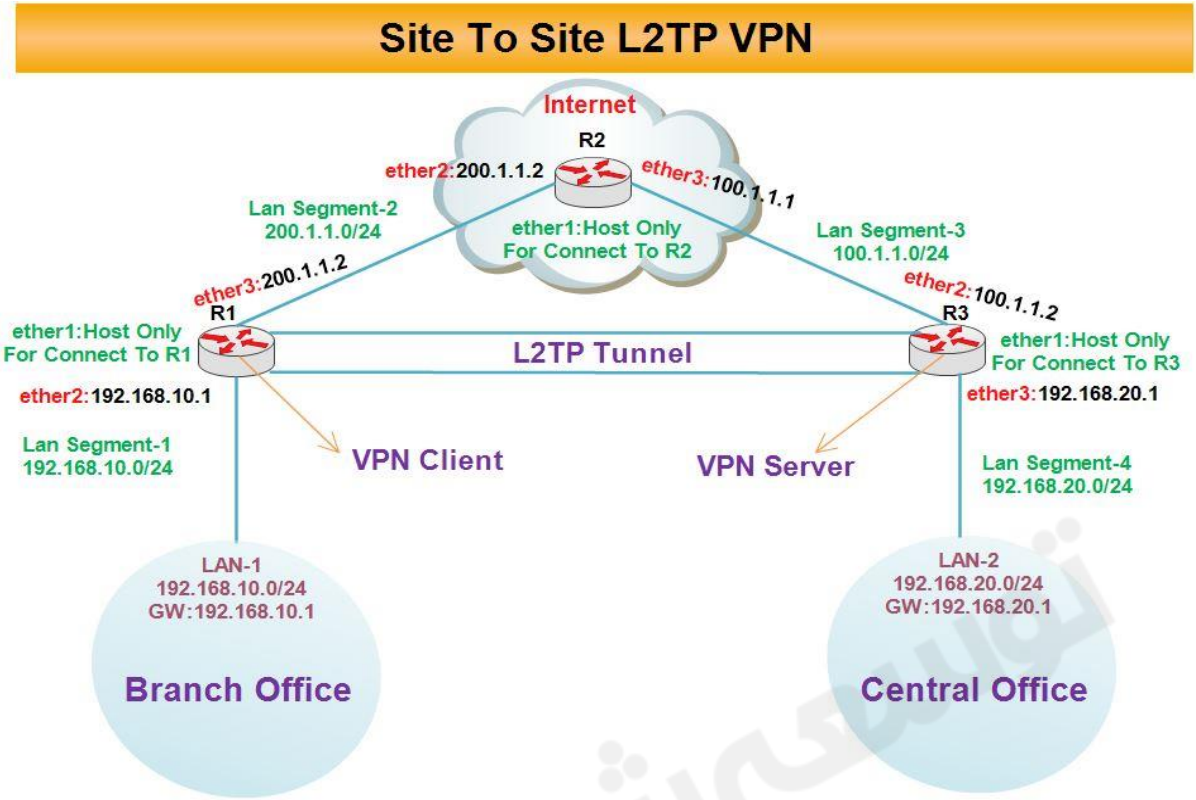
بر روی **Connection** ایجاد شده کلیک راست و بر روی **Connect** کلیک میکنیم.



همان طور که در عکس زیر مشهاده می کنید زمانی که بر روی **connect** کلیک کردید ارتباط کلاینت با شبکه **Lan-2** برقرار می شود.



سناریو ۲ : هدف از بررسی این سناریو پیاده سازی تکنیک **Site To Site** از طریق پروتکل **L2TP** می باشد.

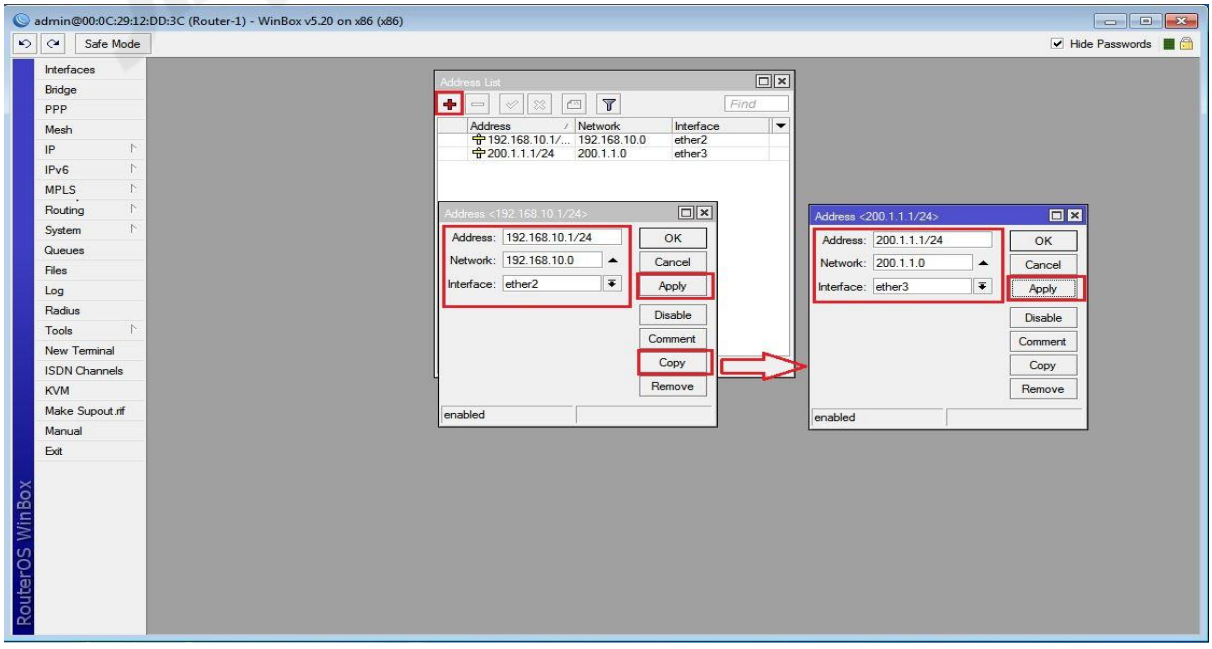


برای پیاده سازی **Site To Site** با استفاده از پروتکل **L2TP** سناریو زیر را بررسی می کنیم :

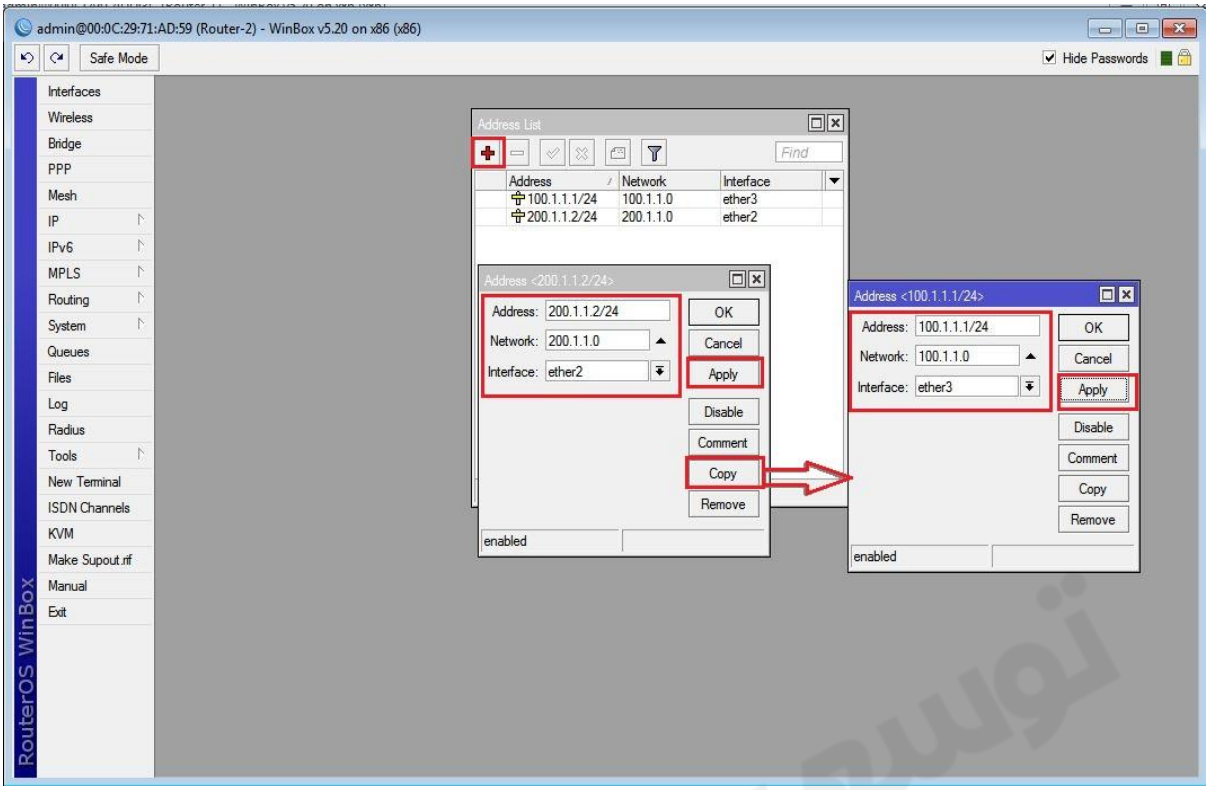
بطور مثال فرض کنید در شعبه مرکزی یک شرکت یک سرور اتوماسیون اداری وجود دارد این سرور یک **IP Valid** از محدود **IP**های شبکه داخلی دارد چنانچه بخواهیم کلاینت های موجود در بقیه شعبه های شرکت نیز بتوانند به این سرور متصل شوند(با استفاده از همان **Invalid IP**) از تکنیک **Site To Site** استفاده می کنیم.

انتساب **IP** به کارت های شبکه روترها :

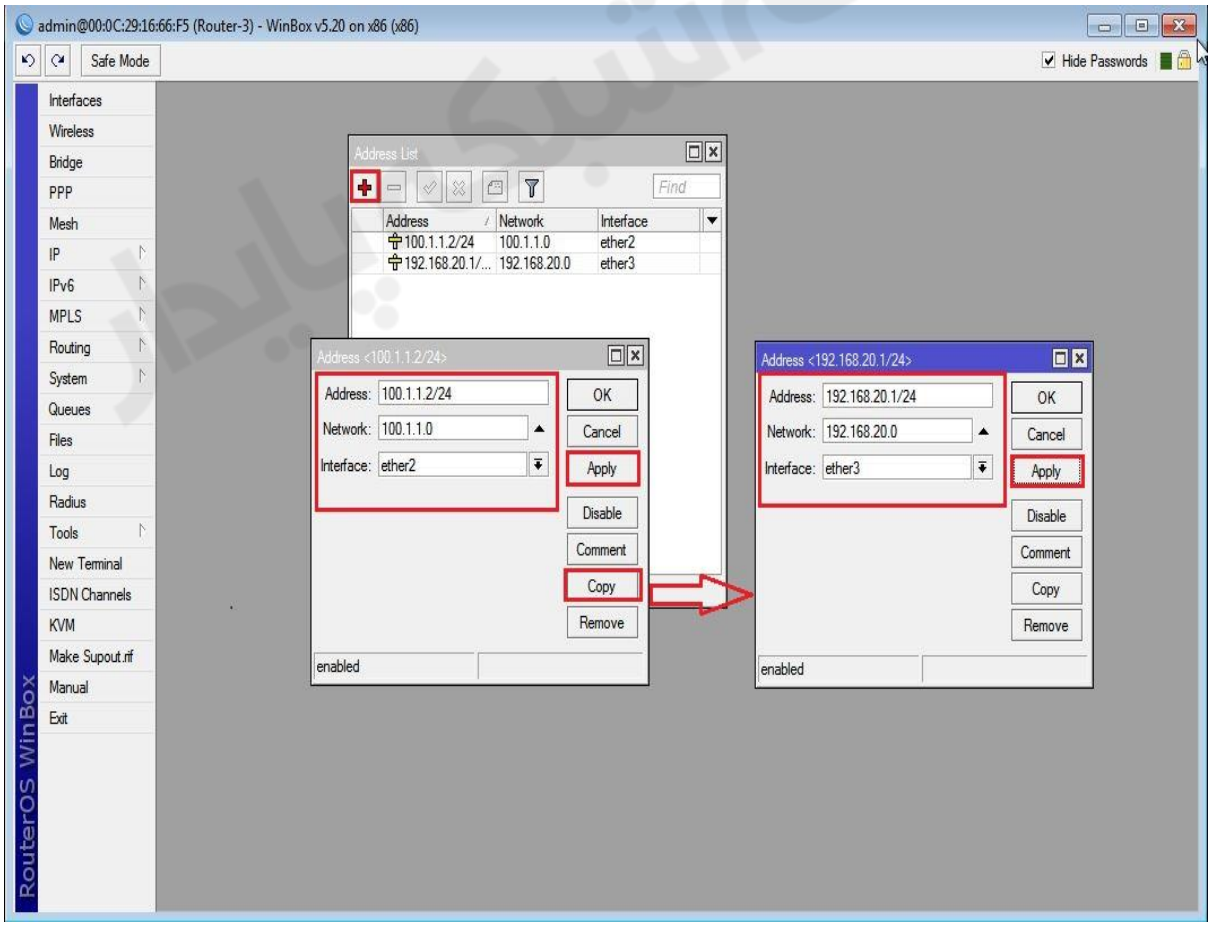
روتر **R1** :



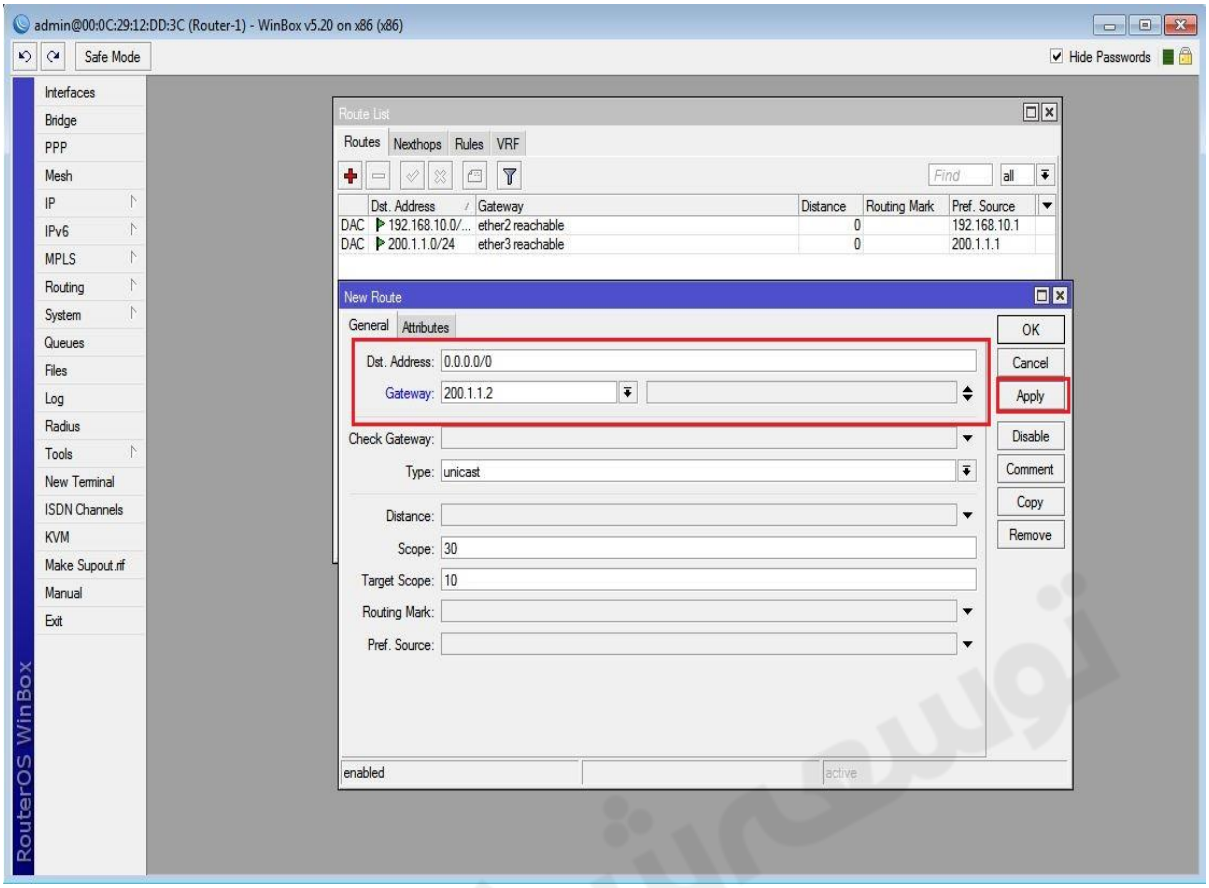
روتر **R2**:



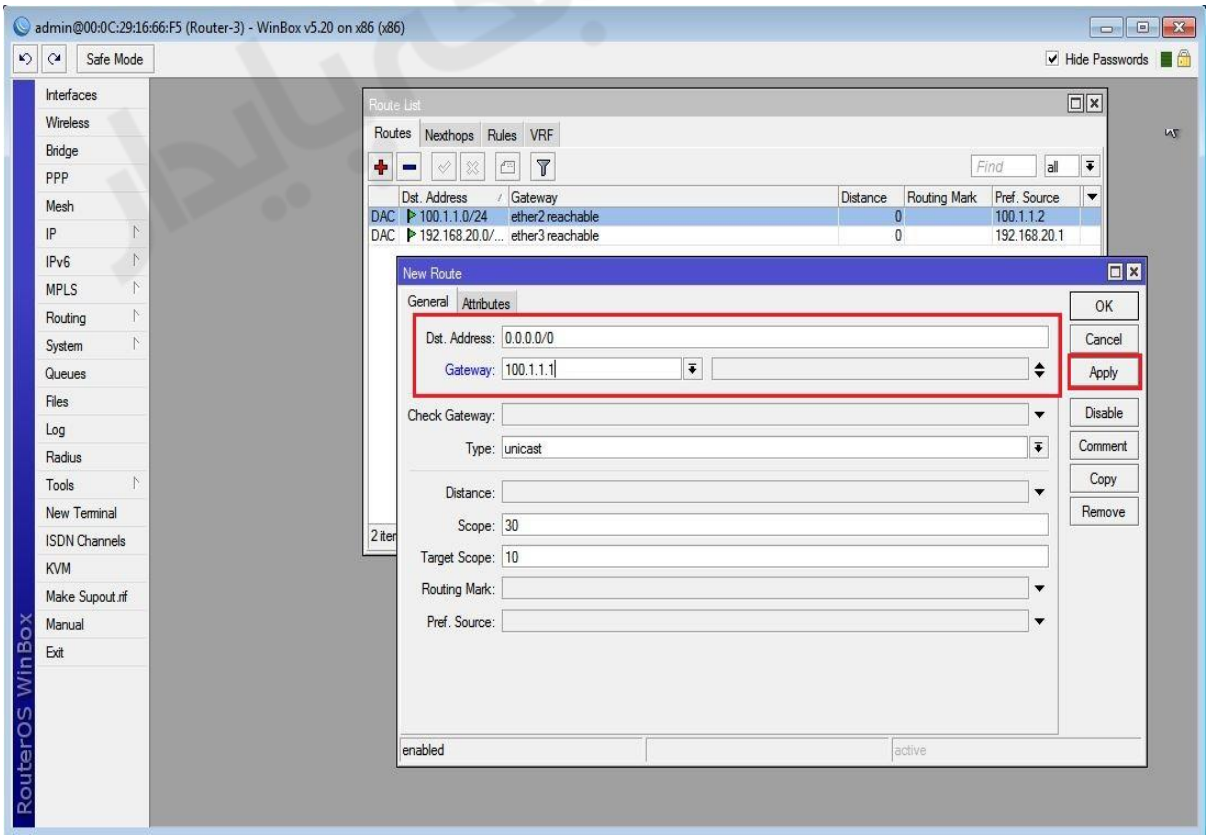
روتر **R3**:



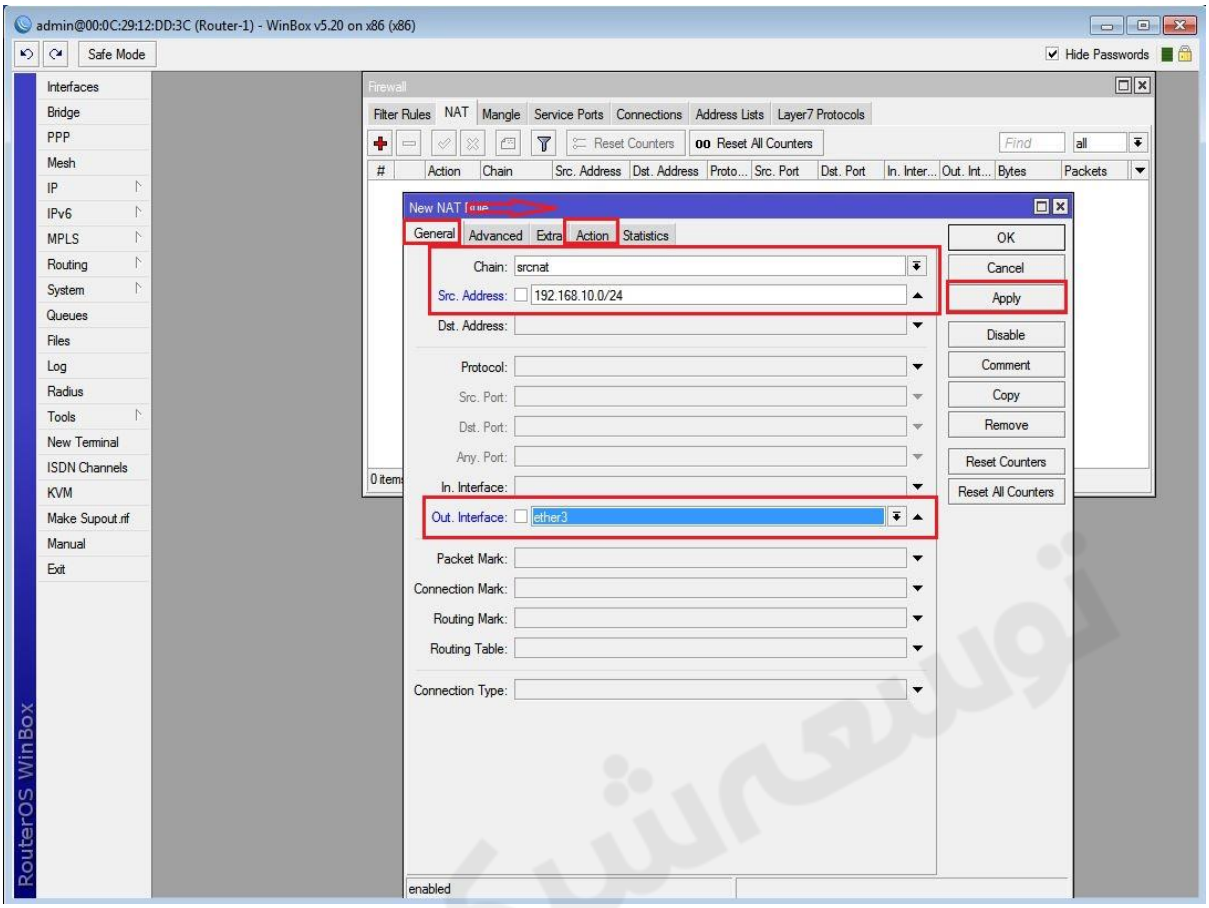
تعریف **Default Route** در روتر **R1** :

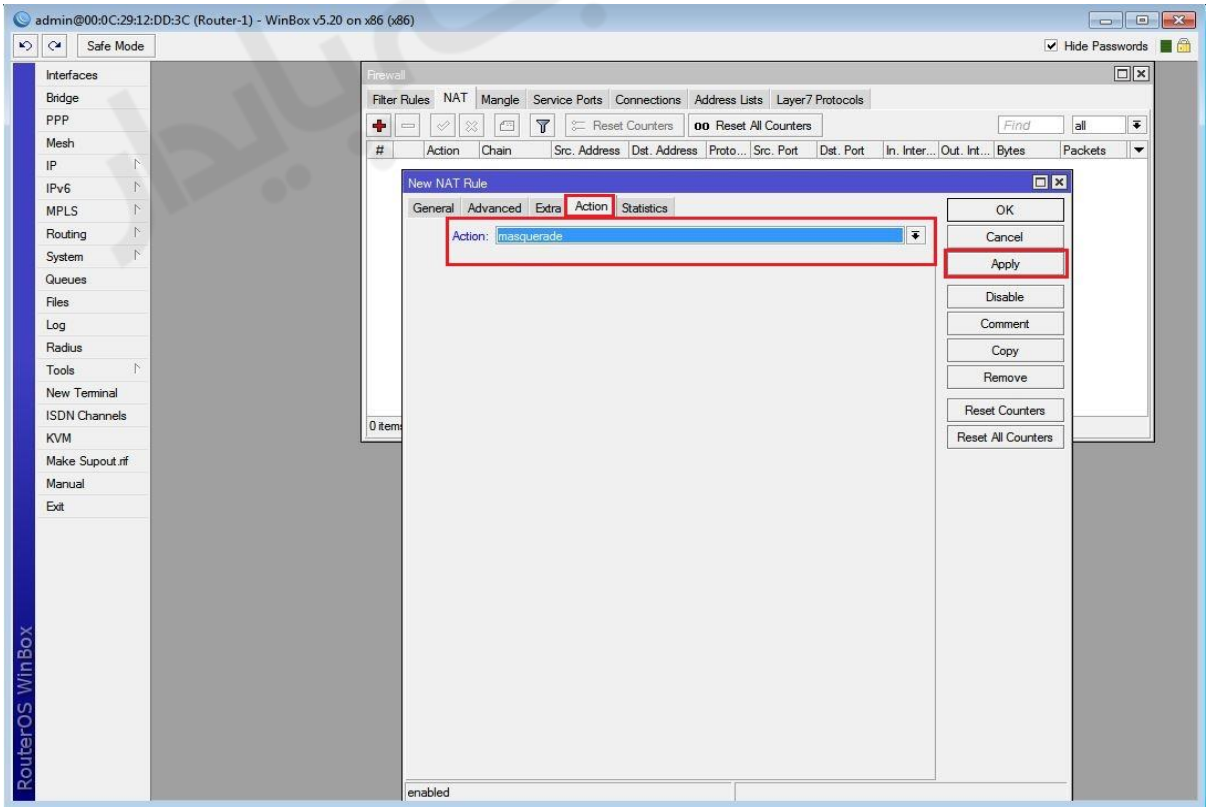


تعریف **Default Route** در **R3** :

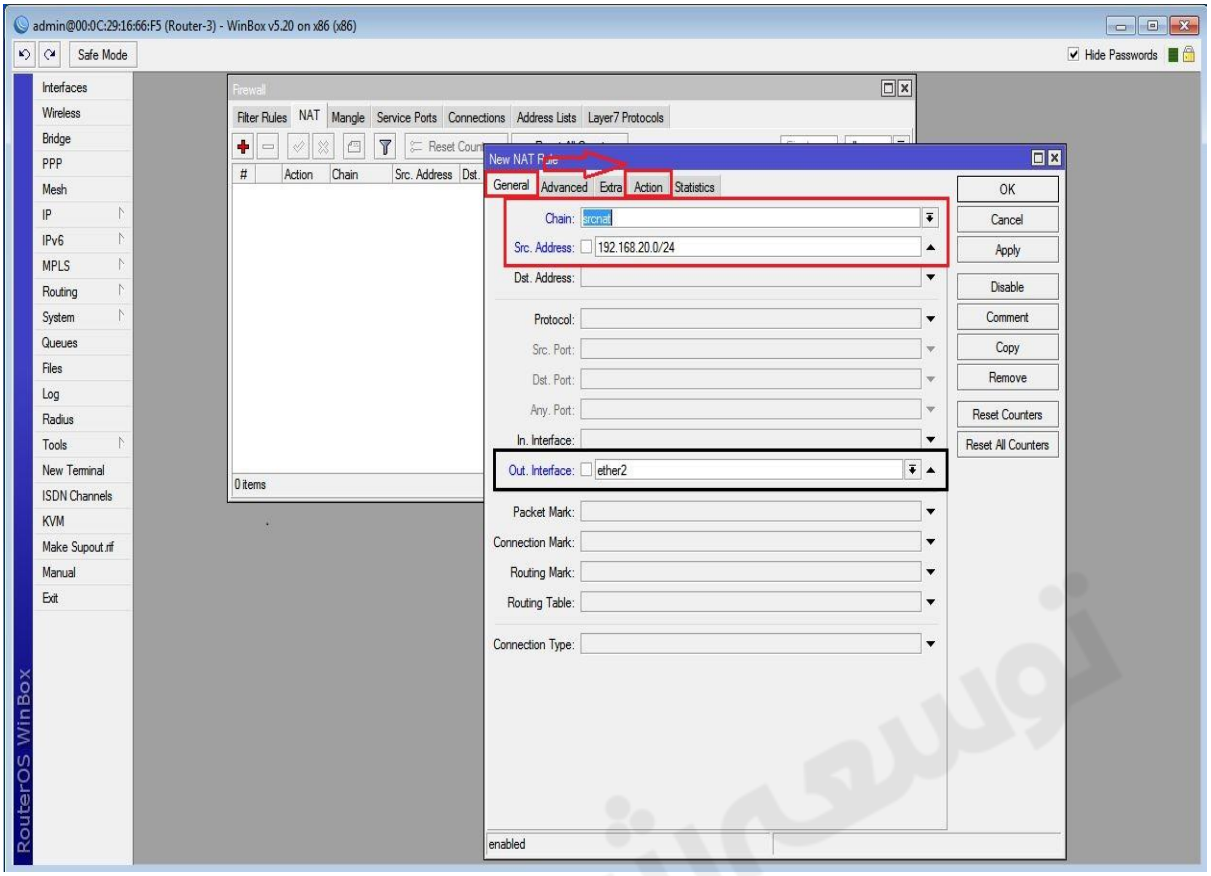


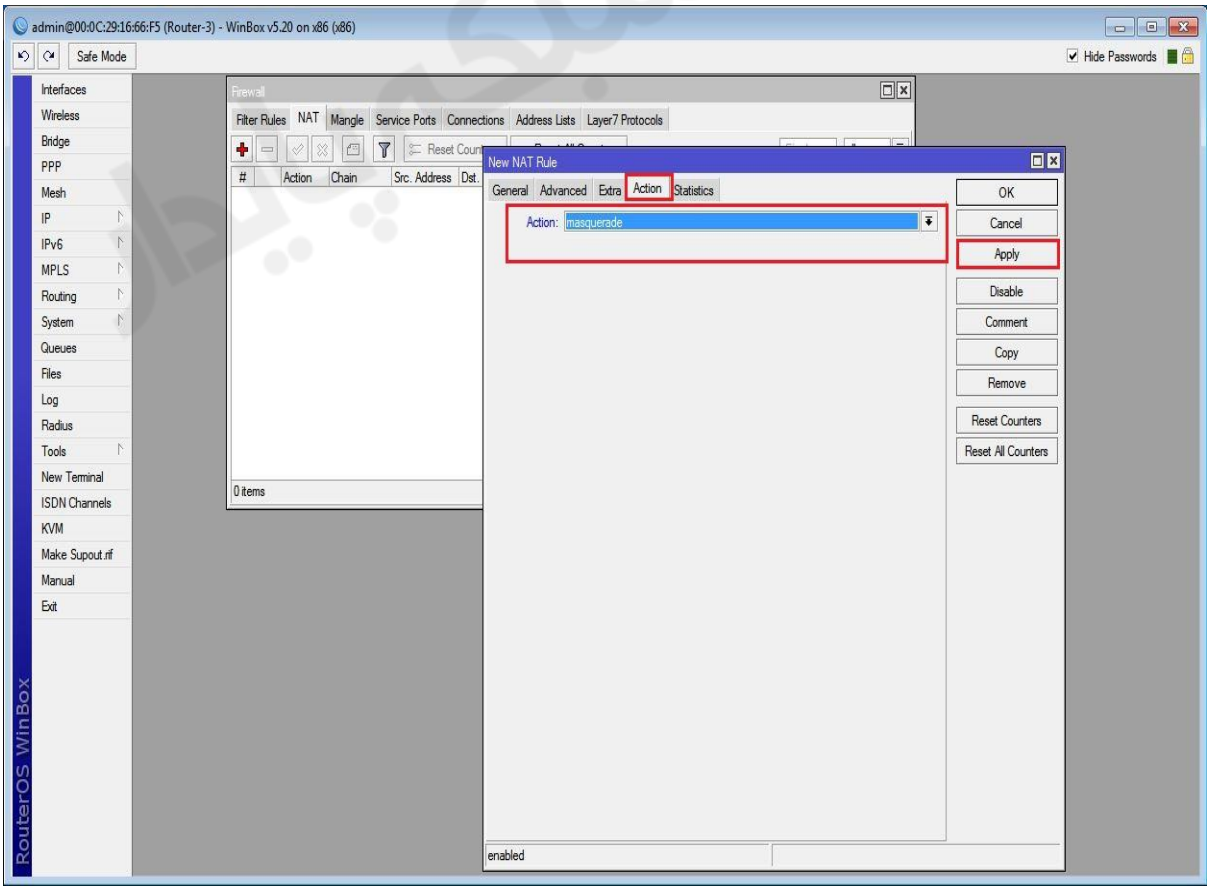
ایجاد Nat در روتر R1 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.



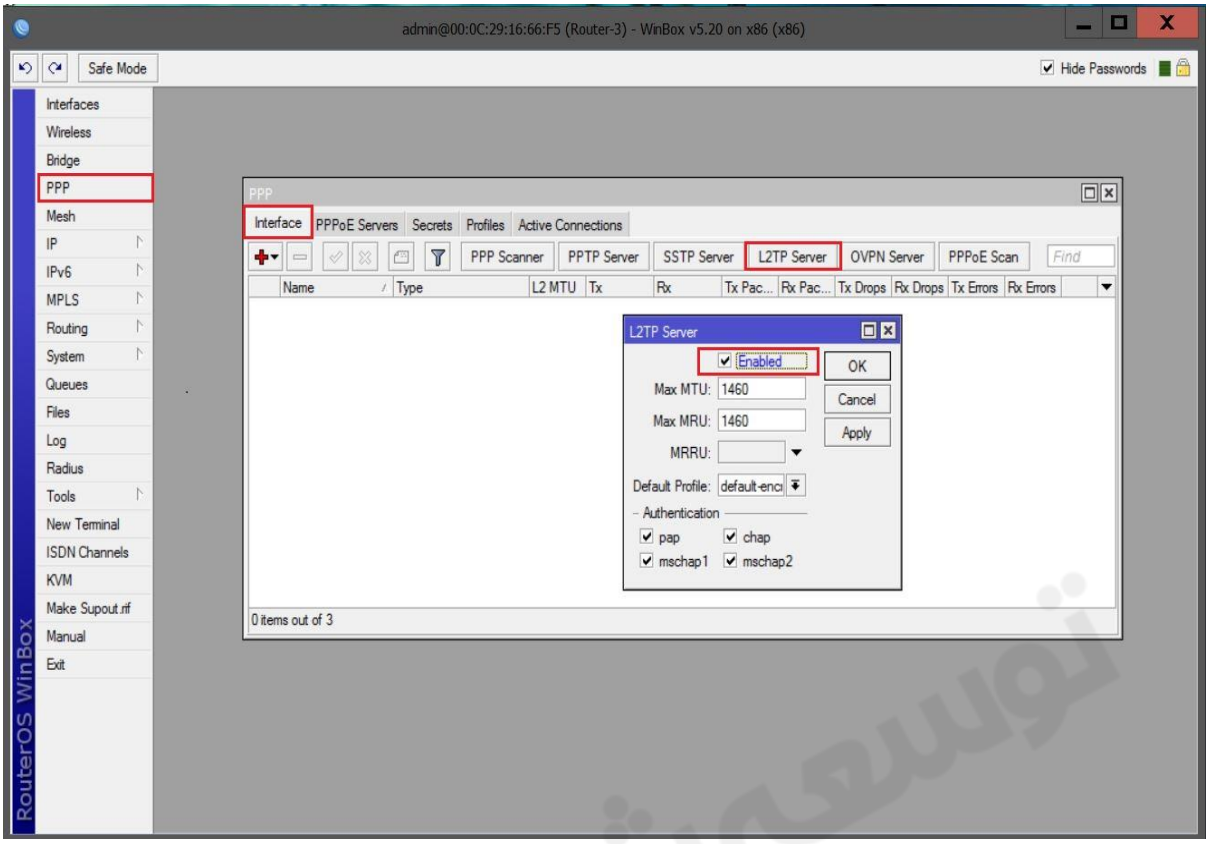


ایجاد Nat در روتر R3 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.

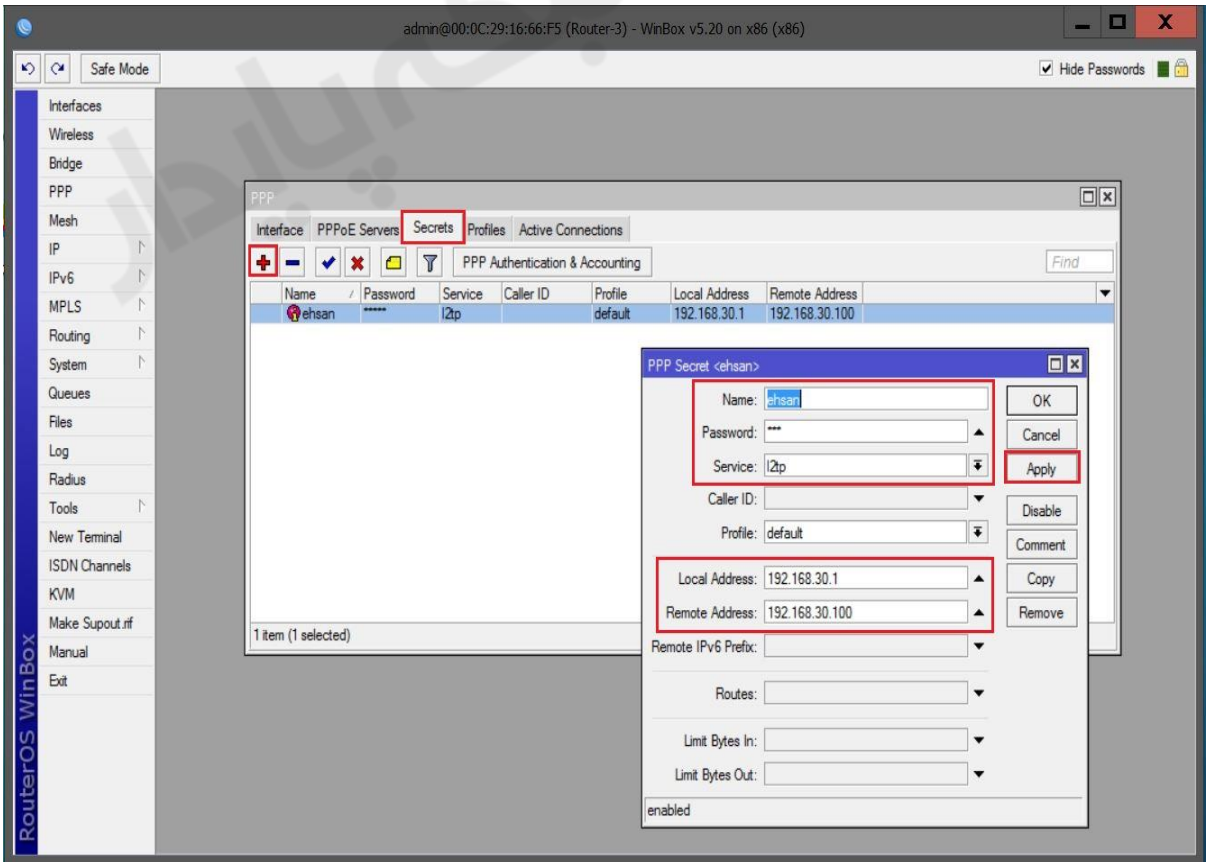




فعال سازی سرویس L2TP Server در روتر R3 :

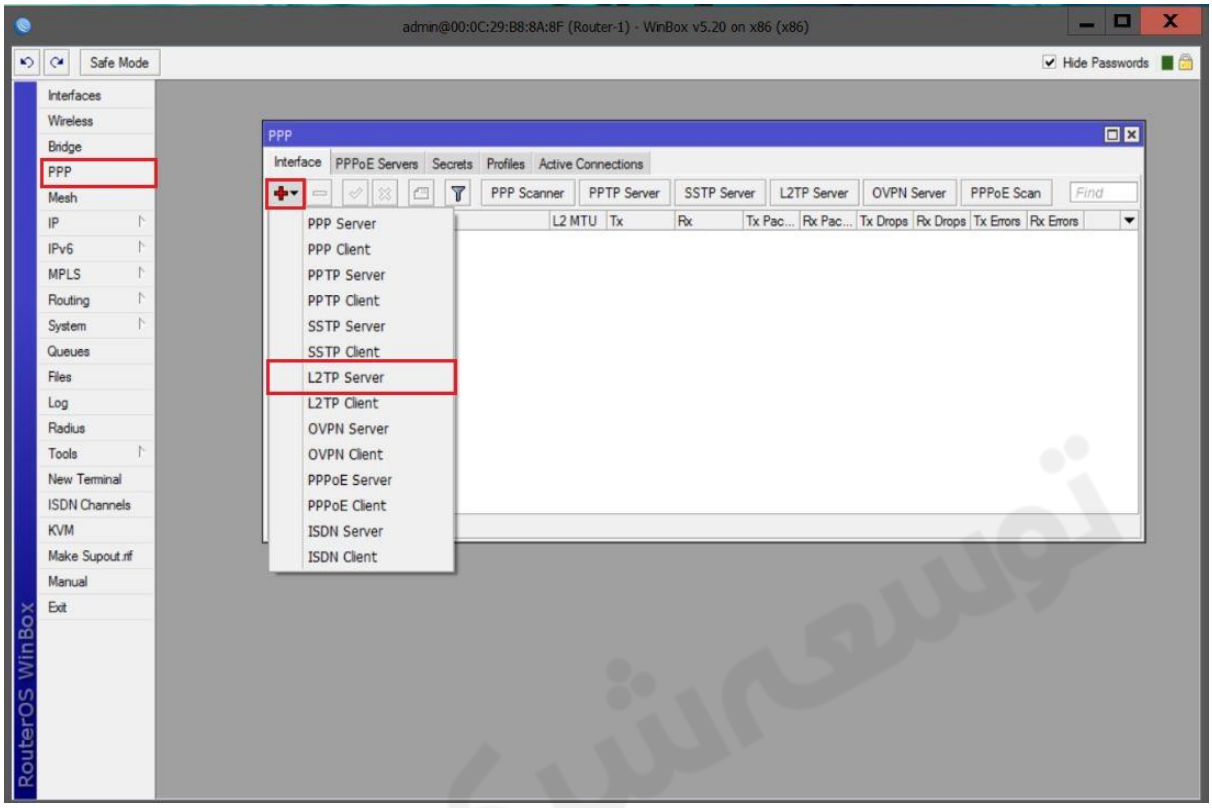


تنظیمات مربوط به سرور در روتر R3:

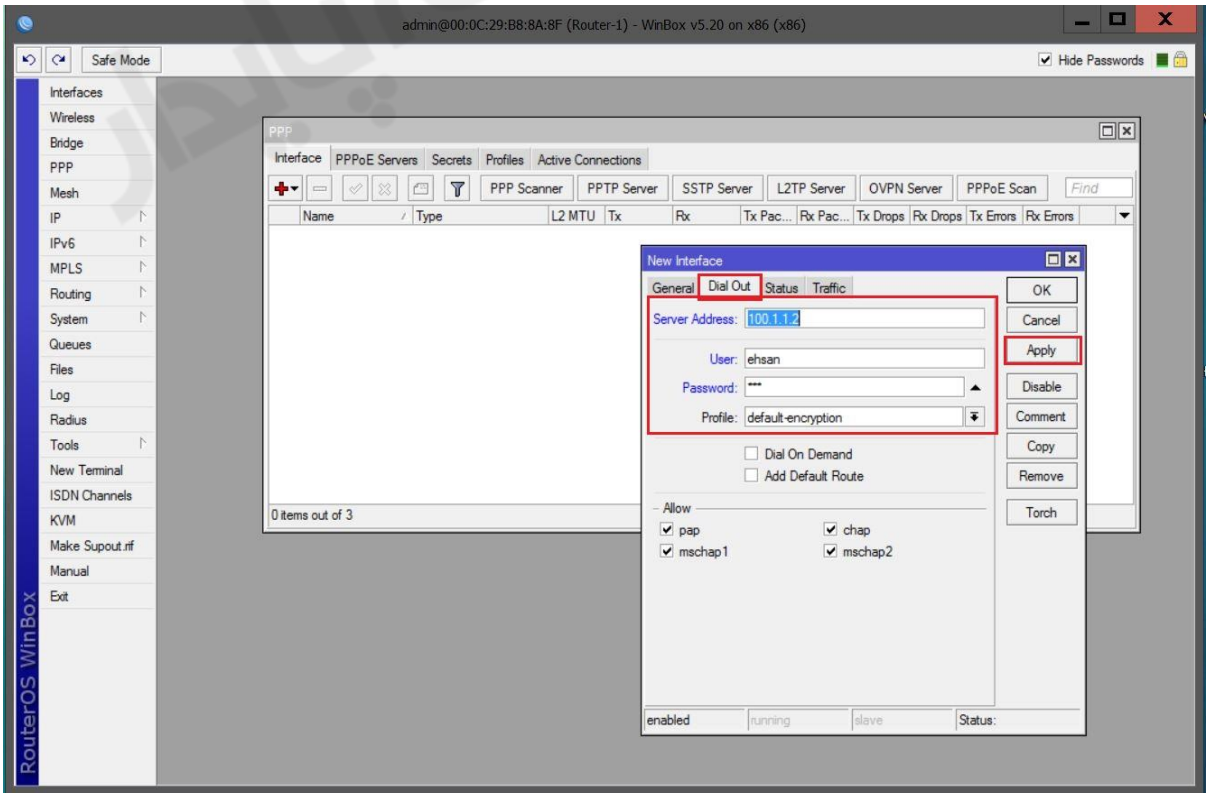


فعال سازی L2TP Client در روتر R1 :

از منوی اصلی PPP را انتخاب و از پنجره باز شده از تب Interface بر روی Add کلیک کرده و از زیر منوی باز شده L2TP Client را انتخاب می کنیم.



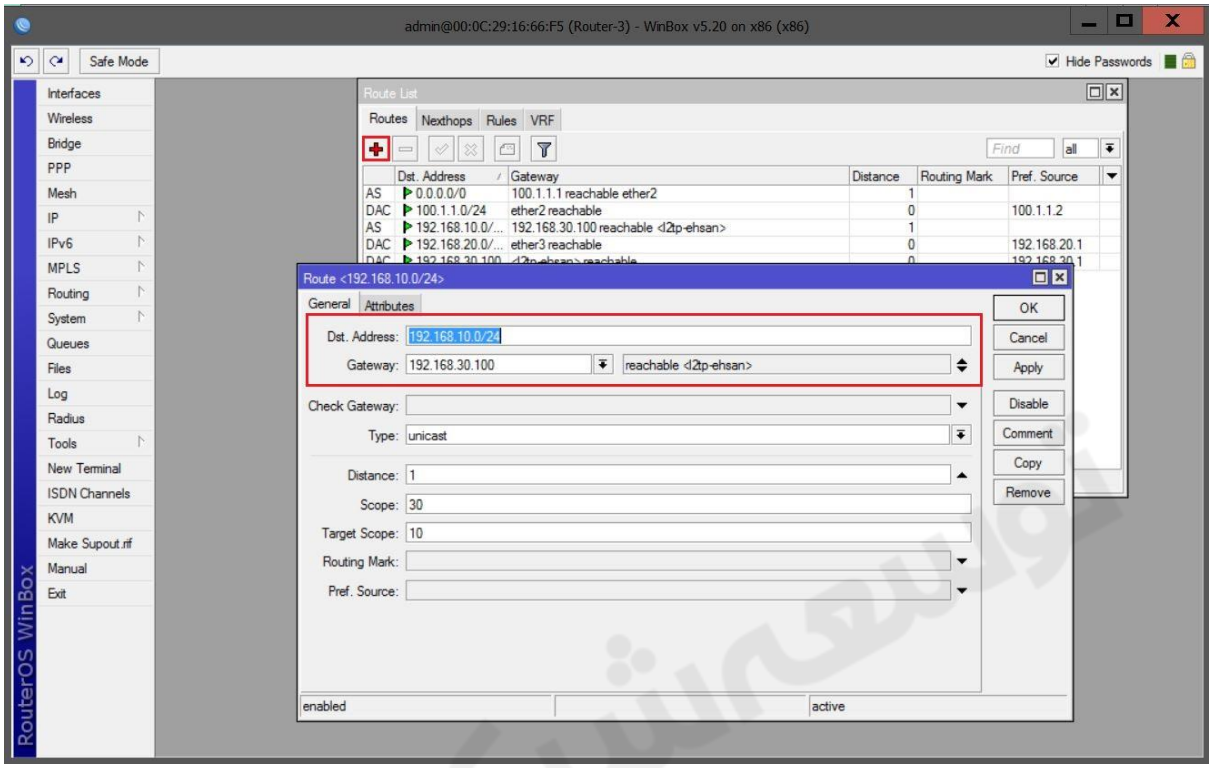
در تب Dial Out در قسمت Connect To آدرس IP ، L2TP Server و یوزرنیم و پسوردی که ساختیم را وارد می کنیم.



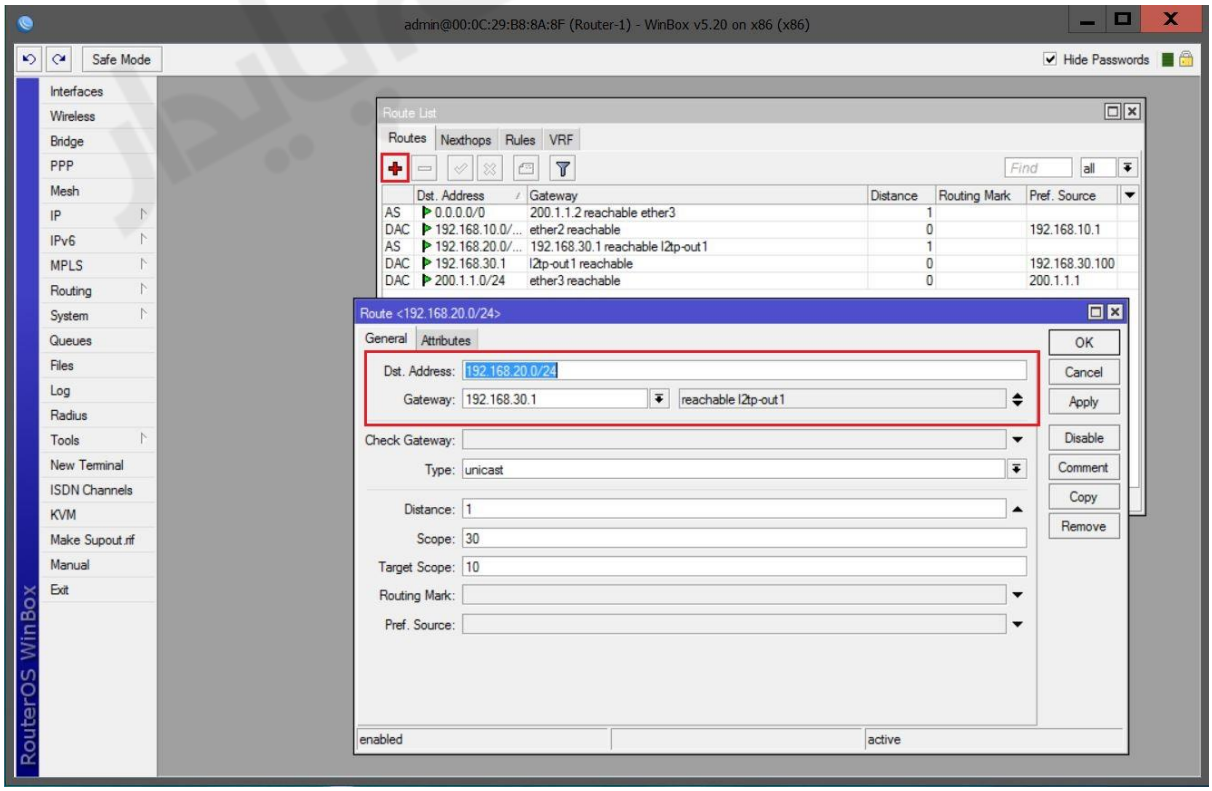
مسیریابی بسته ها در روتر R3 :

Dst.Address : در این قسمت آدرس شبکه مقصد را وارد می کنیم.

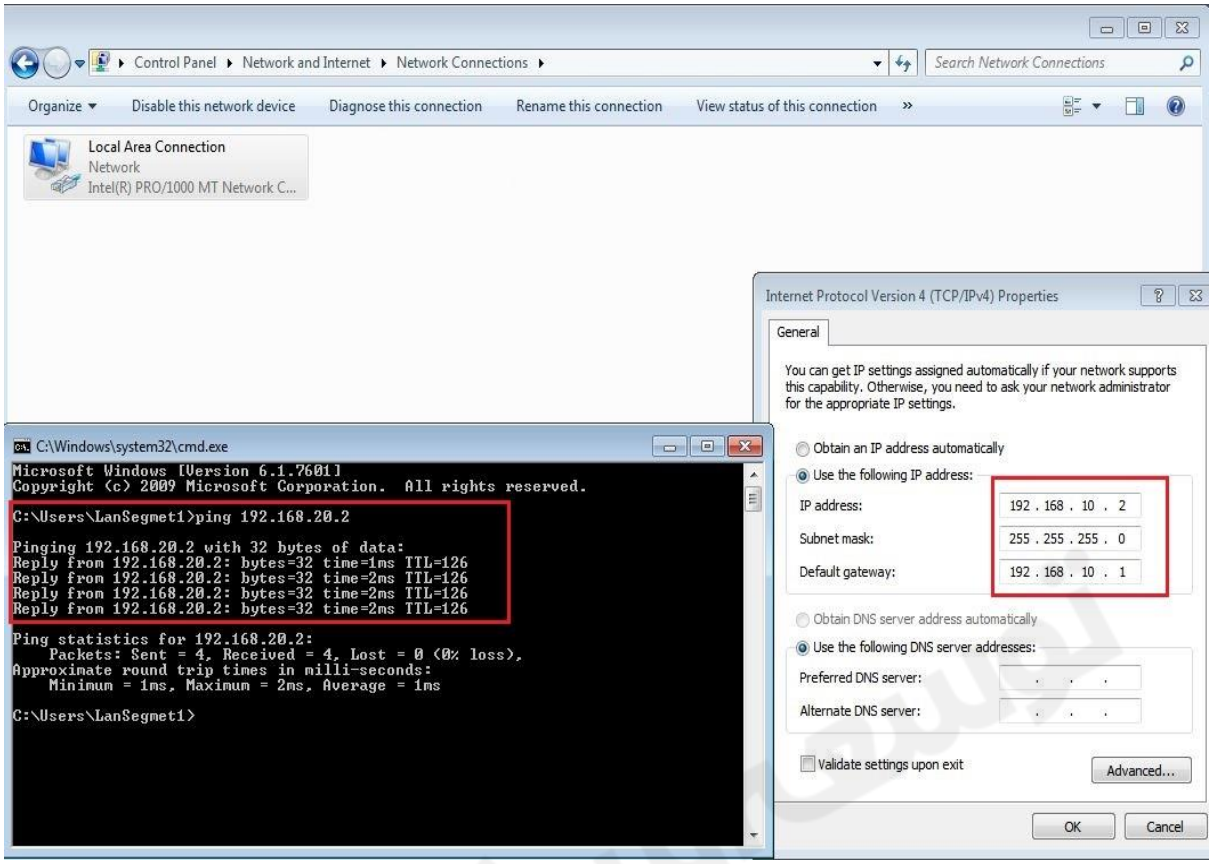
GateWay : در این قسمت آدرس کارت شبکه مجازی مربوط به به **Vpn Client** را وارد می کنیم.آدرسی که بصورت مجازی بعد از اتصال به **Vpn Server** به آن اختصاص داده می شود.

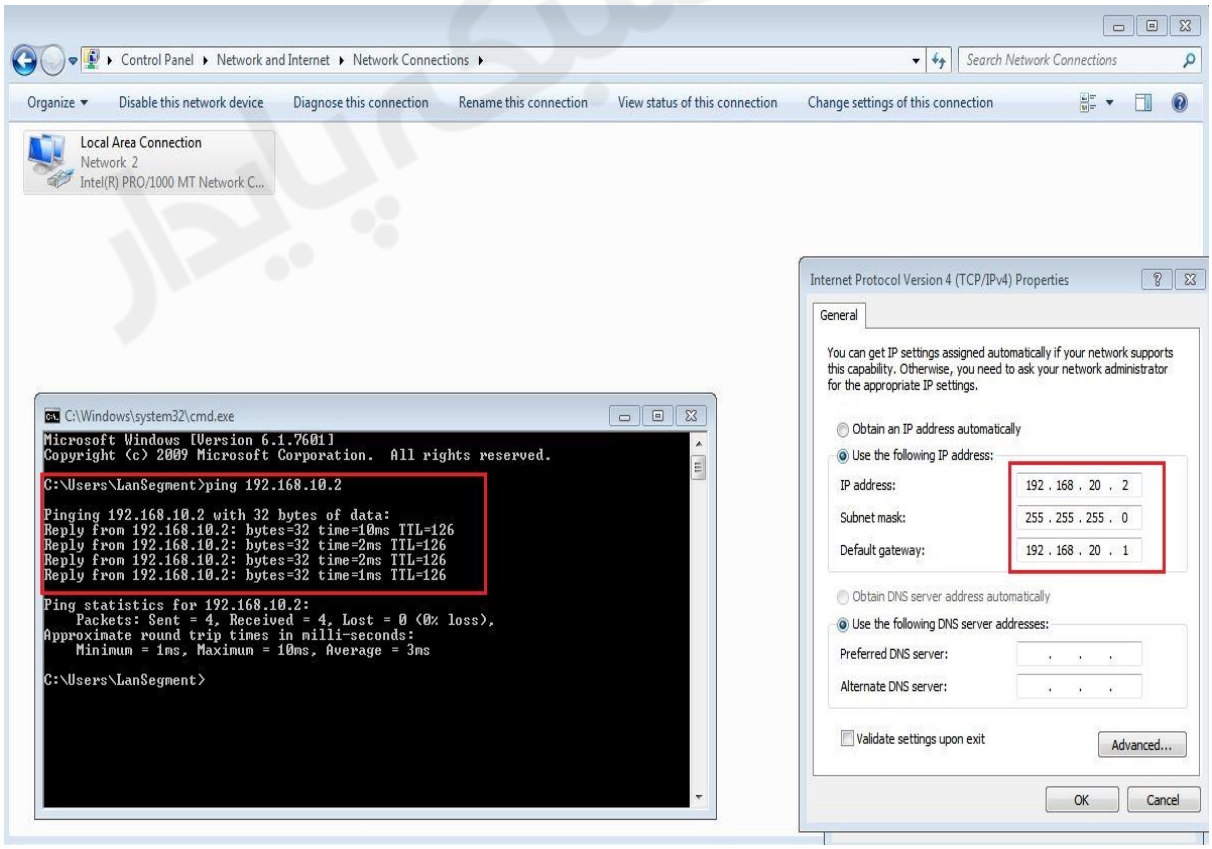


مسیریابی بسته ها در روتر R1 :



تنظیمات کلاینت :





ارتباط بین دو شبکه بصورت **Site To Site** از طریق پروتکل **L2TP** برقرار شده است.

