

MikroTik RouterOS v3

New
Obvious and Obscure
Mikrotik RouterOS v3.0 features

Kernel

- RouterOS 2.9.43
 - Linux kernel version 2.4.31
- RouterOS 3.0beta8
 - Linux kernel version 2.6.20
- For more detailed information see:
<http://www.kernel.org/>

Hardware Compatibility

- SMP (Symmetric Multiprocessing) support



- SATA (Serial-ATA) disk support
- Maximum RAM support increased from 1GB to 2GB
- Latest interface driver support
- Dropped legacy interface support

API Support

- An application programming interface (API) is a source code interface that a computer system provides in order to support requests for services to be made of it by a computer program. (from wikipedia.org)
- To enable API, use “/ip services enable api”
- Default RouterOS API port is 8728 TCP.
- For more information see:
<http://wiki.mikrotik.com/wiki/API>

OpenVPN

- An open source virtual private network
 - Preshared private key, certificate, or username/password authentication
 - AES and Blowfish encryption supported
 - Can be layer-3 (IP packet) or layer-2 (Ethernet frame) carrier
 - Run over a single IP port (TCP or UDP)
- Default RouterOS OpenVPN port is 1194 UDP.

New Web-proxy Implementations

- Completely Mikrotik rewritten web-proxy (no Squid or another pre written source code used)
- Web-proxy package is now fully integrated into main system package
- Web-proxy now is more suitable for Hotspot use
- Web-proxy now works faster and has optimized memory usage

New OSPF Implementation

- Completely MikroTik rewritten OSPF (no Zebra or another pre written source code used)
- Completely new routing-test v3.0 package created (routing-test v2.9 package is now standard routing v3.0 package)
- Several previously unfixable bugs fixed
- OSPF now has potential for further improvements (interface routes, inter-area filters, pre-interface filters, ...)

New VRRP Implementation

- Completely new VRRP implementation, not compatible with previous versions
- Several previously unfixable bugs fixed
- Now it is necessary to create VRRP interfaces instead of just enabling VRRP feature
- VRRP addresses now must be assigned as regular (/32) IP addresses

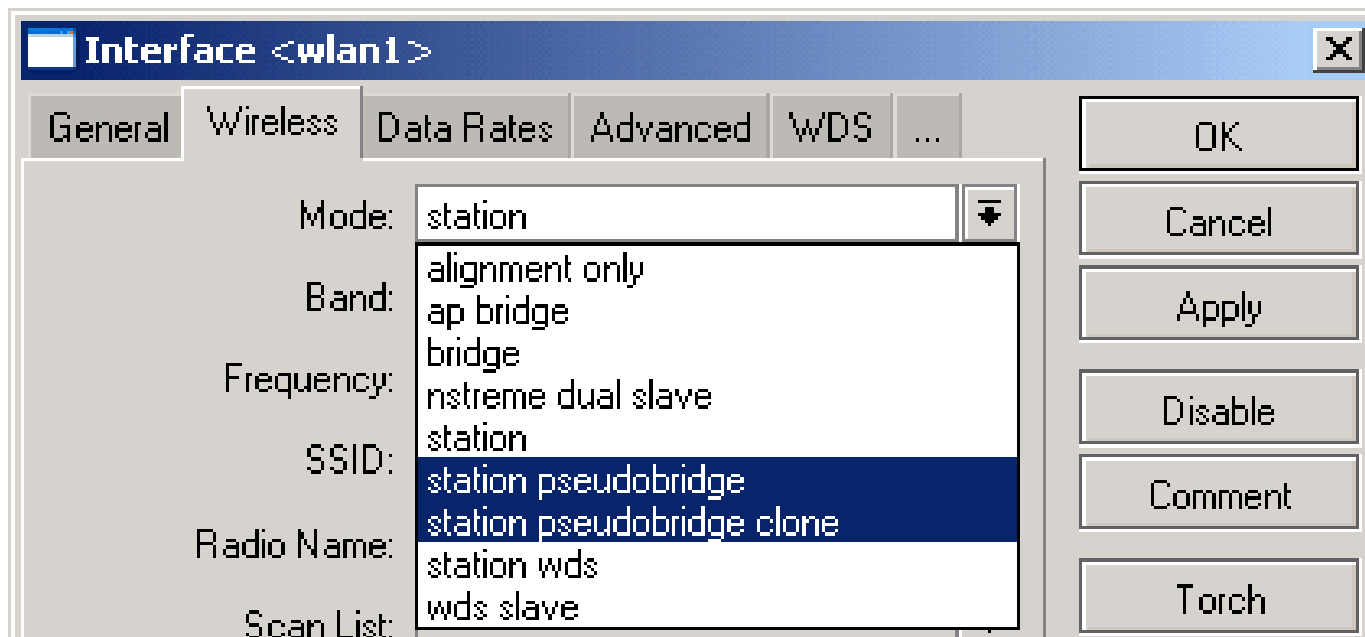
Wireless MultiMedia (WMM)

