راهنمای مدیریت

LAN Suite

و

تنظیمات میکروتیک در حالت های

VPN و HotSpot

نگارش ۱.۸ زمستان ۱۴۰۳

تهران، میدان رسالت، خیابان نیروی دریایی
خیابان شهدای گل، ساختمان شماره ۴
۷۳۰۱۰ (۰۲۱)

No. 4, Gol St., Niruye Daryaei St.
Resalat Square, Tehran, Iran
(+98 21) 7 30 10

www.ghasedak.com

علائم و نکات بکار رفته در نوشتن این راهنما :

 = نکته مهم

 = توجه

توضیحات راهنما

۱-در این راهنما منوی اصلی با علامت ❖)مشخص شده است.

۲-زیر منوها با علامت •)نمایش داده شده است .

۳-منوی سوم که در واقع زیر (زیرمنو)ها نمایش داده می‌شود با علامت(○) مشخص شده است.

۴-کلیک‌های موردی در صفحه‌ها با علامت ✓)نمایش داده می‌شود.

✓ IP سیستمی که LANSuite روی آن نصب است، 192.168.0.230 فرض شده است.

در این مستند سعی شده منو های مربوط به راه اندازی سرویس LANSuite توضیح داده شود.

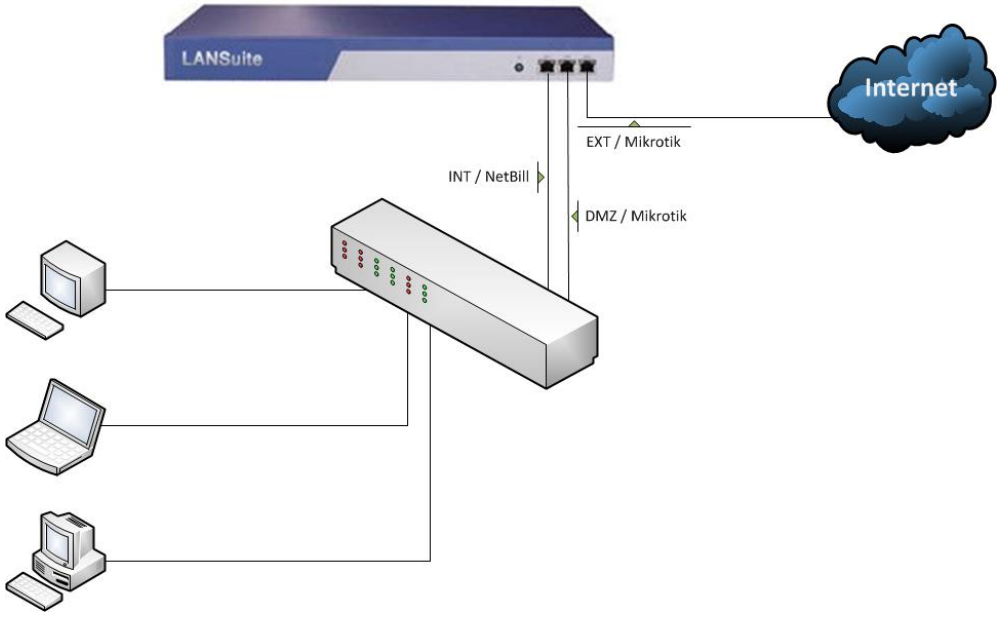
قاعدتا سازمانهایی که مایل به استفاده از NetBill برای سرویس خاص مانند VoIP یا ADSL باشند ، می‌توانند از مستند مربوط به آن سرویس که در سایت www.netbill.ir در دسترس است ، استفاده نمایند.

❖ مقدمه

در LAN Suite سه Interface با نام های EXT ، INT و DMZ موجود می باشد که INT مربوط به نرم افزار NetBill و دو Interface دیگر با نام های EXT و DMZ مربوط به Router OS Mikrotik می باشد.(Router OS Mikrotik بصورت Virtual در LAN Suite تعبیه شده است) و فقط کافیست که Internet ورودی را به یکی از Interfaceهای مربوط به Mikrotik متصل کنید و Interface دیگر آن را به Switch کاربران خود متصل کنید.

همچنین با توجه به نوع چیدمان شبکه خود می توانید Interface مربوط به NetBill را به Switch کاربران و یا اینترنت خود متصل نمایید.

نمونه ای از توپولوژی ذکر شده بصورت زیر می باشد.



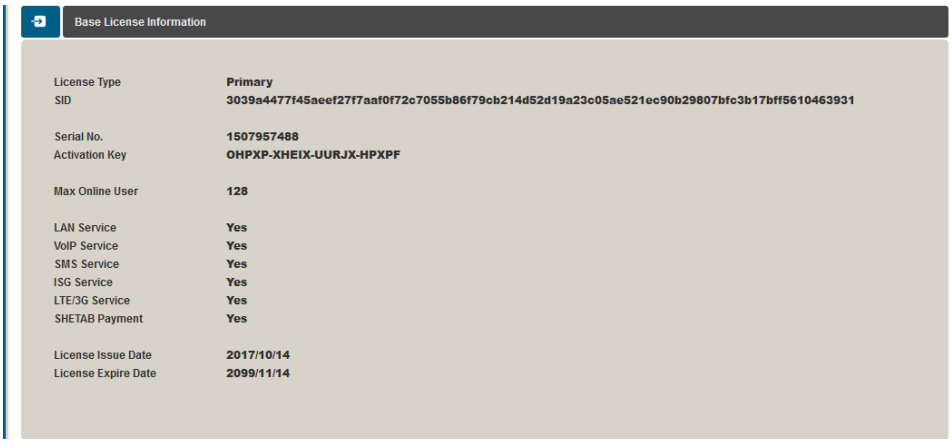
❖ Active Licence در Netbill

احتما قبل از Active می‌بایست وارد پوسته[1] در Netbill شده و دستور (wget netbill.org) را وارد کرده و بعد از ۱۰۰٪ شدن به مرحله بعد مراجعه کنید.

[1] Shell

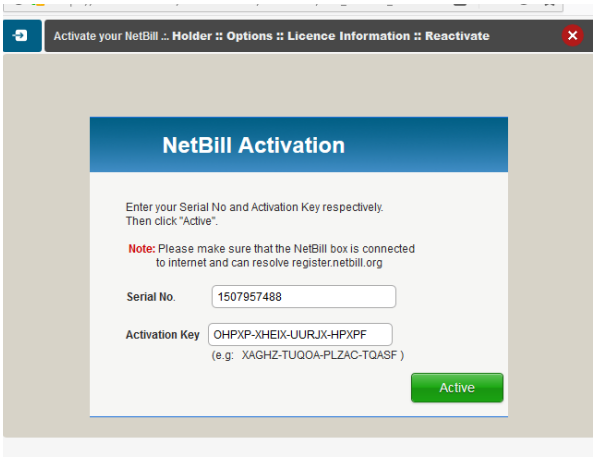
در لایه Holder وارد Option و زیر مجموعه آن وارد Licence Information شوید SID را در سایت http://netbill.ir در قسمت درخواست Licence وارد کنید و برای شرکت قاصدک بفرستید.

Holder → Options → Licence Information →SID



در مرحله بعد روی Activate کلیک کنید Serial و Activation Code را که توسط پست الکترونیک[۲] برای شما فرستاده شده را داخل این قسمت‌ها وارد کنید و روی Active کلیک کنید

[۲] Email



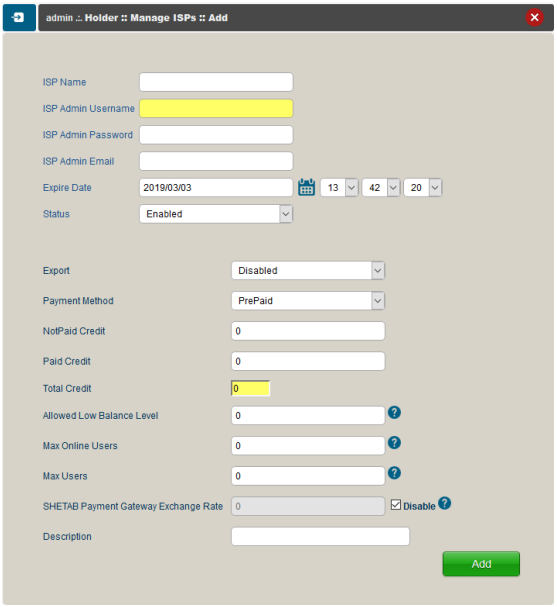
❖ ایجاد ISP در لایه Holder

مطابق ساختار درختی Netbill می‌بایست در لایه Holder یک ISP ایجاد و سرویس مورد نظر خود را به آن متصل کنیم تا این ISP ساخته شده از سرویسی که به آن منتصب می‌شود استفاده نماید ، به ترتیب مراحل زیر را انجام دهید.

برای معرفی Access Server و همچنین ایجاد سرویس در Netbill یک ISP باید ساخته شود تا بتوان این گزینه های ساخته شده را به ISP مورد نظر اتصال داد.

Holder → Manage ISPs

برای اضافه کردن یک ISP وارد Manage ISP شده و بر روی دکمه Add New کلیک کنید صفحه زیر نمایان خواهد شد.



- ISP Name

یک نام برای ISP تعریف کنید.

- ISP Admin Username

نام کاربری مدیر ارشد ISP (که همان نام ISP خواهد بود).

- ISP Admin Password

رمز عبور برای مدیر ISP مورد نظر.

- ISP Admin Email

Email معتبر برای مدیر ISP.

- Expire Date

تاریخ انقضای ISP. بدیهی است پس از آن تاریخ کلیه کاربران و VISP تحت مدیریت این ISP امکان ورود به سیستم نخواهند داشت..

با کلیک بر روی دکمه More می‌توانید به اطاعات بیشتری دسترسی پیدا کنید.

- Status

وضعیت دسترسی آن ISP را مشخص می‌کند که می‌توانید یکی از ۳ گزینه ، فعال ، غیر فعال و منقضی شده را انتخاب کنید.

- Export

از این قسمت می‌توانید مجوز استخراج اطلاعات کاربران را به ISP اعطاء کنید.

- Payment Method

در این روش می‌توانید انتخاب کنید که ISP مورد نظر امکان منفی شدن اعتبار خود را داشته باشد.

✓ اگر PrePaid را انتخاب کنید بدین معنی است که ISP مورد نظر فقط به میزان اعتبار وارد شده حق استفاده دارد

✓ اگر گزینه PostPaid را انتخاب کنید بدین معنی است که ISP مورد نظر می‌تواند اعتبار منفی نیز داده باشد .

- NotPaid Credit

در این قسمت مشخص می کنید که چه میزان اعتبار به ISP اختصاص داده شده که هنوز آن را پرداخت نکرده است (بدهکار).

- Paid Credit

میزان اعتباری که پرداخت شده است را در این قسمت مشخص کنید.

- Total Credit

میزان کل اعتبار ISP را مشخص می کند.

- Allowed Low Balance Level

مشخص می کنید که تا چه میزان بعد از اتمام اعتبار یک ISP به آن اجازه استفاده داده شود (تا چه میزان اعتبار منفی به آن اختصاص پیدا کند).

- Max Online Users

حداکثر تعداد کاربران آنلاین.

- Max Users

حداکثر تعداد کاربران قابل تعریف.

- Description

در این قسمت توضیحاتی که برای کاربران وجود دارد را می توانید وارد کنید .

- Manage VISPs

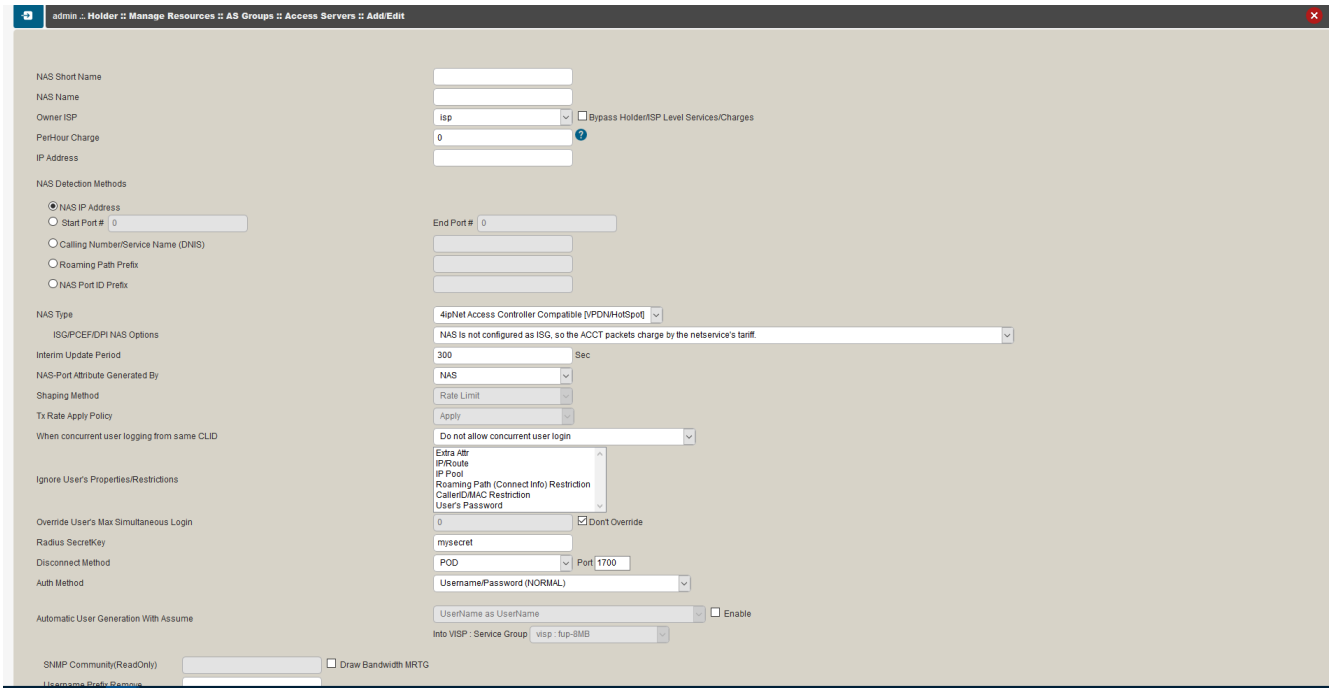
این گزینه برای مدیریت کلی بر روی VISP می‌باشد و می توان اجازه استفاده از IP-Pool و مدیریت آن را پس از انتخاب VISP مورد نظر در صفحه Edit VISP صادر کرد.

❖ تعریف RAS در لایه Holder

Netbill با Access Server ها برای اتصال کاربر به روش Hotspot و VPN کار می‌کند برای اینکار باید Access Server مورد نظر را در Netbill ایجاد کنید.

Holder → Manage Resources → AS Groups → Access Servers

برای تعریف RAS از قسمت Access Servers بر روی دکمه Add New کلیک کنید شکل زیر نمایش داده خواهد شد :



- RotaryPhone#

در این قسمت سر شماره ای که از آن NAS اتصال بر قرار خواهد شد را وارد کنید.

- NAS Name

نامی که NAS در شبکه به آن نام شناخته می‌شود.

- Owner ISP

ISP صاحب این NAS که آنرا برای استفاده در شبکه به اشتراک می گذارد.

- ✓ Bypass Holder/ISP Level Services

برای عدم محاسبه اعتبارها و شارژهای ایجاد شده در NET Services میباشد.

- PerHour Charge

هر NAS متعلق به یک ISP بوده و قیمت خرید هر ساعت سرویس را ISP مزبور مشخص کرده و در این قسمت وارد کنید. در این صورت به ازاء هر ساعت استفاده کاربران سیستم از این NAS به میزان این مقدار به حساب بستانکار ISP مزبور افزوده خواهد شد. هر ISP می‌تواند مقداری را به ازای هر ساعت استفاده از NAS خود از شرکت صاحب NetBill مطالبه کند که این مقدار در این فیلد مشخص خواهد شد.

- IP Address

آدرس IP را برای NAS مشخص کنید.

- NAS Detection Method

✓ NAS IP Address

با انتخاب این گزینه NAS با آی پی حقیقی خود شناسایی می شود.

✓ Start Port

✓ End Port

پورت شروع و پایان را برای RAS مشخص کنید. با استفاده از این گزینه می‌توانید از یک RAS برای دو یا چند سرشماره مختلف (بر حسب شماره شروع و پایان Port) استفاده نمود. مقدار صفر به معنای تمامی پورت‌ها خواهد بود.

✓ Calling Number/Service Name (DNIS)

اگر در Access Server خود چند لینک E1 با سر شماره های مختلف دارید می‌توانید از این گزینه با وارد کردن DNIS برای هر یک از شماره های فوق یک NAS جدا تعریف کرده و آنرا از سایر خطوط جدا نمایید.

✓ Roaming Path Perfix

با انتخاب این گزینه NAS با آی پی حقیقی خود و از مسیری که در تنظیمات Roaming مشخص شده شناسایی می شود.

✓ NAS Port ID Perfix

با انتخاب این گزینه NAS با آی پی حقیقی خود و از آی دی پورتی که در تنظیمات سرور مشخص شده شناسایی می شود.

- Type

از این قسمت نوع NAS را مشخص کنید.

- Interim Update Period

این قسمت را باید طبق تنظیمات Radius سرور خود انجام دهید که برای ارتباط با NetBill این مقدار را برابر ۳دقیقه قرار می‌دهیم ، در غیر این صورت کاربرهای شما از لیست Online User ها در نرم افزار Radius حذف می‌شوند ، در حالی که هنوز متصل هستند.

- NAS Port Attribute Generated By

✓ NAS

با انتخاب این گزینه عمل Attribute کردن Port ها را NAS انجام می دهد.

✓ Netbill

با انتخاب این گزینه Attribute کردن Port ها را Netbill انجام می دهد.

○ Shaping Method

✓ Rate Limit

به صورت Default اکثر روتر سیسکوها و میکروتیک ها از این روش استفاده می کنند که پارامترهای مشخص شده در سرویس گروپ، عینا با دستور rate_limit به راتر ارسال می شوند.

✓ PolicyMap

در بعضی از انواع روتر سیسکوها با ورژن بالا از این روش استفاده کنیم. ابتدا باید PolicyMap هایی با پارامترهای سرویس گروپ و با همان نام مثلا 512kb در راتر ایجاد کرده و سپس نت بیل ، عدد مربوط به Tx ، Rx را عینا بعنوان نام PolicyMap به سمت راتر می فرستد.

○ Remove Concurrent User when same user coming whit the same CLID

هنگامی که وضعیت یک نام کاربری خاص در نت بیل آنلاین است و کاربر دیگری با نام و مک آدرس مشابه قصد آنلاین شدن را دارد ، نتیجه میگیریم کاربر مورد نظر به علت اختلال در مسیر اتصال به نت بیل در وضعیت آنلاین باقی مانده است. با فعال سازی این فیلد نام کاربری که آنلاین مانده دیسکانکت و کاربر جدید آنلاین می شود.

○ Limit Users With Roaming Path Prefix (Connect Info)

با فعال بودن این گزینه کاربران تنها توسط Roaming Path مشخص شده در سرور می توانند به آن متصل شوند.

○ Start Port & End Port

پورت شروع و پایان را برای RAS مشخص کنید. با استفاده از این گزینه می‌توانید از یک RAS برای دو یا چند سرشماره مختلف (بر حسب شماره شروع و پایان Port) استفاده نمود. مقدار ۰ به معنای تمامی پورت‌ها خواهد بود.

- Radius SecretKey

تنظیمات کلمه Secret برای RADIUS

- Disconnect Method

✓ POD

اگر NAS مورد نظر شما این فیلد را پشتیبانی می‌کند مقدار آن را وارد کنید ، از این فیلد برای Disconnect کردن کاربران در بعضی از NAS ها استفاده می‌شود برای فعال سازی آن در روتر های سیسکو می‌توانید از دستور زیر استفاده کنید :

```
Router# aaa pod server auth-type any ignore server-key
```

بهتر است مقدار پیش فرض را برای آن برگزینید.

⚠ برای Disconnect کردن ، تنظیم صحیح گزینه Port الزامی است.

✓ Telnet

اگر NAS مورد نظر شما این فیلد را پشتیبانی می‌کند مانند اکسس سرور Huawei ، با قرار دادن نام کاربری و رمز عبور NAS در این فیلد می توان برای Disconnect کردن کاربران از آن استفاده کنید.

- Auth Method

می‌توانید راه های مختلف برای تعیین هویت (Authentication) مشترک را انتخاب نمایید.

✓ NORMAL

در این روش مشترک با Username تعریف شده در NetBill تعیین هویت می شود.

✓ ANI

در این روش CallerID / MAC مشترک به عنوان Username انتخاب می‌شود

✓ DID

در این روش شماره مقصدی که مشترک انتخاب و شماره گیری می‌کند به عنوان Username آن مشترک ذخیره می‌شود

- ✓ IN

با انتخاب این گزینه Rotary Phone# شما به عنوان Username ذخیره می‌شود

- ○ Automatic User Generation with

تولید خودکار کاربر هنگام اتصال (هر نام کاربری و رمز عبوری که برای بار اول وارد شود در سیستم بعنوان کاربر ایجاد می شود)

- ✓ Username

در این روش کاربر با نام کاربری ایجاد می شود.

- ✓ CallerID / MAC

در این روش کاربر با MAC ورودی آن ایجاد می شود.

- ✓ Into VISP : Service Group

پس از تولید خودکار کاربر ، آنرا به سرویس گروه مشخص شده متصل می کند.

- ○ SNMP Community(ReadOnly)

تنظیمات مربوط به استفاده از SNMP در حالت مانیتورینگ می‌باشد.

- ✓ Draw Bandwith MRTG

با انتخاب این گزینه در MRTG مقدار مصرف پهنای باند را نشان خواهد داد.

