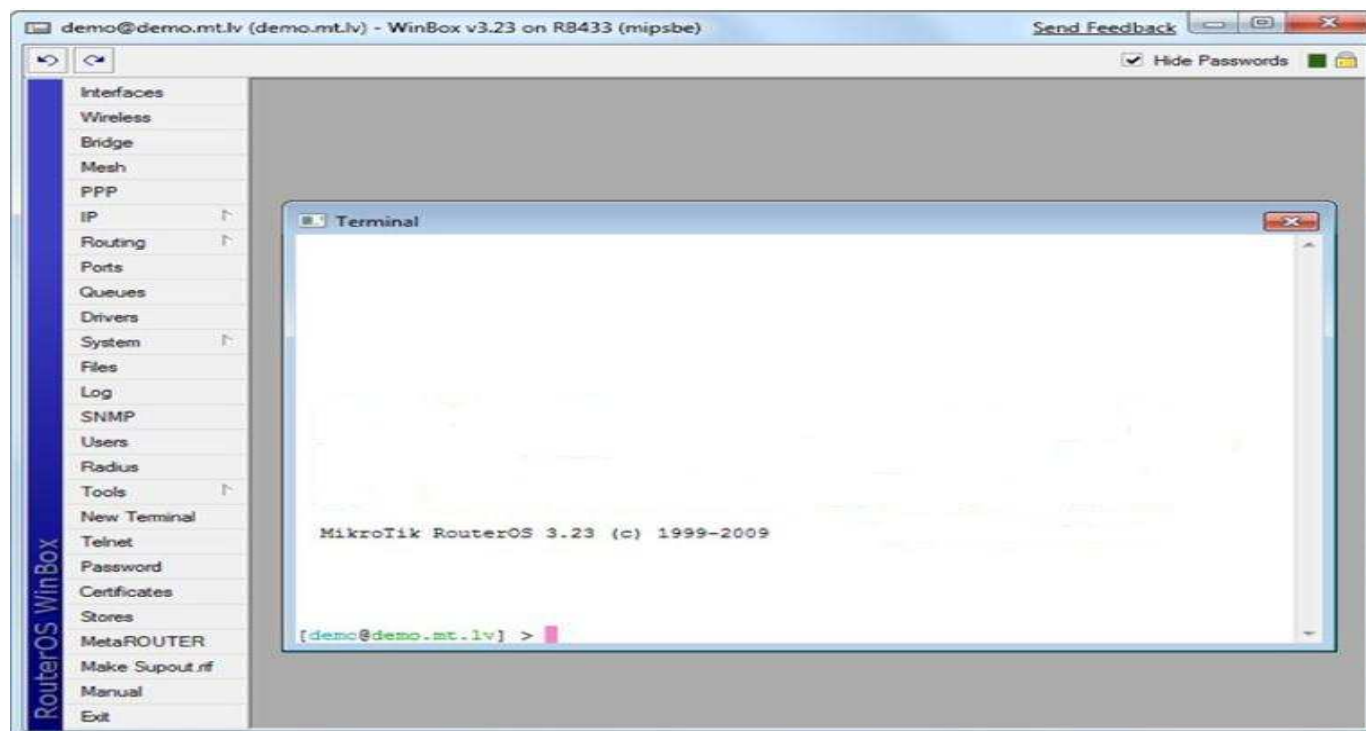


# ویژگیها و خصوصیات میکرووتیک

نویسنده: بیثم خلیلی

تاریخ تهیه: ۱۳۸۹/۰۱/۱۰

# RouterOS



Router OS یک سیستم عامل بر روی سخت افزار Routerboard است. یکی از مزیت های این سیستم عامل نصب بر روی PC و استفاده از آن به عنوان Routing، firewall، bandwidth management، wireless access point، hotspot gateway، backhaul link، vpn server و... است.

Router OS یک سیستم عامل stand alone است که بر پایه linux هسته 2.6 می باشد و علاوه بر سرعت زیاد آن نصب راحت و استفاده ساده آن از جمله برتریهای این سیستم عامل می باشد.

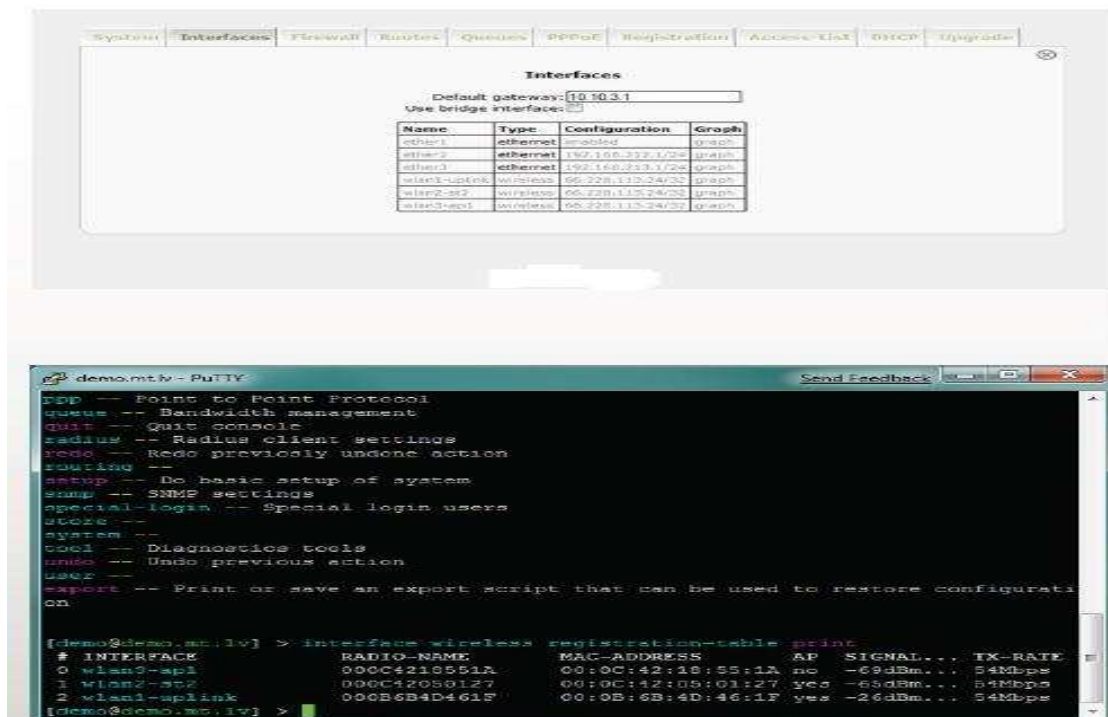
در صفحات بعدی مثالهایی از ویژگیهای مهم Router OS را مشاهده می کنیم.

