Case 1: wireless access

PT. Garda Lintas Cakrawala

- Further improvement:
  - Use dhcp for AP's IP address
  - Centralized database for wireless access points configuration
  - Have APs that can do Multiple SSID & support VLAN

Case 2: network segmentation

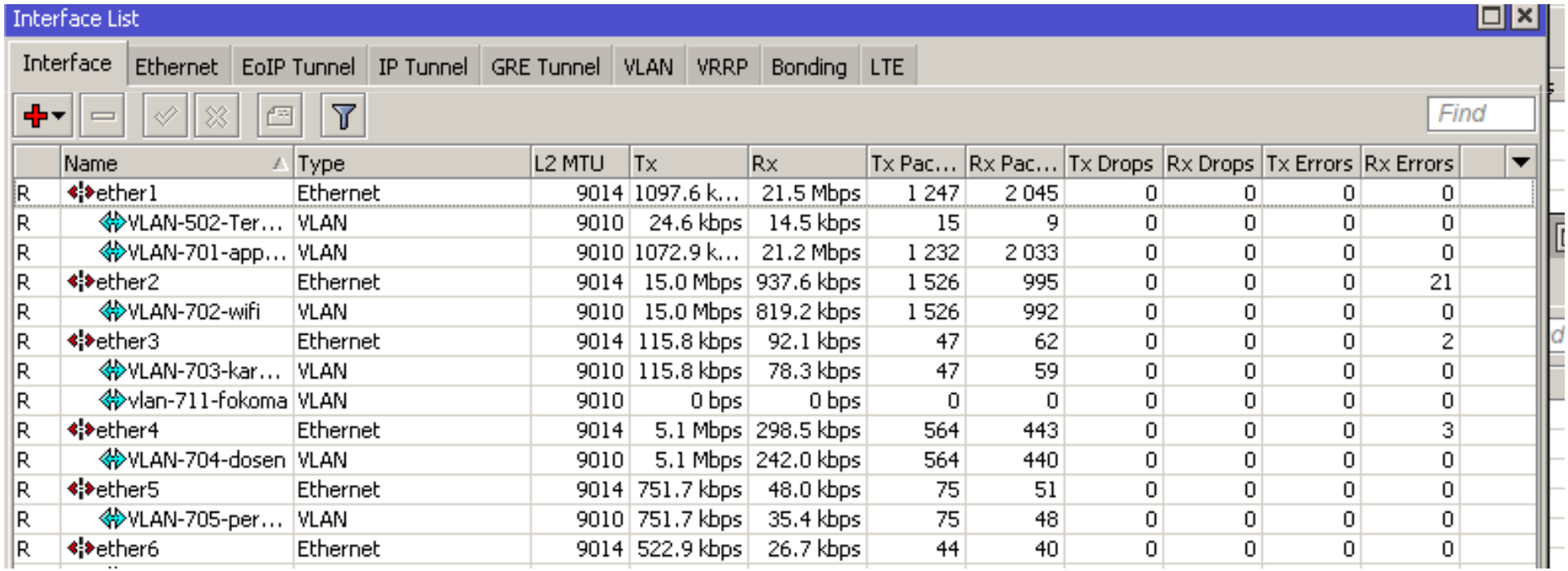
PT. Garda Lintas Cakrawala

- Before:
  - Only one network segment for everybody
  - Difficult for grouping users. E.g. lecturer & students
  - Some incidents happens :-p
- What we did:
  - Replace hub with manageable switch
  - Implementing VLAN

Case 2: network segmentation

PT. Garda Lintas Cakrawala

- Further improvement:
  - Mikrotik produces switches



	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx Drops	Tx Errors	Rx Errors
R	ether1	Ethernet	9014	1097.6 k...	21.5 Mbps	1 247	2 045	0	0	0	0
R	VLAN-502-Ter...	VLAN	9010	24.6 kbps	14.5 kbps	15	9	0	0	0	0
R	VLAN-701-app...	VLAN	9010	1072.9 k...	21.2 Mbps	1 232	2 033	0	0	0	0
R	ether2	Ethernet	9014	15.0 Mbps	937.6 kbps	1 526	995	0	0	0	21
R	VLAN-702-wifi	VLAN	9010	15.0 Mbps	819.2 kbps	1 526	992	0	0	0	0
R	ether3	Ethernet	9014	115.8 kbps	92.1 kbps	47	62	0	0	0	2
R	VLAN-703-kar...	VLAN	9010	115.8 kbps	78.3 kbps	47	59	0	0	0	0
R	vlan-711-fokoma	VLAN	9010	0 bps	0 bps	0	0	0	0	0	0
R	ether4	Ethernet	9014	5.1 Mbps	298.5 kbps	564	443	0	0	0	3
R	VLAN-704-dosen	VLAN	9010	5.1 Mbps	242.0 kbps	564	440	0	0	0	0
R	ether5	Ethernet	9014	751.7 kbps	48.0 kbps	75	51	0	0	0	0
R	VLAN-705-per...	VLAN	9010	751.7 kbps	35.4 kbps	75	48	0	0	0	0
R	ether6	Ethernet	9014	522.9 kbps	26.7 kbps	44	40	0	0	0	0

