

# Welcome Back



**mum**  
Mikrotik User Meeting

**MUM NIGERIA**  
LAGOS, NOVEMBER 28, 2017

# 10 Years On!



# Quality of Service & Bandwidth Management in RouterOS v.6

**Oluyinka Thomas**

thomolar@yahoo.com

MikroTik User Meeting

Lagos, Nigeria

28<sup>th</sup> November, 2017

# About Me

- Electrical/Electronics Engineering graduate from University of Ibadan, Nigeria
- Worked briefly with Procter & Gamble **P&G**
- Worked mostly in the Oil & Gas upstream service industry
  - Coiled Tubing Services **Schlumberger**

# About Me

- Passionate about IT & Telecommunication
- VSAT installer partner for Taide Network AS
  - Taide became Vizada then became part of Astrium
- Love MikroTik RouterOS to bits 
- Started using RouterOS from v.2.9
- Certified in MTCNA, MTCRE, MTCINE, Certified Trainer

# Agenda

- Define Quality of Service
- Define Bandwidth Management
- Highlight Benefits of Both
- Discuss Implementation Tools for Both
- Examine RouterOS Screenshots on Winbox
- Implementation Examples
- Summary & Conclusion

# What is Quality of Service (QoS)?

- Refers to traffic prioritization and resource reservation control mechanisms
- Ability to provide different priorities to different applications, users or data flows
- Guarantee a certain level of performance to a **data flow**

# Objective of QoS

- Anybody can deploy internet services
- Identify what affects overall satisfaction of the client
- Capture traffic usage patterns & customize router to dynamically work for them
- Key objective of QoS is differentiation

# Bandwidth Management

- The process of measuring and controlling the communications (traffic, packets) on a network link
- Objective is to avoid filling the link to capacity or overfilling the link
- Results in network congestion and poor performance of the network if not done



# Benefits to ISP's

- High-cost traffic networks are major assets for ISP's
- Gives the intangible yet significant benefit of seeing what internet traffic is flowing through the network
- Allows ISPs to tier their services to guarantee particular QoS
- Reduces costs and increases the menu of products offered



# Benefits to Enterprises

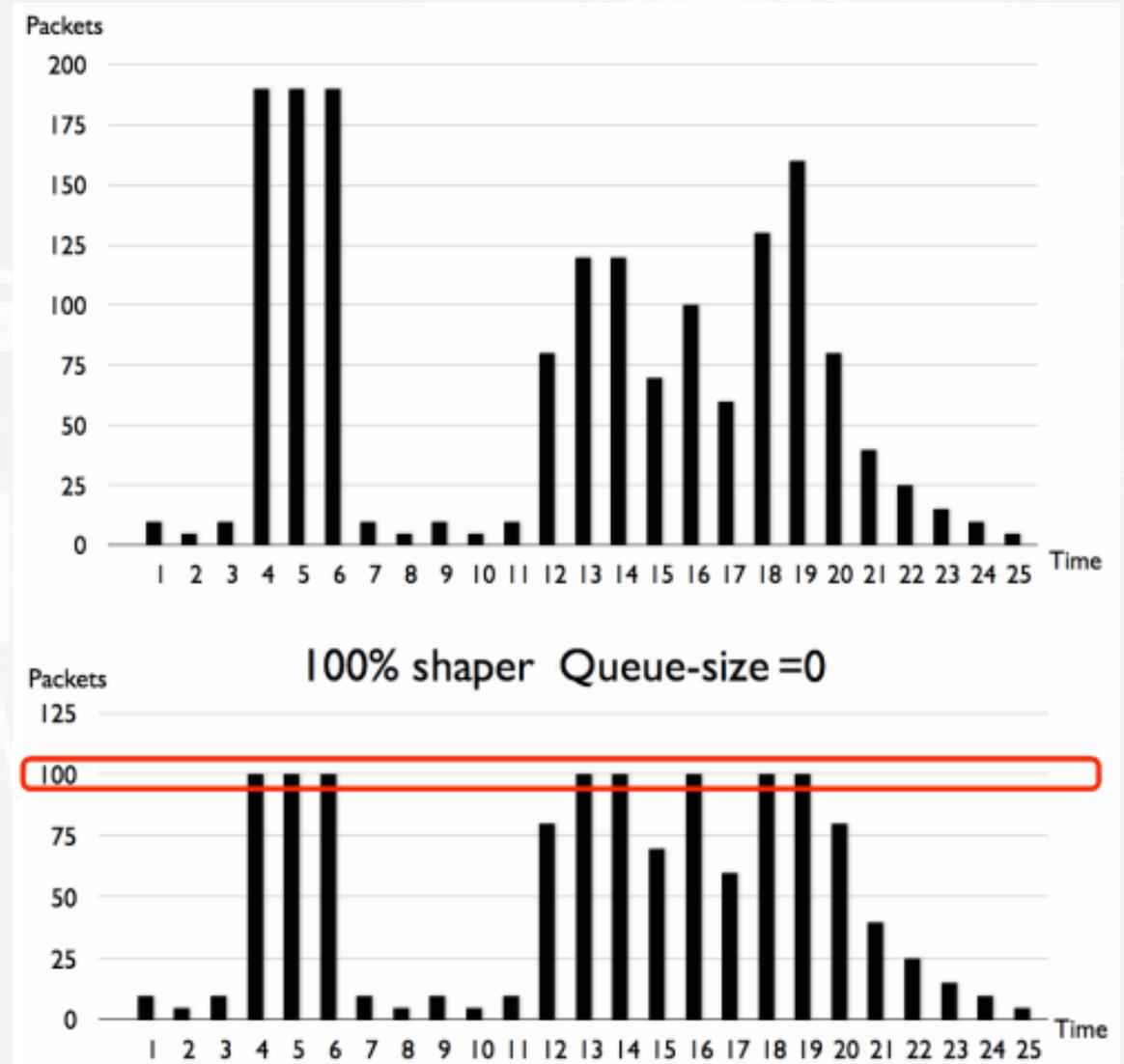
- Applications are centrally hosted at the head office
- Remote offices are expected to pull data from central databases and server farms
- Ensures business-oriented traffic gets priority over best-effort non-critical traffic
- A good means for companies to avoid purchasing additional bandwidth, while properly managing existing resources

# Bandwidth Management in ROS

- MikroTik RouterOS is one of the most advanced and easy to configure operating system for bandwidth management
- Traffic shaping (Rate Limiting)
  - HTB and PCQ
- Traffic equalizing (Rate Scheduler)
  - RED, FIFO, SFQ

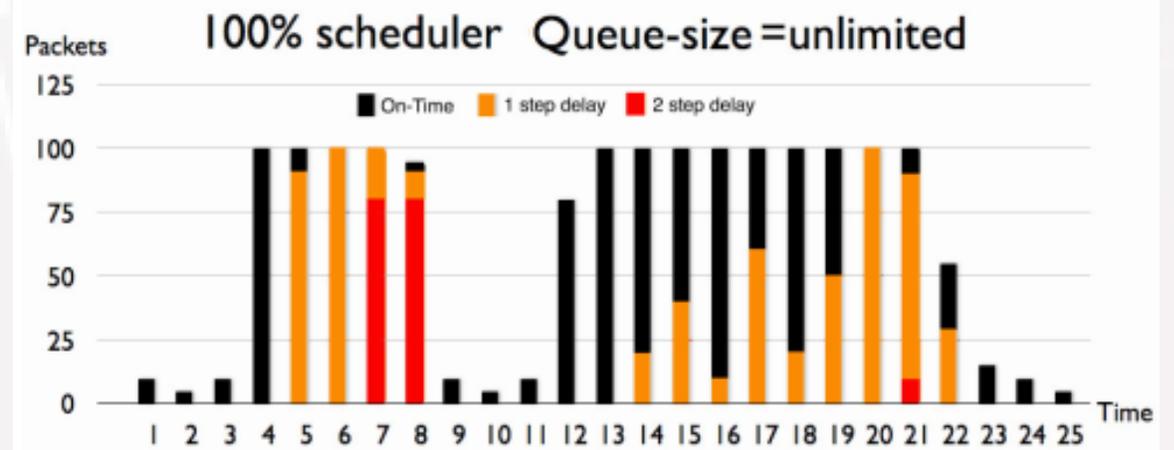
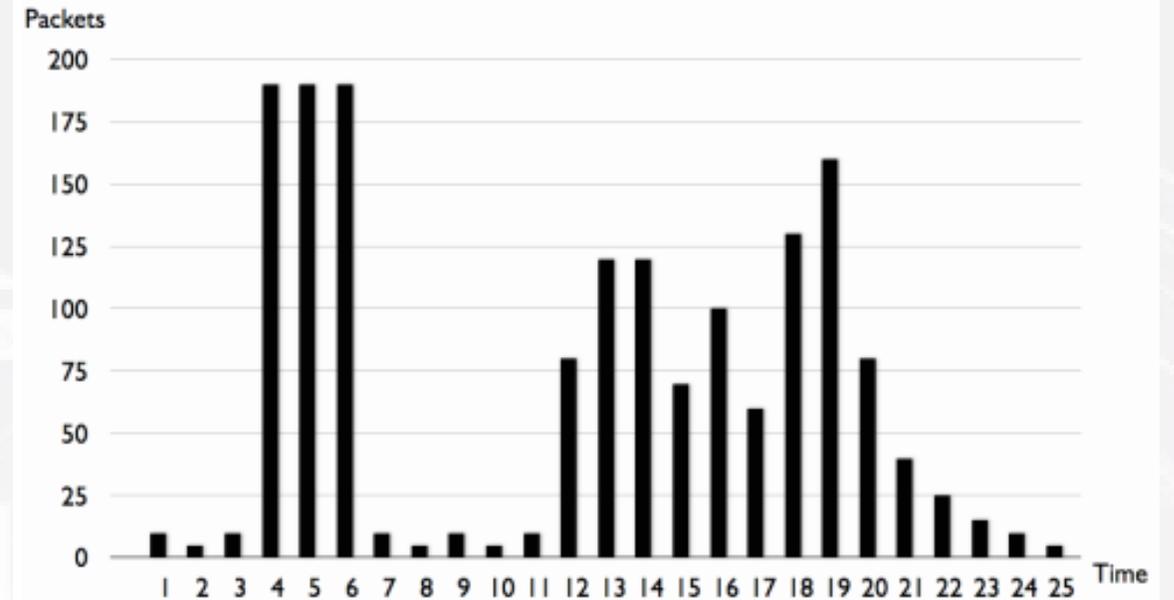
# Rate Limiting

- Assume max-limit is '100'
- 100% shaper has no queue size
- Therefore packets are dropped when it reaches 100
- In this example about 22% is dropped
- Result: Latency is low



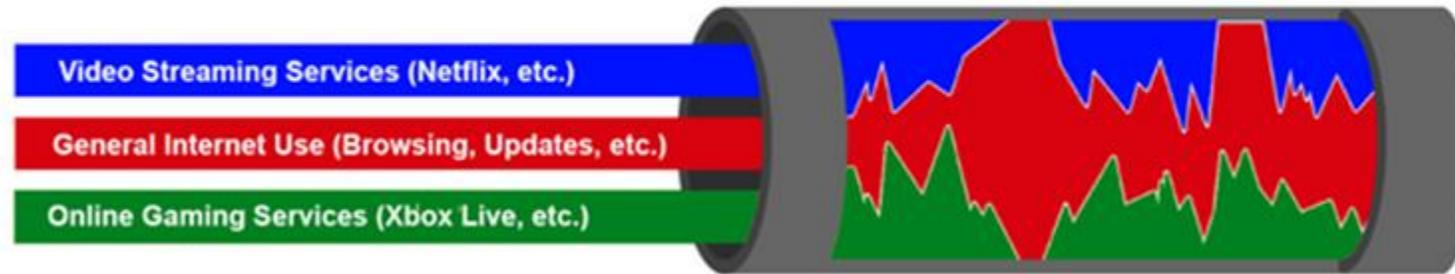
# Rate Scheduler

- Assume max-limit is '100'
- Queue size is unlimited
- Therefore no packets are dropped when it reaches 100
- In this example 39% are delayed once, 11% delayed twice
- Result: Latency is high