# Hardware



Router OS سیستم عاملی است که بر روی Routerboard ها نصب می گردد اما می تواند بر روی PC ها و سخت افزارهای سازگار با x86 هم نصب گردد. شبیه embedded board و سیستم های mini ITX . Router OS به دلیل آنکه بر روی linux هسته v2.6 ساخته شده با کامپیوترهای multi cpu , multi core (SMP) نیز سازگار است . یکی دیگر از ویژگیهای این سیستم عامل نصب بر روی intel Motherboard های اولیه و multi core cpu های جدید است . Router OS قابلیت نصب بر روی SATA, IDE ، usb storage device ، شامل HDDs ، SDD disk, SDcard, CF, و غیره را دارد . همچنین شما نیاز به فضای حداقل 64mb برای نصب Router OS دارید.

# Configuration



Router OS از متدها و راهکارهای مختلف برای پیکر بندی استفاده می کند :

۱- از طریق دسترسی به صورت local و توسط صفحه کلید و نمایشگر

۲- Serial console به همراه یک terminal application

۳- telnet

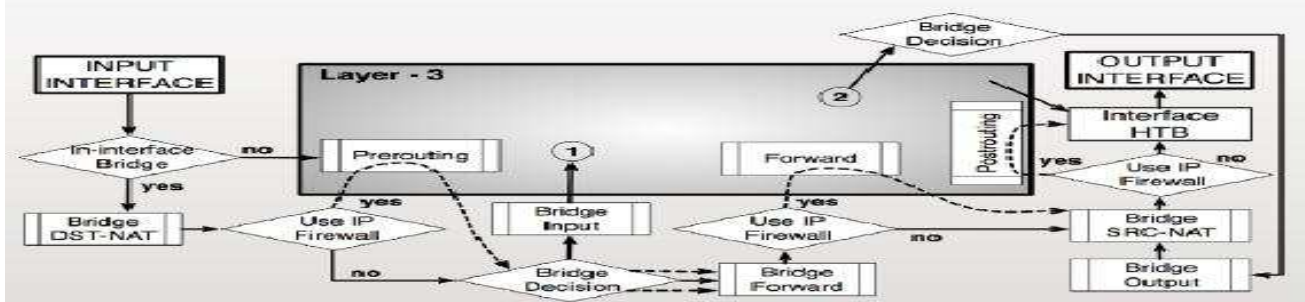
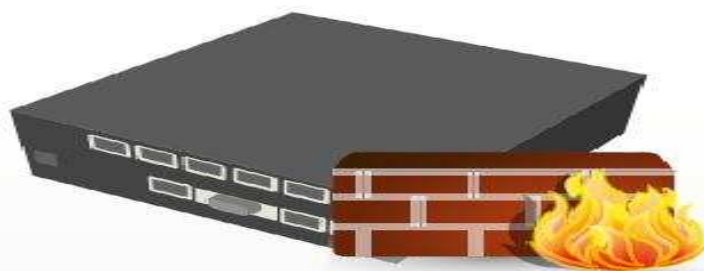
۴- SSH

۵- Winbox که یک ابزار گرافیکی سفارشی محسوب می گردد که WebBase می باشد و کار با آن بسیار ساده می باشد یک API program interface برای تهیه و ایجاد برنامه کنترلی شما و دسترسی آن بر حسب MAC address level است و مشکلات دسترسی بر حسب IP را از بین برده است به این صورت که هنگامی که برای اولین بار Router OS نصب می شود بدون دادن IP و بر حسب Mac address قابل شناسایی و دسترسی است به صورت بسیار ساده .

ویژگی بارز Router OS این است که در عین سادگی بسیار قوی میباشد و حتی دستورات آن برای configure کردن دستگاه برای یادگیری بسیار آسان می باشد. در صورتی که بخواهیم Script جدیدی اضافه کنیم آنرا سفارشی کنیم.

۸- web interface که از طریق IP در Browser می توانیم آنرا کنترل کنیم .

