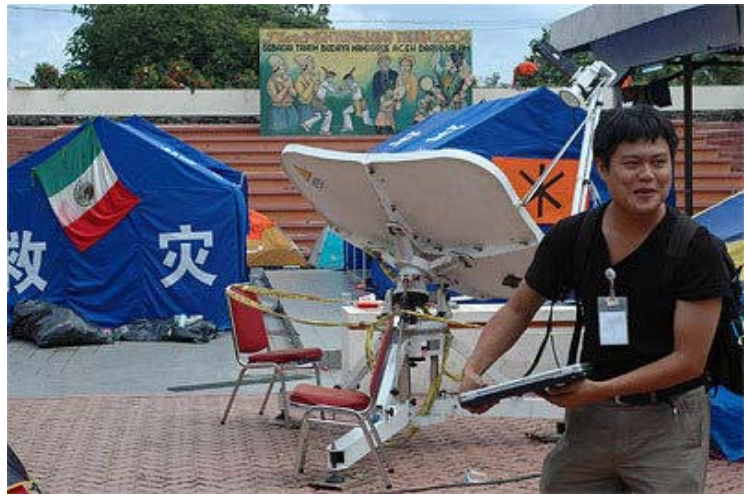
The Magic of
IP Flow

Valens Riyadi
info@mikrotik.co.id
Citraweb Nusa Infomedia
on Mikrotik User Meeting, Krakow
January 25 – 26, 2007

Introduction



- Name: Valens Riyadi
- Country: Indonesia
  - Graduated as Architect 1998
  - 1998 ….. Web developer
  - 2001 ….. Make a WISP
  - 2002 ….. Mikrotik Reseller
  - Photographer
    - Administrator of www.fotografer.net
  - Head of Security Dept, Indonesian ISP Association
  - Volunteer for Airputih Foundation, IT Emergency Task Force
  - Steering Committee for ID-SIRTII
    Indonesia Security Incident Response Team on Information Infrastructure
  - Mikrotik Certified Consultant

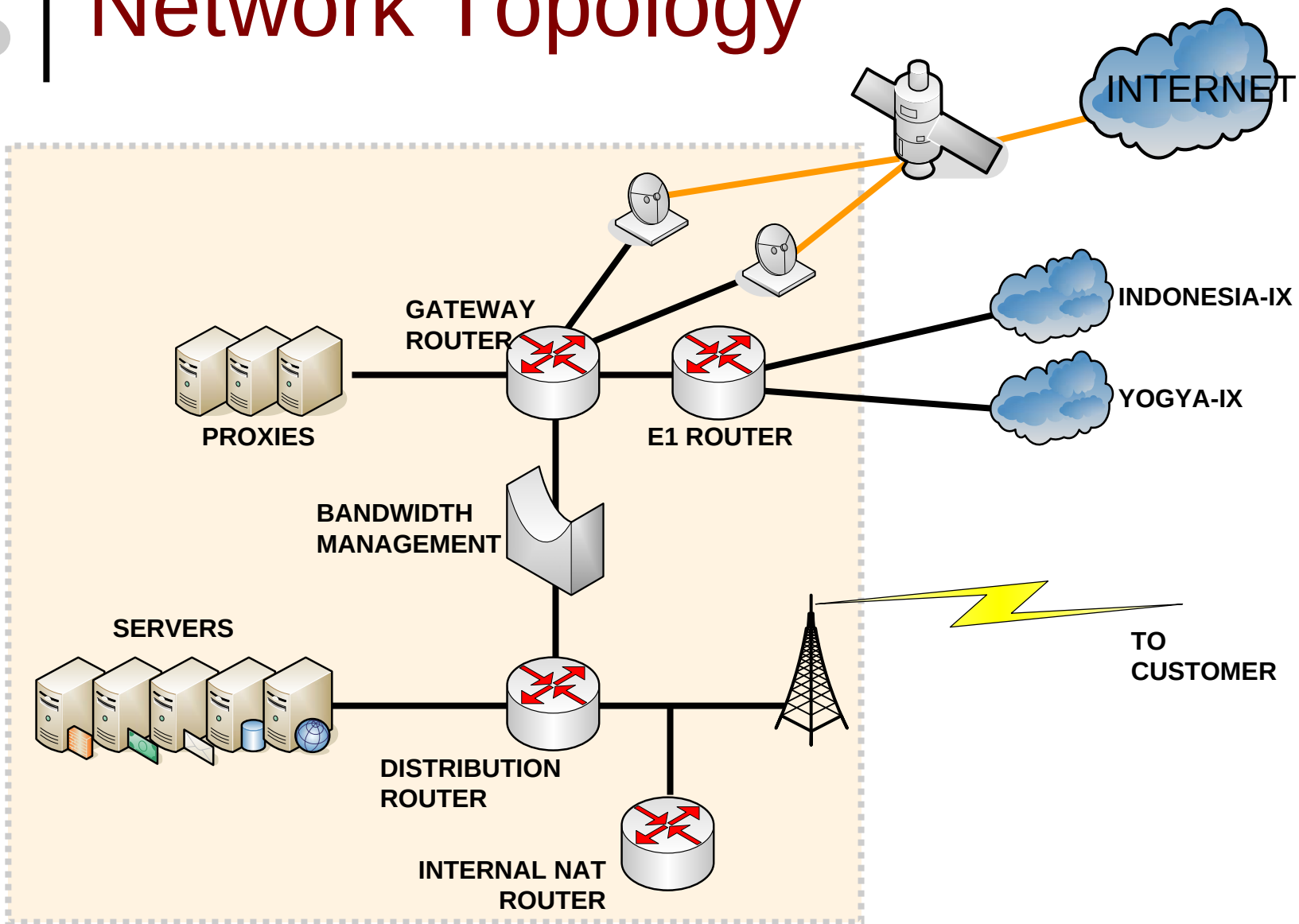
My Company

- Citraweb Nusa Infomedia
  - Web Developer (since 2000)
  - Small ISP (since 2001)
  - Mikrotik Reseller (since 2002)
- Located at : Yogyakarta Indonesia
- Using RouterOS since 2.3.15

Yogyakarta City

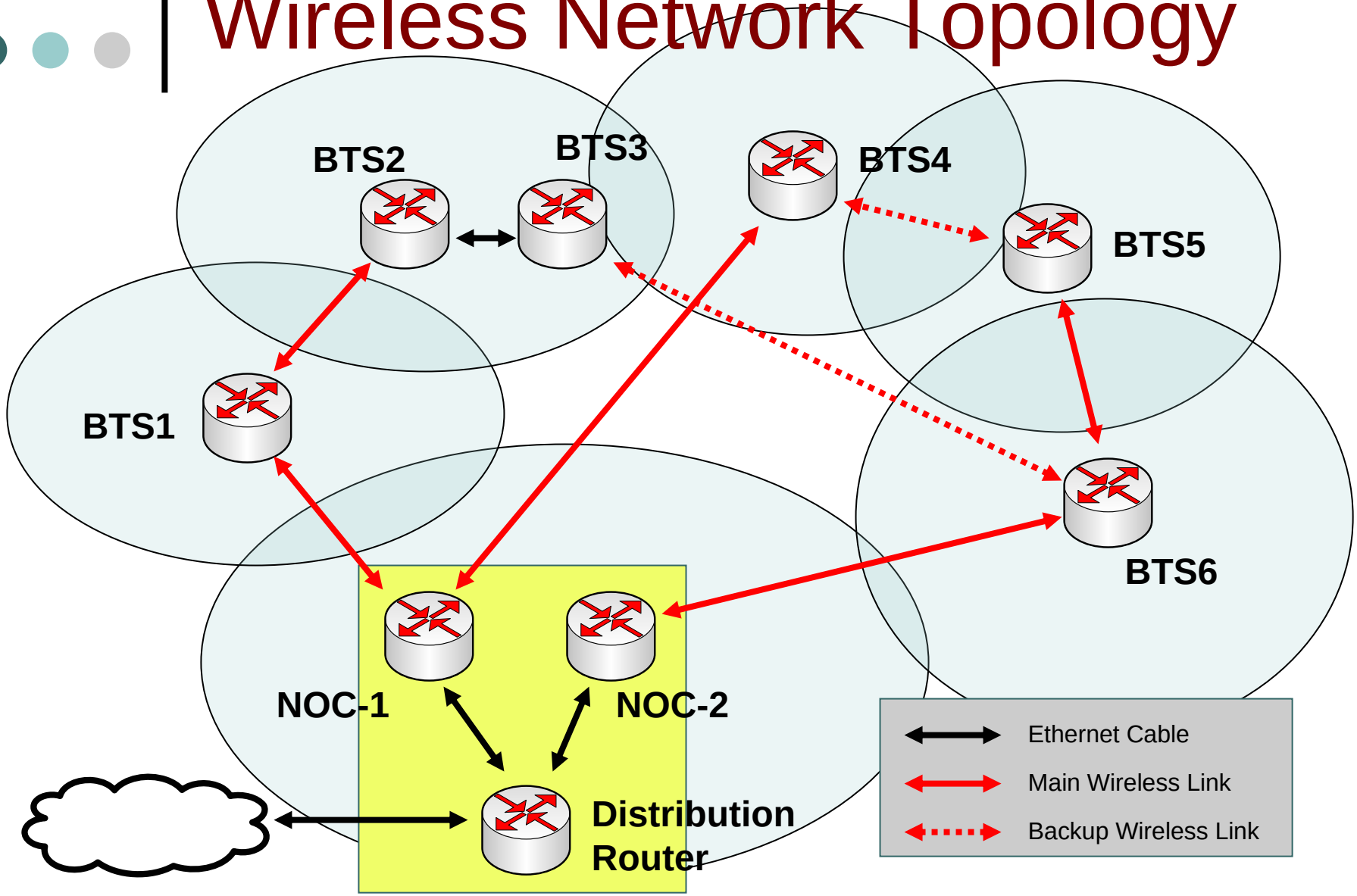
- 3,4 million of population
  - Tourism City
  - Student City
    - Almost 50% of population are students from other cities.
  - Finally ……. Cyber café City

