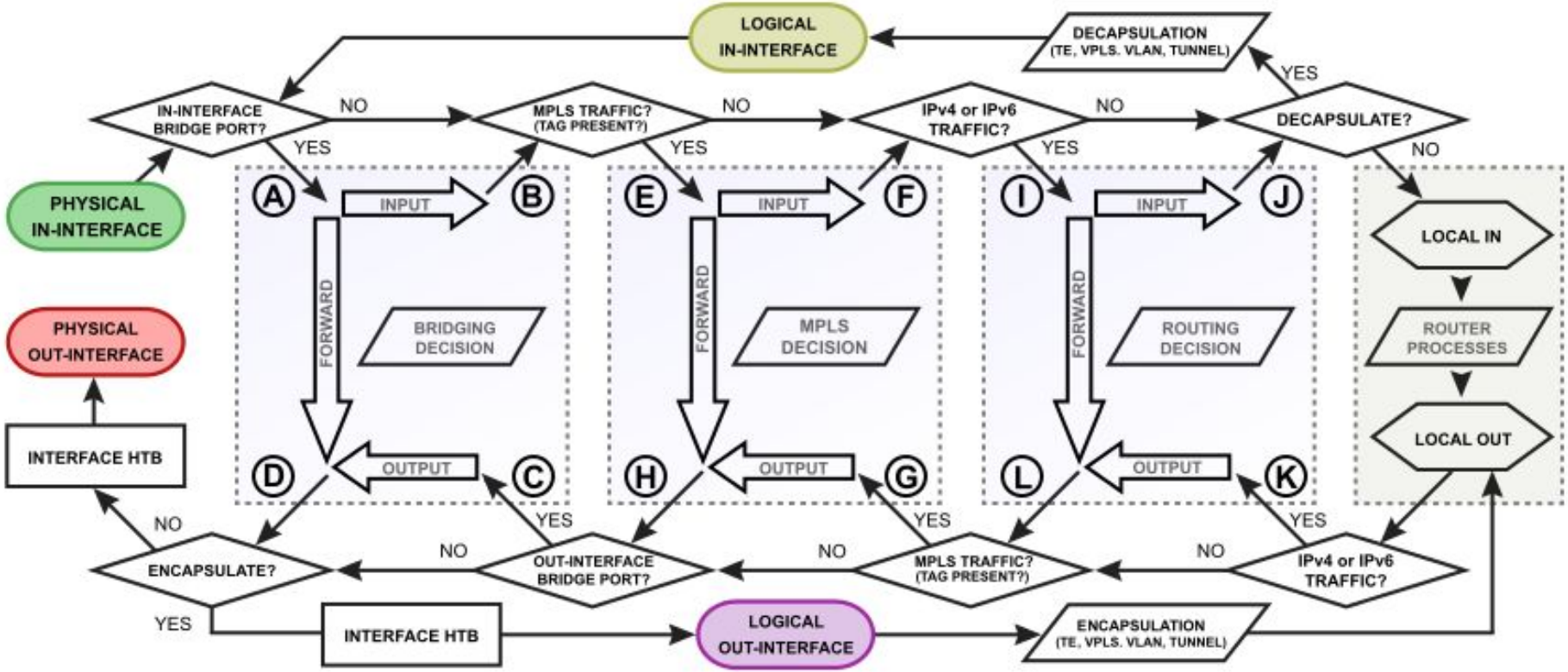
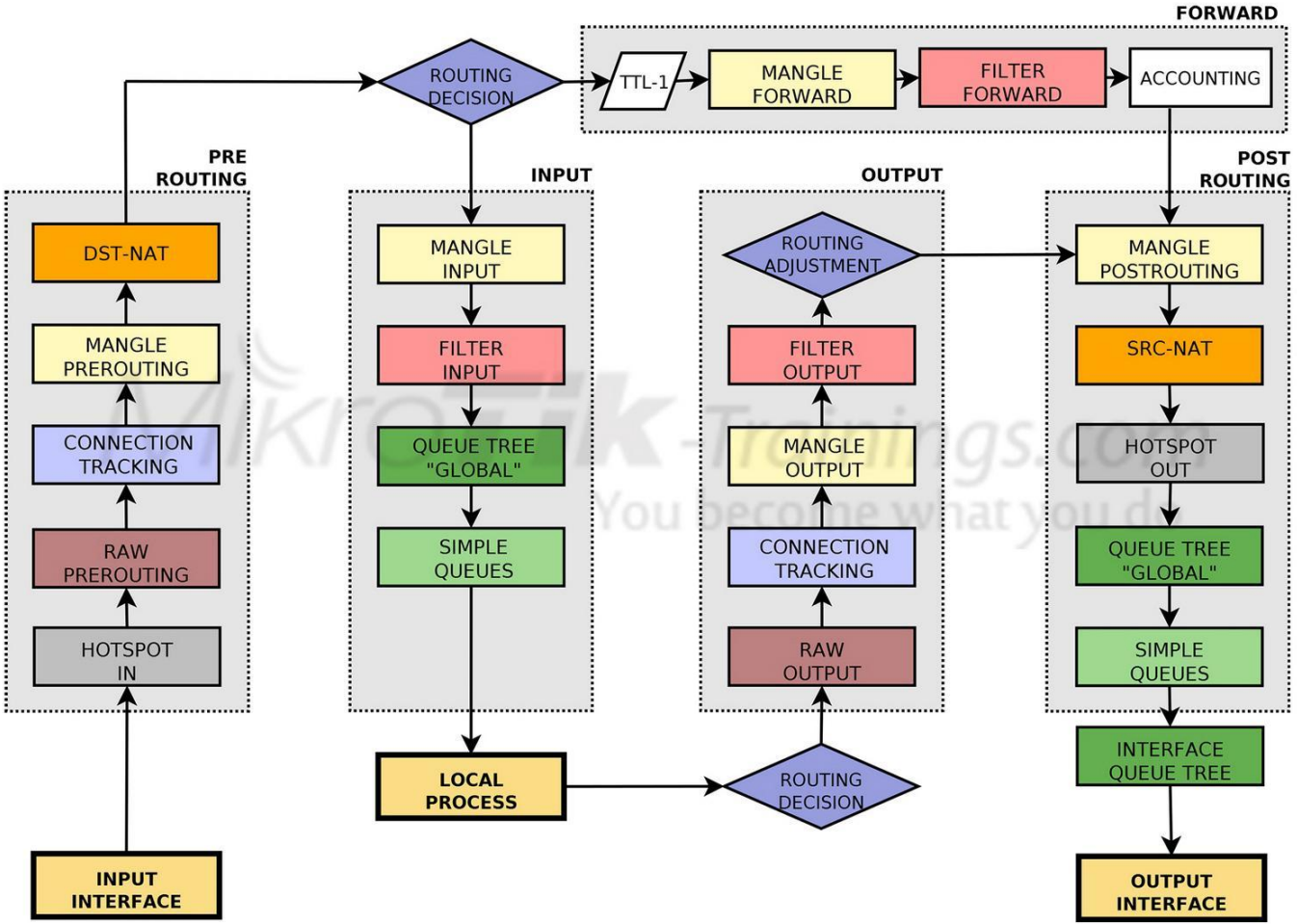
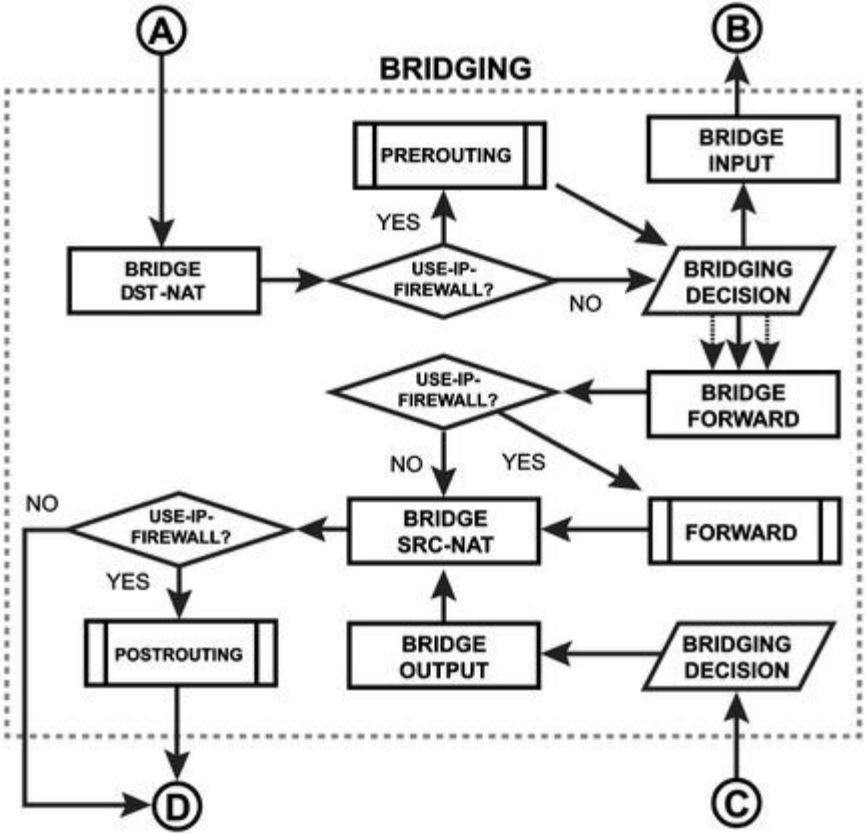
Mikrotik Certified Traffic Control Engineer