فصل چهاردهم : IPIP Tunnel

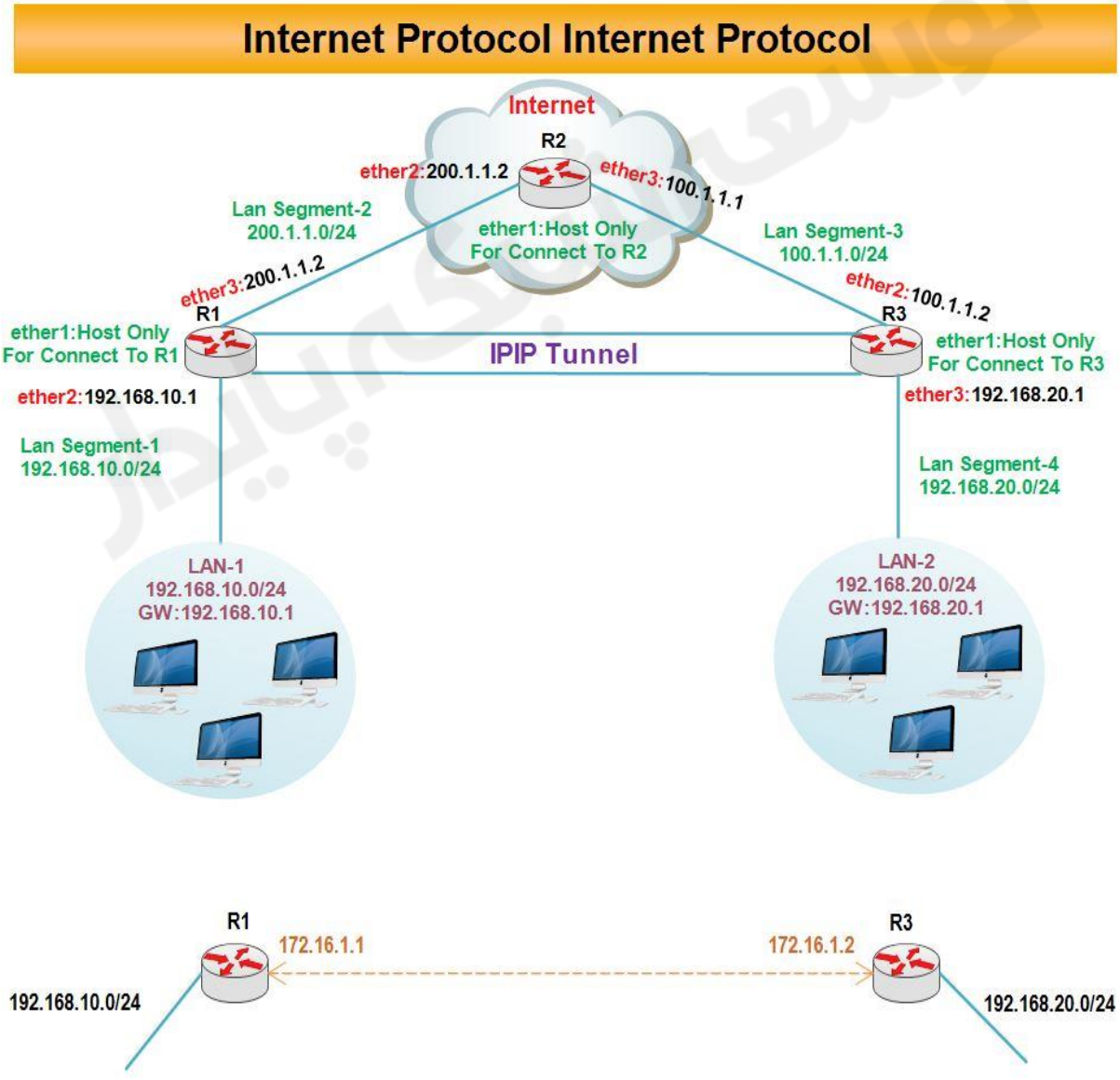
IPIP مخفف کلمه **Internet Protocol Internet Protocol** و یکی دیگر از پروتکل های **Tunneling** می باشد.این پروتکل **Open Standard** است به این معنی که در تمام سیستم عامل ها مورد استفاده قرار می گیرد و نوع سیستم عامل در سیستم مقابل مهم نیست.

این پروتکل بیشتر در محیط اینترنت کاربرد دارد.برای ارتباط روترها بایکدیگر استفاده می شود و در شرایطی خاص در اینترنت نیز پیاده سازی می شود.

عملکرد این پروتکل به این صورت است که بسته های **IP** را درون بسته های **IP** دیگر قرار می دهد و منتقل می کند.با استفاده از پروتکل **IPIP** ، دو شبکه که از لحاظ جغرافیایی دور هستند را یکپارچه می کنیم.

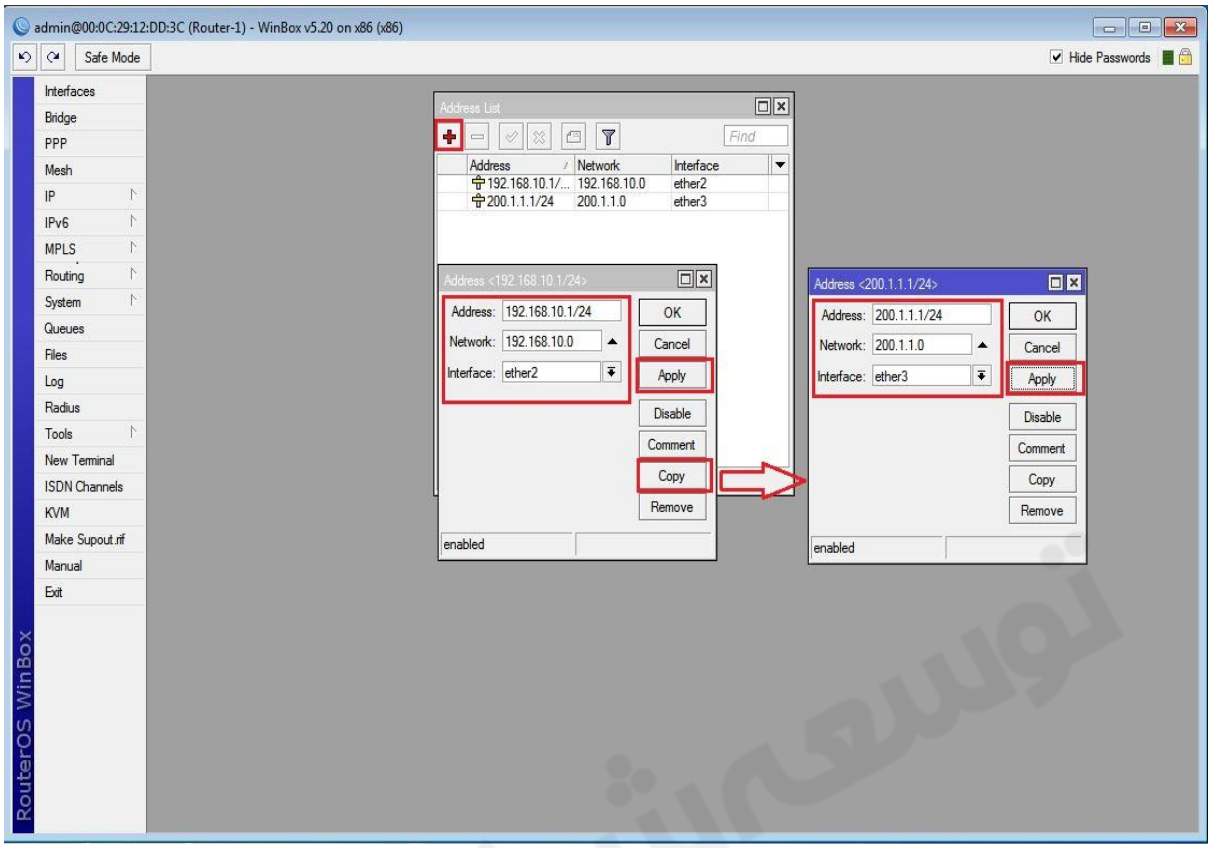
بطور کلی برای پیاده سازی این پروتکل ابتدا به سمت روتر مقابل یک **Route** فراهم می کنیم و سپس روی هر روتر یک کارت شبکه مجازی از نوع **IPIP** تعریف می شود و نهایتا به این کارت شبکه مجازی یک **IP** اختصاص داده می شود.به این ترتیب روترهای هر شبکه با استفاده از یک کابل مجازی به یکدیگر متصل می شوند.

سناریو ۱ : هدف از بررسی این سناریو ، پیاده سازی پروتکل **IPIP** می باشد.

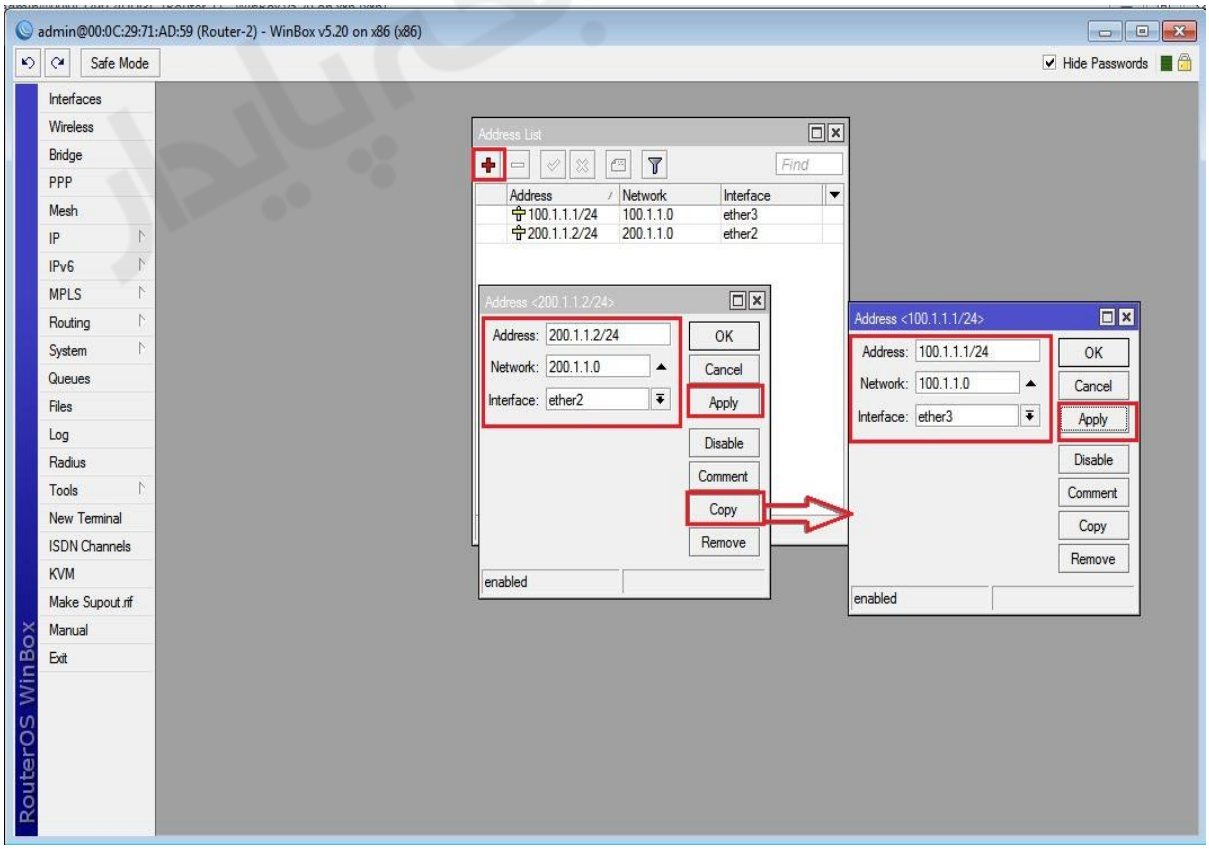


انتساب IP به کارت های شبکه روترها :

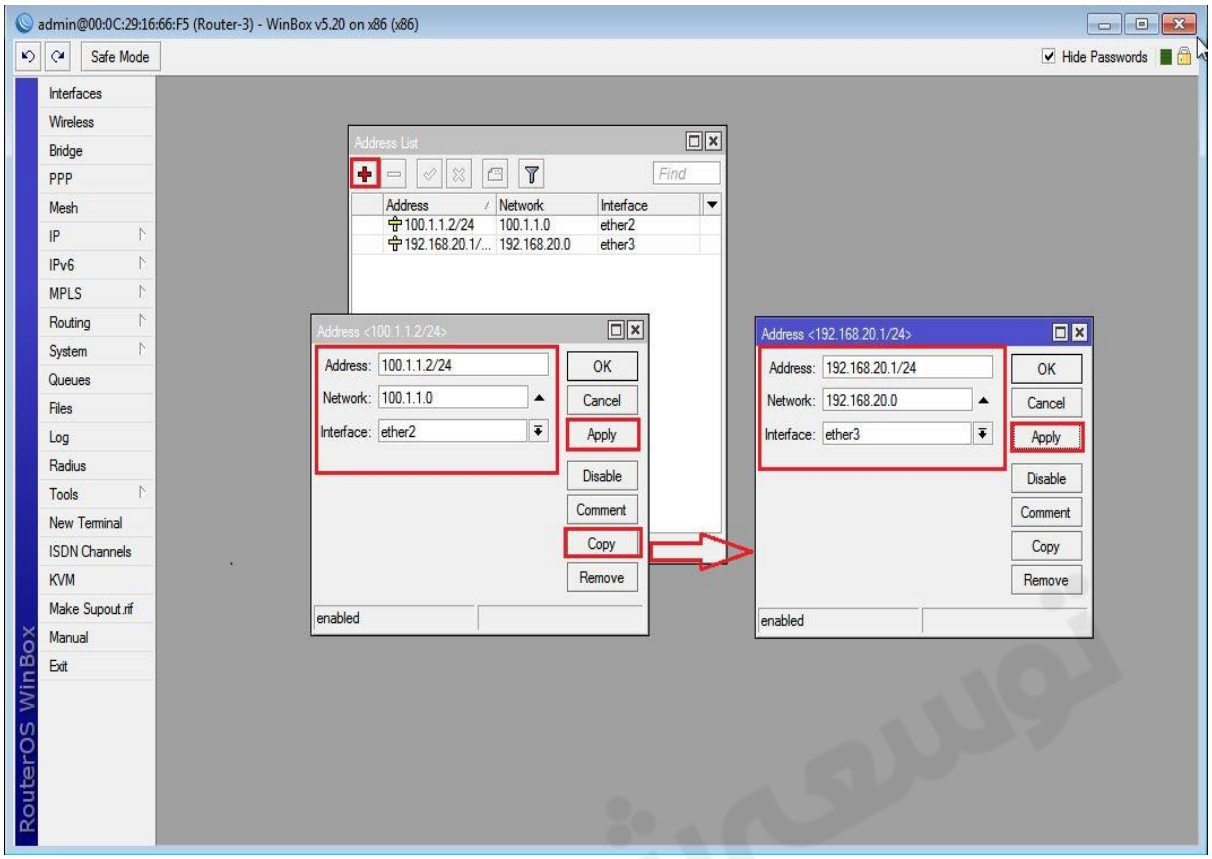
روتر R1 :



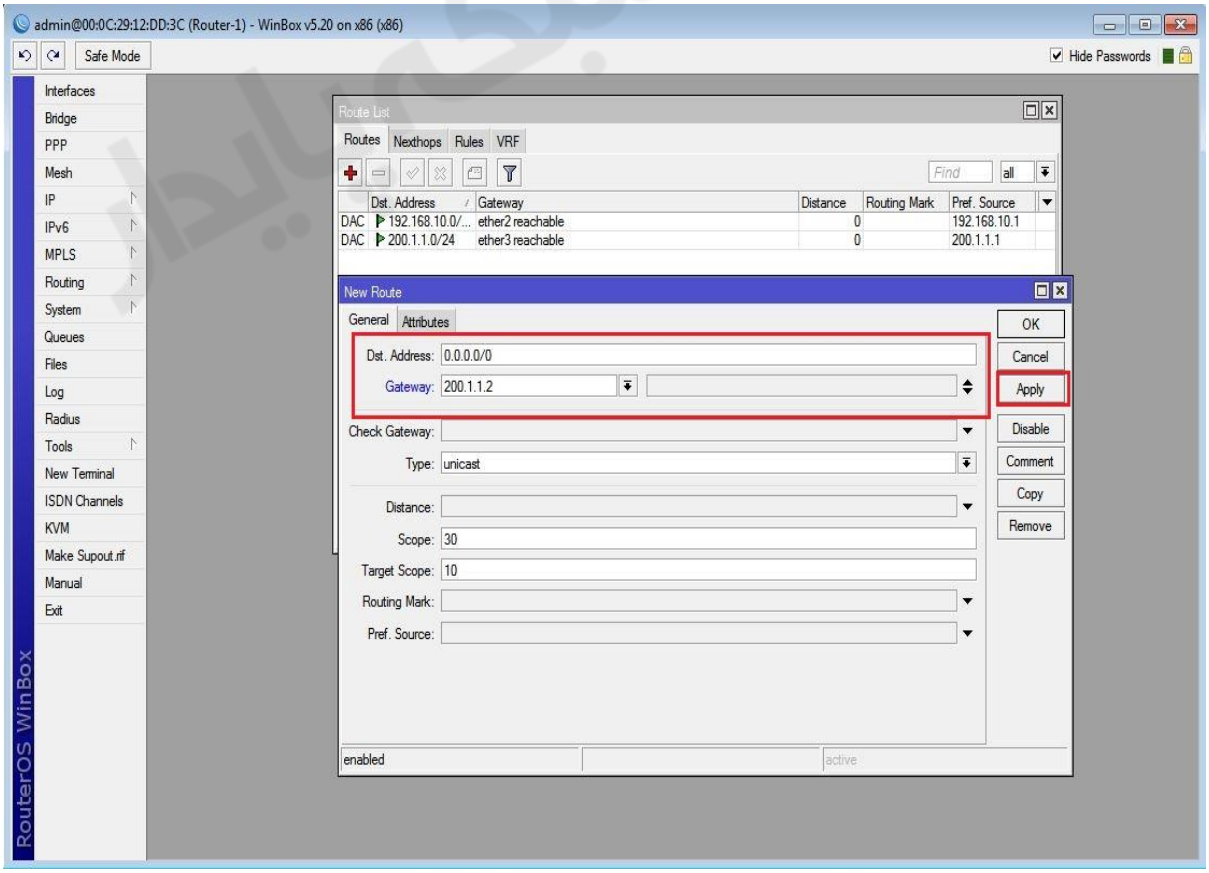
روتر R2 :



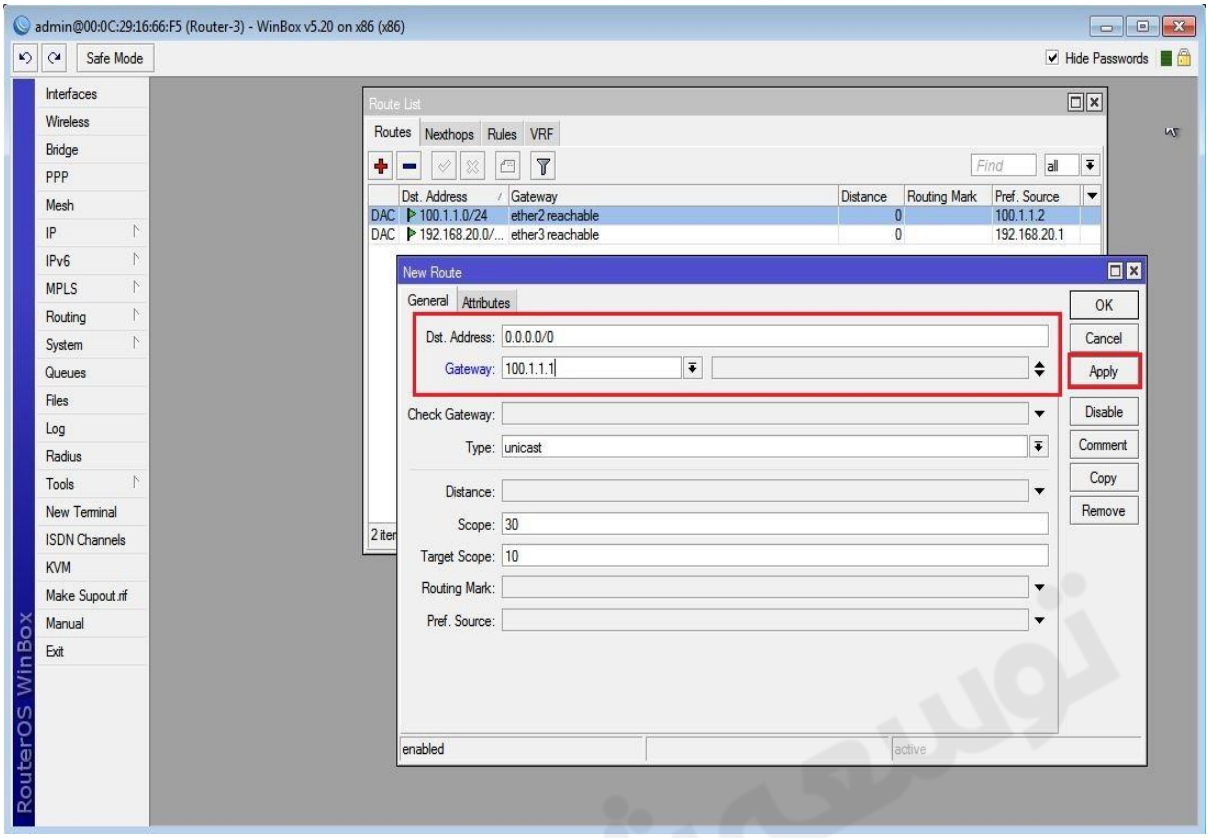
روتر **R3**:



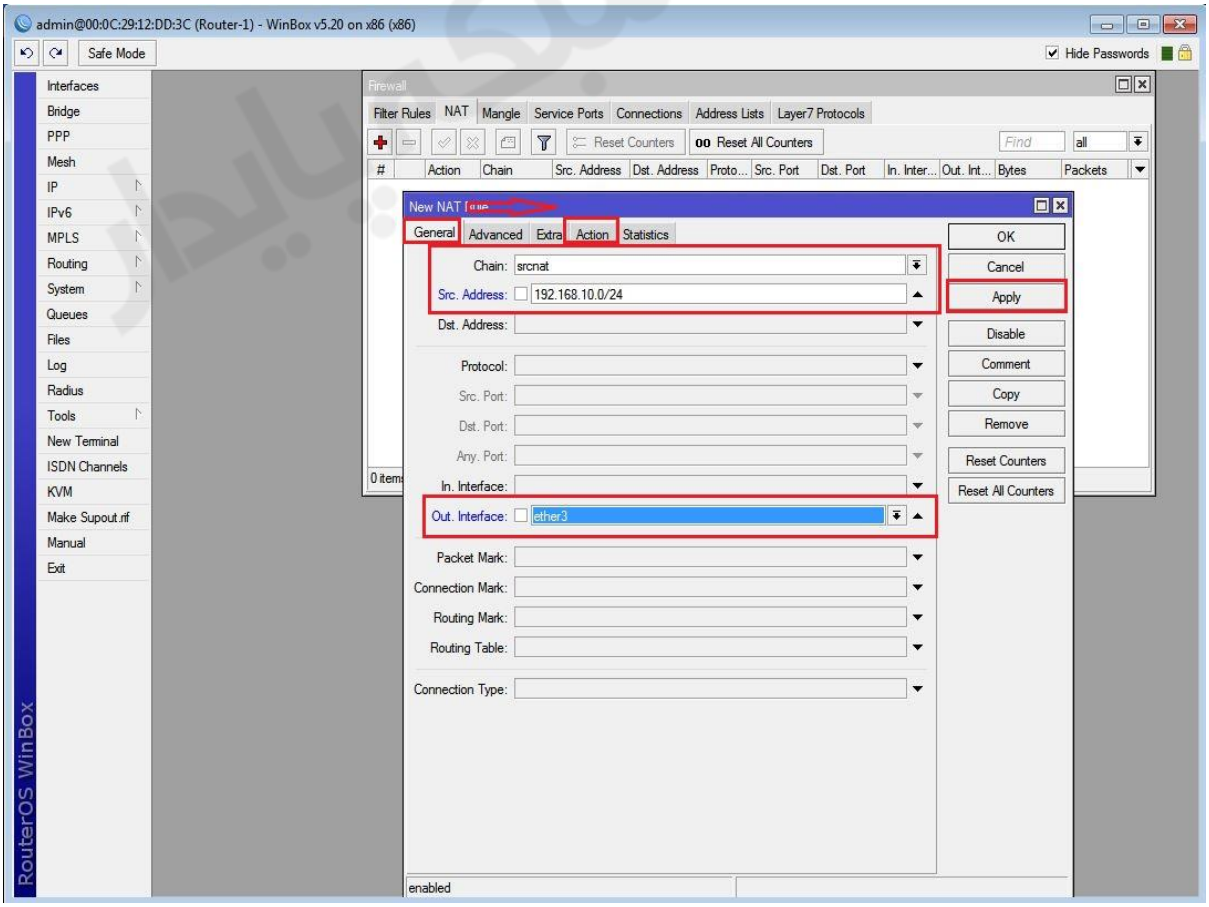
تعریف **Default Route** در روتر **R1**:

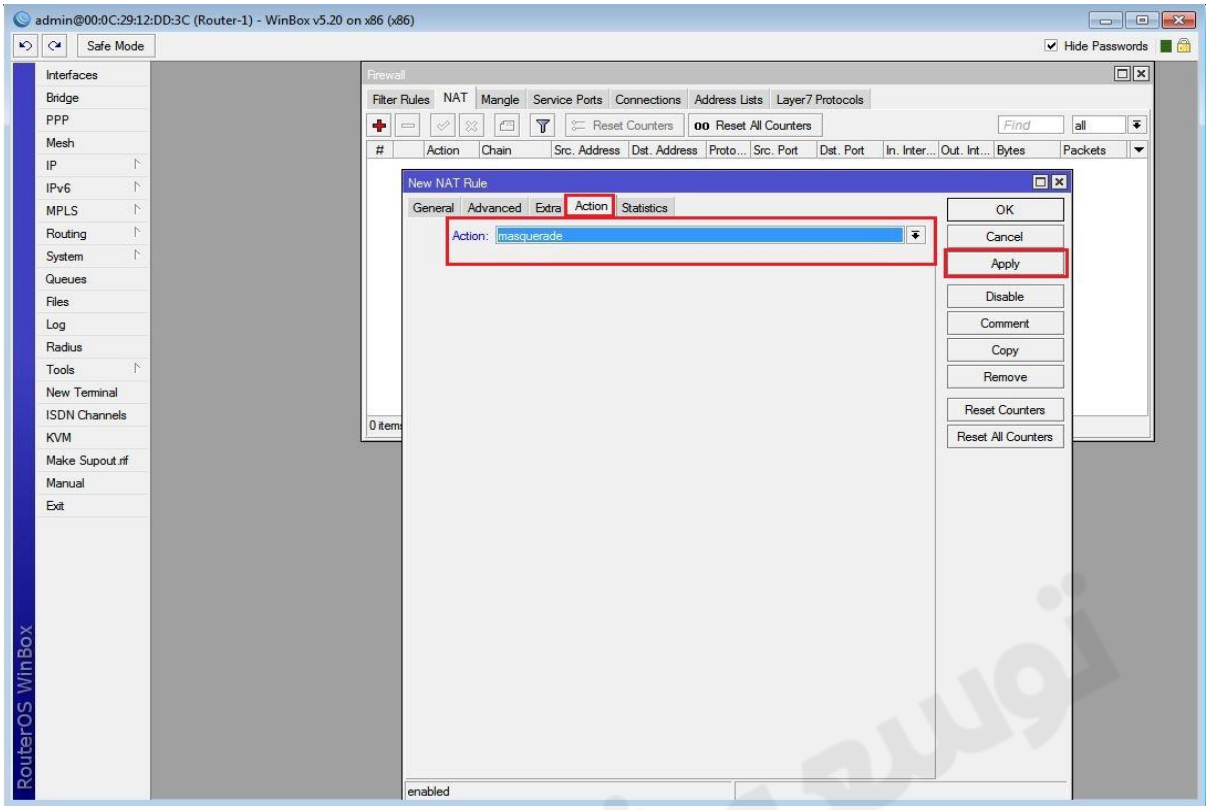


تعریف **Default Route** در **R3** :

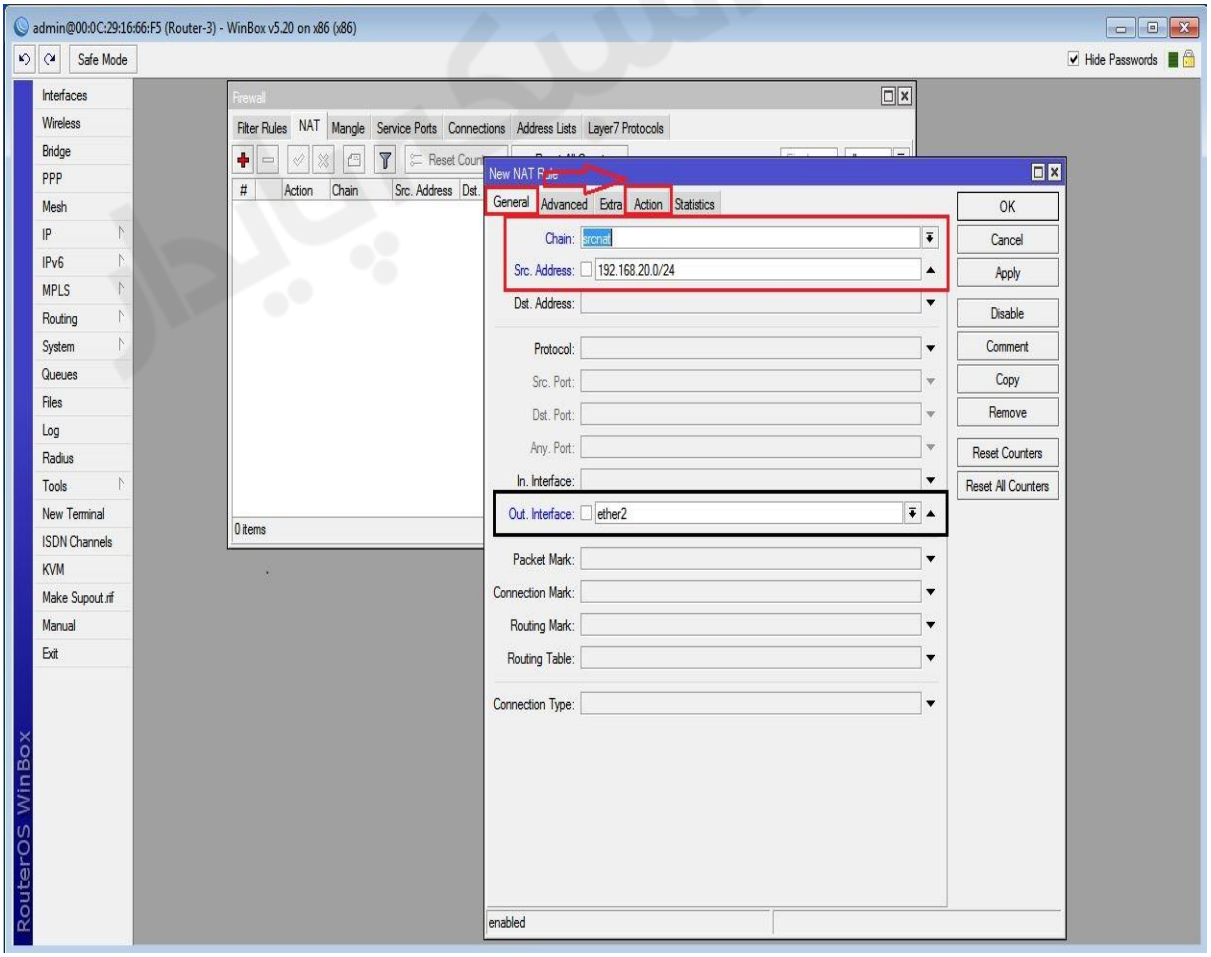


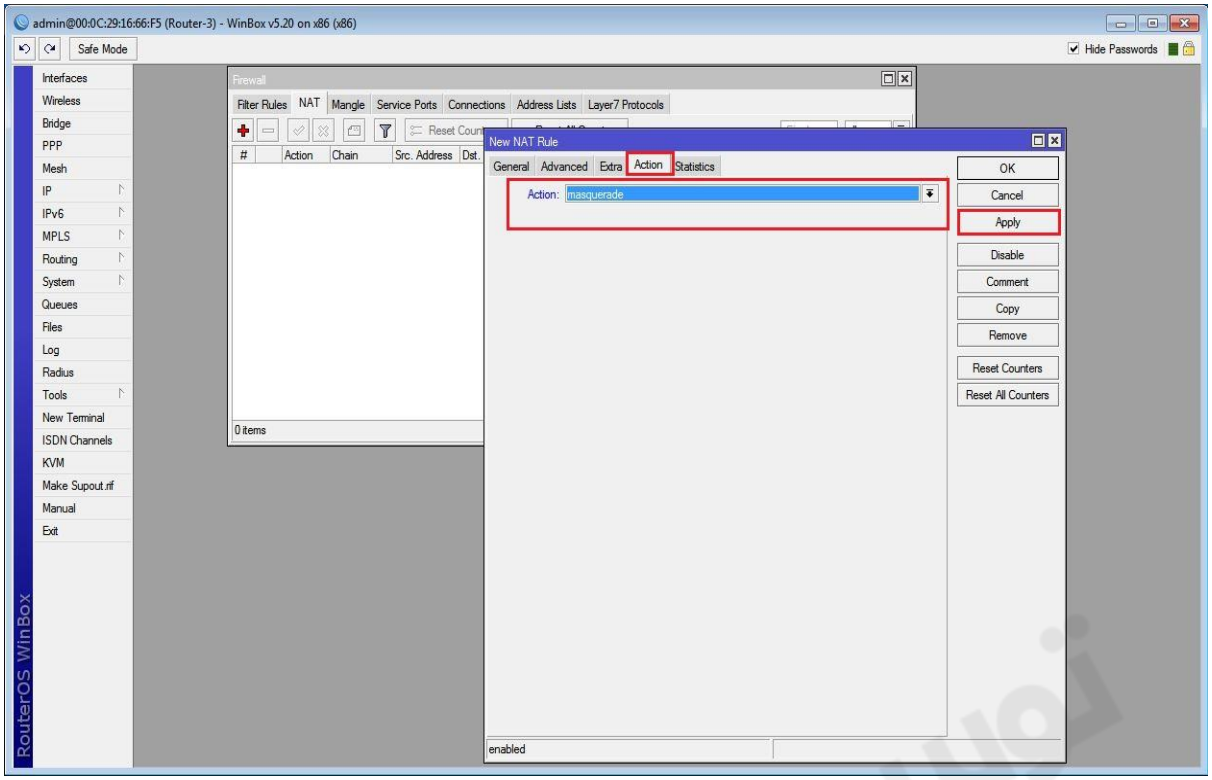
ایجاد Nat در روتر R1 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.





ایجاد Nat در روتر R3 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.





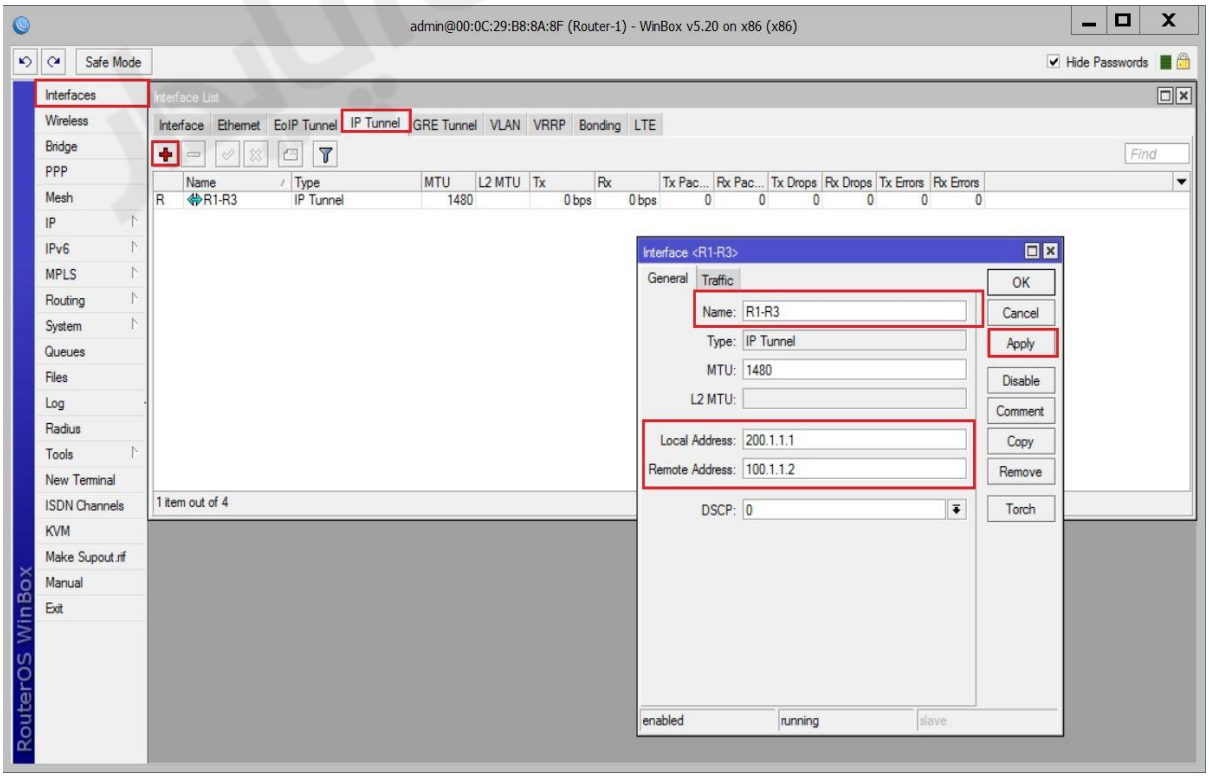
تعریف کارت شبکه مجازی IPIP در روتر R1 :

برای اینکار از منوی اصلی برروی Interface کلیک کرده و از پنجره باز شده به تب IP Tunnel رفته بر روی Add کلیک می کنیم و تنظیمات زیر را انجام می دهیم :

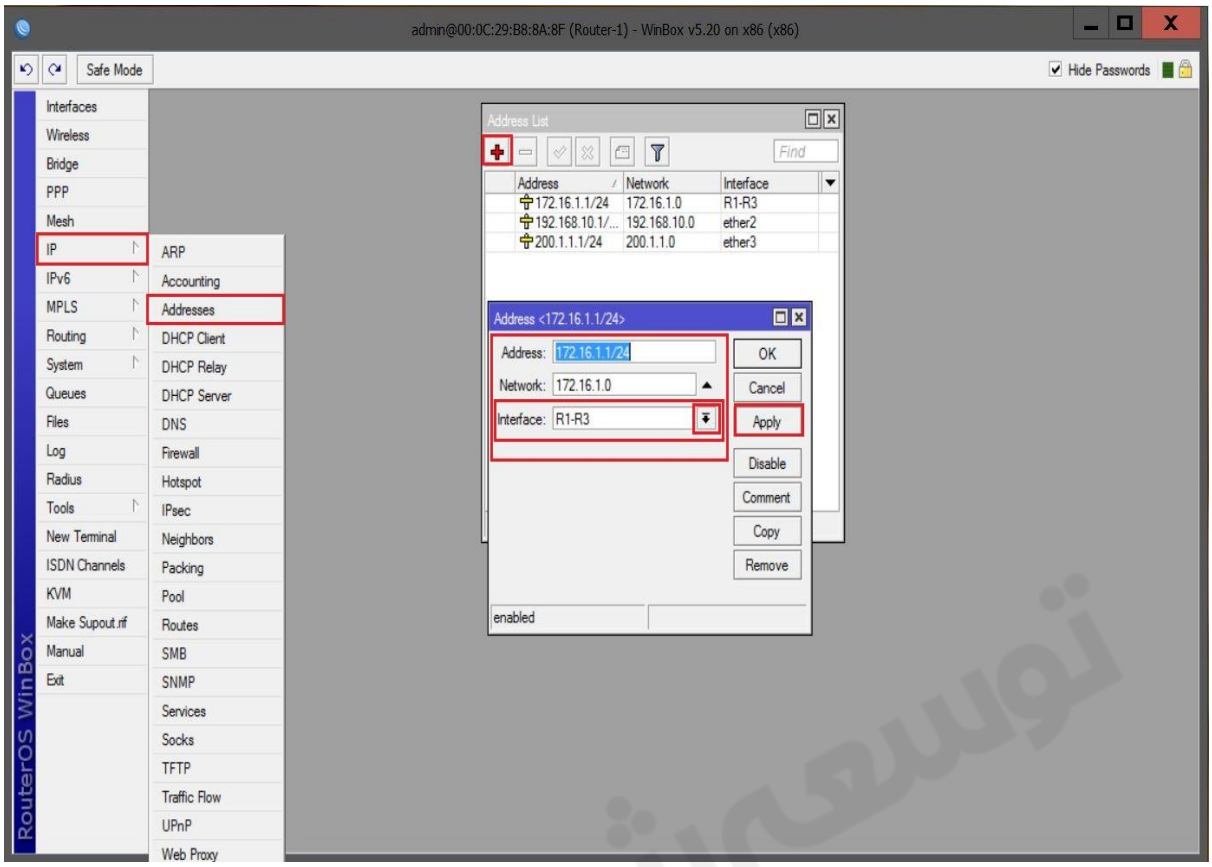
Name : یک نام برای کارت شبکه مجازی IPIP انتخاب می کنیم.

Local Address : آدرس IP (IP Valid) مربوط به کارت شبکه ایی از روتر که بسته ها از آن طریق به روتر مقابل ارسال می شوند.

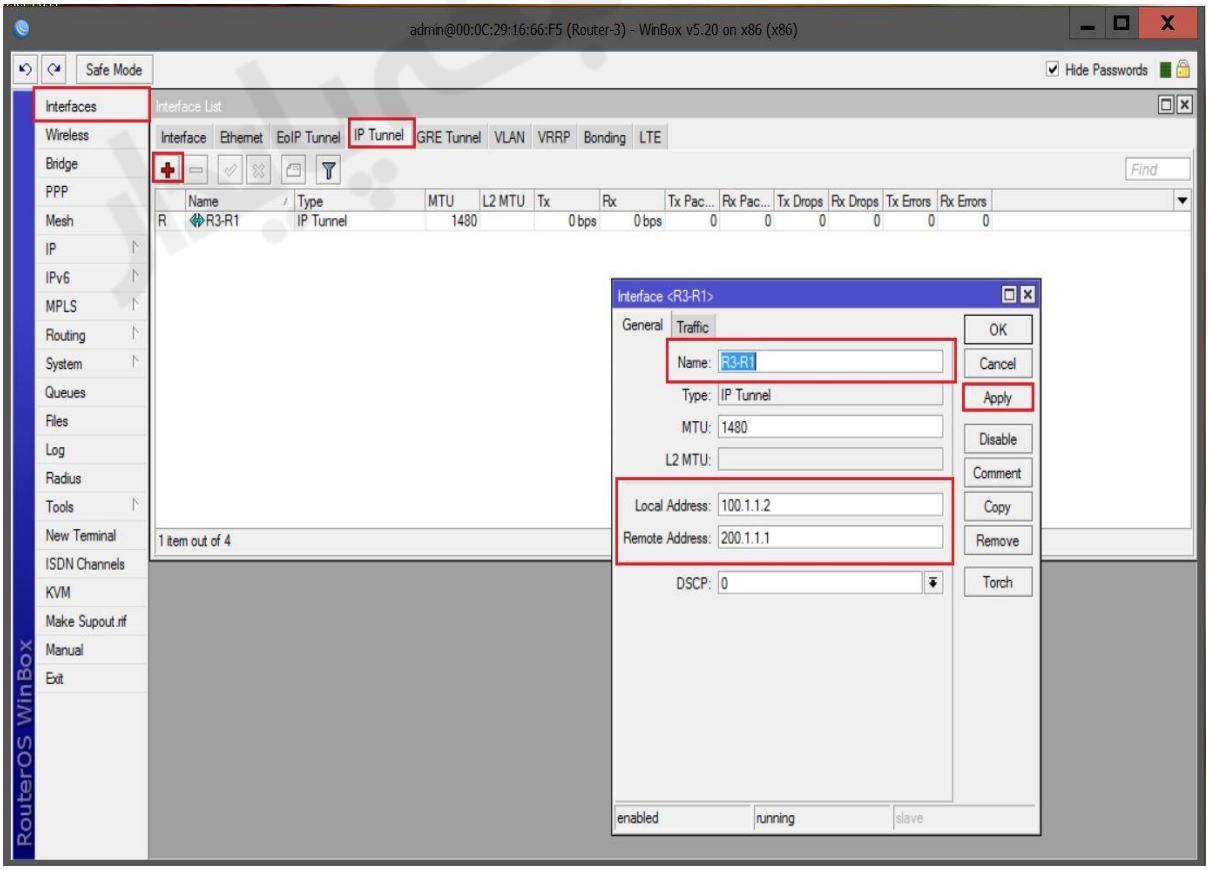
Remote Address : آدرس IP مربوط به روتر مقصد مشخص می شود.



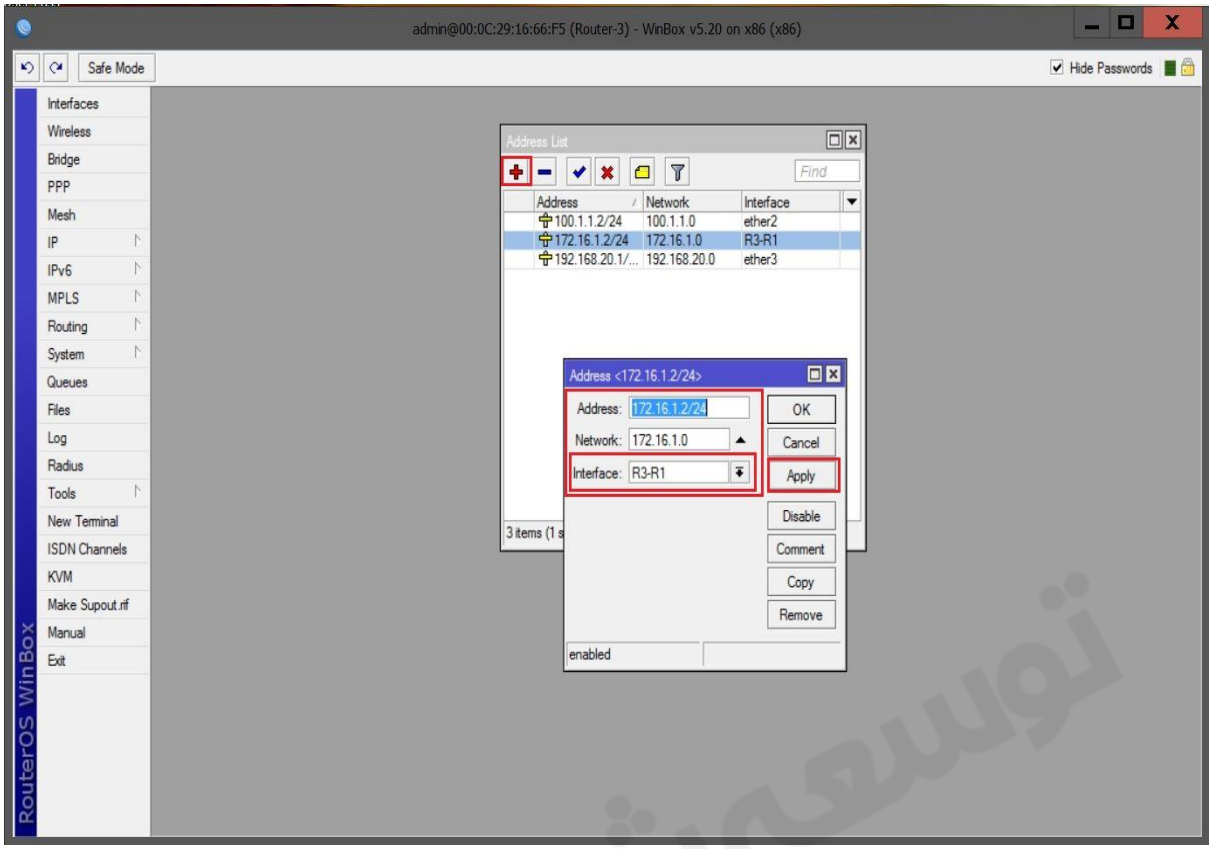
انتساب IP به کارت شبکه مجازی در روتر R1 :



تعریف کارت شبکه مجازی IPIP در روتر R3 :

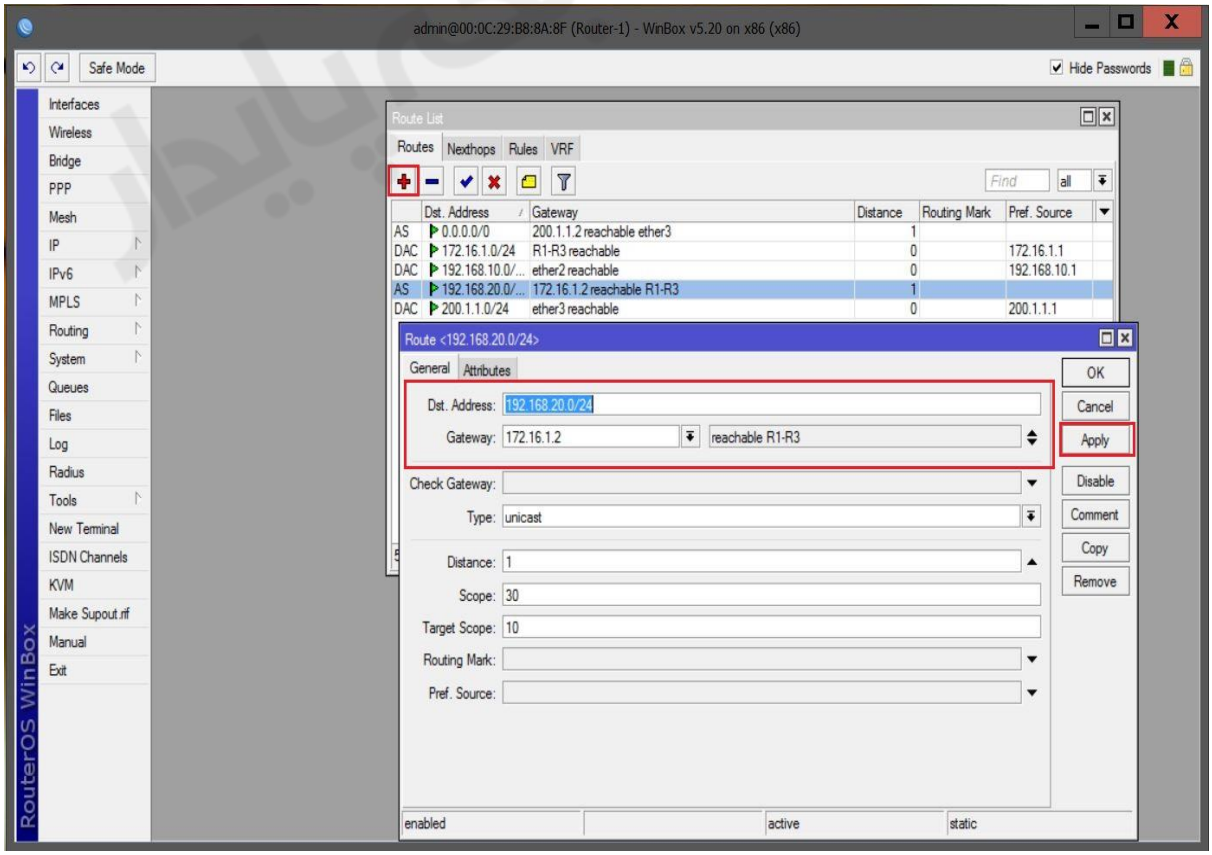


انتساب IP به کارت شبکه مجازی در روتر R3 :



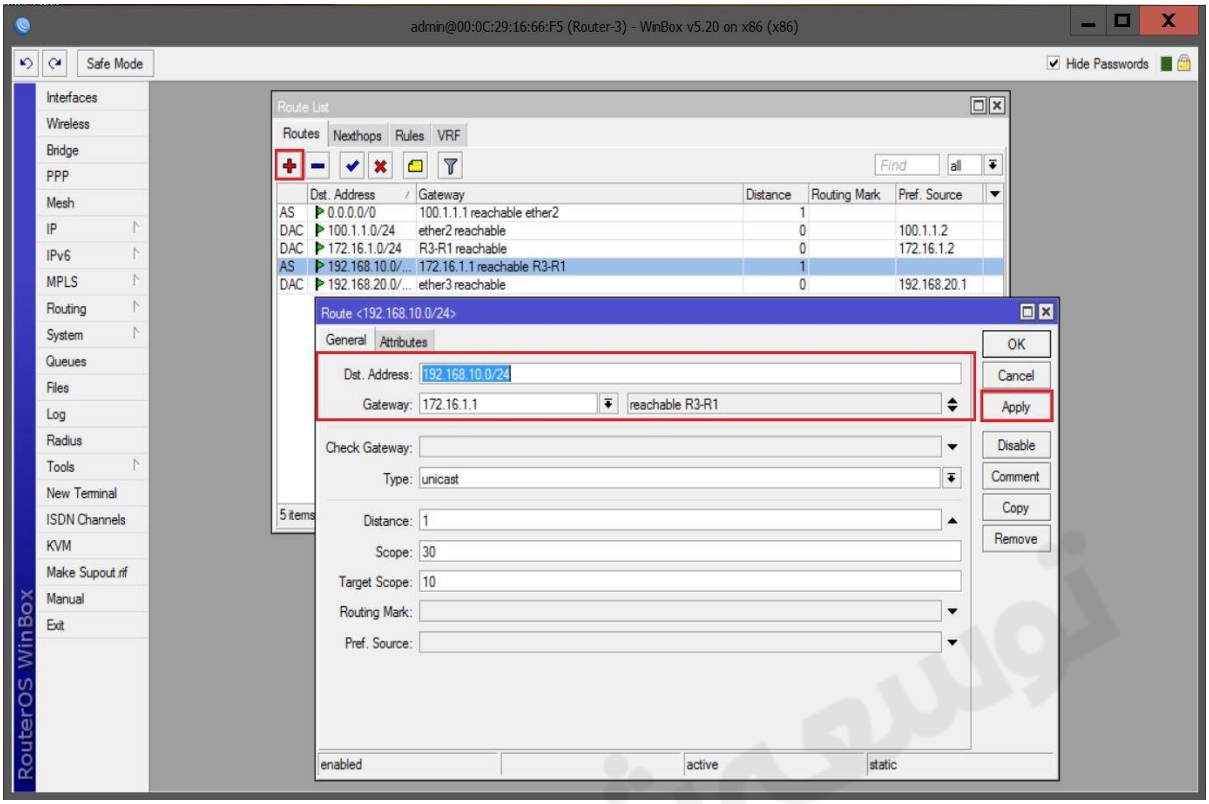
تعریف Static Route در روتر R1 :

برای برقراری ارتباط کلاینت های موجود در Lan-1 با کلاینت های موجود در Lan-2 در روتر R1 ، Static Route زیر را تعریف می کنیم.



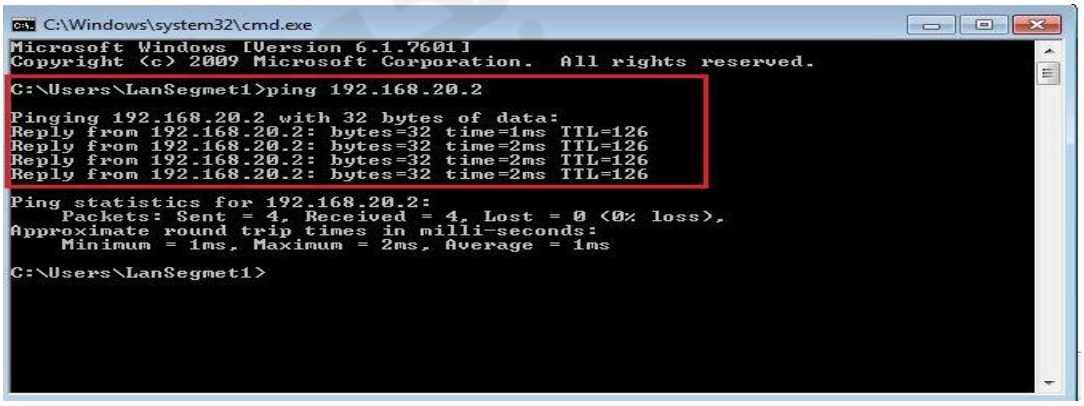
تعریف Static Route در روتر R3 :

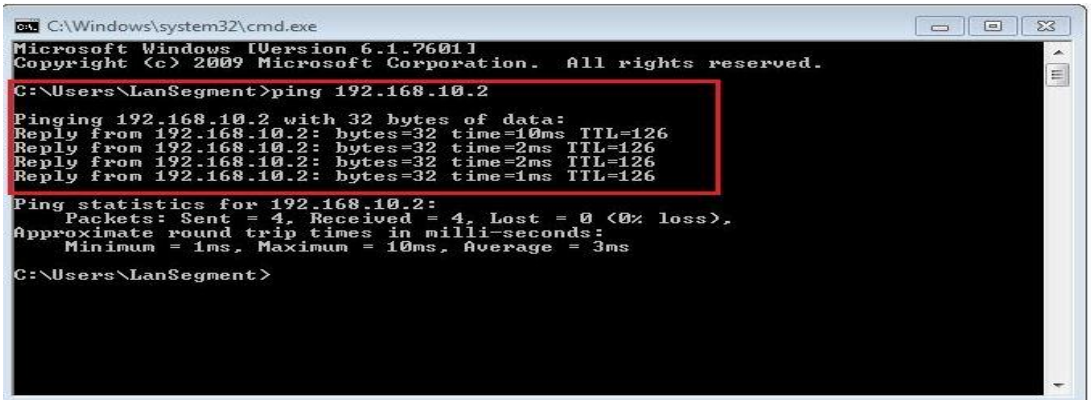
برای برقراری ارتباط کلاینت های موجود در Lan-2 با کلاینت های موجود در Lan-1 در روتر R3 ، Static Route زیر را تعریف می کنیم.



تنظیمات کلاینت :

طبق سناریو به کلاینت ها IP اختصاص می دهیم و برای تست ارتباط از دستور Ping استفاده می کنیم.





