



Advanced Mikrotik Training

Traffic Control

(MTCTCE)



Certified Mikrotik Training - Advanced Class (MTCTCE)
Organized by: Citraweb Nusa Infomedia
(Mikrotik Certified Training Partner)



Schedule - Module

	Sesi 1	Sesi 2	Sesi 3	Sesi 4
Hari 1	Basic Config		L2 Security	
Hari 2		Firewall		L7 Protocol
Hari 3		QOS		Test



Schedule

- Sessi 1 08.30 – 10.15
- Coffee Break 10.15 – 10.30
- Sessi 2 10.30 - 12.15
- Lunch 12.15 – 13.15
- Sessi 3 13.15 – 15.00
- Coffee Break 15.00 – 15.15
- Sessi 4 15.15 - 17.00



New Training Scheme 2009

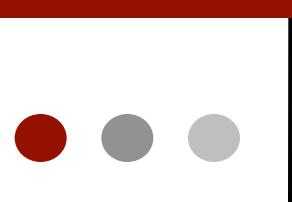
- **Basic / Essential Training**
 - MikroTik Certified Network Associate (MTCNA)
- **Advanced Training**
 - Certified Wireless Engineer (MTCWE)
 - Certified Routing Engineer (MTCRE)
 - Certified Traffic Control Engineer (MTCTCE)
 - Certified User Managing Engineer (MTCUME)
 - Certified Inter Networking Engineer (MTCINE)



Certification Test

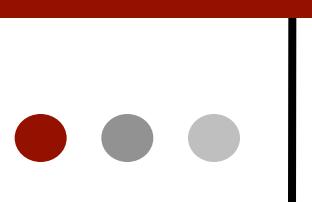
- Diadakan oleh **Mikrotik.com** secara online
- Dilakukan pada sesi terakhir
- Jumlah soal : **25** Waktu: **60 menit**
- Nilai minimal kelulusan : **60%**
- Yang mendapatkan nilai **50%** hingga **59%** berkesempatan mengambil “**second chance**”
- Yang lulus akan mendapatkan sertifikat yang diakui secara internasional





Trainers

- **Novan Chris**
 - MTCNA (2006), Certified Trainer (2008)
 - MTCWE (2008), MTCRE (2008)
 - MTCTCE (2011)
- **Pujo Dewobroto**
 - MTCNA (2009), MTCTCE (2009)
 - MTCWE (2010), MTCRE (2011)
 - Certified Trainer (2011)



Perkenalkan

- Perkenalkanlah :
 - Nama Anda
 - Tempat bekerja
 - Kota / domisili
 - Apa yang Anda kerjakan sehari-hari dan fitur-fitur apa yang ada di Mikrotik yang Anda gunakan



Thank You !



info@mikrotik.co.id

Dijinkan menggunakan sebagian atau seluruh materi pada modul ini, baik berupa ide, foto, tulisan, konfigurasi, diagram, selama untuk kepentingan pengajaran, dan memberikan kredit dan link ke

www.mikrotik.co.id



Basic Configuration, DHCP & Proxy

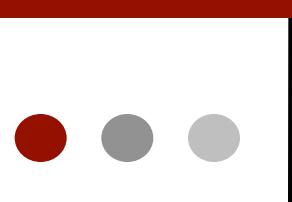


Certified Mikrotik Training - Advanced Class (MTCTCE)
Organized by: Citraweb Nusa Infomedia
(Mikrotik Certified Training Partner)



Objectives

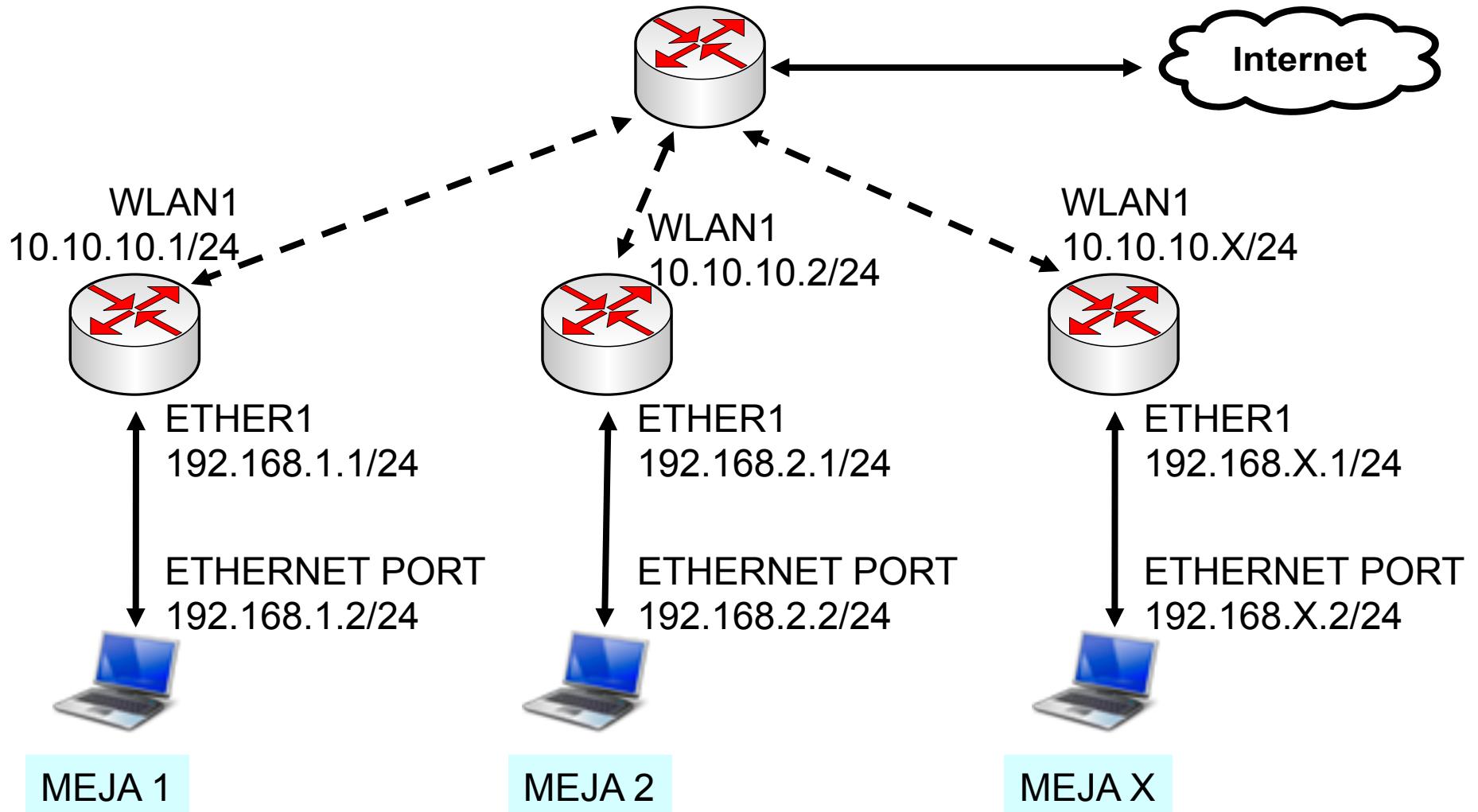
- Pada materi ini akan dibahas :
 - DNS Server
 - DHCP Server
 - DHCP Client
 - DHCP Relay
 - Proxy – Access Control

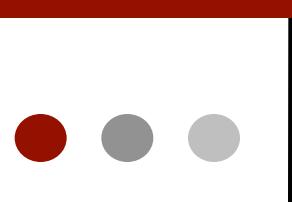


First do First !

- Ubahlah nama Router menjadi :
“XX-NAMA ANDA”.
- Aktifkan **neighbor interface** pada WLAN1.
- Buatlah username baru dan berilah password (group full).
- Proteksilah user Admin (tanpa password) hanya bisa diakses dari 10.10.10.28/30 (grup full).
- Buatlah user “demo” dengan grup read.

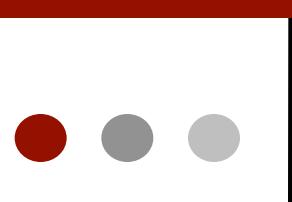
[LAB-1] Konfigurasi Dasar





IP Configuration

- Routerboard Setting
 - WAN IP : **10.10.10.x/24**
 - Gateway : **10.10.10.100**
 - LAN IP : **192.168.x.1/24**
 - DNS : **10.100.100.1**
 - Services: **Src-NAT** and **DNS Server**
- Laptop Setting
 - IP Address : **192.168.x.2/24**
 - Gateway : **192.168.x.1**
 - DNS : **192.168.x.1**

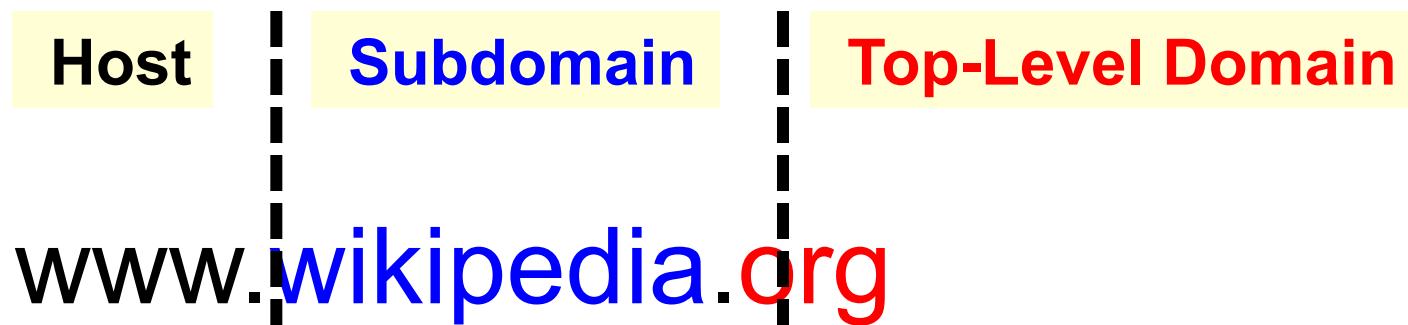


[LAB-2] NTP Client

- NTP Server: **id.pool.ntp.org**
- Wlan1 SSID : **training** (WPA=.....)
- Buatlah file backup! Dan copy file backup tersebut ke laptop

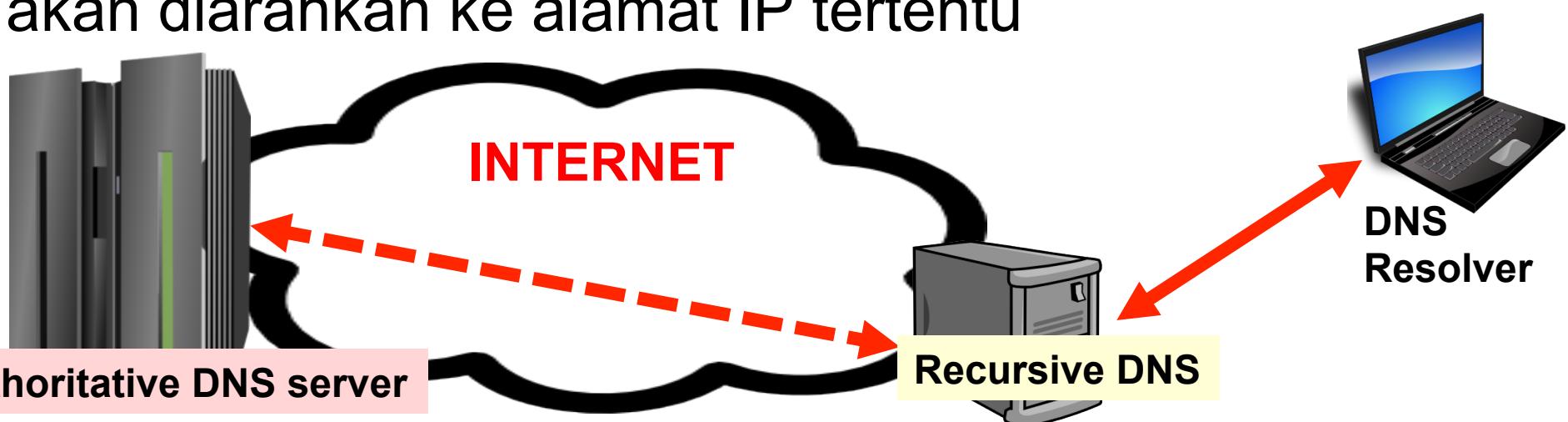
DNS – Domain Name System

- Adalah sebuah sistem yang menyimpan informasi Nama Host maupun Nama Domain dalam bentuk Data Base (distributed database) di dalam jaringan komputer.
- DNS menyediakan alamat IP untuk setiap nama host / server di dalam domain yang hal ini cukup penting untuk jaringan Internet,
- Bilamana perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk pengalaman dan penjaluran (routing).



DNS - 2

- Manusia pada umumnya lebih memilih untuk menggunakan nama host dan nama domain karena mudah diingat.
- Analogi yang umum digunakan untuk menjelaskan fungsi DNS adalah dianggap seperti buku telefon internet dimana saat pengguna mengetikkan nama website(domain) tertentu di internet maka pengguna akan diarahkan ke alamat IP tertentu

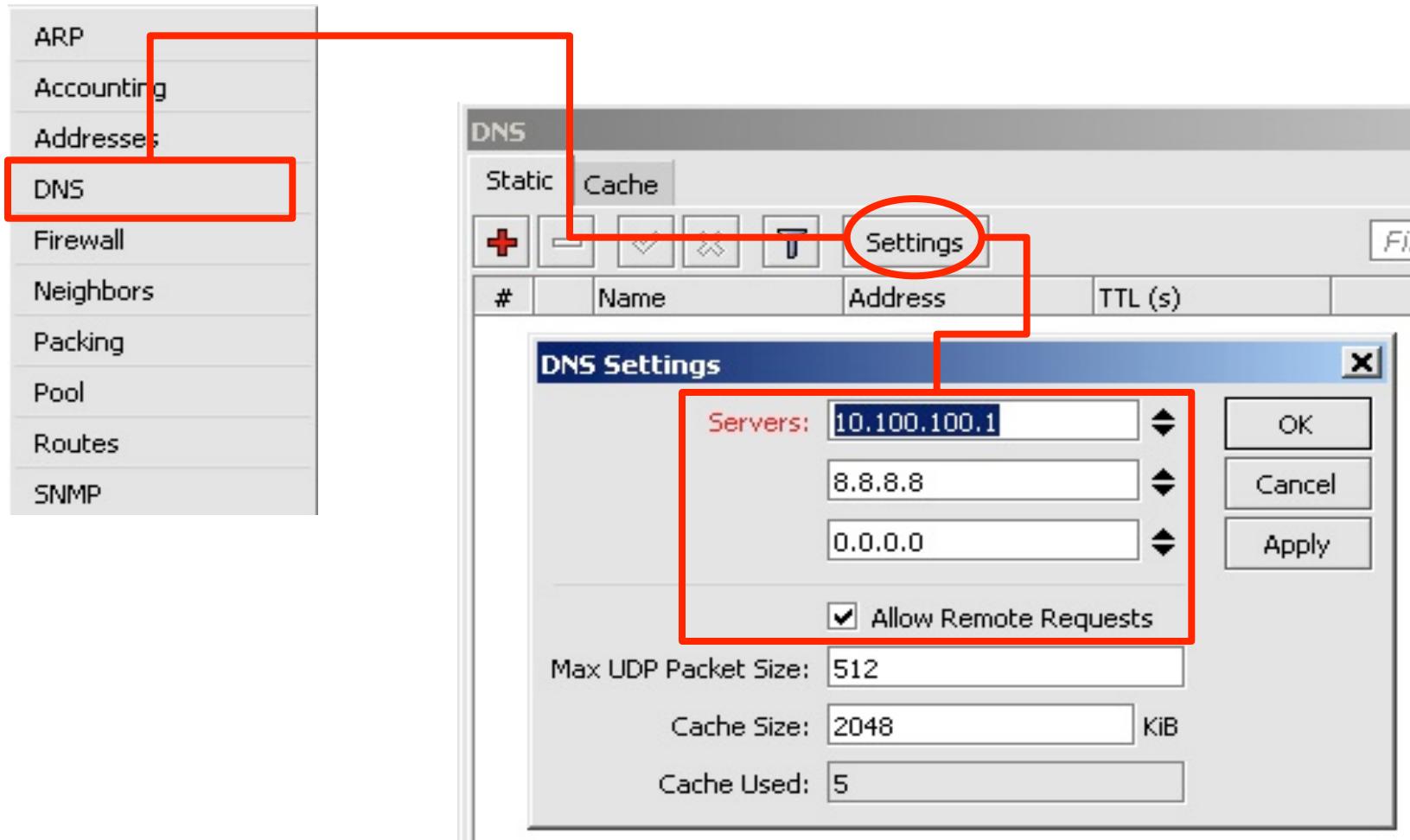




DNS Static & DNS Cache

- Fungsi DNS Static digunakan router pada aplikasi web-proxy dan juga di hotspot.
- Fungsi DNS Cache akan aktif bila konfigurasi “Allow Remote Requests” diaktifkan.
- DNS Cache dapat meminimalkan waktu request DNS dari client.

Konfigurasi Dasar DNS

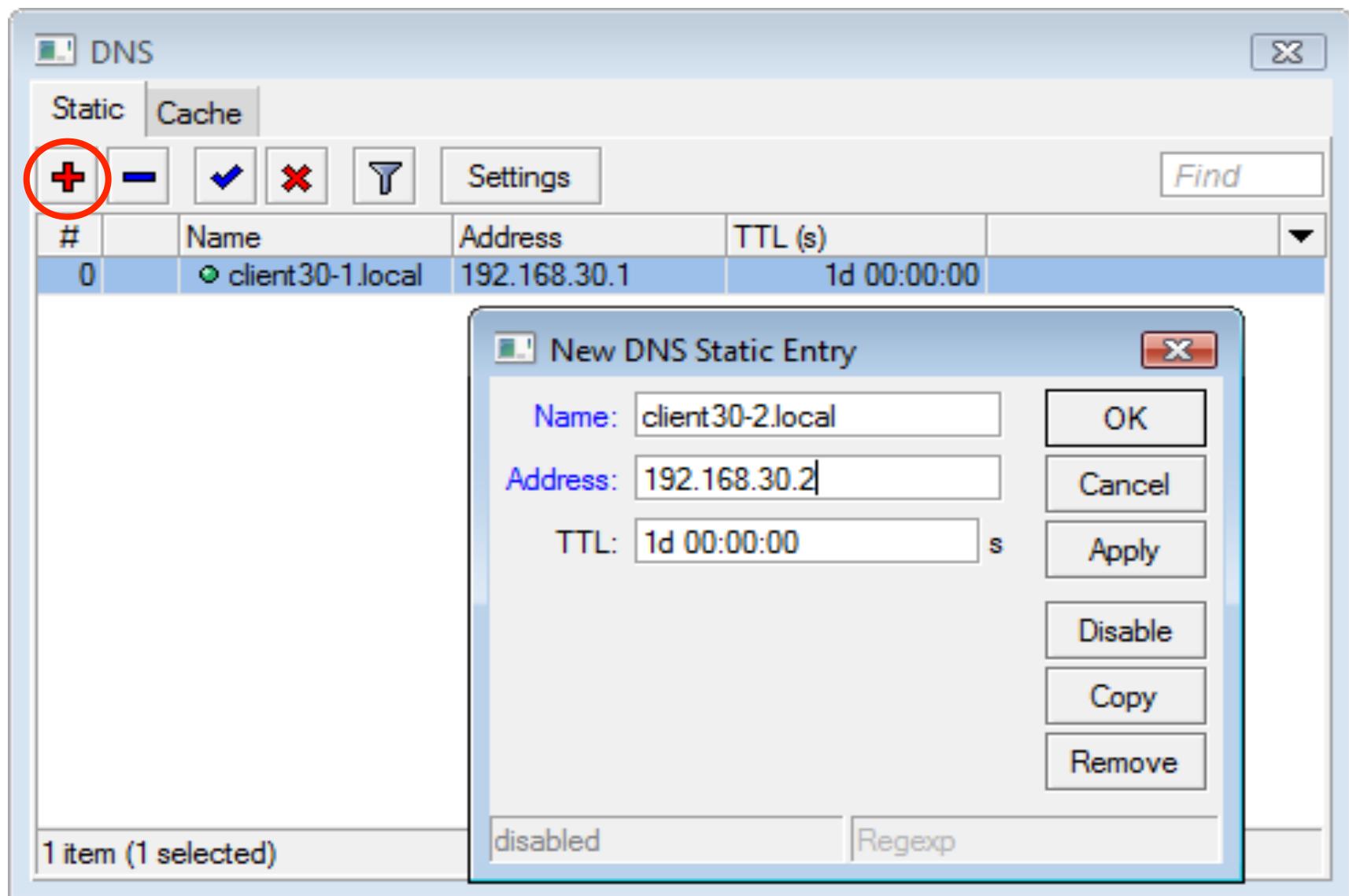




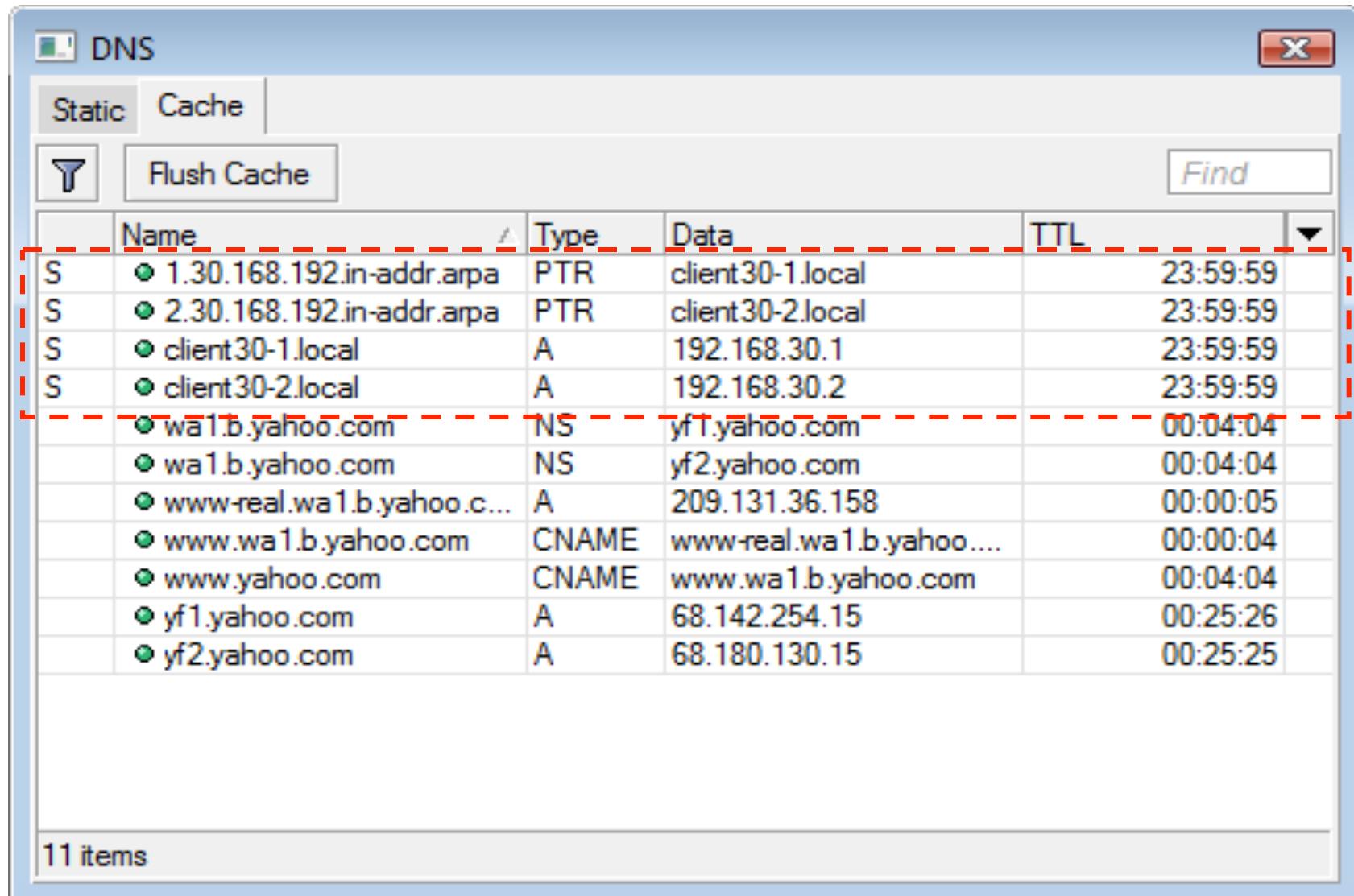
DNS Static & DNS Cache

- DNS Cache juga dapat berfungsi sebagai DNS Server sederhana.
- Untuk setiap setting static DNS, router akan menambahkan parameter “A” dan “PTR” secara otomatis.
 - “A” – Memetakan Alamat Domain ke Alamat IP
 - “PTR” – Untuk memetakan Reverse DNS
- Static DNS akan meng-override dynamic entry yang ada di DNS cache.
- Untuk mempercepat proses trace route di OS Windows, kita bisa menambahkan static DNS untuk IP lokal kita.

[LAB-3] Static DNS



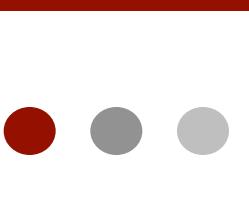
Cache Lists



The screenshot shows the 'Cache' tab of the Winbox DNS interface. The table displays 11 items in the cache, with a red dashed box highlighting the first four entries. The columns are: Name, Type, Data, and TTL.

	Name	Type	Data	TTL
S	1.30.168.192.in-addr.arpa	PTR	client30-1.local	23:59:59
S	2.30.168.192.in-addr.arpa	PTR	client30-2.local	23:59:59
S	client30-1.local	A	192.168.30.1	23:59:59
S	client30-2.local	A	192.168.30.2	23:59:59
<hr/>				
	wa1.b.yahoo.com	NS	yf1.yahoo.com	00:04:04
	wa1.b.yahoo.com	NS	yf2.yahoo.com	00:04:04
	www-real.wa1.b.yahoo.c...	A	209.131.36.158	00:00:05
	www.wa1.b.yahoo.com	CNAME	www-real.wa1.b.yahoo....	00:00:04
	www.yahoo.com	CNAME	www.wa1.b.yahoo.com	00:04:04
	yf1.yahoo.com	A	68.142.254.15	00:25:26
	yf2.yahoo.com	A	68.180.130.15	00:25:25

11 items



DHCP

- Dynamic Host Configuration Protocol digunakan untuk secara dinamik mendistribusikan konfigurasi jaringan, seperti:
 - IP Address dan netmask
 - IP Address default gateway
 - Konfigurasi DNS dan NTP Server
 - Dan masih banyak lagi custom option (tergantung apakah DHCP client bisa support DHCP option tersebut)
- DHCP dianggap tidak terlalu aman dan hanya digunakan pada jaringan yang dipercaya.



Skema Komunikasi DHCP

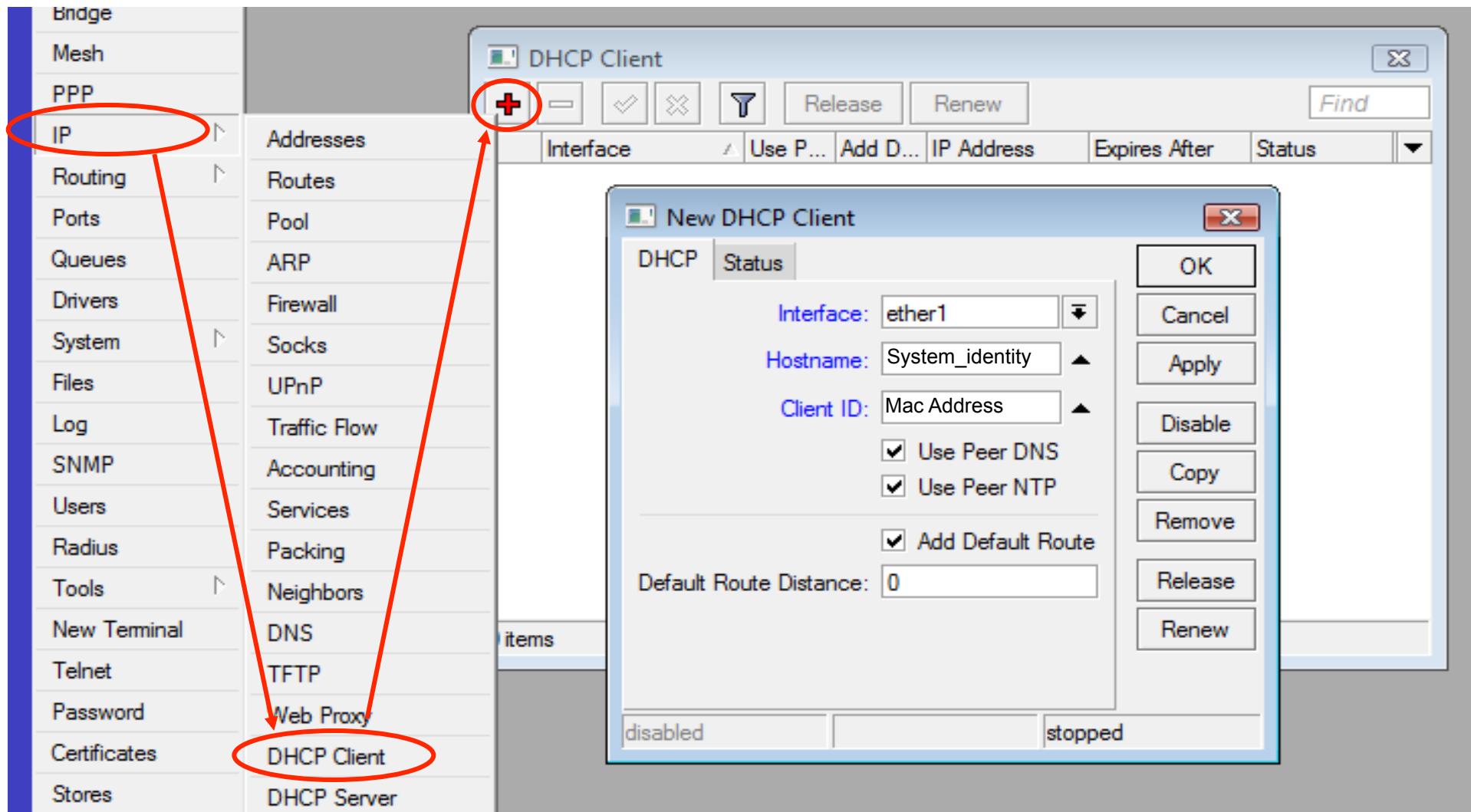
- DHCP Discovery
 - **src-mac=<client>, dst-mac=<broadcast>, protocol=udp, src-ip=0.0.0.0:68, dst-ip=255.255.255.255:67**
- DHCP Offer
 - **src-mac=<DHCP-server>, dst-mac=<broadcast>, protocol=udp, src-ip=<DHCP-Server>:67, dst-ip=255.255.255.255:67**
- DHCP Request
 - **src-mac=<client>, dst-mac=<broadcast>, protocol=udp, src-ip=0.0.0.0:68, dst-ip=255.255.255.255:67**
- DHCP Acknowledgement
 - **src-mac=<DHCP-server>, dst-mac=<broadcast>, protocol=udp, src-ip=<DHCP-Server>:67, dst-ip=255.255.255.255:67**



Identifikasi DHCP Client

- DHCP Server dapat membedakan client berdasarkan proses identifikasi.
- Identifikasi dilakukan berdasarkan:
 - “caller-id” option (dhcp-client-identifier pada RFC2132)
 - Mac-Address, apabila “caller-id” tidak ada
- “hostname” memungkinkan client DHCP yang menggunakan RouterOS mengirimkan tambahan informasi identifikasi ke server, secara bawaan menggunakan “system identity”.

DHCP Client





DHCP Server

- Hanya boleh ada satu DHCP server per kombinasi interface/relay pada router.
- Untuk membuat DHCP Server, kita harus memiliki :
 - IP Address pada interface fisik DHCP
 - Address pool untuk client
 - Informasi jaringan lainnya
- Ketiga informasi di atas harus sesuai satu sama lain.
- “Lease on disk” adalah opsi untuk menuliskan data Lease DHCP ke harddisk.



DHCP Networks & Option

- Pada menu DHCP Networks, kita dapat melakukan konfigurasi DHCP Options tertentu untuk network tertentu
- Beberapa option sudah terintegrasi dengan RouterOS, dan Option lainnya dapat dilakukan custom dalam format raw
 - <http://www.iana.org/assignments/bootp-dhcp-parameters>
- DHCP Server dapat memberikan option apapun
- DHCP Client hanya dapat menerima option yang dikenali



DHCP Options (1)

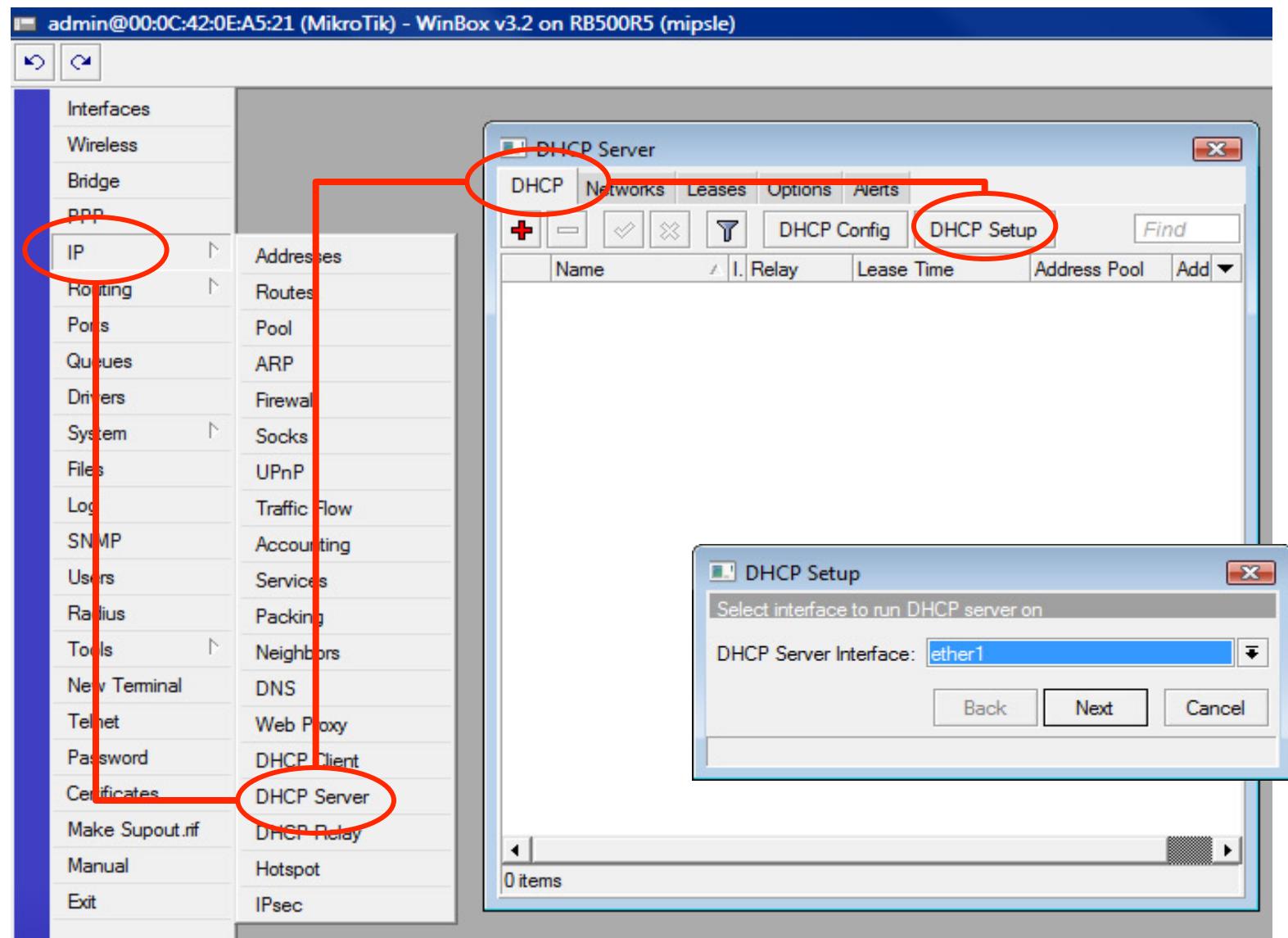
- DHCP Options yang bisa dilakukan:
 - Subnet-mask (option 1) – netmask
 - Router (option 3) – gateway
 - Domain-Server (option 6) – dns-server
 - NTP-Servers (option 42) – ntp-server
 - NETBOIS-Name-Server (option 44) – wins-server
- Custom DHCP options (contoh) :
 - Classless Static Route (option 121) –
“0x100A270A260101” = “network=10.39.0.0/16
gateway=10.38.1.1”



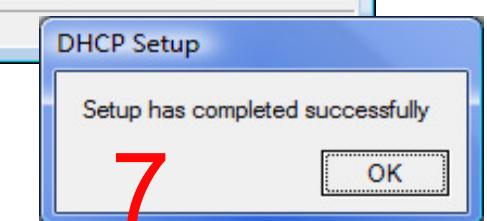
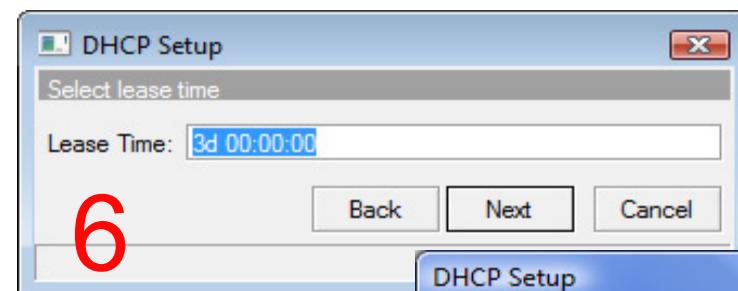
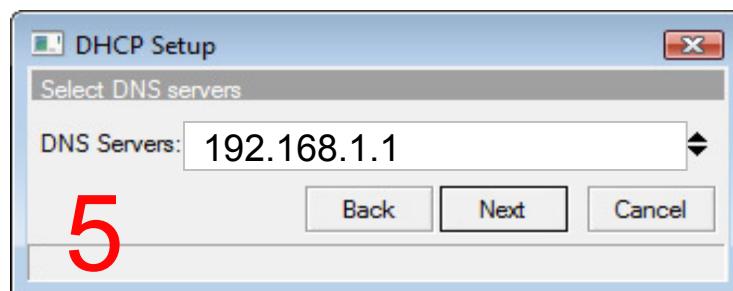
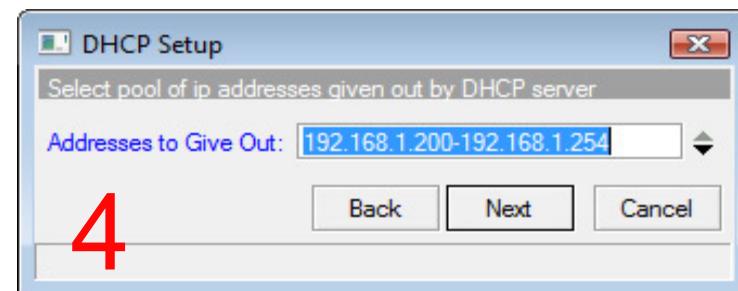
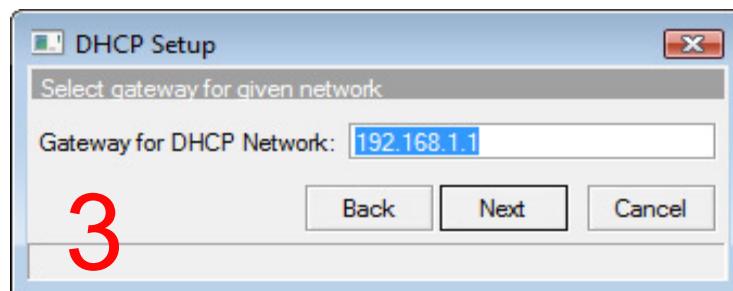
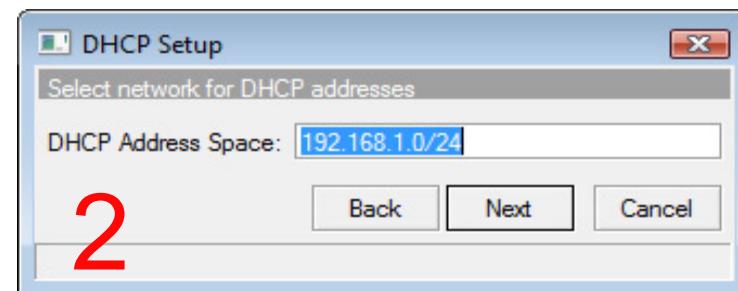
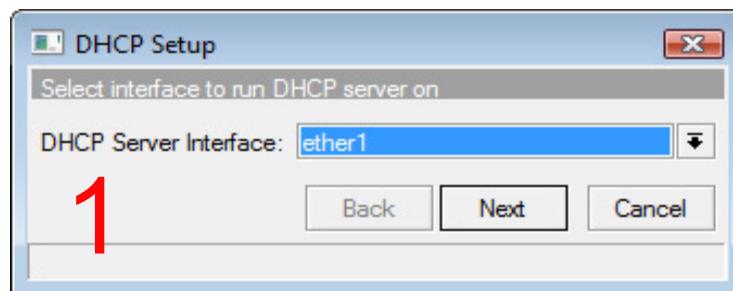
DHCP Options (2)

- Raw Format :
 - 0x | 10 | 0A27 | 0A260101 |
 - 0x – **Hex Number**
 - 10 – **Subnet/Prefix = 16**
 - 0A27 – **Network = 10.39.0.0**
 - 0A260101 – **Gateway = 10.38.1.1**

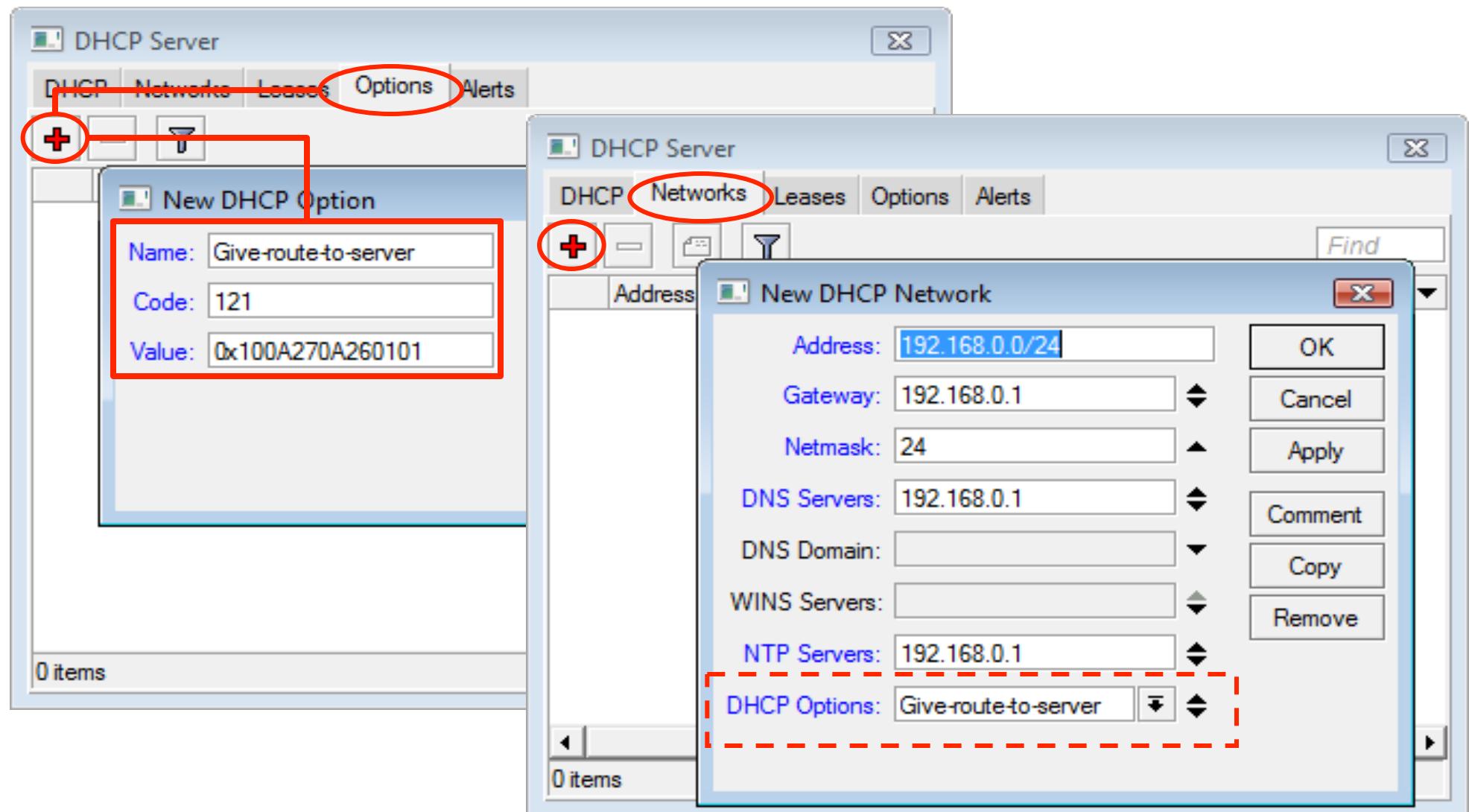
[LAB-4] DHCP Server



DHCP Server (2)



[LAB-5] Custom DHCP Option

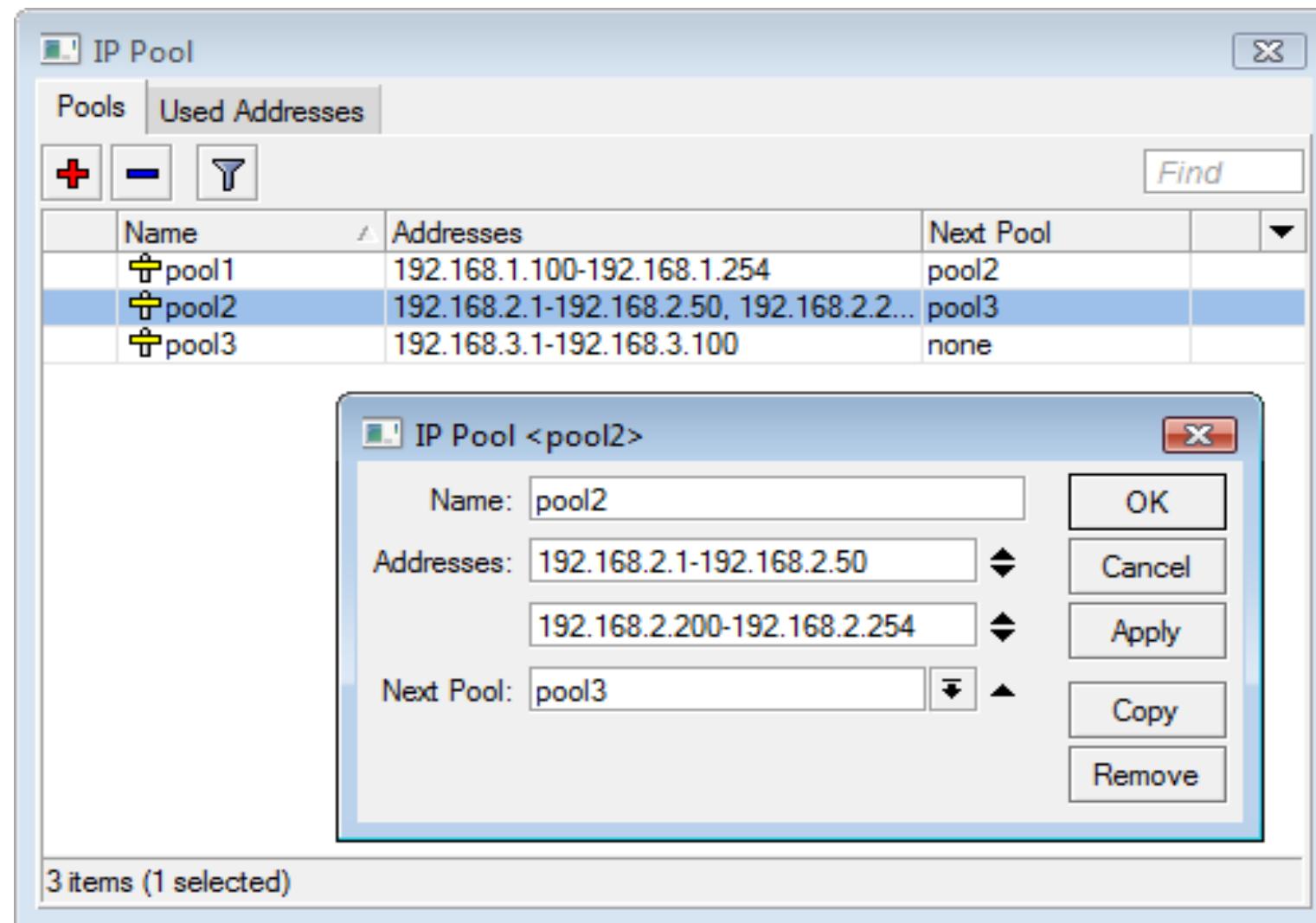




IP Address Pool

- IP address pool digunakan untuk menentukan rentang IP Address yang akan didistribusikan secara dinamik (DHCP, PPP, Hotspot)
- IP address harus selain yang digunakan untuk keperluan lain (misalnya: server)
- Dimungkinkan untuk :
 - Membuat beberapa rentang untuk satu pool
 - Menentukan pool berikut dengan “next pool”

IP Address Pools



Distribusi Address Pool

.1	.2	.3	.4	.5	.6	.7	.8	.9	.10	.11	.12	.13	.14
----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----

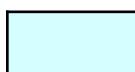
.1	.2	.3	.4	.5	.6	.7	.8	.9	.10	.11	.12	.13	.14
----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----

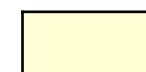
.1	.2	.3	.4	.5	.6	.7	.8	.9	.10	.11	.12	.13	.14
----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----

.1	.2	.3	.4	.5	.6	.7	.8	.9	.10	.11	.12	.13	.14
----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----

.1	.2	.3	.4	.5	.6	.7	.8	.9	.10	.11	.12	.13	.14
----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----

.1	.2	.3	.4	.5	.6	.7	.8	.9	.10	.11	.12	.13	.14
----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----

 address berikutnya

 reserved, tapi tidak digunakan

 tidak digunakan

 address digunakan



Distribusi Address Pool

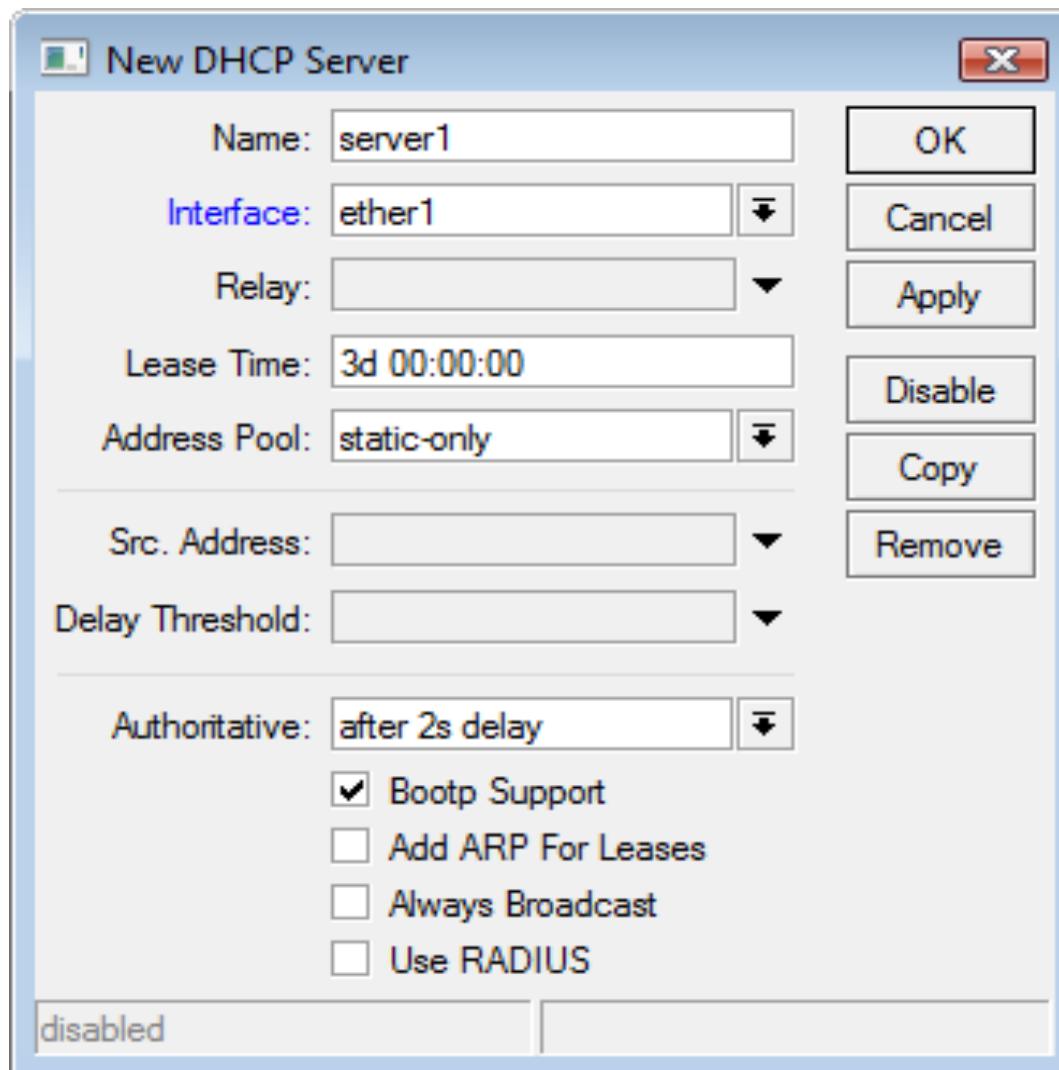
- Secara default Pembagian IP address oleh DHCP-server Mikrotik akan dimulai dari angka ip yang paling besar dari pool yang diberikan.
- Jika ternyata ip yang didapatkan adalah ip yang terkecil maka biasanya ada DHCP option di client yang aktif yang meminta ip terkecil.



DHCP Server Setting

- **Src-address** – menentukan IP Address DHCP server apabila terdapat lebih dari 1 IP Address pada interface DHCP server
- **Delay Threshold** – memberikan prioritas DHCP server yang satu dari yang lainnya (makin besar delay, prioritas makin rendah)
- **Add ARP for Leases** – memperbolehkan menambahkan data entri ARP dari lease DHCP jika interface ARP=reply-only
- **Always Broadcast** – mengijinkan komunikasi dengan client yang tidak standart, misalnya pseudo-bridges

DHCP Server Setting

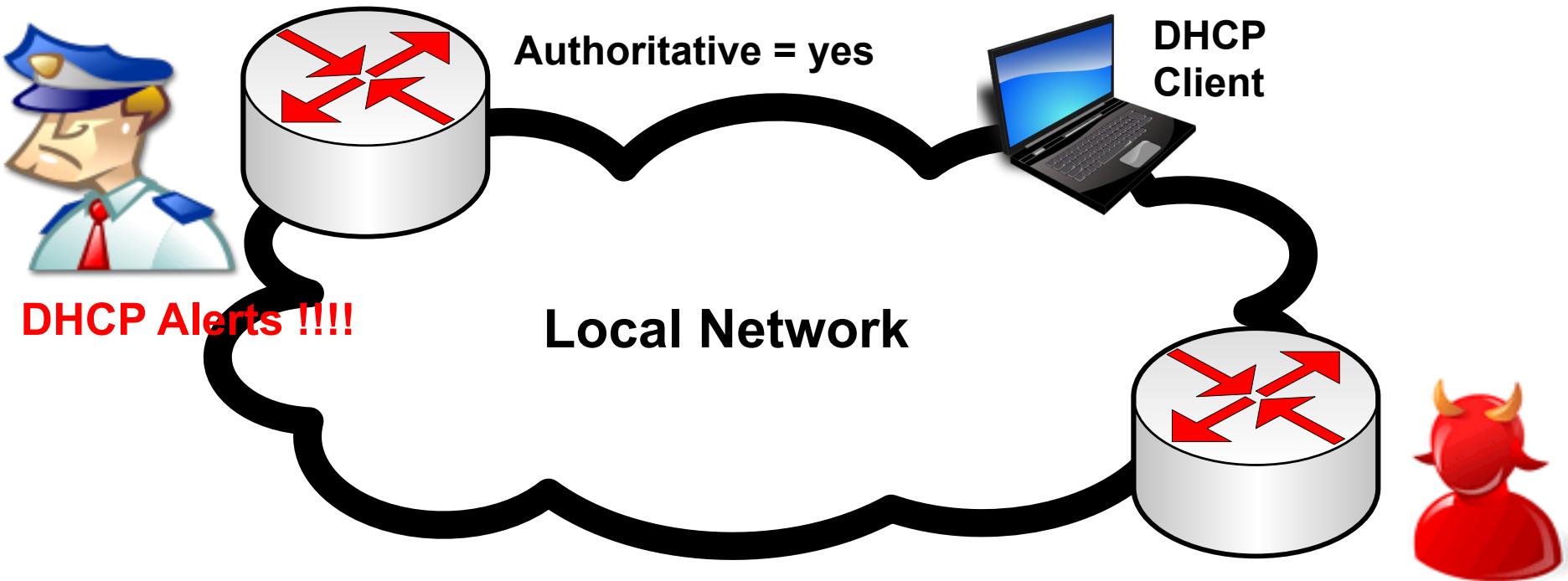




DHCP-Server Alerts!!!