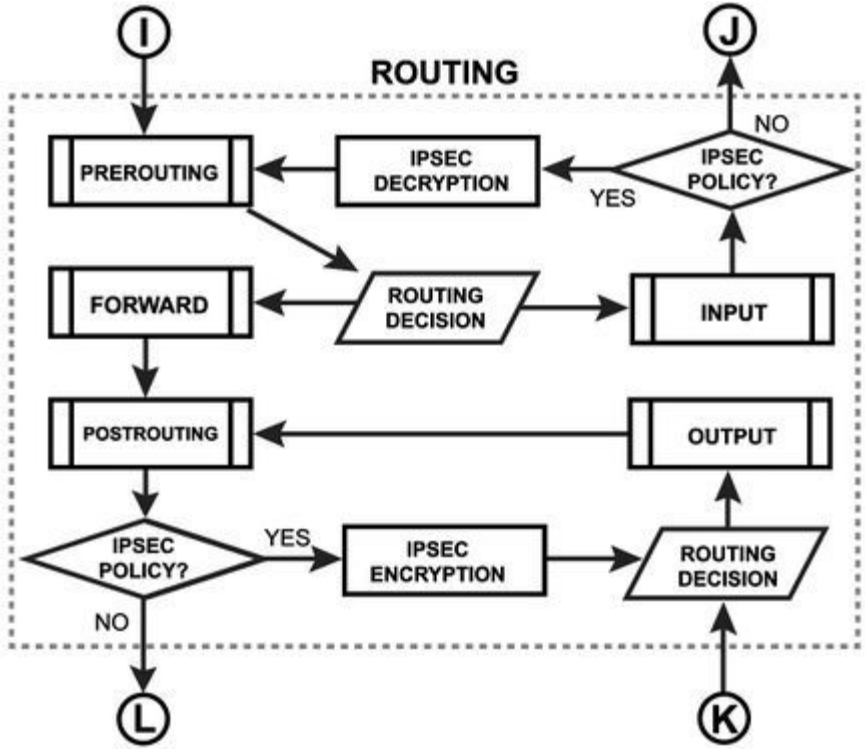
گردآورنده : شاهین واثقی
ویراستار: علیرضا کهن ترابی

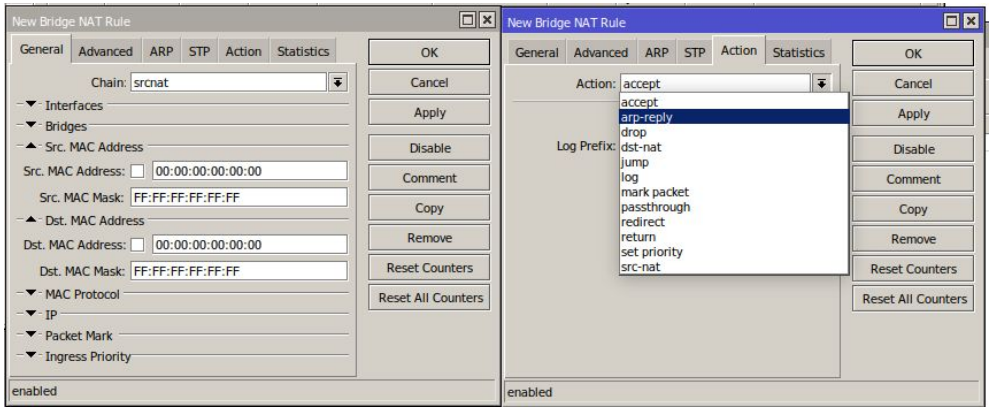
Instagram.com/vaseghi.it
youtube.com/shahin vaseghi
github.com/shahinvaseghi


LOGICAL IN-INTERFACE
DECAPSULATION (TE, VPLS. VLAN, TUNNEL)
YES
IN-INTERFACE BRIDGE PORT?
NO
MPLS TRAFFIC? (TAG PRESENT?)
NO
IPv4 or IPv6 TRAFFIC?
NO
DECAPSULATE?
NO
YES
YES
YES
YES
PHYSICAL IN-INTERFACE
A
INPUT
B
E
INPUT
F
I
INPUT
J
LOCAL IN
FORWARD
BRIDGING DECISION
FORWARD
MPLS DECISION
FORWARD
ROUTING DECISION
ROUTER PROCESSES
PHYSICAL OUT-INTERFACE
LOCAL OUT
INTERFACE HTB
D
OUTPUT
C
H
OUTPUT
G
L
OUTPUT
K
NO
YES
YES
YES
ENCAPSULATE?
NO
OUT-INTERFACE BRIDGE PORT?
NO
MPLS TRAFFIC? (TAG PRESENT?)
NO
IPv4 or IPv6 TRAFFIC?
YES
INTERFACE HTB
LOGICAL OUT-INTERFACE
ENCAPSULATION (TE, VPLS. VLAN, TUNNEL)

