

Router Optimization with Firewall/Raw

Valens Riyadi

PT Citraweb Solusi Teknologi

www.mikrotik.id

 @valensriyadi

 @valensriyadi

Valens Riyadi

Mikrotik Certified Trainer pertama di Asia Pacific

PHP, mySQL, IT on Disaster, Cyber Crime

Head of NIR - IDNIC (APJII) 2009-2015

- PT Citraweb Solusi Teknologi
 - MikroTik Distributor & Training Center
- PT Jembatan Citra Nusantara
 - Internet Service Provider (citra.net)
- PT Citraweb Digital Multisolusi
 - Web developer



Live Streaming

<http://mikrotik.id>

Follow Citraweb on:

 @mikrotik.id

 @mikrotik.indonesia

Sehubungan dengan pelaksanaan acara Final Olimpiade Jaringan 2017 dan MikroTik User Meeting 2017, operasional kantor dan penjualan PT Citraweb Solusi Teknologi diliburkan pada Kamis-Jumat, 26-27 Oktober 2017. Penjualan akan berjalan seperti biasa pada Senin, 30 Oktober 2017. Mohon maklum.

KATEGORI PRODUK
<input type="text" value="Cari produk"/>
<input type="button" value="Cari"/>
Voucher MUM
Lisensi Mikrotik RouterOS
Interface
RouterBoard (only)
mAP & cAP
hAP
hEX
wAP
Groove & Metal
BaseBox & NetMetal
SXT & LHG
OmniTik & mANTBox
SEXTANT & QRT
Disc & DynaDish
Cloud Router Switch
Switch
Router Indoor
Router Outdoor
RouterBoard 2011
RouterBoard 3011 NEW
Cloud Core Router
Mikrobits Router & Switch
Mikrobits Fiber SFP & Patch
Wireless Indoor 800

