CITRAWEB
SOLUSI TEKNOLOGI

Router Optimation with Firewall/Raw

Valens Riyadi

PT Citraweb Solusi Teknologi

www.mikrotik.id

@valensriyadi

@valensriyadi


CITRAWEB
SOLUSI TEKNOLOGI
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

CITRAWEB
SOLUSI TEKNOLOGI

Live Streaming

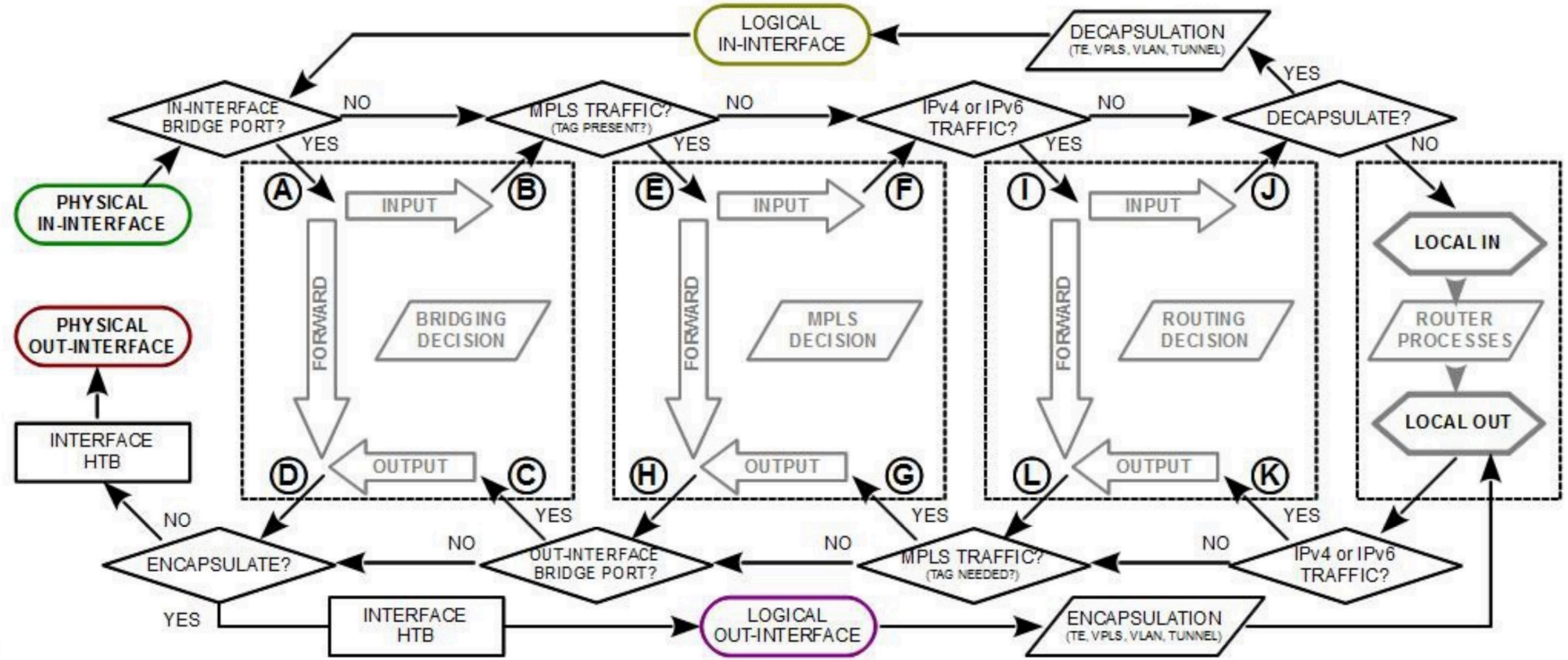
http://mikrotik.id

Follow Citraweb on:

@mikrotik.id

@mikrotik.indonesia

CITRAWEB
SOLUSI TEKNOLOGI



Packet Flow di MikroTik RouterOS

CITRAWEB
SOLUSI TEKNOLOGI

NAT

Mangle

BGP

Bridging

Firewall filter

Switching

QoS

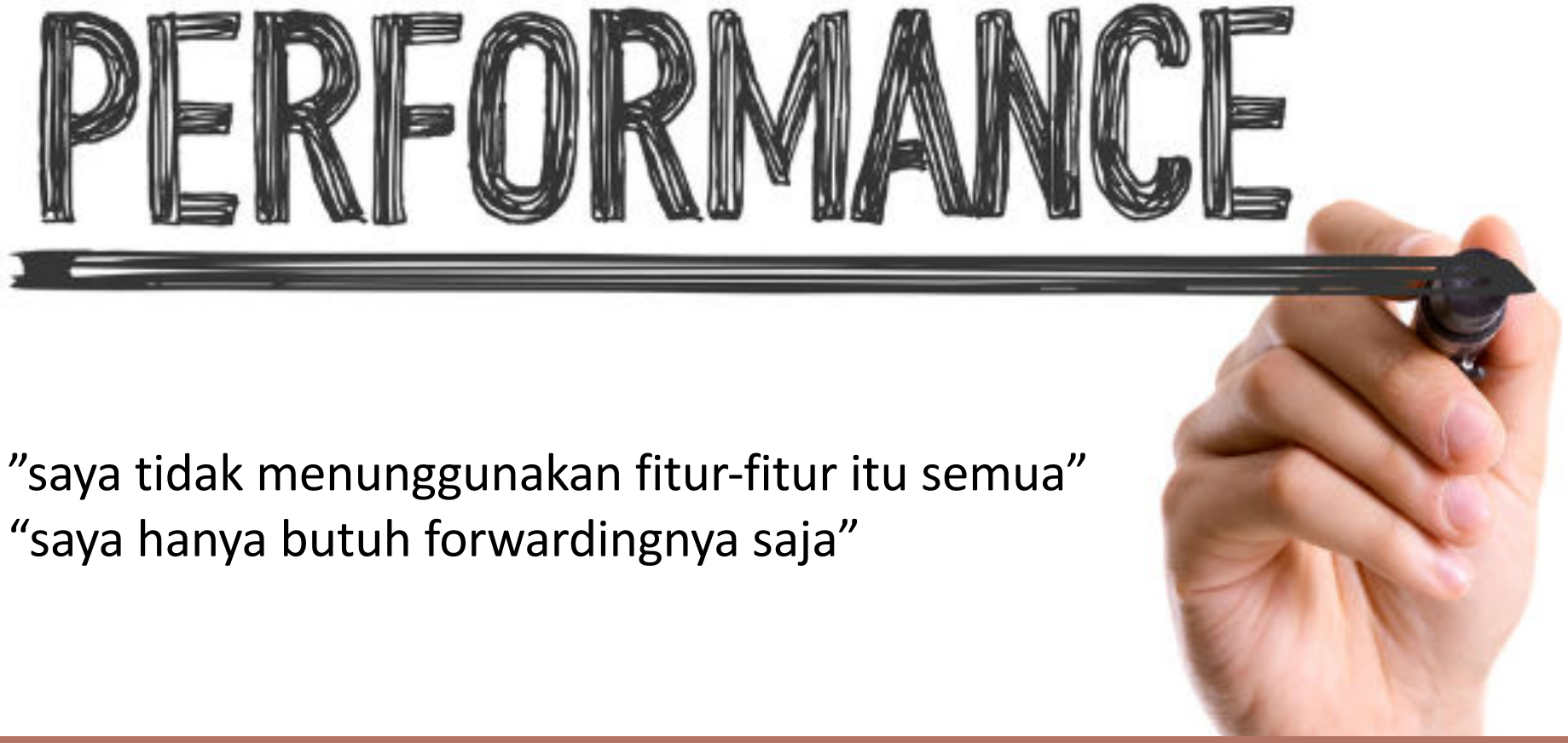
VLAN

Routing

VPN

OSPF

MPLS



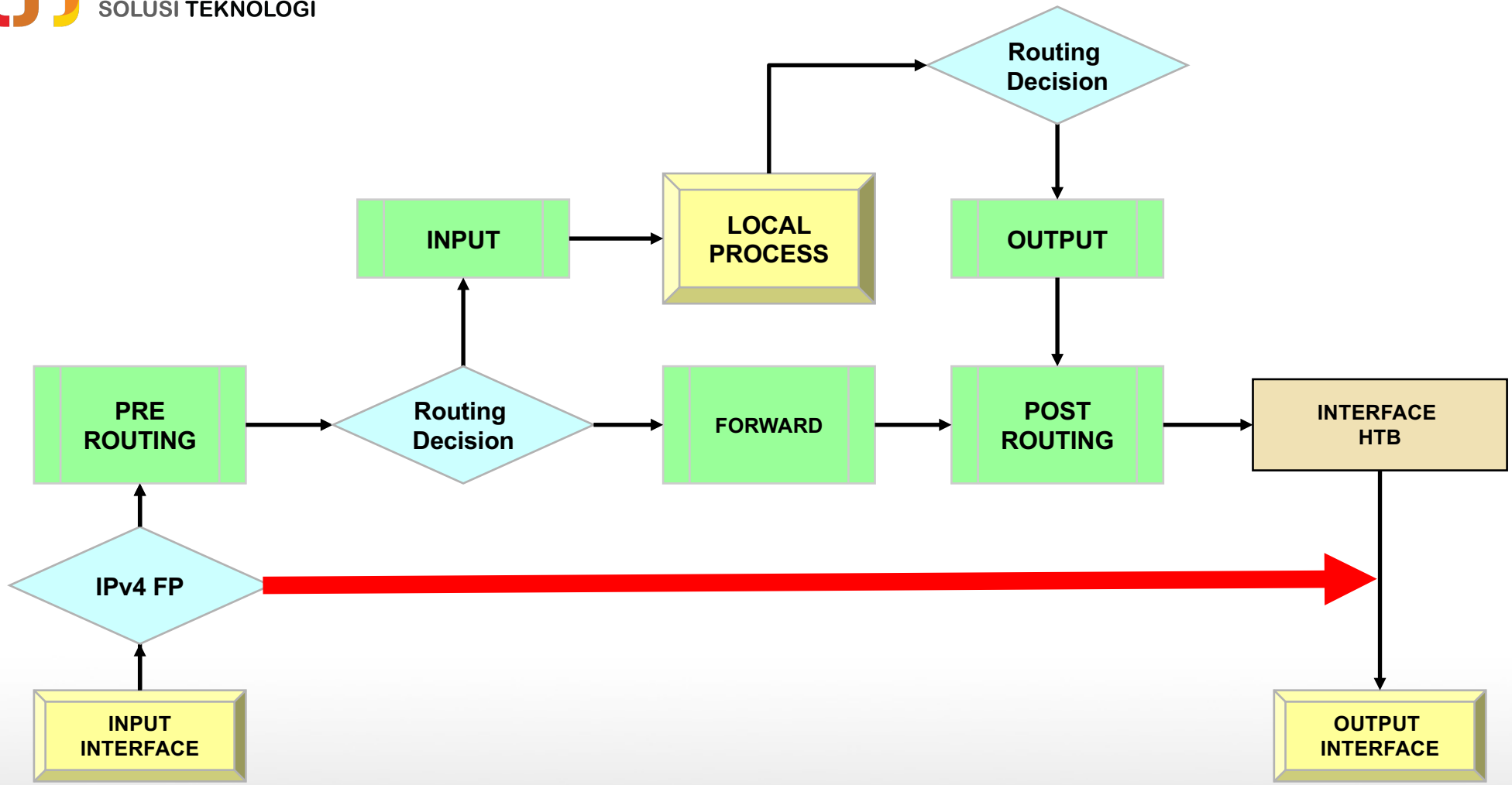
”saya tidak menunggunakan fitur-fitur itu semua”
“saya hanya butuh forwardingnya saja”

