MikroTik™

RouterOS v3

# MikroTik RouterOS v3

New
Obvious and Obscure
Mikrotik RouterOS v3.x features

# Kernel

- RouterOS 2.9.51
  - Linux kernel version 2.4.31
- RouterOS 3.14rc1
  - Linux kernel version 2.6.26.2

- 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

- Application programming interface (API) is source code interface that 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

# IPv6 Support

- RouterOS has IPv6 support for
  - Addressing
  - Routing (simple, ECMP, policy)
  - Firewall (filter and mangle,address-list)
  - DNS
  - RIPNG (RIP New Generation)
  - BGP
  - OSPFv3
- There is a stand-alone IPv6 package

# Multicast Support

- MikroTik supports PIM-SM (Protocol Independent Multicast - Sparse-Mode)
- There is a separate multicast package
- MikroTik supports Source Specific Multicast (SSM) which is part of PIM-SM specification.
- There are no plans to support PIM-DM “dense-mode” - PIM-SM performs good in almost every setup, both sparse and dense.

# The Dude

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

# User Manager

- User Authorization using MSCHAPv1,MSCHAPv2
- User status page
- User sign-up system
- Support for decimal places in credits
- Authorize.net and Paypal 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

# Calea Support

- CALEA stands for Communications Assistance for Law Enforcement Act, in some countries ISPs are required to be able to intercept and log network traffic.
- RouterOS provides CALEA facility by means of firewall rules
- RouterOS can also function as a data retention server
- There is a separate CALEA-server package

# OpenVPN support

- Open source virtual private network
  - Pre-shared private key, certificate, or username/password authentication
  - AES and Blowfish encryption supported
  - Either layer-3 (IP packet) or layer-2 (Ethernet frame) carrier
  - Runs over single TCP/IP port
- Default RouterOS OpenVPN port is 1194 UDP.

# Hardware Bridge Support

- Now it is possible to use bridge chip functionality on RB100 and RB400 series – Ethernets of one bridge chip can be bridged together
- Interfaces have new “S” (Slave) flag for interfaces in bonding or hardware bridge states
  - Slave interface stops working as a regular interface and addresses become invalid

# 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 have optimized memory usage

# New OSPF and OSPFv3 Implementation

- Completely MikroTik rewritten OSPF (no Zebra or another pre written source code used)
- Completely new routing package for OSPF and routing-test for OSPFv3 created
- Several previously unfixable bugs fixed

# New BGP features

- Features available only with routing-test package
- Added support for 4-octet BGP AS numbers
  - New AS number format as=340.6430
  - Old format works as well
- Added default-originate feature for BGP peers.
- Added IPv6 BGP networks and aggregates