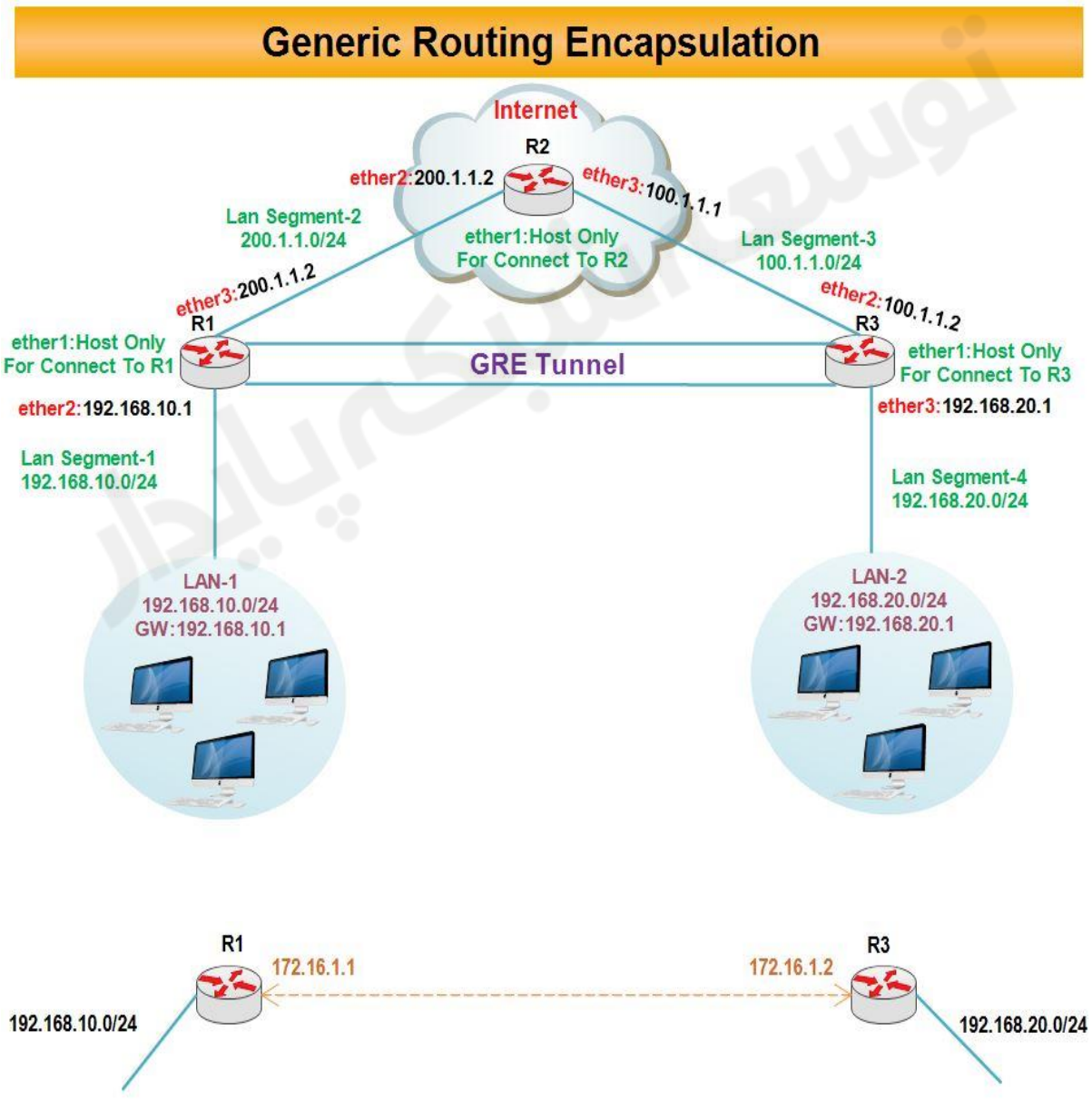
فصل پانزدهم : GRE Tunnel

GRE مخفف کلمه **Generic Routing Encapsulation** می باشد و یکی دیگر از روش های ارتباطی در شبکه پیکربندی تانل **GRE** است.**GRE** پروتکل **Tunneling** شرکت سیسکو می باشد که میکروتیک نیز از آن استفاده می کند.

Encapsulation در **GRE** به معنی کپسوله شدن دیتاهاست.در واقع **GRE** همان **IPIP Tunnel** است که **4** بایت بیشتر از **IPIP** به بسته ها (**Packet**) اضاف می کند.

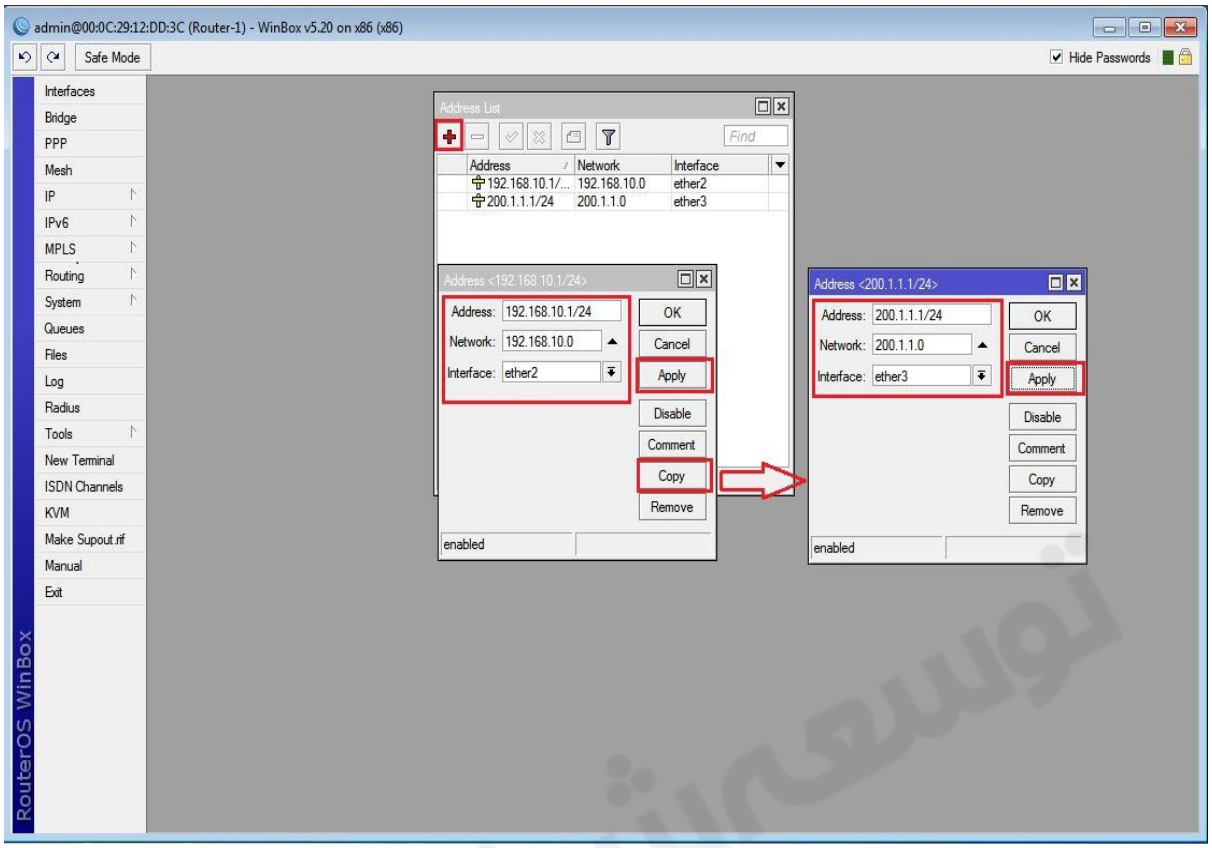
در این نوع تانل هم می بایست در هر دو طرف روتر ها **IP** روتر مقصد را وارد کنیم تا ارتباط برقرار شود و نهایتا امر اختصاص **IP** به اینترفیس های ایجاد شده و انجام عملیات **Static Route** .

سناریو ۱ : هدف از بررسی این سناریو ، پیاده سازی پروتکل **GRE** می باشد.

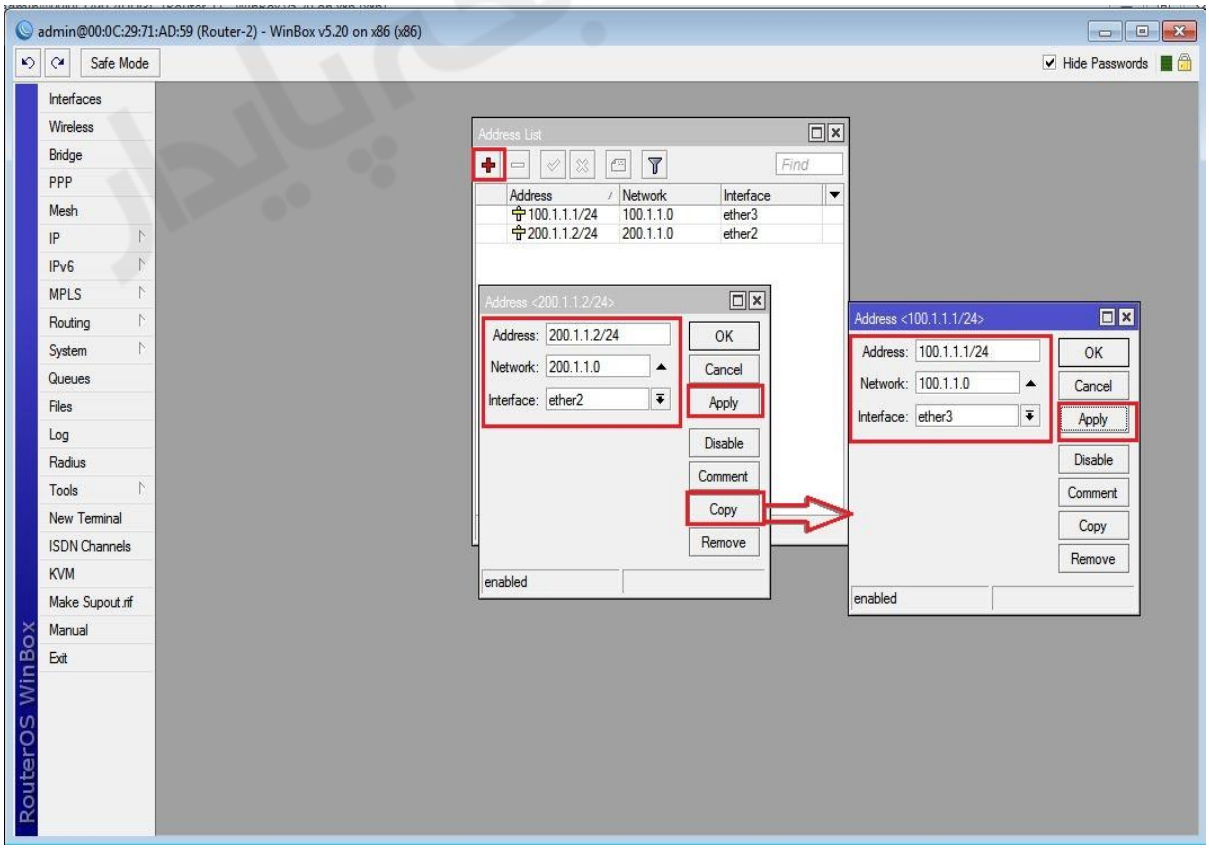


انتساب IP به کارت های شبکه روترها :

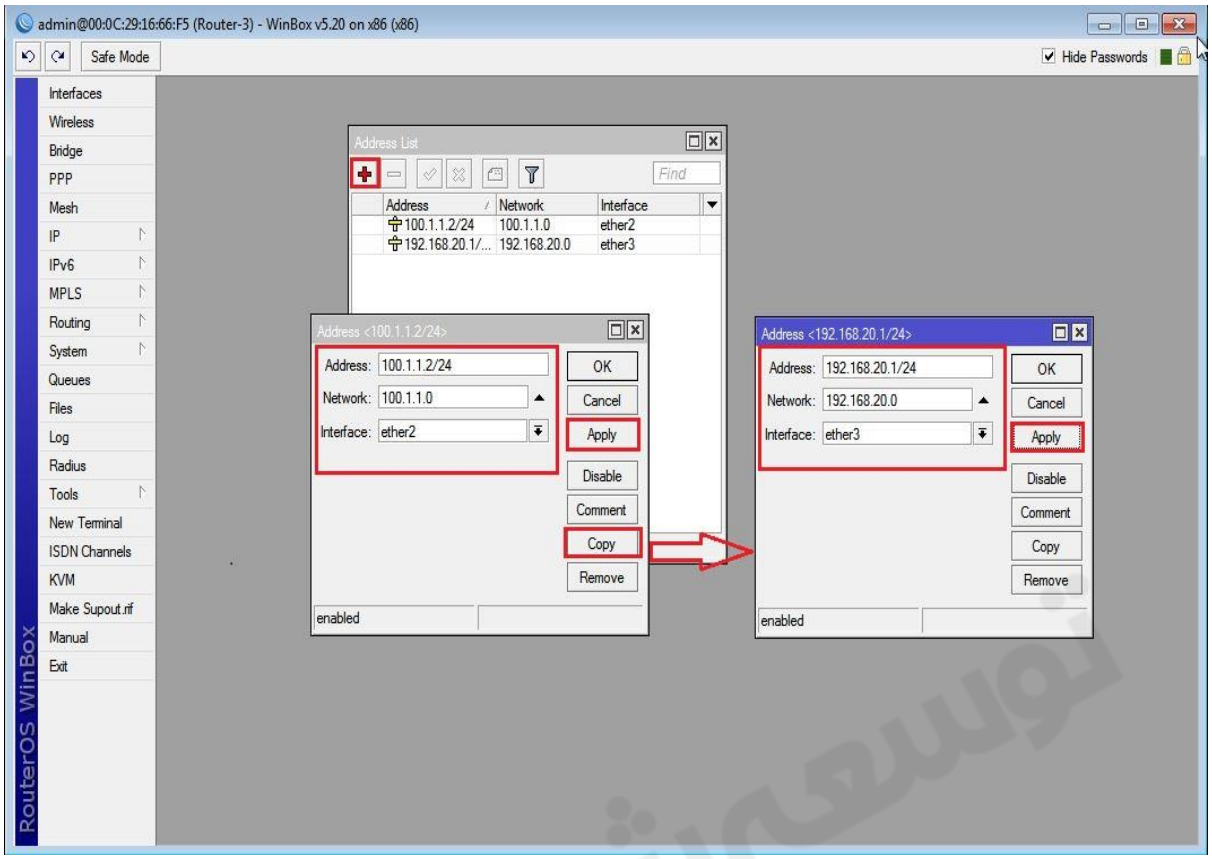
روتر R1 :



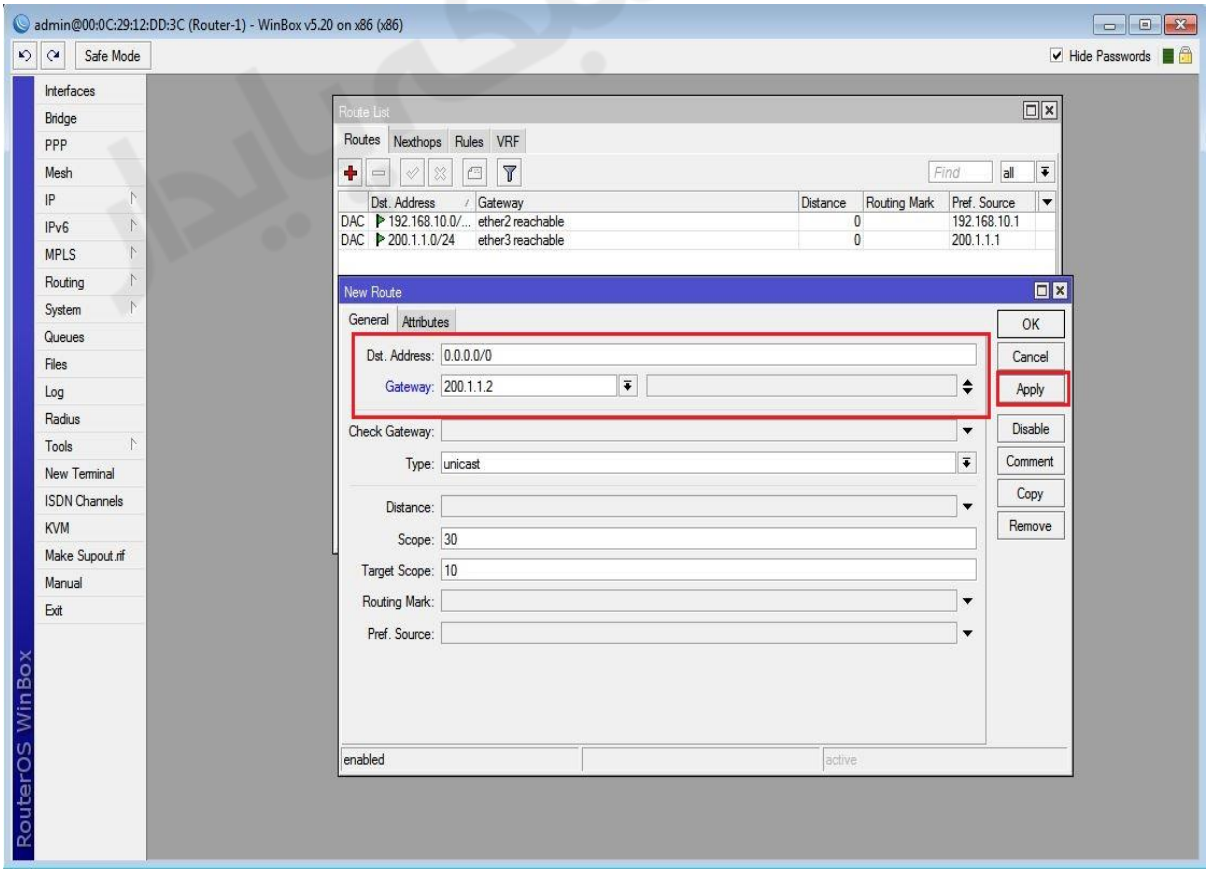
روتر R2 :



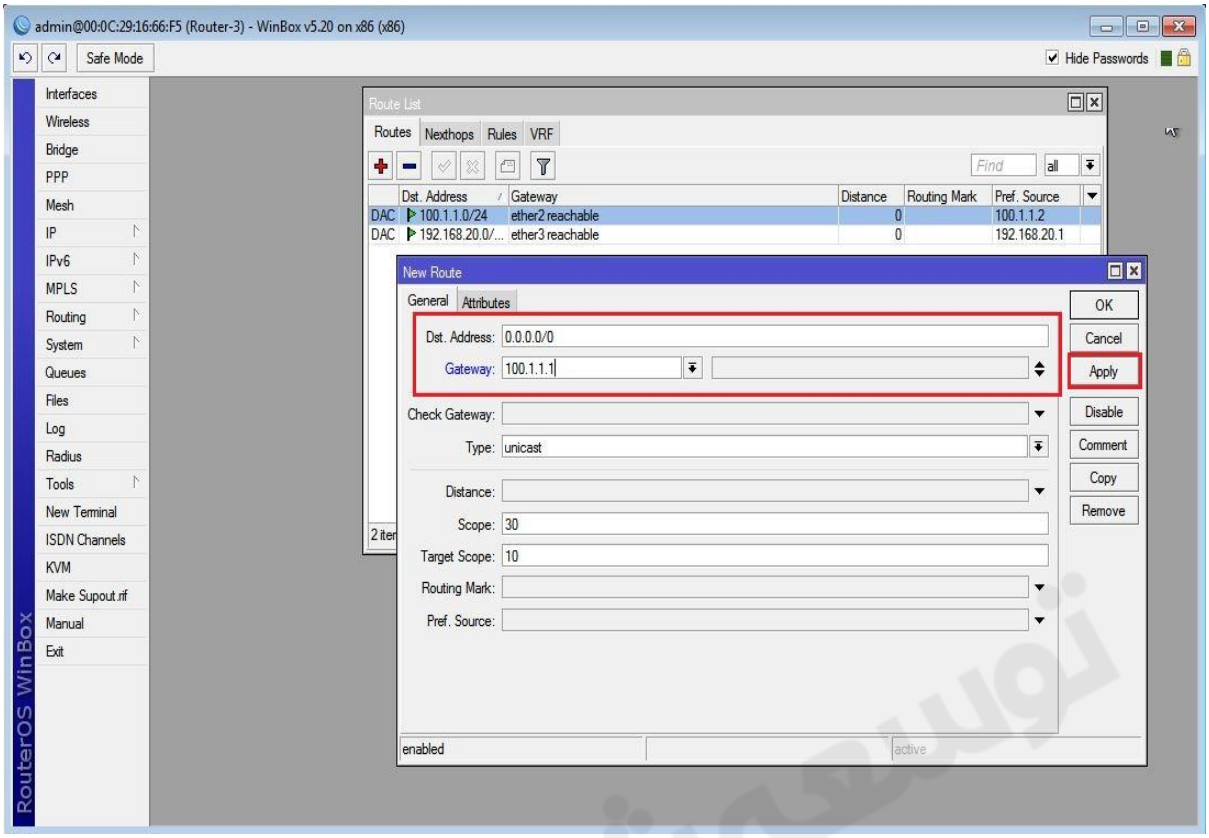
روتر **R3**:



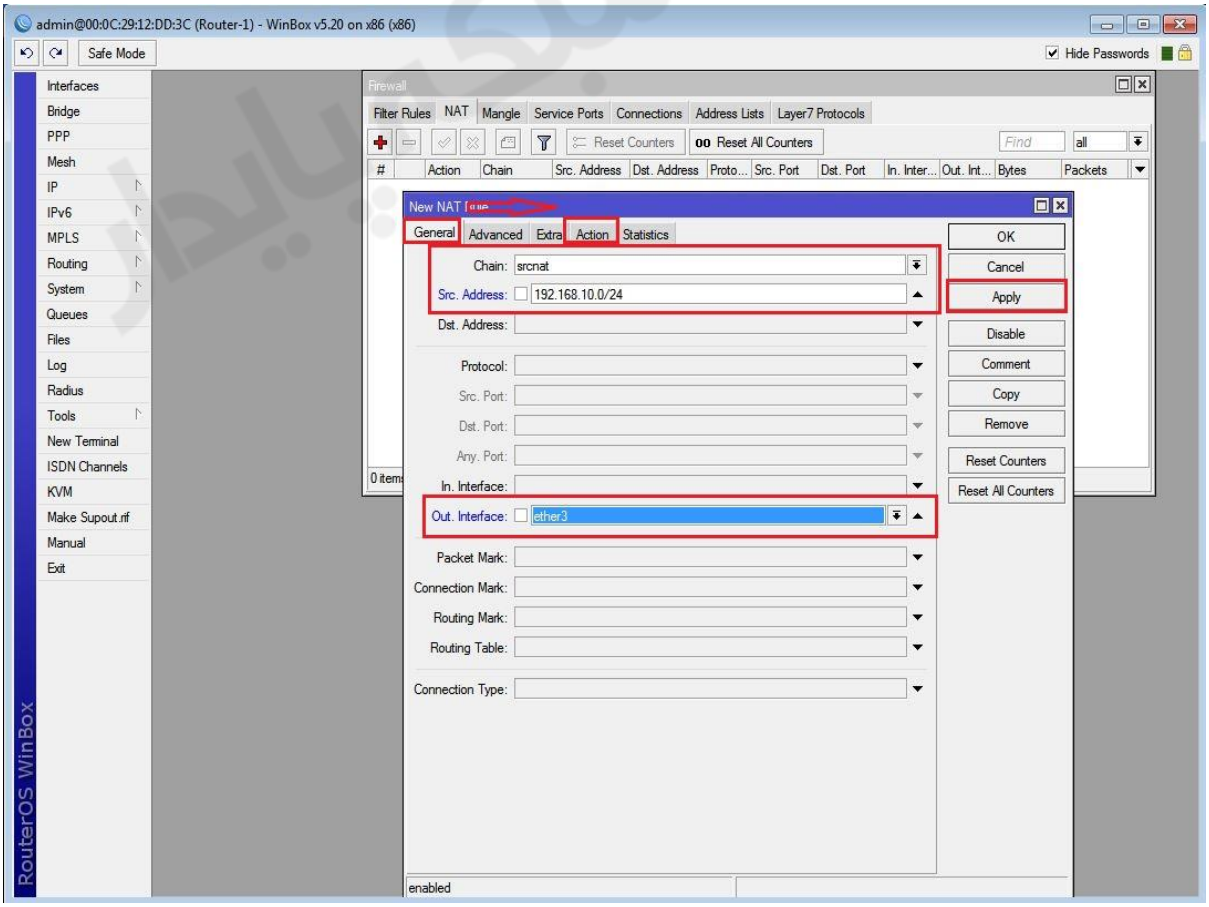
تعریف **Default Route** در روتر **R1**:

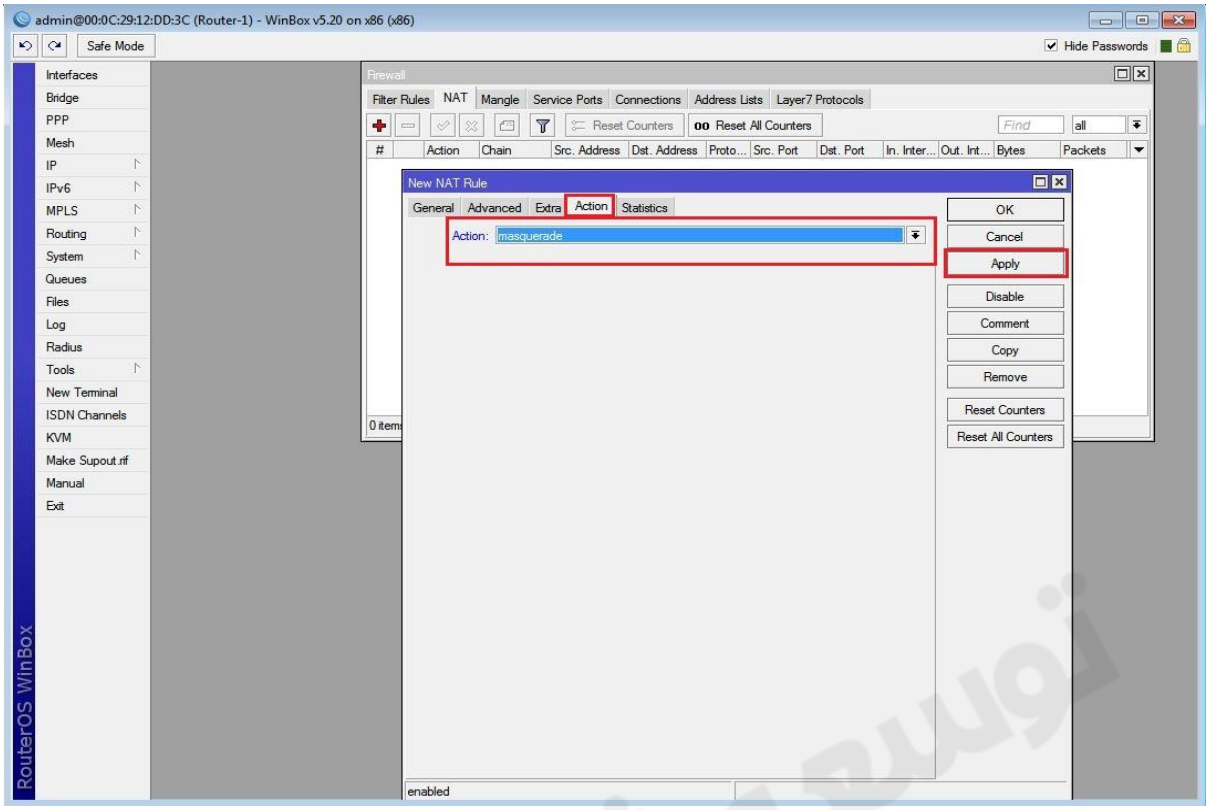


تعریف **Default Route** در **R3** :

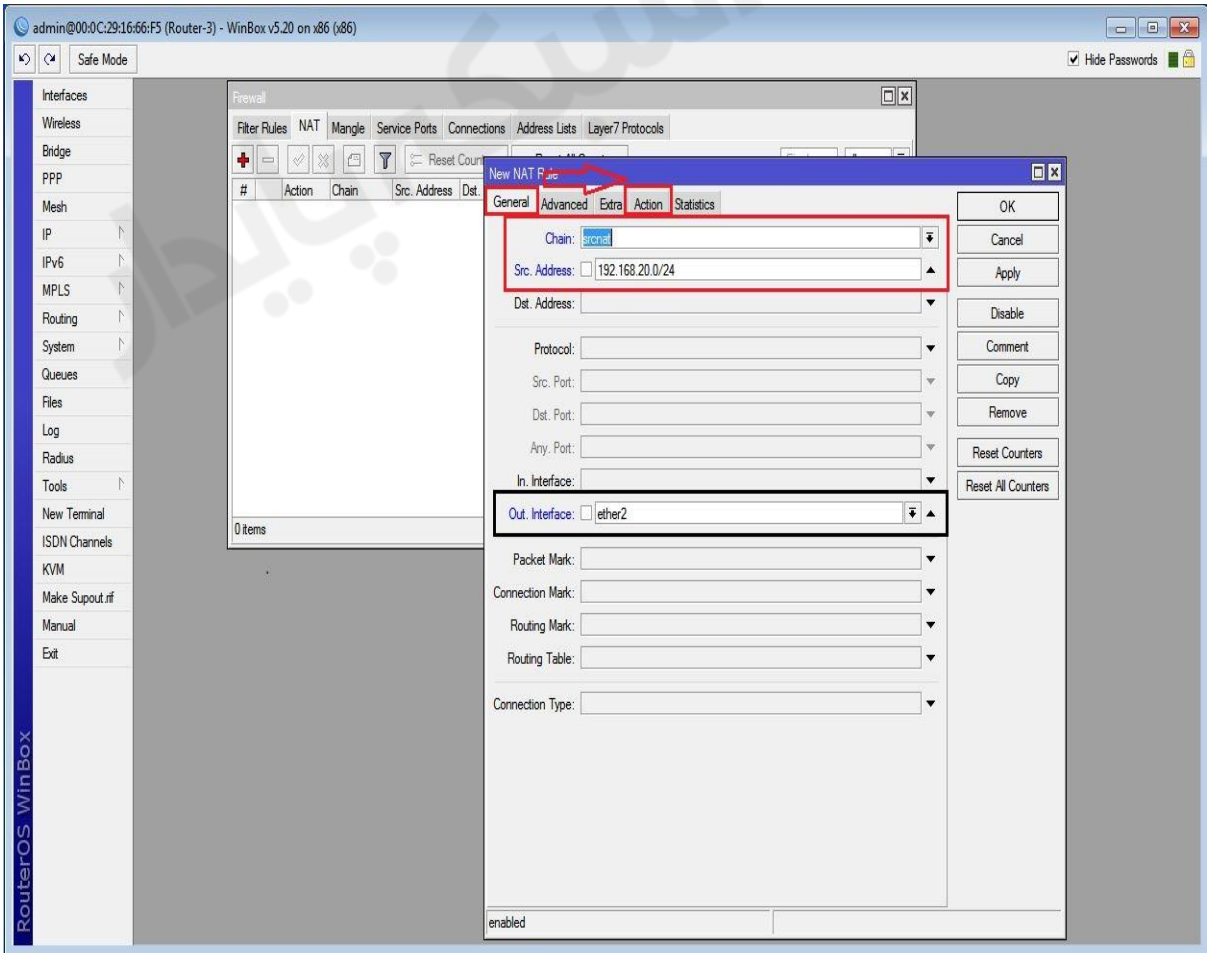


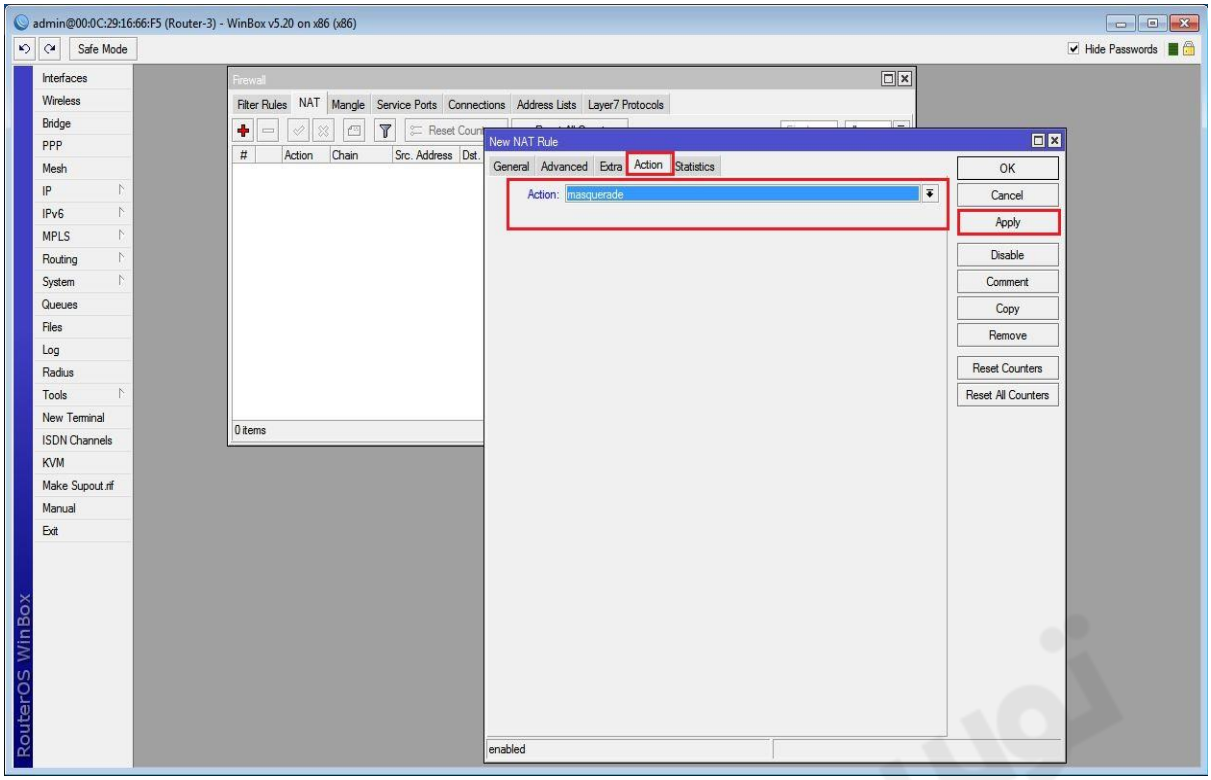
ایجاد Nat در روتر R1 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.





ایجاد Nat در روتر R3 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.



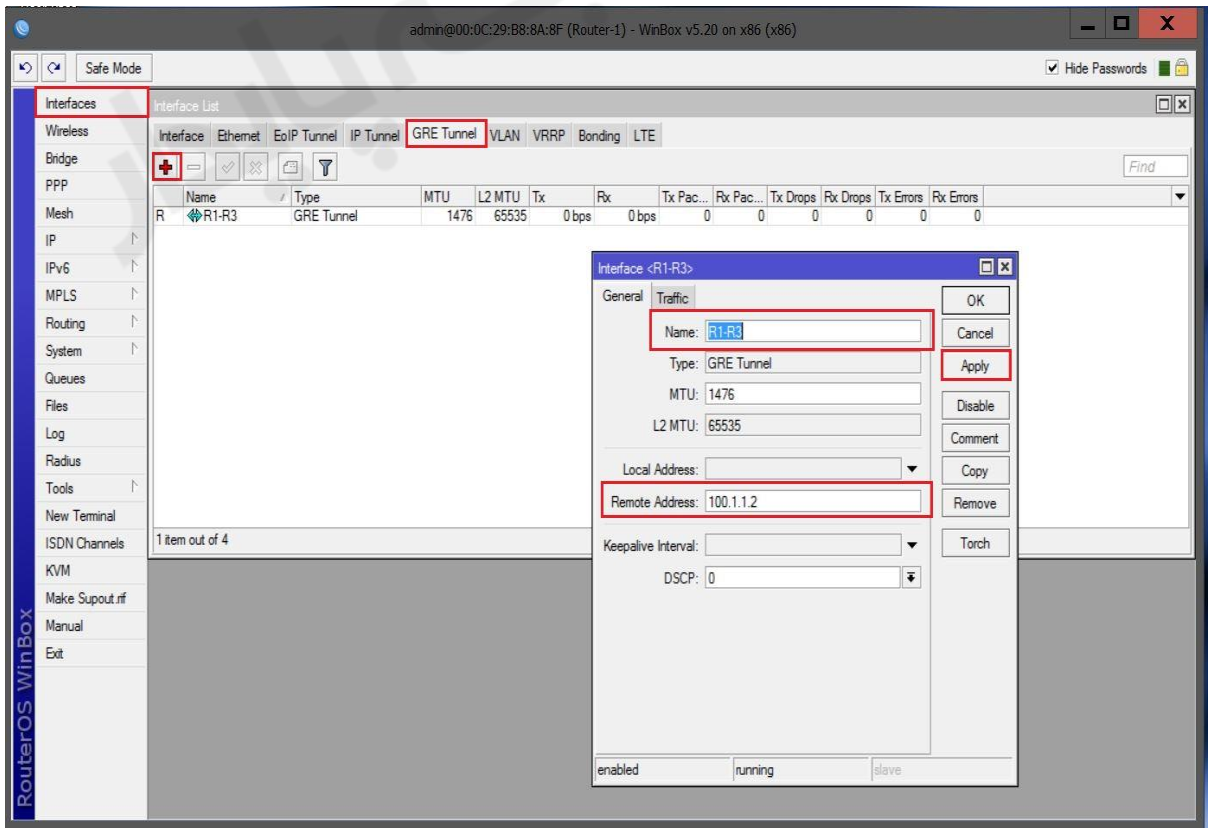


تعریف کارت شبکه مجازی GRE در روتر R1 :

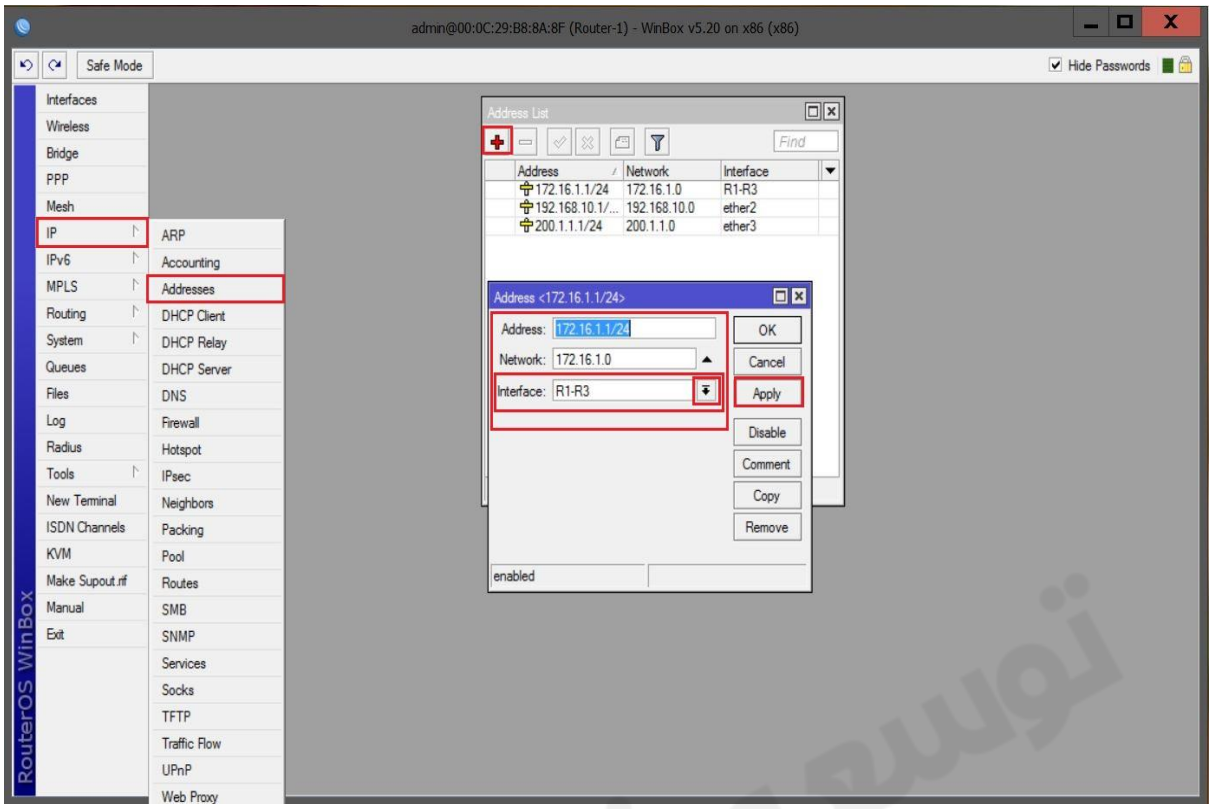
برای اینکار از منوی اصلی برروی Interface کلیک کرده و از پنجره باز شده به تب GRE Tunnel رفته بر روی Add کلیک می کنیم و تنظیمات زیر را انجام می دهیم :

Name : یک نام برای کارت شبکه مجازی IPIP انتخاب می کنیم.

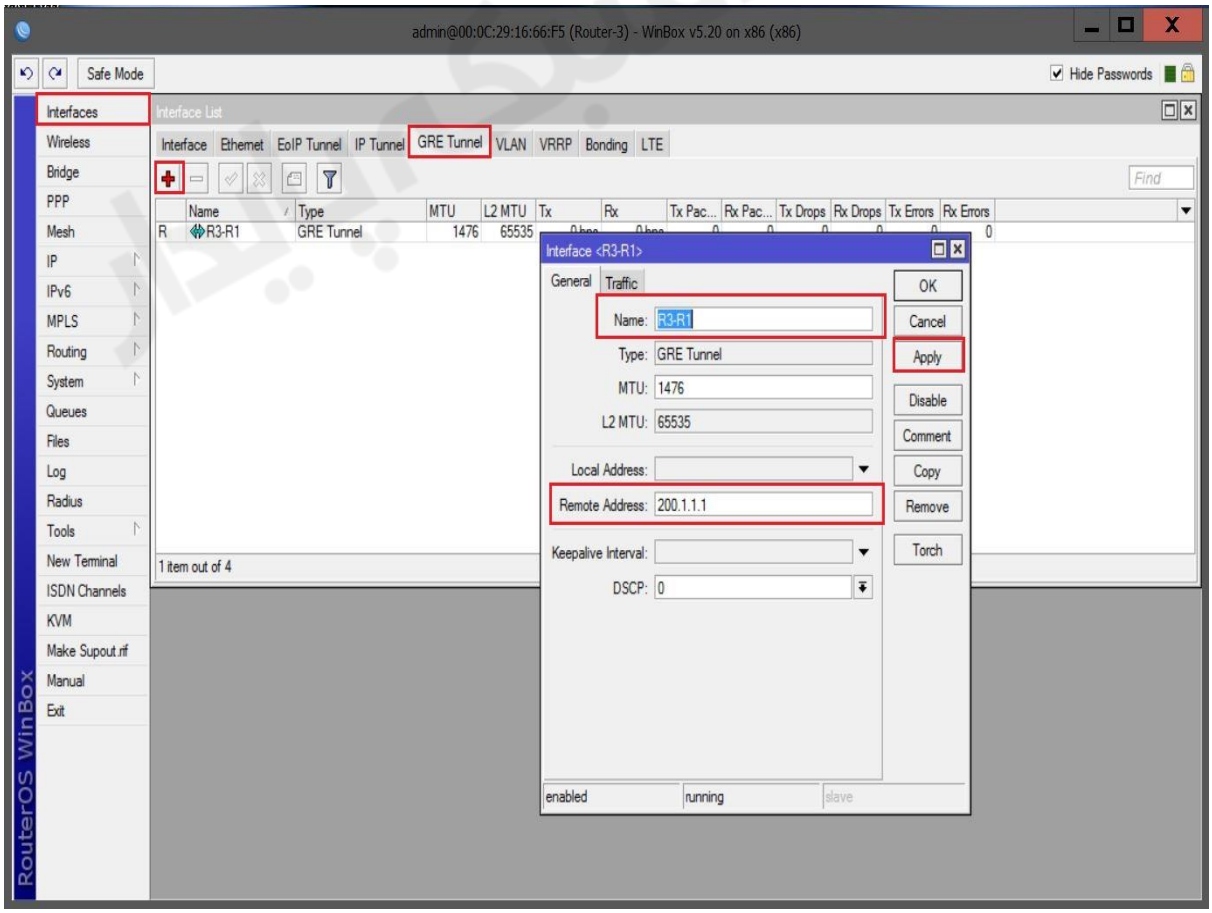
Remote Address : آدرس IP مربوط به روتر مقصد مشخص می شود.



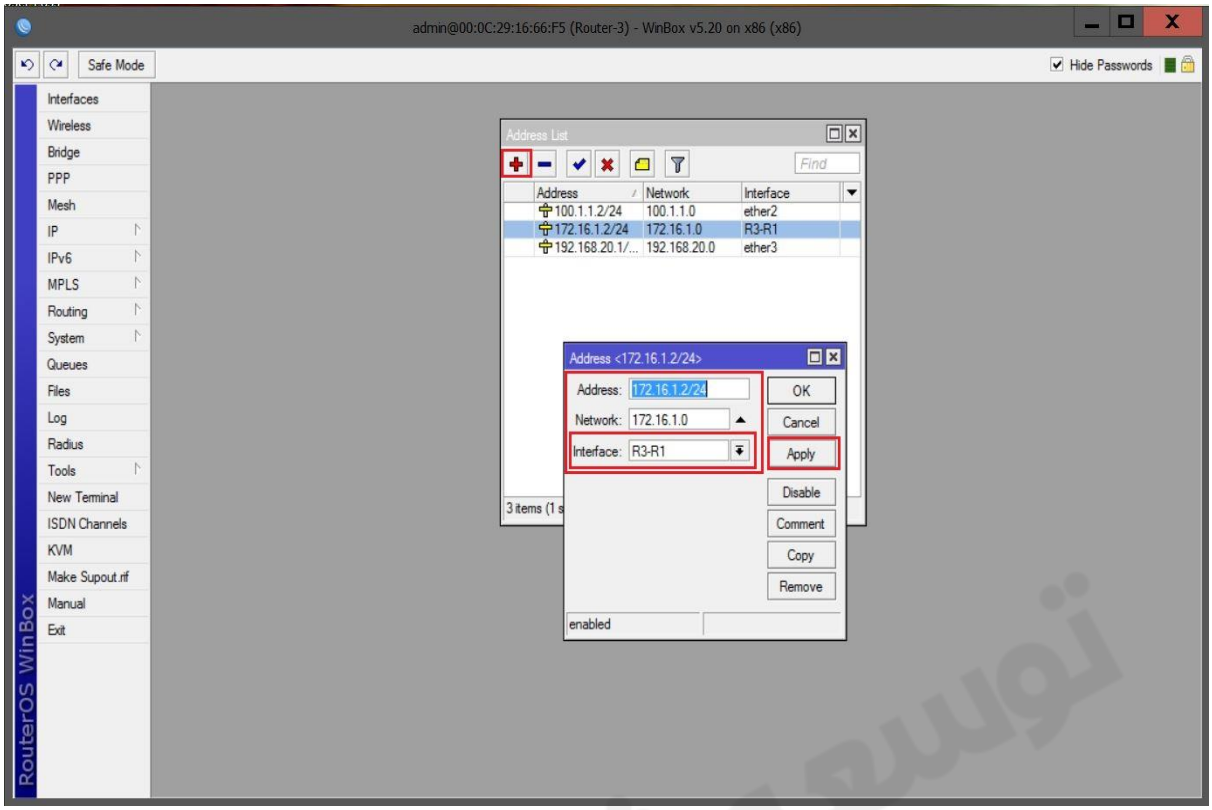
انتساب **IP** به کارت شبکه مجازی در روتر **R1** :



تعریف کارت شبکه مجازی **GRE** در روتر **R3** :

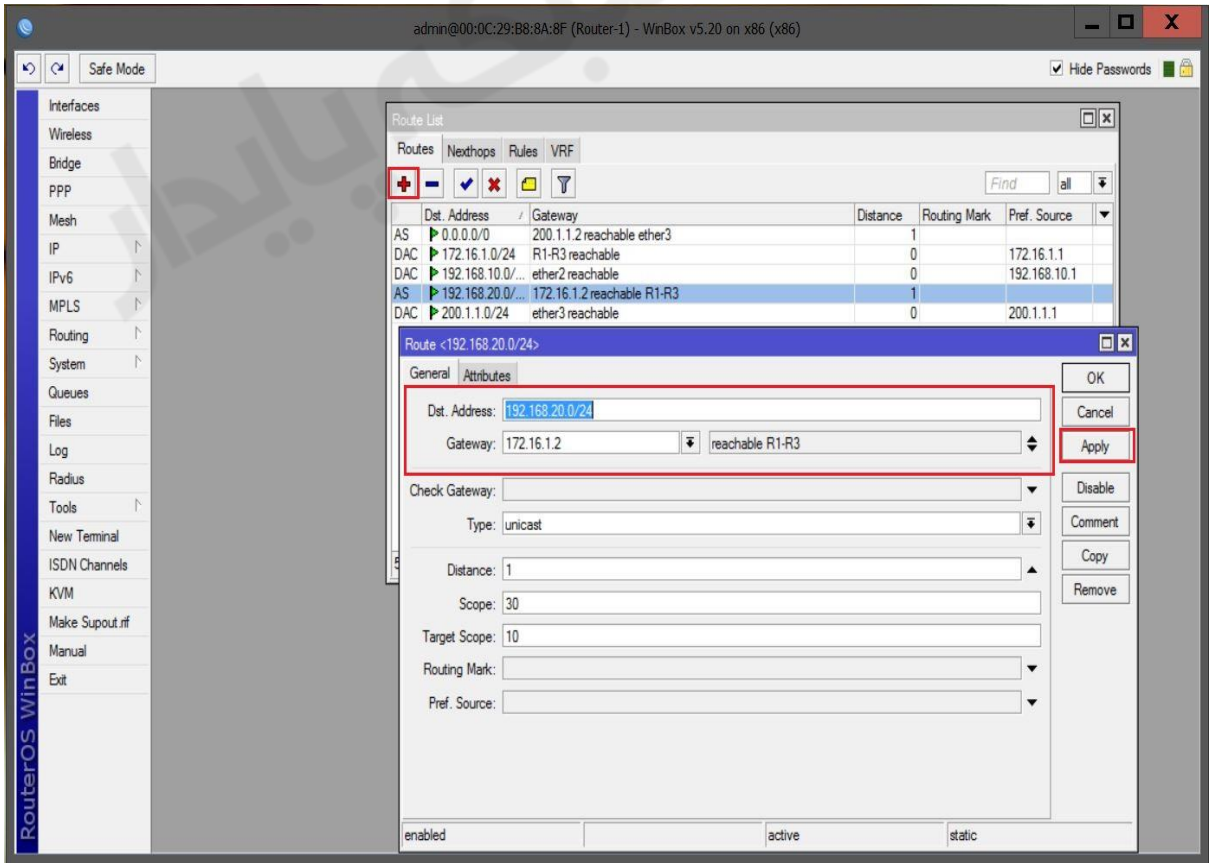


انتساب **IP** به کارت شبکه مجازی در روتر **R3** :



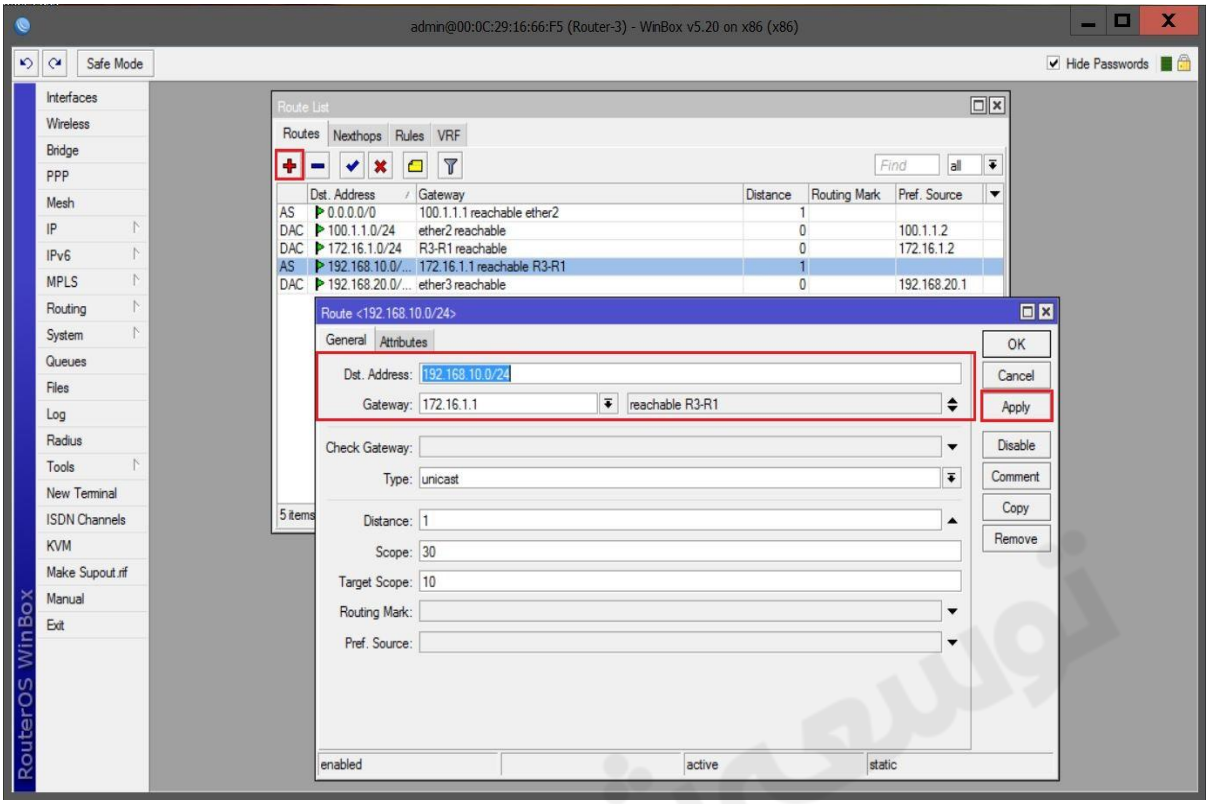
تعریف **Static Route** در روتر **R1** :

برای برقراری ارتباط کلاینت های موجود در **Lan-1** با کلاینت های موجود در **Lan-2** در روتر **R1** ، **Static Route** زیر را تعریف می کنیم.



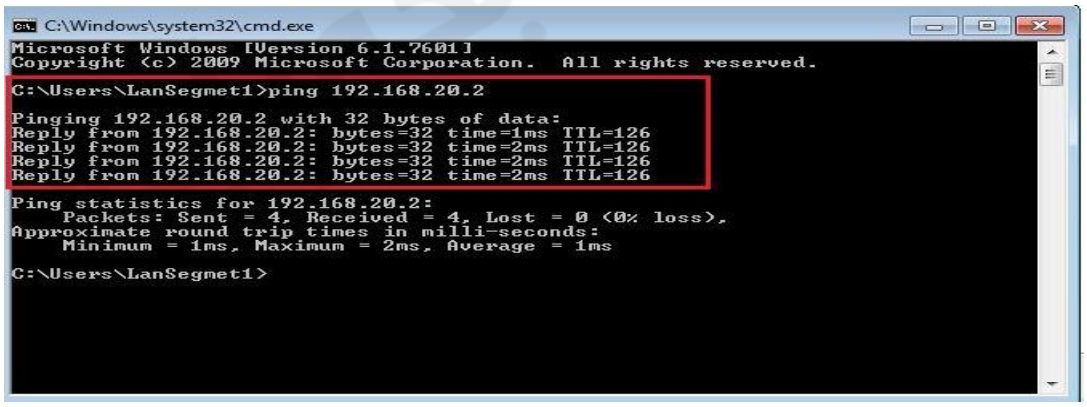
تعریف Static Route در روتر R3 :

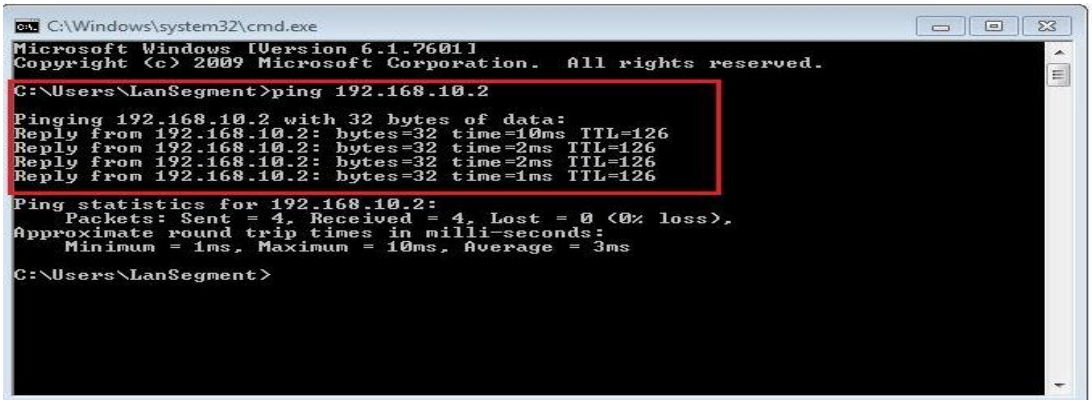
برای برقراری ارتباط کلاینت های موجود در Lan-2 با کلاینت های موجود در Lan-1 در روتر R3 ، Static Route زیر را تعریف می کنیم.



تنظیمات کلاینت :

طبق سناریو به کلاینت ها IP اختصاص می دهیم و برای تست ارتباط از دستور Ping استفاده می کنیم.





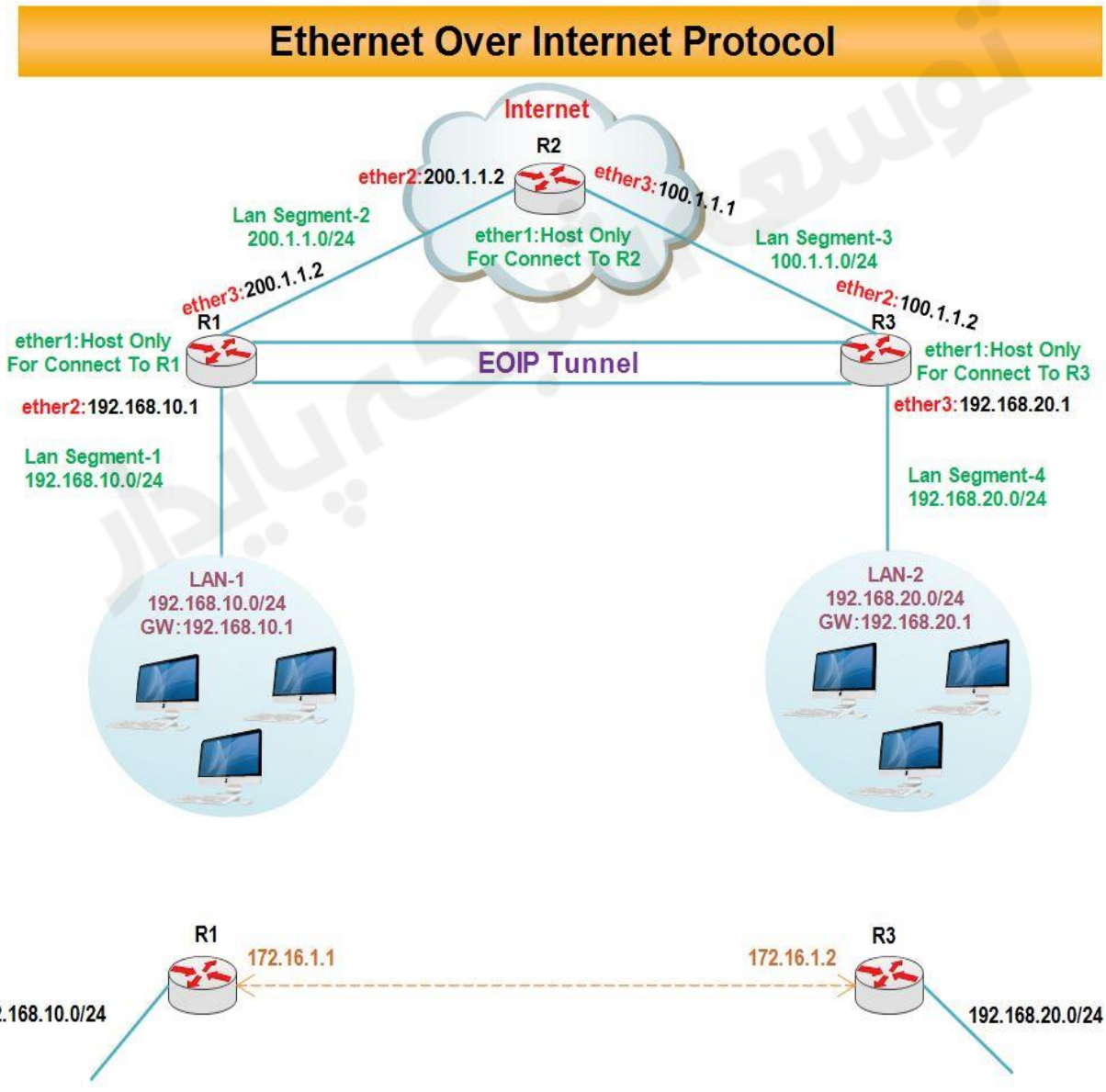
فصل شانزدهم : EOIP Tunnel

EOIP مخفف کلمه **Ethernet Over Internet Protocol** می باشد که توسط شرکت میکروتیک معرفی شده است.بنابراین **Open Standard** نیست و در سیستم عامل های دیگر اعم از سیسکو و ویندوز و .... این مدل تانل وجود ندارد.