- ○ Username Perfix Remove

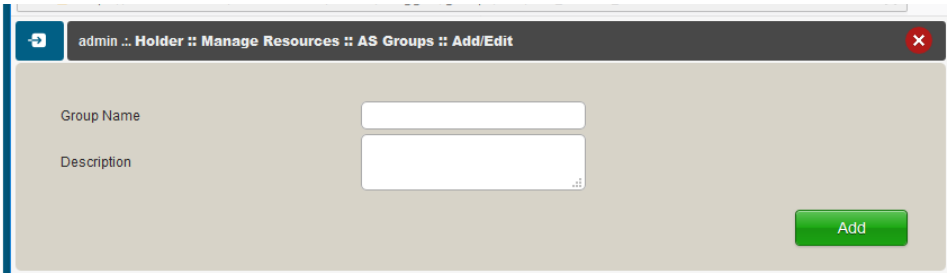
این گزینه برای نادیده گرفتن پیشوند کاربران می باشد که با وارد کردن حروف و یا اعداد مورد نظر در کادر این کار صورت میگیرد.

- ○ Username Suffix Remove

این گزینه برای نادیده گرفتن پسوند کاربران می باشد که با وارد کردن حروف و یا اعداد مورد نظر در کادر این کار صورت میگیرد.

- • AS Groups

در Netbill می‌توان برای Access Server ها گروه تعریف کرد و همزمان چند AS را به یک گروه اضافه کرد. این منو در Netbill این امکان را برای متصل کردن چند AS در مکان‌های مختلف ، برای استفاده از یک Netbill به ما می دهد.



- Group Name

در این قسمت نامی را برای گروه انتخاب کنید. این نام به عنوان گروه Ras های شما می‌باشد و چند Ras همزمان می‌توانند در این گروه باشند.

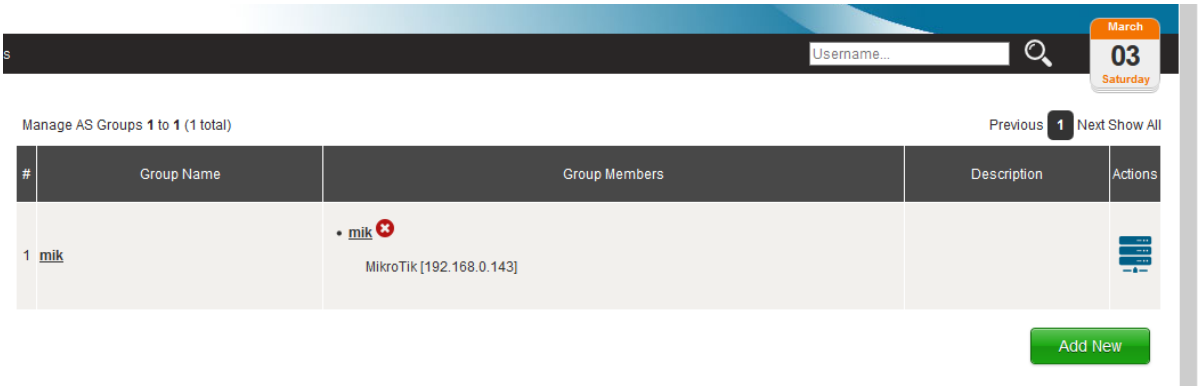
- Description

در اینجا توضیحات لازم برای گروه مورد نظر قرار می دهیم.

❖ انتصاب NAS ایجاد شده به Group

Ras ساخته شده را به AS Group متصل می‌کنیم.

Holder → Manage Resources → AS Groups



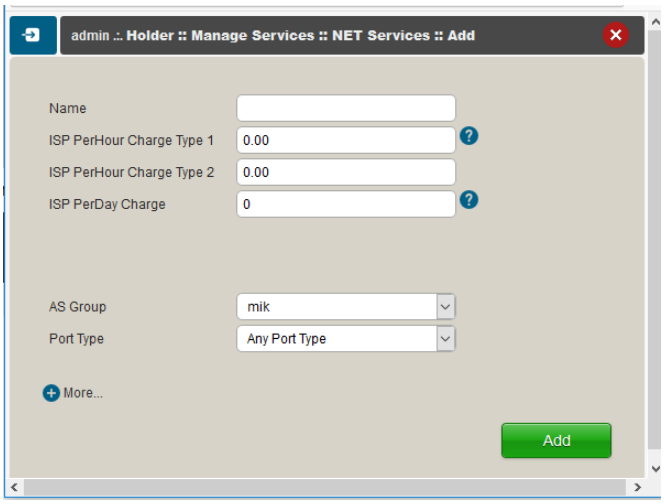
❖ ساخت سرویس در Manage Services در لایه Holder

در Netbill می‌توان از هر لایه ایی که تعریف می‌شود به میزان مشخصی مبلغ چه بر اساس ساعت و چه بر اساس مگابایت از لایه پایین‌تر کم کرد ، برای اینکار باید سرویسی را ایجاد و به آن مبلغ داد توجه داشته باشید چون در این مجموعه آموزش Netbill برای یک لایه ISP و VISP که متعلق به خودمان است می‌باشد و داشتن سرویس درNetbill برای لایه ها اجباری است و چون مبلغی از لایه

پایین‌تر ISP و VISP (که متغلق به خودمان است) نباید کم شود پس سرویسی به نام Default بدون مبلغ را تعریف و به ISP مربوطه متصل می‌کنیم.

وارد Manage Services و زیر مجموعه آن NET Services شده و با کلیک بر روی دکمه Add New صفحه ای مانند شکل زیر نمایش داده می‌شود که می‌توانید به تعریف سرویس جدید بپردازید.

Holder → Manage Services → NET Services



- Name

یک نام برای سرویس خود انتخاب کنید مثال : Default

- AS Group

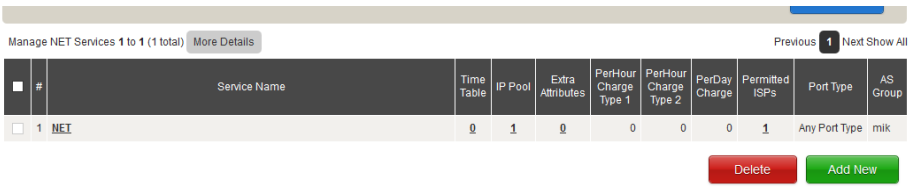
گروهی از RAS ها که می‌توانند از این سرویس استفاده کنند را مشخص کنید.

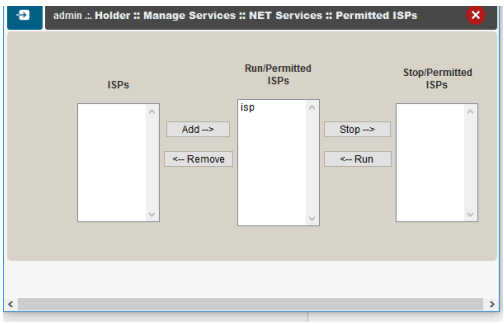
- Port Type

نوع پورتی که کاربران با آن متصل می‌شوند برای کاربران LAN باید گزینه Cable و یا Ethernet را انتخاب کنید.

باید توجه داشته باشید در هر زمان که سرویسی ساخته شد باید حتما این سرویس به ISP مورد نظر Permit شود.

برای انجام این کار روی Permited ISP کلیک کرده و نام ISP مورد نظر را انتخاب مطابق شکل زیر Add کنید.



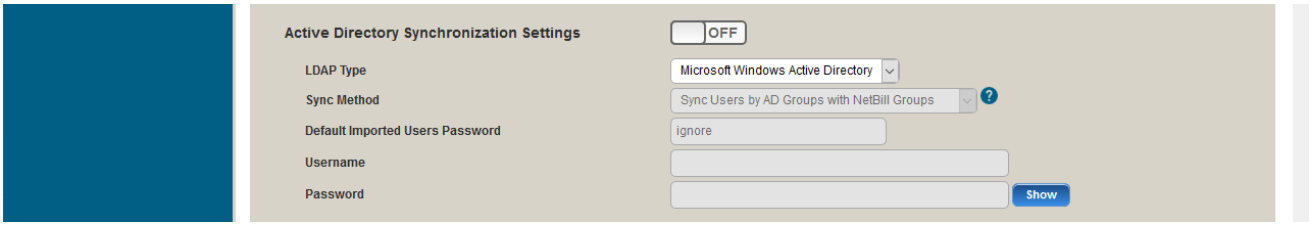


❖ تنظیمات Active Directory در Holder

برای شناساندن Netbill به AD باید وارد سرور AD شده و در بالاترین سطح کاربران آن یکuser و پسورد ایجاد کنید.

در مرحله بعد وارد Netbill در سطح HOLDER شده و در منو Options و زیر مجموعه آن System Profile وارد شده و این user ساخته شده را وارد نمایید.

Holder → Options → System Profile



○ Sync Method

از این گزینه نحوه همگام سازی با Active Directory را مشخص میکنیم که شامل سه راه برای اتصال می باشد:

✓ Sync Users by AD Groups with NetBill Groups

با انتخاب این گزینه و ایجاد گروه همنام با گروههای موجود در Active Directory در لایه VISP نام های کاربری موجود در AD بصورت خودکار وارد گروه ها می شوند.

توجه کنید که گروه های ایجاد شده در NetBill باید دقیقآ همنام با گروه های موجود در AD باشند.

✓ Sync Users by Single AD OUs with NetBill VISPS

این گزینه برای ایجاد کاربر با OU های مختلف استفاده می شود ، با انتخاب این گزینه و ایجاد VISP با نام OU موجود در AD کاربران آن OU بصورت خودکار به یک گروه با نام Default Service Group در همان VISP ایجاد می شوند.

✓ Sync Users by Multiple AD OUs with NetBill VISPS

این گزینه هم مشابه گزینه دوم می باشد با این تفاوت که به شما این امکان را می دهد تا VISP را با نام دلخواه خود ایجاد کرده و OU های موجود در AD را به VISPهای خود اختصاص دهید.

- IP Address

آدرس IP سرور AD را وارد نمایید.

- Domain Name

آدرس دامنه AD را وارد نمایید.

✓ Username

نام کاربری که در AD برای همگام سازی با NetBill را ایجاد نمودید وارد نمایید.

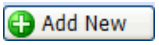
✓ Password

کلمه عبوری که در AD برای همگام سازی با NetBill را ایجاد نموده اید وارد نمایید.

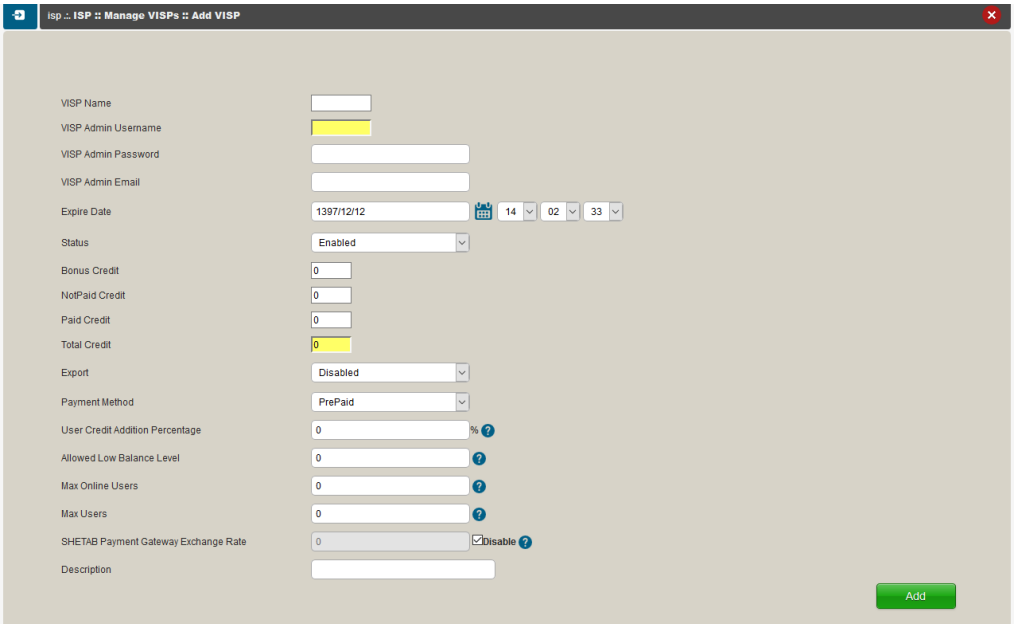
❖ ایجاد VISP در لایه ISP

در لایه ISP شما می‌توانید VISP های مختلف را ایجاد و به مدیران دفاتر دیگر خود نام کاربری VISP ها را داده تا آن‌ها نیز از این Accounting به صورت مرکزی استفاده نمایند.

ISP → Manage VISPs

از این قسمت می‌توانید VISP جدیدی برای خود تعریف کنید برای تعریف یک VISP جدید همانند تعریف یک ISP در سطح Holder بر روی علامت 

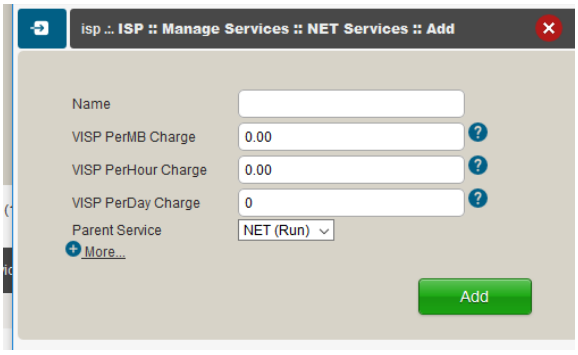
کلیک کنید، کلیه موارد موجود همانند تعریف ISP خواهد بود.



❖ ایجاد سرویس در لایه ISP برای VISP زیر مجموعه

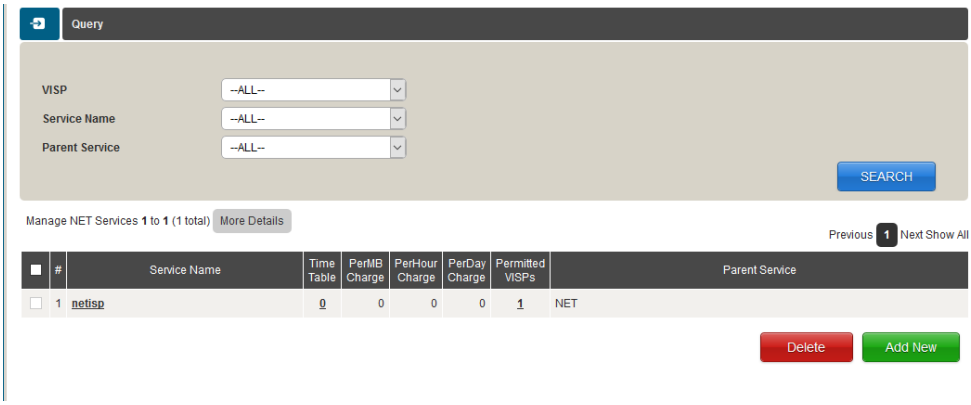
برای اضافه کردن سرویس جدید بر اساس سرویسی که می‌خواهید داشته باشید روی Add New کلیک کنید (برای سرویس اینترنت گزینه NET Services)

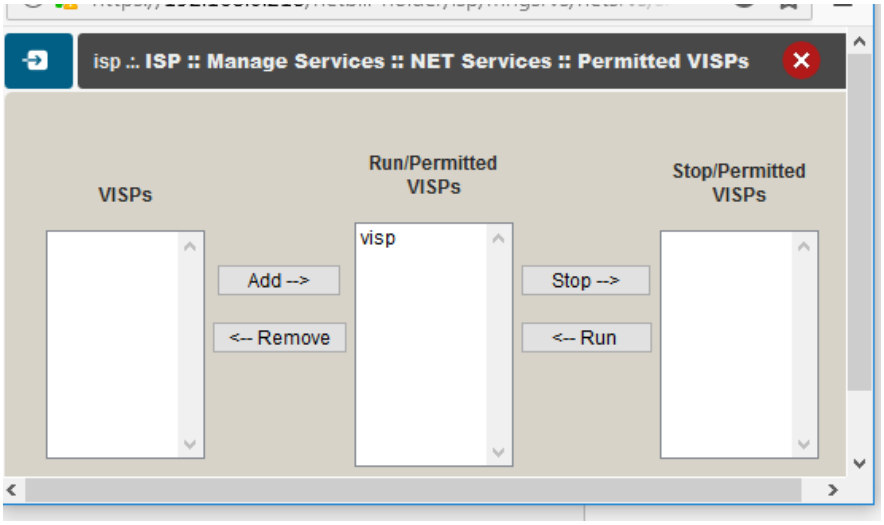
ISP → Manage Services → NET Services



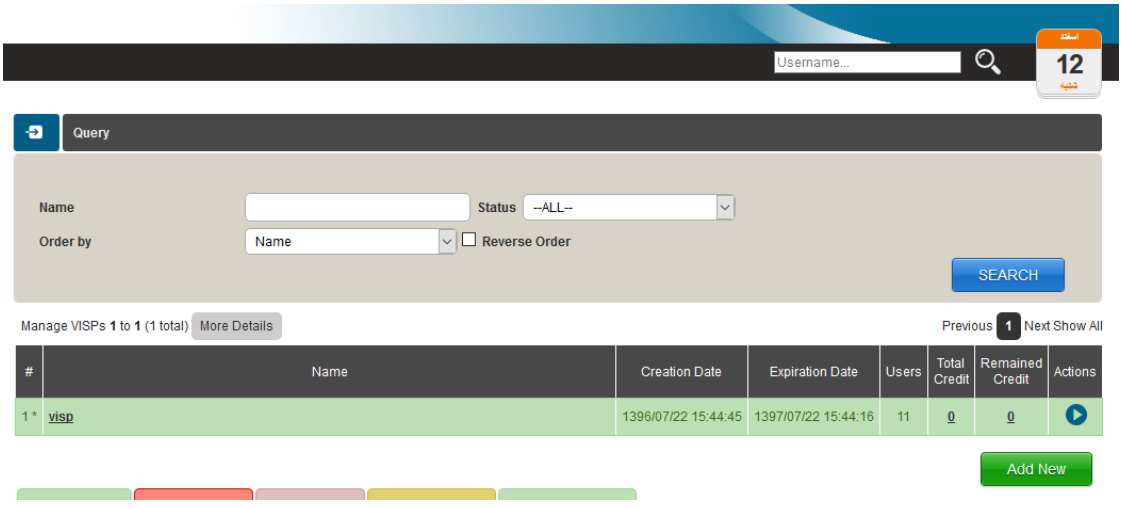
توجه داشته باشید چون برای LAN Acounting خود این گزینه را می‌سازید نیازی به وارد کردن مبلغ نیست و باید مبالغ را صفر وارد کنید.

با ایجاد سرویس صفحه زیر را می‌بینید که مشخصات سرویس ساخته شده را نمایش میدهدحال باید سرویس ساخته شده را به VISPساخته شده Permit کنید برای این کار بر روی Permited VISPs کلیک می‌کنید و VISP مورد نظر خود را به این سرویس اضافه می‌کنید.





برای وارد شدن در سطح VISP می‌توانید با کلیک بر روی Login As با آن سطح دسترسی وارد شوید.

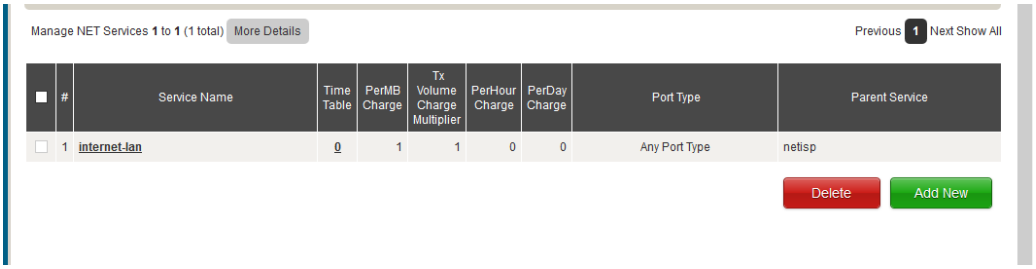


❖ ایجاد سرویس در VISP برای Permit به Service Group

درلایه VISP آخرین سرویس ساخته می‌شود و این سرویس ساخته شده در آخرین مرحله به Service Group ها متصل می‌شود.

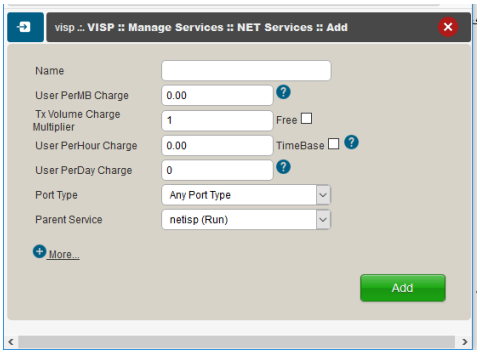
از این قسمت می توانید با توجه به سرویس اختصاص داده شده از طرف VISP برای Service Group های خود سرویس جدیدی تعریف کنید، سرویس یا سرویس‌های اختصاص داده شده توسط VISP را می‌توانید از قسمت Parent Services مشاهده نمایید.

VISP → Manage Services → NET Services



برای اضافه کردن سرویس جدید بر اساس سرویسی که می‌خواهید داشته باشید روی Add New کلیک کنید (برای سرویس اینترنت گزینه NET Service را انتخاب کنید)

در این قسمت می‌توانید با پر کردن گزینه‌ها مقدار شارژی که باید بر اساس ساعت یا حجم از VISP شما کسر شود و همینطور نام سرویس را انتخاب نمایید.



توجه داشته باشید برای LAN Serivce Groups نیازی به وارد کردن مبلغ نیست و می توانید مبالغ را صفر وارد کنید.

