PT. Garda Lintas Cakrawala

Mikrotik implementation on campus network

Achmad Mardiansyah

INDONESIA 🇮🇩

MUM zagreb, march 2013

Agenda

PT. Garda Lintas Cakrawala

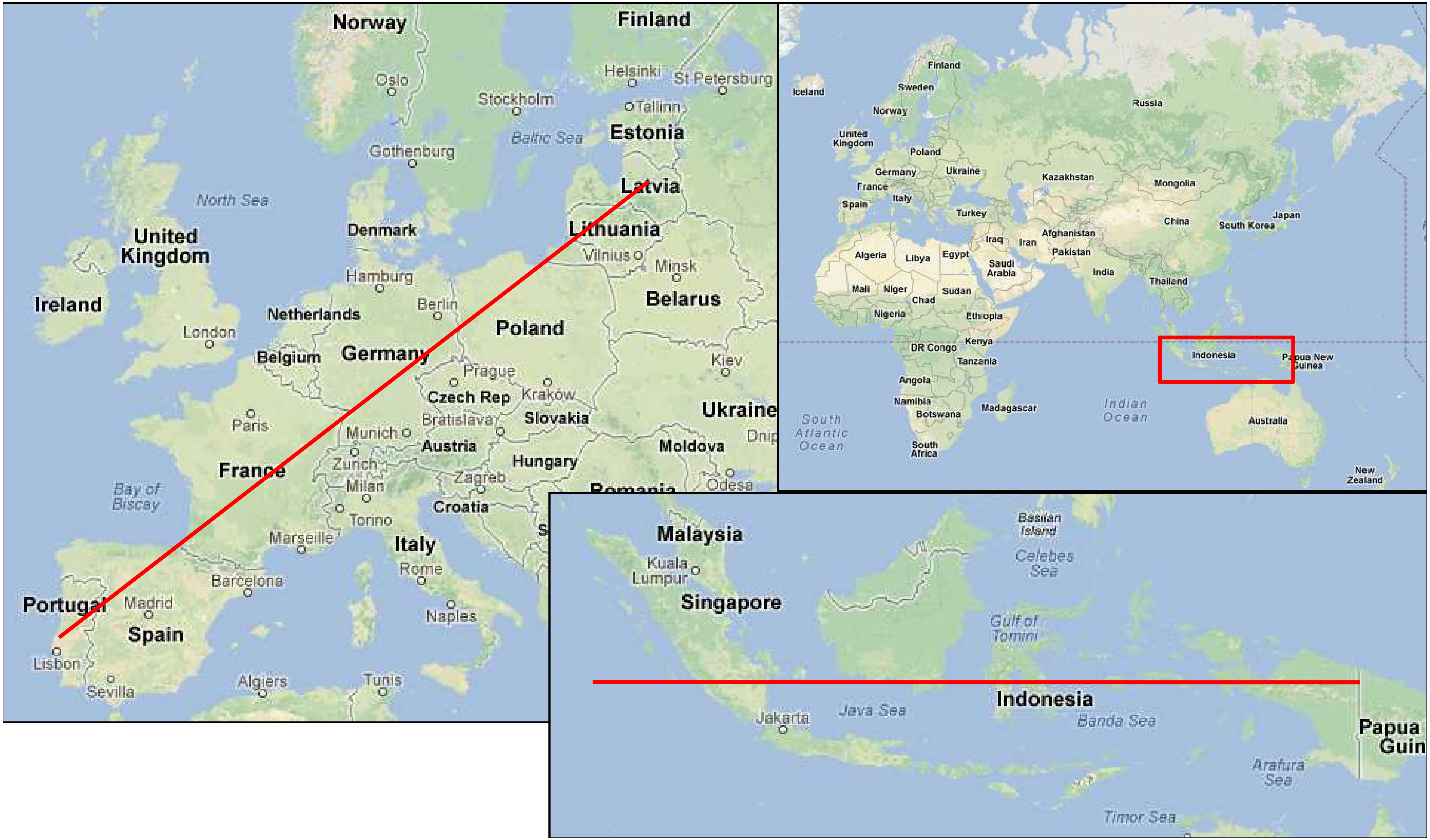
- Introduction
- About the civil engineering school
- Overview about our project
- Some cases & what we did for that
- Demo (if we have time)
- Summary

Introduction

- Name: Achmad Mardiansyah, from Indonesia
- Linux user since 1999, interested in networking & IT, working as teacher in a uni & just got trainer cert
- Topic: “mikrotik implementation on campus network”
- Background: share experience how we developed a mikrotik based solution in our past project

About Indonesia…

PT. Garda Lintas Cakrawala



Civil engineering school

PT. Garda Lintas Cakrawala

- Part of Universitas Gadjah Mada (UGM), the biggest uni in yogyakarta.
- 60+ lecturers, 600+ students, 40+ staffs, and several buildings

Map
Satellite
Hybrid
Google
Imagery ©2013 DigitalGlobe, GeoEye, Map data ©2013 Tele Atlas - Terms of Use

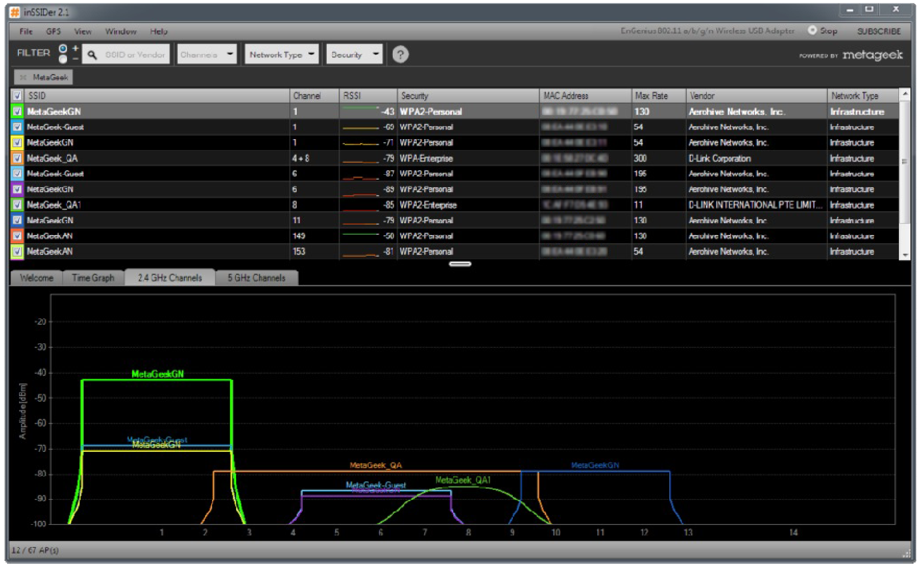
Our project (before start)

- Old cat5 cables
- Lots of hubs & unmanaged switch (lead to looping)
- PC router (linux PC)
- No monitoring
- No authorized access
- No traffic control
- Virus & broadcast problem