- **DHCP-Alerts** – memungkinkan DHCP server untuk mendeteksi adanya DHCP Server Tandingan (Rogue) yang ada di jaringan yang sama.
- **Valid-Server** – Mendaftarkan mac-address dari DHCP server yang valid.
- **On-Alert** – memungkinkan untuk menjalankan script tertentu jika terjadi adanya DHCP-Server tandingan.

DHCP – Alerts !



- Untuk mendeteksi DHCP server lain yang mengganggu maka aktifkan “**DHCP Alerts**”

DHCP – Alerts !

DHCP Alert <ether1>

Interface: ether1

Valid Servers: 00:0C:42:20:94:E0

Alert Timeout: 01:00:00

Unknown Servers: 00:0C:42:D3:95:17
00:0C:42:E9:BB:C6
00:0C:42:E9:BB:D5

Log

Feb/14/2012 14:18:23	dhcp critical error	dhcp alert on ether1: di
Feb/14/2012 14:18:23	dhcp critical error	dhcp alert on ether1: di
Feb/14/2012 14:18:23	script info	ono dhcp kobish
Feb/14/2012 14:18:23	script info	ono dhcp kobish
Feb/14/2012 14:22:54	dhcp info	DHCP server: unknown
Feb/14/2012 14:22:54	dhcp critical error	dhcp alert on ether1: di
Feb/14/2012 14:22:54	dhcp critical error	dhcp alert on ether1: di
Feb/14/2012 14:22:54	script info	ono dhcp kobish
Feb/14/2012 14:22:54	script info	ono dhcp kobish
Feb/14/2012 14:22:54	dhcp critical error	dhcp alert on ether1: discovered unknown dhcp server, mac 6C:F0:49:CE:F8:6E, ip 192.168.130.15
Feb/14/2012 14:22:54	script info	ono dhcp kobish

On Alert:

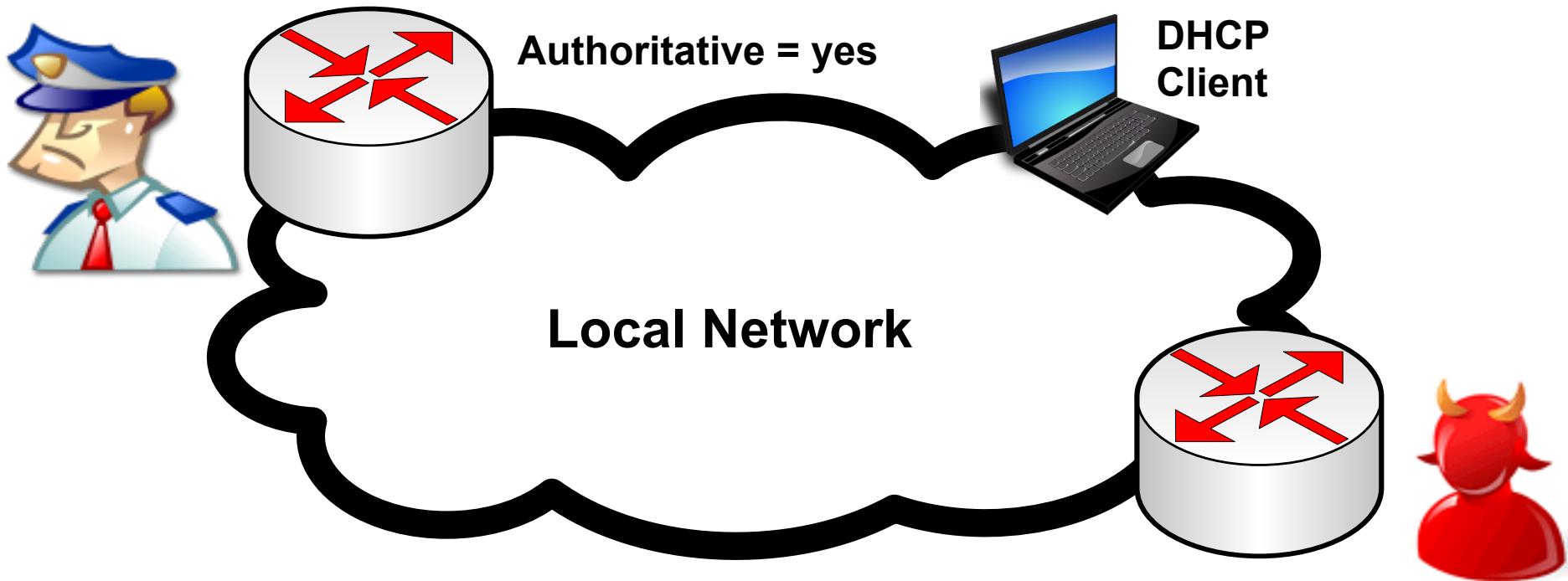
```
:log info message="ono dhcp kobish"
```



Authoritative DHCP Server

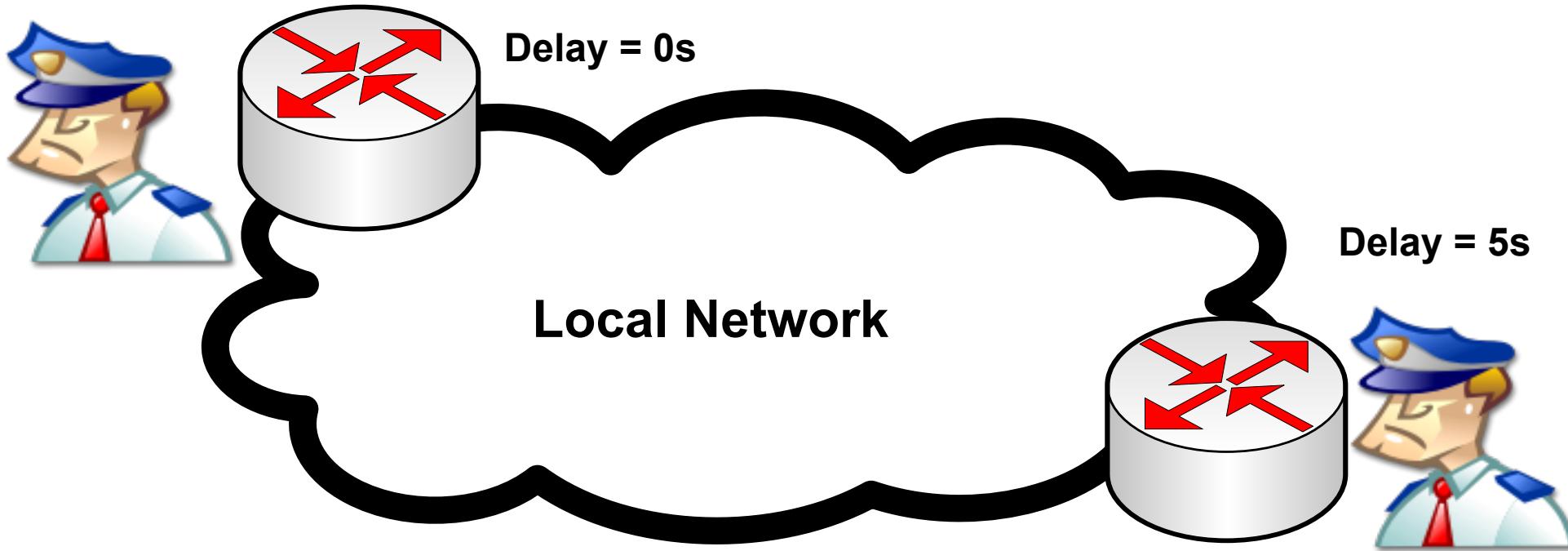
- **Authoritative** – memungkinkan DHCP server menanggapi broadcast client yang tidak dikenali dan meminta client untuk me-restart DHCP lease (client akan mengirimkan sequence broadcast hanya apabila gagal melakukan pembaruan lease)
- Digunakan untuk:
 - Menanggulangi apabila ada DHCP server “tandingan” di dalam network
 - Melakukan perubahan konfigurasi jaringan DHCP dengan lebih cepat

DHCP - Authoritative



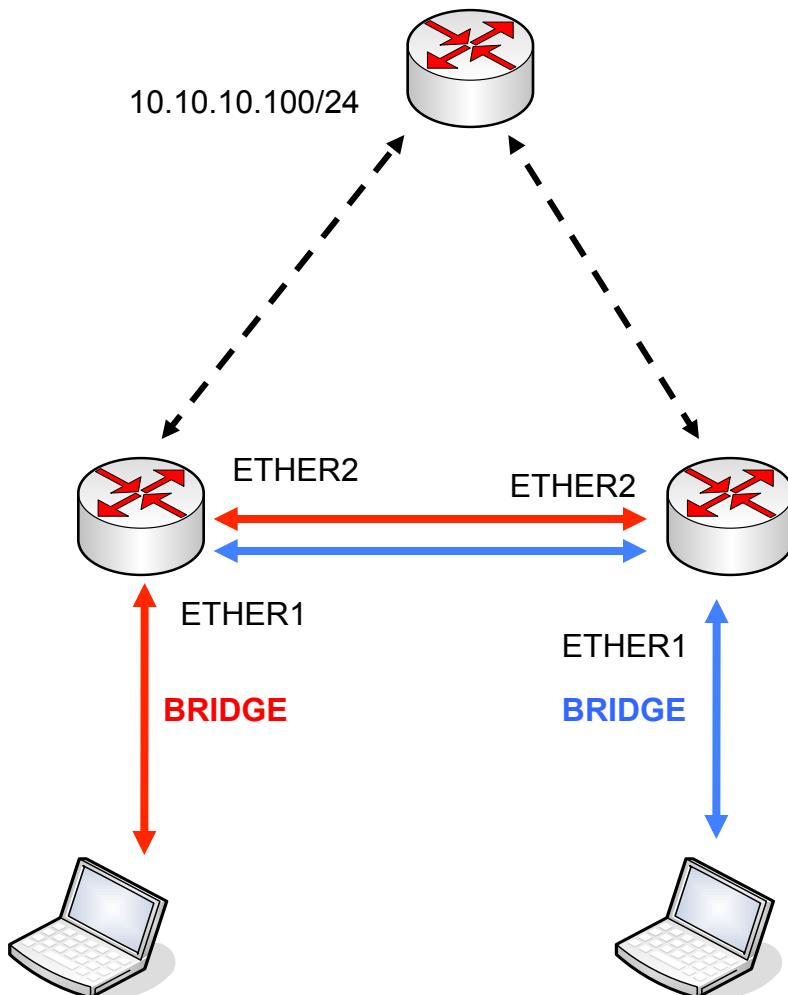
- Untuk menganggulangi adanya DHCP server lain yang mengganggu maka aktifkan "**Authoritative = yes**"

DHCP – Delay Threshold



- Delay Threshold digunakan untuk backup jika DHCP server utama mengalami gangguan atau tidak berfungsi.

[LAB-6] – DHCP Delay



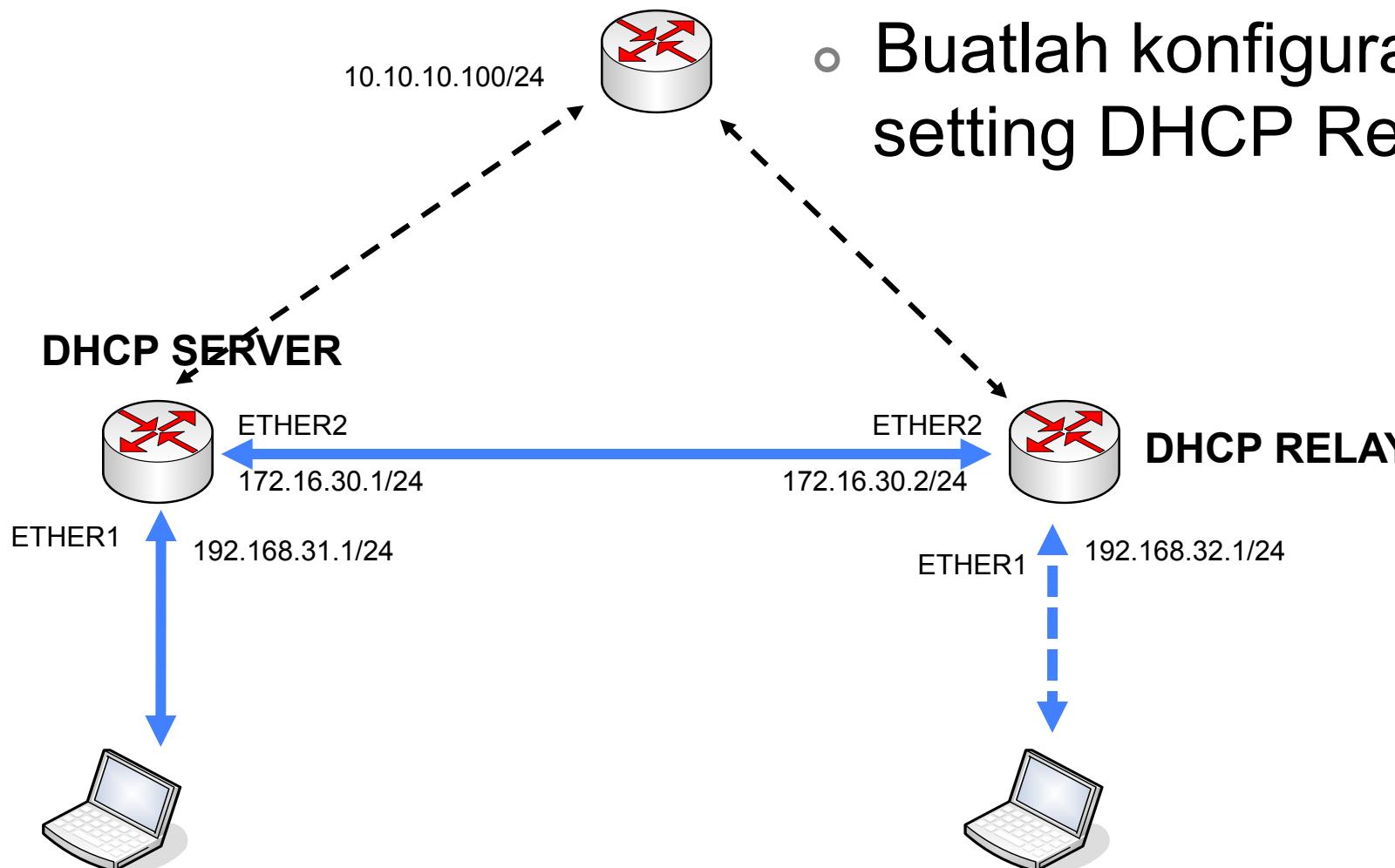
- Hubungkan ether2 Anda dengan router di sebelah
- Buat bridge, masukkan ether1 dan ether2 sebagai bridge port
- Buatlah DHCP server pada interface bridge
- Mainkan delay threshold dan lihatlah apa yang terjadi



DHCP Relay

- DHCP Relay bekerja seperti halnya Web-Proxy, dapat menerima DHCP discovery dan request, dan meneruskannya ke DHCP server
- Hanya bisa ada 1 DHCP relay antara DHCP server dan DHCP client
- Komunikasi DHCP server ke DHCP relay tidak membutuhkan IP Address
- Konfigurasi “local address” pada DHCP relay harus sama dengan “relay address” pada DHCP server.

[LAB-7] – DHCP Relay



- Buatlah konfigurasi setting DHCP Relay

Setting DHCP Server

The image shows the Winbox interface for configuring a DHCP server and its associated network and IP pool settings.

DHCP Server <dhcp1>:

- Name: dhcp1
- Interface: ether2
- Relay: 192.168.32.1
- Lease Time: 3d 00:00:00
- Address Pool: dhcp_pool2
- Src. Address: (empty)
- Delay Threshold: (empty)
- Authoritative: after 2s delay
- Bootp Support
- Add ARP For Leases
- Always Broadcast
- Use RADIUS

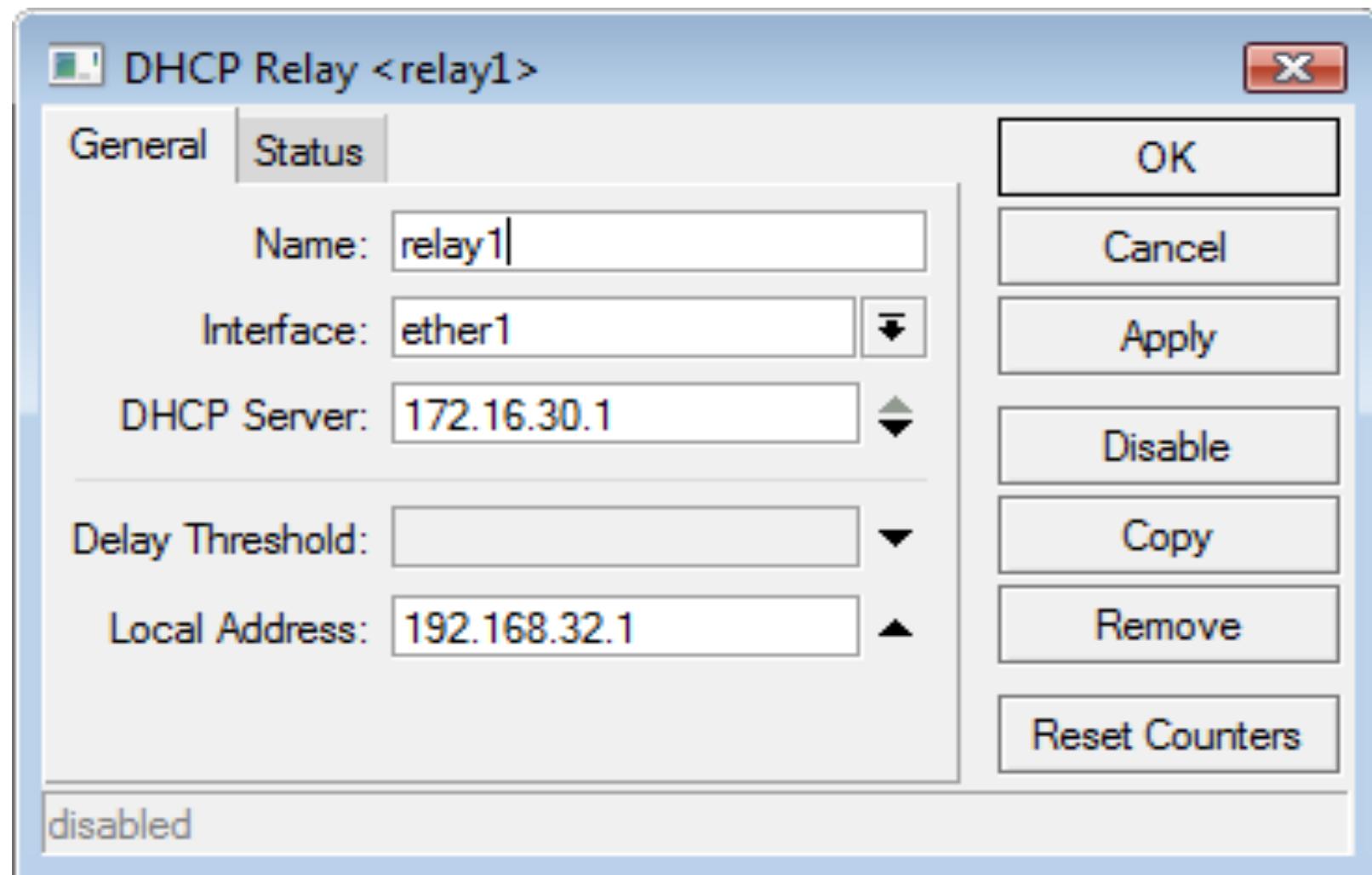
DHCP Network <192.168.32.0/24>:

- Address: 192.168.32.0/24
- Gateway: 192.168.32.1
- Netmask: (empty)
- DNS Servers: 10.100.100.1
- DNS Domain: (empty)
- WINS Servers: (empty)
- NTP Servers: (empty)
- DHCP Options: (empty)

IP Pool <dhcp_pool2>:

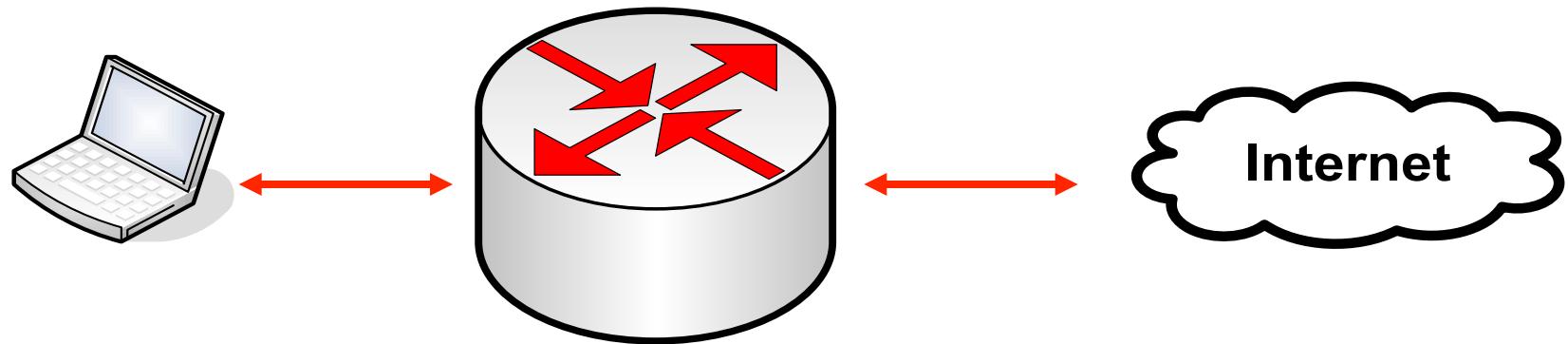
- Name: dhcp_pool2
- Addresses: 192.168.32.2-192.168.32.254
- Next Pool: none

Setting pada DHCP Relay



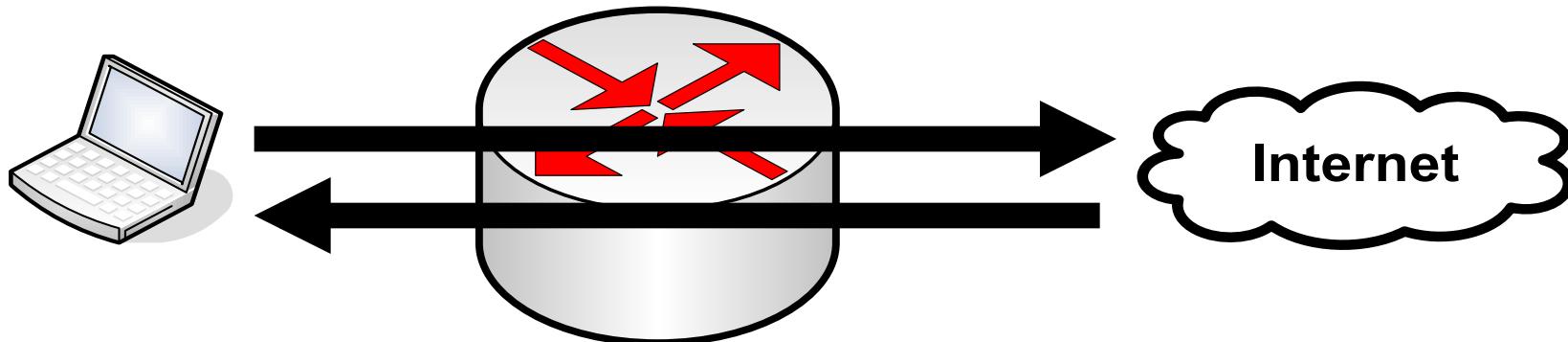
Proxy

- Pada semua level routeros, baik yang diinstall pada PC maupun yang diinstall pada routerboard, kita bisa mengaktifkan fitur proxy

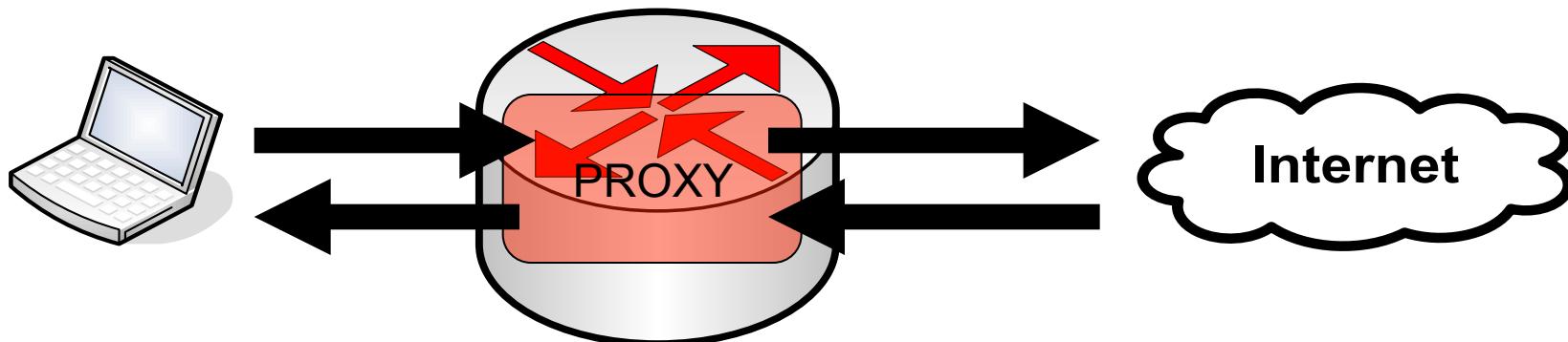


Konsep Proxy

- Koneksi tanpa proxy



- Koneksi dengan proxy





Fitur Proxy di RouterOS

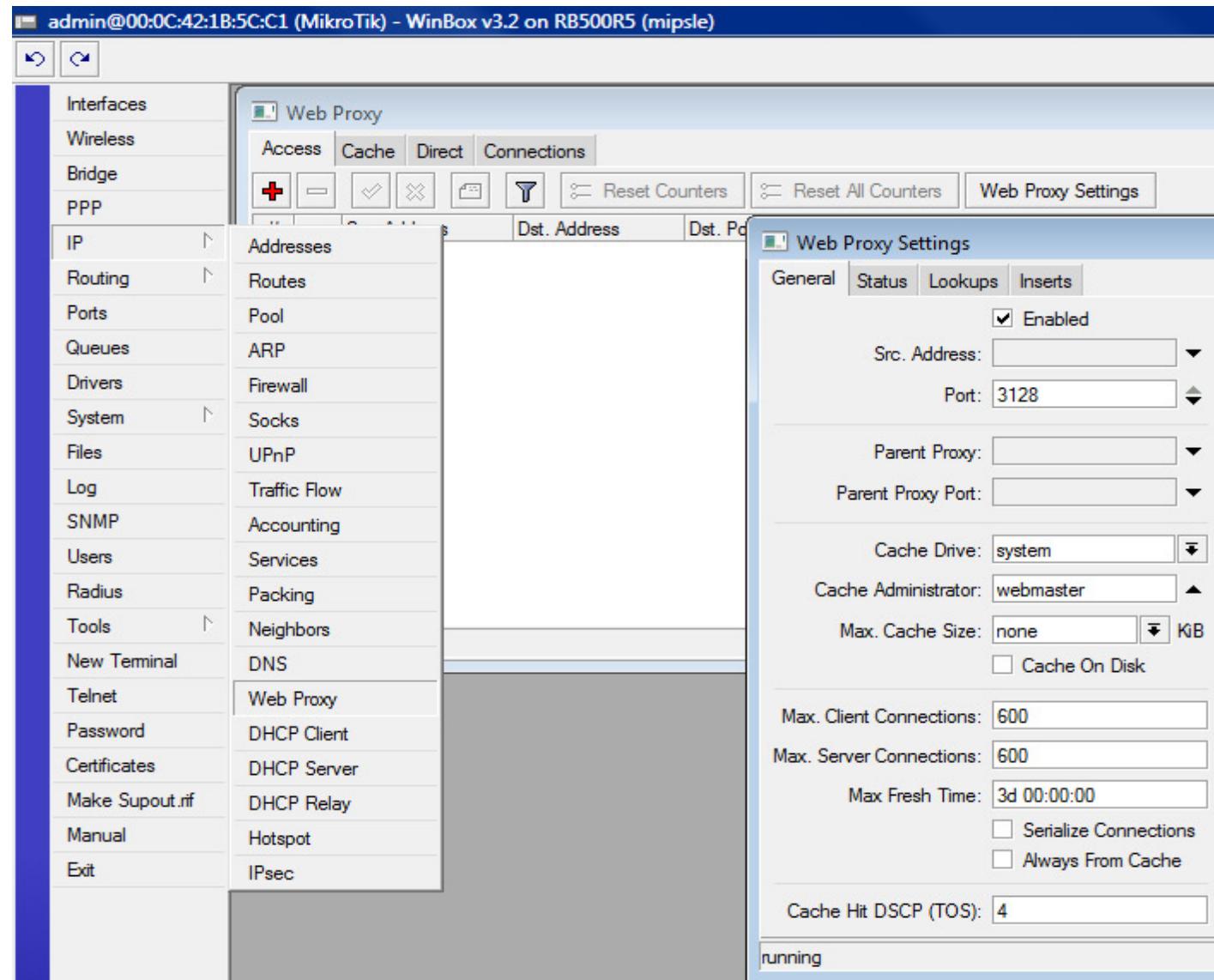
- **Regular HTTP proxy**
- **Transparent proxy**
 - Dapat berfungsi juga sebagai transparan dan sekaligus normal pada saat yang bersamaan
- **Access list**
 - Berdasarkan source, destination, URL dan requested method
- **Cache Access list**
 - Menentukan objek mana yang disimpan pada cache
- **Direct Access List**
 - Mengatur koneksi mana yang diakses secara langsung dan yang melalui proxy server lainnya
- **Logging facility**



Setup Proxy

- Aktifkanlah service web-proxy pada router Anda.
- Konfigurasi browser Anda untuk menggunakan proxy internal Mikrotik.
- Kemudian test koneksi untuk memastikan proxy sudah bisa menerima request.

Mengaktifkan Proxy



Statistik Web Proxy

Web Proxy Settings

General Status Lookups Inserts

Uptime: 21d 01:09:13

Requests: 2057512

Hits: 698936

Cache Used: 21 288 493 KiB

RAM Cache Used: 0 KiB

Total RAM Used: 6 022 KiB

Received From Servers: 46 487 277 KiB

Sent To Clients: 50 634 819 KiB

Hits Sent To Clients: 9 579 179 KiB

Total Disk Size: 28 855 996 KiB

Free Disk Space: 6 150 540 KiB

Web Proxy Settings

General Status Lookups Inserts

Successes: 1 193 715

Not Found: 584 591

Non Cachable: 98 718

Denied: 590 598

Expired: 65 681

No Expiration Info: 1 090

OK Cancel Apply Clear Cache Format Drive... Check Drive...

Web Proxy Settings

General Status Lookups Inserts

Successes: 390 192

Denied: 565 257

Too Large: 0

No Memory: 0

Errors: 23

OK Cancel Apply Clear Cache Format Drive... Check Drive...



Proxy Setting: Access

- Menentukan mana yang boleh melakukan akses dan mana yang tidak, berdasarkan :
 - Layer 3 information
 - URL / Host
 - HTTP Method
- Untuk yang di-denied, kita dapat mengalihkan (redirect) akses ke URL tertentu.

Web Proxy

Access Cache Direct Connections

Web Proxy Rule <192.168.0.23>

#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Redirect To
0	192.168.0.23			www.youtube...			deny	

Src. Address:

Dst. Address:

Dst. Port:

Local Port:

Dst. Host:

Path:

Method:

Action:

Redirect To:

Hits:

disabled

1 item (1 selected)

URL Filtering

`http://www.domain.com/path1/path2/file1.jpg`

Destination host

Destination path

- Special Characters

- * = karakter apapun (bisa banyak)
- ? = satu karakter
 - www.do?ai?.com
 - www.domain.*
 - *domain*



Regular Expressions

- Tuliskan tanda ":" pada awal parameter untuk mengaktifkan mode regex
 - ^ = tidak ada simbol yang diijinkan sebelum pattern
 - \$ = tidak ada simbol yang diijinkan sesudah pattern
 - [...] = karakter pembanding
 - \ = (diikuti karakter dengan fungsi khusus) meniadakan fungsi khusus
- <http://www.regular-expressions.info/reference.html>



[LAB] Proxy RegEx

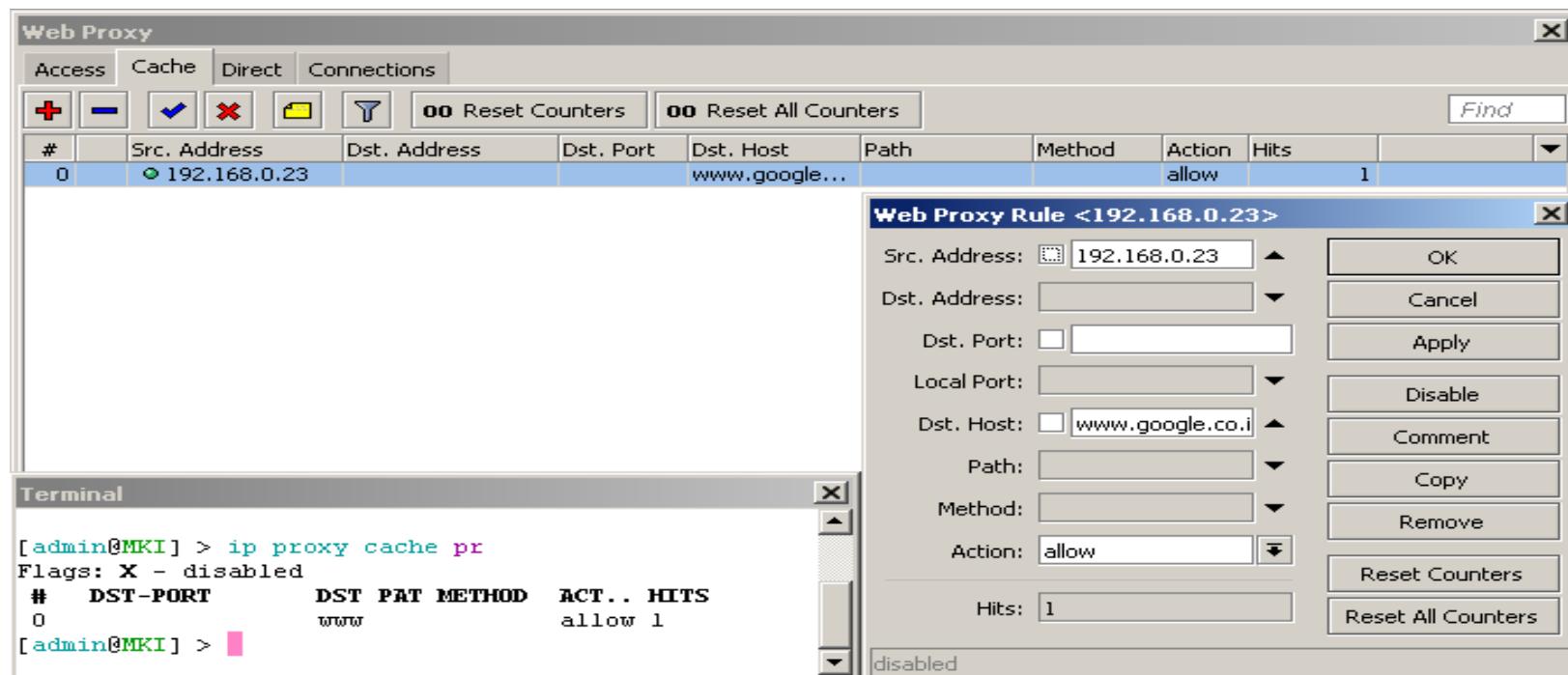
- Untuk melakukan blok terhadap situs torrent
contoh :
 - Dst-Host=“:(torrent|limewire|thepiratebay|torrentz|isohunt)+.*”**

Complete RegEx :

```
: (torrentz|torrent|thepiratebay|isohunt|entertane|  
demonoid|btjunkie|mininova|flixflux|torrentz|vertor|  
h33t|btscene|bitunity|bittoxic|thunderbytes|entertane|  
zoozle|vcdq|bitnova|bitsoup|meganova|fulldl|btbot|  
flixflux|seedpeer|fenopy|gpirate|commonbits)+.*
```

Cache

- Pengaturan penyimpanan objek ke dalam cache





Direct Access list

- Mengatur request dari client untuk diproses oleh parent proxy server
- Berfungsi jika **Parent Proxy** telah didefinisikan.
- Direct-list dst-host=* **action=deny**
 - Akses user akan dikontrol oleh proxy local dibantu parent proxy.
- Direct-list dst-host=* **action=allow**
 - Akses user akan dikontrol sepenuhnya oleh proxy local.



Layer 2 - Security



Certified Mikrotik Training - Advanced Class (MTCTCE)
Organized by: Citraweb Nusa Infomedia
(Mikrotik Certified Training Partner)



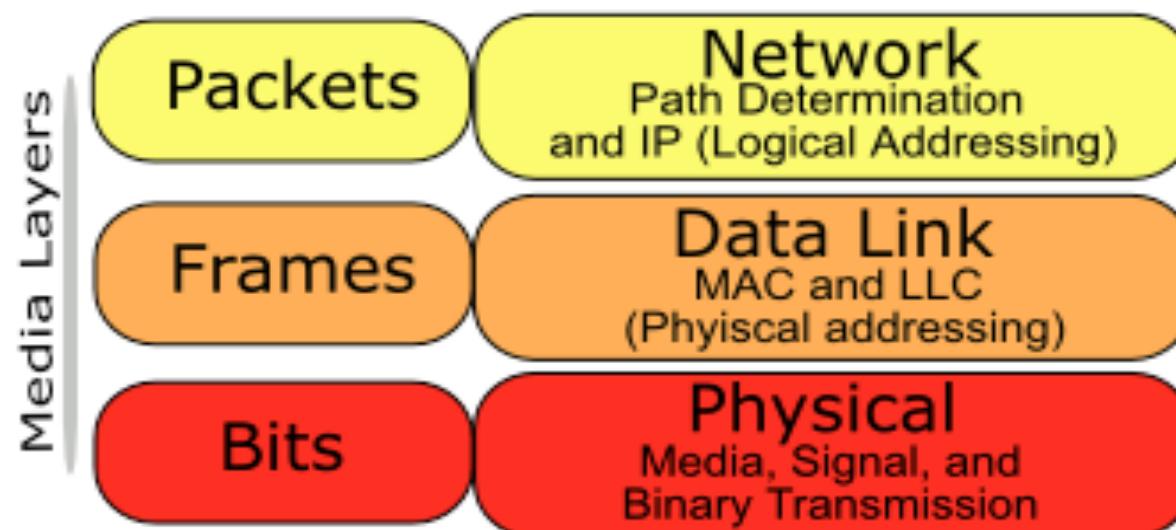
Outline

- LAN dan Layer 2 Network
- Keamanan di jaringan LAN
- Permasalahan yang sering terjadi di Jaringan Layer 2
- Implementasi security menggunakan Mikrotik

- LAN adalah sebuah jaringan yang paling sederhana, yaitu jaringan di area lokal yang didefinisikan dan dinaungi oleh alamat network dan alamat broadcast yang sama.
- Untuk menghubungkan node (device) satu dengan yang lain pada sebuah jaringan LAN maka perlu adanya bantuan perangkat yang disebut dengan **switch** atau **bridge**.

Layer 2 Network

- Komunikasi antar node di jaringan LAN secara fundamental sebenarnya banyak dilakukan di layer 2 OSI, yaitu Layer Data Link.





Keamanan di Jaringan LAN

- Implementasi security biasanya hanya terkonsentrasi antara jaringan public dan jaringan local (LAN).
- Aspek security di tiap layer sebenarnya berpengaruh satu sama lain. Dan biasanya kelemahan security di layer bawah akan mempengaruhi di layer atasnya.
- Tidak banyak administrator jaringan menyadari bahwa jaringan local mereka juga rentan terhadap serangan dari pihak yang tidak bertanggung jawab yang berada di sisi internal jaringan tersebut.
- Dan sebaiknya keamanan di layer Media (Fisik dan Data link) tetap menjadi pertimbangan dan prioritas implementasi keamanan di jaringan tersebut karena pasti juga berpengaruh secara keseluruhan.

Keamanan di Jaringan LAN



- Sudah banyak orang iseng dan bermaksud tidak baik di jaringan Public dan hal tersebut juga bisa terjadi di jaringan Internal.

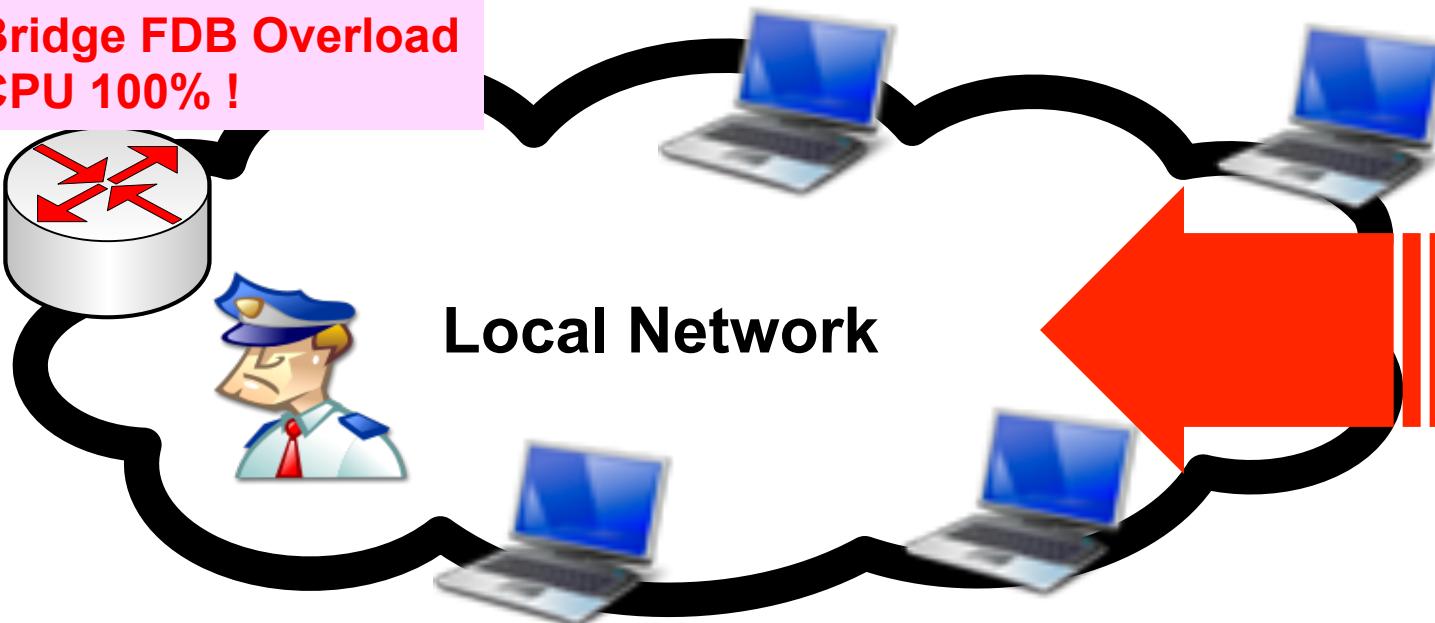


Layer 2 Attack !

- CAM table overflow / Mac Flooding
- Neighborhood Protocols Exploitation.
- DHCP Starvation
- ARP Cache poisoning – MitM Attack
- Defeating users and providers Hotspot and PPPoE based

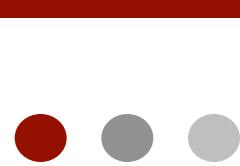
MAC Flood

Bridge FDB Overload
CPU 100% !



Mac-address:
00:0C:42:00:00:00
00:0C:42:00:00:01
00:0C:42:00:00:02
00:0C:42:00:00:03
:
:
00:0C:42:ff:ff:ff

- Terdapat banyak sekali tool yang bisa digunakan untuk melakukan serangan MAC flooding.
- Mac-flooding adalah salah satu serangan terhadap jaringan bridge dengan cara memenuhi jaringan dengan banyak sekali mac-address palsu.



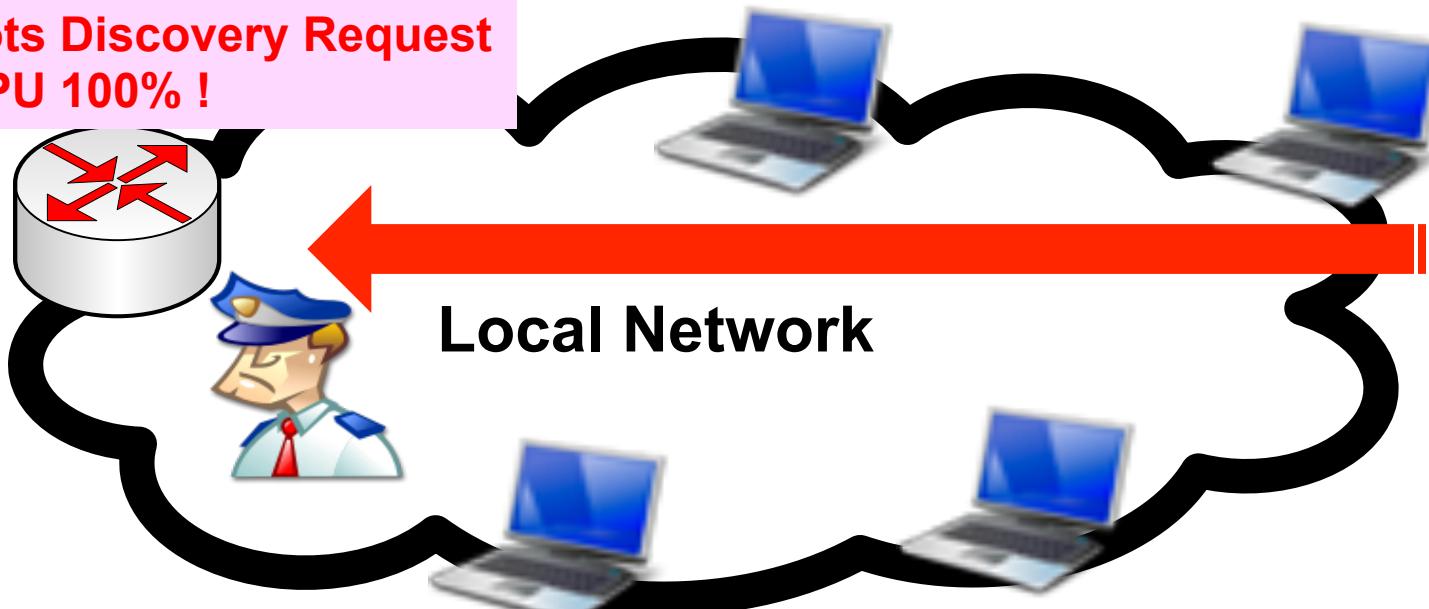
MAC Flood

- Mac flood bisa dilakukan dari semua port yang terhubung ke jaringan bahkan bisa juga di jaringan wireless.
- Akibatnya akan terjadi lonjakan yang sangat signifikan di jumlah host yang ada di bridge host table dan ARP table.
- Network akan mengalami banyak **delay**, Banyak sekali paket yang tidak perlu dan **Jitter** (kepadatan spektral frekuensi konten).
- Tinggal menunggu waktu dan bergantung kekuatan perangkat sebelum network tersebut Fail atau crash !

Exploiting Neighborhood



Lots Discovery Request
CPU 100% !



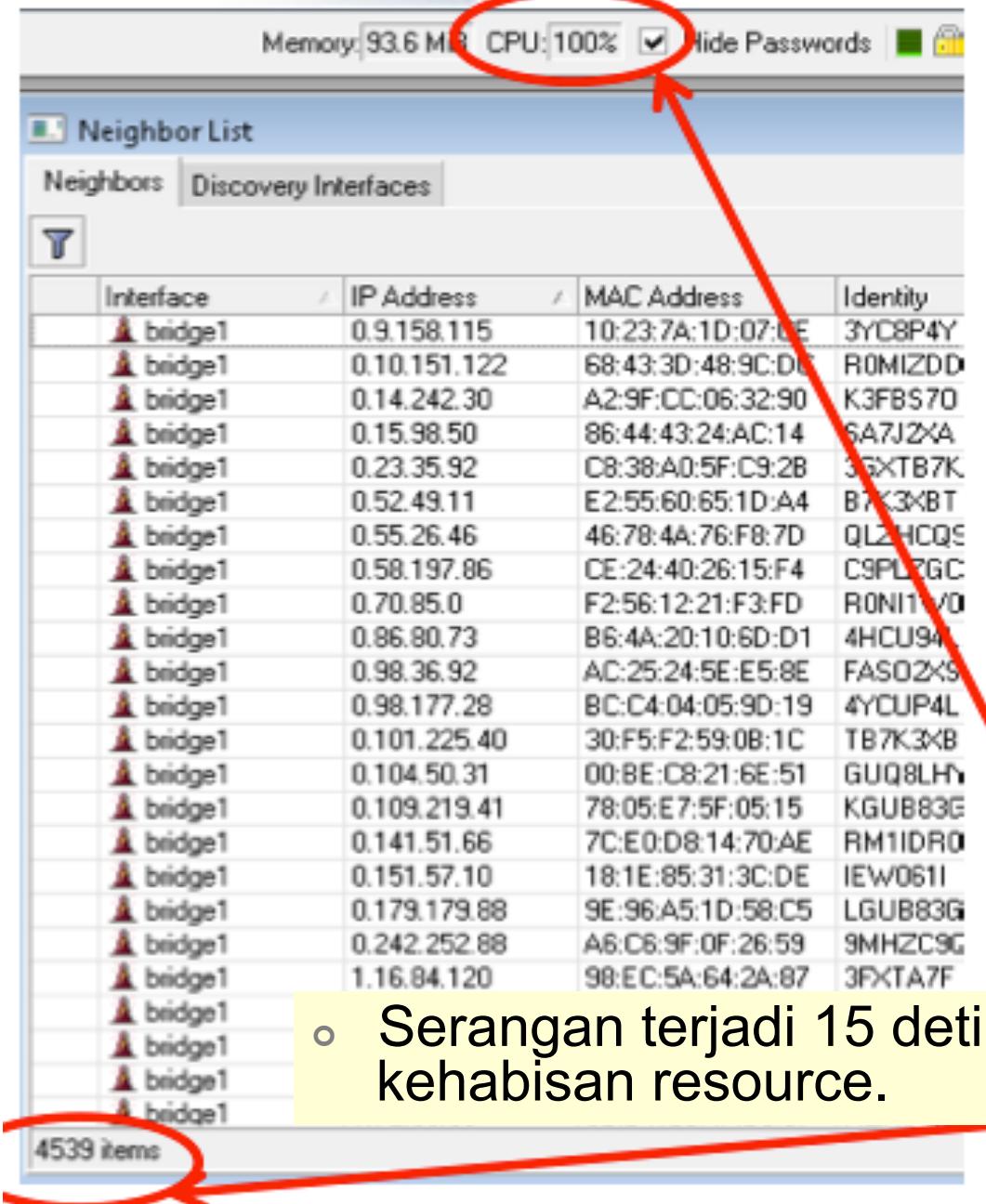
Mac-address:
00:0C:42:00:00:00
00:0C:42:00:00:01
00:0C:42:00:00:02
00:0C:42:00:00:03
.
. .
00:0C:42:ff:ff:ff

- Neighbor Discovery Protocols sangat membantu dalam management sebuah jaringan.
- Mikrotik RouterOS menggunakan **MNDP** - Mikrotik Neighbor Discovery Protocol. (Cisco juga menggunakan protocol yang mirip yaitu **CDP** – Cisco Discovery Protocol).
- Kedua protocol tersebut sama-sama menggunakan **packet broadcast** **protocol UDP port 5678 setiap 60 detik di semua interface yang diaktifkan**.



Exploiting Neighborhood

- Tool-tool hacking yang didevelop untuk menyerang Discovery Router Cisco juga bisa menyerang router mikrotik.
- Tool tersebut bisa digunakan untuk mendapatkan informasi keseluruhan jaringan dan bisa juga untuk menyerang jaringan tersebut yang mengakibatkan Denial of Service.
- Serangan bisa datang kapan saja dari port mana saja yang terhubung ke jaringan yang kebetulan memang mengaktifkan protocol tersebut.

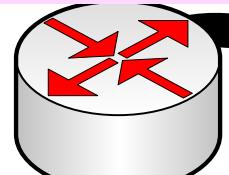


- Serangan terjadi 15 detik dan router akan segera kehabisan resource.

DHCP Starvation

Run-out IP

DHCP Sever FAIL !



Local Network



NEED IP's !

Mac-address:
00:0C:42:00:00:00
00:0C:42:00:00:01
00:0C:42:00:00:02
00:0C:42:00:00:03
.
. .
00:0C:42:ff:ff:ff

- Penyerang akan menggunakan banyak sekali **random mac-address** untuk meminta peminjaman ip dari dari IP-pool DHCP server.
- Tidak perlu waktu lama ketika DHCP server akan kehabisan resource IP untuk dibagikan ke client yang benar-benar membutuhkan.
- Ketika DHCP server tidak lagi mampu maka penyerang bisa saja membuat **Rogue DHCP** server untuk mengganggu jaringan tersebut.



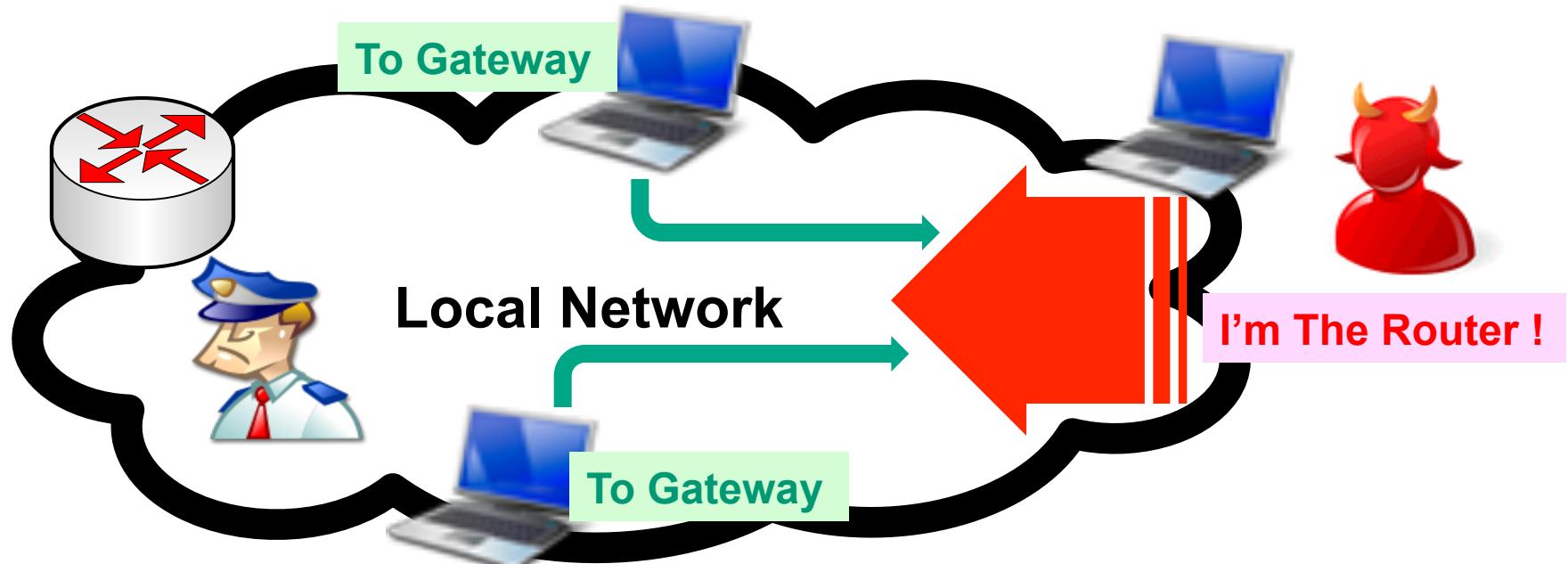
DHCP Starvation

- Ada dua type serangan DHCP Starvation :
 - Penyerang mengenerate banyak sekali mac-address dan menghabiskan pool DHCP server.
 - Penyerang mengenerate banyak sekali DHCP Discovery packet tetapi tidak mengirimkan packet konfirmasi.
- Kedua teknik bisa berakibat Denial of Service karena DHCP Server kehabisan resource IP-pool. Teknik pertama memakan waktu lebih lama tetapi konsisten sedangkan teknik kedua lebih cepat tetapi tidak konsisten.