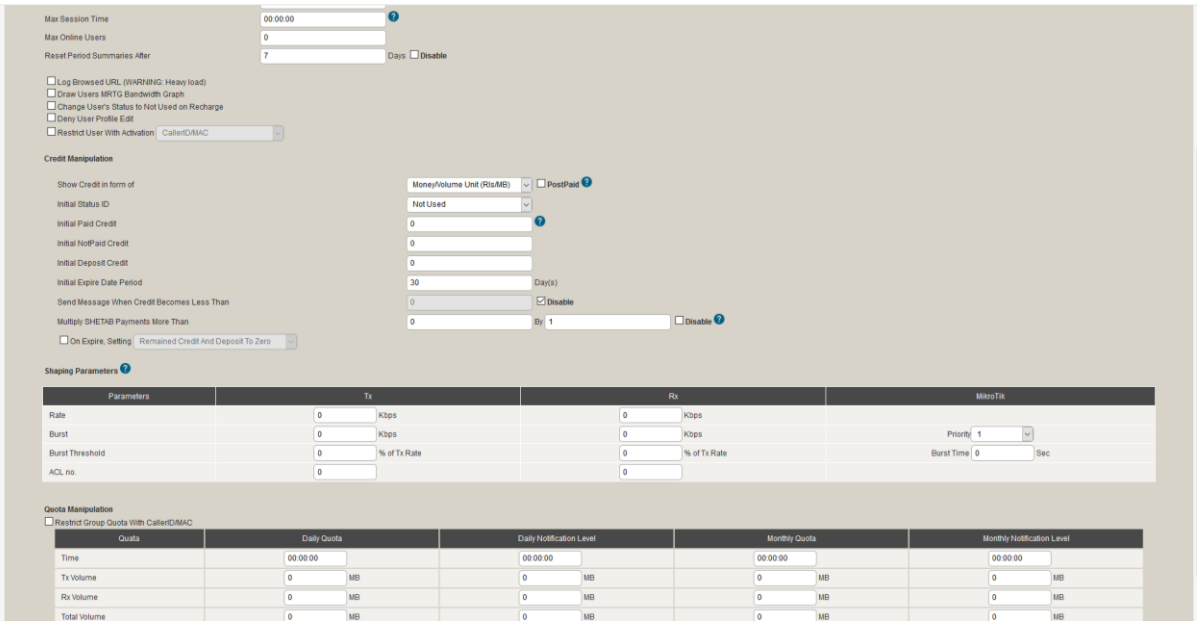
❖ ایجاد Service Group برای انتصاب کاربران به این گروه‌ها

عمده کار اصلی Admin شبکه‌ها با این قسمت می‌باشد در این قسمت با ایجاد گروه‌ها و اختصاص کاربر به این گروه‌ها می‌توانید تعیین کنید که کدام کاربر چه میزان از پهنای باند را مصرف یا چقدر از Bandwith اینترنت شما را مصرف کند.

از این قسمت می‌توانید برای سرویس‌های خود یک گروه تعریف کنید، با کلیک بر روی دکمه Add New می‌توانید به تعریف گروه جدید بپردازید.

VISP → Manage Services → Service Groups

با کلیک بر روی دکمه More می‌توانید اطلاعات بیشتری را مشاهده کنید.



- Name

انتخاب نام برای یک گروه

- Description

توضیحات ویژه برای این گروه

- Type

با انتخاب مدل سرویس Log هایی که در CRA ساخته می‌شود به تفکیک بوده و قابل تشخیص خواهند بود .

- Authenticate Method

نوع‌های Authenticate را می‌توانید مشخص کنید چون در Netbill شما می‌توانید انواع Radius را داشته باشید .

از این قسمت می‌توانید انتخاب کنید که خود Netbill ، Radius باشد یا کاربران از Active Directory خوانده شوند و یا اینکه Radius دیگری را انتخاب کنید.

- Idle TimeOut

مدت زمان بیکار بودن سرویس گروه

- ✓ Max Session Time

حداکثر زمان مجاز در هر اتصال

- Show Credit in form of

در این قسمت مشخص می‌کنید که اعتبار کاربران بر اساس پول نمایش داده شود یا بر اساس زمان.

- Initial Paid Credit

مقدار مبلغ اولیه ایی که پرداخت شده و برای گروه در نظر گرفته می‌شود.

- Initial NotPaid Credit

مقدار مبلغی که به گروه اختصاص داده می‌شود ولی این مبلغ پرداخت نشده است و به حساب بدهکاری گروه و زیر مجموعه‌ها که شامل مشترکان می‌شود زده می‌شود.

- Initial Deposit Credit

مقدار اعتباری که به گروه به عنوان هدیه داده می‌شود.

- Initial Expire Date Period

بعد از اولین ارتباط این گروه ظرف مدت زمان مشخص Expire می‌شود.

- ✓ Log Browsed URL (WARNING: Heavy load)

با انتخاب این گزینه Log کاربران در مورد Browse سایت‌ها در قسمت Report ذخیره و نمایش داده می‌شود

توجه داشته باشید با تیک زدن این قسمت ، بار بالایی روی سرور و روتر شما گذاشته می‌شود.

- ✓ Set Remained Credit to zero on expire

با زدن این تیک بعد از Expire شدن این گروه مقدار باقیمانده اعتبار این گروه صفر می‌شود.

✓ Restrict Group Limitations With CallerID

شما می توانید با زدن این تیک داخل گروه یک USERNAME ایجاد کنید و بعد از ایجاد با این کاربر مقدار محدودی اعتبار دهید و بعد از اعتبار یعنی با این USERNAME همه می توانند اتصال پیدا کنند ولی هر کدام از Client ها فقط می توانند یکبار از این اعتبار استفاده کنند. این گزینه معمولا برای مواقعی انتخاب می شود که شما بخواهید اکانتی را به صورت تستی برای تعدادی برای مقدار محدود ایجاد کنید

✓ Deny User Profile Edit

با زدن این تیک مشترک نمی تواند Profile خود را ویرایش نماید.

✓ Restrict User With Activation CallerID

با زدن این تیک MAC Address یا Caller ID ایی که اولین بار مشترک با رمز خود وصل می شود ثبت شده بنابراین مشترک دیگر نمی تواند با همین رمز از محل دیگری اتصال پیدا کند.

✓ Priority

یک اولویت مشخص می کنید

✓ Tx Rate

سرعت ارسال را مشخص می کند

✓ Rx Rate

سرعت دریافت را مشخص می کند

✓ Min Tx Rate

می توانید با نوشتن مقدار در این گزینه انتخاب کنید که مقدار سرعت ارسال تضمین شده چقدر باشد.

✓ Min Rx Rate

می توانید با نوشتن مقدار در این گزینه انتخاب کنید که مقدار سرعت دریافت تضمین شده چقدر باشد.

✓ TX Burst

مقدار این فیلد به کاربر این اجازه را می‌دهد که مقداری بیشتر از TX Rate را برای مدت زمانی که در فیلد Burst Time مشخص شده ، به ارسال اطلاعات بپردازد.

✓ RX Burst

مقدار این فیلد به کاربر این اجازه را می‌دهد که مقداری بیشتر از RX Rate را برای مدت زمانی که در فیلد Burst Time مشخص شده ، به دریافت اطلاعات بپردازد. بنابراین با استفاده از این گزینه می‌تواند سرویس تعریف کنید که کاربران آن سرویس صرفا در صورتی که برای مدت زمان کوتاهی نیاز به پهنای باند اضافی داشته باشند ، بتوانند از آن استفاده کنند و در غیر اینصورت ، پهنای باند اضافی در اختیار آنان قرار داده نخواهد شد.

✓ Burst Time

مدت زمانی که کاربر می‌تواند از فیلد های Burst استفاده کند.

✓ Daily tx Volume

حداکثر میزان ارسال اطلاعات بر حسب مگابایت در یک روز

✓ Daily Rx Volume

حداکثر میزان دریافت اطلاعات بر حسب مگابایت در یک روز

✓ Daily Connection Time

حداکثر زمان اتصال در یک روز

✓ Monthly tx Volume

حداکثر میزان ارسال اطلاعات بر حسب مگابایت در یک ماه

✓ Monthly Rx Volume

حداکثر میزان دریافت اطلاعات بر حسب مگابایت در یک ماه

✓ Monthly Connection Time

حداکثر زمان اتصال در یک ماه

✓ Idle timeout

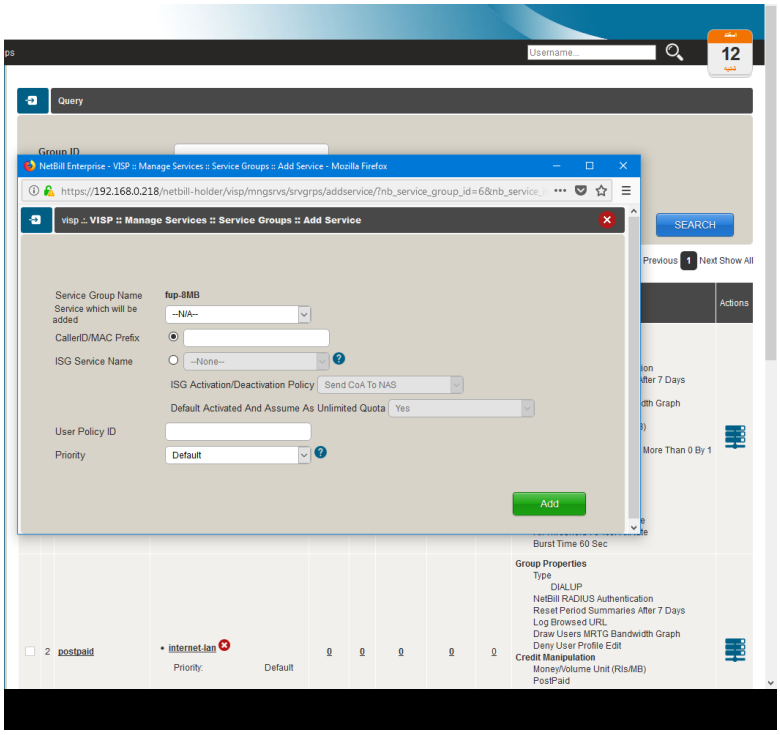
حداکثر مدت زمان بلا استفاده

✓ Max Online Users

حداکثر تعداد کاربران همزمان

اگر از AD[۳] استفاده می‌کنید باید در قسمت Authenticate Method نوع RADIUS را AD انتخاب و در فیلد های بعدی IP و Domain را وارد نمایید.

پس از تعریف گروه از قسمت Add Service می‌توانید سرویس‌های مورد علاقه خود را به گروه اضافه کنید.

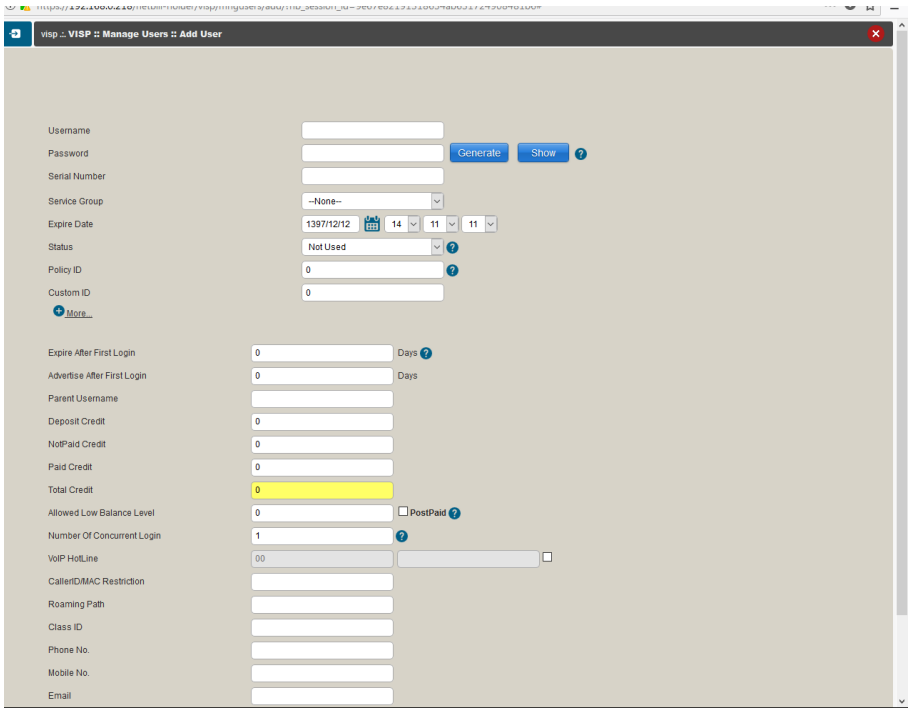


[۳] Active Directory

❖ ایجاد کاربر در لایه VISP :

VISP → Manage Users → Add New

در این قسمت می‌توانید با زدن گزینه Add New شروع به ایجاد کاربر کنید.



- Username

در این قسمت نام کاربری را وارد نمایید

- Password

دراین قسمت کلمه عبور را وارد نمایید .

اگر جای کلمه عبور کلمه import را بزنید اولین کلمه ایی که کاربر به عنوان کلمه رمز وارد کند جای کلمه عبور ذخیره می‌شود اگر ignore را وارد کنید کلمه عبور برای کاربر دیگر لازم نیست

- Service Group

در این قسمت گروه مورد نظر خود را وارد کنید

- Expire Date

تاریخ انقضاء کاربر را مشخص کنید

- Status

وضعیت کاربر که به صورت پیش فرض Not Used پیشنهاد می گردد .

- Expire After First Login

تعداد روز معتبر بودن کاربر بعد از اولین اتصال

- Bonus Credit

میزان اعتبار هدیه به کاربر را در این قسمت وارد می‌کنیم

- NotPaid Credit

میزان اعتباری که به ISP اختصاص داده شده ولی حساب آن پرداخت نشده .

- Paid Credit

میزان اعتباری که به ISP اختصاص داده شده ولی حساب آن پرداخت نشده

- Total Credit

جمع میزان اعتبار پرداخت شده و پرداخت نشده .

- Allowed Low Balance Level

مقدار اعتباری که به کاربر اجازه می‌دهد منفی بشود.

- Number Of Concurent Login

در این قسمت با وارد کردن عدد تعداد افرادی که با یک User همزمان با هم می‌توانند وصل شوند را انتخاب کنید.

- CallerID/MAC Restriction

Username این کاربر بعد از اولین اتصال بر روی MAC و یا CallerID قفل می‌شوند.

- Mobile No.

شماره تلفن همراه کاربر

- Email

آدرس ایمیل کاربر

- Description

در این قسمت توضیحاتی که برای کاربران وجود دارد را می‌توانید وارد کنید .

❖ Import User

از این قسمت می توانید برای اضافه کردن دسته جمعی گروهی از کاربران به سیستم استفاده کنید.

برای این کار بر روی عبارت Import User کلیک کرده ، صفحه آن باز خواهد شد از قسمت Browse فایل خود را انتخاب و از قسمت File Format فرمت فایل خود را مشخص کنید ، با کلیک بر روی Next در صفحه بعد، فیلد های فایل شما به نمایش در خواهد آمد.

در قسمت بعد فیلد های فایل را نمایش داده و از شما می‌خواهد که از منوی مقابل آن نوع این فیلد را مشخص کنید.

برای مثال در فایلی که ما وارد[۴] کردیم ، فیلد اول برابر نام کاربری[۵] فیلد دوم برابر کلمه عبور[۶] و فیلد سوم مقدار اعتبار کاربر بوده است؛

با انتخاب موارد فوق از از کشوی مقابل آن به صفحه بعدی می‌رویم.

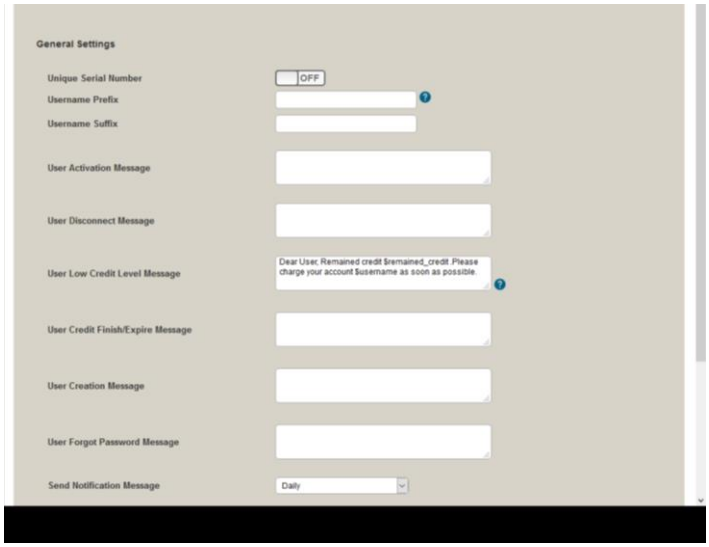
در صفحه بعد اطلاعات اضافی را مانند اعتبار کاربر، تاریخ انقضا و ... می‌توانید مشخص کنید.

و در آخر کاربران به سیستم Import خواهند شد.

اگر از AD[۷] استفاده می‌کنید نیازی به ایجاد کردن کاربر نیست کاربران به صورت اتوماتیک داخل گروه‌ها ایجاد می‌شود .

VISP → Options → VISP Profile

[۴] Import
[۵] UserName
[۶] Password
[۷] Active Directory



- Username Prefix

هنگام Add User این مقدار بصورت خودکار به ابتدای نام کاربری اضافه خواهد شد.

- Username Suffix

هنگام Add User این مقدار بصورت خودکار به انتهای نام کاربری اضافه خواهد شد.

دیگر گزینه های موجود بر روی منو همانند سطح Holder می‌باشد.

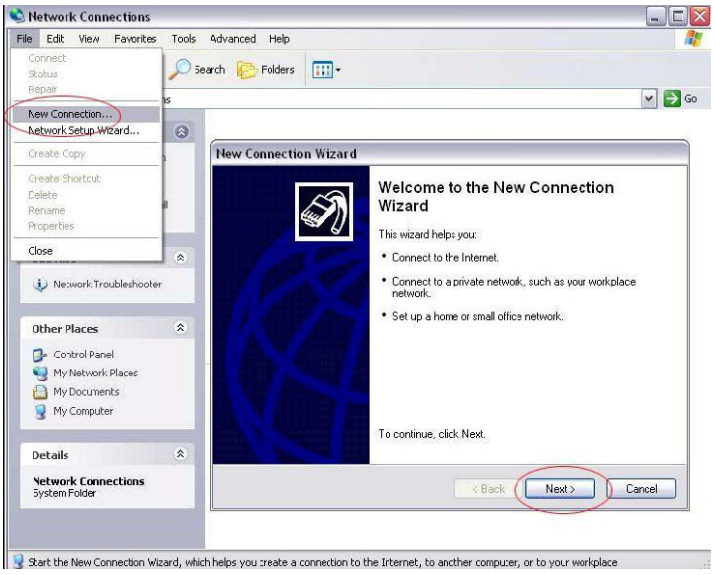
- **طریقه اتصال به نت بیل با استفاده از PPPoE و PPTP**

ساخت PPPoE Connection بر روی windows XP

۱- برای ساخت connection PPPoE روی دکمه start کلیک کرده سپس گزینه Control Panel را انتخاب کنید

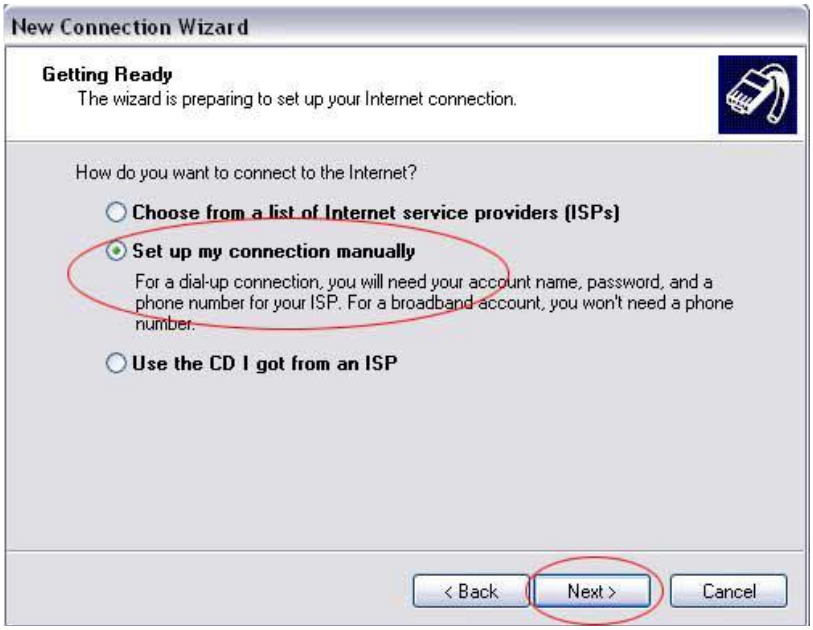
۲- سپس روی گزینه Network Connection دوبار کلیک کنید.

۳- از منوی فایل روی گزینه Create a new Connection کلیک کنید،صفحه New Connection Wizard باز می شود سپس دکمه Next را بزنید.