Case 1: wireless access

PT. Garda Lintas Cakrawala

- Before:
  - Each access point has different SSID
  - Different security policy
- What we did:
  - Setup uniform SSID
  - Uniform security profile
  - Apply client isolation
  - Radio optimization



☑	SSID	Channel	RSSI	Security	MAC Address	Max Rate	Vendor	Network Type
☑	MetaGeekGN	1	-43	WPA2-Personal	[redacted]	130	Aerohive Networks, Inc.	Infrastructure
☑	MetaGeek-Guest	1	-69	WPA2-Personal	[redacted]	54	Aerohive Networks, Inc.	Infrastructure
☑	MetaGeekGN	1	-71	WPA2-Personal	[redacted]	54	Aerohive Networks, Inc.	Infrastructure
☑	MetaGeek_QA	4 + 8	-79	WPA-Enterprise	[redacted]	300	D-Link Corporation	Infrastructure
☑	MetaGeek-Guest	6	-87	WPA2-Personal	[redacted]	195	Aerohive Networks, Inc.	Infrastructure
☑	MetaGeekGN	6	-89	WPA2-Personal	[redacted]	195	Aerohive Networks, Inc.	Infrastructure
☑	MetaGeek_QA1	8	-85	WPA2-Enterprise	[redacted]	11	D-LINK INTERNATIONAL PTE LIMIT...	Infrastructure
☑	MetaGeekGN	11	-79	WPA2-Personal	[redacted]	130	Aerohive Networks, Inc.	Infrastructure
☑	MetaGeekAN	149	-50	WPA2-Personal	[redacted]	130	Aerohive Networks, Inc.	Infrastructure
☑	MetaGeekAN	153	-81	WPA2-Personal	[redacted]	54	Aerohive Networks, Inc.	Infrastructure

Case 1: wireless access

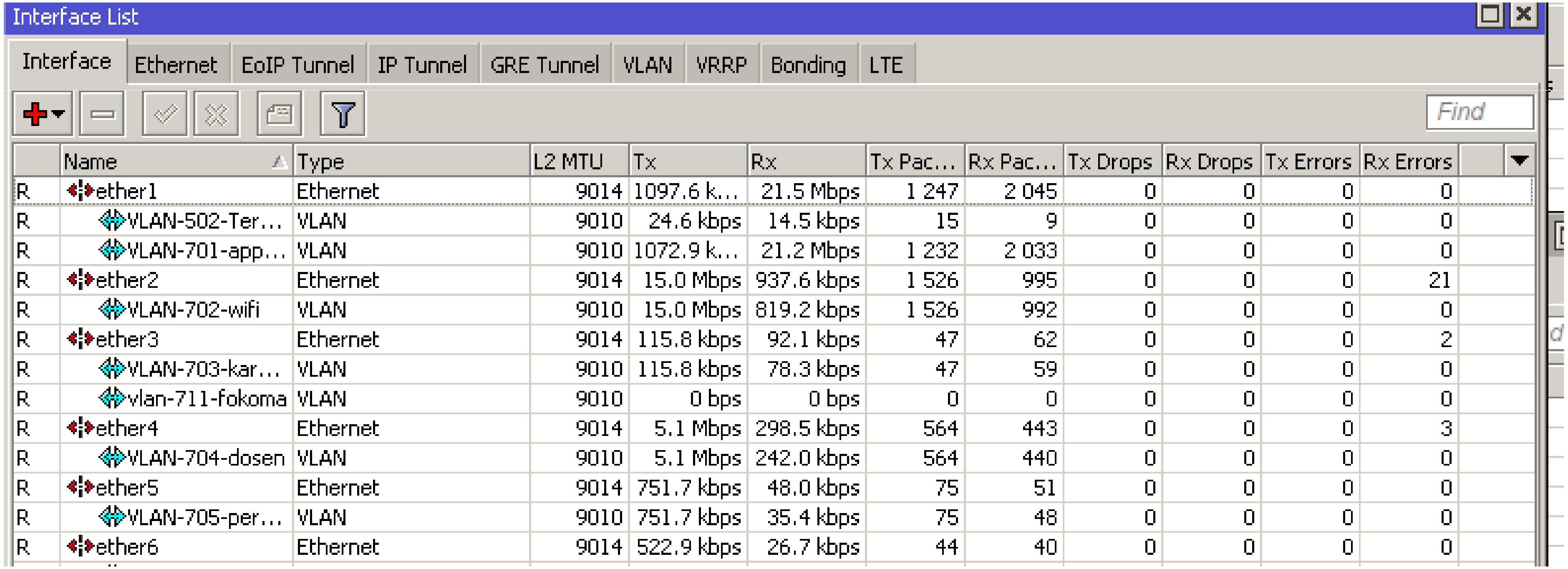
- Further improvement:
  - Use dhcp for AP’s IP address
  - Centralized database for wireless access points configuration
  - Have APs that can do Multiple SSID & support VLAN