Case 3: access control

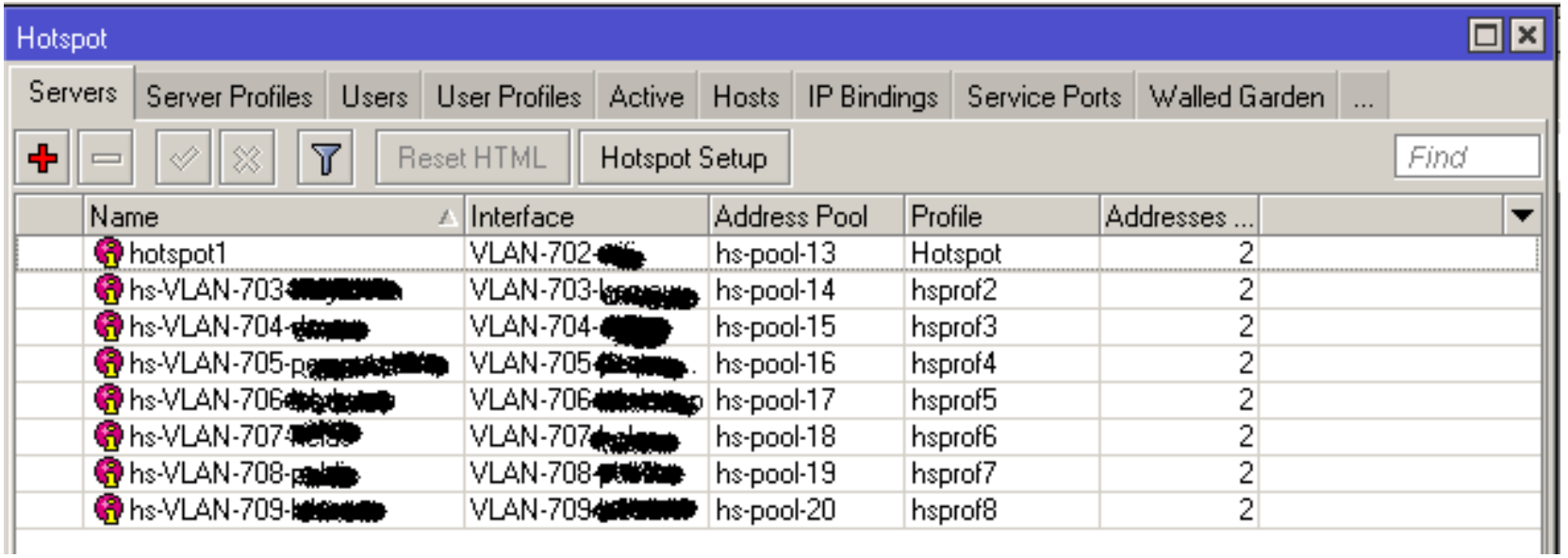
PT. Garda Lintas Cakrawala

- Before:
  - Alien can just access the network by plug-in the network cable
  - Anyone can join wireless access just by knowing the pass-phrase
- What we did:
  - MAC-based access control. however:
    - This makes us busy
    - Not really effective. MAC can be cloned and shared.

Case 3: access control

PT. Garda Lintas Cakrawala

- What we did:
  - Implement mikrotik hotspot. Yes…!!!
    - Applied in wired & wireless network
    - use external radius manager



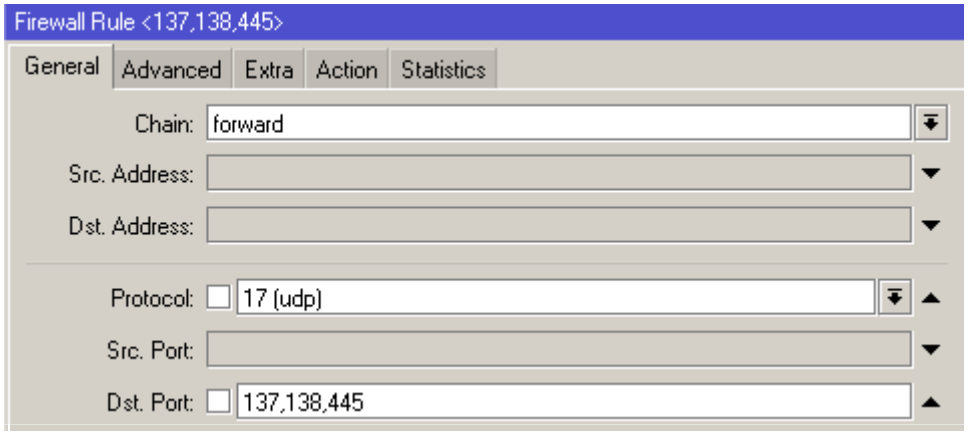
Case 4: transparent firewall

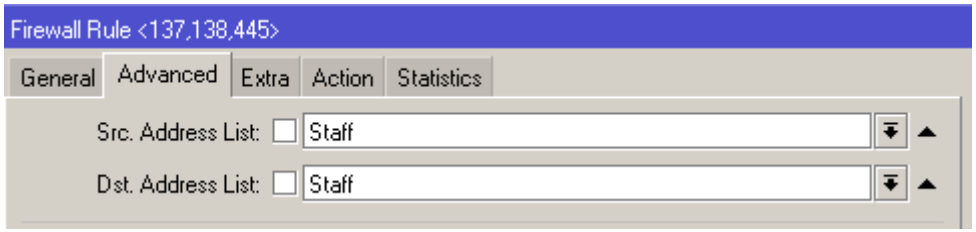
PT. Garda Lintas Cakrawala

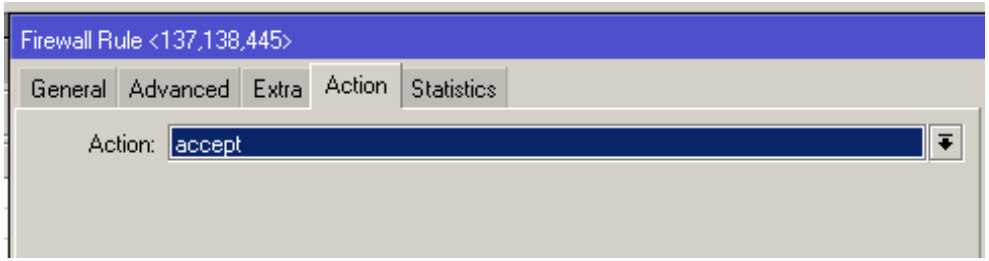
- Before:
  - Client can connect to other clients in the same network. (some incidents happen)
  - Virus can spread easily
  - Broadcast traffic (layer 3)
- What we did:
  - Control traffic among clients in one network (aka. Transparent firewall)
  - We need layer 2 support: VLAN

Case 4: transparent firewall

PT. Garda Lintas Cakrawala







Case 5: QOS

PT. Garda Lintas Cakrawala

- Before:
  - http QOS was done via transparent squid, working well. Not so flexible in term of time, dynamic allocation.
  - No QOS for other protocol. One user dominating the traffic
- What we did:
  - Implement mikrotik queue-tree. We have complex requirements to be satisfied

