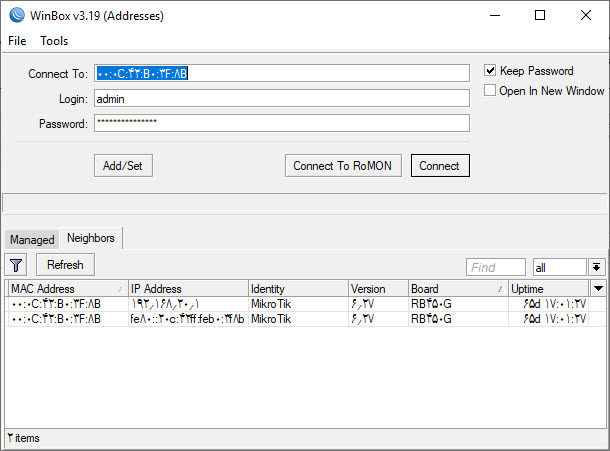
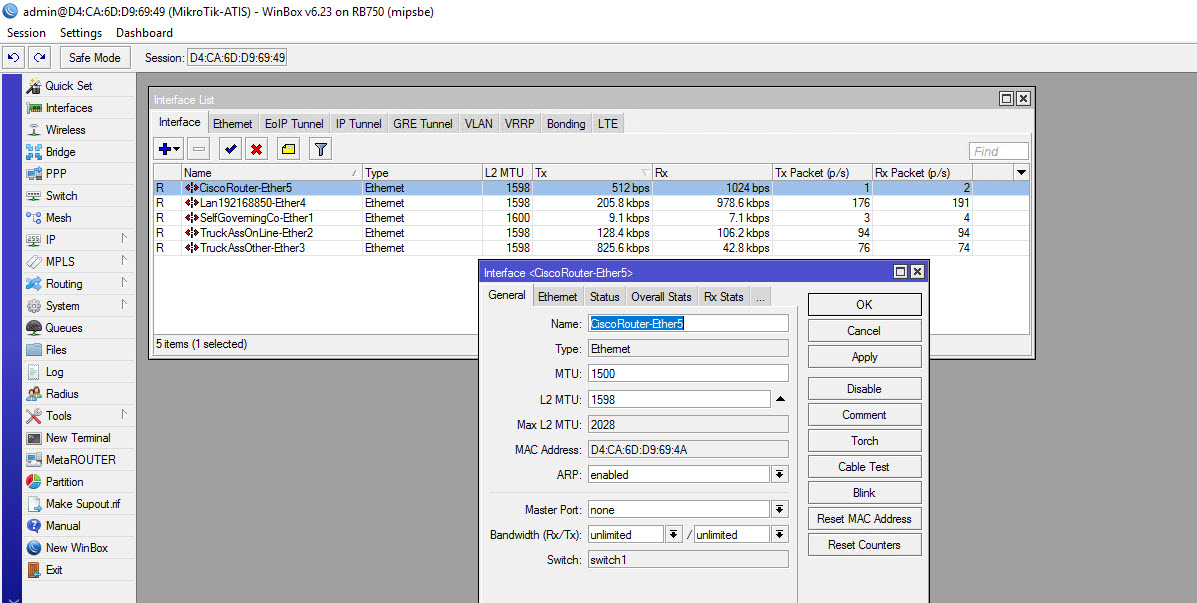
روتر بورد میکروتیک

برای اتصال به روتر ابتدا می بایست برنامه WinBox را دانلود نماییم.WinBox به طور خودکار لیست کاملی از تمامی تجهیزات میکروتیک موجود در شبکه را شناسایی کرده و نمایش می دهد.امکان اتصال هم با MAC وجود دارد و هم با IP . در صورتی که IP تجهیز در دسترس نباشد Mac Address تجهیز مورد نظر را انتخاب و سپس Connect را فشار می دهیم.

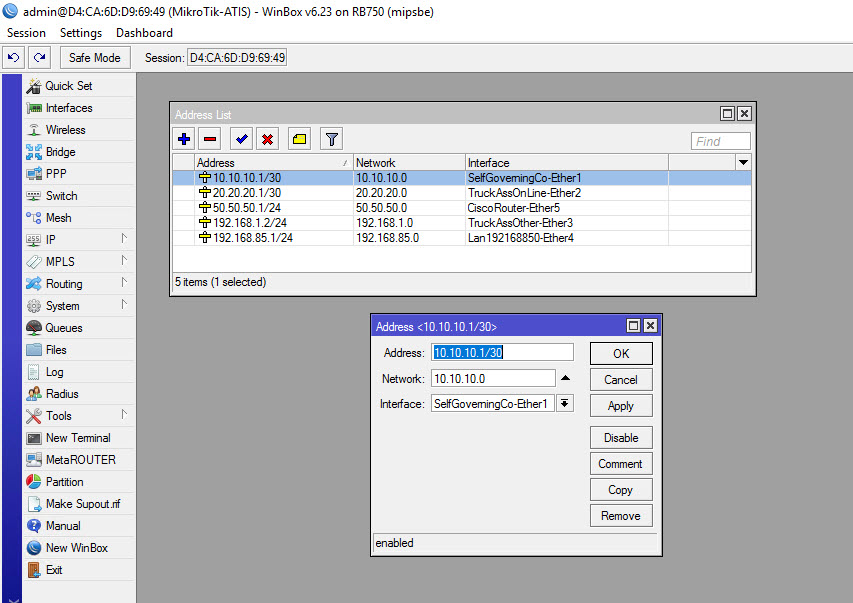
لاگین به روتر میکروتیک پایانه RB750 : Login=admin Password=Biinfo878aC

Interfaces

در قسمت Interfaces لیست اینترفیس های میکروتیک نمایش داده می شود.با دوبار کلیک مشخصات اینترفیس مورد نظر قابل ویرایش است.

|  |  |  |
| --- | --- | --- |
| Interfaces | | |
| Type | Name | Ethernet Port |
| Ethernet | SelfGoverningCo-Ether1 | 1 |
| Ethernet | TruckAssOnLine-Ether2 | 2 |
| Ethernet | TruckAssOther-Ether3 | 3 |
| Ethernet | Lan192168850-Ether4 | 4 |
| Ethernet | CiscoRouter-Ether5 | 5 |

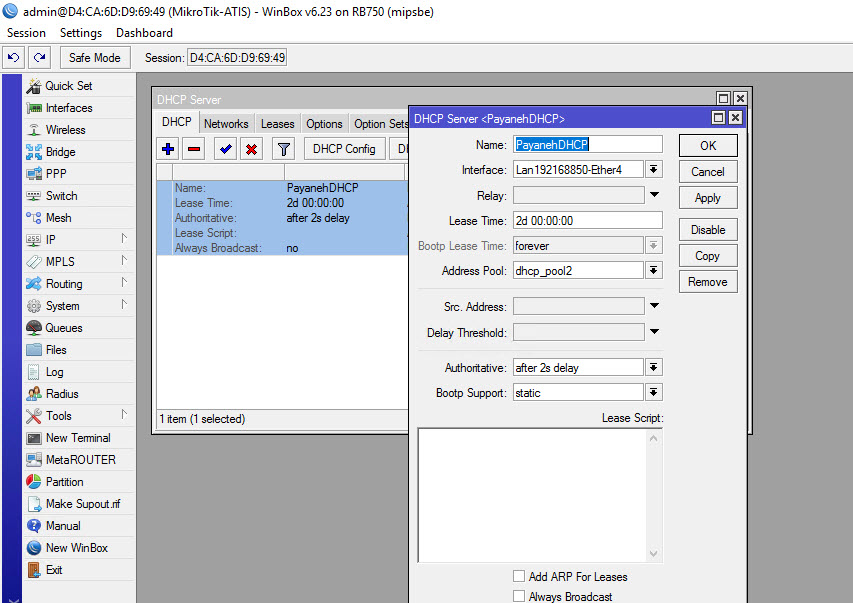
IP/Addresses

در قسمت IP/Addresses امکان تنظیم IP و مشخصات Lan متصل به هر اینترفیس وجود دارد.