Network Topology

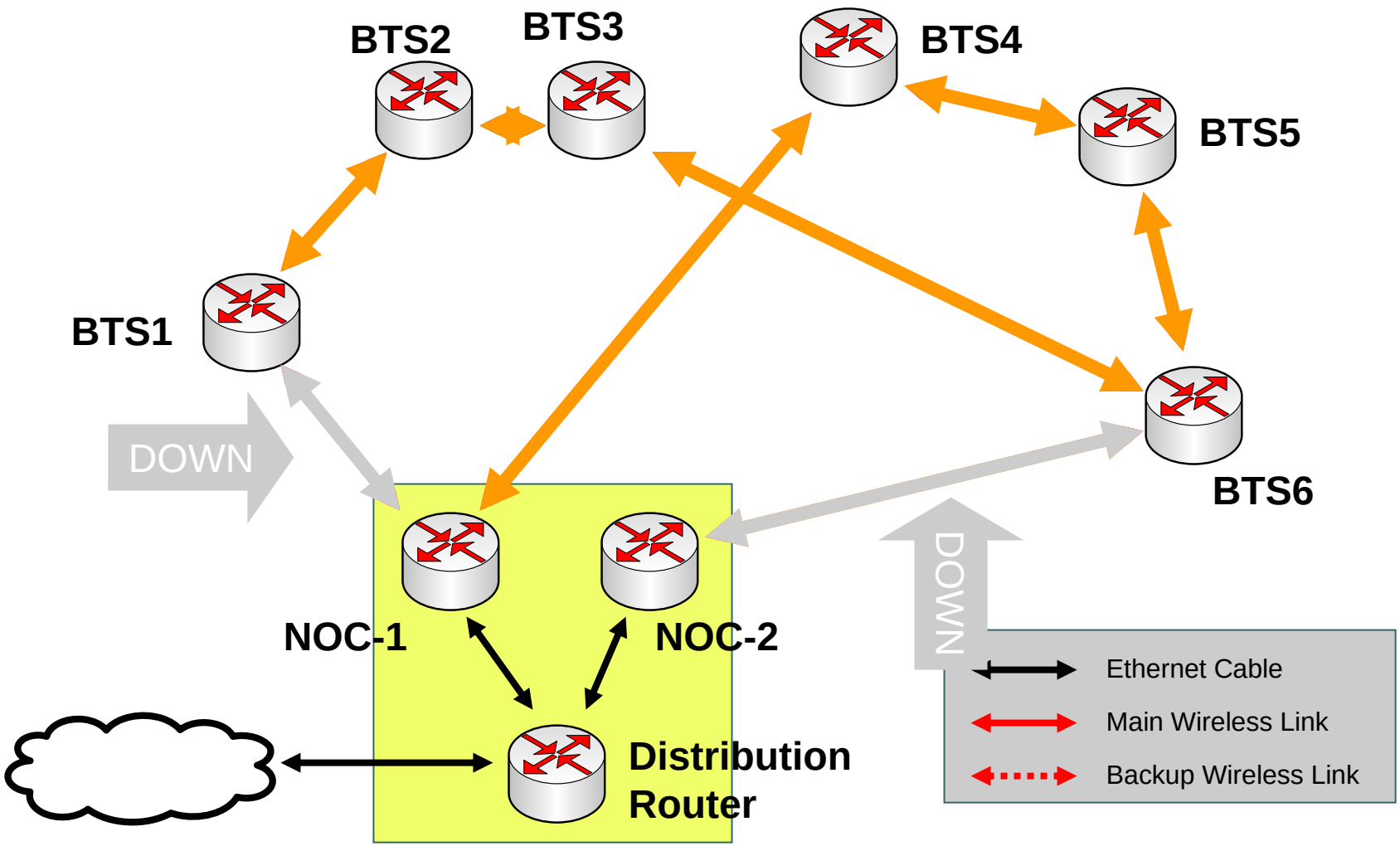


Wireless Instalation

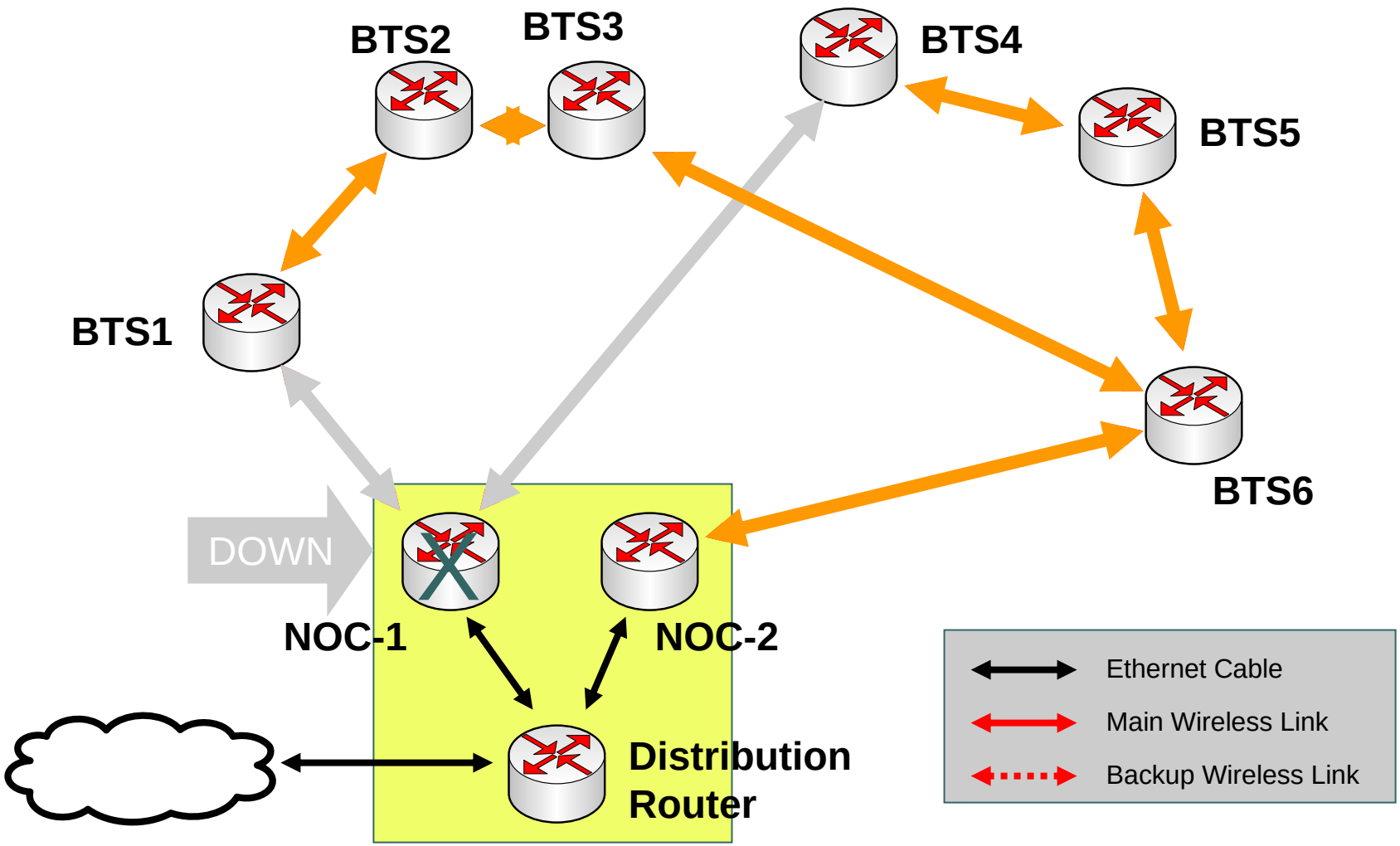
Wireless Network Topology



Fail Over Scenario (1)