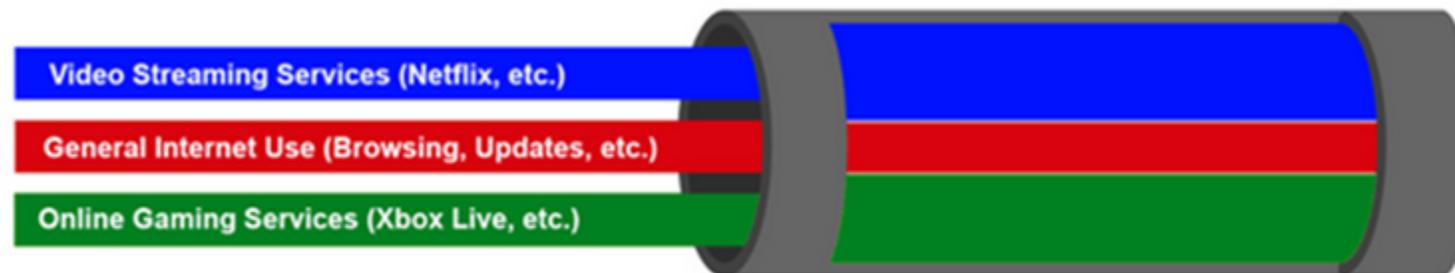


# Bandwidth with & without QoS

Bandwidth with no Quality of Service rules applied



Bandwidth with Quality of Service rules applied



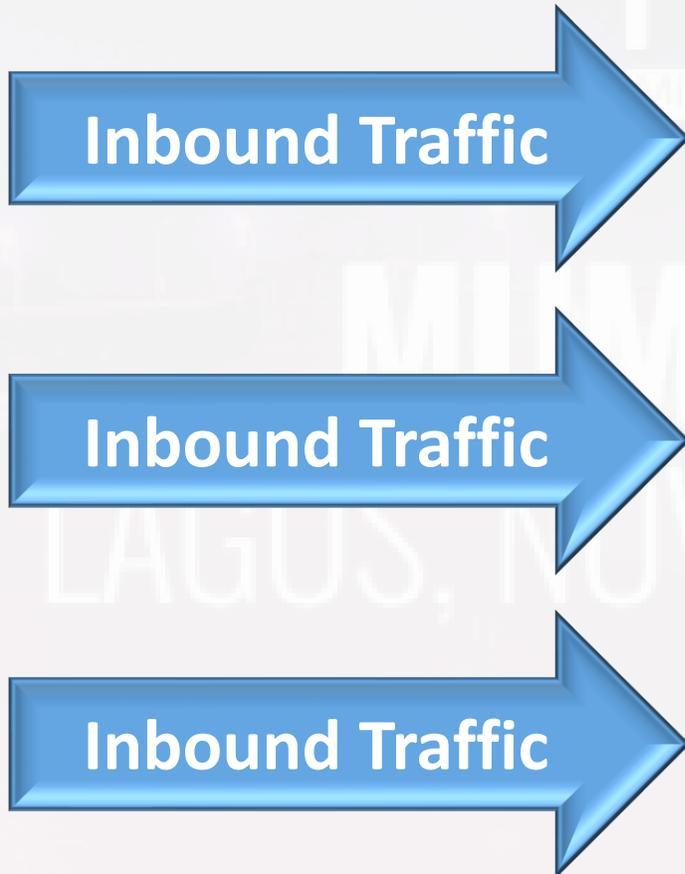
# Fundamental Concepts



- We have no control on how much traffic is being sent to an interface
- Traffic control can only be done as the traffic leaves from the interface
- Hence, all control is done on the outbound interface irrespective of upload or download

# Traffic Control to an Interface

No Control



Full Control



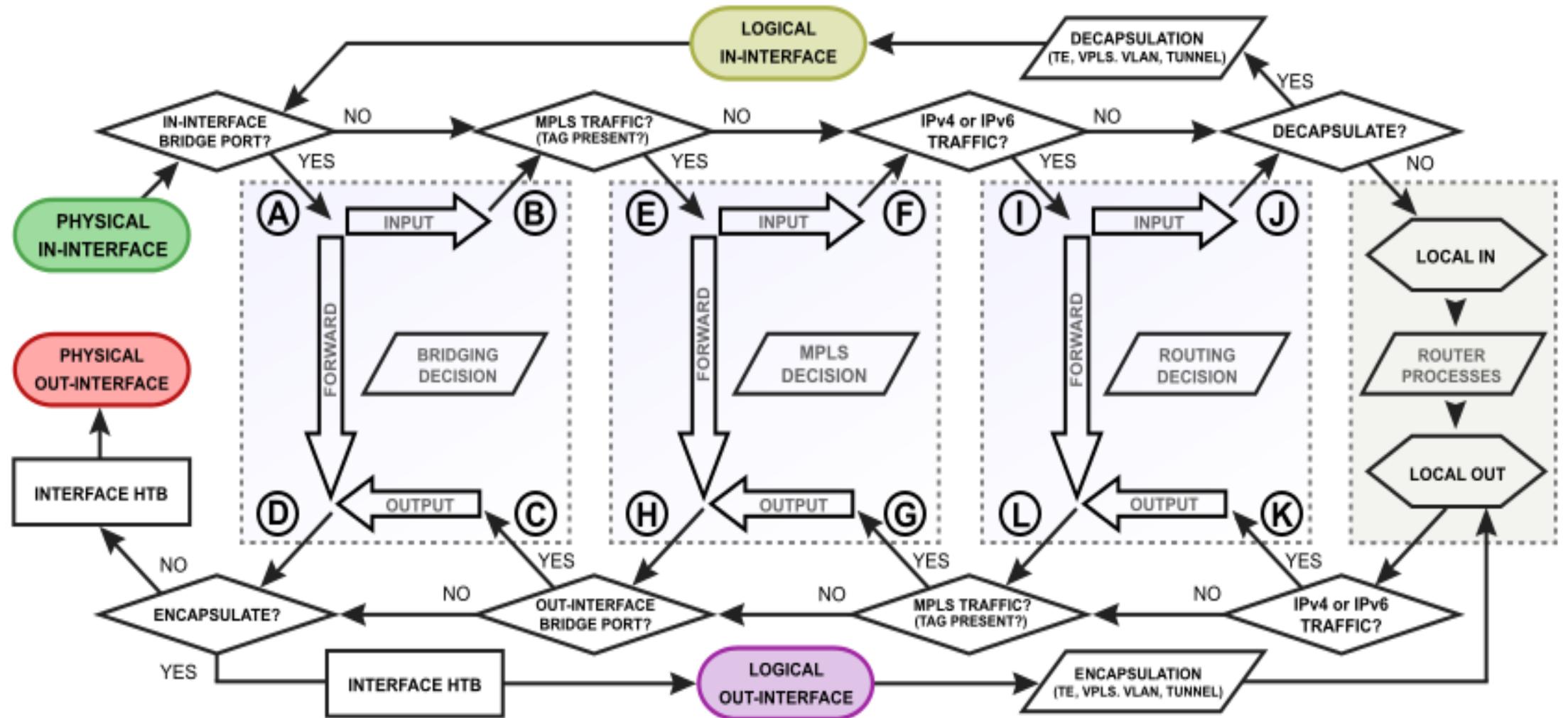
# Tools for Implementing BWM & QoS

- Packet Flow Diagram (ROS v.6)
- Mangle
- Address List
- Simple Queues
- Hierarchical Token Bucket, HTB
- Queue Tree
- Per Connection Queue, PCQ

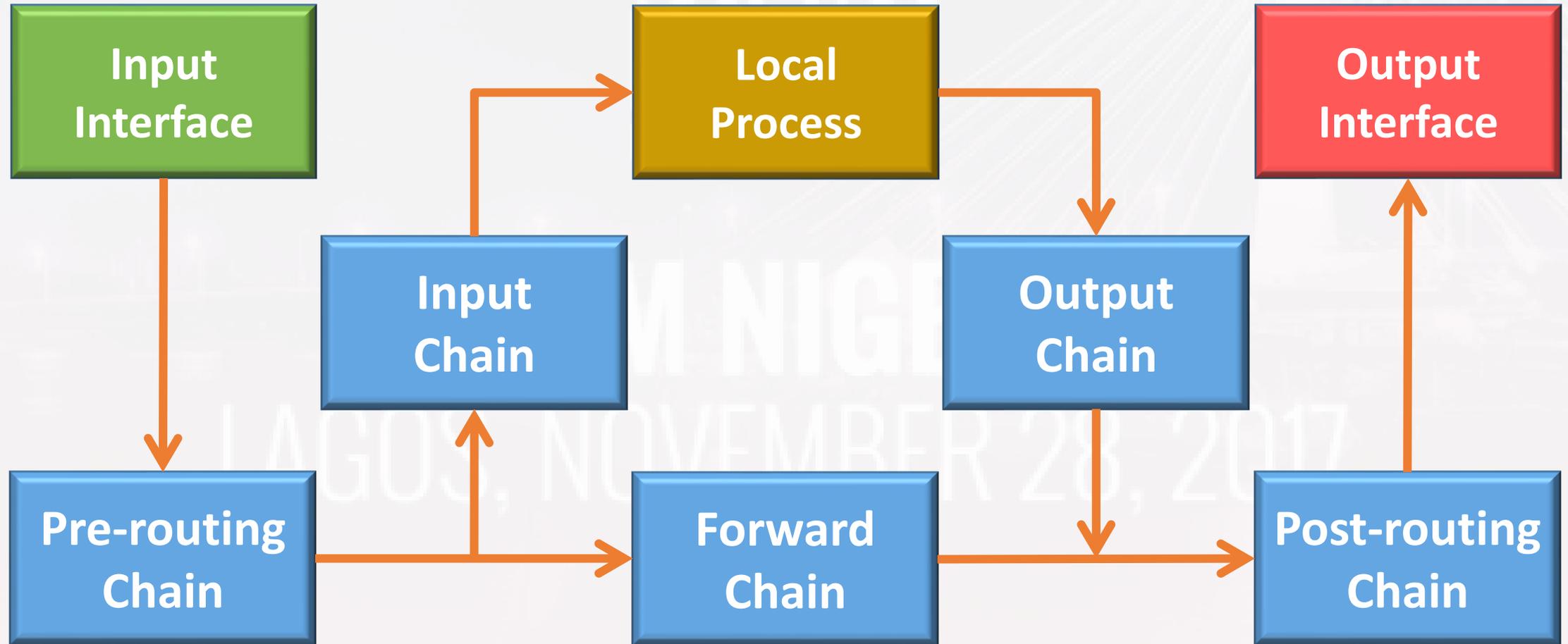
# Packet Flow Diagram (ROS v.6)

- Created to form a basis of understanding how packets flow through MikroTik router
- Used to determine where, when and what actions can be taken at any given point
- Knowledge helps to simplify complicated tasks within the RouterOS facilities

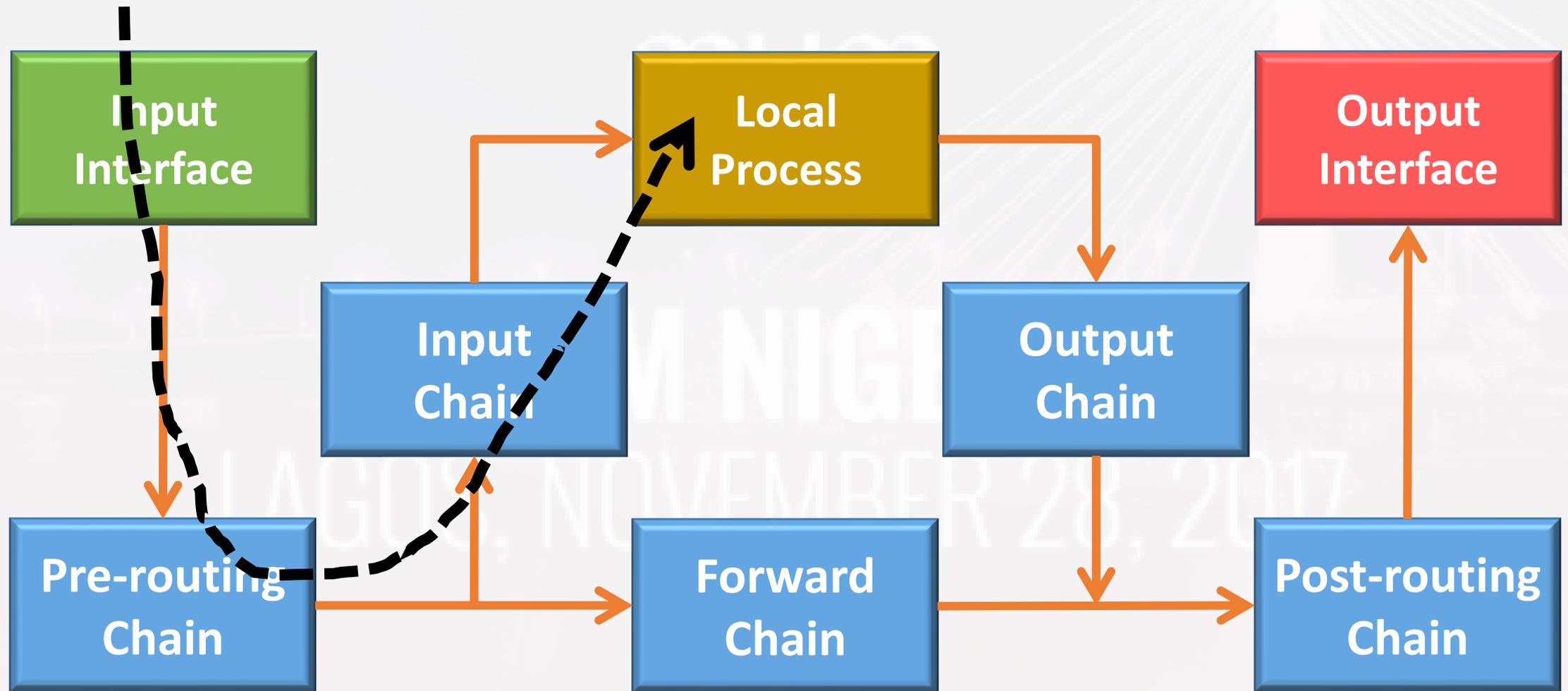
# Packet Flow Diagram (ROS v.6)