CITRAWEB
SOLUSI TEKNOLOGI

Fast Path

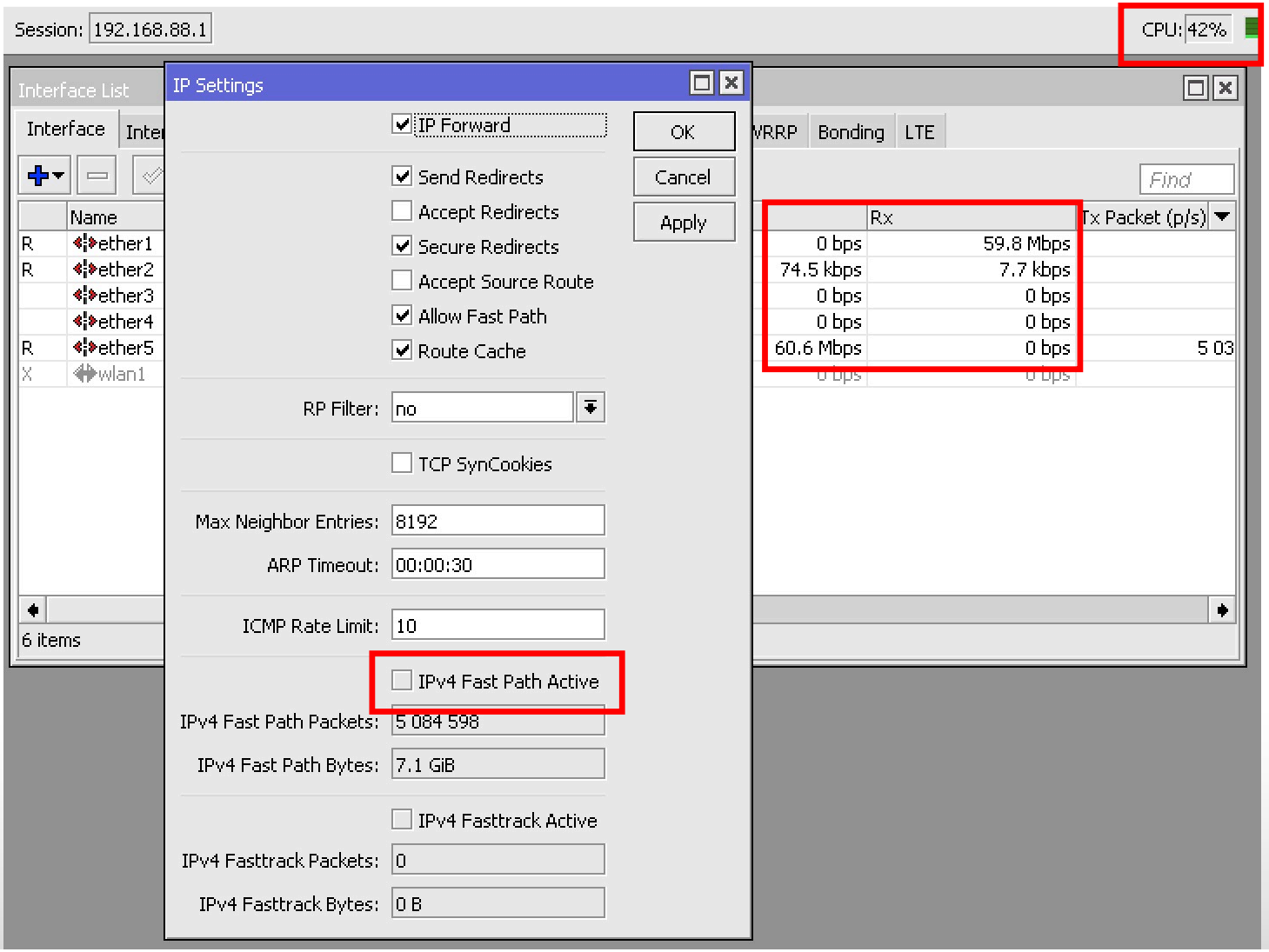
- Mulai RouterOS v6
- Melewatkan traffic tanpa melalui fitur-fitur yang ada di RouterOS, sehingga load CPU lebih rendah dan delay juga lebih rendah.