Live From MUM-ID 2017



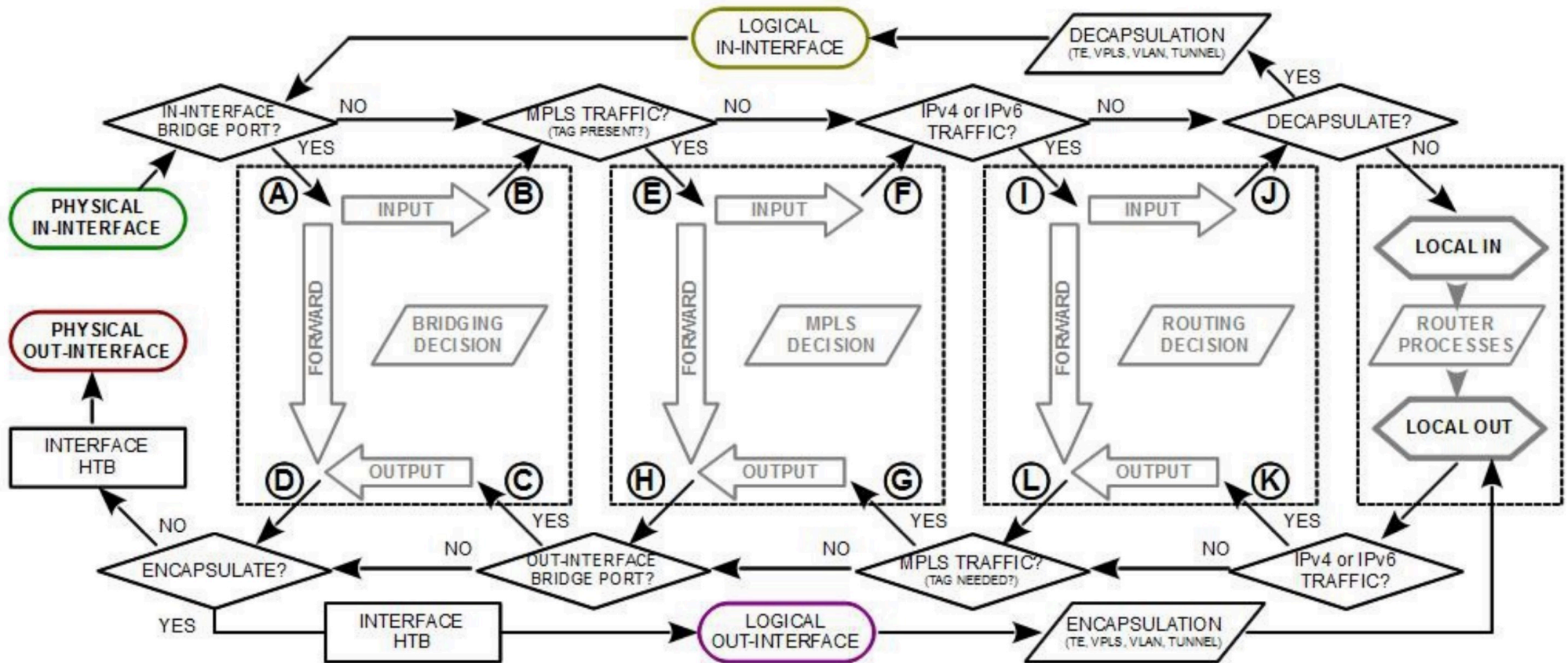
Video Tutorial Mikrotik



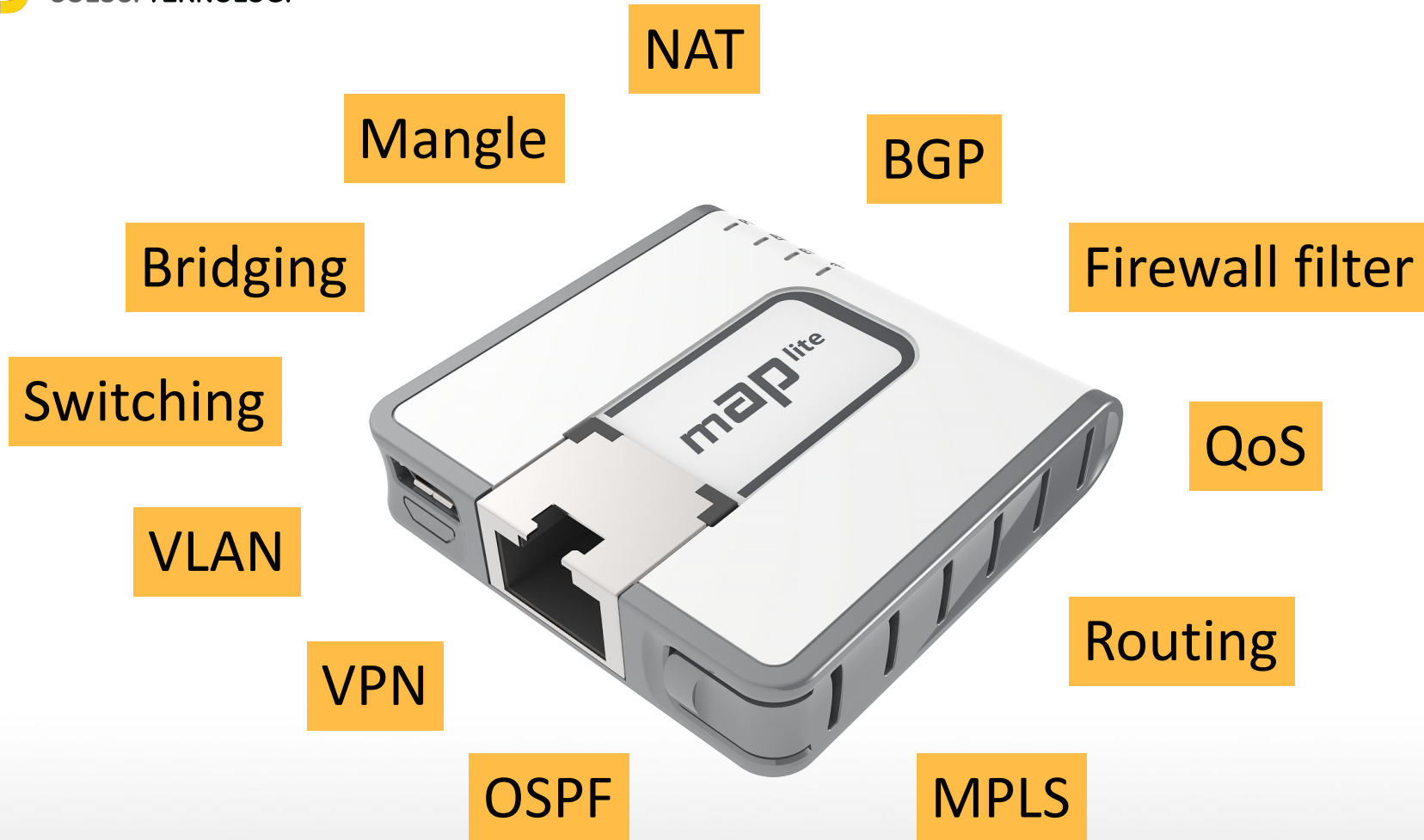
Video lainnya



ARTIKEL BARU



Packet Flow di MikroTik RouterOS



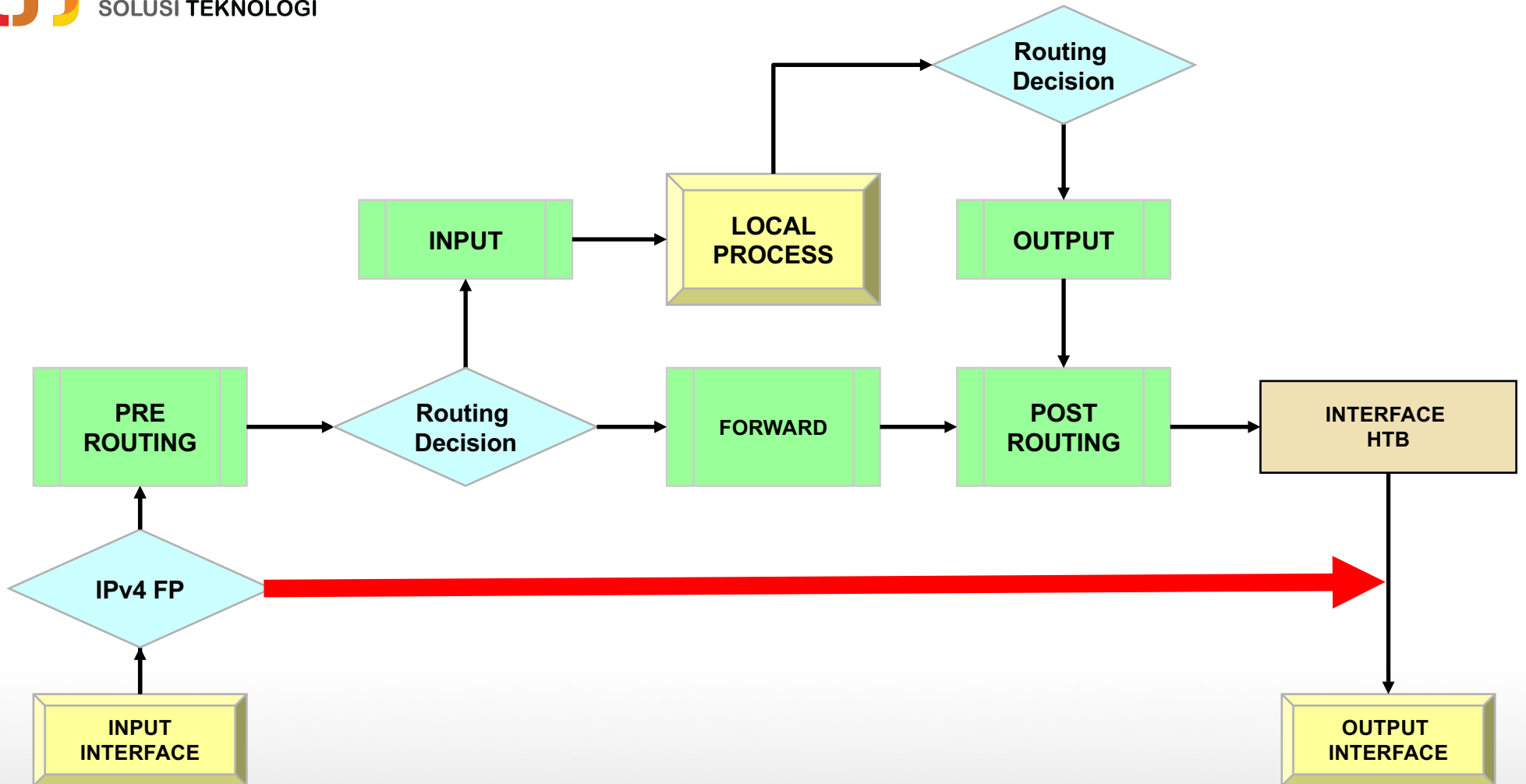
PERFORMANCE

”saya tidak menggunakan fitur-fitur itu semua”
“saya hanya butuh forwardingnya saja”



Fast Path

- Mulai RouterOS v6
- Melewatkan traffic tanpa melalui fitur-fitur yang ada di RouterOS, sehingga load CPU lebih rendah dan delay juga lebih rendah.



Tanpa FastPath

Session: 192.168.88.1 CPU: 42%

Interface List

Interface	Name
