

Приоритизация трафика на оборудовании MikroTik, обзор возможностей и примеры применения

Алексей Чудин
Иркутск, Владивосток, МУМ 2016



Обо мне

Алексей Чудин

Опыт работы с сетями более 10 лет

Сертифицированный тренер MikroTik с 2014 г.

Сертификаты:

MikroTik: MTCNA, MTCRE, MTCWE, MTCTCE, MTCUME, MTCINE, Trainer

Microsoft: MCP, MCSA

Cisco: CCNA, CCNP (R&S)

Обо мне

MikroTik-Courses.ru: ведущий тренинг-центр **MikroTik** в России и СНГ

За 2 года работы:

- обучено 286 специалистов (из них 28 в Иркутске, 26 во Владивостоке)
- выдано 428 сертификатов (из них 43 в Иркутске, 41 во Владивостоке)
- 4 страны СНГ
- 14 городов
- География от Калининграда до Владивостока

Цель презентации

Показать возможности оборудования **MikroTik** в области ограничения пропускной способности и приоритизации трафика. Будут рассмотрены возможности RouterOS, WMM на беспроводных линках, а также возможности switch-chip на коммутаторах серии CRS и RB260

Немного теории

Часто в повседневной работе сетевого или системного администратора встает вопрос об ограничении скорости либо приоритизации определенных типов трафика в условиях ограниченной полосы пропускания:

- трафик, чувствительный к времени задержки (delay):
- трафик, чувствительный к колебаниям времени задержки (jitter)
- трафик, чувствительный к потерям (packet loss)
- также требуется выделять гарантированную полосу пропускания

Немного теории

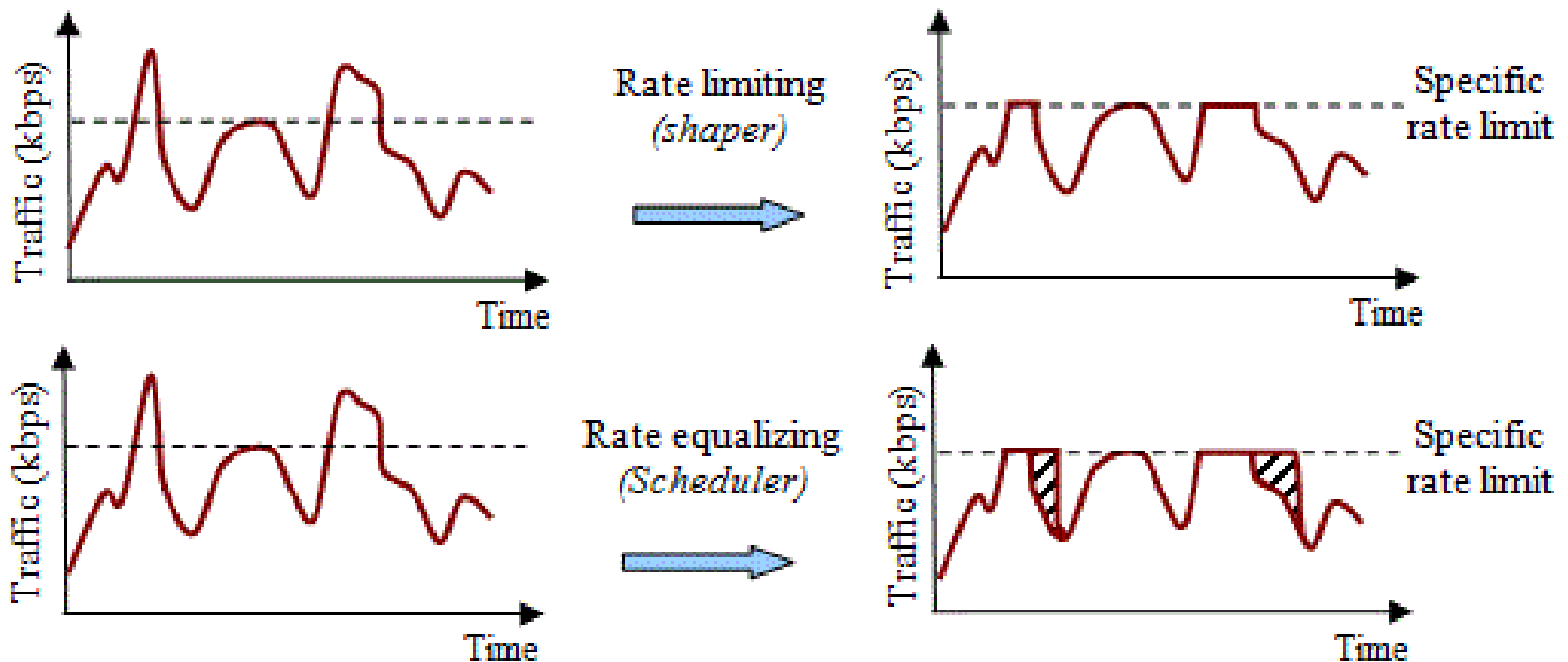
- Какой трафик мы можем приоритизировать?
- Только исходящий, на входящий мы повлиять не можем 😊