# Firewall



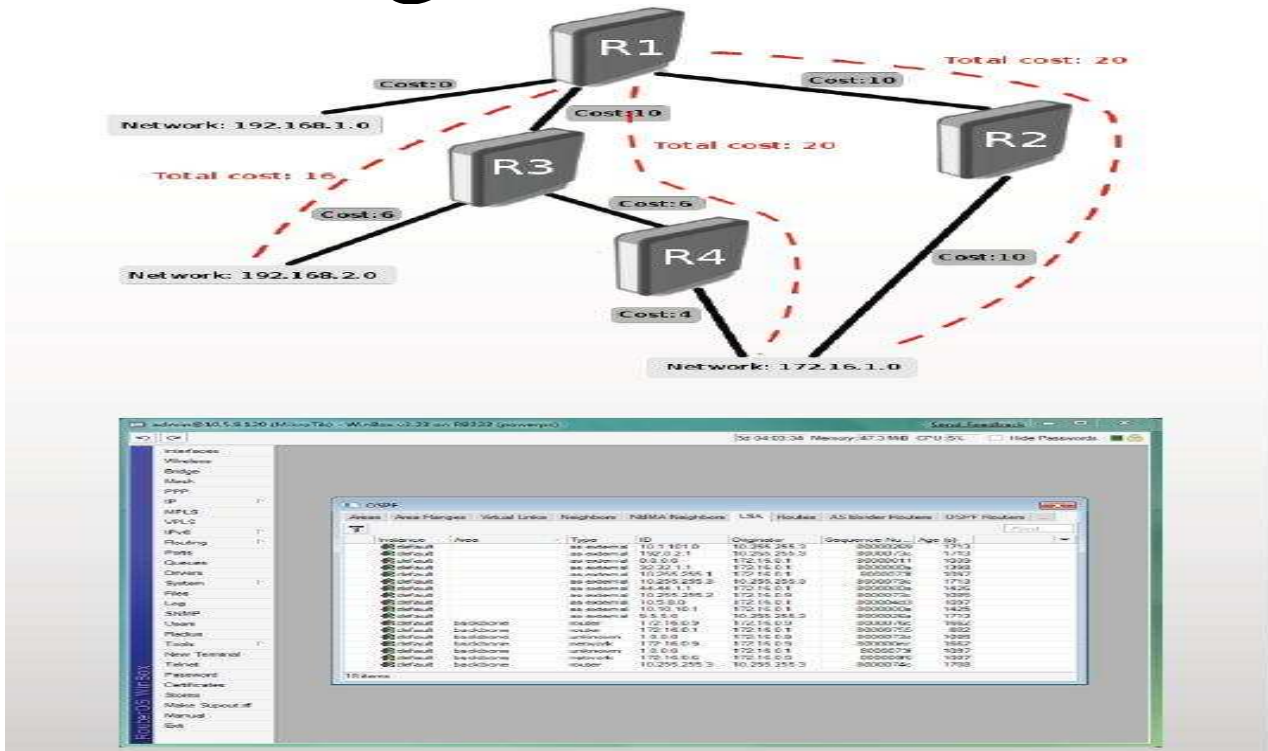
دیوار آتش ابزار **packet filtering** و گسترش متدهای امنیت می باشد که برای کنترل جریان داده ها در یک **Router** که در سرخط شبکه قرار می گیرد استفاده می شود. برای جلوگیری از حملات و دسترسی مستقیم حملات شبکه ای و پس از شناسایی این حملات اجازه ورود آنها را به شبکه شما نمی دهد. **Router OS** دارای ویژگی **state full** است به این معنی که در حقیقت به صورت جزء به جزء **pacet**ها را بازرسی میکند و از به وجود آمدن **hole** در شبکه جلوگیری می کند از **SourceNAT** و **DestinationNAT** پشتیبانی می کند در واقع کمک می کند به **popular application** و **UPnP**.

همچنین از دیگر ویژگی های این firewall استفاده از internal connection ،Routing، packetmark،است. از ویژگی های packetmark، استفاده برای راه اندازی load balancing روی خطوط اینترنت است .

در واقع filter می تواند روی IP address، Port range، Port range، IP address، Static Access List و Dynamic از همچنین گیرد. DSCP، protocol و پارامترهای دیگر صورت گیرد. همچنین از Dynamic و Static Access List پشتیبانی می کند و می تواند packetها را با صفحات و خصوصیات آنها match کند. این ویژگی به طور صریح تر به عنوان layer7 matching خوانده می شود .

یکی دیگر از ویژگی های دیوار آتش Router OS، پشتیبانی از ipv6 به صورت ساده می باشد .

# Routing



Router OS پشتیبانی می کند از static routing و اکثر dynamic routing پروتکلها:

۱- برای ipv4 پشتیبانی از RIP v1, RIP v2, OSPF v1, BGP v4

۲- برای ipv6 پشتیبانی از RIPng, OSPF v3, BGP

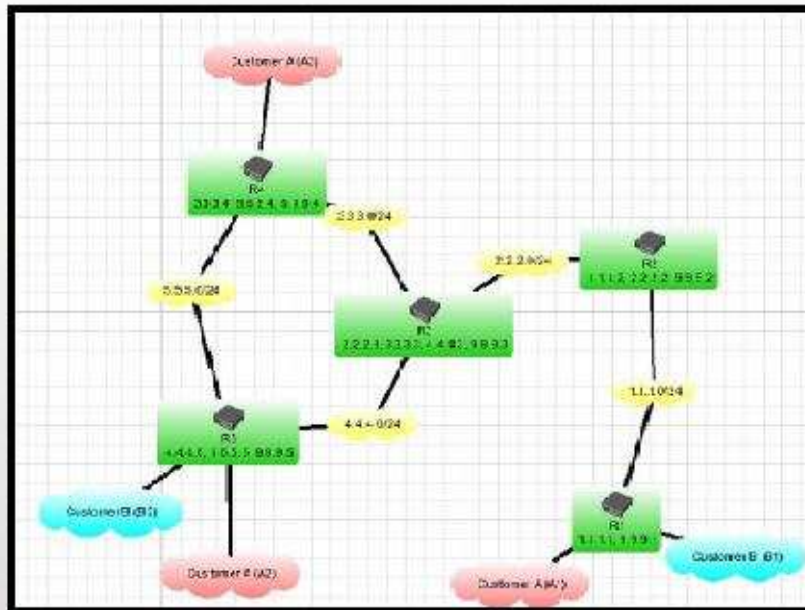
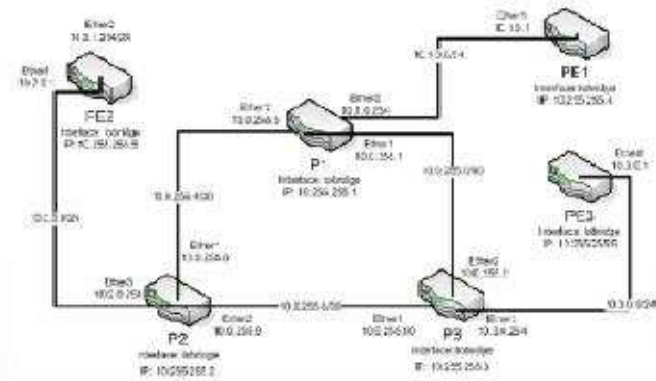
همچنین پشتیبانی از virtual routing and forwarding (VRF), policy based routing و interface based Routing, ECMP routing را انجام می دهد.

