# Mikrotik complete solution for ISP

Flávio Gomes Figueira Camacho

# Introduction

Mikrotik complete solution for ISP

Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

# Summary of the Presentation

- Vipnet is a telecommunications operator in Brazil that uses only Mikrotik.
- I will introduce and show how we implemented:
  - Border, Backbone, Access and CPE with Mikrotik
  - IPv4, IPv6 allocation and CGNAT
  - QoS Rules and Firewall
- The presentation is a tutorial on how Vipnet implement a complete and extremely functional solution with Mikrotik.

# Flávio Gomes Figueira Camacho

- Enginner with master's degree in telecommunications engineering
- Presentations:
  - - MUM 2009BR, MUM 2010BR, MUM 2011BR, MUM 2012BR, MUM 2013BR, MUM 2014BR, MUM 2015BR, MUM 2016BR, MUM 2017BR, MUM 2018UK.
- Certifications: MTCNA, MTCRE, MTCWE, MTCINE, MTCTCE, MTCIPv6 and MTCUME
- Oficial Trainer Mikrotik.

# Mikrotik Technologies

Mikrotik complete solution for ISP

Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

# Introduction

- Importance of Mikrotik for an internet provider
  - User Authentication
  - Bandwidth control over these users
  - Network Routing (OSPF and BGP)
  - Customer management
  - Service quality
  - Monitoring
  - Backbone - Access Network - Distribution Network

# Introduction

# Introduction

- When you receive a link you need a tool to share this link and configure.
  - BGP and Routing - Mikrotik
- Implement security against external attacks from hackers and from customers themselves.
  - Firewall – Mikrotik
- Authenticate users and block defaulters.
  - PPPoE, Hotspot... - Mikrotik

# Introduction

- Control the band and plans of each.
  - Queues  - Mikrotik
- Server for centralized authentication.
  - Radius – Mikrotik (UserManager)
- Internal network routing.
  - OSPF – Mikrotik
- Control of quality of service.
  - QoS – Mikrotik

# Introduction

- Monitoring Devices.
  - Manager – Mikrotik (The Dude)
- Network Interfaces.
  - Fiber, Ethernet, Wireless – Mikrotik
- Build a network to take the internet to customers.
  - Radios, antennas, fiber converters, switchs – Mikrotik

# Introduction

- Mikrotik has it all on a unique and extremely versatile platform. Nothing from multiple vendors with different solutions that are difficult to manage and integrate.

# Vipnet Network Design

Mikrotik complete solution for ISP

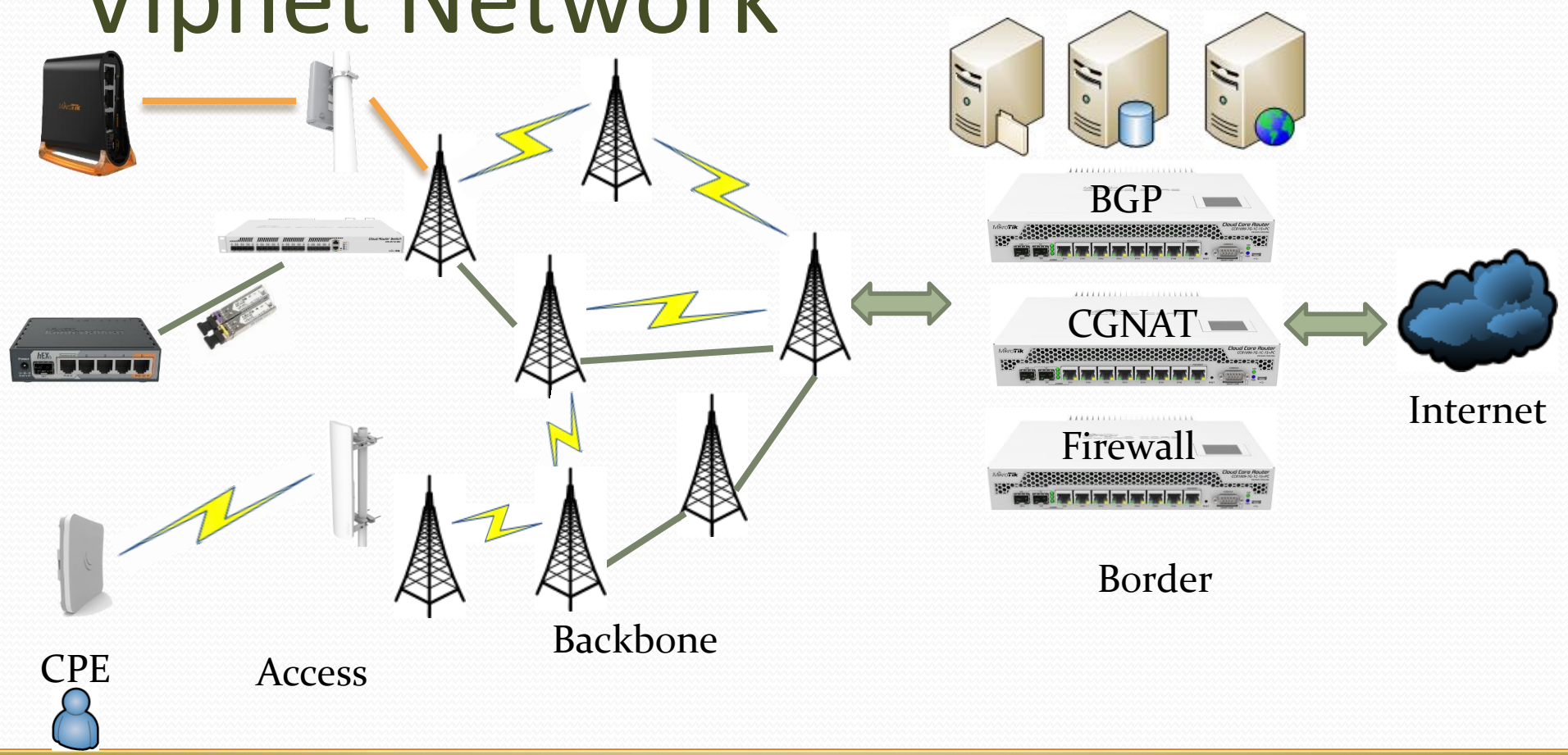
Flávio G. F. Camacho

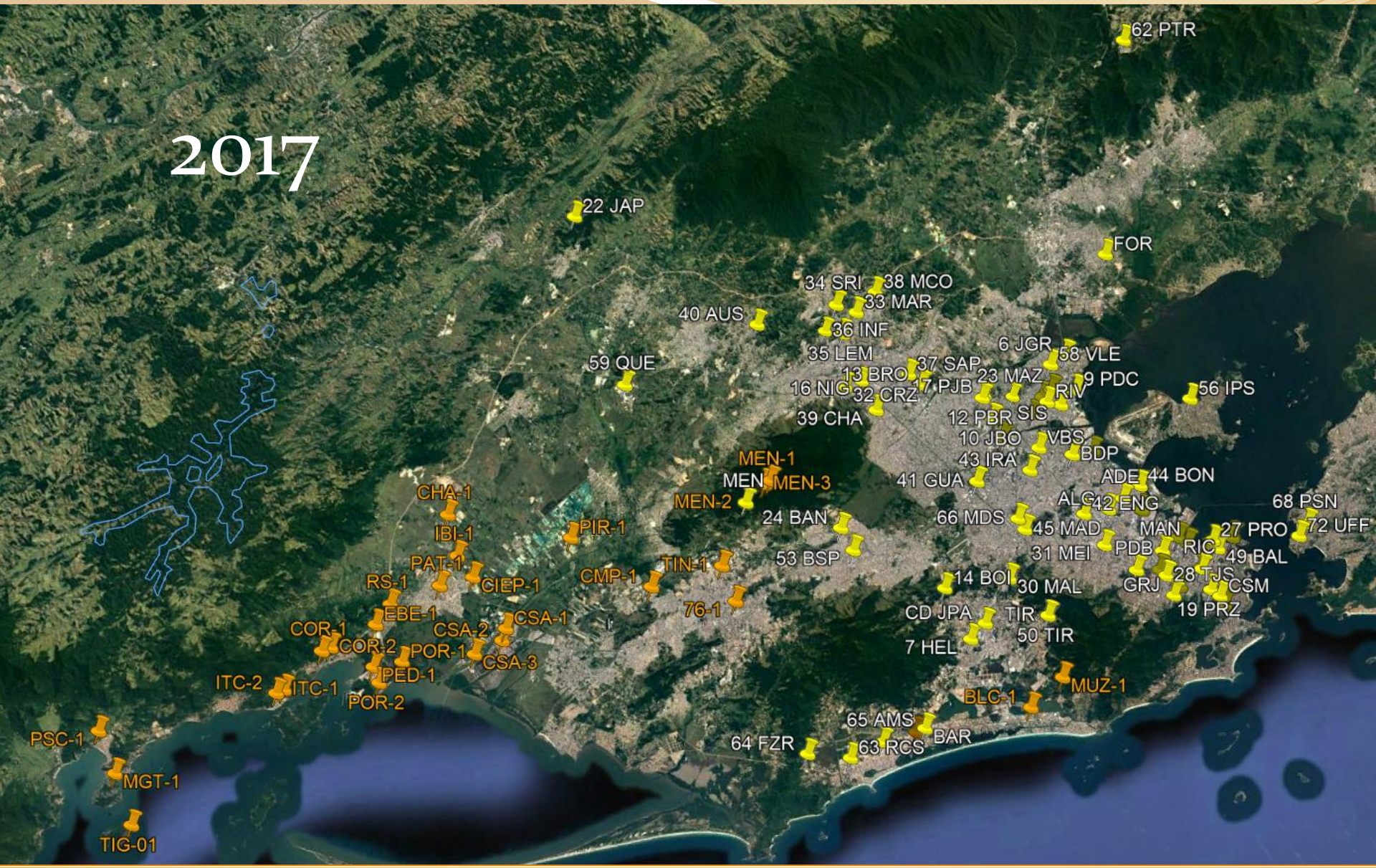
Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

# Vipnet Network

| Network Levels | Function | Equipment |
|---|---|---|
| Border | BGP / Nat / Log / Firewall / QoS / Queues | CCR Router and Servers |
| Backbone | Routing / QoS | PtP - Fiber / Radios |
| Access | PPPoE Server / Firewall / QoS / Queues | FTTH / RouterBoard / AP |
| CPE MK | PPPoE Client / WiFi / DHCP / Slaac ... | hAP light, SXT ... |

# Vipnet Network






How to deploy high availability networks and resistant to failure with Mikotik - OSPF / BGP / VPLS / ECMP / MPLS

Flávio G.F. Camacho - Case of Vipnettelecom

Mikrotik User Meeting in UK
Birmingham October 08, 2018

# Vipnet 2017

| | 2009 | 2012 | 2017 |
|---|---|---|---|
| Active Network Devices | 34 | 194 | 1198 |
| POP - Point of Presence | 10 | 26 | 118 |
| Cities | 2 | 8 | 17 |

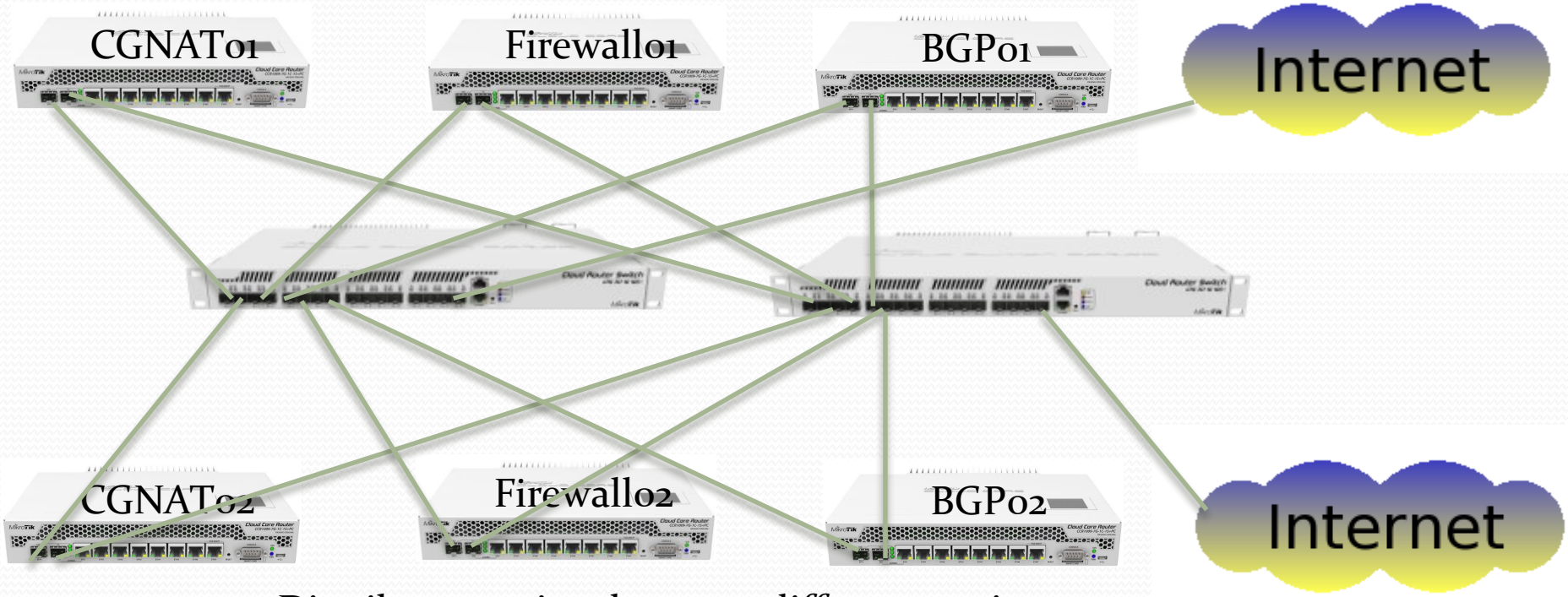
# Vipnet Network Border

Mikrotik complete solution for ISP

Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

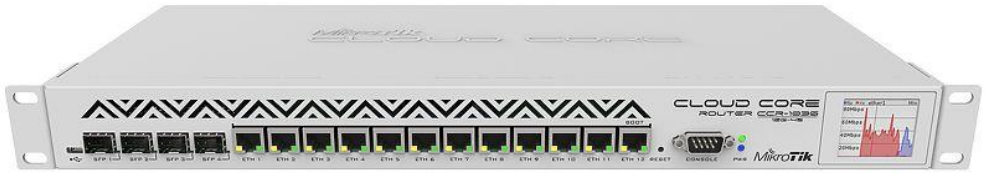
# Border




Distribute services between different equipment
Redundancy of services and equipment