Case 2: network segmentation

- 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

- 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

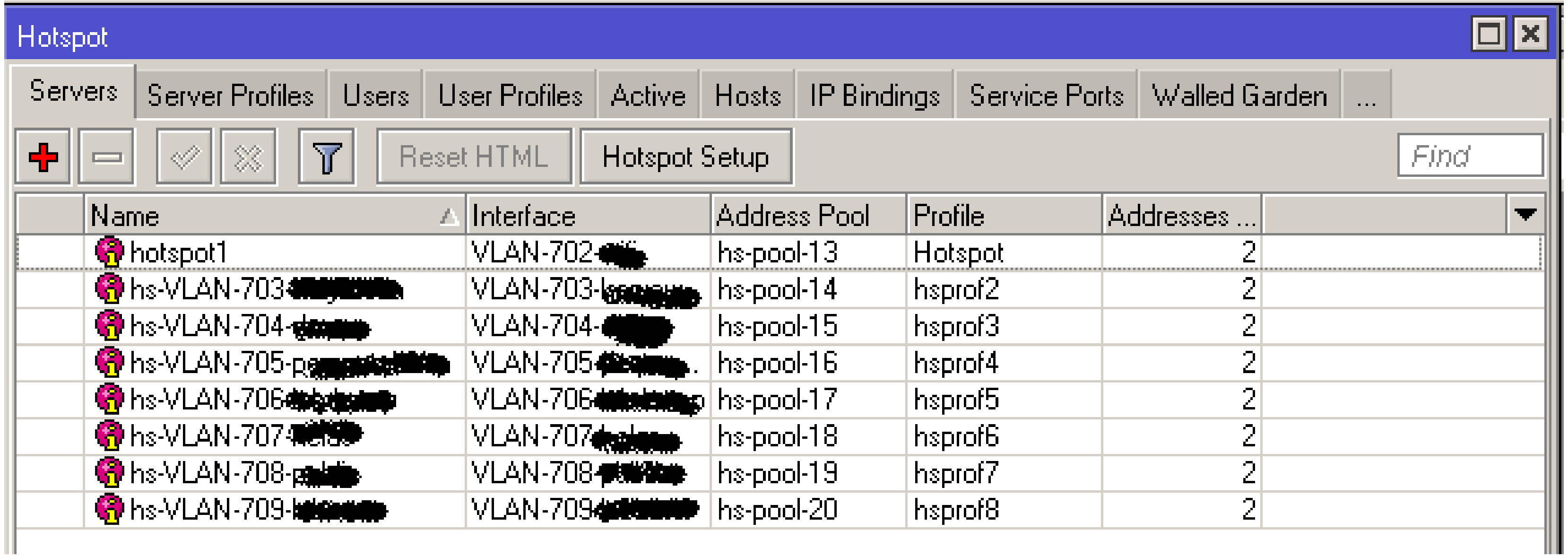
Case 3: access control

- 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



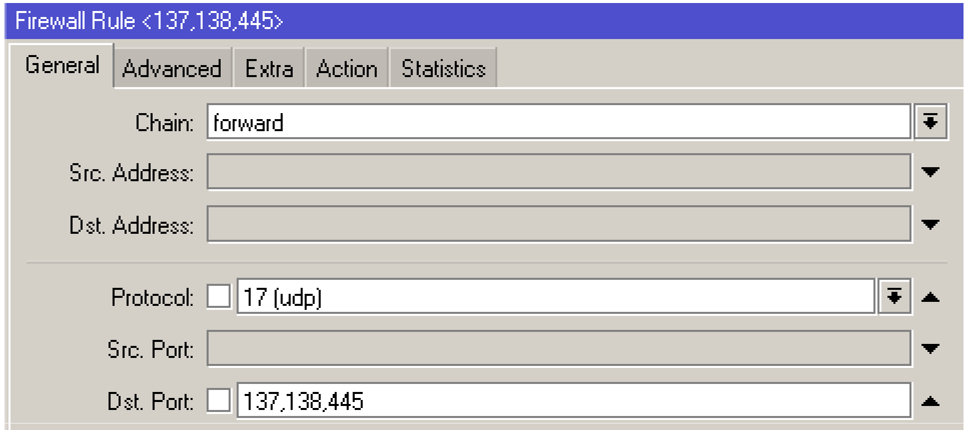
Name	Interface	Address Pool	Profile	Addresses ...
hotspot1	VLAN-702-[redacted]	hs-pool-13	Hotspot	2
hs-VLAN-703[redacted]	VLAN-703-[redacted]	hs-pool-14	hsprof2	2
hs-VLAN-704-[redacted]	VLAN-704-[redacted]	hs-pool-15	hsprof3	2
hs-VLAN-705-[redacted]	VLAN-705[redacted]	hs-pool-16	hsprof4	2
hs-VLAN-706[redacted]	VLAN-706[redacted]	hs-pool-17	hsprof5	2
hs-VLAN-707[redacted]	VLAN-707[redacted]	hs-pool-18	hsprof6	2
hs-VLAN-708-[redacted]	VLAN-708[redacted]	hs-pool-19	hsprof7	2
hs-VLAN-709-[redacted]	VLAN-709[redacted]	hs-pool-20	hsprof8	2

Case 4: transparent firewall

- 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


Firewall Rule <137,138,445>

Chain: forward

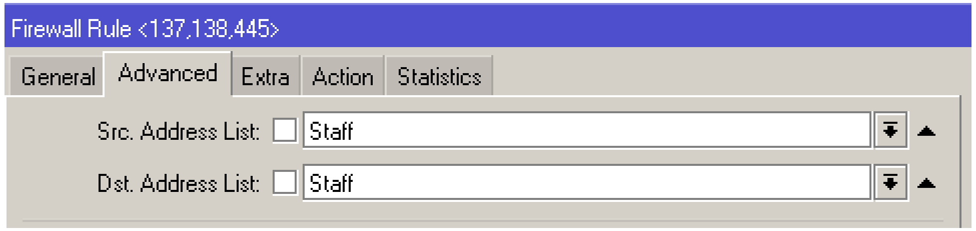
Src. Address:

Dst. Address:

Protocol: □ 17 (udp)

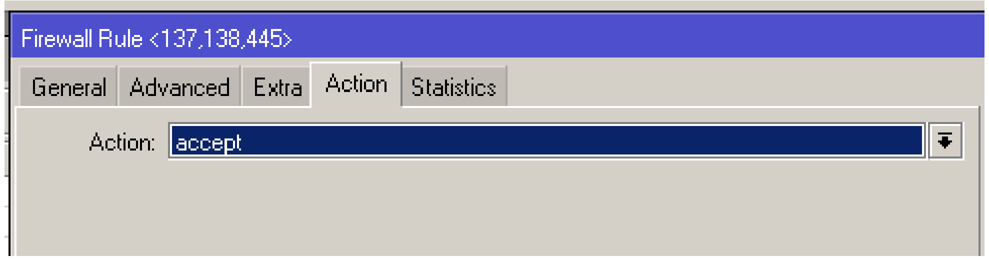
Src. Port:

Dst. Port: □ 137,138,445


Firewall Rule <137,138,445>

Src. Address List: □ Staff

Dst. Address List: □ Staff


Firewall Rule <137,138,445>

Action: accept

Case 5: QOS

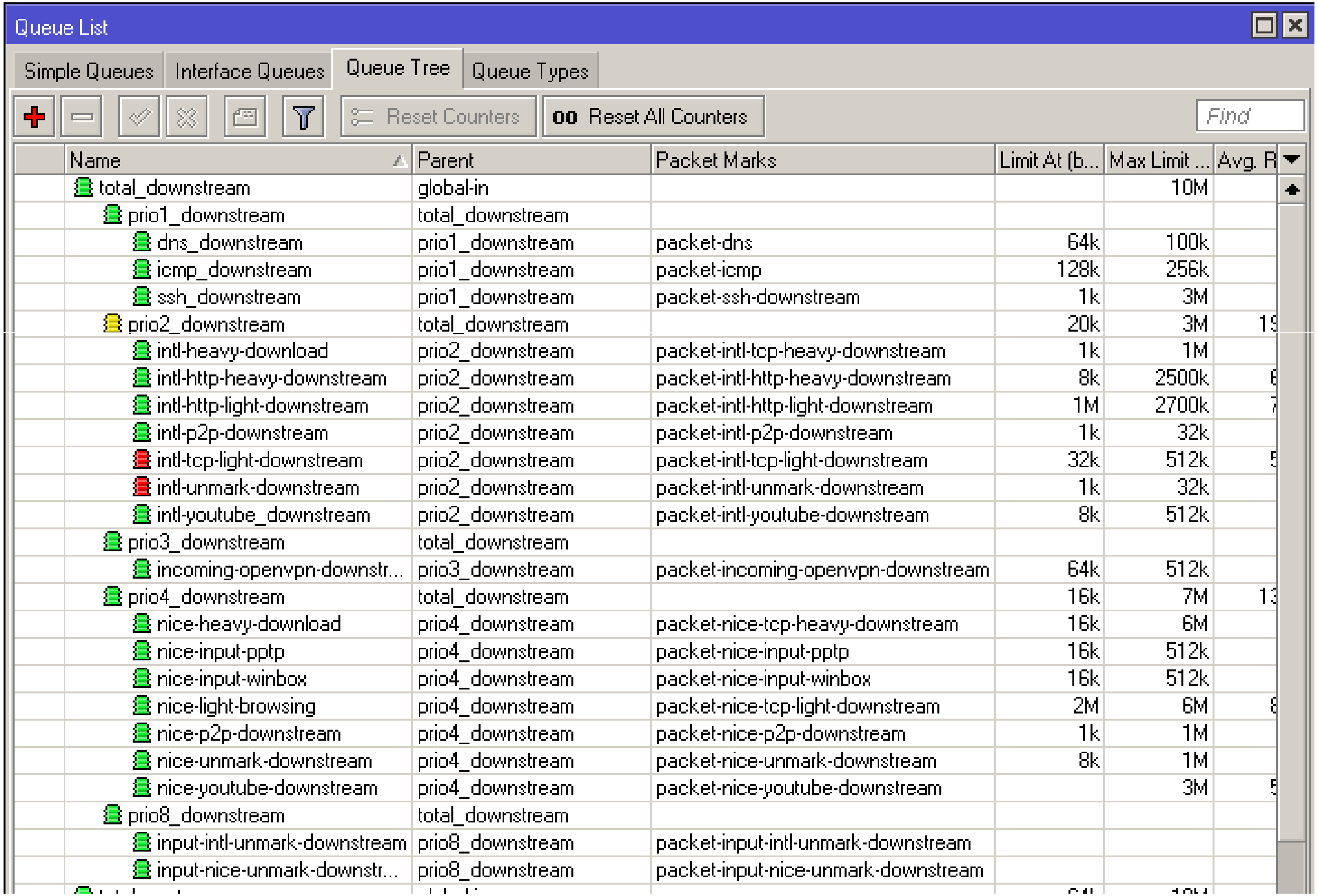
- Before:
  - – http QOS was done via transparent squid, working well. Not so flexible in term of time, dynamic allocation.
  - – No QOS for other protocol. One user dominating the traffic
- What we did:
  - – Implement mikrotik queue-tree. We have complex requirements to be satisfied

Case 6: fighting torrent

- 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	6
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