# New VRRP Implementation

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

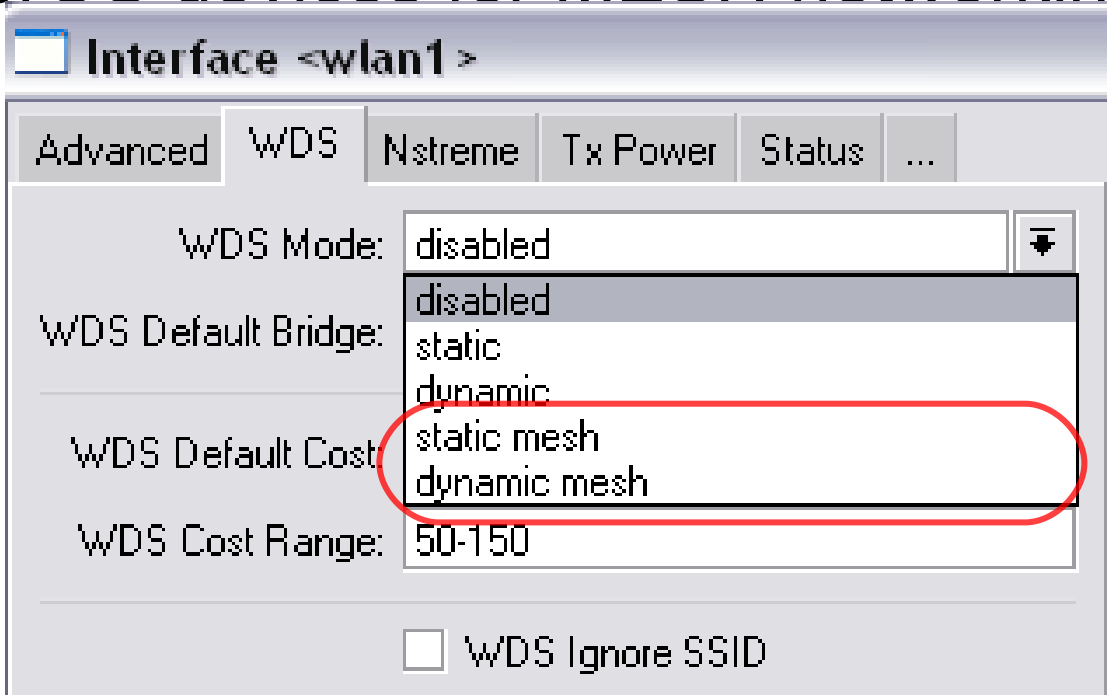
# HWMP for MESH

- Uses MikroTik specific HWMP+ protocol for wireless mesh networks
- Is NOT compatible with HWMP (Hybrid Wireless Mesh Protocol) from 802.11s standard
- Can also work together with RSTP
- Supports multiple entry/exit points for network
- Supports WDS and Ethernet interfaces
- Configuration in '/interface mesh' menu

# Wireless Features

- WDS-MESH
  - WDS-mode=dynamic-mesh/static-mesh

New improved WDS connection between RouterOS devices for MESH networking.



# Wireless Features

- "MAC NAT" bridge
  - Station-pseudobridge

    Learns which IP address has which MAC address and translates it.

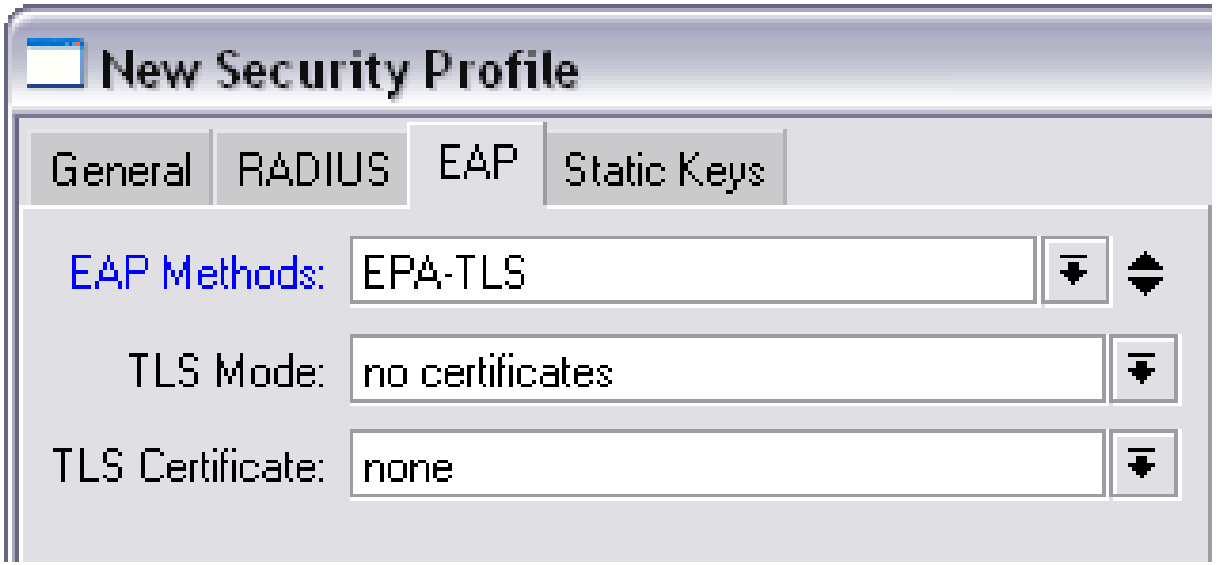
  - Station-pseudobridge-clone

    Uses one MAC address of the device and clones it to the wireless interface.