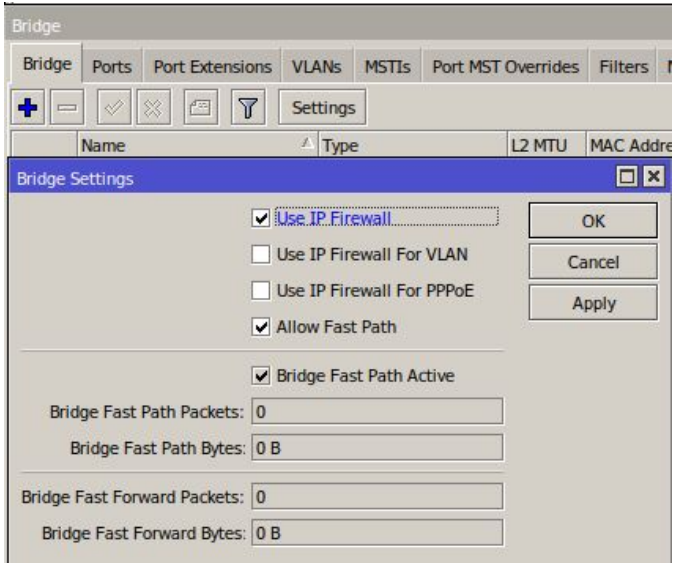

FORWARD
ROUTING DECISION
TTL-1
MANGLE FORWARD
FILTER FORWARD
ACCOUNTING
PRE ROUTING
INPUT
OUTPUT
POST ROUTING
DST-NAT
MANGLE PREROUTING
CONNECTION TRACKING
RAW PREROUTING
HOTSPOT IN
MANGLE INPUT
FILTER INPUT
QUEUE TREE "GLOBAL"
SIMPLE QUEUES
ROUTING ADJUSTMENT
FILTER OUTPUT
MANGLE OUTPUT
CONNECTION TRACKING
RAW OUTPUT
MANGLE POSTROUTING
SRC-NAT
HOTSPOT OUT
QUEUE TREE "GLOBAL"
SIMPLE QUEUES
INTERFACE QUEUE TREE
INPUT INTERFACE
LOCAL PROCESS
ROUTING DECISION
OUTPUT INTERFACE


A
B
BRIDGING
PREROUTING
BRIDGE INPUT
YES
BRIDGE DST-NAT
USE-IP-FIREWALL?
BRIDGING DECISION
NO
USE-IP-FIREWALL?
BRIDGE FORWARD
NO
YES
NO
USE-IP-FIREWALL?
BRIDGE SRC-NAT
FORWARD
YES
POSTROUTING
BRIDGE OUTPUT
BRIDGING DECISION
D
C

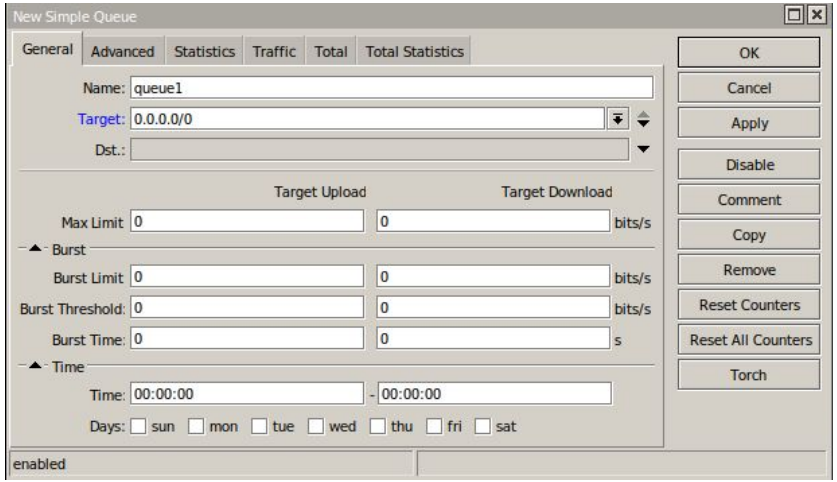

I
J
ROUTING
PREROUTING
IPSEC DECRYPTION
NO
IPSEC POLICY?
YES
FORWARD
ROUTING DECISION
INPUT
POSTROUTING
OUTPUT
IPSEC POLICY?
YES
IPSEC ENCRYPTION
ROUTING DECISION
NO
L
K



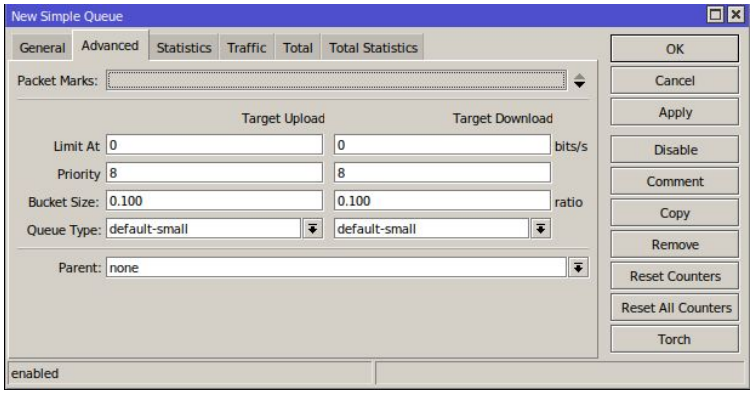
رای راه اندازی Bridge Nat به منو Bridge تب Nat رجوع کنید در این قسمت می توانید Nat برای لایه ۲ یا در اصل عملیات نت کردن مک آدرس ها را انجام دهید.



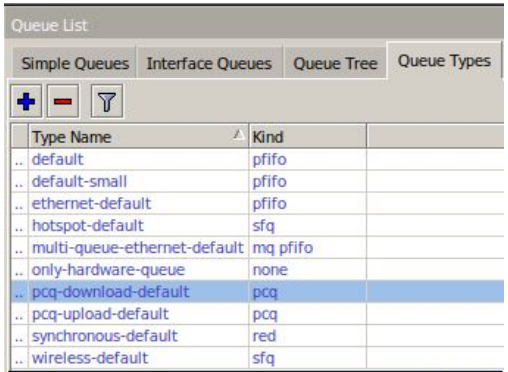
برای اینکه بسته های لایه ۲ به فایروال لایه ۳ بروند و چک بشوند باید در منو Bridge قسمت Setting گزینه Use IP Firewall را فعال کنید.

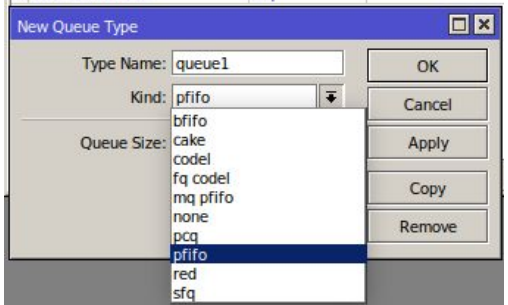


برای مدیریت پهنای باند در میکروتیک از منو Queues استفاده می کنیم .
در این بخش می توانیم دو عمل شکل دادن به ترافیک و اولویت بندی پهنای باند را انجام دهیم .
MIR به معنی حداکثر پهنای باند کاربر است که در میکروتیک Max Limit نام دارد
CIR به معنی حداقل پهنای باند کاربر است که ضروری می باشد و در میکروتیک به آن Limit At می گویند.
اولویت کاربر ها برای استفاده از پهنای باند مازاد در قسمت Priority تعیین می شود که از ۱ تا ۸ است و هرچه کمتر باشد اولویت بالاتری پیدا میکند.
در قسمت Target می توانید آدرس یک کاربر یا رنج یک شبکه یا یک Interface را مشخص کنید و در قسمت Dst میتوانید این آدرس را نسبت به مقصد خاص محدود کنید.
Burst یا پهنای باند تشویقی به کاربری که حد تشویقی تعیین شده را استفاده کرده است پهنای باند بیشتری می دهد.
برای این کار باید برای کاربر Limit At یا حداقل پهنای باند تعیین کنید.
Burst Limit حد تشویقی است که اگر کاربر رعایت کند پهنای باند بیشتری دریافت می کند
. Burst Threshold پهنای باند اضافی است که به کاربر میدهیم.
Burst Time مدت زمانی است که اگر پهنای باند تشویقی را رعایت کند شرط برقرار می شود.
در قسمت Time میتوانید برای این Queue زمان فعال بودن را تعیین کنید.



در تب Advance گزینه Packet Mark تعیین می کند که این Queue فقط روی بسته هایی با این برچسب اعمال شوند.
Limit At حداقل پهنای باند کاربر است.
Priority اولویت این Queue در استفاده از پهنای باند اضافی است.
Queue Type نوع Queue می باشد.
Parent در اصل Queue اصلی است که این Queue زیر مجموعه آن قرار میگیرد.