شما می توانید استفاده کنید از firewall filter برای نشانه گذاری connection های خاص با routing marks و سپس از ترافیک های نشانه گذاری شده برای استفاده isp های مختلف استفاده کنید. در حال حاضر با اضافه کردن MPLS به Router OS, VRF هم معرفی شده است.

Virtual routing و forwarding تکنولوژیهایی هستند که اجازه می دهند routing table های چند گانه در یک router در یک لحظه صورت پذیرد. به خاطر استفاده از چندین routing table, overlapping ip address می تواند بدون وجود conflict بین Routing به کار خود ادامه دهد.

VRFP همچنین امنیت شبکه را افزایش می دهد. این تکنولوژی فقط محدود به شبکه های مبتنی بر MPLS نمی باشد و غالب اوقات می تواند بدون استفاده از MPLS هم استفاده شود.

# MPLS



MPLS برای Mutti Protocol Lable Switching به وجود آمده است که می تواند جایگزین IPRouting شود.

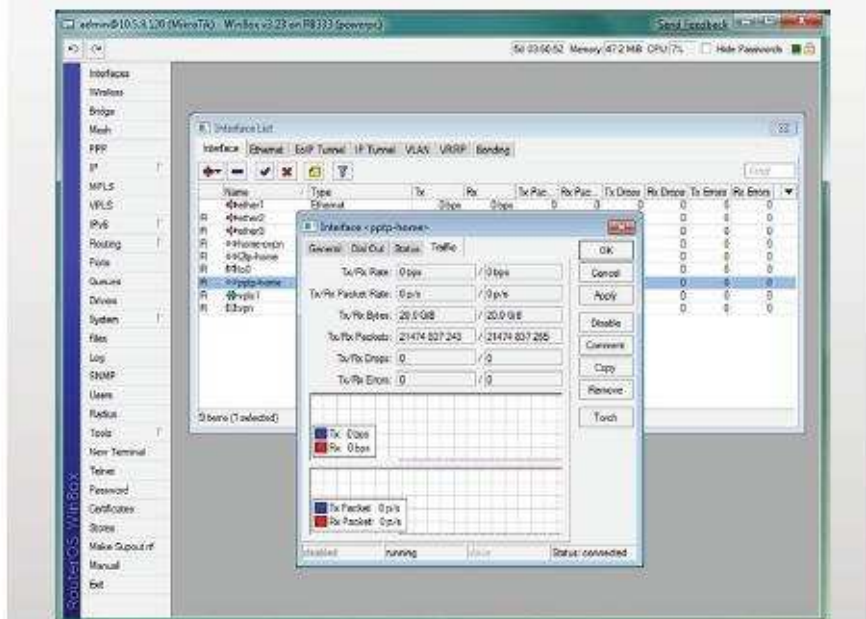
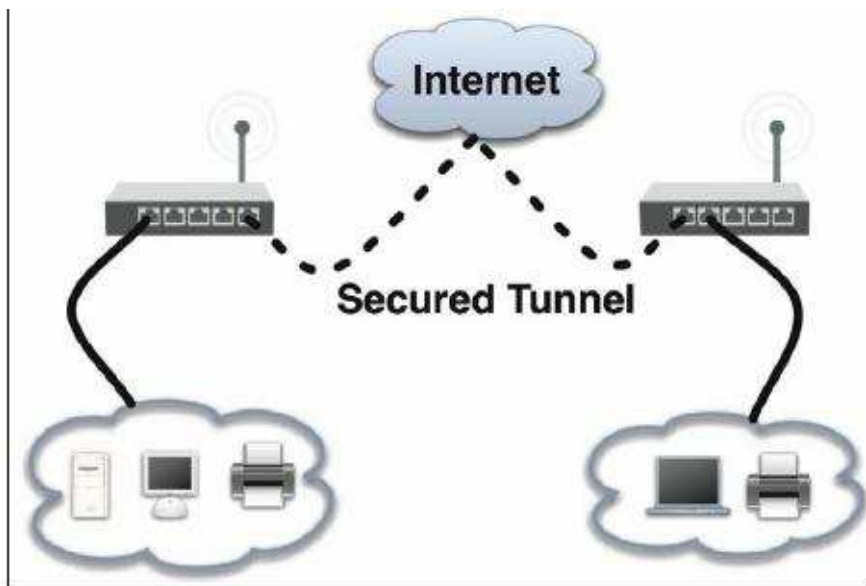
Packet forwarding برای تصمیم‌گیری مدت زمانی را تلف می‌کند در صورتی که MPLS میتواند با نشانه‌گذاری و قرار دادن برچسب روی یک packet خود packet را وادار به تصمیم‌گیری کند که در نتیجه سرعت رسیدن packet به مقصد را افزایش می‌دهد و همچنین باعث کاهش ترافیک در شبکه می‌شود.