|  |  |  |
| --- | --- | --- |
| IP/Address List | | |
| Interface | Network | Address |
| SelfGoverningCo-Ether1 | 10.10.10.0 | 10.10.10.1/30 |
| TruckAssOnLine-Ether2 | 20.20.20.0 | 20.20.20.1/30 |
| TruckAssOther-Ether3 | 192.168.1.0 | 192.168.1.2/24 |
| Lan192168850-Ether4 | 192.168.85.0 | 192.168.85.1/24 |
| CiscoRouter-Ether5 | 50.50.50.0 | 50.50.50.1/30 |

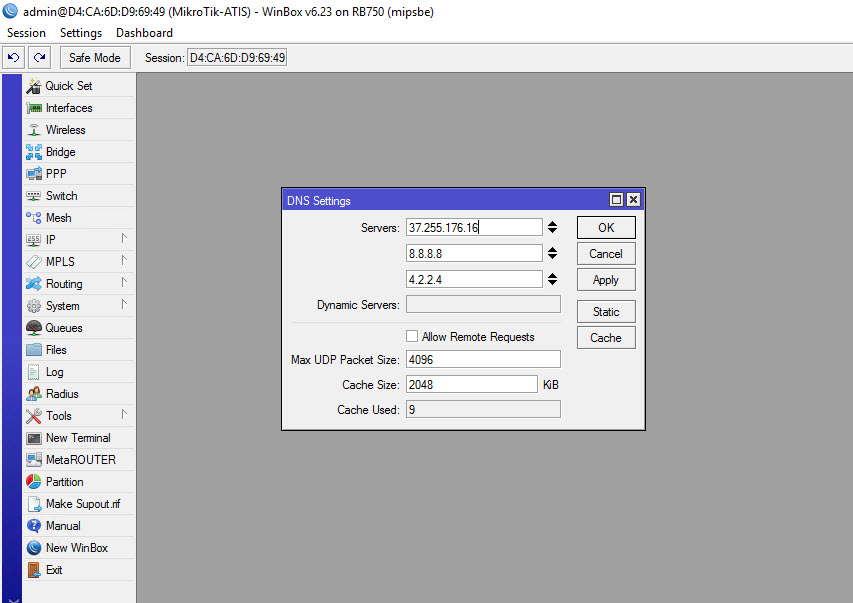
IP/DHCP Server

امکان تعریف چندین DHCP به صورت همزمان در میکروتیک وجود دارد.هر DHCP به صورت مجزا روی یک اینترفیس فعال می باشد.در پایانه DHCP روی اینترفیس Lan192168850-Ether4 فعال می گردد و به شبکه عمومی پایانه سرویس دهی می کند.شبکه بخش مدیریت از طریق روتر سیسکو تغذیه می شود.

نکته : در پایانه آی پی شروع از عدد 51 می باشد.50 آی پی اول 2 روز ، رزرو هستند.

IP/DNS

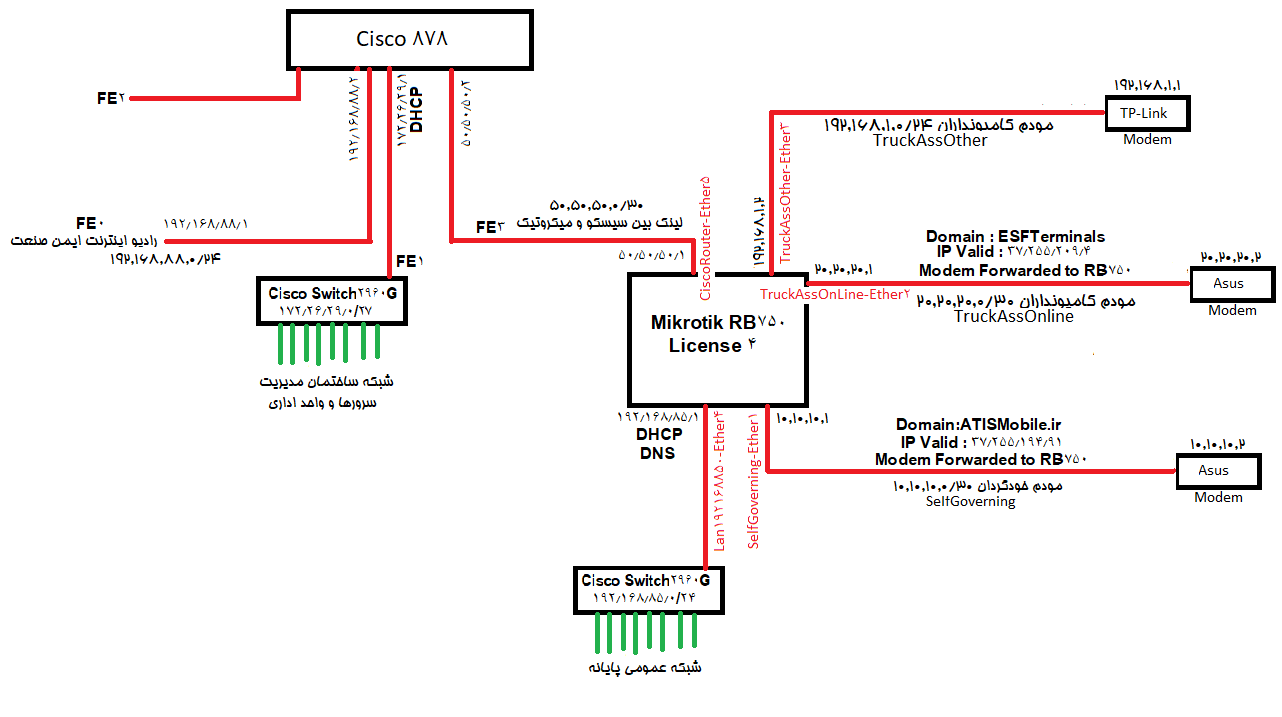
امکان تعریف DNS در میکروتیک نیز وجود دارد تمام سیستم هایی که از میکروتیک IP می گیرند به طور خودکار DNS را هم دریافت می کنند.



برای پروگرام روتر به نحوی که امکان پوشش چندین شبکه و چندین اینترنت وجود داشته باشد می بایست مراحلی را به ترتیب انجام داد.ابتدا لیست آدرس ها در قسمت IP/Firewall/Address Lists تنظیم می گردند سپس از طریق IP/Firewall/Mangle می بایست پاکت ها با Prerouting علامت گذاری گردند و سپس Src-Nat ها و Dst-Nat ها از طریق IP/Firewall/Nat تعریف شوند و سپس فیلترینگ از طریق IP/Firewall/FilterRules انجام گردد.نهایتا از طریق IP/Routes می بایست رکوردهای مسیریابی ایجاد گردد.در روتر بورد RB750 نهایتا 5 اینترفیس موجود است.در روتر مذکور همانطور که در بخش Interfaces آمده ، یک اینترفیس برای ارتباط با Lan عمومی پایانه به نام Lan192168850-Ether4 ، یک اینترفیس برای ارتباط با روتر سیسکو به نام CiscoRouter-Ether5 که شبکه بخش مدیریت پایانه را پوشش می دهد و به نوعی ضمن تامین ارتباط با شبکه مدیریت برای شبکه عمومی پایانه امکان ارتباط با اینترنت شرکت ایمن صنعت (اینترنت سازمان) را نیز فراهم می نماید ، یک اینترفیس برای ارتباط با مودم تامین کننده اینترنت شرکت خودگردان به نام SelfGoverningCo-Ether1 (مودم در اتاق سرور قرار دارد) ، یک اینترفیس برای ارتباط با مودم تامین کننده اینترنت انجمن صنفی کامیونداران با نام TruckAssOther-Ether3 (مودم داخل کانکس هوشمند قرار دارد) و یک اینترفیس برای ارتباط با مودم تامین کننده اینترنت انجمن صنفی کامیونداران با نام TruckAssOnline-Ether2 (مودم در اتاق سرور قرار دارد) در نظر گرفته شده است.