# Border – BGP / Firewall / CGNAT

- CCR1036-12G-4S-EM




- CCR1036-8G-2S + EM

# Switch

- CRS317-1G-16S + RM
  - 1 Gigabit port switch with 16 SFP+


- CRS326-24G-2S+RM
  - 24 Gigabit port switch with 2 SFP+

# Vipnet Network Backbone

Mikrotik complete solution for ISP

Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

# Backbone Radio

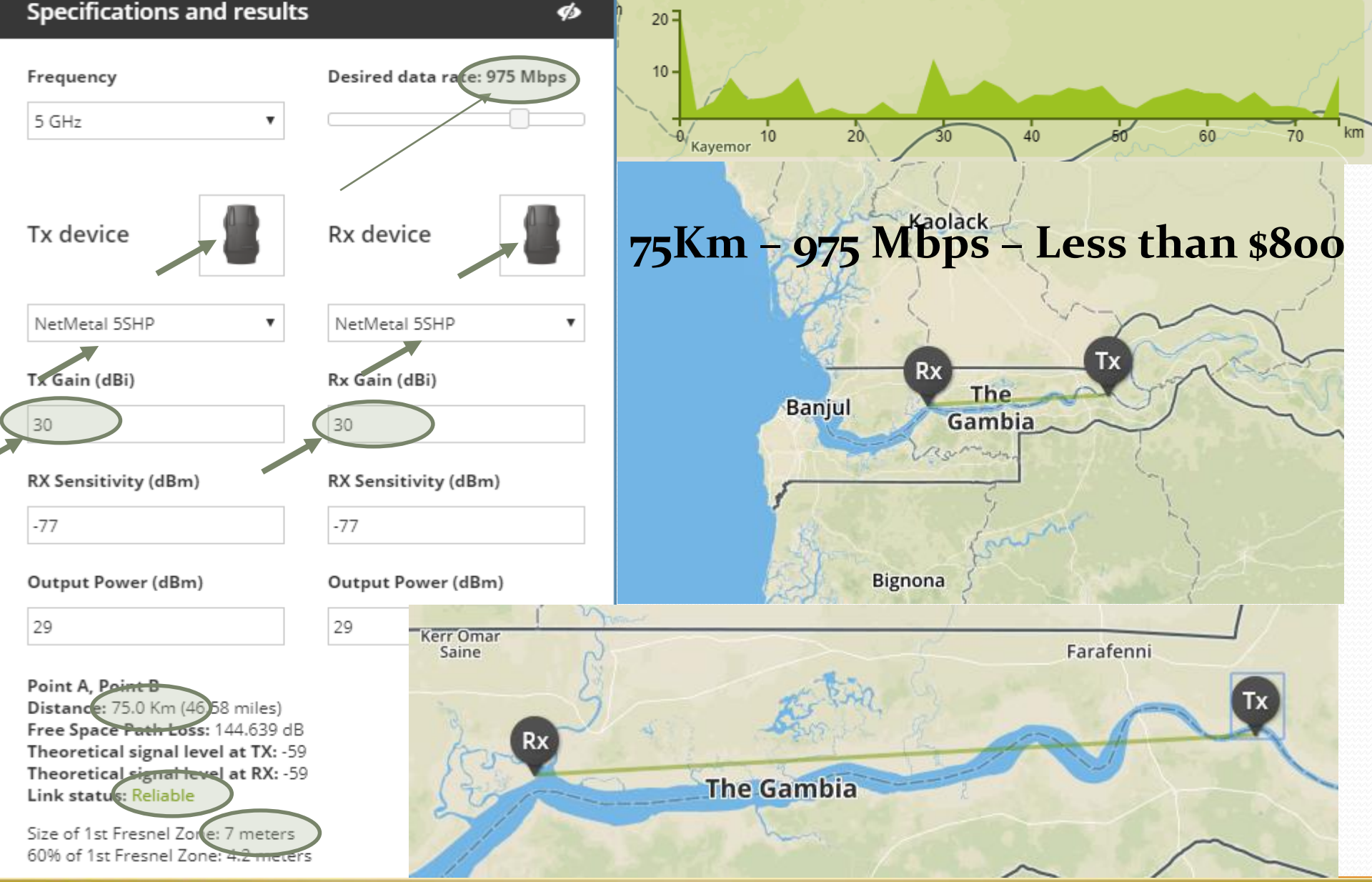
- Radio Backbone
  - Good transport capacity
  - Very accessible prices
  - OSPF Routing
  - Quick to install
  - Reaches great distances

# Backbone Radio – Antennas

- 30dBi
- Sleeve30

# Backbone Radio - PtP – NetMetal

- NetMetal 5SHP - 866Mbps
- NetMetal Trible - 1.3Gbps

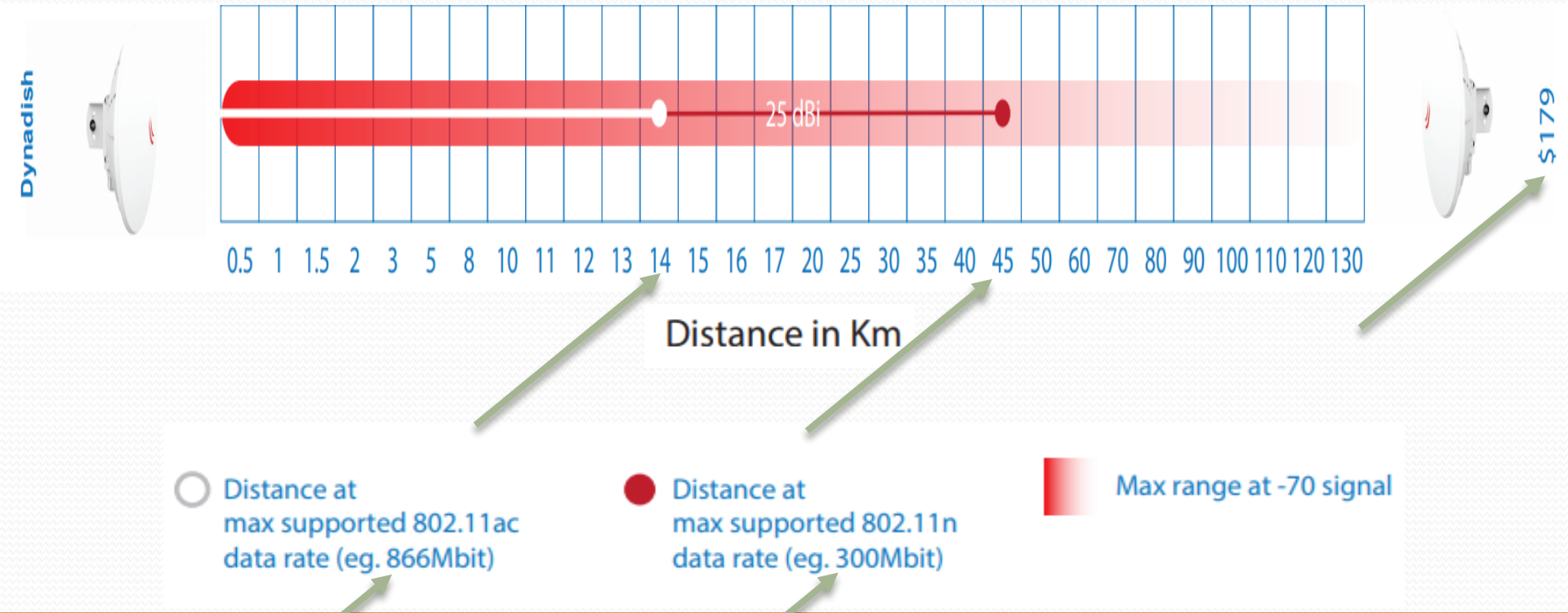



Mikrotik complete solution for ISP

Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

# PtP - Dynadish 25dBi 6GHz



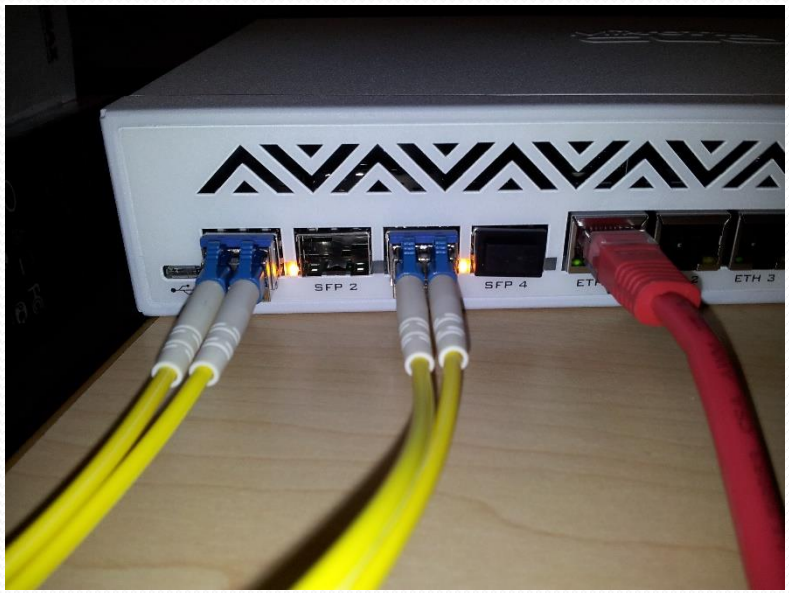
# BackBone Wireless

- Wireless Wire Dish - $ 298,00
- 60GHz – 2Gbps – 1500m

# Backbone Fiber

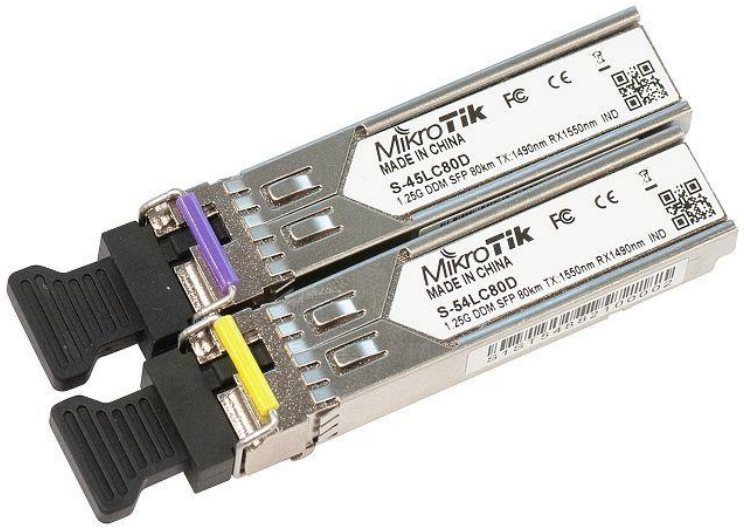
- Fiber is the future has no escape
  - No interference
  - High transport capacity

  But:
  - High cost of deployment
  - High maintenance cost



# Backbone - Fiber

- S-4554LC80D
  - Pair of SFP 1.25G module for 80km links with Single LC-connectors