برتری forwarding process در واقع همان مزیت اصلی MPLS است که خیلی ساده یک virtual links بین نودهای یک شبکه ایجاد می‌کند بدون در نظر گرفتن پروتکرها و encapsulated data. در شبکه‌های مبتنی بر MPLS به دلیل lable گذاری packet ها دارای ترافیک کمتری در شبکه هستیم. packet-forwarding منحصر روی محتویات همان lable است بدون نیاز بازرسی خود packet که اجازه می‌دهد برای به وجود آوردن سیکل end-to-end عبوری از هر نوع از نقل و انتقال با هر نوع پروتکل.

تعدادی از تکنولوژیها که MPLS از آنها پشتیبانی می‌کند.

- Static Label bindings for IPv4
- Label Distribution protocol for IPv4
- RSVP Traffic Engineering tunnels
- VPLS MP-BGP based autodiscovery and signaling
- MP-BGP based MPLS IP VPN

# VPN

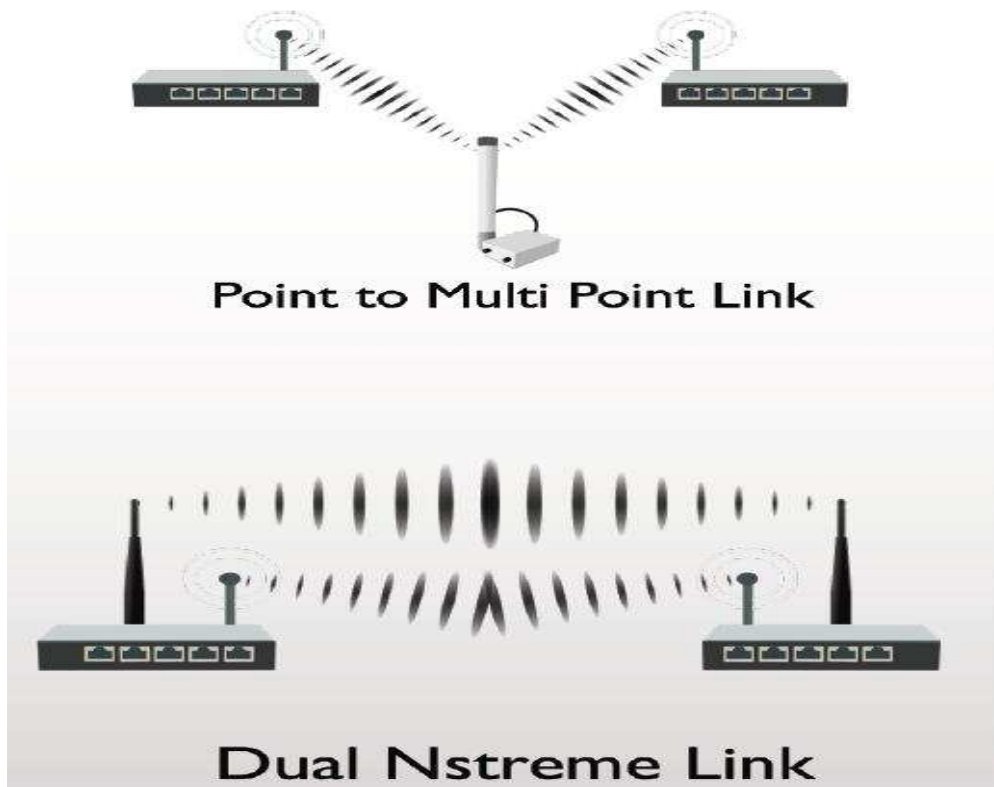


برای به وجود آوردن یک ارتباط امن در open networks یا اینترنت یا ارتباط از راه دور با encrypted links، RouterOS از متد های مختلف VPN و tunnel protocol پشتیبانی می کند که عبارتند از:

- Ipsec – tunnel and transport mode, certificate or PSK, AH and ESP security protocols
- Point to point tunneling (OpenVPN, PPTP, PPPoE, L2TP)
- Advanced PPP features (MLPPP, BCP)
- Simple tunnels (IPIP, EoIP)
- 6to4 tunnel support (IPv6 over IPv4 network)
- VLAN – IEEE802.1q Virtual LAN support, Q-in-Q support
- MPLS based VPNs

بدین معنی که شما می توانید یک ارتباط امن به وجود آورید. هنگامی که مثلاً به صورت remote دو نقطه را با هم مرتبط می کنید یا می خواهید از یک شبکه به شبکه دیگر متصل شوید احساس می کنید کامپیوتر شما در یک شبکه واحد قرار دارد درحالی که این ارتباط به صورتی کاملاً امن و encrypt شده است.

# Wireless



تکنولوژیهای مختلف wireless در RouterOS وجود دارد. اکثر این تکنولوژیها در access point ها و clients وجود دارند. اگر در شبکه یک hotspot کوچک یا یک mesh network در شهر وجود داشته باشد در همه حالت RouterOS می تواند به شما کمک کند. همچنین پشتیبانی می کند از NStreme که اجازه می دهد از دو Firewall استفاده کنید در یک طرف، که یکی برای فرستادن و یکی برای دریافت به کار می رود.