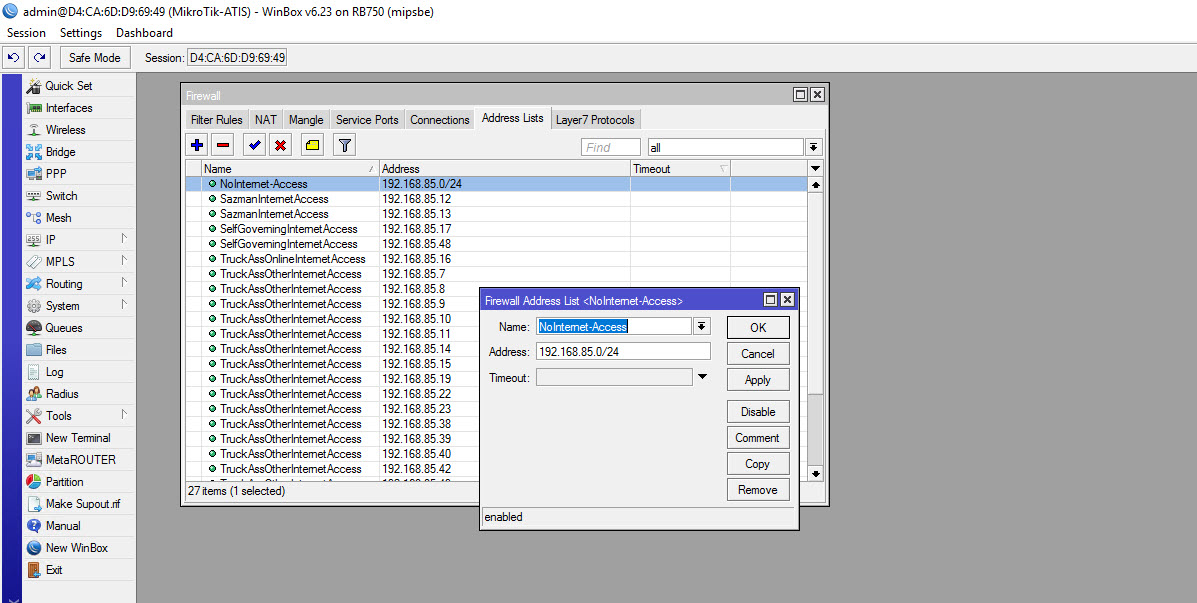
دو Lan در پایانه موجود است که عبارتند از : شبکه اول شبکه Lan عمومی پایانه شامل کلیه شرکت های حمل و نقل ، سالن اعلام بار ، خودگردان و کلیه گیت های تردد با آدرس 192.168.85.0/24 و شبکه دوم شبکه Lan بخش ساختمان مدیریت پایانه است که شامل سرور ها و بخش اداری است با آدرس 172.26.29.0/27 .

|  |
| --- |
| 192.168.85.0/24 255.255.255.0 : 192.168.85.1 192.168.85.254 |
| 172.26.29.0/27 255.255.255.224 : 172.26.29.1 172.26.29.30 |



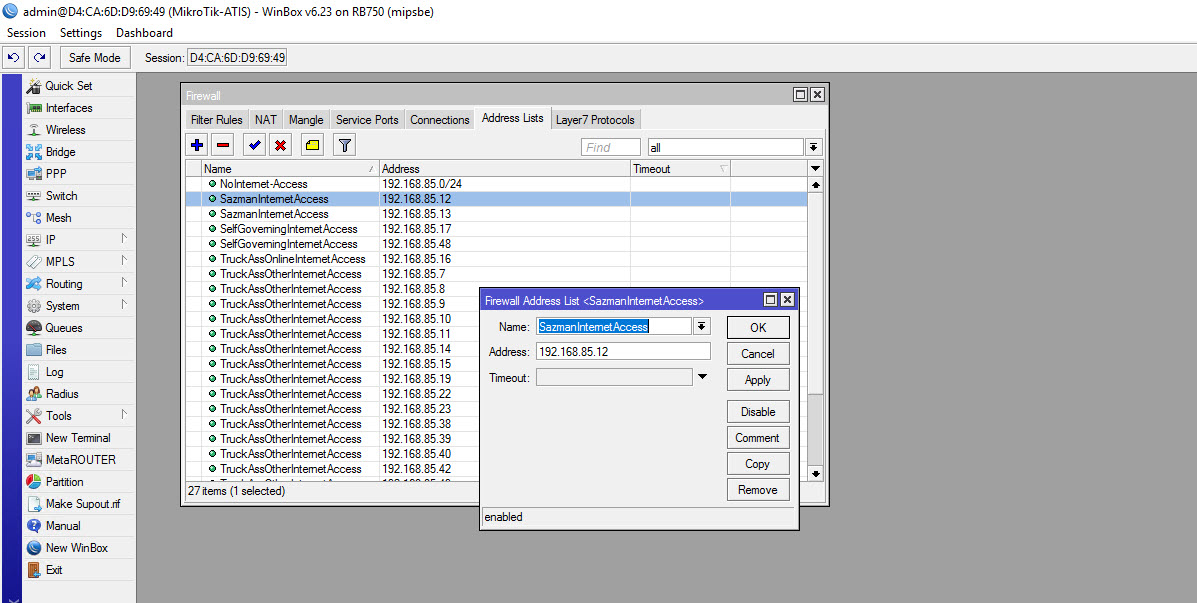
تنظیم و دسته بندی لیست آدرس های شبکه

IP/Firewall/Address Lists

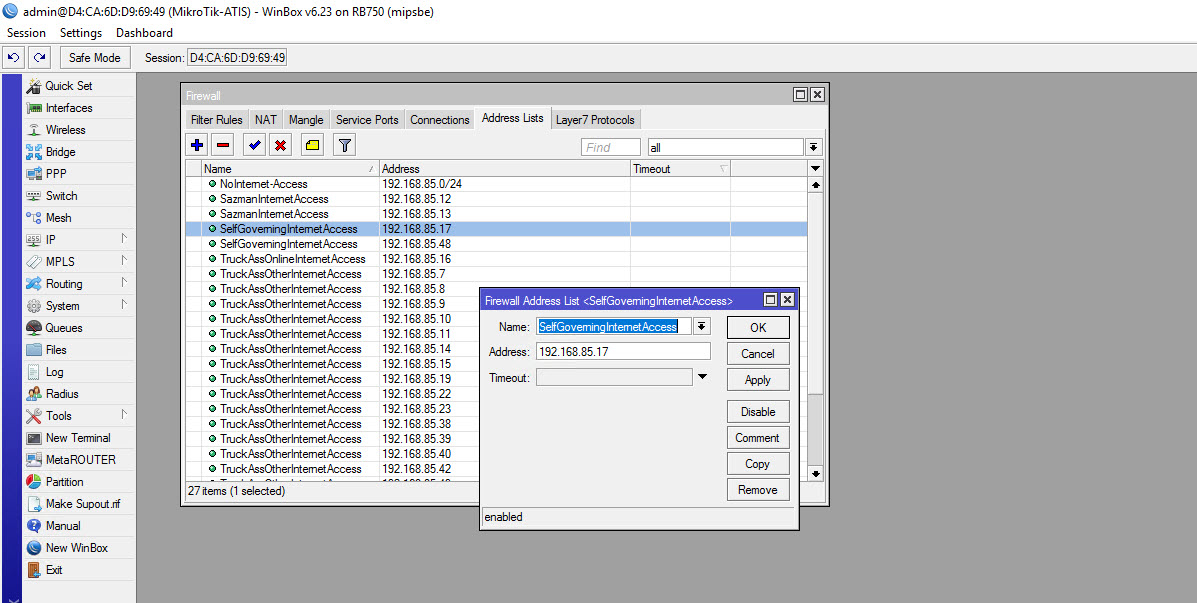
آیتم NoInternet-Access شامل کل شبکه عمومی پایانه است.یعنی 192.168.85.0/24 که آی پی کلیه شرکت های حمل و نقل ، سالن اعلام بار و گیت های تردد و شرکت خودگردان را در بر دارد.با توجه به آنکه تامین اینترنت کل شبکه با ما نیست پس این لیست ایجاد می شود تا از دسترسی آی پی های مورد نظر به خارج از میکروتیک