CITRAWEB
SOLUSI TEKNOLOGI



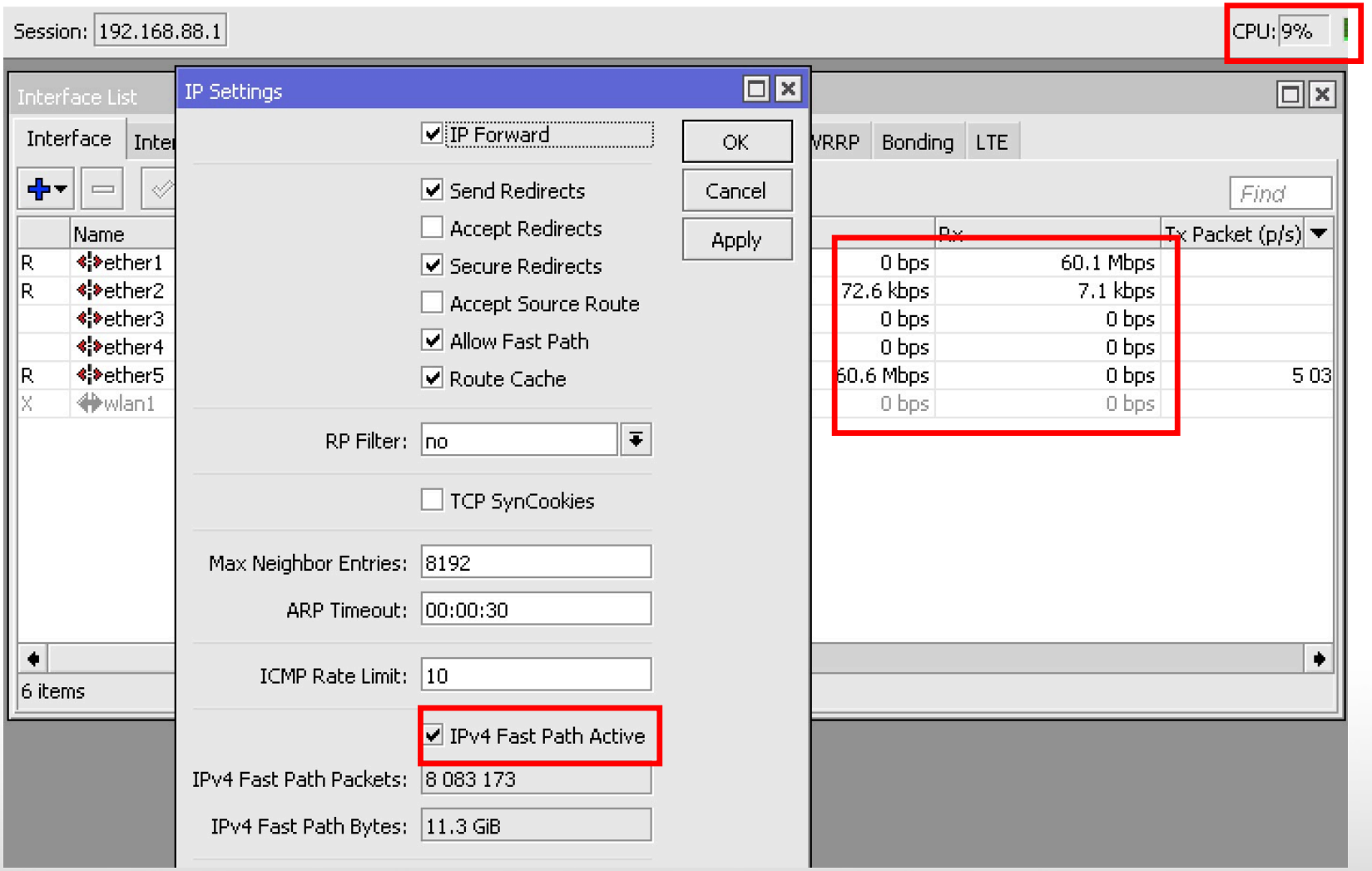
CITRAWEB
SOLUSI TEKNOLOGI

Tanpa FastPath



CITRAWEB
SOLUSI TEKNOLOGI

Dengan FastPath



CITRAWEB
SOLUSI TEKNOLOGI

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

CITRAWEB
SOLUSI TEKNOLOGI

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 trough 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

CITRAWEB
SOLUSI TEKNOLOGI

Syarat FastPath

- firewal 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 hostspot 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

CITRAWEB
SOLUSI TEKNOLOGI

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.

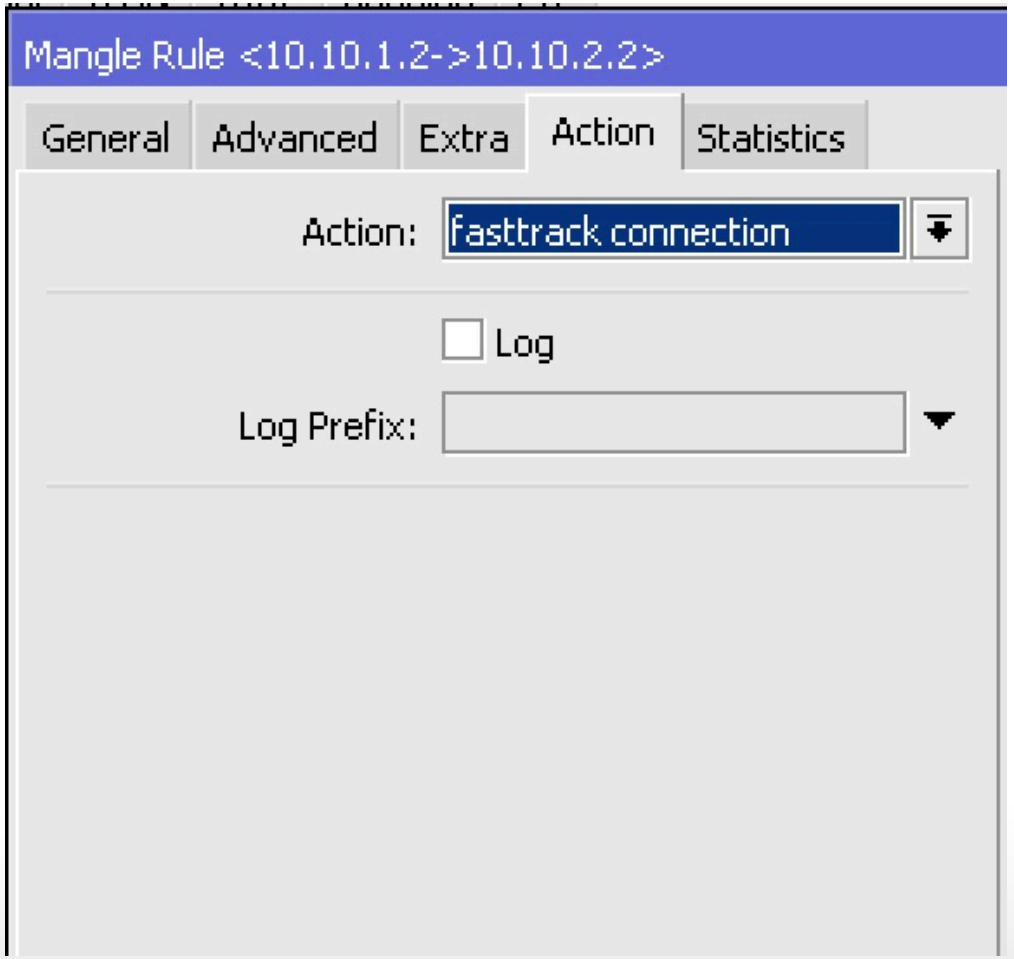
CITRAWEB
SOLUSI TEKNOLOGI

FastTrack

CITRAWEB
SOLUSI TEKNOLOGI

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.