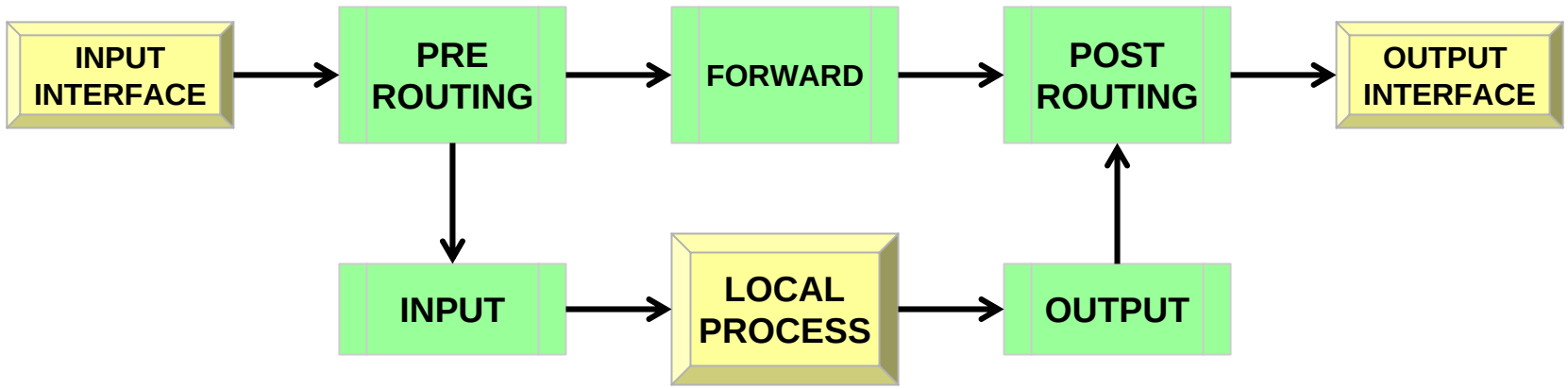


Fail Over Scenario (2)



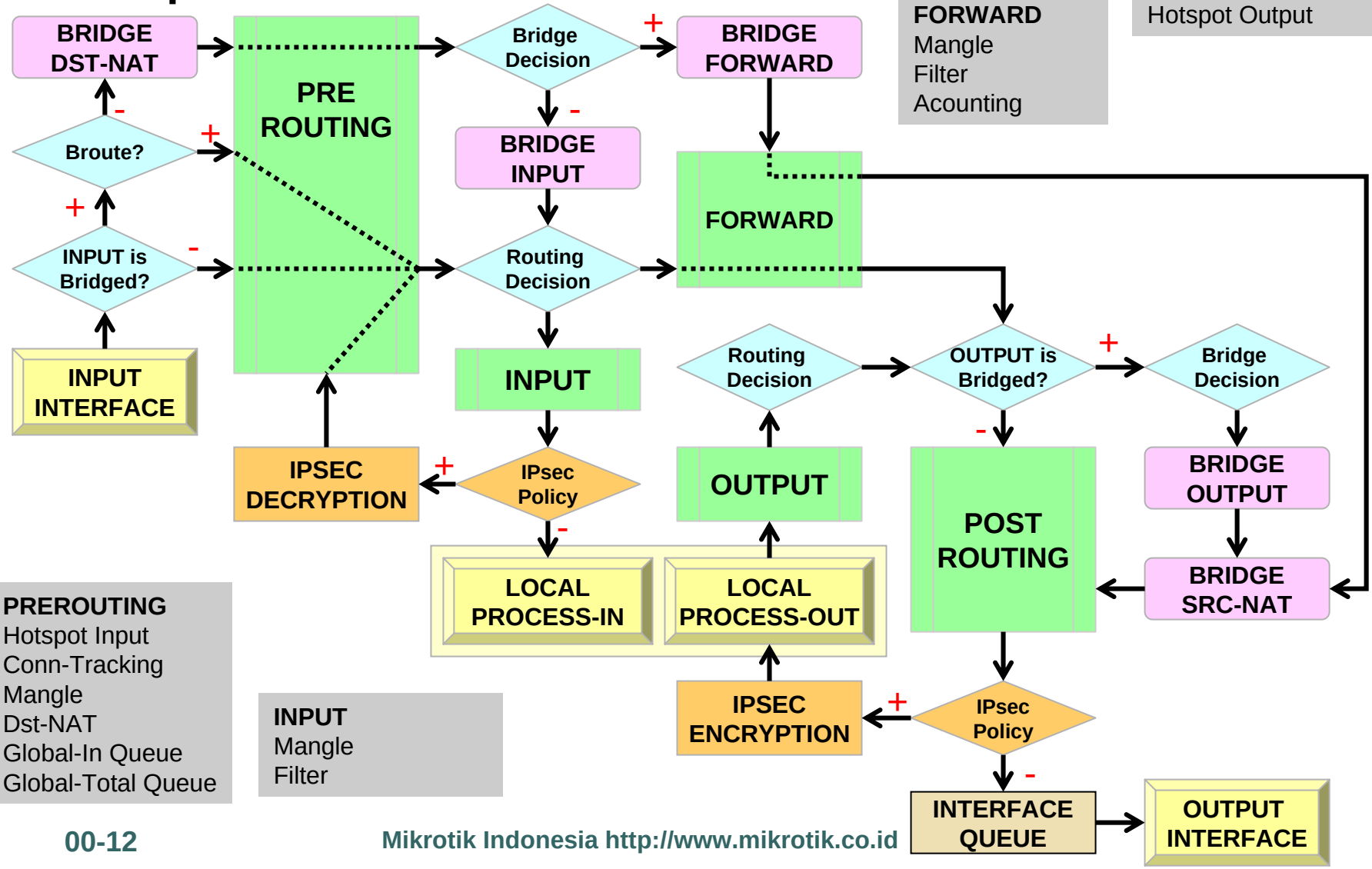
The Basic of IP Flow

IP Flow (simple diagram)



PREROUTING	INPUT	FORWARD	OUTPUT	POSTROUTING
Hotspot Input	Mangle	Mangle	Conn-Tracking	Mangle
Conn-Tracking	Filter	Filter	Mangle	Global-Out Queue
Mangle		Acounting	Filter	Global-Total Queue
Dst-NAT				Source-NAT
Global-In Queue				Hotspot Output
Global-Total Queue				

IP Flow



OUTPUT
Conn-Tracking
Mangle
Filter

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

FORWARD
Mangle
Filter
Acounting

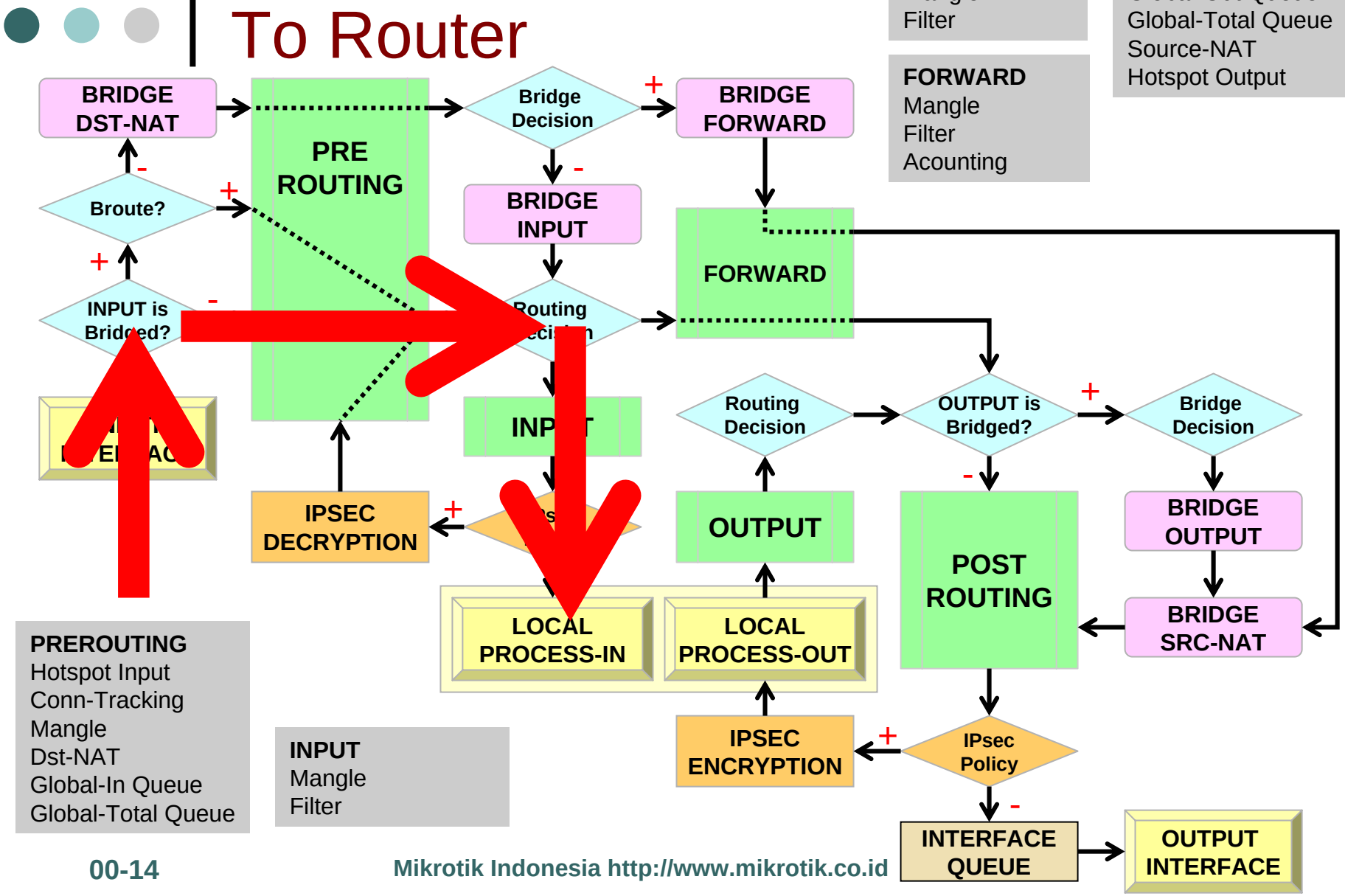
PREROUTING
Hotspot Input
Conn-Tracking
Mangle
Dst-NAT
Global-In Queue
Global-Total Queue