EOIP را می توانیم به دو صورت پیاده سازی کنیم : بصورت لایه دو و به صورت لایه سه ، در ادامه به کانفیگ هر دو خواهیم پرداخت.

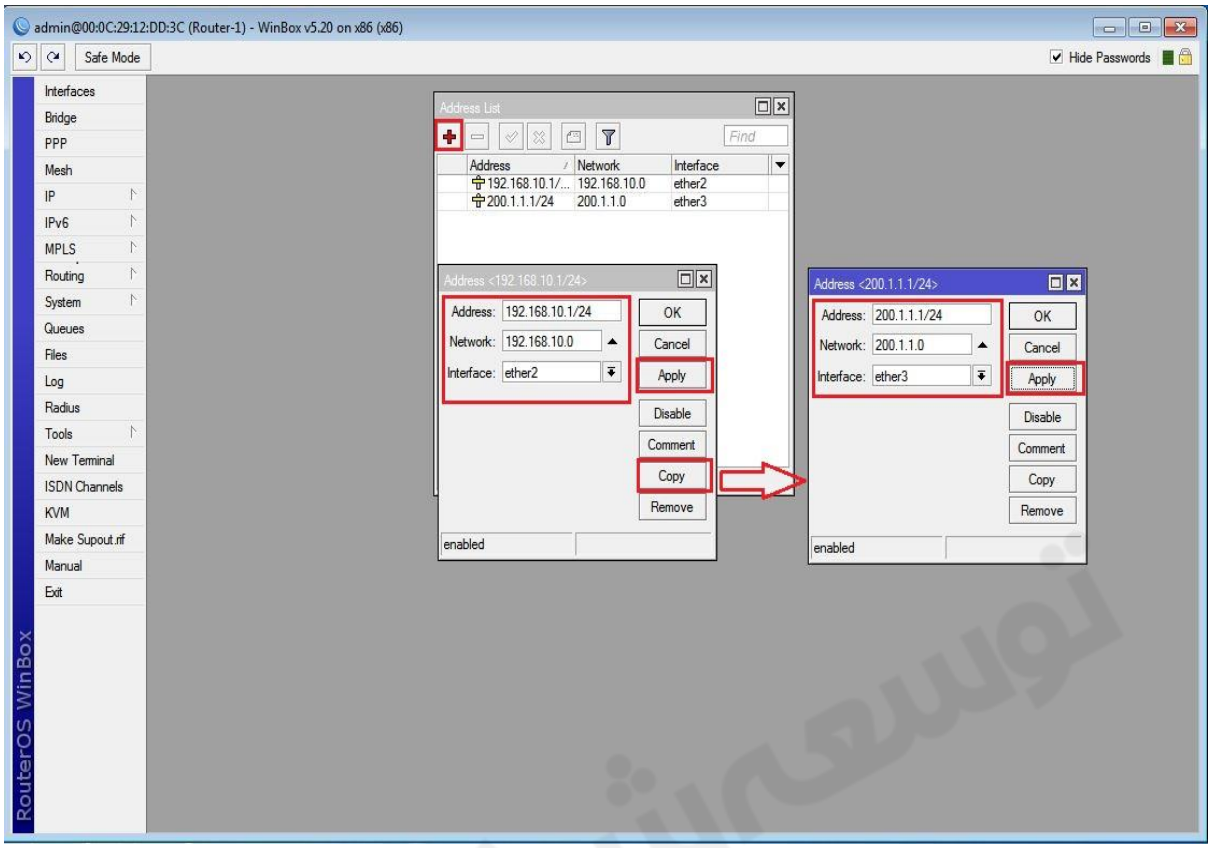
کاربرد **EOIP Tunnel** زمانی است که بخواهیم دو شبکه را با هم یکپارچه کنیم به طوری که هر شبکه در یک **Broadcat Domain** باشند و از منابع موجود در هر شبکه ، از راه دور بهره ببریم.در این حالت چنانچه در یکی اط شبکه ها یک **DHCP** سرور وجود داشته باشد شبکه دیگر که با استفاده از این پروتکل به آن متصل شده است می تواند از آن سرور ، سرویس بگیرد.برای استفاده از **EOIP** باید روترهای میکروتیک به یکدیگر **Tunnel** بزنند . این **Tunnel** برروی بستر اینترنت برقرار می شود و سپس با استفاده از **Bridge** بین **Tunnel** برقرار شده و کارت شبکه روتر که به سمت شبکه داخلی است ارتباط برقرار می کنیم.

سناریو ۱ : هدف از بررسی این سناریو ، پیاده سازی پروتکل **EOIP** بصورت لایه ۳ می باشد.

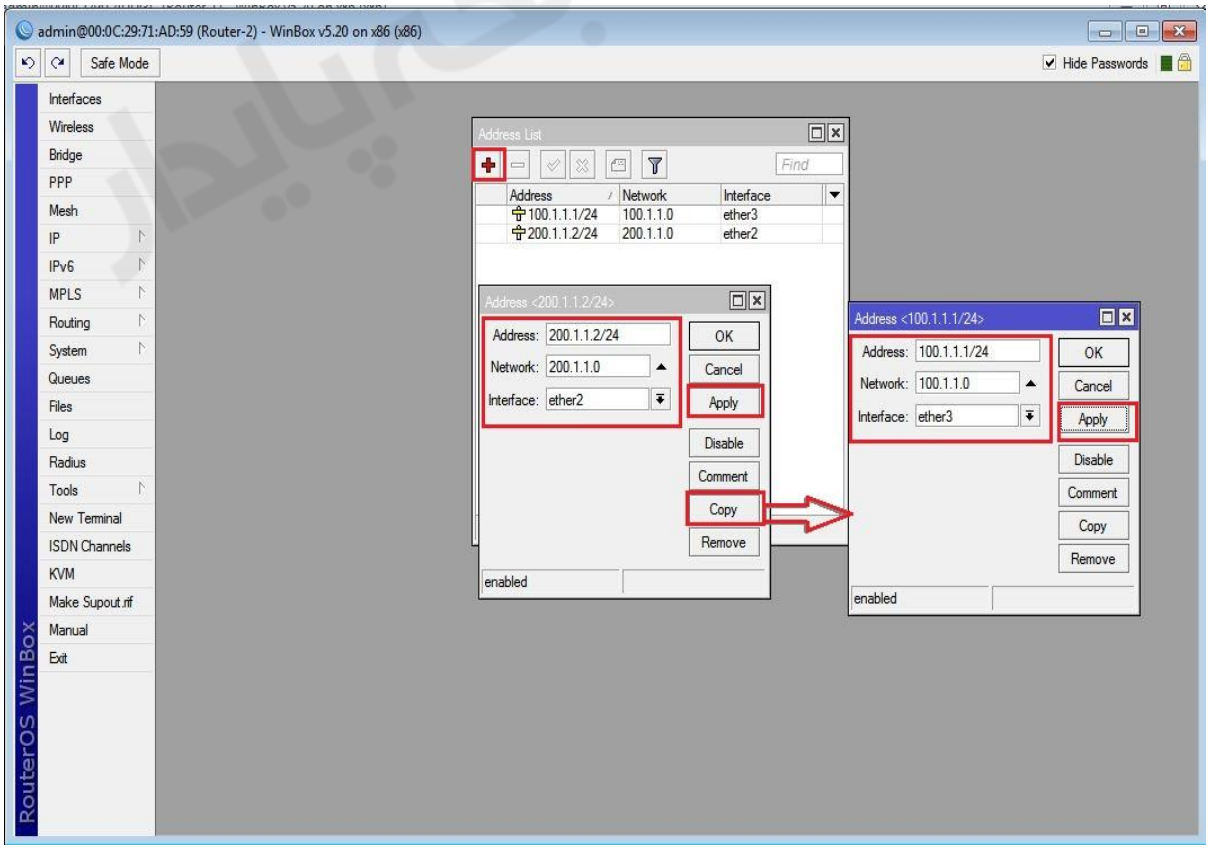


انتساب IP به کارت های شبکه روترها :

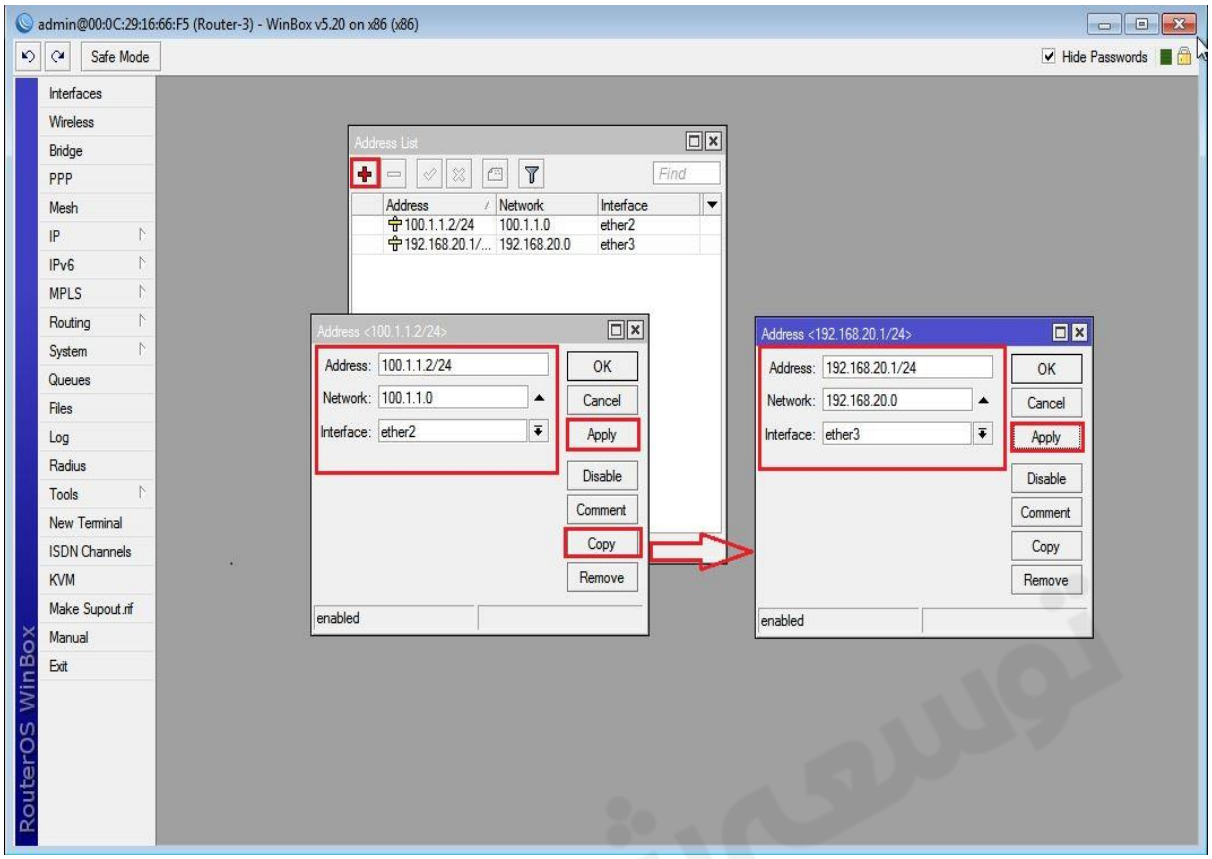
روتر R1 :



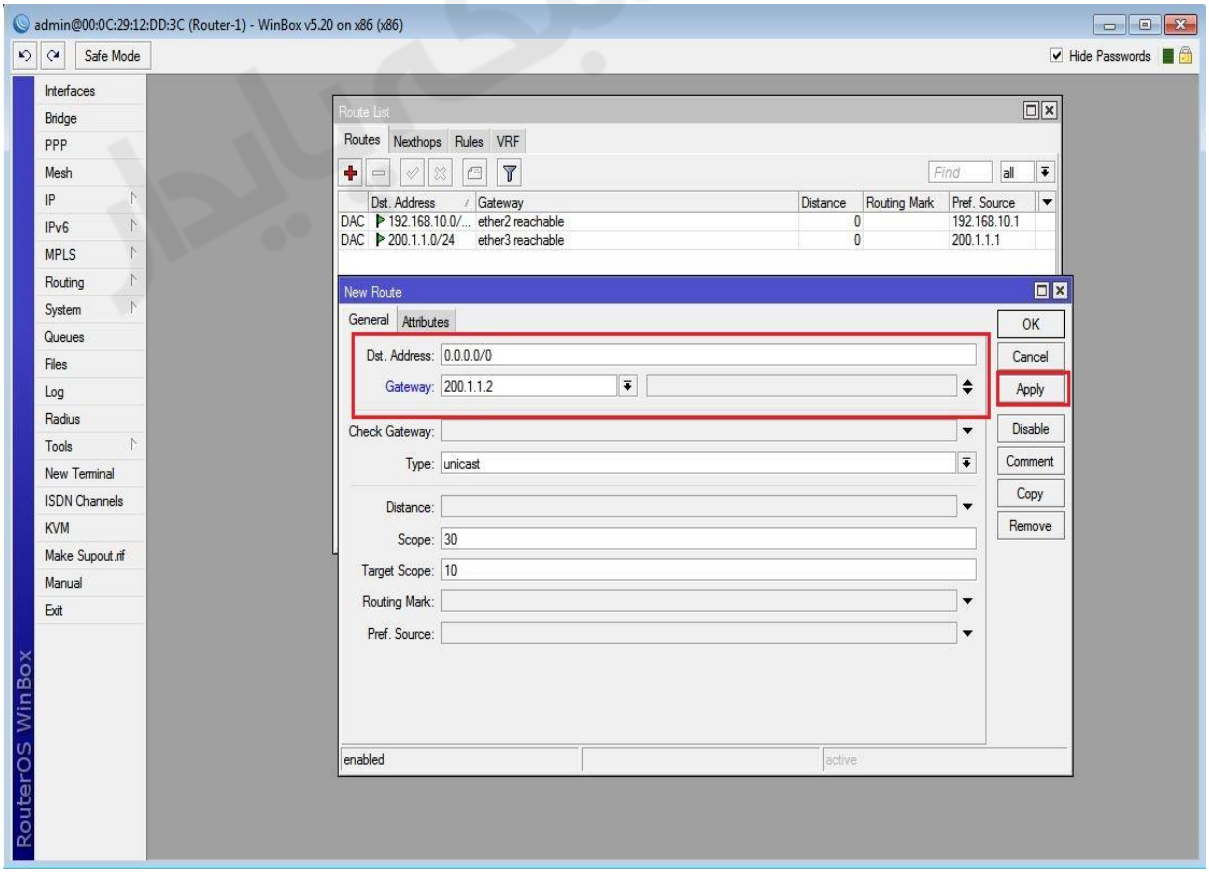
روتر R2 :



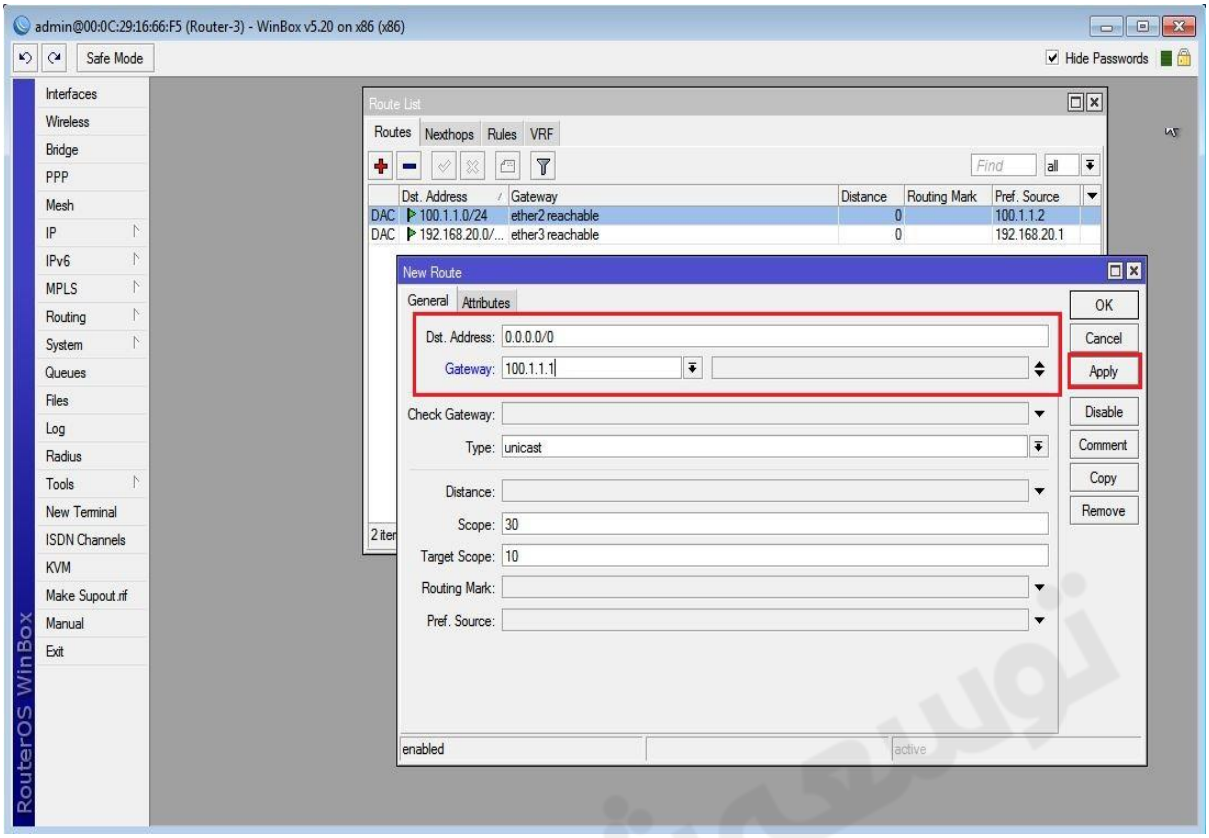
روتر **R3**:



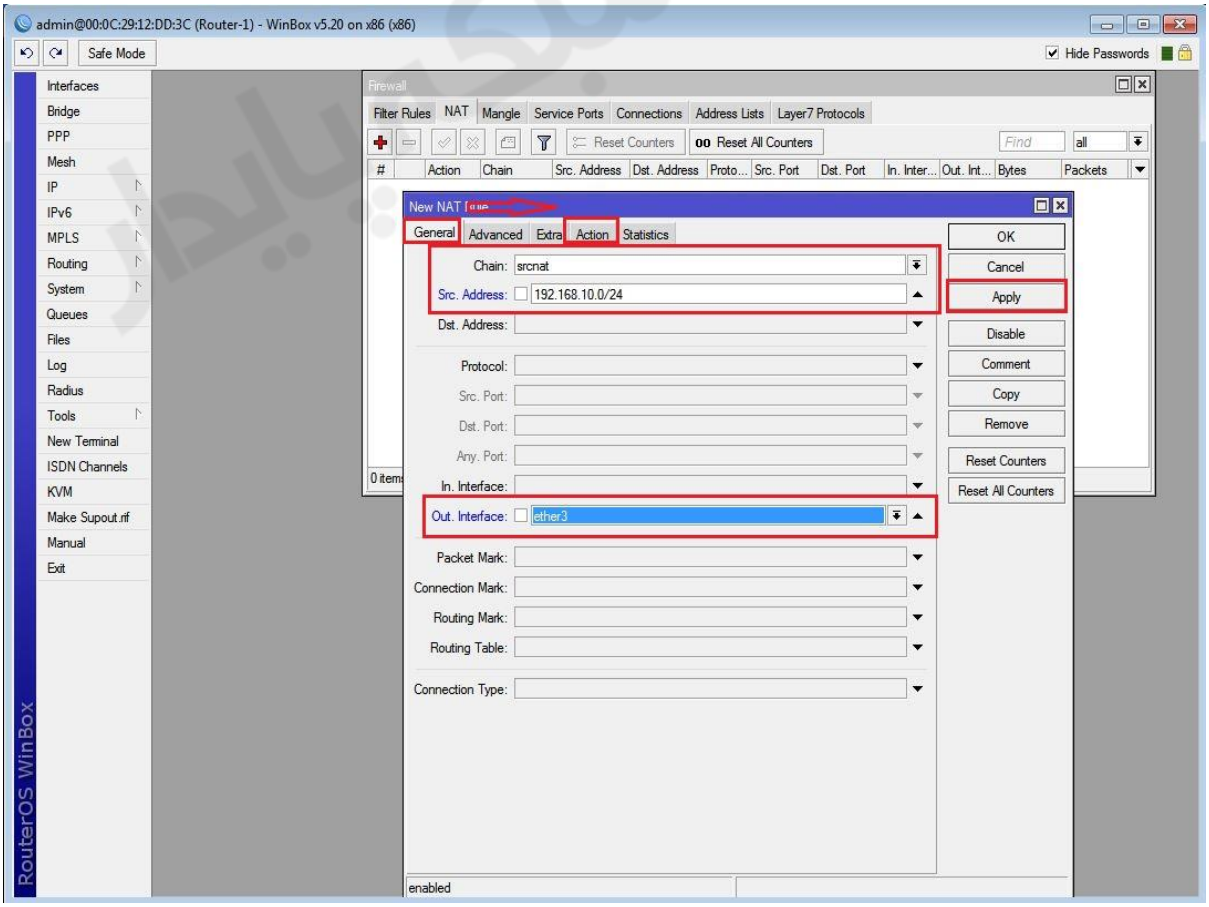
تعریف **Default Route** در روتر **R1**:

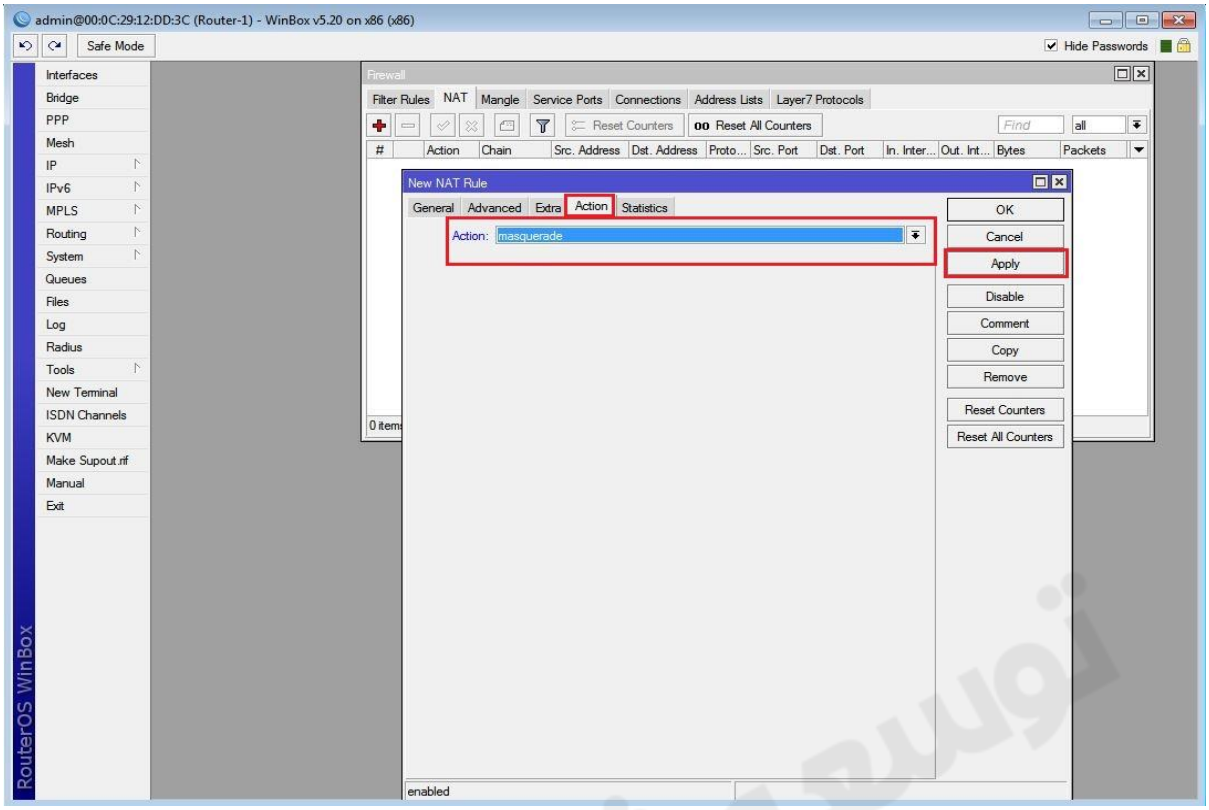


تعریف **Default Route** در **R3** :

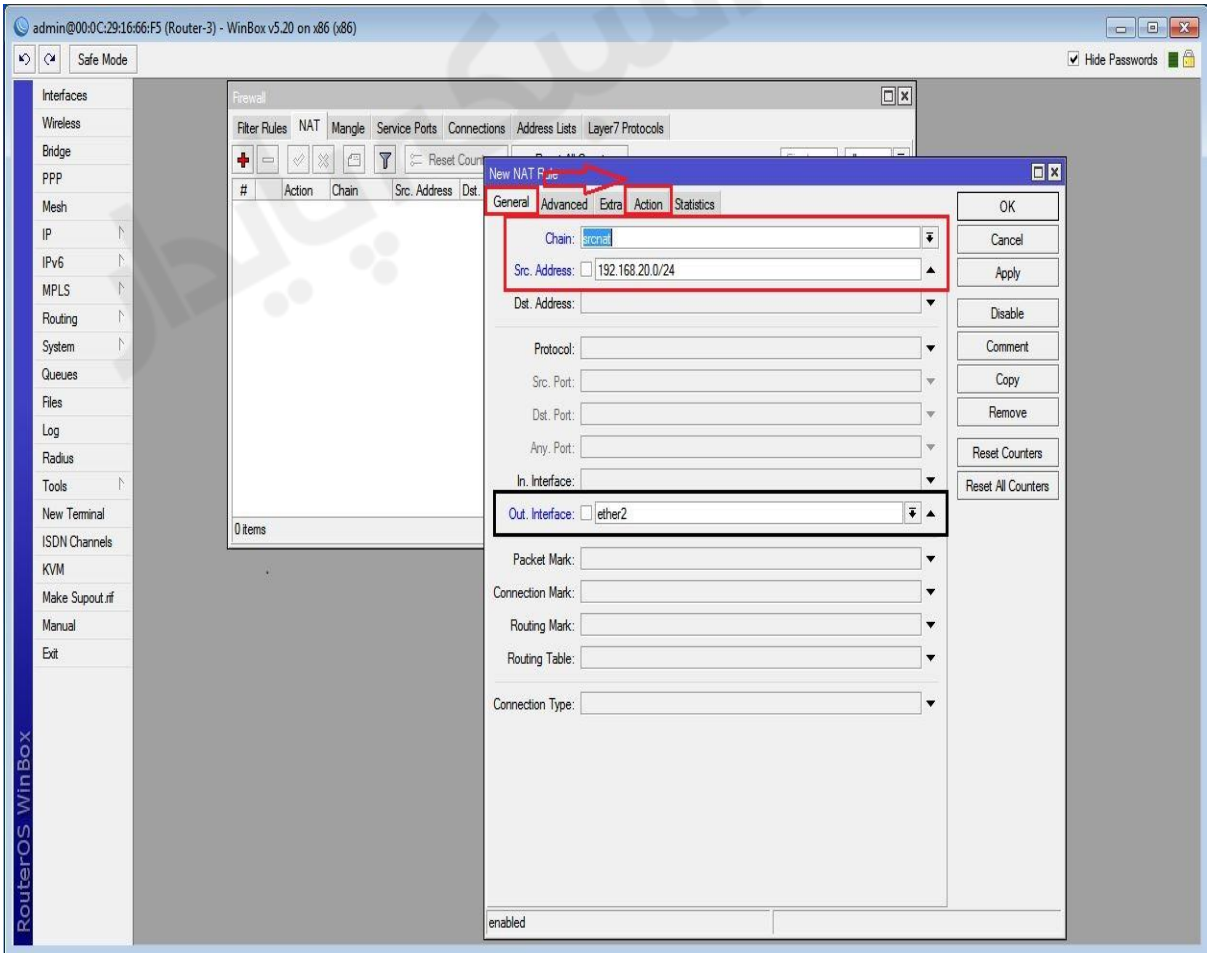


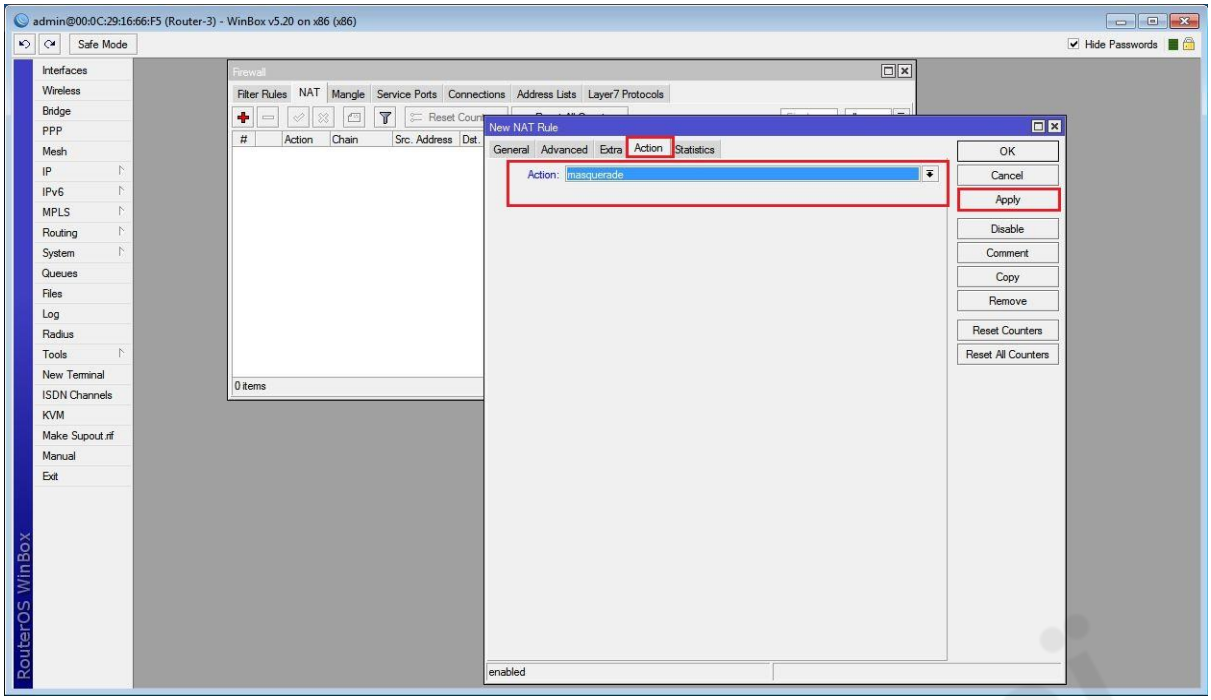
ایجاد Nat در روتر R1 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.





ایجاد Nat در روتر R3 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.





تعریف کارت شبکه مجازی EOIP در روتر R1 :

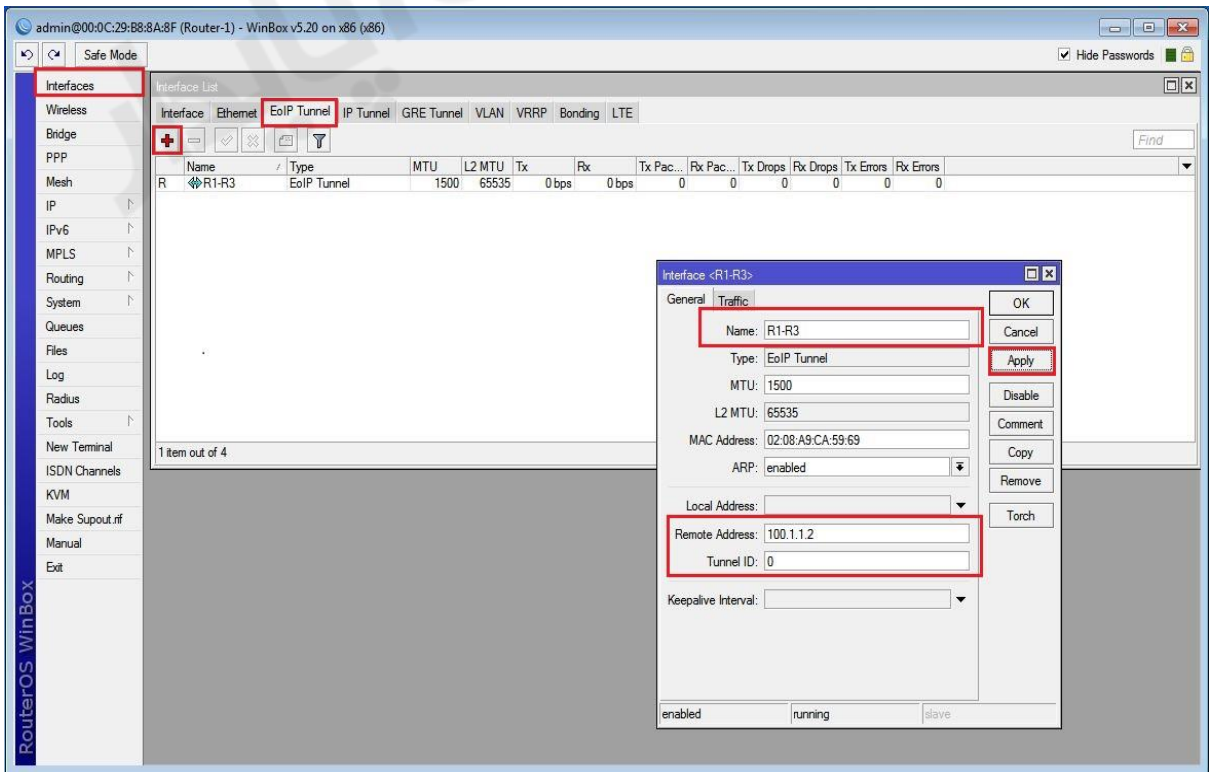
برای اینکار از منوی اصلی برروی Interface کلیک کرده و از پنجره باز شده به تب EOIP Tunnel رفته بر روی Add کلیک می کنیم و تنظیمات زیر را انجام می دهیم :

Name : یک نام برای کارت شبکه مجازی IPIP انتخاب می کنیم.

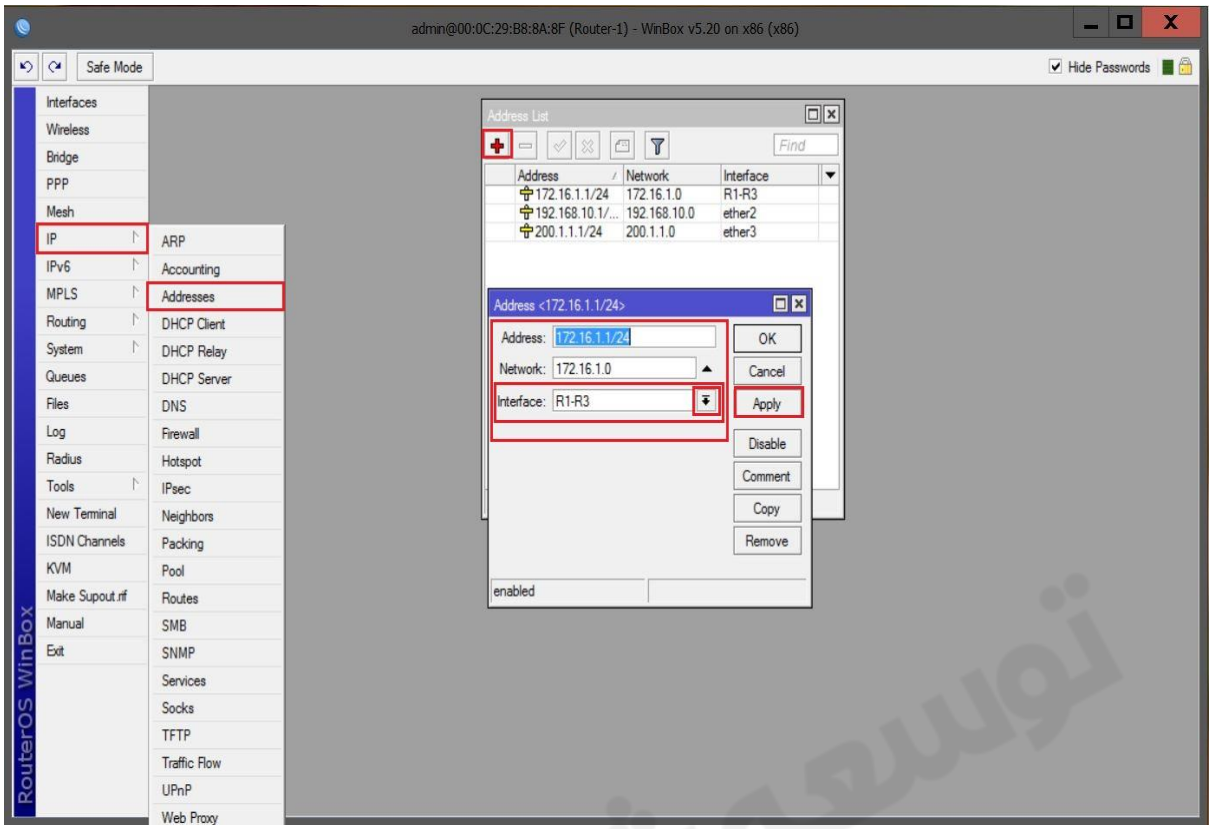
Remote Address : آدرس IP مربوط به روتر مقصد مشخص می شود.

Tunnel ID : در این قسمت باید یک شماره برای Tunnel وارد کنیم که بصورت پیش فرض 0 می باشد.این شماره باید در دوتا روتر یکی باشد وگرنه ارتباط برقرار نمی شود.

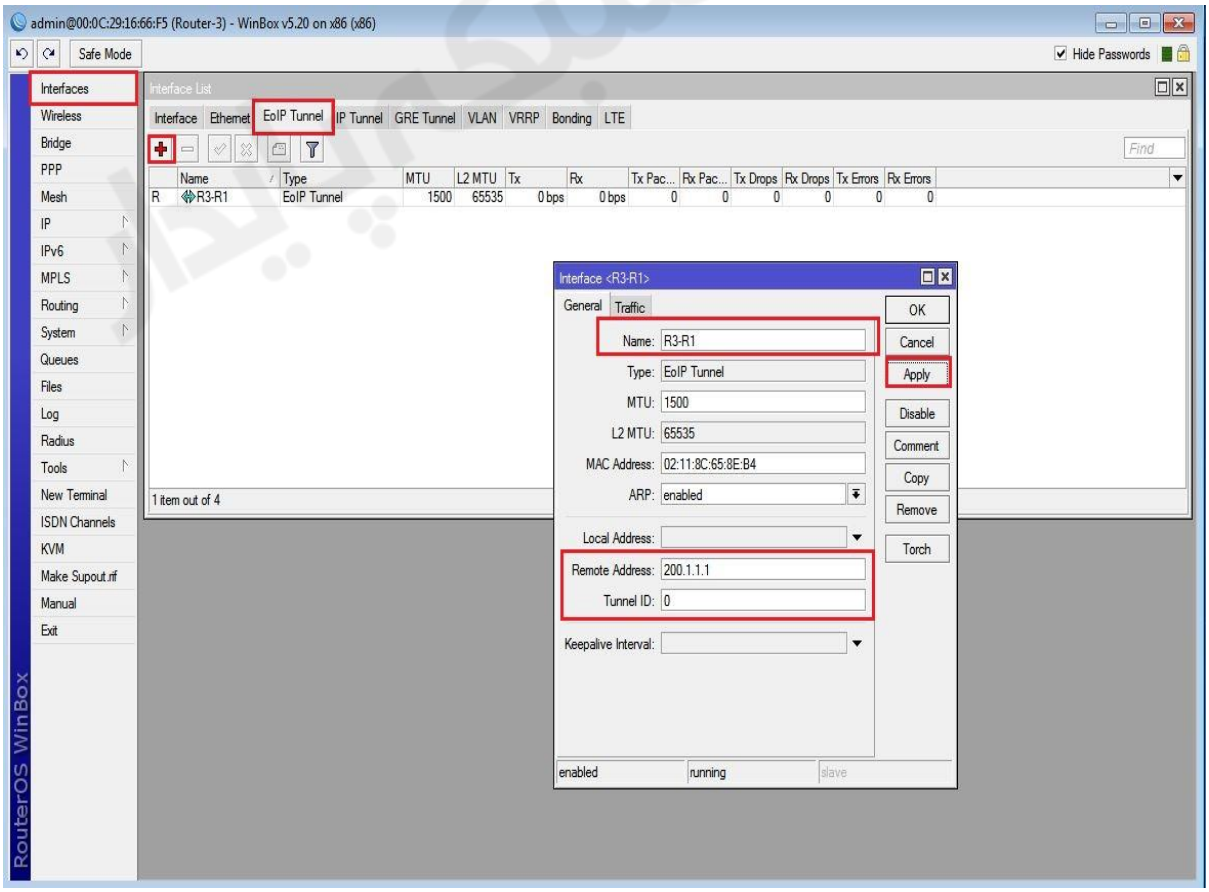
***نکته : در صورتی که چند EOIP Tunnel ایجاد کرده ایم نباید Tunnel ID آنها با هم یکسان باشد.**



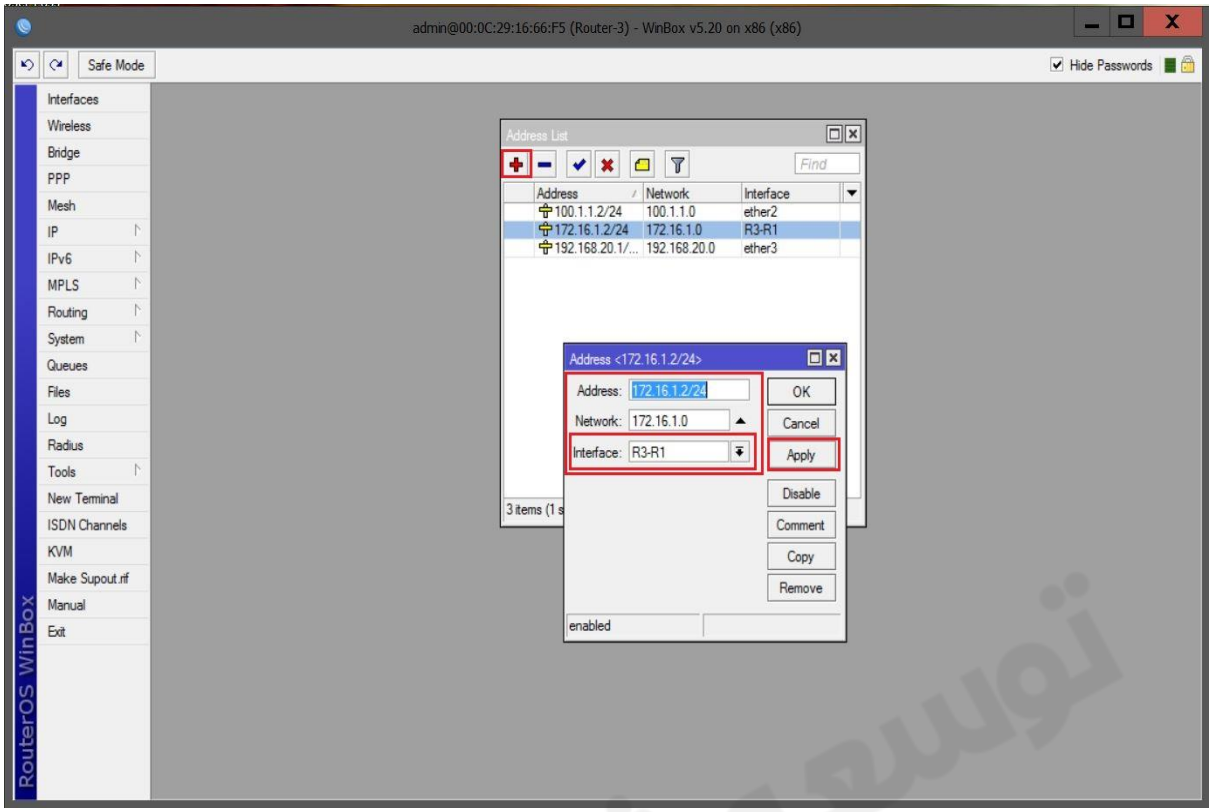
انتساب **IP** به کارت شبکه مجازی در روتر **R1** :



تعریف کارت شبکه مجازی **EOIP** در روتر **R3** :

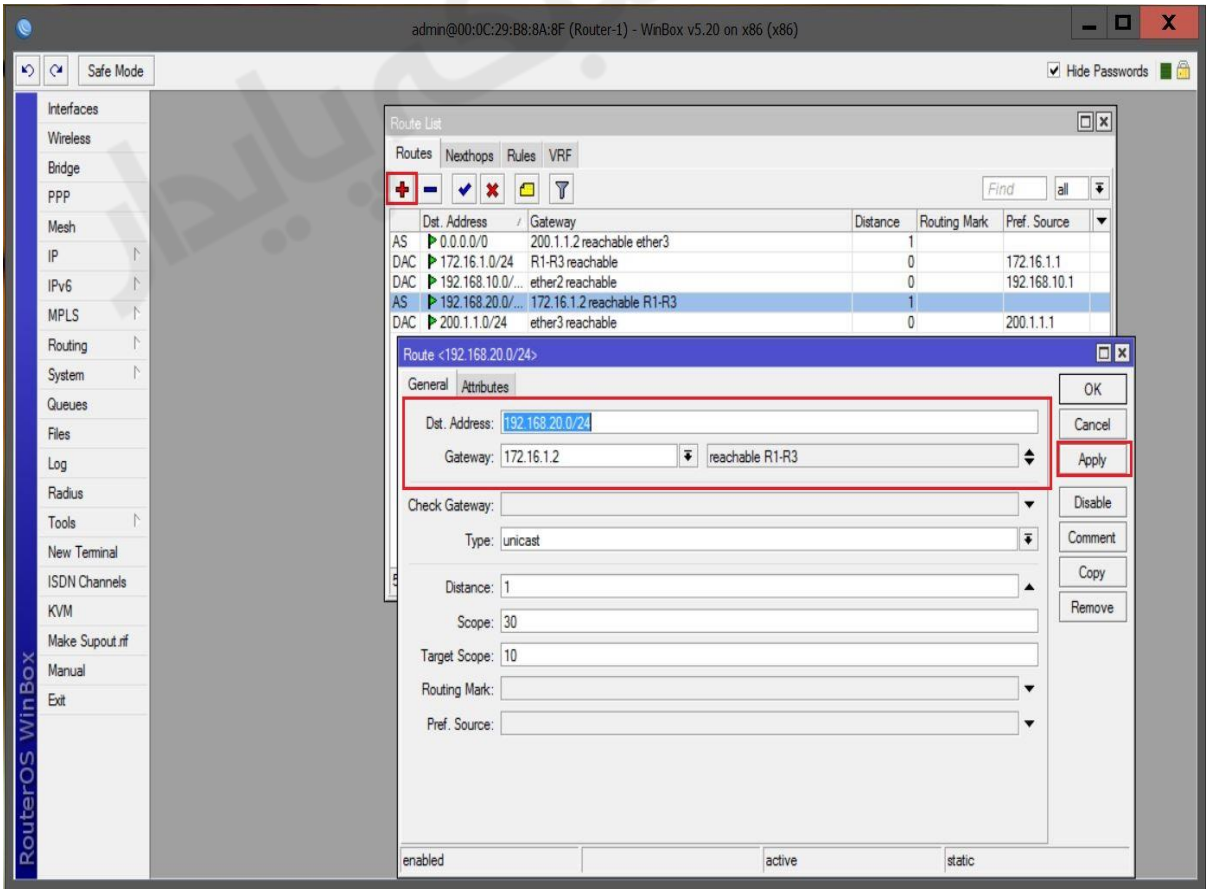


انتساب IP به کارت شبکه مجازی در روتر R3 :



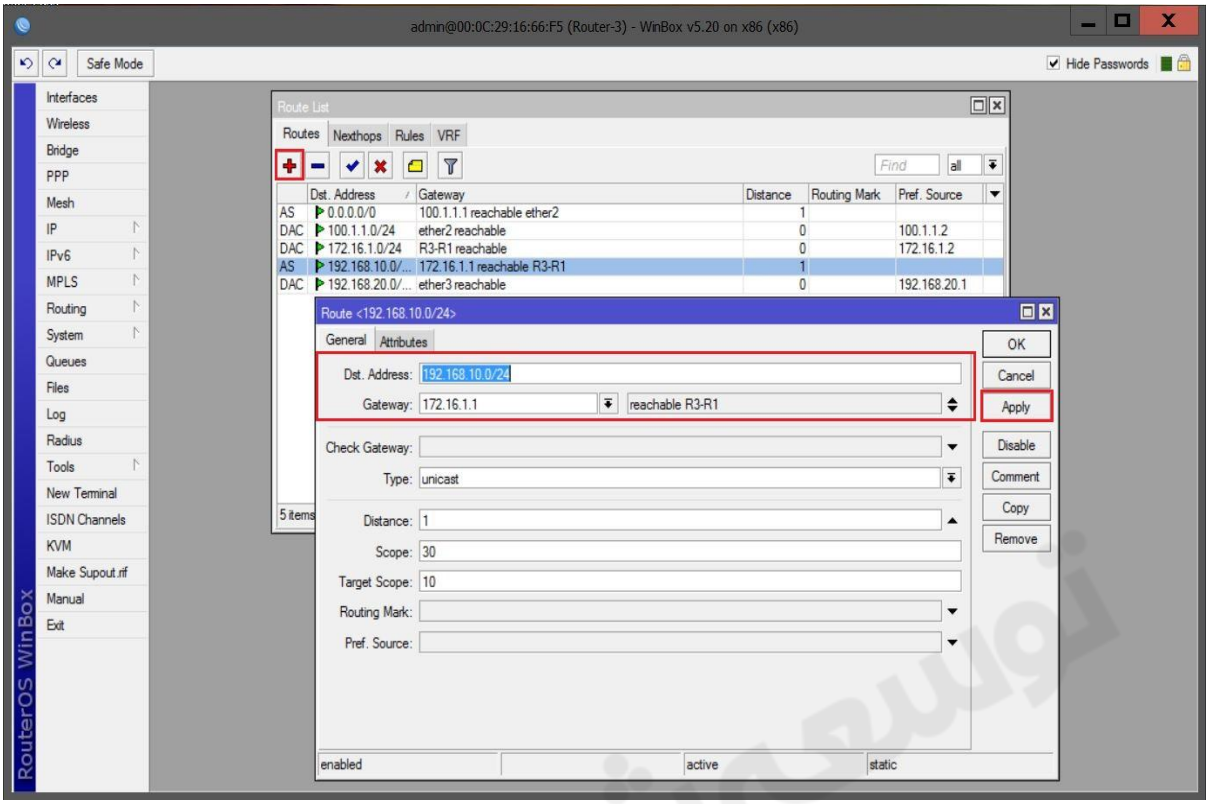
تعریف Static Route در روتر R1 :

برای برقراری ارتباط کلاینت های موجود در Lan-1 با کلاینت های موجود در Lan-2 در روتر R1 ، Static Route زیر را تعریف می کنیم.



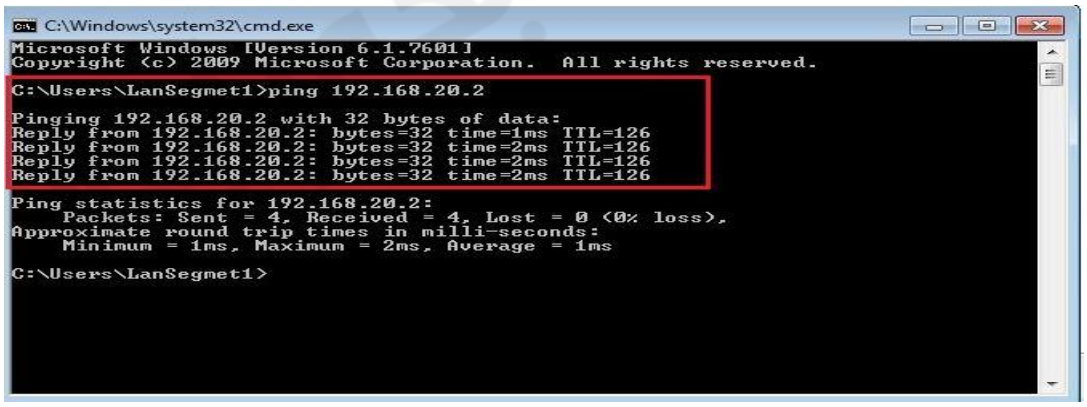
تعریف Static Route در روتر R3 :

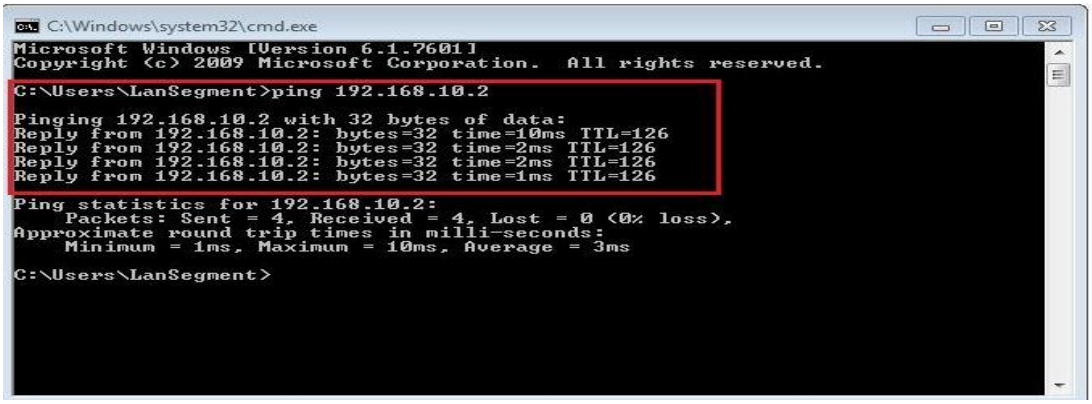
برای برقراری ارتباط کلاینت های موجود در Lan-2 با کلاینت های موجود در Lan-1 در روتر R3 ، Static Route زیر را تعریف می کنیم.



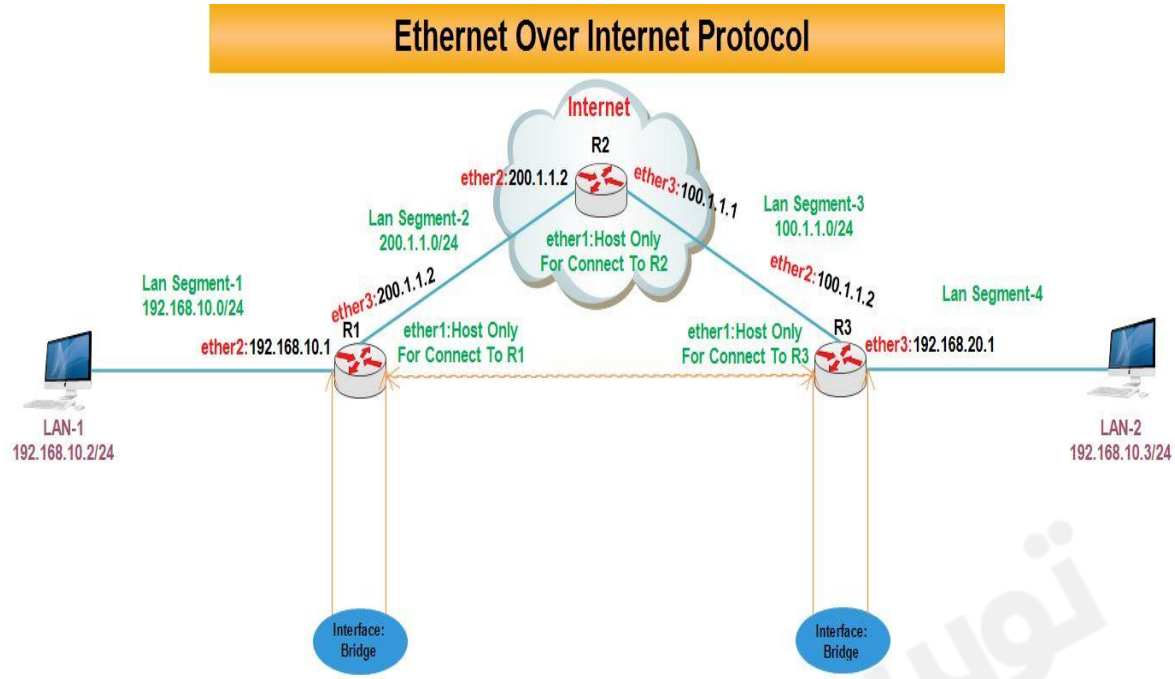
تنظیمات کلاینت :

طبق سناریو به کلاینت ها IP اختصاص می دهیم و برای تست ارتباط از دستور Ping استفاده می کنیم.





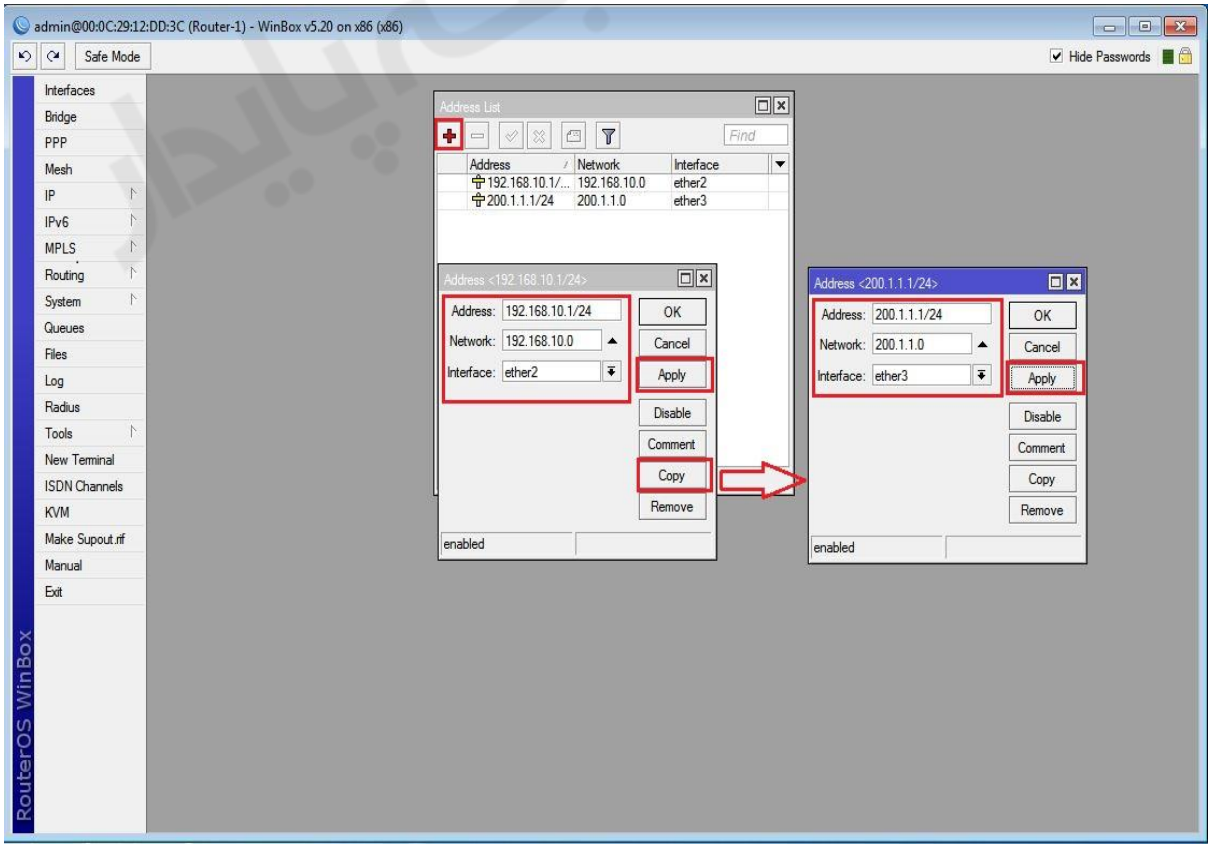
سناریو ۲ : هدف از بررسی این سناریو ، پیاده سازی پروتکل **EOIP** بصورت لایه ۲ می باشد.