CITRAWEB
SOLUSI TEKNOLOGI

Filter/Mangle Accept

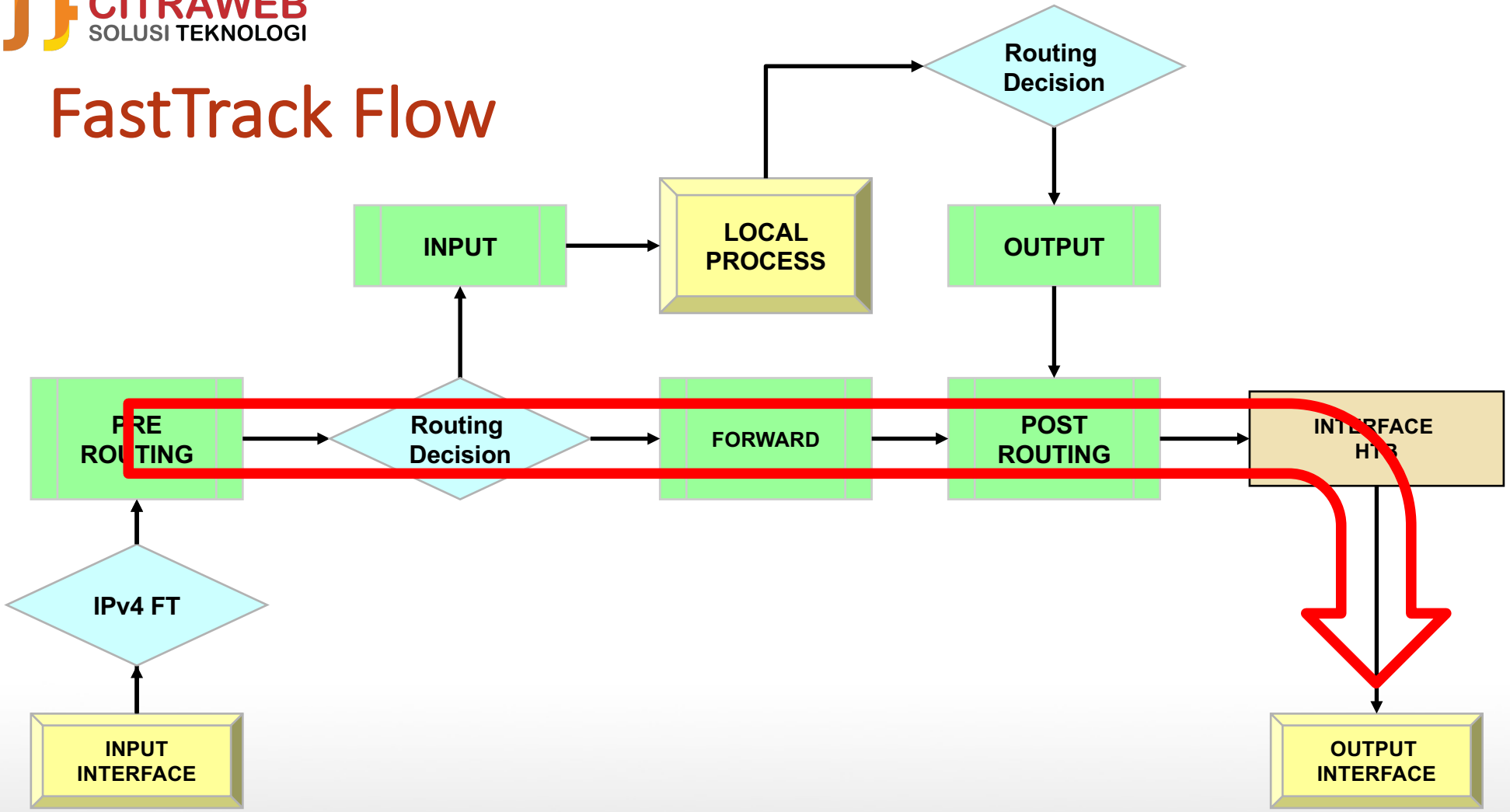
- (established, related - accept)
- Paket data tidak diproses oleh rule berikutnya di chain tersebut, tetapi tetap akan diproses oleh fungsi lain berikutnya.
- Misalnya, firewall/filter chain=forward action=accept, maka paket tetap akan diproses oleh chain postrouting dan QoS.

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.

CITRAWEB
SOLUSI TEKNOLOGI

FastTrack Flow



CITRAWEB
SOLUSI TEKNOLOGI

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;