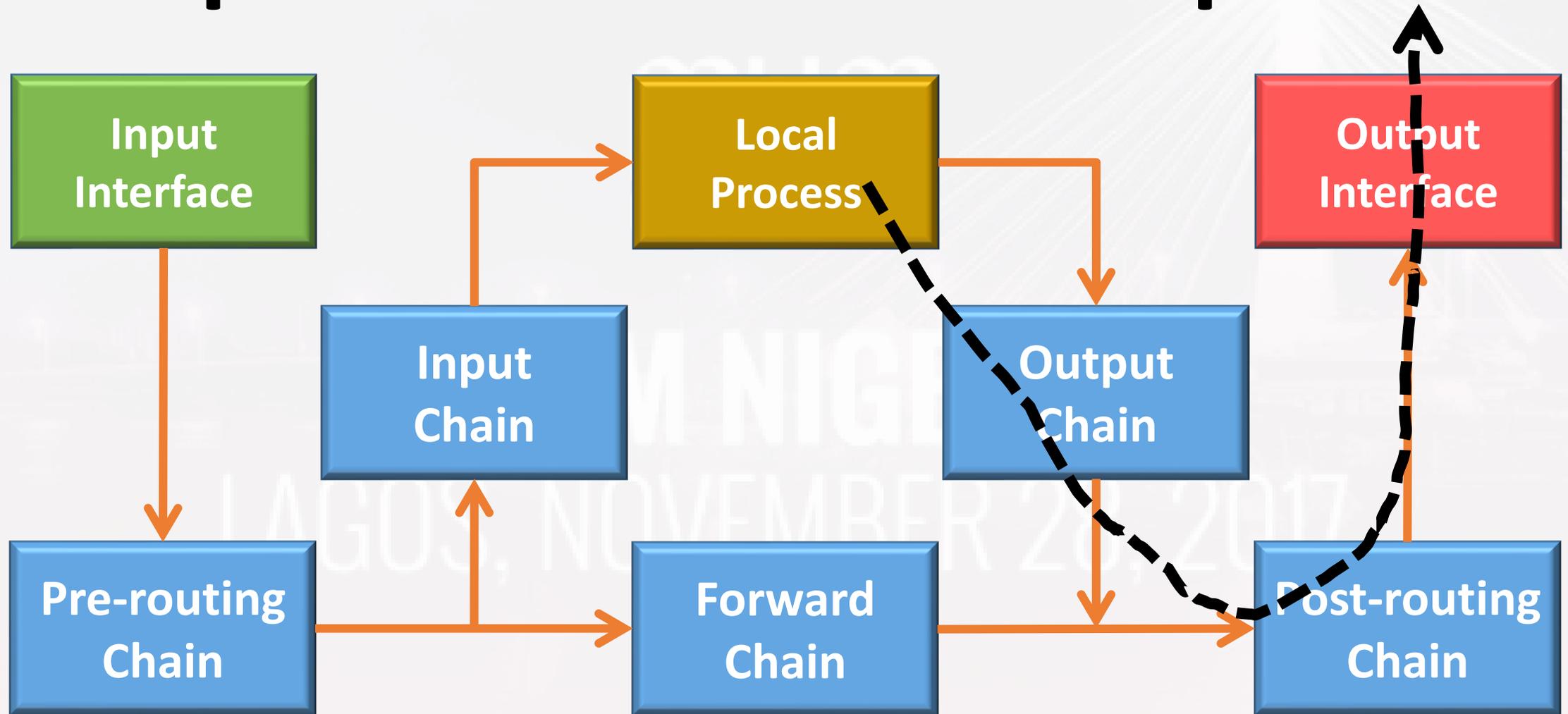
# Packet Flow Simplified Diagram



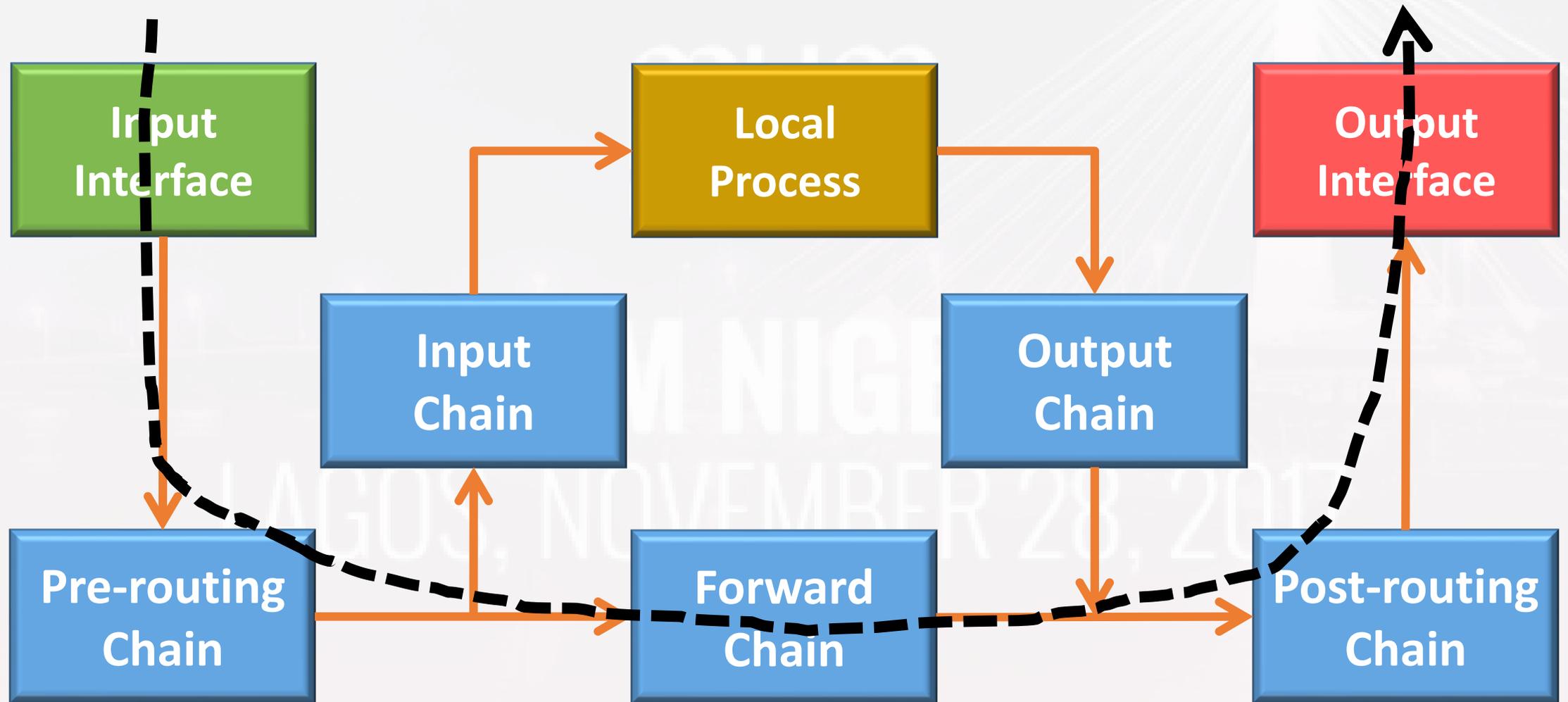
# Input Traffic in PFD Simplified



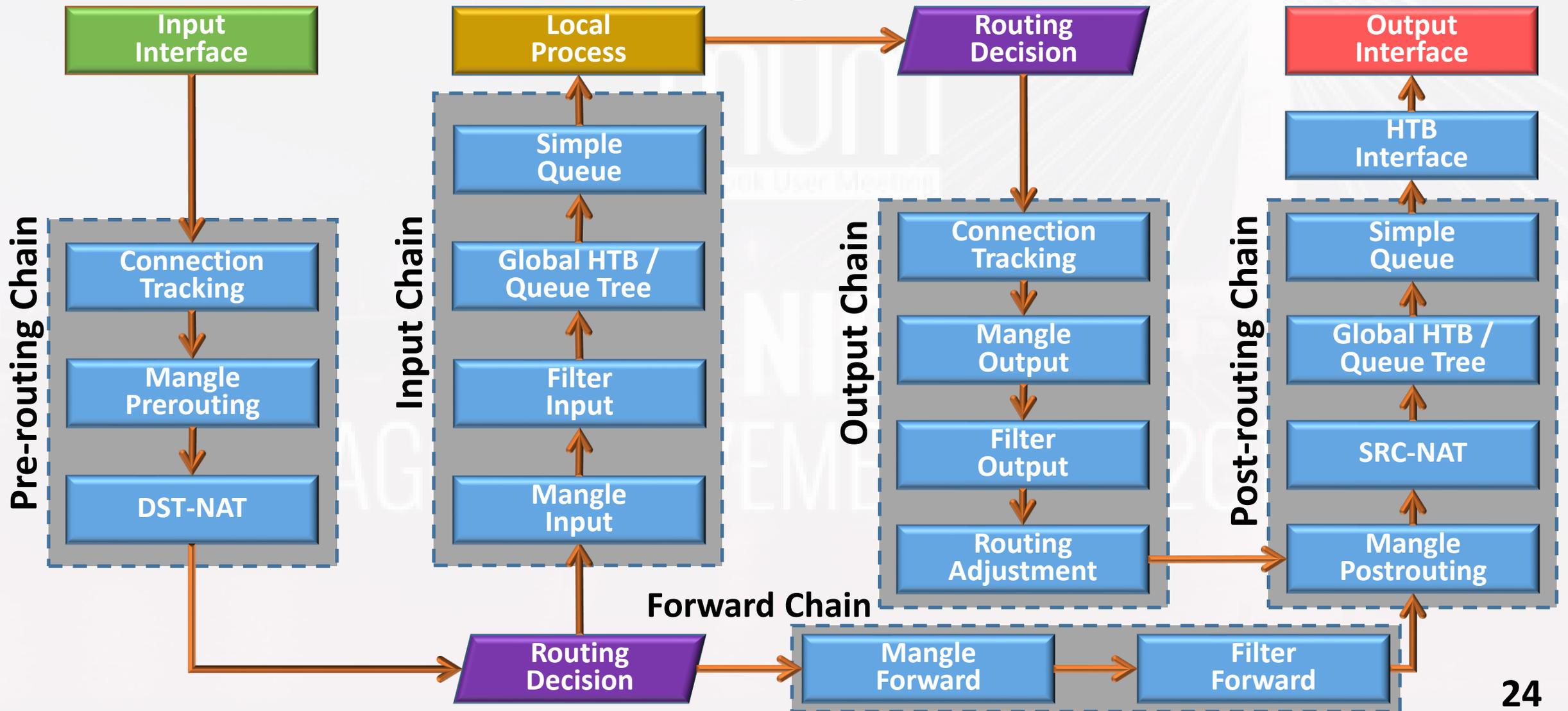
# Output Traffic in PFD Simplified



# Forward Traffic in PFD Simplified



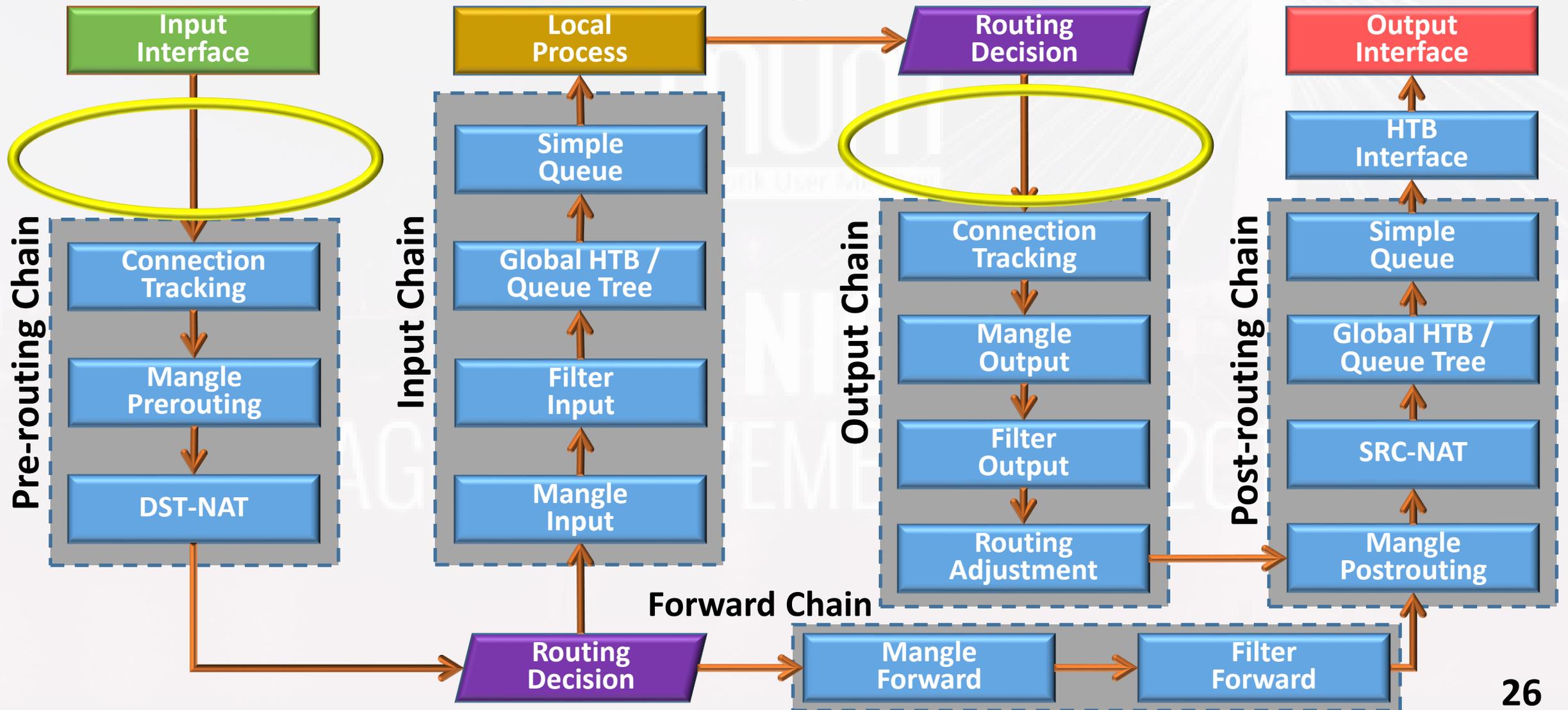
# Packet Flow Diagram (ROS v.6)