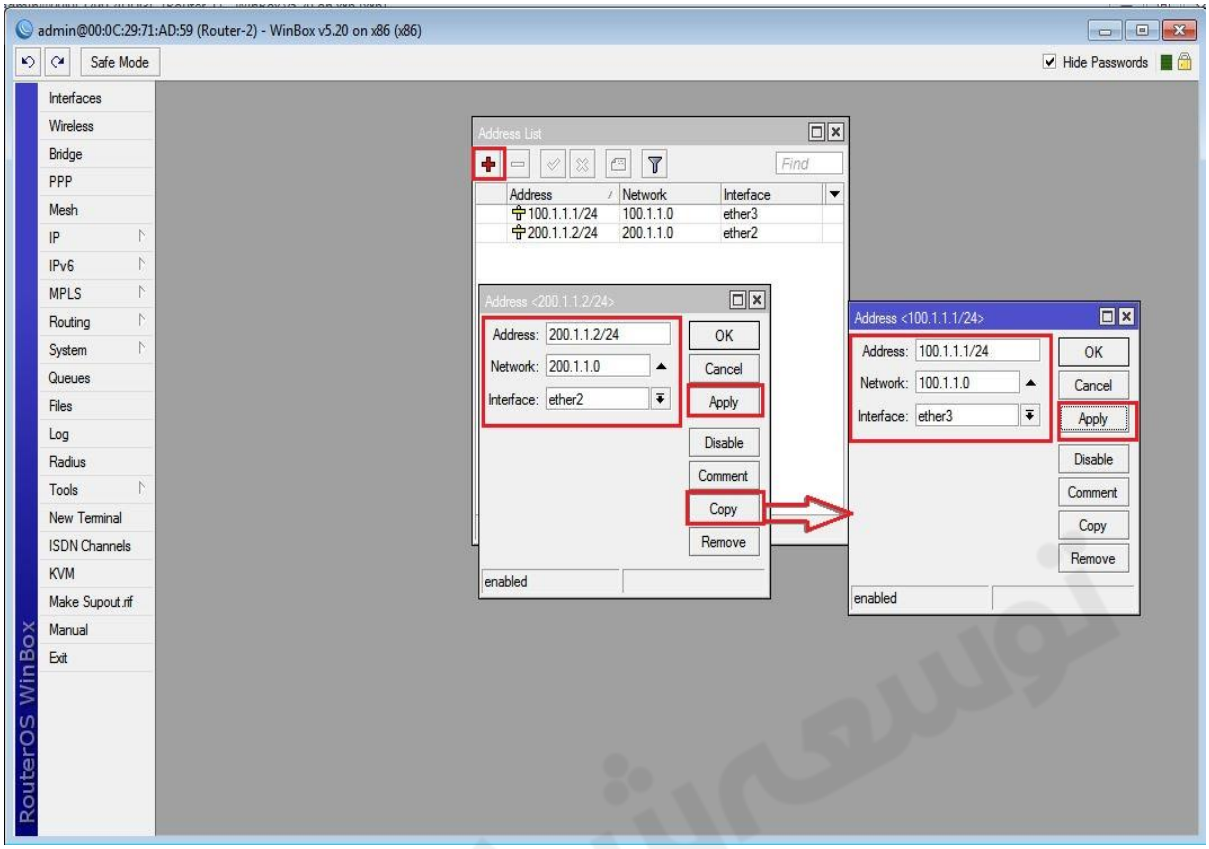
*نکته : برای پیاده سازی **EOIP Tunnel** بصورت لایه ۲ ، باید **Net ID** دو شبکه یکی باشد و نیازی به تعریف کردن **Gateway** در کلاینت ها نیست.

انتساب IP به کارت های شبکه روترها :

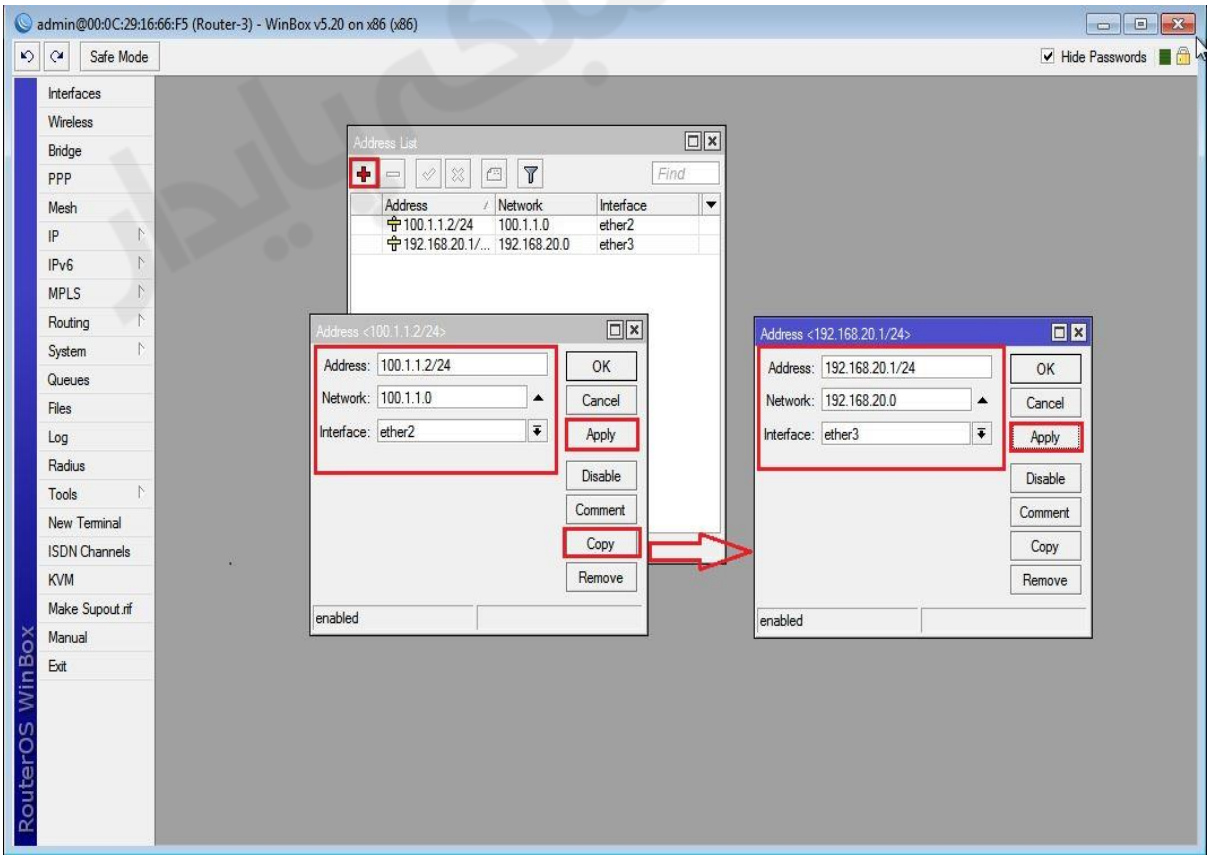
روتر R1 :



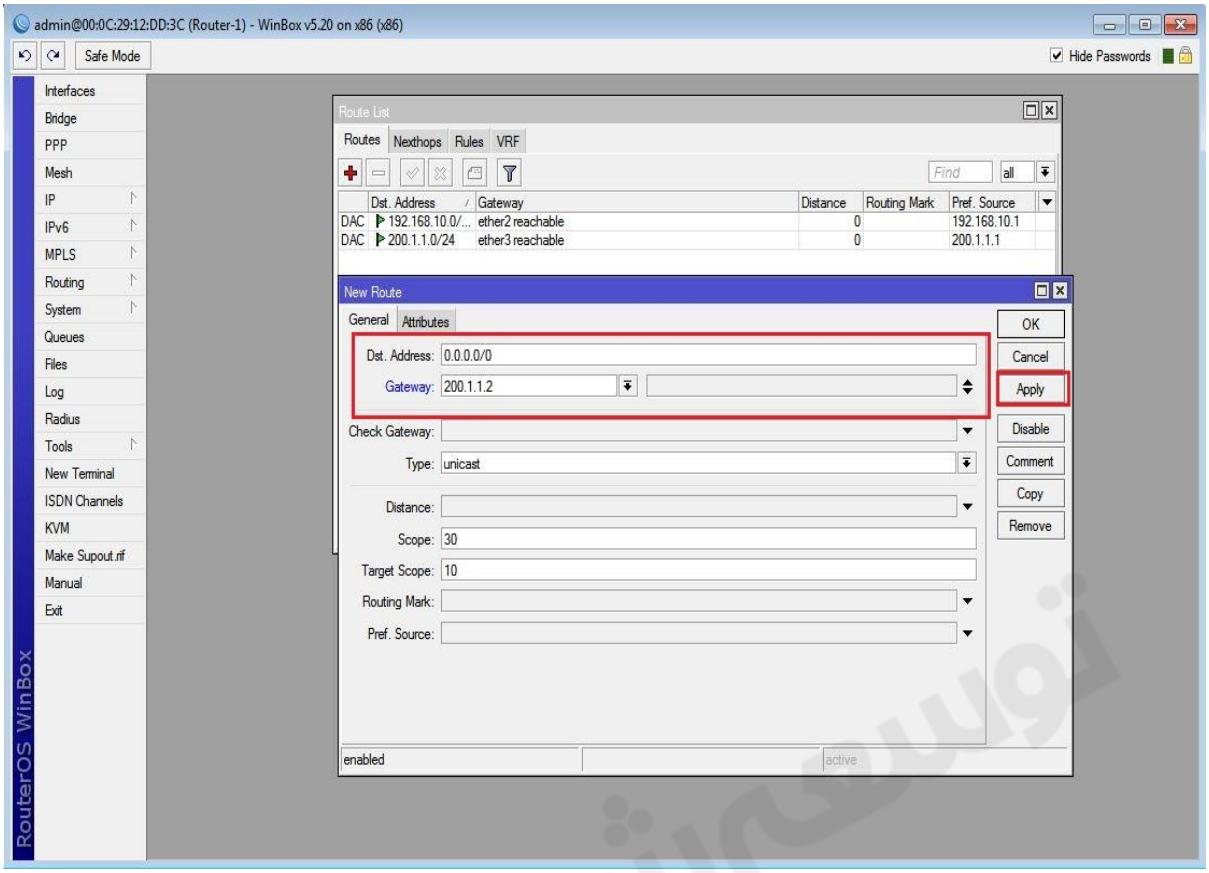
روتر R2 :



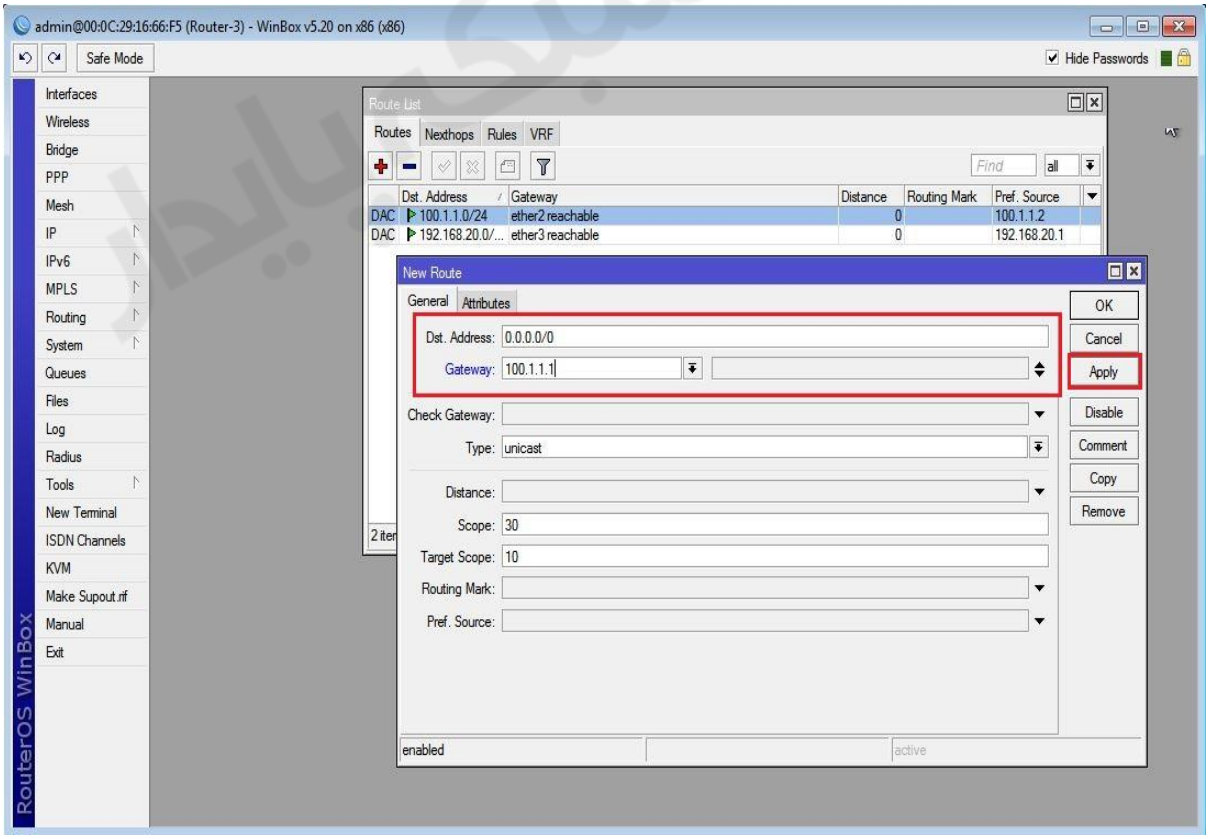
روتر R3 :



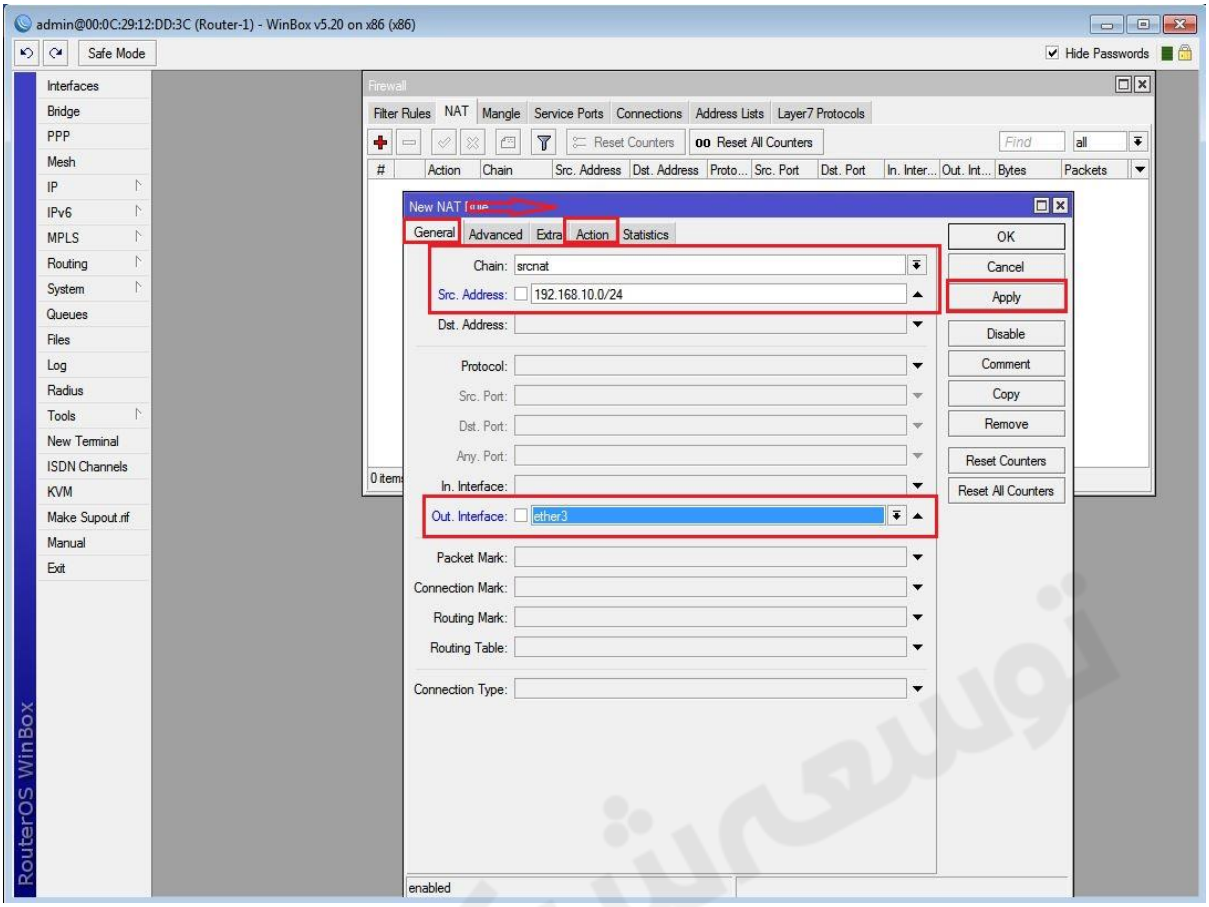
تعریف **Default Route** در روتر **R1** :

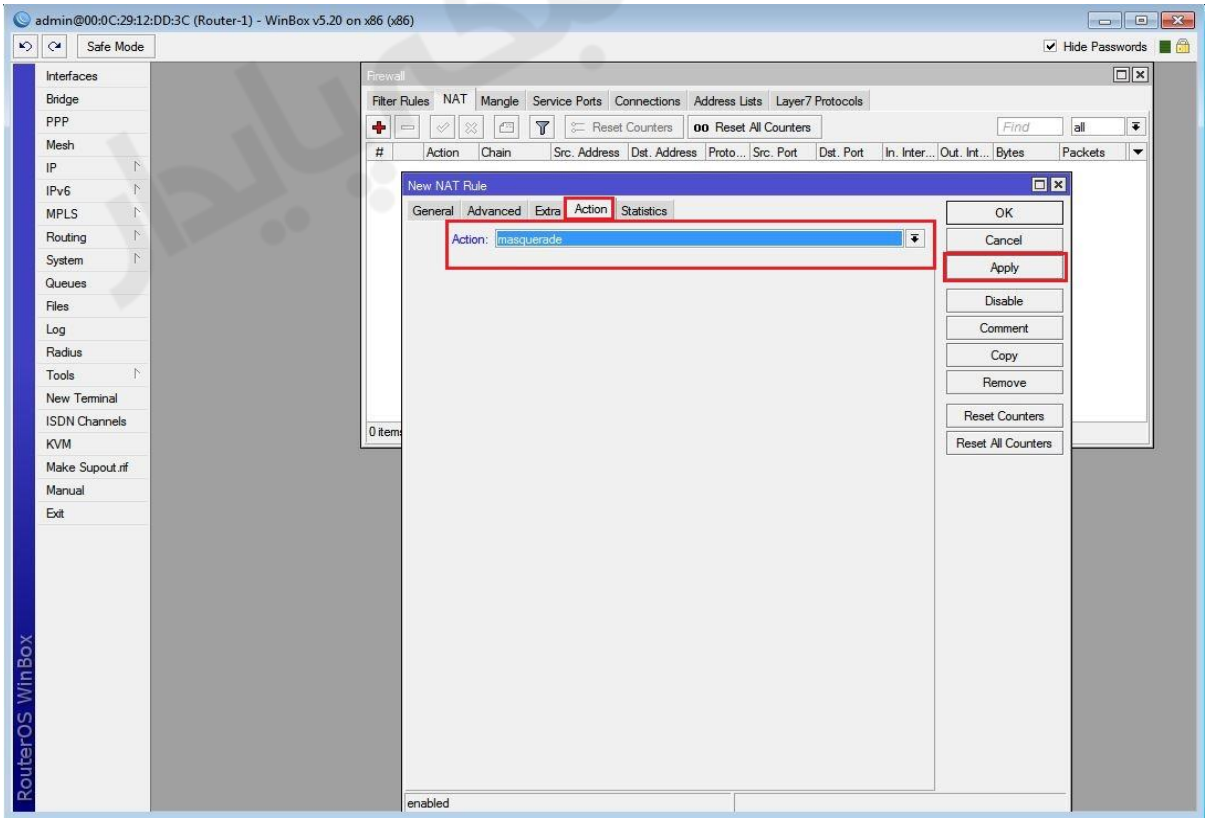


تعریف **Default Route** در **R3** :

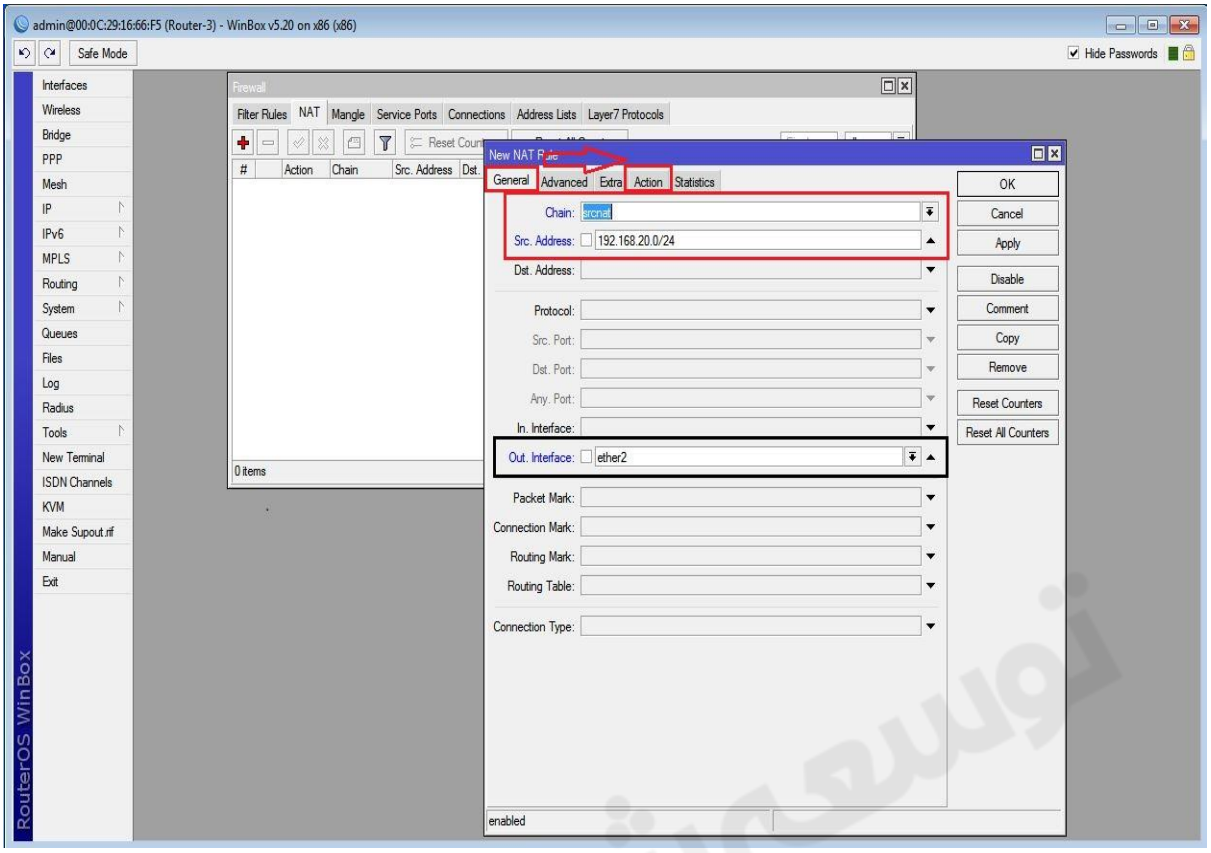


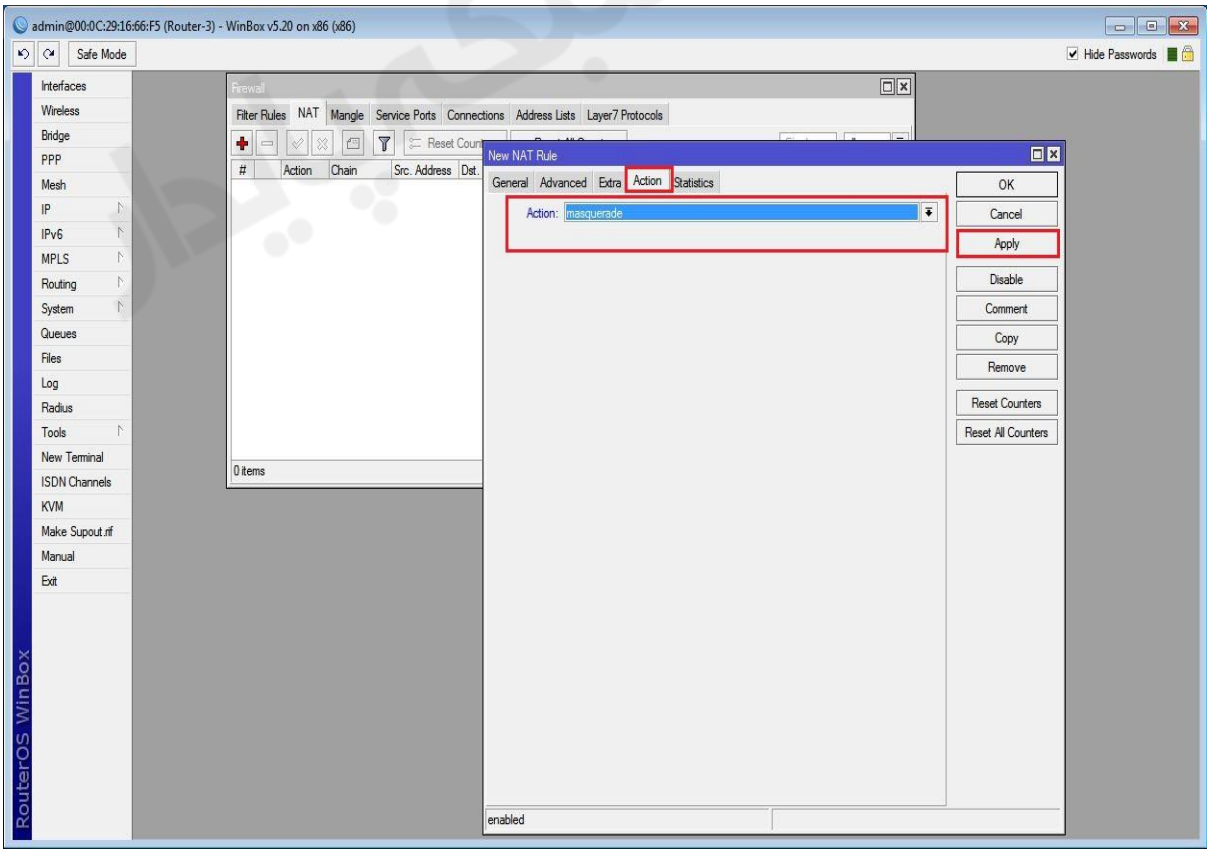
ایجاد **Nat** در روتر **R1** برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.



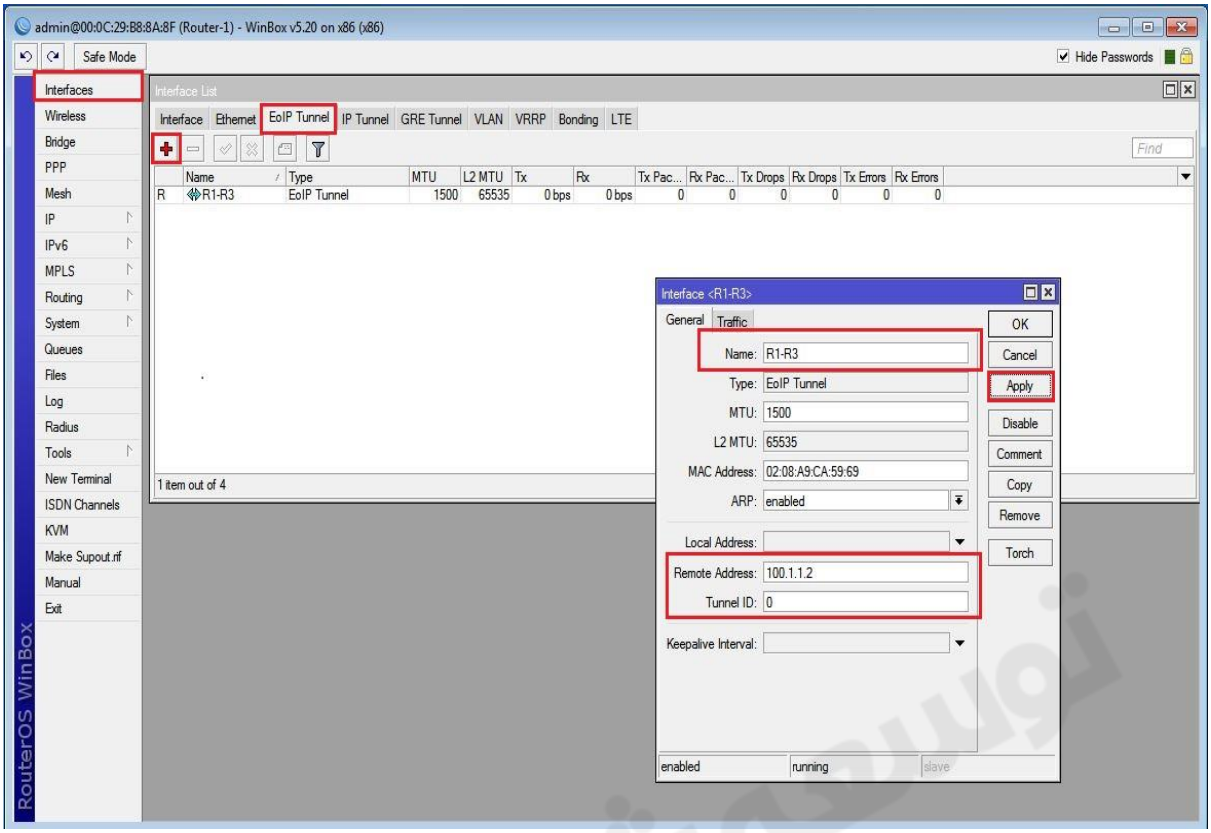


ایجاد Nat در روتر R3 برای اینکه کلاینت ها به اینترنت دسترسی داشته باشند.



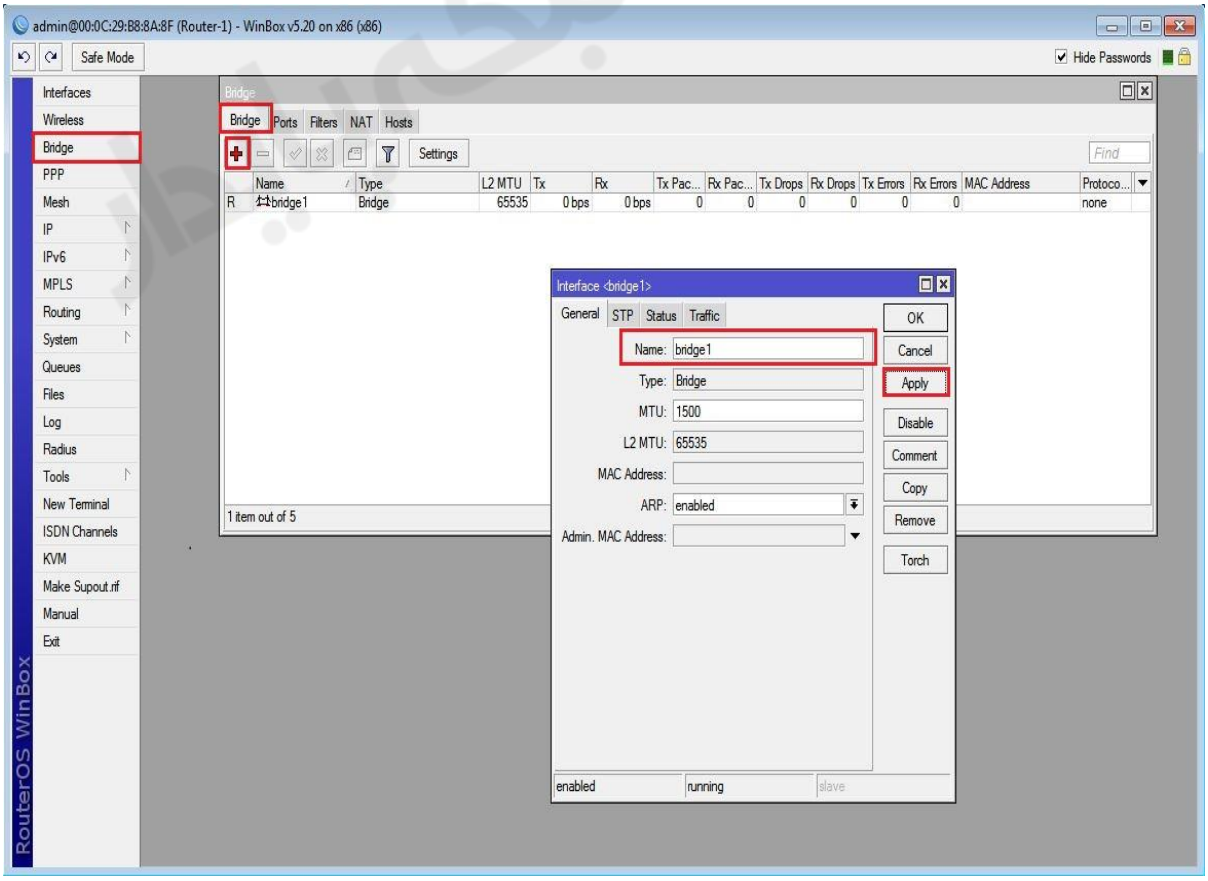


تعریف کارت شبکه مجازی EOIP در روتر R1 :



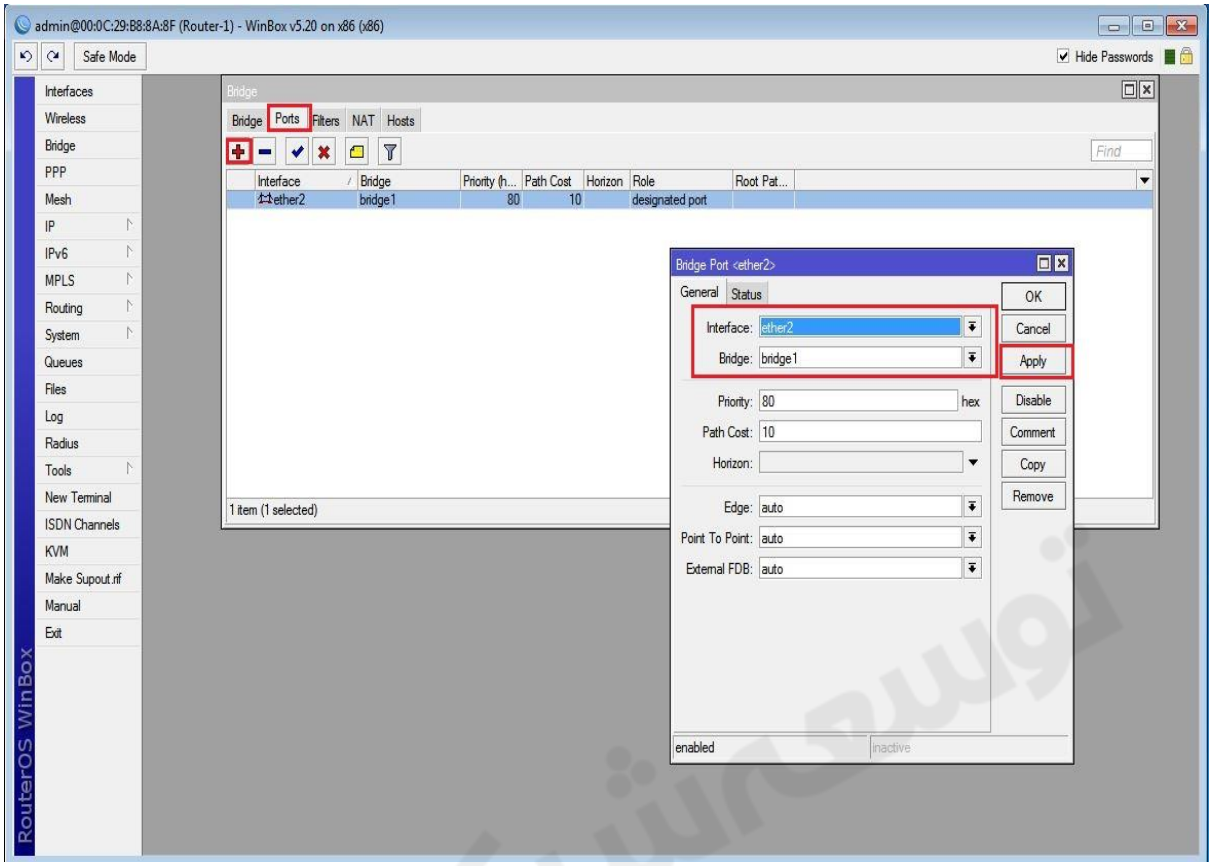
ایجاد کارت شبکه مجازی Bridge در روتر R1 :

برای این کار از منوی اصلی Bridge را انتخاب و از پنجره باز شده از تب Bridge بر روی Add کلیک می کنیم.

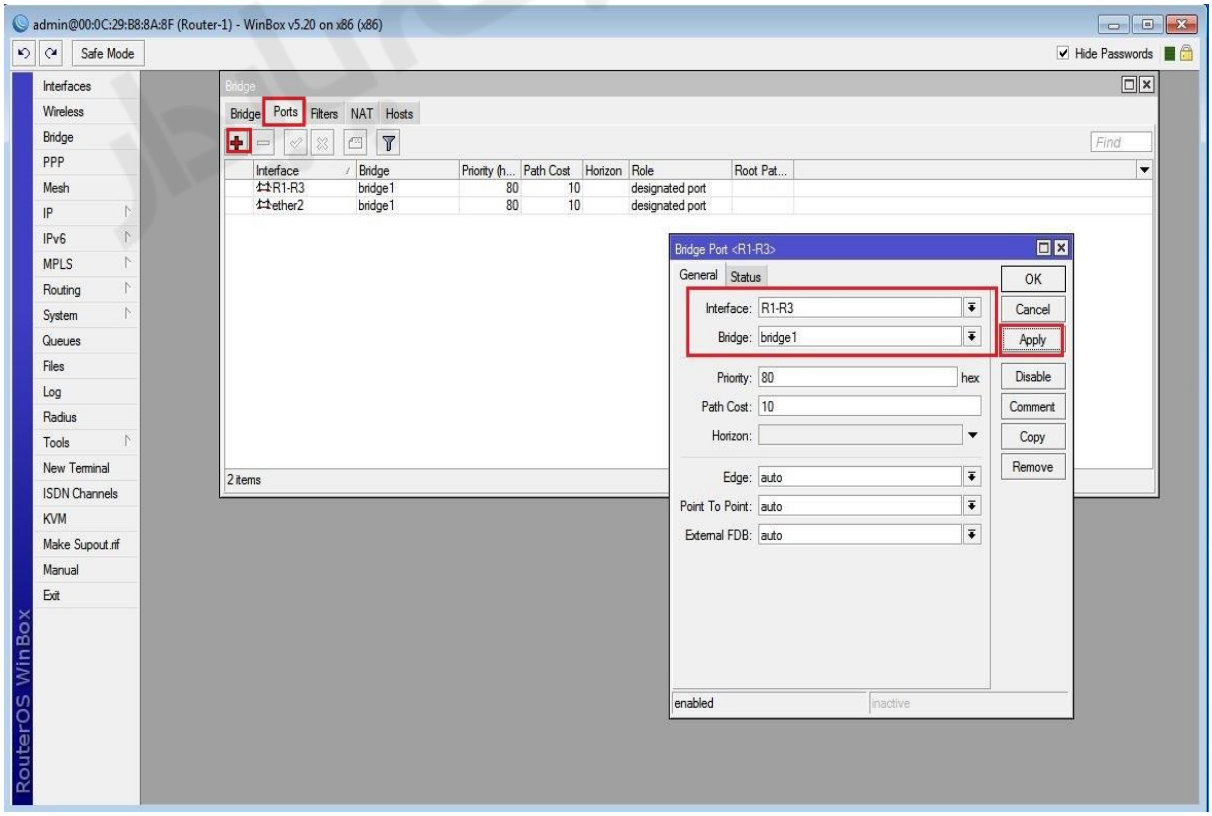


ارتباط کارت شبکه داخلی روتر با کارت شبکه مجازی **Bridge** در روتر **R1** :

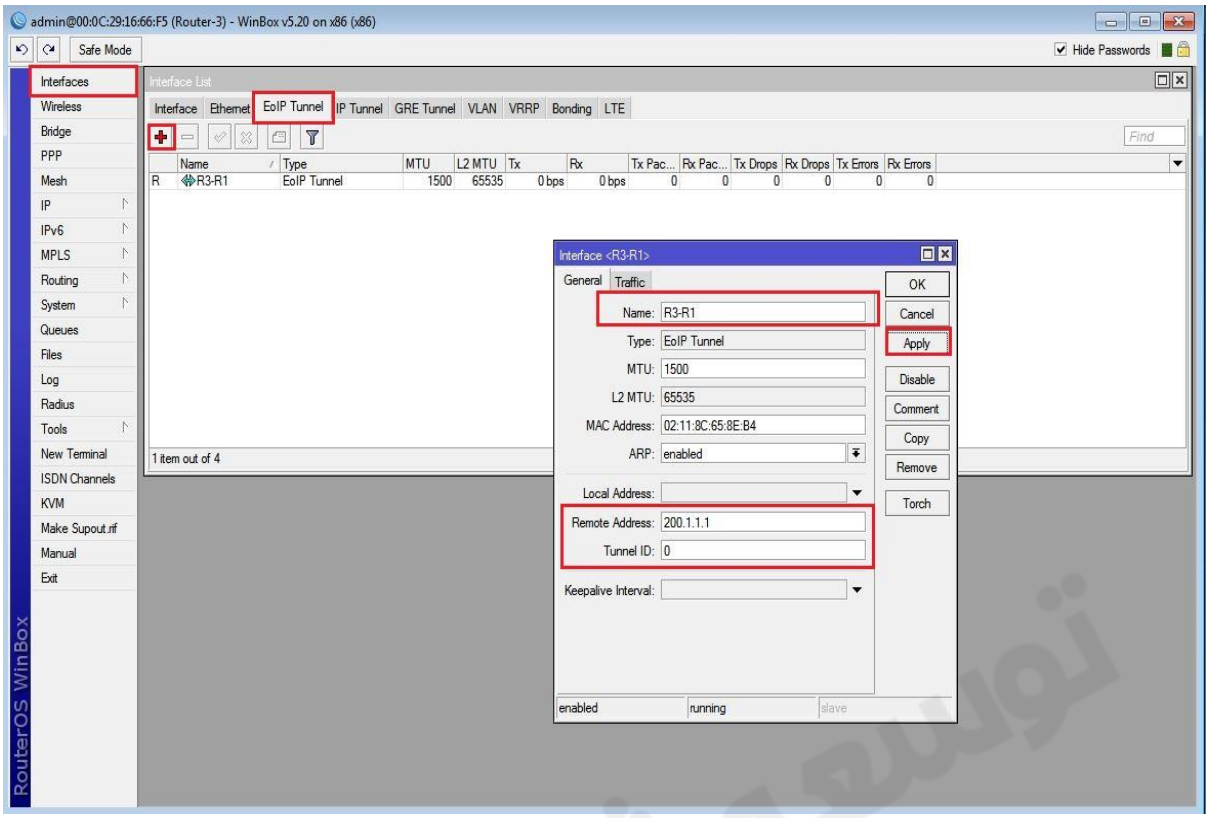
برای این کار به تب **Port** می رویم و بر روی **Add** کلیک می کنیم و تنظیمات را طبق عکس زیر انجام می دهیم.



ارتباط کارت شبکه مجازی **EOIP** با کارت شبکه مجازی **Bridge** در روتر **R1** :

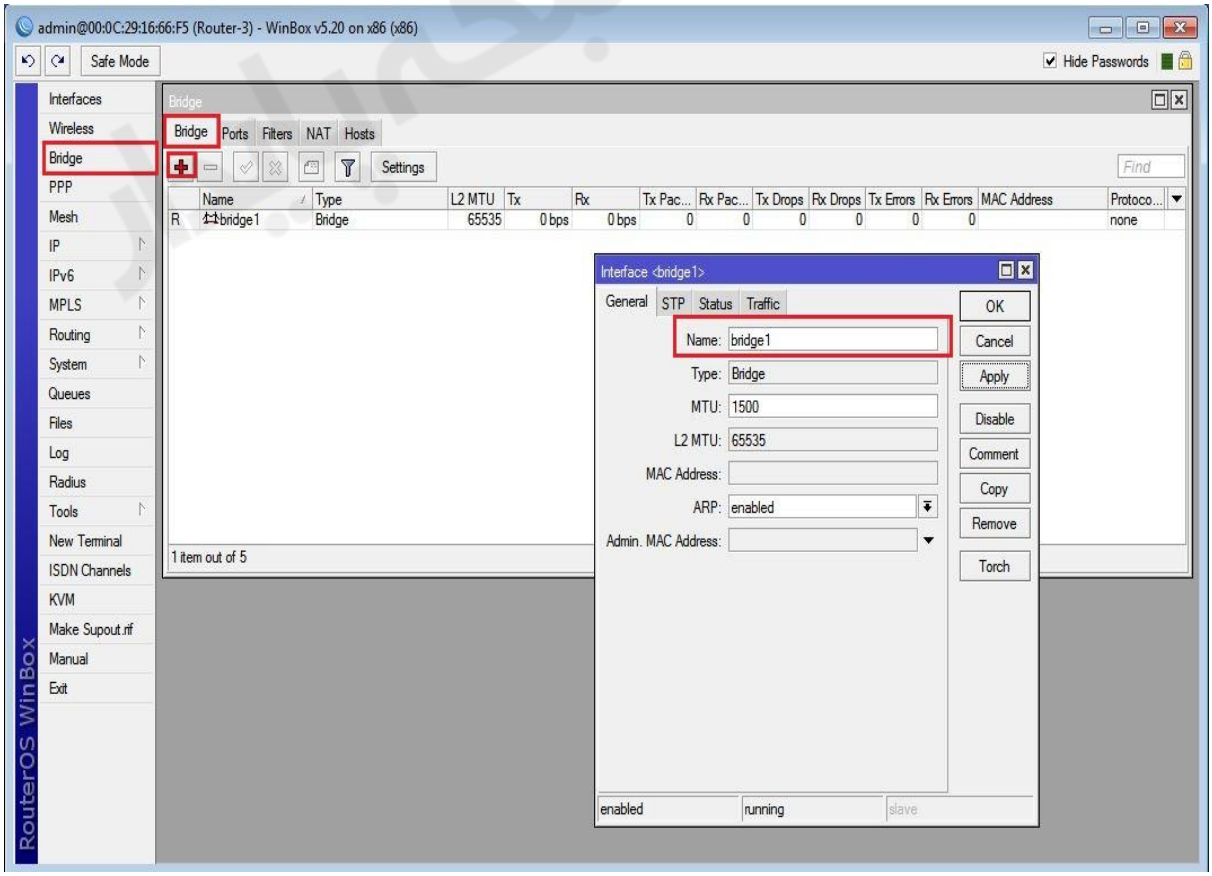


تعریف کارت شبکه مجازی EOIP در روتر R3 :

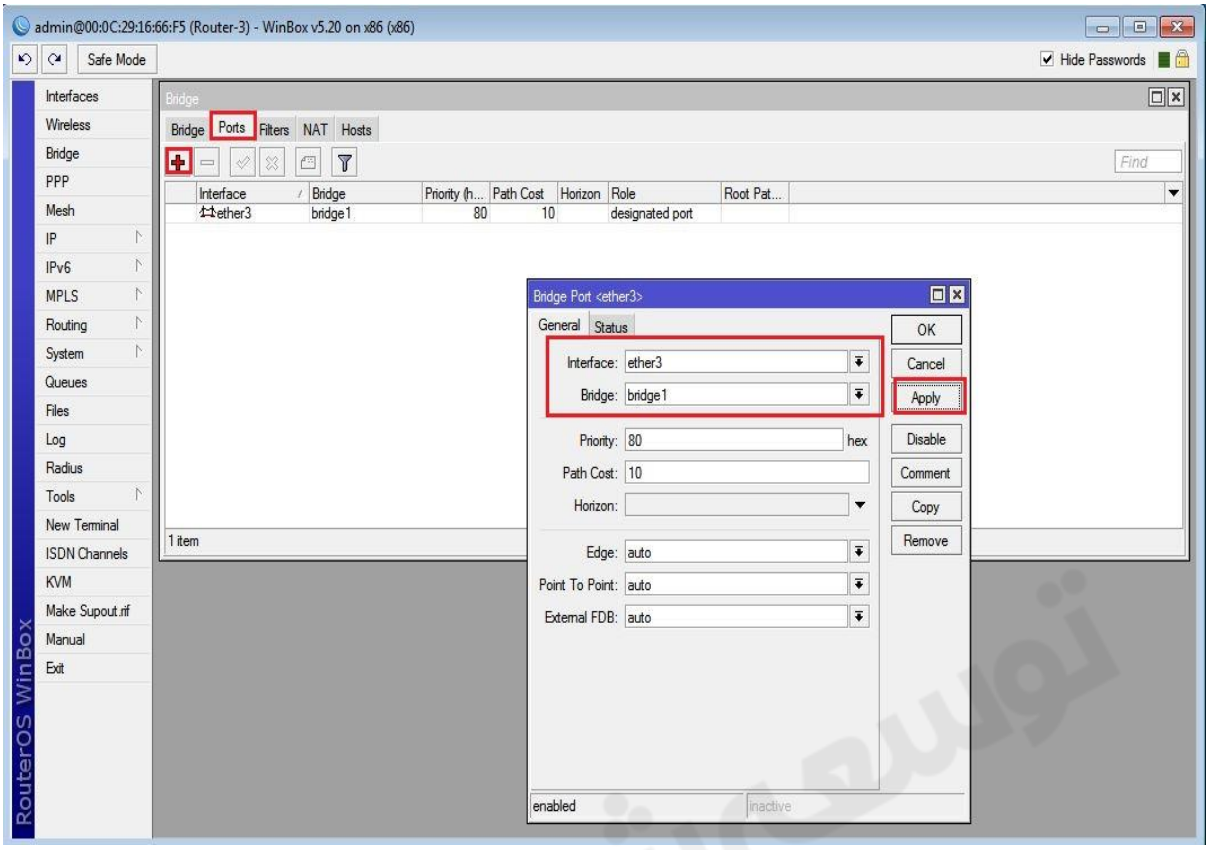


ایجاد کارت شبکه مجازی Bridge در روتر R3 :

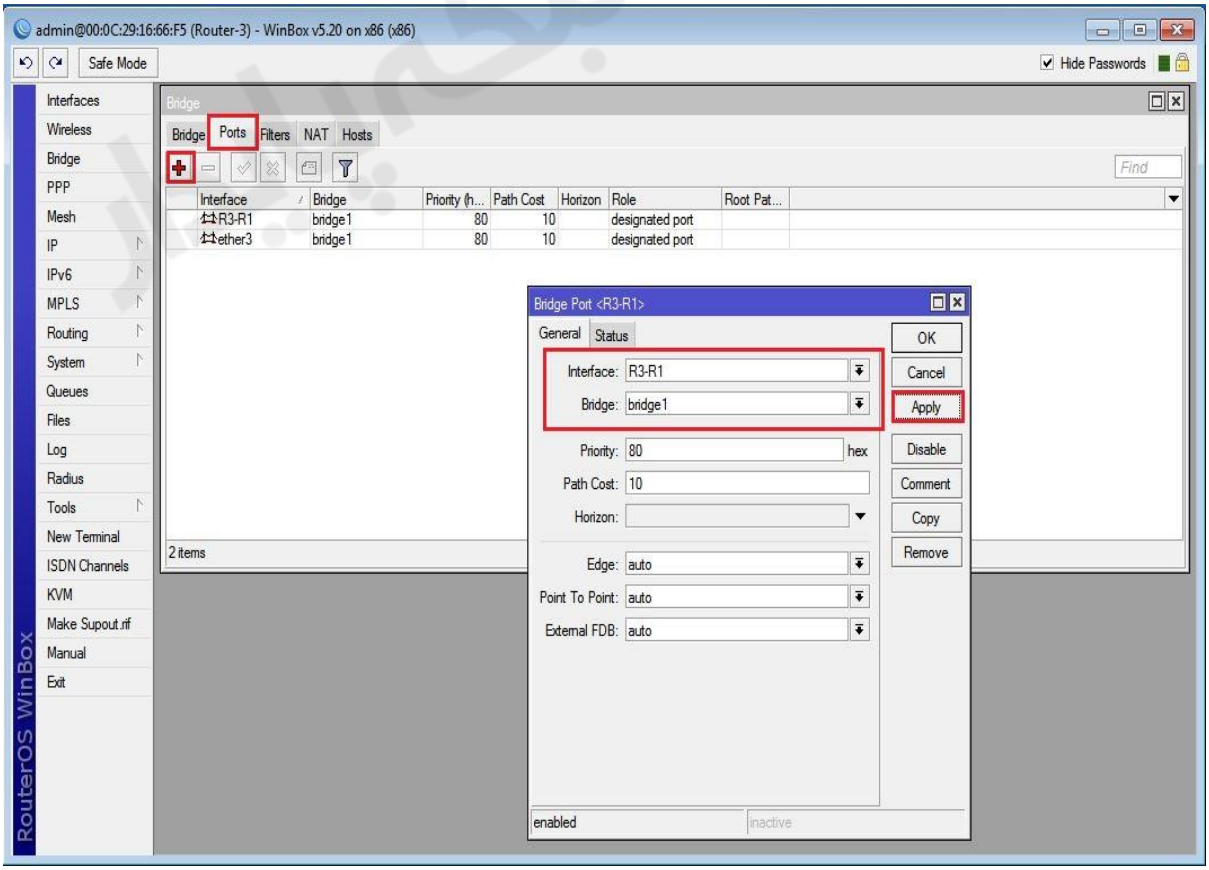
برای این کار از منوی اصلی Bridge را انتخاب و از پنجره باز شده از تب Bridge بر روی Add کلیک می کنیم.



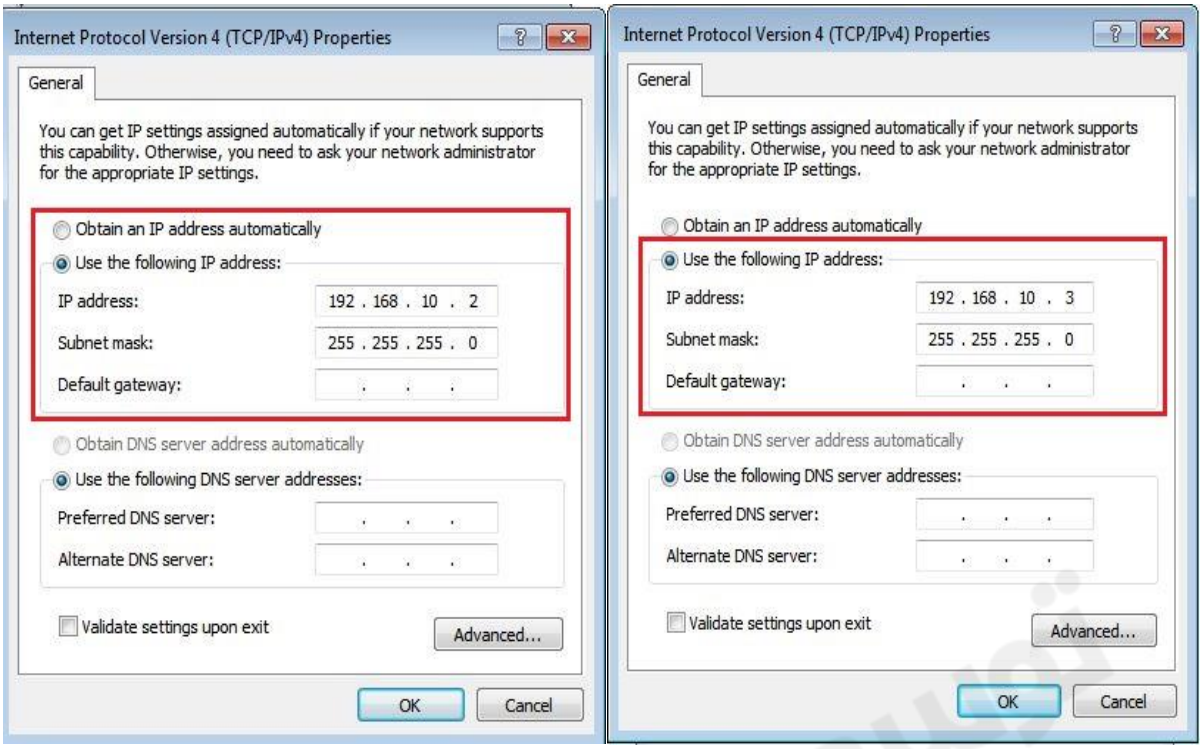
ارتباط کارت شبکه داخلی روتر با کارت شبکه مجازی **Bridge** در روتر **R3** :



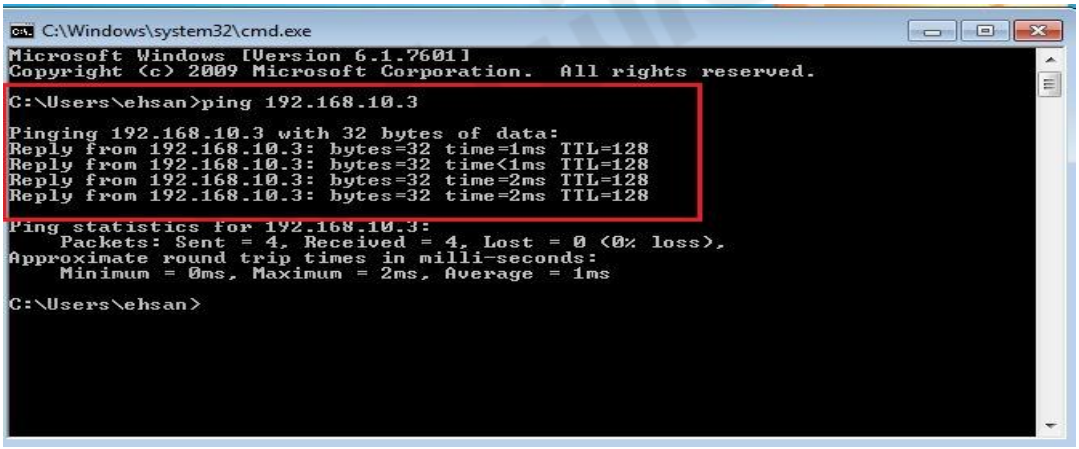
ارتباط کارت شبکه مجازی **EOIP** با کارت شبکه مجازی **Bridge** در روتر **R3** :

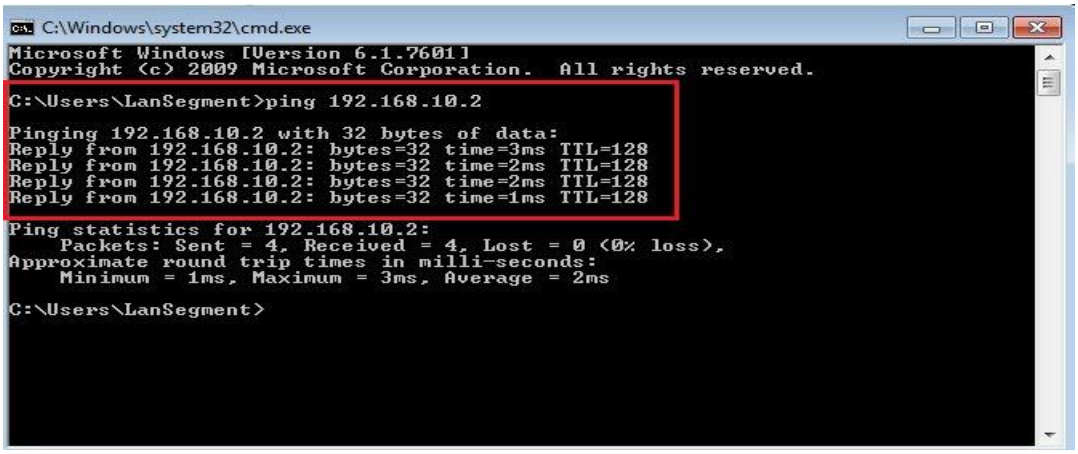


تنظیمات کلاینت :



تست برقراری ارتباط بین کلاینت ها :



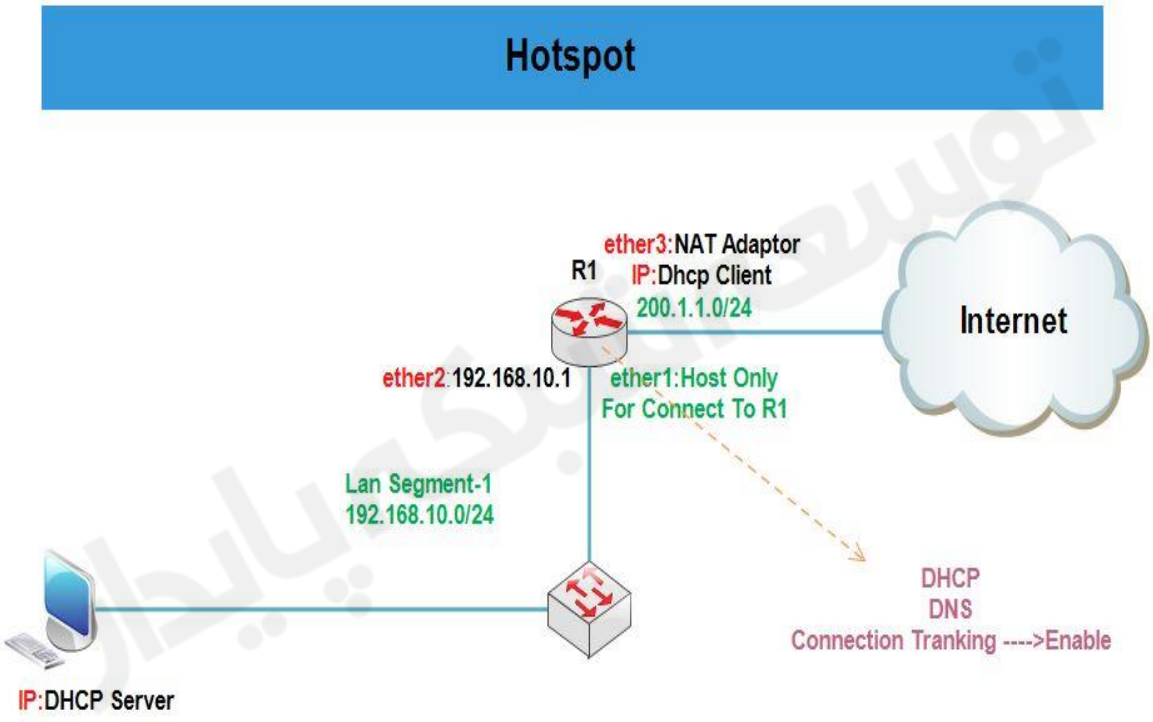


فصل هفدهم : Mikrotik Hotspot Gateway

Hotspot یک نقطه دسترسی عمومی است برای کامپیوترهایی که بصورت کابلی یا بی سیم به شبکه متصل شده اند.در واقع **Hotspot** امکانی برای اعتبار سنجی (**Authentication**) کاربران جهت اتصال به شبکه به وجود می آورد.