R	ether1
R	ether2
	ether3
	ether4
R	ether5
X	wlan1

6 items

IP Settings

IP Forward

Send Redirects

Accept Redirects

Secure Redirects

Accept Source Route

Allow Fast Path

Route Cache

RP Filter: no

TCP SynCookies

Max Neighbor Entries: 8192

ARP Timeout: 00:00:30

ICMP Rate Limit: 10

IPv4 Fast Path Active

IPv4 Fast Path Packets: 5 084 598

IPv4 Fast Path Bytes: 7.1 GiB

IPv4 Fasttrack Active

IPv4 Fasttrack Packets: 0

IPv4 Fasttrack Bytes: 0 B

WRRP Bonding LTE

Find

	Rx	Tx Packet (p/s)
0 bps	59.8 Mbps	
74.5 kbps	7.7 kbps	
0 bps	0 bps	
0 bps	0 bps	
60.6 Mbps	0 bps	5 03
0 bps	0 bps	

Dengan FastPath

Session: 192.168.88.1 CPU: 9%

Interface List

Interface	Inter
R	ether1
R	ether2
	ether3
	ether4
R	ether5
X	wlan1

6 items

IP Settings

- IP Forward
- Send Redirects
- Accept Redirects
- Secure Redirects
- Accept Source Route
- Allow Fast Path
- Route Cache

RP Filter: no

TCP SynCookies

Max Neighbor Entries: 8192

ARP Timeout: 00:00:30

ICMP Rate Limit: 10

- IPv4 Fast Path Active

IPv4 Fast Path Packets: 8 083 173

IPv4 Fast Path Bytes: 11.3 GiB

WRRP Bonding LTE

Find

	Rx	Tx	Packet (p/s)
	0 bps	60.1 Mbps	
	72.6 kbps	7.1 kbps	
	0 bps	0 bps	
	0 bps	0 bps	
	60.6 Mbps	0 bps	5 03
	0 bps	0 bps	

Hardware Compability with FastPath

- RB6xx series ether1,2
- Most of the RB7xx series all ports
- RB800 ether1,2
- RB9xx series all ports
- RB1000 all ports
- RB1100 series ether1-11
- RB2011 series all ports
- RB3011 series all ports
- CRS series routers all ports
- CCR series routers all ports

Virtual Interface

- bridge interfaces (since 6.29)
- vlan, vrrp interfaces (since 6.30)
- bonding interfaces - rx only (since 6.30)
- eoip, gre, ipip interfaces (since 6.33).
Eoip, gre, ipip interfaces have per interface setting "allow-fast-path".