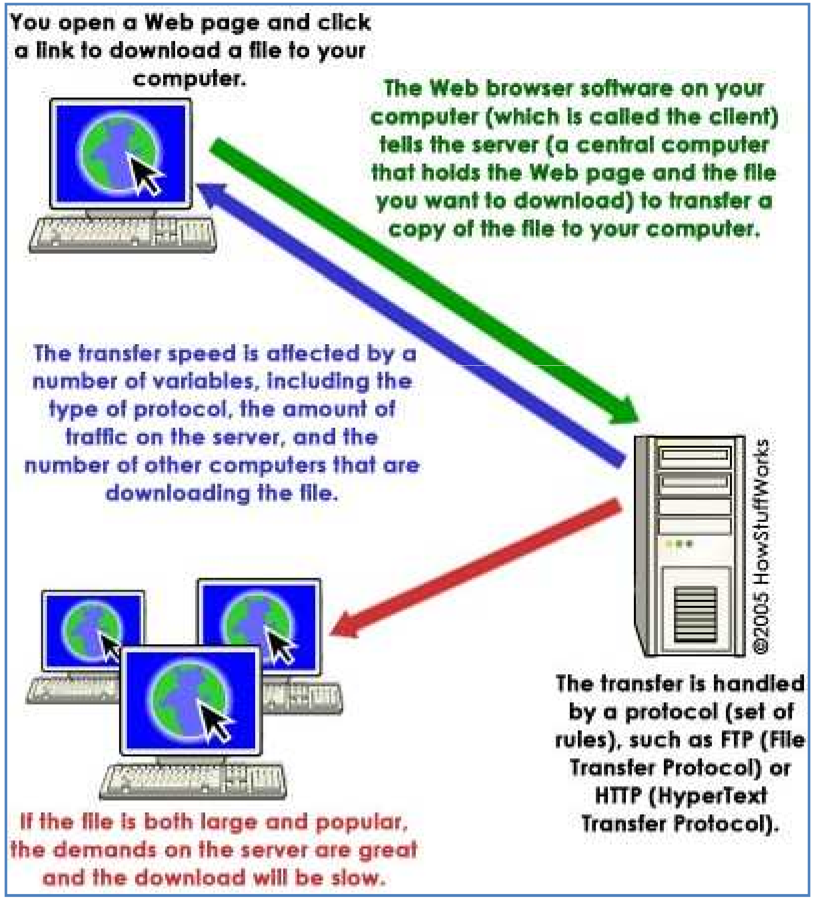
Agenda

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

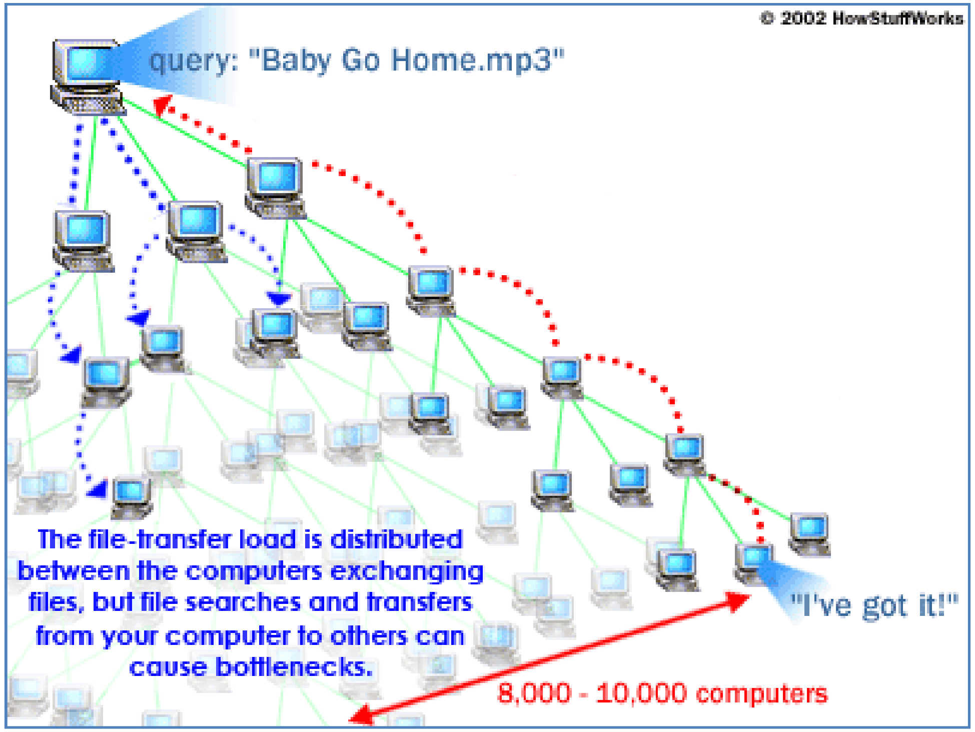
What is torrent…

PT. Garda Lintas Cakrawala

Traditional File transfer

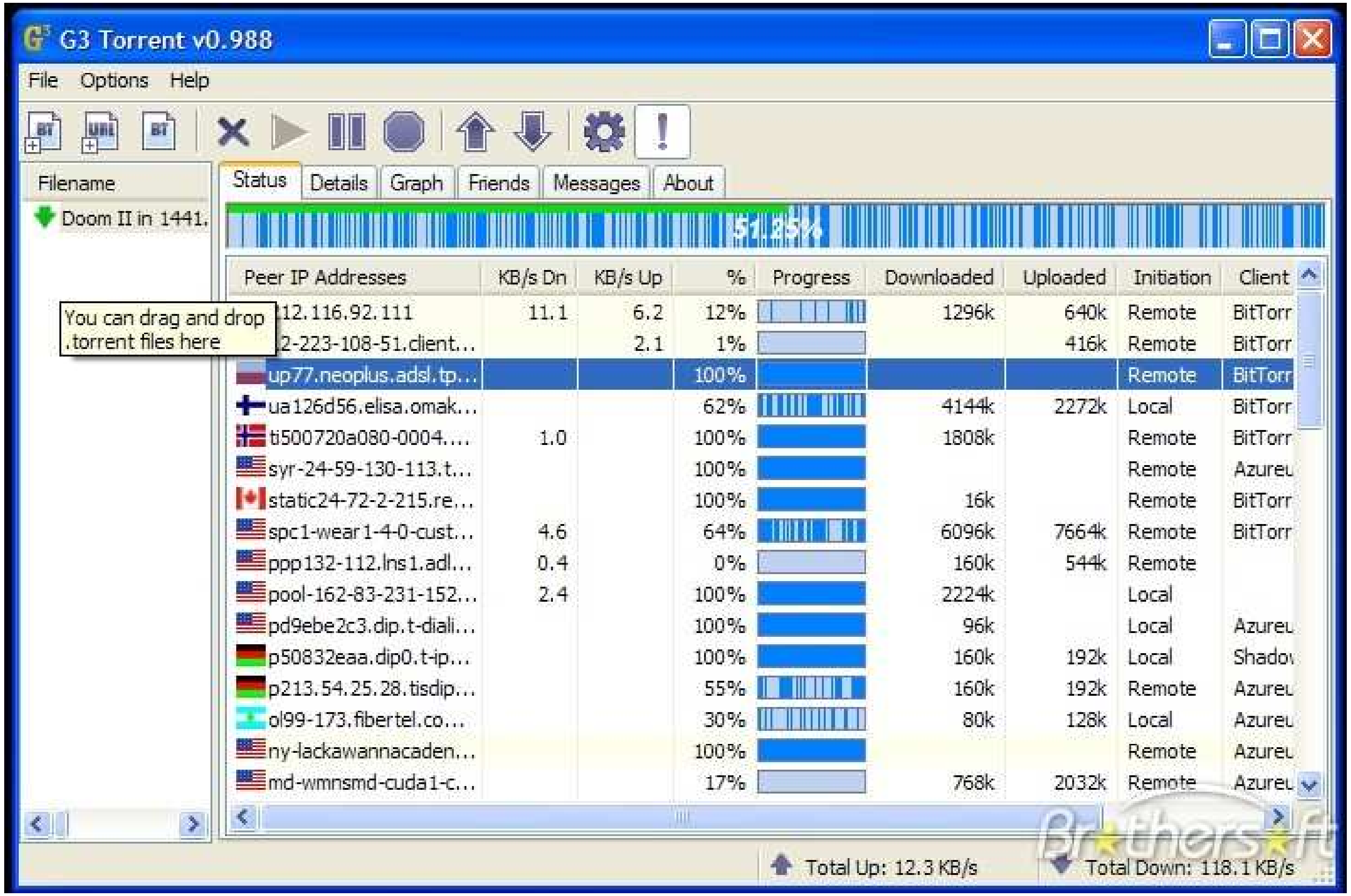

You open a Web page and click a link to download a file to your computer.
The Web browser software on your computer (which is called the client) tells the server (a central computer that holds the Web page and the file you want to download) to transfer a copy of the file to your computer.
The transfer speed is affected by a number of variables, including the type of protocol, the amount of traffic on the server, and the number of other computers that are downloading the file.
©2005 HowStuffWorks
The transfer is handled by a protocol (set of rules), such as FTP (File Transfer Protocol) or HTTP (HyperText Transfer Protocol).
If the file is both large and popular, the demands on the server are great and the download will be slow.

Peer-to-peer file transfer


© 2002 HowStuffWorks
query: "Baby Go Home.mp3"
The file-transfer load is distributed between the computers exchanging files, but file searches and transfers from your computer to others can cause bottlenecks.
"I've got it!"
8,000 - 10,000 computers