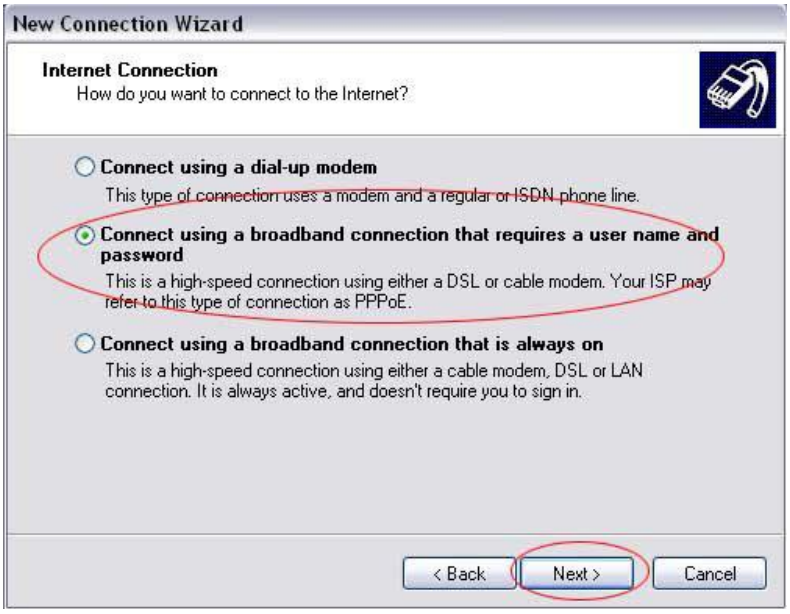


۴- Connect to the Internet را انتخاب و Next را بزنید.

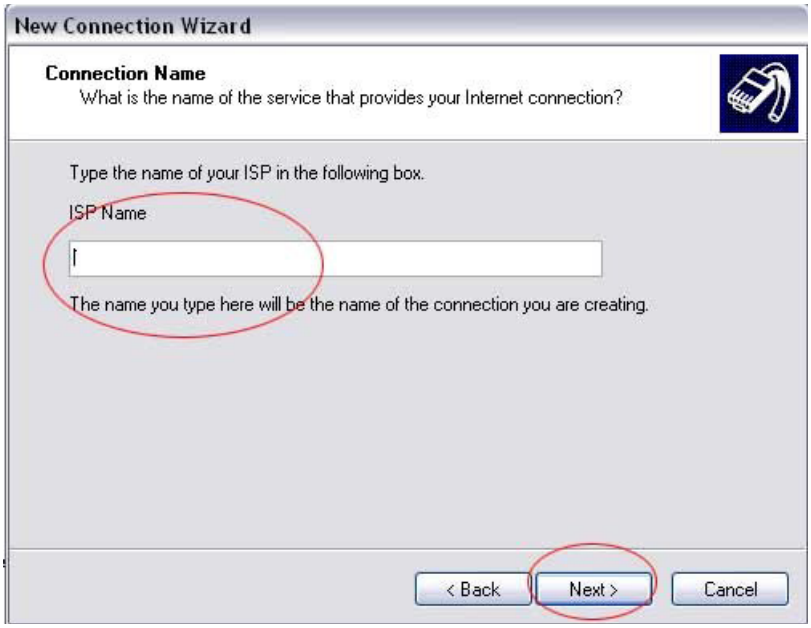
۵- Setup my connection manually را از بین گزینه ها انتخاب و next را می زنیم.



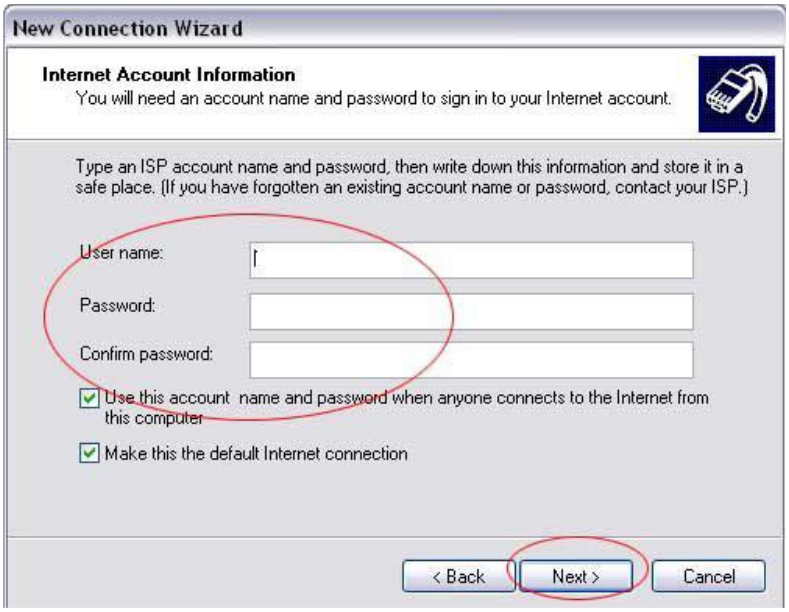
۶- سپس گزینه connect using a broadband را از بین گزینه ها انتخاب کرده و Next می زنیم.



۷- در ISP name نام شرکت یا هر نام دلخواه دیگر را وارد کنید.



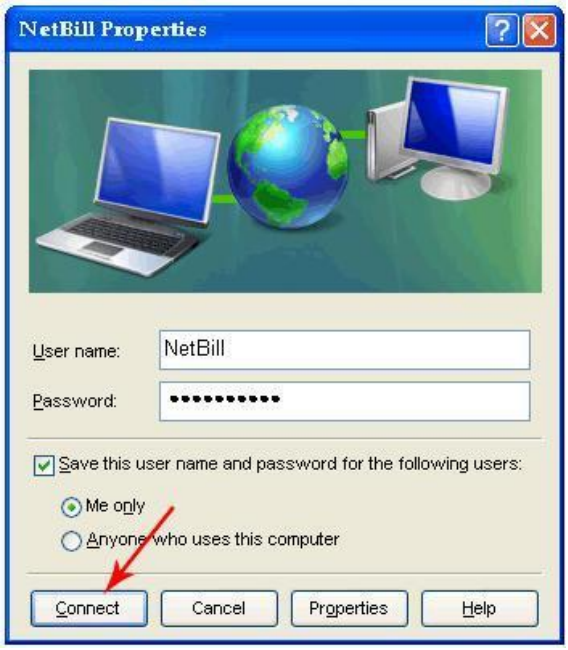
۸- username و passwordخود را وارد نمایید و در password confirm جهت تایید password را دوباره وارد نمایید.



۹- در صورت تمایل می‌توانید گزینه‌ی مربوط به ایجاد Shortcut (میانبر) برروی Desktop را فعال کنید تا میانبری از کانکشن برای دسترسی سریعتر ایجاد شود.

با زدن دکمه Finish کانکشن شما ساخته می شود.

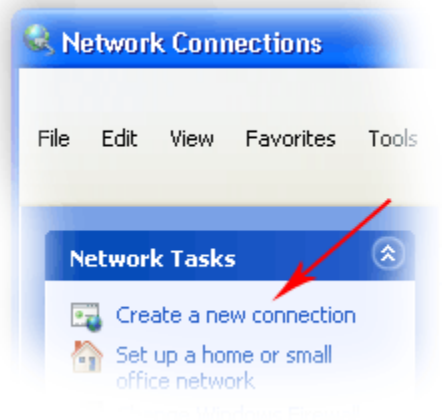
یوزر (شناسه) و پسورد (رمز عبور) که دریافت کرده‌اید را وارد کرده و برروی Connect کلیک کرده و از مزایای این سرویس استفاده کنید.



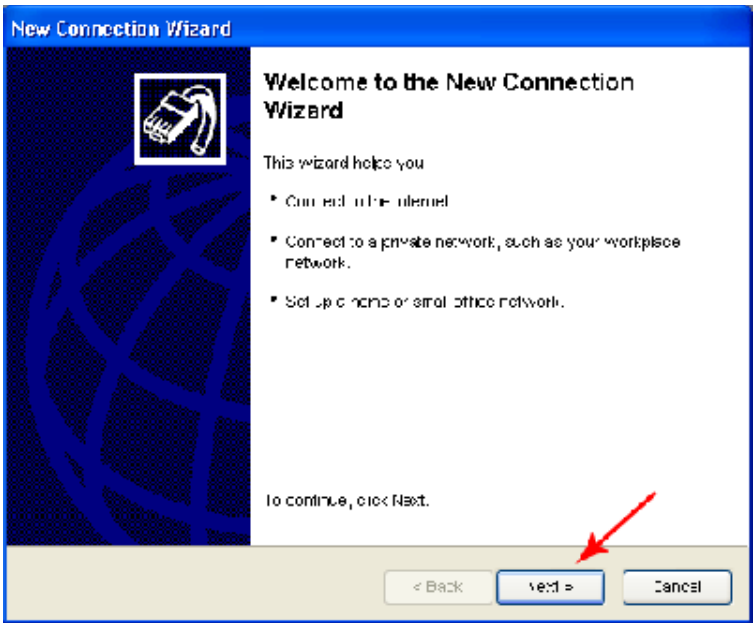
ساخت PPTP Connection بر روی windows XP

برای VPN (PPTP) لازم است که یک کانکشن ساخته شود تا با نام کاربری و رمز عبوری که در اختیار شما قرار داده می‌شود، بتوانید کانال ورودی خود را به اینترنت منتقل نمائید.

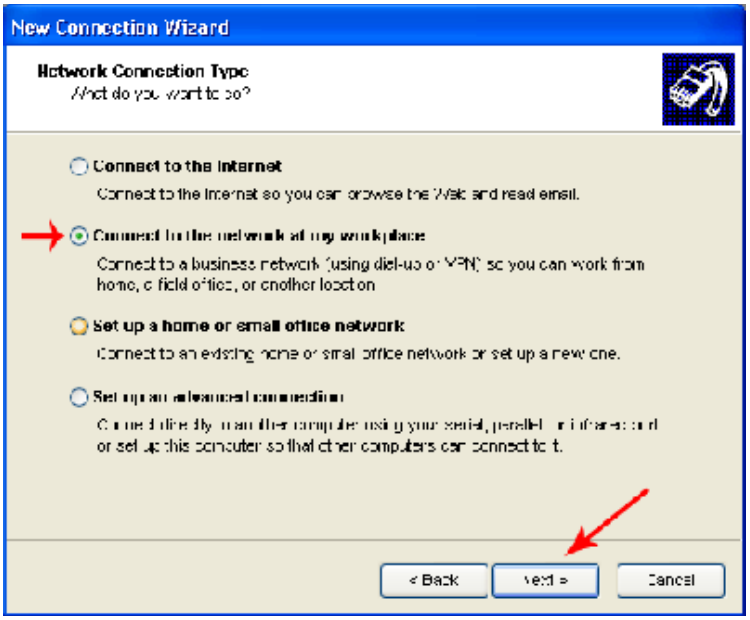
ابتدا به Control Panel و سپس به Network Connections بروید و برروی Create a new connection کلیک کنید



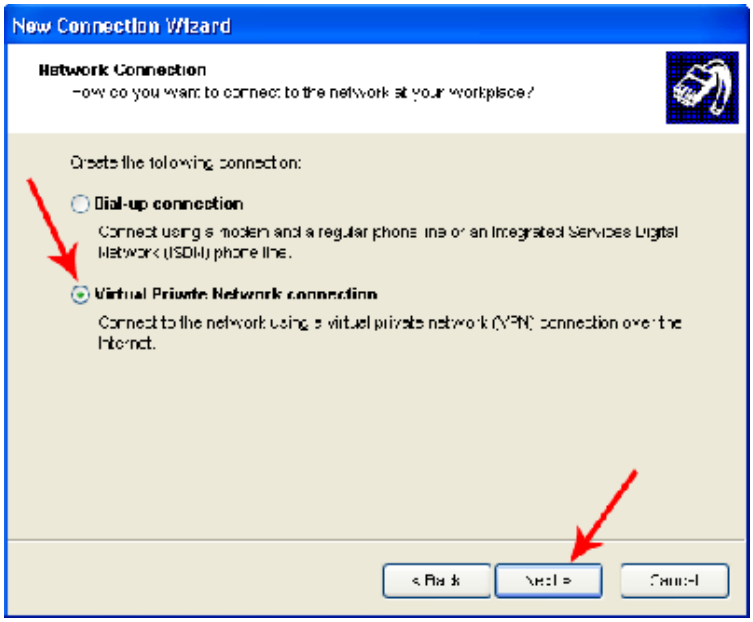
در پنجره‌ی باز شده روی Next کلیک کنید



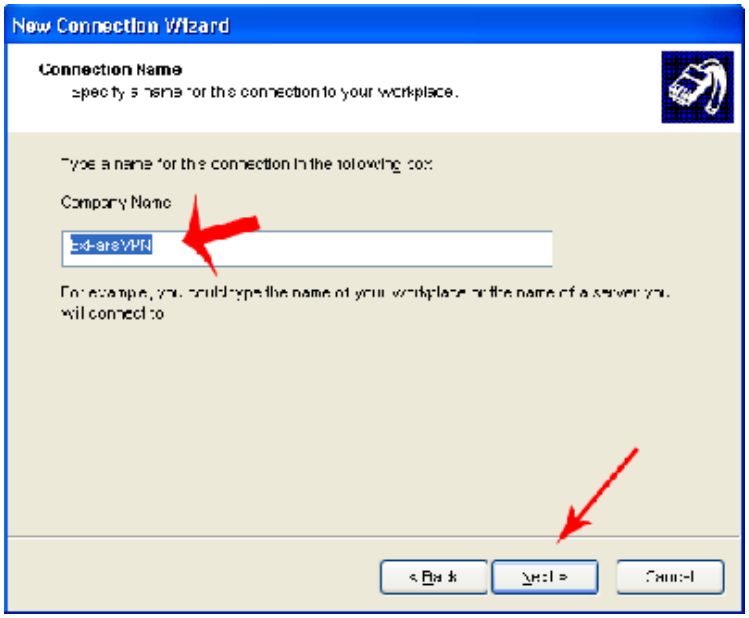
همانند شکل گزینه دوم را انتخاب کرده و برروی Next کلیک کنید.



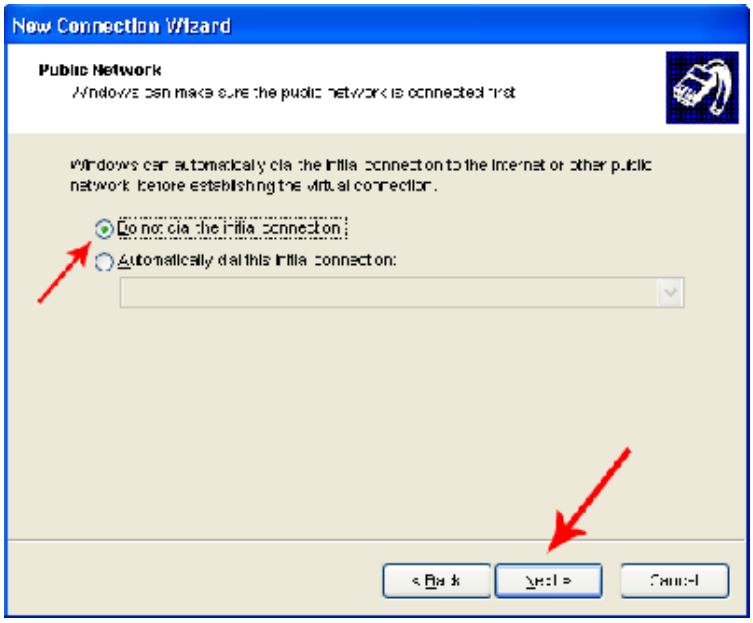
در این مرحله نیز گزینه دوم (VPN) را انتخاب کرده و برروی Next کلیک کنید



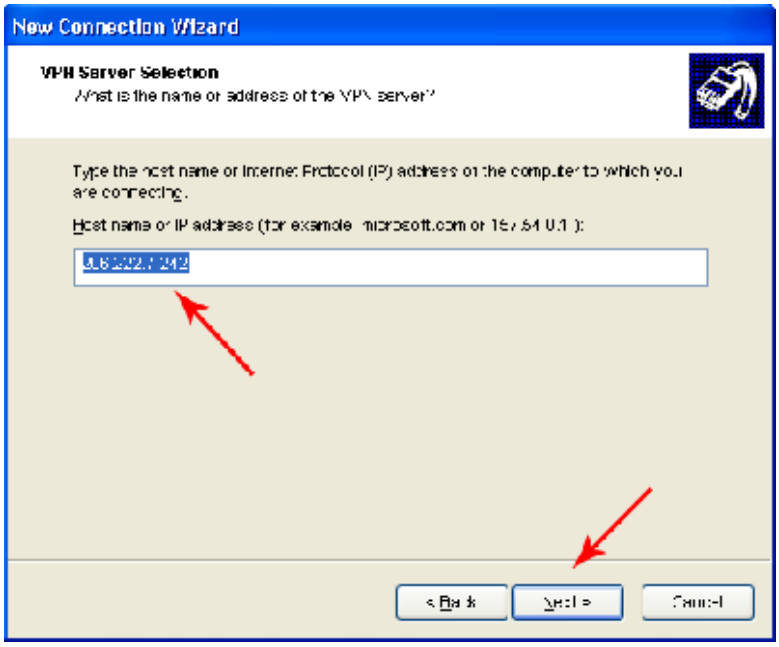
نام دلخواه همانند شکل وارد کرده و برروی Next کلیک کنید.



در صورتیکه پنجره ی زیر را مشاهده کردید گزینه‌ی Do not initial connection را انتخاب کرده و بروی Next کلیک کنید.

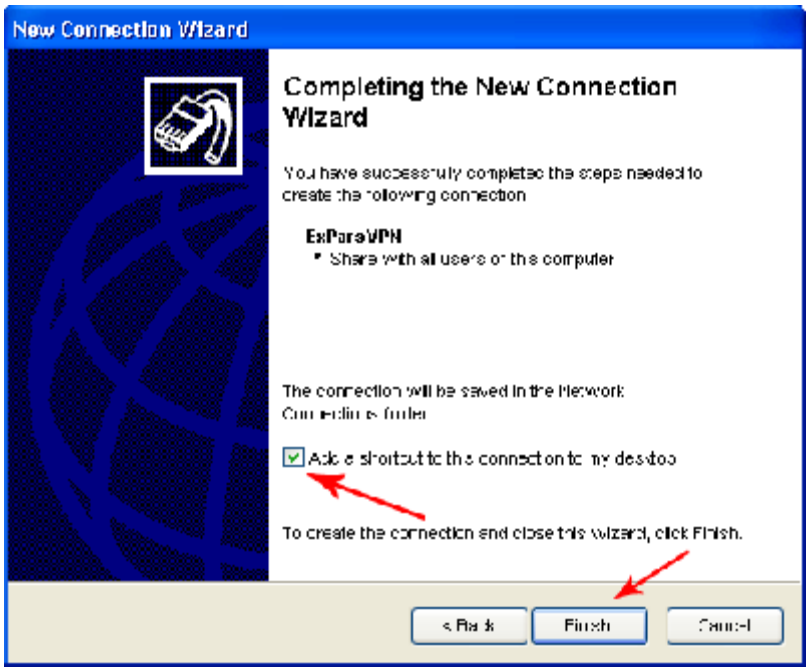


مطابق شکل IP سرویس دهنده NetBill را وارد کنید.

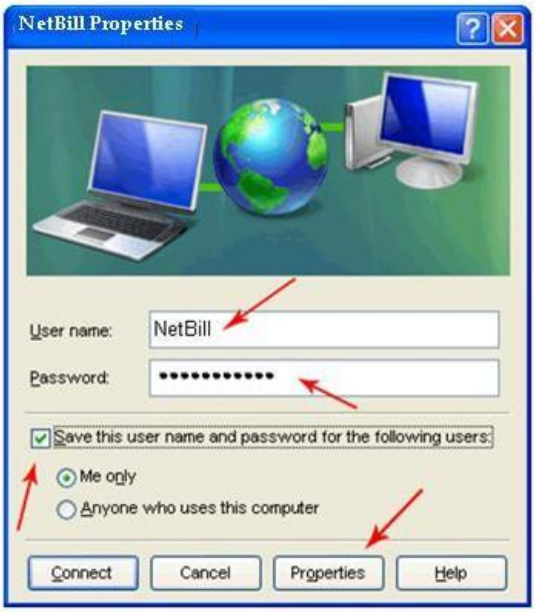


در این مرحله بر روی Finish کلیک کنید تا پنجره‌ی کانکشن ایجاد شده باز گردد.

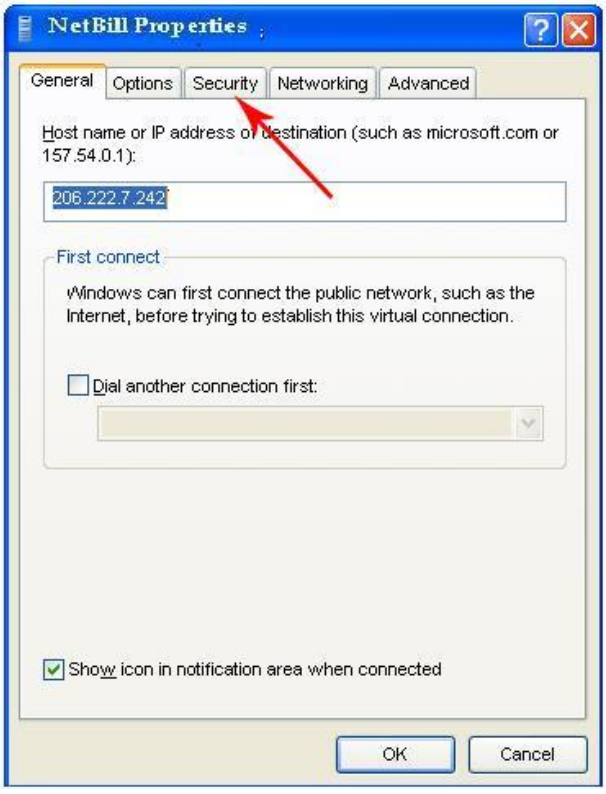
در صورت تمایل می‌توانید گزینه‌ی مربوط به ایجاد Shortcut (میانبر) برروی Desktop را فعال کنید تا میانبری از کانکشن برای دسترسی سریعتر ایجاد شود.