ویژگی خاص **Hotspot** نیاز نداشتن به نرم افزار و یا تنظیمات خاص سمت کاربر می باشد که باعث سهولت بیشتر برای کاربران معمولی می شود ، فقط کافی است در سمت کاربر یک مرورگر وجود داشته باشد.با باز کردن مرورگر درخواستی مبتنی ارسال صفحه وب به **Hotspot** فرستاده می شود و **Hotspot** تمامی درخواست ها را به صفحه پیش فرض **Rediret** می کند(صفحه پیش فرض قابل تغییر است).

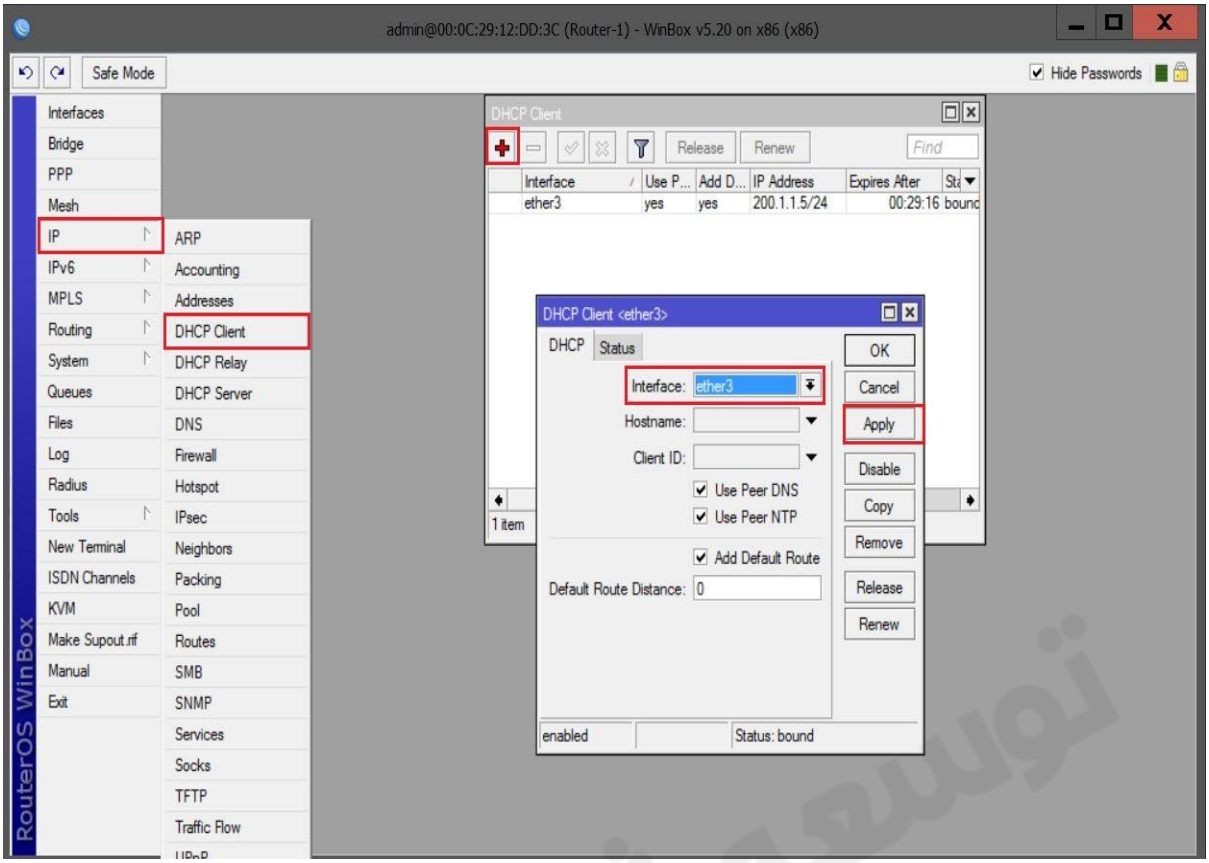
سناریو ۱ : نصب و راه اندازی سرویس **Hotspot** برروی میکروتیک

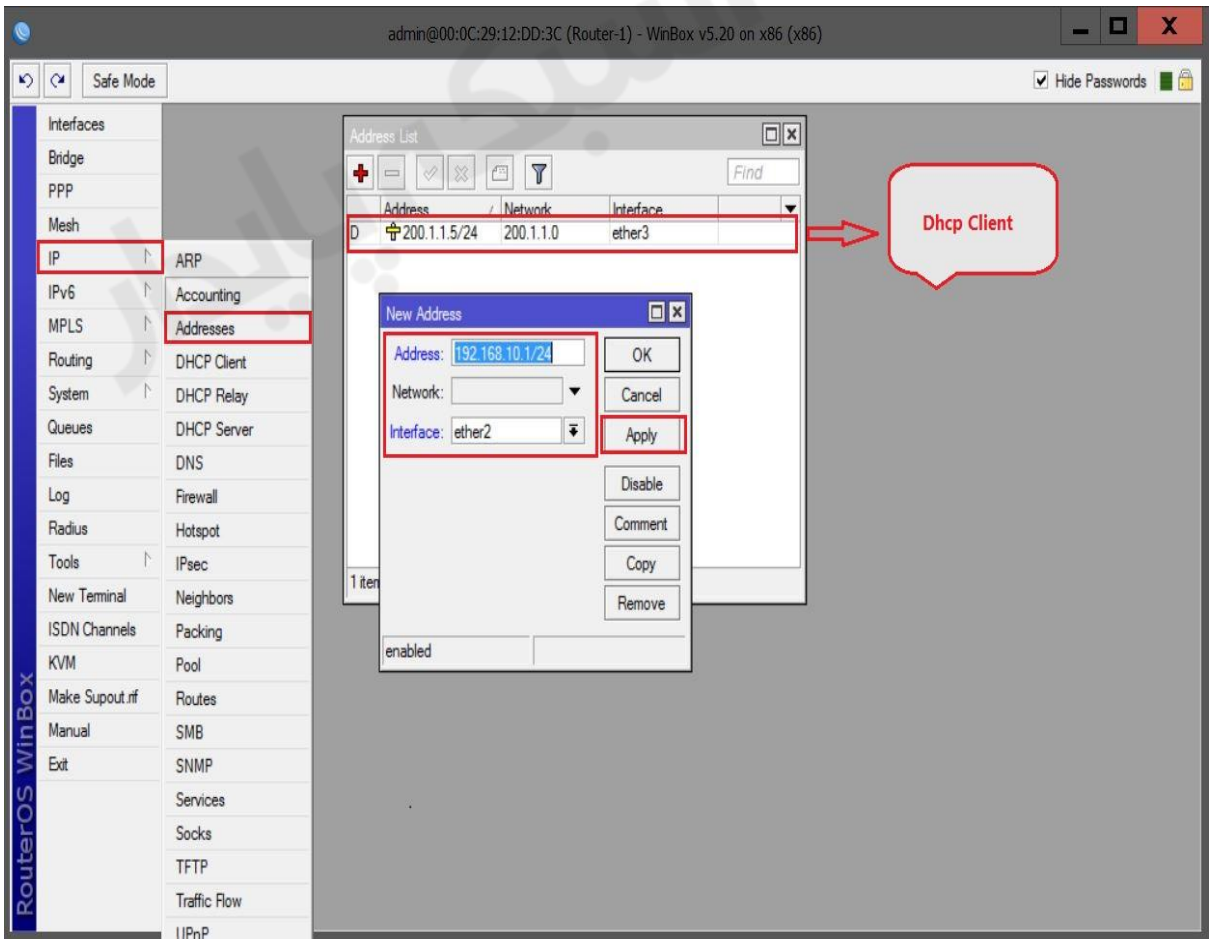


هدف این سناریو این است که سرویس **Hotspot** را بروی روتر میکروتیک راه اندازی کنیم به صورتی که کلاینت ها از **DHCP** سرور **IP** دریافت کنند و در صورتی بتوانند به اینترنت دسترسی داشته باشند که نام کاربری و رمز عبوری که در **Hotspot** تعریف شده است را داشته باشند.

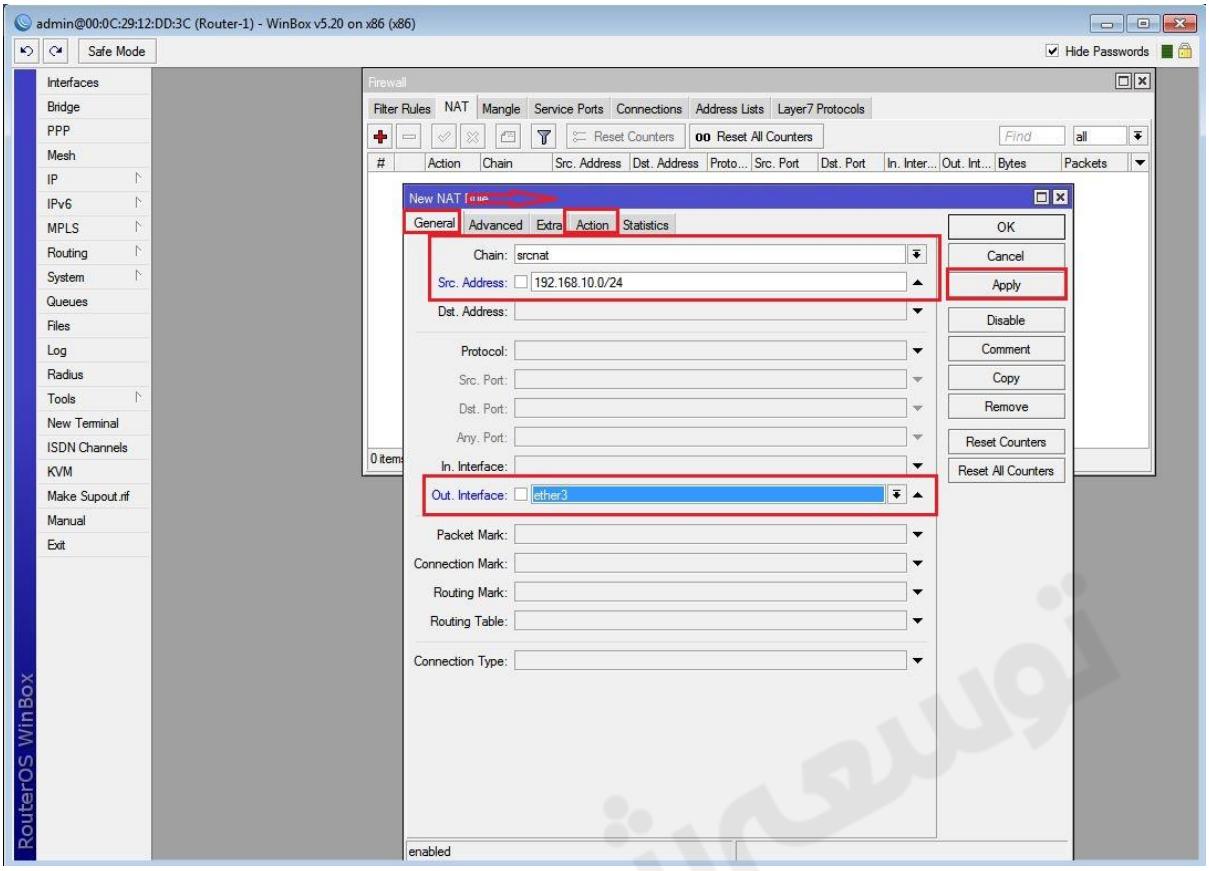
انتساب **IP** به کارت های شبکه روتر **R1** :

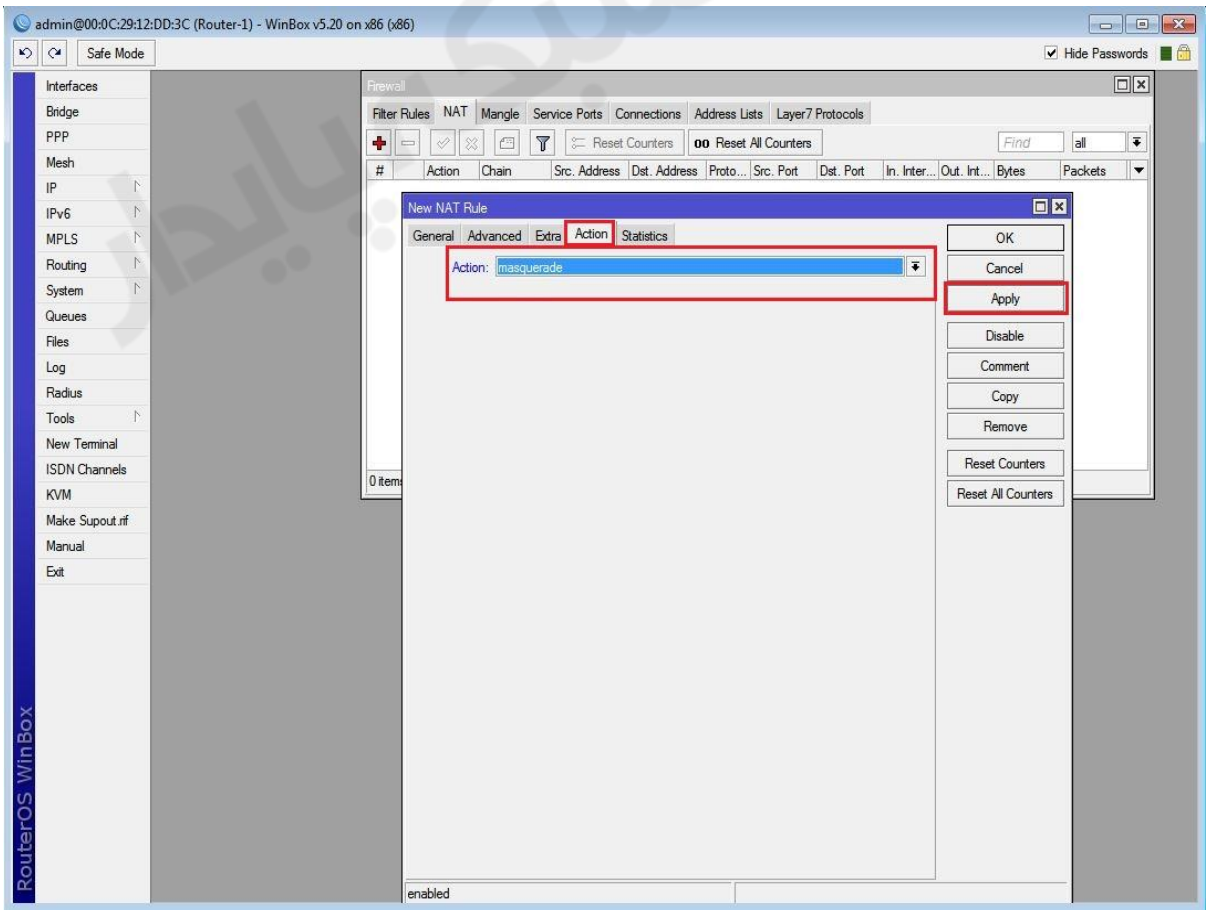
همان طور که در سناریو مشخص کردیم **Ether3** باید از **Dhcp Client** (**Vmware**) آدرس**IP** دریافت کند.برای این کار از منوی اصلی گزینه **IP** و از زیر منوی باز شده **Dhcp Client** را انتخاب میکنیم.در پنجره باز شده بر روی **Add** کلیک و از تب **Dhcp** اینترفیس مورد نظر را انتخاب و **ok** را میزنیم.


admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
RouterOS WinBox
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Socks
TFTP
Traffic Flow
DHCP Client
Release
Renew
Find
Interface
Use P...
Add D...
IP Address
Expires After
ether3
yes
yes
200.1.1.5/24
00:29:16
1 item
DHCP Client <ether3>
DHCP
Status
Interface: ether3
Hostname:
Client ID:
Use Peer DNS
Use Peer NTP
Add Default Route
Default Route Distance: 0
OK
Cancel
Apply
Disable
Copy
Remove
Release
Renew
enabled
Status: bound


admin@00:0C:29:12:DD:3C (Router-1) - WinBox v5.20 on x86 (x86)
Safe Mode
Hide Passwords
RouterOS WinBox
Interfaces
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
Exit
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Socks
TFTP
Traffic Flow
Address List
Find
Address
Network
Interface
D
200.1.1.5/24
200.1.1.0
ether3
Dhcp Client
New Address
Address: 192.168.10.1/24
Network:
Interface: ether2
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled

ایجاد Nat برای دسترسی کلاینت ها به اینترنت :

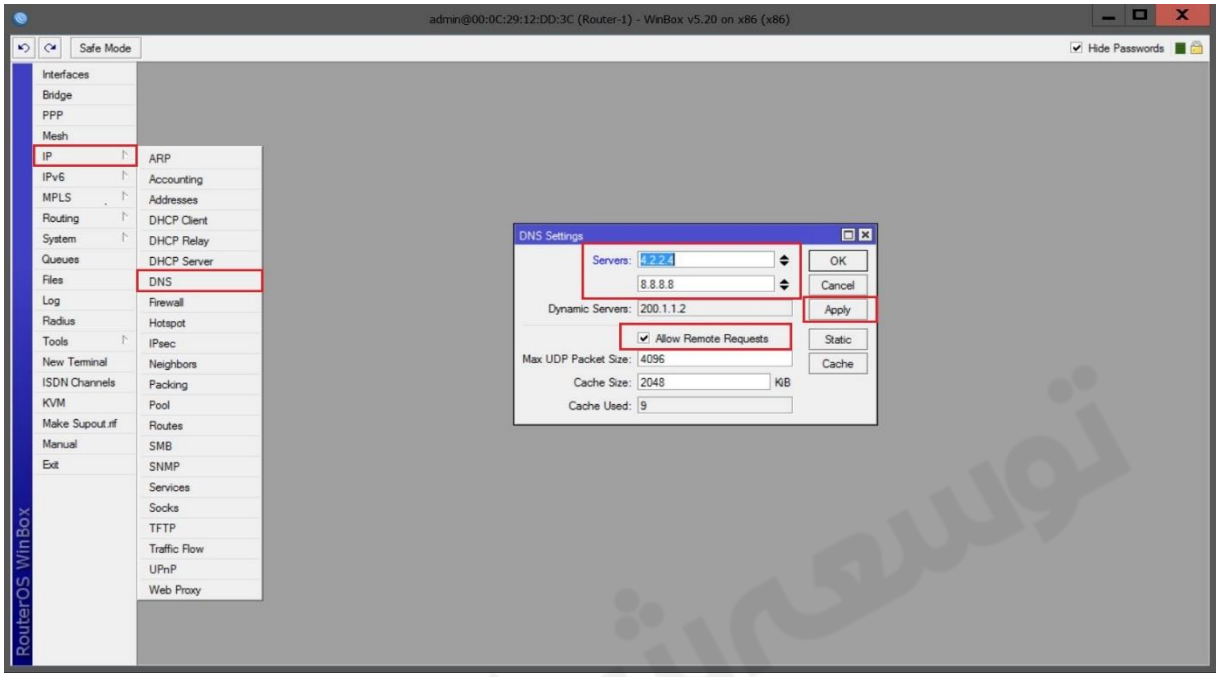




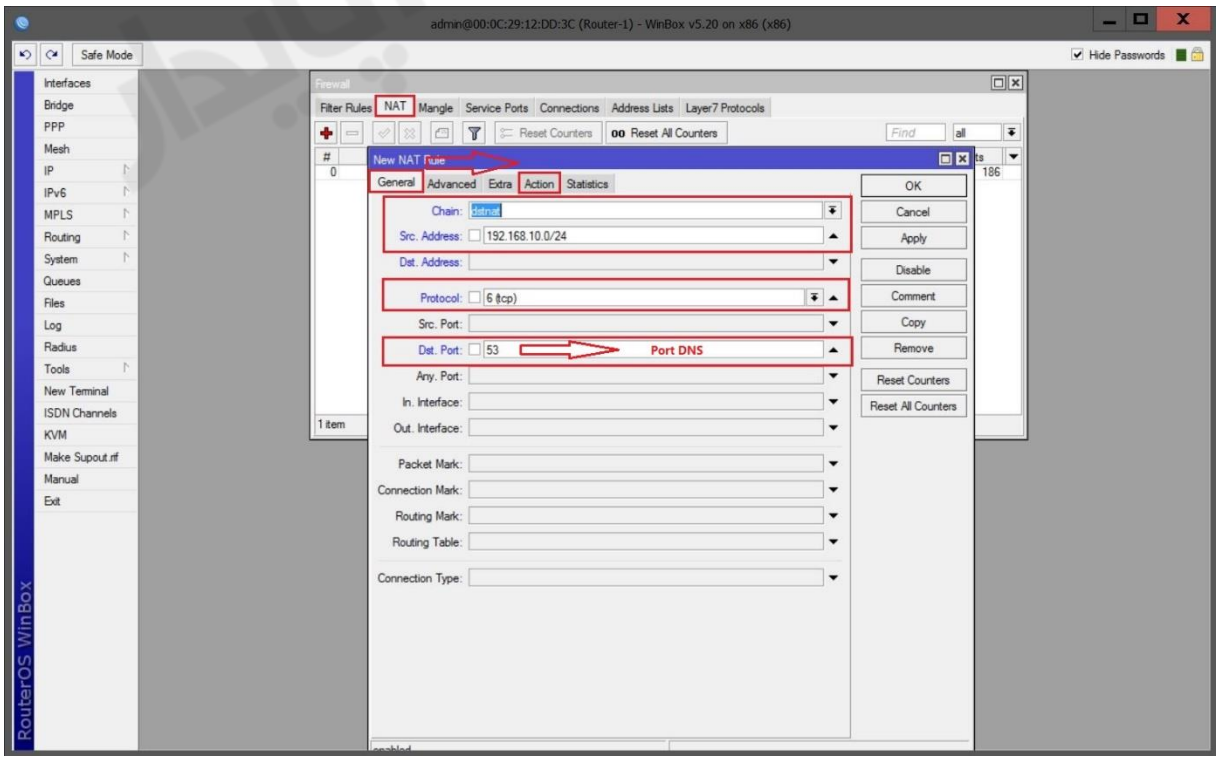
نصب و راه اندازی DNS :

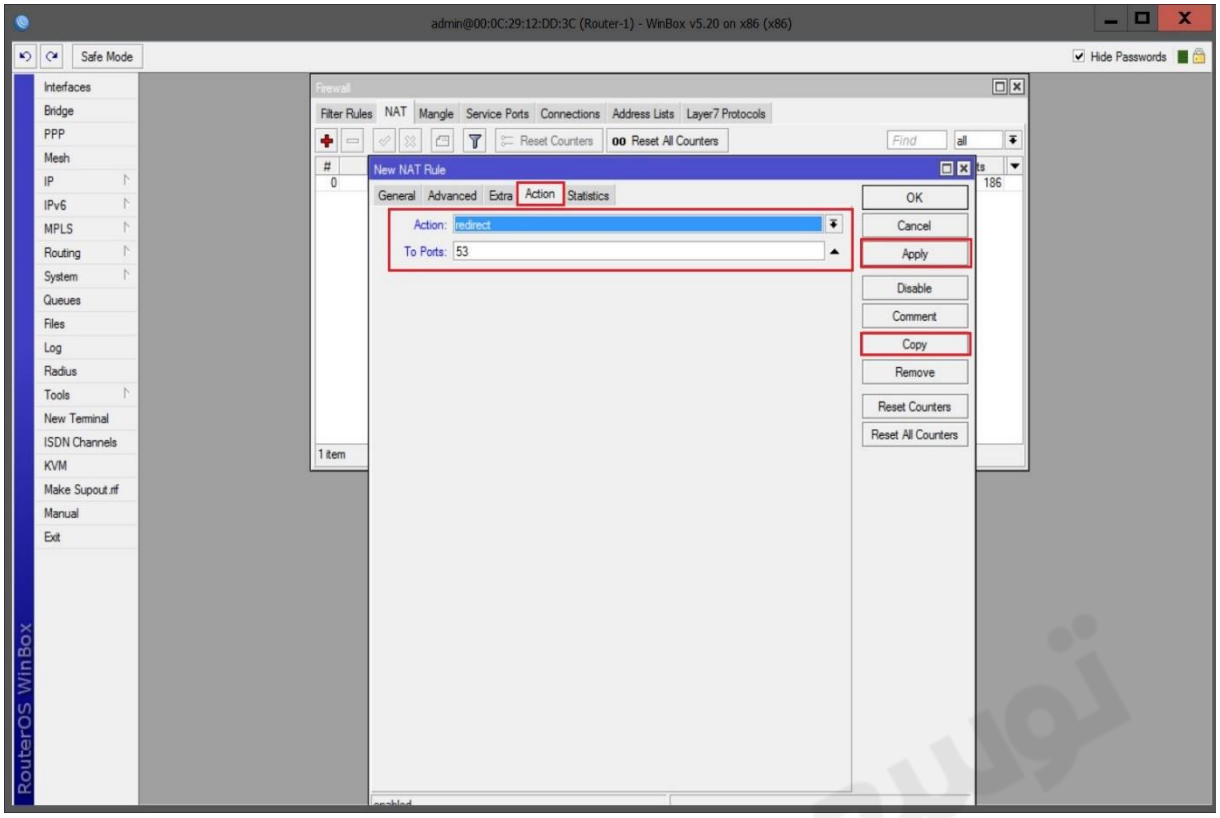
برای این کار از مسیر اصلی گزینه IP را انتخاب و از زیر منوی باز شده بر روی DNS کلیک می کنیم.از پنجره باز شده تنظیمات را طبق عکس زیر انجام می دهیم.

به این نکته توجه داشته باشد در صورتی که تیک گزینه Allow Remote Request فعال شود روتر شما به عنوان DNS سرور شناخته شده و ممکن است در معرض حملات و آسیب های DNSای از طریق اینترنت قرار گیرد.

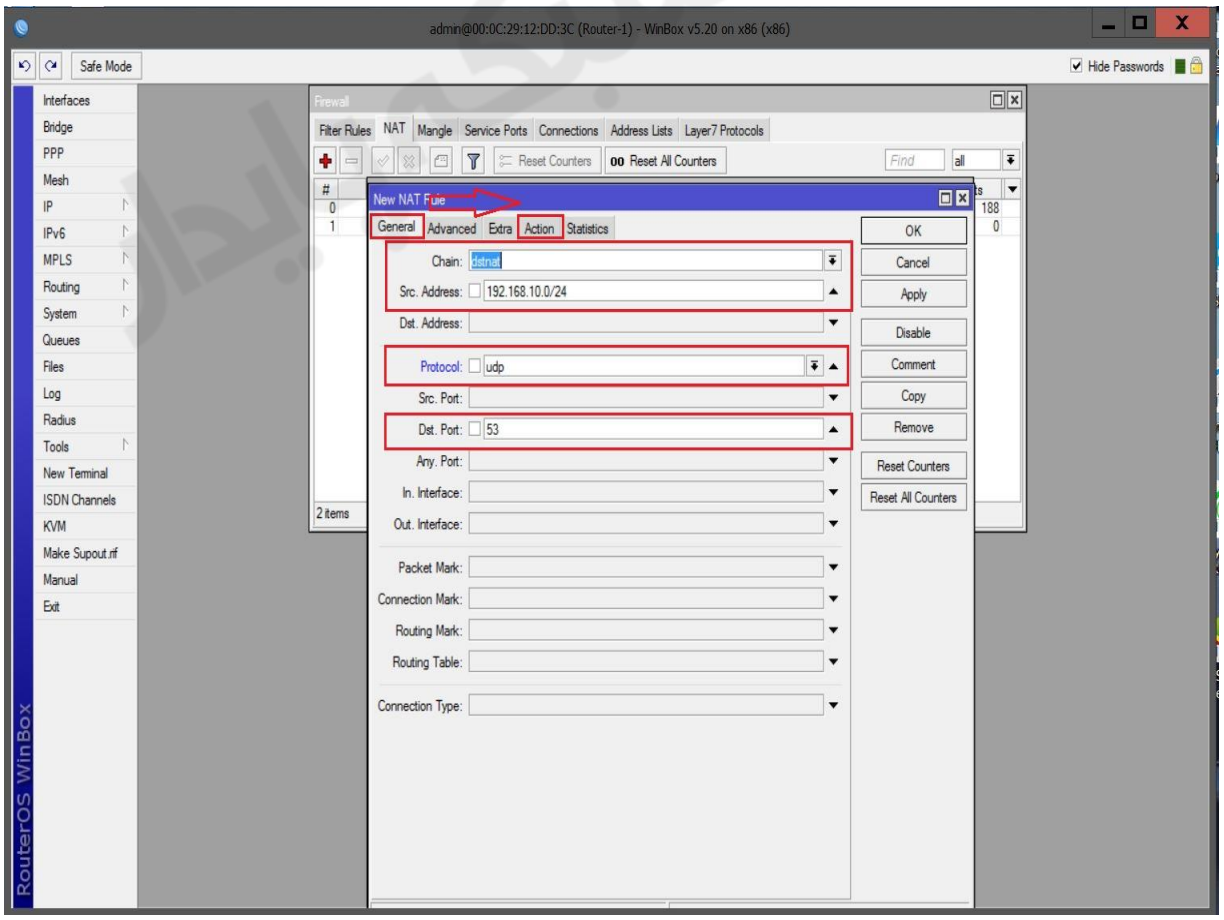


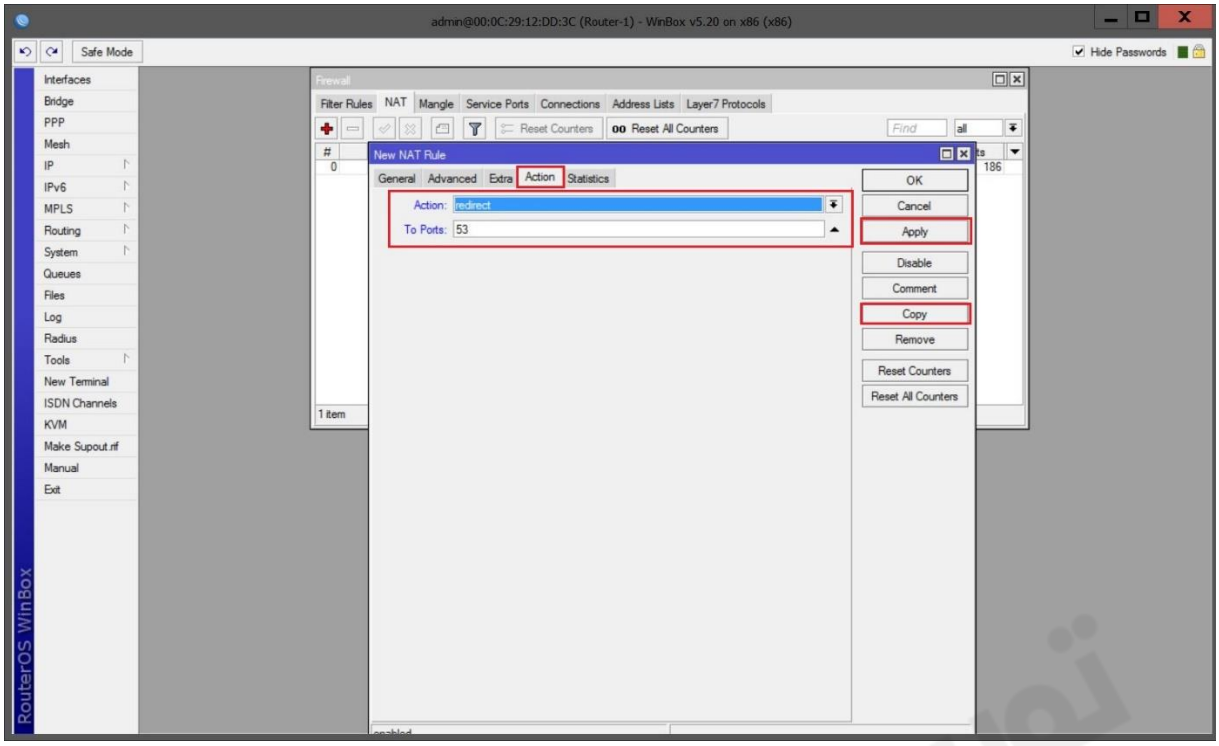
با این تنظیمات پروسه Resolve(تبدیل اسم به IP و یا IP به اسم) انجام میشود اما در صورتی که کاربر به هر علتی IP آدرس DNS را بصورت دستی و اشتباه وارد کند پروسه Resolve اتفاق نمی افتد برای جلوگیری از این مشکل به مسیر زیر رفته و کارها را طبق تنظیماتی که در عکس های زیر مشاهده می کنید انجام میدهیم :





***نکته : چون DNS هم از TCP و هم ازUDP پشتیبانی می کند به همین د لیل هر دو آن را تعریف می کنیم و 53 نیز پورت پیش فرض DNS می باشد.**



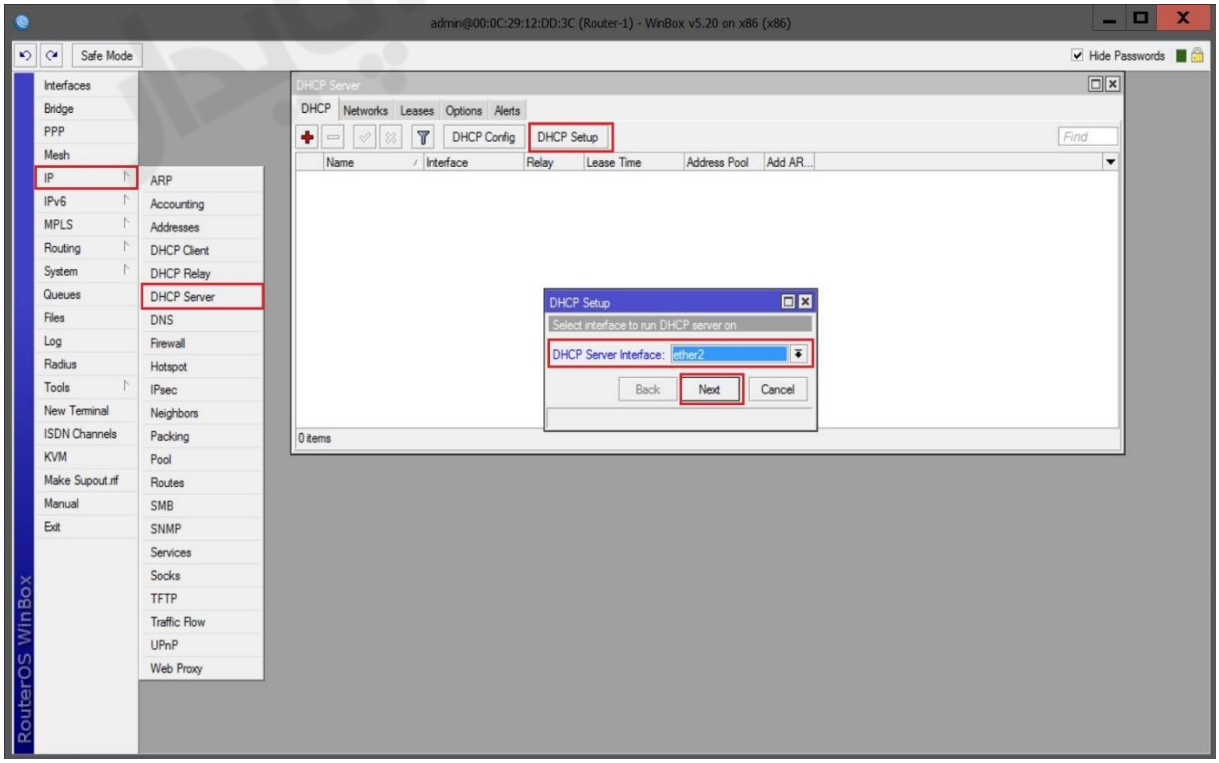


به این ترتیب با این تنظیمات درخواست های **DNS** ای بر روی پورت **DNS** میکروتیک **Redirect** می شود.حال اگر کاربر به هر علتی در تنظیمات **DNS** سیستم خود هر آدرسی را وارد کند حتی اگر آدرس وارد شده اشتباه بود یا یک **IP** آدرس نامتعارف بود ، چون تمامی درخواست های **DNS** ای بر روی پورت **DNS** میکروتیک ارسال می شوند ، پروسه **Resolve** درخواست ها با موفقیت انجام می پذیرند.

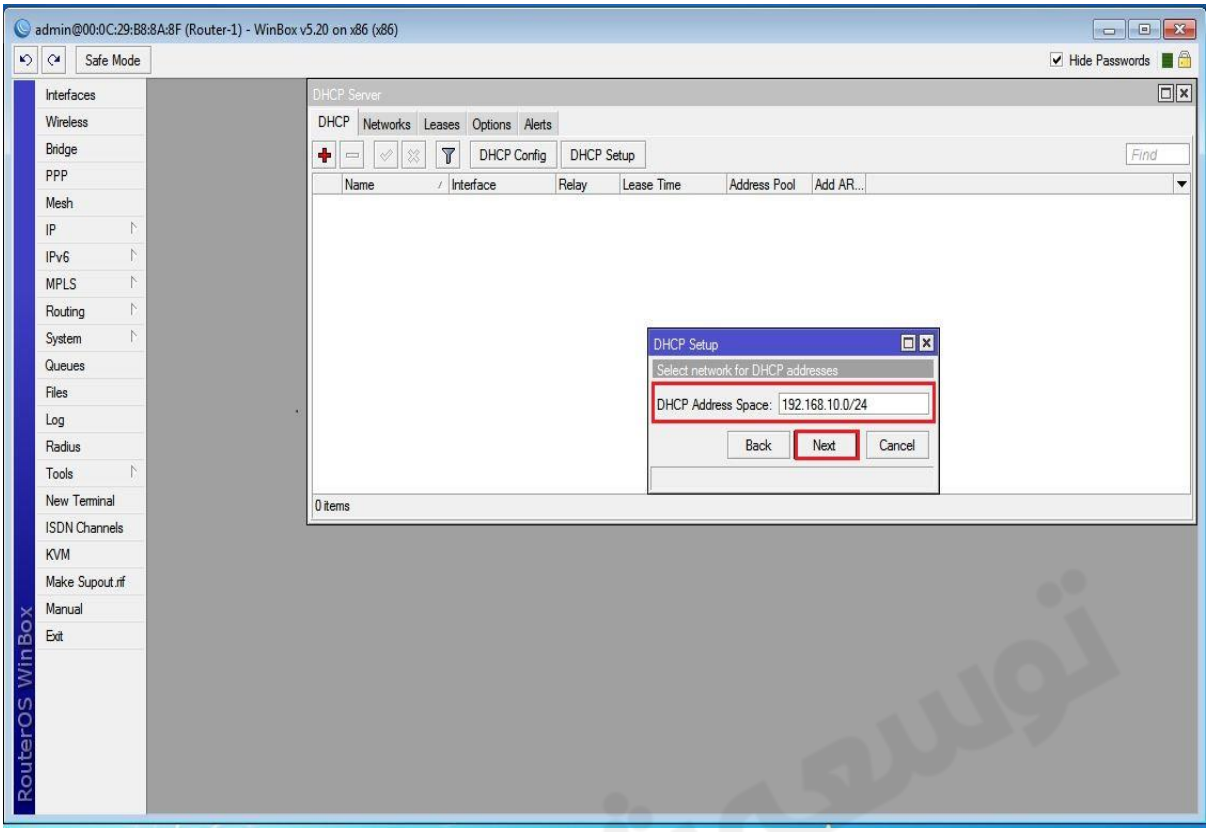
نصب و راه اندازی DHCP سرور :

برای این کار از منوی اصلی گزینه IP را انتخاب و از زیر منوی باز شده DHCP Server را انتخاب می کنیم.از پنجره باز شده و از بخش DHCP گزینه DHCP Setup را انتخاب می کنیم .

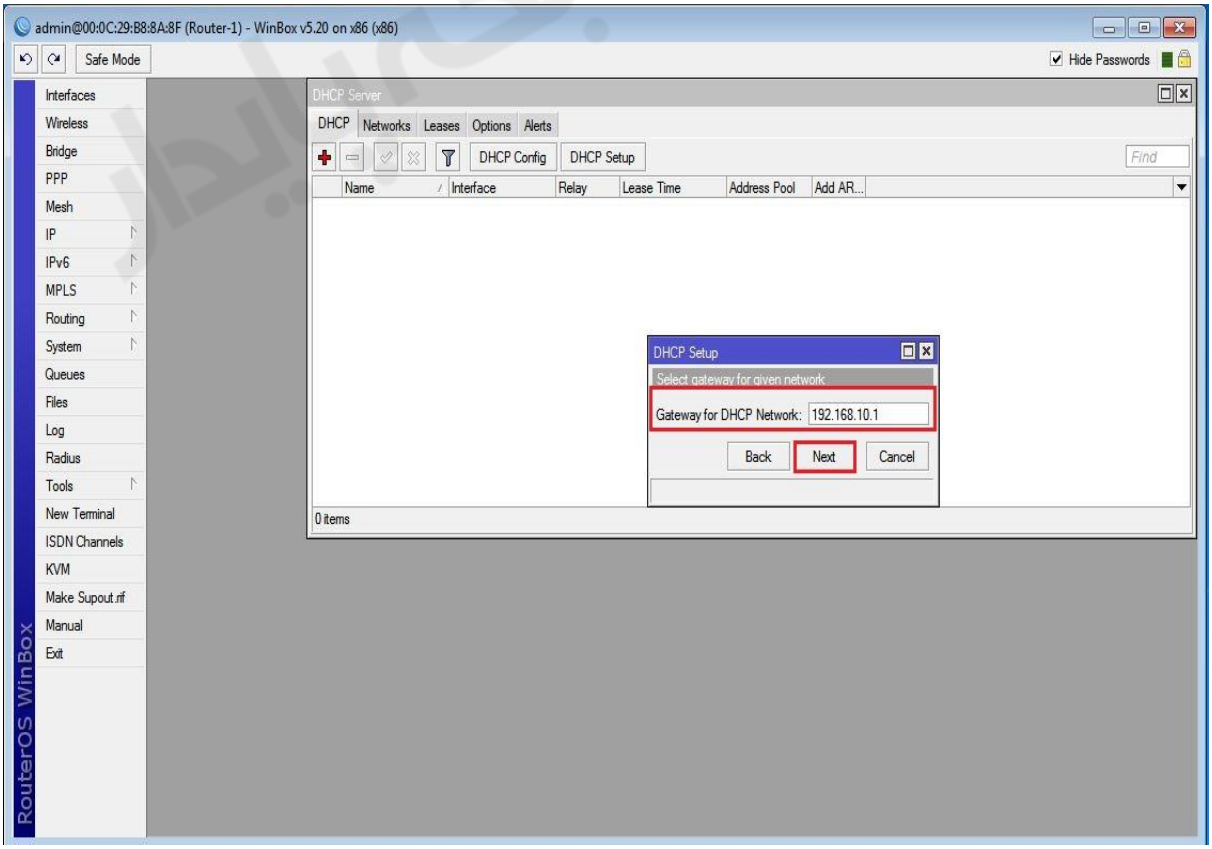
در این مرحله باید کارت شبکه مورد نظر که می خواهیم از طریق آن سرویس DHCP به کلاینت ها IP دهد را انتخاب کنیم.



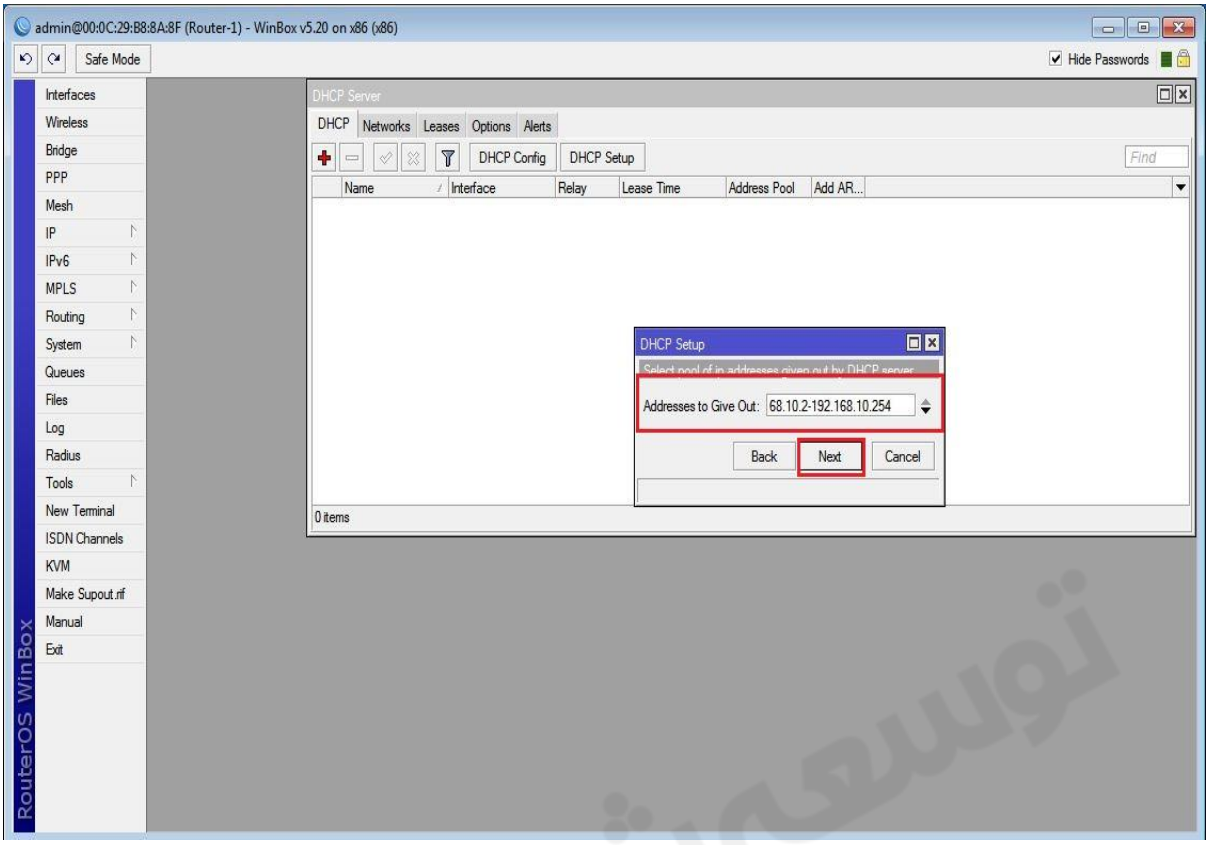
در این مرحله محدوده **IP** مربوط به شبکه ایی که می خواهیم **DHCP** در آن فعال باشد را انتخاب می کنیم.



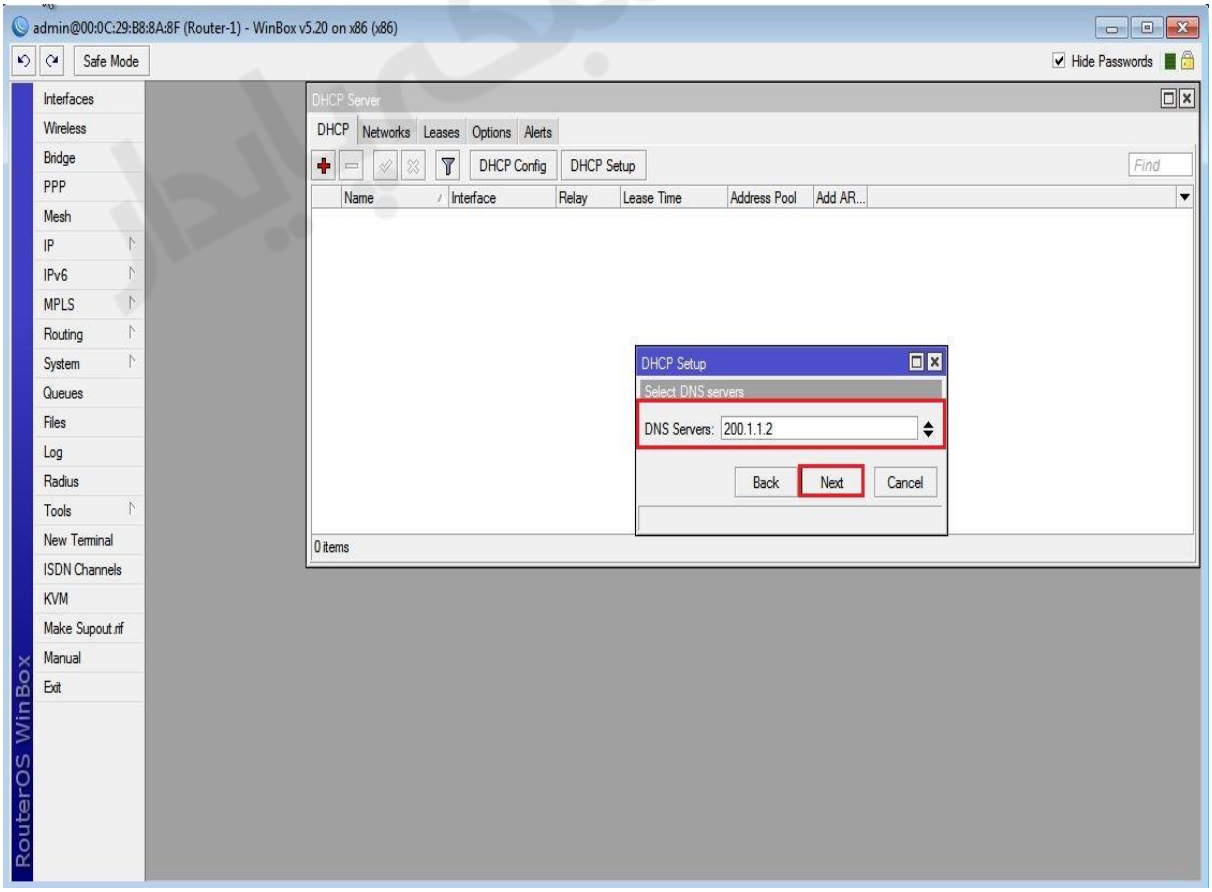
در این قسمت **Gateway** (دروازه) مورد نظر که می خواهیم برای کلاینت ها را **Set** کنیم را وارد میکنیم.این **Option** در حقیقت **IP** مربوط به روتر در شبکه می باشد.



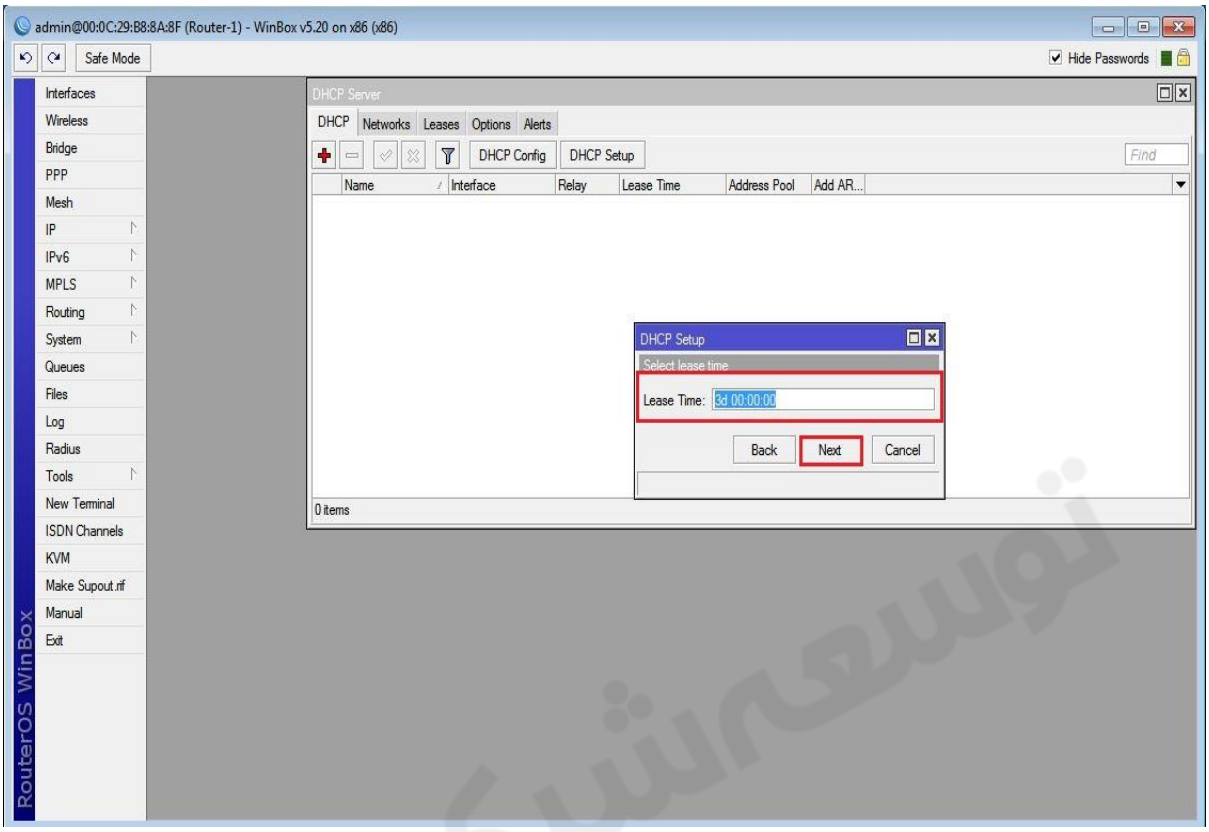
در این قسمت **Pool** یا محدوده ایی از **IP**ها را که می خواهیم **DHCP** برای کلاینت ها شبکه در نظر بگیرد را انتخاب می کنیم.



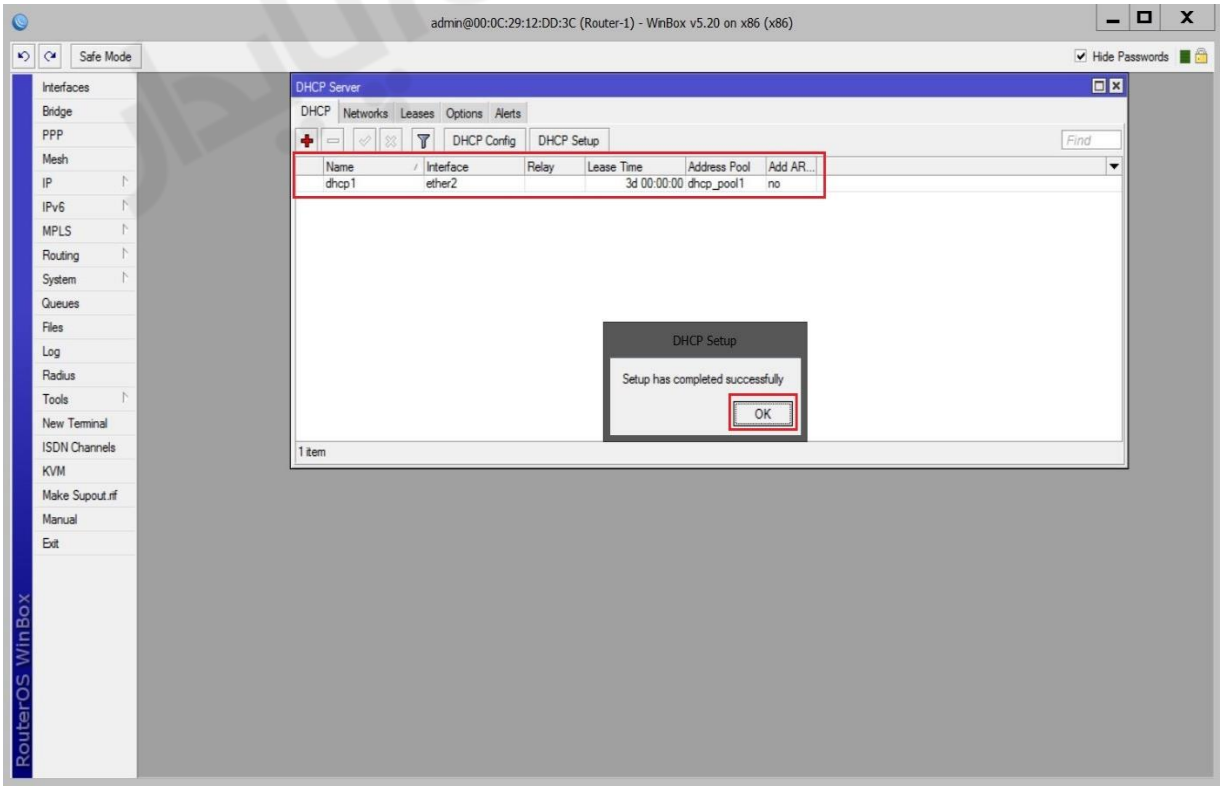
آدرس مربوط به **DNS** سرور موجود در شبکه را وارد میکنیم.