- WMM prioritizes wireless traffic according to 4 access categories :1,2 - background 0,3 - best effort 4,5 - video 6,7 - voice
- Different handling of access categories is applied for transmitted packets - "better" access category has higher probability of getting access to medium
- Details can be studied in 802.11e and WMM specification, or, at:

<http://wiki.mikrotik.com/wiki/WMM>

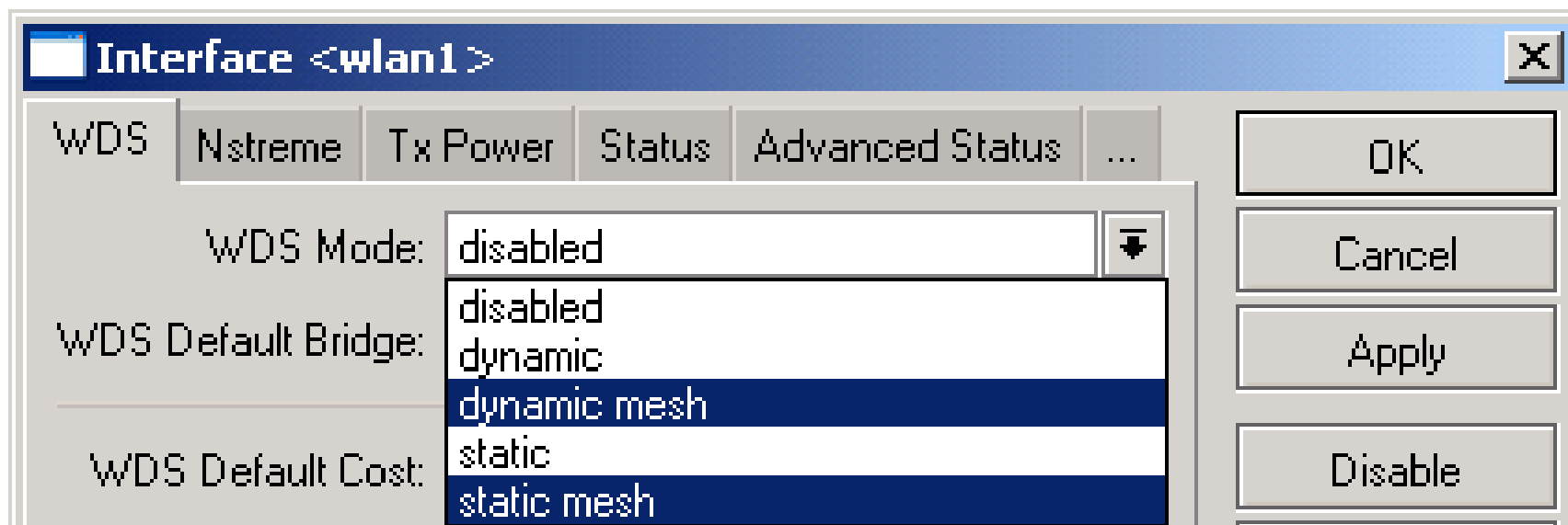
New Wireless Modes

- **Station-pseudobridge** - learns which IP address have which MAC address and translates it.
- **Station-pseudobridge-clone** - uses one MAC address of the device and clones it



New WDS Mesh Implementation

- Two MikroTik proprietary WDS modes added (**dynamic-mesh** and **static-mesh**) to improve WDS-MESH connectivity between MikroTik RouterOS devices



New Access List

- Entries are ordered now, just like in firewall
- Matching by all interfaces “interface=all”
- “Time” - works just like in firewall
- “Signal-range” - client's signal should be within this range to match the rule. If the signal goes outside the range, it is going to be disconnected.
- “Private-pre-shared-key” - each client can have different key; works only when PSK method is used

New Access List

New AP Access Rule [X]

MAC Address:

Interface: ▾

Signal Strength Range:

AP Tx Limit: ▾

Client Tx Limit: ▾

Authentication

Forwarding

Private Key: ▾ 0x

Private Pre Shared Key:

Time

Time: -

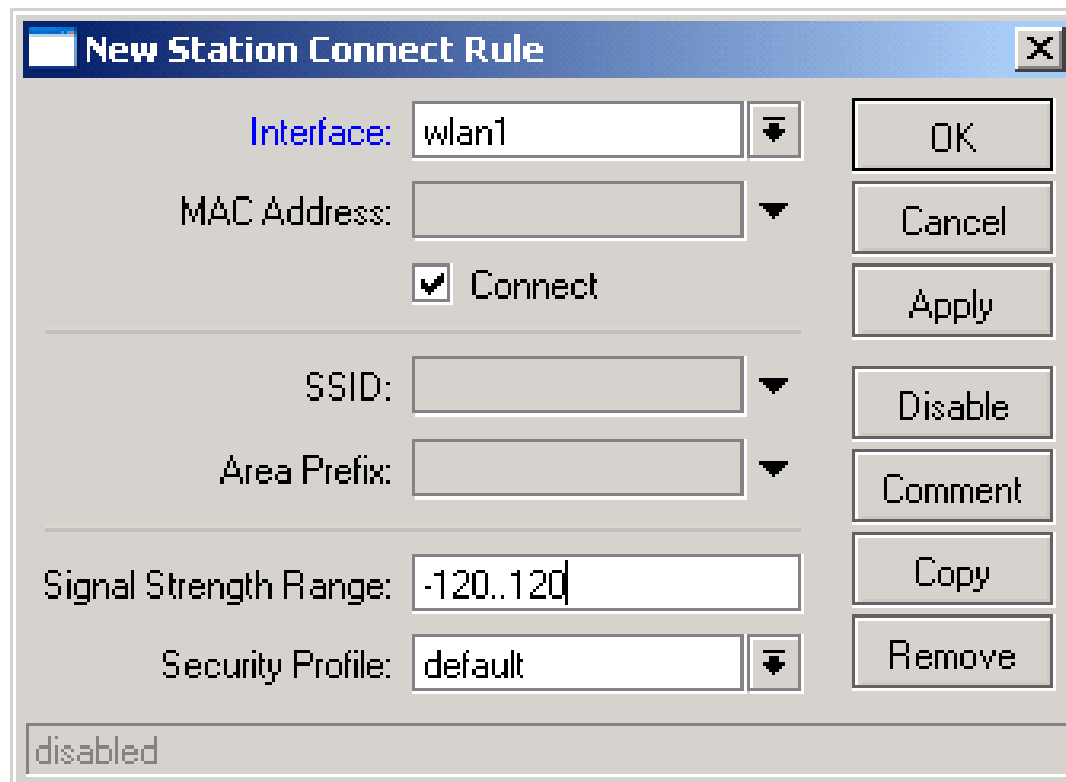
sun mon tue wed thu fri sat

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

New Connect List

- “Signal-range” - client connects to an AP within the specified signal range
- If the signal goes out the range client will disconnect from AP and starts looking for a new AP.



New Station Connect Rule

Interface: wlan1

MAC Address:

Connect

SSID:

Area Prefix:

Signal Strength Range: -120..120

Security Profile: default

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Other Wireless Features

- Full frequency list for Atheros chipset cards using superchannel frequency mode (2192-2539 Mhz)
- “reset-configuration” command for wireless interface
- Nstreme performance improved for lower speed boards (RB100 Series)
- “Disable-csma” added to disable the “medium access” protocol, if the Nstreme polling is enabled

Security profiles RADIUS

- “Radius-mac-accounting” - MAC address is used as user-name
- “Radius-eap-accounting” - EAP supplicant-identity used as user-name
- “Radius-mac-format” - which format should be used to code client's MAC address
- “Radius-mac-mode” - where to put the MAC address “as-username” or “as-username-and-password”

New Security Profiles

New Security Profile

General | RADIUS | EAP | Static Keys

MAC Authentication
 MAC Accounting
 EAP Accounting

Interim Update: 00:00:00

MAC Format: XXX:XX:XX:XX:XX:XX

MAC Mode: as username

OK
Cancel
Apply
Copy
Remove

New Security Profile

General | RADIUS | EAP | Static Keys

EAP Methods: EPA-TLS

TLS Mode: no certificates

TLS Certificate: none

OK
Cancel
Apply
Copy
Remove

New Security Profiles

- Increased speed of the EAP authentication. Useful to decrease the CPU usage when `tls-mode=no-certificate` is used.
- Added WPA2 Pairwise Master Key caching (802.11i optional feature) to increase client reconnection speed

User Manager

- User Authorization using MSCHAPv1,MSCHAPv2
- User status page
- User sign-up system
- Support for decimal places in credits
- Authorize.net payment gateway support
- Database backup feature
- License changes in RouterOS v3.0 for active users:
 - Level3 – 10 active users
 - Level4 – 20 active users
 - Level5 – 50 active users
 - Level6 – Unlimited active users

The Dude

- RouterOS package – works as dude server
- Speed improvements between server/client
- Dude Agents to reach private networks and offload service monitoring
- Reports from any list/table
- Support for SNMP v3