# Backbone - Fiber

- S+2332LC10D
  - Pair of SFP+ (10Gbit) modules, 10km, for single optical cable

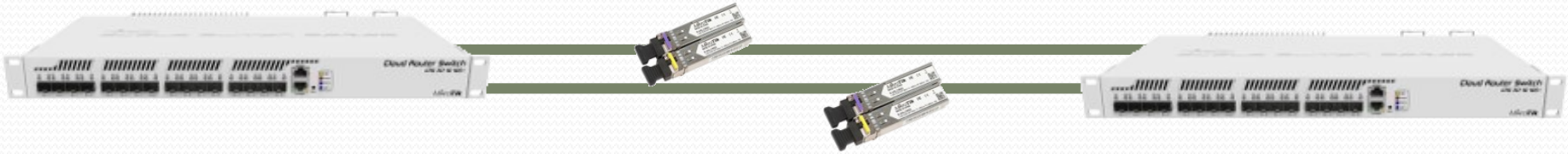
# Backbone – Fiber Switch

- CRS317-1G-16S + RM
  - 1 Gigabit port switch with 16 SFP+


- CRS326-24G-2S+RM
  - 24 Gigabit port switch with 2 SFP+

# Backbone – Fiber

**80 Km - 1.25Gbps**



**80 Km - 2,5Gbps**

**Cable 24F = 30Gbps**

**10 Km - 10Gbps**

# Vipnet Network Access

Mikrotik complete solution for ISP

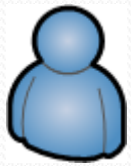
Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

# Vipnet Network Access

- Scenario 1 - Residential Wireless
- Scenario 2 - Residential Ethernet
- Scenario 3 - Residential Fiber
- Scenario 4 - Corporate Fiber
- Scenario 5 - Corporate Radio

# Scenario 1 - Residential Wireless



Customer

CPE Wireless Station
- PPPoE Client
- NV2

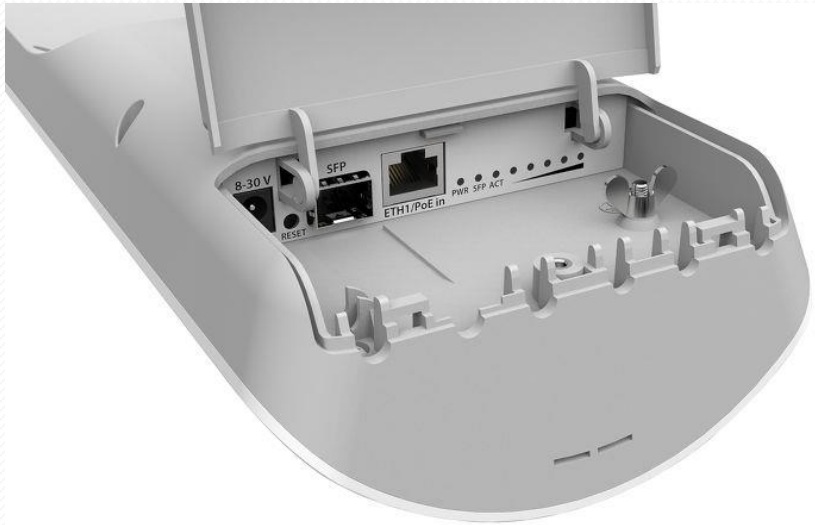
Vipnet AP
- PPPoE Server
- QoS
- Routing OSPF
- Firewall
- Queue
- NV2

Vipnet Backbone

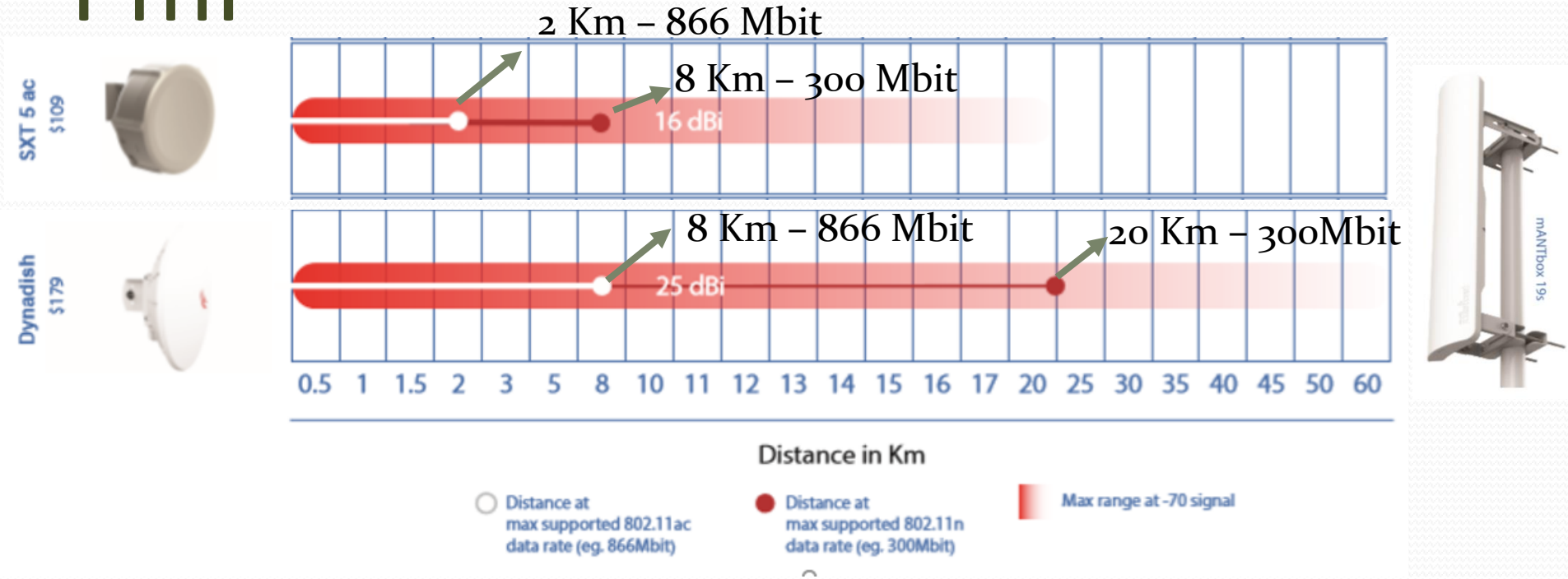
Internet

# AP 802.11ac 120°

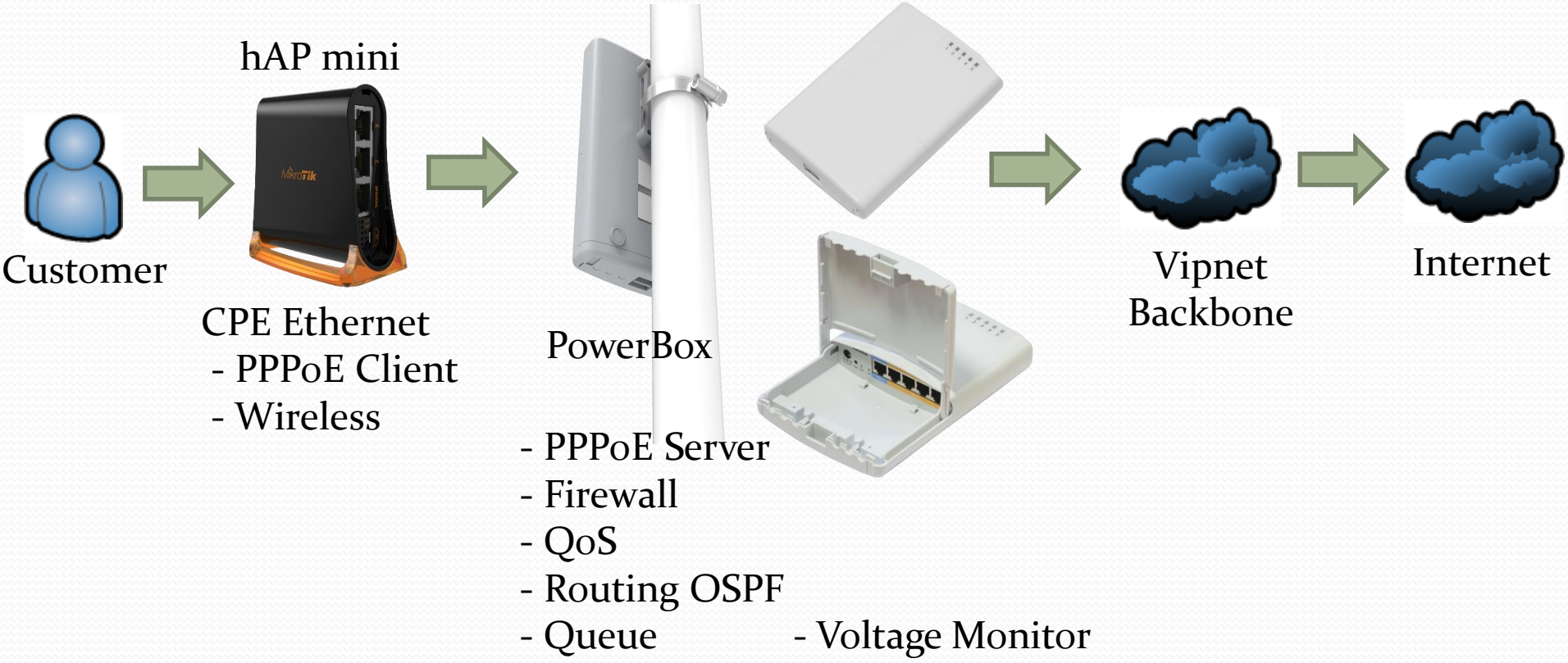
- 15dBi – 31dBm
- 19dBi – 31dBm



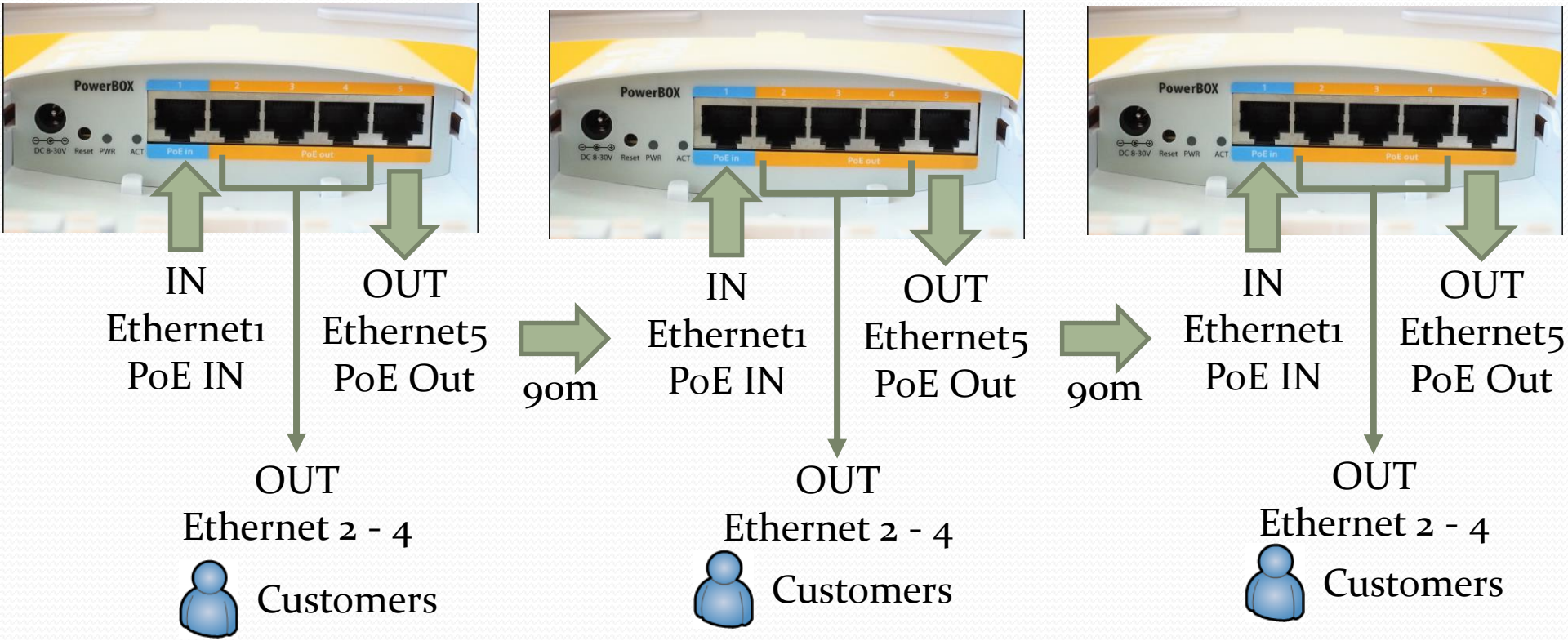

# PmP


SXT 5 ac
$109
Dynadish
$179
2 Km – 866 Mbit
8 Km – 300 Mbit
16 dBi
8 Km – 866 Mbit
20 Km – 300Mbit
25 dBi
0.5 1 1.5 2 3 5 8 10 11 12 13 14 15 16 17 20 25 30 35 40 45 50 60
Distance in Km
Distance at max supported 802.11ac data rate (eg. 866Mbit)
Distance at max supported 802.11n data rate (eg. 300Mbit)
Max range at -70 signal
mANTbox 19s