DHCP						
	Address	Active Address	Active MAC Addre...	Active Hos...	Expires After	Status
D	172.16.1.250	00:16:D3:AD:25:F5	maia		2d 23:52:49	bound
D	172.16.1.254	3E:4D:E3:25:AC:95			00:00:20	offered
D	172.16.1.253	84:F3:C5:10:E6:F5			00:00:20	offered
D	172.16.1.252	80:FE:45:49:DC:30			00:00:20	offered
D	172.16.1.251	38:52:B0:3B:92:99			00:00:20	offered
D	172.16.1.249	9A:7F:69:51:0A:52			00:00:20	offered
D	172.16.1.248	E4:B1:FE:7B:FB:1D			00:00:20	offered
D	172.16.1.247	F2:B1:5C:36:B9:37			00:00:20	offered
D	172.16.1.246	FA:F6:79:0F:D8:09			00:00:20	offered
D	172.16.1.245	64:3B:C6:4B:D0:6E			00:00:20	offered
...						
D	172.16.1.228	AA:76:E5:24:4B:9E			00:00:18	offered
D	172.16.1.227	D8:FD:2A:44:E7:27			00:00:18	offered
D	172.16.1.226	60:AE:2C:74:9F:FE			00:00:18	offered
D	172.16.1.225	74:6D:FF:1F:19:05			00:00:18	offered
D	172.16.1.224	18:87:80:08:CD:AC			00:00:18	offered
D	172.16.1.223	58:DF:F2:40:D1:1D			00:00:18	offered
D	172.16.1.222	EA:8B:DC:28:DA:...			00:00:18	offered
D	172.16.1.221	AC:5E:7E:50:1D:00			00:00:10	offered
253 items						

- Kurang dari 5 detik DHCP Server sudah kehabisan ip 1 blok C

ARP Poisoning / Spoofing



- Penyerang akan mengirimkan pesan ARP ke seluruh network yang menyatakan bahwa mac-address yang dimilikinya adalah mac-address yang valid dari host tertentu (Biasanya mac-address dari gateway).
- Korban pesan ARP palsu ini akan mulai mengirimkan paket data ke penyerang yang dianggap sebagai gateway.

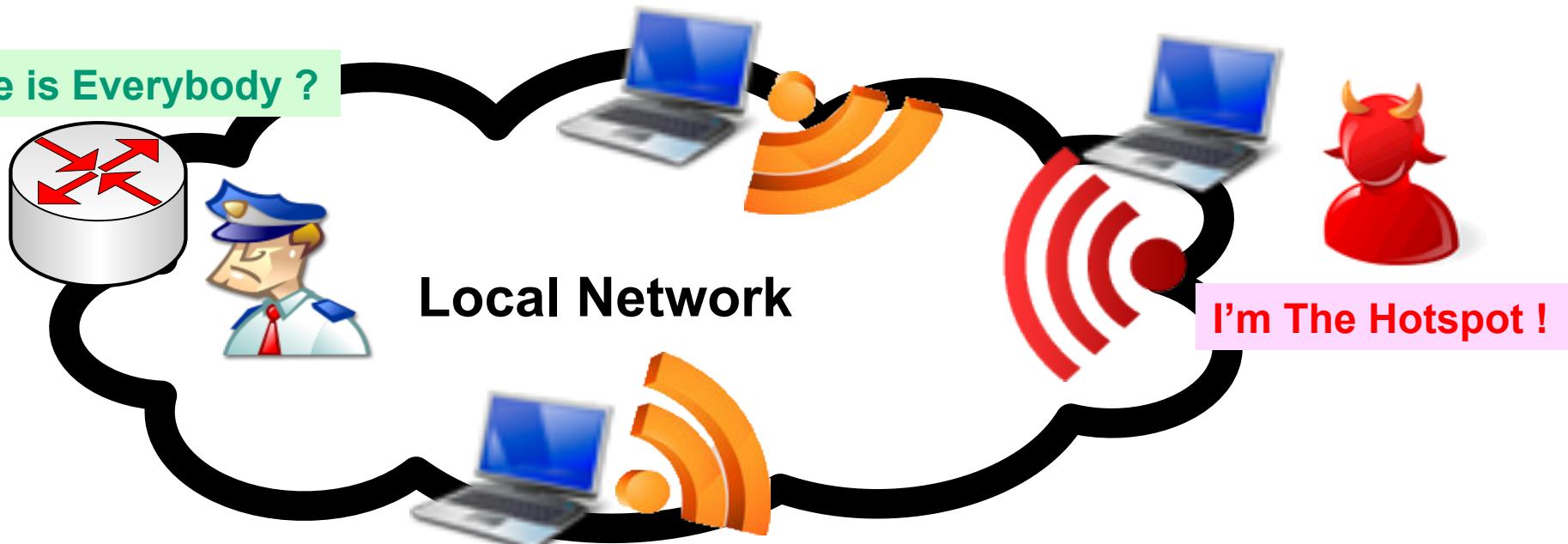


ARP Poisoning / Spoofing

- Dalam pengembangannya si penyerang bisa membuat bidirectional spoofing.
- Si penyerang tidak hanya memanipulasi ARP dari semua client bahwa dia adalah router, karena si penyerang juga bisa saja membuat pesan ARP “gratuitous” ke router bahwa mac-address nya adalah mac-address si korban
- Serangan bidirectional ini berjalan sempurna dan si penyerang bisa leluasa melakukan sniffing atau modifikasi paketnya.

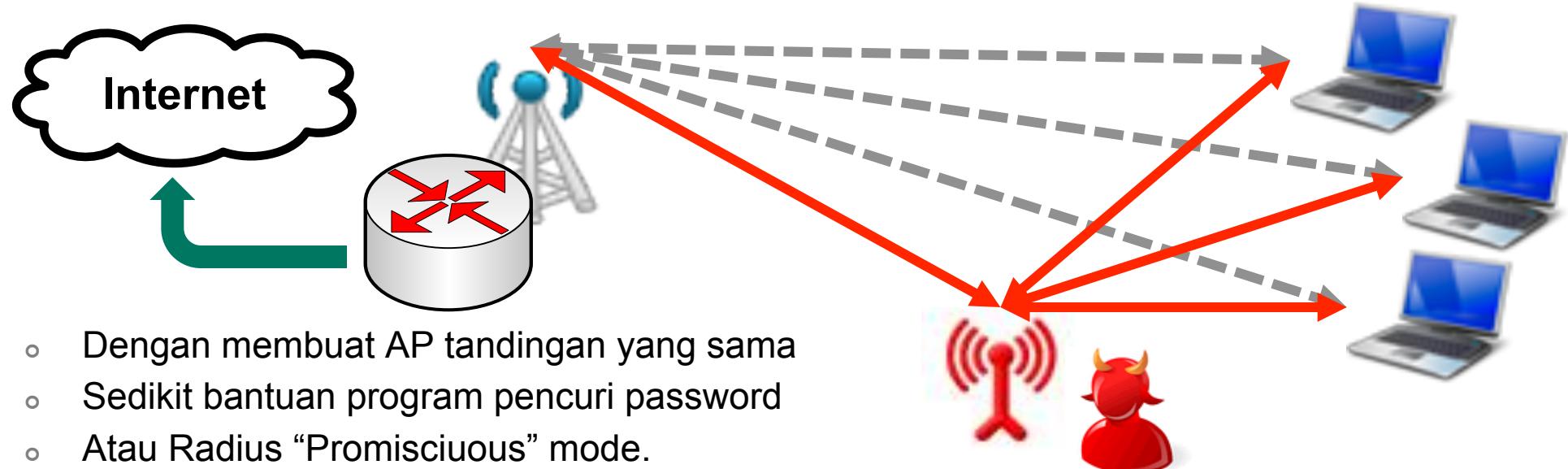
Hotspot & PPPoE Attack

Where is Everybody ?



- Sangat memungkinkan untuk melakukan serangan dengan metode sederhana pada jaringan Hotspot atau PPPoE.
- Hanya dengan membuat AP tandingan dengan SSID dan Band yang sama pada wifi atau membuat service server yang sama pada PPPoE.
- Walaupun jika autentikasi menggunakan RADIUS si penyerang juga bisa menggunakan Radius mode “**promiscuous**”.

Hotspot & PPPoE Attack



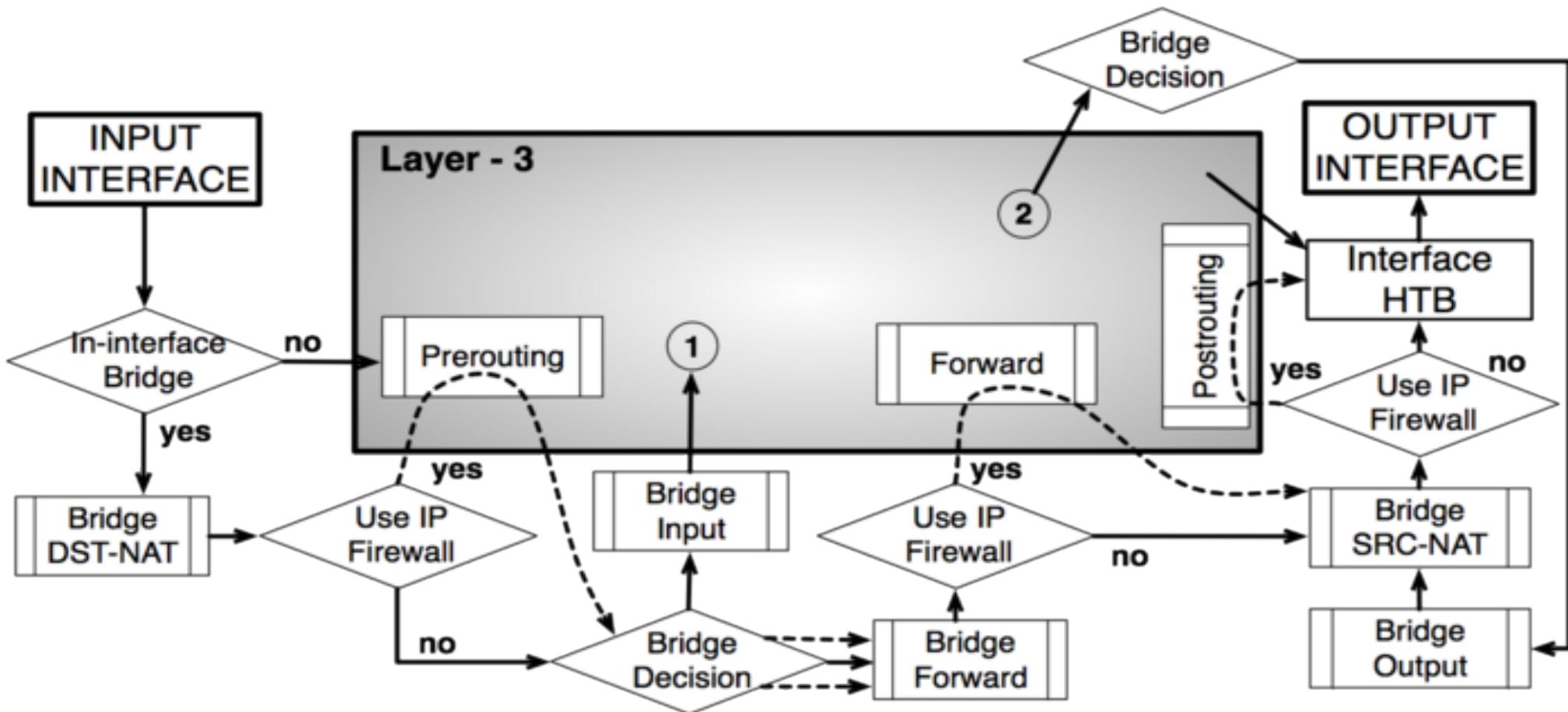
- Dengan membuat AP tandingan yang sama
 - Sedikit bantuan program pencuri password
 - Atau Radius “Promiscuous” mode.
 - Freeradius conf :
 - # Log authentication requests to the log file
 - # allowed values: { no, yes }
 - **log_auth = yes**
 - # Log passwords with the authentication requests
 - # allowed values: { no, yes }
 - **log_auth_badpass = yes**
 - **log_auth_goodpass = yes**



Countermeasures

- Beberapa fungsi Mikrotik bisa menanggulangi atau setidaknya mengurangi beberapa serangan yang sudah disebutkan sebelumnya.
- Pengendalian ARP secara manual juga bisa membantu menhadapi serangan MAC-flooding dan ARP spoofing
- Mikrotik Bridge Filter (filter layer 2) Memiliki kemampuan yang hampir sama di Layer 3 Filter.
- Bridge traffic memiliki Logika IP flow tersendiri.

Mikrotik Layer 2 Filter



- Seperti halnya Firewall di Layer 3, Bridge juga memiliki packet flow tersendiri.

[LAB - 1] MAC Flood



192.168.10.2/24

Meja 1



Bridge

Bridge

Ether3

Ether1

192.168.10.4/24

Meja 2

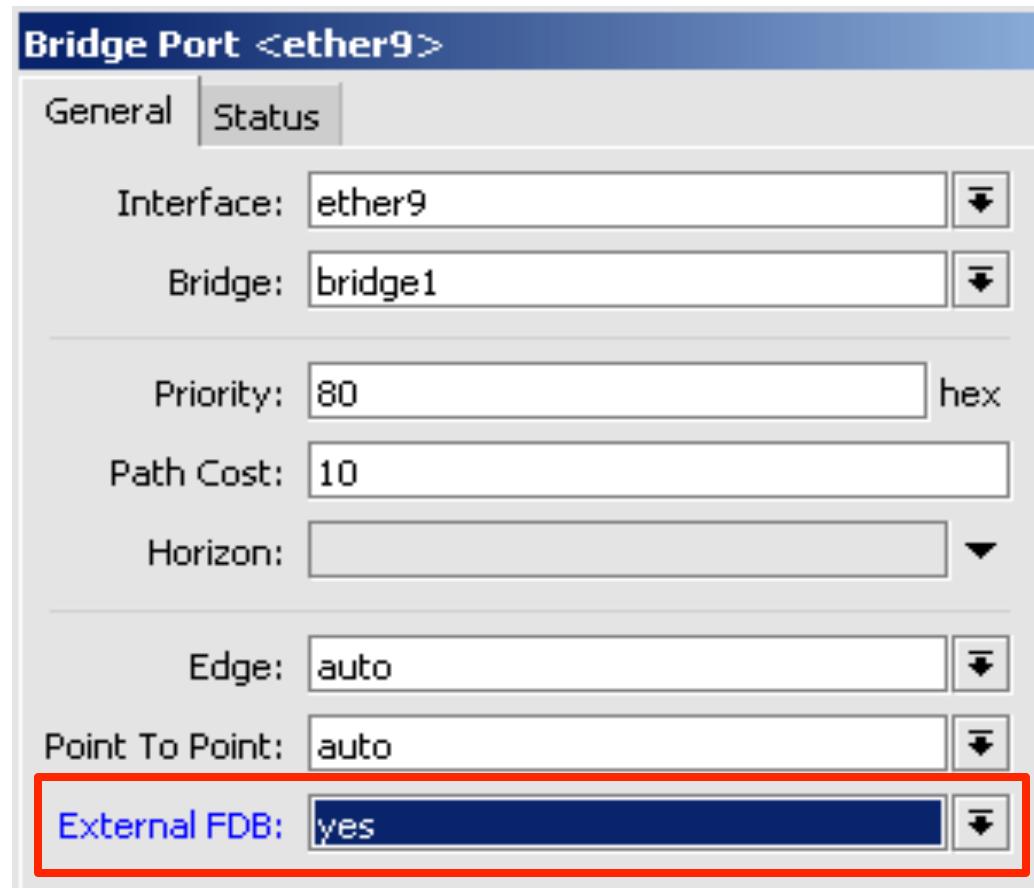


- Silakan download program **etherflood.exe** untuk melakukan simulasi flooding mac-address di jaringan bridge.
- Amati perubahan yang terjadi pada router Anda (Bridge Host, ARP, interface dan CPU).

Mac-address:
00:0C:42:00:00:00
00:0C:42:00:00:01
00:0C:42:00:00:02
00:0C:42:00:00:03
.
.
.
00:0C:42:ff:ff:ff

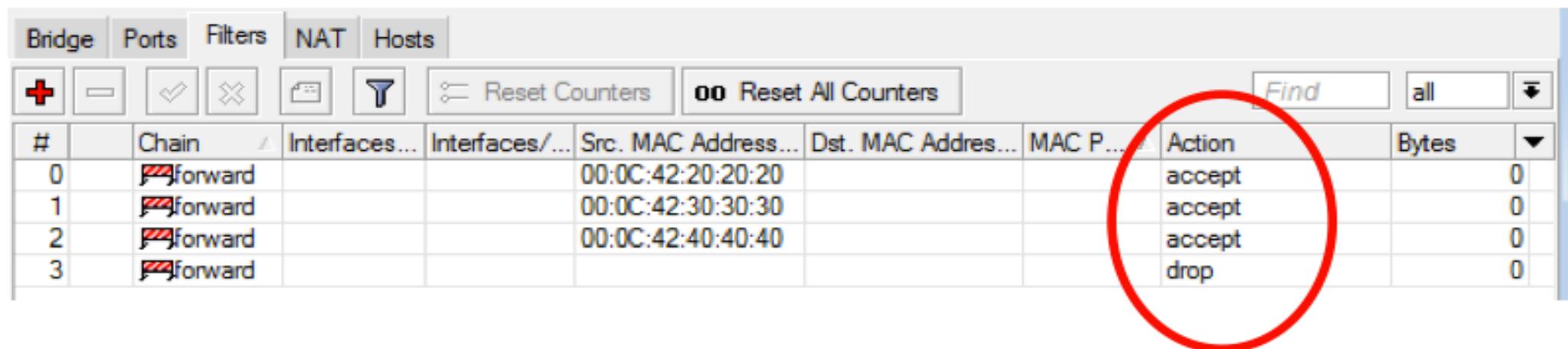
MAC Flood - Countermeasure

- **Border Port** pada Bridge dapat dimodifikasi sehingga menggunakan **external FDB** (Forwarding Data Base) sehingga port tersebut berfungsi seperti sebuah HUB saja.
- Jika terjadi flooding mac-address yang membanjiri port tersebut tidak akan dimasukkan ke dalam FDB.



MAC Flood - Countermeasure

- Walaupun sudah mengamankan FDB serangan tetap terjadi dan akan membanjiri External-FDB, cepat atau lambat external-FDB akan penuh juga.
- Sangat beruntung Mikrotik memiliki filter di Bridge network yang bisa mengatasi serangan tersebut.
- Daftarkan mac-address apa saja yang memang valid pada filter (accept) dan (drop) untuk mac-address yang lain.



#	Chain	Interfaces...	Interfaces/...	Src. MAC Address...	Dst. MAC Address...	MAC P...	Action	Bytes
0	Forward			00:0C:42:20:20:20			accept	0
1	Forward			00:0C:42:30:30:30			accept	0
2	Forward			00:0C:42:40:40:40			accept	0
3	Forward						drop	0

● ● ● Countermeasure – Exploiting Neighborhood

Neighbor List										
Neighbors		Discovery Interfaces								
<input type="button" value="Find"/> <input type="button" value="T"/>										
	Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	
	bridge-local	192.168.5.50	00:0C:42:82:52:AD	MikroTik	MikroTik	4.17	RB750	no	47	
	bridge-local	192.168.5.10	00:0C:42:0D:AA:1A	MikroTik	MikroTik	4.6	RB532	no	26	
	bridge-local	192.168.5.29	00:0C:42:40:7B:1F	RB433...	MikroTik	5.0rc10	RB433LIAH	no	55	
	ether2	192.168.200.2	00:04:C0:71:0A:D8	Switch	cisco ...	Ci	Neighbor List			

- Matikan MNDP di semua inter

Neighbors		Discovery Interfaces											
	Interface	bridge1	ether1	ether2	ether3	ether4	ether5	ether6	ether7	ether8	ether9	vlan5	wlan1
X	bridge1												
X	ether1												
X	ether2												
X	ether3												
X	ether4												
X	ether5												
X	ether6												
X	ether7												
X	ether8												
X	ether9												
X	vlan5												
X	wlan1												

Countermeasure – Exploiting Neighborhood

- Ketika MNDP sudah dimatikan, serangan exploit terhadap network discovery tetap terjadi.
- Gunakan Bridge Filter untuk melakukan blok traffic MNDP.

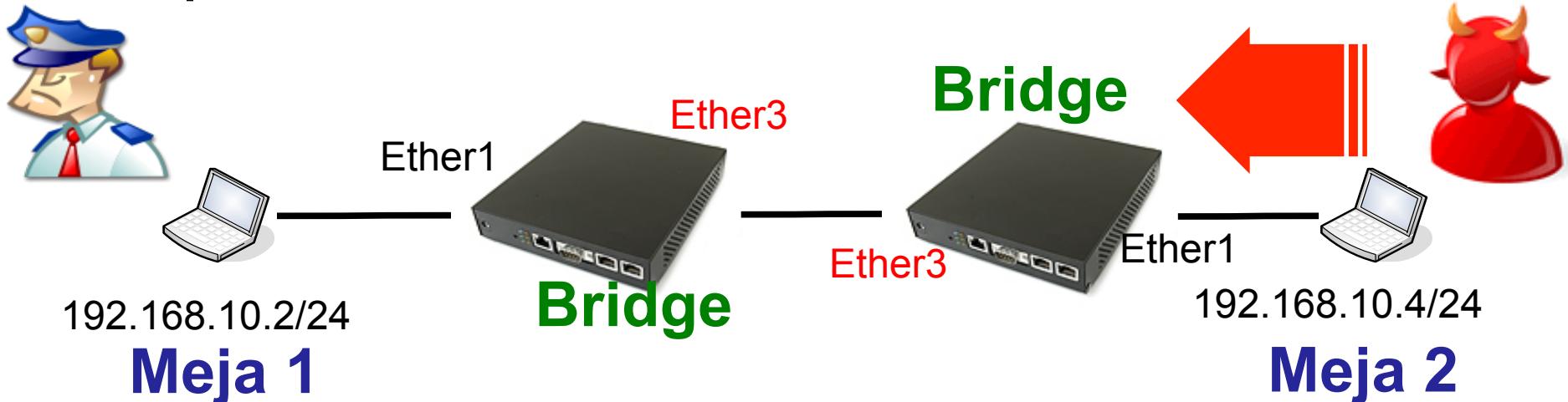
General	Advanced	ARP	STP	Action	Statistics
Chain: forward					
-▼ Interfaces					
-▼ Bridges					
-▼ Src. MAC Address					
-▼ Dst. MAC Address					
-▲ MAC Protocol					
MAC Protocol-Num: <input type="checkbox"/> ip <input type="button" value="hex"/>					
-▲ IP					
Src. Address: <input type="text"/>					
Src. Port: <input type="text"/>					
Dst. Address: <input type="text"/>					
Dst. Port: <input type="checkbox"/> 5678 <input type="button" value="▲"/>					
Protocol: <input type="checkbox"/> udp <input type="button" value="hex"/> <input type="button" value="▲"/>					
-▼ Packet Mark					
-▼ Ingress Priority					



Countermeasure – DHCP Starving

- Hampir sama seperti MAC-flooding pada serangan DHCP Starving sama-sama akan mengenerate mac-address palsu secara masive.
- Sehingga aktifkan external FDB dan juga mac filter tetap harus dilakukan.
- Gunakan static lease untuk mengamankan DHCP server.

[LAB - 2] ARP Spoofing



- Download dan aktifkan program **Netcut**
- Lakukan serangan pada network bridge

Countermeasure - ARP Poisoning / Spoofing

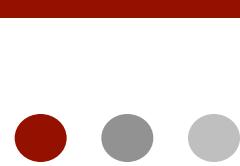
- ARP Poisoning / Spoofing bisa dikurangi dengan Mengubah tingkah laku ARP.
 - ARP = Disabled** – semua client harus mendaftarkan mac-address dari seluruh jaringan pada masing-masing tabel ARP secara **static**.

New Interface

General	STP	Status	Traffic
Name:	bridge1		
Type:	Bridge		
MTU:	1500		
L2 MTU:			
MAC Address:			
ARP:	disabled		
Admin. MAC Address:			

New ARP

IP Address:	192.168.0.234	
MAC Address:	00:01:02:03:04:05	
Interface:	bridge1	▼



Countermeasure - ARP Poisoning / Spoofing

- **ARP = Reply-Only** – pada network multipoint seperti Wireless maka pada konsentrator saja yang di configure Static-ARP.
- Konsekuensi yang didapatkan :
 - Static ARP pada semua host pasti sangat sulit untuk diimplementasikan.
 - ARP reply only tidak akan melindungi client dari serangan.



Countermeasure - ARP Poisoning / Spoofing

- Metode yang lain yang bisa dilakukan adalah mengisolasi traffic layer 2.
- Jika dilihat lebih detail pada jaringan LAN secara umum, traffic yang terjadi sebagian besar adalah dari client menuju ke gateway.
- Dengan mengisolasi traffic hanya dari client menuju ke gateway maka teknik-teknik ARP poisoning bisa dikurangi dan di cegah.

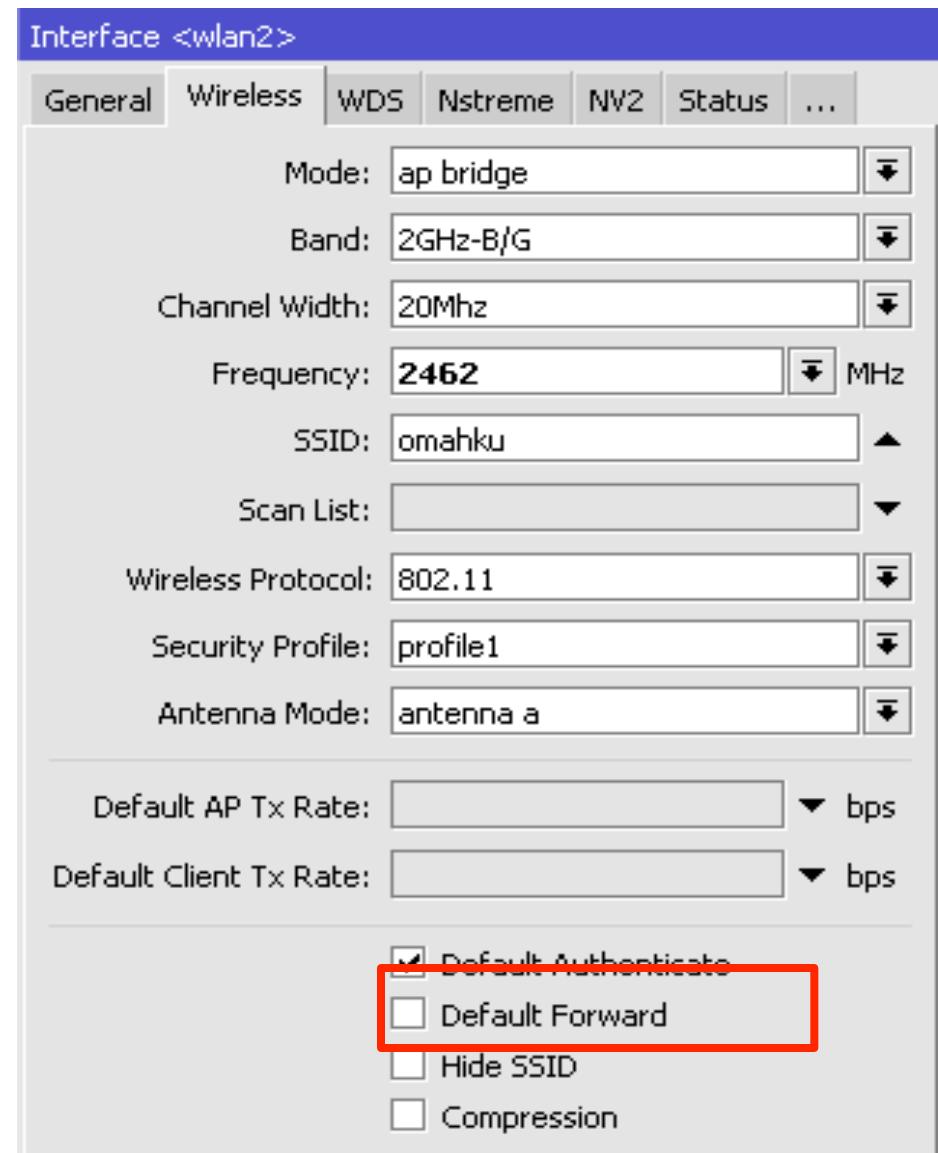


Resource Sharing

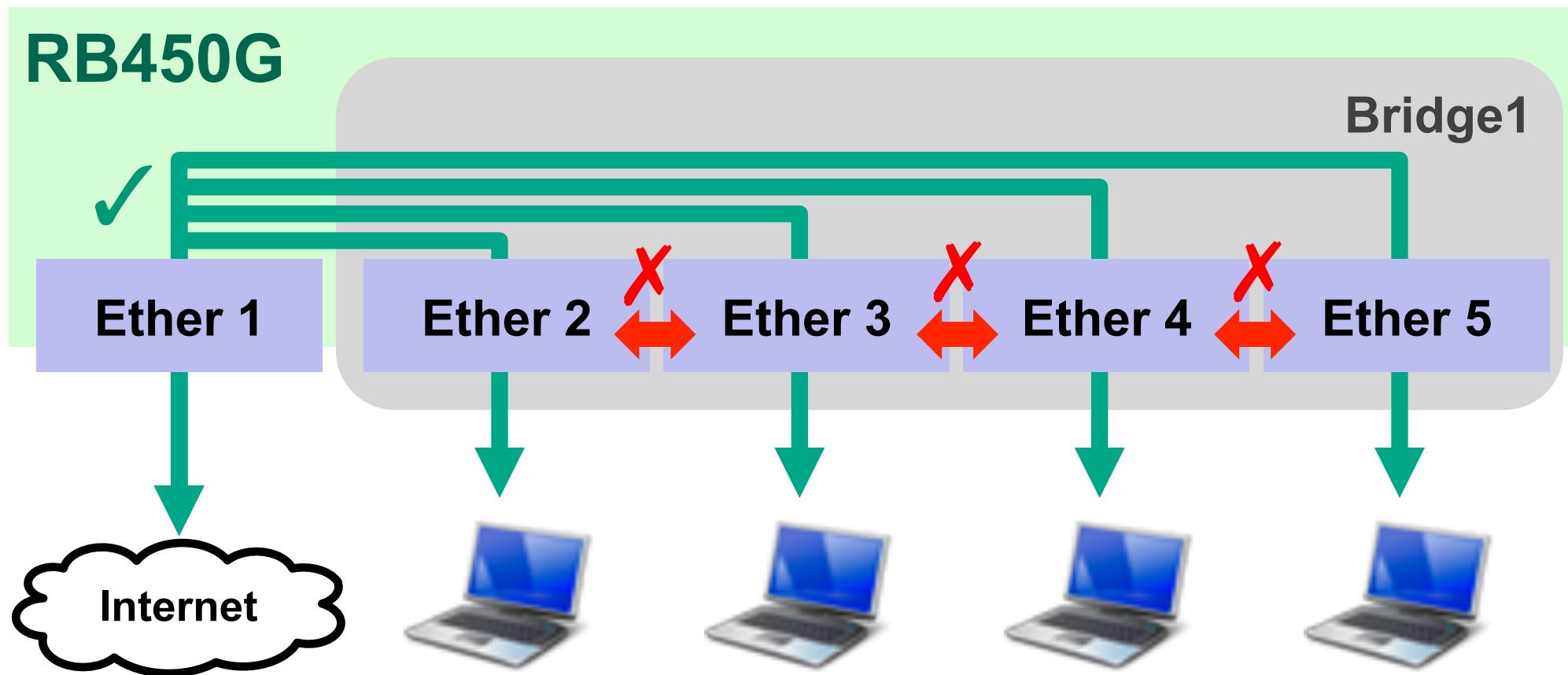
- Di jaringan LAN memang sering dibutuhkan resource sharing traffic seperti sharing file atau printer.
- Bisa mulai diimplementasikan penggunaan file server terpusat atau printer server di segmen yang berbeda, tetapi masih terhubung satu sama lain dengan bantuan router.
- Selain mencegah serangan, penyebaran virus jaringan juga bisa sekaligus dikurangi.

Wireless - Default Forward

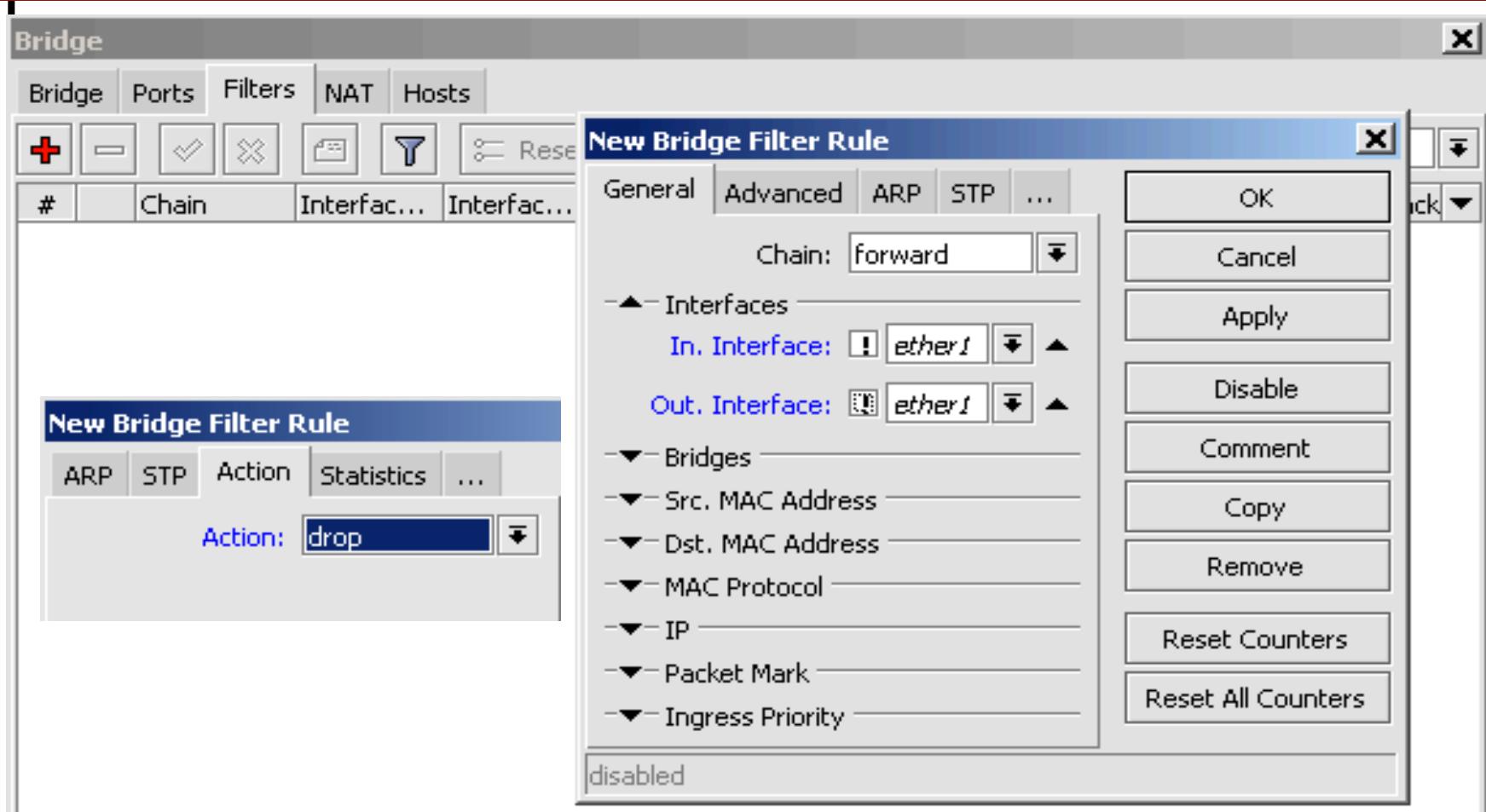
- Matikan Default Forward pada Wireless Mikrotik.



Bridge Forwarding filter



- Implementasikan Filter di bridge

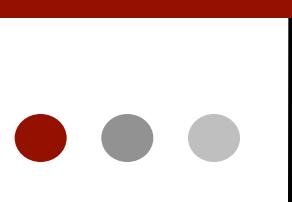


- Bridge Filter :
 - In-interface=ether1 out-interface=ether1 action=drop

Forwarding on SWOS

	Port1	Port2	Port3	Port4	Port5
Forwarding					
From Port 1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
From Port 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
From Port 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
From Port 4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
From Port 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

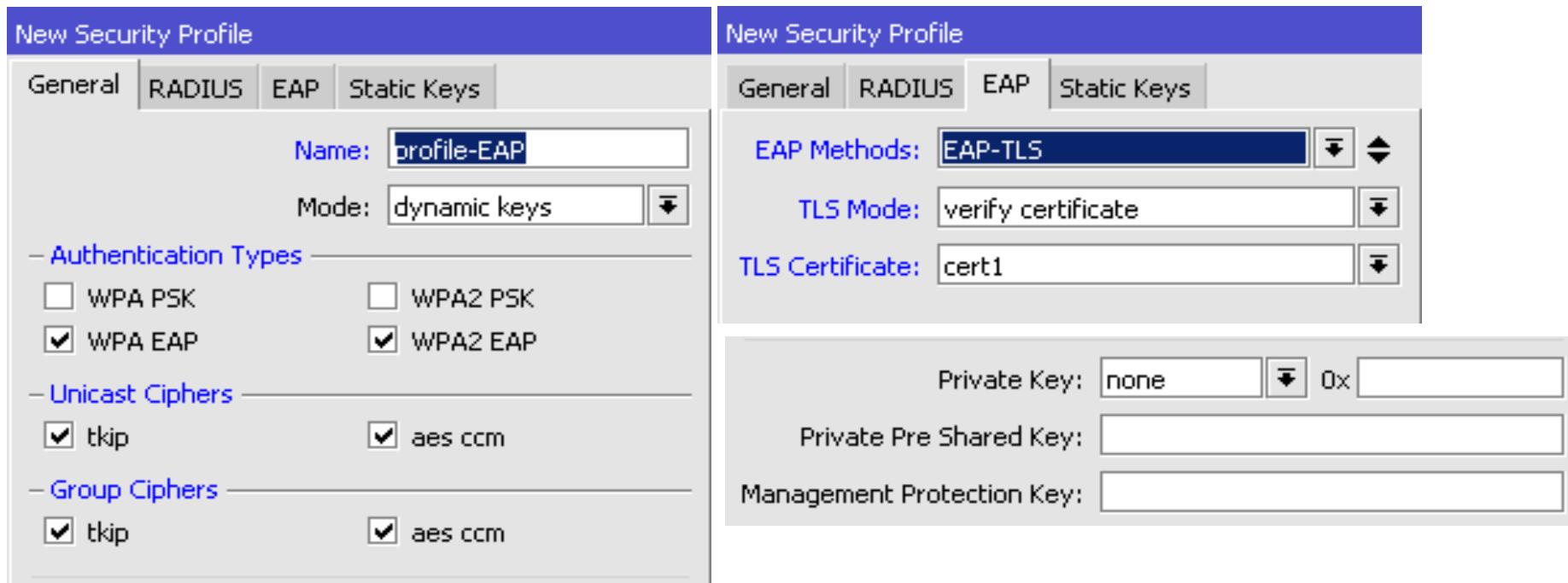
- Non-aktifkan forwarding pada port yang terhubung antar client di **RB250GS**.
- Asumsi **Port1** terhubung ke router, port lain terhubung ke client.



Hotspot & PPPoE Attack - Countermeasure

- Hanya menggunakan skema enkripsi yang baik yang bisa menanggulangi serangan ini.
- Adalah pengertian yang salah bahwa network tanpa security enkripsi adalah network yang aman.
- Enkripsi bisa diimplementasikan pada wireless atau PPPoE network, dan mikrotik sudah mampu melakukan hal tersebut di **Security Profile**.
- Metode yang paling secure adalah EAP-TLS yang mengimplementasikan certificate SSL di semua jaringan.
- Memang tidak semua perangkat support metode enkripsi EAP-TLS tetapi perlu dipertimbangkan juga bahwa segala metode enkripsi apapun yang digunakan akan setidaknya membuat si penyerang tidak leluasa melakukan exploitasi jaringan tersebut.

Encryption



New Security Profile

General RADIUS EAP Static Keys

Name: profile-EAP

Mode: dynamic keys

Authentication Types

WPA PSK WPA2 PSK

WPA EAP WPA2 EAP

Unicast Ciphers

tkip aes ccm

Group Ciphers

tkip aes ccm

New Security Profile

General RADIUS EAP Static Keys

EAP Methods: EAP-TLS

TLS Mode: verify certificate

TLS Certificate: cert1

Private Key: none 0x

Private Pre Shared Key:

Management Protection Key:

- Wireless Mikrotik termasuk perangkat yang memiliki kemampuan implementasi security terlengkap.



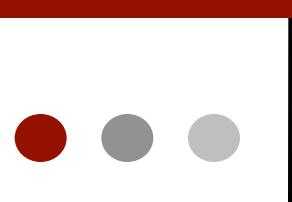
Firewall



Certified Mikrotik Training - Advanced Class (MTCTCE)

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)



Objectives

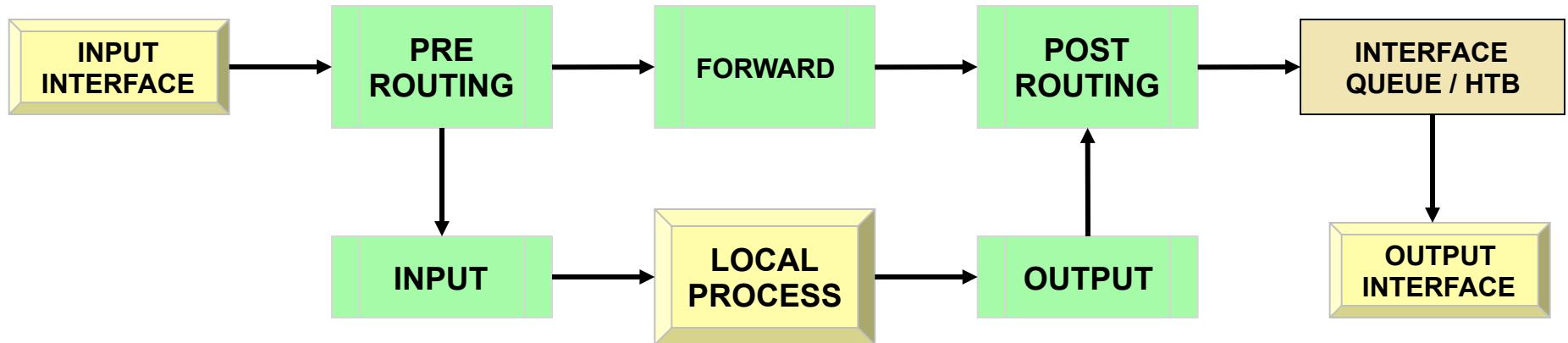
- Packet Flow
- Firewall Mangle
 - Conn Mark
 - Packet Mark
 - Routing Mark
- Firewall Filter
 - IP Address List
 - Advanced Parameter
- NAT



Packet Flow

- Diagram yang menunjukkan alur proses paket data yang keluar dan masuk di router
- Terdapat perbedaan cukup mendasar antara paket flow di versi 3 dengan versi sebelumnya
 - Use IP Firewall di bridge
 - Posisi routing decision
 - BROUTE dihilangkan

IP Flow (simple diagram)



PREROUTING

Hotspot Input
Conn-Tracking
Mangle
Dst-NAT
Global-In Queue
Global-Total Queue

INPUT

Mangle
Filter

FORWARD

Bridge Decision
TTL = TTL - 1
Mangle
Filter
Accounting

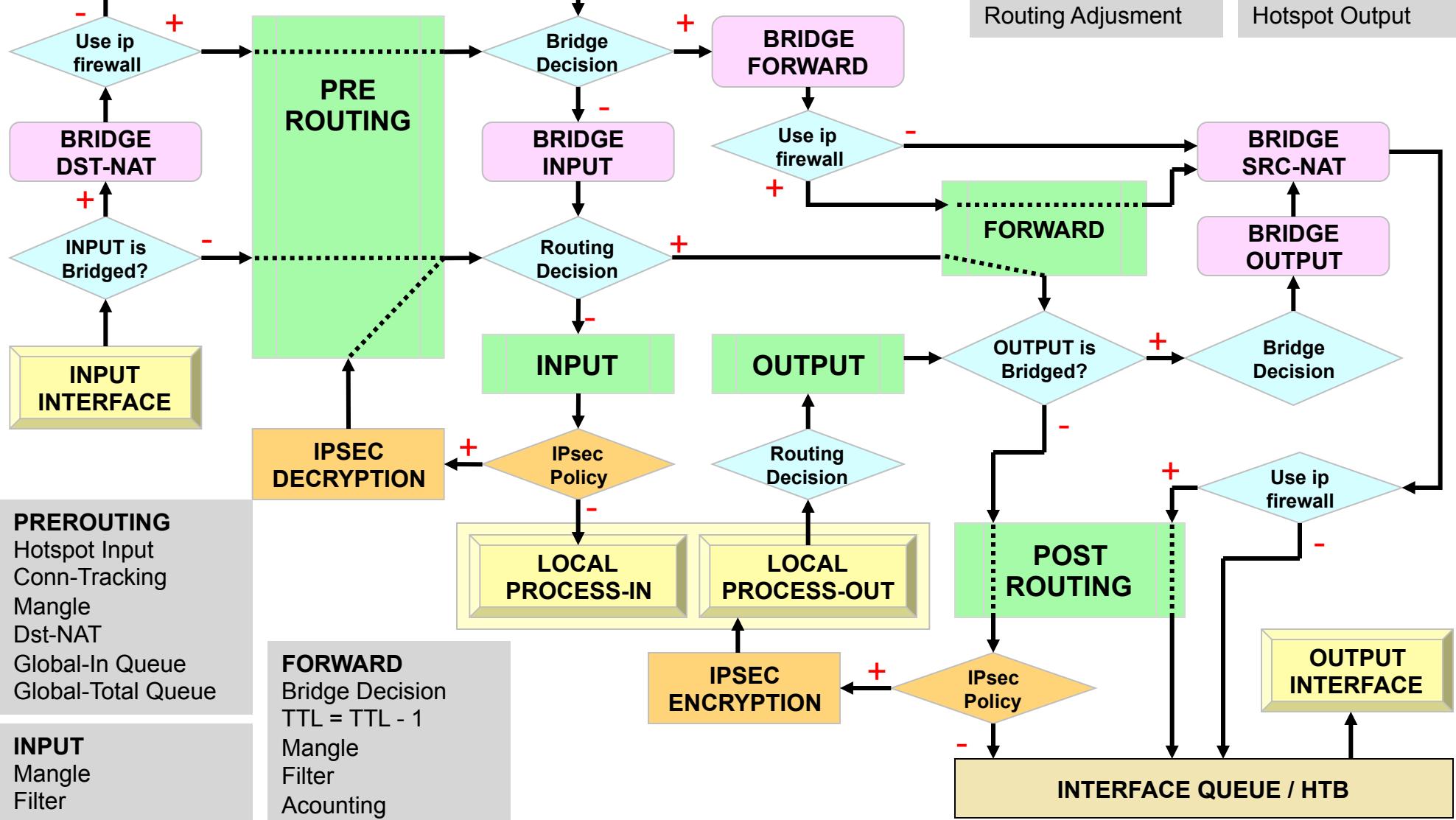
OUTPUT

Bridge Decision
Conn-Tracking
Mangle
Filter
Routing Adjustment

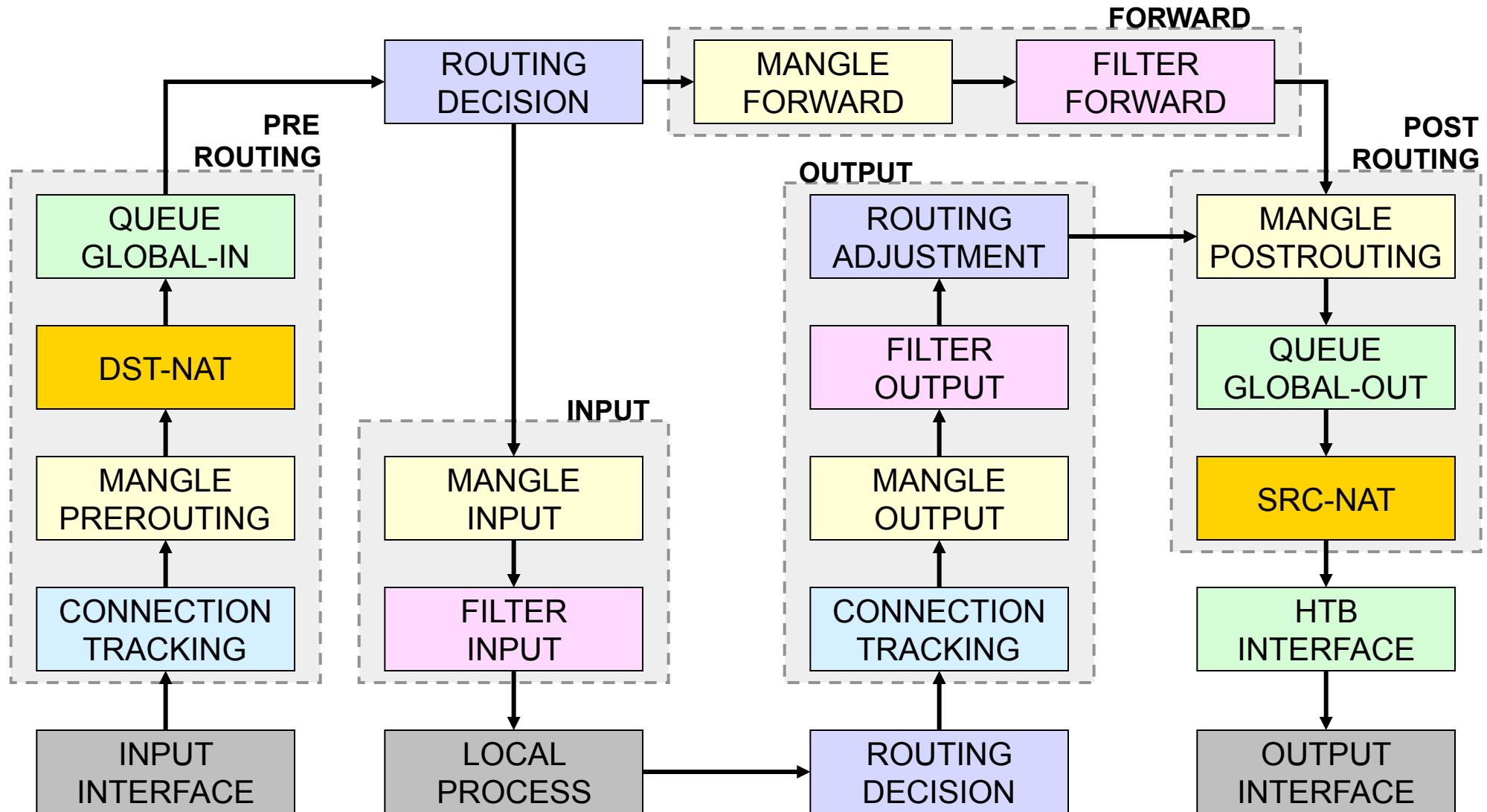
POSTROUTING

Mangle
Global-Out Queue
Global-Total Queue
Source-NAT
Hotspot Output

IP Flow (RoSv3)



Simple Packet Flow





Packet Flow

- Input / Output Interface / Local Process
- Routing Decision / Routing Adjustment
- Mangle
- Filter
- NAT
- Queue / HTB – on other chapter



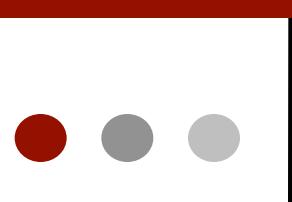
Input Interface

- Adalah interface yang dilalui oleh paket data, tepat ketika masuk di router.
- Pada saat proses “uplink” atau “request” yang dimaksud dengan input interface adalah interface yang mengarah ke client (local/lan interface).
- Pada saat proses “downlink” atau “response” yang dimaksud dengan input interface adalah interface yang mengarah ke internet (public/WAN interface)
- Jika client menggunakan IP Address publik, proses request juga bisa dilakukan dari internet, sehingga input interface adalah interface WAN.



Output Interface

- Adalah interface yang dilalui oleh paket data tepat ketika keluar dari router.
- Pada saat proses “uplink” atau “request” yang dimaksud dengan output interface adalah interface yang mengarah ke internet (WAN interface).
- Pada saat proses “downlink” atau “response” yang dimaksud dengan output interface adalah interface yang mengarah ke client (lokal/LAN interface).