Torrent in action…

PT. Garda Lintas Cakrawala



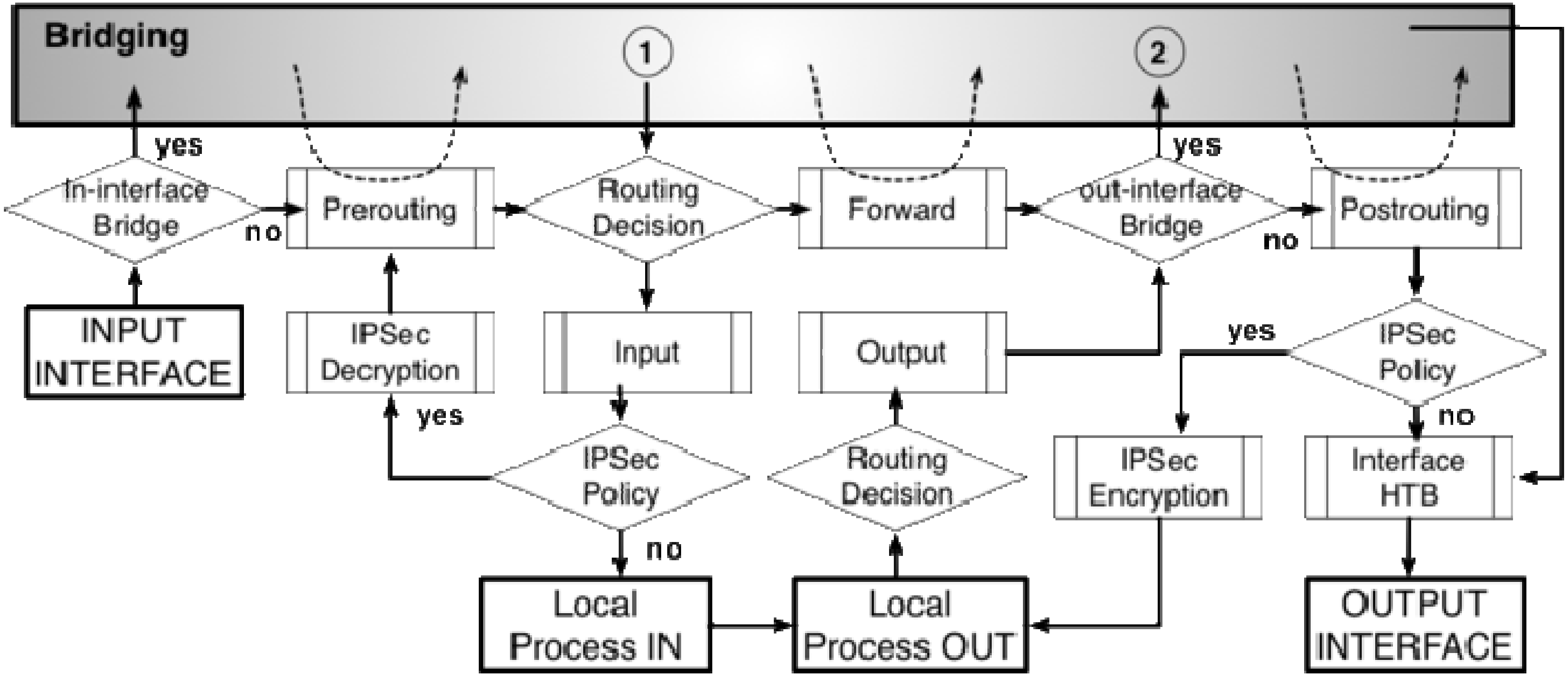
Peer IP Addresses	KB/s Dn	KB/s Up	%	Progress	Downloaded	Uploaded	Initiation	Client
12.116.92.111	11.1	6.2	12%		1296k	640k	Remote	BitTorr
2-223-108-51.client…		2.1	1%			416k	Remote	BitTorr
up77.neoplus.adsl.tp…			100%				Remote	BitTorr
ua126d56.elisa.omak…			62%		4144k	2272k	Local	BitTorr
ti500720a080-0004.…	1.0		100%		1808k		Remote	BitTorr
syr-24-59-130-113.t…			100%				Remote	Azureu
static24-72-2-215.re…			100%		16k		Remote	BitTorr
spc1-wear1-4-0-cust…	4.6		64%		6096k	7664k	Remote	BitTorr
ppp132-112.lns1.adl…	0.4		0%		160k	544k	Remote	
pool-162-83-231-152…	2.4		100%		2224k		Local	
pd9ebe2c3.dip.t-diali…			100%		96k		Local	Azureu
p50832eaa.dip0.t-ip…			100%		160k	192k	Local	Shado
p213.54.25.28.tisdip…			55%		160k	192k	Remote	Azureu
ol99-173.fibertel.co…			30%		80k	128k	Local	Azureu
ny-lackawannacaden…			100%				Remote	Azureu
md-wmnsmd-cuda1-c…			17%		768k	2032k	Remote	Azureu