INPUT
Mangle
Filter

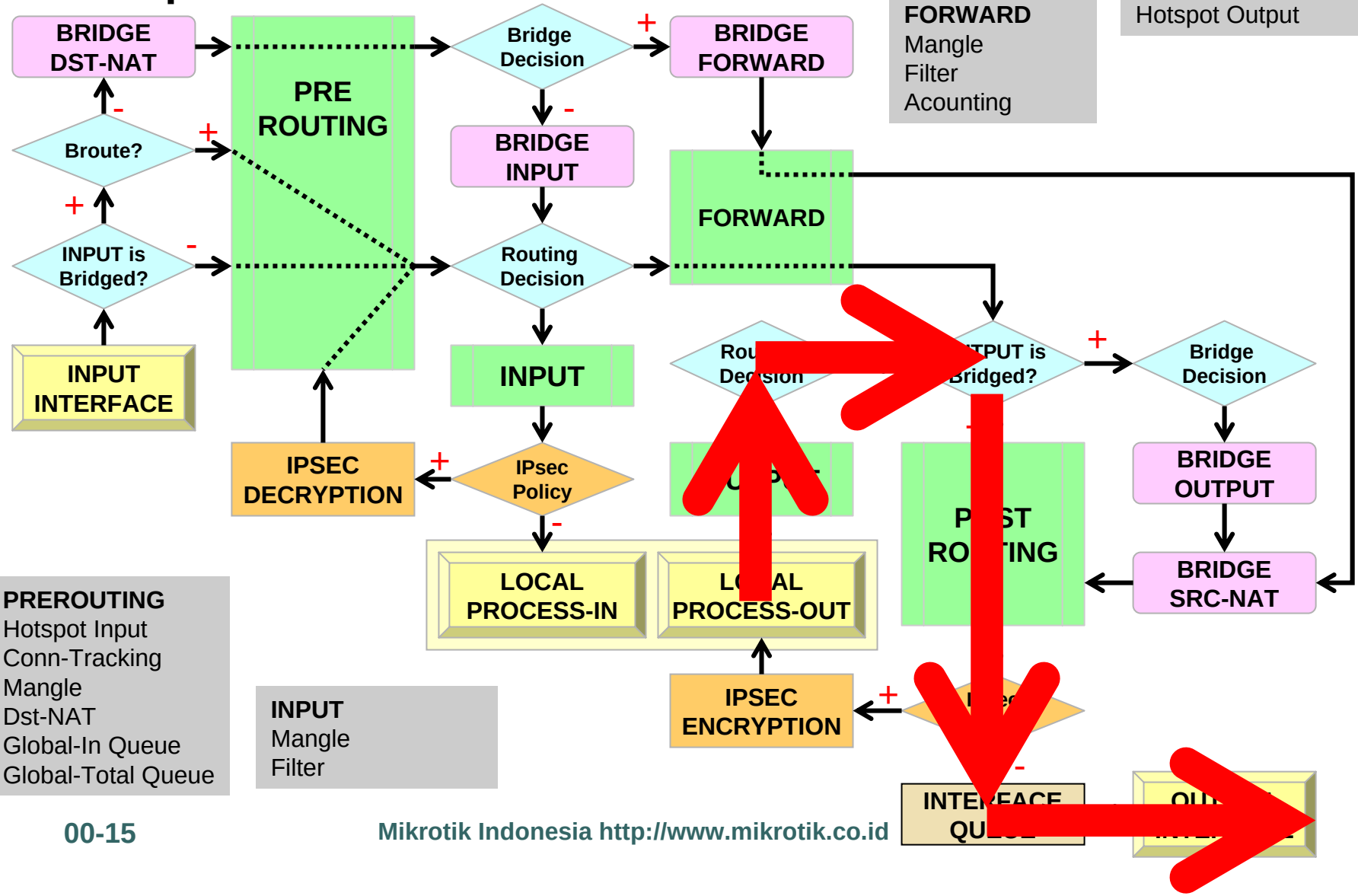
From – To Traffic?

- For each data packet, you have to know:
  - Source of packet
    - From outside
    - From local Process
  - Destination of packet
    - To Local Process
    - To outside

Routed Traffic To Router



Routed Traffic From Router



OUTPUT
Conn-Tracking
Mangle
Filter

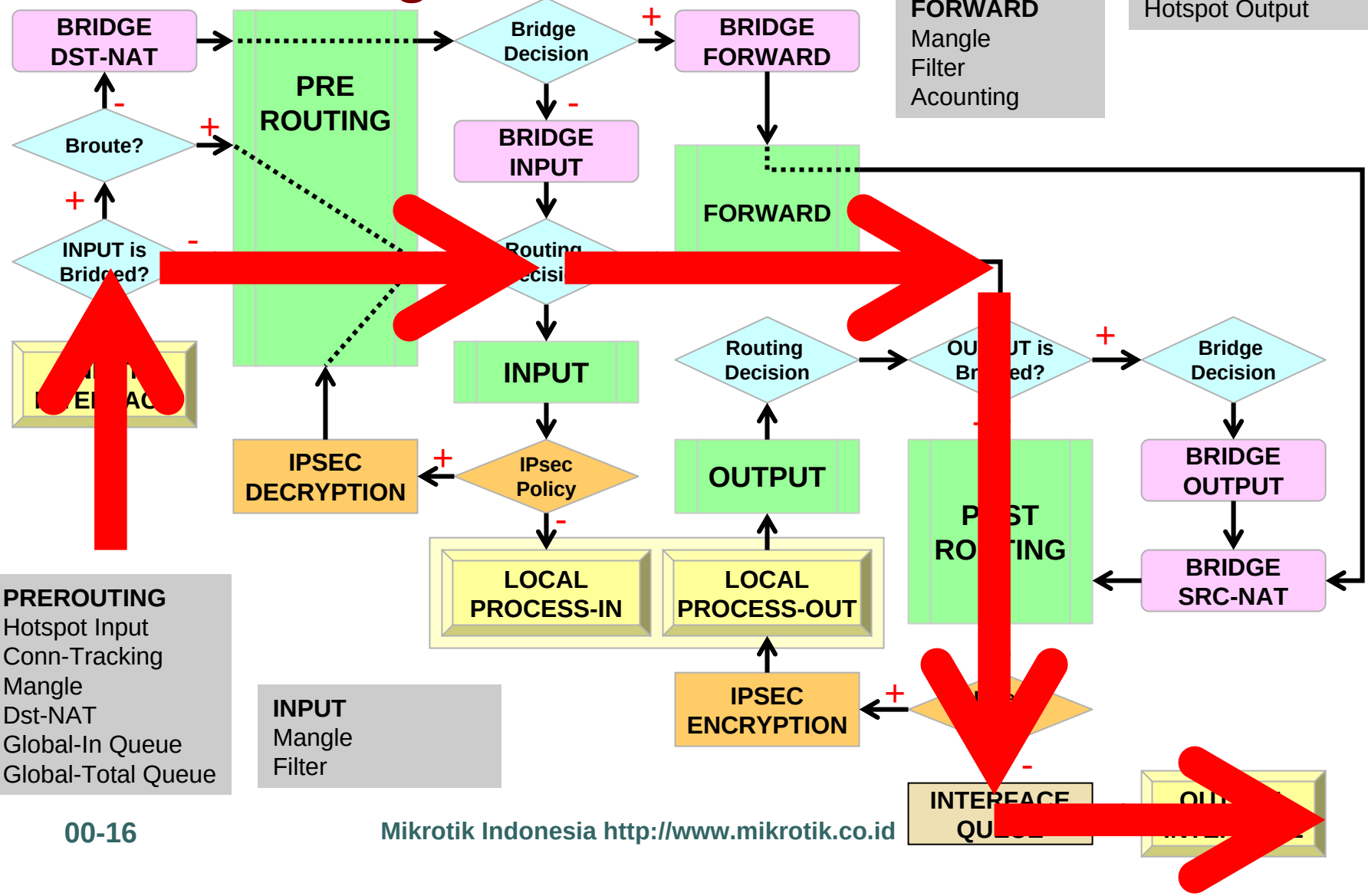
POSTROUTING
Mangle
Global-Out Queue
Global-Total Queue
Source-NAT
Hotspot Output