Local Process

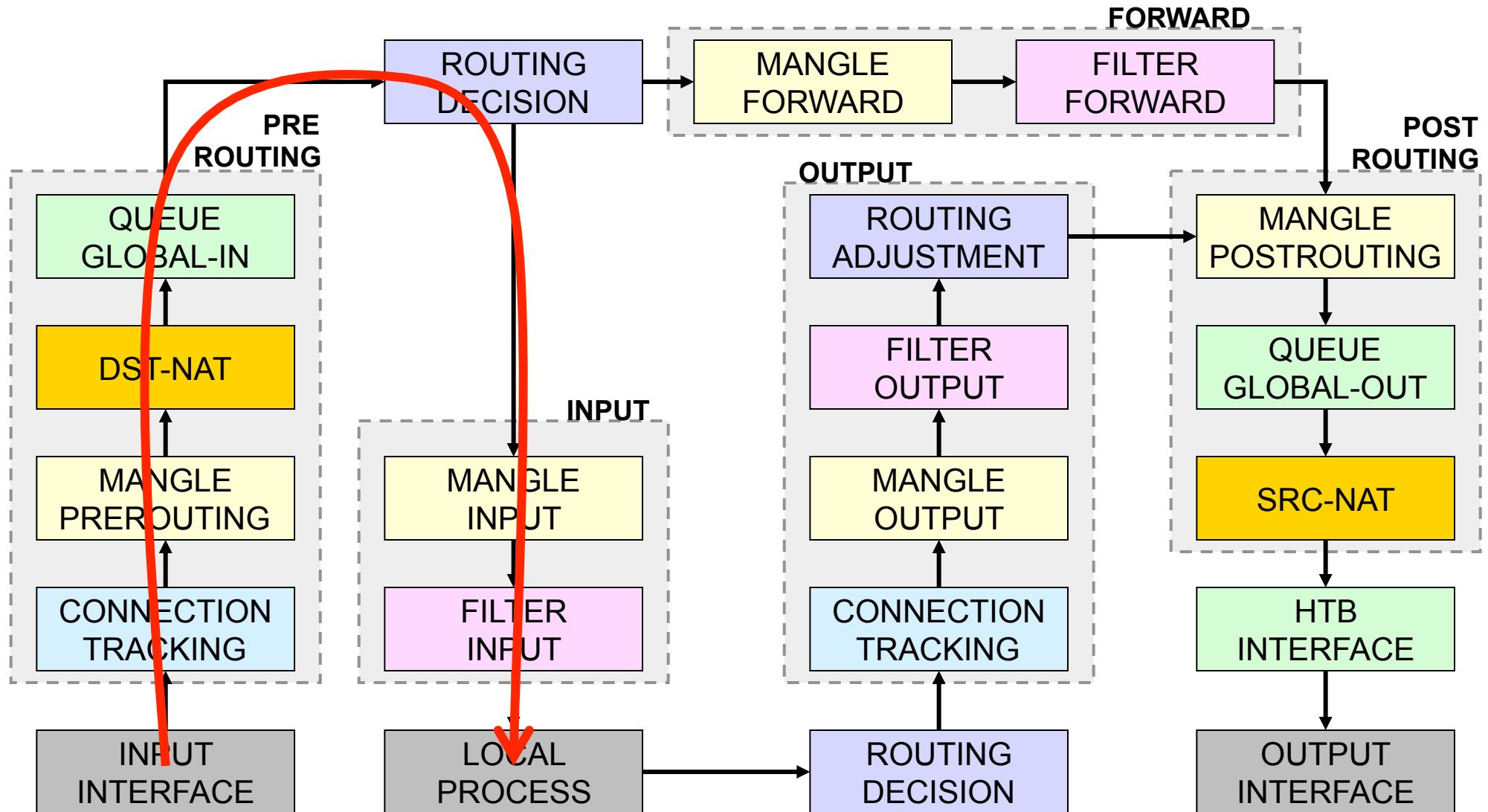
- Adalah router itu sendiri, jika ada paket data yang menuju ke router, misalnya:
 - Ping dari client ke IP router
 - Request Winbox dari client ke router
 - Proses response http akibat request dari web proxy
- Adalah router itu sendiri, jika ada paket data yang berasal dari router, misalnya:
 - Ping dari router ke internet atau ke client
 - Proses request http dari web proxy



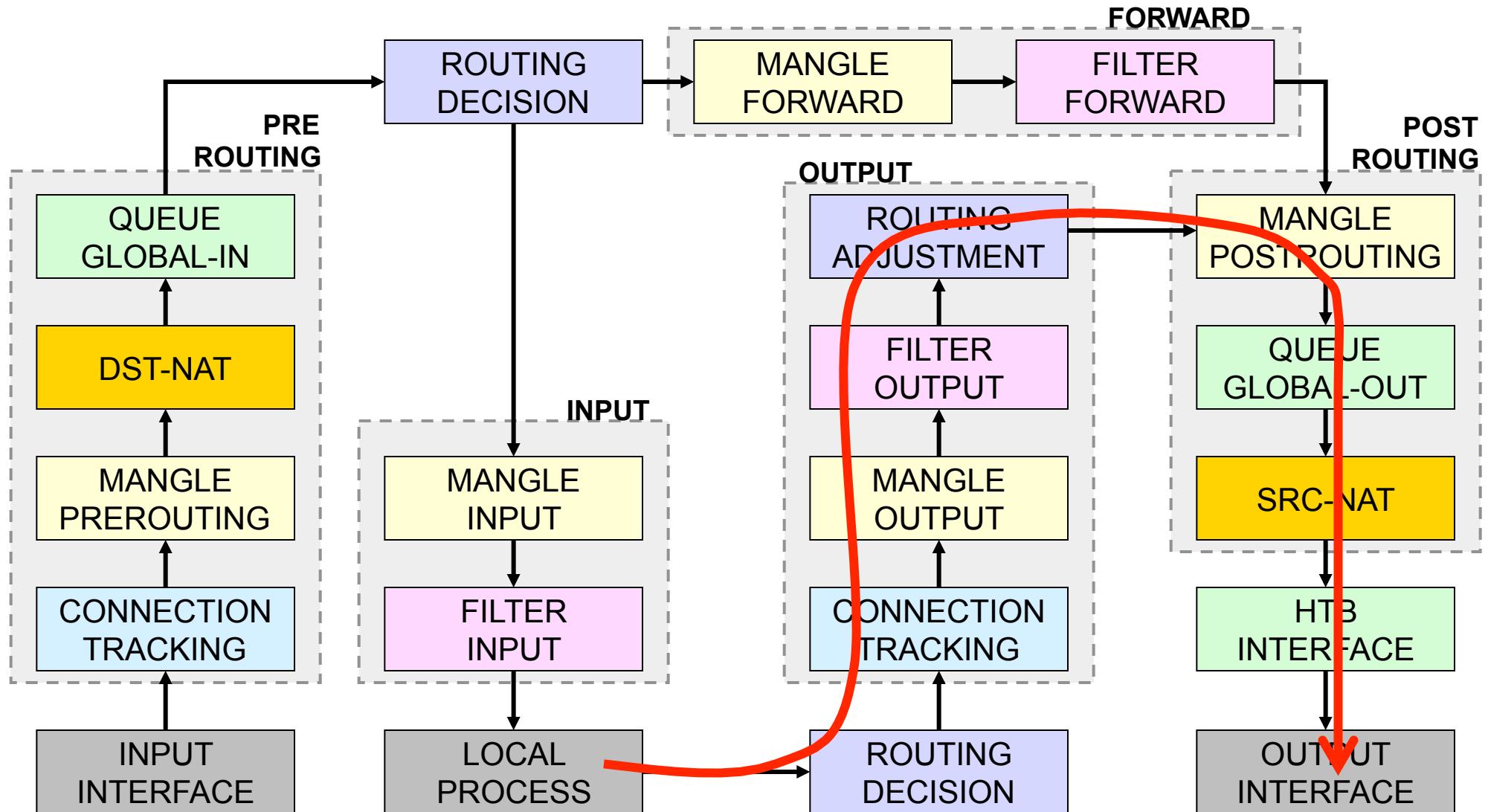
Routing Decision

- Adalah proses yang menentukan apakah paket data akan disalurkan ke luar router, atau menuju ke router itu sendiri.
- Proses ini juga menentukan interface mana yang akan digunakan untuk melewatkkan paket data keluar dari router.
- Pada chain output (setelah mangle, dan filter) terdapat **Routing Adjustment** yang berfungsi memperbaiki routing decision yang diakibatkan oleh **route-mark** pada mangle di chain **output**.

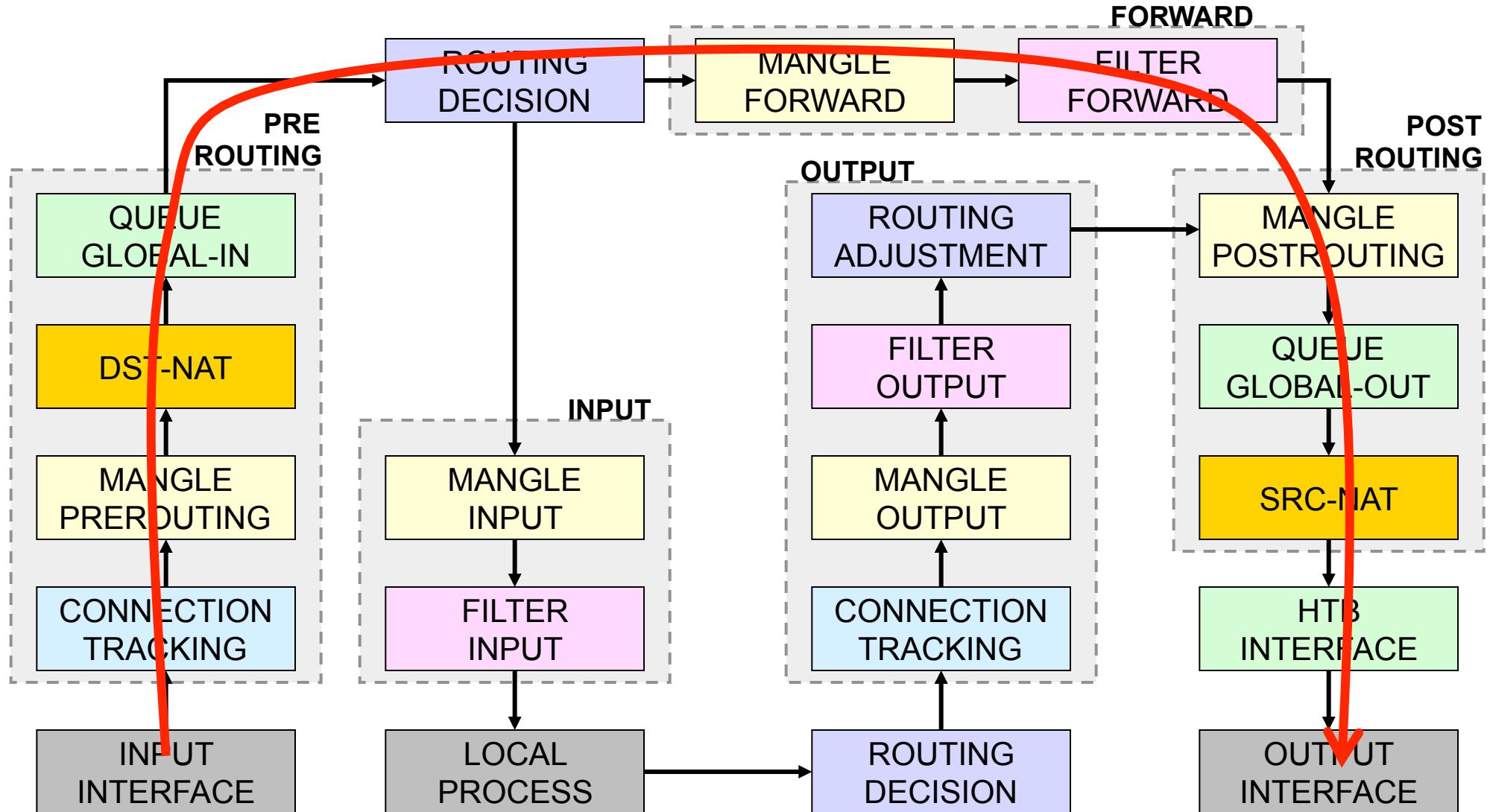
Trafik Menuju Router



Trafik dari Router



Trafik Melalui Router

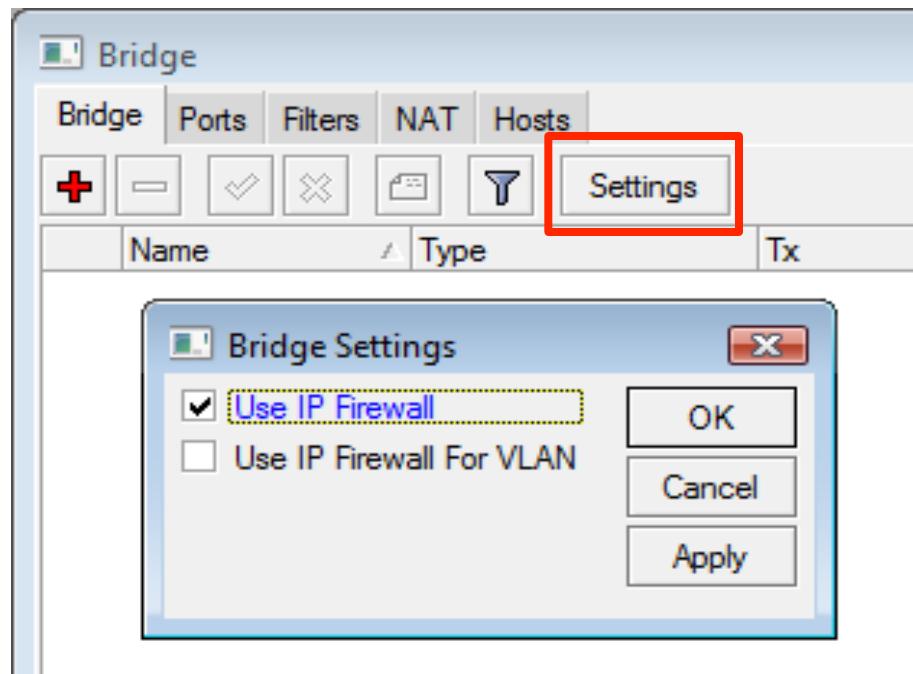


Posisi Chain / Parent

From	To	Mangle	Firewall	Queue
Outside	Router/ Local Process	Prerouting		Global-In
		Input	Input	Global-Total
Router/ Local Process	Outside	Output	Output	Global-Out
		Postrouting		Global-Total
				Interface
Outside	Outside	Prerouting		Global-In
		Forward	Forward	Global-Out
		Postrouting		Global-Total
				Interface

Use IP Firewall – on Bridge

- Jika kita menggunakan fungsi bridge, dan ingin menggunakan logika firewall ataupun mangle (Leyer 3), kita harus mengaktifkan setting use ip firewall.



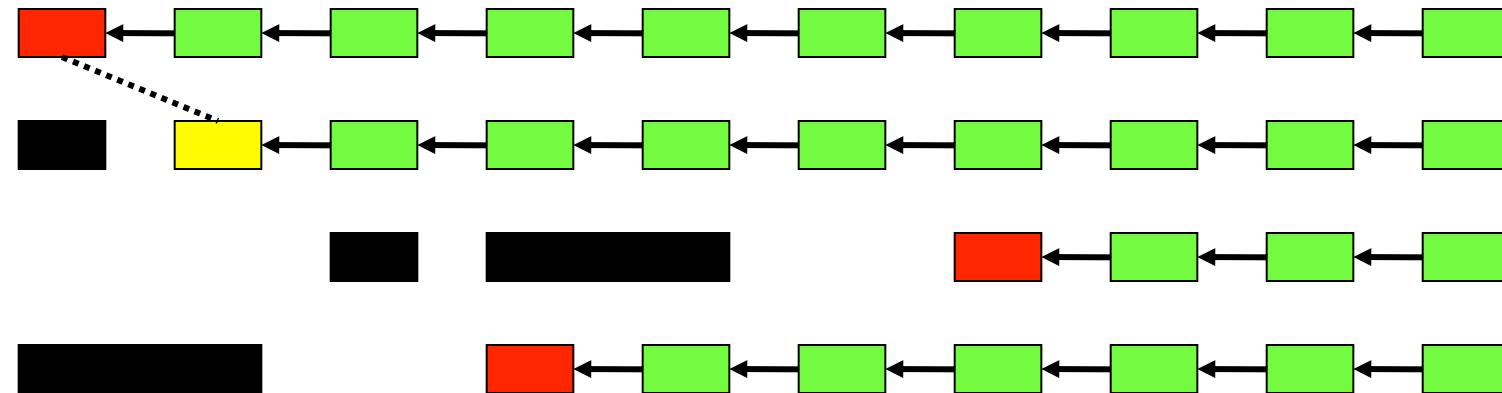


Connection State

- Setiap paket data yang melewati router memiliki status:
 - **Invalid** – paket tidak dimiliki oleh koneksi apapun, tidak berguna
 - **New** – paket yang merupakan pembuka sebuah koneksi/paket pertama dari sebuah koneksi
 - **Established** – merupakan paket kelanjutan dari paket dengan status new.
 - **Related** – paket pembuka sebuah koneksi baru, tetapi masih berhubungan dengan koneksi sebelumnya.
 - Contoh connection Related adalah komunikasi FTP yang membuka connection related di port 20 setelah connection new di port 21 sudah dilakukan.

Connection State

Firewall



New



Established



Related

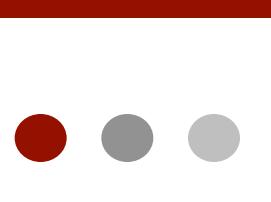


Invalid



Firewall Mangle

- Mangle adalah cara untuk menandai paket-paket data tertentu, dan kita akan menggunakan tanda (Marking) tersebut pada fitur lainnya, misalnya pada filter, routing, NAT, ataupun queue.
- Tanda mangle ini hanya bisa digunakan pada router yang sama, dan tidak terbaca pada router lainnya.
- Pembacaan / pelaksanaan rule mangle akan dilakukan dari atas ke bawah secara berurutan.

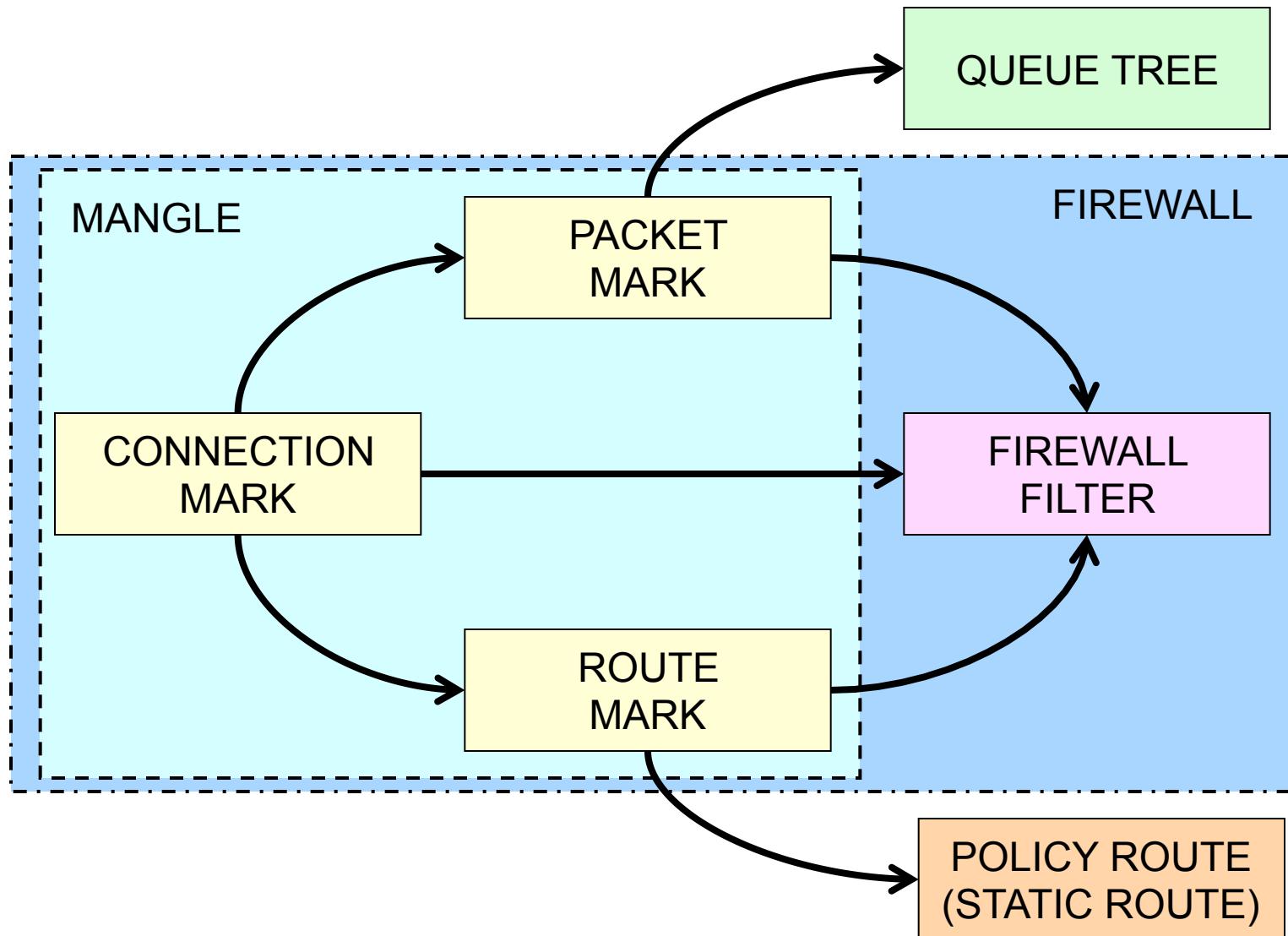


Type of Mark

- Flow Mark / Packet Mark
 - Penandaan untuk setiap paket data
- Connection Mark
 - Penandaan untuk suatu koneksi (request dan response)
- Route Mark
 - Penandaan paket khusus untuk routing

Setiap paket data hanya bisa memiliki maksimal 1 conn-mark, 1 packet-mark, dan 1 route-mark

Penggunaan Mangle





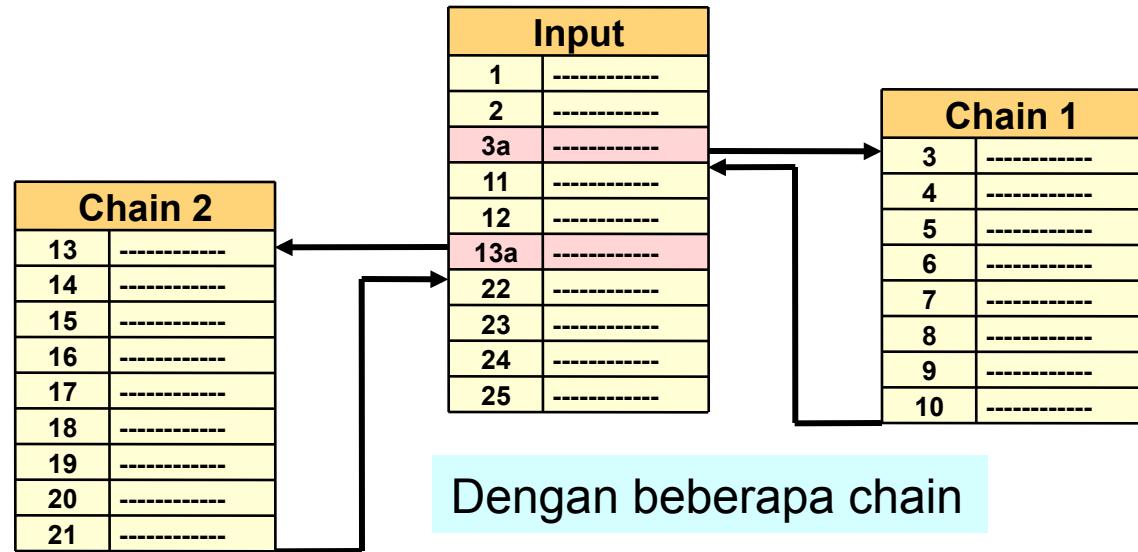
Mangle Action

- **accept** - Paket data yang datang ke chain diterima dan tidak dicek lagi di rule bawahnya serta langsung keluar dari chain.
- **jump** – Paket data akan dilempar ke chain lain sesuai parameter **Jump-Target**.
- **return** – Paket data akan dikembalikan ke chain asal sesuai urutan rule firewall jump sebelumnya.
- **log** – akan menambahkan informasi paket di system log
- **passthrough** – mengabaikan rule dan akan diteruskan ke rule dibawahnya.
- **add-dst-to-address-list** – menambahkan informasi dst-address dari paket ke address-list tertentu.
- **add-src-to-address-list** – menambahkan informasi src-address dari paket ke address-list tertentu.

Penggunaan “Jump” & Chain Tambahan

Input
1 -----
2 -----
3 -----
4 -----
5 -----
6 -----
7 -----
8 -----
9 -----
10 -----
11 -----
12 -----
13 -----
14 -----
15 -----
16 -----
17 -----
18 -----
19 -----
20 -----
21 -----
22 -----
23 -----
24 -----
25 -----

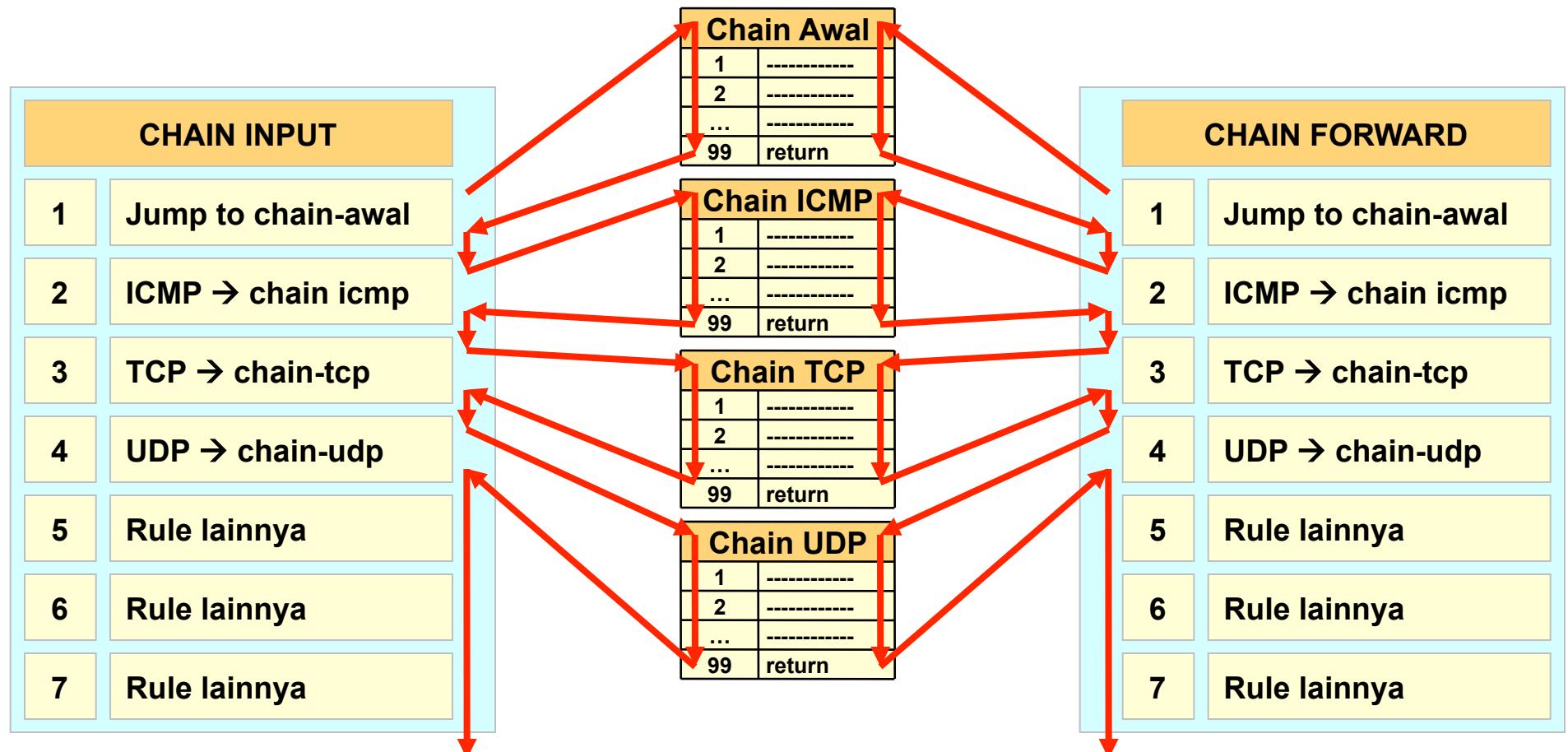
Tanpa chain tambahan,
hanya flat table



Dengan beberapa chain

Jika suatu trafik tidak memenuhi syarat parameter no 3a dan 13a, maka paket data tersebut tidak perlu dilewatkan rule pada chain 1 dan chain 2. Hal ini dapat menghemat beban CPU pada router.

Aplikasi Penggunaan Jump





More Mangle Actions

- **mark-connection** – melakukan penandaan paket “new” dari sebuah connection traffic.
- **mark-packet** – Menandai semua paket data yang melewati router sesuai klasifikasinya.
- **mark-routing** – Menandai paket data dan akan digunakan untuk menetukan routing dari paket tersebut.
- **change MSS** – Mengubah besar MSS dari paket di paket header.
 - biasanya digunakan untuk menghindari adanya fragmentasi pada paket data ketika menggunakan koneksi VPN.
- **change TOS** – Mengubah parameter TOS dari paket di paket header
- **change TTL** - Mengubah besar TTL dari paket di paket header
- **strip IPv4 options**



Parameter Firewall (General)

- **Chain Input**

- Tidak bisa memilih out-interface
- Untuk trafik yang menuju router (Local Proses)

- **Chain Forward**

- Bisa menentukan in-interface dan out-interface
- Untuk trafik yang melalui / melewati router

- **Chain Output**

- Tidak bisa memilih in-interface
- Untuk trafik yang berasal dari router (local proces)



Parameter Mangle

- **Chain Prerouting**

- Tidak bisa memilih out-interface
- Untuk trafik yang menuju router (local proces) dan melalui router

- **Chain Postrouting**

- Tidak bisa memilih in-interface
- Untuk trafik yang berasal dari router (local proces) dan yang melalui router



Connection Mark

- Dilakukan untuk proses request (pada paket pertama “NEW” dalam suatu koneksi)
- “Mutlak” digunakan untuk melakukan mangle per src-address pada jaringan dengan **src-nat** jika menggunakan chain prerouting.
- Sebaiknya digunakan untuk melakukan mangle berdasarkan protocol tcp dan dst-port
- Dilakukan sebelum packet-mark atau route-mark
- Setting **passthrough** biasanya “yes”



Packet Mark

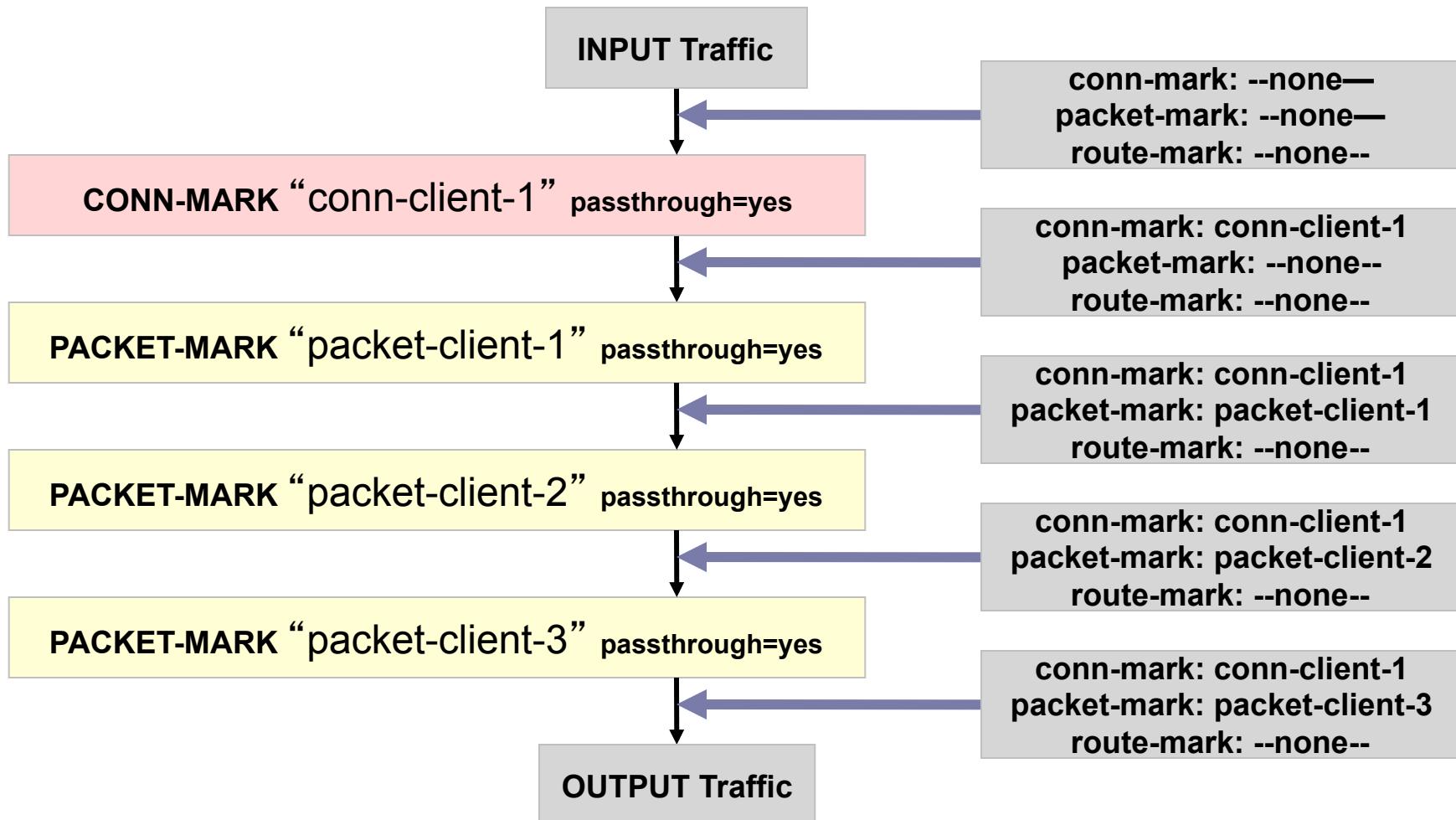
- Untuk jaringan dengan nat, dan untuk protokol tcp (dan dst port), sebaiknya dibuat berdasarkan conn-mark.
- Mark ini Dibuat untuk digunakan pada queue tree, simple queue, dan bisa juga filter.
- Setting **passthrough** biasanya “no”.



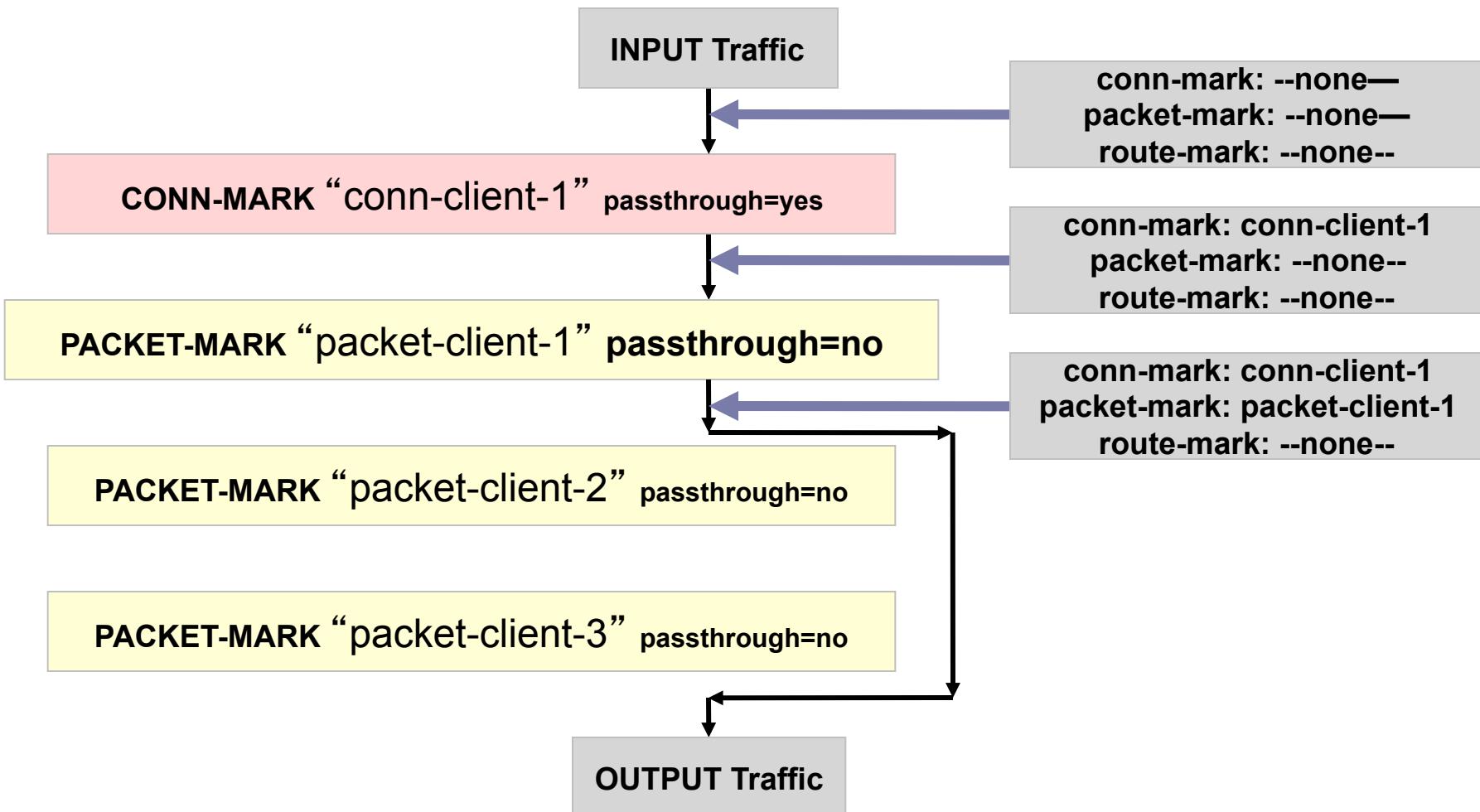
Route-Mark

- Dilakukan untuk penandaan pada **policy route / static route**
- Sebaiknya dibuat berdasarkan conn-mark supaya keutuhan koneksinya terjaga
- Hanya bisa dilakukan pada chain prerouting atau output, karena harus dilakukan sebelum proses **“routing decision”** atau **“routing adjustment”**
 - untuk trafik ke router → prerouting
 - trafik melalui router → prerouting
 - trafik dari router → output

Passthrough on Mangle

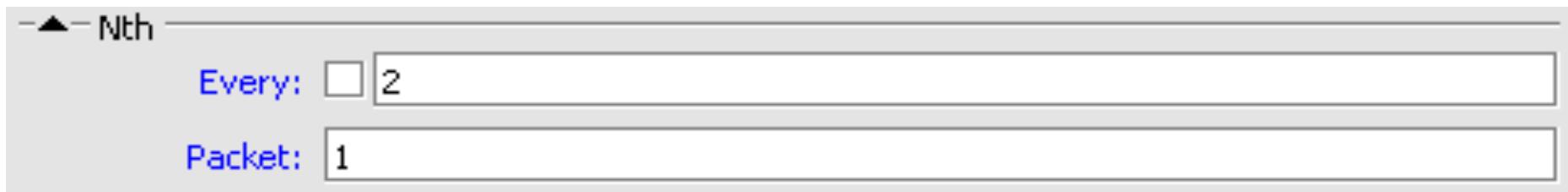


Passthrough on Mangle



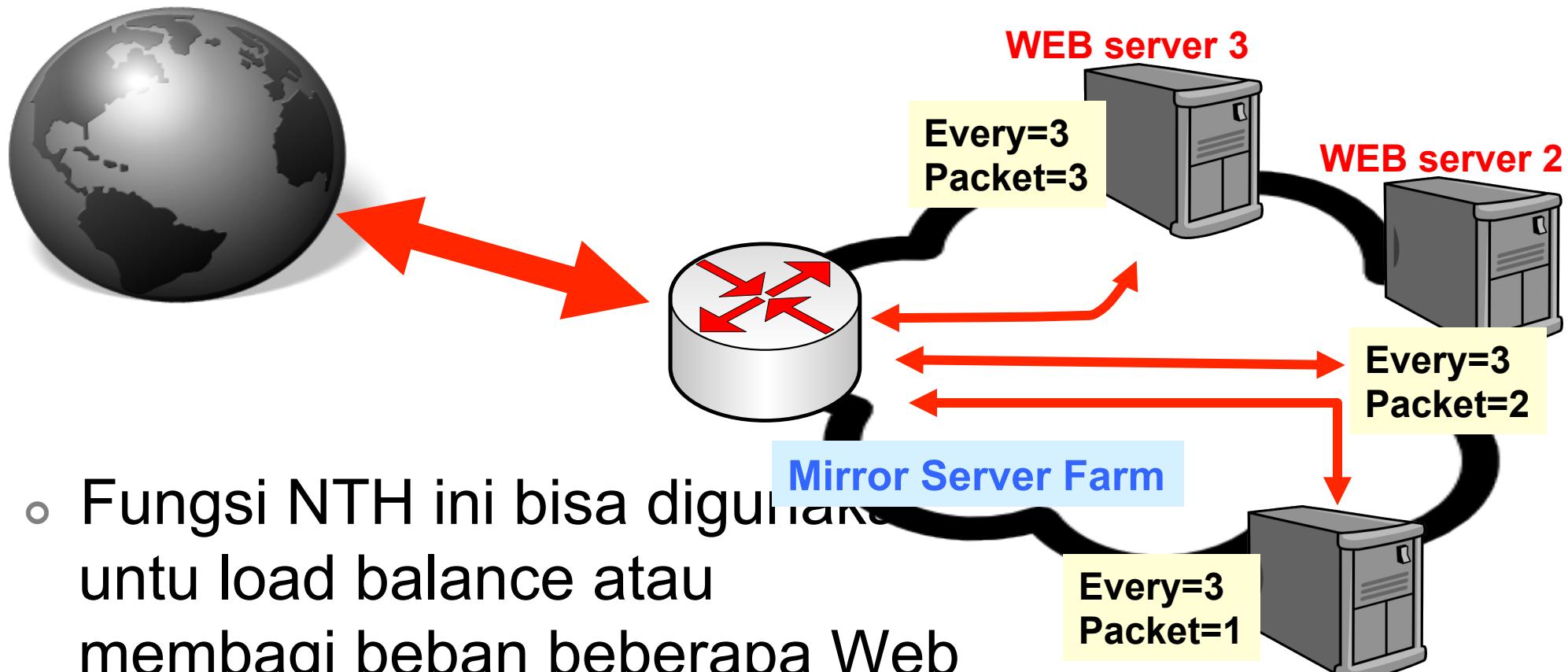
Mangle - NTH

- NTH adalah salah satu fitur firewall yang digunakan untuk penghitung “Counter” packet atau connection (packet new).
- Parameter “every” adalah parameter penghitung, sedangkan parameter “packet” adalah penunjuk paket keberapa rule tersebut akan dijalankan.



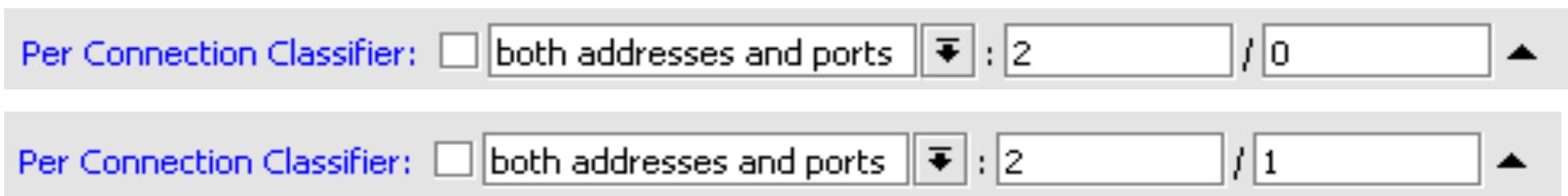
- Dari contoh di atas maka router akan menghitung semua paket yang lewat menjadi 1 dan 2, dan rule tersebut akan dijalankan pada paket 1.

NTH – Implementation Example



Mangle - PCC

- PCC adalah penyempurnaan dari NTH.
- Selain melakukan counter seperti NTH, PCC juga mampu mengingat dan menjaga karakteristik dari paket atau connection tertentu (src-address,dst-address,src-port,dst-port) untuk tetap menggunakan rule yang sama.
- Hal ini akan menjaga konsistensi dari sebuah counter.

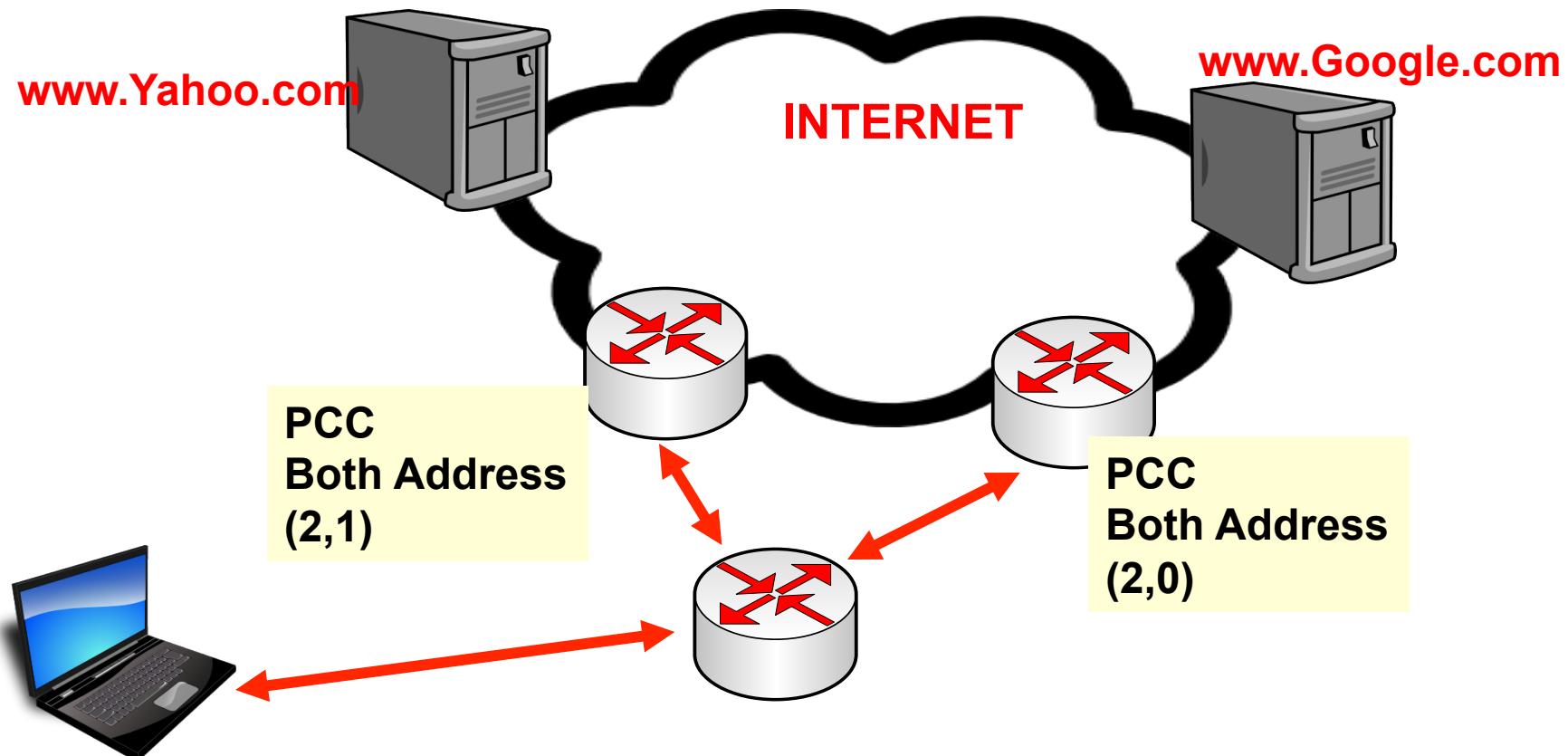


The image shows two identical configuration lines for 'Per Connection Classifier'. Each line includes a checkbox labeled 'both addresses and ports', a dropdown menu set to '2', and two input fields for '0' and '1'.

Per Connection Classifier: both addresses and ports : 2 / 0

Per Connection Classifier: both addresses and ports : 2 / 1

PCC – Implementation Example



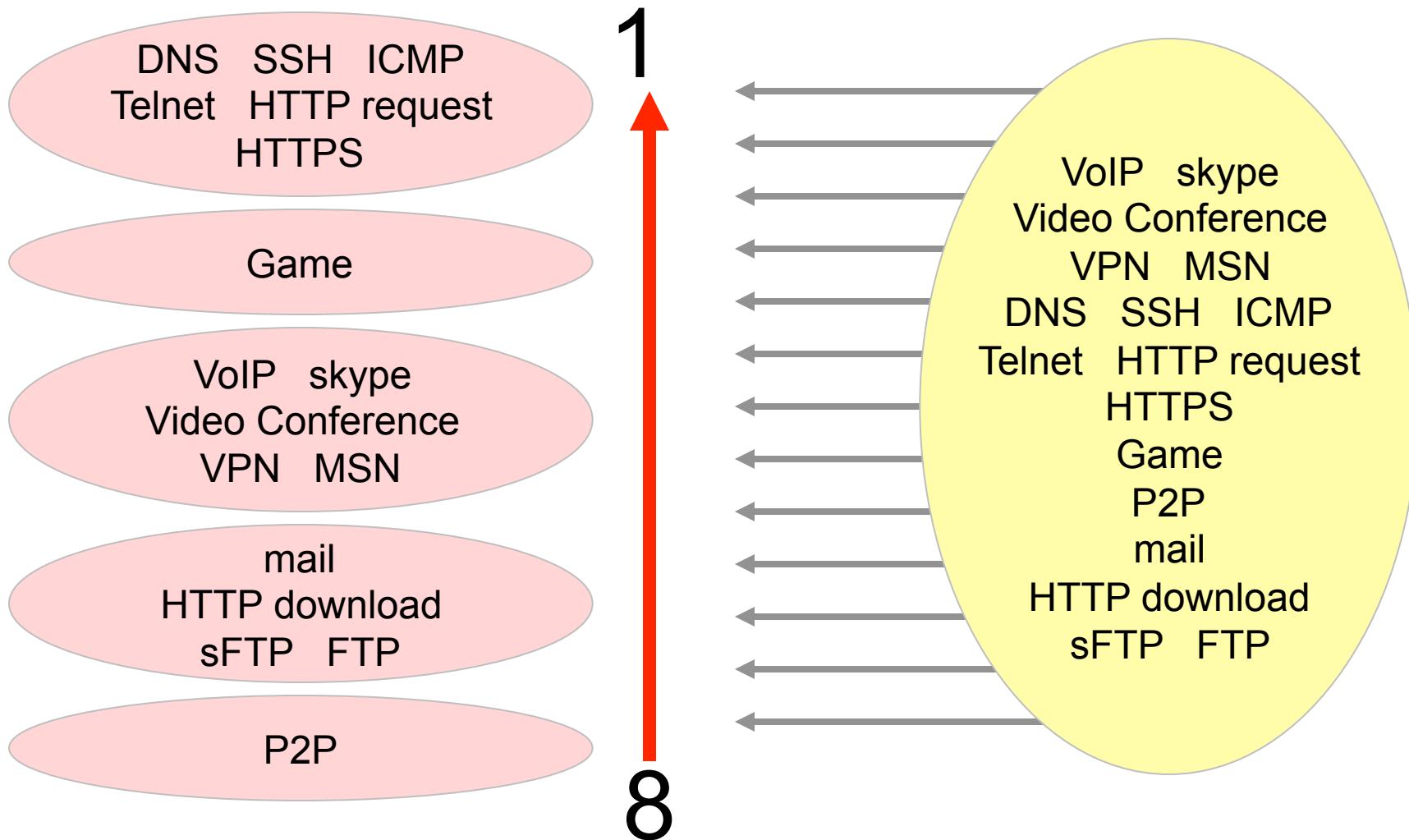
- Implementasi PCC sangat cocok untuk load balance beberapa Koneksi Internet.



[LAB-1] Mangle Protocol

- Buatlah mangle untuk mengidentifikasi trafik downstream berdasarkan protokol
- Kelompokkanlah protokol-protokol tersebut menjadi 5 grup berdasarkan prioritasnya
- Test setiap mangle traffic berdasarkan protocolnya sudah berjalan sesuai atau belum.
- Kemudian lakukan Backup !
 - */system backup save name="backup-mangle-prioritas"*

Rencana Prioritas



How to mark?

Group	Priority	Service	Protocol	Dst-Port	Other Conditions
P2P_services	8	P2P			p2p=all-p2p
Download services	7	Mails	TCP	110	
			TCP	995	
			TCP	143	
			TCP	993	
			TCP	25	
		HTTP downloads	TCP	80	Connection-bytes=500000-0
		FTP	TCP	20	
			TCP	21	
		SFTP	TCP	22	Packet-size=1400-1500
		DNS	TCP	53	
			UDP	53	
Ensign services	1	ICMP	ICMP	-	
		HTTPS	TCP	443	
		Telnet	TCP	23	
		SSH	TCP	22	Packet-size=0-1400
		HTTP requests	TCP	80	Connection-bytes=0-500000
User requests	3	Online game servers			dst-address-list of server
Communication services	5	VoIP			
		Skype			
		Video Conference			
		VPN			
		MSN			

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists

prerouting

Reset Counters **Reset All Counters**

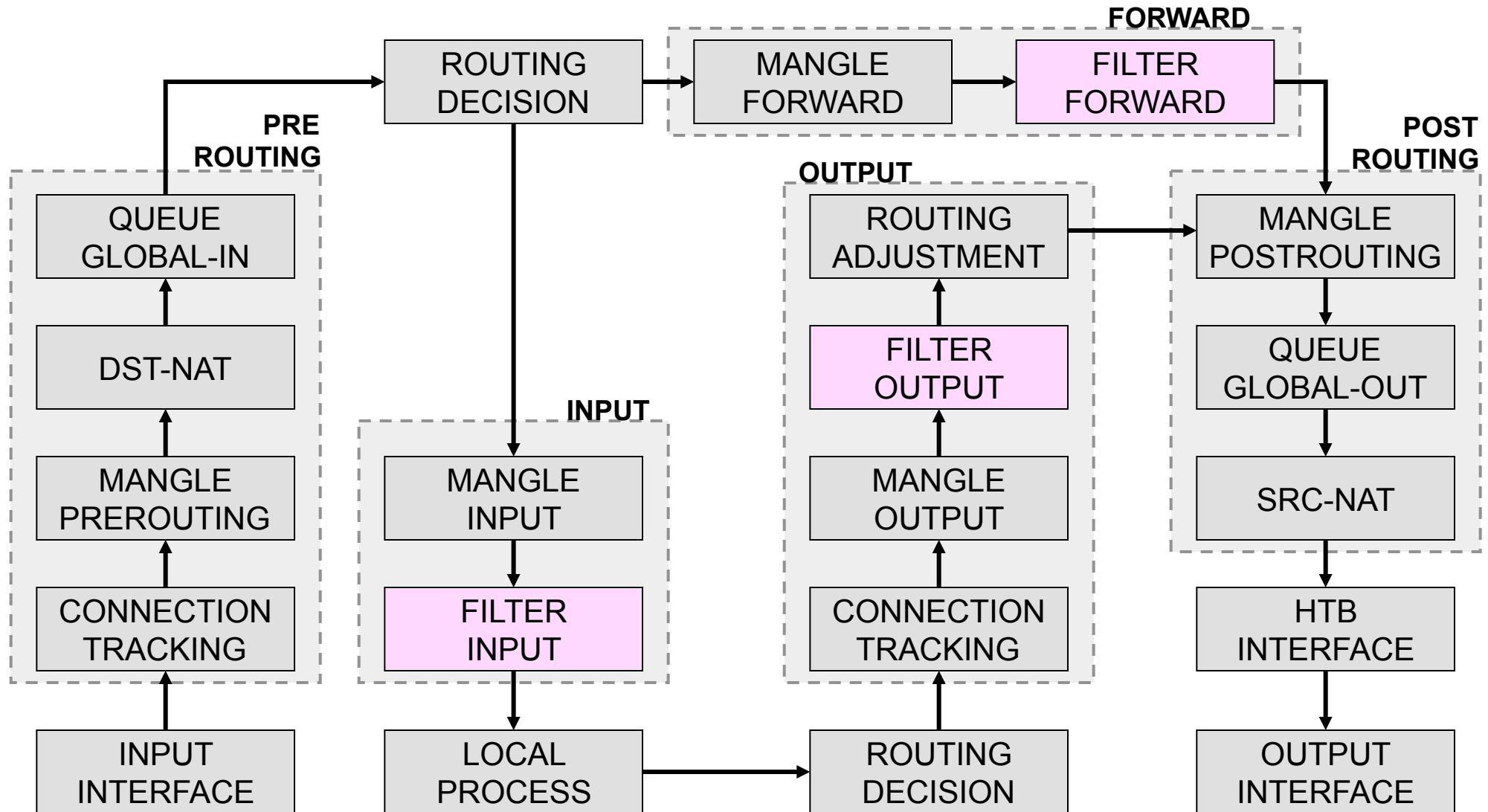
#	Action	Chain	Protocol	Src. Address List	Dst. Address List	New Packet Mark	P...	New Connection Mark	B
12	mark conn...	prerouting						prio_conn_p2p	17.5
13	mark packet	prerouting				prio_p2p_packet	no		17.4
14	mark conn...	prerouting	6 (tcp)					prio_conn_download...	0
15	mark conn...	prerouting	6 (tcp)					prio_conn_download...	0
16	mark conn...	prerouting	6 (tcp)					prio_conn_download...	0
17	mark conn...	prerouting	6 (tcp)					prio_conn_download...	0
18	mark conn...	prerouting	6 (tcp)					prio_conn_download...	0
19	mark conn...	prerouting	6 (tcp)					prio_conn_download...	0
20	mark conn...	prerouting	6 (tcp)					prio_conn_download...	0
21	mark conn...	prerouting	6 (tcp)					prio_conn_download...	0
22	mark packet	prerouting				prio_download_packet	yes		0
23	mark conn...	prerouting	6 (tcp)					prio_conn_ensign_se...	0
24	mark conn...	prerouting	17 (udp)					prio_conn_ensign_se...	0
25	mark conn...	prerouting	1 (icmp)					prio_conn_ensign_se...	0
26	mark conn...	prerouting	6 (tcp)					prio_conn_ensign_se...	0
27	mark conn...	prerouting	6 (tcp)					prio_conn_ensign_se...	36.2
28	mark conn...	prerouting	6 (tcp)					prio_conn_ensign_se...	36.2
29	mark conn...	prerouting	6 (tcp)					prio_conn_ensign_se...	0
30	mark packet	prerouting				prio_ensign_packet	no		0
31	mark conn...	prerouting			user_request			prio_conn_user_servi...	0
32	mark packet	prerouting				prio_request_packet	yes		0
33	mark conn...	prerouting	6 (tcp)					prio_conn_comm_ser...	0
34	mark conn...	prerouting	6 (tcp)					prio_conn_comm_ser...	0
35	mark conn...	prerouting	4 (ipen...					prio_conn_comm_ser...	0
36	mark conn...	prerouting	47 (gre)					prio_conn_comm_ser...	0
37	mark conn...	prerouting	94 (ipip)					prio_conn_comm_ser...	0
38	mark conn...	prerouting	98 (enc...					prio_conn_comm_ser...	0
39	mark packet	prerouting				prio_comm_packet	no		0



Firewall Filter

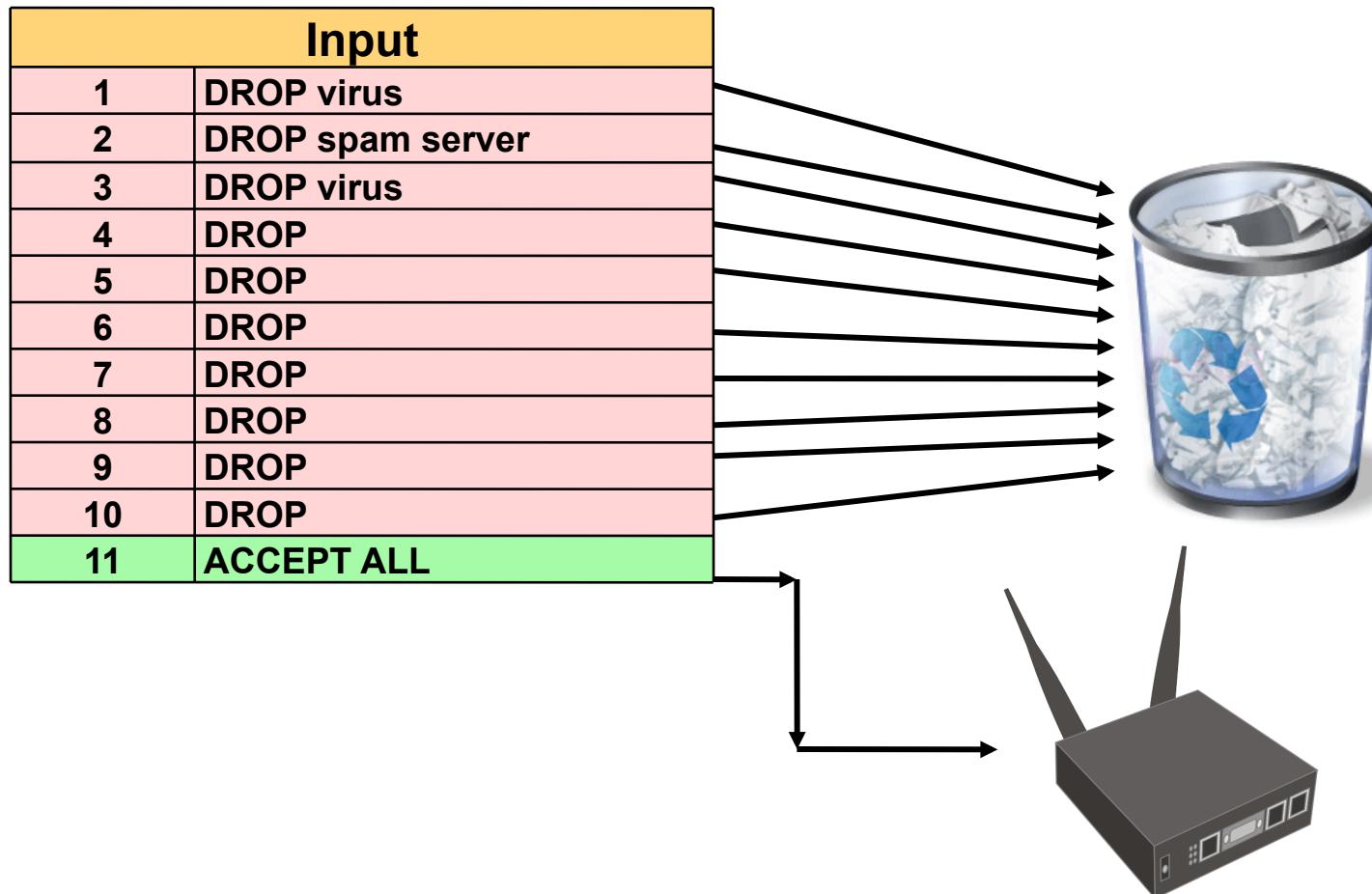
- Adalah cara untuk memfilter paket, dilakukan untuk meningkatkan keamanan jaringan, dan mengatur flow data dari, ke client, ataupun router
- Hanya bisa dilakukan pada chain **Input, Output, Forward**
- By default: policy untuk semua traffic yang melewati router adalah **accept**.