برخی از ویژگیهایی که توسط RouterOS پشتیبانی میشوند عبارتند از:

- IEEE802.11a/b/g/n wireless client and access point
- Nstreme and Nstreme2 proprietary protocols
- Client polling
- RTS/CTS
- Wireless Distribution System (WDS)
- Virtual AP
- WEP, WPA, WPA2 encryption
- Access control list
- Wireless client roaming
- WMM
- HWMP+ Wireless MESH protocol
- MME wireless routing protocol

# Hotspot

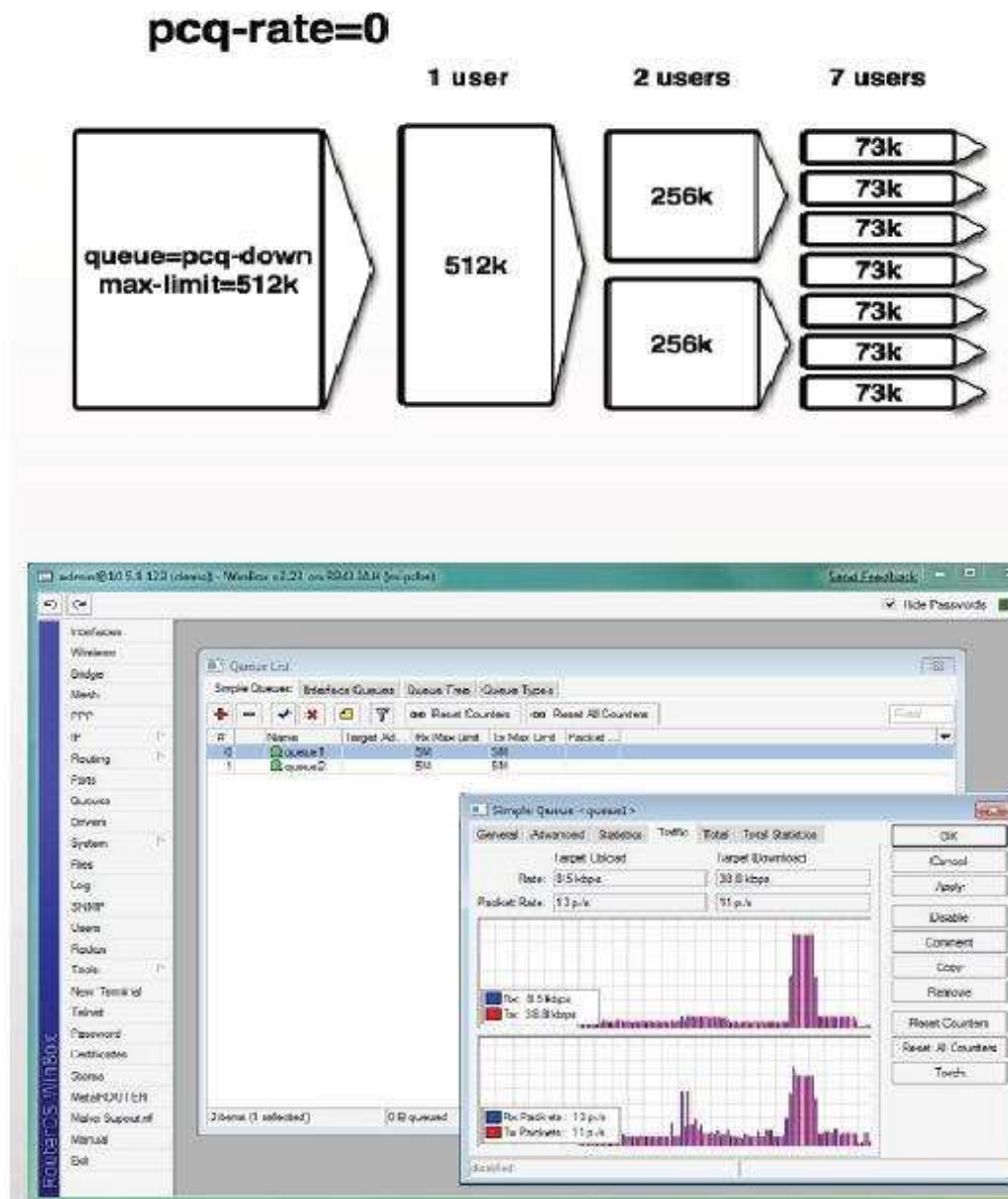


تکنولوژی hotspot برای دسترسی کاربران از طریق سیم و بی سیم برای ارتباط به اینترنت به کار می رود. به طوری که وقتی کاربران web browser خود را باز می کنند صفحه login را مشاهده می کنند که در این صفحه حتی شما می توانید آرم سازمان خود را قرار دهید. کاربر پس از وارد کردن user, password مورد نظر اجازه دسترسی به اینترنت را دارد. این تکنولوژی زمانی کاربرد دارد که مدیر شبکه قدرت کنترل روی کاربران کامپیوترها در شبکه را ندارد. هر کاربر یک profile مخصوص خود که توسط مدیر شبکه ساخته می شود را دارد و توسط آن می تواند به اینترنت وصل شود و حتی محدودیت در زمان و upload و download و سرعت استفاده

از اینترنت را داشته باشد، hotspot می تواند روی Radius server ها و یا حتی userهای خود RouterOS اعمال گردد که در واقع می تواند مدیریت مرکزی روی کاربران شبکه را به شما دهد. شما توسط HotSpot حتی می توانید دسترسی تعدادی از کاربران را به برخی از سایتها محدود کنید.

- Plug-n-Play access to the Network
- Authentication of local Network Clients
- User Accounting
- RADIUS support for Authentication and Accounting
- Configurable bypass for non-interactive devices
- Walled garden for browsing exceptions
- Trial user and Advertisement modes

# Quality of Service & Bandwidth Shaping



کنترل پهنای باند مکانیزمی است که اختصاص و محاسبه داده ها را کنترل می کند. مفهوم Quality of Service (QoS) این است که روتر می تواند اولویت بندی و تقسیم ترافیک شبکه را انجام دهد.