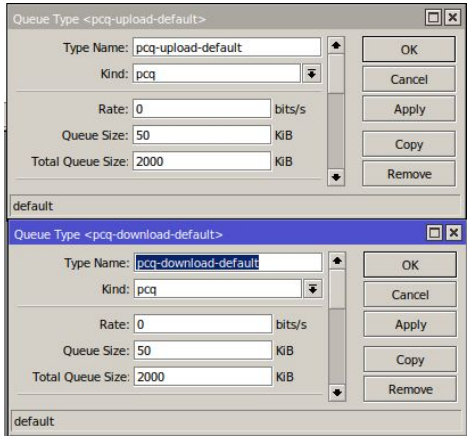


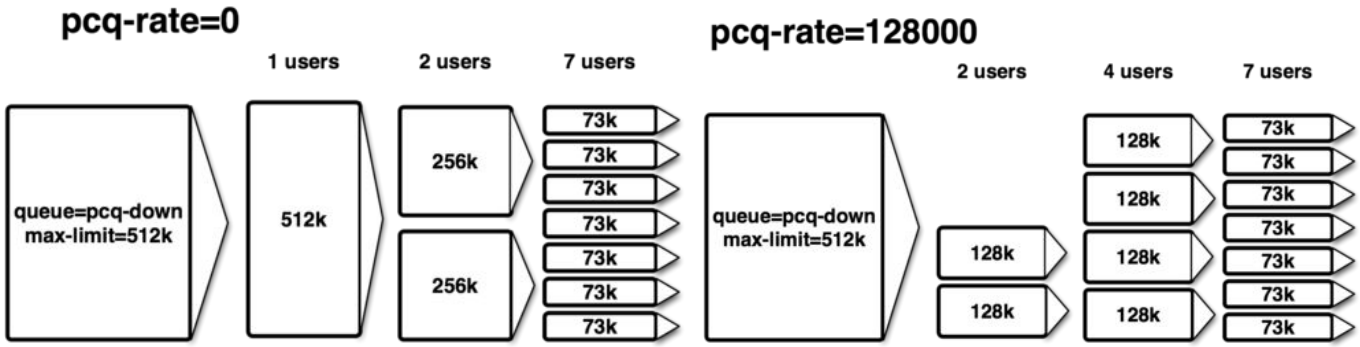


در میکروتیک Queue Type های متنوعی وجود دارد که برای اولویت دهی به بسته ها روش های متفاوتی استفاده می کنند .
pfifo به معنی Packet First In First Out است یا اولین بسته ای که وارد شود اولین بسته ای است که خارج می شود.
bfifo به معنی Byte First In First Out است یا اولین بایتی که وارد شود اولین بایتی است که خارج می شود.
mq-pfifo همان pfifo است با قابلیت transmit queues چندگانه

Pcq را در ادامه مفصل توضیح می دهیم

Queue Type پیشفرض در Queue ها default-small است که از روش pfifo استفاده می کند.





برای استفاده از pcq در میکروتیک اگر Rate انتخاب نکنیم از اول به طور عادلانه کل پهنای باند رو بین کاربران تقسیم میکند اگر Rate تعیین کنیم در ابتدا به مقدار Rate به کاربران میدهد و بعد که کاربران بیشتر شدند شروع به کم کردن پهنای باند می کند.

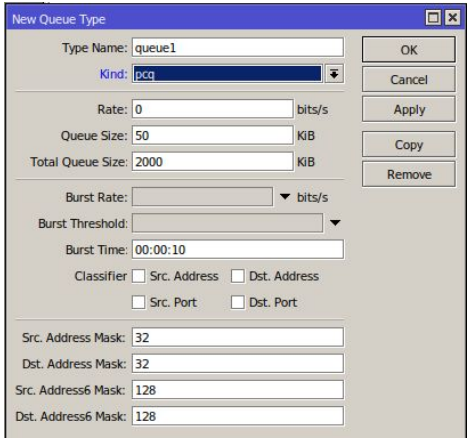
برای استفاده از pcq باید در Queue نوع Queue Type را حتما pcq انتخاب کنید.

برای ایجاد Queue Type جدید از نوع pcq میتوانید تنظیمات زیر را انجام دهید:

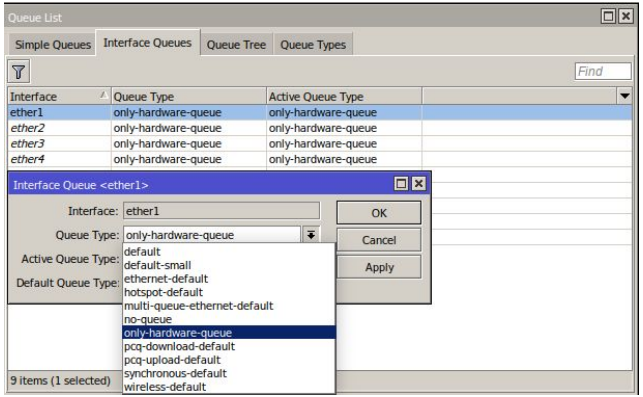
Classifier : کاربران این Queue را نسبت به چی انتخاب کنیم

Src Address Mask این Queue بر اساس آدرس Src بر روی شبکه ی چند کاربره اعمال شود.

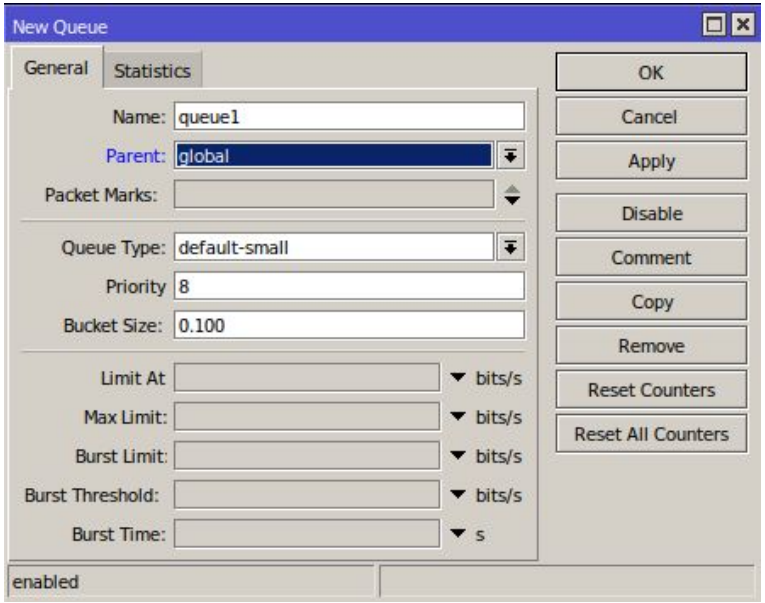
Dst Address Mask این Queue بر اساس آدرس Dst بر روی شبکه ی چند کاربره اعمال شود.



برای اعمال pcq یا هر نوع Queue Type دیگری بر روی Interface ها این کار را از طریق Interfaces Queues انجام می دهید.