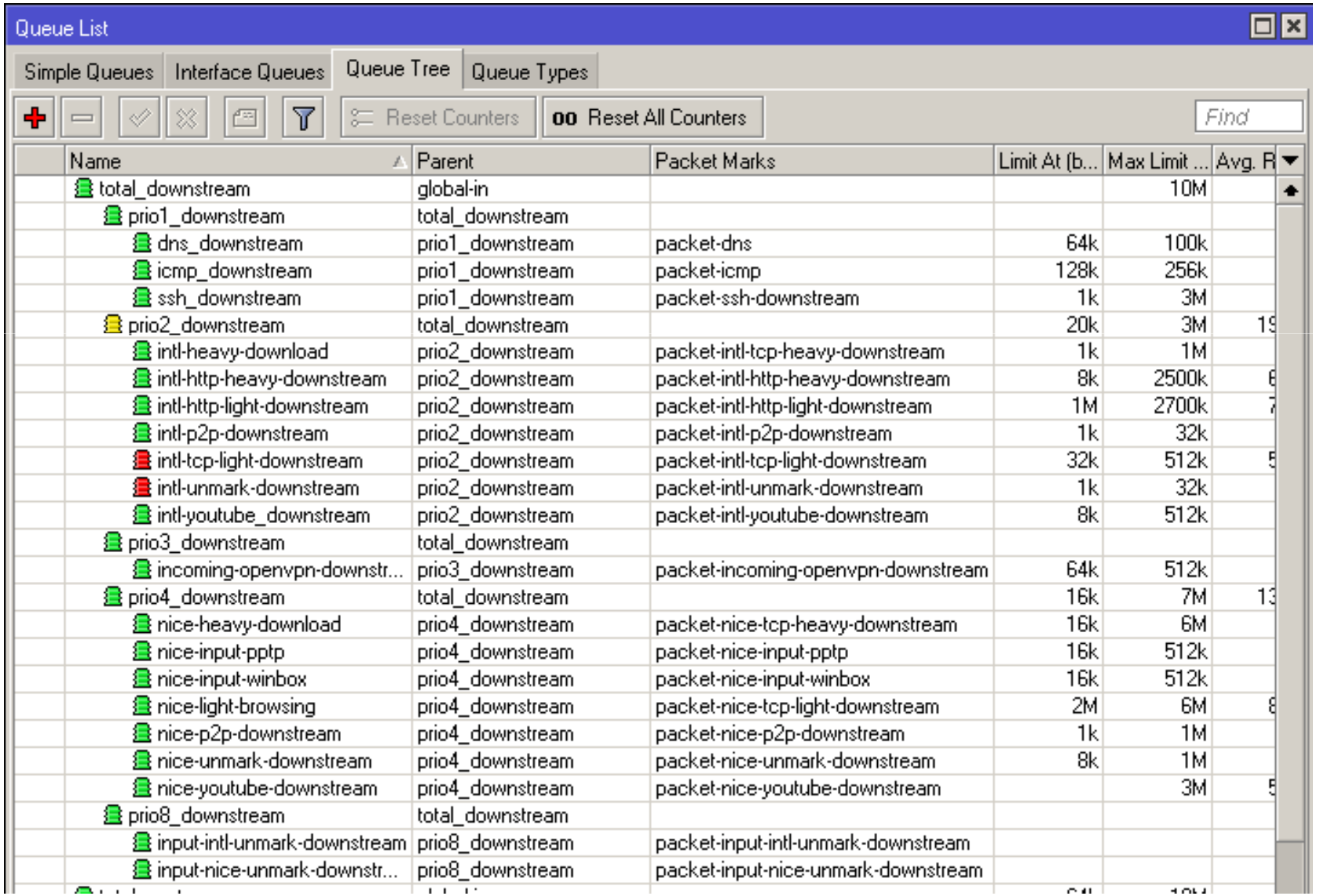
Case 6: fighting torrent

PT. Garda Lintas Cakrawala

- Before:
  - P2p traffic was one of big problem in the network.
  - Cant be handle by squid
  - And its tricky. Its challenging to identify the traffic
- What we did:
  - Queueing known application
  - Don’t forget to queue the unmarked traffic

Case 6: fighting torrent

PT. Garda Lintas Cakrawala



Name	Parent	Packet Marks	Limit At (b...	Max Limit ...	Avg. R
total_downstream	global-in			10M	
prio1_downstream	total_downstream				
dns_downstream	prio1_downstream	packet-dns	64k	100k	
icmp_downstream	prio1_downstream	packet-icmp	128k	256k	
ssh_downstream	prio1_downstream	packet-ssh-downstream	1k	3M	
prio2_downstream	total_downstream		20k	3M	19
intl-heavy-download	prio2_downstream	packet-intl-tcp-heavy-downstream	1k	1M	
intl-http-heavy-downstream	prio2_downstream	packet-intl-http-heavy-downstream	8k	2500k	8
intl-http-light-downstream	prio2_downstream	packet-intl-http-light-downstream	1M	2700k	7
intl-p2p-downstream	prio2_downstream	packet-intl-p2p-downstream	1k	32k	
intl-tcp-light-downstream	prio2_downstream	packet-intl-tcp-light-downstream	32k	512k	5
intl-unmark-downstream	prio2_downstream	packet-intl-unmark-downstream	1k	32k	
intl-youtube_downstream	prio2_downstream	packet-intl-youtube-downstream	8k	512k	
prio3_downstream	total_downstream				
incoming-openvpn-downstr...	prio3_downstream	packet-incoming-openvpn-downstream	64k	512k	
prio4_downstream	total_downstream		16k	7M	13
nice-heavy-download	prio4_downstream	packet-nice-tcp-heavy-downstream	16k	6M	
nice-input-pptp	prio4_downstream	packet-nice-input-pptp	16k	512k	
nice-input-winbox	prio4_downstream	packet-nice-input-winbox	16k	512k	
nice-light-browsing	prio4_downstream	packet-nice-tcp-light-downstream	2M	6M	8
nice-p2p-downstream	prio4_downstream	packet-nice-p2p-downstream	1k	1M	
nice-unmark-downstream	prio4_downstream	packet-nice-unmark-downstream	8k	1M	
nice-youtube-downstream	prio4_downstream	packet-nice-youtube-downstream		3M	5
prio8_downstream	total_downstream				
input-intl-unmark-downstream	prio8_downstream	packet-input-intl-unmark-downstream			
input-nice-unmark-downstr...	prio8_downstream	packet-input-nice-unmark-downstream			