تعدادی از ویژگیهای کنترل ترافیک RouterOS در زیر آمده است:

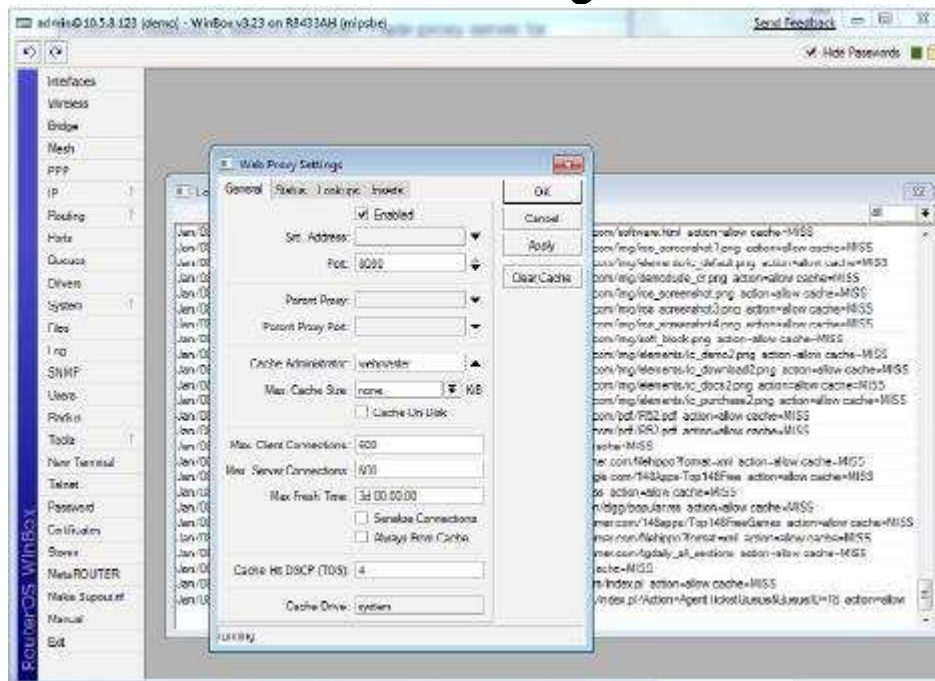
- limit data rate for certain IP addresses, subnets, protocols, ports, and other parameters
- limit peer-to-peer traffic
- prioritize some packet flows over others

Priority به این مفهوم است که اگر مدیر شبکه بخواهد از پهنای باند استفاده کند و اولویت بالاتری داشته باشد کاربر معمولی از اولویت پایین تری برای استفاده برخوردار می شود.

- use queue bursts for faster web browsing
- apply queues on fixed time intervals
- share available traffic among users equally, or depending on the load of the channel

همچنین از (Hierarchical Token Bucket (HTB، Advanced Queuing، QoS system with CIR, MIR, burst و Priority پشتیبانی می کند. QOS به صورت خیلی ساده قابل پیاده سازی است.

# Web Proxy



ابزار Router OS میتواند به عنوان proxy server برای cache کردن web استفاده گردد و باعث بالا رفتن سرعت باز کردن صفحات به خاطر کپی شدن آنها در سرور محلی و تحویل آنها به user ها گردد.

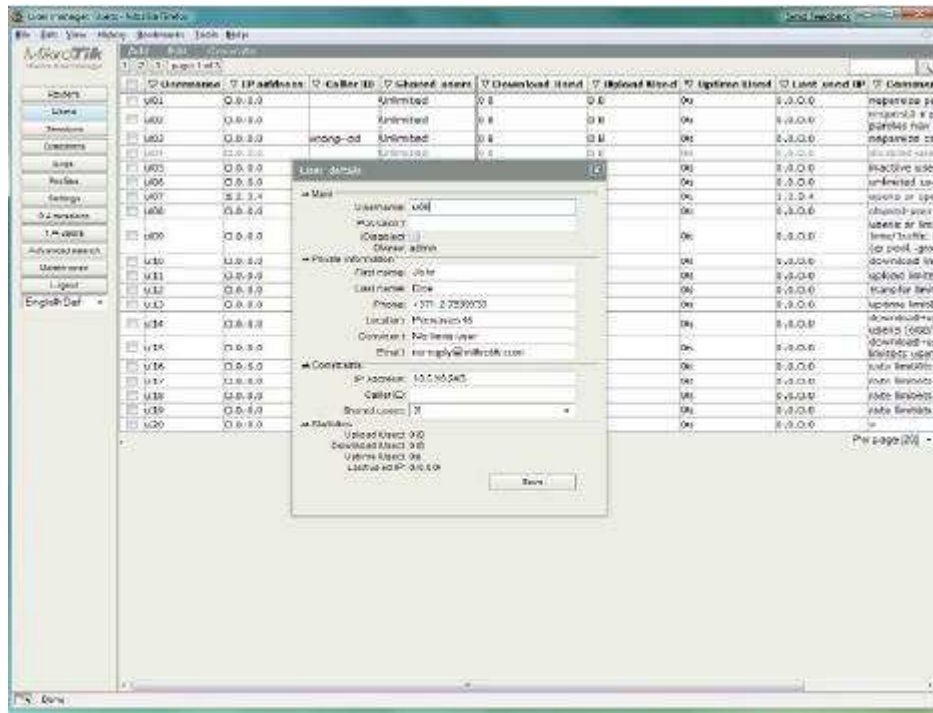
Router OS ابزارهای proxy server را مطابق زیر پیاده سازی می کند:

- Regular HTTP proxy
- Transparent proxy
- Access list by source, destination, URL and requested method( HTTP firewall)
- Cache access list to specify which object to cache, and which not.