Allowing fast path on eoip, gre, ipip interfaces have side effect of bypassing firewall, connection tracking, simple queues, queue tree with parent=global, ip accounting, ipsec, hotspot universal client, vrf assignment for encapsulated packets that go through fastpath. Note that allowing fast path for tunnel does not guarantee that all packets will go fastpath, so for slowpath packets regular processing happens as before

Syarat FastPath

- firewall rules are not configured;
- firewall address lists are not configured;
- Simple and queue trees with parent=global are not configured;
- no mesh, metarouter interface configuration;
- sniffer, torch and traffic generator is not running;
- connection tracking is not active;
- ip accounting is disabled (/ip accounting enabled=no);
- VRFs are not set (/ip route vrf is empty);
- Hotspot is not used (/ip hotspot has no interfaces);
- IpSec policies are not configured (ROS v6.8);
- /tool mac-scan is not actively used;
- /tool ip-scan is not actively used;
- route cache must be enabled

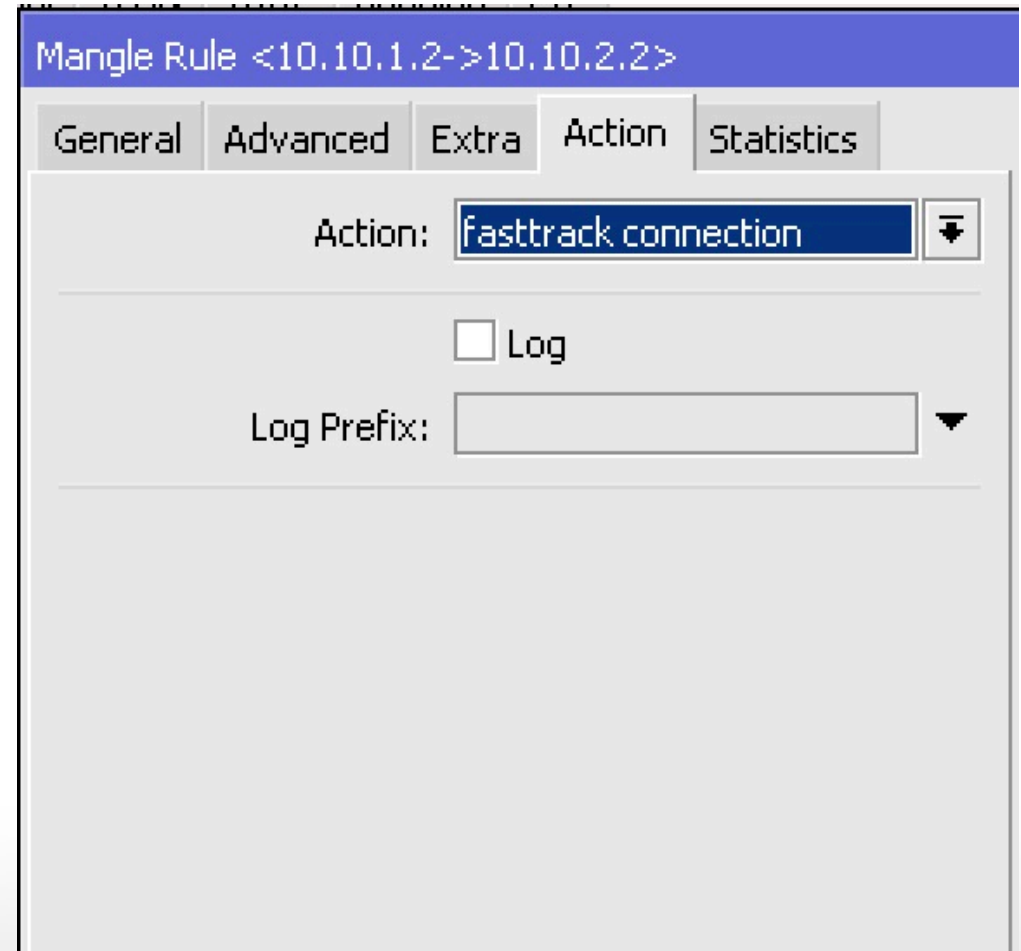
Kekurangan FastPath

- Tidak bisa dijalankan di semua hardware/interface.
List lengkap, cek di wiki...
- On-off berlaku untuk keseluruhan trafik pada router tersebut, tidak bisa memilih mana trafik yang FastPath dan mana yang SlowPath
- Banyak fungsi yang sama sekali tidak bisa jalan: firewall, mangle, torch, etc.

FastTrack

FastTrack

Fitur pada mangle dan filter, di mana kita bisa memilih connection tertentu untuk menjadi “fast-track”, sehingga paket established dan related berikutnya tidak lagi diperiksa di mangle, filter, QoS, dll.



Filter/Mangle Accept

- (established, related - accept)
- Paket data tidak diproses oleh rule berikutnya di chain tersebut, tetapi tetap akan diproses oleh fungsi lain berikutnya.
- Misalnya, firewall/filter chain=forward action=accept, maka paket tetap akan diproses oleh chain postrouting dan QoS.

FastTrack

- Paket yang masuk FastTrack tidak akan diproses fungsi berikutnya, langsung ke interface keluar.
- Misalnya, firewall/filter chain=forward action=fasttracked-connection, maka paket tidak akan diproses oleh chain postrouting dan QoS.

FastTrack Restrictions

- no mesh, metarouter interface configuration;
- sniffer, torch and traffic generator is not running;
- /tool mac-scan is not actively used;
- /tool ip-scan is not actively used;

FastPath atau FastTrack ?