CITRAWEB
SOLUSI TEKNOLOGI

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

CITRAWEB
SOLUSI TEKNOLOGI

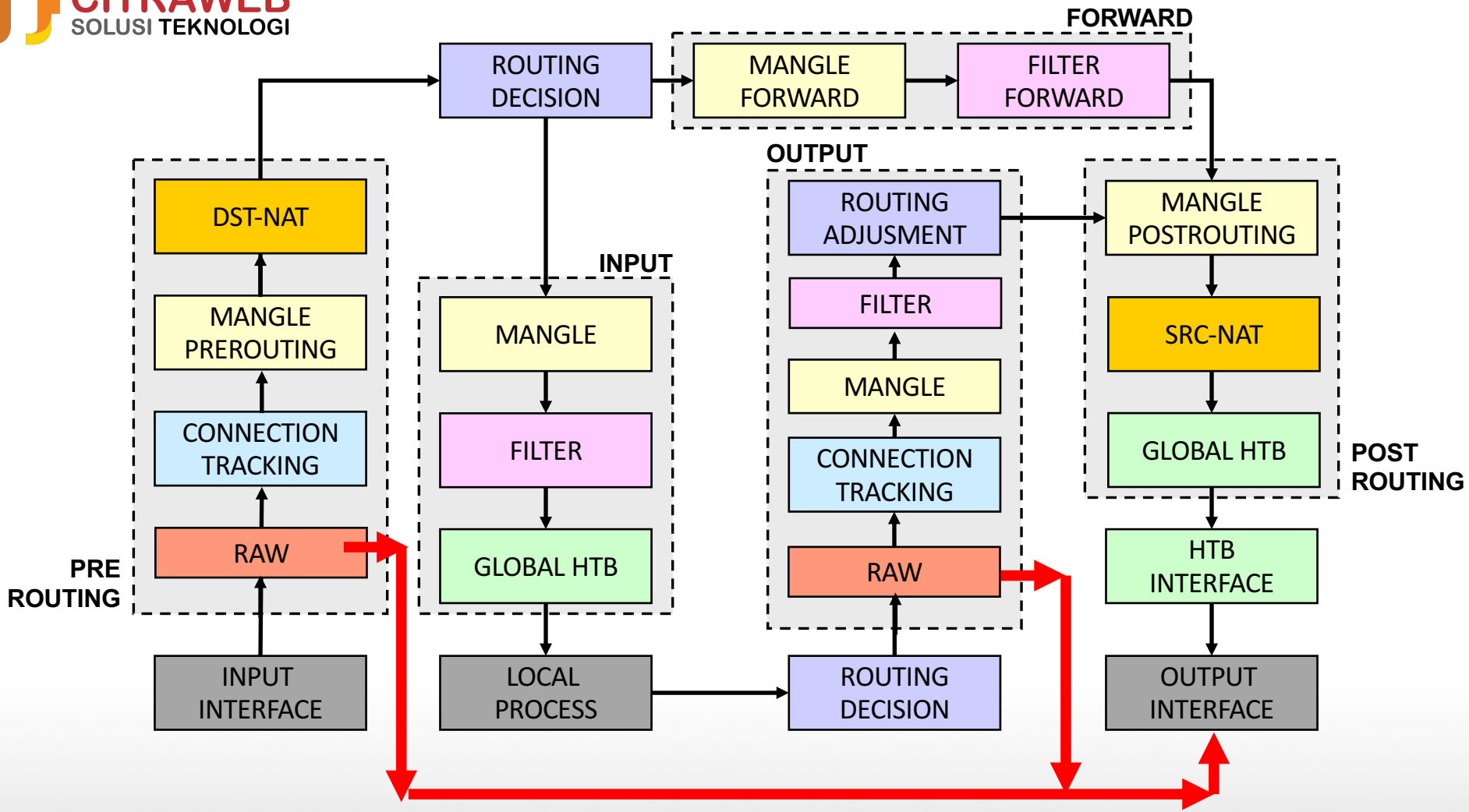
RAW

CITRAWEB
SOLUSI TEKNOLOGI

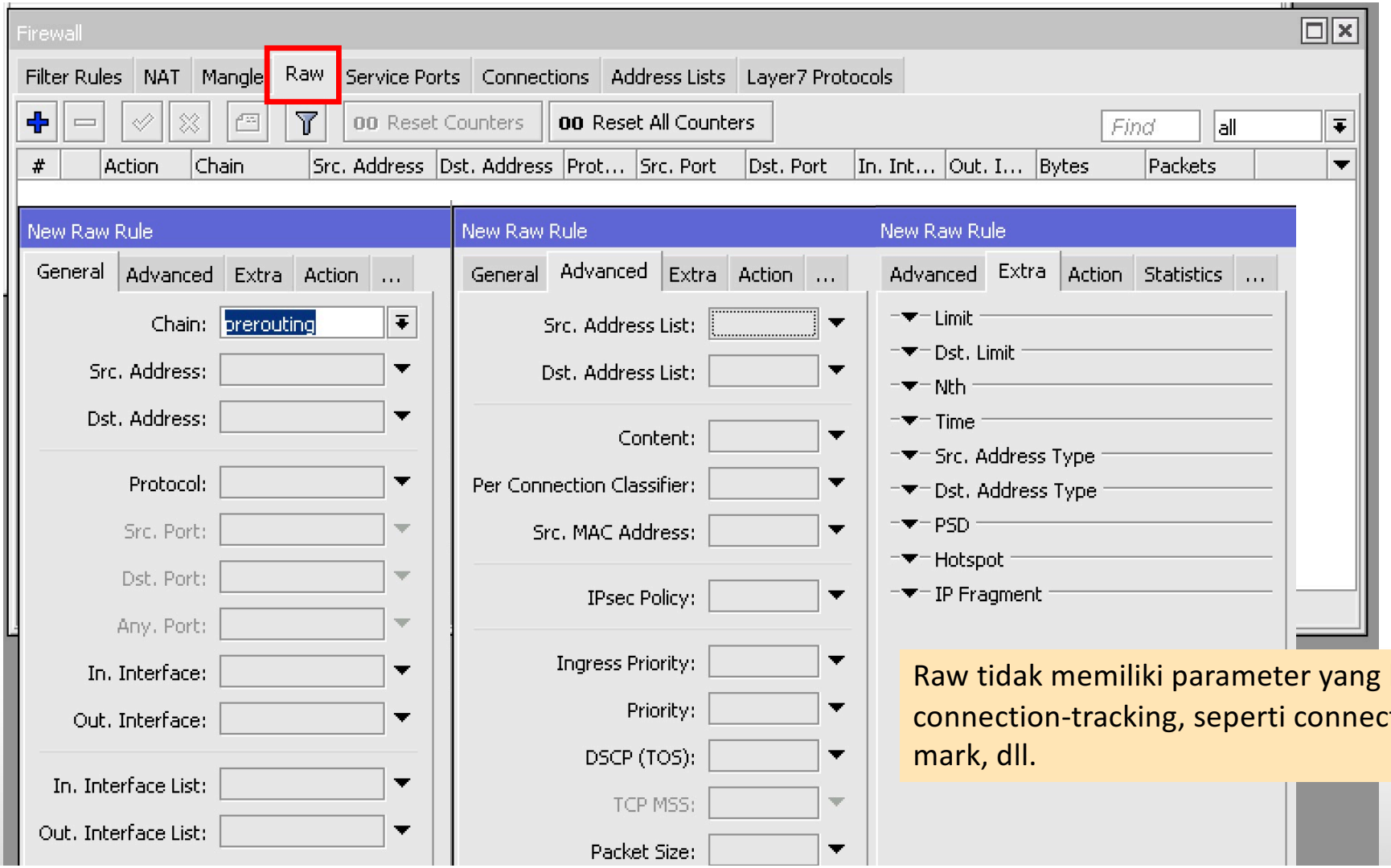
Firewall-RAW

- 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.