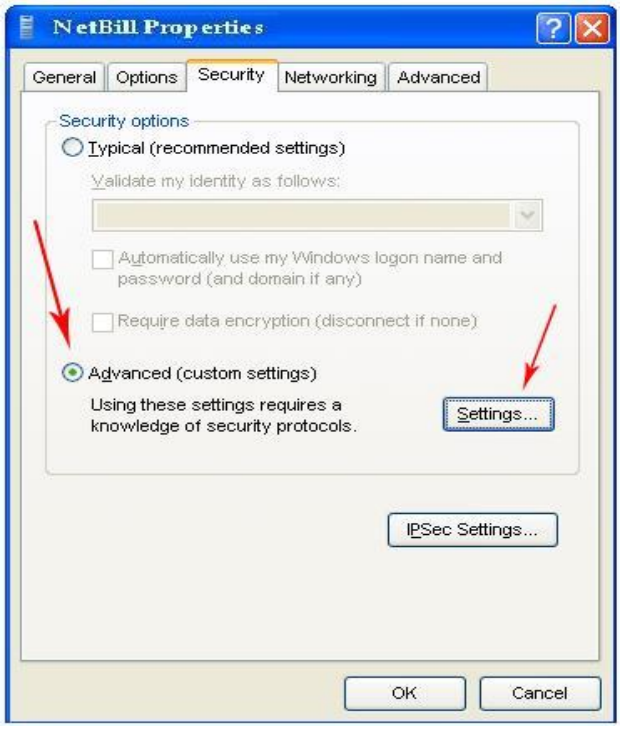
یوزر (شناسه) و پسورد (رمز عبور) که دریافت کرده‌اید را وارد کرده و گزینه‌ی مربوط به ذخیره این اطلاعات را فعال کنید و برروی Properties کلیک کنید.



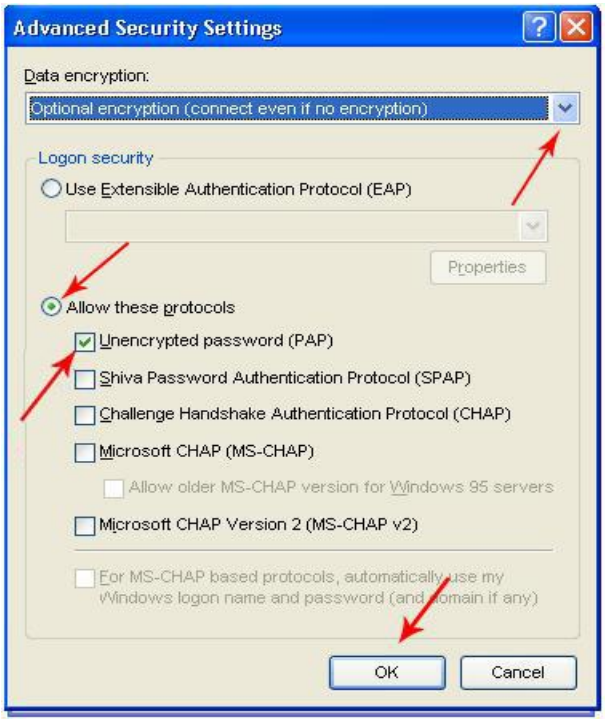
همانند شکل به بخش Security بروید.



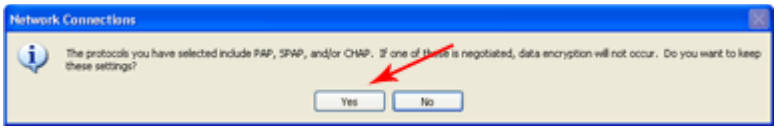
گزینه‌ی Advance را فعال کرده و برروی Settings کلیک کنید.



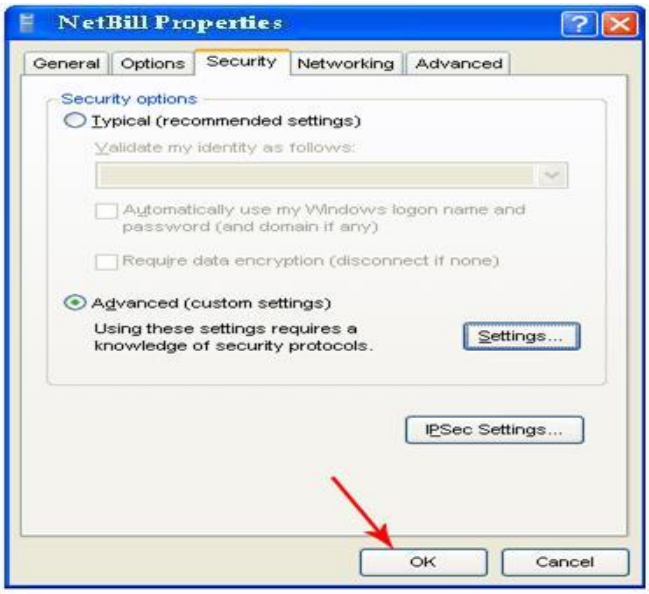
از منوی Data encryption همانند شکل Optional encryption را انتخاب کرده و گزینه‌ها را همانند شکل زیر تغییر داده و برروی OK کلیک کنید.



در سئوال پرسیده شده برروی Yes کلیک کنید.



درنهایت برروی Ok کلیک کنید تا تغییرات اعمال شود.



پس از برقراری ارتباط با اینترنت برروی Connect کلیک کرده و مزایای این سرویس استفاده کنید.

استفاده از **dialler** قاصدک

مصرف کننده گرامی:

حسن انتخابتان را در استفاده از نرم افزار دایلر قاصدک تبریک میگوئیم و خوشحالیم که توانسته ایم نرم افزاری پیشرفته منطبق با نیازهای مدیران و کاربران ایرانی عرضه کنیم. از نرم افزار دایلر قاصدک میتوانید برای اتصال به شبکه هایی که بر پایه Windows Connection بنا نهاده شده اند، استفاده کنید. نرم افزار دایلر قاصدک برای دو گونه از کاربران طراحی شده است:

- **کاربران خدمات ADSL/WireLess سرویس دهندگان اینترنت پرسرعت**
- **کاربران LAN در سازمانها و موسسات**

تذکر: برای استفاده کاربران از این نرم افزار لازم است ابتدا مدیران شبکه ها و سرویس دهندگان تنظیماتی را در سمت Server انجام دهند تا کاربران آنها بتوانند از این نرم افزار

استفاده نمایند. بدون انجام این تنظیمات، استفاده از دایلر قاصدک برای کاربران ممکن نخواهد بود.

مدیران شبکه ها و سرویس دهندگان در ابتدا لازم است یک **WebServer** که (بدون نیاز به اتصال و بطور همیشگی در دسترس کاربران قراردارد) آماده کرده و فولدر **qsdk_dialer** را در **WebRoot** آن ایجاد کنند. سپس فایلهای زیر را در این فولدر قراردهید.:

- **/qsdk_dialer/qsdk_dialer.exe**
- **/qsdk_dialer/config.xml**
- **/qsdk_dialer/connetion.cnf**

❖ فایل **qsdk_dialer.exe**: در ابتدا، آخرین ورژن فایل اجرائی نرم افزار دایلرقاصدک در این پوشه قرارداده میشود. در هر بار اجرای نرم افزار دایلر توسط کاربر، ورژن فایل موجود در سمت کاربر با ورژن نسخه موجود در این فولدر مقایسه شده و در صورتیکه این نسخه بروزتر بود، نسخه موجود در سمت کاربر بصورت خودکار با این نسخه جایگزین میشود.

❖ فایل **config.xml**: از این فایل برای انجام تنظیمات نرم افزار دایلرقاصدک کاربران استفاده میشود. با این فایل، مدیر شبکه/سرویس دهنده میتواند تمامی تنظیمات لازم برای اتصال صحیح سمت کاربر را بصورت مرکزی تدوین کرده و دایلر کاربر در هربار اتصال، این تنظیمات را بصورت خودکار بارگذاری و اجرا مینماید. به این ترتیب هزینه های پشتیبانی و اختلالات ناشی از اشتباهات سمت کاربر کاهش یافته و مدیر سیستم میتواند سیاستی واحد را برای کلیه کاربران اجرا نماید. ساختا این فایل به شکل زیر است:

```
<config>
<ToolTipText>SomeTextShowInToolTip</ToolTipText>
<OnConnect>SomeCommand1</OnConnect>
<OnConnect>SomeCommand2 </OnConnect>
<OnDisConnect>SomeCommand1</OnDisConnect>
<OnDisConnect>SomeCommand2</OnDisConnect>
<OnExit>SomeCommand1</OnExit>
<OnExit>SomeCommand2</OnExit>
<Version>1.0.1.0</Version>
<FooterText>SomeTextShowsInDialerFooter</FooterText>

<CustomerLogo>http://192.168.0.253/qsdk_dialer/clogo.png</CustomerLogo>
<CustomerText>SomeTextForLogo</CustomerText>
</config>
```

هر یک از اجزاء این فایل به قرار زیر است:

- **ToolTipText**: **متنی است که زمان قرار گرفتن ماوس روی آیکون اتصال نمایش داده میشود.**
- **OnConnect** و **OnDisConnect** و **OnExit**: **دستوراتی است که بهنگام اتصال، قطه اتصال و خروج از برنامه دایلر بصورت خودکار در CMD سیستم کاربر اجرا میشوند. محدودیتی در تعداد این دستورات نیست.**
- **Version**: **ورژن نسخه موجود در سرور در این قسمت درج میشود. در هر بار اجرای نرم افزار دایلر توسط کاربر، ورژن فایل موجود در سمت کاربر با ورژن نسخه موجود در این فولدر مقایسه شده و در صورتیکه این نسخه بروزتر بود، نسخه موجود در سمت کاربر بصورت خودکار با این نسخه جایگزین میشود.**
- **FooterText** **متنی است که در پایین دایلر و در تمام TAB ها نمایش داده میشود.**

- **CustomerLogo** و **CustomerText** : لوگو و متن مورد نظر مدیر شبکه/سرویس دهنده در **TAB** درباره ما نمایش داده میشود. بهترین رزولیشن لوگو سایز **320*110** و به صورت **transparent** میباشد.

❖ فایل **connection.cnf**: این فایل تعیین کننده پارامترهای اتصال کاربر اعم از پروتکل ارتباطی (**PPPoE, PPTP, L2TP, ...**)، نوع رمزنگاری، نحوه احراز هویت (**PAP, CHAP, EAP, ...**) و نظائر آن است. مدیر شبکه/سرویس دهنده برای تولید این فایل کافیست بر روی دستگاه خود، یک **Windows Connection** با نام **qsdk_dialer** ساخته و تمامی تنظیمات لازم برای اتصال صحیح به سرویس را در آن انجام دهد. بدیهی است این تنظیمات باید همانی باشد که قرار است کاربران ملزم به استفاده از آن شوند.

سپس قسمت مربوط به **qsdk_dialer** را از فایل:

C:\Users\[YOUR_USERNAME]\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk

برداشته و در فایلی با نام **connection.cnf** در مسیر **qsdk_dialer** در **WebRoot** در **WebServer** فوق کپی کنید. ساختار این فایل چیزی شبیه این خواهد بود:

```
[qsdk_dialer]
Type=2
MEDIA=rastapi
Port=VPN3-0
Device=WAN Miniport (PPTP)

DEVICE=vpn
PhoneNumber=192.168.0.254
```

دقت داشته باشید در فایل **connection.cnf** حتما با **[qsdk_dialer]** آغاز شده باشد.

با انجام مراحل فوق، نرم افزار دایلرقاصدک آماده بکار میشود. کافیست نرم افزار را روی سیستم یکی از کاربران اجرا کنید و در **TAB** تنظیمات، **WebServer IP** ای که فولدر **qsdk_dialer** در **WebRoot** آن با شرائط بالا ساخته شده است را وارد نموده دکمه اتصال را بزنید. دایلر در صورت اتصال صحیح به سرور (مشاهده فولدر با ساختار و فایلهای بالا) پیام اتصال به سرور موفقیت آمیز بود را نمایش خواهد داد. پس از آن کافیست نام کاربری و کلمه عبور کاربر را وارد کرده و به شبکه دسترسی پیدا کنید.

شایان ذکر است نرم افزار دایلرقاصدک با تمامی **AAA** ها و **Accounting**های مبتنی بر **RADIUS** و انواع اتصالات **PPP** قابل استفاده است اما در صورت استفاده از نرم افزار پیشرفته **NetBill AAA/LAN Accounting** امکانات پیشرفته نظیر پیام رسان، آخرین گزارشات خرابی، آخرین گزارشات اتصال و ... نیز قابل استفاده خواهد بود. برای تهیه نرم افزار **NetBill** به سایت **http://netbill.ir** مراجعه نمائید.

لطفا نظرات و پیشنهادات خود را برای بهینه سازی دایلر قاصدک به **info@ghasedak.com** ارسال نمائید.

- راهنمای تنظیمات میکروتیک در حالت VPN و HotSpot:

- امکاناتی که میکروتیک VPN Server فراهم می‌کند

اعتبارسنجی کاربران با استفاده از دیتابیس محلی ایجاد شده روی خود میکروتیک و یا Radius سرور NetBill

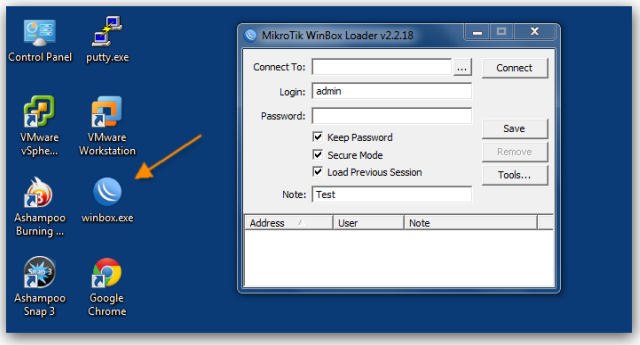
حسابرسی کاربران با استفاده از دیتابیس محلی ایجاد شده روی خود میکروتیک و یا Radius سرورNetBill

- راه اندازی سریع

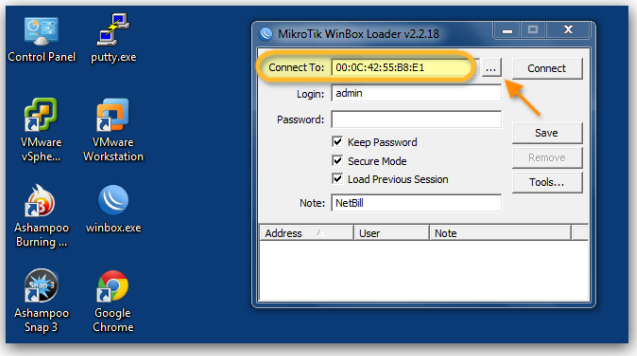
ابتدا برای سادگی کار از مسیر زیر نرم افزار winbox را دانلود می‌کنیم و جهت اتصال به سیستم عامل میکروتیک از آن استفاده می کنیم.

http://netbill.ir/files/winbox.exe

بعد از دریافت Winbox برای اتصال به میکروتیک مانند شکل زیر عمل می‌کنیم.



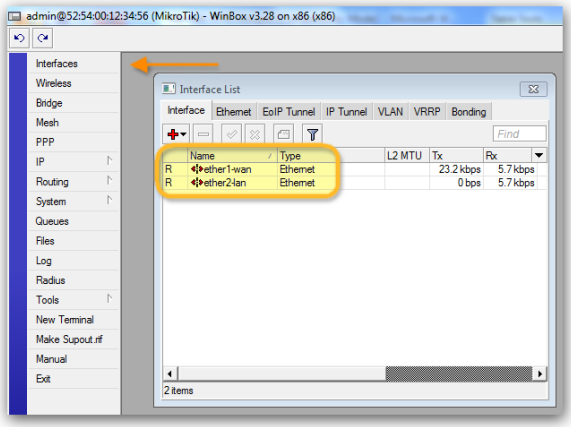
اگر اولین بار است که به میکروتیک وصل می‌شوید باید Device میکروتیک را به یک Hubswitch و رایانه خود را نیز با یک کابل شبکه به همان سوئیچ و یا مستقیم به رایانه خود وصل کنید و با اجرای نرم افزار Winbox با استفاده از MAC Address به آن Login کنید.



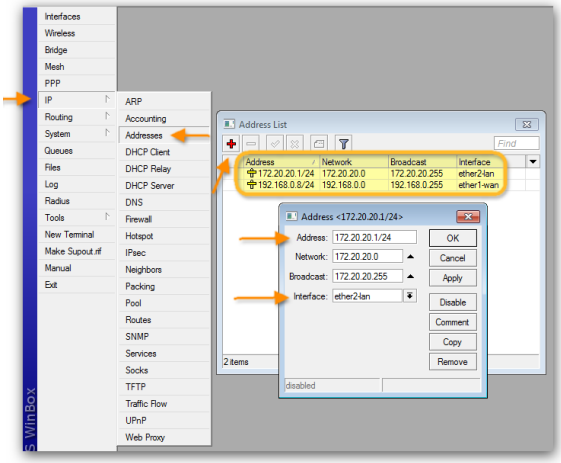
برای راه اندازی VPN Server به حداقل دو کارت شبکه (interface) نیاز دارید یکی Public که به اینترنت متصل است و دومی Local که کاربرهای LAN به آن متصل شوند. روی هر Interface امکان راه اندازی فقط یک VPN Server وجود دارد.

- **نام گذاری Interface ها**

جهت جلوگیری از اشتباه ، Interfaceهای ether1 و ether2 را به مانند زیر ، یکی را برای ارتباط با اینترنت Public Ip و دیگری را برای اتصال کاربران Local به ترتیب با نام ether1-Wan و ether2-Lan نام گذاری می‌کنیم.

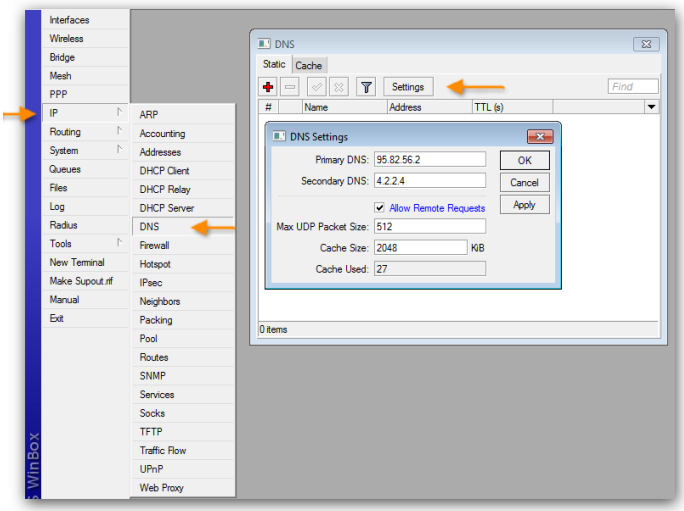


بعد از نام گذاری Interface ها برای تنظیمات IP و Gateway ابتدا وارد Address → IP شده و با کلیک بر روی  Add مانند شکل زیر به Interface ها IP می‌دهیم.



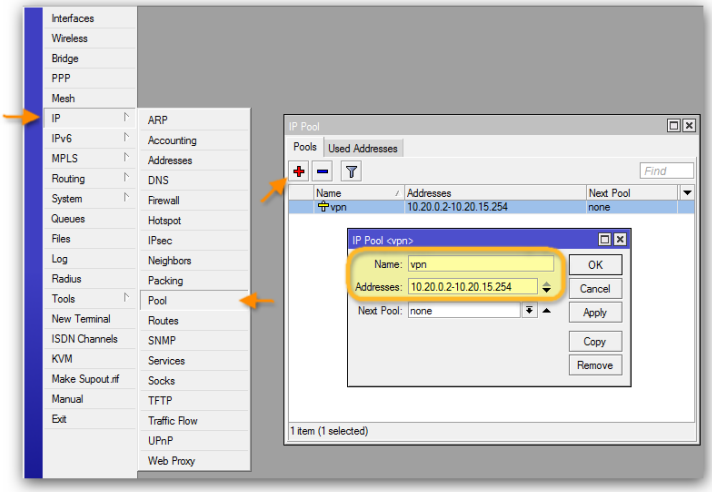
- تنظیم DNS

برای تنظیم DNS Server مانند تصویر از منوی IP گزینه DNS را انتخاب کرده و سپس در کادر باز شده روی Settings کلیک می‌کنیم و Primary DNS را 95.82.56.2 و همچنین Secondary DNS را ۴,۲,۲,۴ وارد کرده و گزینه Allow Remote Requests را تیک می‌زنیم.



- تنظیمات IP Pool جهت راه اندازی VPN

برای تنظیم و راه اندازی PPTP & PPPoE VPN Server ابتدا نیاز به یک IP Pool داریم که از منوی سمت چپ با کلیک بر روی گزینه IP→Pool به مانند شکل زیر یک رنج IP تعریف می‌کنیم که این IPها به صورت Dynamic فقط در زمان اتصال کاربر جهت برقراری ارتباط به آن کاربر اختصاص داده می‌شود.



- تنظیمات NAT در میکروتیک جهت اینترنت دار نمودن رنج IP Pool

NAT یا Network Address Translation یک استاندارد در اینترنت است که به کامپیوتر های داخل یک شبکه این اجازه را می دهد که از یک رنج IP برای ارتباط داخلی و از یک رنج دیگر برای ارتباط خارجی استفاده کنند. برای ایجاد NAT باید در شبکه داخلی یک عدد NAT Gateway داشته باشیم که ترجمه آدرسها در آن صورت گیرد.