# Scenario 2 - Residential Ethernet



# Scenario 2 - Residential Ethernet



# Scenario 2 - Residential Ethernet


OUT
Ethernet5
PoE Out
Next Router
Other Box

IN
Ether net1
PoE IN


OUT
Ethernet 2 - 3

Customers

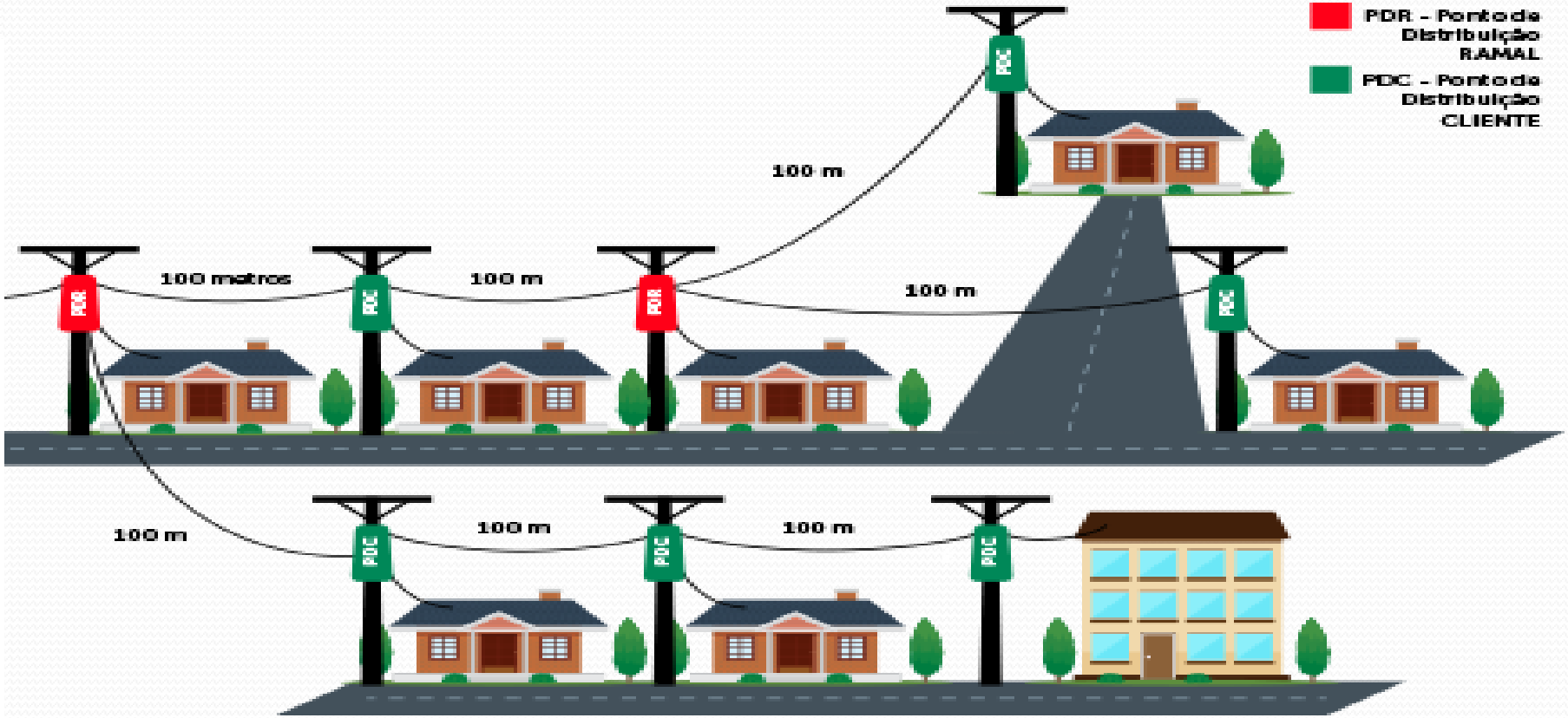
IN
Ether net1
PoE IN

OUT
Ethernet 2 - 5

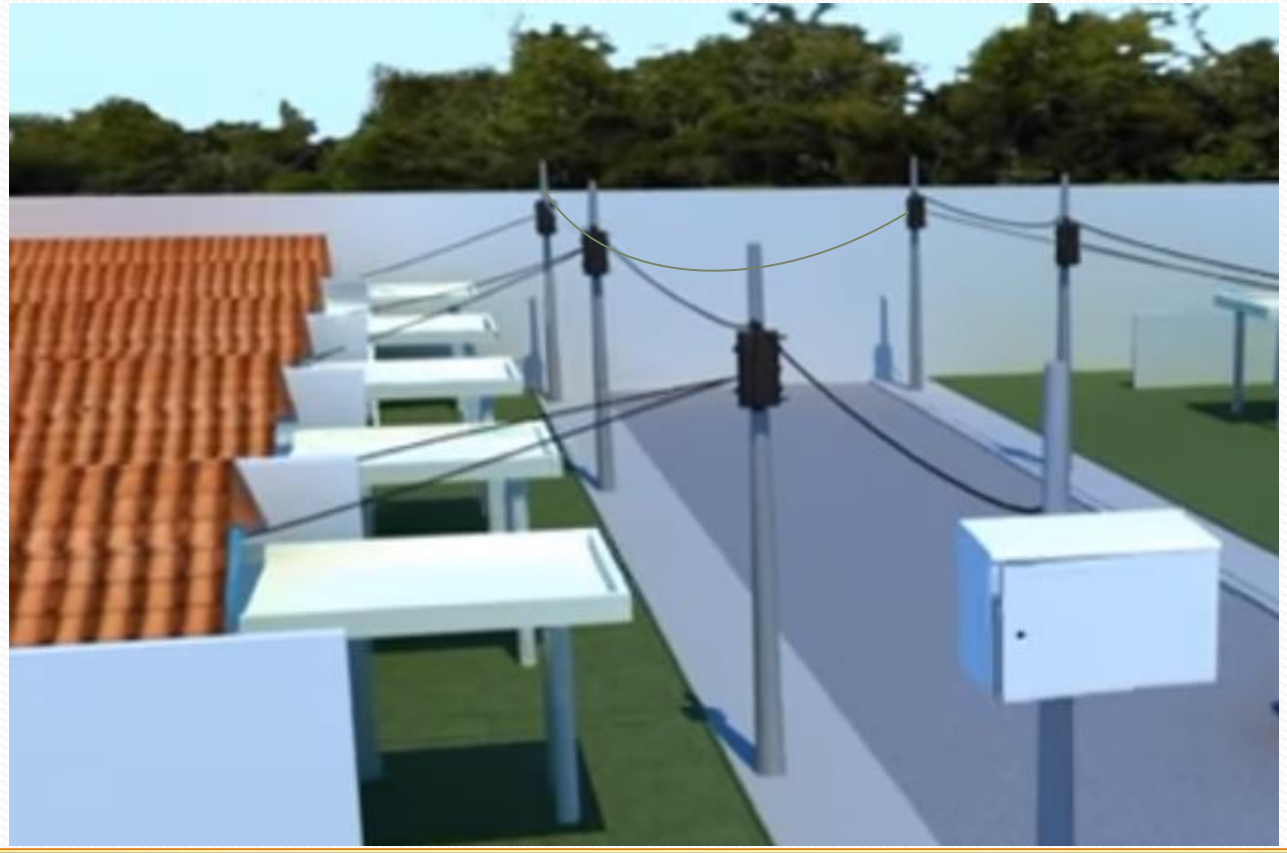
Customers

# Scenario 2 - Residential Ethernet

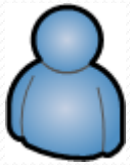
# Scenario 2 - Residential Ethernet



# Scenario 2 - Residential Ethernet



# Scenario 3 - Residential Fiber



Customer

CPE SFP ONU
- PPPoE Client

OLT

- PPPoE Server
- Firewall
- QoS
- Routing OSPF
- Queue

Vipnet
Backbone

# Scenario 3 - Residential Fiber

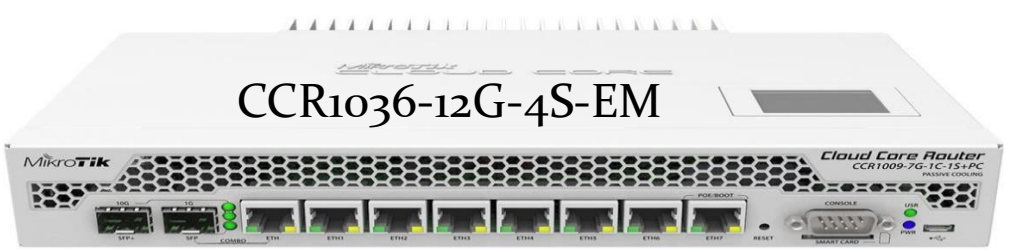

IN
Network
Fiber

More Clients with only one fiber and SFP.

# Scenario 4 - Corporate Fiber


Customer

CPE SFP
- PPPoE Client
- Firewall
- QoS




Concentrator
- PPPoE
- Firewall
- QoS
- Routing OSPF

Vipnet Backbone

# Scenario 5 - Corporate Radio

Customer

CPE PtP
Wireless Bridge
- PPPoE Client
- NV2

Vipnet PtP
Wireless Bridge
- PPPoE Server
- QoS
- Routing OSPF
- Firewall
- Queue
- NV2

Vipnet
Backbone

Internet

# Distribution of IPs

Mikrotik complete solution for ISP

Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

# Distribution of IPs

- RFC 6598 100.64.0.0/10
  - 100.64.0.0/11 customers (100.64.0.0-100.95.255.255)
  - Each concentrator receives a / 19 that holds 1024 clients, and can be summarized by OSPF.
  - Ex.
    - Concentrator 1 100.64.0.0/19 IP 100.64.0.0 – 100.64.15.64
    - Concentrator 2 100.64.16.0/19 IP 100.64.16.0 – 100.64.31.64
  - 100.127.0.0/16 for addressing the internal routers of the network.

# Distribution of IPs

- Each public IP has 1000 ports associated with the IP of the clients, this association is fixed, so it is easy through the logs to locate the client.
  - Ex. 192.0.2.1 ports 1101-2100 – 100.64.0.1
  - Ex. 192.0.2.1 ports 2101-3100 - 100.64.0.2
  - Ex. 192.0.2.1 ports 3101-4100 - 100.64.0.3
  - …
  - Ex. 192.0.2.1 ports 63101-64100 - 100.64.0.63
  - Ex. 192.0.2.1 ports 64101-65100 - 100.64.0.64

# Distribution of IPs

- IPv4
  - 100.64.0.1
  - 100.64.0.2
  - 100.64.0.3
  - ...
  - 100.64.0.63
  - 100.64.0.64

# Distribution of IPs

- Currently recommended allocation size (RFC6177):
  - /56 for residential customers
  - /48 for business customers

# Distribution of IPs

| IPv4 | |
|---|---|
| 100.XX.YY.ZZ | |
| ZZ = 1-64 - 64 possibilities | Each /24 they fit 64 customers |
| YY = 0-99 - 100 possibilities | With 100 /24 = 6.400 customers |
| XX = 64-95 – 31 possibilities | Each 31 /24 they fit = 198.400 customers |

# Distribution of IPs

| IPv4 | IPv6 |
|---|---|
| 100.XX.YY.ZZ | 2001:db8:XXYY:ZZ::/56 |
| | |
| Ex: | |
| 100.64.0.1 | **2001:db8:6400:01::/56** |
| 100.76.53.63 | **2001:db8:7653:63::/56** |
| 100.95.99.64 | **2001:db8:9599:64::/56** |

# CPE - Customer Premises Equipment

Mikrotik complete solution for ISP

Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

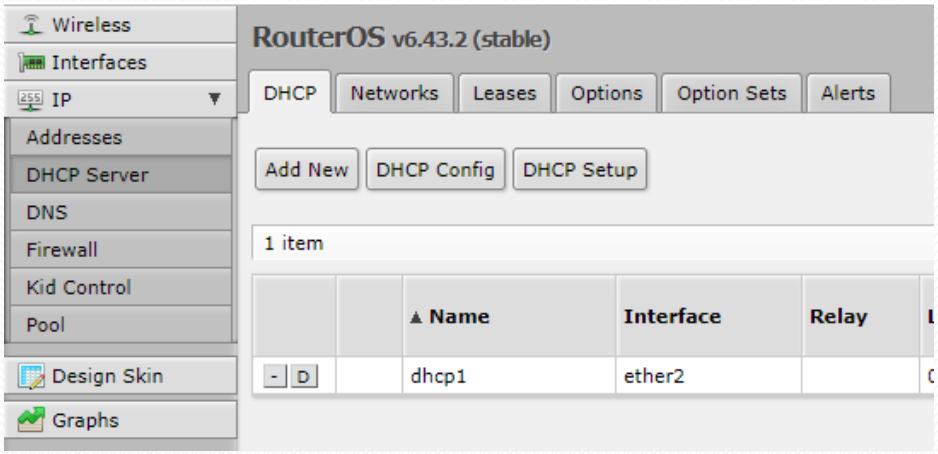
# CPE - Customer Premises Equipment

- The importance of a Mikrotik client CPE on each client.
  - Customer management
  - Client isolation from the rest of the network
  - Implementing bandwidth and firewall controls directly in the client's home
  - Offer a wireless service to add value
  - Mark client packages to implement QoS
  - Very low cost
  - Provide graphics services for usage monitoring.

# CPE - Customer Premises Equipment

- Each residential client has a CPE hAP light where the client has access to a web password with unique function rename the AP and the password of the same.
- This CPE connects in the access network where there is a PPPoE server and no IP configured in the interface.
- The CPE has a DHCP server enabled to facilitate the client's browsing.