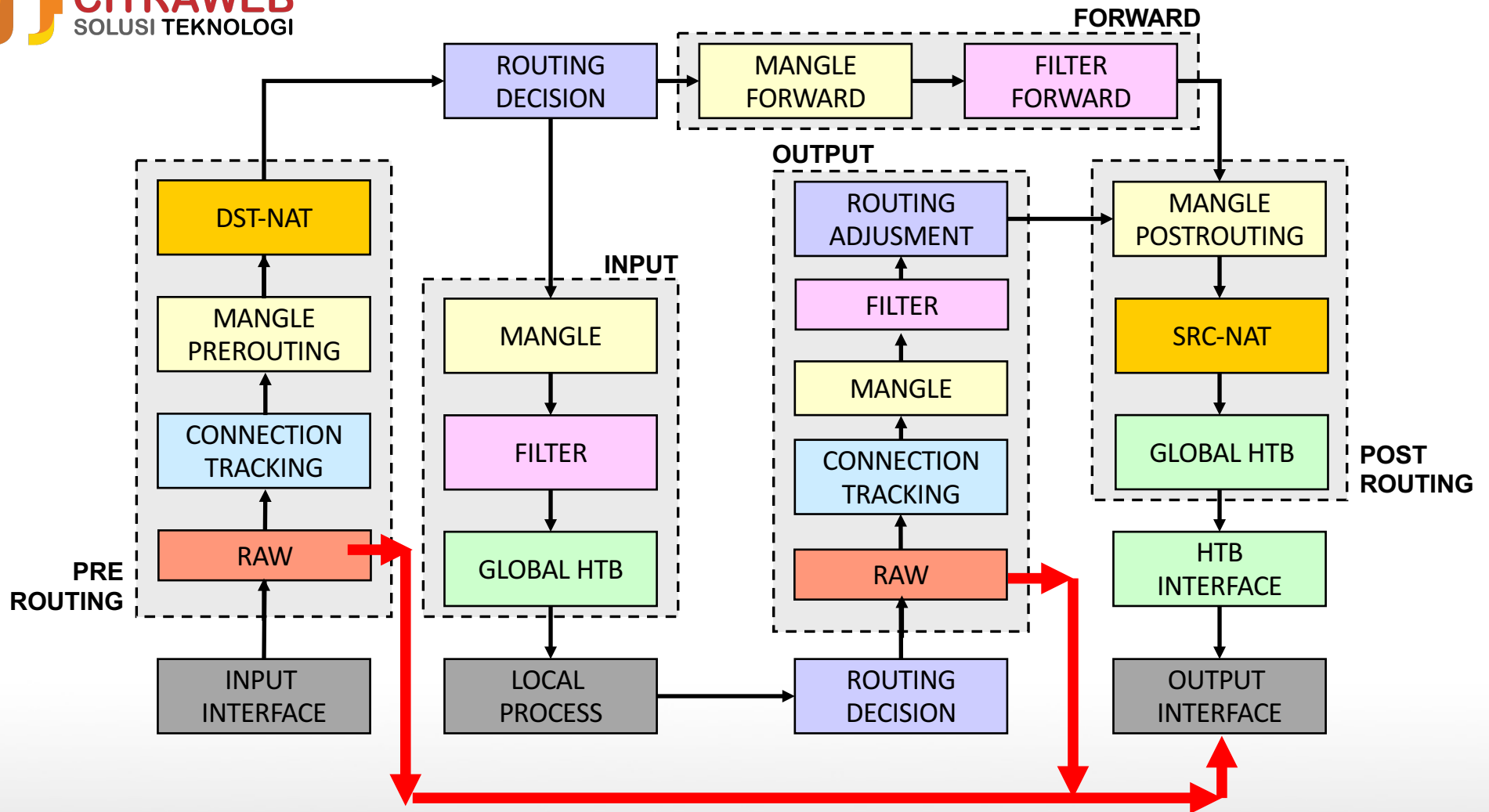
Tanpa connection-tracking
Berlaku untuk seluruh sistem
Untuk traffic apapun

Berdasarkan connection-tracking
Untuk paket established dan related
Hanya untuk TCP dan UDP
Bisa memilih koneksi yg fast-track
Tidak berjalan untuk paket tanpa koneksi

RAW

Firewall-RAW

- Mulai ROS 6.36rc21
- Firewall RAW memungkinkan kita memilih untuk melewatkan atau mendrop paket SEBELUM connection tracking, sehingga menghemat load CPU.
- Sangat berguna untuk DDOS mitigation.
- Hanya bisa dilakukan pada chain prerouting dan output, posisinya tepat sebelum connection tracking.



Firewall

Filter Rules NAT Mangle **Raw** Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ 📄 🗑️ 00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets
---	--------	-------	--------------	--------------	---------	-----------	-----------	------------	-----------	-------	---------

New Raw Rule

General Advanced Extra Action ...

Chain: prerouting

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

New Raw Rule

General Advanced Extra Action ...

Src. Address List:

Dst. Address List:

Content:

Per Connection Classifier:

Src. MAC Address:

IPsec Policy:

Ingress Priority:

Priority:

DSCP (TOS):

TCP MSS:

Packet Size:

New Raw Rule

Advanced Extra Action Statistics ...

- Limit
- Dst. Limit
- Nth
- Time
- Src. Address Type
- Dst. Address Type
- PSD
- Hotspot
- IP Fragment

Raw tidak memiliki parameter yang berhubungan dengan connection-tracking, seperti connection-state, L7, packet-mark, dll.

Tanpa FastPath– 30-50% CPU Load

admin@192.168.88.1 (MikroTik) - WinBox v6.40.4 on RB751U-2HnD (mipsbe)

CPU: 37%

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRPP	Bonding	LTE
R	ether1	Ethernet							
R	ether2	Ethernet							
	ether3	Ethernet							
	ether4	Ethernet							
R	ether5	Ethernet							
X	wlan1	Wireless (Atheros AR...							