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP/Firewall/Address Lists** | | | | |
| NoInternet-Access | SazmanInternetAccess | TruckAssOnlineInternetAccess | TruckAssOtherInternetAccess | SelfGoverningInternetAccess |

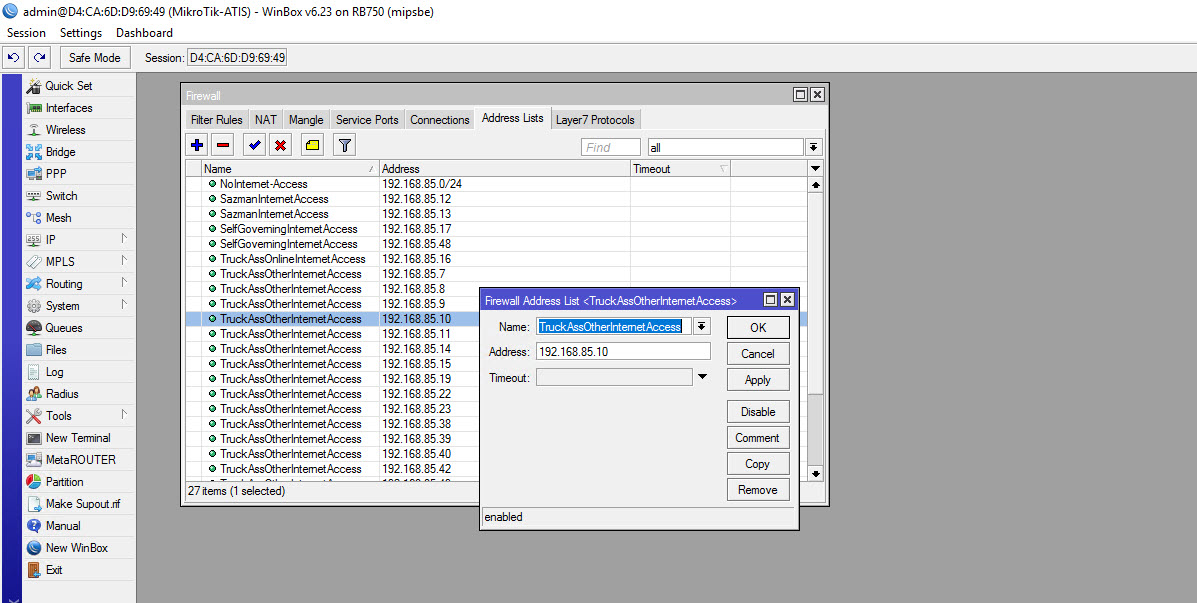
آیتم SazmanInternetAccess مواردی هستند که می خواهیم از اینترنت سازمان (دکل بالای سقف سالن اعلام بار رادیو وایرلس شرکت ایمن صنعت تلفن 32731320-32731321 با آی پی 192.168.88.1) استفاده کنند در واقع پاکت های این لیست از طریق RB750 به سمت اینترفیس 50.50.50.1 که به روتر سیسکو متصل هست (آی پی اینترفیس سیسکو 50.50.50.2 ) می باشد مسیریابی می شوند.در روتر سیسکو اینترفیس متصل به RB750 دارای آی پی 50.50.50.2 است و پاکت های رسیده از 50.50.50.1 را با مقصد 0.0.0.0/0 به سمت اینترفیس 192.168.88.2 متصل به رادیو اینترنت سازمان شرکت ایمن صنعت مسیریابی می کند.آی پی رادیو هم 192.168.88.1 می باشد.



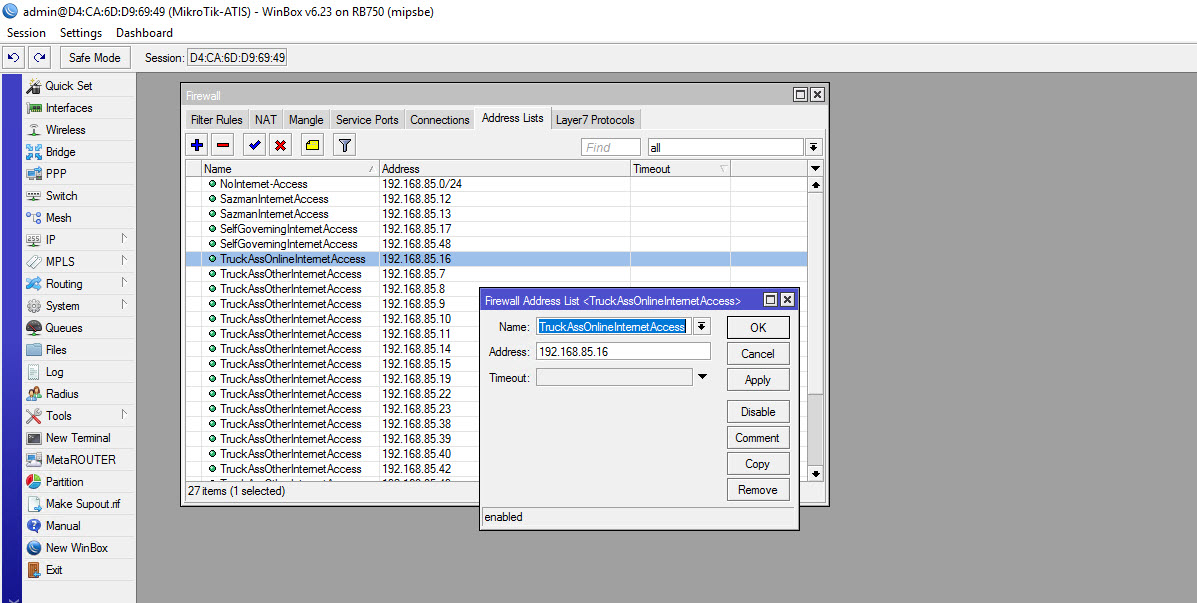
لیست SelfGoverningInternetAccess شامل آی پی هایی است که می خواهیم از اینترنت شرکت خودگردان پایانه استفاده نمایند.خط تلفن 33868350 از طریق کابلی از کافو به رک اتاق سرور منتقل شده است و شامل اینترنت ADSL و آی پی استاتیک با شماره 37.255.194.91 است.مودم AsusN14 برای ارتباط استفاده شده است و مودم دارای آی پی 20.20.20.2 می باشد و در رک اتاق سرور مستقر می باشد.در مودم مذکور در بخش DMZ می بایست پاکت ها به سمت اینترفیس 20.20.20.1 روتر RB750 فوروارد شوند.در روتر RB750 و توسط Dst-Nat پاکت های مذکور به آی پی 192.168.85.17 مسیریابی می شوند.192.168.85.17 سرور آتیس است که سایت ATIS و وب سرویس های مرتبط با ATISMobile بر روی آن قرار دارند.سرور مذکور خود یک هاست اینترنتی است که دارای DNS Server به منظور میزبانی از دامنه ATISMobile.ir است.