Немного теории

- Приоритизация – это буферизация трафика с отбрасыванием (drop) тех пакетов/кадров, которые имеют низкий приоритет
- То есть мы не переставляем порядок следования пакетов/кадров!
- Задержка при прохождении пакета/кадра через буфер зависит от его размера: чем больше размер буфера, тем меньше мы отбрасываем трафика, но тем больше задержка, и наоборот. Подбирается экспериментально

Немного теории

Shaping vs Scheduling

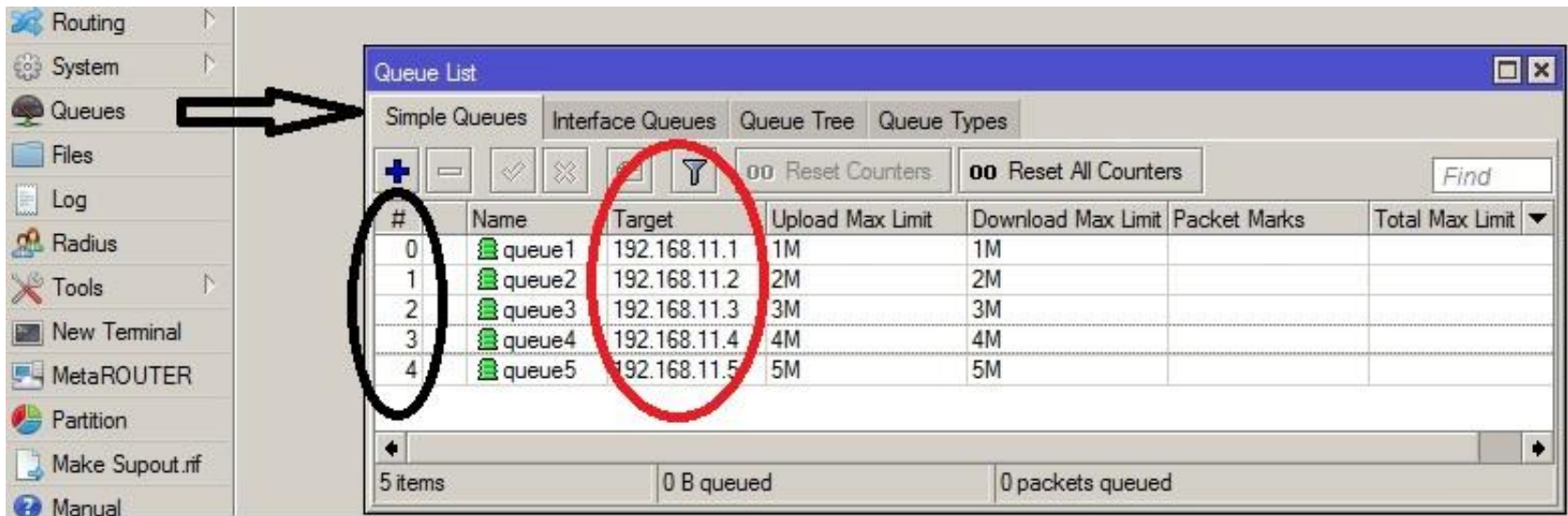


QoS в RouterOS

- В MikroTik RouterOS существует 2 подхода к реализации QoS:
- **Simple queues** (простые очереди)
- **Queue tree** (дерево очередей)