Filter - Packet Flow



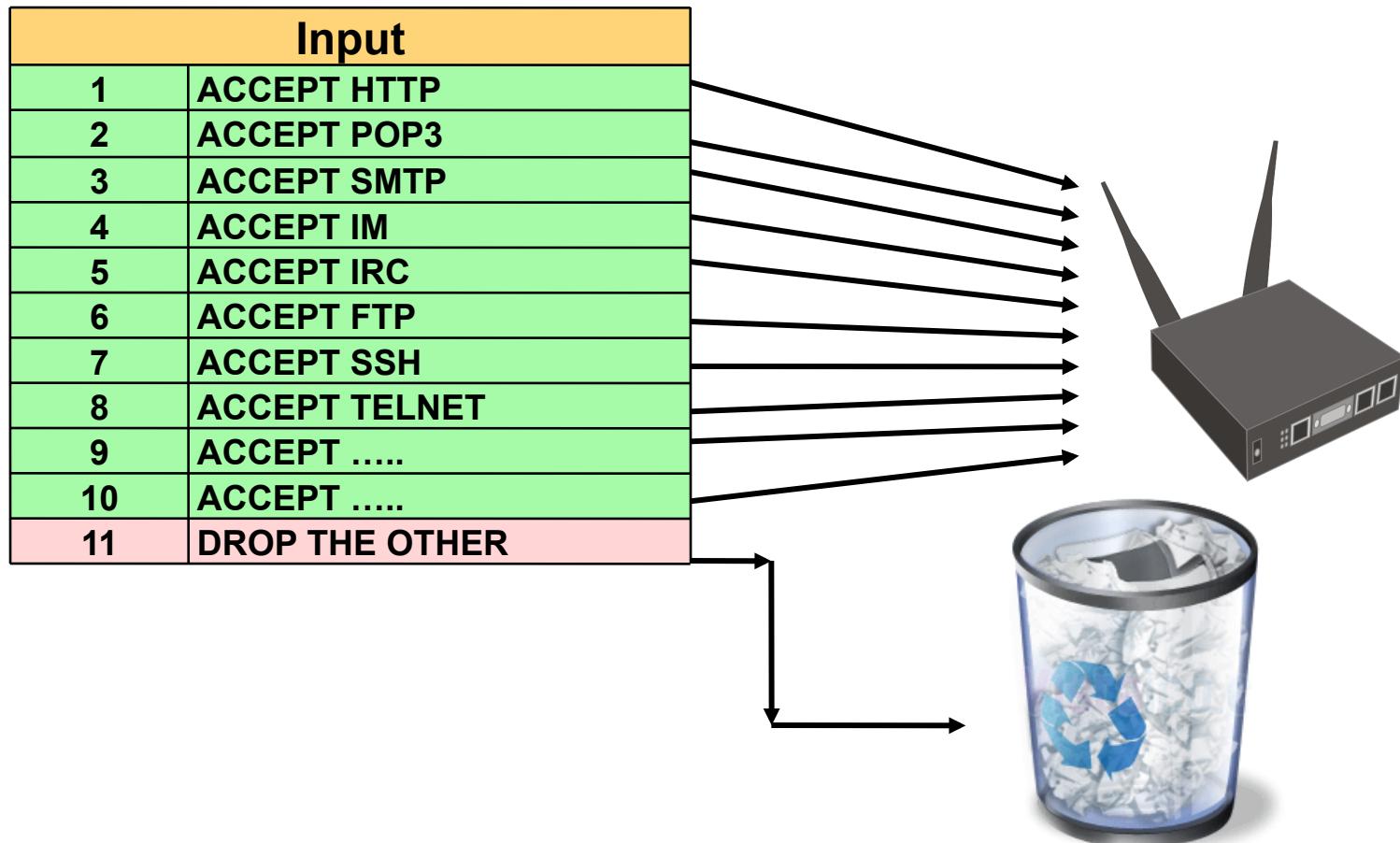
Firewall Tactics (1)

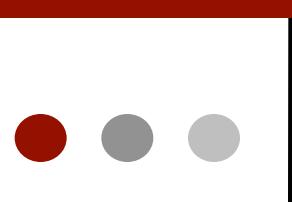
Drop all unneeded, accept everything else



Firewall Tactics (2)

Accept only needed, drop everything else





RouterOS v3 Services

PORT	PROTOCOL	DESCRIPTION
1	20	tcp
2	21	tcp
3	22	tcp
4	23	tcp
5	53	tcp
6	80	tcp
7	179	tcp
8	443	tcp
9	646	tcp
10	1080	tcp
11	1723	tcp
12	1968	tcp
13	2000	tcp
14	2210	tcp
15	2211	tcp
16	2828	tcp
17	3128	tcp
18	8291	tcp
19	8728	tcp
20	---	/1
21	---	/2
22	---	/4

PORT	PROTOCOL	DESCRIPTION
23	53	udp
24	123	udp
25	161	udp
26	500	udp
27	520	udp
28	521	udp
29	646	udp
30	1698	udp
31	1699	udp
32	1701	udp
33	1812	udp
34	1813	udp
35	1900	udp
36	1966	udp
37	5678	udp
38	---	/46
39	---	/47
40	---	/50
41	---	/51
42	---	/89
43	---	/103
44	---	/112



Bogon IP Address

- /ip firewall address-list
- add list=BOGONS address=192.168.0.0/16
- add list=BOGONS address=10.0.0.0/8
- add list=BOGONS address=172.16.0.0/12
- add list=BOGONS address=169.254.0.0/16
- add list=BOGONS address=127.0.0.0/8
- add list=BOGONS address=224.0.0.0/3
- add list=BOGONS address=223.0.0.0/8
- add list=BOGONS address=198.18.0.0/15
- add list=BOGONS address=192.0.2.0/24
- add list=BOGONS address=185.0.0.0/8
- add list=BOGONS address=180.0.0.0/6
- add list=BOGONS address=179.0.0.0/8
- add list=BOGONS address=176.0.0.0/7
- add list=BOGONS address=175.0.0.0/8
- add list=BOGONS address=104.0.0.0/6
- add list=BOGONS address=100.0.0.0/6
- add list=BOGONS address=49.0.0.0/8
- add list=BOGONS address=46.0.0.0/8
- add list=BOGONS address=42.0.0.0/8
- add list=BOGONS address=39.0.0.0/8
- add list=BOGONS address=36.0.0.0/7
- add list=BOGONS address=31.0.0.0/8
- add list=BOGONS address=27.0.0.0/8
- add list=BOGONS address=23.0.0.0/8
- add list=BOGONS address=14.0.0.0/8
- add list=BOGONS address=5.0.0.0/8
- add list=BOGONS address=2.0.0.0/8
- add list=BOGONS address=0.0.0.0/7
- add list=BOGONS address=128.0.0.0/16

Address List

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists

	Name	Address
●	not_in_internet	0.0.0.0/8
●	not_in_internet	172.16.0.0/12
●	not_in_internet	192.168.0.0/16
●	not_in_internet	10.0.0.0/8
●	not_in_internet	169.254.0.0/16
●	not_in_internet	127.0.0.0/8
●	not_in_internet	224.0.0.0/3

all

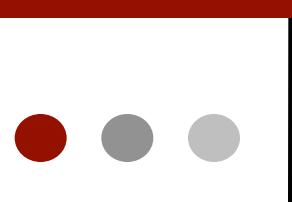
Firewall Address List <not_in_internet>

Name: not_in_internet

Address: 0.0.0.0/8

OK Cancel Apply Disable Comment Copy Remove

disabled

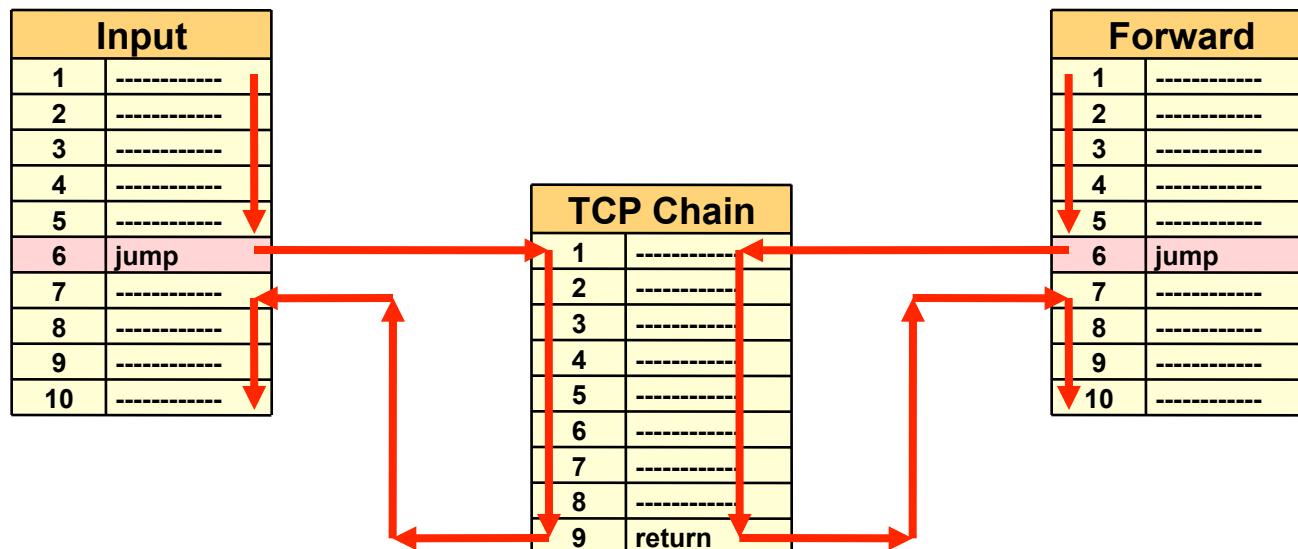


[LAB-2] IP Filtering

- Buatlah firewall filter untuk melakukan:
 - Mengijinkan paket data established dan related
 - Memblok paket data invalid
 - Mengijinkan paket menuju network apabila:
 - dari IP Address publik yang valid
 - menuju IP Address client yang valid
- Mengijinkan paket keluar dari network apabila:
 - menuju IP Address publik yang valid
 - dari IP Address client yang valid

Penggunaan Chain tambahan

Chain tambahan dapat digunakan sebagai target jump dari beberapa chain default, sehingga kita tidak perlu menulis rule yang sama dua kali.





Action Filter (1)

- **accept** – paket diterima dan tidak melanjutkan membaca baris berikutnya
- **drop** – menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP)
- **reject** – menolak paket dan mengirimkan pesan penolakan ICMP
- **tarpit** – menolak, tetapi tetap menjaga TCP connections yang masuk (membalas dengan SYN/ACK untuk paket TCP SYN yang masuk)
- **log** – menambahkan informasi paket data ke log



Action Filter (2)

- **add-dst-to-address-list** – menambahkan IP Address tujuan ke dalam daftar **address-list** tertentu
- **add-src-to-address-list** - menambahkan IP Address asal ke dalam daftar **address-list** tertentu
- **jump** – berpindah ke chain lainnya, sesuai dengan parameter **jump-target**
- **return** – kembali ke chain sebelumnya (jika sudah mengalami **jump**)
- **passthrough** – tidak melakukan action apapun, melanjutkan ke baris berikutnya



Parameter Filter (General) 1

- Chain input
 - Tidak bisa memilih out-interface
 - Untuk trafik yang menuju router
- Chain forward
 - Bisa menentukan in-interface dan out-interface
 - Untuk trafik yang melalui router
- Chain output
 - Tidak bisa memilih in-interface
 - Untuk trafik yang berasal dari router



Parameter Filter (General) 2

- Penulisan **src-address** dan **dst-address**:
 - Satu alamat IP (192.168.0.1)
 - Blok alamat IP (192.168.0.0/24)
 - IP range (192.168.0.1-192.168.0.32)



Parameter Filter (General) 2

- Pemilihan port hanya bisa dilakukan pada protokol tertentu, misalnya TCP dan UDP
- Port bisa dituliskan dengan :
 - single port (contoh: 80)
 - port range (contoh: 1-1024)
 - multi port (contoh: 21,22,23,25)
- **any-port** = sesuai dengan (salah satu) src-port atau dst-port
- Contoh untuk trafik http
 - Untuk memblok **request** http, digunakan **dst-port=80**
 - Untuk memblok **response** http, digunakan **src-port=80**
 - Untuk memblok **keduanya**, digunakan **any-port=80**



Parameter Filter (interface)

- Jika router menggunakan mode routing, parameter **in/out bridge port** tidak digunakan.
- Jika router menggunakan mode bridge:
 - **In/out interface** → gunakan nama bridge (contoh: bridge1)
 - **In/out bridge port** → gunakan nama interface fisik (contoh: ether1, ether2)



Parameter Filter (Advanced)(1)

- **src-mac-address** hanya dapat digunakan jika client terkoneksi langsung ke router (tidak bisa jika sudah melalui router lainnya)
- **random** → action hanya akan dilakukan secara random, dengan kemungkinan sesuai parameter yang ditentukan (1-99)
- **ingress-priority** → priority yang didapatkan dari protokol VLAN atau WMM (0-63)



Parameter Filter (Advanced)(2)

- **connection-byte**

- merupakan range dari besar data yang lewat di suatu koneksi, bukan angka tunggal
contoh: 100000-45000000
(kita tidak pernah tahu berapa tepatnya besar conn-byte yang akan lewat)
- Untuk jaringan dengan src-nat, sulit diimplementasikan untuk downlink dengan parameter IP Address client (membutuhkan connection mark), karena conn-track dilakukan sebelum pembalikan nat di prerouting.



Parameter Filter (Advanced)(3)

- **packet-size** → besarnya packet data yang lewat, untuk mendeteksi besar packet.
- **L7 protocol** → sesuai dengan namanya layer 7 protokol, yaitu tool untuk mengklasifikasikan paket data sesuai dengan aplikasinya (Layer OSI 7).
- L7 dijelaskan di Sesi yang lain.



Parameter Filter (Advanced)(4)

- **icmp-type**

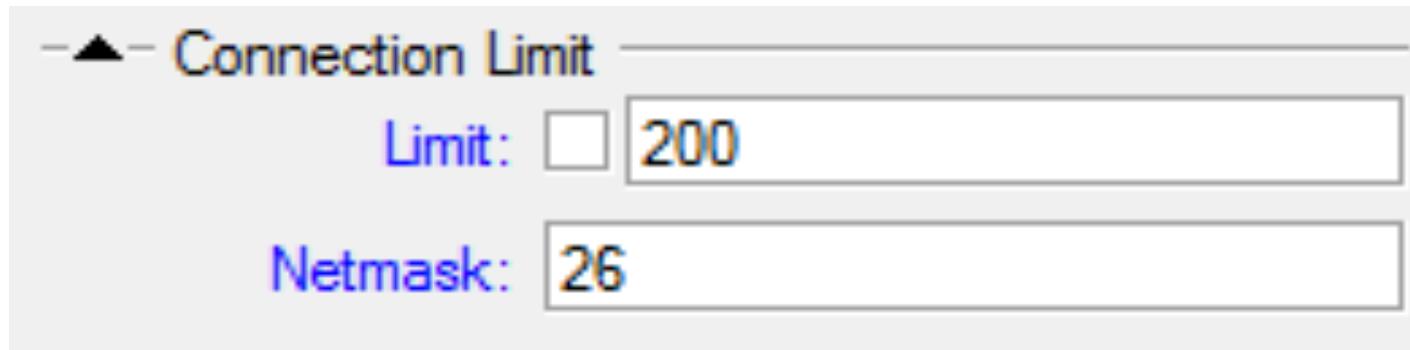
- icmp type yang biasa digunakan :
 - PING – message 0:0 dan 8:0
 - TRACEROUTE – message 11:0 dan 3:3
 - Path MTU discovery – message 3:4
- type lainnya sebaiknya di blok.

- **Contoh block Traceroute only :**

- /ip firewall filter chain=forward action=drop protocol=icmp icmp-options=11:0
- /ip firewall filter chain=forward action=drop protocol=icmp icmp-options=3:3

Parameter Filter (Extra)

- connection-limit
 - membatasi jumlah koneksi per IP Address atau per blok IP address
 - contoh:
membatasi 200 koneksi untuk setiap /26



The image shows a configuration dialog for 'Connection Limit'. At the top, there is a title 'Connection Limit' with a small up/down arrow icon to its left. Below the title, there are two input fields. The first field is labeled 'Limit:' and contains the value '200'. The second field is labeled 'Netmask:' and contains the value '26'.

- Dari rule diatas maka rule akan dijalankan ketika connection dibawah 200.



[LAB-3] DoS Attack

- IP Address yang memiliki 10 koneksi ke router dapat “diasumsikan” sebagai pelaku DoS Attack
- Jika kita mendrop TCP connection, berarti kita mengijinkan penyerang untuk membuat koneksi yang baru
- Untuk membloknya, kita menggunakan tarpit



IDM Detection

- Fungsi ini bisa sangat berguna untuk mendeteksi adanya program downloader yang aktif.
- `/ip firewall filter add action=accept chain=forward comment="IDM Detection" connection-limit!=15,32 dst-port=80 protocol=tcp src-address=192.168.X.0/24`
- `/ip firewall filter add action=add-src-to-address-list address-list=idm address-list-timeout=5m chain=forward connection-limit=100,32 dst-port=80 protocol=tcp src-address=192.168.X.0/24`
- `/ip firewall filter add action=accept chain=forward connection-limit!=8,32 dst-port=20-21 protocol=tcp src-address=192.168.X.0/24`
- `/ip firewall filter add action=add-src-to-address-list address-list=idm address-list-timeout=5m chain=forward connection-limit=100,32 dst-port=20-21 protocol=tcp src-address=192.168.X.0/24`

Parameter Filter (Extra)

- limit

- membatasi paket data, biasanya untuk paket data non-connection
- contoh: data icmp





[LAB-4] ICMP Flood Lab

- Buatlah chain baru “ICMP”
- Buatlah pada chain **icmp** rule untuk meng-accept 5 tipe icmp yang memang digunakan pada jaringan
- Buatlah pada chain **icmp** limit 5 pps dengan 5 paket burst, dan drop icmp berikutnya
- Buatlah rule jump ke chain icmp dari chain input dan chain forward
- Test flood menggunakan fungsi **/tool flood-ping**



Parameter Filter (Extra)

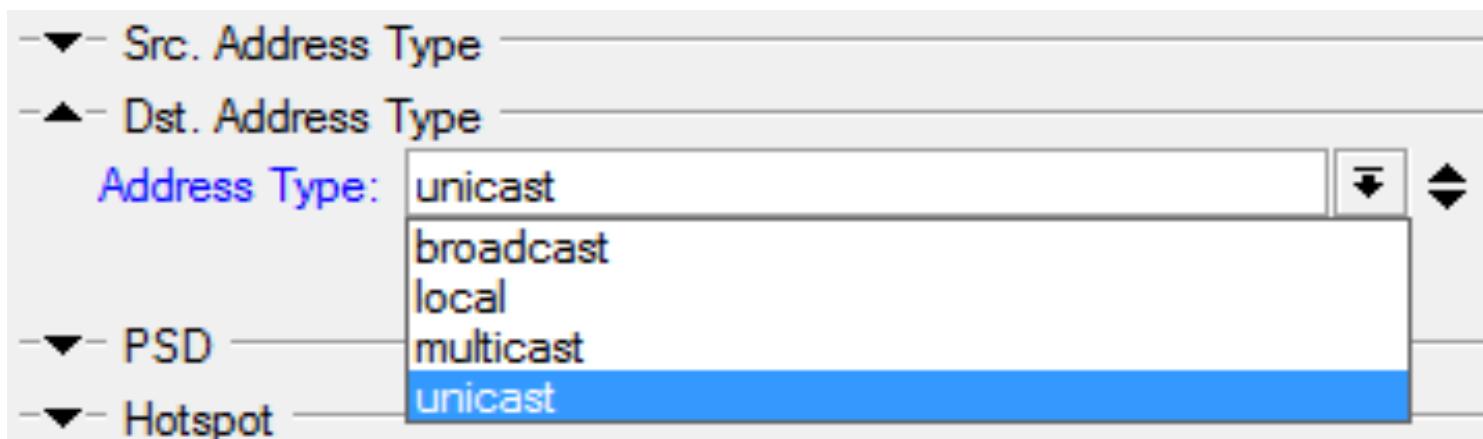
- **dst-limit**

- melimit jumlah paket per detik untuk setiap IP Address tujuan atau port tujuan
- clasifier :
 - addresses and dst-port
 - dst-address
 - dst-address and dst-port
 - src-address and dst-address
- expire :
 - waktu kapan router akan melupakan informasi per classifier

Parameter Filter (Extra)

- **src/dst-address-type:**

- **unicast** – IP Address yang biasa kita gunakan
- **local** – jika IP Address tsb terpasang pada router
- **broadcast** – IP Address broadcast
- **multicast** – IP yang digunakan untuk transmisi multicast



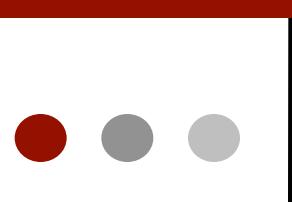
Parameter Filter (Extra)

◦ PSD (Port Scan Detection)

- untuk mengetahui adanya port scan (TCP)
- low port : 0 – 1023
- high port : 1024 - 65535

—▲— PSD

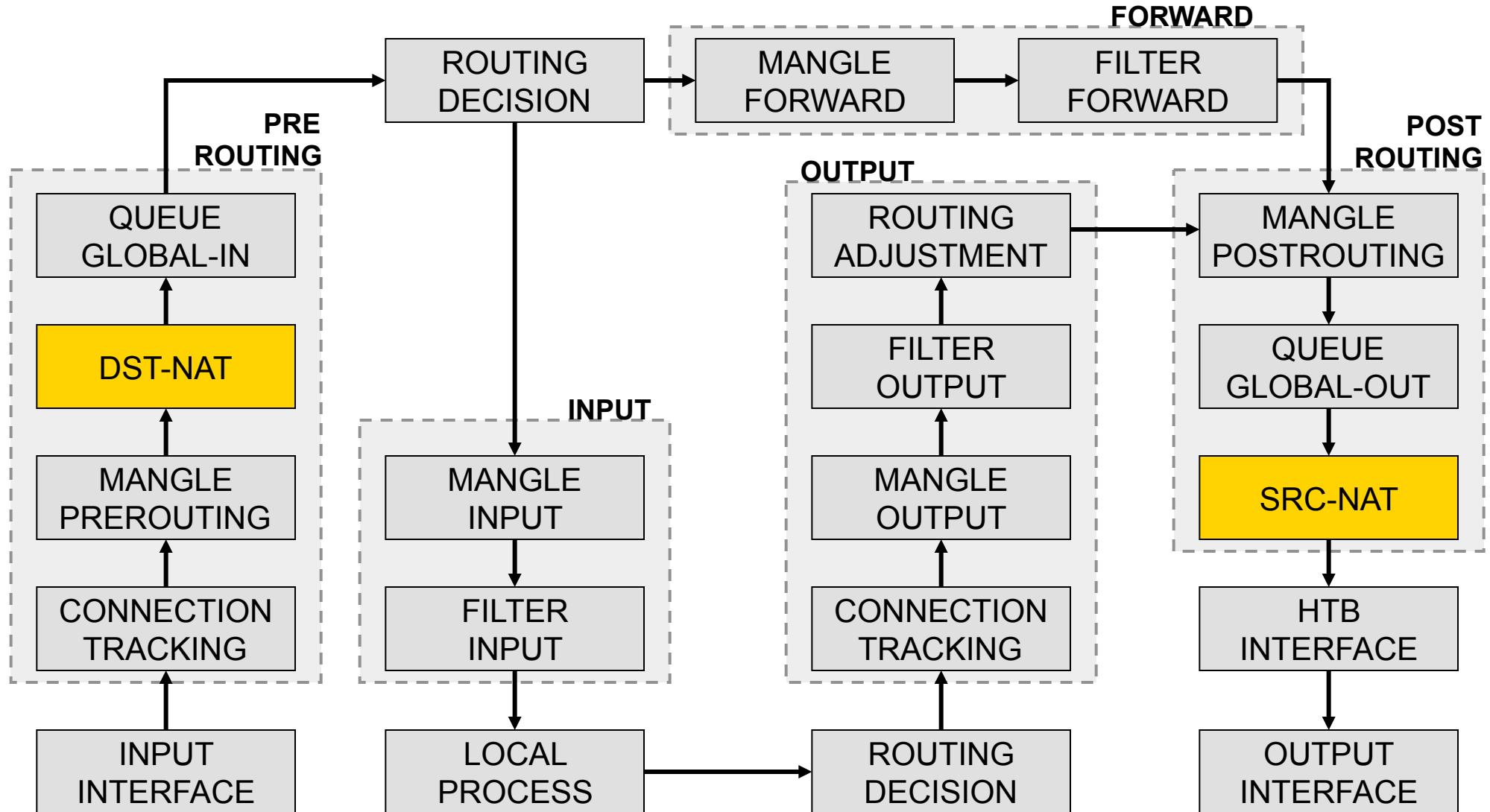
Weight Threshold:	21
Delay Threshold:	00:00:03
Low Port Weight:	3
High Port Weight:	1



NAT

- Merupakan proses manipulasi packet header, terutama pada parameter 32-bit-src-address dan 32-bit-dst-address.
- Khusus untuk src-nat, akan dilakukan proses otomatis pembalikan (dst-nat) pada pre-routing.
- Setelah paket data pertama dari sebuah connection terkena NAT, maka paket berikutnya pada connection tersebut otomatis terkena NAT

NAT - Packet Flow





Chain srcnat

- Untuk menyembunyikan IP Address lokal dan menggantikannya dengan IP Address publik yang sudah terpasang pada router
- **src-nat**
 - Kita bisa memilih IP Address publik yang digunakan untuk menggantikan.
- **masquerade**
 - Secara otomatis akan menggunakan IP Address pada interface publik.
 - Digunakan untuk mempermudah instalasi dan bila IP Address publik pada interface publik menggunakan IP Address yang dinamik (misalnya DHCP, PPTP atau EoIP)

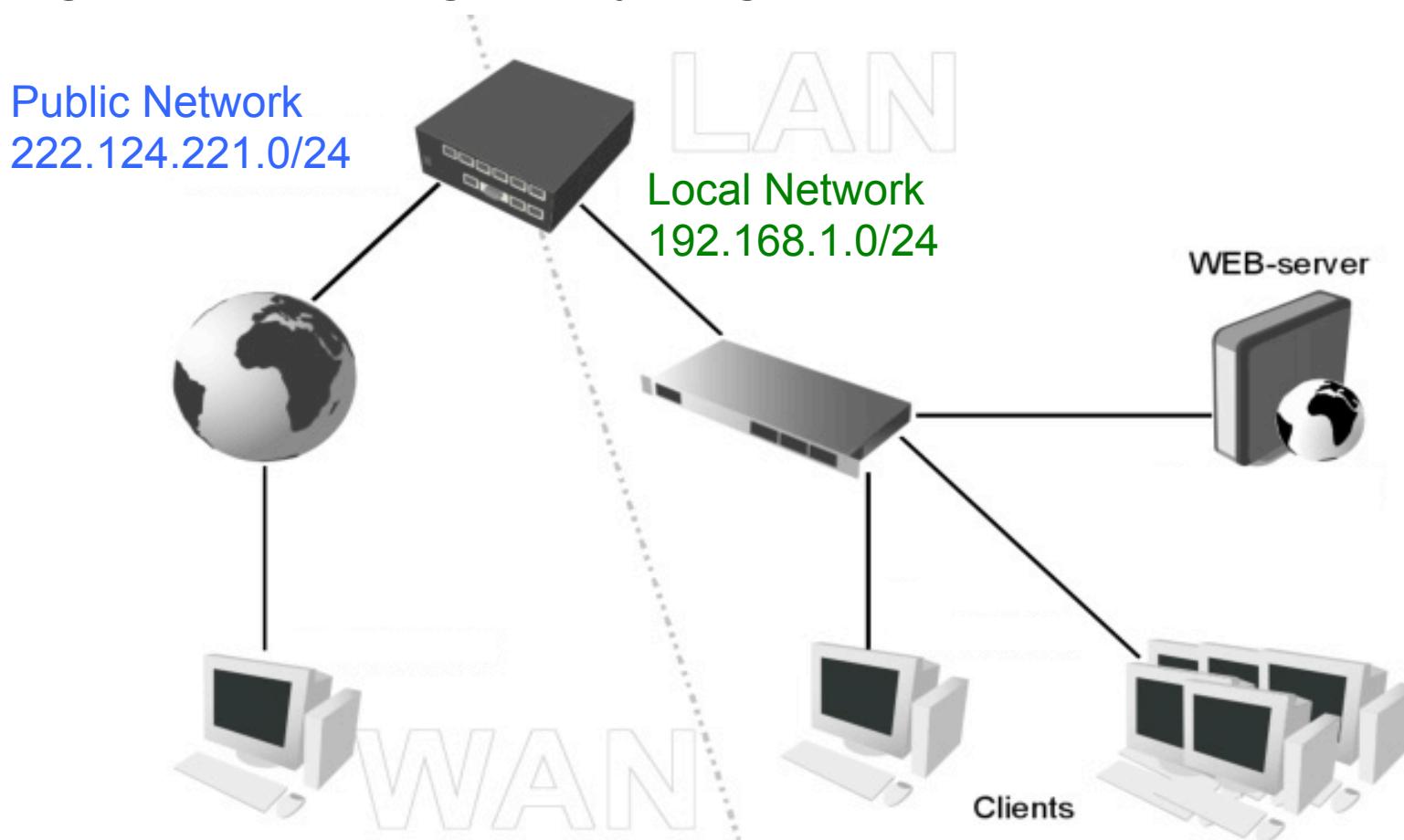


Chain dstnat

- Untuk melakukan penggantian IP Address tujuan, atau mengarahkan koneksi ke localhost.
- **dst-nat**
 - Kita bisa mengganti IP Address dan port tujuan dari sebuah koneksi.
- **redirect**
 - Untuk mengalihkan koneksi yang tadinya melwati router, dan dialihkan menuju ke localhost

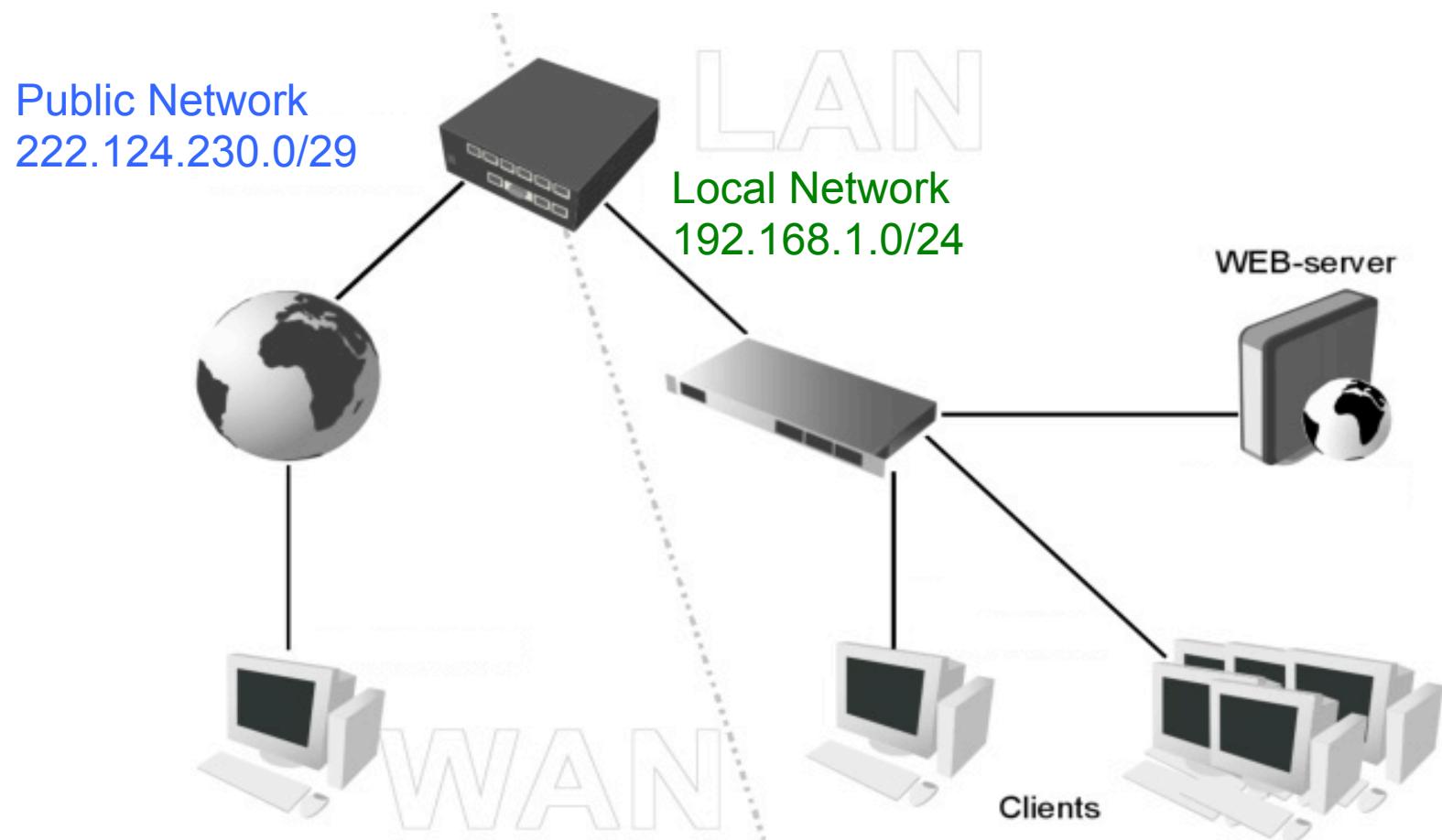
NAT – netmap

- **Netmap** – Melakukan mapping NAT 1:1 dari suatu range ip ke range ip yang lain.



NAT - same

- **Same** – Hampir sama dengan netmap tetapi range ip antara kedua network boleh berbeda. Router akan menjaga penggunaan kombinasi ip yang sama untuk koneksi yang sama.

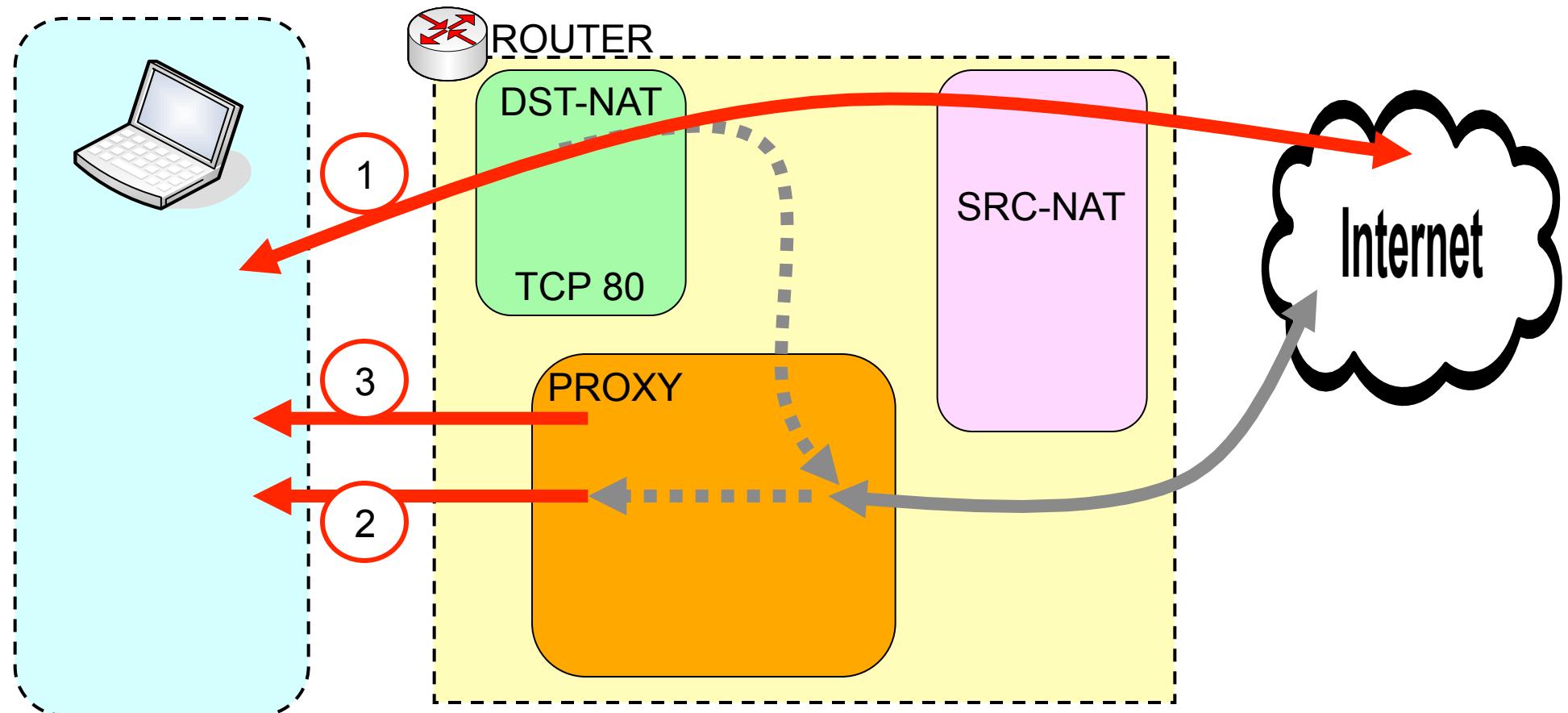




[LAB-5] Mangle... dan proxy

- Pada router terdapat proxy server
- Buatlah mangle trafik internet yang:
 - direct
 - melalui proxy : HIT
 - melalui proxy : MISS

Proxy (single gateway)



1 Direct

2 MISS

3 HIT



Proxy – HIT - MISS

- Web Proxy bertugas menyimpan data file yang diakses user, dan memberikan kepada user berikutnya jika mengakses file yang sama.
 - Jika tersedia di cache Akan langsung diberikan disebut HIT
 - Jika tidak tersedia, proxy akan meminta ke server, menyimpannya di cache, dan memberikan ke client disebut MISS

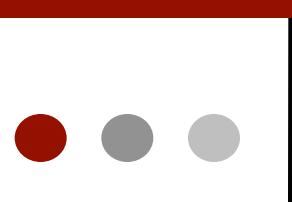


Pengenalan HIT

- Jika terjadi akses HIT di proxy, proxy akan memberikan nilai TOS = 4 (nilai 4 bisa diubah sesuai kebutuhan)
- Nilai TOS = 4 ini bisa digunakan sebagai parameter pada Mangle.

Setting Mangle

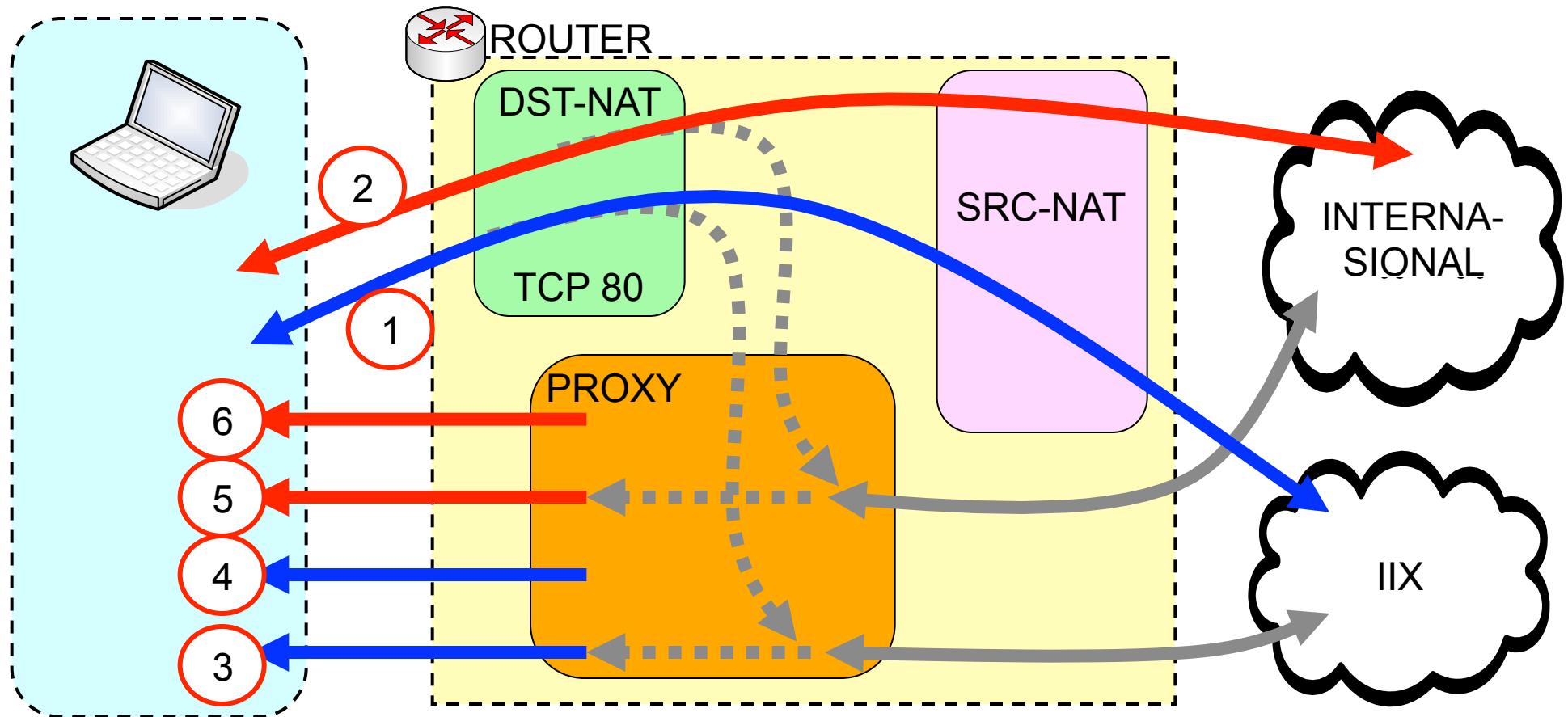
- 0 chain=prerouting action=mark-connection new-connection-mark=conn-client passthrough=yes in-interface=ether1
- 1 chain=prerouting action=mark-packet new-packet-mark=packet-client passthrough=no connection-mark=conn-client
- 2 chain=output action=mark-packet new-packet-mark=packet-hit passthrough=no out-interface=ether1 connection-mark=conn-client dscp=4
- 3 chain=output action=mark-packet new-packet-mark=packet-client passthrough=no out-interface=ether1 connection-mark=conn-client dscp=!4



[LAB] Mangle... dual gateway

- Buatlah mangle untuk memisahkan gateway internasional dan gateway IIX.
- Pada router menjalankan web proxy.
- Koneksikan wlan2 ssid “training2” sebagai gateway IIX

Proxy dan Dual Gateway



1. Direct IIX
2. Direct Internasional
3. MISS IIX
4. HIT IIX
5. MISS Internasional
- 6 HIT Internasional

Pengaturan Dual Gateway

- Untuk memisahkan trafik domestik dan internasional, kita menggunakan daftar IP Address List NICE
→ www.mikrotik.co.id Download area

Script

Script IP Address NICE

Script untuk mengimport IP Address di router NICE ke Address-List NICE di RouterOS. Di generate pada 25 March 2009 17:17:34 WIB ... 631 lines.

[\[panduan\]](#)

[nice.rsc](#) (25.1 KByte, didownload 36796 kali)

Address List NICE

```
# Script untuk menambahkan IP Address BGP yang terdaftar di Router NICE (OIXP)
# ke RouterOS dalam ADDRESS-LIST dengan nama "nice"
# Script created by: Valens Riyadi @ www.mikrotik.co.id
# Generated at 25 March 2009 17:17:34 WIB ... 631 lines
# Generated in 32.736 seconds
# How-to: http://www.mikrotik.co.id/artikel_lihat.php?id=23

/sys note set show-at-login=yes note="Using nice.rsc from www.mikrotik.co.id, 25

/ip firewall address-list
add list=nice address="1.2.3.4"
remove [find list="nice"]
add list=nice address="114.120.0.0/13"
add list=nice address="114.56.0.0/14"
add list=nice address="125.166.0.0/15"
add list=nice address="125.162.0.0/16"
add list=nice address="125.163.0.0/16"
add list=nice address="125.160.0.0/16"
add list=nice address="125.161.0.0/16"
add list=nice address="125.164.0.0/16"
add list=nice address="125.165.0.0/16"
add list=nice address="120.163.0.0/16"
add list=nice address="120.162.0.0/16"
...
```

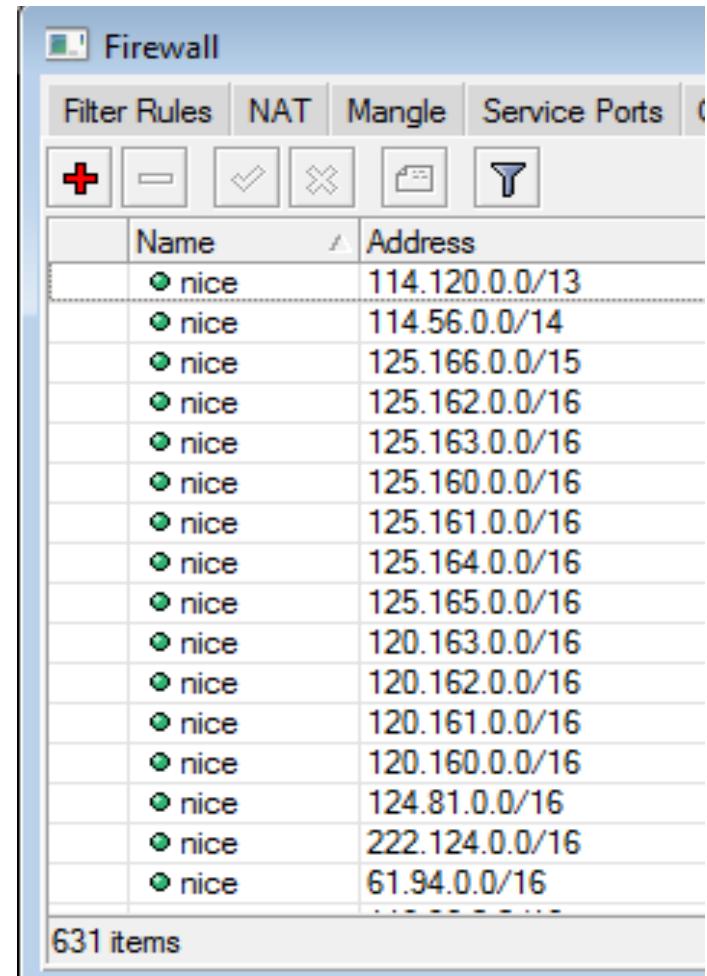


Import

- Copy ke router, lalu jalankan dengan perintah “/import nice.rsc”
- Copy-paste pada terminal
- Download otomatis :
lihat di :
http://www.mikrotik.co.id/artikel_lihat.php?id=23

Address-List

- Saat ini ada sekitar 1000-an baris address-list
- Daftar ini merupakan hasil optimasi dari 2000an baris pada BGP IIX
- Proses optimasi dilakukan setiap jam



The screenshot shows a screenshot of the MikroTik Winbox interface, specifically the Firewall Filter Rules table. The table lists 631 items, each with a green 'nice' icon, a 'Name' column (all entries are 'nice'), and an 'Address' column. The addresses listed are: 114.120.0.0/13, 114.56.0.0/14, 125.166.0.0/15, 125.162.0.0/16, 125.163.0.0/16, 125.160.0.0/16, 125.161.0.0/16, 125.164.0.0/16, 125.165.0.0/16, 120.163.0.0/16, 120.162.0.0/16, 120.161.0.0/16, 120.160.0.0/16, 124.81.0.0/16, 222.124.0.0/16, and 61.94.0.0/16.

Name	Address
• nice	114.120.0.0/13
• nice	114.56.0.0/14
• nice	125.166.0.0/15
• nice	125.162.0.0/16
• nice	125.163.0.0/16
• nice	125.160.0.0/16
• nice	125.161.0.0/16
• nice	125.164.0.0/16
• nice	125.165.0.0/16
• nice	120.163.0.0/16
• nice	120.162.0.0/16
• nice	120.161.0.0/16
• nice	120.160.0.0/16
• nice	124.81.0.0/16
• nice	222.124.0.0/16
• nice	61.94.0.0/16



Mangle 1

- 0 chain=prerouting action=mark-connection new-connection-mark=conn-client-int passthrough=yes dst-address-list=!nice in-interface=ether1
- 1 chain=prerouting action=mark-packet new-packet-mark=packet-client-int passthrough=no connection-mark=conn-client-int
- 2 chain=prerouting action=mark-connection new-connection-mark=conn-client-iix passthrough=yes dst-address-list=nice in-interface=ether1
- 3 chain=prerouting action=mark-routing new-routing-mark=route-iix passthrough=yes dst-address-list=nice connection-mark=conn-client-iix
- 4 chain=prerouting action=mark-packet new-packet-mark=packet-client-iix passthrough=no connection-mark=conn-client-iix



Mangle 2

- 5 chain=output action=mark-routing new-routing-mark=route-iix passthrough=no dst-address-list=nice
- 6 chain=output action=mark-packet new-packet-mark=packet-hit-int passthrough=no out-interface=ether1 connection-mark=conn-client-int dscp=4
- 7 chain=output action=mark-packet new-packet-mark=packet-client-int passthrough=no out-interface=ether1 connection-mark=conn-client-int dscp=!4
- 8 chain=output action=mark-packet new-packet-mark=packet-hit-iix passthrough=no out-interface=ether1 connection-mark=conn-client-iix dscp=4
- 9 chain=output action=mark-packet new-packet-mark=packet-client-iix passthrough=no out-interface=ether1 connection-mark=conn-client-iix dscp=!4



NAT

0 chain=srcnat action=masquerade out-interface=wlan1

1 chain=srcnat action=masquerade out-interface=wlan2

2 chain=dstnat action=redirect to-ports=8080 protocol=tcp in-interface=ether1 dst-port=80

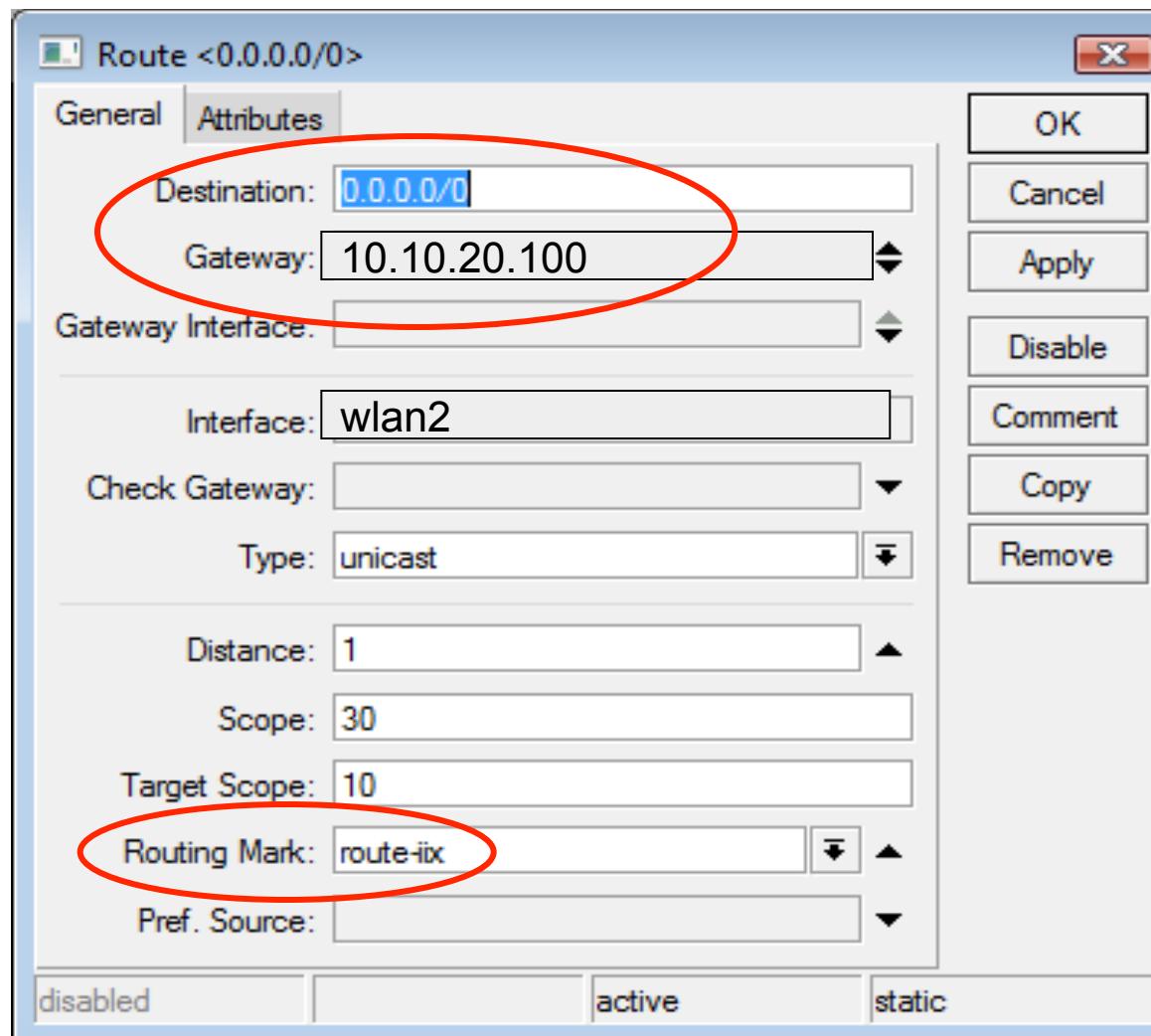


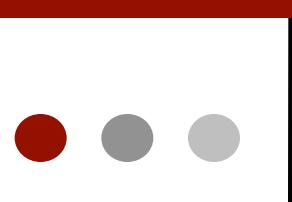
Route

```
0 dst-address=0.0.0.0/0 gateway=10.20.20.100  
distance=1 scope=30 routing-mark=route-iix
```

```
1 dst-address=0.0.0.0/0 gateway=10.10.10.100  
distance=1 scope=30
```

Policy Routing





Test!