در کل ۲ نوع NAT وجود دارد

- SRCNAT یا Source Nat

از این فرم Nat وقتی استفاده می کنیم که می خواهیم IP های Invalid یک شبکه داخلی را به یک Valid IP ترجمه کنیم. در این حالت هر پکتی که به gateway برسد IP آن به یک Valid IP ترجمه گشته و بر روی اینترنت ارسال می شود. عکس این عمل برای پکت هایی که به پکت های قبلی Reply می شوند صادق است و عکس این عمل صورت میگیرد.

- DSTNAT یا Destination Nat

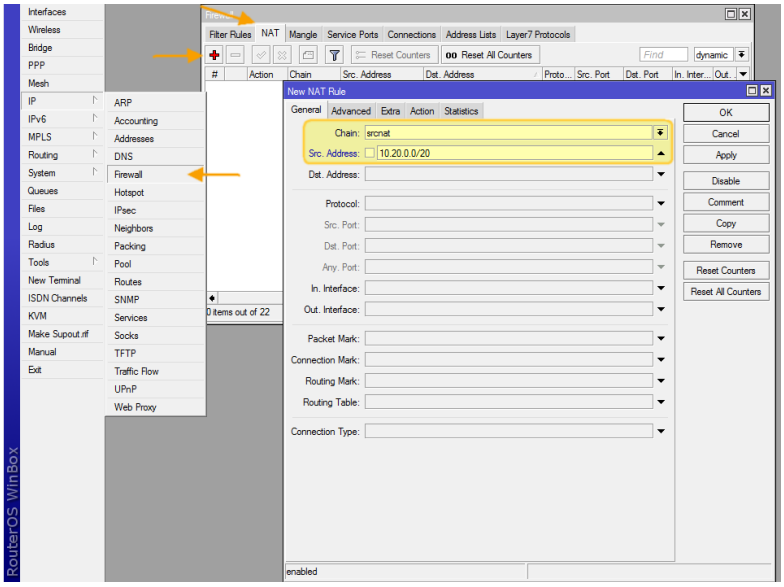
این فرم NAT را وقتی انجام می دهیم که بخواهیم یک شبکه private را برای شبکه public خود قابل دسترسی قرار دهیم. در این عمل Valid IP خود را به Invalid IP ترجمه میکنیم.

- Redirect Nat و Masquerade Nat

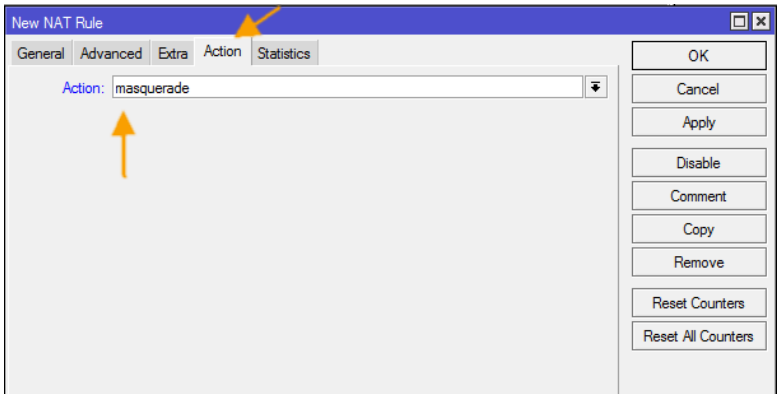
Redirect و Masquerade یک نوع خاص dstnat و srcnat است. Redirect یک نوع از dstnat است که نیازی به تعریف to-address ندارد و تنها شناساندن Interface ورودی کافی است و Masquerade یک نوع srcnat است که نیازی به تعریف to-address ندارد و تنها معرفی یک اینترفیس خروجی کافی است. در این حالات دیگر فرقی ندارد که چه IP به اینترفیس ها متصل میگردد هر IP در رنج IP های add شده به Interface عمل می کند. در Redirect فیلد to-port برای فرستادن کل ترافیک به یک پورت خاص است که بیشتر برای اعمالی نظیر web-proxy استفاده می شود.

حال پس از درک مفهوم NAT در این قسمت با توجه به تصویر زیر به NAT کردن اینترنت برای رنج IP Pool ایجاد شده می پردازیم.

ابتدا از منوی سمت چپ با کلیک بر روی IP→Firewall و ورود به سربرگ NAT بر روی گزینه  جهت افزودن NAT Roule کلیک می کنیم. در قسمت Chain گزینه srcnat را انتخاب نموده و در قسمت Src. Address آدرس محدوده IP Pool تعریف شده را بصورت CIDR وارد میکنیم.

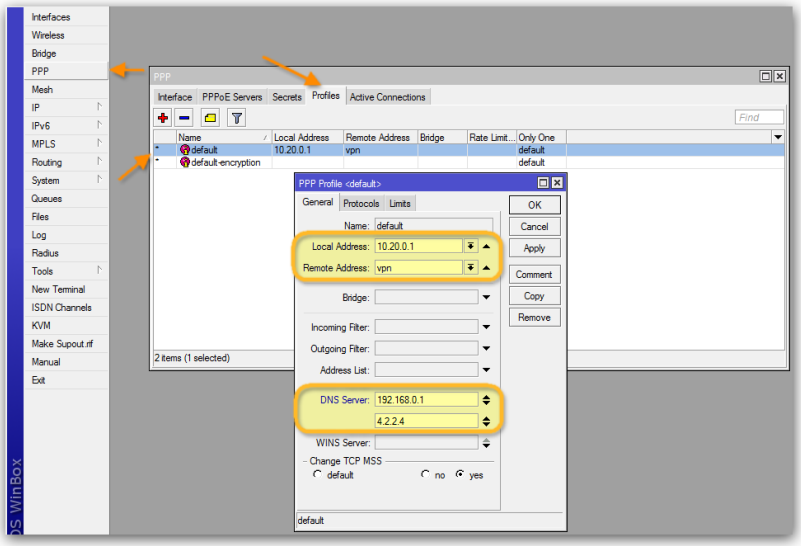


پس از انجام مراحل فوق با مراجعه به سربرگ Action و انتخاب گزینه masquerade بر روی OK کلیک می کنیم، حال با این کار کاربران پس از اتصال اینترنت خواهند داشت.



- **تنظیمات PPP جهت راه اندازی** PPTP & PPPoE Server

برای تنظیم و راه اندازی PPTP & PPPoE VPN Server از منوی سمت چپ با کلیک بر روی گزینه PPP و انتخاب سربرگ Profiles یا با Add کردن یک Profile جدید و یا با ویرایش Default Profile و تنظیم آن به مانند شکل زیر یک Profile جهت اختصاص به PPTP & PPPoE Server و اتصال کاربران ایجاد می‌کنیم.

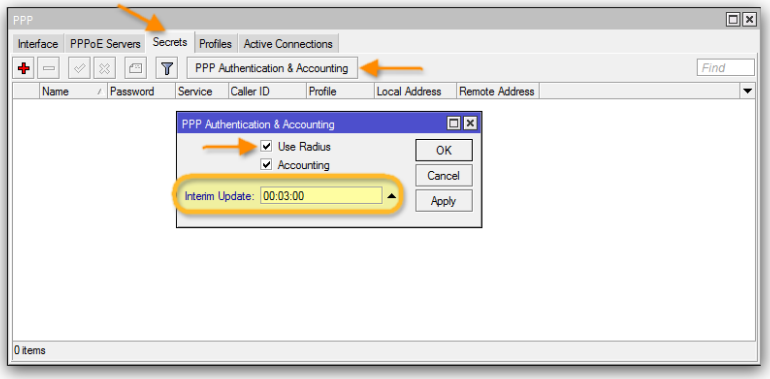


در قسمت Local Address ، IP اول Address Pool را جهت برقراری Tunnel می‌نویسیم. (در این قسمت IP خود Mikrotik را نیز می‌توان قرار داد)

در قسمت Remote Address با کلیک بر روی منوی کشویی باز شدنی گزینه VPN (نام IP Pool) تعریف شده را انتخاب می‌کنیم.

در قسمت DNS Server به دلیل راه اندازی DNS Cache خود Mikrotik در Tab اول IP خود Mikrotik که در اینجا ۱۹۲.۱۶۸.۰.۱ می‌باشد را می‌نویسیم و با کلیک بر روی منوی بازشدنی در زیر آن یک DNS دیگر جهت اطمینان می‌نویسیم تا اگر زمانی DNS Cache میکروتیک از کار افتاد از آن DNS دوم استفاده کند.

همچنین مطابق تصویر زیر در سربرگ Secrets با کلیک بر روی PPP Autentication & Accounting در صفحه باز شده تنظیمات را اعمال می‌کنیم.



- **توضیحی مختصر در مورد پروتکل‌های PPTP ، L2TP و PPPoE**

عمده‌ترین پروتکل‌هایی که برای دسترسی به VPN استفاده می‌شوند عبارتند از L2TP ، PPTP ، PPPoE

- پروتکلPPTP

پروتکل Tunneling نقطه به نقطه، بخش توسعه یافته ای از پروتکل PPP است که فریم‌های پروتکل PPP را به صورت IP برای تبادل آن‌ها از طریق یک شبکه IP مانند اینترنت توسط یک سرایند، کپسوله می‌کند. این پروتکل می‌تواند در شبکه های خصوصی از نوعLAN-to-LAN نیز استفاده گردد.

PPTPیک ارتباط TCP را(که یک ارتباط Connection Oriented بوده و پس از ارسال پکت منتظر Acknowledgment آن می‌ماند) برای نگهداری تونل و فریم‌های PPP کپسوله شده توسط (GRE) Generic Routing Encapsulation که به معنی کپسوله کردن مسیریابی عمومی است، برای Tunneling کردن اطلاعات استفاده می‌کند. ضمناً اطلاعات کپسوله شده PPP قابلیت رمزنگاری و فشرده شدن را نیز دارا هستند.

- پروتکلL2TP

پروتکل L2TP ترکیبی است از پروتکل‌های PPTP و (L2F) Layer 2 Forwarding که توسط شرکت سیسکو توسعه یافته است. این پروتکل ترکیبی است از بهترین خصوصیات موجود در L2F و PPTP - L2TP نوعی پروتکل شبکه است که فریم‌های PPP را برای ارسال بر روی شبکه های IP مانند اینترنت و علاوه بر این برای شبکه های مبتنی بر X.25 ، Frame Relay و یا ATM کپسوله می‌کند.

L2TP برای نگهداری تونل از یک سری پیغام‌های L2TP و نیز از پروتکل UDP پروتکل تبادل اطلاعات به صورت Les Connection که پس از ارسال اطلاعات منتظر دریافت Acknowledgment نمی‌شود و اطلاعات را ، به مقصد رسیده فرض می‌کند استفاده می‌کند.

- پروتکلPPPoE

Pont-to-Point Protocol over Ethernet یک پروتکل لایه ۲ می‌باشد و همانطور که از اسم آن بر می‌آید از دسته پروتکل‌های PPP است.

PPPoE تمامی خاصیت‌های یک پروتکل PPP را دارد اما با این خصوصیت که بر روی شبکه Ethernet نیز قابل اجراست. یعنی شما می‌توانید ارتباط هایی مانند کانکشن PPTP را بر روی لایه ۲ داشته باشید. این پروتکل توسط اولین ISP با هدف تجاری دنیا یعنی UUNET ابداع شده است که اطلاعات کامل این پروتکل با RFC2516 قابل دسترس است. معمولا ISP ها بیشتر از این پروتکل استفاده می‌کنند, یکی به دلیل Isolation آن و دیگری به دلیل نیاز به کمترین تنظیمات سمت مشترک.

اصول کار PPPoE همانند DHCP ست. که طی ۴ مرحله کلاینت را به سرور متصل می‌کند.

✓ PPPoE Active Discovery Initiation (PADI)

این درخواست به صورت Broadcast از طرف کلاینت در شبکه منتشر شده که سرور این Broadcast را جواب می‌دهد و اعلام آمادگی می‌نماید.

✓ PPPoE Active Discovery Offer (PADO)

کلاینت پس از ارسال Broadcast با ذکر MAC Address خود به سرور یک Packet ارسال می‌کند. که حاوی پیشنهادی برای برقراری ارتباط است.

✓ PPPoE Active Discovery Request (PADR)

پس از ارسال پیشنهاد PPPoE Server در صورت توافق شرایط یک تائیدیه از سرور به کلاینت می‌فرستد. که شرایط مورد توافق می‌تواند مسائلی نظیر Authentication Protocol یا فعال بودن یا نبودن Encryption باشد.

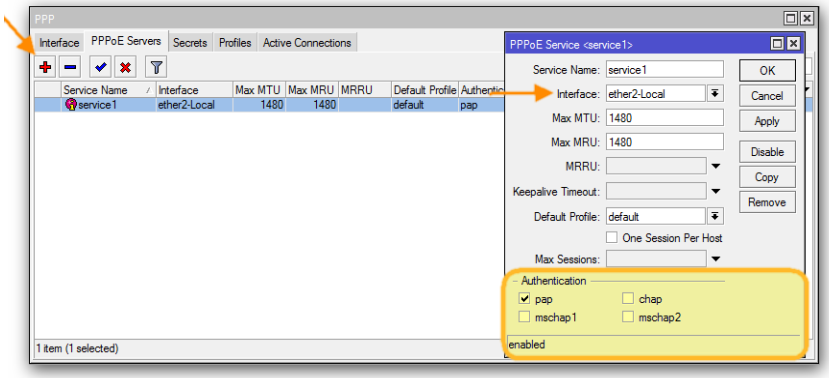
۱. PPPoE Active Discovery Session-confirmation (PADS)

و در مرحله آخر PPPoE Server درخواست کلاینت را با یک تائیدیه قبول می‌کند و ارتباط برقرار می‌شود.

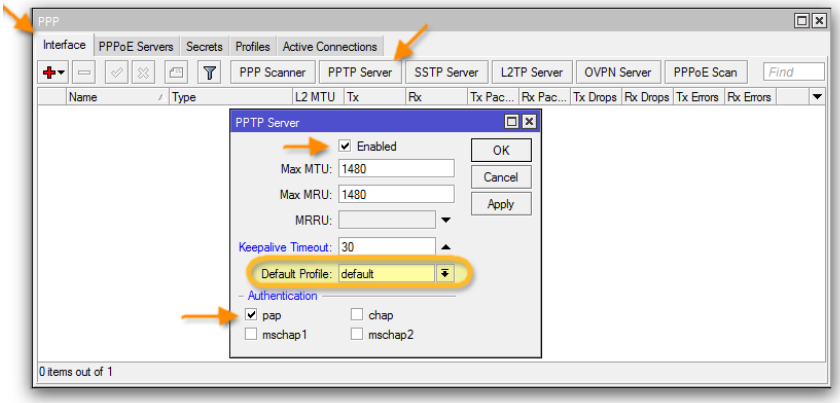
با بررسی موارد فوق خواهیم دید که لازمه برقراری یک ارتباط PPPoE وجود یک LAN و امکان ارسال Broadcast است.

برای راه اندازی سرویس PPPoE به مانند تصویر زیر از سربرگ PPPoE Server روی گزینه ADD کلیک می‌کنیم. در قسمت Interface جهت راه اندازی سرویس PPPoE به مانند تصویر ether2-Local را انتخاب می‌کنیم.

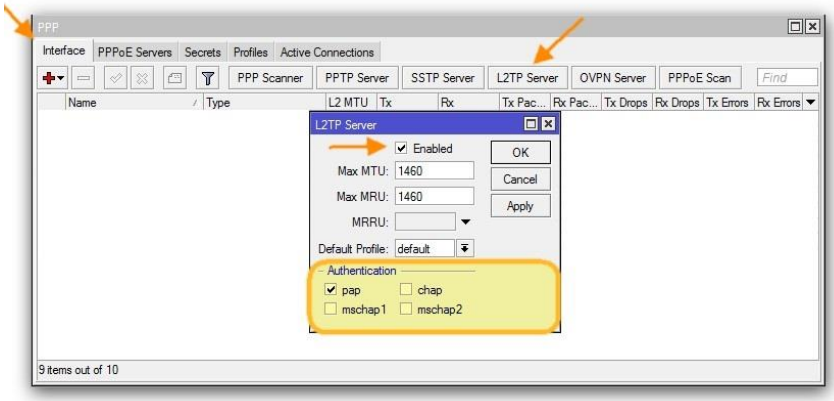
توجه کنید که در قسمت Authentication فقط گزینه PAP فعال باشد.



برای فعال کردن PPTP Server در سربرگ Interface با کلیک بر روی گزینه PPTP Server و فعال کردن گزینه Enabled و انتخاب Profile Default و فقط انتخاب گزینه pap از قسمت Authentication سرویس PPTP Server را راه اندازی می‌کنیم.

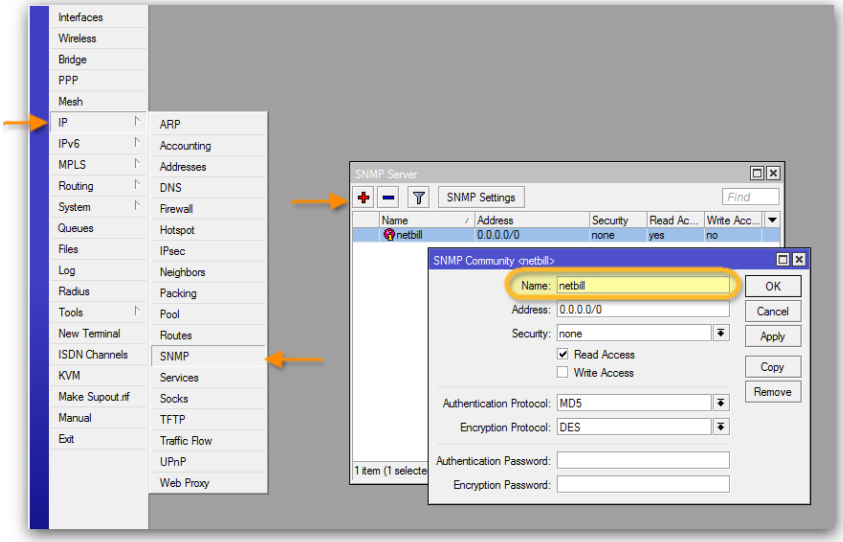


برای فعال کردن L2TP Server در سربرگ Interface با کلیک بر روی گزینه L2TP Server و فعال کردن گزینه Enabled و انتخاب Profile Default و فقط انتخاب گزینه pap از قسمت Authentication سرویس L2TP Server را راه اندازی می‌کنیم.

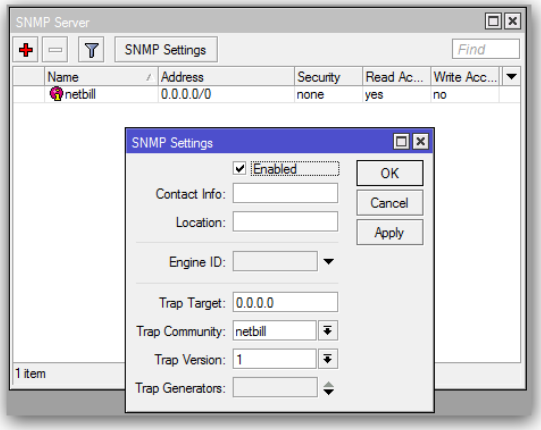


- **تنظیم SNMP برای تهیه و ثبت Graph**

برای راه اندازی و تنظیم SNMP جهت تهیه و ثبت گزارشات Graph در NetBill به مانند تصویر زیر از منوی IP گزینه SNMP را انتخاب و به مانند تصویر با کلیک بر روی ADD یک SNMP فقط خواندنی اضافه می‌کنیم.



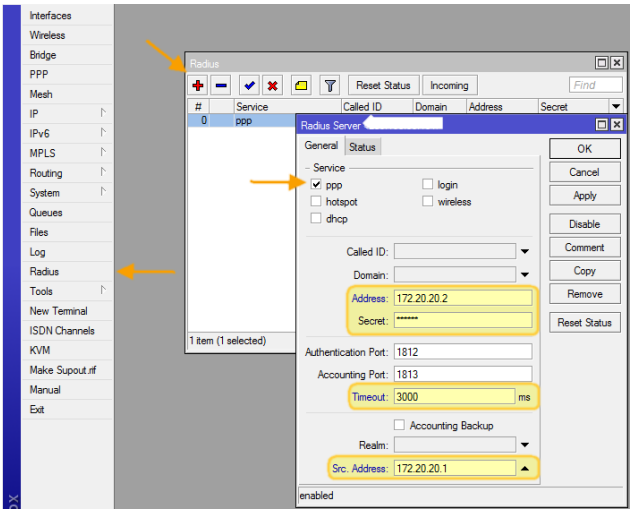
در مر حله بعد مانند شکل زیر با کلیک بر روی SNMP Setting و فعال کردن گزینه Enabled آنرا فعال می‌کنیم.



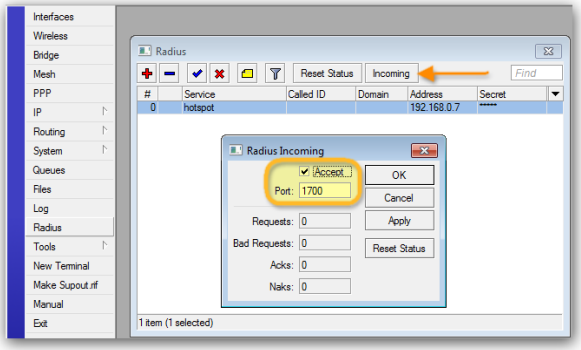
- **تنظیمات Radius برای اتصال به NetBill**

برای تنظیم ارتباط Mikrotik HotSpot RAS Server به NetBill مانند شکل زیر از قسمت Radius روی کلیک می‌کنیم، در قسمت Service گزینه HotSpot را انتخاب می‌کنیم، گزینه Address همان IP سرور NetBill باید باشد که در اینجا ۱۷۲.۲۰.۲۰.۲ می‌باشد. در قسمت Secret یک کلمه رمز برای ارتباط Mikrotik با NetBill انتخاب می‌کنیم. توجه کنید که

این کلمه رمز را باید در NetBill نیز وارد کنید. Timeout را برابر 3000 ms قرار می‌دهیم و Src. Address همان IP میکرو تیک می‌باشد.