در این قسمت مدت زمانی که IP به کلاینت تخصیص داده می شود را انتخاب می کنیم.بصورت پیش فرض ۳ روز این IP به کلاینت اختصاص داده می شود و بعد از این مدت IP از کلاینت گرفته می شود و چنانچه درخواست برای IP از سیستم دیگری زودتر به DHCP Server برسد این IP به کلاینت دیگر اختصاص داده می شود.



و در نهایت پس از این مرحله DHCP راه اندازی شده و شما با پیغام زیر رو به رو خواهید شد :



NTP (Network Time Protocol) :

تنظیمات تاریخ و ساعت و آپدیت بودن آن بر روی روترها و سوییچ های سخت افزاری ، خصوصا در مواقعی که از میکروتیک فایل پشتیبان تهیه می شود و یا Hotspot راه اندازی می شود و... بسیار حائز اهمیت است.اگر تارخ و زمان را بصورت دستی تغییر دهید ، با خاموش شدن روتر تغییرات ایجاد شده به حالت قبل باز می گردد.

برای به روز بودن تنظیمات ساعت و تاریخ می توان به سرورهایی متصل شد که بصورت خودکار ساعت و تاریخ را تنظیم می کنند به این سرورها NTP Server گفته می شود و برای تنظیم زمان از پروتکل NTP استفاده می کنند.NTP مخفف Network Time Protocol است و پروتکلی برای تنظیم زمان سرورها و کلاینت ها با ساعت جهانی می باشد.

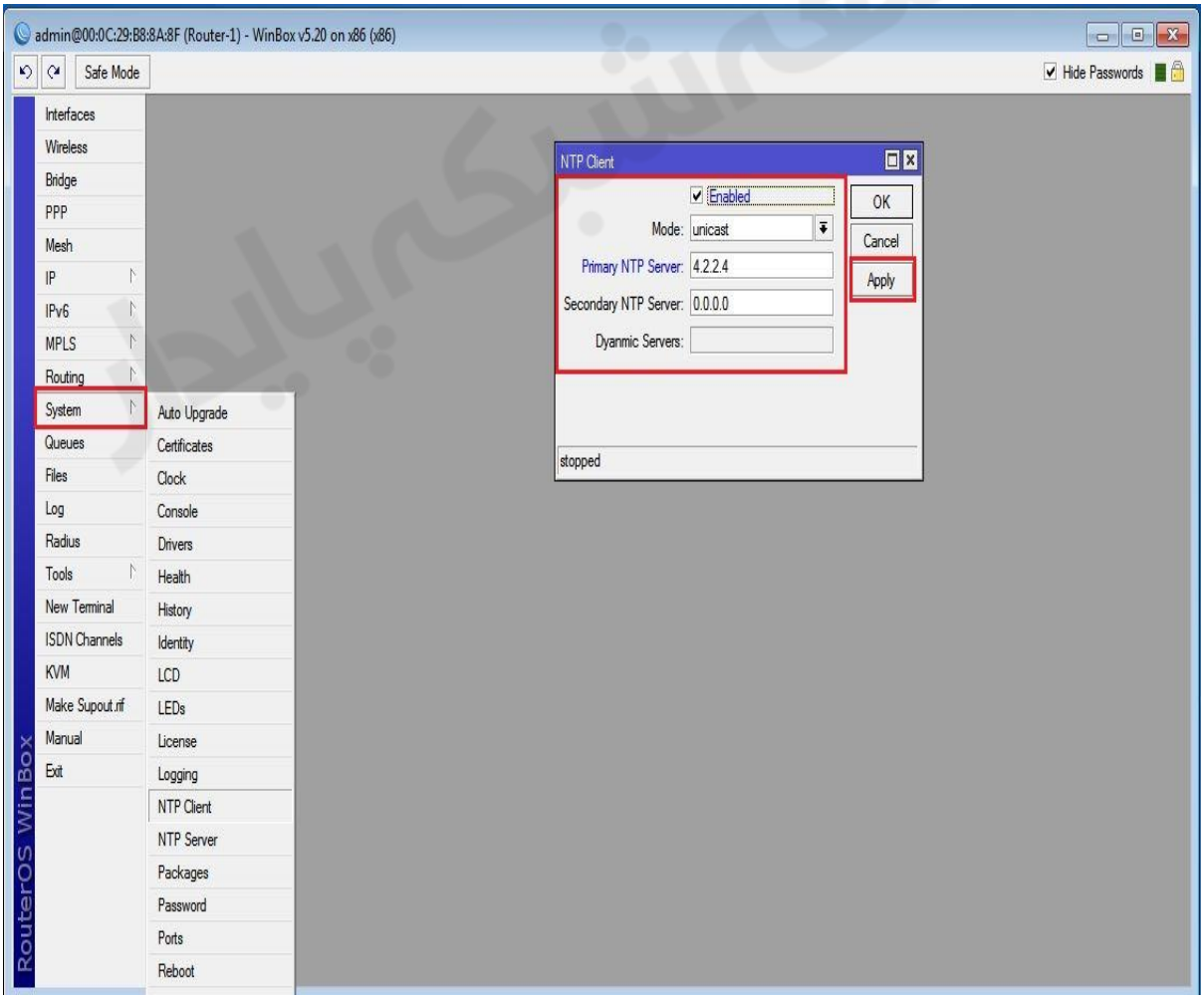
در سیستم عامل میکروتیک می توان NTP را به صورت کلاینت (NTP Client) یا سرور (NTP Server) راه اندازی نمود.NTP سرور با پروتکل UDP و با شماره پورت 123 کار می کند.

تنظیم NTP Client :

برای اینکار از منوی اصلی بروروی System رفته و از زیرمنوی باز شده NTP Client را انتخاب می کنیم.در پنجره NTP Client تیک Enable را فعال می کنیم و در قسمت Mode گزینه Unicast را انتخاب می کنیم.

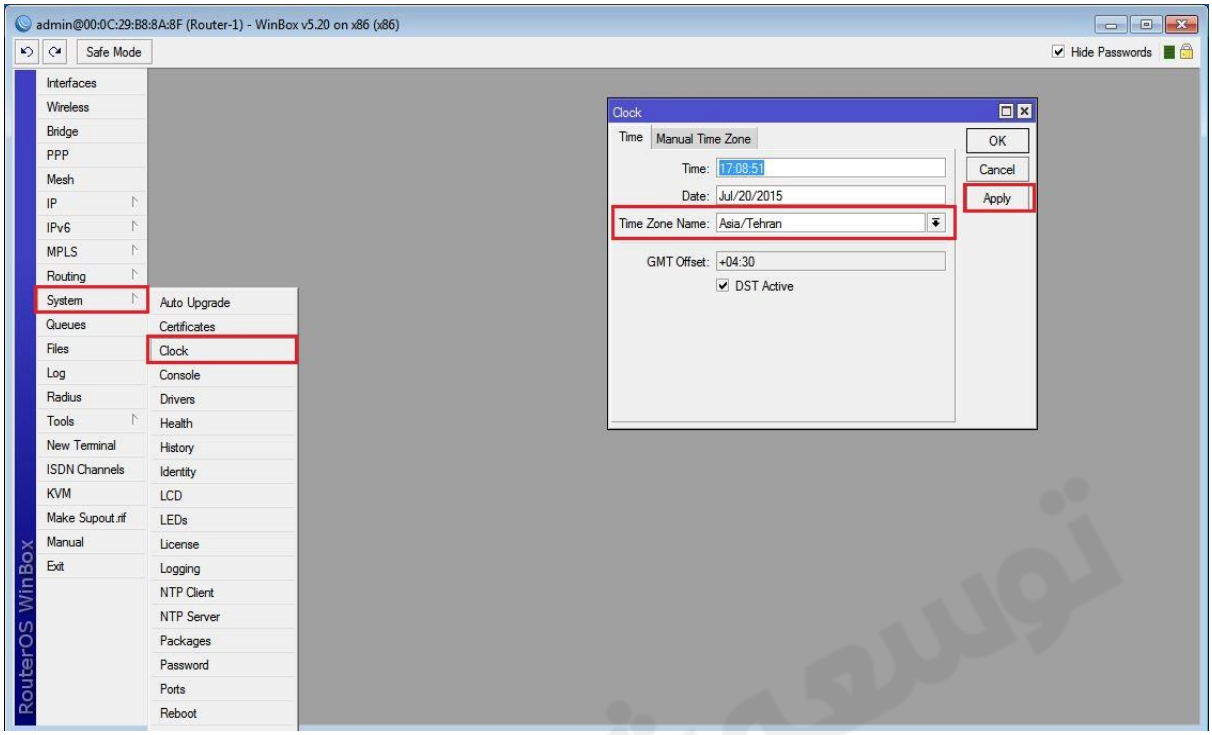
Unicast : در این مد NTP Client فقط با سرورهایی کار می کند که در دو فیلد Primary NTP Server و Secondary NTP Server درج شده است ، پس از متصل شدن به سرور با آنها سینک می گردد.

Primary NTP Server : در این فیلد نام و یا IP یکی از NTP Server هایی که وجود دارد را وارد می کنیم.



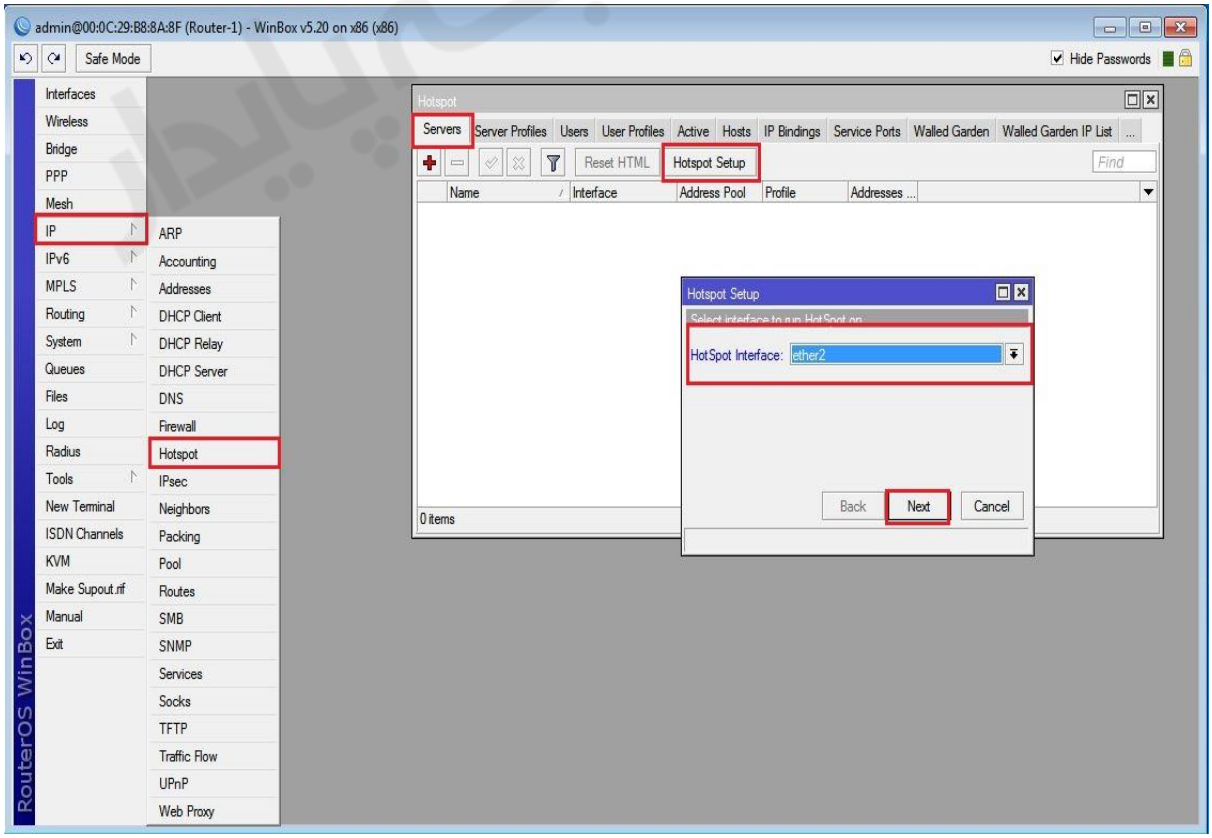
تنظیم ساعت و تاریخ سیستم :

برای اینکار از منوی اصلی برووی System رفته و از زیرمنوی باز شده Clock را انتخاب میکنیم و از پنجره باز شده Time Zone Name را برابر Asia/Tehran قرار می دهیم.

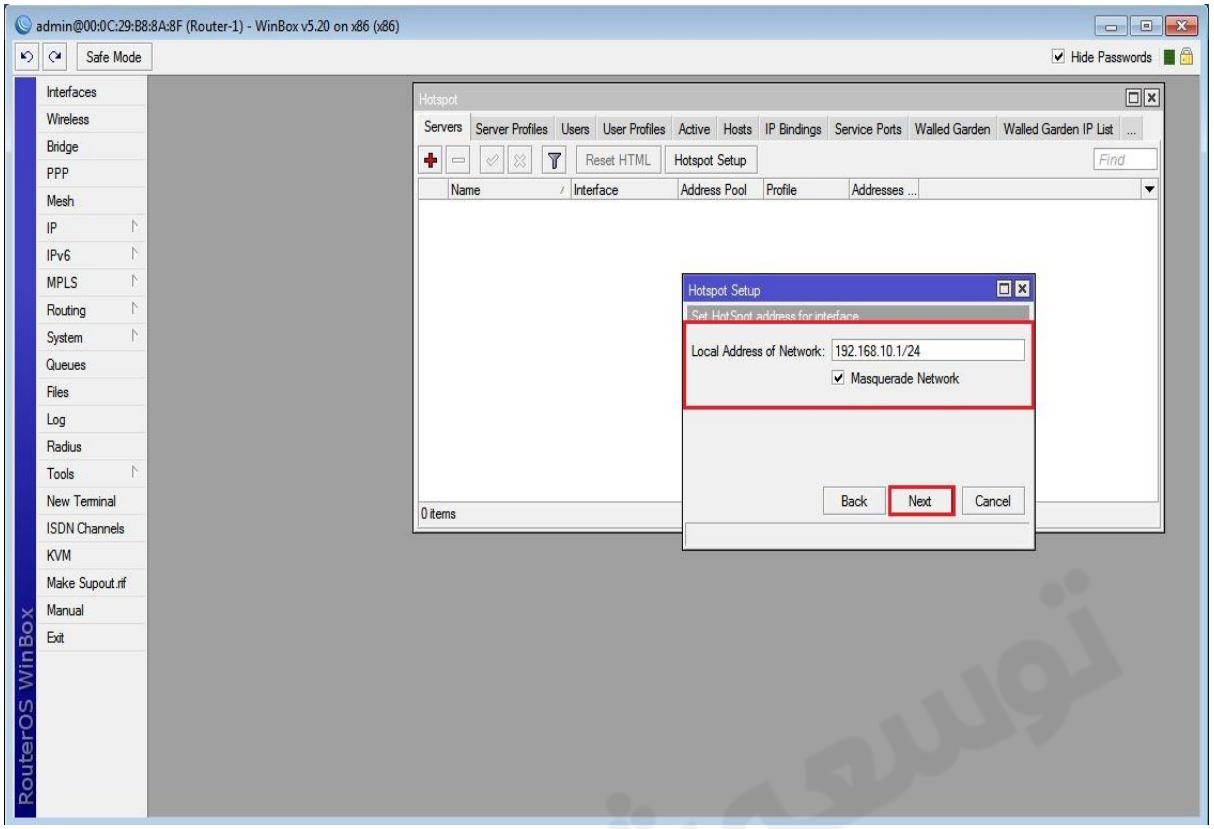


نصب سرویس Hotspot :

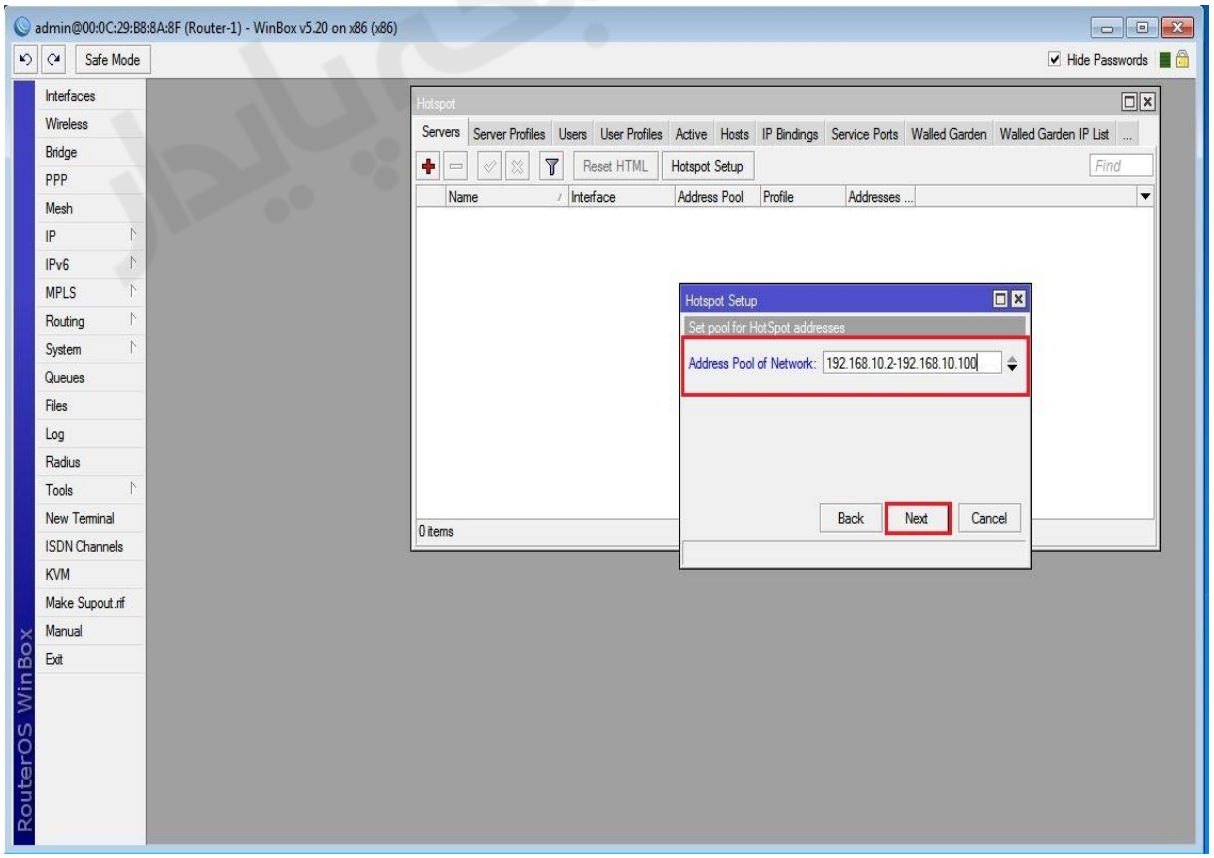
برای نصب این سرویس از منوی اصلی برروی IP رفته و از زیرمنوی باز شده Hotspot را انتخاب می کنیم.از پنجره باز شده به تب Servers رفته و Hotspot Setup را انتخاب می کنیم.در این مرحله اینترفیسی که Hotspot برروی آن باید سرویس دهی کند را انتخاب میکنیم.

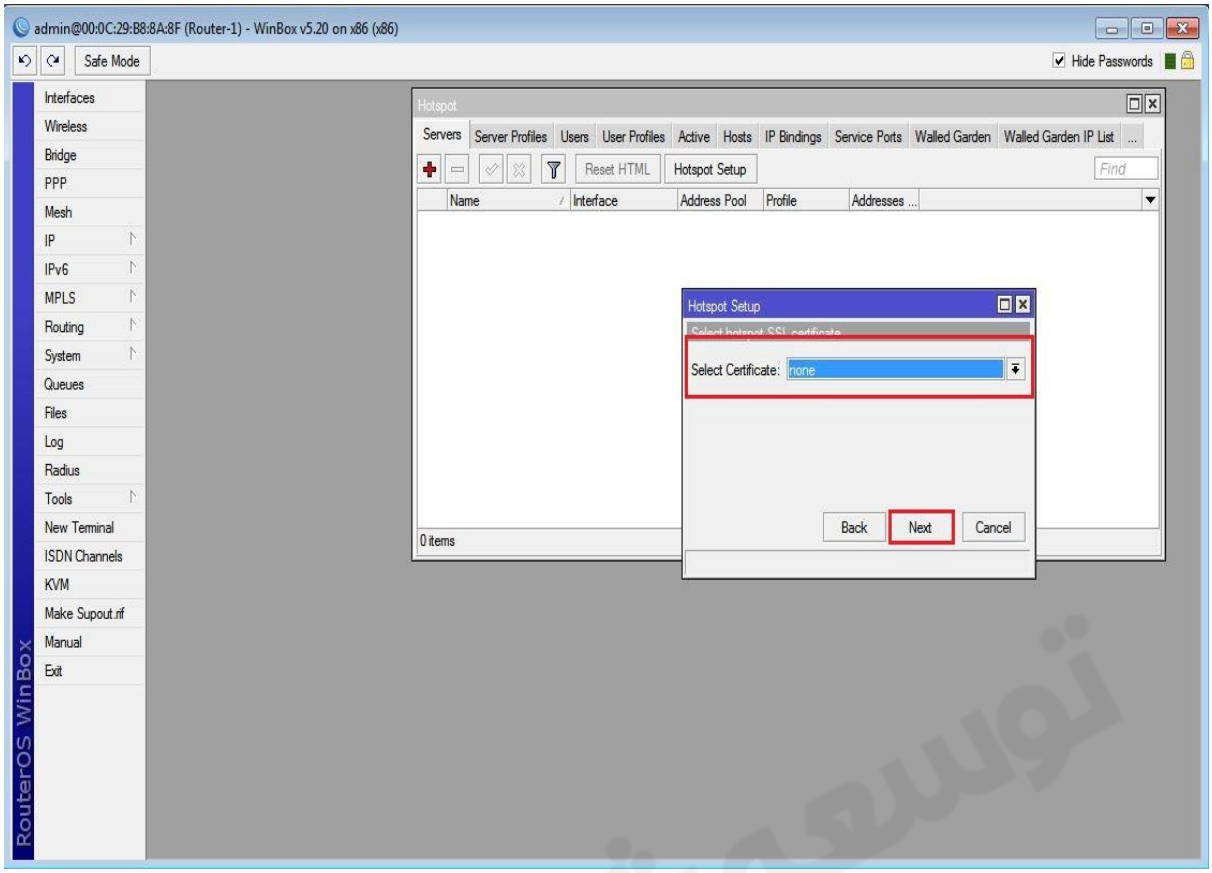


در این مرحله رنج آدرسی که برای سرویس **Hotspot** استفاده خواهد شد نمایش داده می شود.

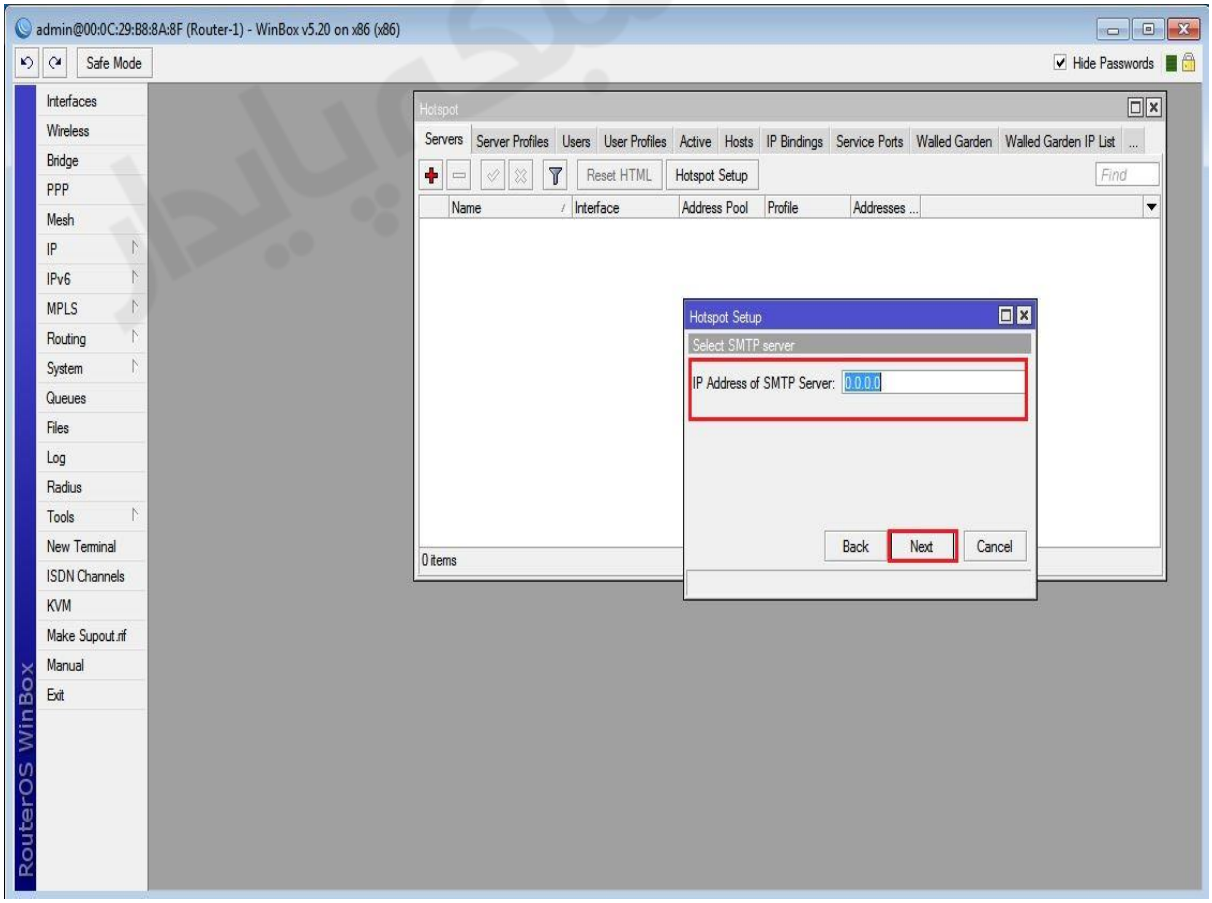


در این مرحله **Pool** مربوط به **DHCP** سروری که به کلاینت ها **Hotspot** آدرس **IP** اختصاص می دهد تنظیم می شود.این **Pool** حتما باید از رنج آدرسی باشد که برروی اینترفیس **Hotspot** وجود دارد.

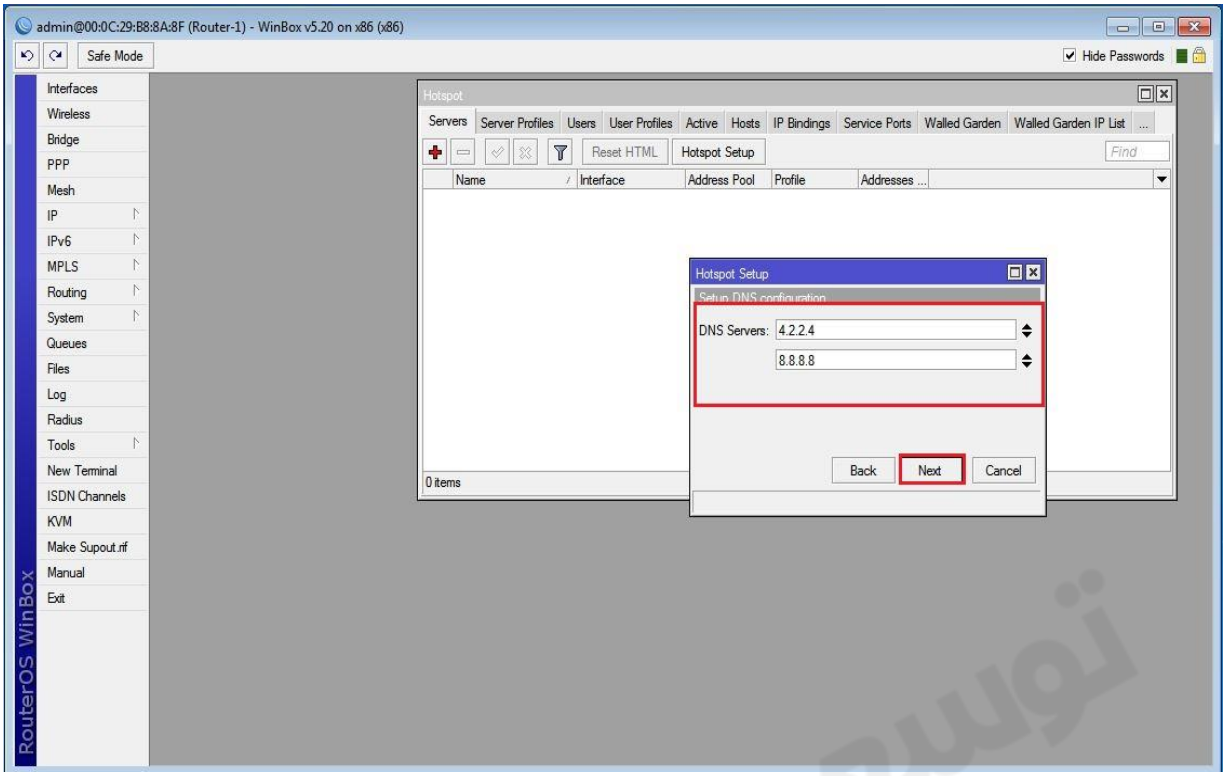




اگر در شبکه SMTP سرور برای ارسال ایمیل وجود داشت آدرس IP آن را در این قسمت وارد می کنیم.

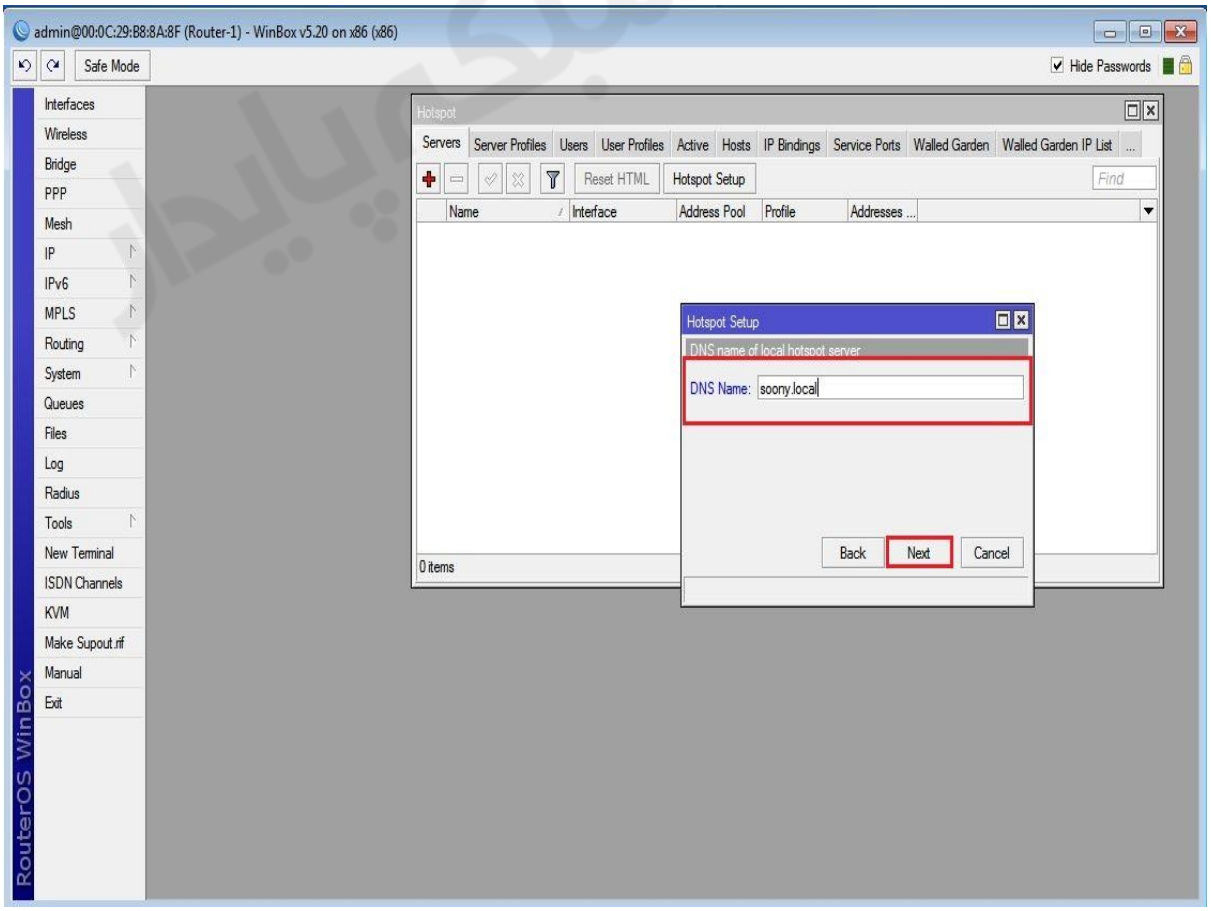


آدرس **DNS** سرور را وارد میکنیم.

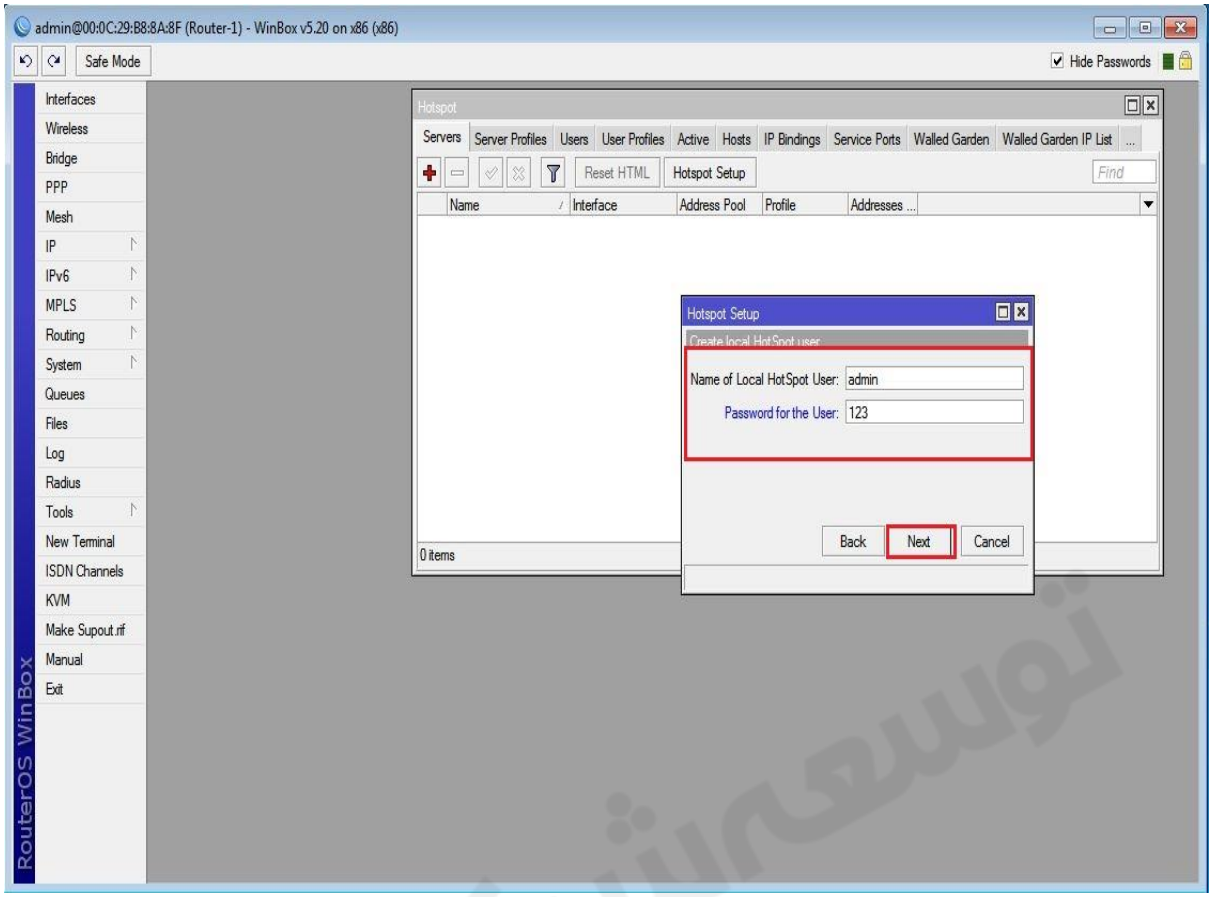


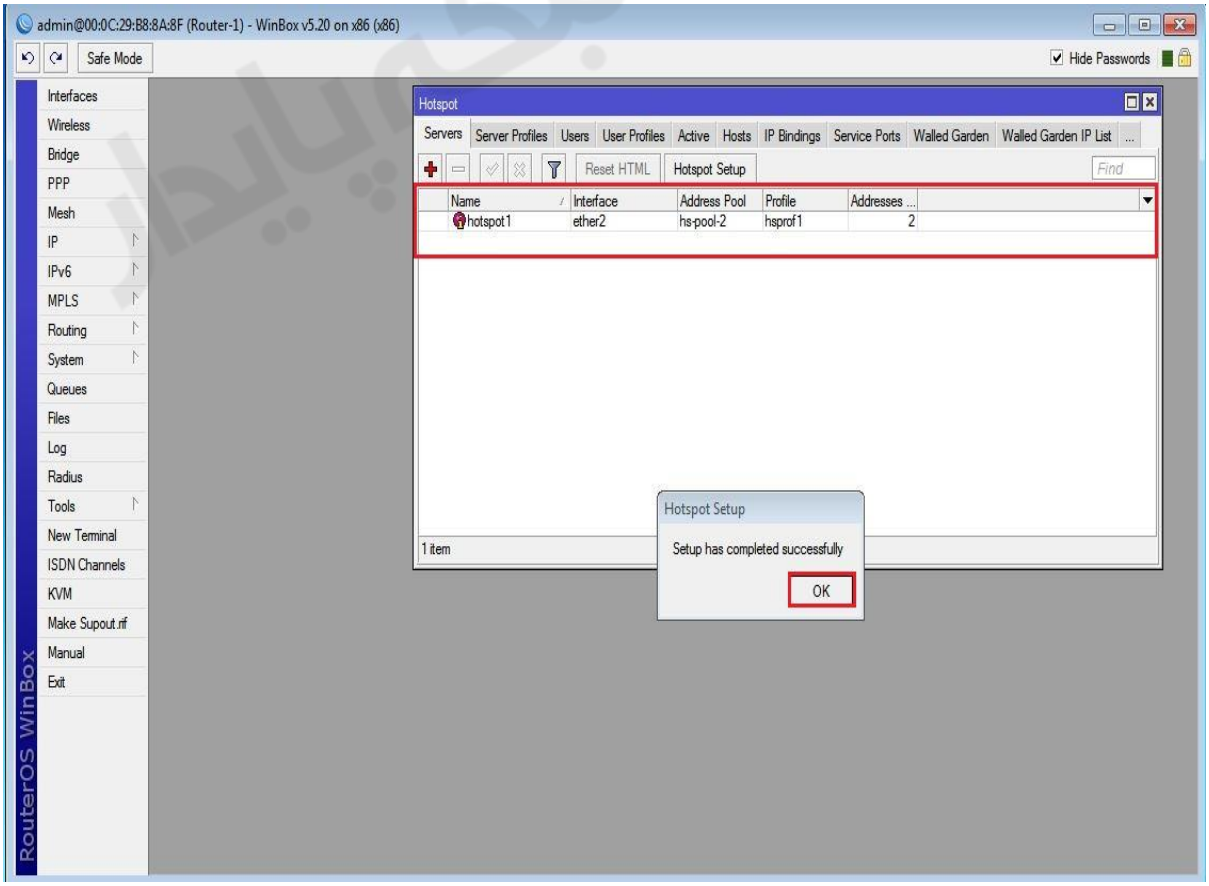
اگر دامنه ایی دارید که صفحه وب میکروتیک از طریق آن باز شود آدرس را در این مرحله وارد می کردید.

***کلاینت ها برای مشاهده اطلاعات و همچنین خروج از Hotspot از این ادرس استفاده می کنند.**



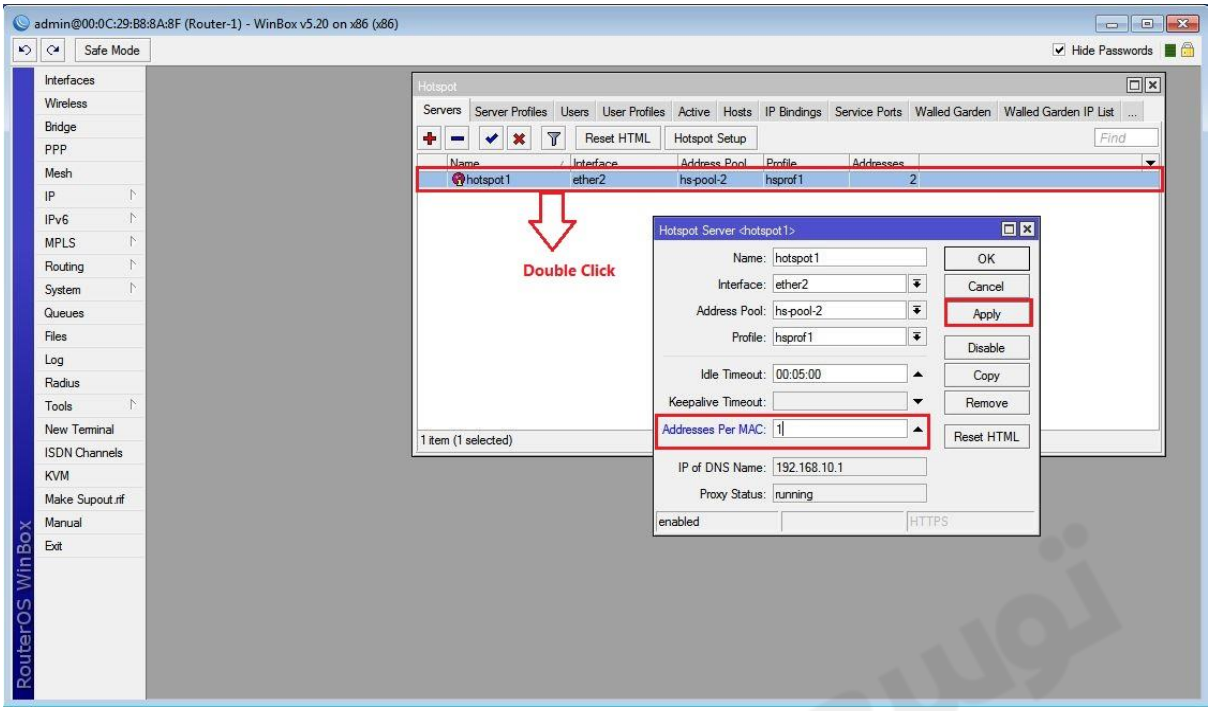
در این مرحله یک کاربر برروی میکروتیک برای سرویس **Hotspot** ساخته می شود.



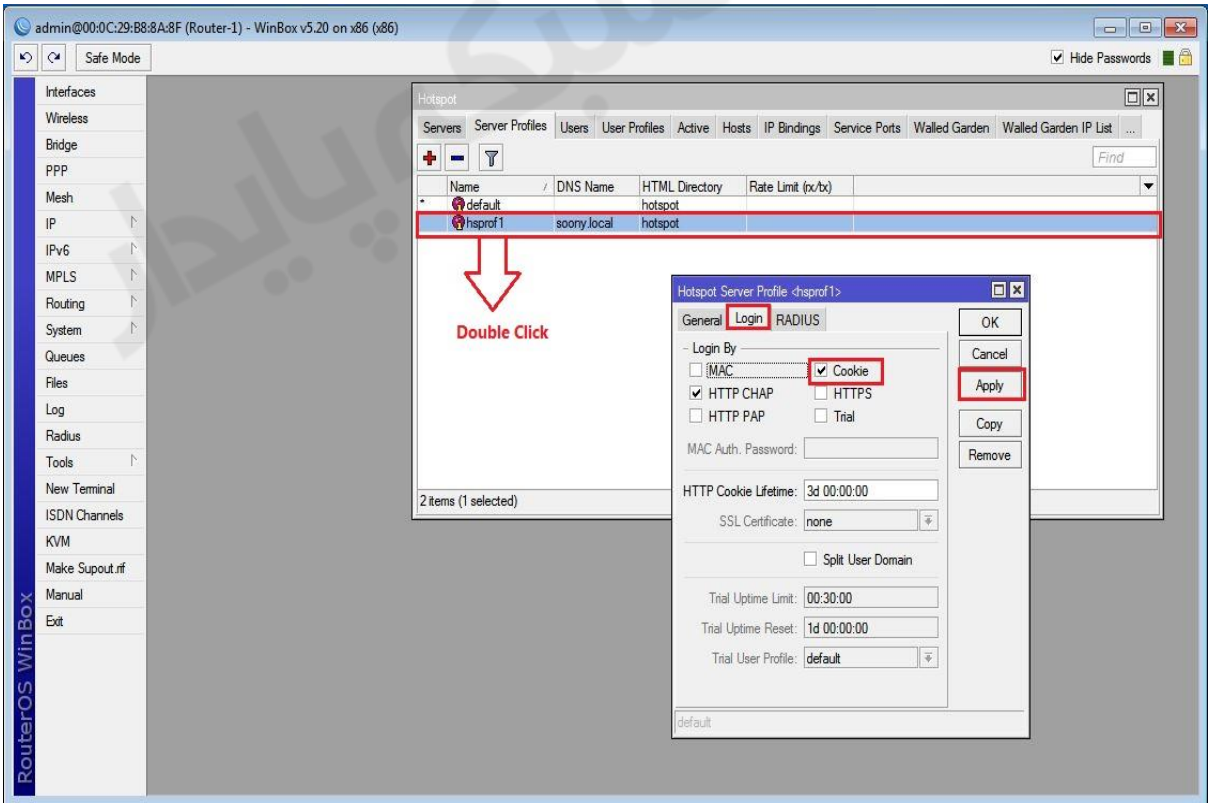


حال برای امنیت بیشتر دو عملیات زیر را انجام می دهیم :

۱) از پنجره **Hotspot** به تب **Servers** رفته و بروی **Hotspot** ایجاده شده دابل کلیک می کنیم و **Addresses Per Mac=1** قرار میدهیم.



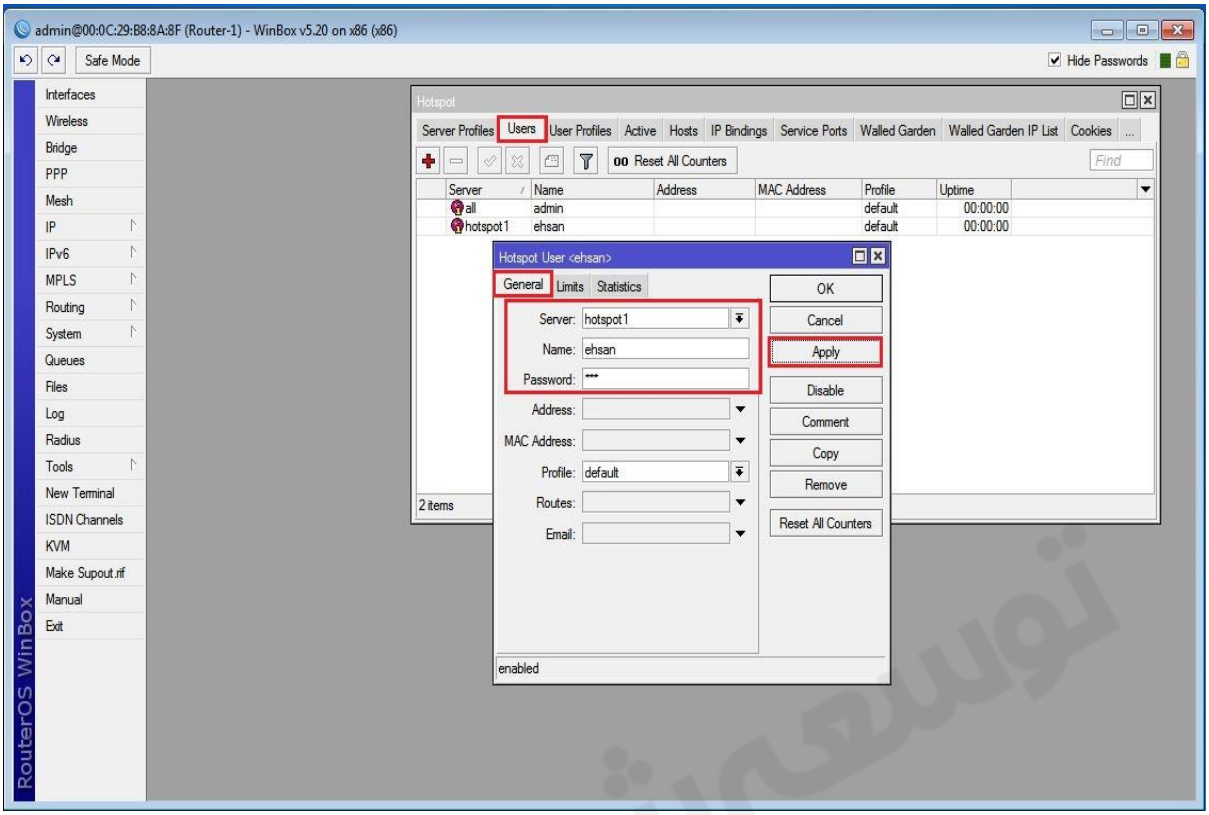
۲) از پنجره **Hotspot** به تب **Server Profile** رفته و بروی پروفایل ساخته شده (در اینجا **Hsprof1**) دابل کیلیک کرده و از پنجره باز شده به تب **Login** رفته و تیک گزینه **Cookie** را فعال می کنیم.



تا این مرحله **Hotspot** کامل راه اندازی شده است و آماده سرویس دهی از طریق کاربران **Local** (کاربرانی که بروی میکروتیک شاخته می شوند) می باشد.

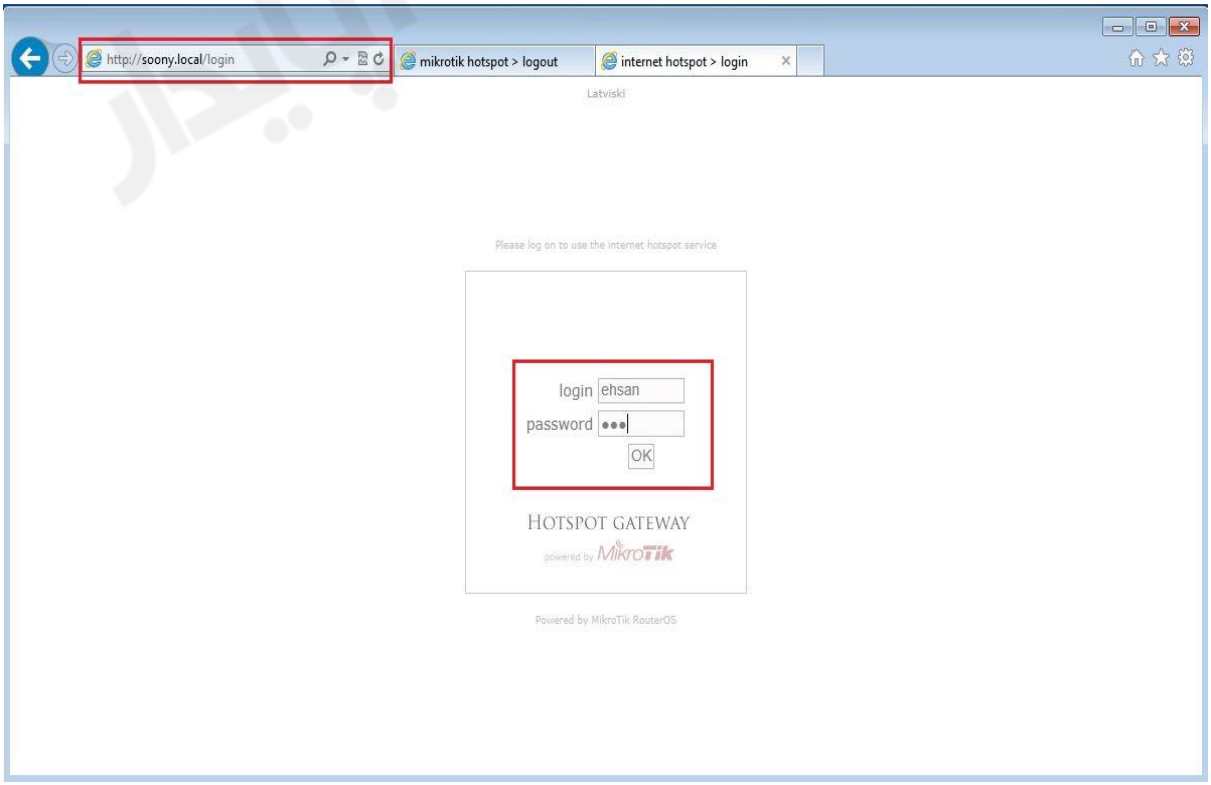
ایجاد User :

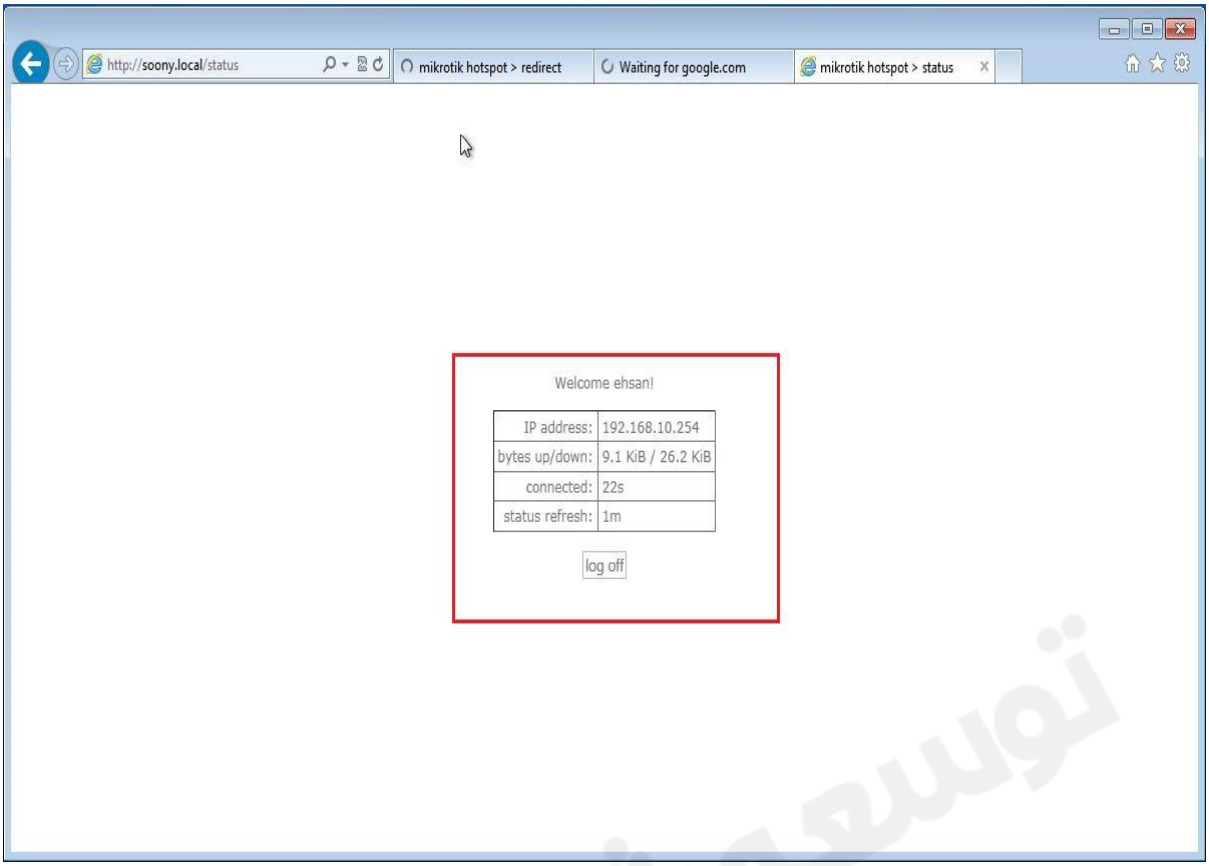
برای ایجاد کاربر به تب User رفته و برروی ADD کلیک میکنیم و هر چندتا کاربر که نیاز باشد را ایجاد می کنیم.



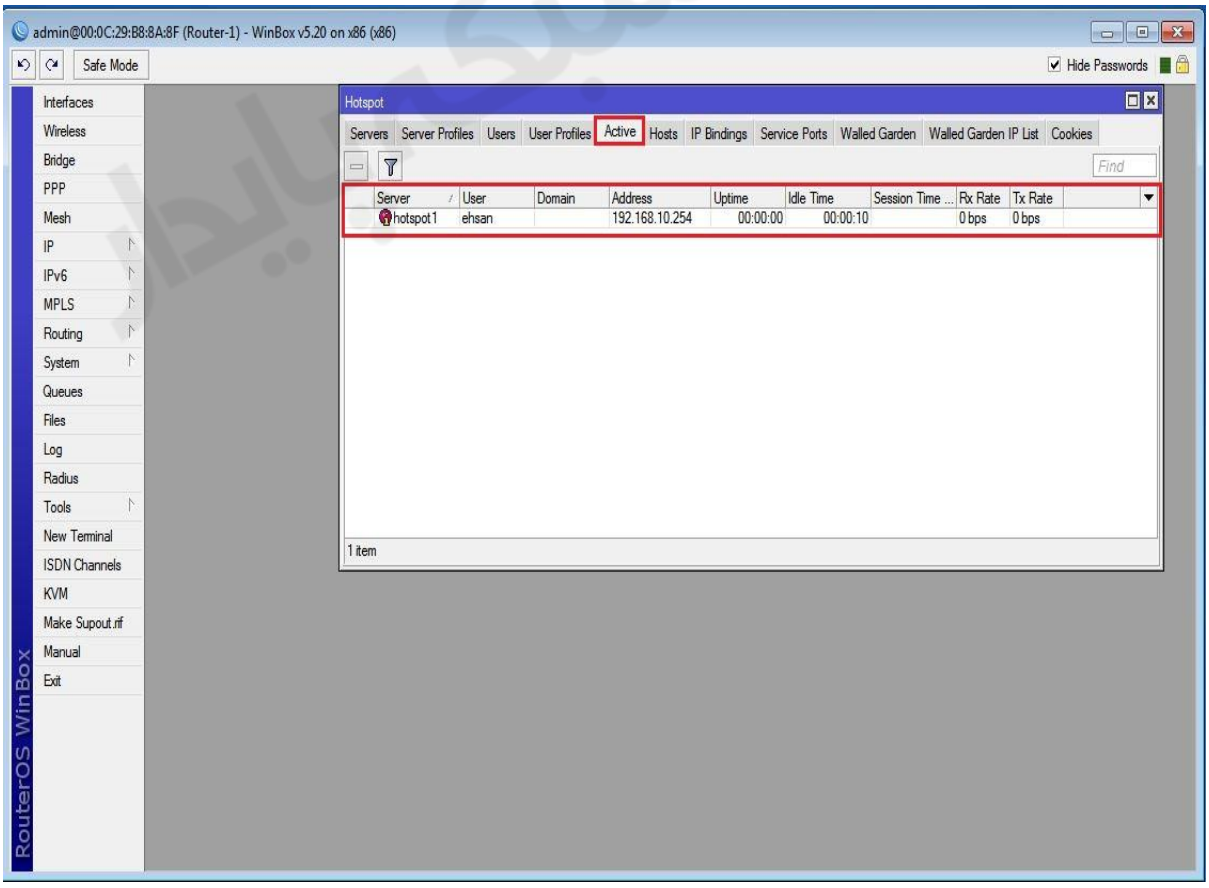
تنظیمات کلاینت :

طبق سناریو کلاینت باید از DHCP سرور IP دریافت کند.و با این تنظیمات که برروی روتر انجام دادیم کلاینت ها باید به Hotspot دسترسی داشته باشد.