CITRAWEB
SOLUSI TEKNOLOGI



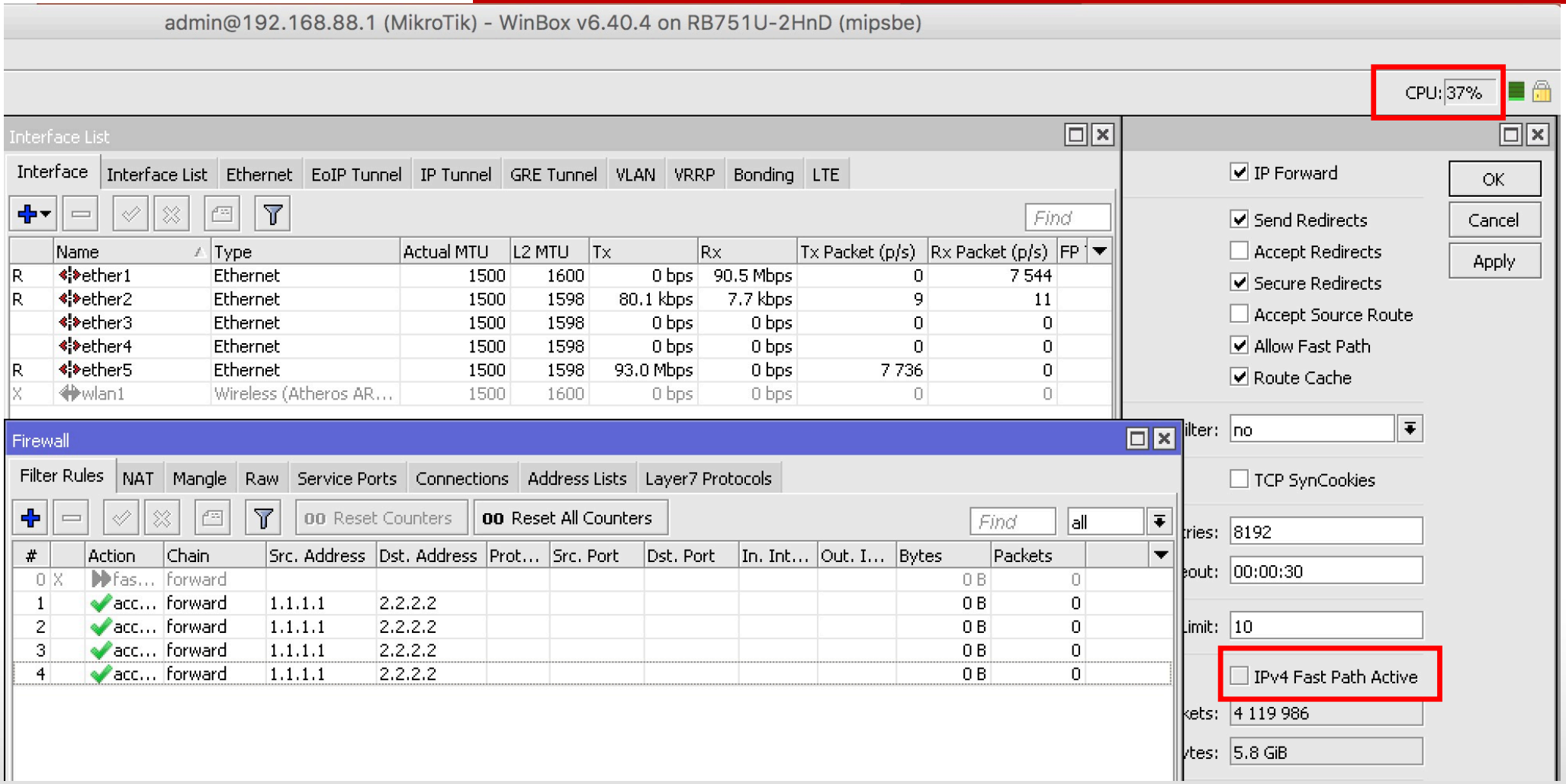
CITRAWEB
SOLUSI TEKNOLOGI



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

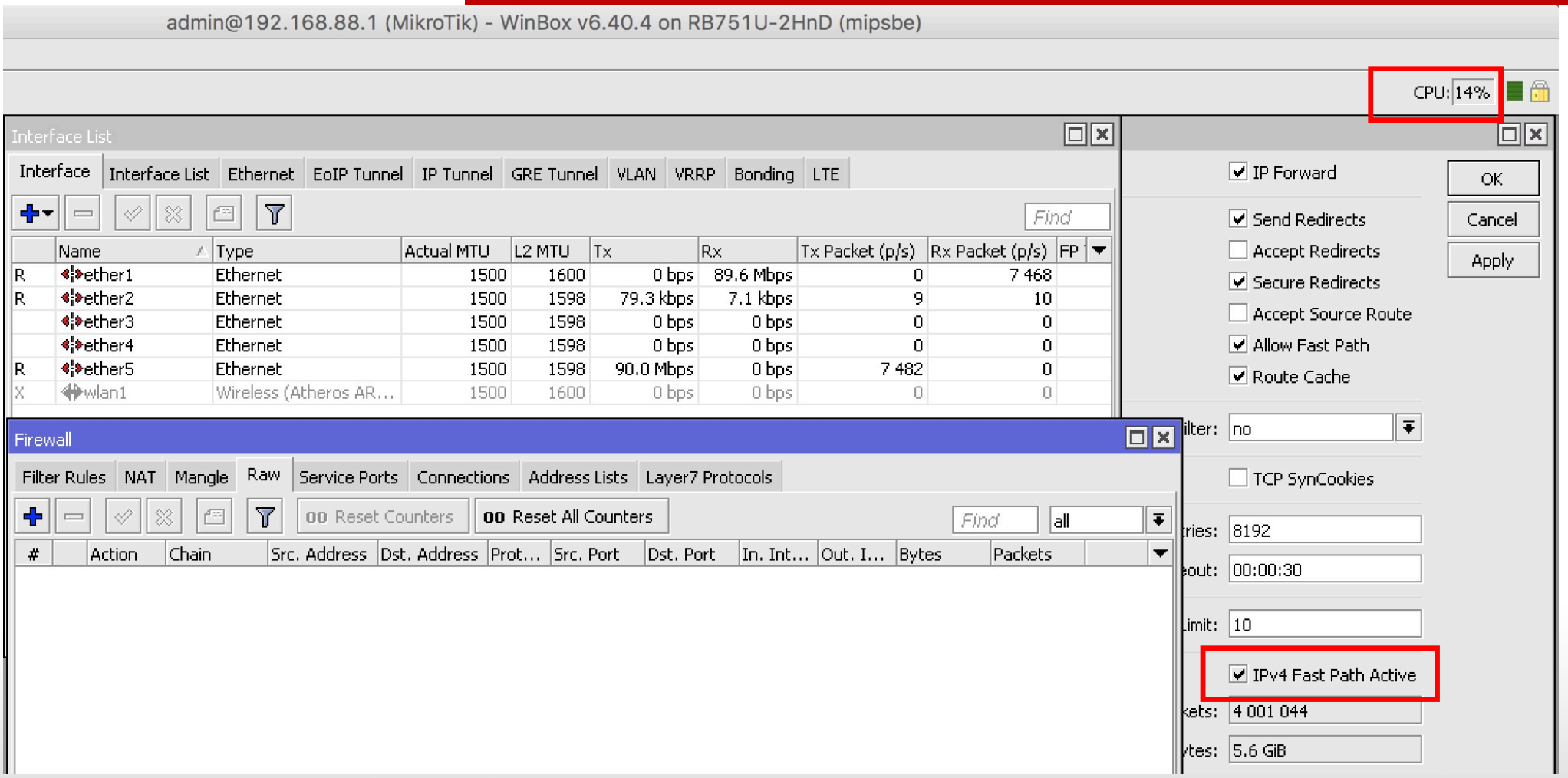
CITRAWEB
SOLUSI TEKNOLOGI

Tanpa FastPath– 30-50% CPU Load



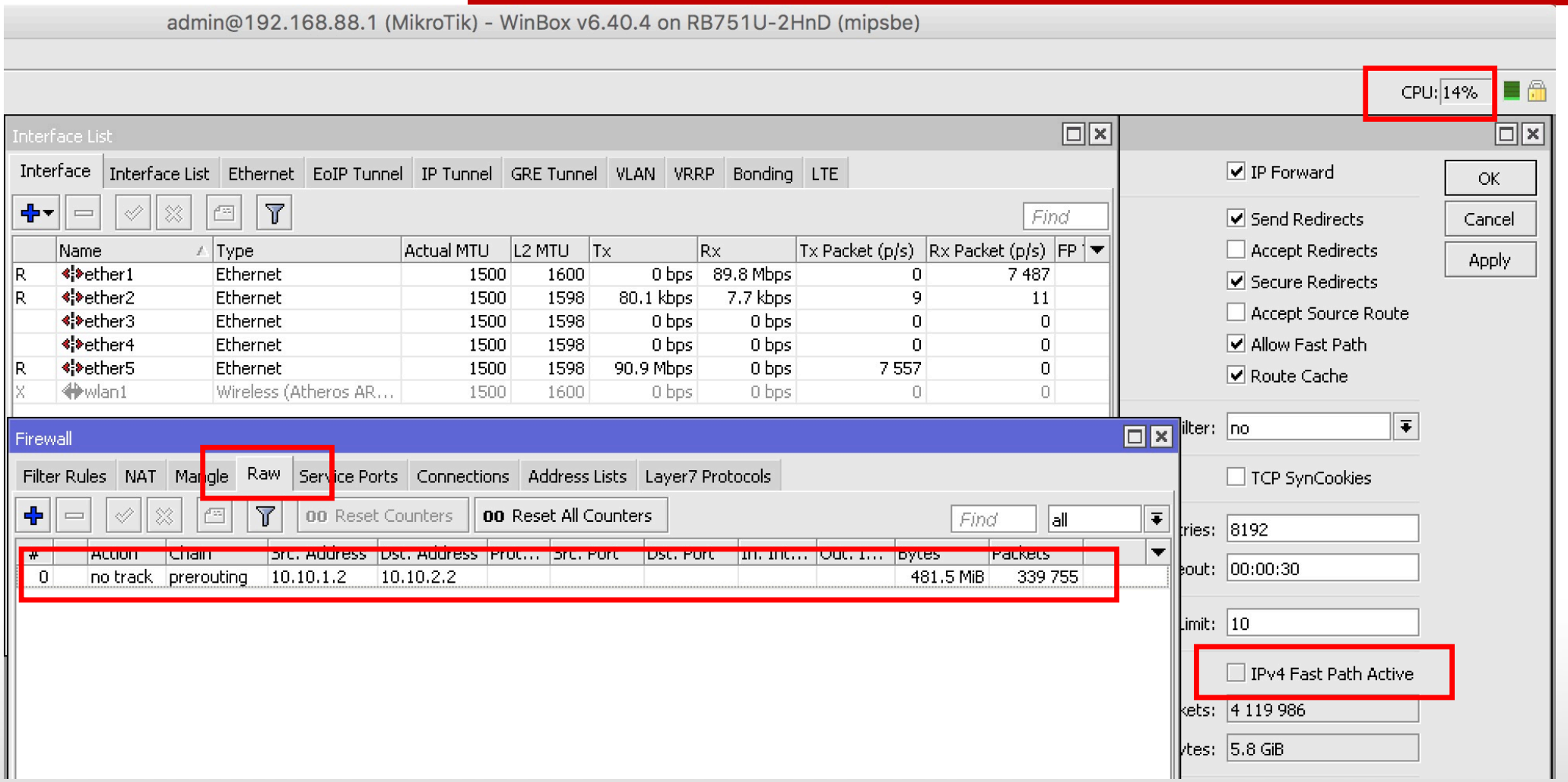
CITRAWEB
SOLUSI TEKNOLOGI

Dengan FastPath– 10-20% CPU Load



CITRAWEB
SOLUSI TEKNOLOGI

Dengan RAW – 10-20% CPU Load



CITRAWEB
SOLUSI TEKNOLOGI

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

CITRAWEB
SOLUSI TEKNOLOGI

FastPath

FastTrack

Raw

CITRAWEB
SOLUSI TEKNOLOGI

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 komplex lainnya
- Bisa digunakan untuk connection-less traffic (di Fast-Track tidak bisa)
- RAW juga bisa digunakan melakukan drop

CITRAWEB
SOLUSI TEKNOLOGI

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

CITRAWEB
SOLUSI TEKNOLOGI

Thank You!

Valens Riyadi

PT Citraweb Solusi Teknologi

www.mikrotik.id

@valensriyadi

@valensriyadi