Case 6: fighting torrent

demo

End of presentation

PT. Garda Lintas Cakrawala

Thank you for your attention

☺

PT. Garda Lintas Cakrawala

Torrent shaping demo

Achmad Mardiansyah

INDONESIA 

MUM Zagreb, march 2013

Agenda

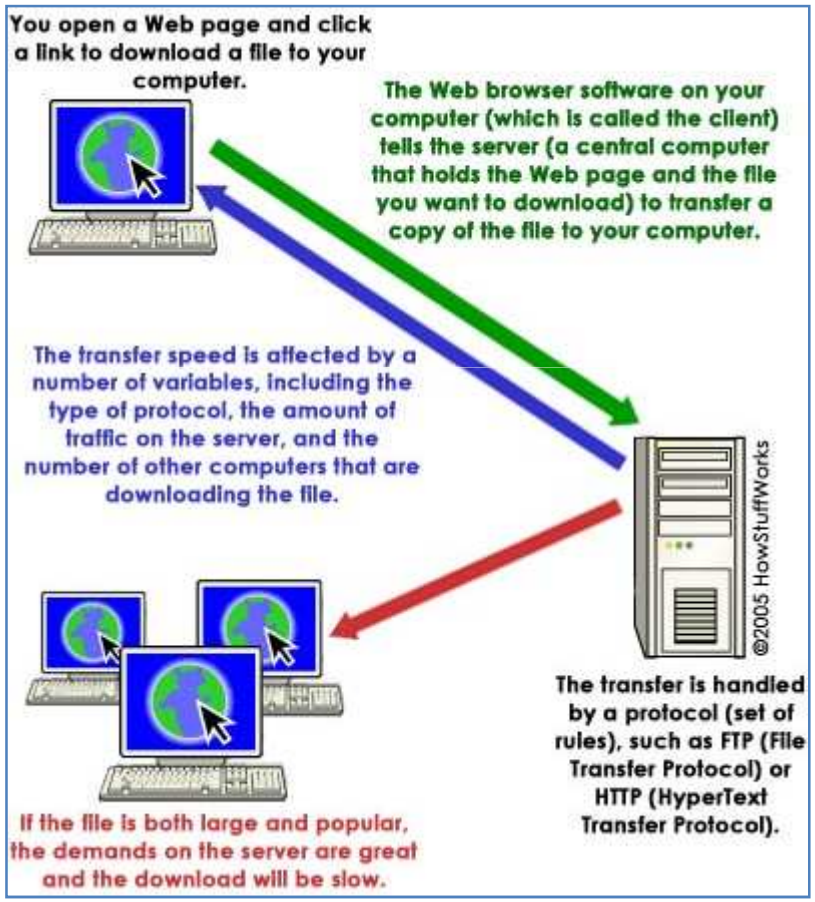
PT. Garda Lintas Cakrawala

- How torrent works
- Packet flow
- Firewall mangle
- Queue tree
- Scenario 1
- Scenario 2
- summary

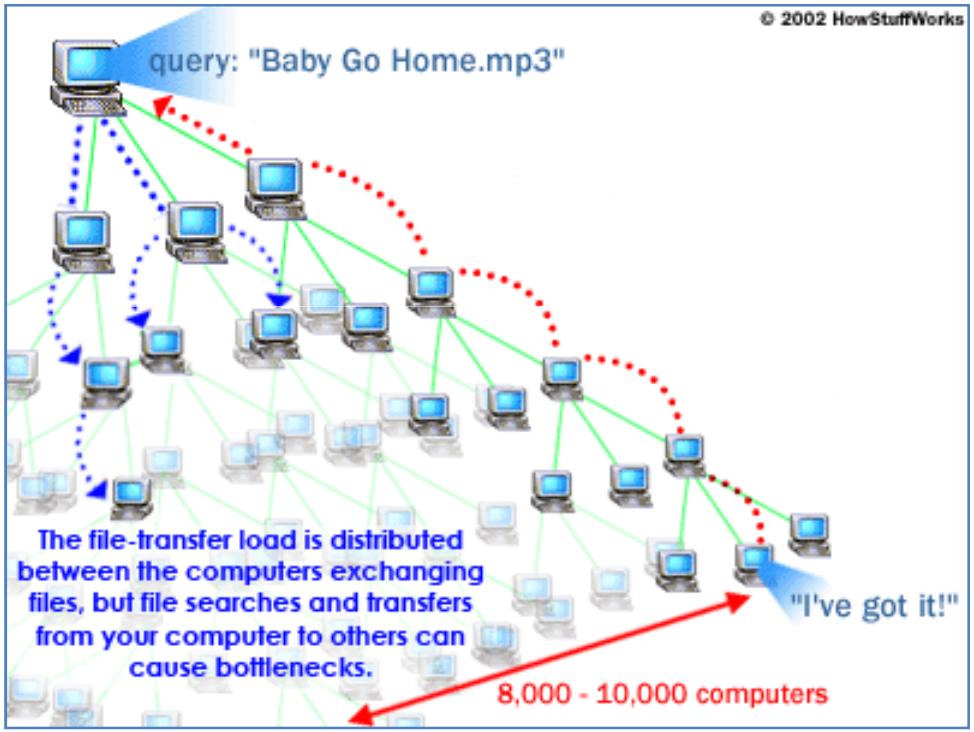
What is torrent...