# CPE Customer




- Provides DHCP.
- Implements firewall.
- Provides Wifi
  - There is a page where the client can configure the wi-fi password and the network name, besides being able to modify the IP of the internal network, and to see the graphics, besides redirection of doors.
- Bridge between Wi-Fi and network ports.
- It has a PPPoE dialer.
- Implements SLAAC.

# CPE Customer

- DHCP
  - IP with port 80 reserved 192.168.88.80
  - IP with port 22 reserved 192.168.88.22
  - IP with port 443 reserved 192.168.88.43
  - IP with port 53 reserved 192.168.88.53
  - IP with port 110 reserved 192.168.88.110
  - IP with port XX reserved 192.168.88.XX
  - Pool available by DHCP 192.168.88.200-253
  - Gateway 192.168.88.254

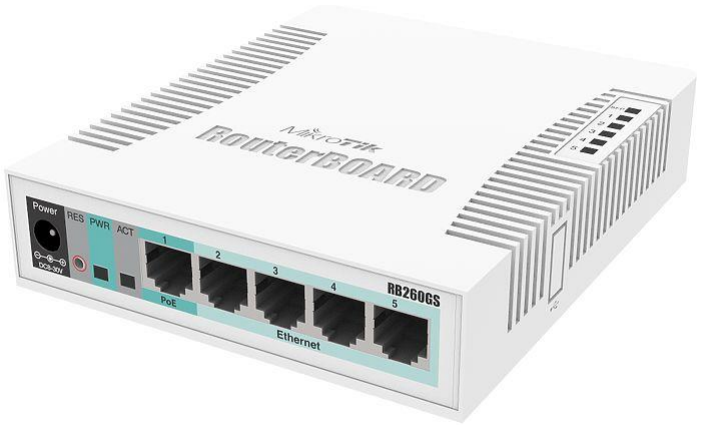
# CPE – Home Ethernet

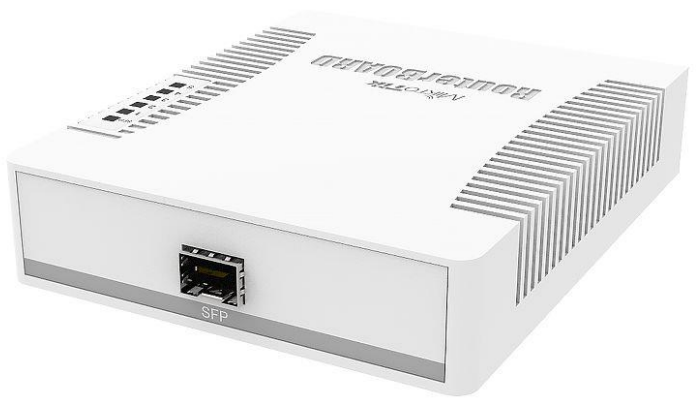
- hAP mini $19,95
- hAP Lite TC $21,95



# CPE - SFP

- hEX S
- RB260 GS

# CPE - Wireless

- 16dBi -- <8Km
- SXTsq - SXTsq 5 ac

- 24,5dBi
- LHG5 - LHG 5 ac

- 27 dBi -- 25Km
- LHG XL HP5 - LHG XL 5 ac

# ONU - FTTx

- Mikrotik S-GPON

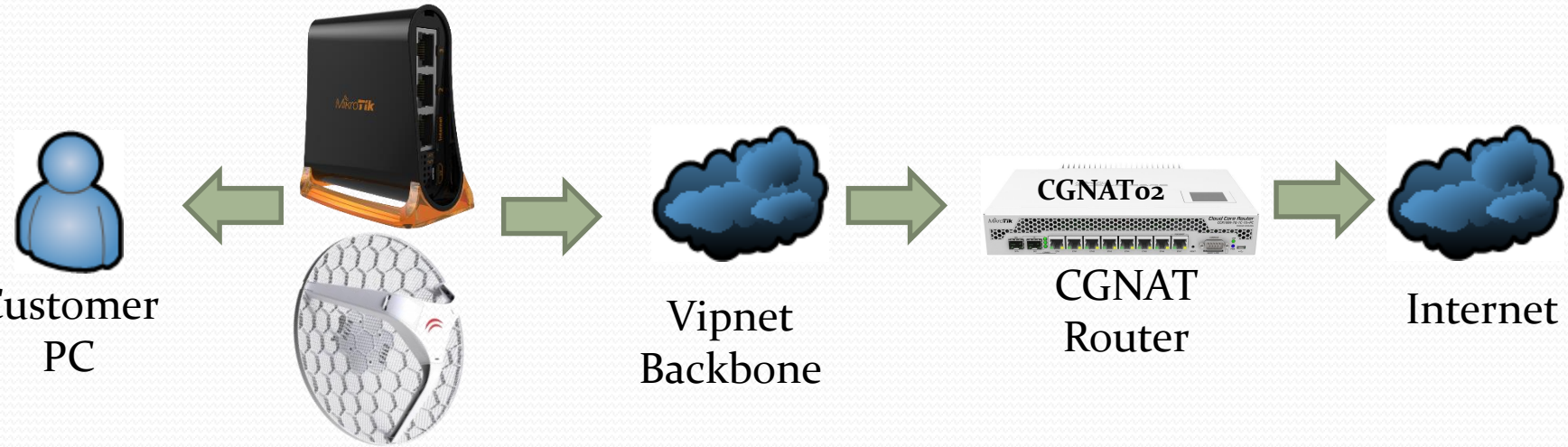
# CGNAT

Mikrotik complete solution for ISP

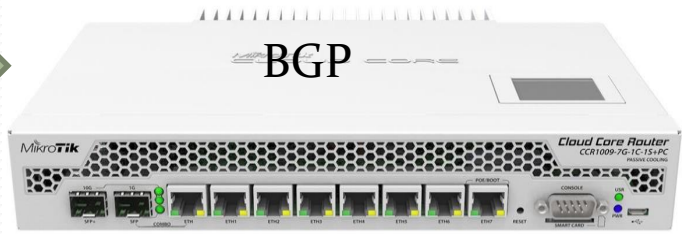
Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

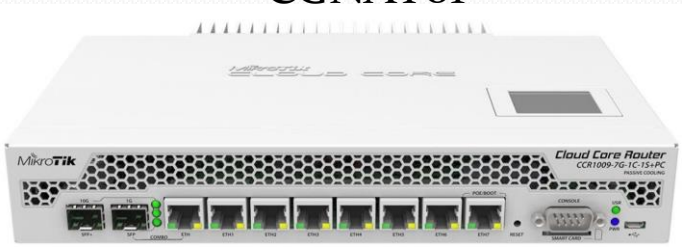
# CGNat - Three different IPv4 address spaces are involved.



# CGNAT - Backbone

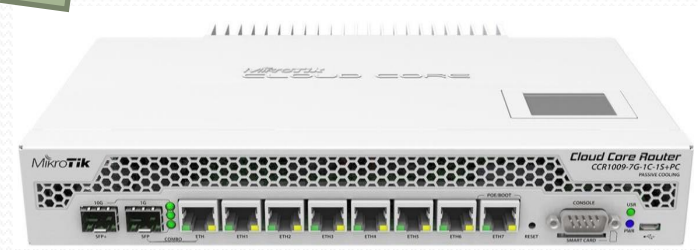




CGNAT01




192.0.2.0/26 > 100.64.0.0/18

CGNAT02




192.0.2.128/25 > 100.64.64.0/18

Each CGNAT do Nat for 4096 customers

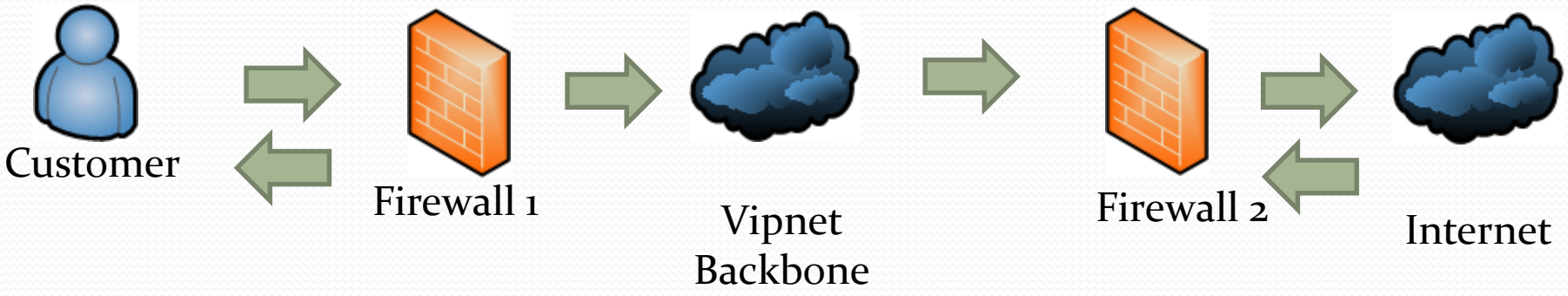
# Firewall

Mikrotik complete solution for ISP

Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

# Firewalls Vipnet

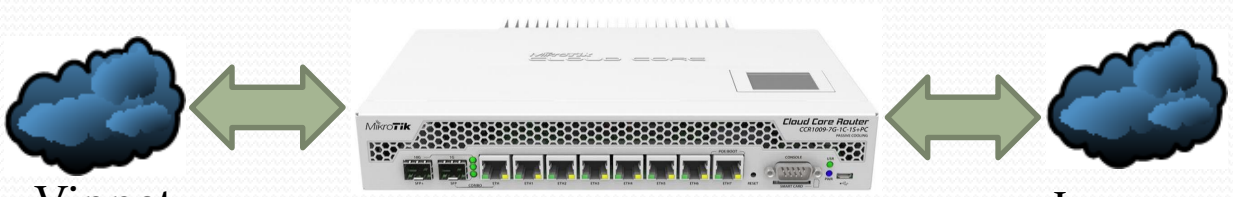


# Firewall 1

- Control de trafic from the customers to the network.
- Implemented in AP or First Router.

# Firewall 2

- Control de trafic from the internet.
- Implemented in CCR



# Firewalls Vipnet – Anti-spoof


✗ Src-adr ≠ 192.0.2.0/24

Drop packets from LAN that does not have LAN IP.
192.0.2.0/24 is local network used subnet

# Firewalls Vipnet – Anti-spoof


Src-adr ≠ 192.0.2.0/24

Drop packets to Internet
that does not have LAN IP

# Firewall – Bogons

| | |
|---|---|
| 0.0.0.0/8 | 192.0.0.0/24 |
| 172.16.0.0/12 | 192.0.2.0/24 |
| 192.168.0.0/16 | 198.51.100.0/24 |
| 10.0.0.0/8 | 203.0.113.0/24 |
| 169.254.0.0/16 | 100.64.0.0/10 |
| 127.0.0.0/8 | 240.0.0.0/4 |
| 224.0.0.0/4 | 192.88.99.0/24 |
| 198.18.0.0/15 | |

- RFC 1918, 3069, 5735, 6598 adn 6890

# Firewalls Vipnet – Drop Bogon


Src-adr = Bogon

Drop packets from Internet that does not have valid IP

# Firewalls Vipnet – Drop Bogon


Dst-adr = Bogon

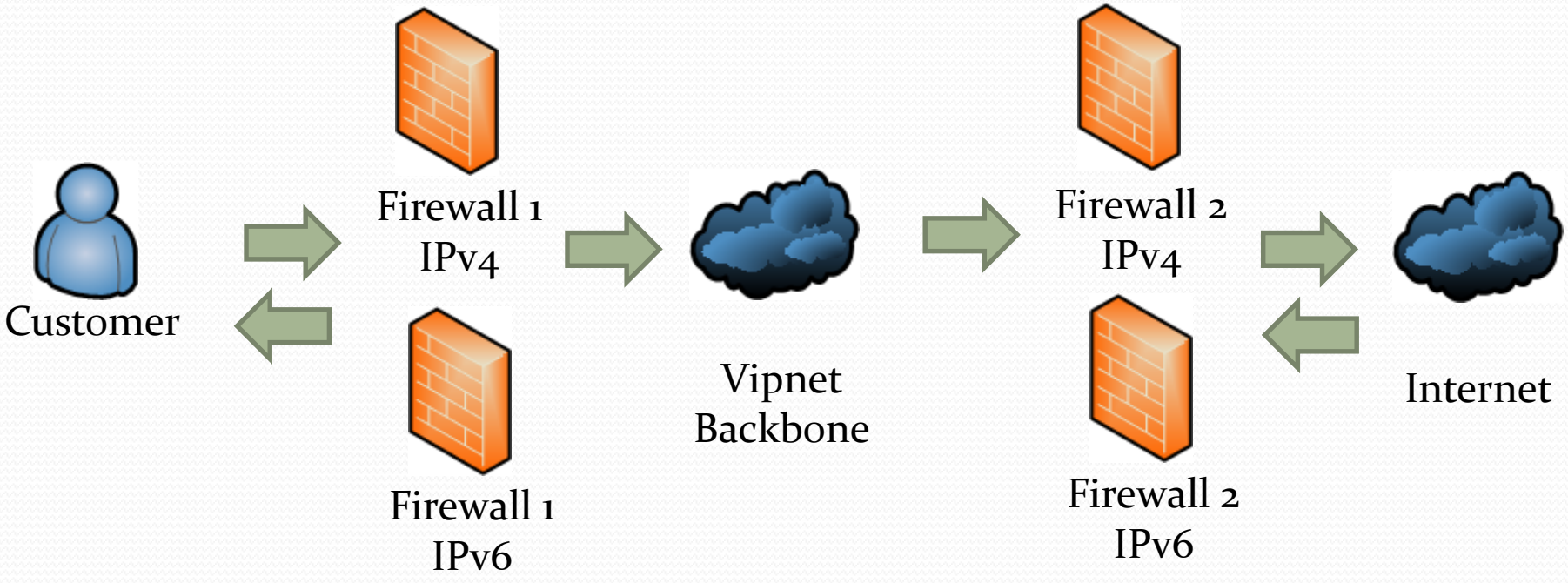
Drop packets to Internet that does not have valid IP

# Firewall – Input

- Create address-list for IP addresses, that are allowed to access your router;
  - ✓ IPs from routers for OSPF work
  - ✓ IPs of management.