FORWARD
Mangle
Filter
Acounting

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

INPUT
Mangle
Filter

Routed Traffic Through Router



OUTPUT
Conn-Tracking
Mangle
Filter

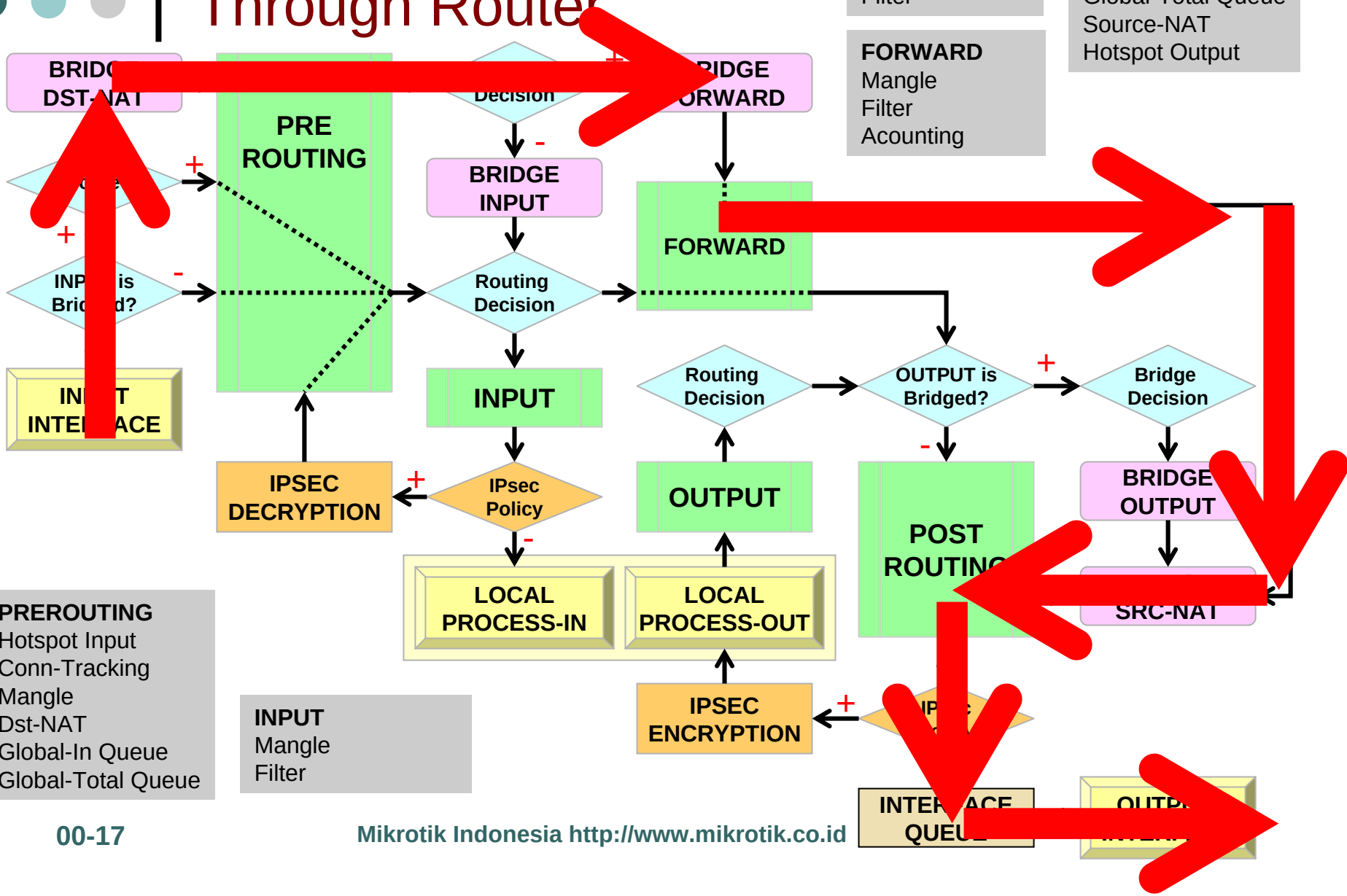
POSTROUTING
Mangle
Global-Out Queue
Global-Total Queue
Source-NAT
Hotspot Output