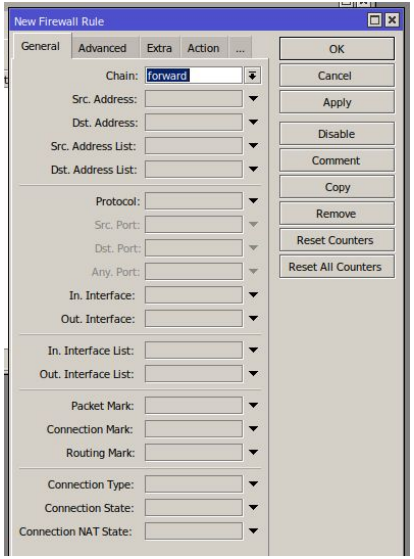


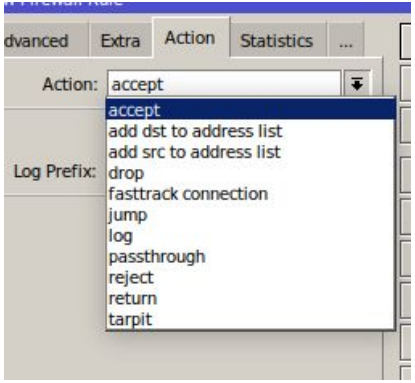
در میکروتیک برای تعیین پهنای باند پروتکل های مختلف باید از Queue Tree استفاده کنید. قبل از ایجاد پروتکل باید ترافیک ها را از طریق Mangle تفکیک کنید.
میکروتیک توصیه می کند ابتدا به طور کلی ترافیک آپلود و دانلود را جدا کنید سپس ترافیک پروتکل های مورد نظرتان را تفکیک کنید .



برای جدا کردن ترافیک آپلود در روتر بسته های ورودی که از Interface سمت Lan می آیند. (مثلا فرض کنید که در روتر یک Bridge دارید که ۳ پورت روتر عضو این Bridge است و شبکه های داخلی به این ۳ پورت متصل است. پس تمام ترافیک آپلود به سمت اینترنت از این Bridge می آید.) باید با استفاده از منگل prerouting کانکشن بسته هایی که از این Interface می آید را mark connection کنید. پس از آن با یک منگل prerouting دیگر بسته هایی که mark connection بسته های بالا را دارند mark packet کنید.

ترافیک های دانلود ترافیک هایی هستند که از Interface اینترنت وارد می شوند. (مثلا Ether 4 روتر به اینترنت متصل است و این Interface اینترنت است). اکنون باید با استفاده از منگل forward کانکشن بسته ها را mark connection کنید. حال با یک منگل forward دیگر بسته هایی که mark connection بالا را دارند را mark packet کنید .
حالا با منگل های forward و تعیین شرط از طریق mark packet بسته های دانلود و آپلود پروتکل های مختلف را mark packet کنید .
در Queue Tree ابتدا یک ظرف کلی به اندازه کل آپلود برای آپلود ایجاد میکنیم و یک ظرف کلی نیز به اندازه کل دانلود برای دانلود. برای اینکار mark packet های مربوط را در Queue Tree انتخاب کنید. حالا پروتکل های مختلف که mark packet کرده اید را به عنوان Child این Parent های کلی آپلود و دانلود و سرعت مورد نظرتان را انتخاب میکنید.





ما در Filter Rule محدودیت هایی در ارتباطات ایجاد میکنیم. برای اینکار ابتدا در General یک سری شرط تعیین می کنیم که بنا بر آنها بسته هایی که باید شامل این فیلتر بشوند انتخاب می شوند سپس در Action اقدامی که باید برای این بسته ها اتفاق بیفتد را مشخص می کنید. قسمت های مختلف این منو به شرح زیر است:

۱. Chain : در این منو ۳ گزینه وجود دارد : ۱.۱ Input : بسته هایی که مقصدشان خود روتر است ، ۱.۲ Forward : بسته هایی که از روتر عبور میکنند یعنی از یک پورت وارد می شوند و از پورت دیگری خارج می شوند

۲. Src.Address : فیلد آدرس فرستنده هدر IP بسته ۳.. Dst.Address : فیلد آدرس گیرنده هدر IP بسته

۴. Protocol : قسمت پروتکل هدر IP بسته که پروتکل کلی بسته را به ما نشان میدهد (مثلا TCP / ICMP / FTP و ..)

۵. Src.Port فیلد پورت فرستنده در هدر لایه ۴ بسته ۶. Src.Port فیلد پورت گیرنده در هدر لایه ۴ بسته

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

۹. Out.Interface : پورت خروجی ۱۰. In.Interface List : لیست پورت های ورودی 11. Out.Interface List : لیست پورت های خروجی ۱۲. PacketMark : برچسب بسته ۱۳. Connection Mark : برچسب ارتباط

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

باکسی که کنار شروط است برای note یا غیر از این استفاده می شود

اقداماتی که روی بسته قابل انجام است به شرح زیر است :

۱. accept : پذیرفتن بسته ۲. add dst to address list : اضافه کردن آدرس گیرنده بسته به یک لیست

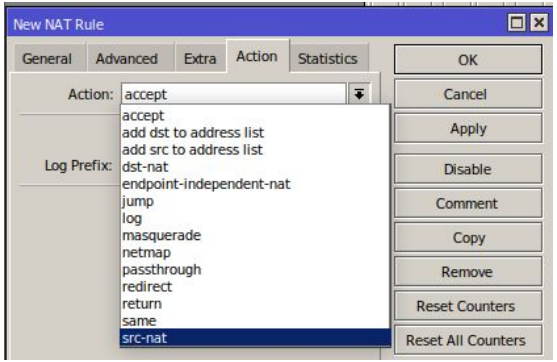
۳. add src to address list : اضافه کردن آدرس فرستنده بسته به یک لیست ۴. drop : انداختن بسته

۵. بسته را در لیست ارتباطات fast track قرار دادن ۶. jump : پریدن به نقطه مشخص شده از لیست فایروال ها

۷. log : اطلاعات کامل از بسته را log میکند ۸. passthrough : یکی به امار بسته اضافه میکند

۹. reject : انداختن بسته و ارسال یک پیام icmp به فرستنده ۱۰. return : بازگرداندن بسته به جایی که jump شده.

۱۱. tarpit : دریافت بسته و باز نگه داشتن ارتباط TCP



Action های مختلف Nat که متفاوت هستند :

۱. accept : عملیات Nat را انجام نده

۲. dst-nat : آدرس Dst-IP و Dst-Port بسته هایی که شامل شروط این نت هستند را با آدرس های مشخص شده تعویض کنید.

۳. endpoint-independent-nat : بسته های شامل فیلتر و مپینگ independent endpoint می شوند. این حالت تنها روی بسته های udp ممکن است.

۴. masquerade : آدرس Src-IP بسته های خروجی از هر اینترفیس را با آدرس تنظیم شده بر روی آن پورت تعویض کنید.

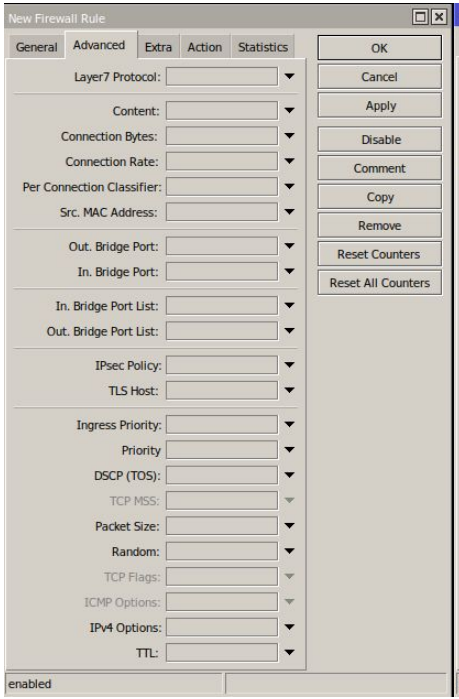
۵. netmap : آدرس ها را ۱ به ۱ به یک گروه مپ می کند.