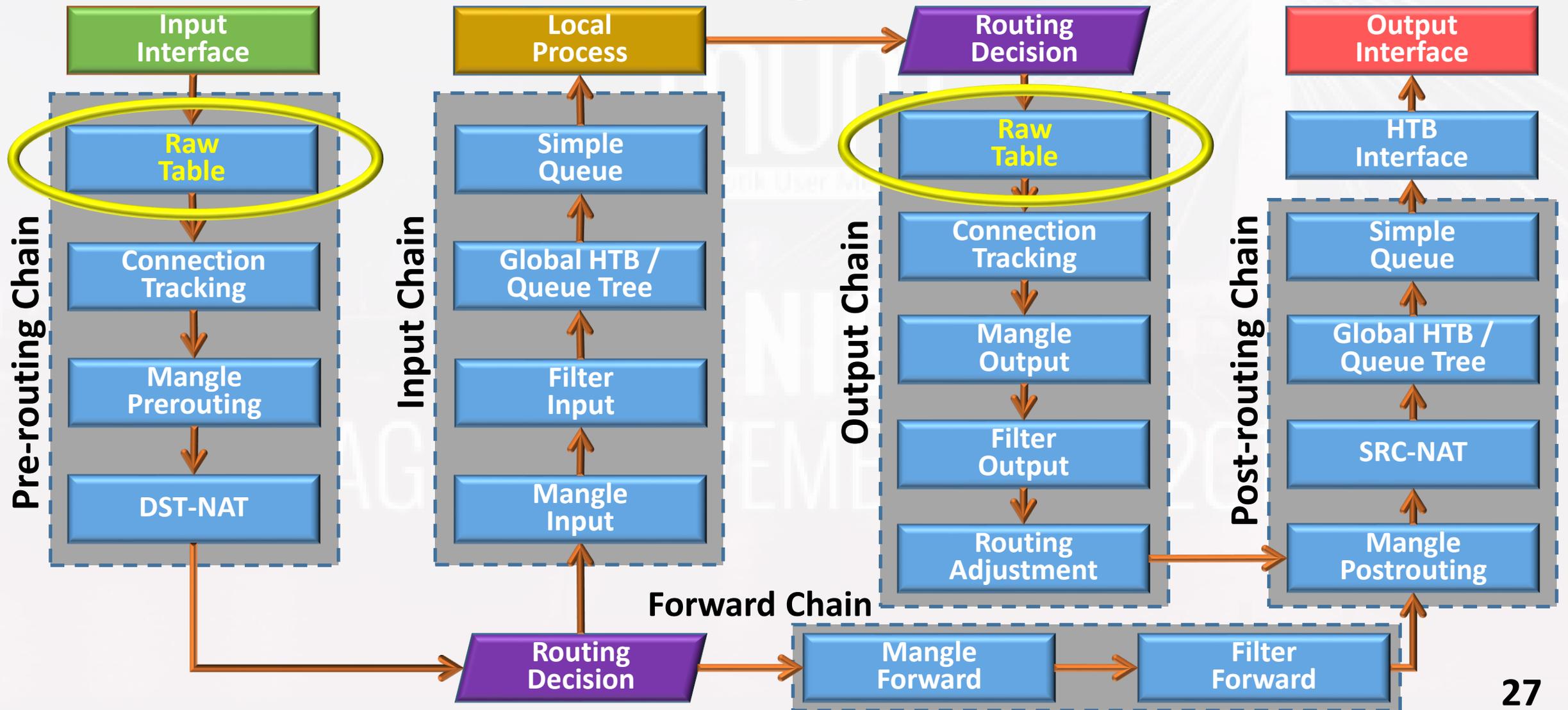
# Distributed Denial-of-Service (DDoS)

- A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system
- The incoming disruptive traffic comes from different IP addresses
- This effectively makes it impossible to stop the attack simply by using ingress filtering
  - Connection tracking, a CPU intensive process, already engaged

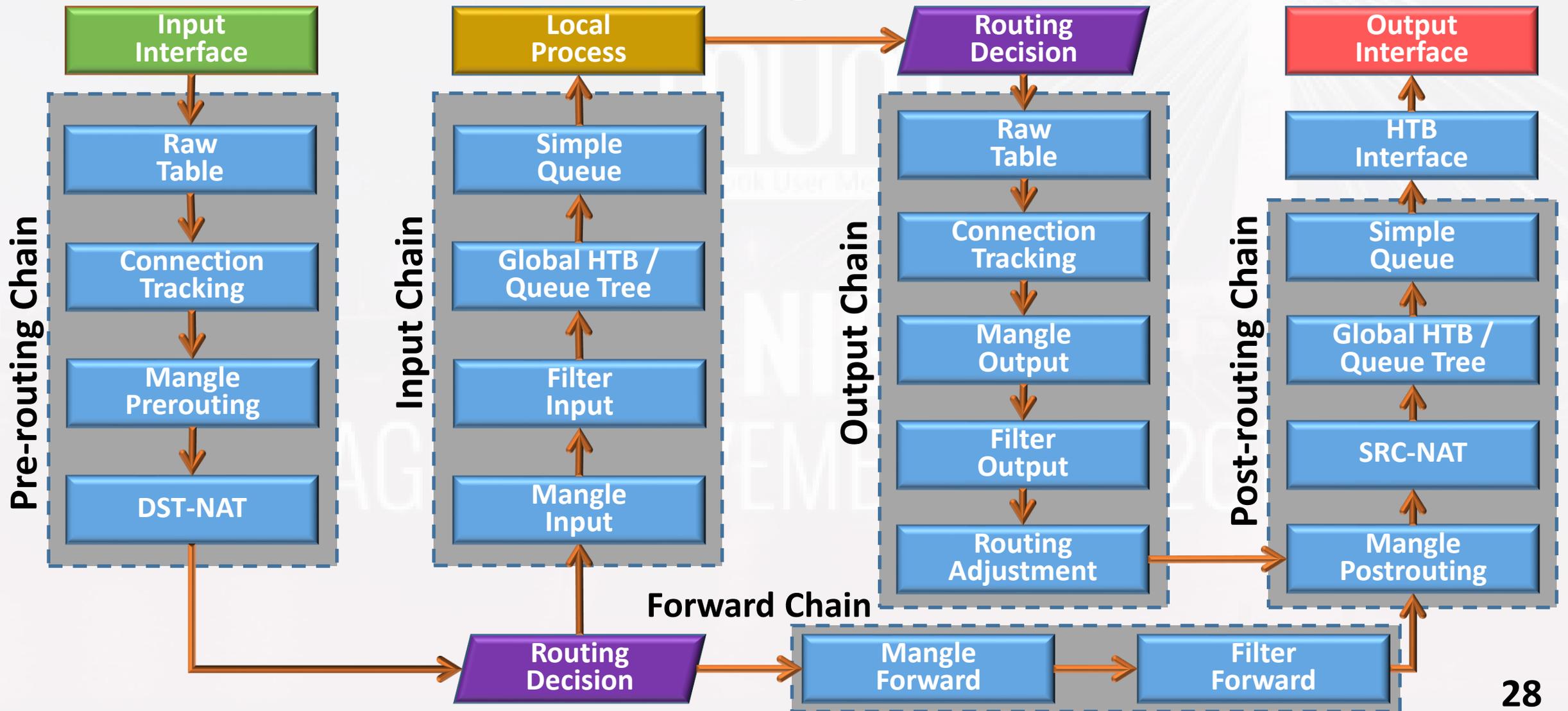
# Packet Flow Diagram (ROS v.6)



# Packet Flow Diagram (ROS v.6)



# Packet Flow Diagram (ROS v.6)



# Raw Table

- Very useful tool for DDOS attack mitigation
- Allows to selectively bypass or drop packets before connection tracking
  - Significantly reducing load on CPU
- Does not have matchers that depend on connection tracking (like connection-state, L-7, etc)
- If packet is marked to bypass connection tracking packet de-fragmentation will not occur

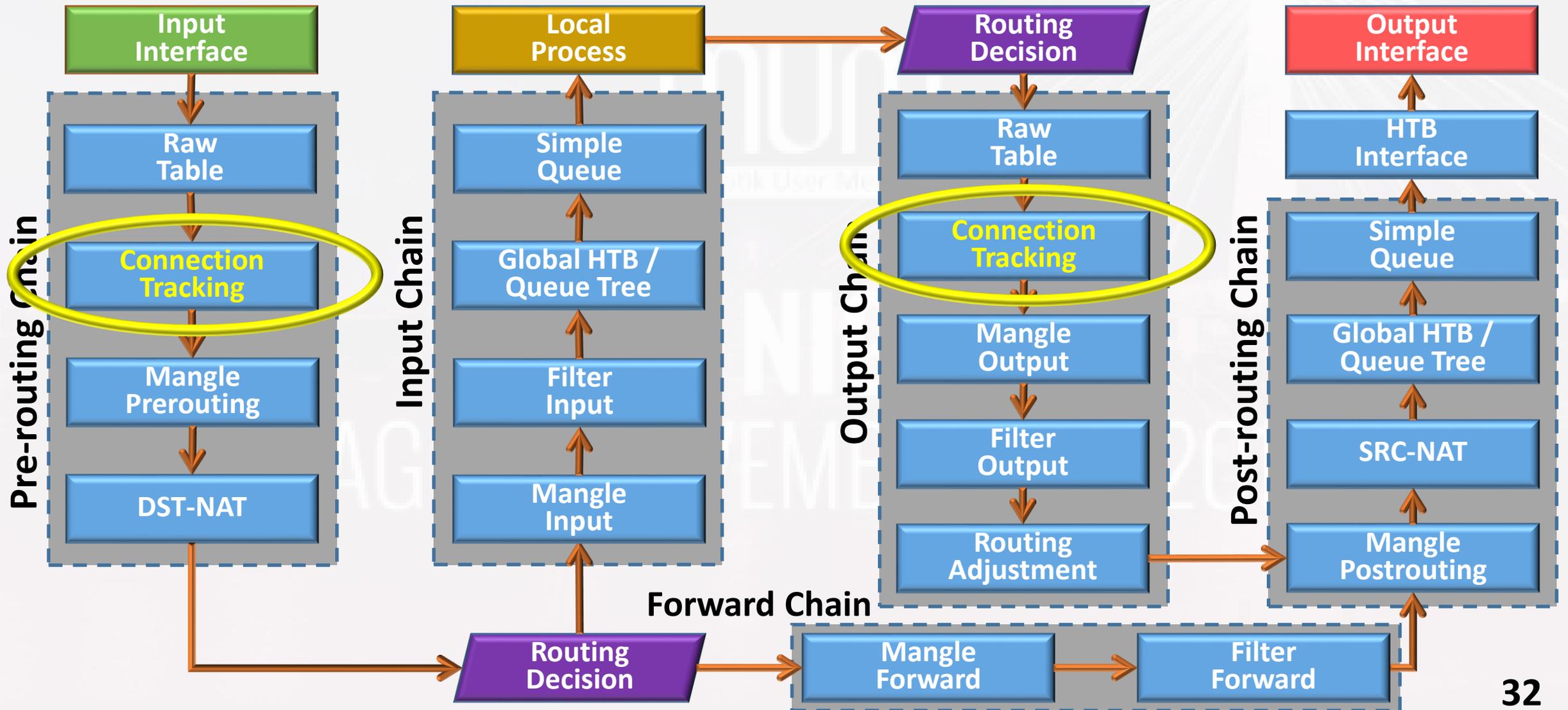
# IP → Firewall → Raw → +

The screenshot displays the Mikrotik WinBox interface. On the left sidebar, the 'IP' menu item is highlighted with a green box, and an arrow points to the 'Firewall' menu item, which is also highlighted with a green box. From the 'Firewall' menu, an arrow points to the 'Raw' tab in the main window. The 'Raw' tab is highlighted with a green box, and an arrow points to the '+' icon for creating a new rule. Below this, a 'New Raw Rule' dialog box is open, with its title bar highlighted in green. The 'Chain' dropdown menu is set to 'prerouting'. Other fields like 'Src. Address', 'Dst. Address', 'Protocol', 'Src. Port', and 'Dst. Port' are visible but empty. On the right side of the dialog, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.