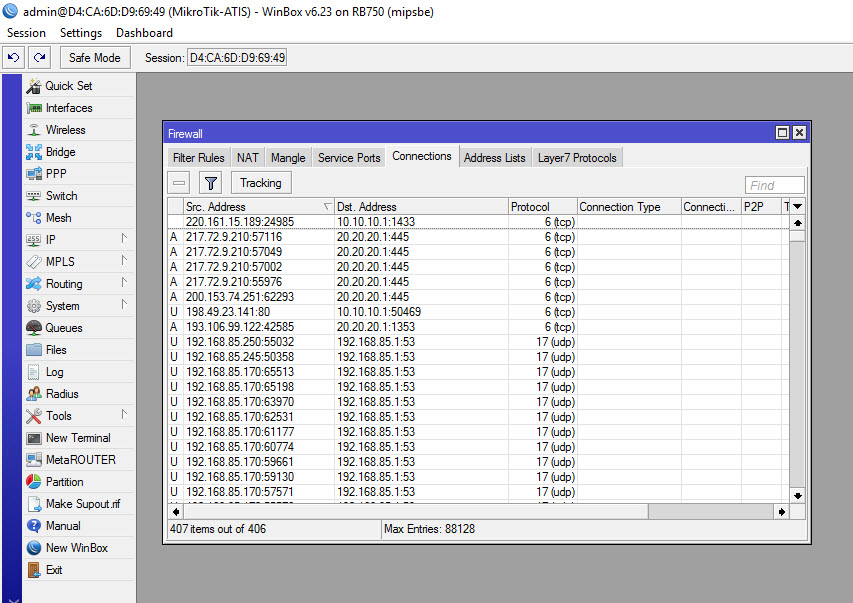
انجمن کامیونداران دارای دو مودم می باشد که با نام TruckAssOnLine و TruckAssOther در مجموعه نام گذاری شده اند.لیست مرتبط با TruckAssOnline با نام TruckAssOnLineInternetAccess ایجاد شده است و لیست مرتبط با TruckAssOther با نام TruckAssOtherInternetAccess ایجاد شده است.مودم مرتبط با لیست TruckAssOtherInternetAccess در کانکس هوشمند خود انجمن قرار دارد و با یک کابل به اتاق سرور مرتبط است.کابل مذکور هوایی و از طریق سقف سالن اعلام بار داخل سینی کابل ها منتقل شده است. آی پی مودم 192.168.1.1 می باشد.آی پی اینترفیس RB750 دارای شماره 192.168.1.2 می باشد.در این لینک آی پی استاتیک نداریم.هزینه شارژ و نگهداری مودم مذکور از طریق خود انجمن مستقیما صورت می گیرد.



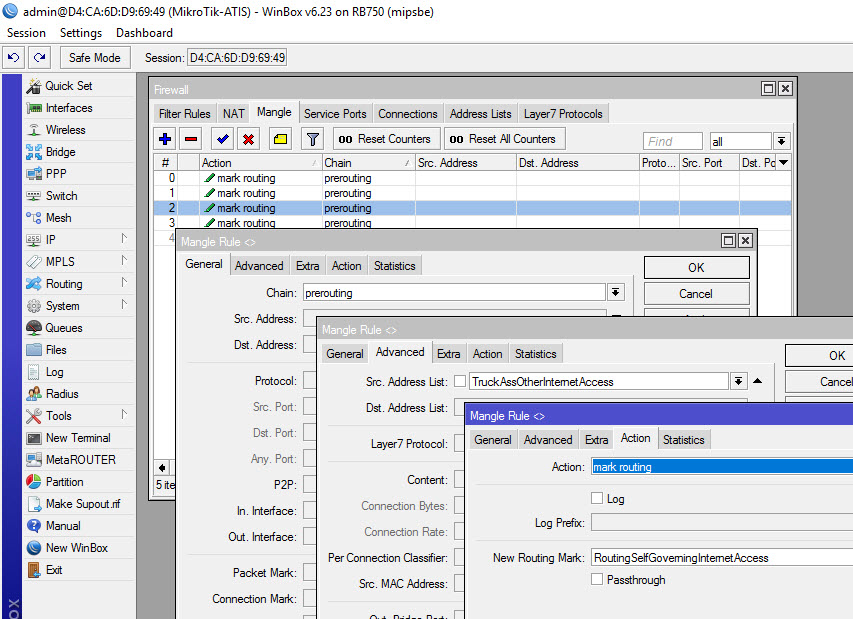
مودم مرتبط با لیست TruckAssOnLineInternetAccess از نوع AsusN14 هست و در رک اتاق سرور قرار دارد.اینترنت ADSL دارد با شماره 33870111 و کابل آن از کافو به اتاق سرورهمراه با خطوط 33868350 و 33863070 و 33863080 و 33864300 منتقل شده است.آی پی استاتیک 37.255.209.4 در خط موجود است و از طریق مودم بخش DMZ به آی پی 20.20.20.1 یعنی اینترفیس روتر فوروارد شده است.از طریق آی پی استاتیک مذکور وب سرویس آنلاین نوبت با پایانه های استان مرتبط است و سیستم TWS را شامل می شود.در RB750 از طریق Dst-Nat پاکت های رسیده از مودم مذکور به آی پی 192.168.85.16 فوروارد می شوند.



از طریق IP/Firewall/Connections می توان کانکشن های فعال را مشاهده نمود.



مرحله بعد در پروگرام روتر نشانه گذاری پاکت ها است که از طریق IP/Firewall/Mangle انجام می گردد.

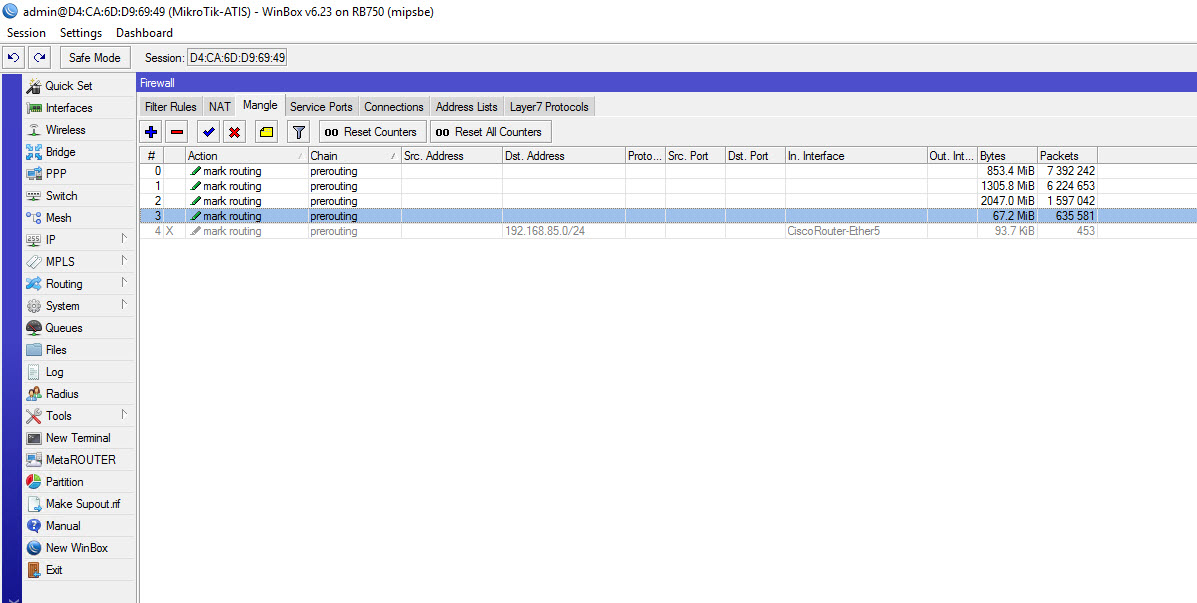


در این قسمت در تب General می بایست Chain=Prerouting باشد و در تب Advanced باید Src.AddressList=TargetList باشد.منظور از TargetList لیستی است که از طریق IP/Firewall/Address Lists ایجاد شده است.در تب Action می بایست Action=Mark Routing باشد و در قسمت New Routing Mark نیز یک نام جدید تایپ نماییم.