FORWARD
Mangle
Filter
Acounting

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

INPUT
Mangle
Filter

Bridge Traffic Through Router

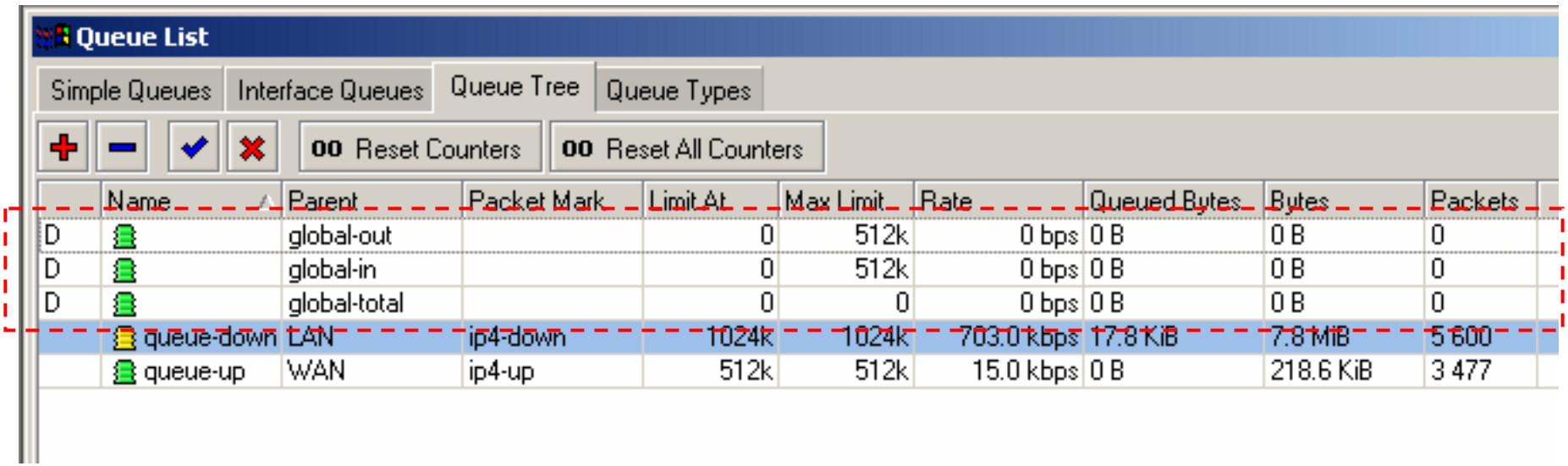


Chain Position

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

Simple Queue

- Simple Queue is located at Global-In and Global-Out…. and also at Global Total

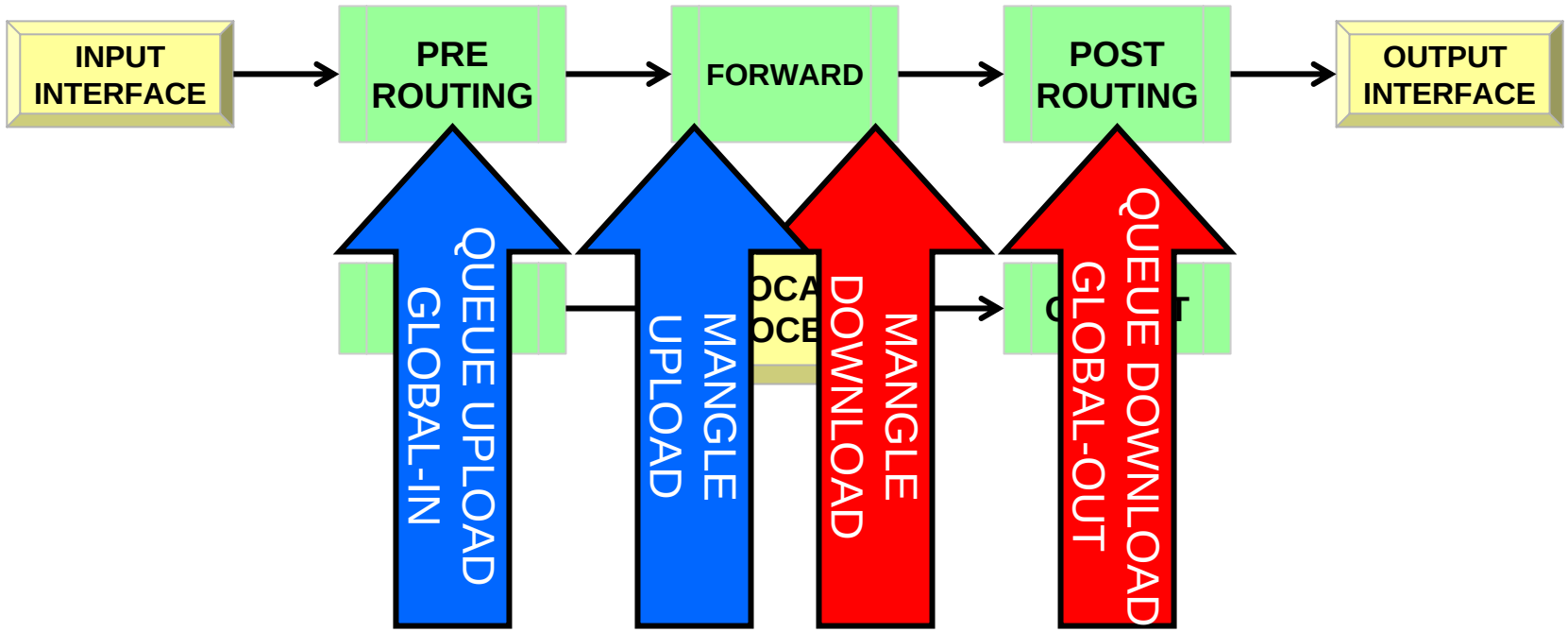


	Name	Parent	Packet Mark	Limit At	Max Limit	Rate	Queued Bytes	Bytes	Packets
D		global-out		0	512k	0 bps	0 B	0 B	0
D		global-in		0	512k	0 bps	0 B	0 B	0
D		global-total		0	0	0 bps	0 B	0 B	0
	queue-down	LAN	ip4-down	1024k	1024k	703.0 kbps	17.8 KiB	7.8 MiB	5 600
	queue-up	WAN	ip4-up	512k	512k	15.0 kbps	0 B	218.6 KiB	3 477

Mangle & Simple Queue

- Mangle
  - chain=forward in-interface=LAN src-address=192.168.0.4 action=mark-packet new-packet-mark=client passthrough=no
  - chain=forward out-interface=LAN dst-address=192.168.0.4 action=mark-packet new-packet-mark=client passthrough=no
- Simple Queue
  - name="queue1" interface=all parent=none packet-marks=client direction=both max-limit=512000/512000

IP Flow (simple diagram)

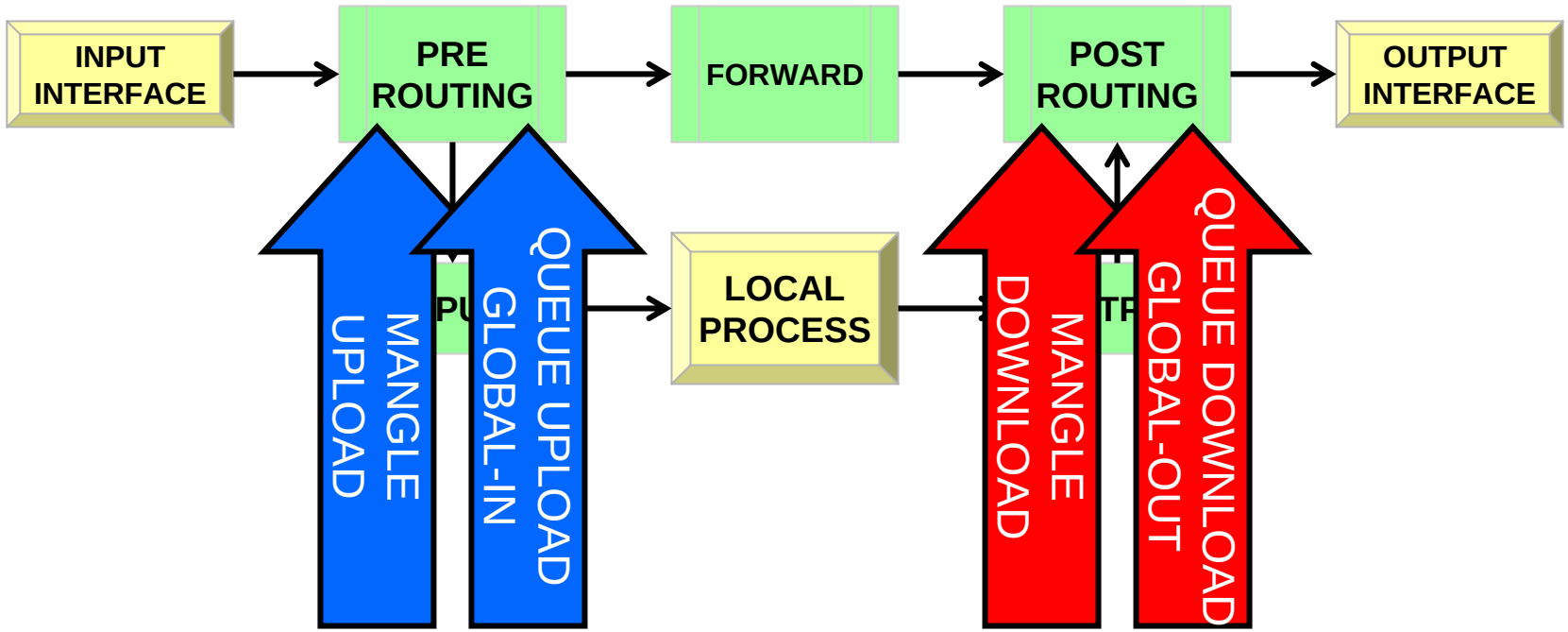


PREROUTING	INPUT	FORWARD	OUTPUT	POSTROUTING
Hotspot Input	Mangle	Mangle	Conn-Tracking	Mangle
Conn-Tracking	Filter	Filter	Mangle	Global-Out Queue
Mangle		Acounting	Filter	Global-Total Queue
Dst-NAT				Source-NAT
Global-In Queue				Hotspot Output
Global-Total Queue				

Mangle & Simple Queue

- This sample :
  - will work for download limiting
  - **will not work for upload limiting**
    - because mangle will be done after simple queue process
    - mangle : chain=forward
    - simple queue → global-in (prerouting)
  - mangle should be in prerouting (for upload) and postrouting (for download)

IP Flow (simple diagram)