- Direct access list to specify which resources should be accessed directly, and which-through another proxy server
- Logging facility
- SOCKS proxy support
- Parent proxy support
- Cache storage on external drive

Router OS میتواند به عنوان transparent caching عمل کند بدون نیاز به configuration در client ها. در واقع server router از طریق گرفتن همه http request ها و redirect user به Transparent می کند که نتیجه آن بالا رفتن سرعت دسترسی کاربران به صفحات وب می باشد.

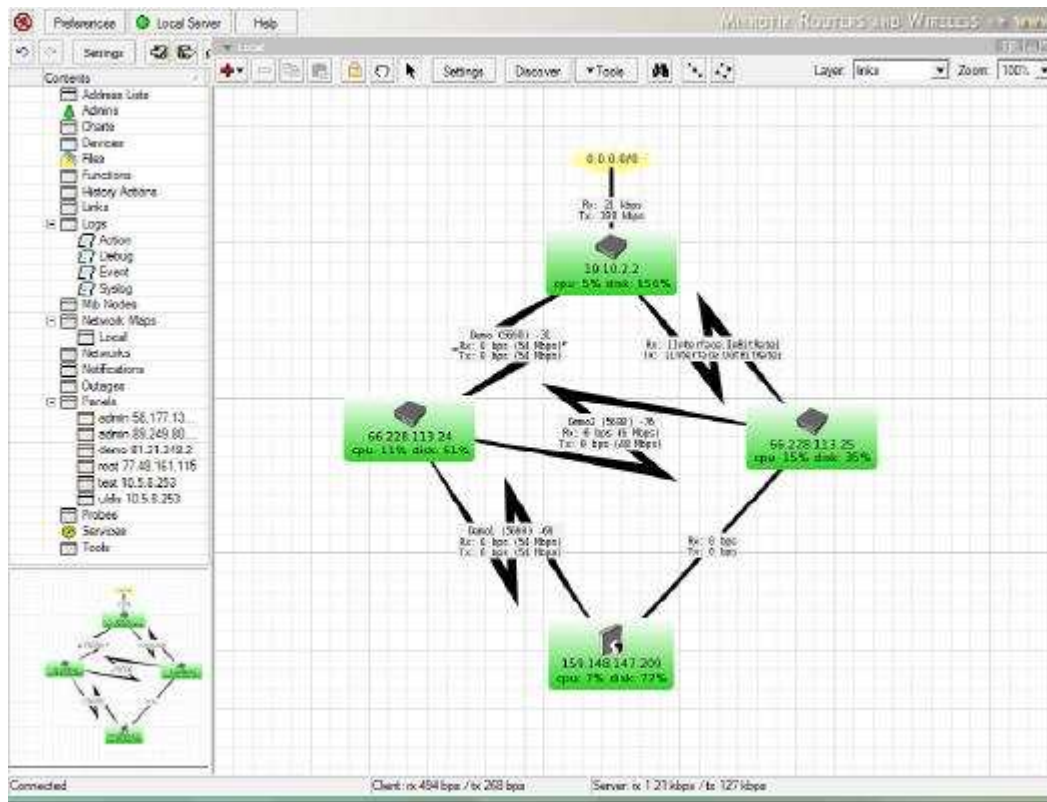
# Tools



برای کمک به مدیریت شبکه شما Router OS از ابزار زیر استفاده میکند:

- Ping , traceroute
- Bandwidth test , ping flood
- Packet sniffer, torch
- telnet, SSH
- e-mail and SMS send tools
- automated script execution tools
- CALEA data mirroring
- File fetch tool
- Active connection table
- NTP client and server
- TFTP server
- Dynamic DNS updater
- VRPR redundancy support
- SNMP for providing graphs and stats
- RADIUS client and server(user manager) (به accounting عمل میکند.)  
عنوان

# TheDude



Dude network یک application نمایشی است که راه حلی برای مدیریت ساده تر محیط شبکه شما می باشد. این application میتواند به صورت اتوماتیک همه device های شبکه شما را با subnet های مختلف scan کند و نقشه و طرح شبکه شما را به صورت خیلی جالب به شما در زمانی کوتاه تحویل دهد. همچنین سرویس های موجود در شبکه را نمایش میدهد و هشدارهای لازم در مورد مشکلات موجود را به شما میدهد.

در ضمن شما قادر خواهید بود ترافیک و availability graphs , outage reports و . . . رابه وسیله ابزار dude برای log file استفاده کنید. حتی این ابزار میتواند مدیریت کند دستگاه های Router OS موجود در شبکه شما را برای به روز کردن نرم افزار های آنها.

# Licenses

Level number	0 (FREE)	1 (DEMO)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Upgradable To	-	no upgrades	ROS v4.x	ROS v4.x	ROS v5.x	ROS v5.x
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h limit	-	-	yes	yes	yes
Wireless Client, Bridge	24h limit	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h limit	-	yes	yes	yes	yes
EoIP tunnels	24h limit	1	1	unlimited	unlimited	unlimited
PPPoE tunnels	24h limit	1	1	200	500	unlimited
PPTP tunnels	24h limit	1	1	200	unlimited	unlimited
L2TP tunnels	24h limit	1	1	200	unlimited	unlimited
OVPN tunnels	24h limit	1	1	200	unlimited	unlimited
VLAN interfaces	24h limit	1	1	unlimited	unlimited	unlimited
P2P firewall rules	24h limit	1	1	unlimited	unlimited	unlimited
NAT rules	24h limit	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h limit	1	1	200	500	unlimited
RADIUS client	24h limit	-	yes	yes	yes	yes
Queues	24h limit	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h limit	-	yes	yes	yes	yes
User manager active sessions	24h limit	1	10	20	50	Unlimited