QoS в RouterOS

- Simple queues (простые очереди)



The screenshot shows the Mikrotik WinBox interface. On the left sidebar, the 'Queues' menu item is highlighted with a black arrow. The main window displays the 'Queue List' configuration page, with the 'Simple Queues' tab selected. A table lists five queues, with the first column (IDs 0-4) circled in black and the 'Target' column circled in red.

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit
0	queue1	192.168.11.1	1M	1M		
1	queue2	192.168.11.2	2M	2M		
2	queue3	192.168.11.3	3M	3M		
3	queue4	192.168.11.4	4M	4M		
4	queue5	192.168.11.5	5M	5M		

At the bottom of the window, the status bar shows: 5 items, 0 B queued, 0 packets queued.

QoS в RouterOS

- **Simple queues** (простые очереди):
- Обработка в порядке следования
- Простота, удобство конфигурирования
- Возможность обойтись без **packet mark** (target)
- Хорошо обрабатываются многоядерными процессорами (семейство роутеров CCR)
- Типичное применение: ограничение скорости для конкретных пользователей по их IP-адресу

QoS в RouterOS

The screenshot displays the MikroTik WinBox interface for configuring PPP. The left sidebar shows the navigation tree with 'Tools' expanded. The main window is titled 'PPP' and contains several tabs: 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', 'Active Connections', and 'L2TP Secrets'. The 'Secrets' tab is active, showing a table with one entry: 'user' with a password of '*****', service 'any', and profile '10M'. Below this, the '10M' profile is selected, and the 'Limits' tab is active. The 'Limits' tab shows a 'Rate Limit (p/x/b)' of '10m/10m' circled in black. Other tabs in the profile window include 'General', 'Protocols', 'Queue', and 'Scripts'. The 'Queue' tab is also visible, showing a 'Rate Limit (p/x/b)' of '10m/10m' circled in black. The 'Limits' tab also shows 'Session Timeout' and 'Idle Timeout' fields, and a 'Only One' section with radio buttons for 'no', 'yes', and 'default' (selected).

Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
user	*****	any		10M	10.0.0.1	10.0.0.2	

1 item

PPP Secret <user>

Name: user
Password: *****
Service: any
Caller ID:
Profile: 10M
Local Address: 10.0.0.1
Remote Address: 10.0.0.2
Routes:
Limit Bytes In:
Limit Bytes Out:
Last Logged Out:

PPP Profile <10M>

General Protocols Limits Queue Scripts

Session Timeout:
Idle Timeout:
Rate Limit (p/x/b): 10m/10m
Only One
☐ no ☐ yes ☒ default

QoS в RouterOS

- Queue Tree (дерево очередей)