# Connection Tracking

- A way to see what connections are making their way to, from & through the router
- Required for several Firewall facilities in the router to function
  - NAT, Mangle, Filter, etc will stop working if disabled
- Displays source & destination IP addresses and ports associated with a specific connection
- A CPU intensive feature

# Connection Tracking in PFD (ROS v.6)



# IP → Firewall → Connections

The screenshot shows the Mikrotik WinBox interface. On the left sidebar, the 'IP' menu item is highlighted with a green box, and a green arrow points to the 'Firewall' menu item, which is also highlighted with a green box. Another green arrow points from the 'Firewall' menu to the 'Connections' tab in the main window. The 'Connections' tab is also highlighted with a green box. The main window displays a table of active connections.

	Src. Address	Dst. Address	Proto...	Connection Mark	Timeout	TCP State
Cs	192.168.88.242:41115	52.9.49.21:443	6 (tcp)		00:40:22	established
SACFs	192.168.88.243:41155	52.9.49.21:443	6 (tcp)		01:13:37	established
SACFs	192.168.88.243:41209	52.9.49.21:443	6 (tcp)		02:19:23	established
SACFs	192.168.88.243:41211	52.9.49.21:443	6 (tcp)		02:20:23	established
SACFs	192.168.88.243:41229	52.9.49.21:443	6 (tcp)		02:33:29	established
SACFs	192.168.88.243:41276	52.9.49.21:443	6 (tcp)		03:51:08	established
SACFs	192.168.88.243:41278	52.9.49.21:443	6 (tcp)		03:51:58	established
SACFs	192.168.88.243:41315	52.9.49.21:443	6 (tcp)		04:39:04	established
SACFs	192.168.88.243:41327	52.9.49.21:443	6 (tcp)		05:08:39	established
SACFs	192.168.88.243:41478	52.9.49.21:443	6 (tcp)		08:44:21	established
SACFs	192.168.88.243:41550	52.9.49.21:443	6 (tcp)		09:16:16	established
SACFs	192.168.88.243:41680	52.9.49.21:443	6 (tcp)		10:40:07	established
SACFs	192.168.88.243:41685	52.9.49.21:443	6 (tcp)		10:49:16	established
SACFs	192.168.88.243:41851	52.9.49.21:443	6 (tcp)		11:05:57	established
SACFs	192.168.88.243:42107	52.9.49.21:443	6 (tcp)		15:56:39	established
SACFs	192.168.88.243:42204	52.9.49.21:443	6 (tcp)		17:20:16	established
SACFs	192.168.88.243:42285	52.9.49.21:443	6 (tcp)		19:16:51	established
SACFs	192.168.88.243:42329	52.9.49.21:443	6 (tcp)		19:33:53	established
SACFs	192.168.88.243:42330	52.9.49.21:443	6 (tcp)		19:33:54	established
SACFs	192.168.88.243:42564	52.9.49.21:443	6 (tcp)		23:58:45	established
SACFs	192.168.88.242:44831	52.9.68.198:443	6 (tcp)		10:49:29	established
SACFs	192.168.88.242:60611	52.9.68.198:443	6 (tcp)		00:04:05	established
SACFs	192.168.88.242:41312	52.9.87.70:80	6 (tcp)		17:00:41	established

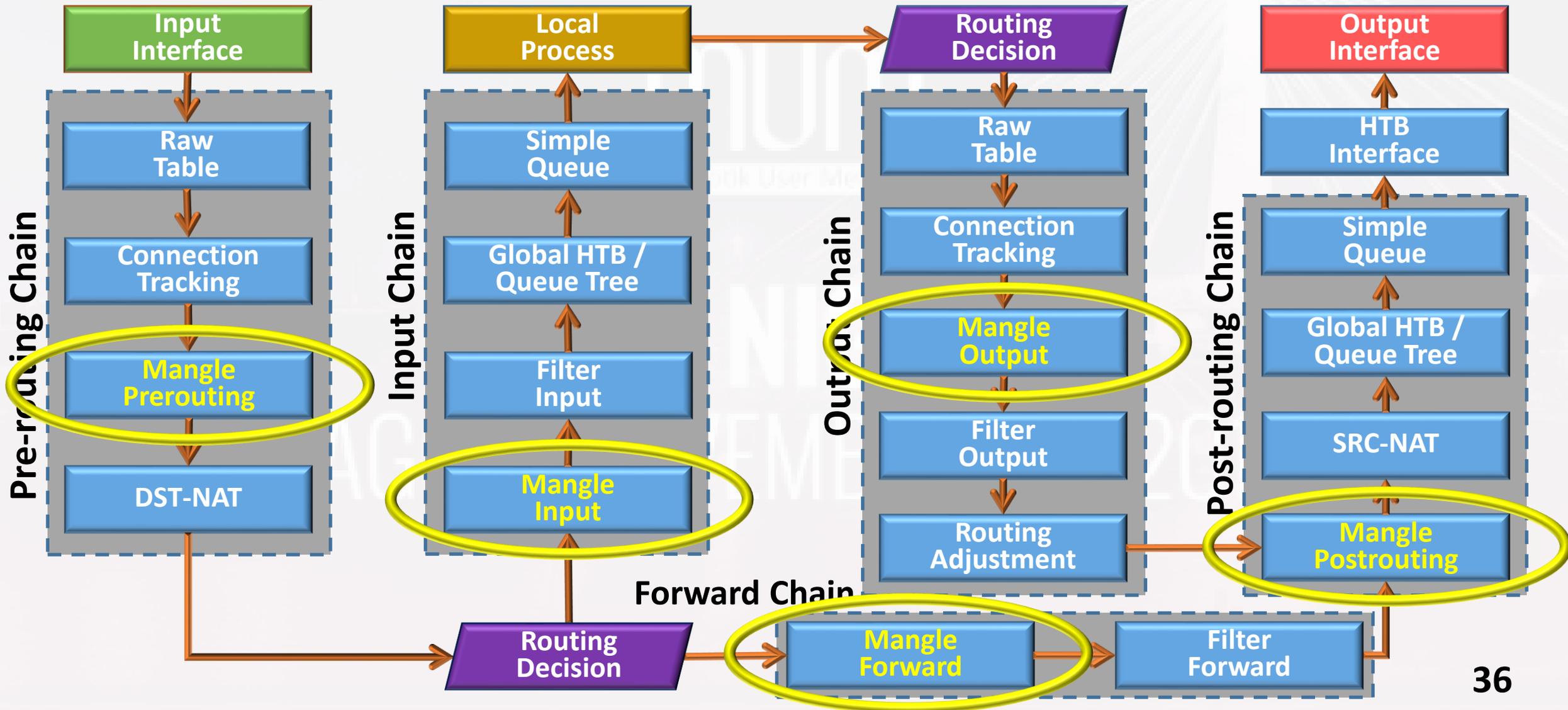
# Mangle

- Marks IP connections (bidirectional) and packets (unidirectional) with special marks
- These marks are used for future processing within the same router
  - Filter, Queue and Routing facilities use these marks
- Used to modify some fields in the IP header
  - DSCP (TOS), TTL and MSS fields can be changed

# Mangle

- Mangle rules are organised in 5 default chains
  - Prerouting
  - Input
  - Forward
  - Output
  - Postrouting
- Custom user-defined chains can be added

# Mangle Chains in PFD (ROS v.6)



# IP → Firewall → Mangle → +

The screenshot shows the Mikrotik WinBox interface. On the left sidebar, the 'IP' menu item is highlighted with a green box. A green arrow points from 'IP' to the 'Firewall' menu item, which is also highlighted with a green box. Another green arrow points from 'Firewall' to the 'Mangle' tab in the main window, which is also highlighted with a green box. A third green arrow points from the '+' icon in the Firewall window to the 'New Mangle Rule' dialog box.

The Firewall window shows a table of rules:

#	Action	Chain	Proto...	Src. Port	Dst. Port	Bytes	Packets
0	jump	prerouting	6 (tcp)			1000.2 KB	13 902
1	jump	prerouting	17 (u...)			8.8 MiB	61 133
2	jump	prerouting				327.1 KB	8 085
3	mar...	tcp-services	6 (tcp)	1024-65535	20-21	0 B	0
4	mar...	tcp-services	6 (tcp)	513-65535	22	0 B	0
5	mar...	tcp-services	6 (tcp)	1024-65535	23	0 B	0

The 'New Mangle Rule' dialog box is open, showing the following fields:

- Chain: prerouting
- Src. Address: [empty]
- Dst. Address: [empty]
- Protocol: [empty]

Buttons: OK, Cancel, Apply, Disable, Comment.

# Address List

- Allows to create action for multiple IPs at once
- Possible to automatically add an IP address to the address list
- IP address can be added to the address list permanently or for a defined timeout period
- Address list can contain one IP address, an IP range or a whole subnet

# IP → Firewall → Address Lists → +

The screenshot shows the Mikrotik WinBox interface. On the left, the 'IP' menu item is highlighted with a green box, and an arrow points to the 'Firewall' menu item, which is also highlighted with a green box. A second arrow points from the 'Firewall' menu to the 'Address Lists' tab in the main window, which is also highlighted with a green box. A third arrow points from the 'Address Lists' tab to the 'New Firewall Address List' dialog box, which is open in the foreground. The dialog box has a title bar 'New Firewall Address List' and contains the following fields:

- Name:
- Address:
- Timeout:

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

Name	Address	Timeout
My src-nated local network hosts		
nat-addr	172.168.153.0/24	
Mobile phones		
mobile	172.168.153.2-172.16...	
My local network		
local-addr	172.168.153.0/24	
illegal-addr	10.0.0.0/8	
Could be my local address block; need to check		
illegal-addr	172.16.0.0/12	
illegal-addr	192.168.0.0/16	

# Queues

- Limit data rate for IP addresses, subnets, protocols, ports, interfaces and other parameters
- Prioritize some packet flows over others
- Configure traffic bursts for faster web browsing
- Share available traffic among users equally, depending on the load
- Limit peer-to-peer traffic

# Queue Properties

- **limit-at:** Normal data rate that is guaranteed to a target
- **max-limit:** Maximal data rate that is allowed for a target to reach, if available
- **burst-threshold:** Basically, this is burst on/off switch
- **burst-limit:** Maximal data rate which can be reached while the burst is active
- **burst-time:** Period of time over which the average data rate is calculated (not the time of actual burst)

# Queue Properties

- **parent:** Top queue in the HTB that assigns bandwidth to the child queues below
- **priority:** Responsible for distribution of remaining parent queue's traffic to child queues so that they are able to reach max-limit
- **packet marks:** Use marked packets from Firewall → Mangle
- **queue type:** Choose queue type created Queue → Type
- **bucket size:** A function of token bucket & max-limit

# Simple Queues

- The simplest way to limit data rate for specific IP addresses, interfaces and/or subnets
  - Limit client's download (↓) speed, upload (↑) speed and total speed (↓ + ↑) independently
- All rules are processed sequentially from top

# Simple Queues (ROS v.6)

- Not only for “simple” tasks anymore
- Traffic identified based on src-address, interface, dst-address, etc, hence no need to mark packets
- Fast hash algorithm, especially on multicore hardware
  - Number of simple queues no more relevant
  - Can have thousands of them without heavily loading CPU
- Can be easily created dynamically or by scripting