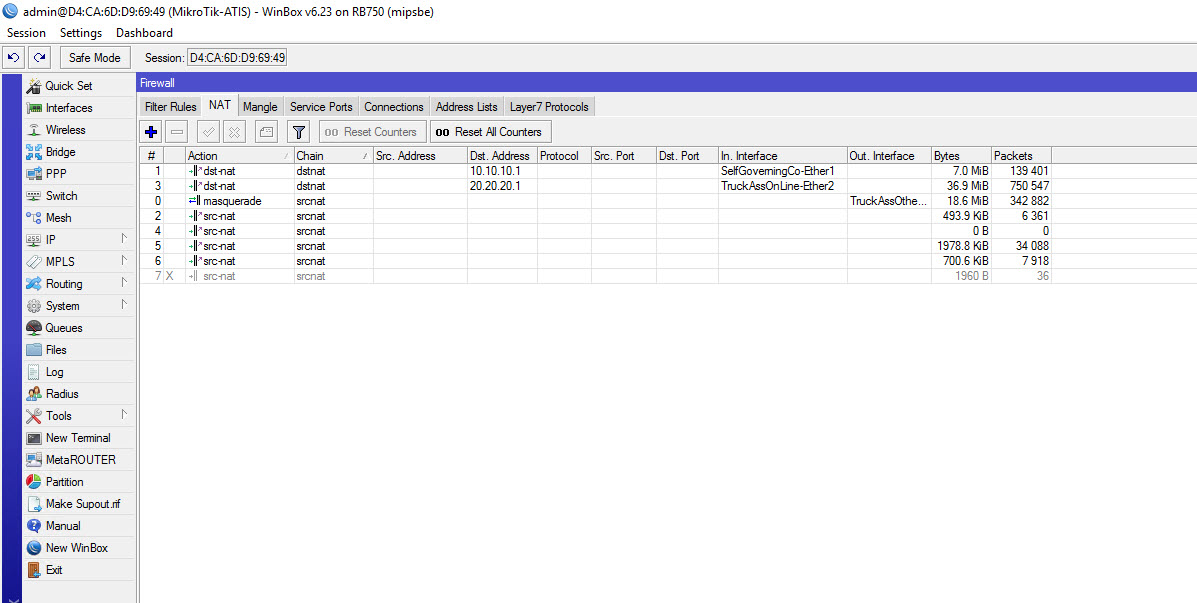
نکته : اگر نام هایی ایجاد نماییم ولی بعد نام جدید دیگری تایپ نماییم و از نام های قبلی در Nat یا Filter و یا Route استفاده نکنیم با یک بار Reboot روتر ، نام ها حذف می گردند.

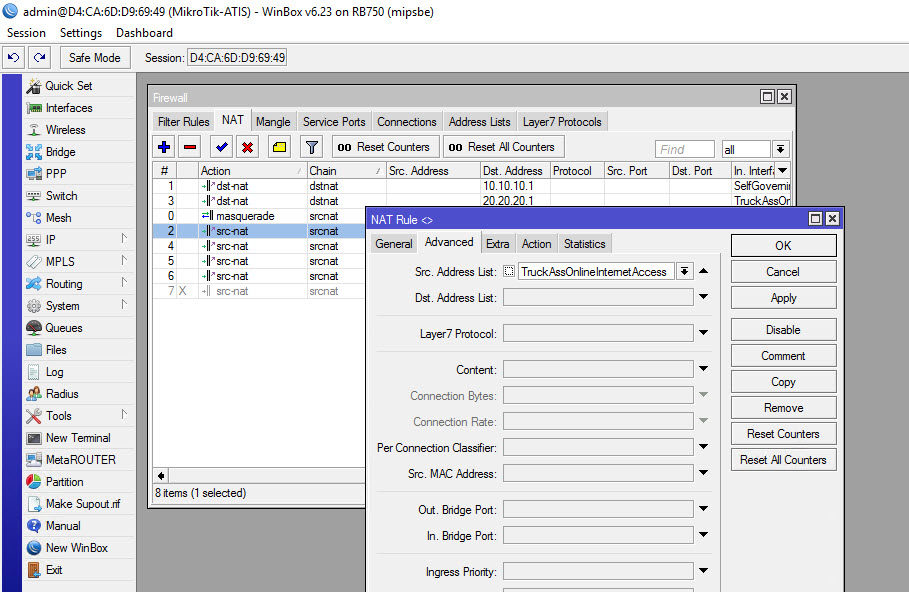
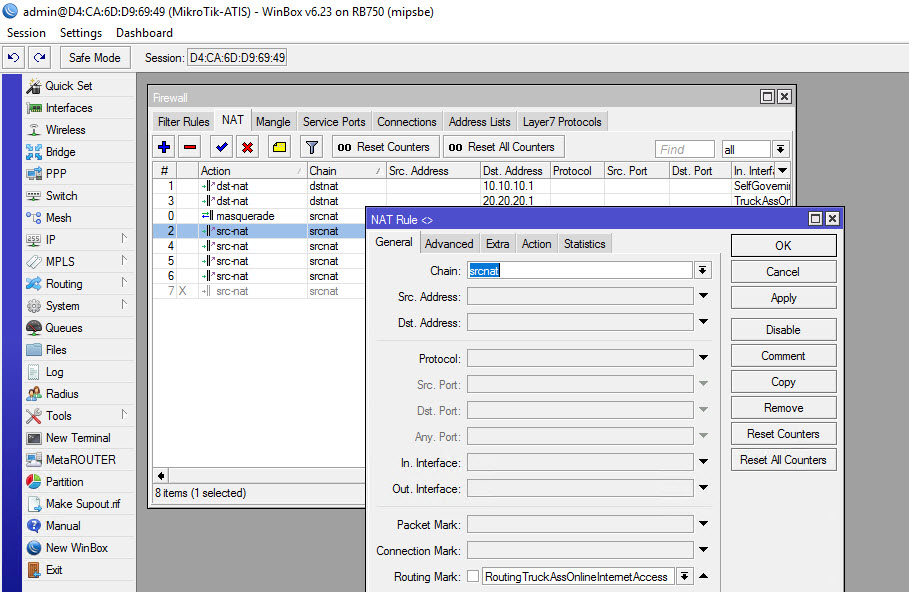
به طور کلی می بایست برای تمام لیست های موجود در IP/Firewall/Address Lists مانگل ایجاد کرد که در پایانه از Chain=Prerouting استفاده می کنیم.

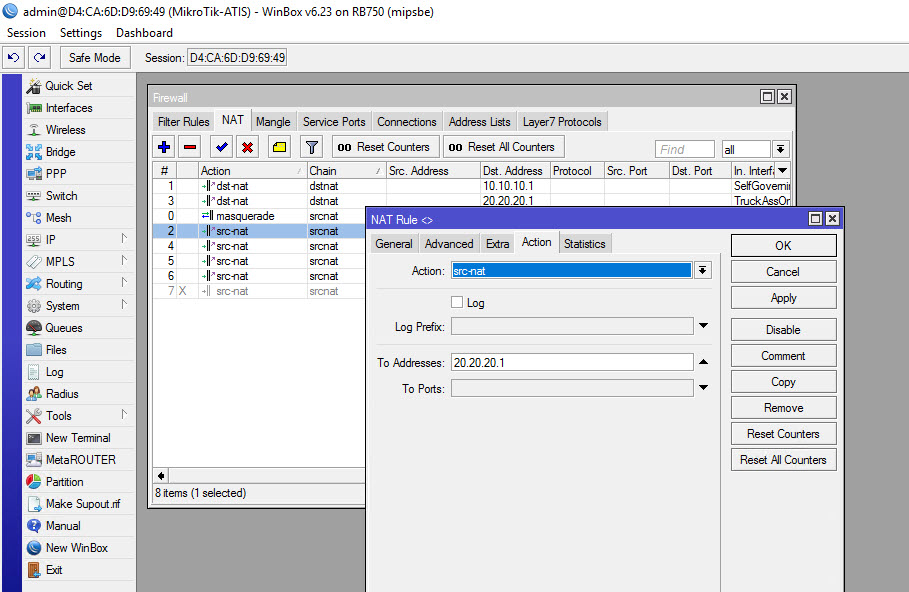
|  |  |  |  |
| --- | --- | --- | --- |
| IP/Firewall/Mangle | | | |
| **Action/New Routing Mark** | **Action/Action** | **Advanced/Src.Address List** | **General/Chain** |
| RoutingTruckAssOnlineInternetAccess | MarkRouting | TruckAssOnlineInternetAccess | Prerouting |
| RoutingTruckAssOtherInternetAccess | MarkRouting | TruckAssOtherInternetAccess | Prerouting |
| RoutingSelfGoverningInternetAccess | MarkRouting | SelfGoverningInternetAccess | Prerouting |
| RoutingSazmanInternetAccess | MarkRouting | SazmanInternetAccess | Prerouting |



مرحله بعد از ایجاد مانگل یا نشانه گذاری پاکت ها باید عملیات Nat انجام گردد.طی این عملیات می بایست Src-Nat ها و Dst-Nat ها را ایجاد نماییم.برای کلیه اینترفیس هایی که برای تامین اینترنت در نظر گرفته ایم می بایست Src-Nat ایجاد گردد و حتی برای اینترفیس CiscoRouter-Ether5 نیز باید Src-Nat ایجاد نماییم.برای اینترفیس هایی که آی پی پابلیک دارند نیز باید Dst-Nat ایجاد نماییم.