# Wireless Features

- WPA2 Pairwise Master Key caching
  - 802.11i optional feature

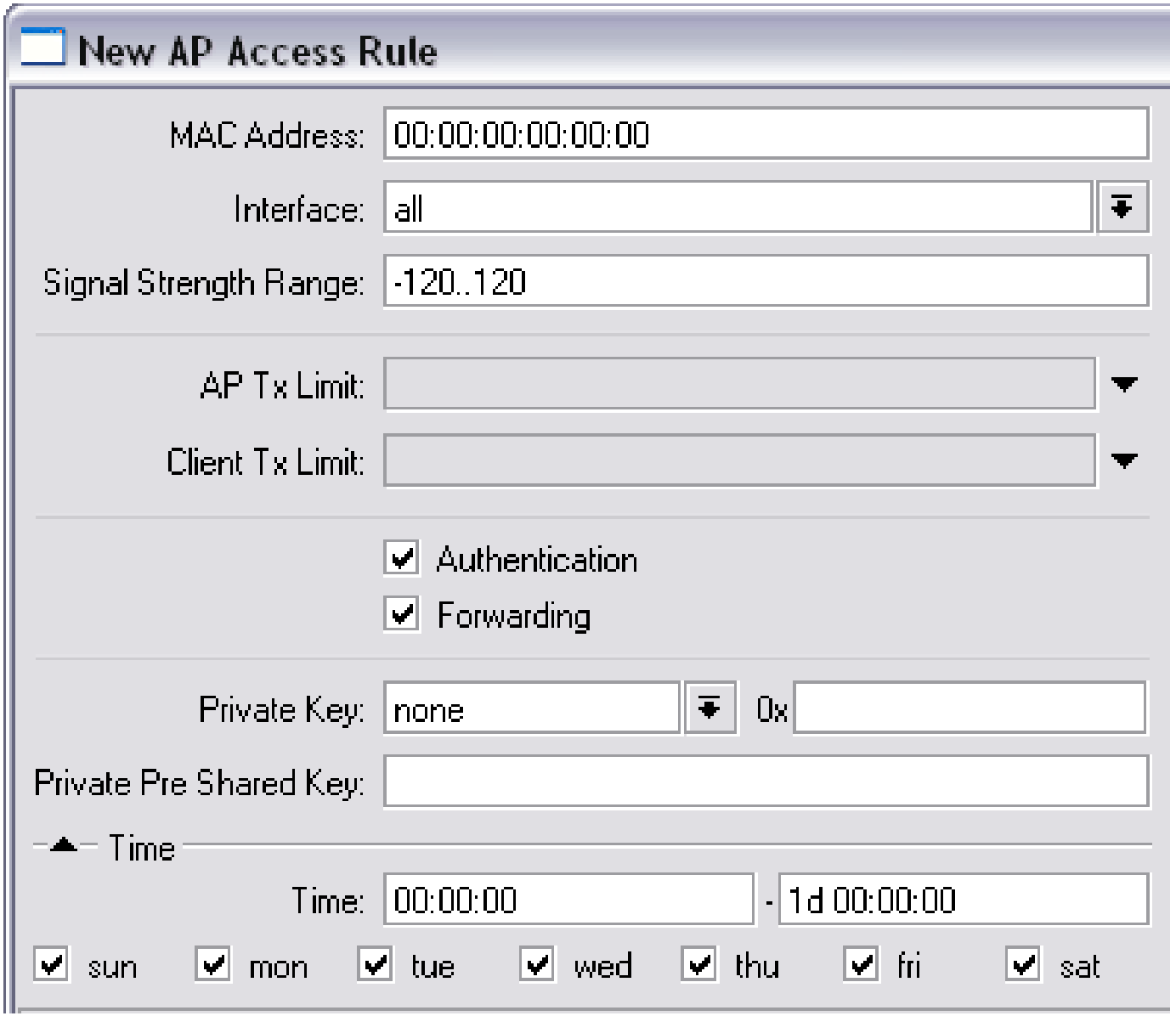
    Increased speed of the EAP authentication;
    Useful to decrease the CPU usage when using the tls-mode=no-certificate.