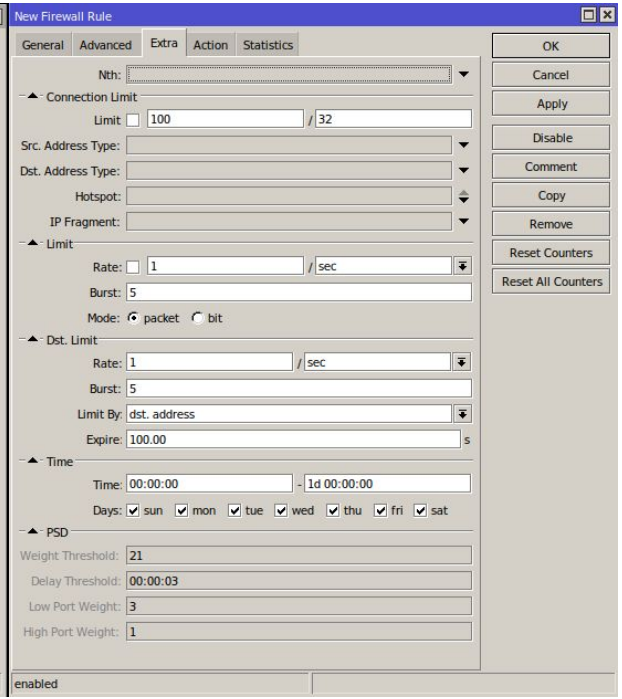
۶. passthrough : یکی به آمار اضافه کن و از این رول بگذر ، برای آمار مفید است.

۷. redirect : بسته های این رول را به پورت مشخص ارسال کن

۸. same : بسته های یک کاربر مشخص را به یک آدرس و پورت مشخص ارسال کن

۶. src-nat : آدرس Src-IP و Src-Port بسته هایی که شامل شروط این نت هستند را با آدرس و پورت مشخص شده تعویض کنید.





گزینه های تب Advance به شرح زیر است:

۱. Layer 7 Protocol : بعد از اینکه RegEx های لایه ۷ ای را در تب Layer 7 Protocol ایجاد کرده باشید در این قسمت میتوانید به شروط اضافه کنید.

۲. Content : بسته حاوی این کلمات باشد.

۳. Connection Bytes : حجم این Connection

۴. Connection Rate : پهنای باند این Connection

۵. Pre Connection Classifier : قابلیت PCC میکروتیک برای ادغام پهنای باند .

۶. Src. MAC Address : مک آدرس فرستنده .

۷. Out. Bridge Port : پورت Bridge خروجی

۸. In. Bridge Port : پورت Bridge ورودی

۹. TCP Flag : فلگ های بسته های Tcp

گزینه های تب Extra به شرح زیر است :

۱. Connection Limit : محدودیت ایجاد کانکشن نسبت به تعداد کاربر مشخص شده در سابنت

۲. Src. Address Type : ماهیت Src Add مانند broadcast , multicast و ...

۳. Dst. Address Type : ماهیت Dst Add

۴. Hotspot : نوع بسته Hotspot

۵. IP Fragmentation : قطعه قطعه کردن بسته

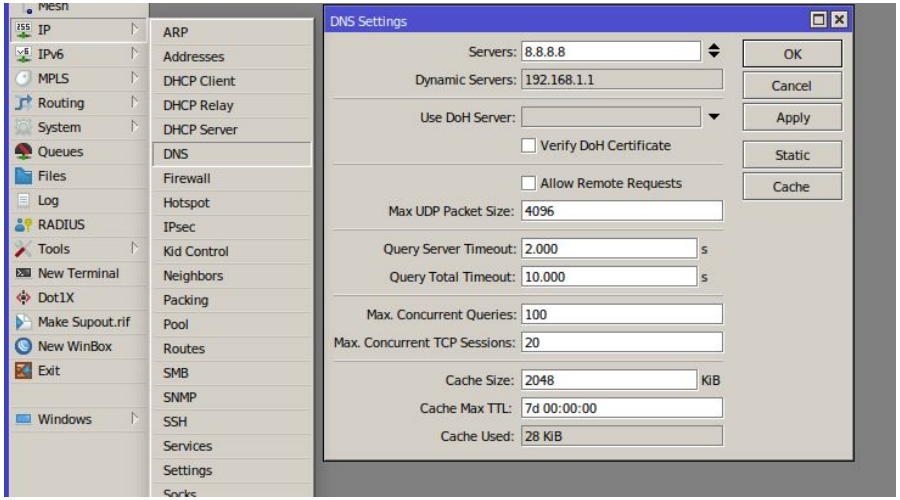
۶. Limit : تعداد بسته یا بیت عبوری در واحد زمانی مشخص شده

۷. Dst. Limit : تعداد بسته های عبوری در یک واحد زمانی مشخص نسبت به یک مبدا یا مقصد مشخص

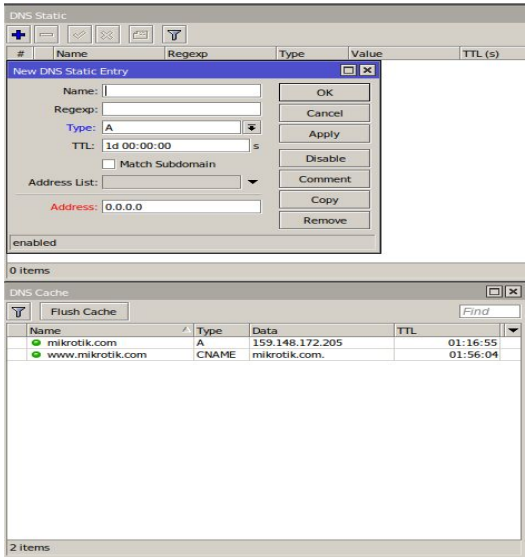
۸. Time : این رول در چه بازه زمانی فعال باشد

۹. PSD : Port Scan Detect

در صورتی که یک Chain جدید ایجاد کرده اید در پروسس های فایروال اجرا نمی شوند و در صورتی که بخواهید اجرا شوند با یک Chain معمولی بسته هایی که میخواهید به آن Chain جدید منتقل شوند باید Action ه jump را انجام دهید.

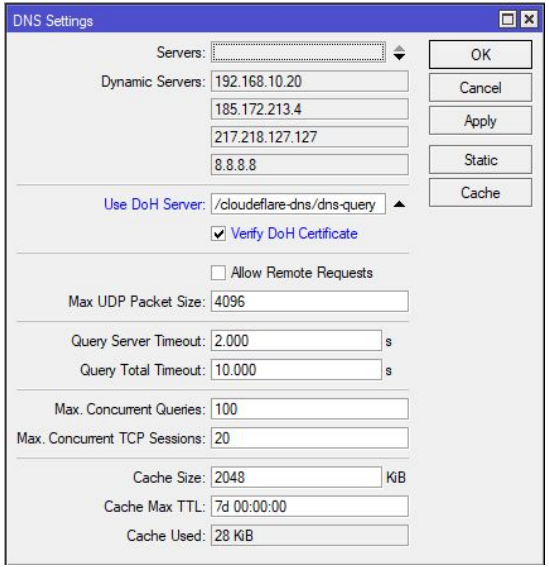


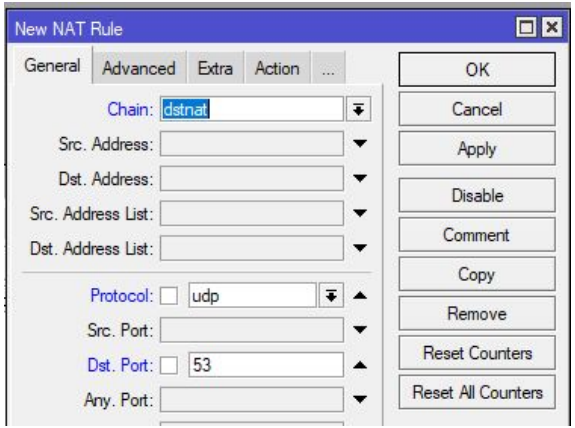
برای تنظیم کردن DNS Server باید به منو IP > DNS رجوع کنید.
در قسمت Server میتوانید سرور های DNS را ست کنید.
در قسمت Dynamic Server میتوانید سرور هایی که به صورت خودکار تنظیم شده اند را مشاهده کنید.
برای اینکه بتوانید از روتر میکروتیک به عنوان DNS Server دیگر دستگاه ها استفاده کنید حتما باید تیک گزینه Allow Remote Request را انتخاب کنید.