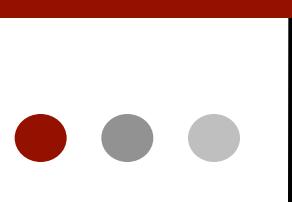
- Cek apakah ping ke IIX melalui gateway 2
- Cek apakah browsing ke IIX melalui gateway 2
- Lakukan backup !



L7 Filter



Certified Mikrotik Training - Advanced Class (MTCTCE)
Organized by: Citraweb Nusa Infomedia
(Mikrotik Certified Training Partner)



Outline

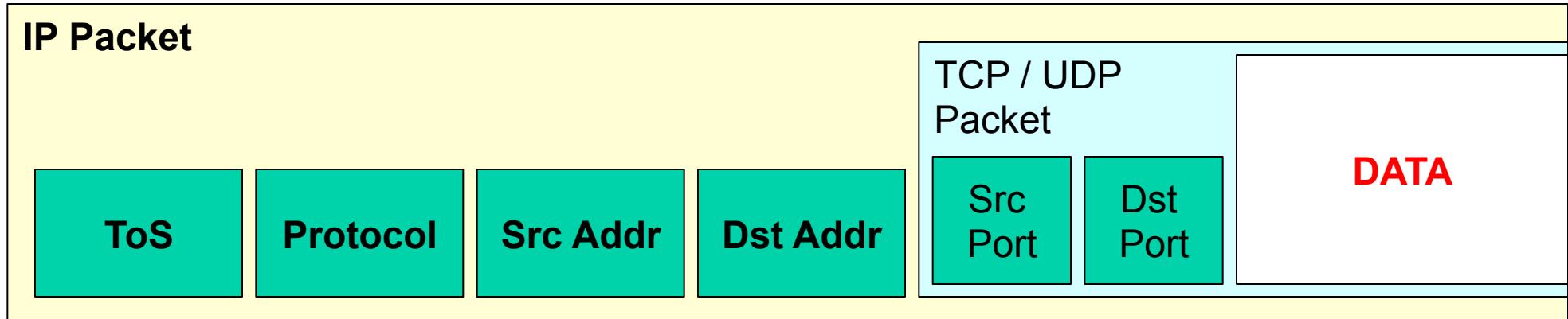
- Cara Kerja L7 Filter
- Regular Expression
- Implementasi di Mikrotik routerOS
- Keuntungan dan Konsekuensi penggunaan L7



Traffic Clasifier

- L7 adalah sebuah packet classifier yang sebenarnya digunakan oleh Netfilter (Linux) untuk melakukan identifikasi paket data berdasarkan Layer aplikasi (Layer 7).
- Dengan menggunakan L7 packet classifier ini maka memunginkan firewall atau Bandwidth limiter mengembangkan fungsinya ke level yang lebih tinggi.
- Keterbatasan logika Firewall mikrotik yang sebelumnya hanya bisa memproses packet header dijawab oleh L7 sehingga bisa memetakan paket data lebih detail.
- Firewall mikrotik sudah mampu mengenali nama domain, variasi p2p, Audio-video traffic dan masih banyak lagi

Packet Flow - Content



- L7 classifier secara default akan melakukan inspeksi berdasarkan “patern” yang diinstruksikan ke dalam **10** paket pertama atau sekitar **2KB** dari sebuah connection.
- Seberapa Besar atau jumlah paket yang di-inspeksi tidak dapat diubah.



L7 Requirement

- L7 dapat bekerja maksimal jika bisa melihat kedua arah traffic (request & response) sehingga disarankan untuk meletakkan L7 classifier di chain **forward**.
- Jika ingin diletakkan di chain **prerouting/input** maka rule yang sama juga harus diletakkan di **postrouting/output**.
- L7 memiliki karakteristik haus akan memory (RAM) sehingga disarankan untuk digunakan sesuai kebutuhan.



Layer 7 Protocol

- L7 sudah bisa mengenali berbagai traffic seperti protocol aplikasi, file-type, malware dan masih banyak lagi.
- Sekitar **150 patern** sudah bisa digunakan
- Tetapi perlu diingat juga bahwa Tidak semua koneksi bisa diidentifikasi.
- L7 tetap belum bisa melakukan inspeksi terhadap traffic yang ter-enkripsi seperti traffic yang melewati SSL tunnel. Karena data yang terlihat pada proses handshake adalah hanya certificate ssl nya saja.



Regular Expression

- L7 menggunakan Regular Expression untuk melakukan inspeksi content dari sebuah connection.
- Regular Expression adalah sebuah “string” text untuk mendeskripsikan pencarian patern yang diinginkan.
- Contoh :
 - "hello" messages such as "220 ftp server ready", "* ok", or "HTTP/1.1 200 ok".



RegEx Quick Reference

- “^” (caret) Matches the begining of input
- “\$” Matches the end of input
- “.” Matches any single character
- “?” 0 or 1 occurrences of proceeding string
- “*” (star) 0 or more occurrences of preceding string
- “[...]” Matches any on the enclosed characters
e.g. ca[tr] matches cat and car
- “|” (pipe) Logical “or”, match either the part on the left side, or the part on the right side



RegEx – Usefull

- `[\x09-\x0d -~]` printable characters, including whitespace
- `[\x09-\x0d]` any whitespace
- `[!-~]` non-whitespace printable characters



RegEx – How To

- Selidiki dan cari detail spesifikasi dari protocol yang ingin di-filter. Jika masih menggunakan standard Internet bisa menggunakan RFC, jika proprietary protocol maka coba cari reverse-engineering specification.
- Gunakan software sniffer jika perlu (ex. Wireshark) untuk melihat detail paket datanya.
- Gunakan patern RegEx yang bisa cocok dengan beberapa paket pertama dari koneksi protocol tersebut.
- Test telebih dahulu.



RegEx - Example

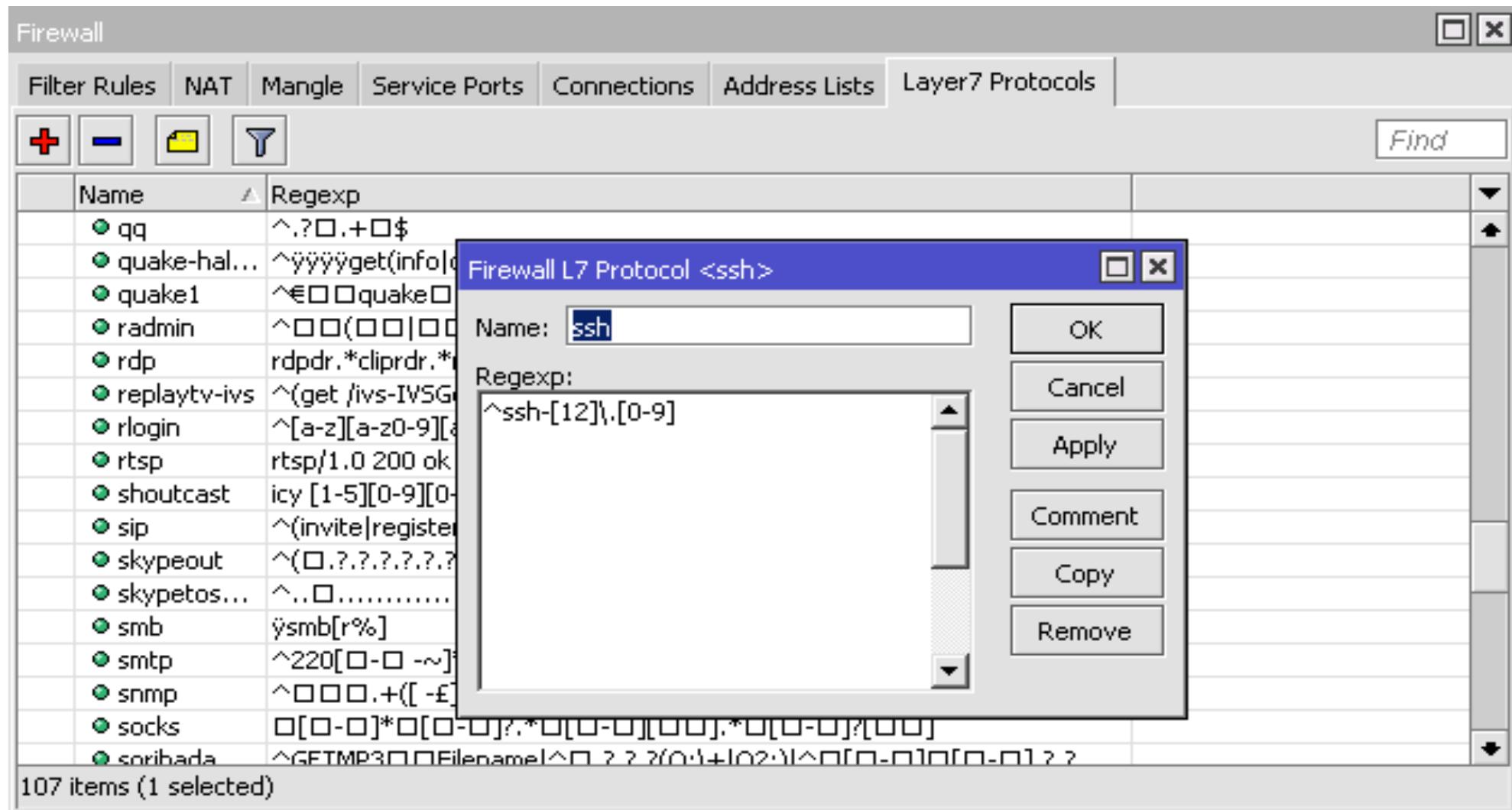
- **SSH :**
 - `^ssh-[12]\.[0-9]`
- **FTP :**
 - `^220[\x09-\x0d -~]*ftp`
- **Yahoo :**
 - `^(ymsg|ypns|yhoo).?.?.?.?.?.?[|wt].*\xc0\x80`



RegEx Pattern Resourse

- Pattern libraries can be found on:
 - http://protocolinfo.org/wiki/Main_Page
 - <http://I7-filter.sourceforge.net/protocols>
- Script for Mikrotik with common programs list:
 - [*www.mikrotik.com/download/I7-protos.rsc*](http://www.mikrotik.com/download/I7-protos.rsc)

L7 RegEx on Mikrotik



L7 for Firewall or Mangle

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol: **Content:** **Connection Bytes:** **Connection Rate:** **Per Connection Classifier:**

unknown
ssh
ssl
stun
subspace
subversion
teamspeak
telnet
tesla
tftp



[LAB-1] Block Yahoo Msg

The image shows a stack of three Firewall Rule configuration windows, each with a red box highlighting a specific field. The top window is for a rule on the 'forward' chain. The middle window is for a rule with a Layer7 protocol of 'yahoo'. The bottom window is for an 'Action: drop' rule.

Top Window (highlighted): Firewall Rule <>
General Advanced Extra Action Statistics
Chain: **forward**

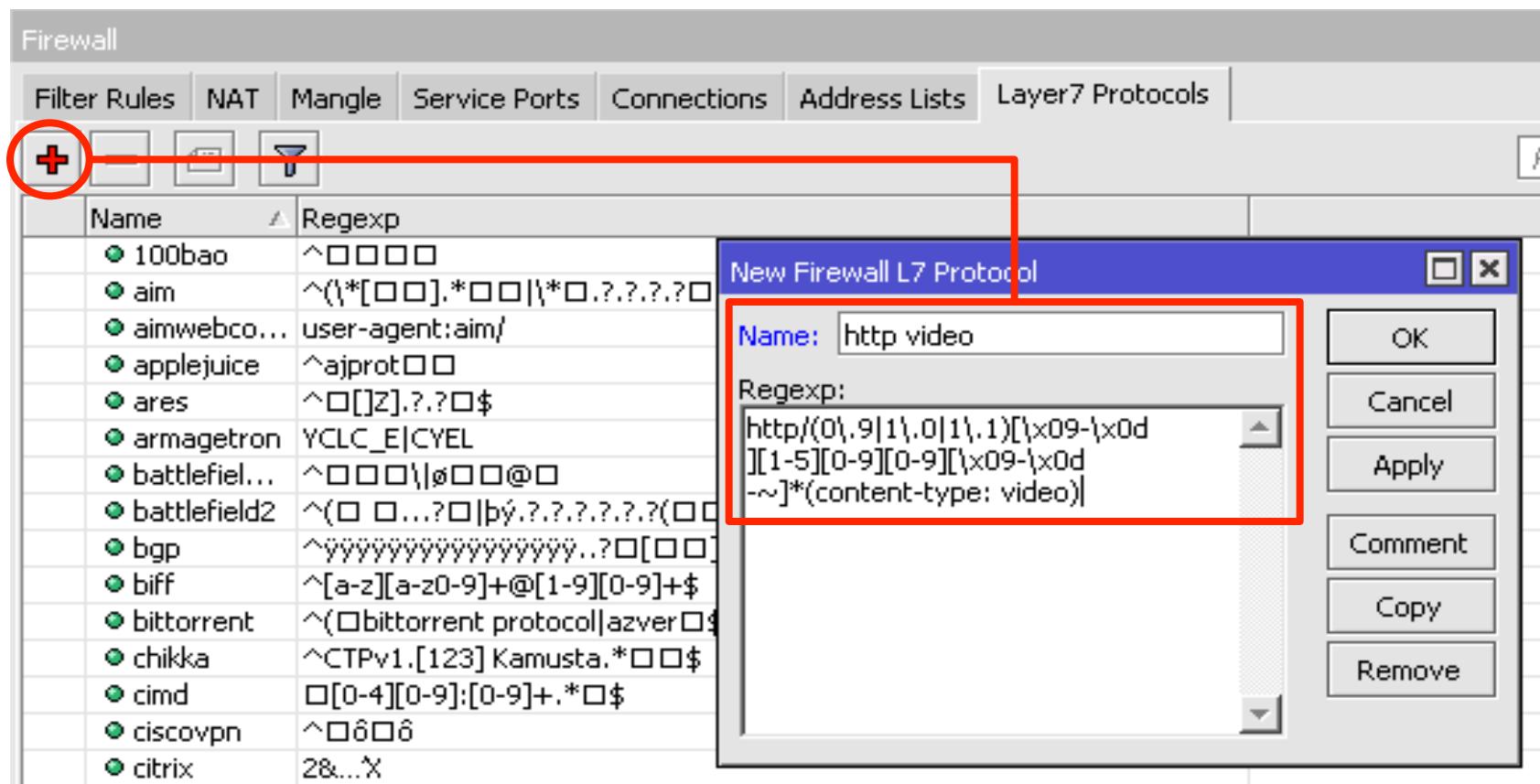
Middle Window (highlighted): Firewall Rule <>
General Advanced Extra Action Statistics
Src. Address List: **.....**
Dst. Address List: **.....**
Layer7 Protocol: **yahoo**

Bottom Window (highlighted): Firewall Rule <>
General Advanced Extra Action Statistics
Action: **drop**

[LAB-2] Limit Traffic Video

- http Video RegEx :

- `http/(0\.9|1\.0|1\.1)[\x09-\x0d][1-5][0-9][0-9][\x09-\x0d -~]*`(content-type: video)



L7 - Video Mangle

The screenshot shows the configuration of an L7 Mangle Rule. The rule is defined in three stacked windows:

- Top Window (Mangle Rule <>):** Contains tabs for General, Advanced, Extra, Action, and Statistics. The "Chain: forward" field is highlighted with a red box.
- Middle Window (Mangle Rule <>):** Contains tabs for General, Advanced, Extra, Action, and Statistics. The "Src. Address" and "Dst. Address" fields are present. The "Layer7 Protocol: http video" field is highlighted with a red box.
- Bottom Window (Mangle Rule <>):** Contains tabs for General, Advanced, Extra, Action, and Statistics. The "Action: mark packet" field is highlighted with a red box. Below it, the "New Packet Mark: packet-video" field and the "Passthrough" checkbox are also highlighted with a red box.

L7 - Video Queue

Simple Queue <limiter-video>

General Advanced Statistics Traffic Total Total Statistics

Name: limiter-video

Target Address:

Target Upload Target Download

Max Limit: 512k 512k bits/s

Simple Queue <limiter-video>

General Advanced Statistics Traffic Total Total Statistics

P2P:

Packet Marks: packet-video

Dst. Address:

Interface: all



L7 - Conclusion

- Keuntungan :
 - Memperkaya kemampuan firewall
 - Meningkatkan Keakurasiang firewall
 - Mampu membedakan paket walau menggunakan port yang sama
- Konsekuensi :
 - CPU load tinggi
 - Haus RAM
 - Masih belum bisa mengenali traffic yang terenkripsi



QoS



Certified Mikrotik Training - Advanced Class (MTCTCE)
Organized by: Citraweb Nusa Infomedia
(Mikrotik Certified Training Partner)



Materi QoS

- Konsep Dasar QoS
- Queue Type
- Parent Queue
- HTB
- Burst Calculation
- Implementasi Simple Queue
- Implementasi Queue Tree



Quality of Service

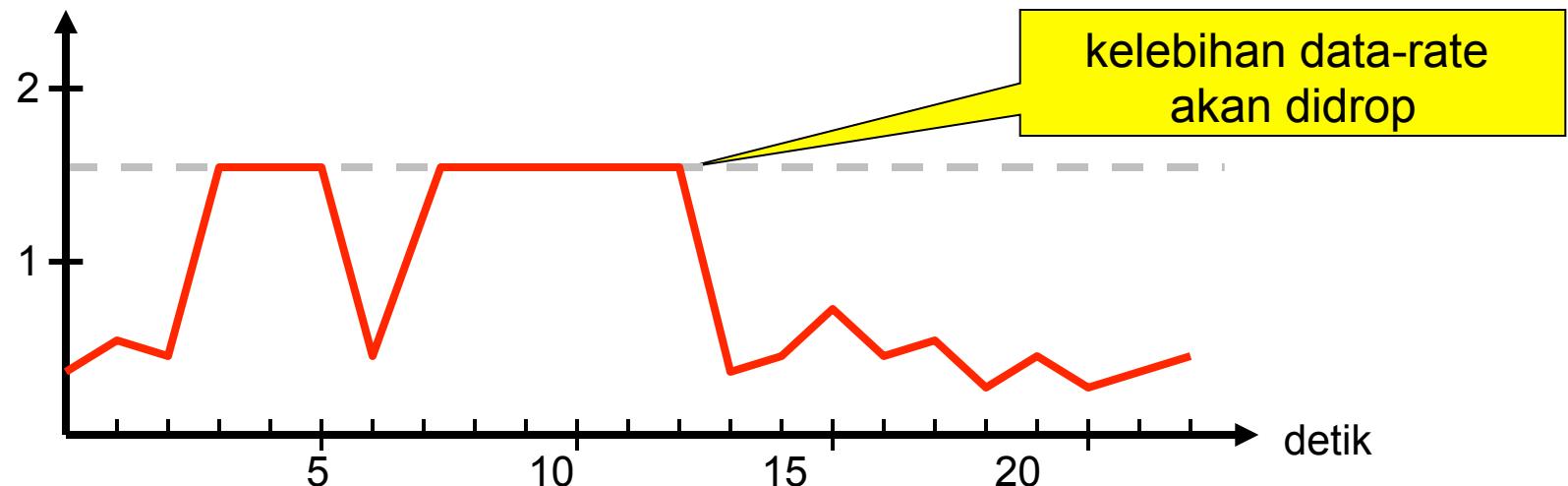
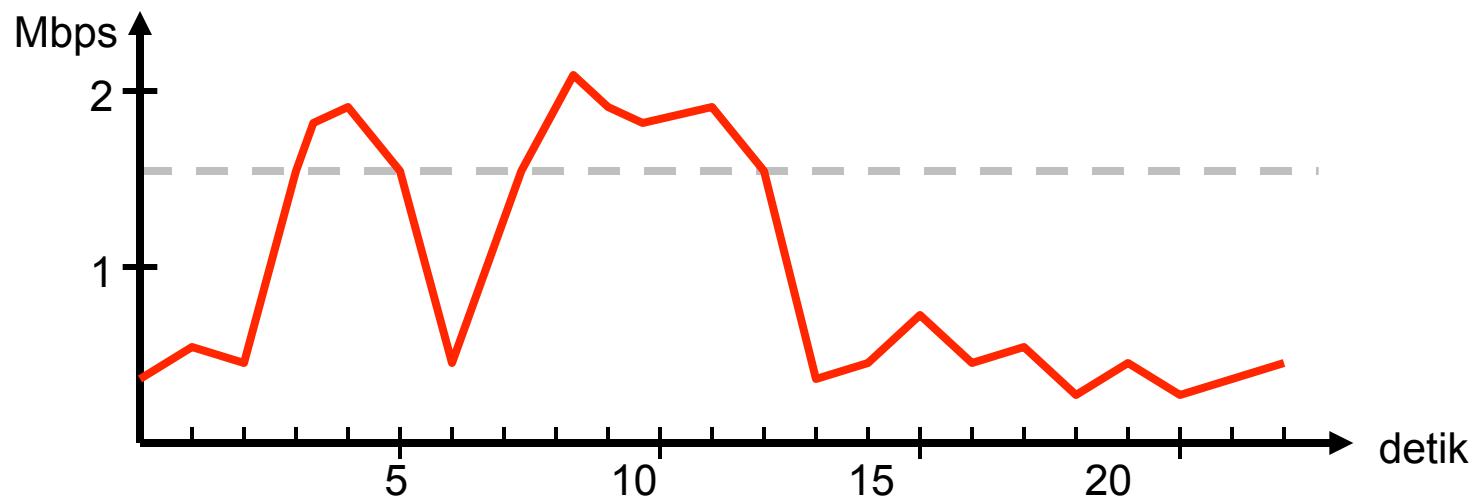
- QoS tidak selalu berarti pembatasan bandwidth
- Adalah cara yang digunakan untuk mengatur penggunaan bandwidth yang ada secara rasional.
- QoS tidak selalu berarti pembatasan bandwidth, QoS bisa digunakan juga untuk mengatur prioritas berdasarkan parameter yang diberikan, menghindari terjadinya trafik yang memonopoli seluruh bandwidth yang tersedia.



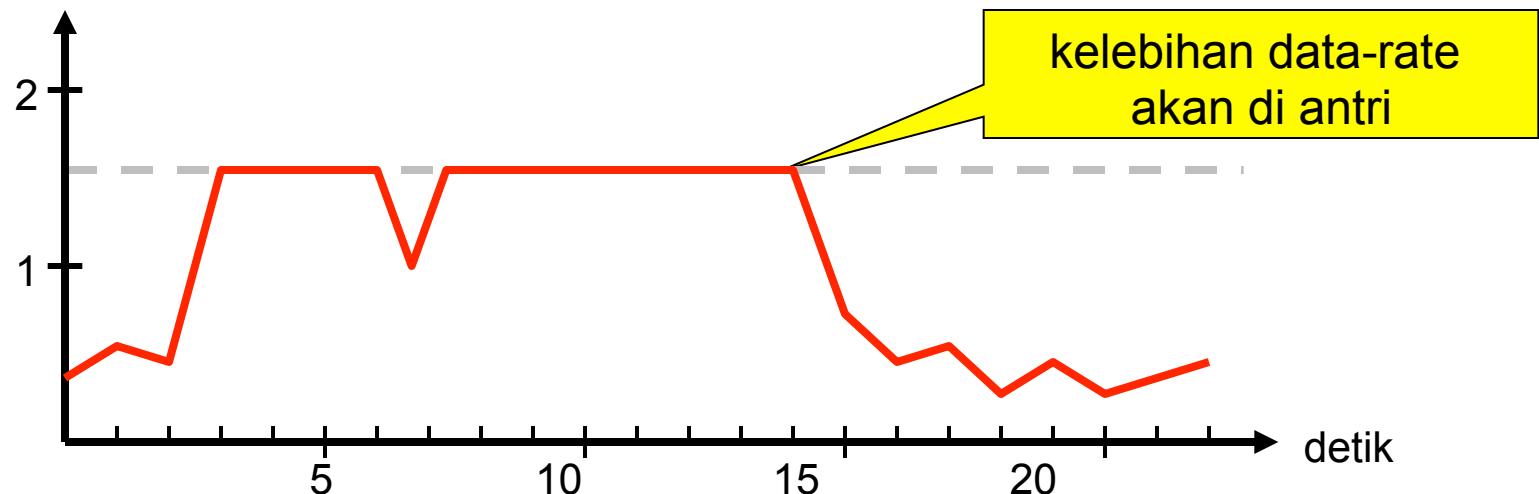
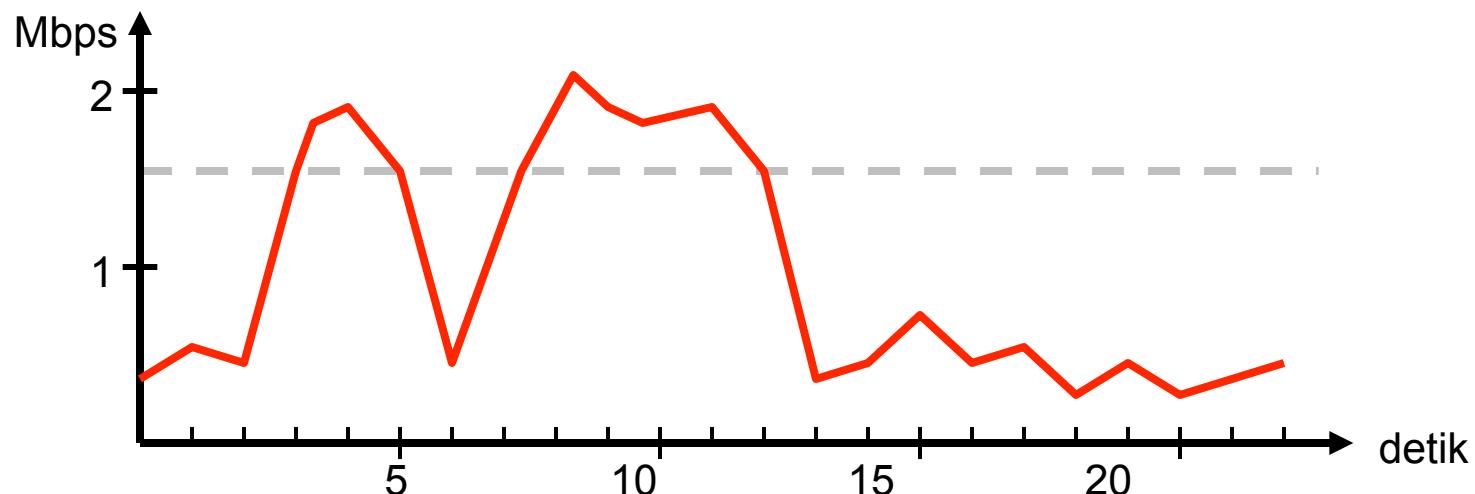
Queue Disciplines

- Queuing disciplines dapat dibedakan menjadi 2:
 - Scheduler queues
 - Mengatur packet flow, sesuai dengan jumlah paket data yang “menunggu di antrian”, dan bukan melimit kecepatan data rate.
 - Shaper queues
 - Mengontrol kecepatan date rate.

Shaper



Scheduler



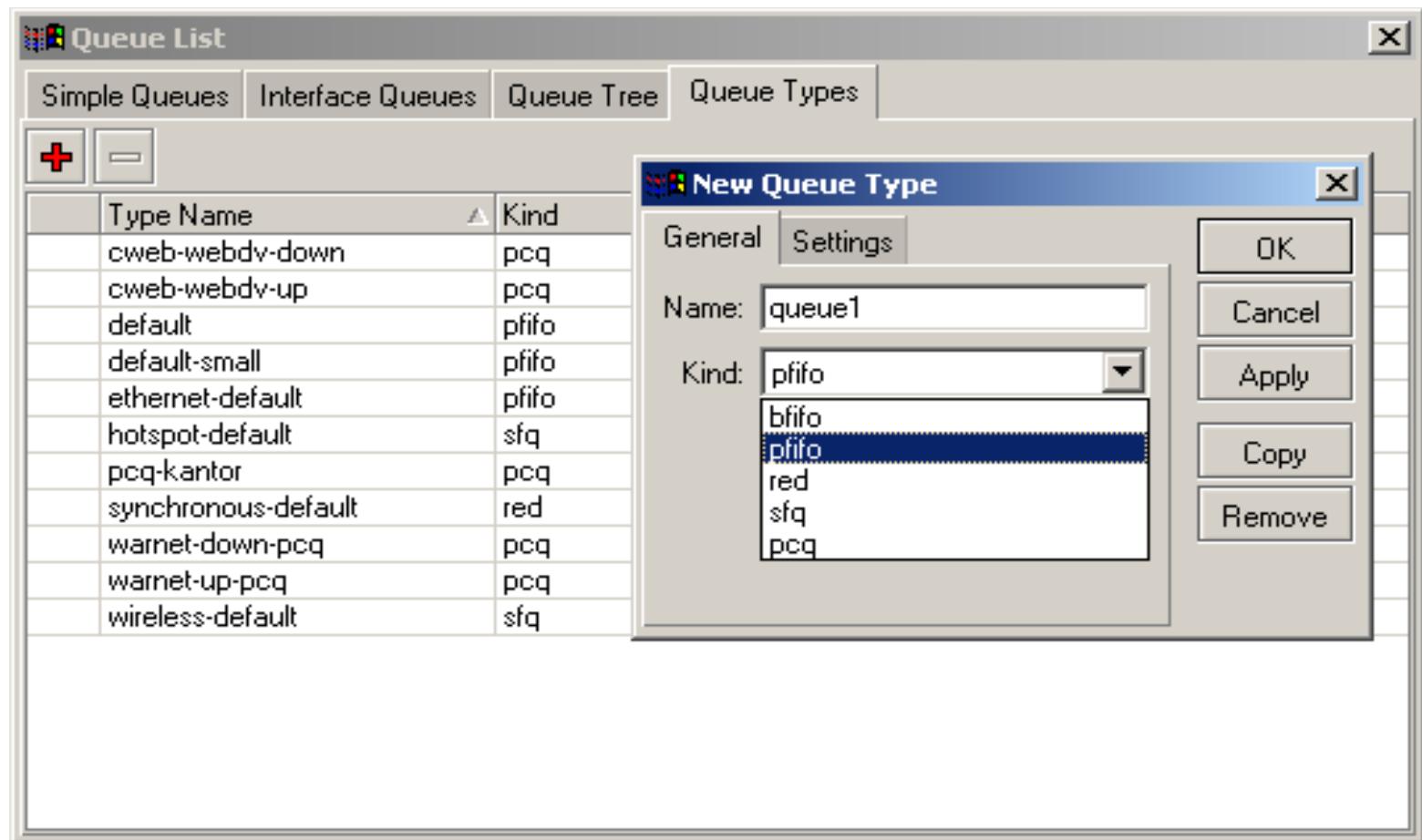


Queue Kinds

- Scheduler queues:
 - BFIFO (Bytes First-In First-Out)
 - PFIFO (Packets First-In First-Out)
 - MQ-PFIFO (Multi Queue Packets First-In First-Out)
 - RED (Random Early Detect)
 - SFQ (Stochastic Fairness Queuing)
- Shaper queues:
 - PCQ (Per Connection Queue)
 - HTB (Hierarchical Token Bucket)
- You can configure queue properties in “/queue type”

Queue Kinds

- Kita dapat mengatur tipe queue pada “/queue type”

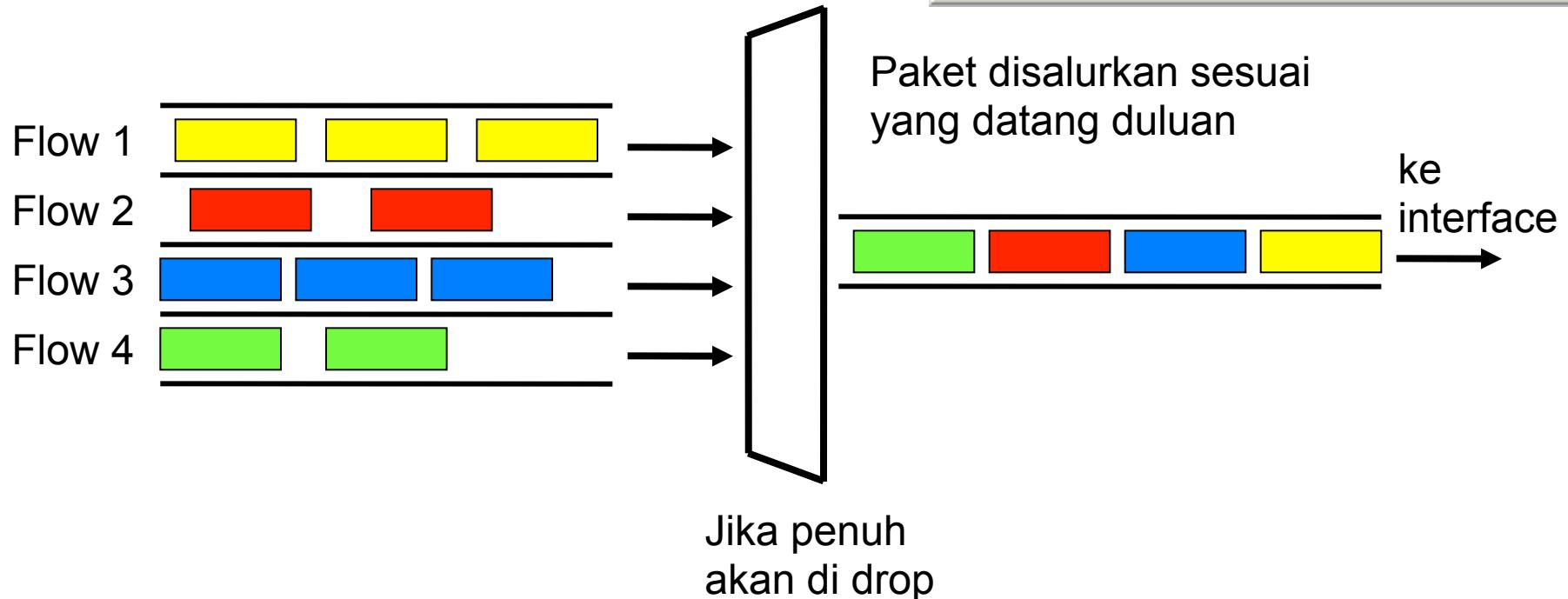
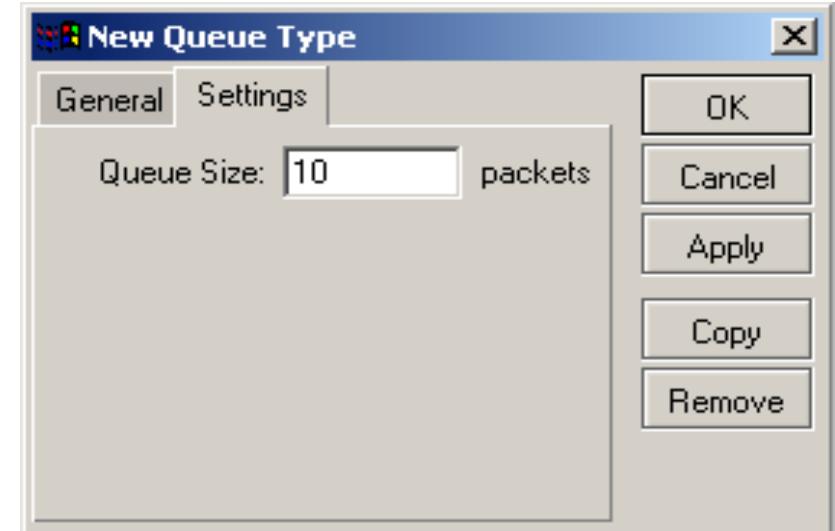




FIFO (First In First Out)

- **PFIFO** dan **BFIFO** keduanya menggunakan algoritma FIFO, dengan buffer yang kecil.
- FIFO tidak mengubah urutan paket data, hanya menahan dan menyalurkan bila sudah memungkinkan.
- Jika buffer penuh maka paket data akan di drop
- FIFO baik digunakan bila jalur data tidak congested
- Parameter pfifo-limit dan bfifo-limit menentukan jumlah data yang bisa diantrikan di buffer
- **MQ-FIFO** – adalah sebuah mekanisme fifo yang dikhususkan pada system hardware yang sudah SMP (multi core processor) dan harus pada interface yang support multiple transmit queues.

Skema FIFO

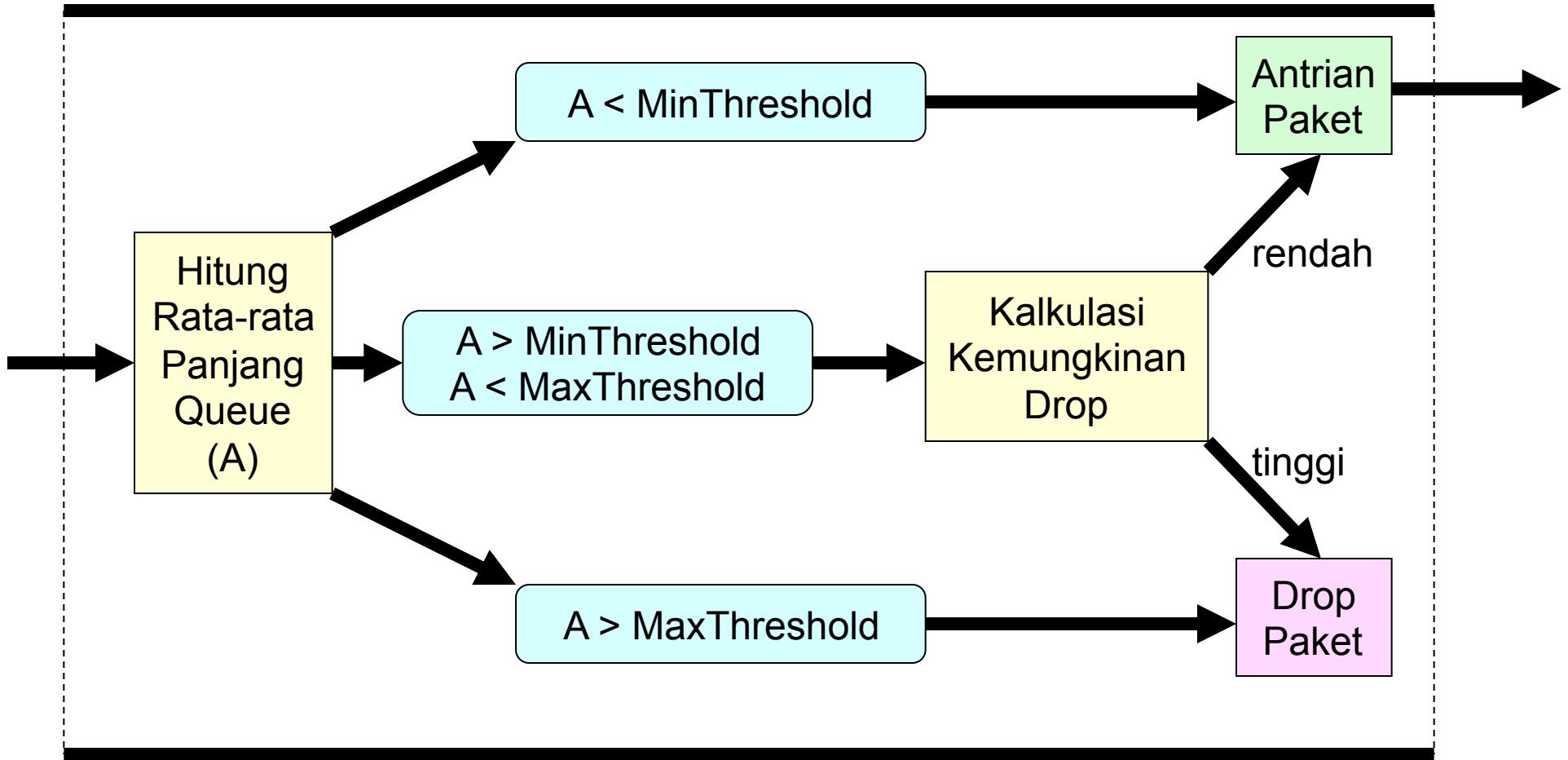




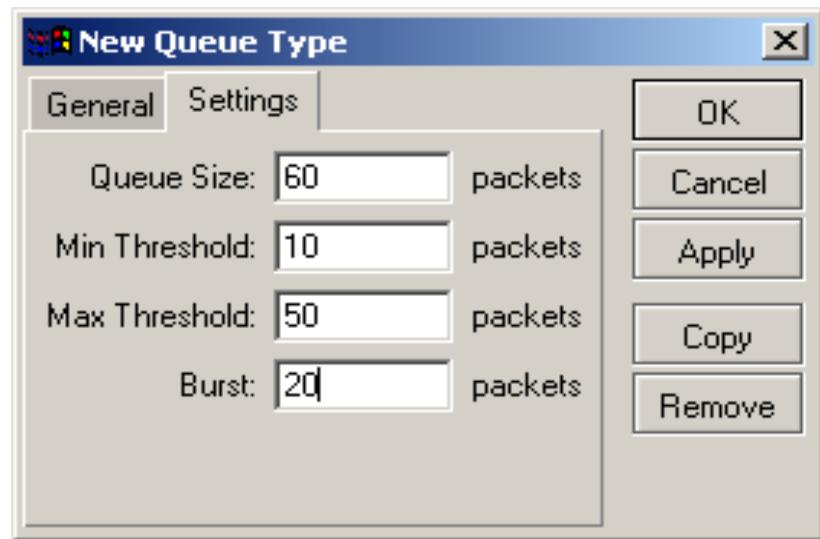
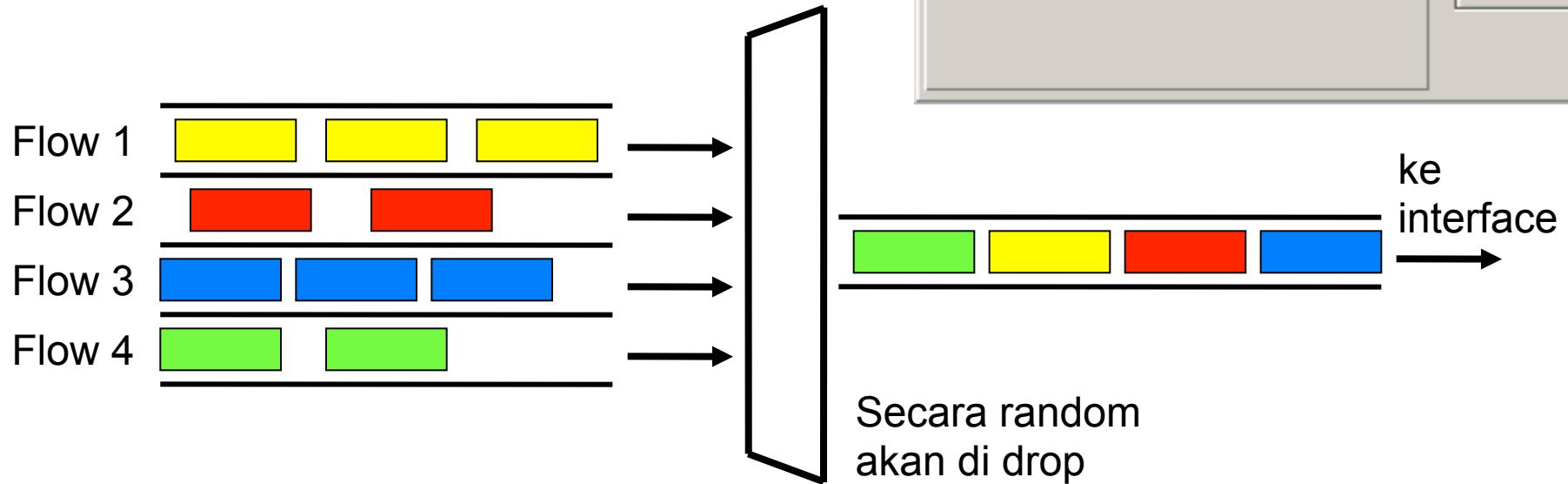
RED (Random Early Detect)

- RED tidak melimit kecepatan, tetapi bila buffer sudah penuh, maka secara tidak langsung akan menyeimbangkan data rate setiap user.
- Saat ukuran queue rata-rata mencapai min-threshold, RED secara random akan memilih paket data untuk di drop
- Saat ukuran queue rata-rata mencapai max-threshold, paket data akan di drop
- Jika ukuran queue sebenarnya (bukan rata-ratanya) jauh lebih besar dari **red-max-threshold**, maka semua paket yang melebihi **red-limit** akan didrop.
- RED digunakan jika kita memiliki trafik yang congested. Sangat sesuai untuk trafik TCP, tetapi kurang baik digunakan untuk trafik UDP.

Logika RED



Skema RED



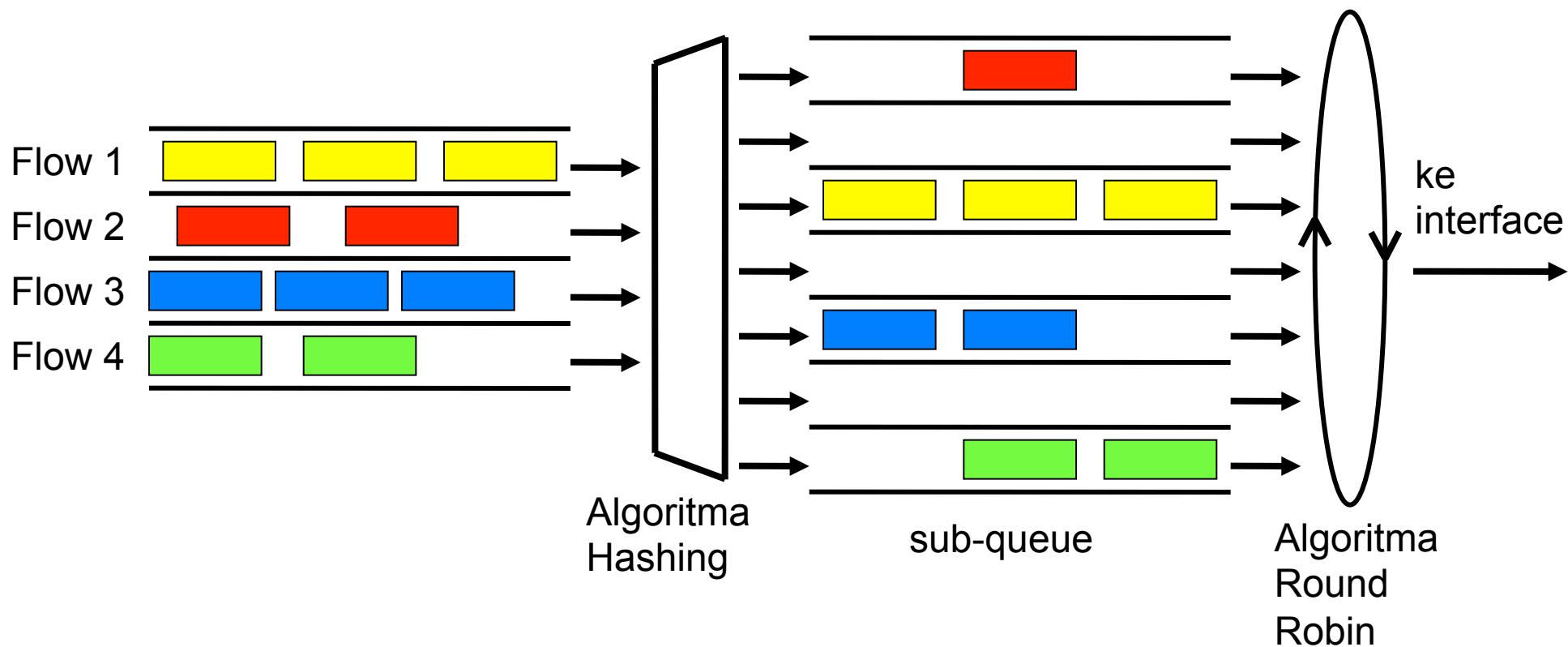
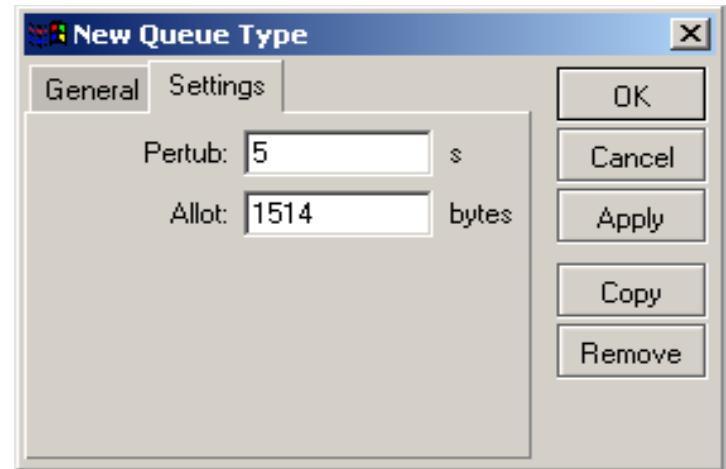


SFQ (Stochastic Fairness Queuing)

- SFQ sama sekali tidak dapat melimit trafik. Fungsi utamanya adalah menyeimbangkan flow trafik jika link telah benar-benar penuh.
- Dapat digunakan untuk TCP maupun UDP.
- SFQ menggunakan metoda hasing dan round robin.
- Total SFQ queue terdiri dari 128 paket.
- Algoritma hasing dapat membagi trafik menjadi 1024 sub queue, dan jika terdapat lebih maka akan dilewati.
- Algoritma round robin akan melakukan queue ulang sejumlah bandwidth (allot) dari setiap queue.