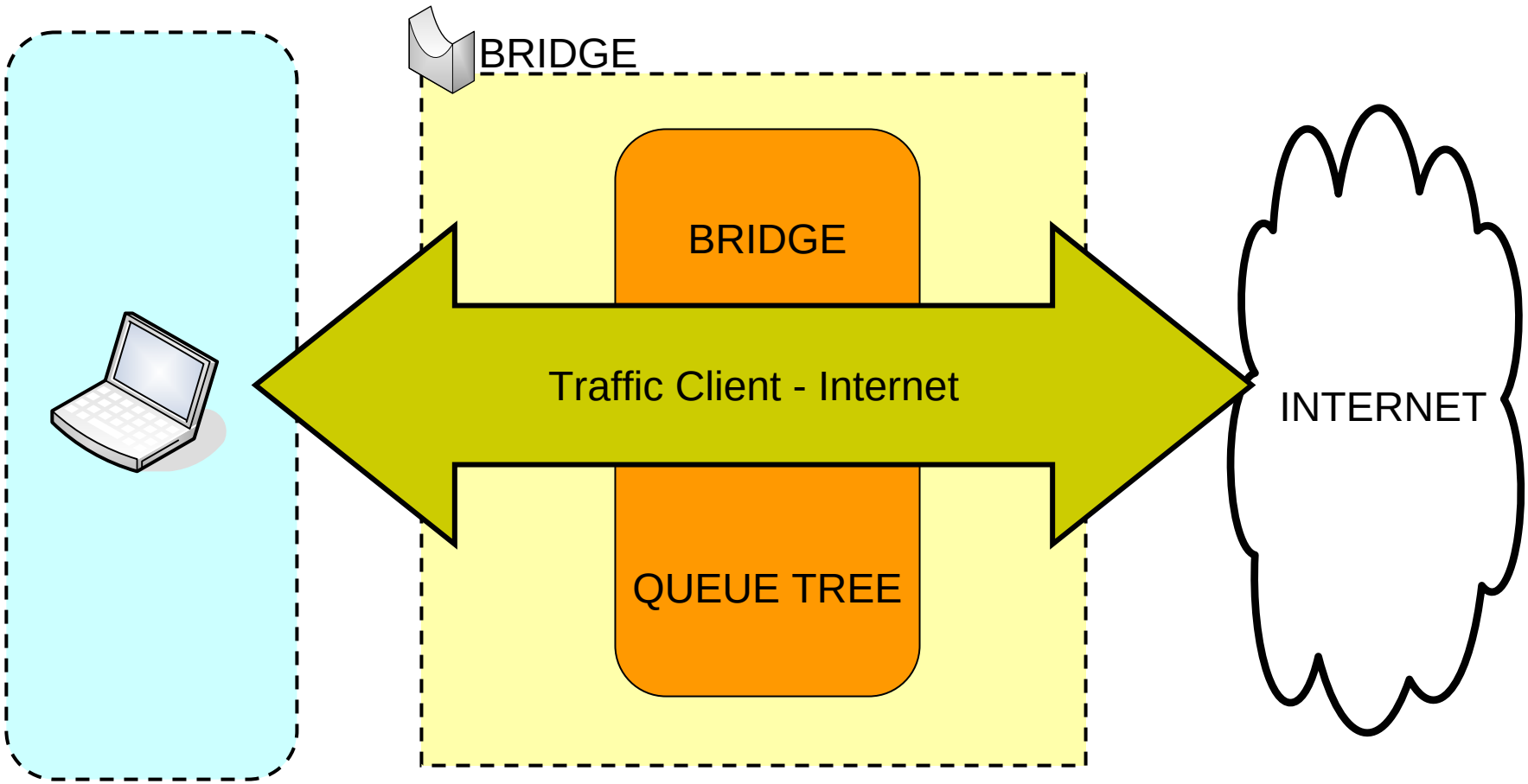


PREROUTING	INPUT	FORWARD	OUTPUT	POSTROUTING
Hotspot Input	Mangle	Mangle	Conn-Tracking	Mangle
Conn-Tracking	Filter	Filter	Mangle	Global-Out Queue
Mangle		Acounting	Filter	Global-Total Queue
Dst-NAT				Source-NAT
Global-In Queue				Hotspot Output
Global-Total Queue				

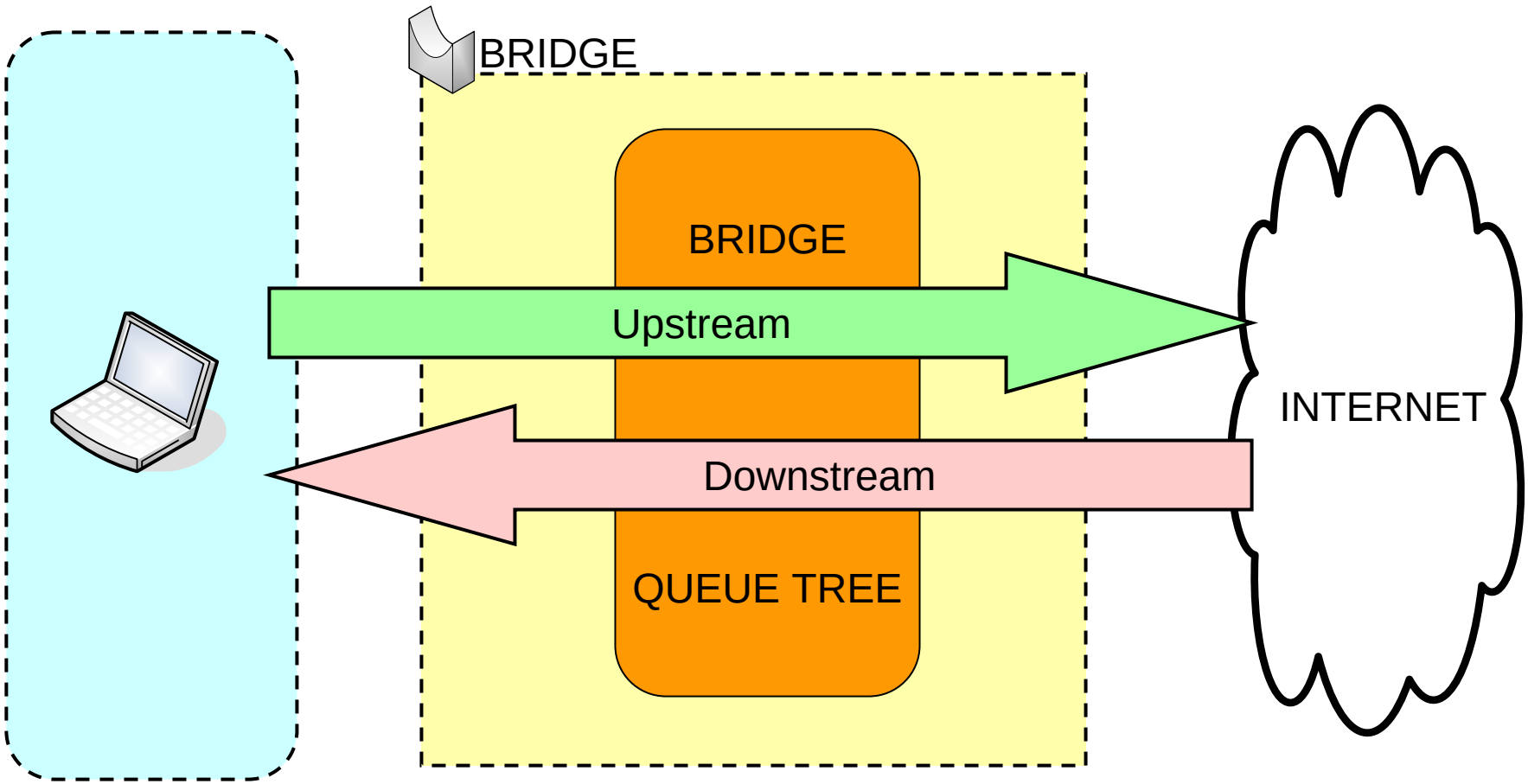
Test Case (1)

Transparant
Bandwidth Management

Queue with Bridge



Queue with Bridge



Interface Setup

[admin@MikroTik] > in pr
Flags: X - disabled, D - dynamic, R - running

#	Name	Type	RX-RATE	TX-RATE	MTU
0	R LAN	ether	0	0	1500
1	R WAN	ether	0	0	1500
2	R bridge1	bridge	0	0	1500

[admin@MikroTik] interface bridge port> pr
Flags: X - disabled, I - inactive, D - dynamic

#	INTERFACE	BRIDGE	PRIORITY	PATH-COST
0	WAN	bridge1	128	10
1	LAN	bridge1	128	10

Mangle Setup

```
[admin@MikroTik] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=prerouting in-interface=LAN
     src-address=192.168.0.0/24 action=mark-packet
     new-packet-mark=data-up passthrough=no

 1   chain=postrouting out-interface=LAN
     dst-address=192.168.0.0/24 action=mark-packet
     new-packet-mark=data-down passthrough=no
```