# Wireless Features

- Access-list
  - The order of entries is important, just like for 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, client disconnects.
  - “Private-pre-shared-key” - each client can have different key; works only when PSK method is used

# Wireless Features



# Wireless Features

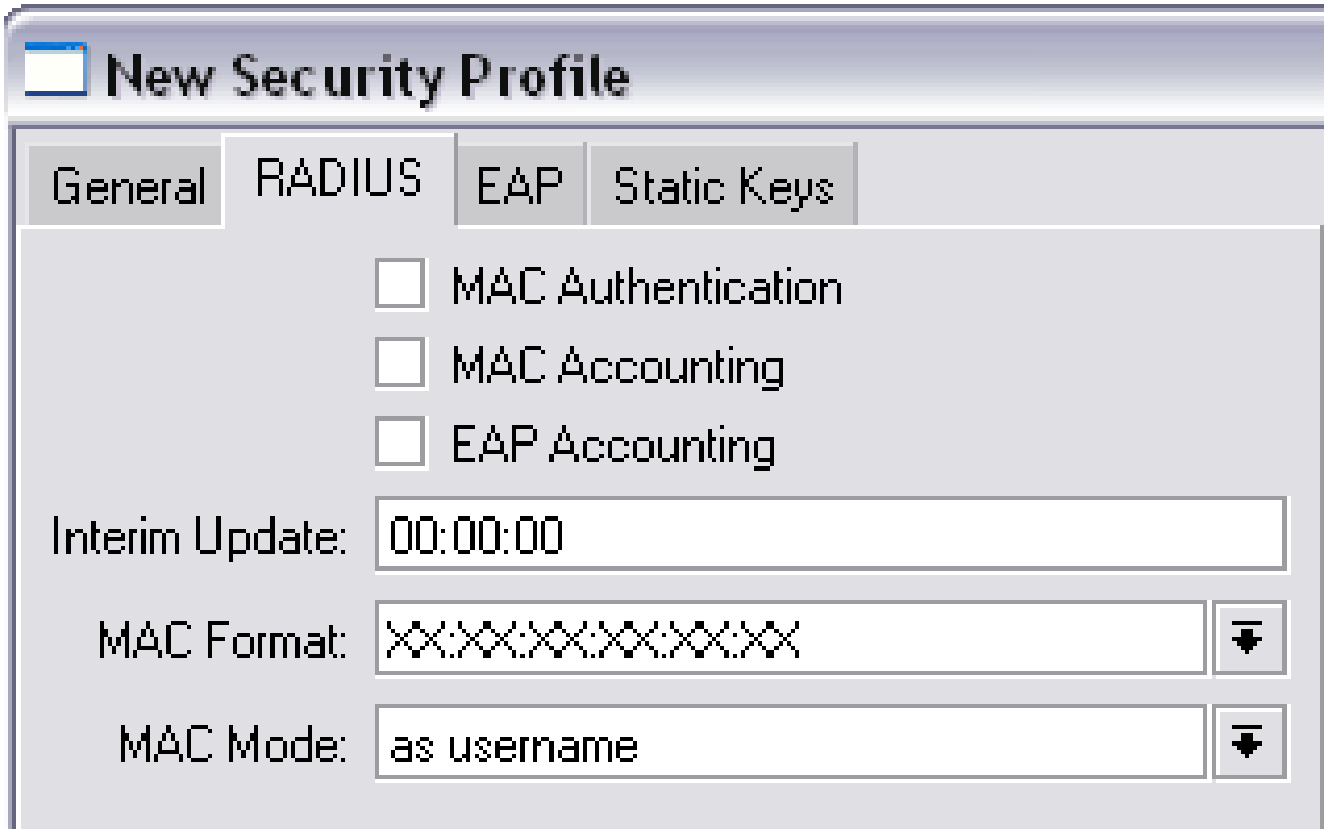
- Connect-list
  - “Signal-range” - client will connect to the AP which will be within this signal range. If the signal goes out of the range client disconnects from AP and starts searching for a new AP by checking the connect-list entries.
- Nstreme
  - Improved performance on lower speed boards (RB100 Series)
  - “Disable-csma” - disables the “medium access” protocol if the polling is enabled