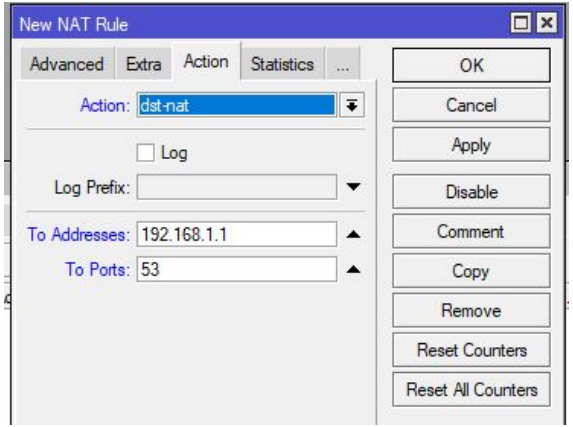


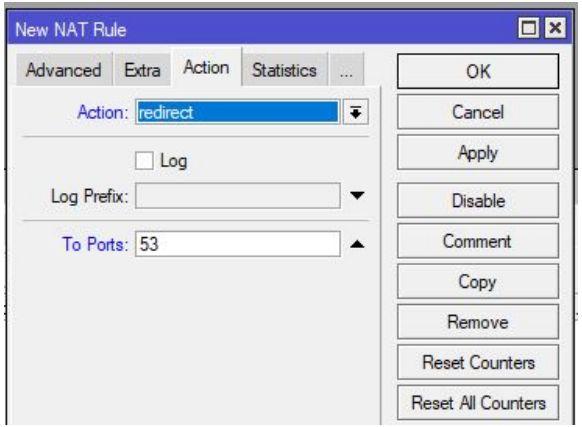
در Cache شما می توانید درخواست های DNS که توسط روتر انجام شده است را ببینید.
در قسمت DNS میتوانید به صورت دستی IP ها را به URL ها نسبت دهید . در اینصورت می توانید درخواست های DNS شبکه را Hijack کنید و پاسخ های مورد نظر خودتان را به آنها بدهید.

در منو DNS > IP اگر گزینه Allow Remote Request را فعال کنید کاربرهای دیگر میتوانند به شما درخواست های DNS ارسال کنند.
این مساله خطر DNS Cache Attack را ایجاد می کند.
برای استفاده از Doh یا DNS over Https که باعث امن شدن بسته های DNS و غیرقابل شنود شدن بسته می شود باید گزینه Use Doh Server را فعال کنید و یک DoH Server مانند : https://cloudflare-dns/dns-query انتخاب کنید
برای ایجاد Transparent DNS Cache (یعنی ما بسته های DNS را دریافت کنیم اما به مقصد اصلی تحویل ندهیم و به یک DNS سرور دیگر تحویل دهیم) باید یک DST-Nat ایجاد کنید که بر روی بسته های UDP 53 اعمال شود. حال می توانید این بسته ها را در Action را روش dst-nat به پورت 53 یک DNS Server دیگر ارسال کنید یا با redirect به پورت 53 روتر خودتان تحویل دهید.

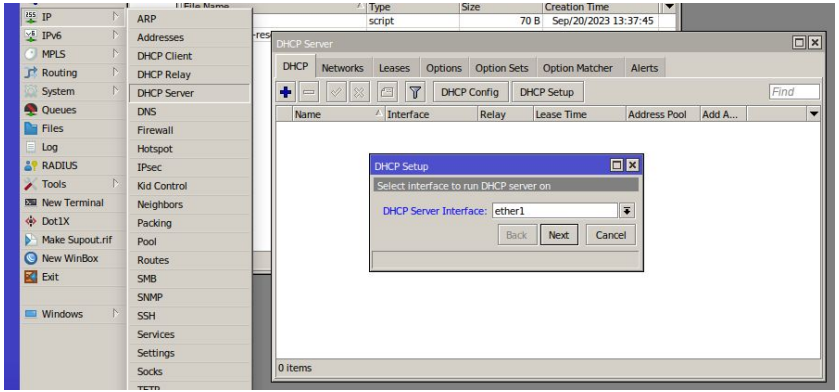




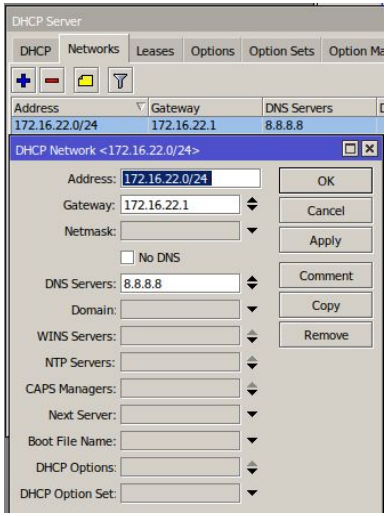




برای راه اندازی DHCP Server باید مراحل زیر را انجام دهید :
برای این کار بر روی منو IP > DHCP Server رفته و بر روی گزینه DHCP Setup کلیک میکنید؛ به ترتیب سوالات زیر پرسیده می شود:
۱. DHCP Server Interface : همانطور که پیشتر اشاره کردیم DHCP تنها میتواند در یک برودکست دامین کار کند و هر پورت روتر در برادکست دامین متفاوتی کار میکند به همین علت باید پورتی که میخواهیم سرویس ارائه آدرس را انجام دهد انتخاب کنیم.
. DHCP Address Space : آدرس رنجی که قصد دارید آی پی ها را در آن توزیع کنید (همان آدرس برودکست دامین).
۳. Gateway for DHCP Network : آدرس Default Gateway یا همان Default Route مورد نظر که به Client ارائه می شود.
۴. Address to Give Out :آدرس های قابل ارائه یا همان IP Pool که ظرف آدرس های یک DHCP Server است.
در این بخش می توانید تک آدرس بدهید یا با علامت - به منظور از یک آدرس تا یک آدرس انتخاب کنید یا یک رنج آدرس بدهید.
۵.DNS Server : آدرس DNS Server مورد نظری که میخواهید به Client ها ارائه دهید.
۶. Lease Time : مدت زمان اشغال آدرس توسط کاربر است که بعد از تمام شدن زمان تا قطع شدن کارت شبکه کاربر از شبکه همچنان آدرس را نزد کاربر نگه می دارد.



در منو Leases میتوانید آدرس هایی که ارائه کرده اید را مدیریت کنید.
آدرس های Dynamic را Static کنید یا آدرس های Static ایجاد کنید.



در تب Network منو DHCP Server میتوانید تنظیمات مربوط به آدرس های DNS یا Gateway و DHCP Option ها را انجام دهید

برای ایجاد DHCP Option ها به تب Option رجوع کنید و یک گزینه جدید بسازید:

Name : اسم دلخواه

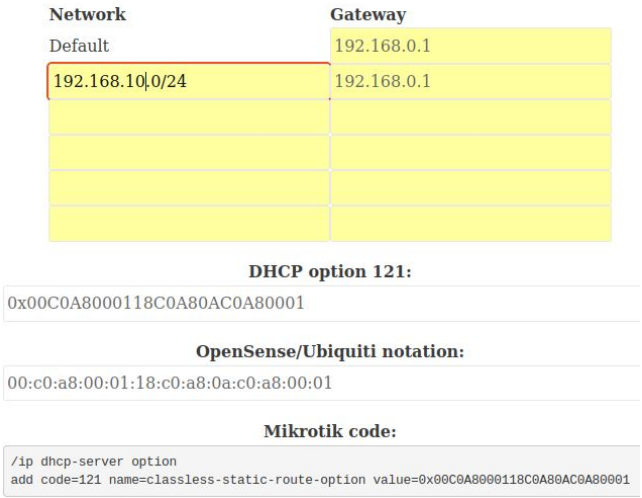
Code : کد اپشن مورد نظری که می خواهید ارائه دهید.