PT. Garda Lintas Cakrawala

Traditional File transfer

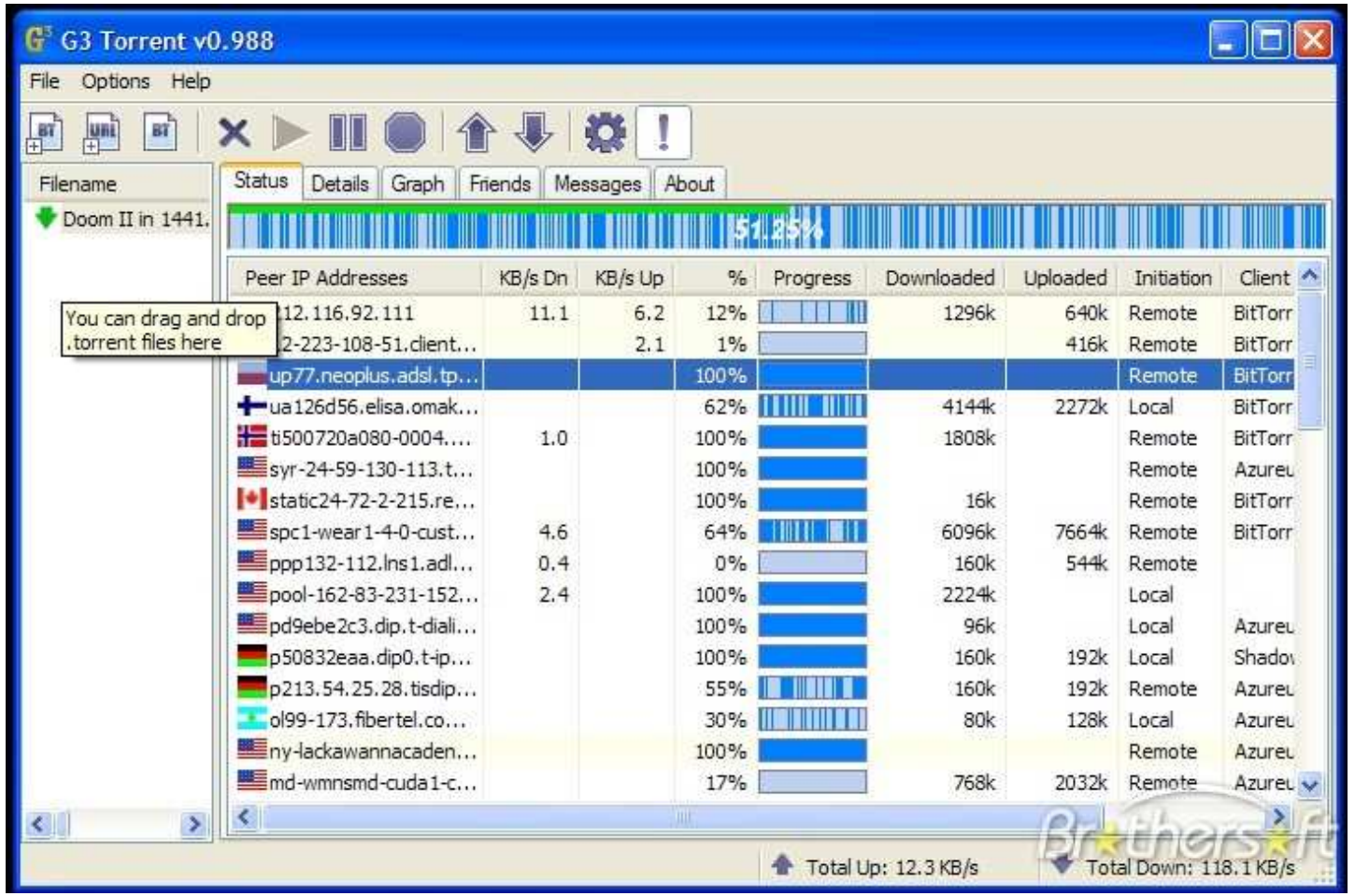


Peer-to-peer file transfer



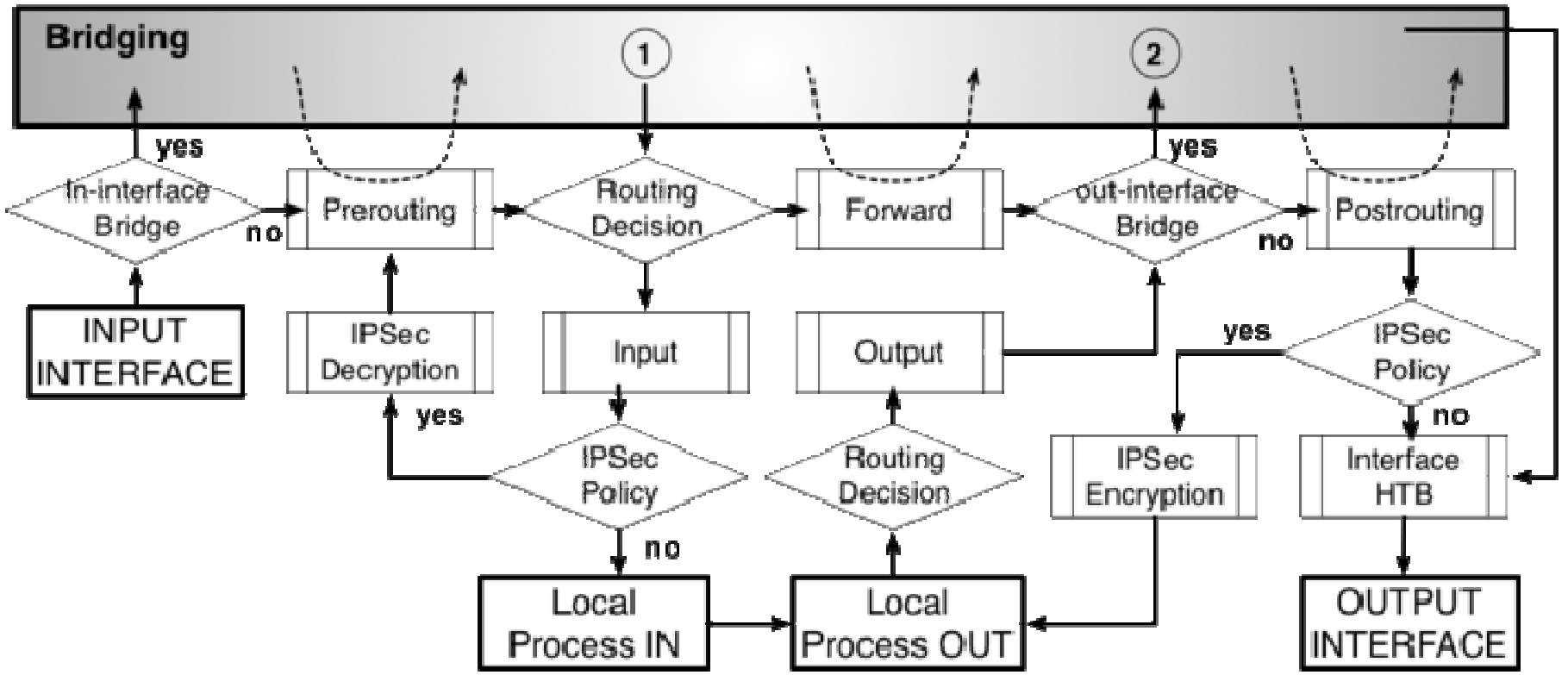
Torrent in action…

PT. Garda Lintas Cakrawala



Packet flow

PT. Garda Lintas Cakrawala

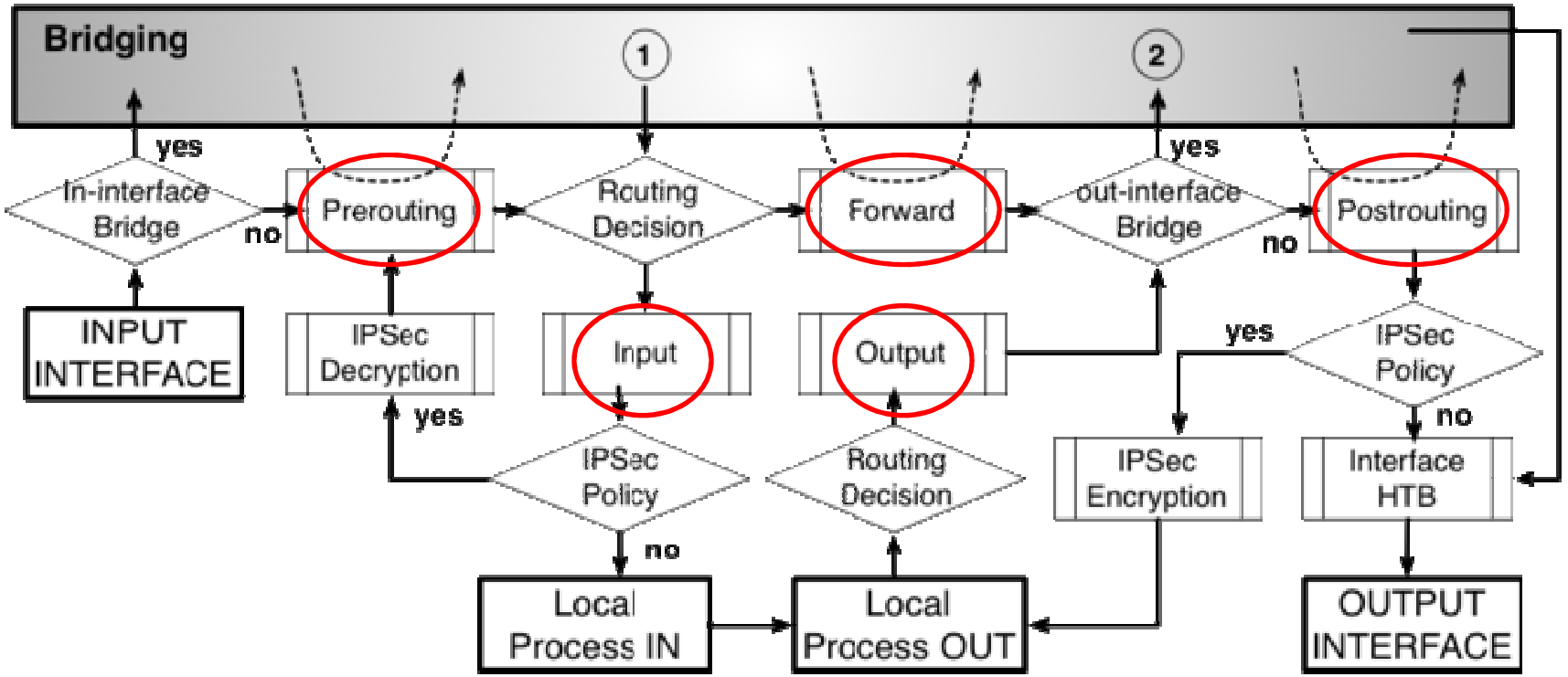