# Simple Queues Caution

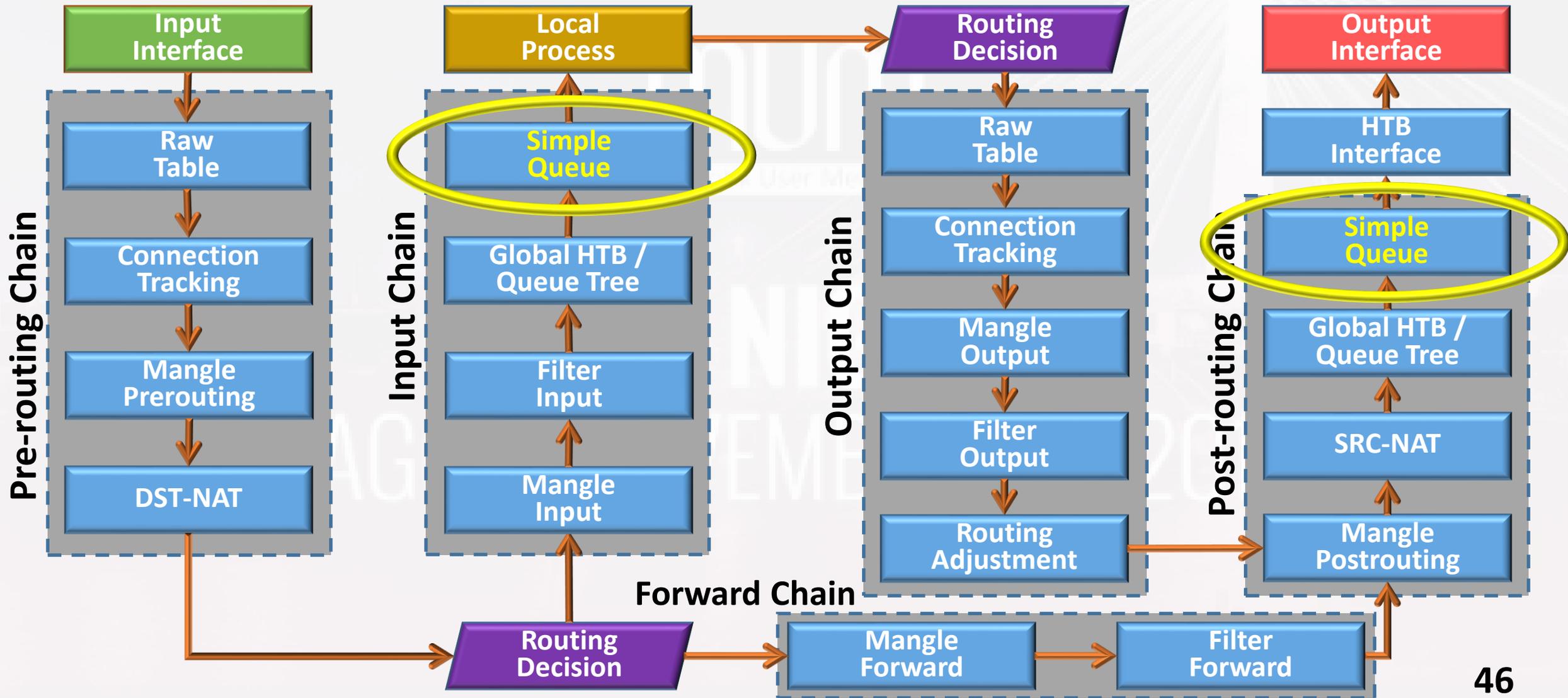


- FastTrack rule in Firewall → Filter needs to be disabled for Simple Queues to work

MUM NIGERIA

LAGOS, NOVEMBER 28, 2017

# Simple Queue in PFD (ROS v.6)



# Queues → Simple Queues → +

Winbox

The screenshot displays the RouterOS WinBox interface. On the left is a vertical sidebar with various configuration categories. The 'Queues' category is highlighted with a green box, and a green arrow points from it to the 'Simple Queues' tab in the main window. The 'Simple Queues' tab is also highlighted with a green box. Below the sidebar, a 'New Simple Queue' dialog box is open, with its title bar highlighted in green. The dialog has several tabs: 'General', 'Advanced', 'Statistics', 'Traffic', 'Total', and 'Total Statistics'. The 'General' tab is active, showing fields for 'Name' (set to 'queue1'), 'Target' (set to '0.0.0.0/0'), and 'Dst.'. Below these are sections for 'Target Upload' and 'Target Download' with 'Max Limit' and 'Burst' settings, all currently set to 'unlimited'. At the bottom, there are 'Burst Threshold' and 'Burst Time' settings. On the right side of the dialog are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', 'Reset All Counters', and 'Torch'. The main window shows a table of Simple Queues with one entry:

#	Name	Target	Upload Max Limit	Download Max Limit
0	dhcp<00:27:10:43:92:8C/...	172.168.153.5	5M	5M

# Hierarchical Token Bucket (HTB)

- Classful queuing method that is useful for handling different kinds of traffic
- Allows to create a hierarchical queue structure
- Determines relations between queues
  - Like "parent-child" or "child-child"
  - Priority, burst possibility, etc

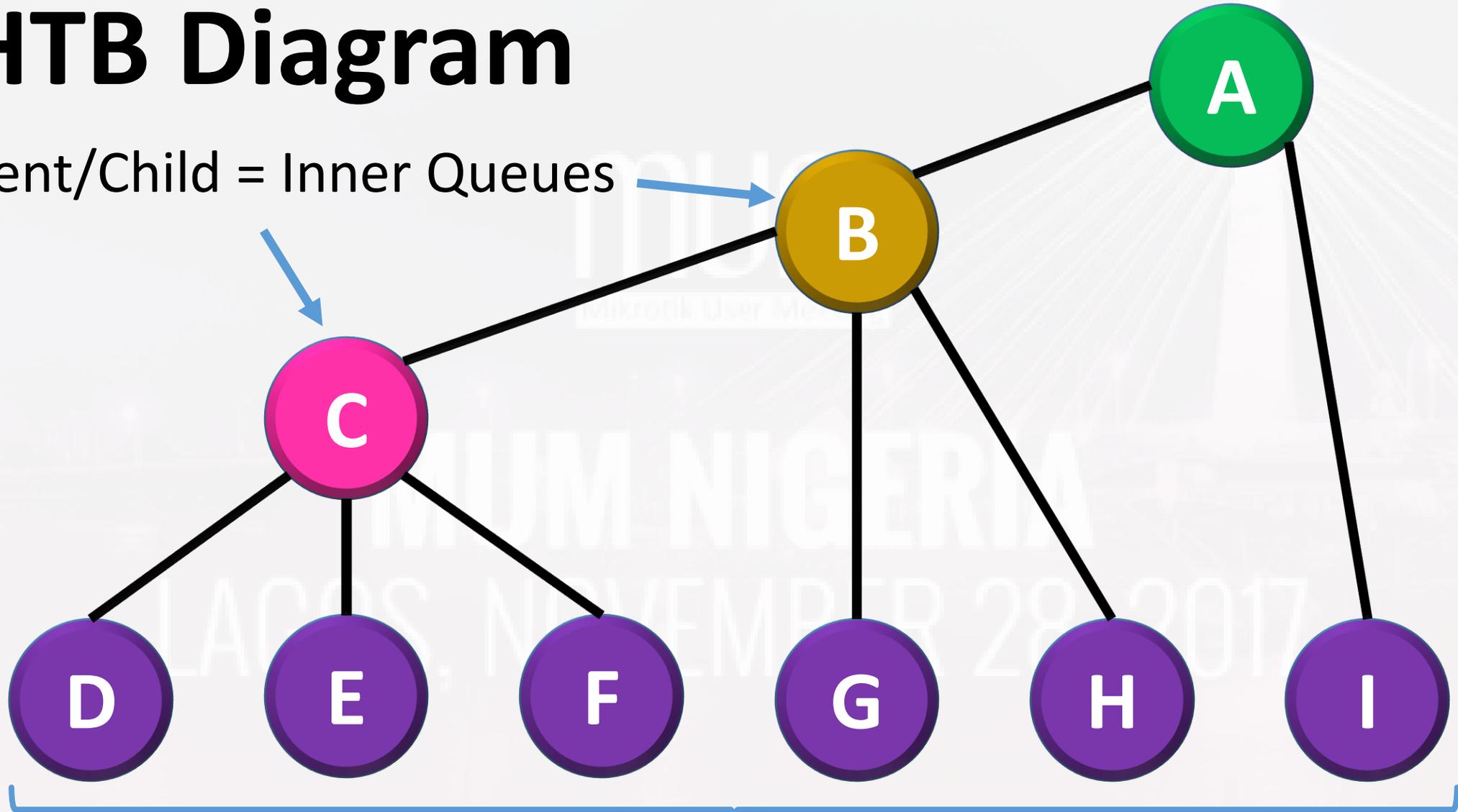
# HTB in RouterOS

- Bandwidth management implementation in RouterOS is mostly based on HTB
- Three basic steps required to create HTB:
  - Match and mark traffic
  - Create rules/policies to mark traffic
  - Attach policy for specific interface(s)

# HTB Diagram

Parent/Child = Inner Queues

Top Parent Queue

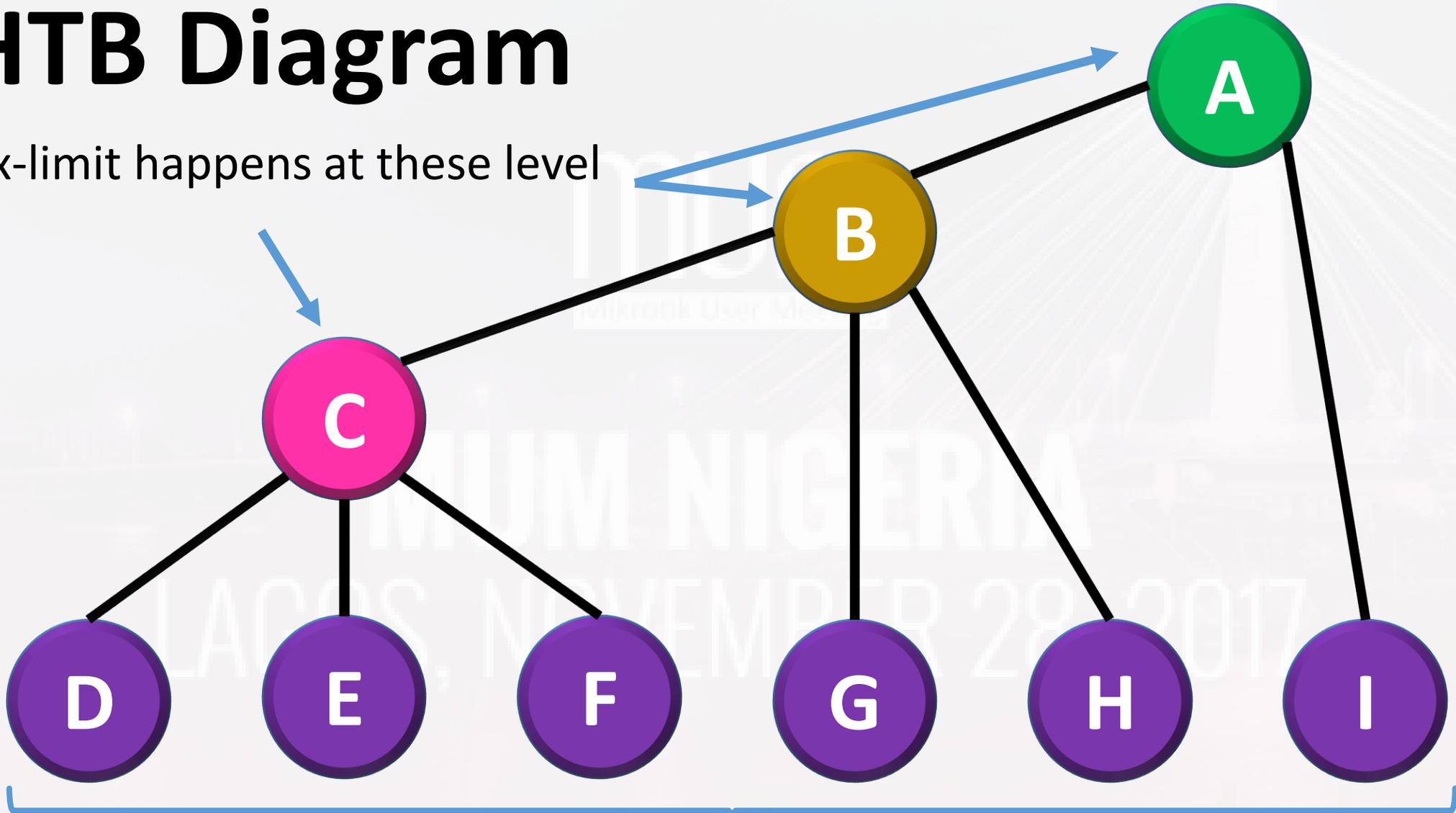


Child = Leaf Queues

# HTB Diagram

Max-limit happens at these level

Top Parent Queue



Limit-at and priority happen at this level

# Queues → Queue Tree → +

The screenshot shows the Mikrotik WinBox interface. On the left sidebar, the 'Queues' menu item is highlighted with a green box. The main window displays the 'Queue List' configuration page, where the 'Queue Tree' tab is selected and highlighted with a green box. A green arrow points from the 'Queue Tree' tab to the 'Queue Tree' icon in the toolbar. The table below shows a hierarchical queue structure:

Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate	Queued Bytes	By
A	global				0 bps	0 B	
B	A				0 bps	0 B	
C	B				0 bps	0 B	
D	C				0 bps	0 B	
E	C				0 bps	0 B	
F	C				0 bps	0 B	
G	B				0 bps	0 B	
H	B				0 bps	0 B	
I	A				0 bps	0 B	