ابتدا به ساکن یک Src-Nat=Masquerade باید ایجاد نماییم به نحوی که اینترفیسی از روتر که اینترنت عمومی را فراهم می کند باید در Out-Interface قرار گیرد و Action=Masquerade باشد.سپس می بایست برای هر لیست یک Src-Nat ایجاد نماییم و لیست مورد نظر را به یک اینترفیس Nat نماییم.





امکان ایجاد Nat روی یک اینترفیس با چند لیست وجود ندارد و برای هر اینترفیس فقط میشه یک Nat ایجاد کرد که منطقی نیز هست و دو Nat به نوعی یک درخواست غیرمنطقی هست.

پس از ایجاد Src-Nat ها باید برای اینترفیس هایی که آی پی Public دارند Dst-Nat ایجاد نماییم.

در واقع می بایست آی پی Public را به آی پی Static در شبکه که اصولا یک سرور می باشد Dst-Nat نماییم.سرور مذکور دارای وب سرویس ها و سرویس هایی است که به صورت Public می بایست در اینترنت قابل دسترس باسند.حتی امکان Remote Desktop یک سرویس است که باید برای دسترسی به یک سرور قبلا Dst-Nat ایجاد شده باشد.

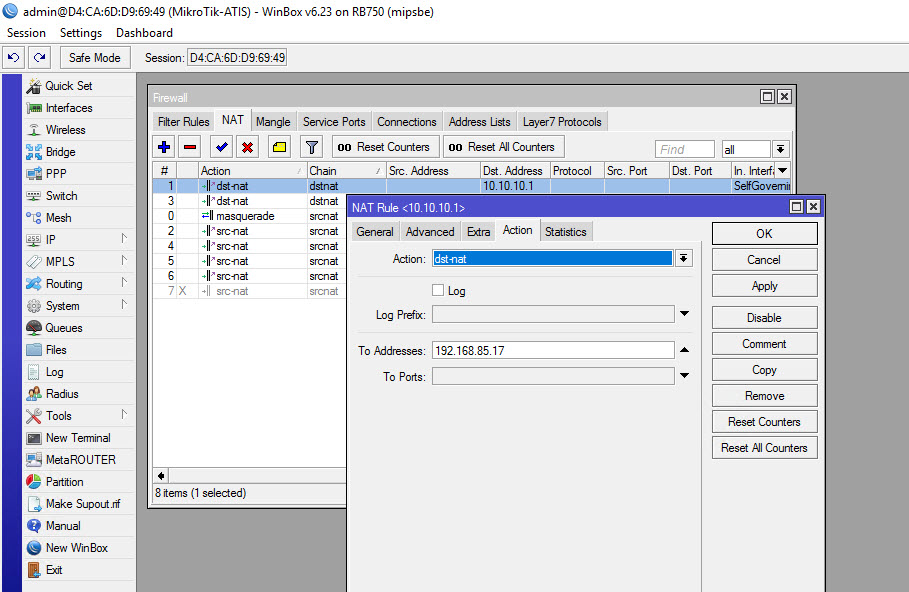
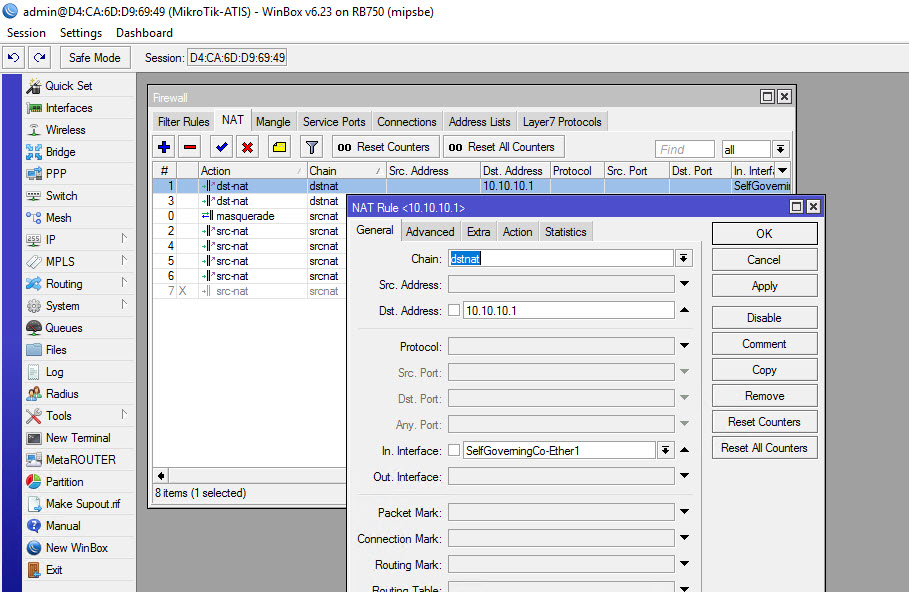
نکته : وقتی مودم به صورت مستقیم به شبکه متصل باشد و نیاز به دسترسی ریموت به شبکه از طریق اینترنت باشد باید در مودم Forwarding انجام داد که معمولا در بخش DMZ مودم وجود دارد.

نکته : در پایانه آی پی 37.255.194.91 روی اینترفیس SelfGoverningCo-Ether1 قرار دارد و به آی پی 192.168.85.17 باید Dst-Nat شود.همینطور آی پی 37.255.209.4 روی اینترفیس TruckAssOnline-Ether2 قرار دارد و به آی پی 192.168.85.16 باید Dst-Nat شود.

نکته : باید توجه کنیم که هر لیست آدرس را که نام گذاری کرده ایم به اینترفیس هم نام خودش Nat نماییم.

نکته : در پایانه روی RB750 برای همه اینترفیس ها باید Src-Nat ایجاد شود.

نکته : با توجه به تعداد آی پی های پابلیک باید 2 مورد Dst-Nat ایجاد نماییم.



نکته : مودم ها به خطوط تلفن وصل می شوند.اینترفیس های روتر RB750 به یکی از پورت های شبکه مودم ها متصل می گردد.از طرفی RB750 از طریق اینترفیس CiscoRouter-Ether5 با آی پی 50.50.50.1 به روتر سیسکو متصل می گردد.لیست SazmanInternetAccess به همین منظور ایجاد شده است تا اگر نیاز باشد امکان تامین اینترنت از روتر سیسکو مهیا باشد.اینترنت در سیسکو از شرکت ایمن صنعت تامین شده است.

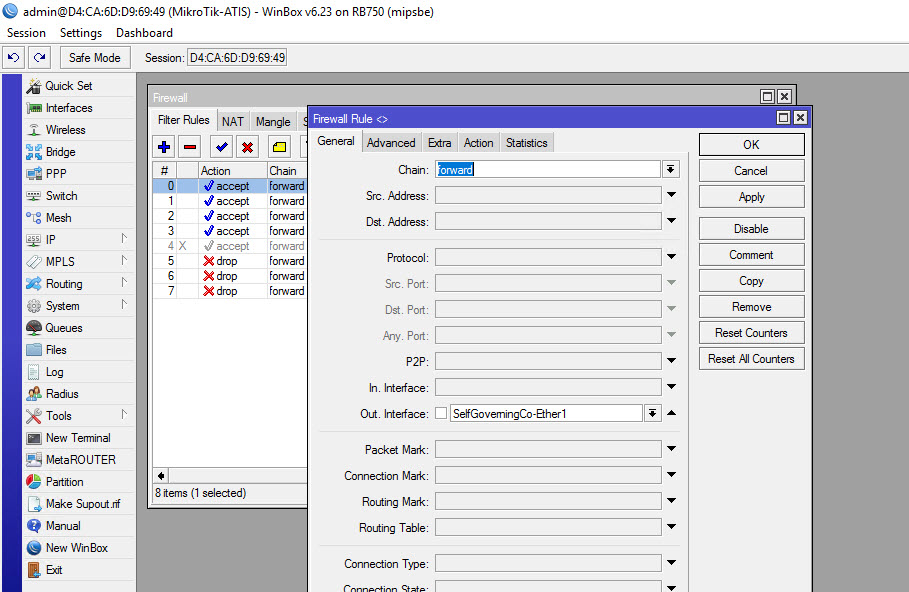
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Src-Nat | | | | |
| **Action/To Addresses** | **Action/Action** | **Src.Address List** | **Routing Mark** | **Chain** |
| 20.20.20.1 | Src-Nat | TruckAssOnlineInternetAccess | RoutingTruckAssOnlineInternetAccess | Src-Nat |
| 192.168.1.2 | Src-Nat | TruckAssOtherInternetAccess | RoutingTruckAssOtherInternetAccess | Src-Nat |
| 10.10.10.1 | Src-Nat | SelfGoverningInternetAccess | RoutingSelfGoverningInternetAccess | Src-Nat |
| 50.50.50.1 | Src-Nat | SazmanInternetAccess | RoutingSazmanInternetAccess | Src-Nat |