- Drop everything else and log

# Firewalls Vipnet



# QoS

Mikrotik complete solution for ISP

Flávio G. F. Camacho

Mikrotik User Meeting in EU
Viena, March 07 - 08, 2019

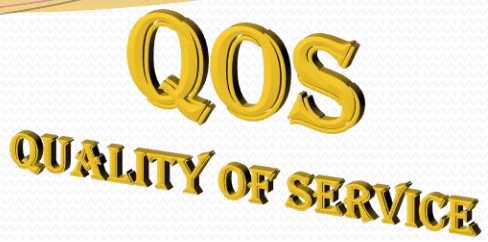
# QoS - Vipnet

- We have five diferente classes of service:
  - **Monitoring**: At this class we have the network of monitoring and the routers. Bigger priority
  - **VoIP**: At this class we have the VoIP servers.
  - **VIP**: At this class we have the clientes with full garantie of band and the more important.
  - **Business**: Companies with more garanted band.
  - **Residential**: Residential customers with low ticket. Smaller Priority

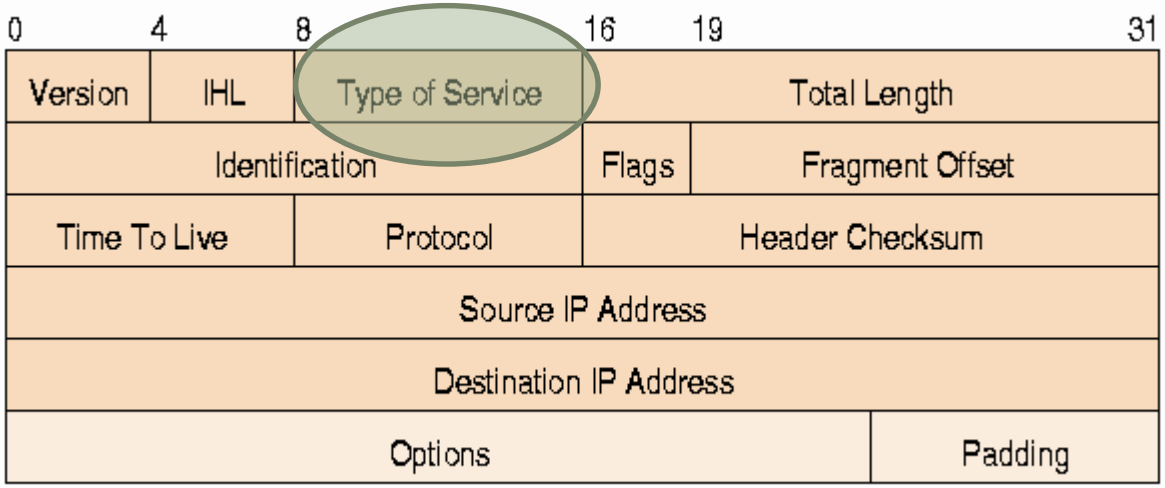
# QoS - Vipnet 2 3 5 6 7

| Class | Max-Limit | Limit-at | Priority | Packet Mark (TOS) |
|---|---|---|---|---|
| Monitoring | Small | = Max-Limit | 2 | 2 |
| VoIP | Medium | = Max-Limit | 3 | 3 |
| VIP | Variable | = 100% Max-Limit | 5 | 5 |
| Business | Variable | = 50% Max-Limit | 6 | 6 |
| Residential | Variable | = 25% Max-Limit | 7 | 7 |

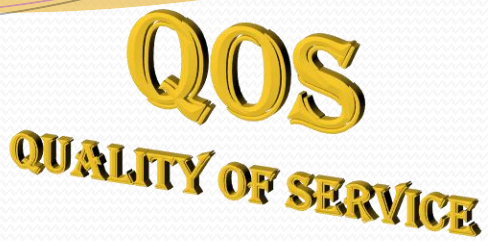
# QoS – Type of Service



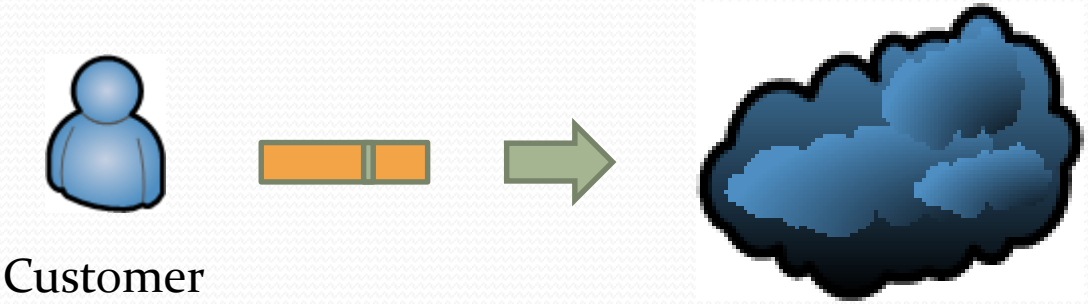

- What is Type of Service?



# QoS – Type of Service




- Why we use is Type of Service?



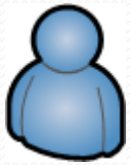
# QoS – VoIP internal

- IP based marking for VoIP Server

VoIP Server

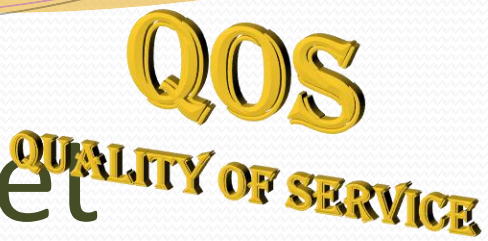
Src-address = VoIP Server

Dst-address = VoIP Server

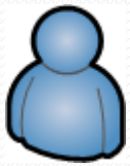


Customer

# QoS – Customer > Internet




- Paquet Mark with TOS



Customer

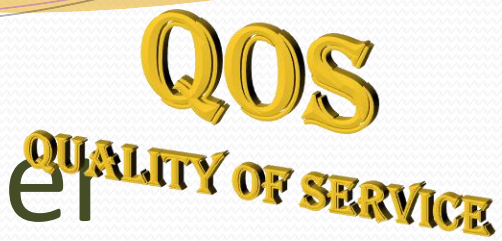
Src-address = Customer

First MK router


Packet Marqued TOS

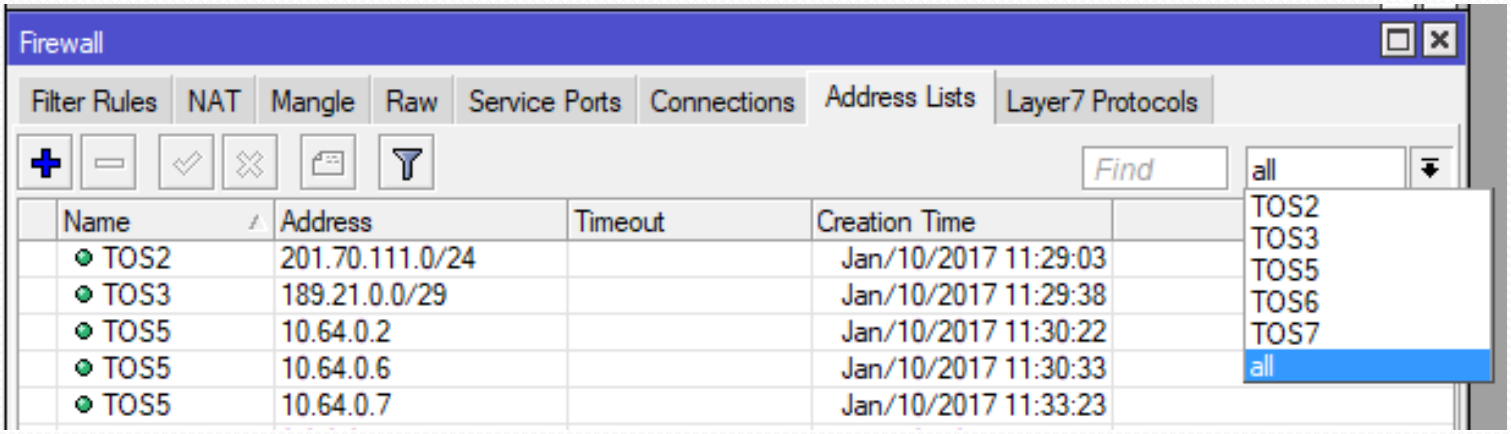
Vipnet Backbone

# QoS – Internet > Customer

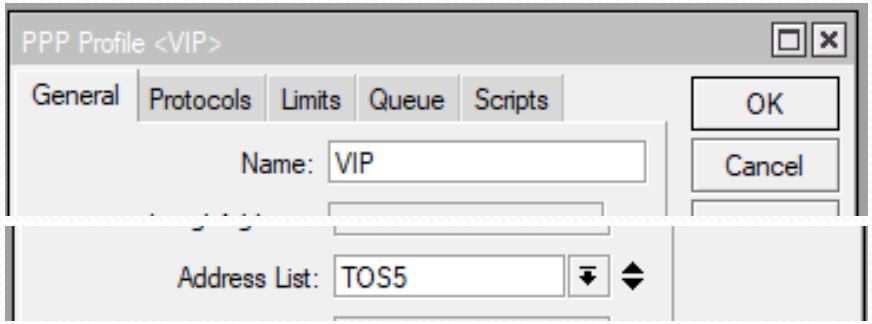



- Paquet Mark with TOS

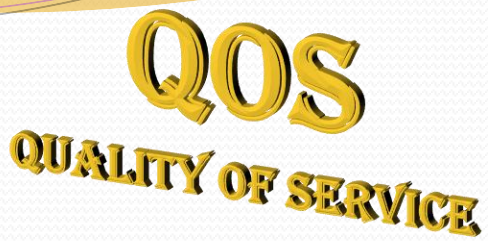
# QoS - Use of Address Lists




- PPP Profile
  - Address List



# QoS – VoIP Server



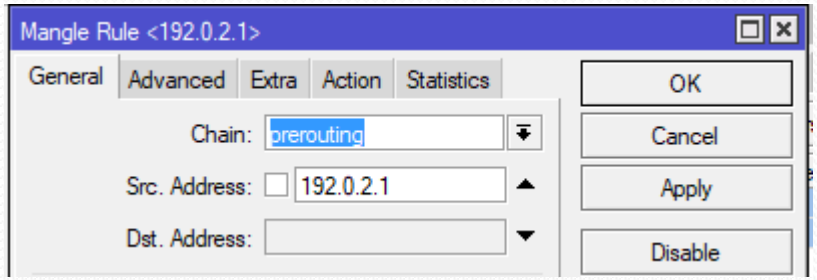

Firewall

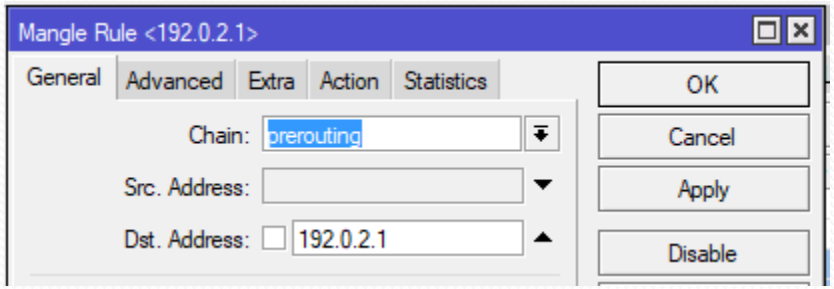
Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

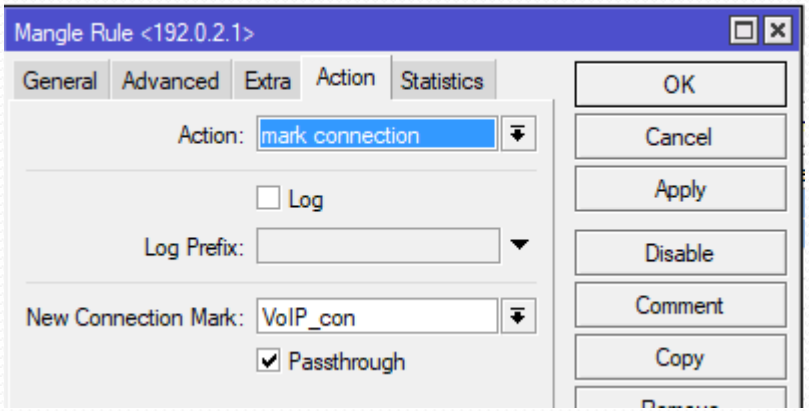
00 Reset Counters | 00 Reset All Counters