# HTB Configuration Caution



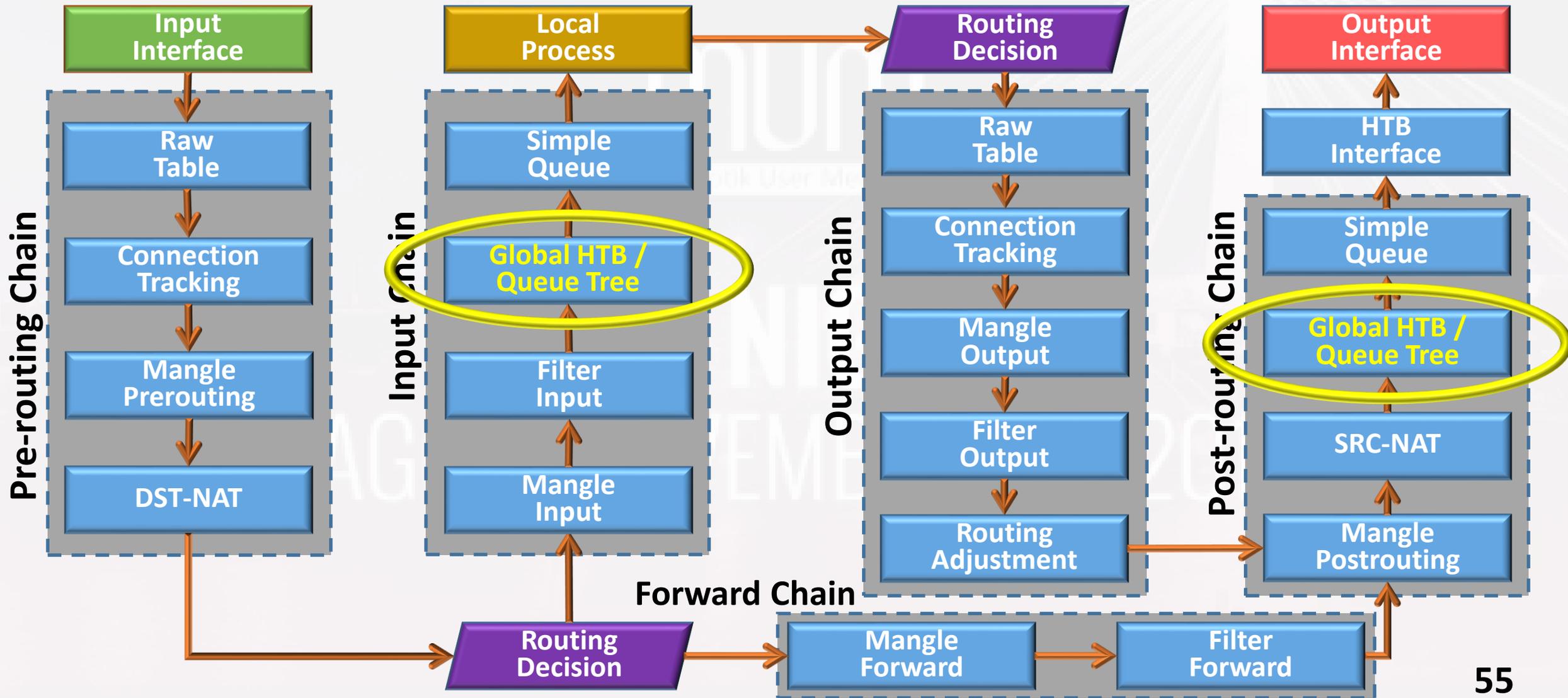
- Limit-at and priority will not work if there is no parent in the hierarchy
- Limit-at and priority happen at the leaf queues

MUM  
MUM NIGERIA  
LAGOS, NOVEMBER 28, 2017

# Queue Trees

- Unidirectional queue in one of the HTBs
- Requires 2 rules per full duplex traffic control
- All rules are processed simultaneously
  - Highly efficient on CPU load
- Parent, priority & packet mark are very important for efficient operation

# Queue Tree in PFD (ROS v.6)



# Queues → Queue Tree → +

The screenshot shows the Mikrotik WinBox interface. On the left sidebar, the 'Queues' menu item is highlighted with a green box. In the main window, the 'Queue List' tab is active, and the 'Queue Tree' sub-tab is selected, also highlighted with a green box. A green arrow points from the 'Queue Tree' sub-tab to the 'New Queue' dialog box. The 'New Queue' dialog is open, showing the 'General' tab with the following fields:

- Name: queue1
- Parent: global
- Packet Marks: (empty)
- Queue Type: default-small
- Priority: 8
- Bucket Size: 0.100
- Limit At: (empty) bits/s
- Max Limit: (empty) bits/s

The 'Queue List' table in the background shows the following data:

Name	Parent	Packet M...	Priority	Limit At ...	Max Limit ...	Avg. Rate	Queued Bytes	Bytes	Packets
total-download-traffic	global		8		20M	80 bps	0 B	14.3 MiB	17 615
download	total-downloa...	download	8	10M	15M	80 bps	0 B	2019.6 ...	1 749 3...
heavyu-download	total-downloa...	traff-heavyu	8	5M	10M	0 bps	0 B	0 B	0
other-download-tr...	total-downloa...	other-fwd-...	8	5M	5M	0 bps	0 B	0 B	0
					20M	160 bps	0 B	2212.0 ...	2 931 3...
					10M	0 bps	0 B	0 B	0
					5M	0 bps	0 B	0 B	0
					15M	160 bps	0 B	206.7 ...	1 199 6...

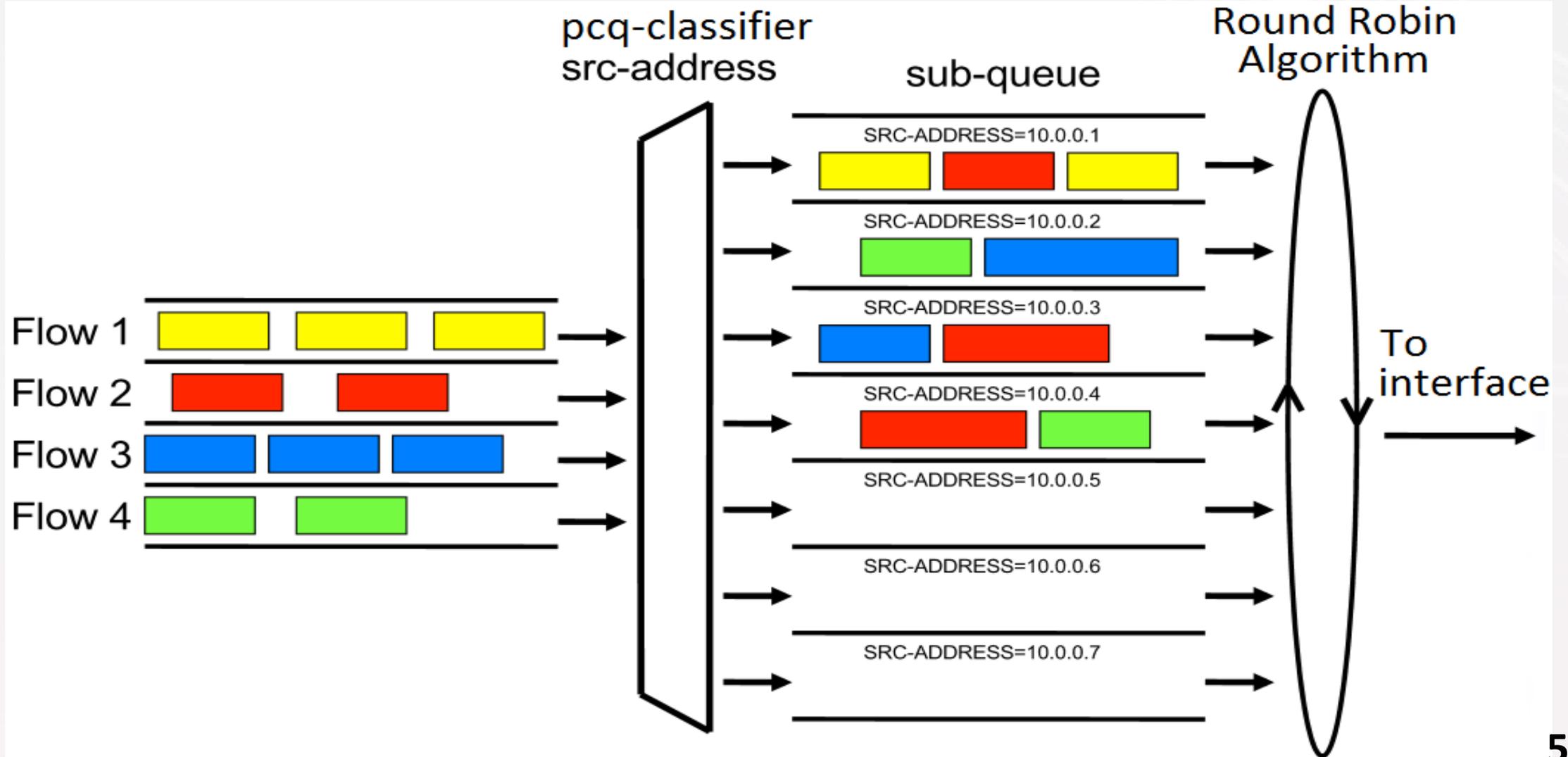
At the bottom of the 'Queue List' window, there is a table showing the status of queues:

Queue Name	Packets queued
traff-filedownload	386.
traff-heavyu	386.
other-fwd-traff	17.

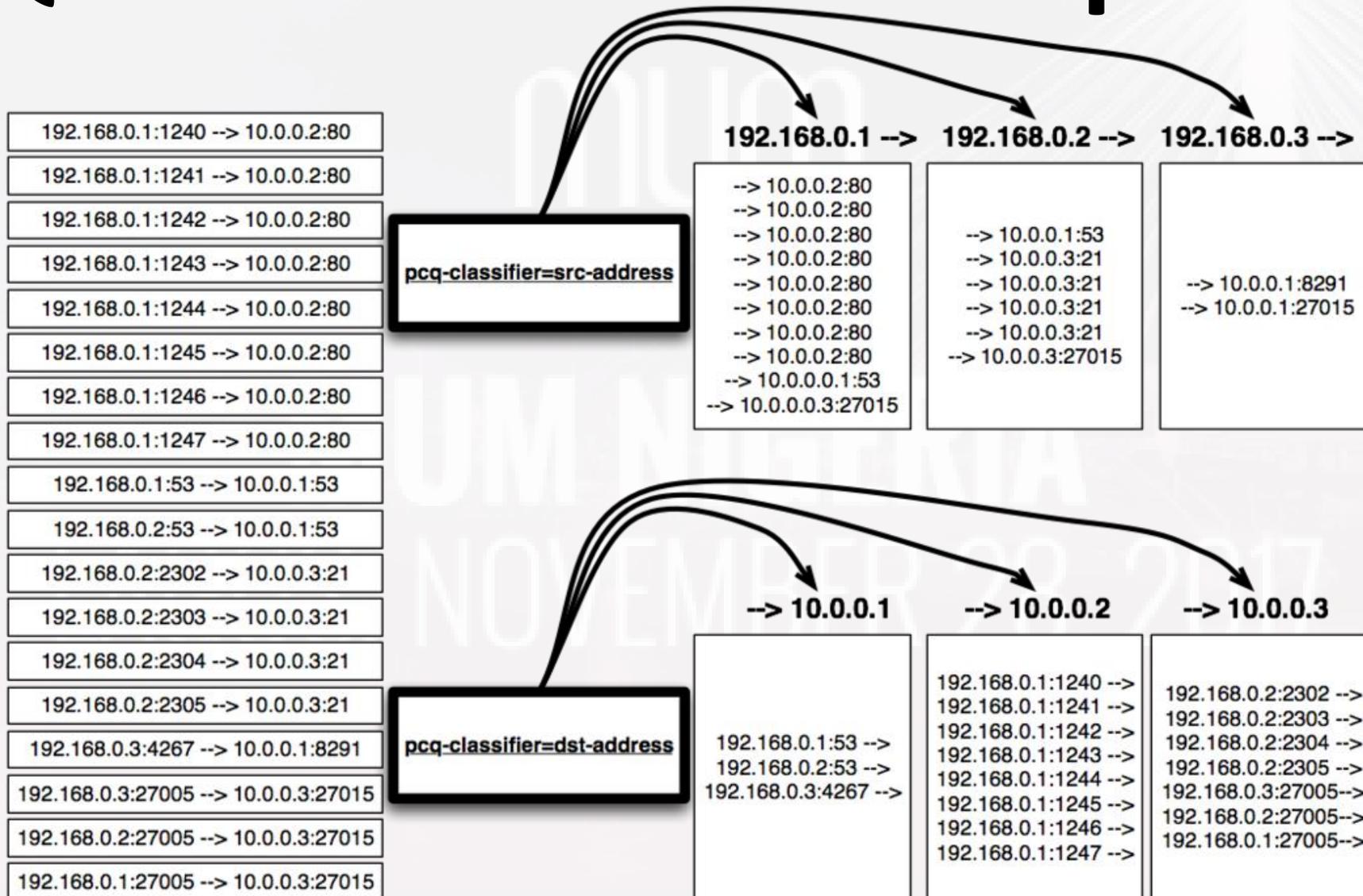
# Per Connection Queue (PCQ)