Queue Tree Setup

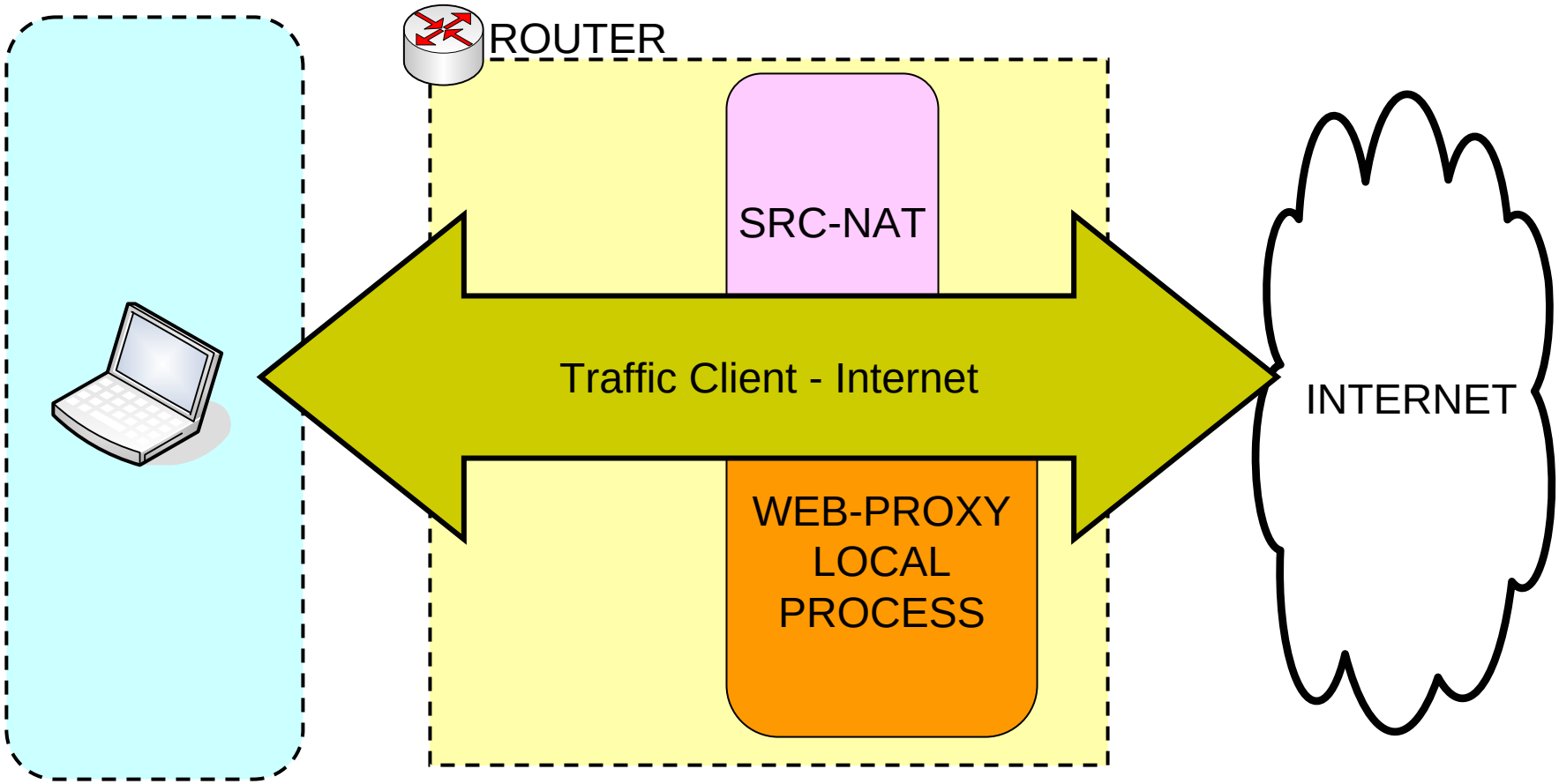
```
[admin@MikroTik] > queue tree print
Flags: X - disabled, I - invalid
 0  name="queue-up" parent=WAN
    packet-mark=data-up limit-at=512000
    queue=default priority=8 max-limit=512000
    burst-limit=0 burst-threshold=0 burst-time=0s
 1  name="queue-down" parent=LAN
    packet-mark=data-down limit-at=1024000
    queue=default priority=8 max-limit=1024000
    burst-limit=0 burst-threshold=0 burst-time=0s
```

Test Case (2)

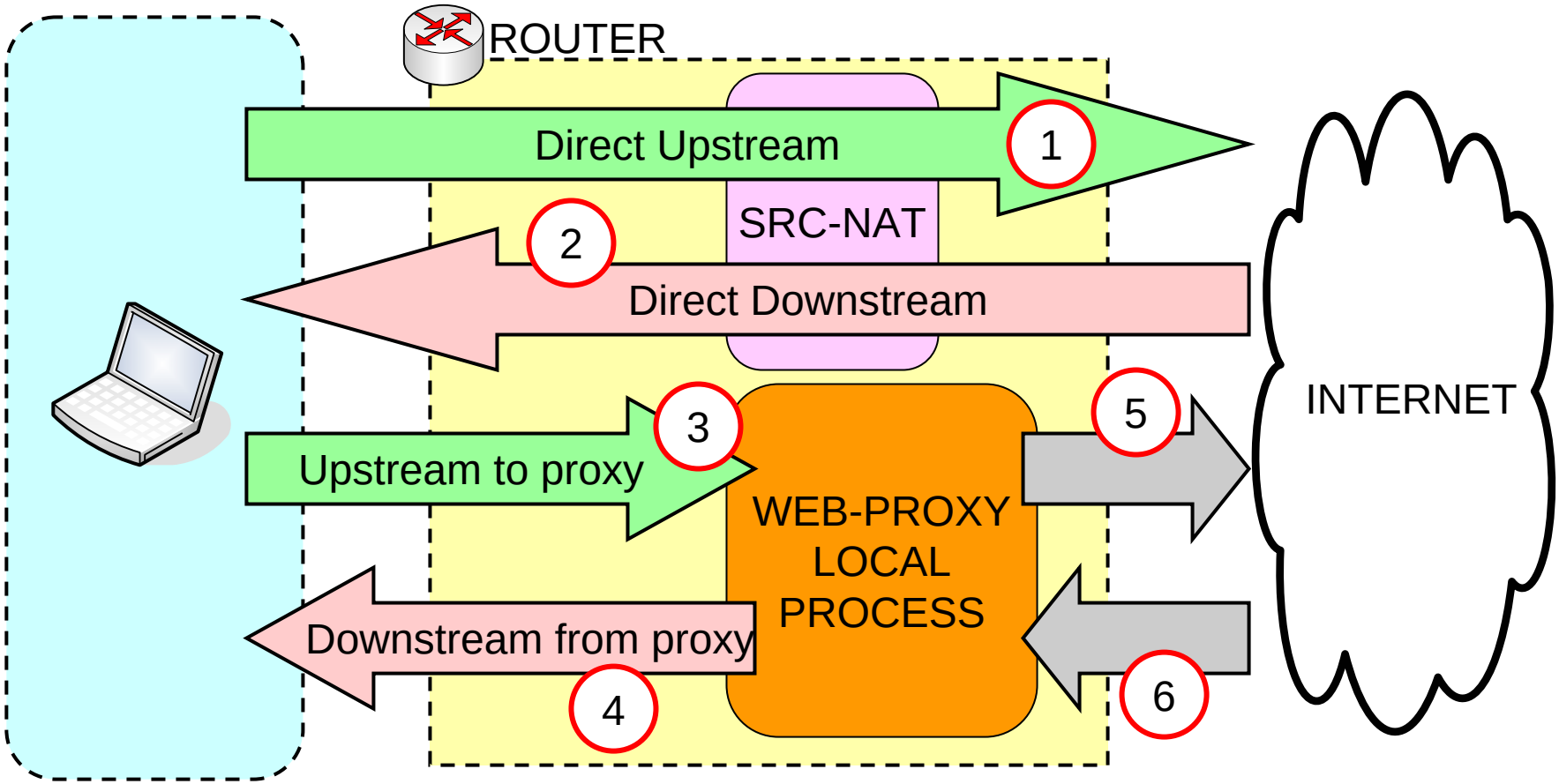
Queue with

Src-NAT and Internal Proxy

Queue with SRC-NAT & Internal Proxy



Queue with SRC-NAT & Internal Proxy



Web-Proxy Setup

```
> ip web-proxy pr enabled: yes
    src-address: 0.0.0.0
    port: 3128
    hostname: "proxy"
    transparent-proxy: yes
    parent-proxy: 0.0.0.0:0
    cache-administrator: "webmaster"
    max-object-size: 4096KiB
    cache-drive: system
    max-cache-size: none
    max-ram-cache-size: unlimited
    status: running
    reserved-for-cache: 0KiB
    reserved-for-ram-cache: 154624KiB
```

Firewall Setup

- [admin@instaler] ip firewall nat> pr
  Flags: X - disabled, I - invalid, D - dynamic

0 chain=srcnat out-interface=public
src-address=192.168.1.0/24
action=masquerade

1 chain=dstnat in-interface=lan
src-address=192.168.1.0/24 protocol=tcp
dst-port=80 action=redirect to-ports=3128

Mangle Setup

0 ;;; UP TRAFFIC / Traffic #1 and #3
chain=**prerouting** in-interface=lan
src-address=192.168.1.0/24 action=mark-packet
new-packet-mark=**test-up** passthrough=**no**

1 ;;; CONN-MARK
chain=**forward** src-address=192.168.1.0/24 action=mark-
connection new-connection-mark=**test-conn** passthrough=**yes**

2 ;;; DOWN-DIRECT CONNECTION / Traffic #2
chain=**forward** in-interface=public
connection-mark=**test-conn** action=mark-packet
new-packet-mark=**test-down** passthrough=**no**

3 ;;; DOWN-VIA PROXY / Traffic #4
chain=**output** out-interface=lan dst-address=192.168.1.0/24
action=mark-packet new-packet-mark=**test-down**
passthrough=**no**

Queue Setup

```
0  ;;; For traffic #2 and #4 (download)
   name="downstream" parent=lan
   packet-mark=test-down limit-at=1024000
   queue=default priority=8 max-limit=1024000
   burst-limit=0 burst-threshold=0 burst-time=0s
1  ;;; For traffic #1 and #3 (upload)
   name="upstream" parent=global-in
   packet-mark=test-up limit-at=256000
   queue=default priority=8 max-limit=256000
   burst-limit=0 burst-threshold=0 burst-time=0s
```

Traffic #5 & #6

- We can not manage traffic #5 and #6 based on client IP Address, because after the traffic hits the proxy, it will change the source IP Address, and the traffic will be a new one:
  - Source : Web Proxy (local process)
  - Destination : Web Server on Internet

Thank You

- **Valens Riyadi**
- info@mikrotik.co.id