Source: http://wiki.mikrotik.com/wiki/Packet_Flow#Diagram

Iptables mangle

PT. Garda Lintas Cakrawala

The places (chains) to mark packets

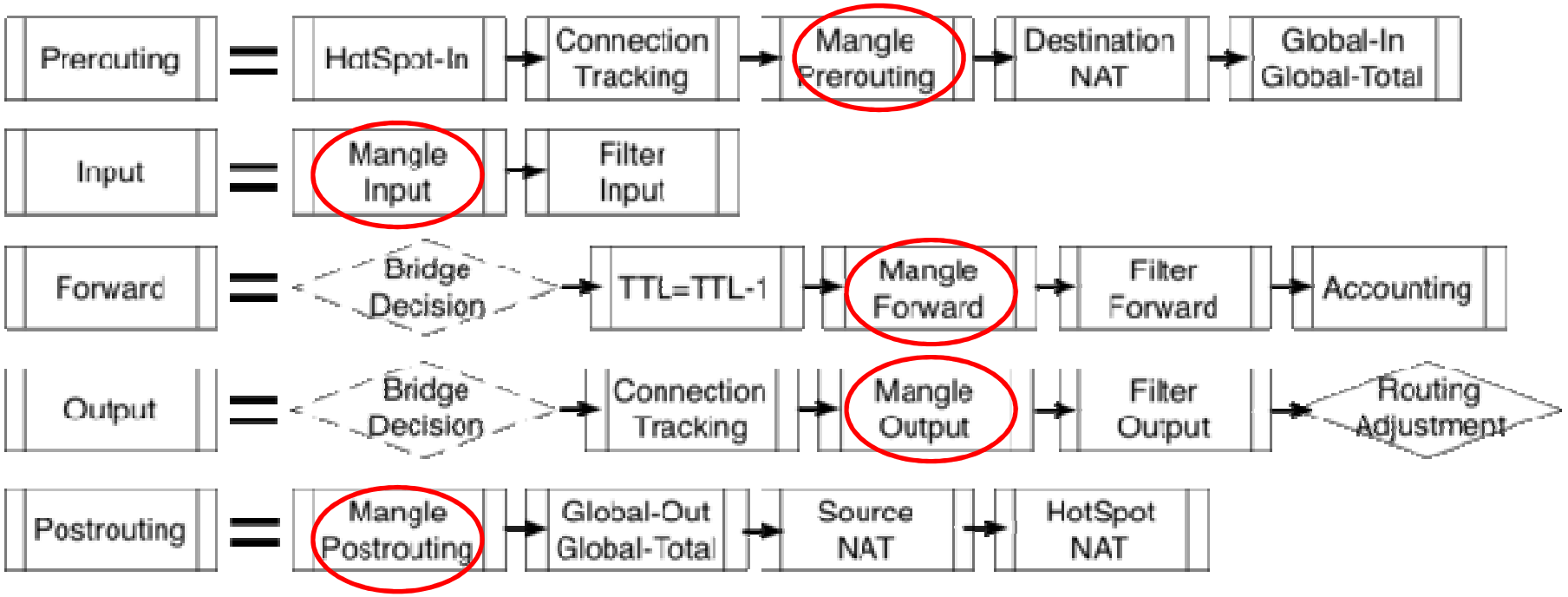


Source:
http://wiki.mikrotik.com/wiki/Packet_Flow#Diagram

Chain in mangle table

(zoomed view)