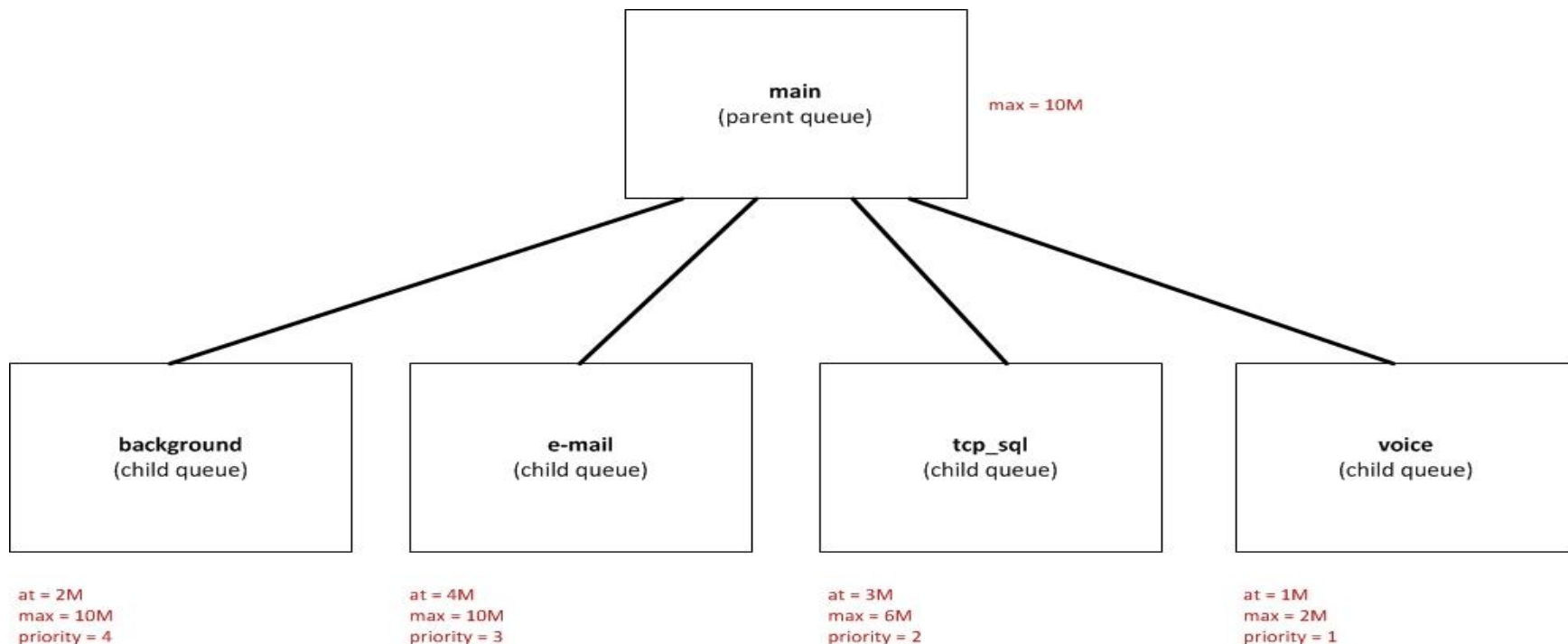
The screenshot shows the Mikrotik WinBox interface with the 'Queue List' window open. The 'Queue Tree' tab is selected. A table lists the queue configuration:

Name	Parent	Packet Marks	Priority	Limit At (b...	Max Limit ...	Avg. R...	Queued Bytes	Bytes	Pack
main	global		8	8	10M	0 bps	0 B	0 B	
background	main	background	8	2M	10M	0 bps	0 B	0 B	
e-mail	main	e-mail	3	4M	10M	0 bps	0 B	0 B	
tcp_sql	main	tcp_sql	2	3M	6M	0 bps	0 B	0 B	
voice	main	voice	1	1M	3M	0 bps	0 B	0 B	

Annotations on the screenshot include a black circle around the 'Packet Marks' column, a red oval around the 'Priority' column, a green oval around the 'Limit At (b...' column, and a blue oval around the 'Max Limit ...' column. The status bar at the bottom indicates '5 items', '0 B queued', and '0 packets queued'.

QoS в RouterOS

- Queue Tree (дерево очередей)



Limit at = CIR (committed information rate) = гарантированная скорость

Max limit = MIR (maximum information rate) = максимальная скорость

Классификация и маркировка

- Для того, чтобы трафик попал в очередь, нужно его выделить и промаркировать специальной меткой
- В RouterOS есть 3 типа виртуальных меток, которые существуют только внутри ОС, не выходя за пределы роутера:
 - mark connection
 - mark routing (policy routing)
 - mark packet (QoS)
- Маркируем трафик мы в таблице Mangle:
/ip firewall mangle