Console: Colors

```
[admin@RB_7] > interface export
# jan/01/2000 00:26:40 by RouterOS 3.0beta5
# software id = RD45-3TT
#
/interface ethernet
set 0 arp=enabled auto-negotiation=yes cable-settings=default comment="" disable-running-check=yes \
  disabled=no full-duplex=yes mac-address=00:0C:42:0D:4B:37 mtu=1500 name="ether1" speed=100Mbps
set 1 arp=enabled auto-negotiation=yes cable-settings=default comment="" disable-running-check=yes \
  disabled=no full-duplex=yes mac-address=00:0C:42:0D:4B:38 mtu=1500 name="ether2" speed=100Mbps

[admin@RB_7] > :put "Name : ${/system identity get name}\r\nOk"
Name : RB_7
Ok
[admin@RB_7] > error █
```

- Console consumes less memory, it has faster startup and fast export time
- References to items, commands, prompts and exports are coloured
- Currently no way to turn colours off, except running under a dumb terminal

Multi-line Commands

```
[admin@r4] > :put [  
line 2 of 2>         /system \  
line 3 of 3>         package \  
line 4 of 4> get system version]  
3.0beta5
```

- If input line ends with backslash, or has unclosed braces / brackets / quotes / parentheses, then the next line is automatically prompted
- Prompt shows "line N of M>" while editing multi-line command
- History walks through multi-line commands line-by-line

Scripting

```
[admin@RE_7] > :global conntack [:parse "/i f c t p"]
[admin@RE_7] > $conntack
bad command name i (line 1 column 2)
[admin@RE_7] > :global conntack [:parse "/ip f c t p"]
[admin@RE_7] > :environment pr
Global Variables
"conntack"=>{[/ip firewall connection tracking print]}

Automatic Variables

[admin@RE_7] > $conntack
                enabled: yes
        tcp-syn-sent-timeout: 5s
        tcp-syn-received-timeout: 5s
```

- Errors now show line position
- New console command “:parse” - transforms text into Mikrotik RouterOS command
- Non-existing command now generates runtime error instead of parse-time error

Scripting (part 2)

- Updated console command “:typeof”

```
[admin@RB_7] > :put (a=>1)
a=1
[admin@RB_7] > :put [:typeof (a=>1)]
pair
[admin@RB_7] > :put [:typeof ({a=>1;b=>2})]
array
[admin@RB_7] > :put [:typeof ({a=>1;b=>2}->b)]
str
[admin@RB_7] > :put ({a=>1;b=>2}->b)
2
```


Scripting (part 3)

```
[admin@r4] > :put ([/in et pr as-value ])  
.id=*1;comment=;name=ether1;mtu=1500;mac-address=52:54:00:64:03:00;arp=enabled;  
.id=*2;comment=;name=ether2;mtu=1500;mac-address=52:54:00:64:03:01;arp=enabled;  
.id=*3;comment=;name=ether3;mtu=1500;mac-address=52:54:00:64:03:02;arp=enabled  
[admin@r4] > :put [:typeof ([/in et pr as-value ])]  
array  
[admin@r4] > :put ([/in et get ether1]->"mac-address")  
52:54:00:64:03:00
```

- Arrays can be written as { item ; item ; item } inside expressions
- New “print” argument “as-value” - allows returning content of the menu as one array
- Each item now has unique, constant ID (.id), it could be used instead of item numbers

NAT Traversal

- NAT Traversal (NAT-T) is a workaround allowing specific services to establish connections from masqueraded TCP/IP networks
 - Introduced NAT-T for SIP
 - Introduced NAT-T for IPSec
 - Rewritten NAT-T for h323
 - Rewritten NAT-T for PPTP

Interface Bridge Settings

- There is a new menu in RouterOS v3.0
 - /interface bridge settings
- There are two new options
 - use-ip-firewall (yes|no, default:no)- whether to pass internal bridge packet through the IP firewall (conntrack, filters, mangle, nat), or not
 - use-ip-firewall-for-vlan (yes|no, default:no) – if “use-ip-firewall=yes” whether to pass bridge VLAN packet through the IP firewall (conntrack, filters, mangle, nat), or not

Use-ip-firewall Option

- By disabling “use-ip-firewall” option you can increase bridge performance by:
 - ◆ Up to 40% with random size packets on the RouterBOARD 200 series
(up to 65% with small and up to 20% with big packets)
 - ◆ Up to 65% with random size packets on the RouterBOARD 100 series
(up to 80% with small and up to 45% with big packets)
 - ◆ Up to 80% with random size packets on the RouterBOARD 500 series
(up to 100% with small and up to 65% with big packets)

To be continued...
... it is only beta8 ;)

Questions?