IP Forward

Send Redirects

Accept Redirects

Secure Redirects

Accept Source Route

Allow Fast Path

Route Cache

Firewall

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets
0 X	Fas...	forward								0 B	0
1	acc...	forward	1.1.1.1	2.2.2.2						0 B	0
2	acc...	forward	1.1.1.1	2.2.2.2						0 B	0
3	acc...	forward	1.1.1.1	2.2.2.2						0 B	0
4	acc...	forward	1.1.1.1	2.2.2.2						0 B	0

IPv4 Fast Path Active

Dengan FastPath– 10-20% CPU Load

admin@192.168.88.1 (MikroTik) - WinBox v6.40.4 on RB751U-2HnD (mipsbe)

CPU: 14%

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
R	ether1	Ethernet							
R	ether2	Ethernet							
R	ether3	Ethernet							
R	ether4	Ethernet							
R	ether5	Ethernet							
X	wlan1	Wireless (Atheros AR...							

IP Forward

Send Redirects

Accept Redirects

Secure Redirects

Accept Source Route

Allow Fast Path

Route Cache

Firewall

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets
---	--------	-------	--------------	--------------	---------	-----------	-----------	------------	-----------	-------	---------

filter: no

TCP SynCookies

tries: 8192

out: 00:00:30

Limit: 10

IPv4 Fast Path Active

kets: 4 001 044

ytes: 5.6 GIB

Dengan RAW – 10-20% CPU Load

admin@192.168.88.1 (MikroTik) - WinBox v6.40.4 on RB751U-2HnD (mipsbe)

CPU: 14%

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
R	ether1	Ethernet							
R	ether2	Ethernet							
R	ether3	Ethernet							
R	ether4	Ethernet							
R	ether5	Ethernet							
X	wlan1	Wireless (Atheros AR...							

- IP Forward
- Send Redirects
- Accept Redirects
- Secure Redirects
- Accept Source Route
- Allow Fast Path
- Route Cache

Firewall

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Int...	Out. Int...	Bytes	Packets
0	no track	prerouting	10.10.1.2	10.10.2.2						481.5 MIB	339 755

- Filter: no
- TCP SynCookies
- tries: 8192
- out: 00:00:30
- Limit: 10
- IPv4 Fast Path Active
- ackets: 4 119 986
- ytes: 5.8 GiB

Contoh Aplikasi RAW

- RAW untuk trafik yang melalui router, sedangkan pengamanan “input” tetap bisa menggunakan L7, connection-tracking, dll.
- Firewalling, port-scan, ddos detection menggunakan firewall forward. Jika terdeteksi ada serangan, add-src-to-ddress-list.
- RAW action=drop untuk trafik yang berasal dari address-list penyerang tersebut
- CPU load yang dibutuhkan untuk melakukan drop pada RAW jauh lebih kecil dibandingkan Filter-drop

FastPath



FastTrack

Raw

FastPath

- Berlaku pada seluruh trafik di router tersebut, tidak bisa memilih
- Tidak bisa menjalankan connection-tracking, firewall, dll

RAW

- RAW adalah matcher untuk masuk 'fast-path'
- Berlaku sesuai dengan matcher, traffic lainnya bisa melalui "slow-path" atau "fast-track"
- Connection-tracking tetap dapat berfungsi untuk trafik non-RAW, juga fitur kompleks lainnya
- Bisa digunakan untuk connection-less traffic (di Fast-Track tidak bisa)
- RAW juga bisa digunakan melakukan drop

Lihat lebih detail:

- FastPath: https://wiki.mikrotik.com/wiki/Manual:Fast_Path
- FastTrack: <https://wiki.mikrotik.com/wiki/Manual:IP/Fasttrack>
- RAW: <https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Raw>

Thank You!

Valens Riyadi

PT Citraweb Solusi Teknologi

www.mikrotik.id

 @valensriyadi

 @valensriyadi