Total Up: 12.3 KB/s

Total Down: 118.1 KB/s

Packet flow

PT. Garda Lintas Cakrawala

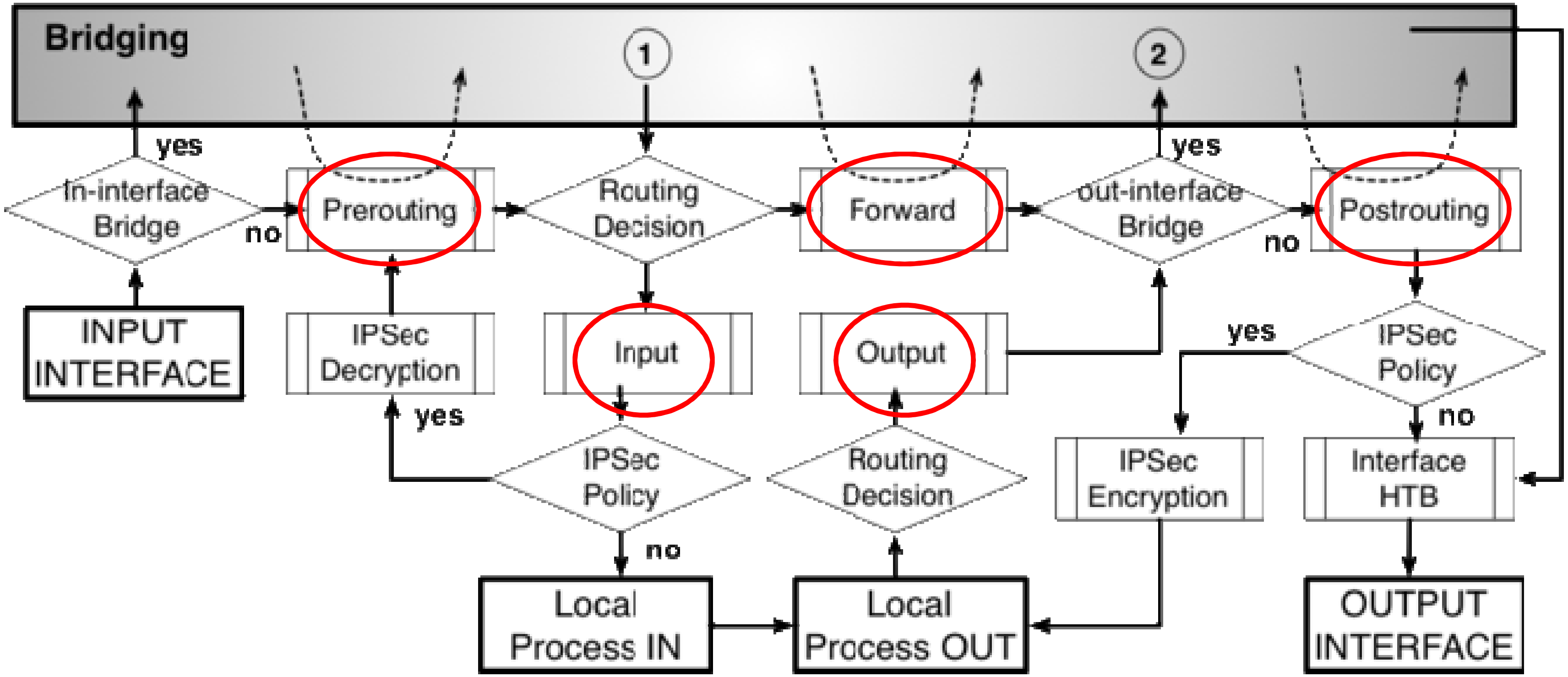


Source: http://wiki.mikrotik.com/wiki/Packet_Flow#Diagram

Iptables mangle

PT. Garda Lintas Cakrawala

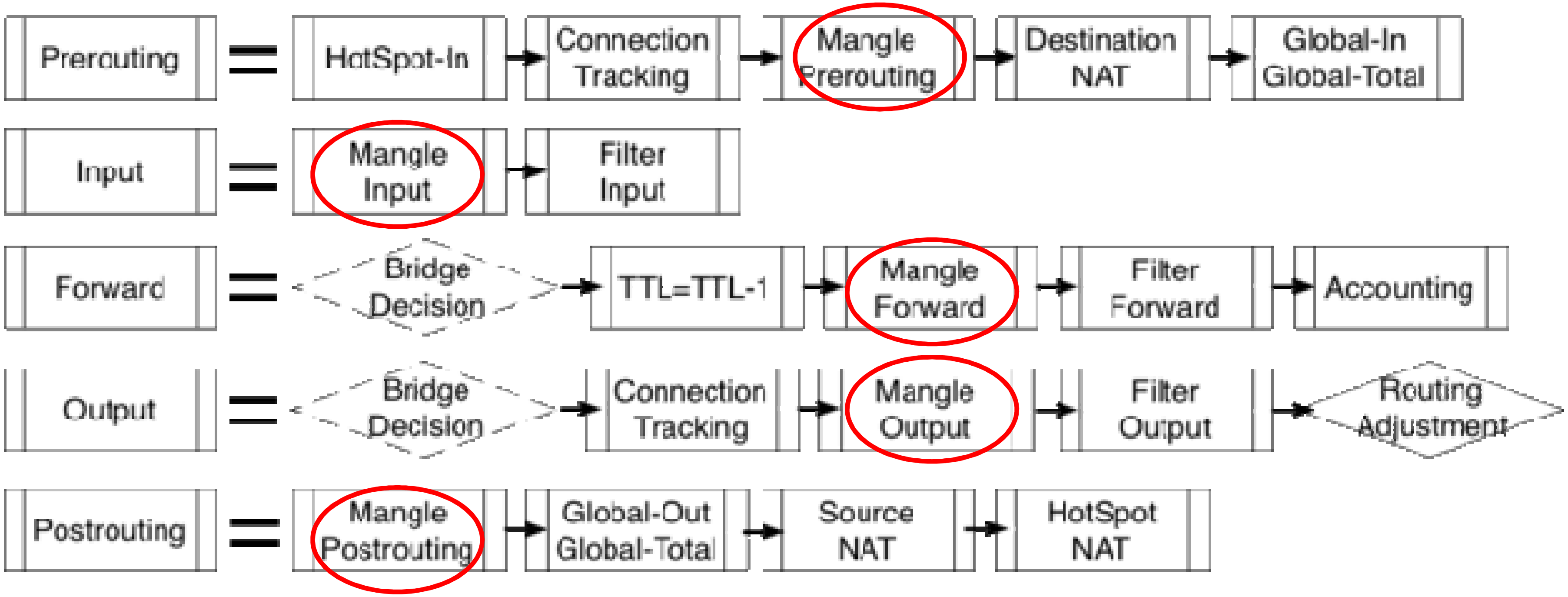
The places (chains) to mark packets



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

Chain in mangle table

(zoomed view)



Prerouting = HotSpot-In → Connection Tracking → Mangle Prerouting → Destination NAT → Global-In Global-Total

Input = Mangle Input → Filter Input

Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting

Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment

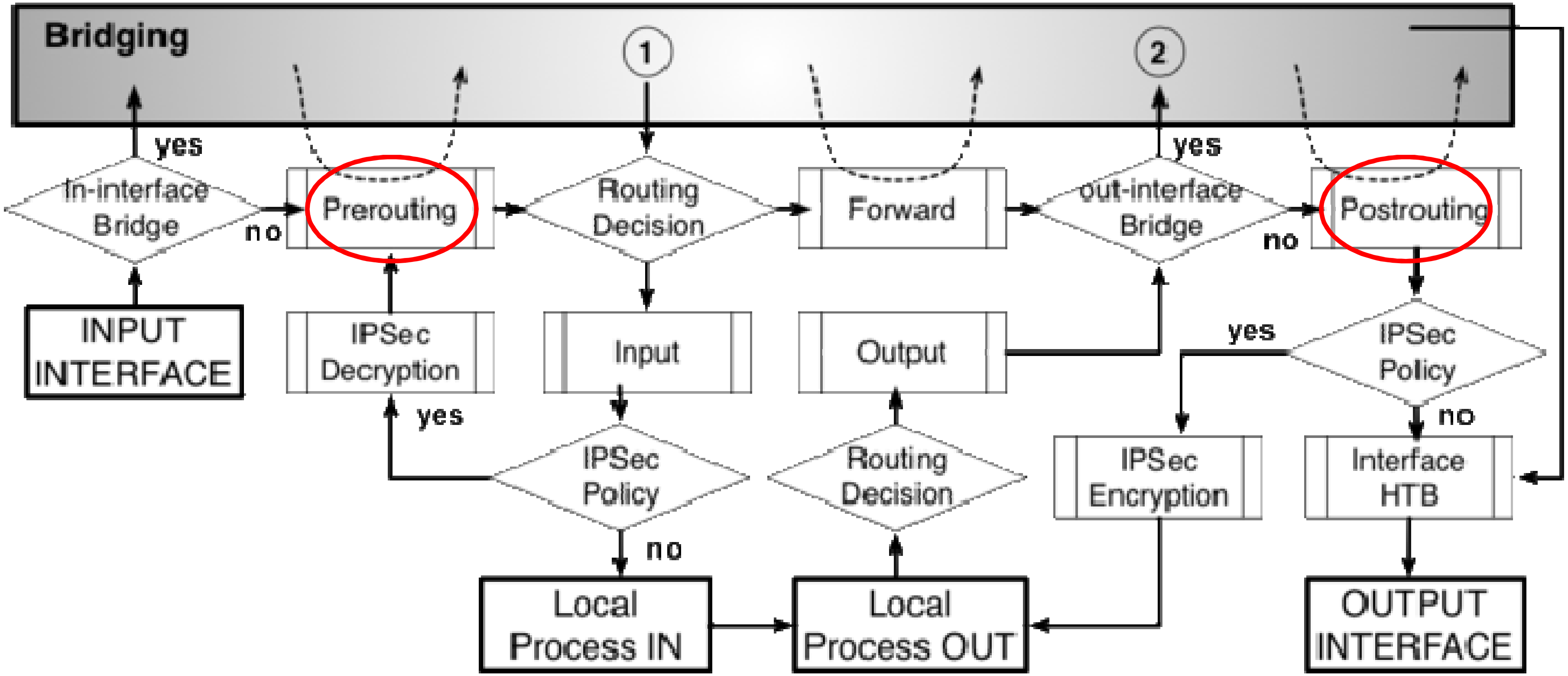
Postrouting = Mangle Postrouting → Global-Out Global-Total → Source NAT → HotSpot NAT