Skema SFQ

- Setelah **Perturb** detik algoritma hasing akan berganti dan membagi session trafik ke sub-queue lainnya dengan **Allot** besar packet

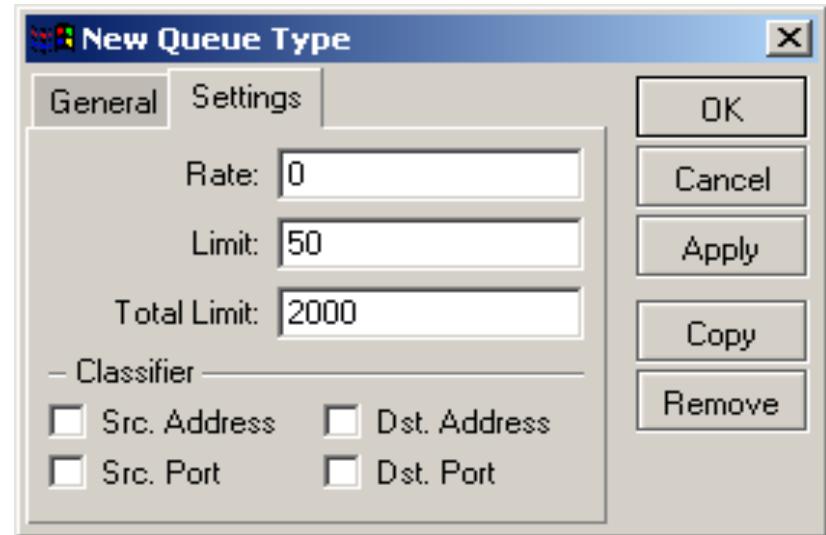




PCQ (Per Connection Queue)

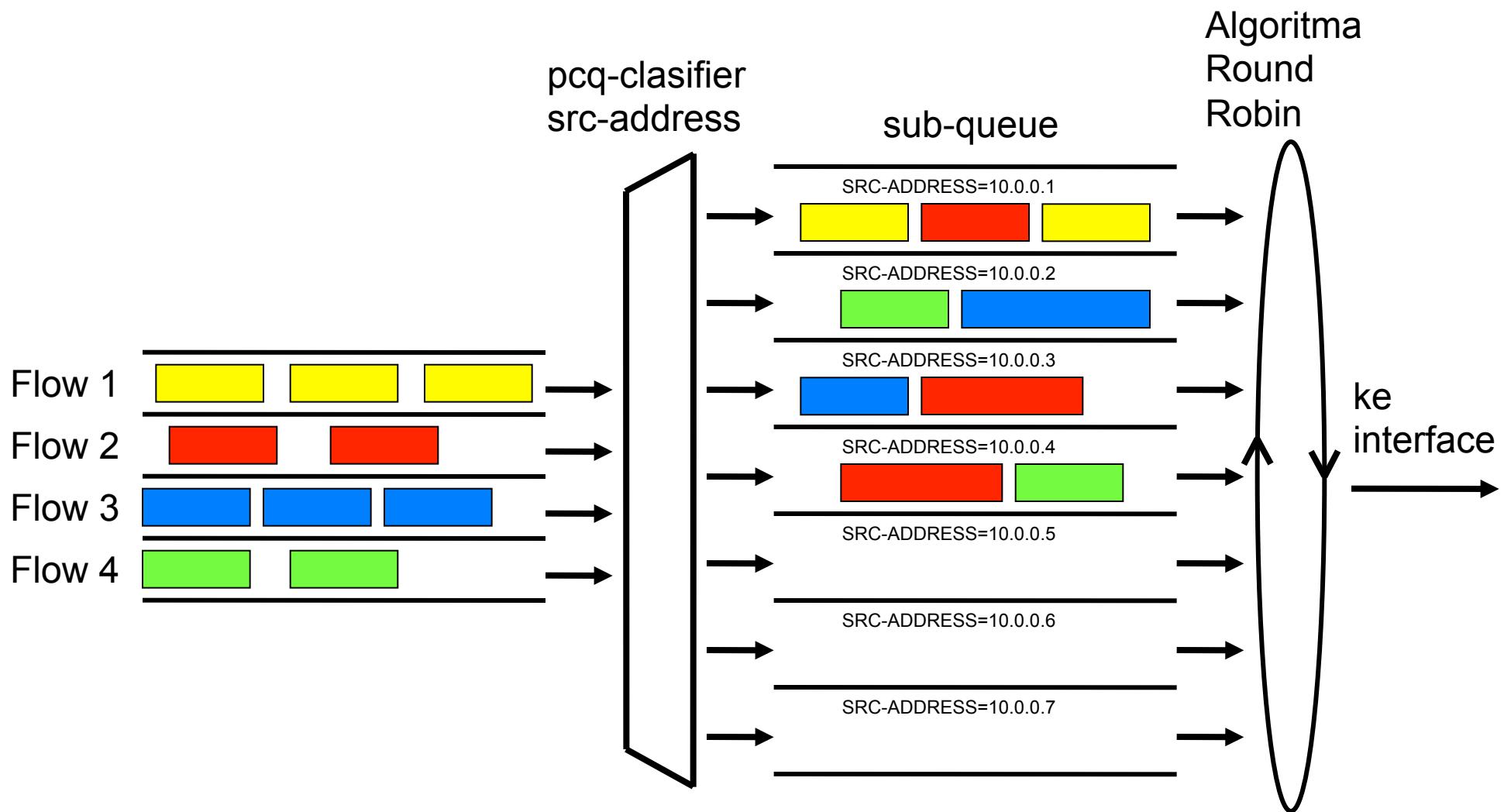
- PCQ dibuat sebagai penyempurnaan SFQ.
- PCQ tidak membatasi jumlah sub-queue
- PCQ membutuhkan memori yang cukup besar

Setting PCQ



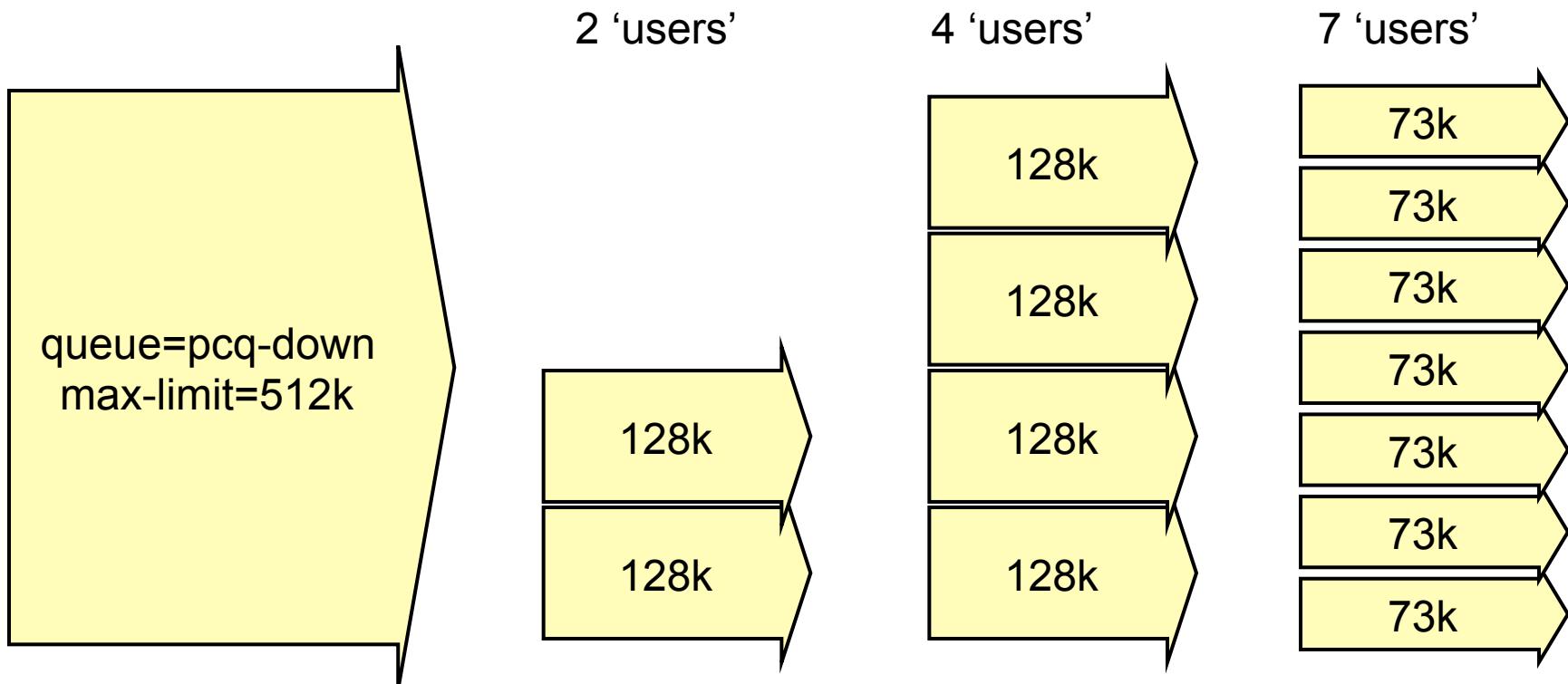
- PCQ akan membuat sub-queue, berdasarkan parameter **pcq-classifier**, yaitu: *src-address*, *dst-address*, *src-port*, *dst-port*
- Dimungkinkan untuk membatasi maksimal data rate untuk setiap sub-queue (**pcq-rate**) dan jumlah paket data (**pcq-limit**)
- Total ukuran queue pada PCQ-sub-queue tidak bisa melebihi jumlah paket sesuai **pcq-total-limit**

Skema PCQ



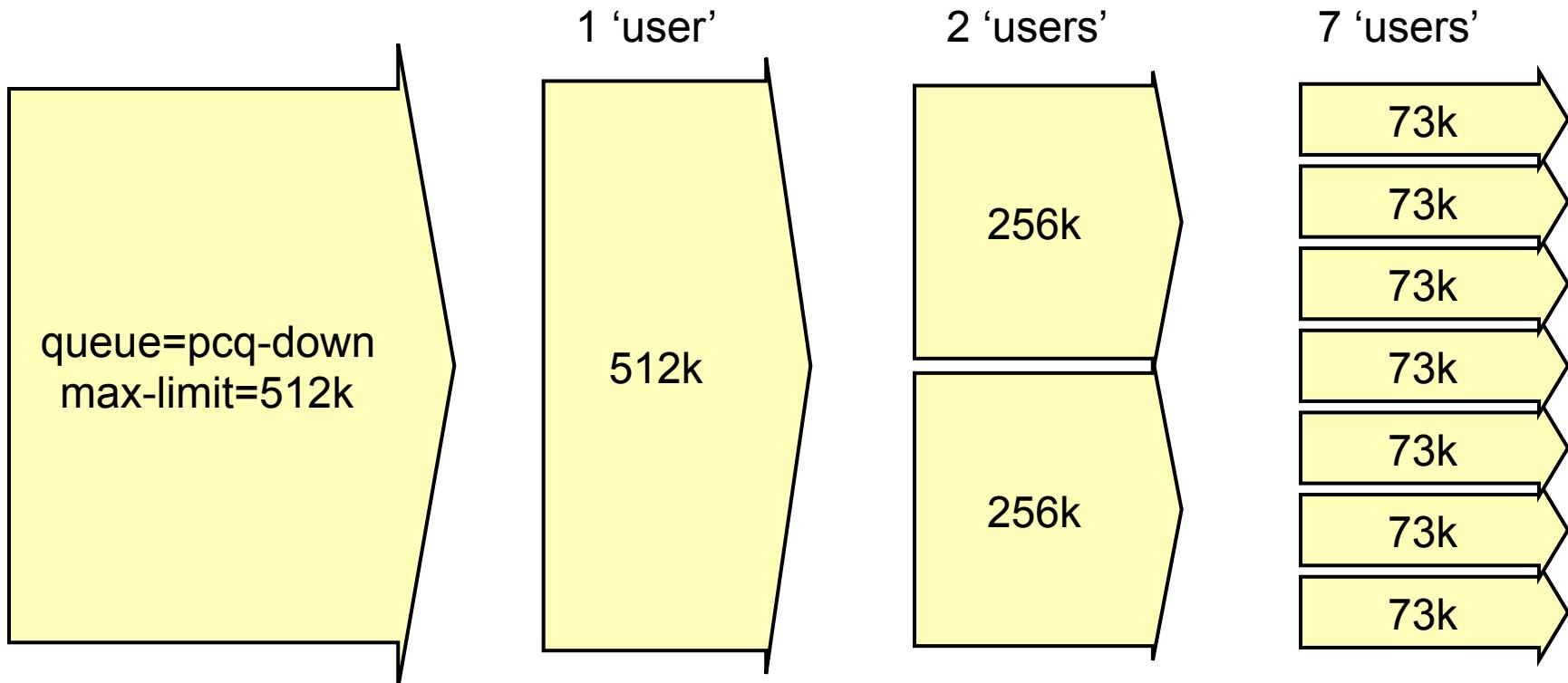
PCQ in Action (1)

- $\text{Pcq-rate} = 128000$



PCQ in Action (2)

- Pcq-rate=0



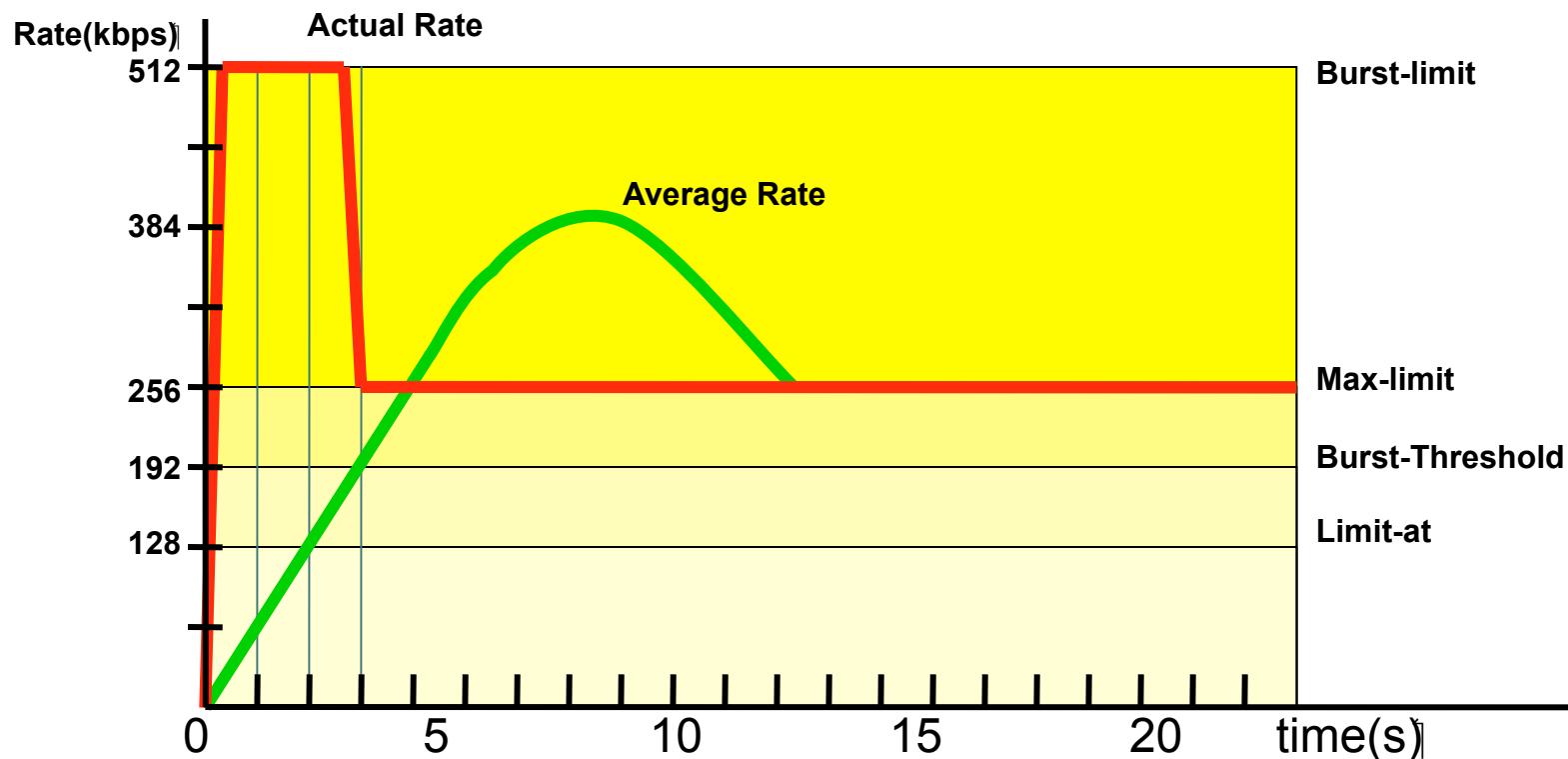


Burst

- Burst adalah salah satu cara menjalankan QoS
- Burst memungkinkan penggunaan data-rate yang melebihi max-limit untuk periode waktu tertentu
- Jika data rate lebih kecil dari **burst-threshold**, burst dapat dilakukan hingga data-rate mencapai **burst-limit**
- Setiap detik, router mengkalkulasi data rate rata-rata pada suatu kelas queue untuk periode waktu terakhir sesuai dengan **burst-time**
- **Burst time** tidak sama dengan waktu yang diijinkan untuk melakukan burst.

Contoh Burst (1)

- **Limit-at=128kbps, max-limit=256kbps, burst-time=8, burst-threshold=192kbps, burst-limit=512kbps.**

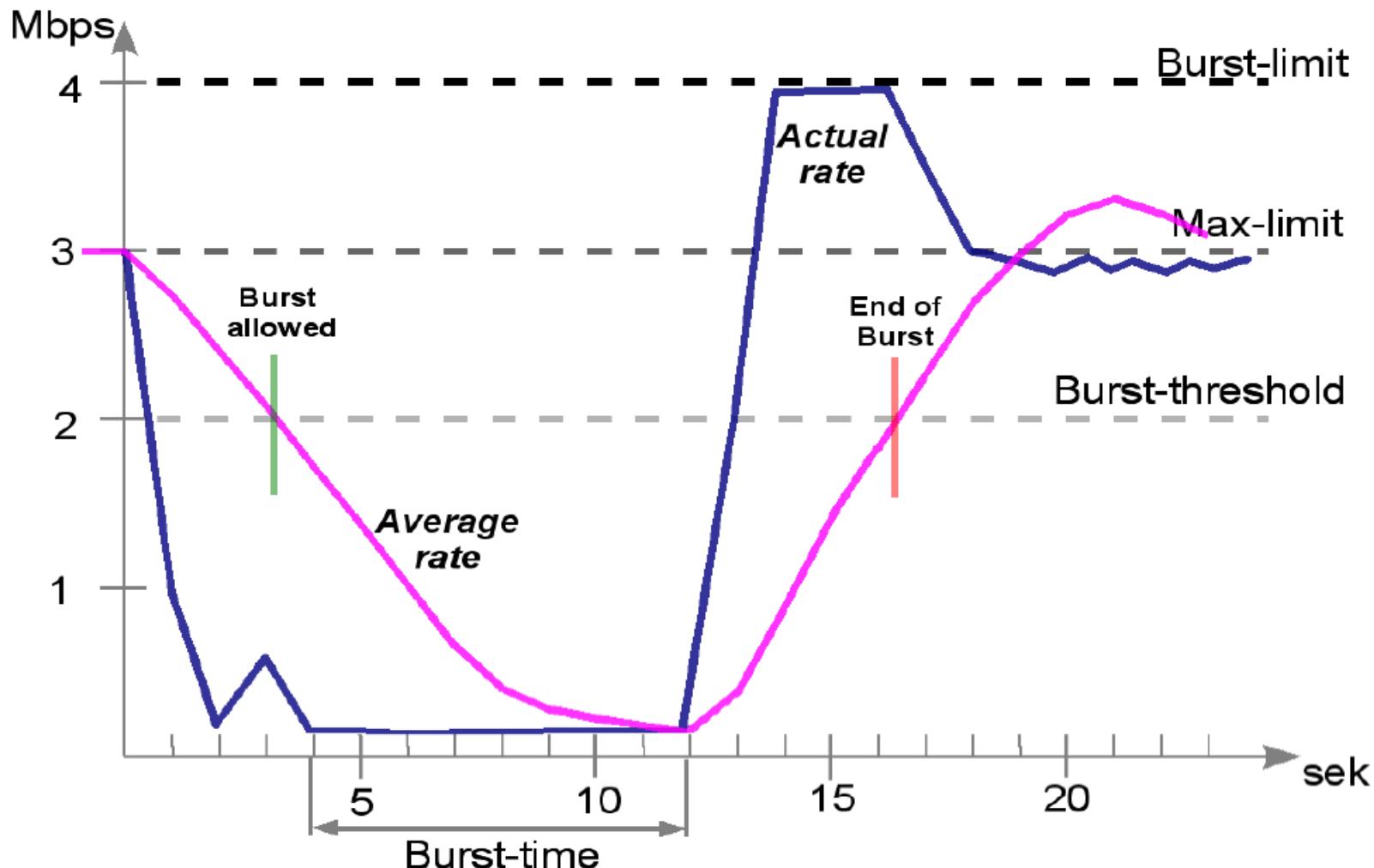




Contoh Burst (1)

- Pada awalnya, data rate rata-rata dalam 8 detik terakhir adalah 0 kbps. Karena data rate rata-rata ini lebih kecil dari **burst-threshold**, maka burst dapat dilakukan.
- Setelah 1 detik, data rate rata-rata adalah $(0+0+0+0+0+0+512)/8=64$ kbps, masih lebih kecil dari **burst-threshold**. Burst dapat dilakukan.
- Demikian pula untuk detik kedua, data rate rata-rata adalah $(0+0+0+0+0+512+512)/8=128$ kbps.
- Setelah 3 detik, tiba-tiba pada saat di mana data rate rata-rata lebih besar dari **burst-threshold**. Burst tidak dapat lagi dilakukan, dan data rate turun menjadi **max-limit** (256 kbps).

Contoh Burst (2)



PCQ - Burst

- Di versi 5.x pada queue-type PCQ terdapat fitur baru yaitu PCQ-Burst yang memungkinkan mengimplementasikan Burst di substream (sub-queue).
- Parameter PCQ-Rate digunakan sebagai pengganti parameter Max-limit di perhitungan PCQ-Burst.
- Logika kalkulasi burst di PCQ-burst masih sama dengan fungsi Burst yang ada di queue.

The image shows a configuration interface with three input fields for PCQ-Burst parameters:

- Burst Rate: 1m
- Burst Threshold: 256k
- Burst Time: 00:00:30

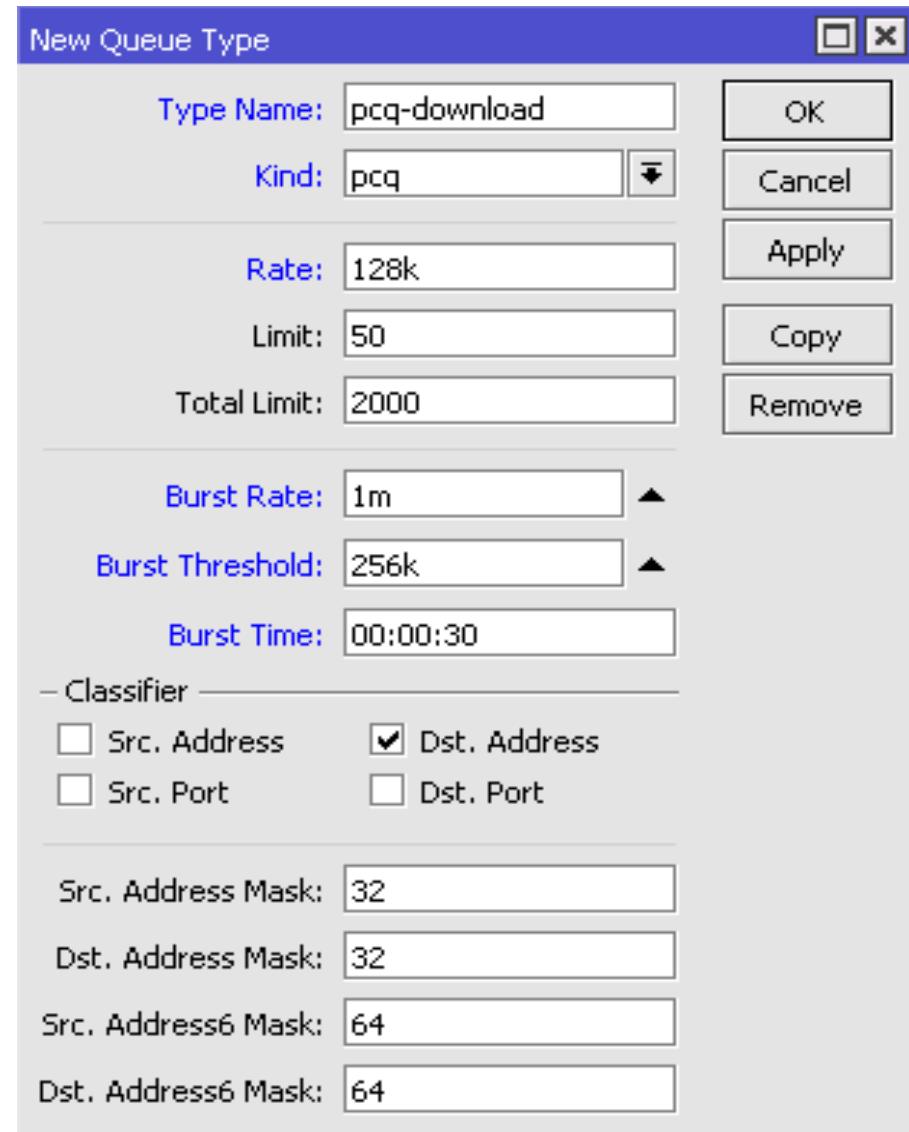
PCQ - Burst

- Di Versi 5.x juga sudah ditambahkan fitur baru yaitu **Address-mask** pada PCQ.
- Parameter ini memungkinkan untuk grouping beberapa ip client di dalam satu substream-queue
- Address-mask juga berguna jika PCQ ingin digunakan sebagai limiter di IPv6.

Src. Address Mask:	29
Dst. Address Mask:	25
Src. Address6 Mask:	64
Dst. Address6 Mask:	64

[LAB-1] PCQ Burst Calculation

- Cobalah bermain dengan parameter burst untuk mendapatkan konfigurasi burst yang nyaman untuk seorang client yang ada di dalam PCQ-substream.

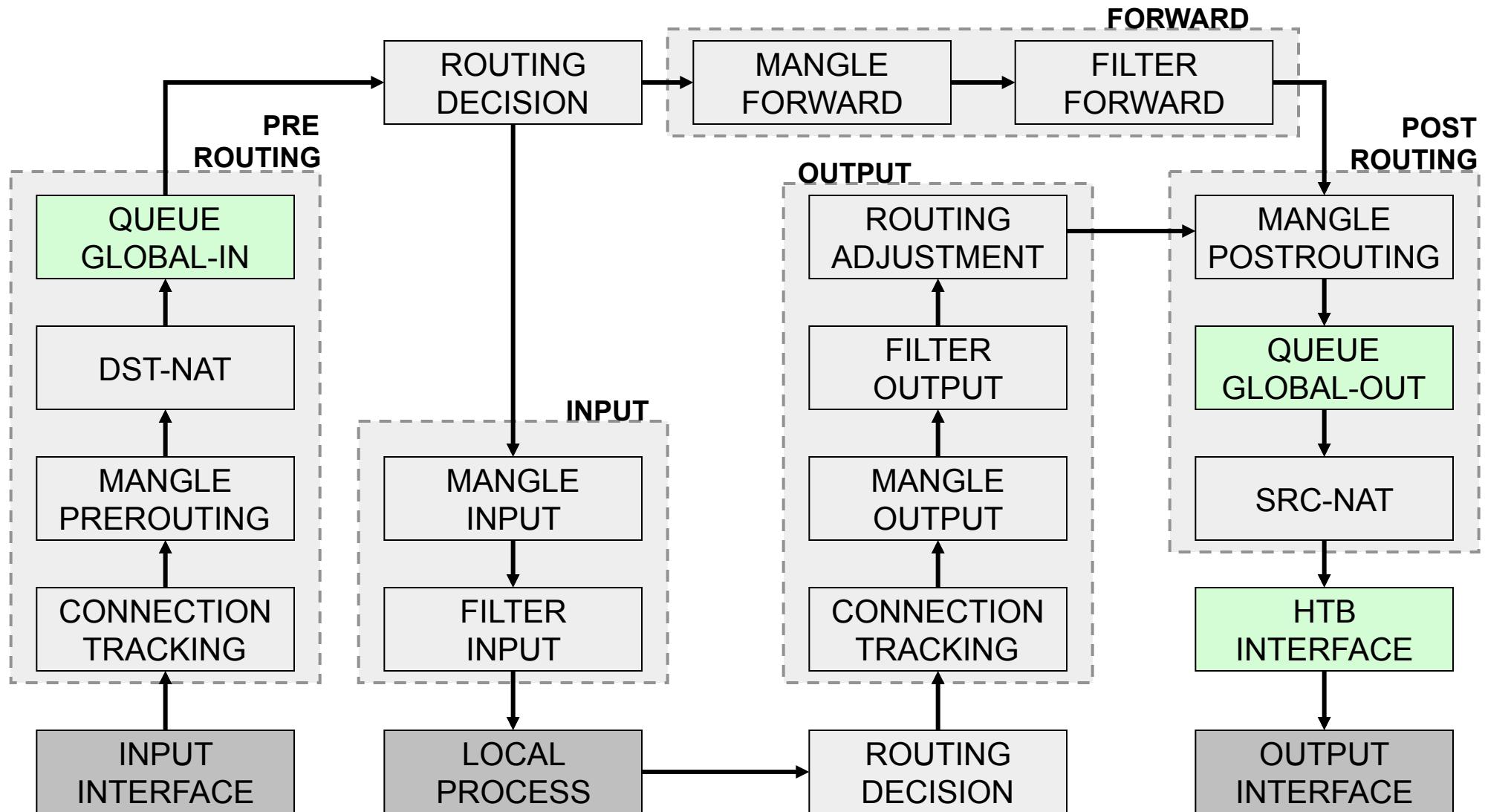




Posisi Queue

- Queue pada RouterOS dilakukan pada parent:
 - Interface
 - Virtual:
 - Global In
 - Global Out
 - Global Total
- **Simple-Queue** tidak bisa melakukan queue pada parent interface sehingga secara otomatis menggunakan Virtual Interface.

Simple Packet Flow





Penggunaan Mangle

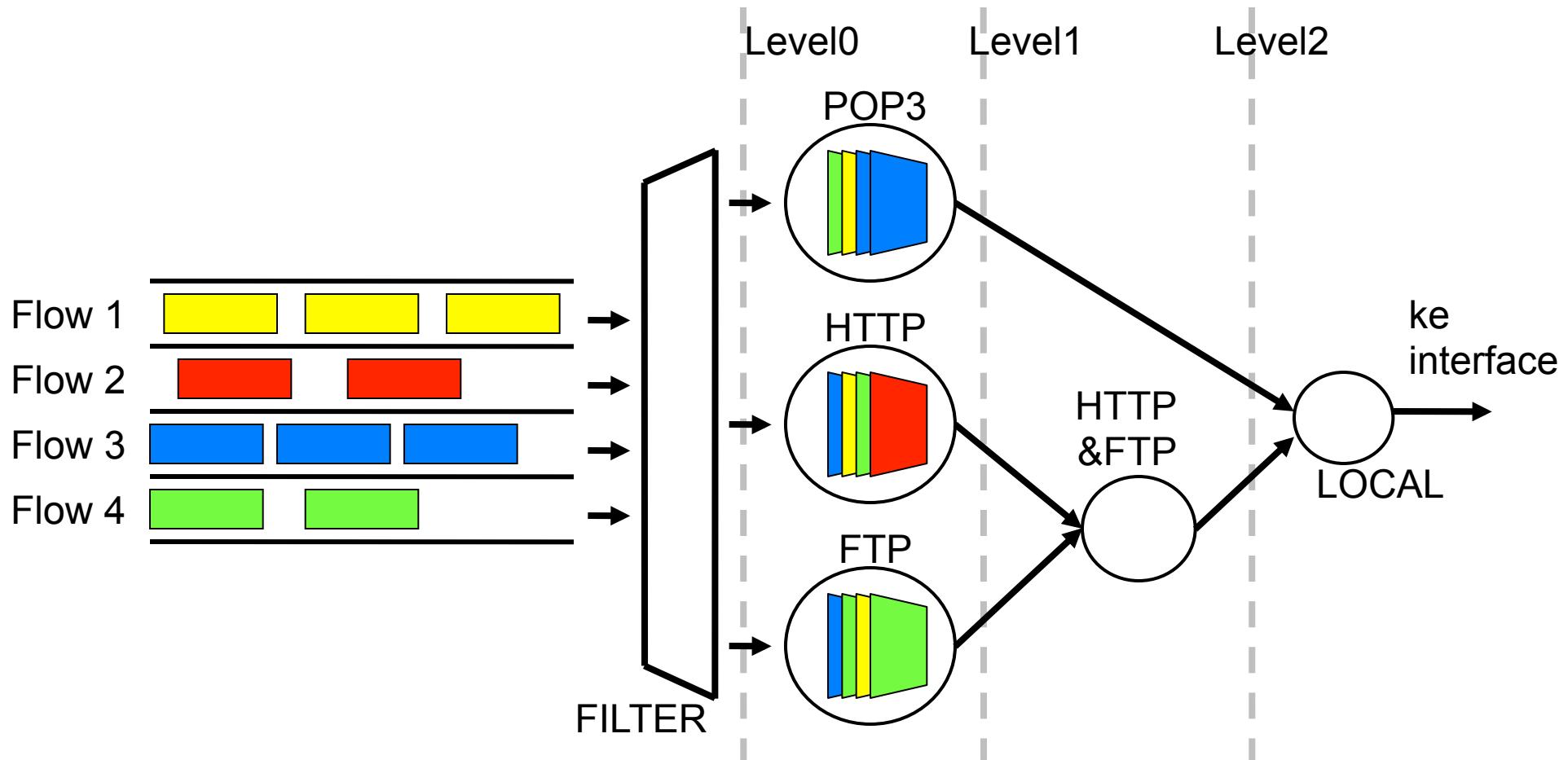
- Parameter mangle yang digunakan adalah “packet-mark”
- Khusus untuk “global-in” mangle harus dilakukan pada chain “prerouting”



HTB (Hierarchical Token Bucket)

- HTB adalah classful queuing discipline yang dapat digunakan untuk mengaplikasikan handling yang berbeda untuk beberapa jenis trafik.
- Secara umum, kita hanya dapat membuat 1 tipe queue untuk setiap interface. Namun dengan HTB di RouterOS, kita dapat mengaplikasikan properti yang berbeda-beda.
- HTB dapat melakukan prioritas untuk grup yang berbeda.

Skema Hirarki pada HTB





HTB States

- **hijau**
 - Posisi di mana data-rate lebih kecil dari limit-at.
 - Nilai limit-at pada kelas tersebut akan dilihat terlebih dahulu daripada parent classnya.
 - Contoh, sebuah class memiliki limit-at 512k, dan parent-nya memiliki limit-at 128k. Maka class tersebut akan selalu mendapatkan data-rate 512k.
- **kuning**
 - Posisi di mana data-rate lebih besar dari limit-at, namun lebih kecil dari max-limit.
 - Dijinkan atau tidaknya penambahan trafik bergantung pada :
 - posisi parent, jika prioritas class sama dengan parentnya dan parentnya dalam posisi kuning
 - posisi class itu sendiri, jika parent sudah berstatus kuning.
- **merah**
 - Posisi di mana data-rate sudah melebihi max-limit.
 - Tidak dapat lagi meminjam dari parentnya.



Staged Limitation

- Pada RouterOS, dikenal 2 buah limit:
 - CIR (Committed Information Rate)
 - dalam keadaan terburuk, client akan mendapatkan bandwidth sesuai dengan “**limit-at**” (dengan asumsi bandwidth yang tersedia cukup untuk CIR semua client)
 - MIR (Maximal Information Rate)
 - jika masih ada bandwidth yang tersisa setelah semua client mencapai “**limit-at**”, maka client bisa mendapatkan bandwidth tambahan hingga “**max-limit**”



Struktur HTB

- Setiap queue bisa menjadi parent untuk queue lainnya
- Semua child queue (tidak peduli berapa banyak level parentnya) akan berada pada level HTB yang sama (paling bawah)
- Semua Child queue akan mendapatkan trafik sekurang-kurangnya sebesar limit-at



Parent & Dual Limitation (1)

- Max-limit child harus kurang atau sama dengan max-limit parentnya :
 - $\text{max-limit}(\text{parent}) \geq \text{max-limit}(\text{child1})$
 - $\text{max-limit}(\text{parent}) \geq \text{max-limit}(\text{child2})$
 - $\text{max-limit}(\text{parent}) \geq \text{max-limit}(\text{childN})$
- Jika max-limit child lebih besar dari max-limit parent, maka child tidak akan pernah mendapatkan trafik sebesar max-limit child.



Parent & Dual Limitation (2)

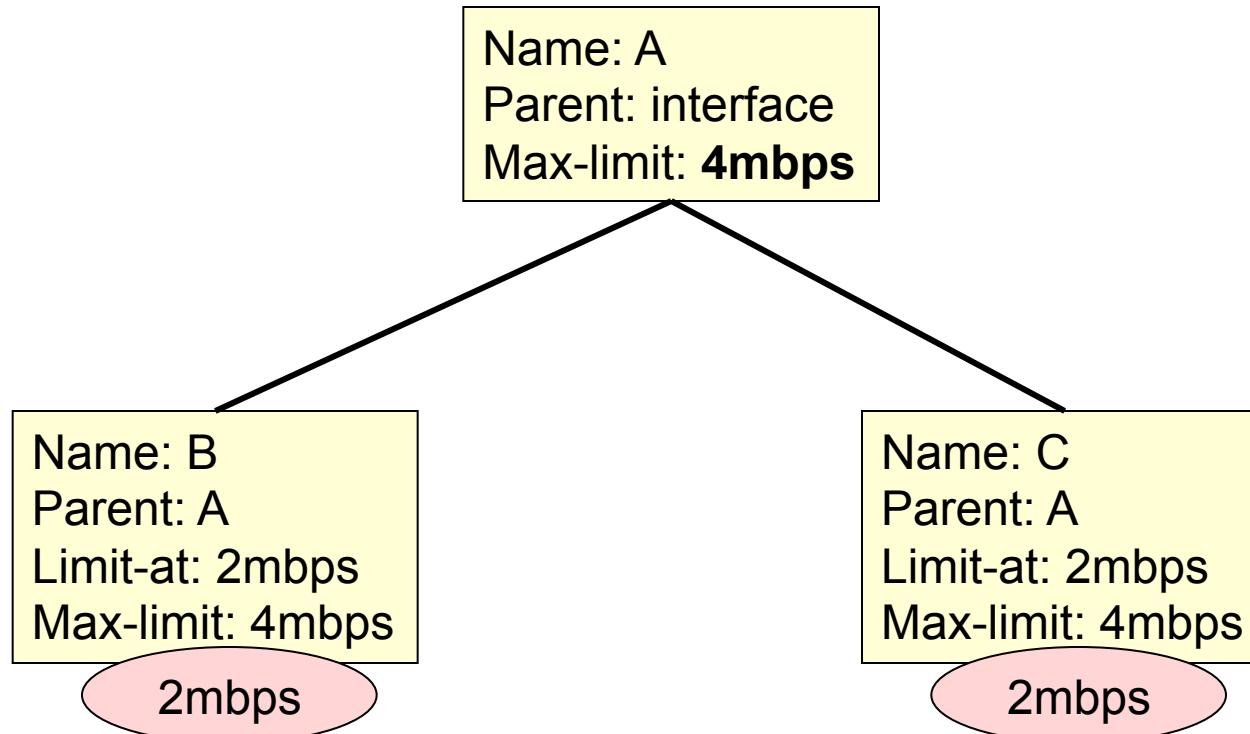
- Max-limit parent harus lebih besar atau sama dengan jumlah limit-at clientnya
 - $\text{max-limit}(\text{parent}) \geq \text{limit-at}(\text{child1}) + \dots + \text{limit-at}(\text{child}^*)$
- Contoh :
 - queue1 – limit-at=512k – parent=parent1
 - queue2 – limit-at=512k – parent=parent1
 - queue3 – limit-at=512k – parent=parent1
 - max-limit parent1 sekurang-kurangnya (512k*3), jika kurang, maka max-limit akan bocor



Tips

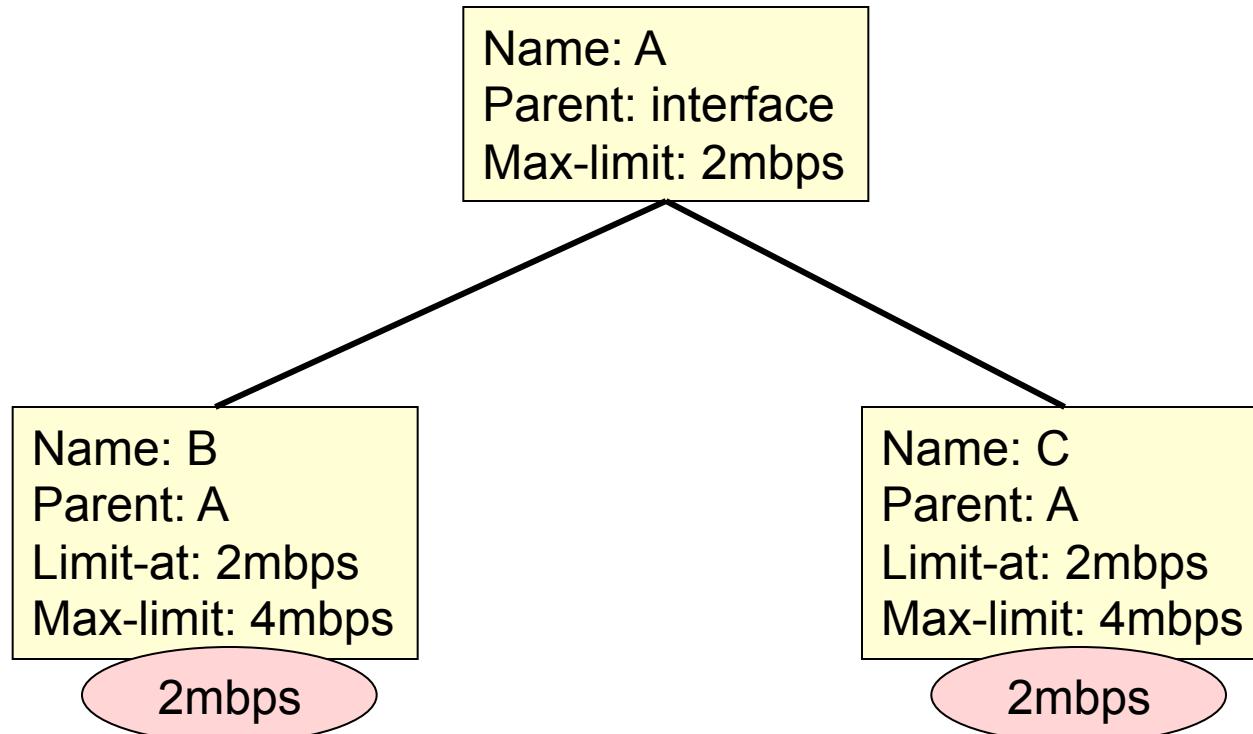
- Rule untuk parent paling atas, hanya membutuhkan max-limit, tidak membutuhkan limit-at dan priority
- Priority hanya bekerja pada child paling bawah
- Priority hanya berfungsi (diperhitungkan) untuk meminjam bandwidth yang tersisa dari parent setelah semua queue child mendapatkan limit-at nya.

HTB Distribution (1)



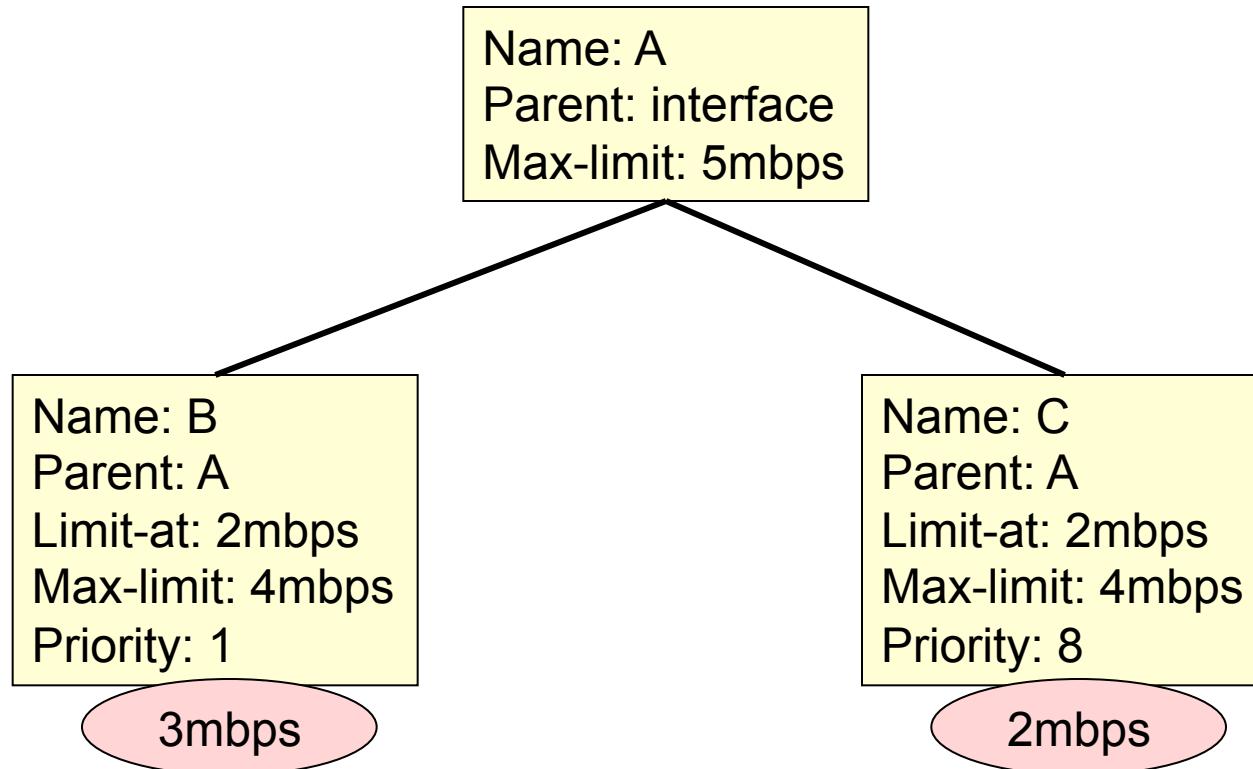
Jika semua menggunakan internet sebanyak-banyaknya, maka :
B dan C masing-masing akan mendapatkan 2mbps.
Jika C tidak menggunakan internet, maka B akan mendapatkan 4mbps.

HTB Distribution (2)



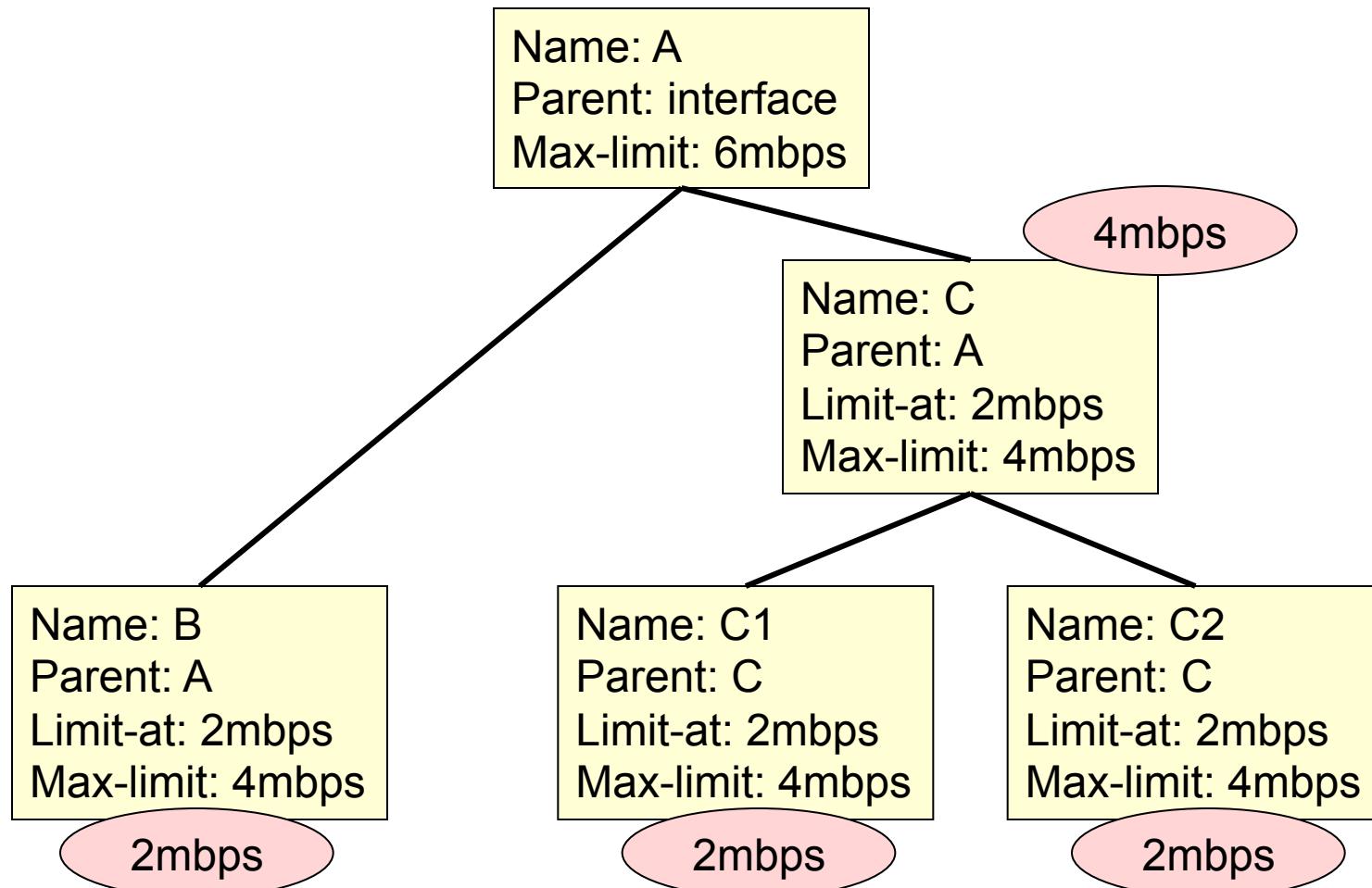
Meskipun max-limit A hanya 2mbps, tetapi B dan C masing-masing akan tetap mendapatkan 2 mbps. Max Limit parent harus \geq total limit-at client.
Jika B tidak menggunakan internet, C tetap hanya mendapatkan 2mbps, tidak bisa naik ke 4 mbps

HTB Distribution (3)



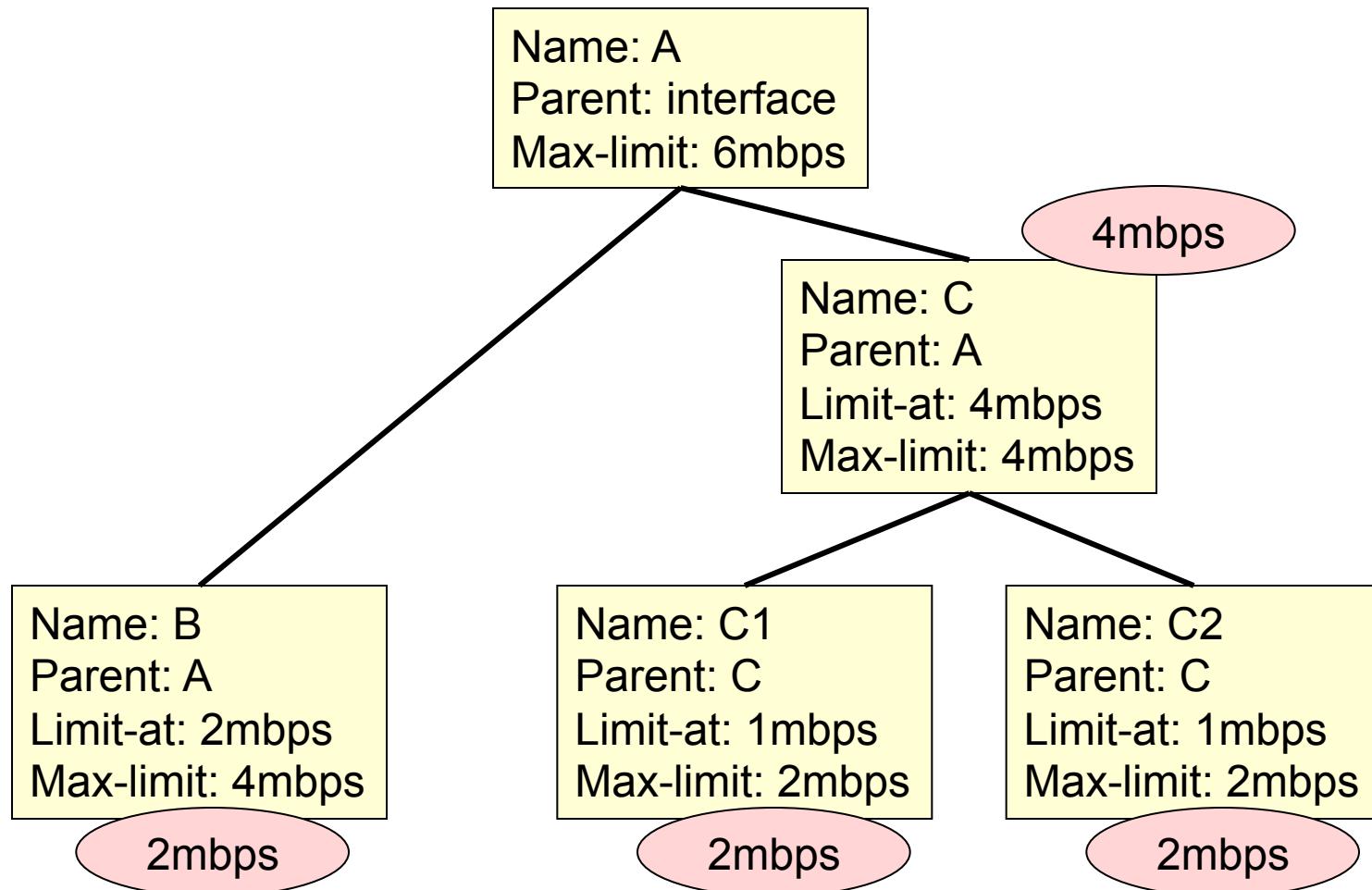
B memiliki prioritas (1) lebih tinggi dari pada C (8).

HTB Distribution (4)



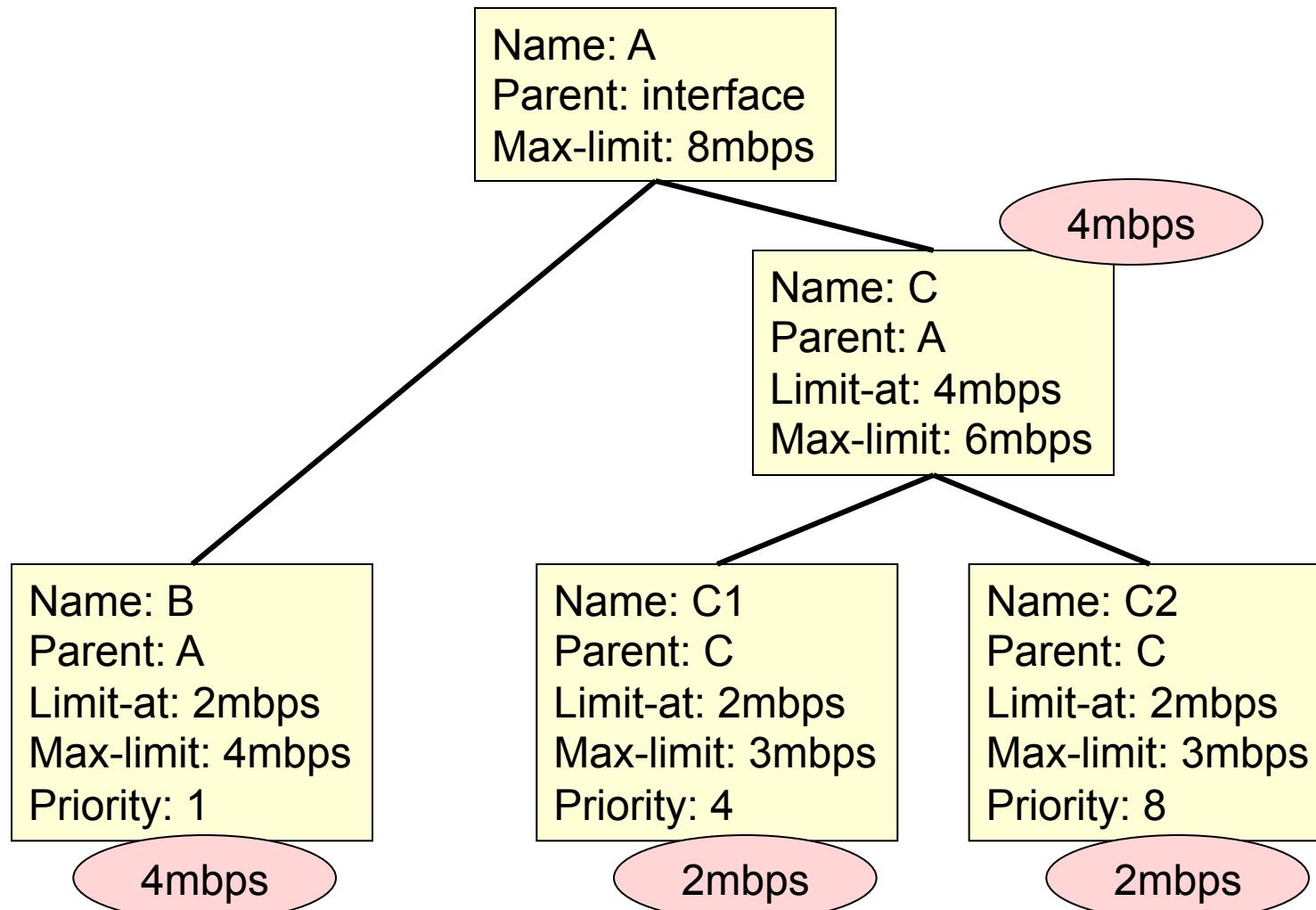
Client B, C1 dan C2, masing-masing akan mendapatkan 2mbps, sesuai dengan limit-at nya masing-masing

HTB Distribution (5)



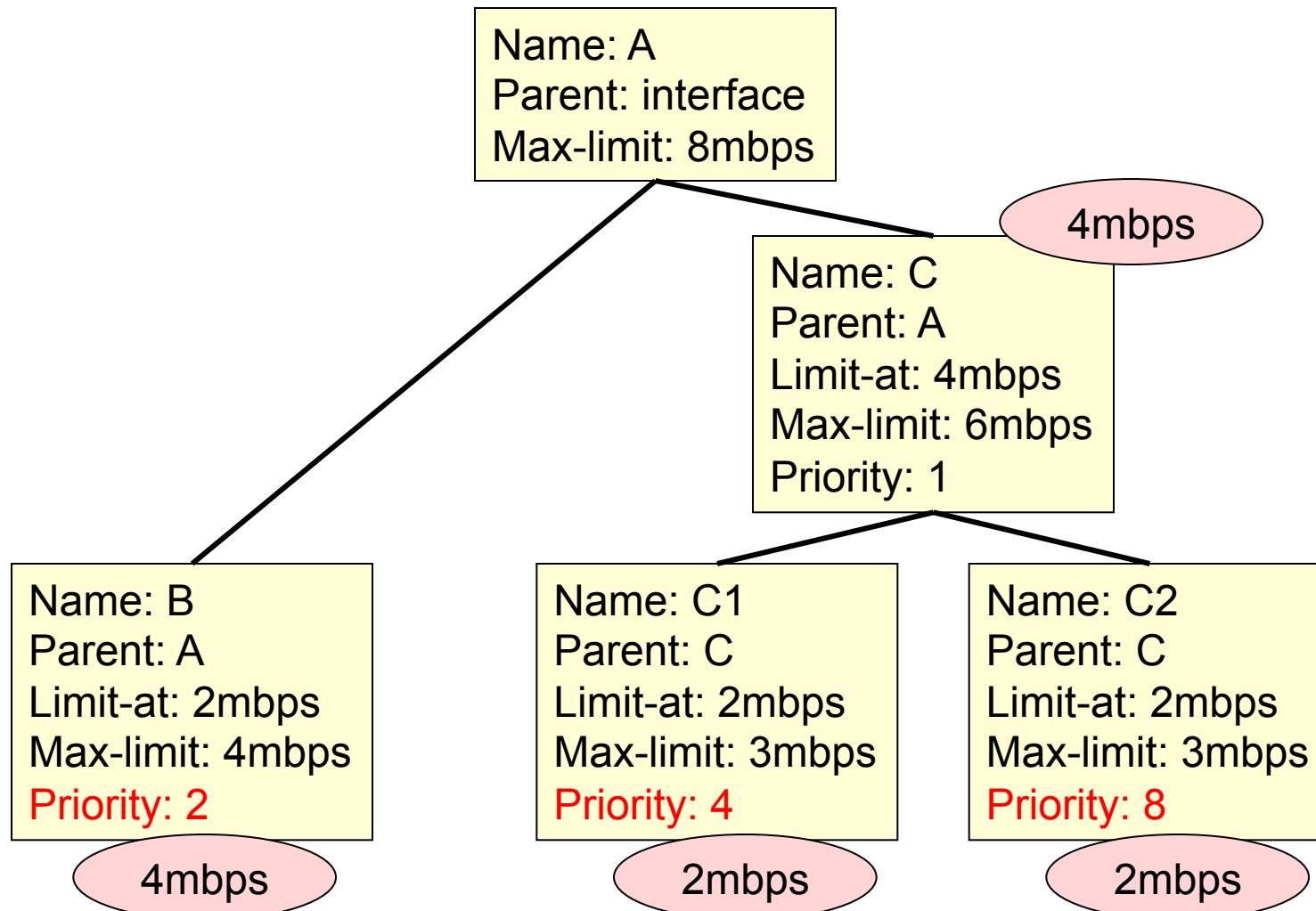
C1 dan C2 bisa naik hingga max-limit, karena parentnya (C) memiliki limit-at hingga 4mbps.