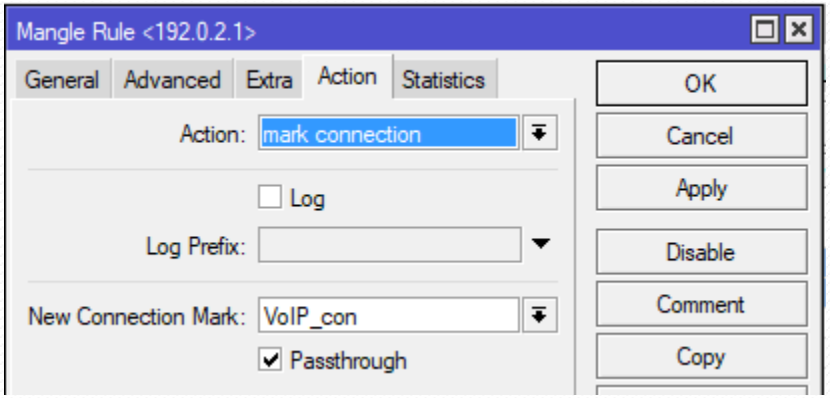
| # | | Action | Chain | Src. Address | Dst. Address | New DSCP (TOS) |
|---|---|---|---|---|---|---|
| ;;; Mark connection VoIP Server | | | | | | |
| 0 | | mark connection | prerouting | 192.0.2.1 | | |
| ;;; Mark connection VoIP Server | | | | | | |
| 1 | | mark connection | prerouting | | 192.0.2.1 | |
| ;;; Mark packets VoIP Server | | | | | | |
| 2 | | mark packet | prerouting | | | |
| ;;; Change TOS packets VoIP Server | | | | | | |
| 3 | | change DSCP (TOS) | prerouting | | | 3 |