Queue tree

- 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

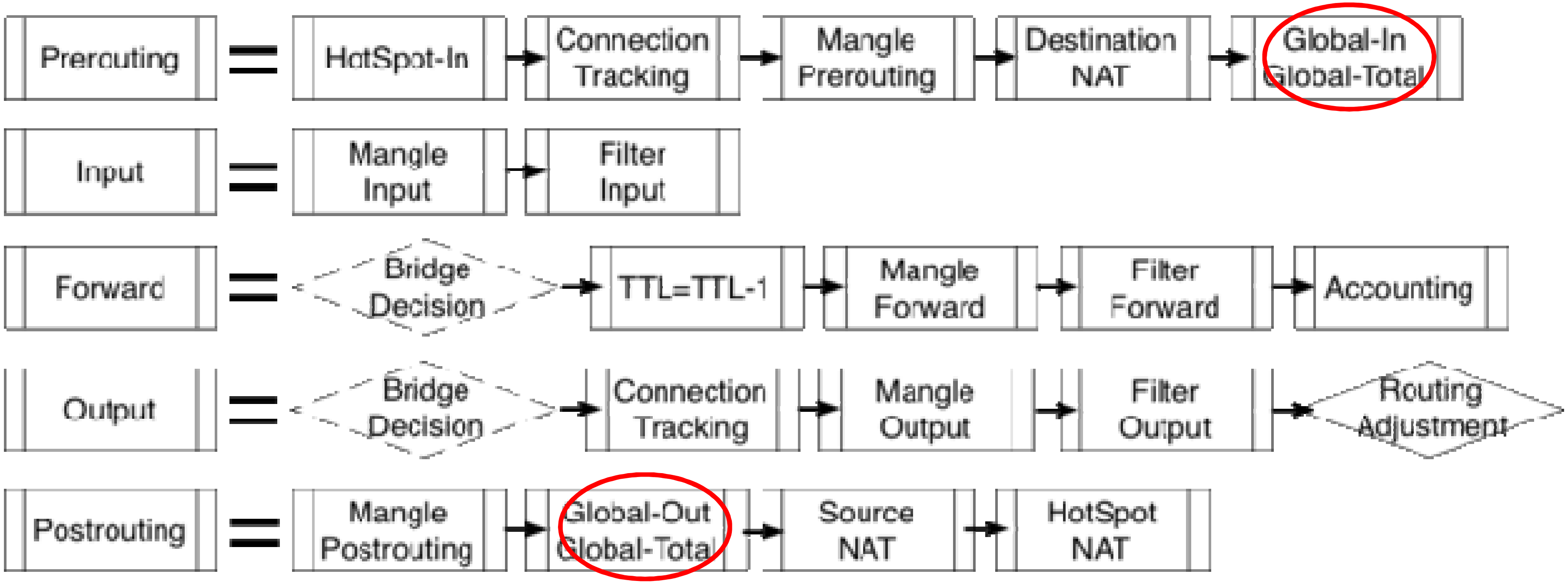
PT. Garda Lintas Cakrawala



PT. Garda Lintas Cakrawala

Place to queue the packets

(zoomed view)



Prerouting = HotSpot-In → Connection Tracking → Mangle Prerouting → Destination NAT → Global-In Global-Total

Input = Mangle Input → Filter Input

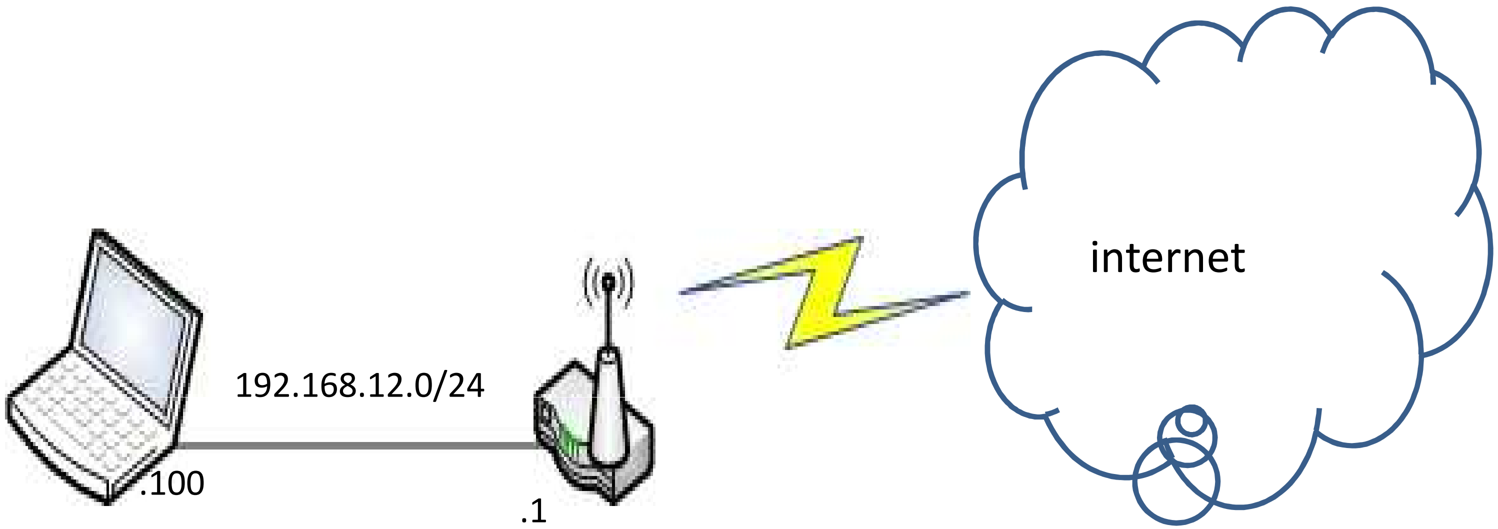
Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting

Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment

Postrouting = Mangle Postrouting → Global-Out Global-Total → Source NAT → HotSpot NAT

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

Demo (topology)



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

Demo (scenario 1), part 1

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

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

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

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?

Demo (scenario 2), part 1

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

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

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

Thank you for your attention