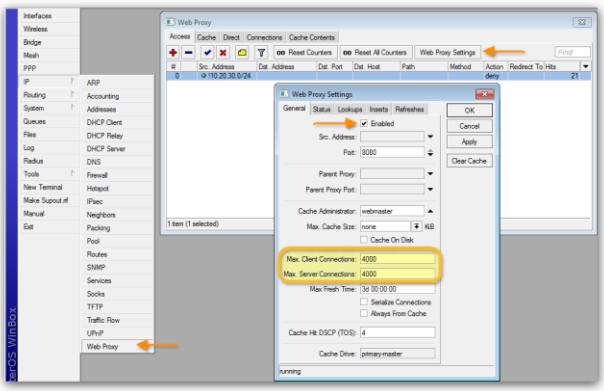


همچنین مطابق شکل زیر با کلیک بر روی گزینه Incomming مقدار Port را برابر ۱۷۰۰ قرار می‌دهیم.

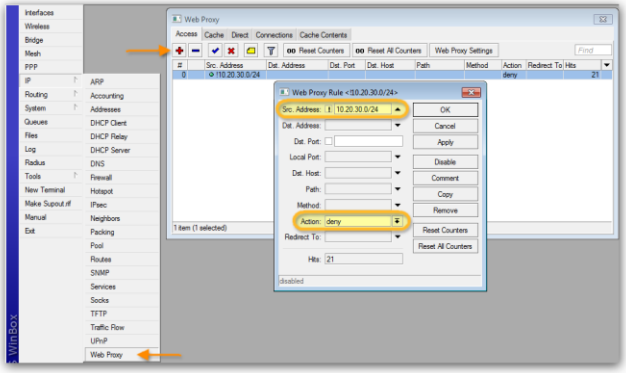


- **تنظیمات مربوط** Web Proxy **برای تهیه گزارش** Log Browse URL

ابتدا مطابق تصویر زیر Web Proxy Settings (Web proxy → IP) را تنظیم می‌کنیم.

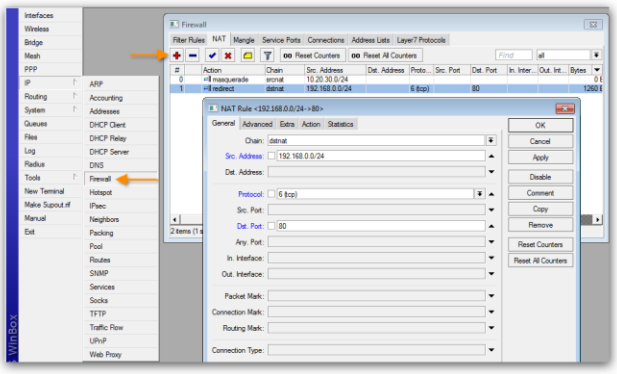


سپس از سربرگ Access روی گزینه  کلیک می‌کنیم، در اینجا دسترسی غیر از Source Address داخلی خود را به Web Peoxy ممنوع می‌کنیم.

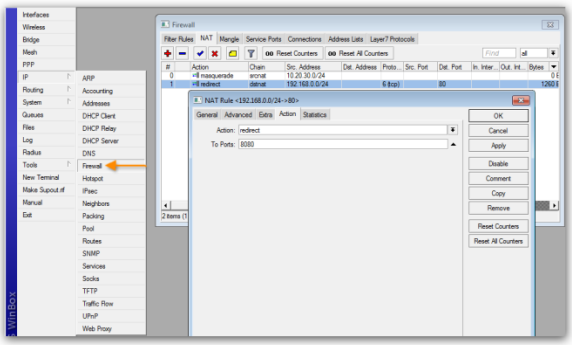


حال باید از قسمت NAT → Firewall → IP یک Redirect NAT تعریف کنیم که کاربران بعد از اتصال به Web Proxy هدایت شوند. Redirect یک نوع از dstnat است که نیازی به تعریف to-address ندارد و تنها شناساندن اینترفیس ورودی کافی است در Redirect فیلد to-port برای فرستادن کل ترافیک به یک پورت خاص است که بیشتر برای اعمالی نظیر web-proxy استفاده می‌شود.

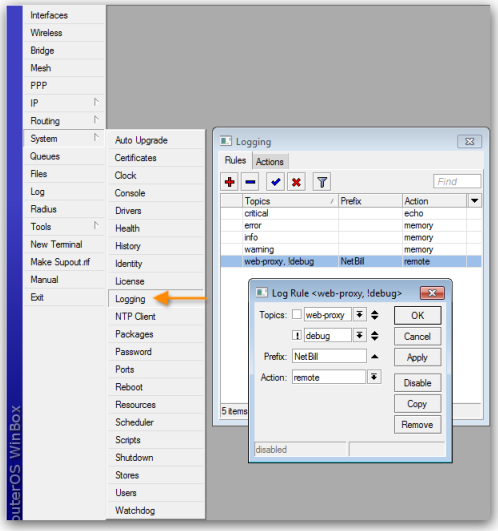
مانند تصویر زیر عمل می‌کنیم



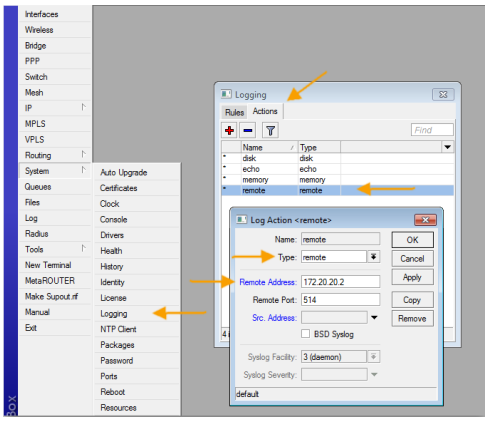
در سربرگ Action گزینه Redirect را انتخاب می‌کنیم و در قسمت To Ports همان پرت Web Proxy یعنی ۸۰۸۰ را می‌نویسیم. با این کار تمامی درخواست‌های کاربران به Web Proxy ارجاع داده می‌شود.



سپس از قسمت System → Logging مانند تصویر زیر با کلیک بر روی Add یک Roule جدید ایجاد می‌کنیم و از قسمت Topics گزینه web-proxy و با کلیک بر روی پیکان زیرین یک Box دیگر ایجاد و گزینه Debug! را انتخاب کنید، در قسمت Perfix یک نام به عنوان مثال Netbill را وارد کنید و همچنین با انتخاب گزینه Remote در Action و با کلیک بر روی Ok یک Roule ایجاد کرده‌ایم که Debug Web Proxy! Log را تهیه می‌کند و به Remote ارجاع می‌دهد.



حال از سربرگ Action مانند تصویر زیر Type: remote را انتخاب کرده و در قسمت Remote Address آدرس Netbill را وارد می‌کنیم.



Hotspot یک نقطه دسترسی عمومی است برای کامپیوترهایی که به صورت کابلی یا بی سیم به شبکه متصل شده‌اند. در واقع Hotspot امکانی برای اعتبارسنجی (Authenticate) کاربران جهت اتصال به شبکه به وجود می‌آورد.

ویژگی خاص Hotspot نیاز نداشتن به نرم افزار و یا تنظیمات خاص سمت کاربر است که باعث سهولت بیشتر برای کاربران معمولی می‌شود. فقط کافی است در سمت کاربر یک Internet Browser وجود داشته باشد ، با بازکردن مرورگر درخواستی مبتنی بر ارسال صفحه وب به Hotspot فرستاده می‌شود ، Hotspot تمام درخواست‌ها را به صفحه پیش فرض Servlet Page or Login Redirect Page می‌کند. (صفحه پیش فرض قابل تغییر است) ، صفحه پیش فرض معمولا شامل فرم درخواست نام کاربری و کلمه عبور است. بعد از اعتبار سنجی کاربر به صفحه دلخواه Redirect می‌شود. برای خروج هم کافی است از صفحه Status که به صورت Popup باز می‌شود Logout را انتخاب کنند.

❖ امکانات Hotspot

اعتبارسنجی کاربران با استفاده از دیتابیس محلی ایجاد شده روی خود میکروتیک و یا Radius سرور NetBill

حسابرسی کاربران با استفاده از دیتابیس محلی ایجاد شده روی خود میکروتیک و یا Radius سرور NetBill

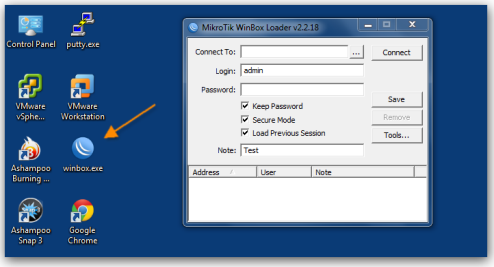
سیستم Walled-garden (دسترسی به بعضی از سایت‌ها بدون اعتبار سنجی)

❖ اتصال به میکروتیک

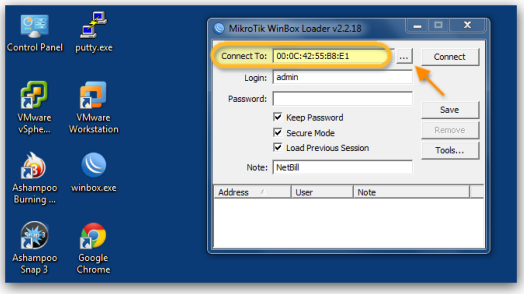
ابتدا برای سادگی کار از مسیر زیر نرم افزار Winbox را دانلود می‌کنیم و جهت اتصال به سیستم عامل میکروتیک از آن استفاده می‌کنیم.

http://Netbill.ir/files/winbox.exe

بعد از دریافت Winbox برای اتصال به میکروتیک مانند شکل زیر عمل می‌کنیم.



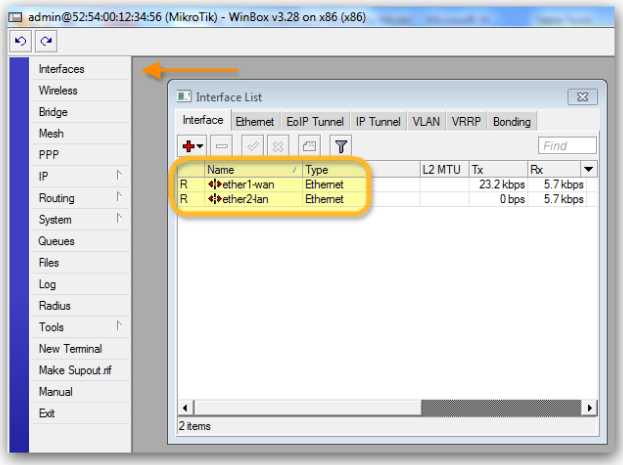
اگر اولین بار است که به میکروتیک وصل می‌شوید باید Device میکروتیک را به یک Hubswitch و رایانه خود را نیز با یک کابل شبکه به همان سوئیچ و یا مستقیم به رایانه خود وصل کنید و با اجرای نرم افزار Winbox با استفاده از MAC Address به آن Login کنید.



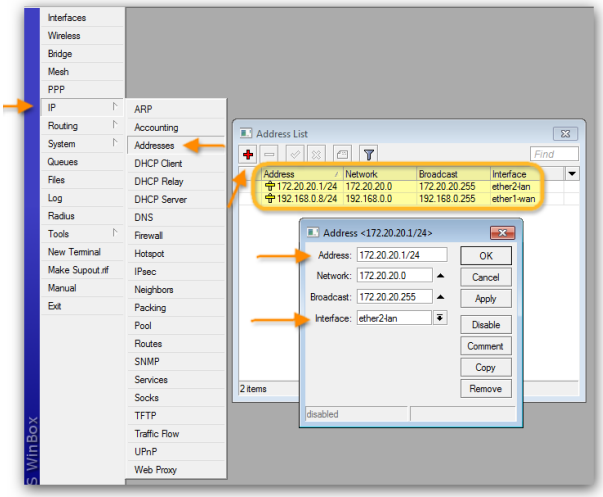
برای راه اندازی Hotspot به حداقل دو کارت شبکه (Interface) نیاز دارید یکی Public که به اینترنت متصل است و دومی Local که کاربرهای Hotspot به آن متصل شوند. روی هر Interface امکان راه اندازی فقط یک Hotspot سرور وجود دارد.

❖ نام گذاری Interface ها

جهت جلوگیری از اشتباه، Interface های ether1 و ether2 را به مانند زیر یکی را برای ارتباط با اینترنت Public IP و دیگری را برای اتصال کاربران Local به ترتیب با نام ether1-Wan و ether2-Lan نام گزاری می‌کنیم.

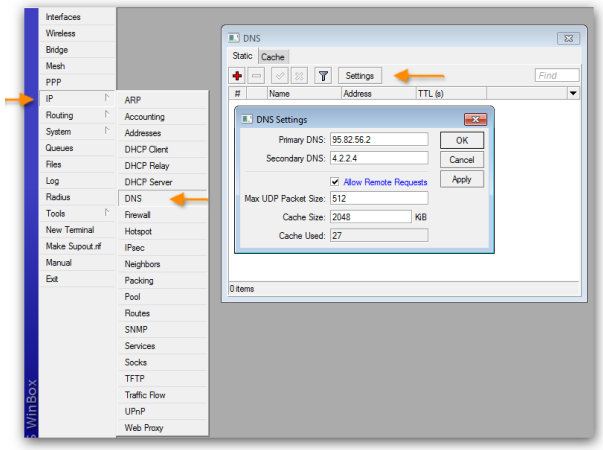


بعد از نام گزاری Interface ها برای تنظیمات IP و Gateway ابتدا وارد Address → IP شده و با کلیک بر روی Add مانند شکل زیر به Interface ها IP می‌دهیم)



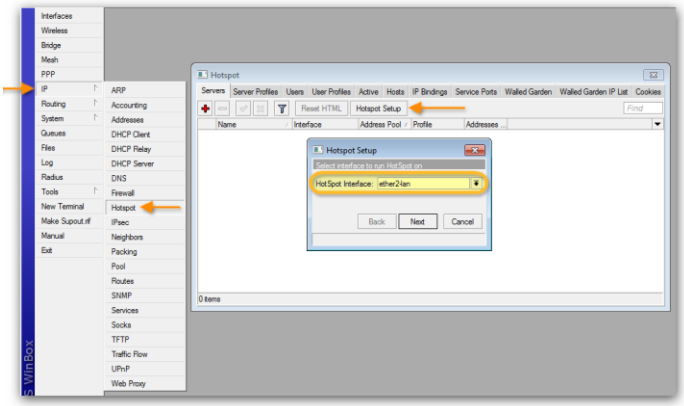
❖ تنظیم DNS

برای تنظیم DNS Server مانند تصویر از منوی IP گزینه DNS را انتخاب کرده و سپس در کادر باز شده روی Settings کلیک می‌کنیم و Primary DNS را 95.82.56.2 و همچنین Secondary DNS را 4.2.2.4 وارد کرده و گزینه Allow Remote Requests را تیک می‌زنیم.

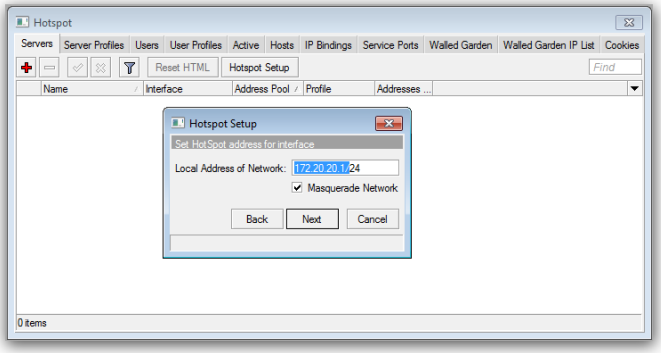


❖ راه اندازی سریع

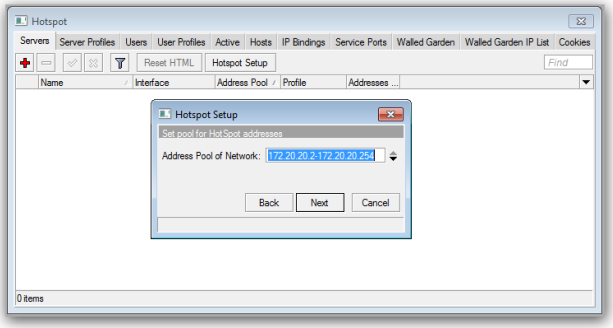
برای راه اندازی Hotspot مطابق شکل زیر ابتدا روی Hotspot→ IP در پنجره باز شده در سربرگ Servers روی Hotspot Setup کلیک می‌کنیم، حال در این قسمت Interface مورد نظر را جهت راه اندازی Hotspot انتخاب می‌کنیم که در اینجا ether2-Lan می‌باشد.



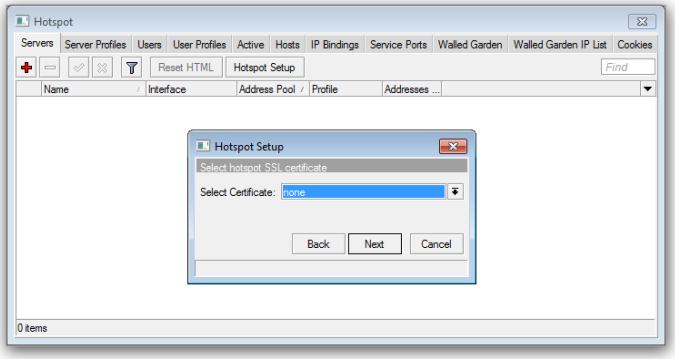
در قسمت Set Hotspot address for interface آدرس IP ، LAN Interface را به همراه محدوده IP که در اینجا /24 می‌باشد نمایش می‌دهد، مطابق شکل زیر روی Next کلیک می‌کنیم.



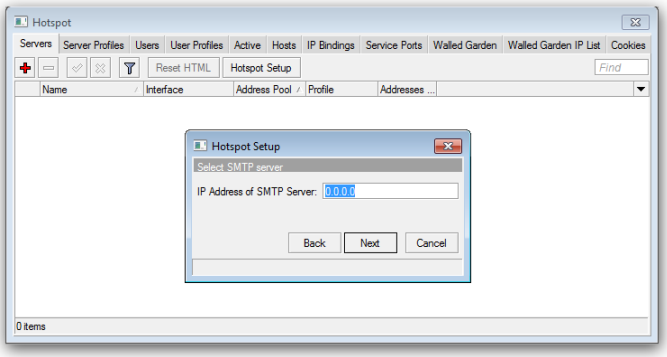
در قسمت Set Pool for Hotspot address آدرس IP ، LAN Interface را به همراه محدوده IP که در اینجا /24 می‌باشد نمایش می‌دهد، مطابق شکل زیر روی Next کلیک می‌کنیم.



در این قسمت مطابق تصویر Hotspot SSL Certificate را none انتخاب می‌کنیم و روی Next کلیک می‌کنیم.

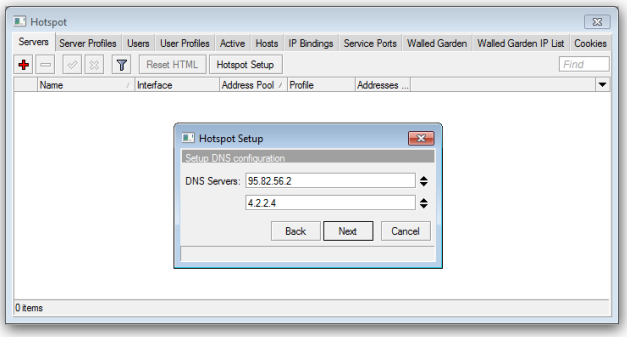


در قسمت زیر هم روی Next کلیک می‌کنیم.



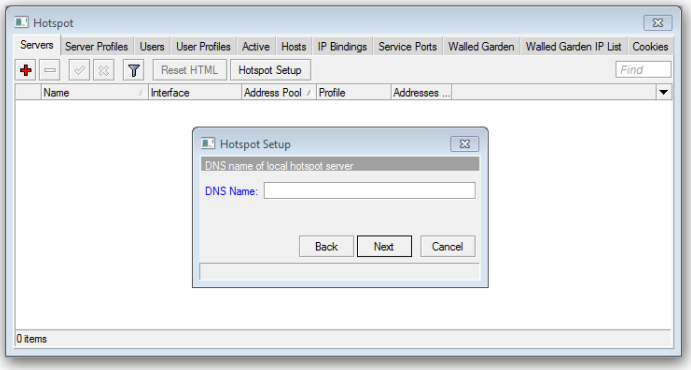
- Setup DNS configuration

این قسمت مربوط به تنظیمات DNS می‌باشد که در مراحل قبل انجام داده‌ایم و نیازی به تغییرات نمی‌باشد ، روی Next کلیک می کنیم.



- DNS name of local server

در این قسمت می‌توانید نامی را برای DNS سرور Hotspot انتخاب کنید ، این مقدار را نیز خالی رها کنید و روی Next کلیک کنید.



اکنون Hotspot راه اندازی شده است.