- Queue type for optimizing large QoS deployments by limiting per 'sub-stream'
- Substitute multiple queues with one
- Using flow identifiers to differentiate traffic
- Several classifiers can be used:
  - Source/destination IP address
  - Source/destination port

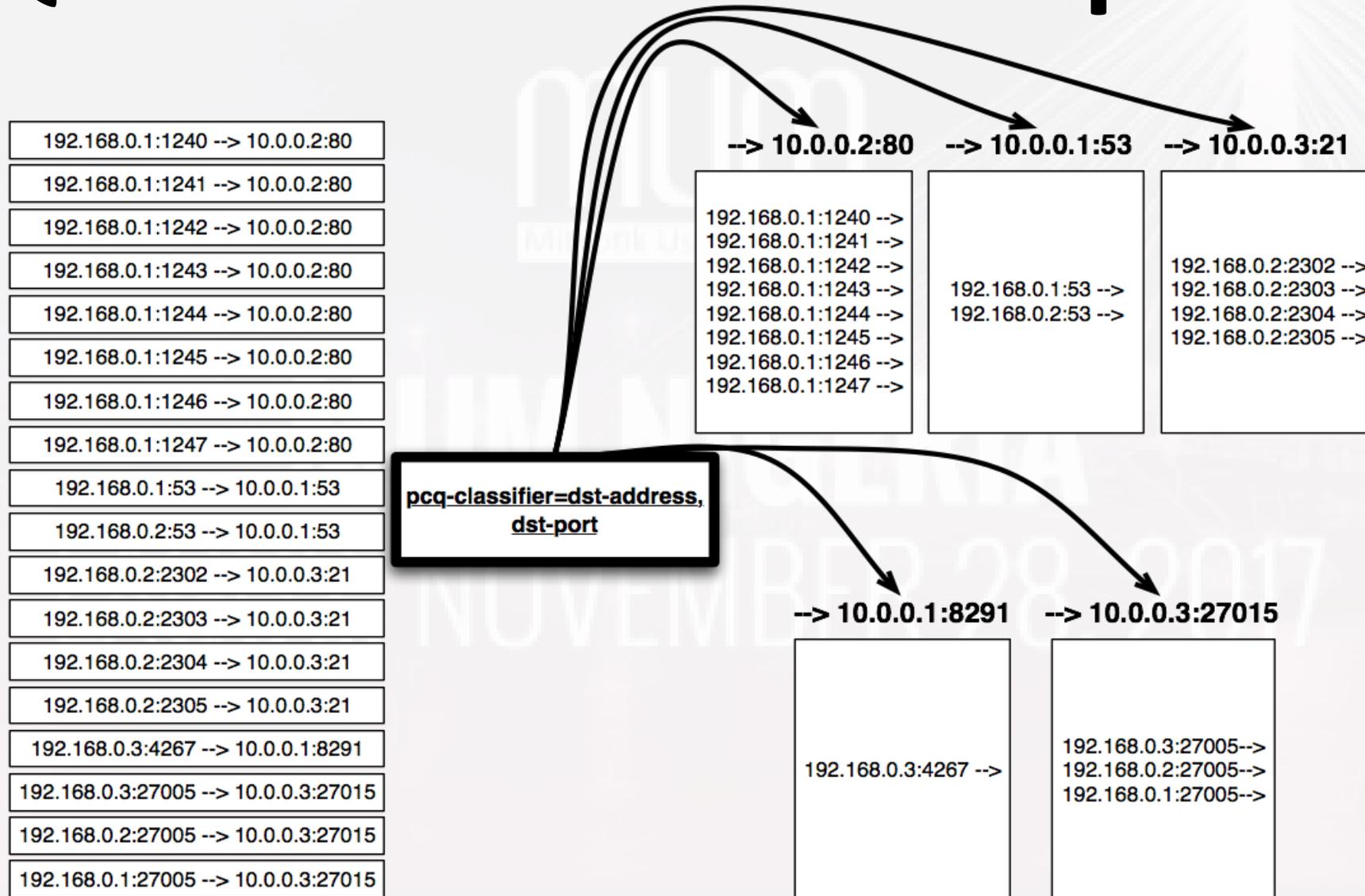
# PCQ Flow



# PCQ Classification Example

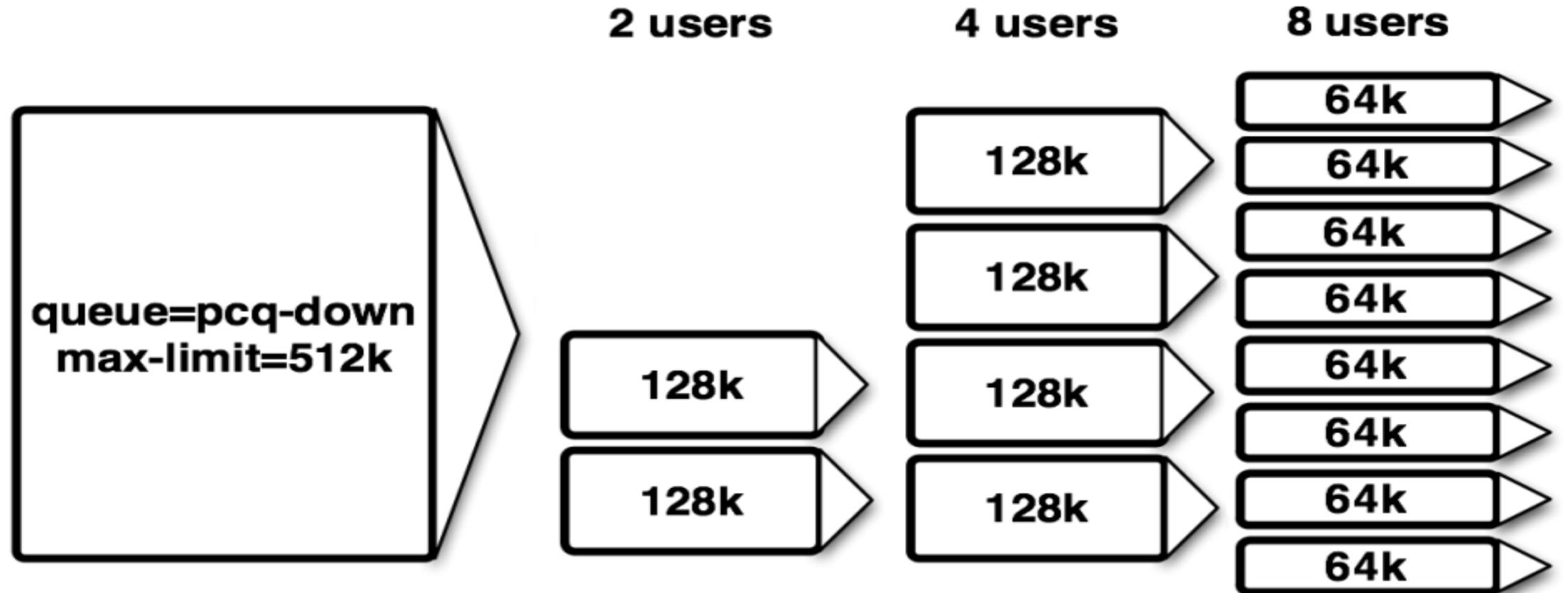


# PCQ Classification Example



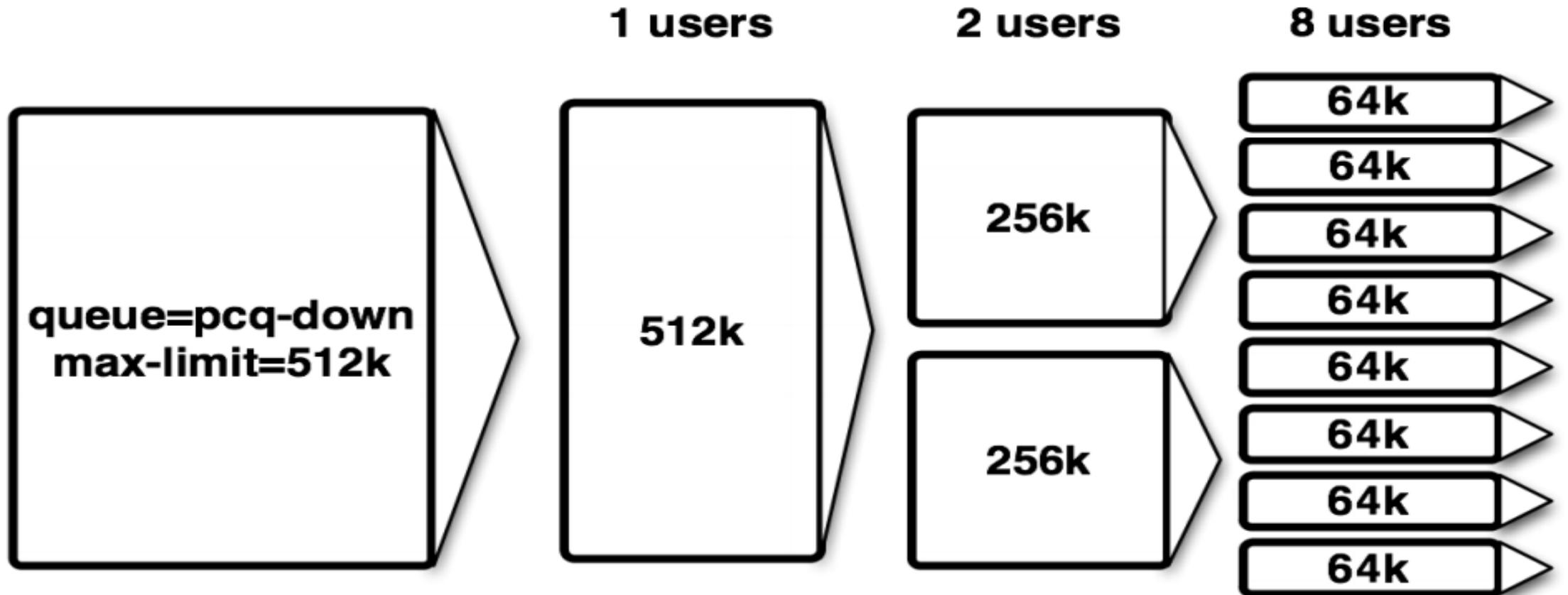
# PCQ in Action

**pcq-rate=128000**



# PCQ in Action

**pcq-rate=0**



# Queues → Queue Types → +

The screenshot displays the RouterOS WinBox interface. On the left is a vertical menu with 'Queues' highlighted. The main window shows the 'Queue List' tab with a table of existing queue types. A 'New Queue Type' dialog is open, showing configuration for 'queue1-upload'. A second 'New Queue Type' dialog is also open, showing configuration for 'queue2-download'. Green arrows indicate the workflow from the 'Queues' menu to the 'Queue Types' tab, then to the 'New Queue Type' dialog, and finally to the configuration fields.

Type Name	Kind
wireless-default	sfq
synchronous-default	rr
pcq-upload-default	pcq
pcq-download-default	pcq

**Queue 1 Configuration:**  
Type Name: queue1-upload  
Kind: pcq  
Rate: 0  
Limit: 50  
Total Limit: 2000  
Burst Rate: [ ]  
Burst Threshold: [ ]  
Burst Time: 00:00  
Classifier:  Src  Src

**Queue 2 Configuration:**  
Type Name: queue2-download  
Kind: pcq  
Rate: 0 bits/s  
Limit: 50 KB  
Total Limit: 2000 KB  
Burst Rate: [ ] bits/s  
Burst Threshold: [ ]  
Burst Time: 00:00:10

# PCQ Configuration Caution



- PCQ takes its data from Connection Tracking
  - Connection Tracking must be enabled
- If both limits (pcq-rate and max-limit) are unspecified, queue behavior can be imprecise
- So it is strongly suggested to have at least one of these options set

# Simple Queues & Queue Tree Combo

- A major aspect of QoS is traffic prioritization
- A major aspect of Bandwidth Management is client limitation
- Prioritization can be done on Forward Mangle & Queue Tree
- Limitation can be done with Simple Queue by targeting IP address

# Implementation Summary

- We used Mangle, Address List, Simple Queues and Queue Tree:
  - Mark packets by traffic type in Mangle Chain
  - Classify clients by IP address in Address List
  - Prioritize and limit traffic by type in Global HTB
  - Limit traffic per client in Simple Queue
  - Utilize PCQ to ensure a good Quality of Experience

# Conclusion

- MikroTik RouterOS is one of the most advanced (and easy to configure) OS for bandwidth management and QoS
- Understanding the packet flow diagram is required to set the ball rolling
- A knowledgeable combination of the right tools (mangle, simple queue, queue tree, etc) will bring about the desired results



# Acknowledgements

- This presentation would not have been possible without the vision behind TikTube
  - Thank you MikroTik & the Latvia crew
  - Please, kindly rename your YouTube Channel to TikTube
- Valens Riyadi
  - King of QoS
  - He has several related video presentations & PDF slides online



# Thank you



**mum**  
Mikrotik User Meeting

**MUM NIGERIA**  
LAGOS, NOVEMBER 28, 2017

# Questions