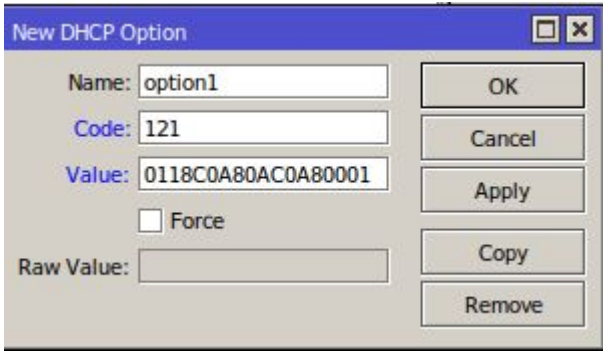
Value : مقداری که قصد دارید با این Option به کاربر یاد بدهید، این کار را باید به صورت Hex انجام دهید.

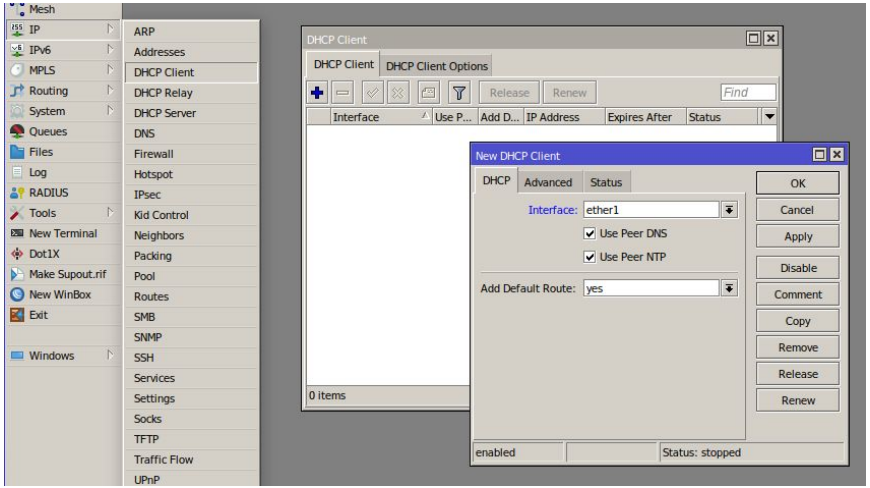
برای اینکار سایت های زیادی وجود دارند، برای مثال Option کد ۱۲۱ به کاربر Route یاد می دهد. برای ساخت Hex این مقدار می توانید مانند تصویر زیر از سایت زیر استفاده کنید :

https://www.medo64.com/2018/01/configuring-classless-static-route-option/

یا عبارت dhcp option 121 generator را در گوگل سرچ کنید.







روتر ها مانند تجهیزات EndPoint ما مثل گوشی ها و لپتاپ ها به صورت خودکار از DHCP Server آدرس دریافت نمی کنند و ما باید به صورت دستی این کار را انجام دهیم.

برای انجام این کار در میکروتیک به منو IP > DHCP Client مراجعه کنید و بر روی Add کلیک کنید.

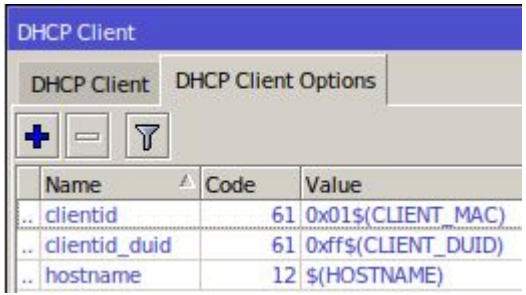
در صفحه جدیدی که باز می شود چند گزینه داریم :

۱. اینترفیس : ما میدانیم که هر پورت روتر در برودکست متفاوتی کار می کند پس با انتخاب اینترفیس برای دریافت آدرس، برودکست مورد نظر خودتان را انتخاب میکنید

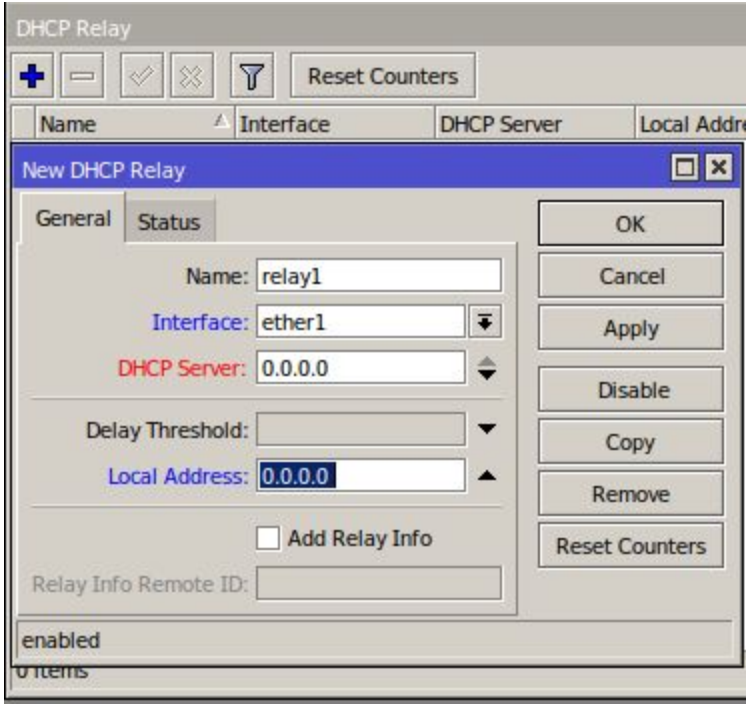
۲. برای دریافت سرور DNS به همراه آدرس تیک گزینه Use Peer DNS را انتخاب کنید.

۳. برای دریافت سرور تنظیم ساعت به همراه آدرس تیک گزینه Use Peer NTP را انتخاب کنید.

۴. ما میدانیم که برای ارتباط با سیستم های غیر هم رنج باید از Default Gateway استفاده کنیم که در روتر ها به نام Default Route می باشد؛ پس برای دریافت اینترنت این گزینه را روی Yes قرار دهید.



DHCP Client در میکروتیک به طور پیشفرض ۳ Option را ارسال میکند که حاوی مک آدرس، User ID و HostName است.



همانطور که میدانید بسته های DHCP به صورت Broadcast ارسال می شوند پس باید بین DHCP Server و Client یک ارتباط لایه ۲ برقرار باشد.
حالا به هر دلیلی اگر بین DHCP Server و Client یک روتر قرار داشت، برای آنکه آن روتر بسته های Broadcast از نوع DHCP را عبور دهد باید بر روی آن DHCP Relay راه اندازی شود.
برای این کار به منو IP > DHCP Relay رجوع کنید و یک گزینه جدید اضافه کنید :
Name : یک اسم دلخواه
Interface : پورتی که از طریق آن به آن شبکه ی DHCP CLient متصل هستید را انتخاب می کنید.
DHCP Server : آدرس DHCP Server مورد نظری که قصد دارید Relay آن شوید.
Local Address : آدرس خود روتر در شبکه DHCP Client