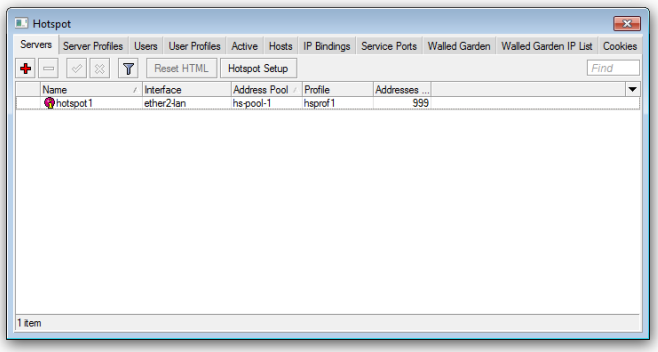
در سمت کلاینت باید تنظیمات TCP/IP را انجام دهید. به صورت پیش فرض تنظیم روی اتوماتیک قرار دارد و همین برای گرفتن یک IP از IP Pool MikroTik کفایت می کند ولی توصیه می‌شود برای مدیریت بهتر در مورد پهنای باند از IP استاتیک استفاده کنید. یک IP در رنج Interface Local به کارت شبکه کلاینت اختصاص دهید، DNS و Gateway سرور MikroTik را بدهید. می توانید با باز کردن مرورگر روی یک کامپیوتر که به Interface local متصل شده است از این موضوع مطمئن شوید.

باید صفحه خوشامدگویی Hotspot Login به نمایش درآید.

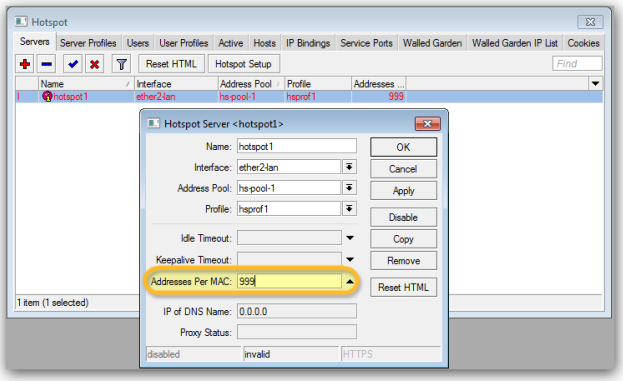
به صورت پیش فرض در هنگام اتصال کاربران یک رول مبتی بر NAT در قسمت IP → Firewall → NAT به صورت دینامیک ایجاد می‌شود.

❖ مدیریت Hotspot

در نرم افزار Winbox از منوی IP قسمت Hotspot را انتخاب کنید.



در اینجا سرور Hotspot ایجاد شده با نام hotspot1 روی ether2-Lan با Address Pool و مشخصه hsprof1 را مشاهده می‌کنیم و با کلیک روی آن مقدار Addresses Per MAC را به تعداد ۹۹۹ تغییر می‌دهیم.



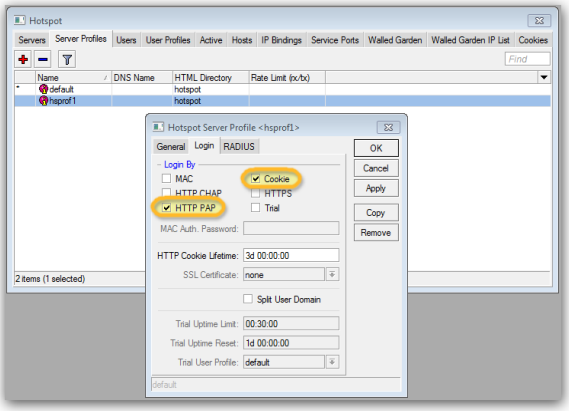
این گزینه بدین معنی می‌باشد که HotSpot بتواند تعداد ۹۹۹ ، MAC Address را Authenticate کند.

گزینه Profiles امکانی برای تنظیمات همزمان سرورهای مختلف ایجاد می‌کند. برای مثال شما چند پروفایل با تنظیمات مختلف ایجاد می‌کنید. سپس سرورهای مختلف Hotspot را به هر کدام که مایل باشد ارجاع می‌دهید و نیازی به تنظیم جداگانه هر سرور نخواهید داشت سوای آن بسیاری از تنظیمات کلیدی و اساسی Hotspot در همین جا انجام خواهد گرفت.

برای نمونه با کلیک روی پروفایل hsprof1 آن را جهت تنظیمات با Radius NetBill آماده می‌کنیم.

در قسمت Login نوع اعتبار سنجی کاربران را مشخص می‌کنید که فقط گزینه HTTP PAP را فعال می‌کنیم.

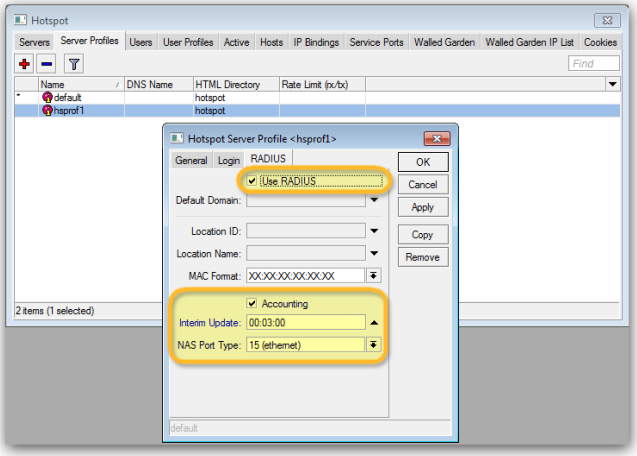
گزینه Cookie مربوط به ذخیره نام کاربر و رمز عبور هنگام ورود در بار اول برای کاربران Hotspot می‌باشد که فعال کردن آن اختیاری است.



در قسمت Radius مشخص می‌کنید که این سرور برای اعتبار سنجی و حسابرسی از Radius استفاده کند یا نه. چون برای اکانتینگ از Radius سرور استفاده می‌کنید باید تیک Accounting را بزنید نکته مهم قسمت Interim Update است. این قسمت را باید

طبق تنظیمات Radius سرور خود انجام دهید که برای ارتباط با NetBill این مقدار را برابر ۳ دقیقه قرار می‌دهیم ، در غیر این صورت کاربرهای شما از لیست Online User ها در نرم افزار Radius حذف می‌شوند در حالی که هنوز متصل هستند.

در سربرگ RADIUS با فعال کردن Use RADIUS و انتخاب گزینه (Ethernet) از قسمت NAS Port Type مشخصه Hotspot را برای اتصال با NetBill تنظیم می‌کنیم.



❖ نکات مهم

در قسمت General گزینه HTML Directory مکان قرار گرفتن فایل‌های وب Login Page است.

بنابراین این امکان وجود دارد که سرورهای مجزای Hotspot Login Page های متفاوتی داشته باشند. برای استفاده از این گزینه باید با نحوه کپی کردن فایل‌ها در Mikrotik با استفاده از FTP و یا Winbox آشنا باشید.

در قسمت Rate limit این امکان وجود دارد که پهنای باند کل یک سرور Hotspot را محدود کنید.

در قسمت HTTP Proxy می‌توانید پروکسی سرور مورد استفاده این Hotspot را مشخص کنید.

پس می‌توانید از پروکسی‌های مختلف برای سرورهای مختلف استفاده کنید.

○ Hosts

در این قسمت کلیه کاربران داخل شبکه ما که پشت Hotspot Server قرار دارند نمایش داده می‌شوند.

○ Active

در این قسمت لیست کاربرهای آنلاین به همراه اطلاعات مفید دیگر را به شما نشان می‌دهد.

قسمت IP Bindings یکی از مهم‌ترین قسمت‌های Hotspot به شمار میاید.

برای یادگیری این قسمت باید مفهومی به نام One to one NAT را درک کنید.

کاربر برای ارتباط با Hotspot باید یک IP در رنج Hotspot ست و یا اینکه از DHCP Server که به همراه نصب Hotspot راه اندازی می‌شود IP بگیرد. برای این مورد الزامی وجود ندارد کاربر می‌تواند هر IP دلخواهی ست کند و فقط DNS ، Gatewayرا سرور Hotspot بدهد. (در غیر اینصورت صفحه Login نمایش داده نخواهد شد) تمامی در خواست‌ها حالا با هر IP که باشند به Hotspot می‌رسند و Hotspot درخواست‌ها را به Login Page ارجاع می‌دهد اگر کاربر بتواند با موفقیت مرحله ورود را پشت سر بگذارد و به اصطلاح Authenticate شود از آن پس Hotspot یک IP به کاربر اختصاص می‌دهد که این IP معادل IP کاربر است نه الزاماً مشابه آن. این تکنیک به One to one NAT مشهور است. (Universal Client هم نامیده می‌شود) پس Hotspot می‌تواند هر IP آدرسی را به صورت ترانسپرنت تغییر دهد و این قابلیت بسیار کاربردی است.

اکنون می‌توانید با IP Bindings کار کنید. MAC آدرس کاربر را مشخص کنید Address را خالی بگذارید و To Address را با آدرس دلخواه جایگزین کنید. کاربر هر IP هم که ست کند باز با IP دلخواه شما به شبکه وصل خواهد شد. پس مشکلی به نام IP Conflict نخواهید داشت.

نکته مهم Type اتصال کاربر است که با کلیک کردن روی هر IP که Bind کرده‌اید می‌توانید آن را تنظیم کنید. سه نوع Type مختلف وجود دارد:

✓ **Regular**

حالت پیش فرض که کاربر باید اعتبار سنجی شود تا وارد شود.

✓ **Bypassed**

که کاربر را از قید اعتبار سنجی خلاص می‌کند. یعنی اگر کاربری این آدرس را داشت وارد شود بدون گذر از مرحله اعتبار سنجی.

✓ **Blocked**

که کاربر را بلوکه می‌کند و کاربر نمی‌تواند وصل شود.

در IP Bindings هنگامی که بخواهیم به کاربری مستقیم دسترسی به اینترنت بدهیم و بدون اینکه در Host لاگین کند به صورت مستقیم و دائم اینترنت داشته باشد به صورت زیر عمل می‌کنیم.

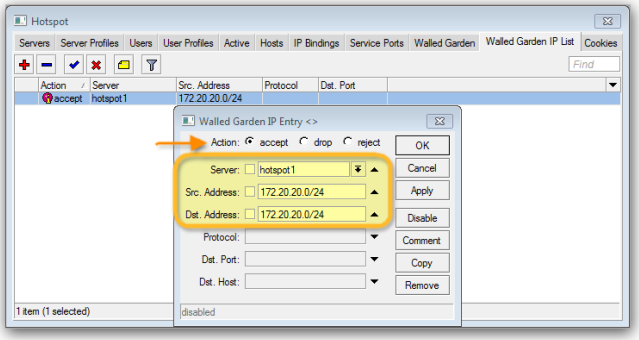
البته این کار را نیز می‌توانیم در قسمت Host با کلیک راست بر روی IP / MAC مورد نظر نیز انجام دهیم.

به عنوان مثال چون NetBill هم در همان سوئیچ کاربران Host قرار می‌گیرد با Bind کردن به آن به صورت مستقیم و دائم اینترنت می‌دهیم.

❖ Walled Garden IP List

قسمت مهم دیگر Walled-garden است که اجازه دسترسی کاربران به سایت‌ها یا IP های تعریف شده توسط مدیر سیستم را بدون گذر از مرحله اعتبار سنجی می‌دهد. مثال می توانید تنظیماتی اعمال کنید که کاربران برای اتصال به سایت شما و چک کردن گزارشات نیازی به وارد کردن نام کاربری و رمز عبور نداشته باشند و یا ...

به عنوان مثال : یک سرویس وب سرور Local در رنج داخلی شبکه خود داریم و لازم نیست که کاربران برای اتصال به آن Authenticate شوند ، برای این کار به صورت زیر عمل می‌کنیم.



نکته : در تصویر فوق گفته‌ایم که اگر کاربری از مبدأ رنج IP داخلی شبکه ، درخواست سرویسی از همان رنج (با مقصد رنج IP داخلی شبکه) را دارد به آن دسترسی داشته باشد و نیازی به Authenticate در HotSpot Server نداشته باشد.

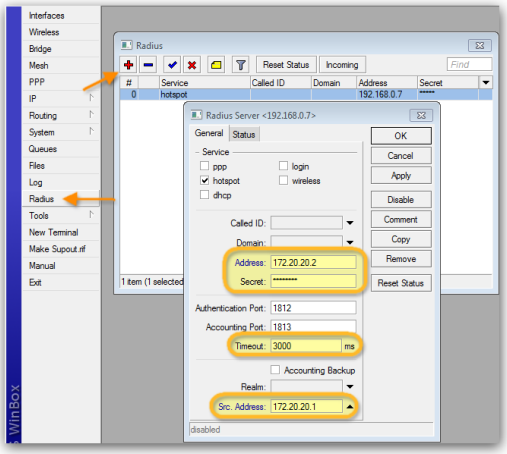
و اما قسمت Cookies که لیستی از کوکی‌های فعال و کوکی‌های اجاره داده شده به همراه زمان انقضای آن‌ها را نشان می‌دهد به شرطی که روش اعتبار سنجی با کوکی را انتخاب کرده باشید در غیر این صورت خالی خواهد بود.

❖ اختصاصی کردن صفحات Hotspot

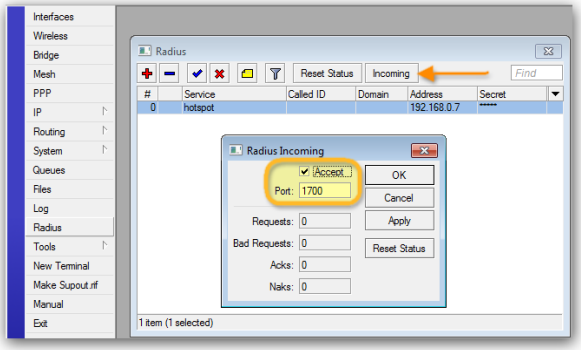
برای اختصاصی کردن صفحات Hotspot باید از طریق FTP و یا رابط Winbox متصل شده صفحات را دانلود کنید تغییرات را اعمال کرده (مسلماً باید تا حدودی زبان HTML بدانید) و سپس صفحات را به جای صفحات اصلی قرار دهید. نگران نباشید در صورت بروز هر گونه اشتباه به راحتی می‌توانید صفحات پیش فرض را جایگزین کنید.

❖ تنظیمات Radius برای اتصال به NetBill

برای تنظیم ارتباط Mikrotik Hotspot RAS Server به NetBill مانند شکل زیر از قسمت Radius روی  کلیک می‌کنیم ، در قسمت Service گزینه Hotspot را انتخاب می‌کنیم ، گزینه Address همان IP سرور NetBill باید باشد که در اینجا ۱۷۲,۲۰,۲۰,۲ می‌باشد. در قسمت Secret یک کلمه رمز برای ارتباط Mikrotik با NetBill انتخاب می‌کنیم. توجه کنید که این کلمه رمز را باید در NetBill نیز وارد کنید. Timeout را برابر 3000 ms قرار می‌دهیم و Src.Address همان IP میکروتیک می‌باشد.

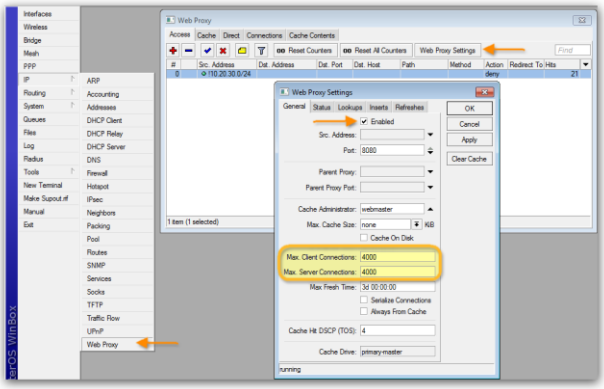


همچنین مطابق شکل زیر با کلیک بر روی گزینه Incomming مقدار Port را برابر ۱۷۰۰ قرار می‌دهیم.

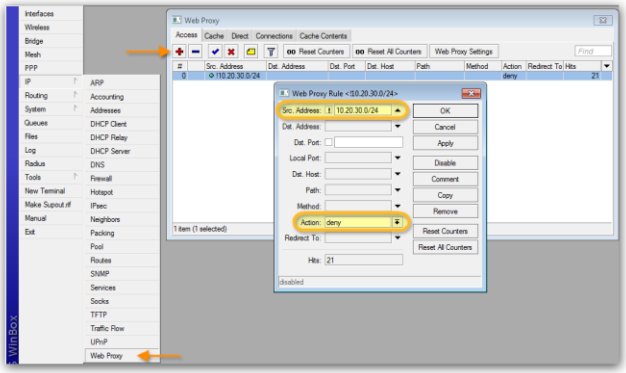


❖ تنظیمات مربوط Web Proxy برای تهیه گزارش Log Browse URL :

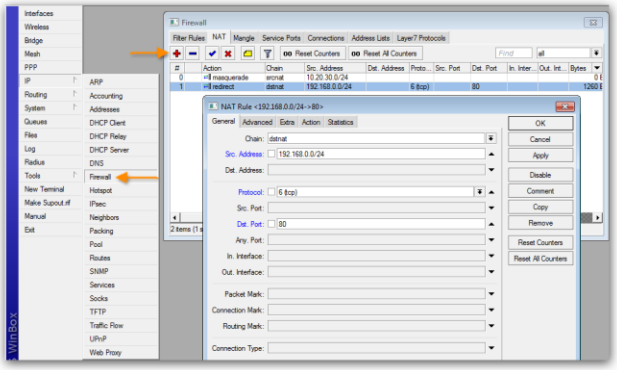
ابتدا مطابق تصویر زیر IP → Web proxy → Web Proxy Settings را تنظیم می‌کنیم.

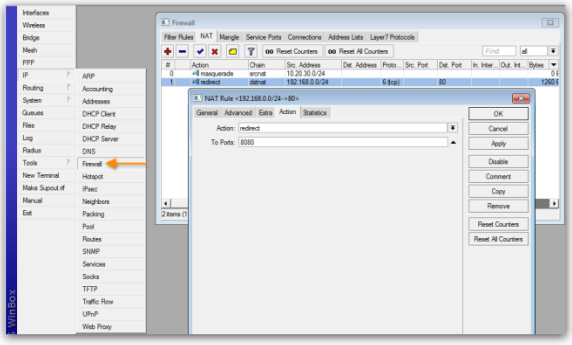


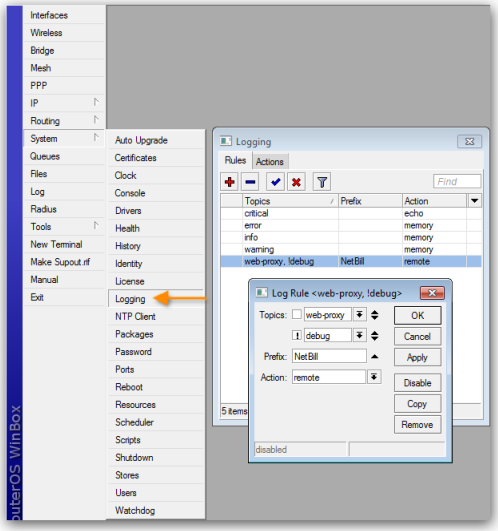
سپس از سربرگ Access روی گزینه  کلیک می‌کنیم، در اینجا دسترسی غیر از Source Address داخلی خود را به Web Proxy ممنوع می‌کنیم.

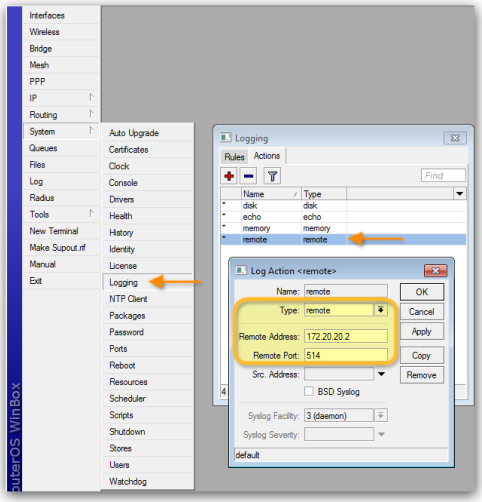


حال باید از قسمت NAT → Firewall → IP یک Redirect NAT تعریف کنیم که کاربران بعد از اتصال به Web Proxy هدایت شوند. مانند تصویر زیر عمل می‌کنیم.



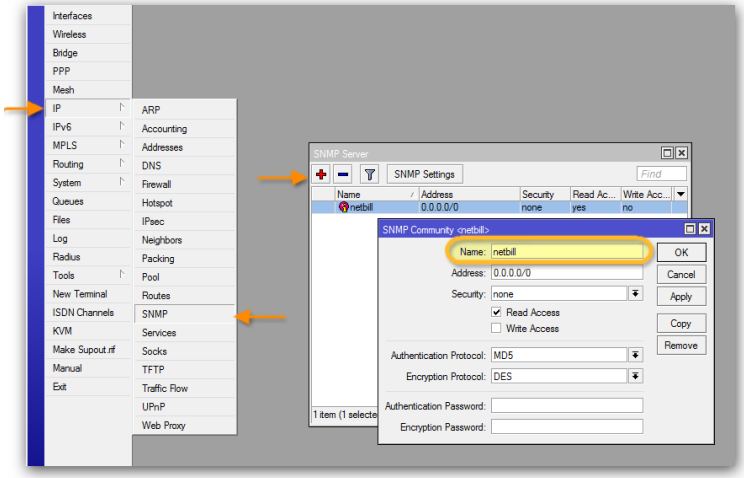






❖ تنظیم SNMP برای تهیه و ثبت Graph

برای راه اندازی و تنظیم SNMP جهت تهیه و ثبت گزارشات Graph در NetBill به مانند تصویر زیر از منوی IP گزینه SNMP را انتخاب و به مانند تصویر با کلیک بر روی Add یک SNMP فقط خواندنی اضافه می‌کنیم.



در مر حله بعد مانند شکل زیر با کلیک بر روی SNMP Setting و فعال کردن گزینه Enabled آنرا فعال می‌کنیم.