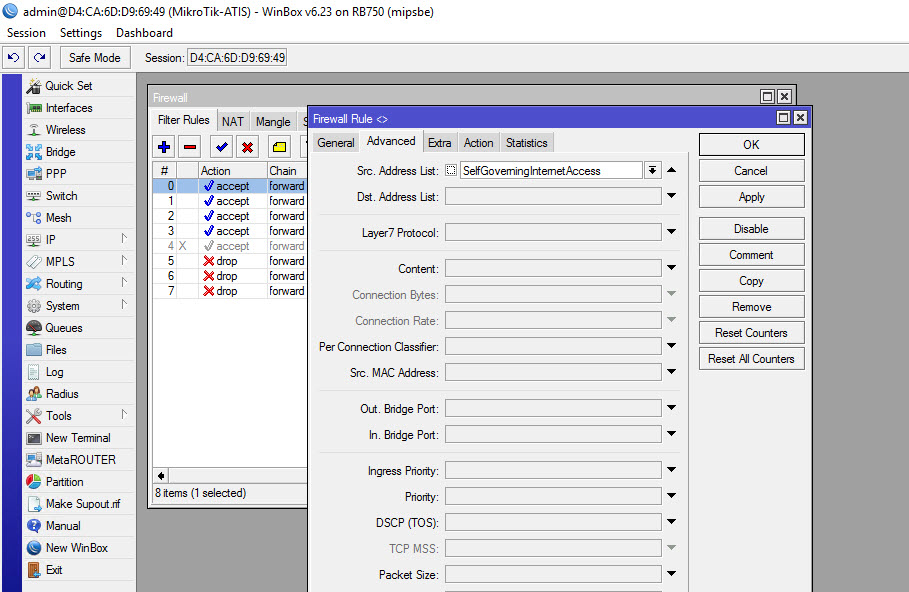
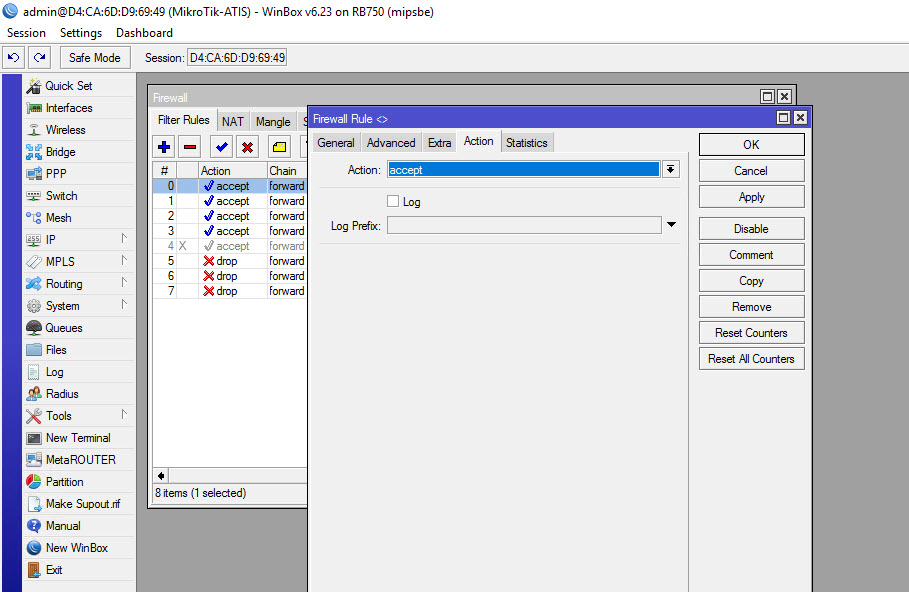
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dst-Nat | | | | |
| **Action/To Addresses** | **Action/Action** | **In.Interface** | **Dst.Address** | **Chain** |
| 192.168.85.17 | Dst-Nat | SelfGoverningCo-Ether1 | 10.10.10.1 | Dst-Nat |
| 192.168.85.16 | Dst-Nat | TruckAssOnline-Ether2 | 20.20.20.1 | Dst-Nat |

مرحله بعدی در پروگرام روتر میکروتیک ایجاد Filter Rules ها است.برای دسترسی به آن از مسیر IP/Firewall/Filter Rules استفاده می کنیم.نیاز است تا دو نوع فیلتر ایجاد گردد.نوع Drop که دسترسی لیست NoInternet-Access را به اینترنت می بندد و دیگری Accept که دسترسی لیست های مجاز به اینترنت را فراهم می نماید.

نکته (بسیار مهم) : باید دقت کنیم که Drop ها بعد از Accept قرار گیرند وگرنه کلیه دسترسی ها قطع می شوند.

نکته : در پایانه برای 4 لیست موجود باید 4 عدد Accept ایجاد گردد.برای بستن دسترسی لیست NoInternet-Access هم باید 3 عدد Drop ایجاد گردد.





|  |  |  |  |
| --- | --- | --- | --- |
| Filter Rules | | | |
| **Action/Action** | **Advanced/Src.Address List** | **General/Out.Interface** | **General/Chain** |
| accept | SelfGoverningInternetAccess | SelfGoverningCo-Ether1 | forward |
| accept | TruckAssOtherInternetAccess | TruckAssOther-Ether3 | forward |
| accept | TruckAssOnlineInternetAccess | TruckAssOnline-Ether2 | forward |
| accept | SazmanInternetAccess | CiscoRouter-Ether5 | forward |
| Drop | NoInternet-Access | SelfGoverningCo-Ether1 | forward |
| Drop | NoInternet-Access | TruckAssOther-Ether3 | forward |
| Drop | NoInternet-Access | TruckAssOnline-Ether2 | forward |

مرحله بعد در پروگرام روتر میکروتیک تنظیم رکوردهای Route هست که بر اساس سیستم های موجود در پایانه مطابق جدول زیر است.نوع DAC را خود روتر پس از تنظیم Interface ها و IP/Address ها ایجاد می کند و نوع AS رو باید ما ایجاد کنیم.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IP/Route List | | | | | |
| **Pref.Source** | **Routing Mark** | **Distance** | **Gateway** | **Dst.Address** | **Type** |
| 10.10.10.1 |  | 0 | SelfGoverningCo-Ether1 | 10.10.10.0/30 | DAC |
| 20.20.20.1 |  | 0 | TruckAssOnline-Ether2 | 20.20.20.0/30 | DAC |
| 50.50.50.1 |  | 0 | CiscoRouter-Ether5 | 50.50.50.0/30 | DAC |
| 192.168.1.2 |  | 0 | TruckAssOther-Ether3 | 192.168.1.0/24 | DAC |
| 192.168.85.1 |  | 0 | Lan192168850-Ether4 | 192.168.85.0/24 | DAC |
|  | RoutingSelfGoverningInternetAccess | 1 | 10.10.10.2 | 0.0.0.0/0 | AS |
|  | RoutingTruckAssOnlineInternetAccess | 1 | 20.20.20.2 | 0.0.0.0/0 | AS |
|  | RoutingSazmanInternetAccess | 1 | 50.50.50.2 | 0.0.0.0/0 | AS |
|  | RoutingTruckAssOtherInternetAccess | 1 | 192.168.1.1 | 0.0.0.0/0 | AS |

21/09/1399

پایان