HTB Distribution (6)



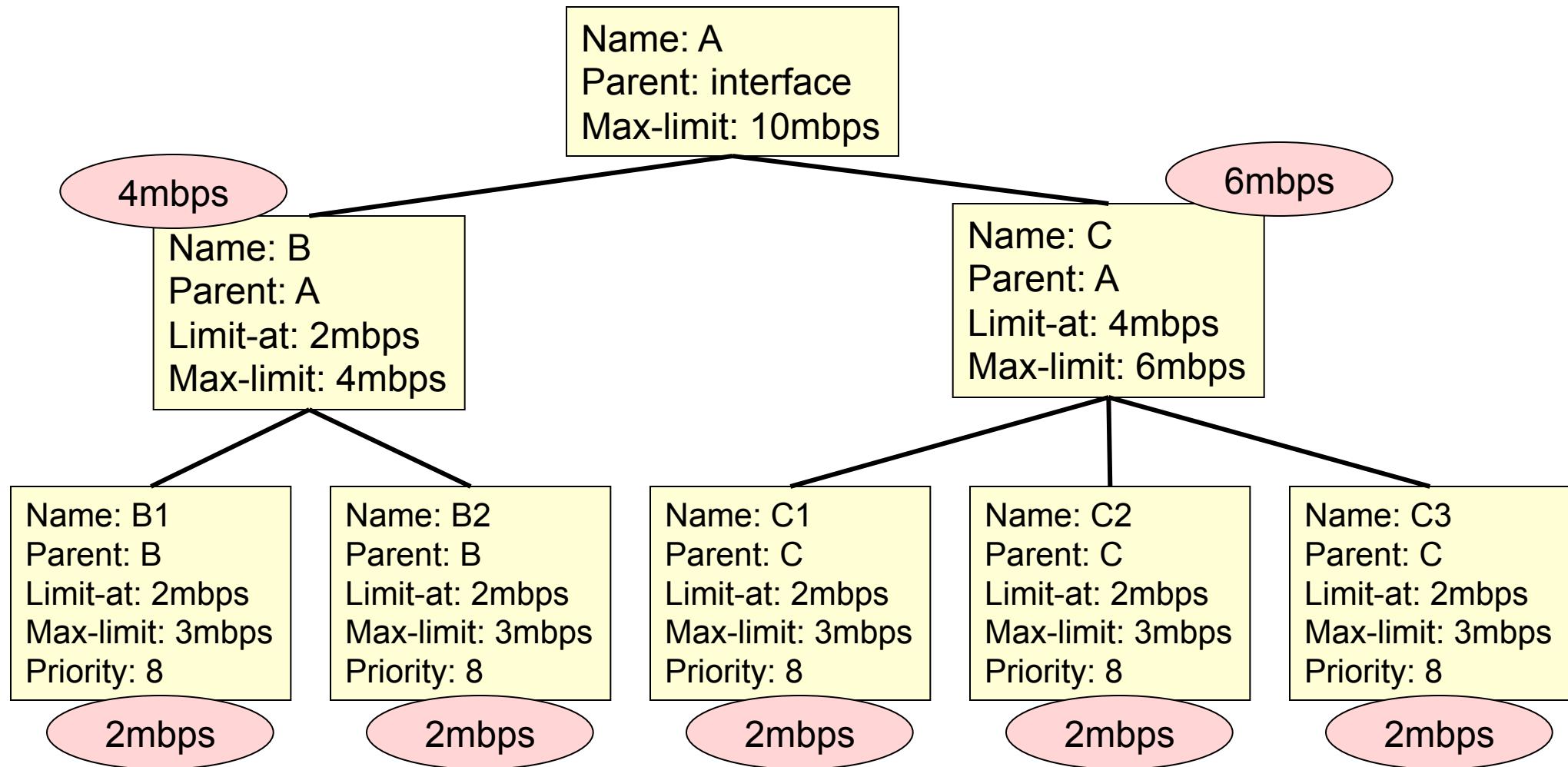
Pada saat semua limit-at sudah tercapai, sisa kapasitas akan dibagikan berdasarkan prioritas.

HTB Distribution (7)



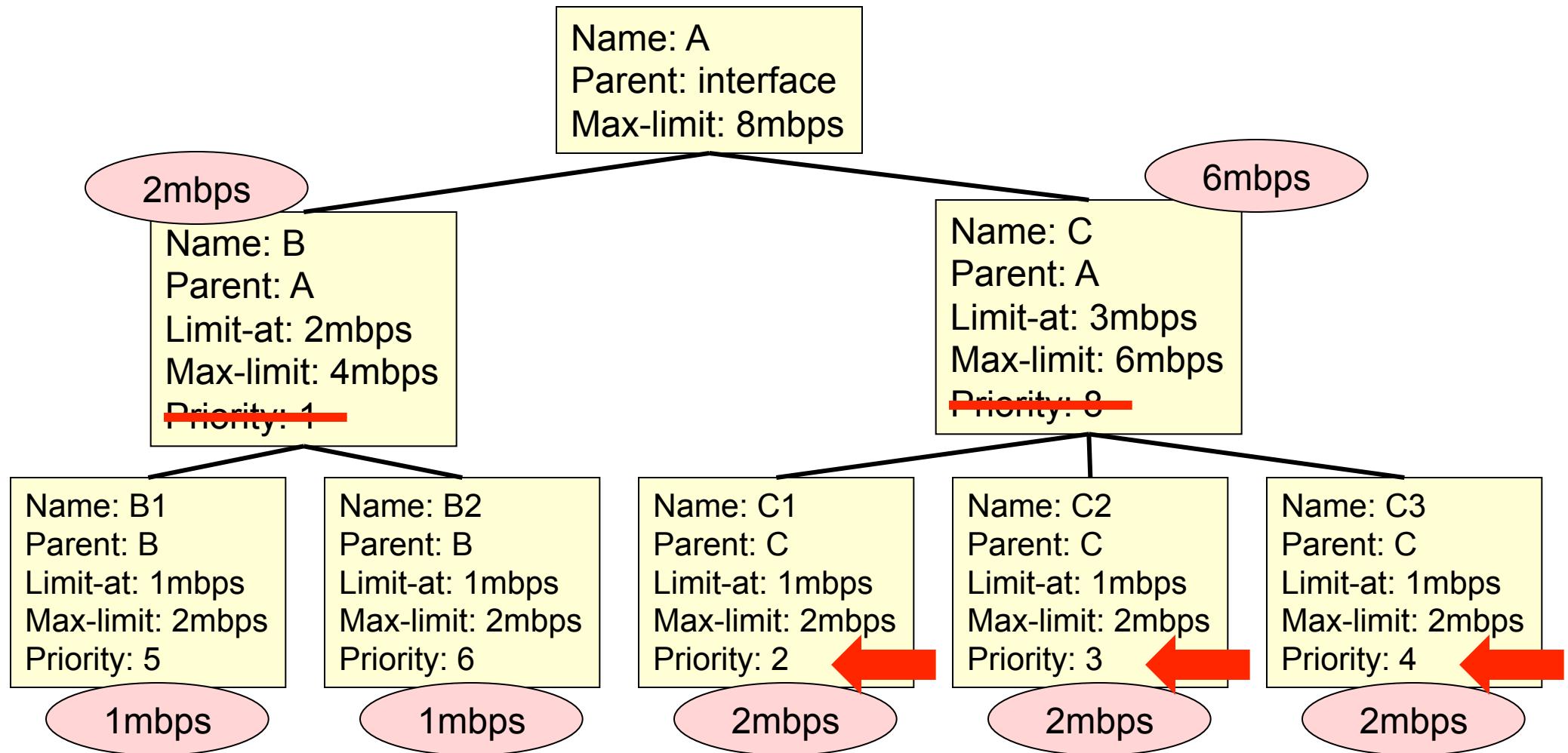
Priority pada parent (rule yang bukan level 0) tidak berpengaruh.

HTB Distribution (8)



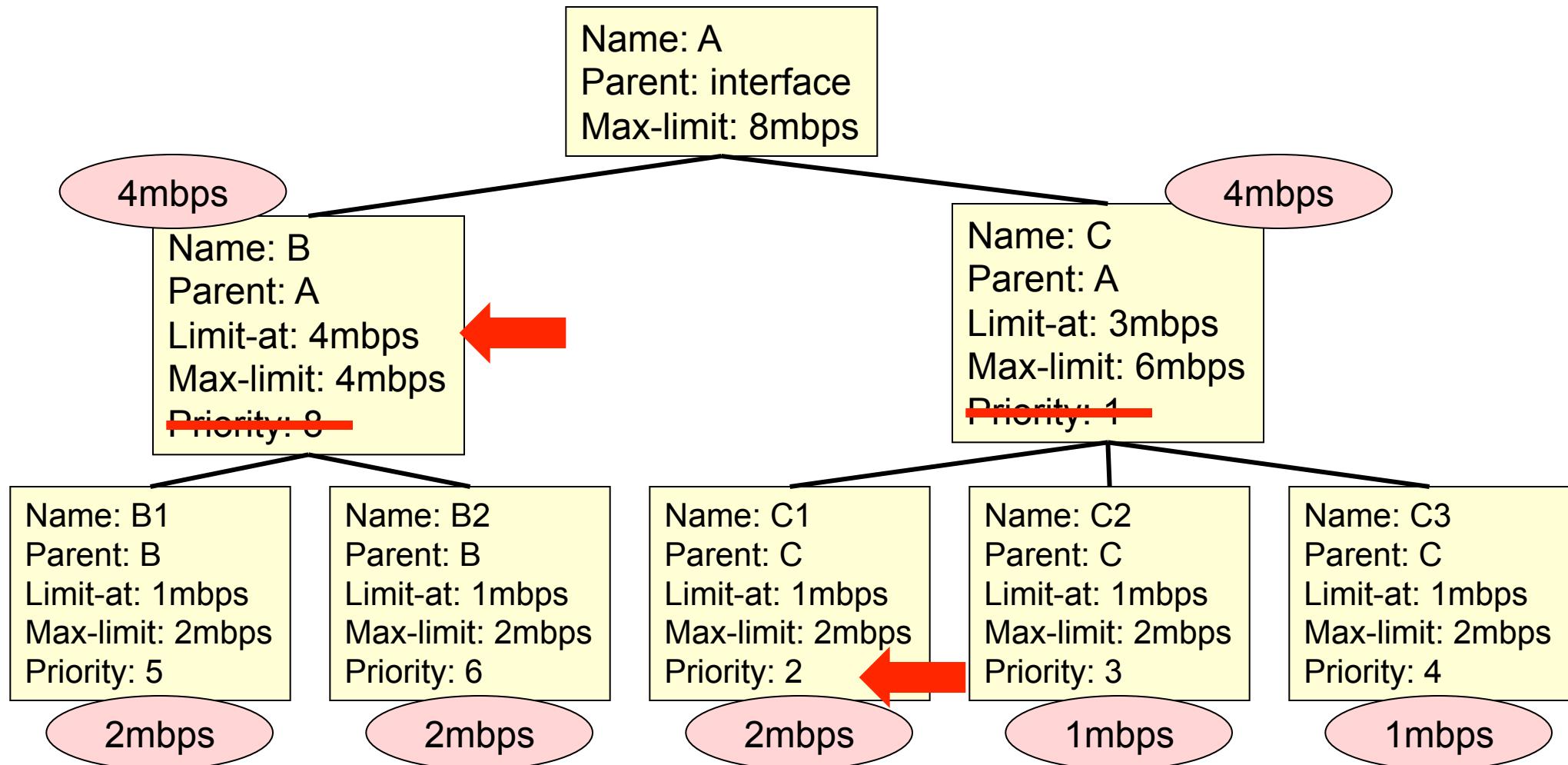
Semua child akan mendapatkan trafik 2mbps

HTB Distribution (9)



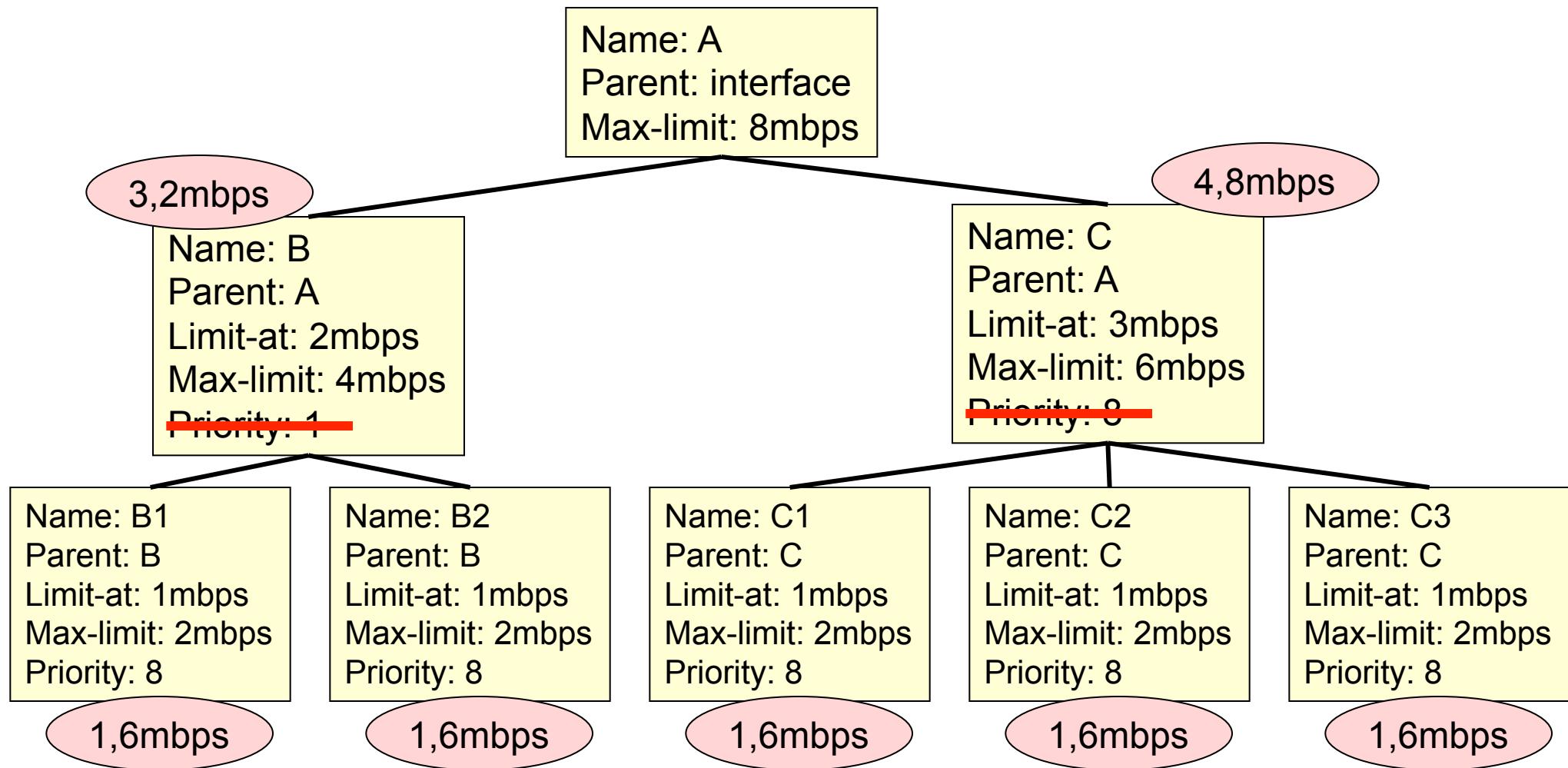
C1, C2, C3 mendapatkan 2mbps karena priority-nya lebih tinggi dari B1 dan B2

HTB Distribution (10)



Queue-B akan mendapatkan 4mbps karena limit-at nya.
C1 > C2 dan C1 > C3 karena priority-nya

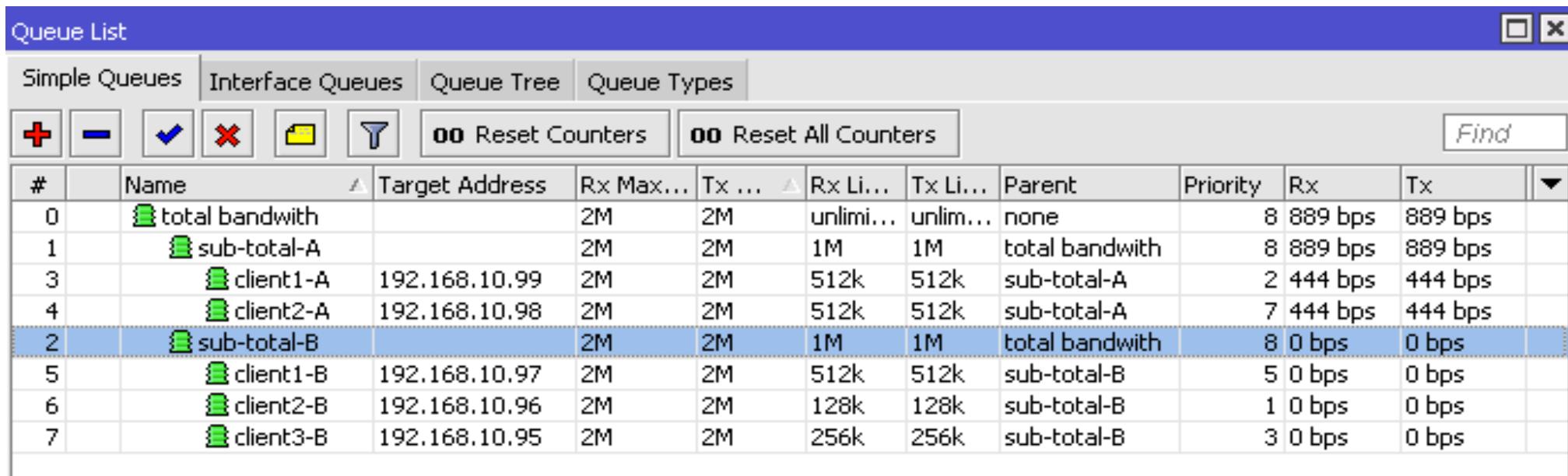
HTB Distribution (11)



Bandwidth dibagi rata ke semua child karena priority-nya sama

[LAB-2] HTB Implementation

- Silahkan lakukan pengecekan dan percobaan untuk contoh-contoh HTB di halaman sebelumnya.
- Tambahkan ip local network di Laptop untuk simulasi client
- Gunakan bandwidth test untuk simulasi traffincnya



The screenshot shows the 'Queue List' window in the MikroTik configuration interface. The window has a blue header bar with tabs: 'Simple Queues' (selected), 'Interface Queues', 'Queue Tree', and 'Queue Types'. Below the tabs are several buttons: a red plus sign, a minus sign, a checkmark, a red X, a yellow folder, and a filter icon. There are also two 'Reset' buttons: 'Reset Counters' and 'Reset All Counters'. A 'Find' input field is on the right. The main area is a table with the following data:

#	Name	Target Address	Rx Max...	Tx ...	Rx Li...	Tx Li...	Parent	Priority	Rx	Tx	
0	total bandwidth		2M	2M	unlim...	unlim...	none	8	889 bps	889 bps	
1	sub-total-A		2M	2M	1M	1M	total bandwidth	8	889 bps	889 bps	
3	client1-A	192.168.10.99	2M	2M	512k	512k	sub-total-A	2	444 bps	444 bps	
4	client2-A	192.168.10.98	2M	2M	512k	512k	sub-total-A	7	444 bps	444 bps	
2	sub-total-B		2M	2M	1M	1M	total bandwidth	8	0 bps	0 bps	
5	client1-B	192.168.10.97	2M	2M	512k	512k	sub-total-B	5	0 bps	0 bps	
6	client2-B	192.168.10.96	2M	2M	128k	128k	sub-total-B	1	0 bps	0 bps	
7	client3-B	192.168.10.95	2M	2M	256k	256k	sub-total-B	3	0 bps	0 bps	

Simple Queue

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Name: queue1

Target Address:

Target Upload Target Download

Max Limit: unlimited bits/s

Burst

Burst Limit: unlimited bits/s

Burst Threshold: unlimited bits/s

Burst Time: 0 s

Time

Time: 00:00:00 - 1d 00:00:00

sun mon tue wed thu fri sat

disabled

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

P2P:

Packet Marks:

Dst. Address:

Interface: all

Target Upload Target Download

Limit At: unlimited bits/s

Queue Type: default-small

Parent: none

Priority: 8

disabled

Simple queue is not simple anymore



Simple Queue

- Hanya bisa menggunakan parent Global-in dan global-out (dan global-total)
- Dalam satu rule, bisa langsung melimit trafik up, down, dan total
- Bisa menggunakan target address, atau menunjuk interface tempat client terkoneksi
- Bisa menggunakan lebih dari satu packet-mark
- Bisa menggunakan parameter waktu

Target Address

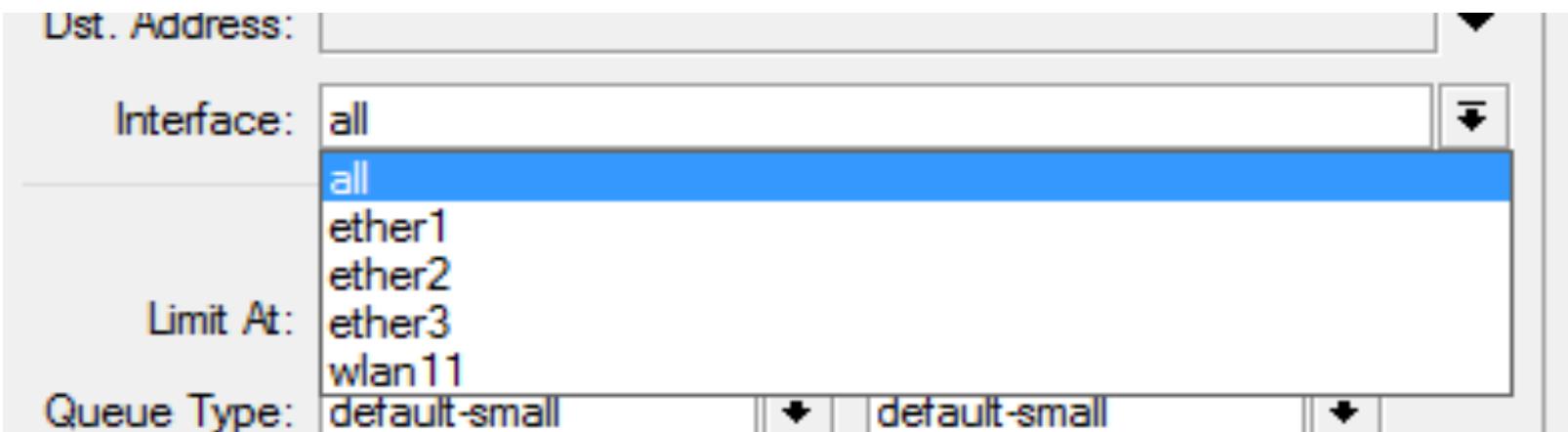
- Target address adalah IP Address yang ingin dilimit.
- Untuk 1 rule simple queue, kita bisa menentukan lebih dari 1 target address
- Router akan mengkalkulasi di interface mana terkoneksi target address
- Jika kita menentukan target address, biasanya kita tidak perlu menentukan interface

The screenshot shows the configuration of a queue named 'queue1'. The 'Name' field is set to 'queue1'. The 'Target Address' field contains three entries: '192.168.0.0/28', '192.168.0.128/28', and '192.168.0.192/28'. Under the 'Target Upload' and 'Target Download' sections, both checkboxes are checked. The 'Max Limit' field is set to 'unlimited' for both upload and download, with a unit of 'bits/s'. There is also a 'Burst' field at the bottom.

Name:	queue1		
Target Address:	192.168.0.0/28		
	192.168.0.128/28		
	192.168.0.192/28		
<input checked="" type="checkbox"/> Target Upload	<input checked="" type="checkbox"/> Target Download		
Max Limit:	unlimited	unlimited	bits/s
Burst			

Interface

- Interface adalah interface terkoneksi client. Kita perlu menentukan interface apabila kita tidak menyebutkan target address.

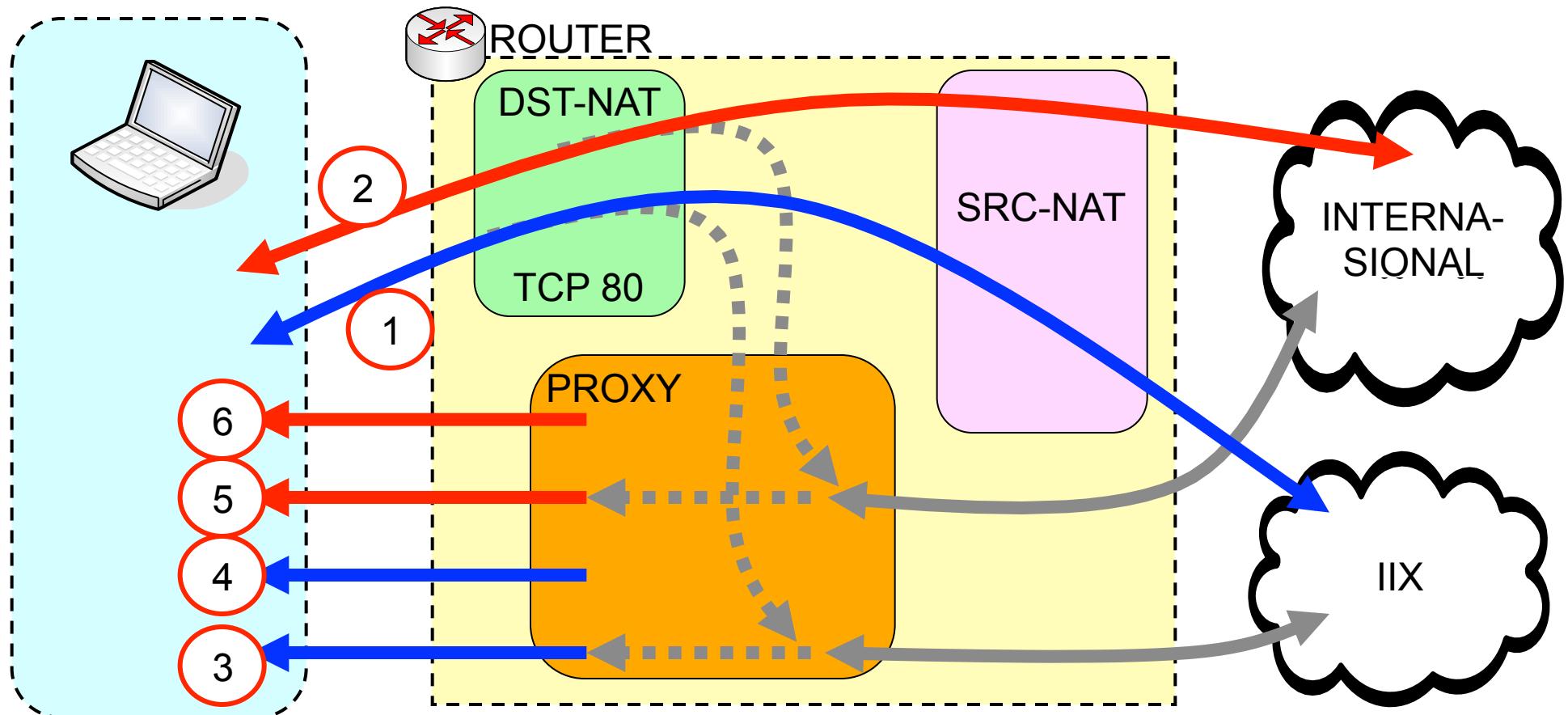




[LAB-3] Simple Queue

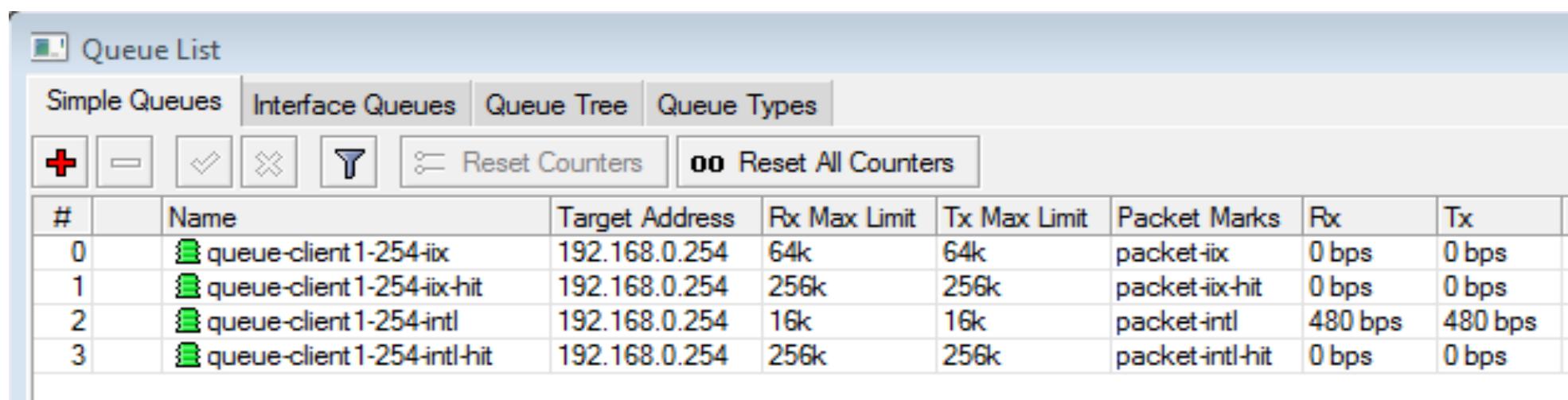
- Lanjutkanlah membuat simple queue untuk LAB yang telah kita lakukan pada materi Firewall “Dual gateway dengan internal proxy”
- Buatlah simple queue untuk trafik direct, miss, dan hit

Proxy dan Dual Gateway



1	Direct IIX	3	MISS IIX	5	MISS Intl
2	Direct Intl	4	HIT IIX	6	HIT Intl

Simple Queue



The screenshot shows the 'Queue List' interface in MikroTik. The top navigation bar includes tabs for 'Simple Queues' (selected), 'Interface Queues', 'Queue Tree', and 'Queue Types'. Below the tabs are several icons: a red plus sign for adding, a minus sign for deleting, a checkmark for selecting, a delete icon, a filter icon, and two buttons for 'Reset Counters' (one for individual and one for all). The main table displays four entries:

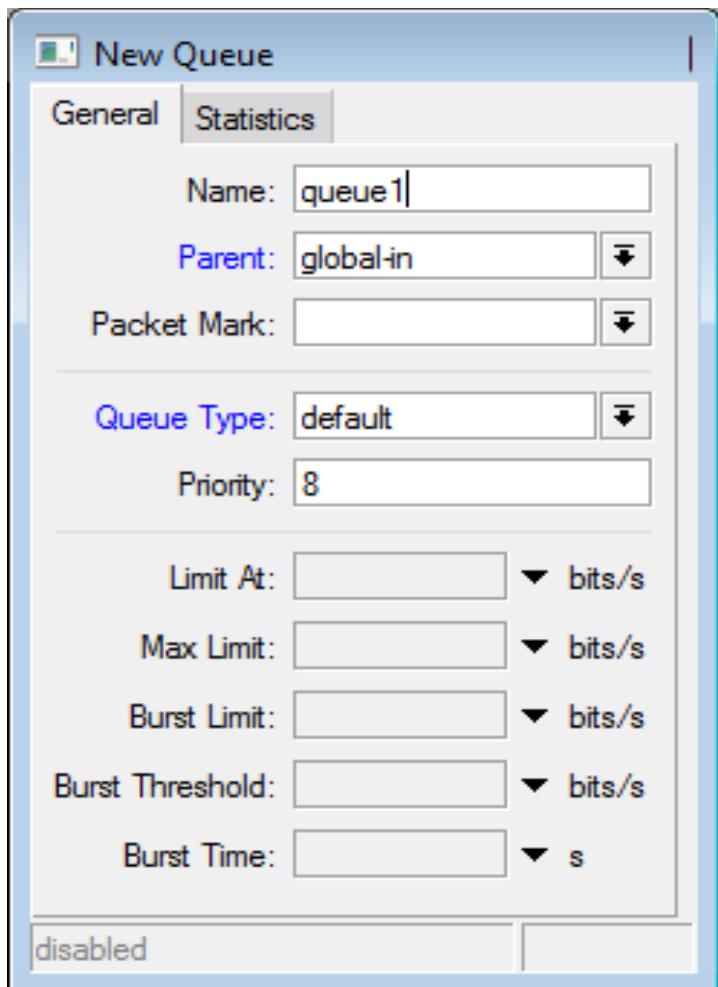
#	Name	Target Address	Rx Max Limit	Tx Max Limit	Packet Marks	Rx	Tx
0	queue-client1-254-iix	192.168.0.254	64k	64k	packet-iix	0 bps	0 bps
1	queue-client1-254-iix-hit	192.168.0.254	256k	256k	packet-iix-hit	0 bps	0 bps
2	queue-client1-254-intl	192.168.0.254	16k	16k	packet-intl	480 bps	480 bps
3	queue-client1-254-intl-hit	192.168.0.254	256k	256k	packet-intl-hit	0 bps	0 bps



Simple Queue

- 0 name="queue-client1-254-iix" target-
addresses=192.168.0.254/32 packet-marks=packet-iix
max-limit=64000/64000
- 1 name="queue-client1-254-iix-hit" target-
addresses=192.168.0.254/32 packet-marks=packet-iix-
hit max-limit=256000/256000
- 2 name="queue-client1-254-intl" target-
addresses=192.168.0.254/32 packet-marks=packet-intl
max-limit=16000/16000
- 3 name="queue-client1-254-intl-hit" target-
addresses=192.168.0.254/32 packet-marks=packet-intl-
hit max-limit=256000/256000

Queue Tree



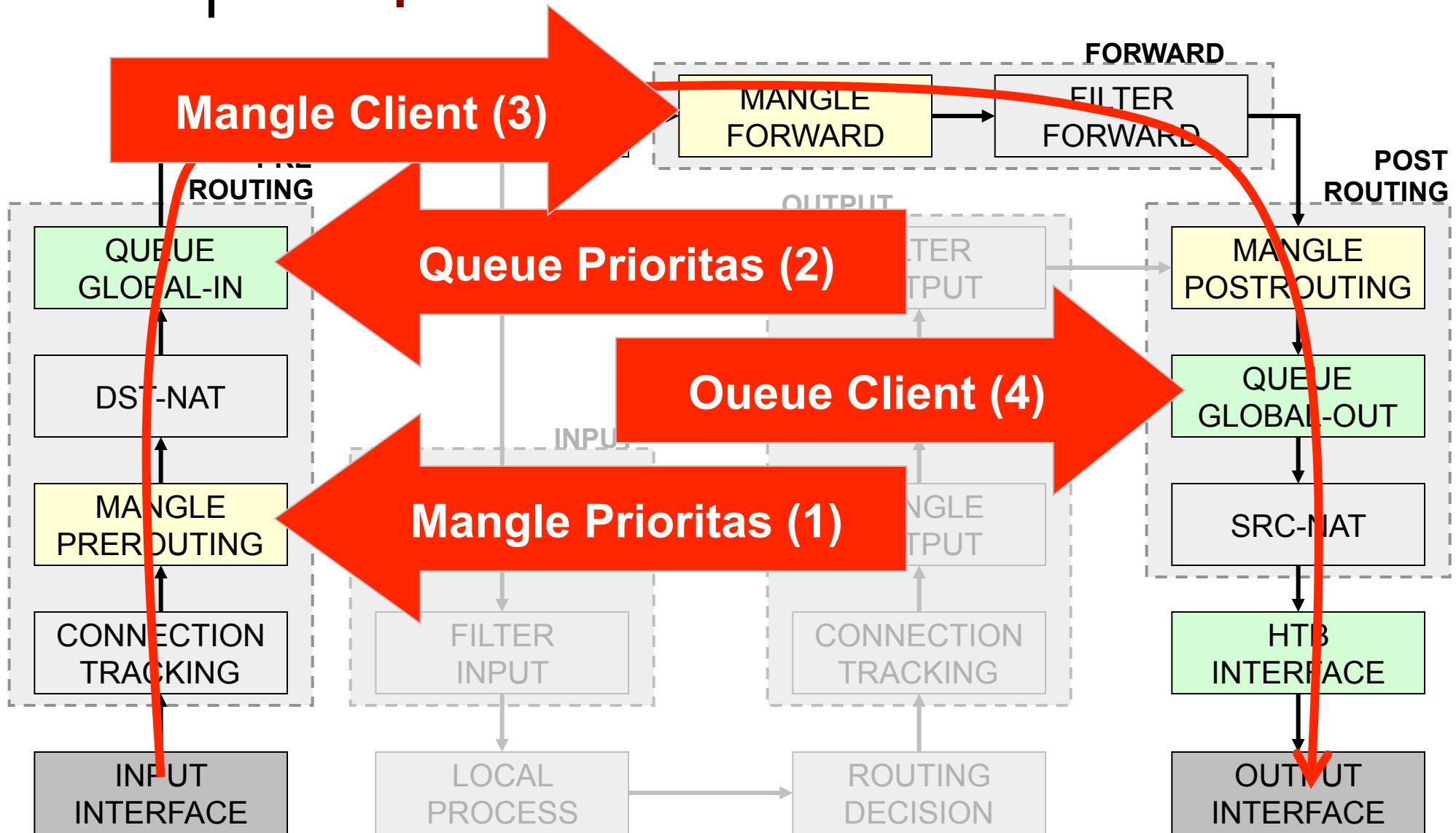
- Konfigurasi queue tree jauh lebih sederhana daripada simple queue.
- Keunggulan queue tree, kita bisa memilih untuk menggunakan interface queue.
- Tetapi bisa menjadi lebih kompleks karena harus menggunakan Mangle.



[LAB-4] Queue Tree

- Lanjutkanlah membuat queue tree untuk mengatur prioritas trafik, melanjutkan yang sudah dilakukan pada LAB di materi Firewall.
- Lakukanlah Dual Limitasi (prioritas trafik dan juga melimit koneksi user)

Simple Packet Flow





Mangle Client - 1

- 6 chain=forward action=mark-connection new-connection-mark=conn-client1 passthrough=yes src-address=192.168.5.1-192.168.5.100
- 7 chain=forward action=mark-packet new-packet-mark=packet-client1-upload passthrough=no out-interface=wlan1 connection-mark=conn-client1
- 8 chain=forward action=mark-packet new-packet-mark=packet-client1-download passthrough=no out-interface=ether1 connection-mark=conn-client1



Mangle Client - 2

- 9 chain=forward action=mark-connection new-connection-mark=conn-client2 passthrough=yes src-address=192.168.5.101-192.168.5.254
- 10 chain=forward action=mark-packet new-packet-mark=packet-client2-upload passthrough=no out-interface=wlan1 connection-mark=conn-client2
- 11 chain=forward action=mark-packet new-packet-mark=packet-client2-download passthrough=no out-interface=ether1 connection-mark=conn-client2



Mangle Client - 3

- 12 chain=forward action=mark-connection new-connection-mark=conn-client3 passthrough=yes src-address=10.5.50.0/24
- 13 chain=forward action=mark-packet new-packet-mark=packet-client3-upload passthrough=no out-interface=wlan1 connection-mark=conn-client3
- 14 chain=forward action=mark-packet new-packet-mark=packet-client3-download passthrough=no out-interface=ether2 connection-mark=conn-client3

Queue-tree

Queue List												
Simple Queues		Interface Queues		Queue Tree		Queue Types						
+	-	✓	✗	✖	✖	Filter	Reset Counters		Reset All Counters			
Name	Parent	Packet Marks	Priority	Limit At...	Max Limit...	Avg. Rate	Queued Bytes	Bytes	Packets	PCQ Queues		
priority browsing	global-in	packet-browsing	1			8.5 kbps	0 B	81.2 MiB	234 935			
priority email	global-in	packet-email	2			0 bps	0 B	31.5 KiB	516			
priority remote	global-in	packet-remote	3			0 bps	0 B	13.0 KiB	149			
total upload	global-out		8		10M	20.3 kbps	0 B	203.4 MiB	598 454			
queue-client1-upload	total upload	packet-client1-upload	8	3M	10M	19.5 kbps	0 B	36.5 MiB	170 517	5		
queue-client2-upload	total upload	packet-client2-upload	8	3M	10M	408 bps	0 B	5.8 MiB	20 895	1		
queue-client3-upload	total upload	packet-client3-upload	8	3M	10M	344 bps	0 B	158.8 MiB	402 901	1		
total-download	global-out		8		10M	59.2 kbps	0 B	288.6 MiB	351 186			
queue-client1-downl...	total-download	packet-client1-download	8	3M	10M	48.8 kbps	0 B	146.7 MiB	217 547	5		
queue-client2-downl...	total-download	packet-client2-download	8	3M	10M	10.1 kbps	0 B	18.6 MiB	21 920	2		
queue-client3-downl...	total-download	packet-client3-download	8	3M	10M	232 bps	0 B	135.3 MiB	123 661	1		



Advanced Mikrotik Training

Traffic Control

(LAB Session)



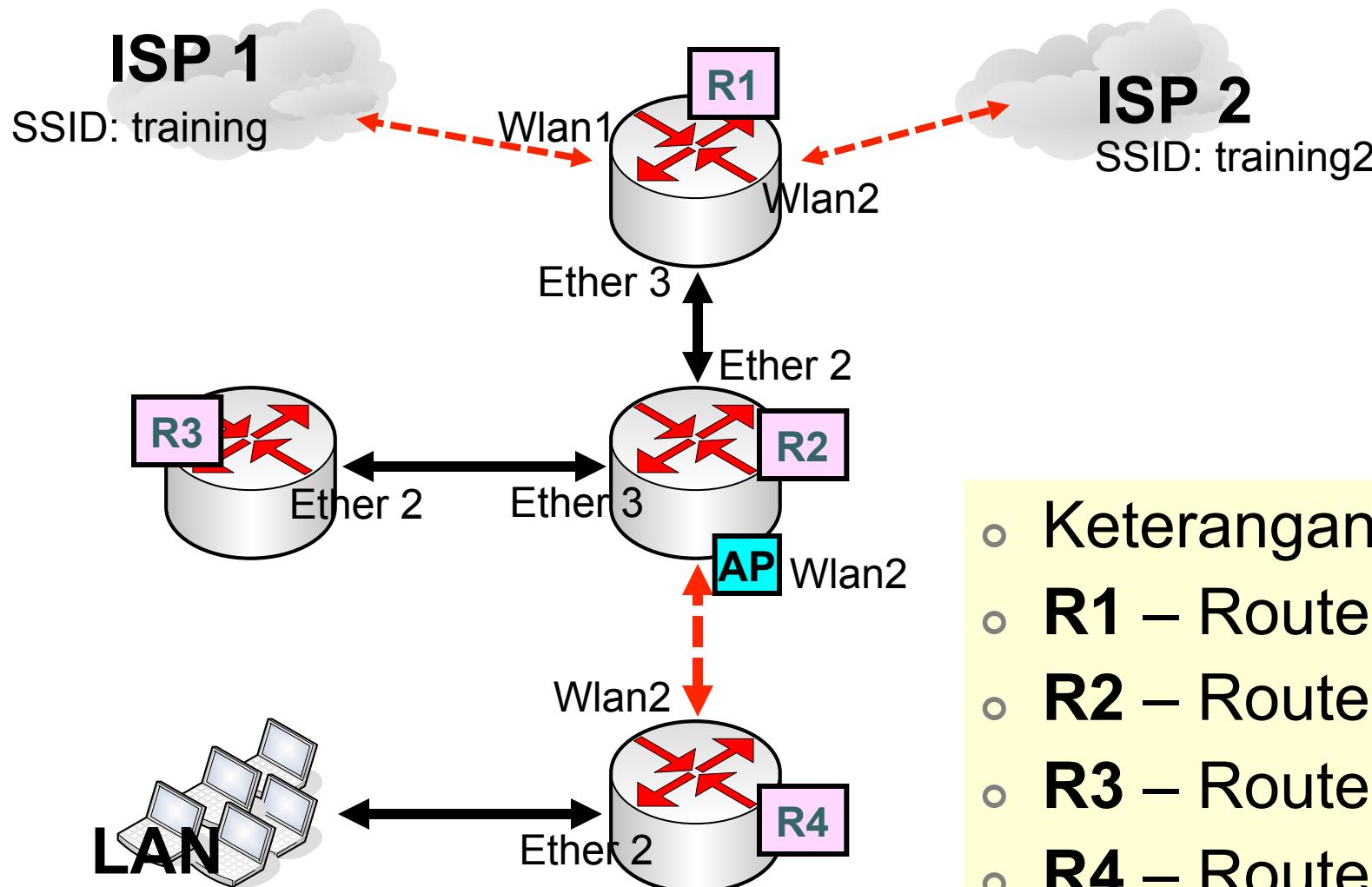
Certified Mikrotik Training - Advanced Class (MTCTCE)
Organized by: Citraweb Nusa Infomedia
(Mikrotik Certified Training Partner)



KONSEP

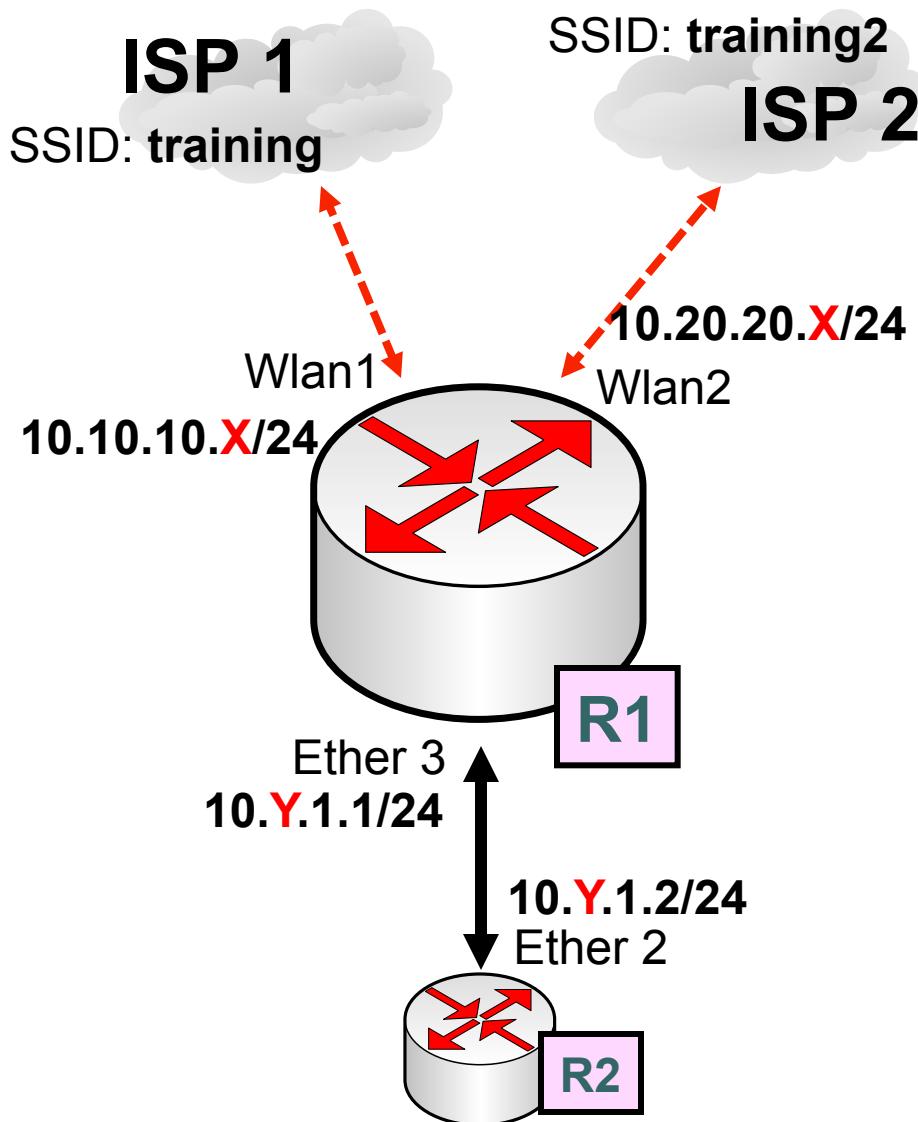
- Lab Praktek ini dibuat berkelompok, dengan memanfaatkan 4 router dan 4 Peserta.
- Tiap kelompok membuat konfigurasi beberapa router sehingga lengkap menjadi sebuah sistem kerja ISP yang sudah mengimplementasikan Materi Traffic Control.

Network Topology



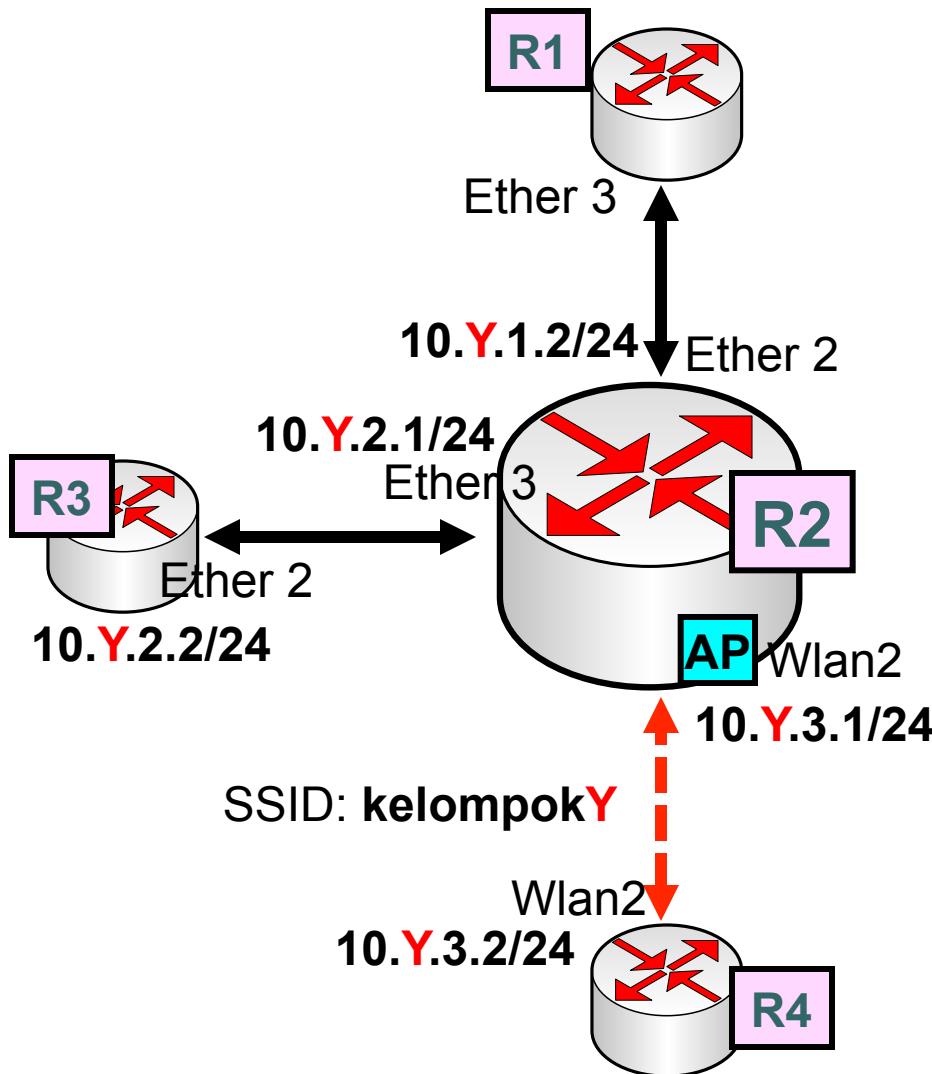
- Keterangan :
- **R1** – Router Backbone
- **R2** – Router BM
- **R3** – Router Proxy
- **R4** – Router Distribusi

R1 – Router Backbone



- Router R1 sebagai Router backbone terkoneksi dengan 2 ISP menggunakan wireless.
- Konfigurasi LoadBalance ke kedua ISP menggunakan metode PCC.
- Aktifkan NAT untuk semua koneksi internet.
- Gunakan routing untuk interkoneksi seluruh network kelompok.

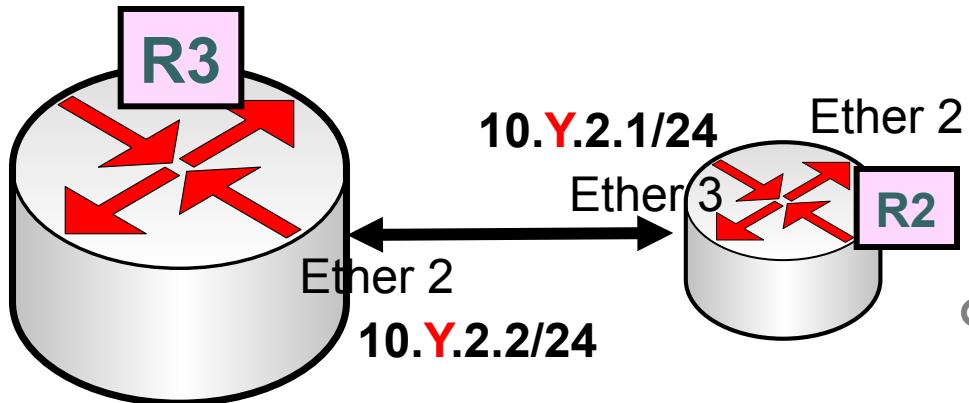
R2 – Router BM



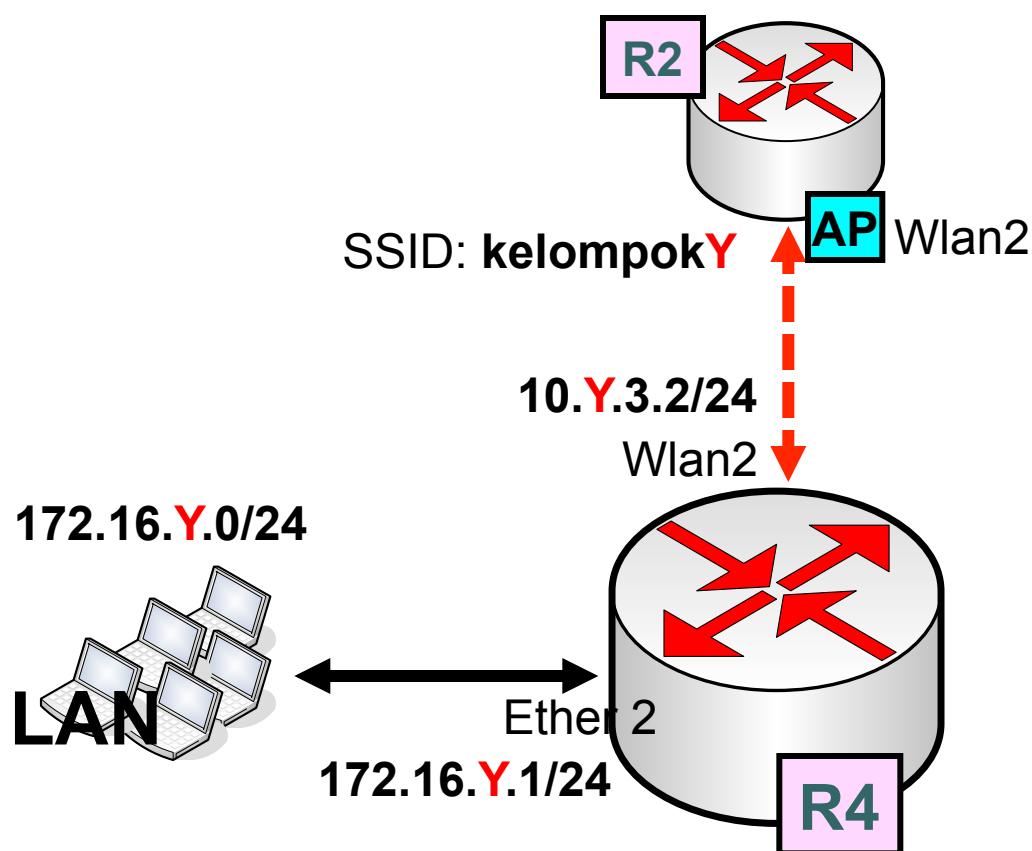
- Router R2 adalah sebagai Router Bandwidth Management.
- Konfigurasi routing untuk interkoneksi seluruh network kelompok.
- Pisahkan bandwidth Internet dan IIX secara **Merata** untuk semua traffic (proxy dan client).
- Gunakan mark routing untuk membelokkan traffic web ke proxy.
- Bypass khusus traffic HIT dari Proxy.

R3 – Router Proxy

- **Router R3** adalah sebagai Router Proxy.
- Aktifkan proxy dan juga fungsi cache untuk menyimpan object dari website.
- Gunakan semua filter (proxy / firewall / DNS) untuk melakukan block website yang berhubungan dengan pornografi.



R4 – Router Distribusi



- Router **R4** adalah sebagai Router Distribusi.
- Konfigurasi bandwidth **merata** di semua client berdasarkan protocol :
 - TCP
 - UDP
 - ICMP
- Pastikan koneksi internet client (LAN) tidak bisa menggunakan free proxy contohnya menggunakan program “Ultrasurf”



Selamat Mengerjakan !



info@mikrotik.co.id

Dijinkan menggunakan sebagian atau seluruh materi pada modul ini, baik berupa ide, foto, tulisan, konfigurasi, diagram, selama untuk kepentingan pengajaran, dan memberikan kredit dan link ke www.mikrotik.co.id