PT. Garda Lintas Cakrawala



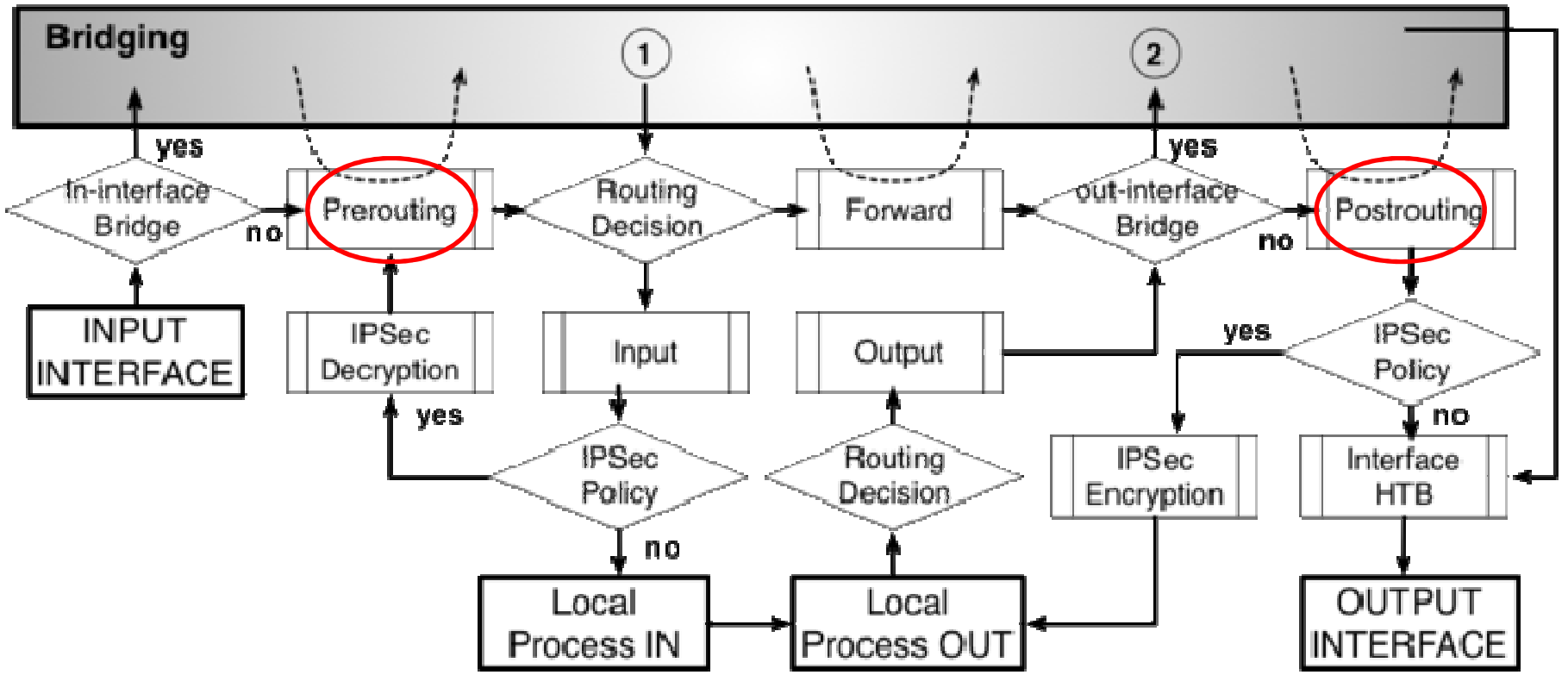
Queue tree

PT. Garda Lintas Cakrawala

- A method to limit and prioritize traffic
- An alternative to simple queue
- It works by queuing packets that are marked by iptables mangle
- Benefits:
  - Subqueue
  - All queue rules are processed together, not sequential (like simple queue)
  - **We can focus on a specific traffic marked by mangle. In this case: torrent traffic**

Place to queue the packets

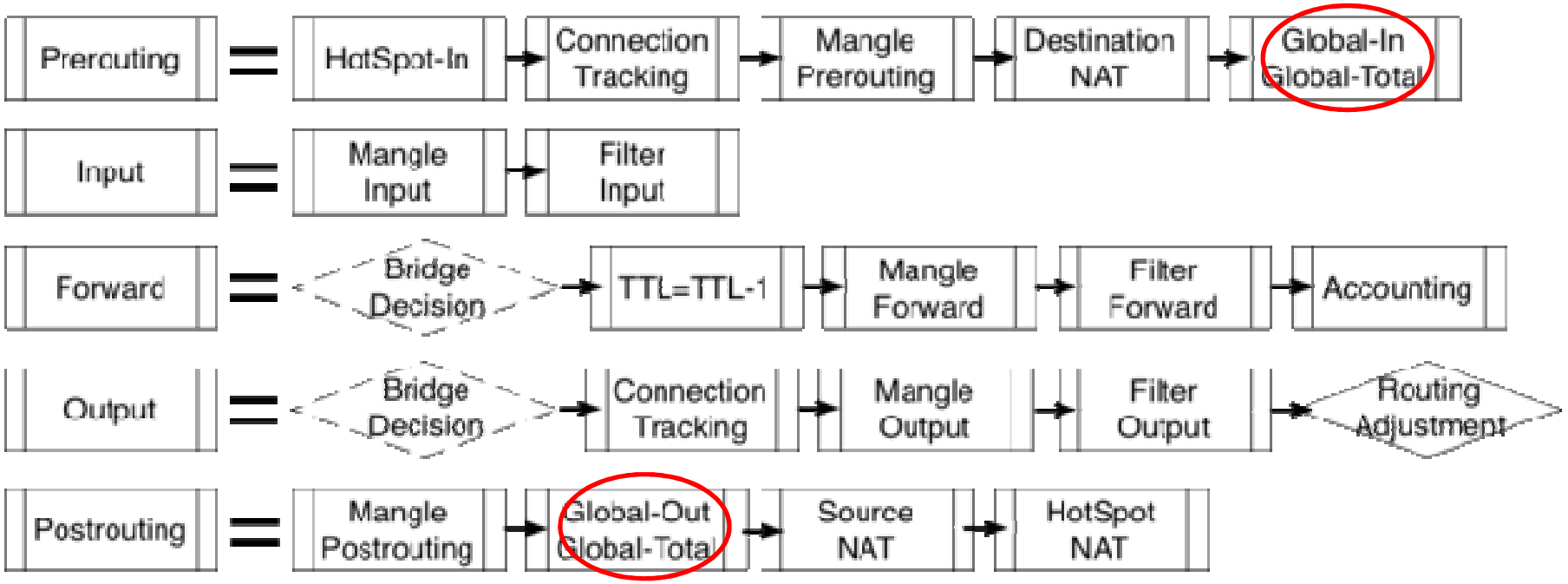
PT. Garda Lintas Cakrawala



Place to queue the packets

(zoomed view)