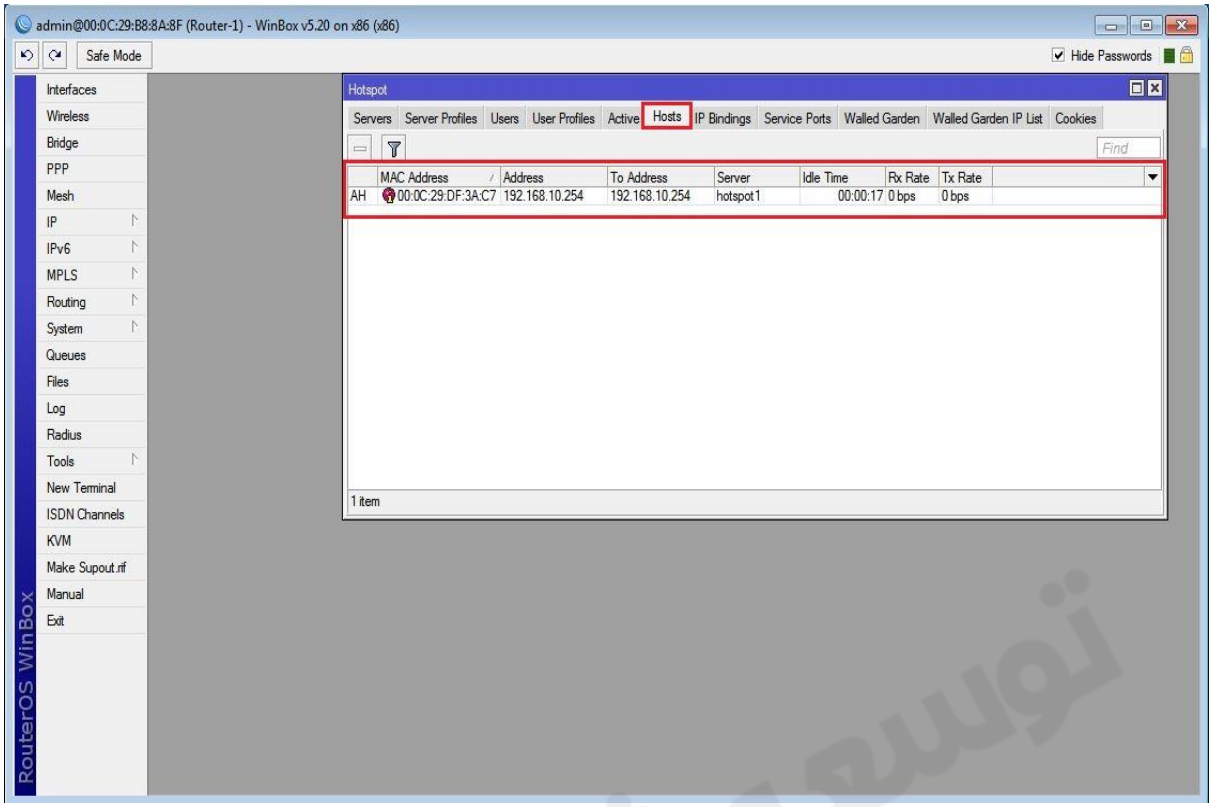




برای مشاهده کاربران متصل به **Hotspot** به تب **Active** می رویم.

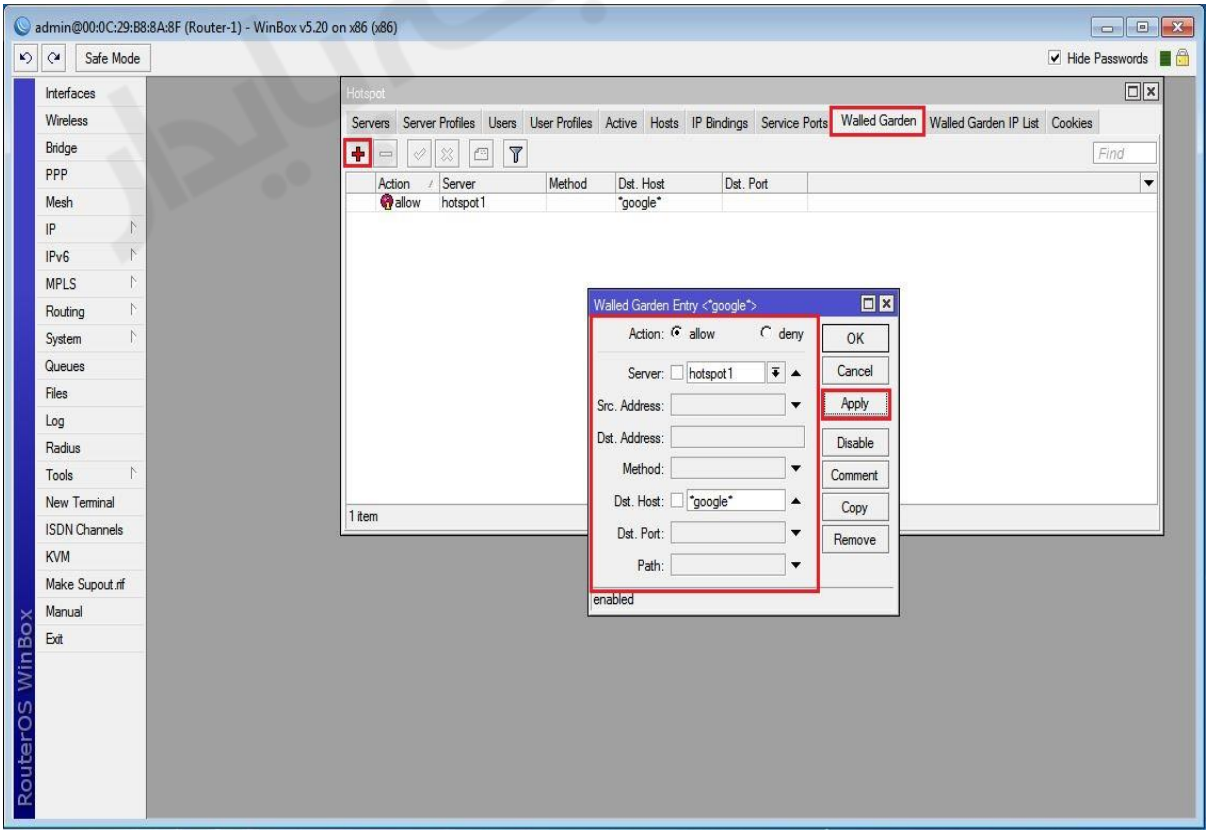


برای مشاهده لیست سیستم هایی که به اینترفیس **Hotspot** متصل هستند به تب **Hosts** می رویم.



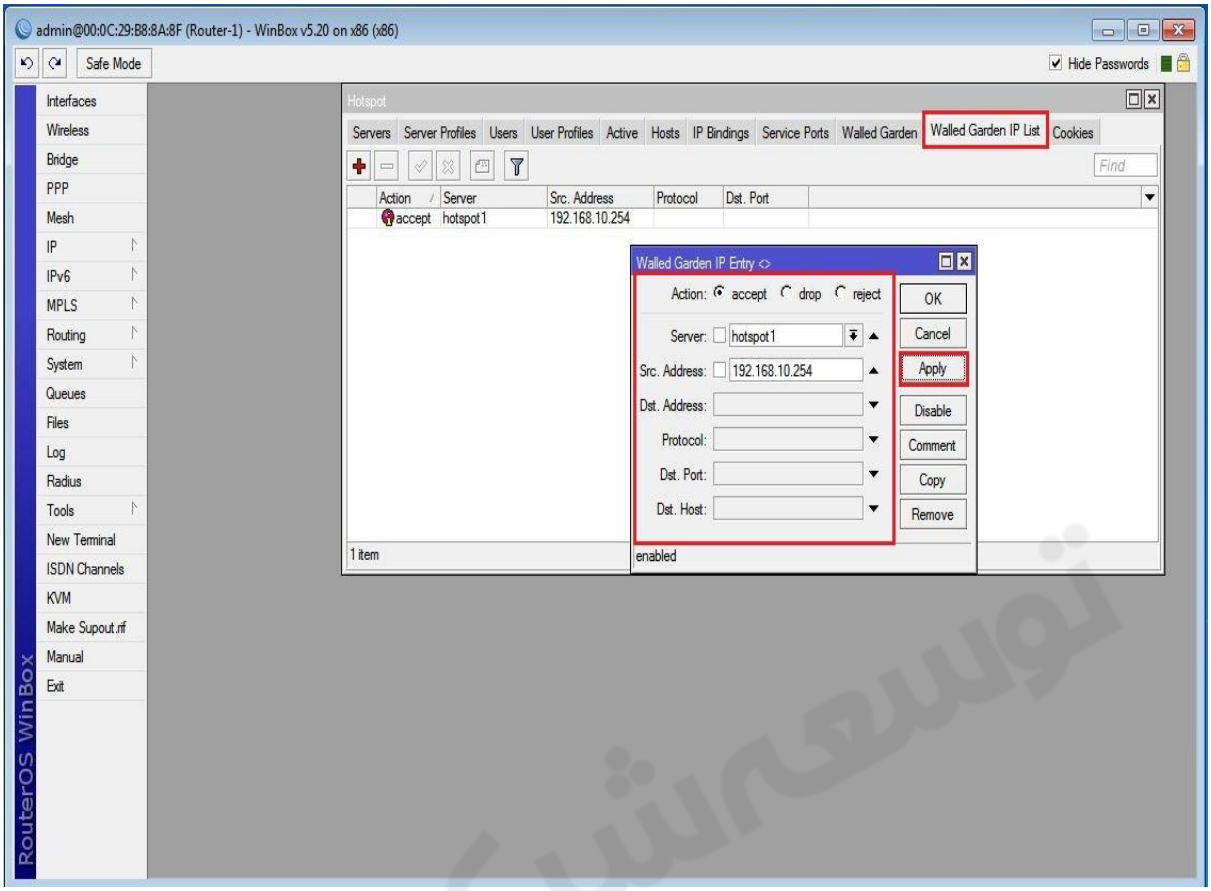
باز گذاشتن دسترسی به یک سری از سایت ها بدون احراز هویت :

برای این کار به تب Walled Garden رفته و بروی Add کلیک میکنیم و براساس نیاز سایتها را برای کاربران بدون نیاز به یوزرنیم و پسورد Hotspot باز می گذاریم.



دسترسی کاربری خاص به اینترنت از طریق Hotspot بدون نیاز به احراز هویت :

برای این کار به تب Walled Garden IP List رفته و بروی Add کلیک میکنیم.



سناریو ۲: نصب و راه اندازی سرویس Hotspot میکروتیک به همراه اکانتینگ User Manager

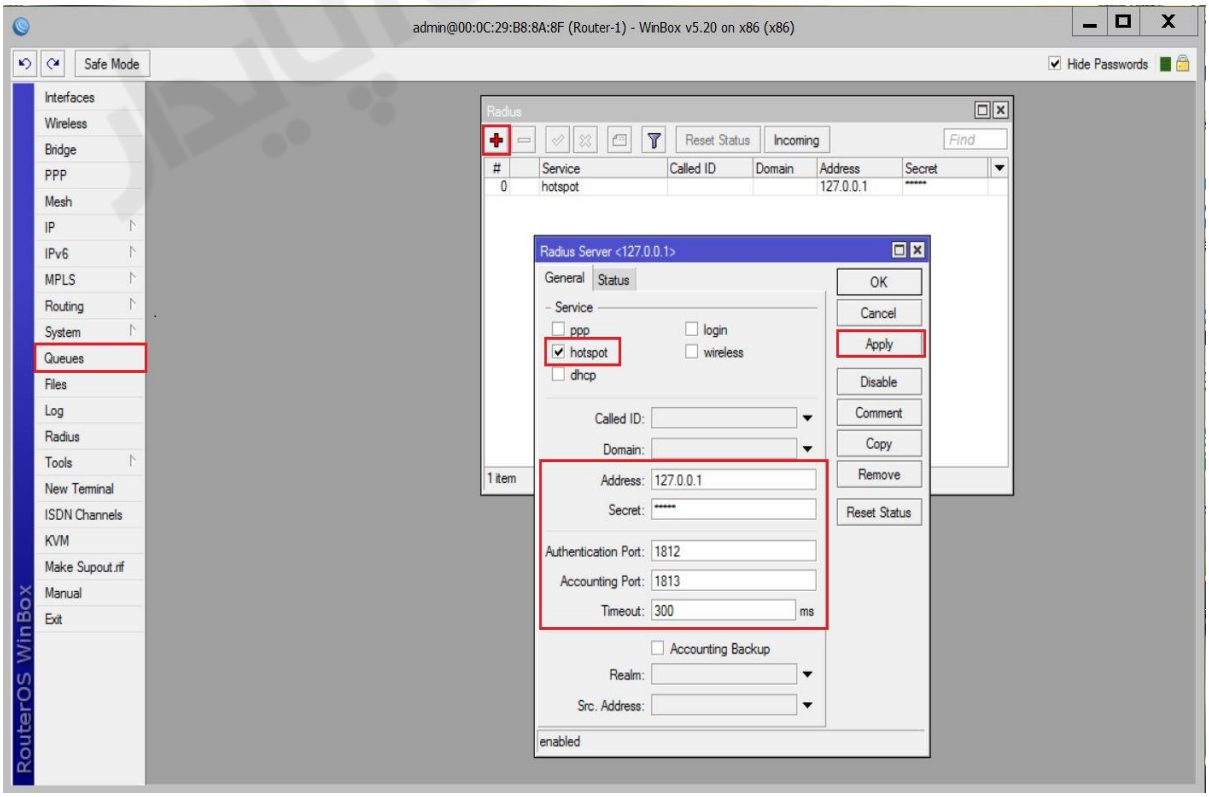
۱. تنظیمات اولیه میکروتیک (DHCP – DNS – NTP Client)
۲. نصب و راه اندازی Hotspot
۳. تنظیم Radius در میکروتیک
۴. نصب و راه اندازی User Manager

*مراحل ۱ و۲ را در سناریو قبل انجام دادیم از اینجا به بعد مراحل ۳و۴ را انجام می دهیم.

چرا سرویس اکانتینگ را با استفاده از امکان User Manager میکروتیک استفاده می کنیم ؟

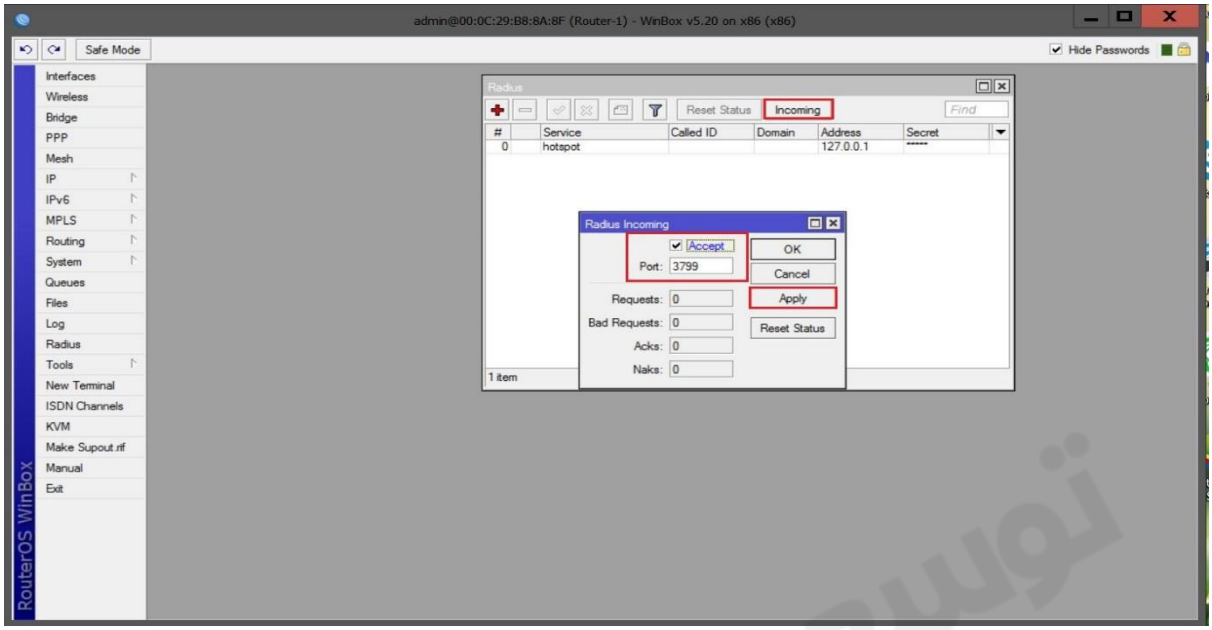
User Manager یک اکانتینگ ساده میکروتیک برای مدیریت کاربران است که پکیج مدیریتی تحت وب می باشد و با استفاده از Radius به همه روترها متصل می شود.
امکاناتی که User Manager در اختیار مدیران شبکه قرار می دهد شامل تعریف گروه های کاربری ، امکان گزارش گیری از سایت های بازدید شده توسط کاربران از زمان اتصال و Disconnect کاربران ، اختصاص دادن پهنای باند به هر کاربر و اعمال محدودیت برای آنها می باشد.

تنظیم Radius در میکروتیک :
برای اینکه کاربران Hotspot توسط Radius در روتربردهای میکروتیک احراز هویت شوند در ابتدا لازم است که یک Radius Client برای ارتباط با User Manager ایجاد کنیم.برای اینکار از منوی Radius را انتخاب میکنیم و از پنجره باز شده برروی Add کلیک میکنیم.
تیک گزینه Hotspot را فعال کرده و تنظیمات را مشابه عکس زیر انجام می دهیم.
*چون سرور رادیوس بر روی همین دستگاه نصب شده است آدرس آن را 127.0.0.1 وارد می کنیم.
*کلمه وارد شده در Secret را به یاد داشته باشید چرا که در زمان تنظیم User Manager هم می بایست وارد شود.
*از IP ی که برروی اینترفیس Hotspot تنظیم شده است برای Radius استفاده نکنید.



در مرحله بعد از پنجره **Radius** برروی **Incoming** کلیک کرده و از پنجره باز شده تیک گزینه **Accept** را فعال میکنیم و **Port=3799** قرار می دهیم.

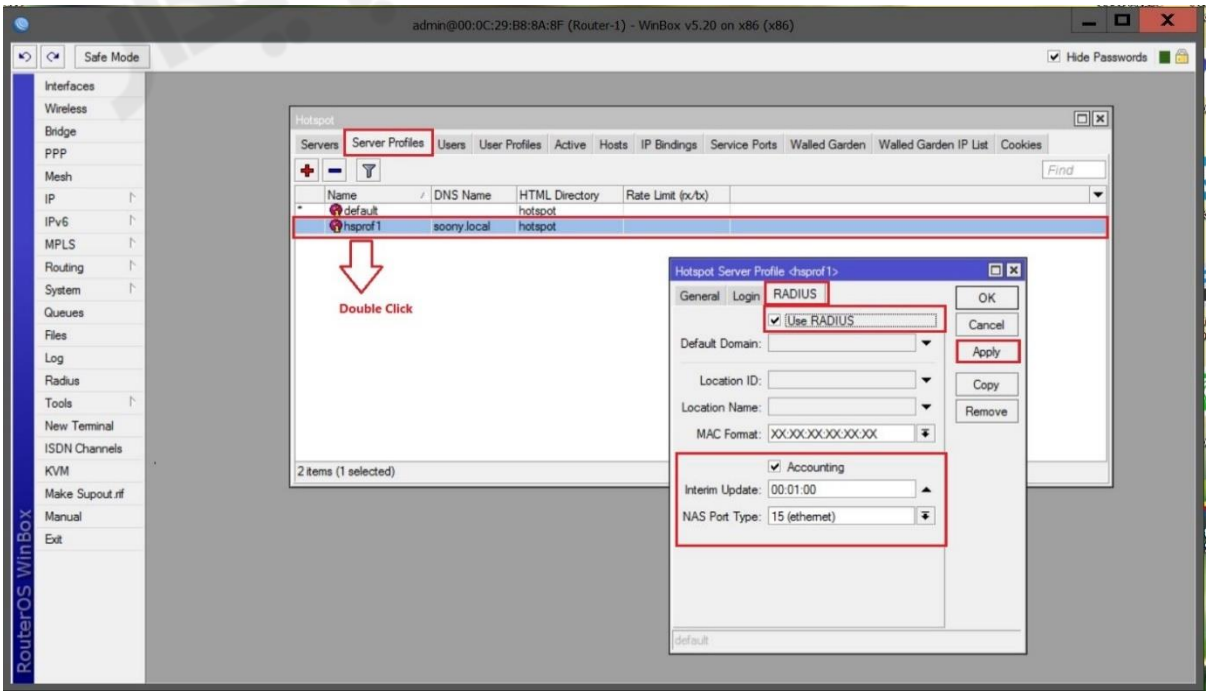
*این گزینه برای این است که اگر **Session Time** کاربرها تمام شد ارتباط آن کاربر را قطع کند.روش کار این پورت به این صورت است که اگر هرگونه تغییری که **Radius Server** در رابطه با کاربران انجام می دهد روی کاربران اعمال شود.



حال باید در **Hotspot** تعریف کنید که از **Radius Client** برای اعتبارسنجی استفاده کند.

برای اینکار از تب **Server Profile** برروی **Hotspot**ای که قبلا ایجاد کردیم دابل کلیک میکنیم و از پنجره باز شده از تب **Radius** ، تیک گزینه **Use radius** را فعال میکنیم و **Interim Update** را تنظیم می کنیم.

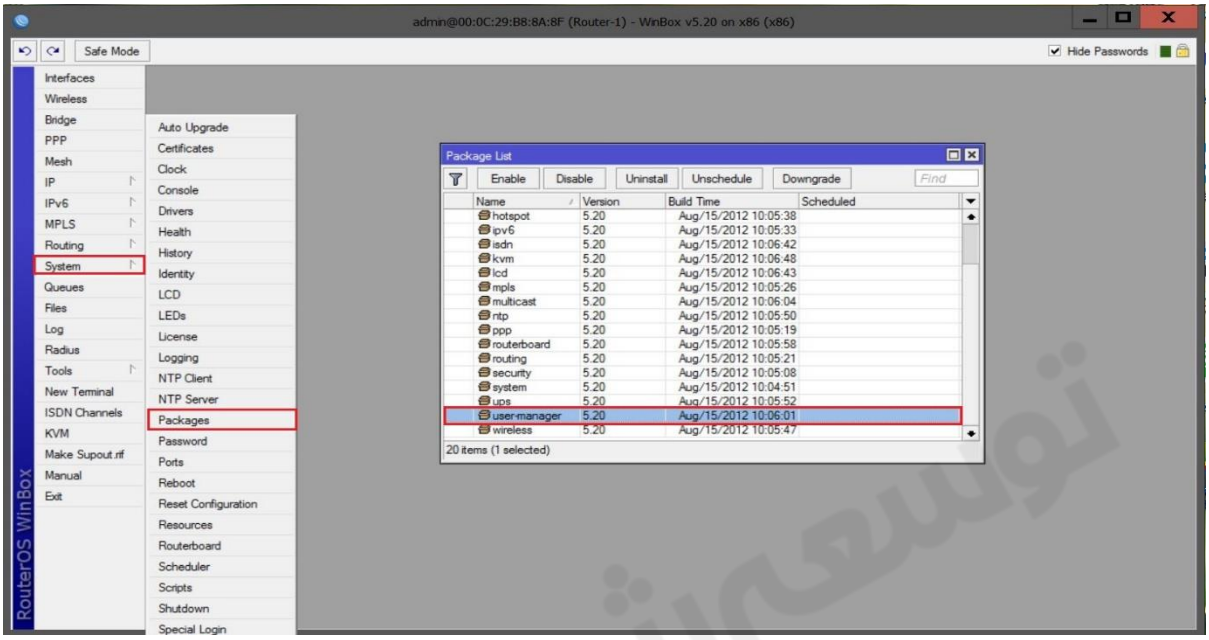
Interim Update : پکت های اعتبارسنجی کاربران و مشخص کردن اینکه چه کاربری **Disconnect** شده است را به سمت **Radius Server** می فرستد تا **Radius** آن کاربر را قطع کند . معمولا **Interim Update** را روی یک دقیقه تعیین می شود یعنی اینکه هر یک دقیقه یکبار ارتباط کاربران چک می شود و به سمت **Rdius Server** پیغامی مبتنی بر اینکه ارتباط برقرار است یا نه ، فرستاده می شود.قسمت **Interim Update** را باید طبق تنظیمات **Radius Server** خود انجام دهید وگرنه کاربران شما از لیست **Online User** ها در نرم افزار **Radius** حذف می شوند در حالی که هنوز متصل هستند.



نصب و راه اندازی User Manager :

برای استفاده از User Manager می بایست Package مربوط به آن در میکروتیک نصب شده باشد.برای چک کردن آن از منوی اصلی System و از زیرمنوی باز شده Package را انتخاب می کنیم.همان طور که در عکس زیر مشاهده می کنید پکیج User Manager نصب می باشد.

در صورتی که User Manager وجود نداشت آن را از سایت میکروتیک براساس نسخه OS ی که نصب کرده ایم دانلود میکنیم و در این قسمت نصب میکنیم سپس یکبار سیستم را ریستارت می کنیم.



برای تنظیم کردن User Manager به آدرس زیر از طریق مرورگر خود بروید :

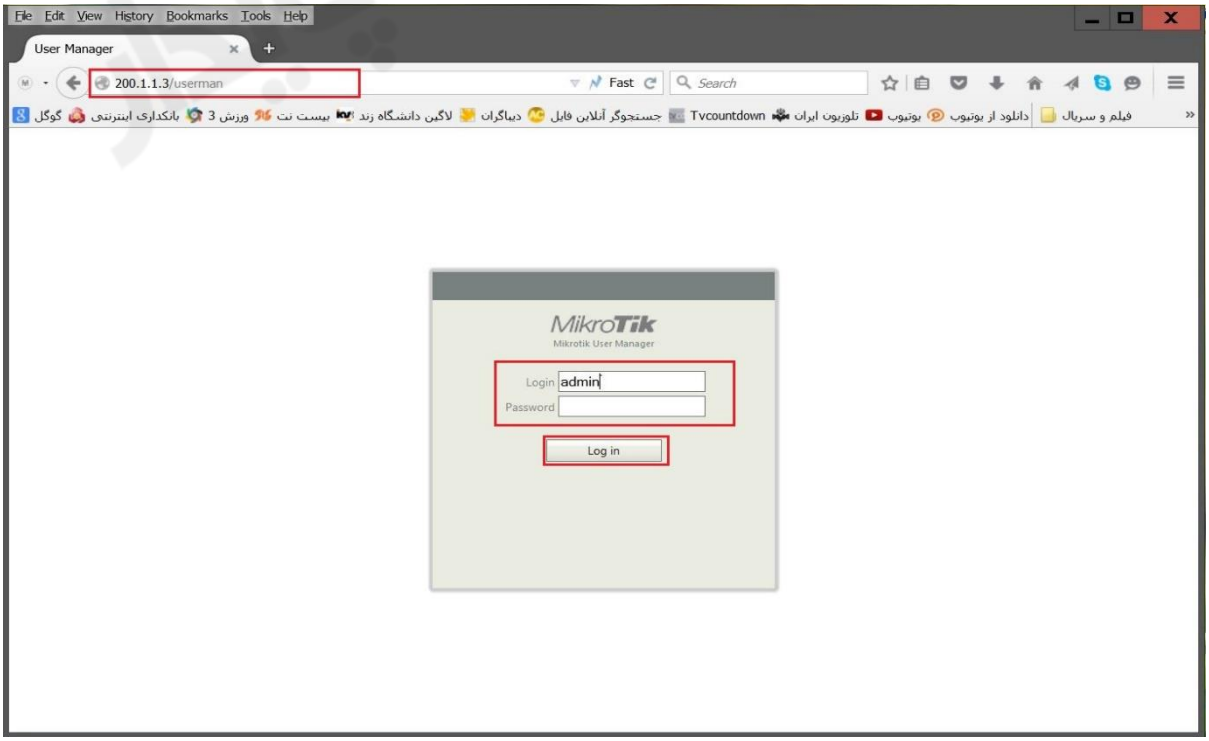
HTTP://Mikrotik IP Address / Userman

HTTP://200.1.1.3 / userman

طبق این سناریو :

بعد از اینکه آدرس را در مرورگر وارد کردید باید یوزرنیم و پسورد را وارد کنید.

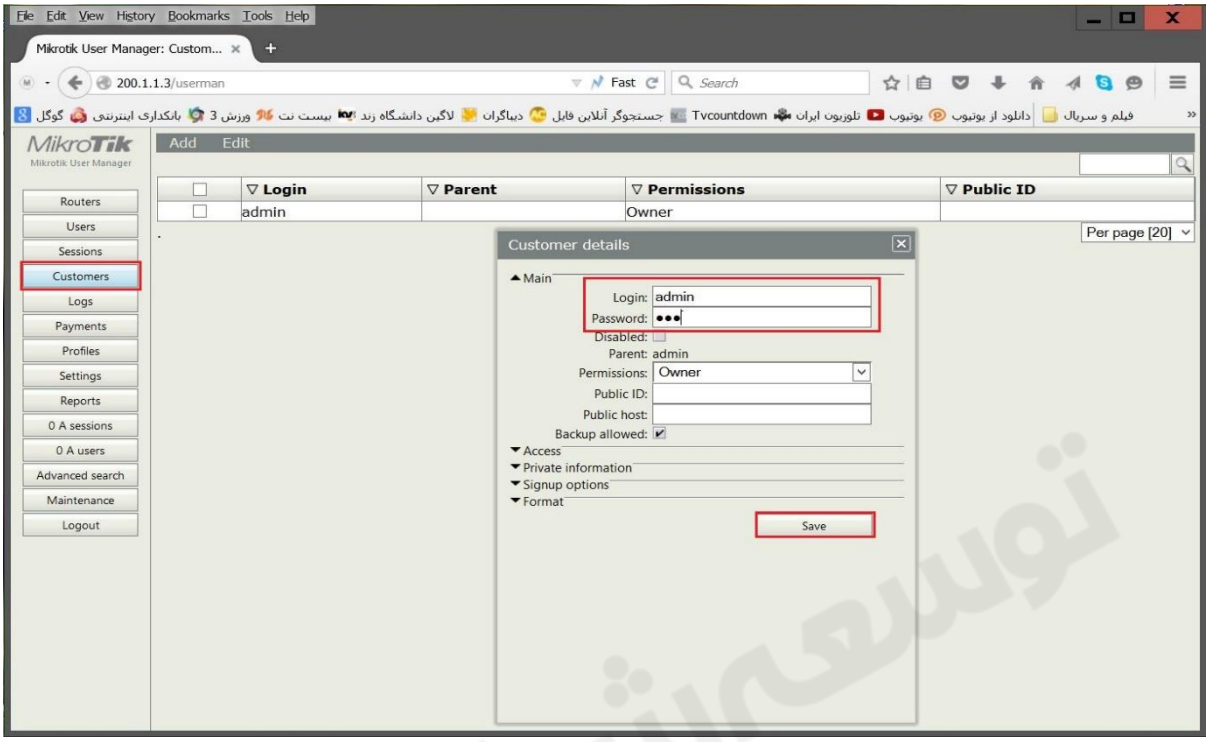
*از میکروتیک نسخه ۳ به بعد یک User بنام Admin و بدون پسورد برای دسترسی به User Manger ساخته می شود.



*دقت داشته باشید برای دسترسی به **User Manager** باید اگر فایروال را فعال کرده اید دسترسی ایجاد کنید.

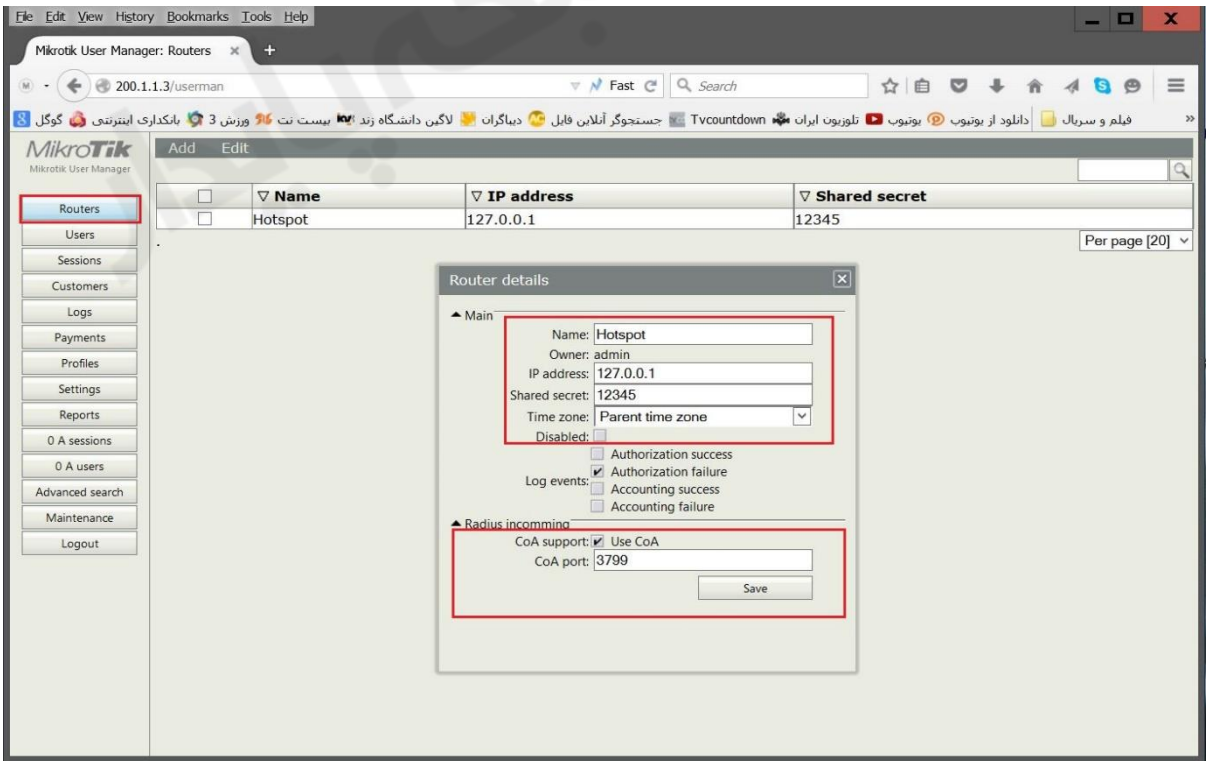
*سرویس **WWW** باید حتما فعال باشد.(**IP→Service**)

اولین کاری که بعد از ورود به **User Manager** میکنیم این است که برای دسترسی به صفحه وب مدیریت **User Manager** پسورد تنظیم می کنیم.از منوی اصلی گزینه **Customer** را انتخاب کرده و برای **Admin** پسورد ست می کنیم.



اتصال **User Manager** به میکروتیک :

از منوی اصلی گزینه **Routers** را انتخاب کرده و از پنجره باز شده برروی **New→Add** کلیک کرده و تنظیمات را انجام می هیم.

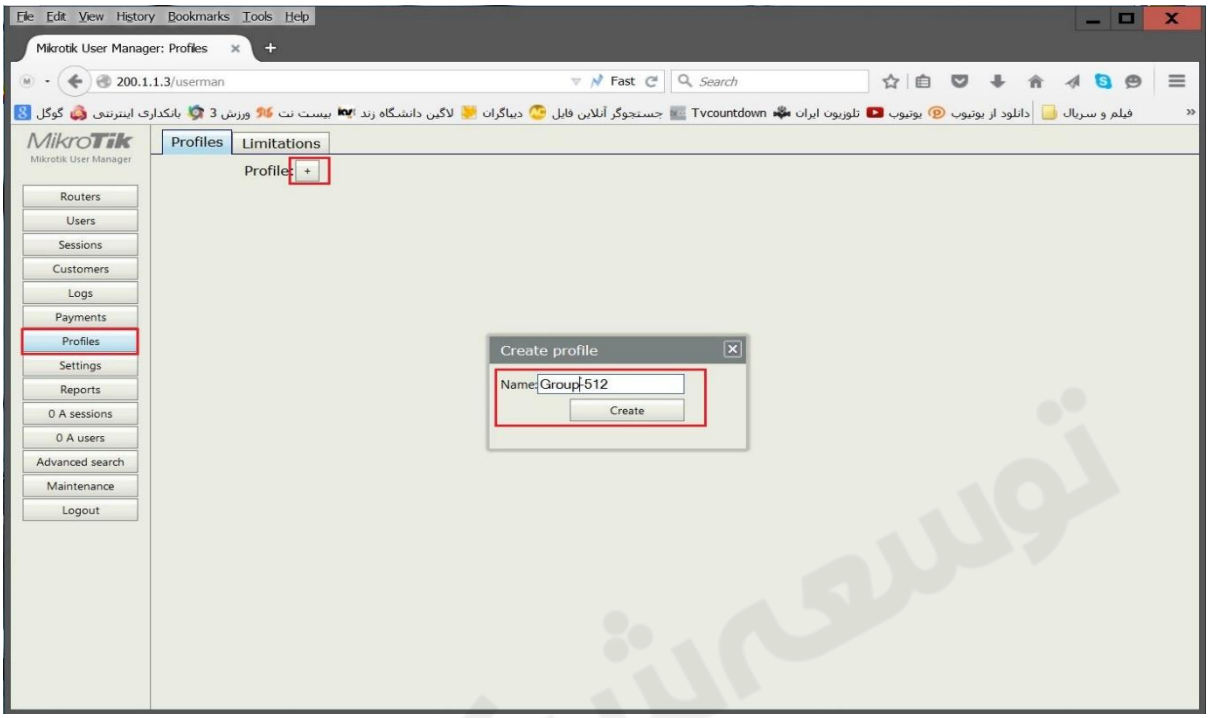


اتصال میکروتیک به **User Manager** برقرار شد.هم اکنون کاربر ساخته شده در **User Manager**میتوانند از سرویس **Hotspot** استفاده کنند.

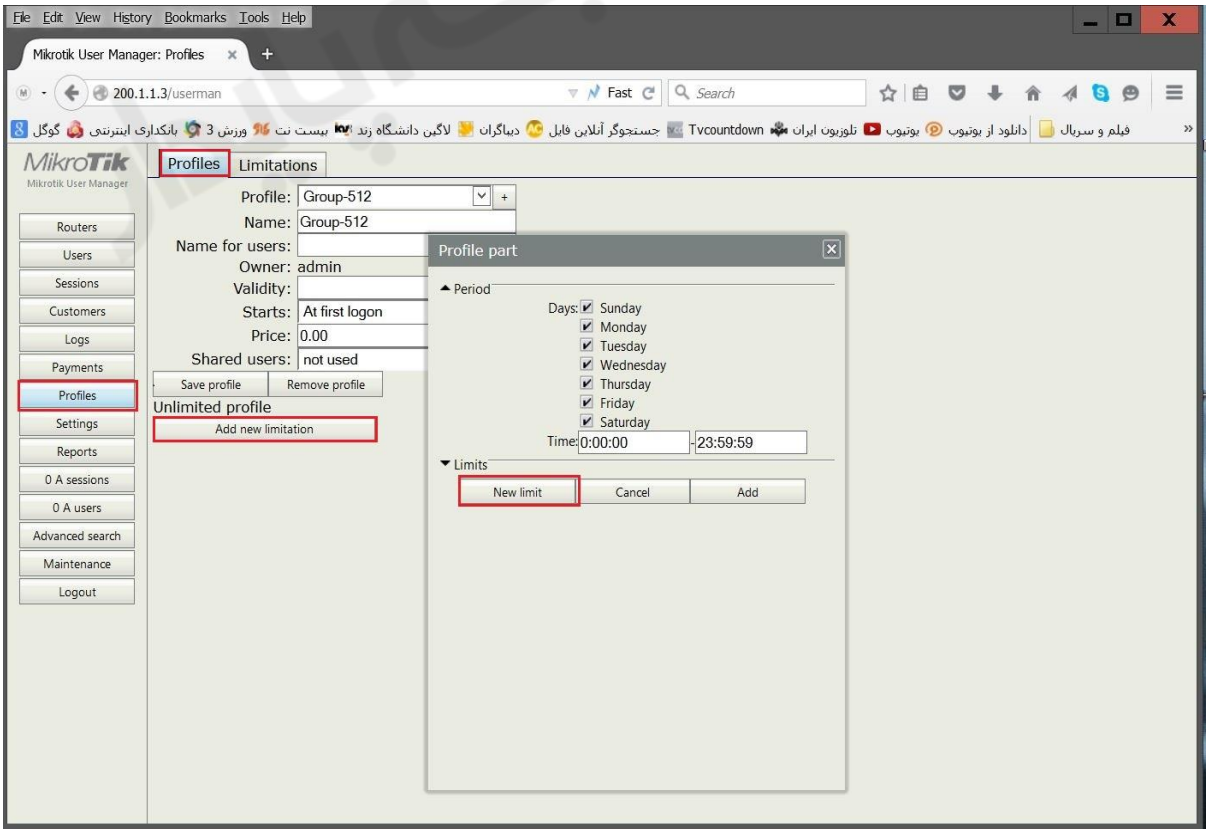
برای ساختن **User** ابتدا می بایست یک **Profile** ایجاد کرد سپس محدودیت های لازم را به **Profile** اختصاص داد و در نهایت **User** را با **Profile** مورد نظر ایجاد کرد.

ساخت **Profile** :

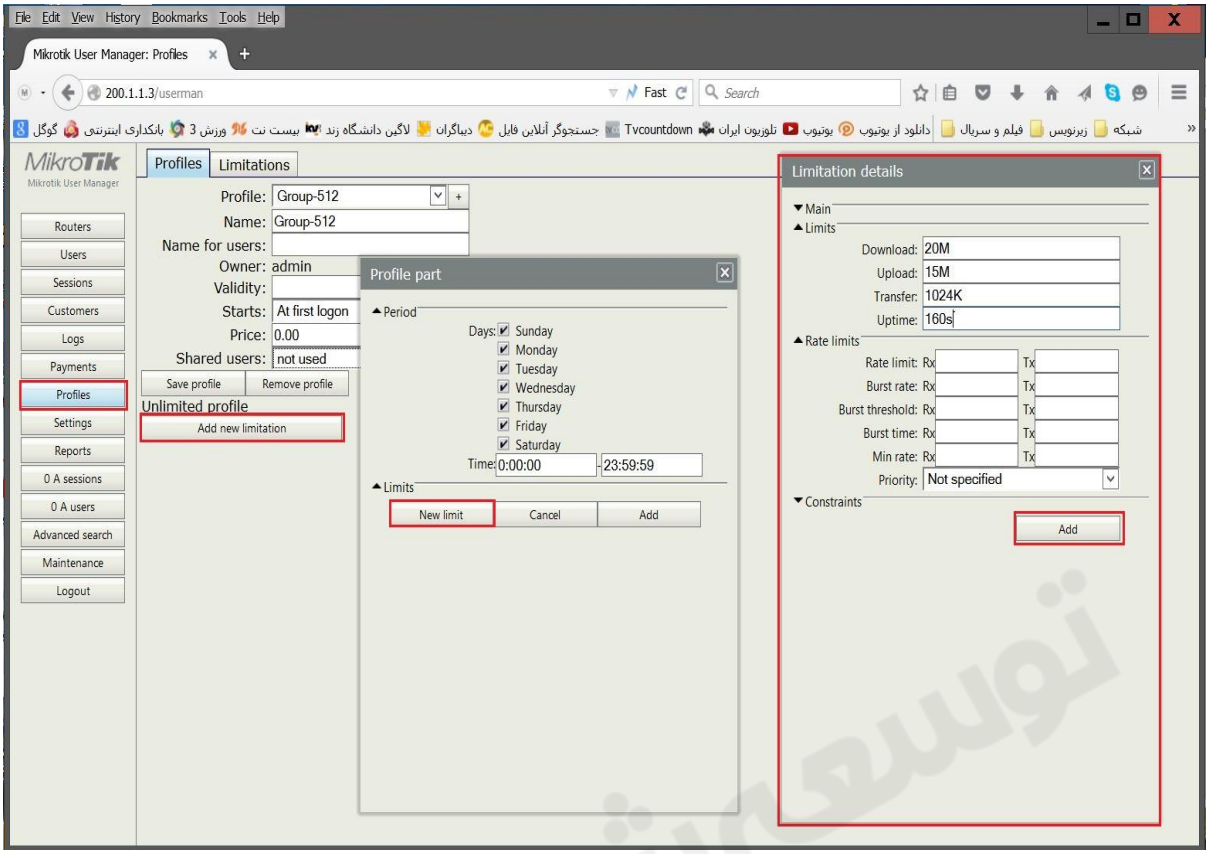
از منوی اصلی **Profiles** را انتخاب کرده از پنجره باز شده به تب **Profile** رفته و برروی **Add** کلیک می کنیم و یک نام برای **Profile** انتخاب می کنیم.

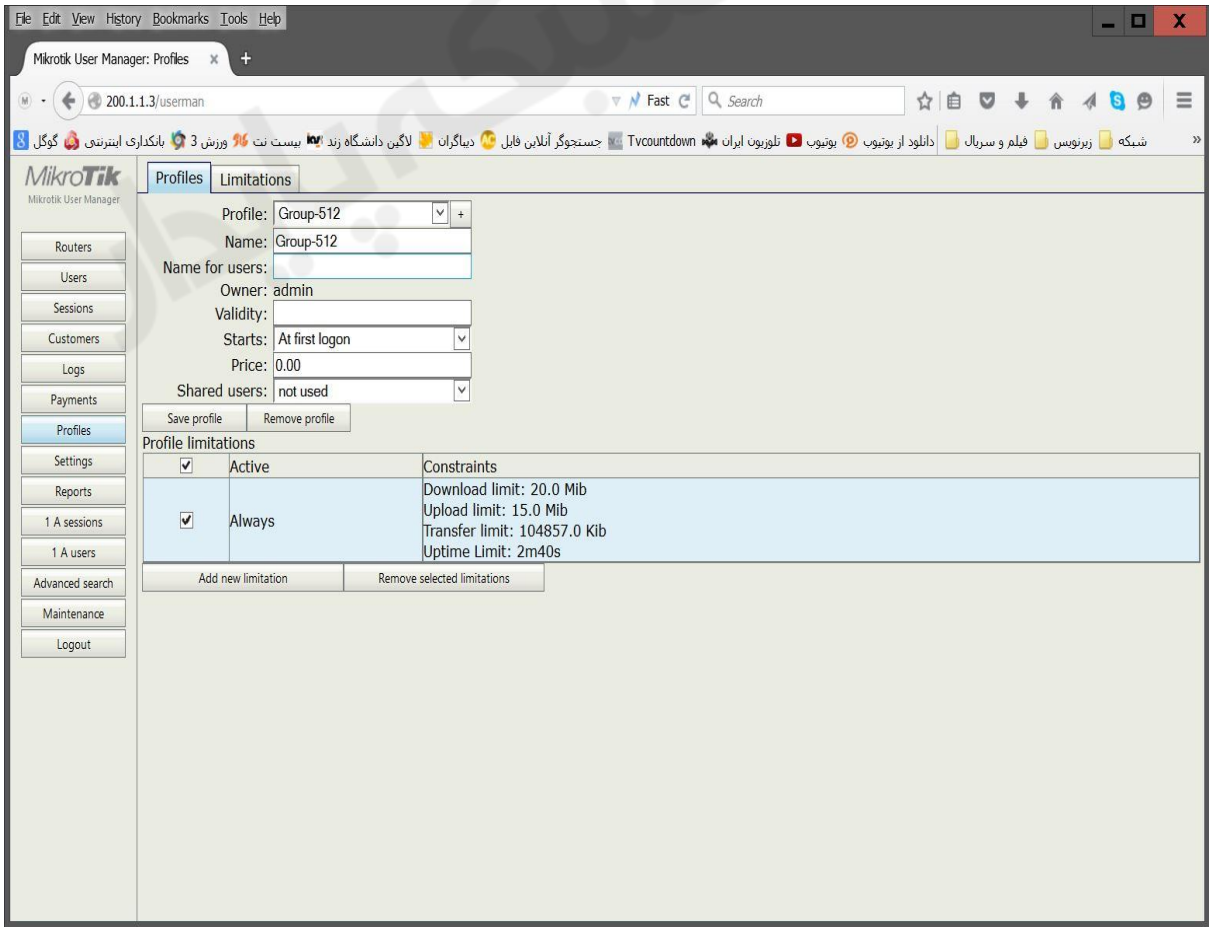


برای ایجاد محدودیت که کاربران در چه روز و ساعتی به اینترنت دسترسی داشته باشند برروی **Add New Limitation** کلیک کرده و از پنجره باز شده تنظیمات را انجام می دهیم.



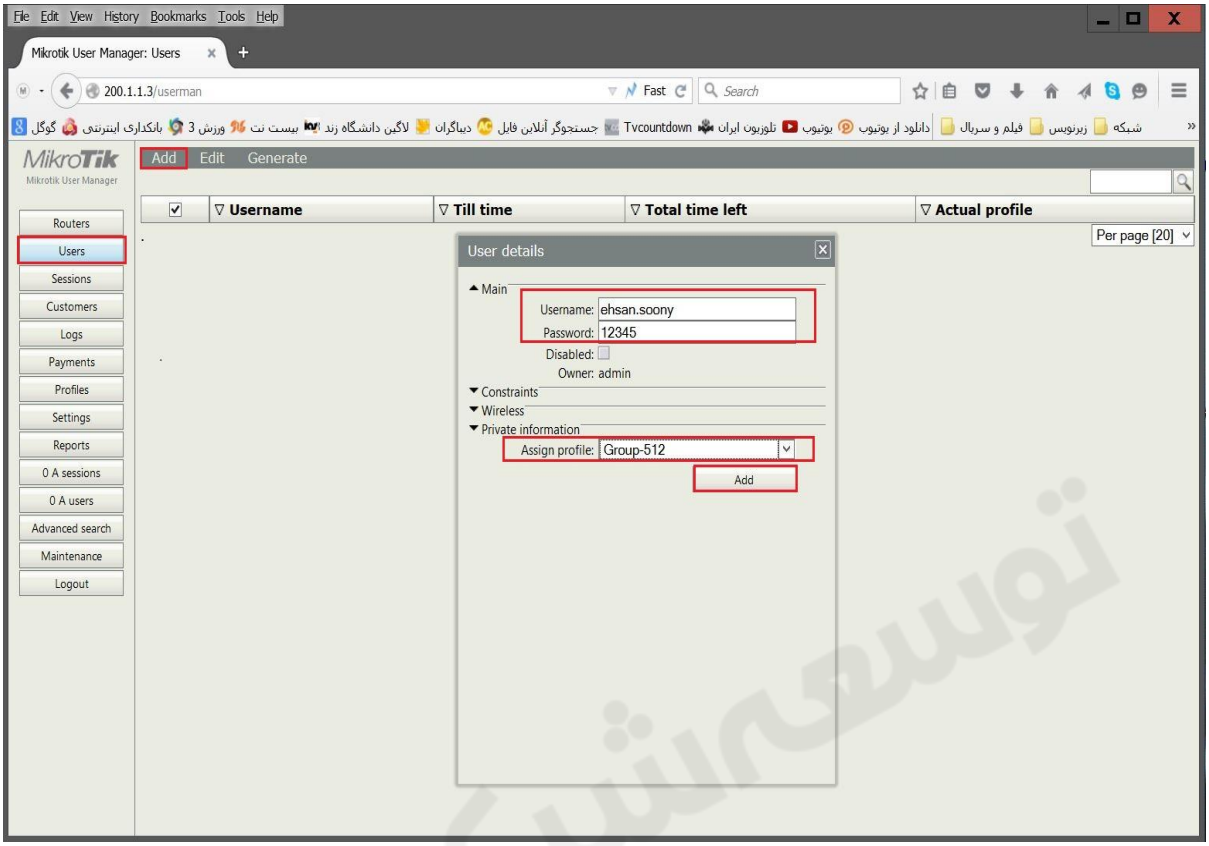
برای ایجاد محدودیت میزان دانلود ، میزان آپلود ، **UpTime** ، سرعت دانلود و .... برروی **New Limit** کلیک کنید.

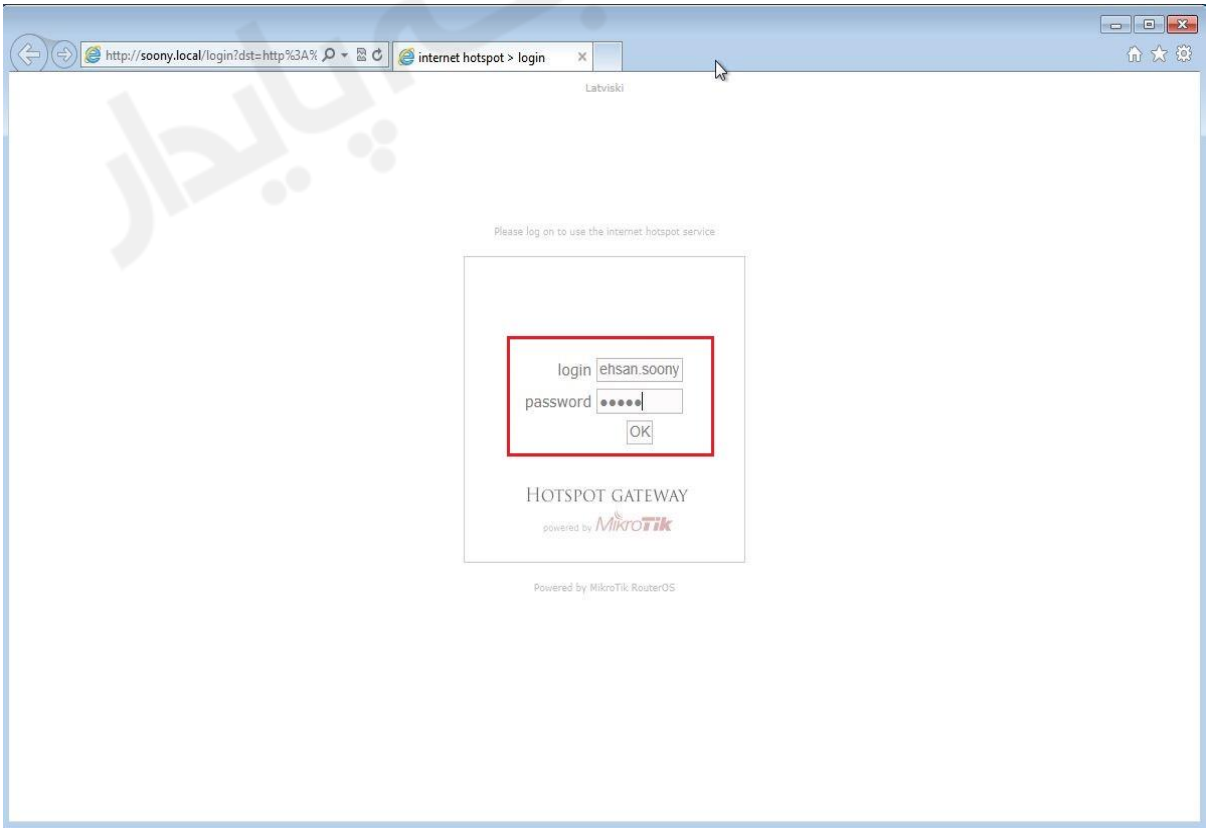


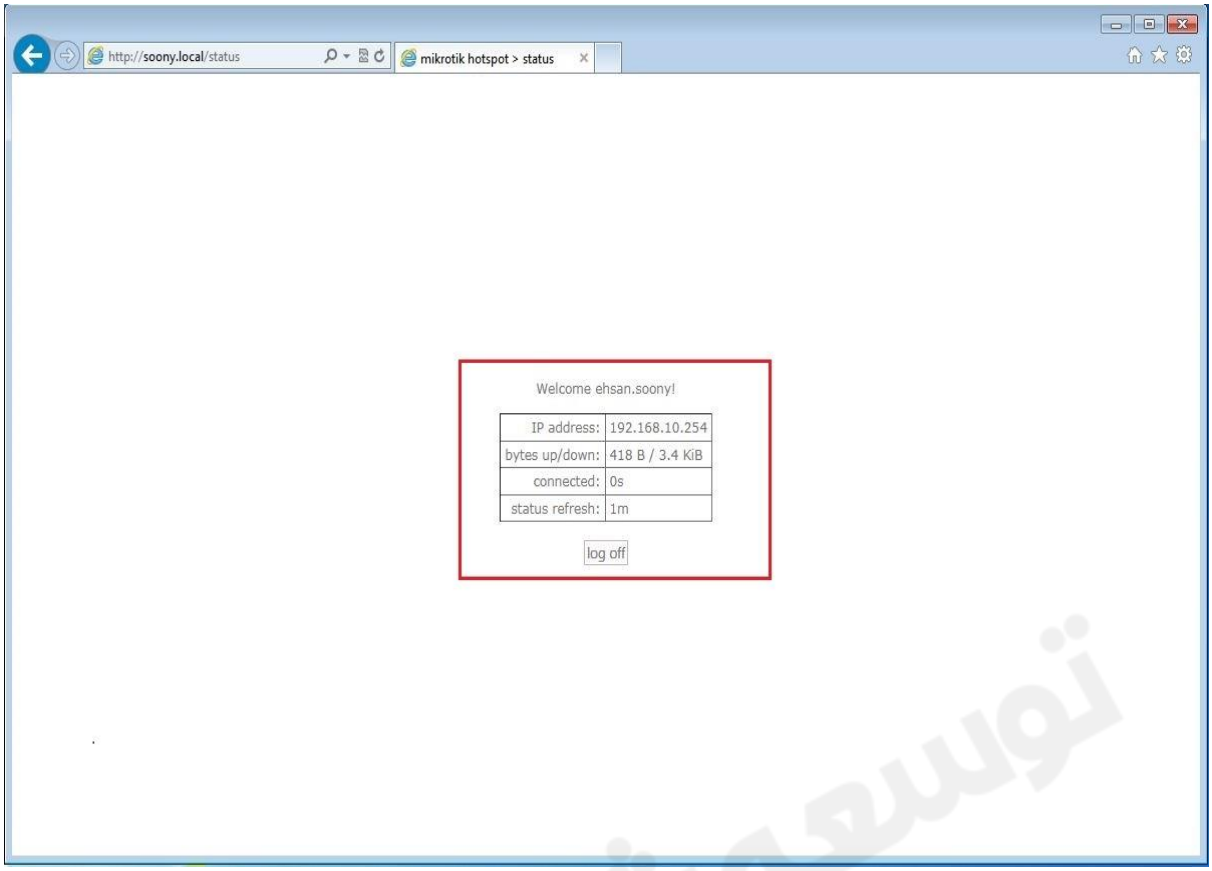


ساخت کاربر :

برای اینکار از منوی اصلی Users را انتخاب کرده از پنجره باز شده Add→One را انتخاب می کنیم و از پنجره باز شده برای کاربر یوزرنیم و پسورد و Profile تنظیم می کنیم.







از قسمت Sessions می توانیم مشخصات کاربری که به Hotspot متصل شده است را ببینیم.