# Wireless Features

- Security-profile
  - “Radius-mac-accounting” - MAC address 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”

# Wireless Features

- Security-profile



# 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 export
- References to items, commands, prompts and exports are coloured
- Added options to turn off console colours by adding +c after username

# 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 next line is automatically prompted
- Prompt shows "line N of M>" if editing multi-line command
- History walks through multi-line commands line-by-line

# Scripting

```
[admin@RB_7] > :global conntrack [:parse "/i f c t p"]
[admin@RB_7] > $conntrack
bad command name i (line 1 column 2)
[admin@RB_7] > :global conntrack [:parse "/ip f c t p"]
[admin@RB_7] > :environment pr
Global Variables
"conntrack"=>{[/ip firewall connection tracking print]}

Automatic Variables

[admin@RB_7] > $conntrack
                    enabled: yes
      tcp-syn-sent-timeout: 5s
  tcp-syn-received-timeout: 5s
```

- Errors now show line position
- New console command “:parse” to parse text into Mikrotik RouterOS command
- Non-existing command 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 contents of the menu as one array
- Each item now has unique, constant ID (.id), could be used instead of item numbers

# Scripting (part 4)

```
[admin@RouterA] > :global a {1,2,3}; :global b {4,5,6}
[admin@RouterA] > :put ($a,$b)
1;2;3;4;5;6
[admin@RouterA] > :foreach i in="10.$a.$b.0/24" do={:put $i}
10.1.4.0/24
10.1.5.0/24
10.1.6.0/24
10.2.4.0/24
10.2.5.0/24
10.2.6.0/24
10.3.4.0/24
10.3.5.0/24
10.3.6.0/24
[admin@RouterA] >
```

- ',' operator can be used inside expressions to concatenate arrays
- Changed behaviour of '.' operator when one or both of operands are arrays

# Layer-7 Filter

- layer7-protocol is a method of looking for patterns in connections
- Patterns must be specified as Regexp strings in the “/ip firewall layer7-protocol” menu
- Regexp example:
  skype to skype – regexp="^..\02....."
  world of warcraft - regexp="^\06\EC\01"

# 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

# PPP Support for MP

- MRRU is a new setting for PPP, PPTP, L2TP & PPPoE (not ISDN) that specifies maximum packet size that can be received on the link
- Multilink PPP protocol support over single link is enabled by specifying MRRU, large packets are split into smaller ones
- Multilink PPP client support over multiple links – usernames and passwords must be the same for every incoming PPP link.

# PPP Support for BCP

- BCP(Bridge Control Protocol) allows sending raw Ethernet packets over PPP tunnel
- To make it work, specify “bridge” setting in "ppp profile"
- Tunnel must be bridged at both ends
- The bridge should have MAC address set manually, or at least one regular Ethernet interface added to it, because ppp interfaces do not have MAC addresses.

# Interface Bridge Settings

- There is 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) - 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 get bridge performance boost:
  - Up to 2,5x-3x on the RouterBOARD 100,500,300 series
  - Up to 2x-2,5x on the RouterBOARD 400,600,1000 series
- By disabling “use-ip-firewall” option you will also loose all ip firewall features (conntrack, mangle, filter, nat) only for traffic going through the bridge

# Virtualization by Xen

- Multiple OS within single RouterOS box;
  - Ability to run multiple RouterOS;
  - Ability to run other OS for more functions;
  - Unlimited functionality all-in-one box;
- Currently available for x86 boxes;
- Development in progress for RouterBOARDs;

# MPLS

- Extremely efficient routing-label forwarding process;
- Packet forwarding based on labels attached;
- RSVP TE(Traffic Engineering) support available;
- VPLS(Virtual Private LAN Service);
- Compatible with other vendors MPLS;

# To be continued...

# Thank you!