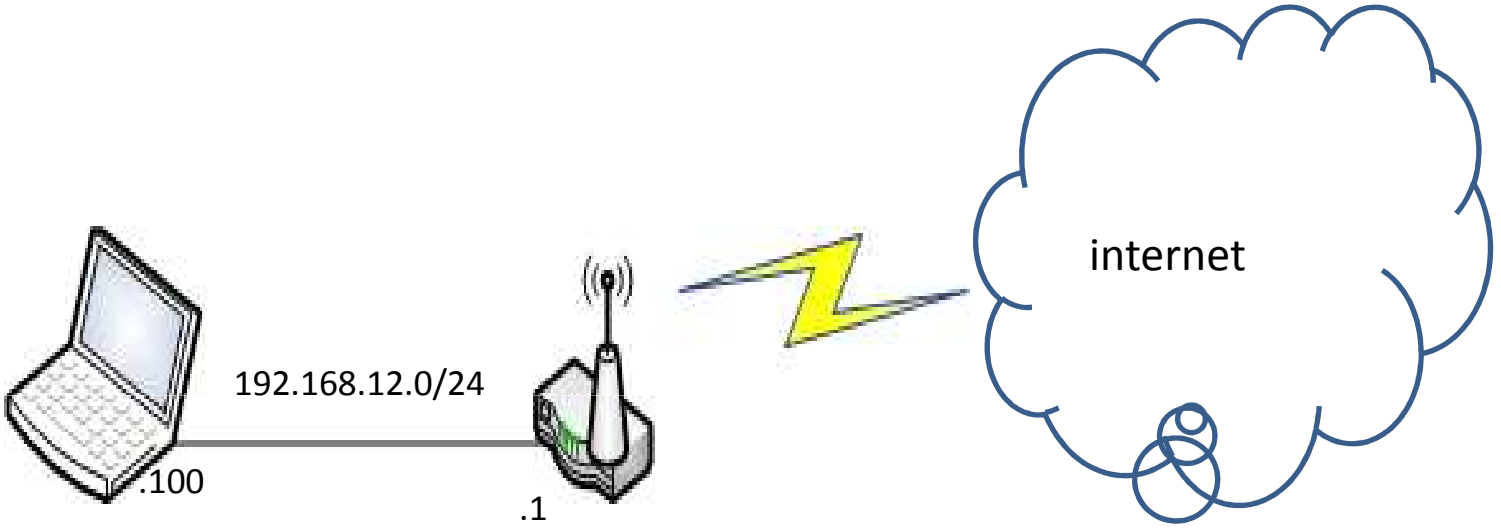
PT. Garda Lintas Cakrawala



Source: http://wiki.mikrotik.com/wiki/Packet_Flow#Diagram

Demo (topology)

PT. Garda Lintas Cakrawala



I will be downloading a file via torrent from my laptop, and the mikrotik will control the torrent traffic

Demo (scenario 1), part 1

PT. Garda Lintas Cakrawala

Setup NAT

/ip firewall nat

add action=masquerade chain=srcnat disabled=no out-interface=wlan1

Setup address-list for local network

/ip firewall address-list

add address=192.168.12.0/24 disabled=no list=local

Demo (scenario 1), part 2

PT. Garda Lintas Cakrawala

Setup MANGLE for marking the packets

/ip firewall mangle

add action=mark-connection chain=prerouting comment=conn-internet disabled=no dst-address-list=!local new-connection-mark=conn-internet passthrough=yes src-address-list=local

add action=mark-connection chain=prerouting comment=conn-p2p connection-mark=conn-internet disabled=no new-connection-mark=conn-p2p p2p=all-p2p passthrough=yes

add action=mark-packet chain=prerouting comment=conn-p2p connection-mark=conn-p2p disabled=no new-packet-mark=packet-p2p-downstream passthrough=no src-address-list=!local

Demo (scenario 1), part 3

PT. Garda Lintas Cakrawala

Setup queue type

/queue type

add kind=pcq name=pcq-downstream pcq-burst-rate=0 pcq-burst-threshold=0 pcq-burst-time=10s pcq-classifier=dst-address pcq-dst-address-mask=32 pcq-dst-address6-mask=64 pcq-limit=50 pcq-rate=0 pcq-src-address-mask=32 pcq-src-address6-mask=64 pcq-total-limit=2000

Demo (scenario 1), part 4

PT. Garda Lintas Cakrawala

Setup queue tree

/queue tree

add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=1M name=total-downstream packet-mark="" parent=global-in priority=1

add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=512k name=p2p-downstream packet-mark=packet-p2p-downstream parent=total-downstream priority=8queue=pcq-downstream

Demo (scenario 1), part 5

Download a file using torrent.

Make sure only torrent application running on your laptop.

Please check:

- Connection tracking
- Queue tree

Any missing traffic?

Demo (scenario 2), part 1

PT. Garda Lintas Cakrawala

Add new MANGLE, for unmarked traffic

/ip firewall mangle

add action=mark-connection chain=prerouting comment=conn-unmark connection-mark=conn-internet disabled=no new-connection-mark=conn-unmark passthrough=yes

add action=mark-packet chain=prerouting comment=packet-unmark-downstream connection-mark=conn-unmark disabled=no new-packet-mark=packet-unmark-downstream passthrough=no src-address-list=!local

Demo (scenario 2), part 1

PT. Garda Lintas Cakrawala

Add new queue tree, for unmarked packets

/queue tree

add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=512k name=unmark-downstream packet-mark=packet-unmark-downstream parent=total-downstream priority=1 queue=pcq-downstream

Demo (scenario 2), part 2

PT. Garda Lintas Cakrawala

Download a file using torrent.

Make sure only torrent application running on your laptop.

Please check:

- Connection tracking
- Queue tree

Any missing traffic?

Summary…

PT. Garda Lintas Cakrawala

- Shaping torrent traffic is tricky, because the nature of the protocol, and often encrypted
- Be careful with unmarked traffic, make sure you have it at the end of your mangle
- Needs different way of thinking

There is no the best system in the world, but there is always a better system

End of demo

PT. Garda Lintas Cakrawala

Thank you for your attention