# QoS – VoIP Server

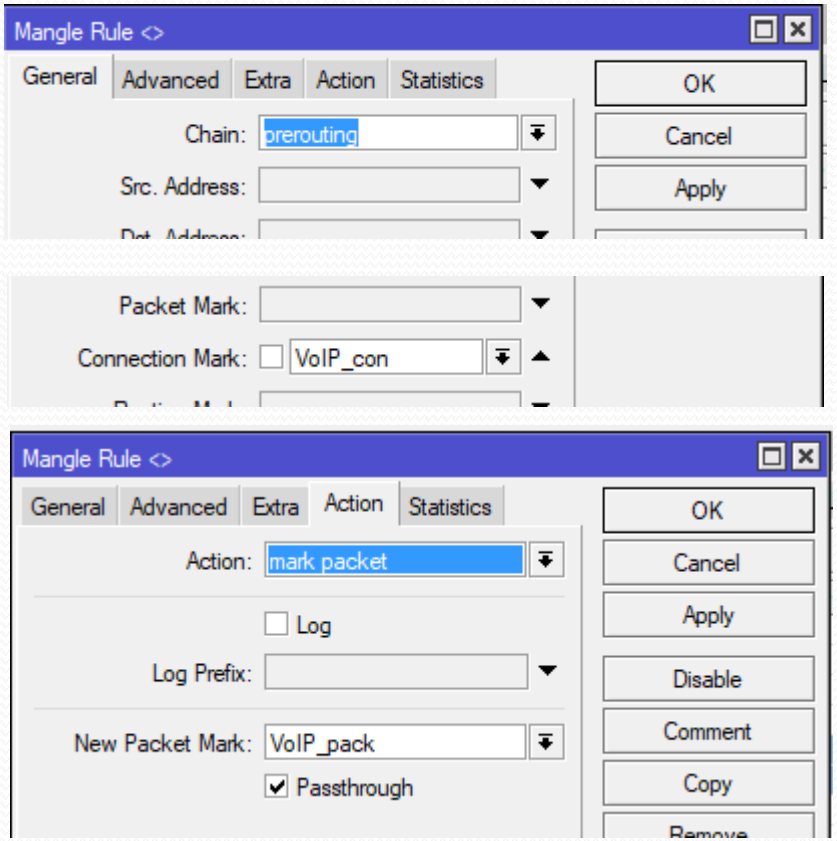


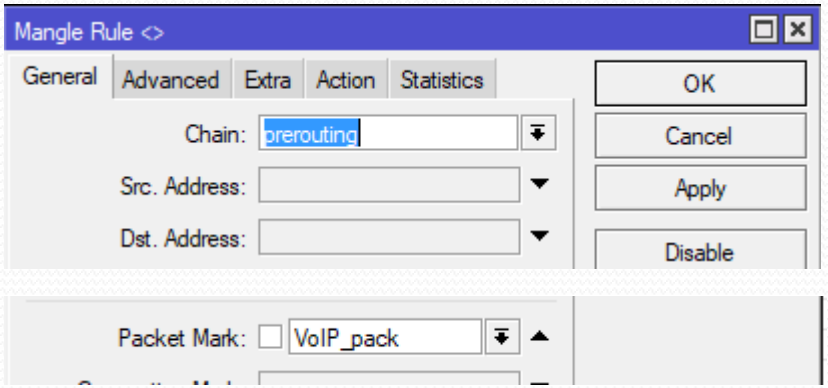



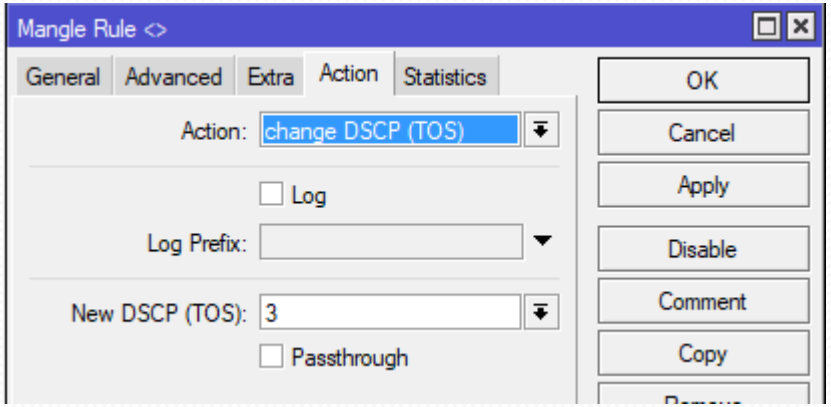
# QoS – VoIP Server



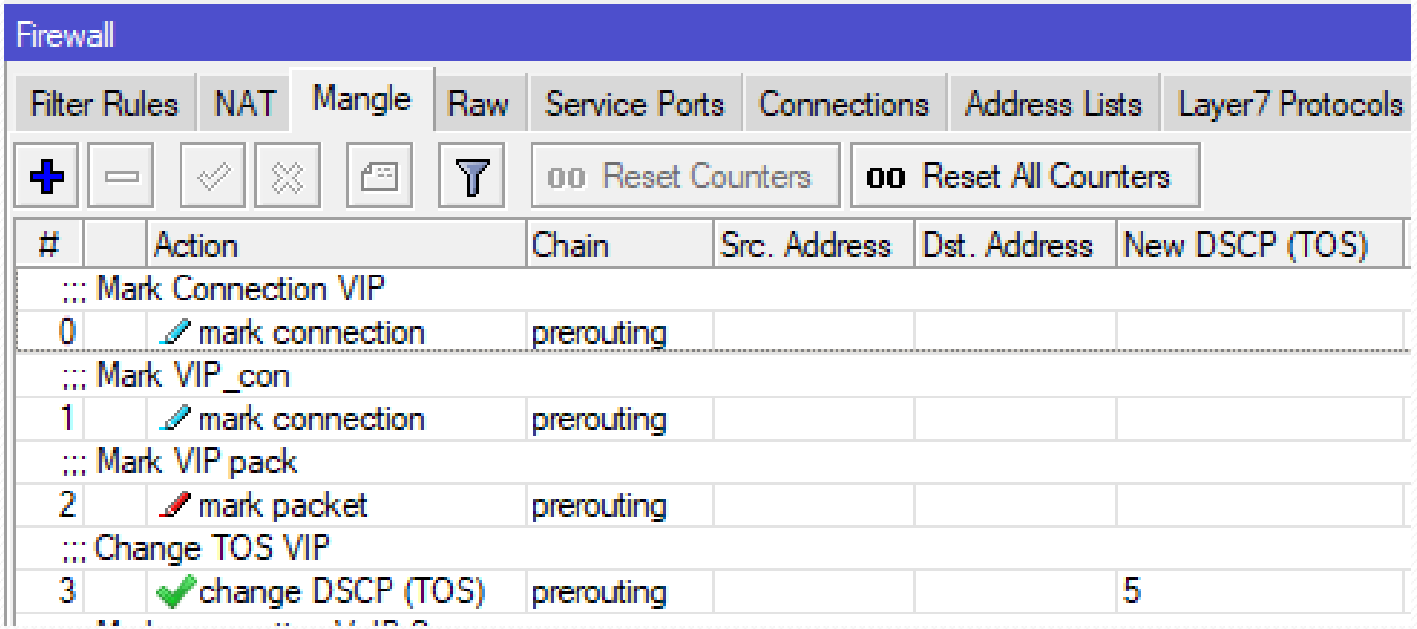





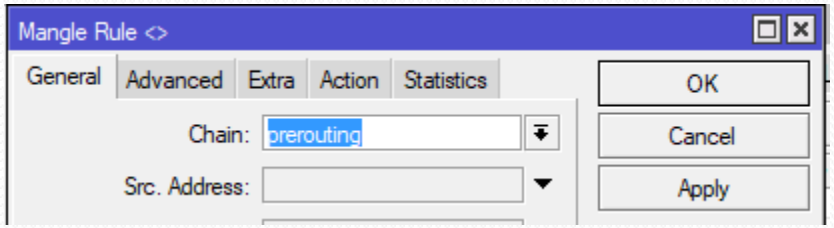


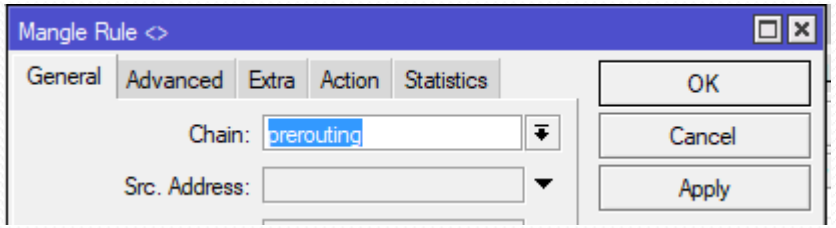


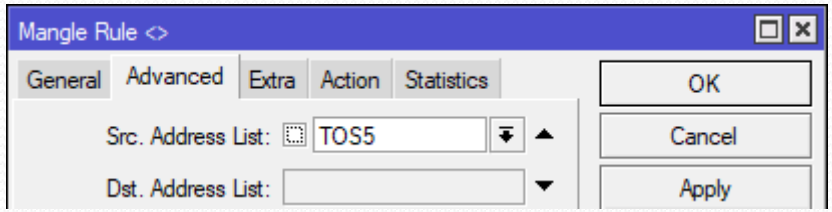
# QoS – Pack Clients Access

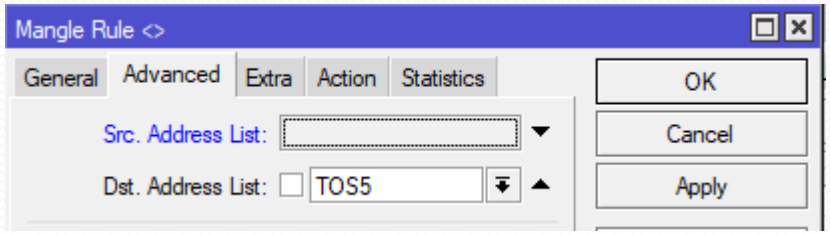


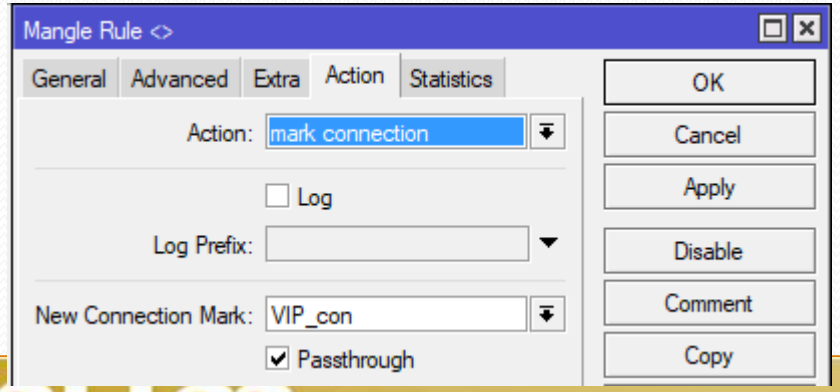
# QoS – Pack Clients Access

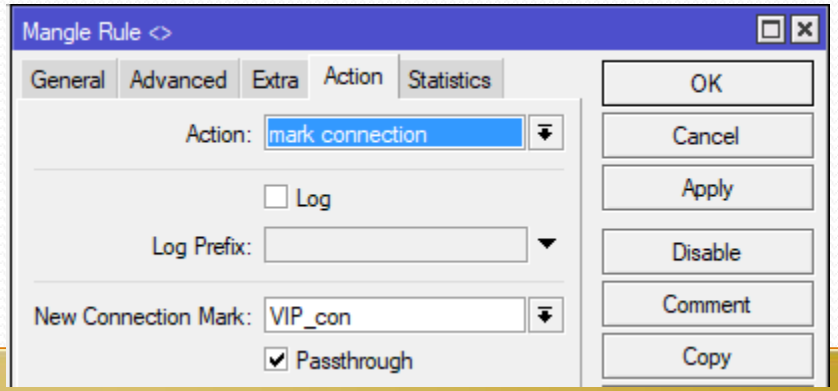


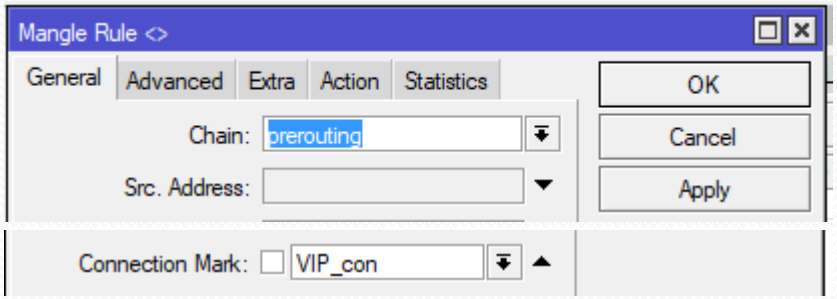



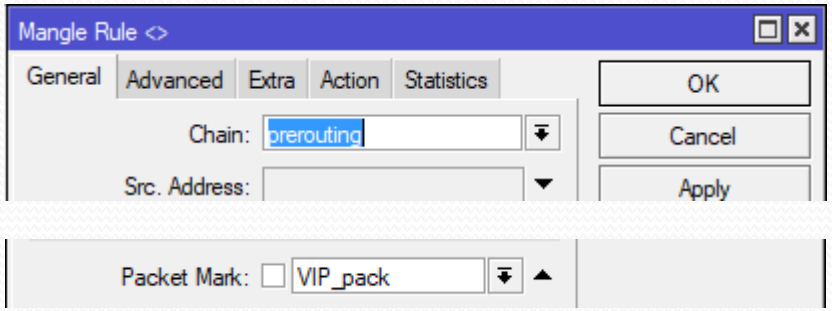



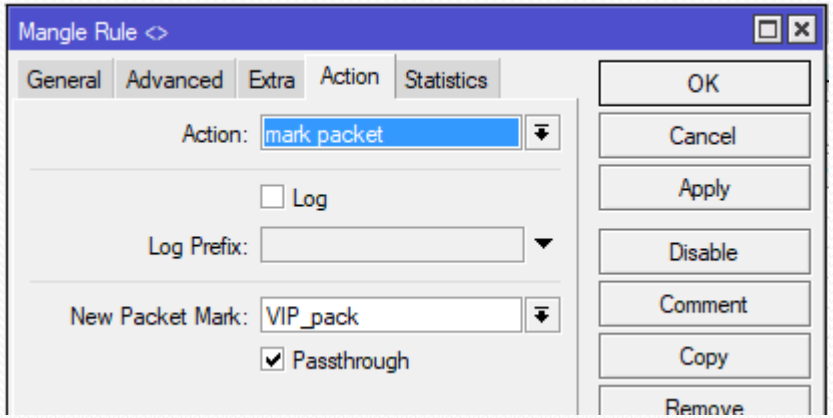



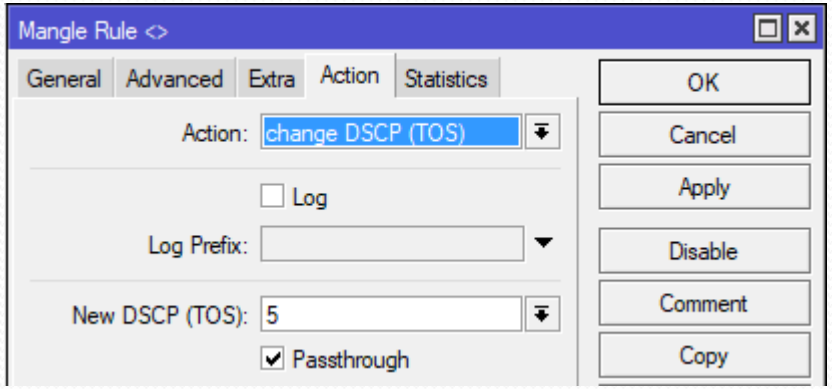



# QoS – Pack Clients Access

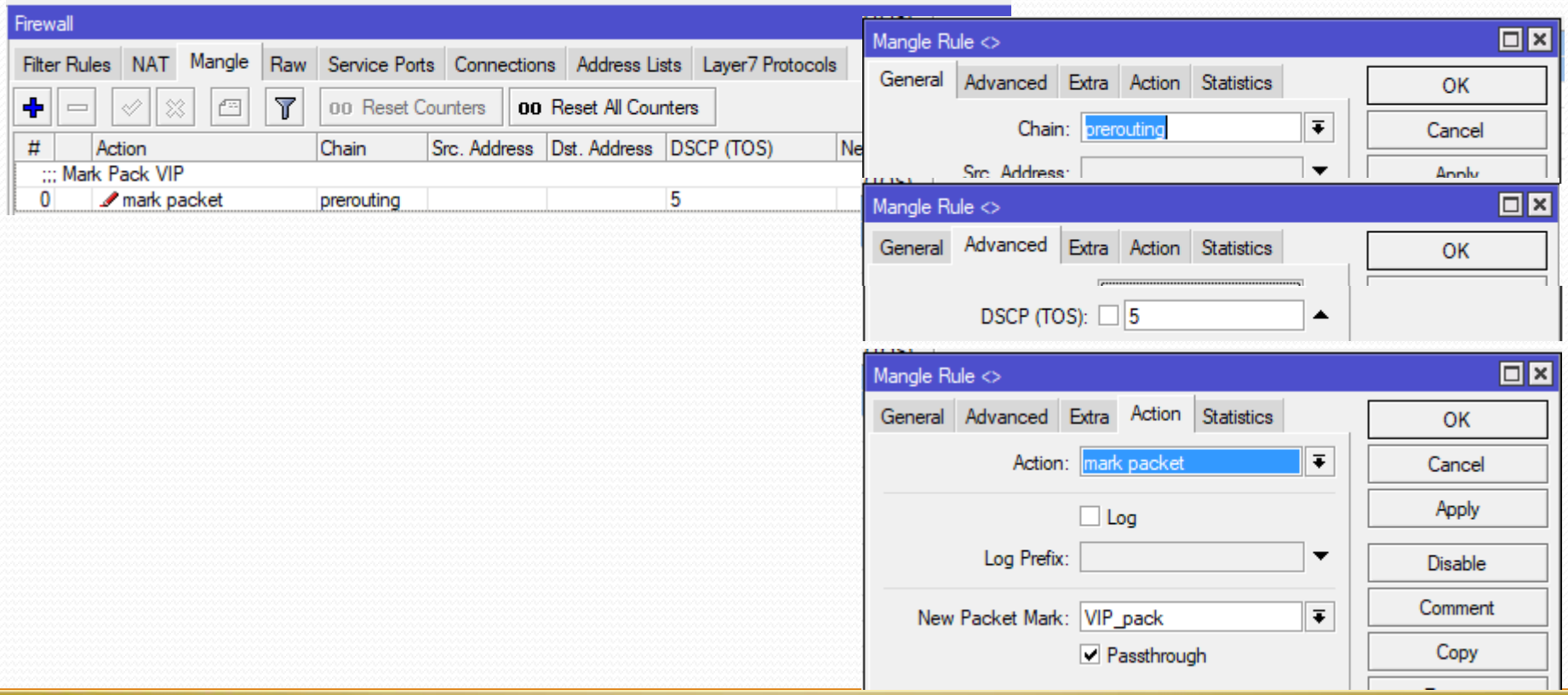


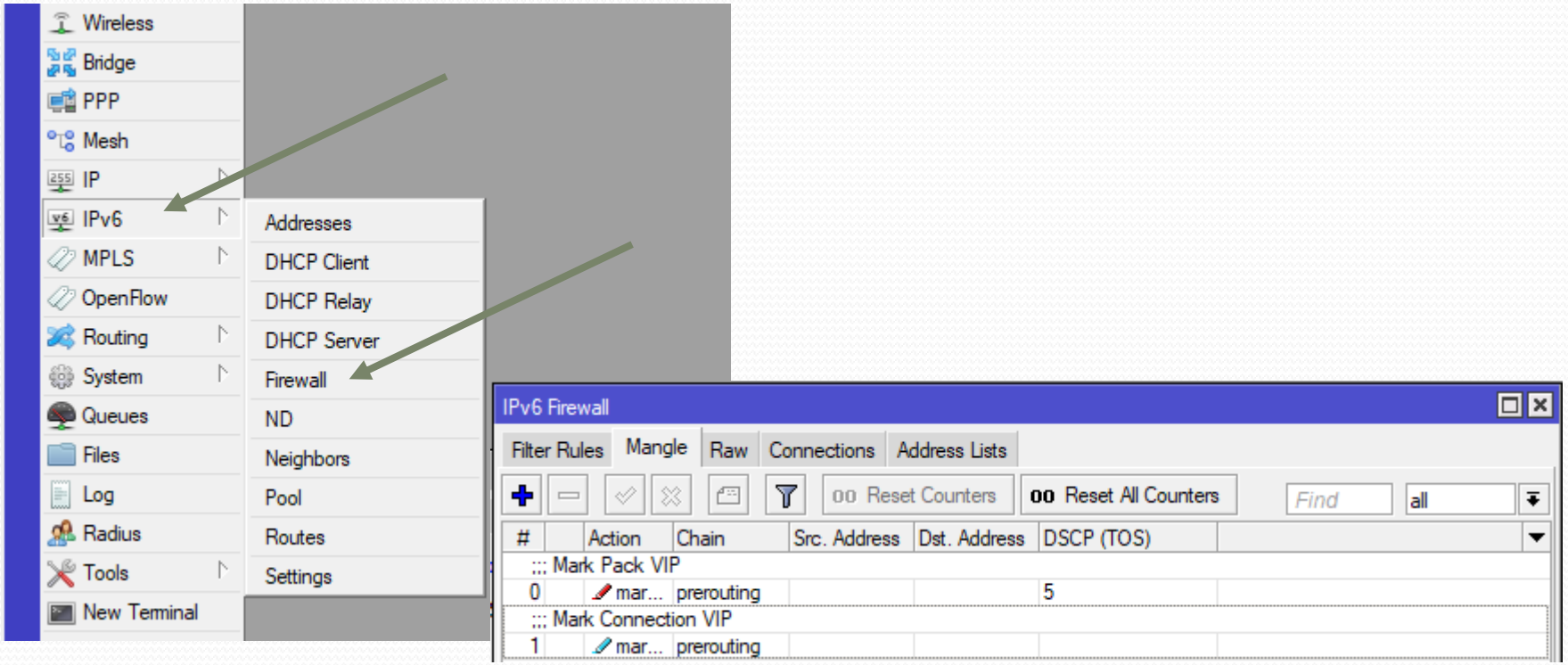



# QoS – Routers


Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
00 Reset Counters
00 Reset All Counters
# Action Chain Src. Address Dst. Address DSCP (TOS)
::: Mark Pack VIP
0 mark packet prerouting 5
Mangle Rule <>
General Advanced Extra Action Statistics
Chain: prerouting
Src. Address:
OK
Cancel
Apply
Mangle Rule <>
General Advanced Extra Action Statistics
DSCP (TOS): 5
OK
Mangle Rule <>
General Advanced Extra Action Statistics
Action: mark packet
Log
Log Prefix:
New Packet Mark: VIP_pack
Passthrough
OK
Cancel
Apply
Disable
Comment
Copy

# QoS – IPv6


Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Addresses
DHCP Client
DHCP Relay
DHCP Server
Firewall
ND
Neighbors
Pool
Routes
Settings
IPv6 Firewall
Filter Rules
Mangle
Raw
Connections
Address Lists
Reset Counters
Reset All Counters
Find
all
# Action Chain Src. Address Dst. Address DSCP (TOS)
;;; Mark Pack VIP
0 mar... prerouting 5
;;; Mark Connection VIP
1 mar... prerouting

# Conclusion

The Vipnet Company started operating in 2004, in 2007 we started using Mikrotik, in 2017 we had 14,000 customers using only Mikrotik radios and routers.

We are a success story and Mikrotik is part of that.

# Thank you!

Flavio G. F. Camacho

flavio@grupovipnet.com.br

(+351) 965869277