Классификация и маркировка

- Классифицируем

New Mangle Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

Any. Port:

P2P:

In. Interface: ether1-master-local

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

enabled

- Маркируем

New Mangle Rule

General Advanced Extra Action Statistics

Action: mark packet

Log

Log Prefix:

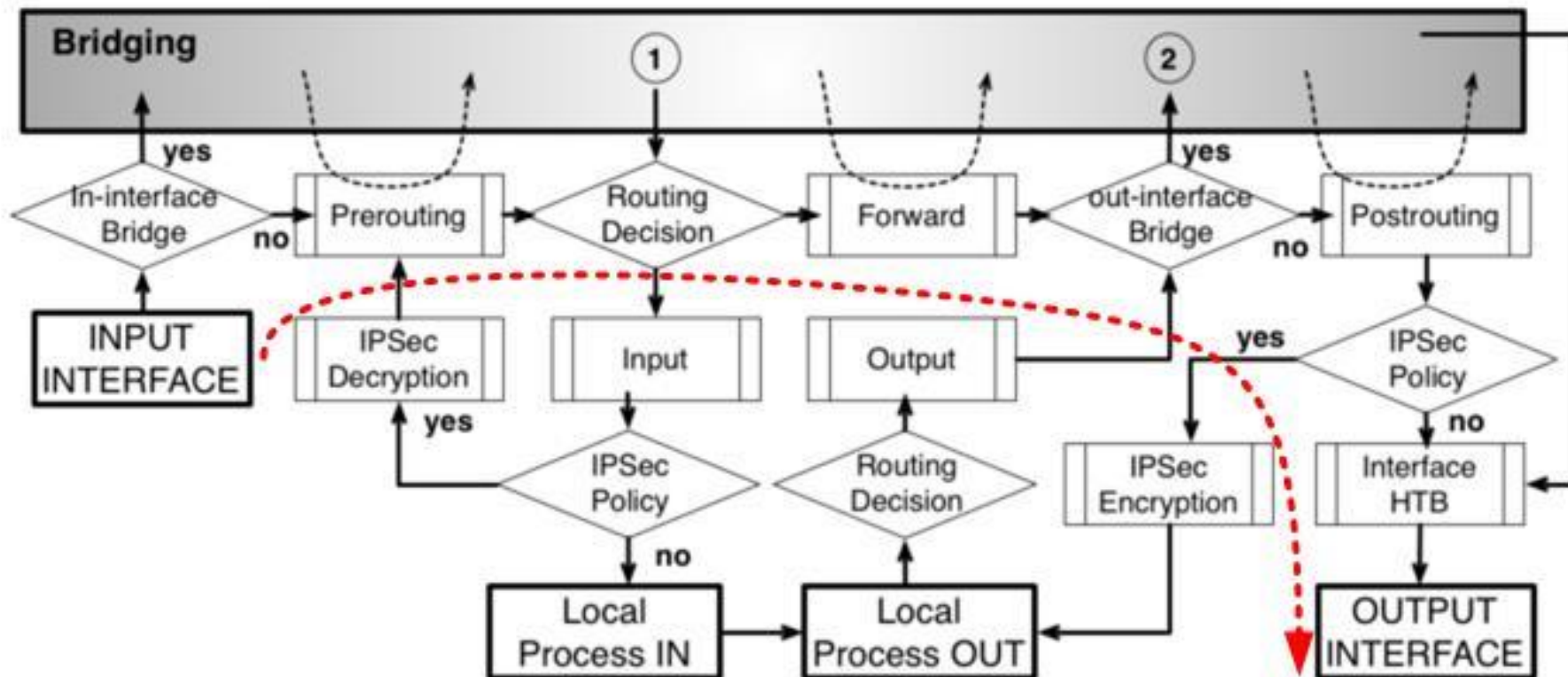
New Packet Mark: http

Passthrough

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

enabled

Fasttrack



Fasttrack

New Firewall Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol: ☐ udp

Src. Port:

Dst. Port: 5060,5061

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

New Firewall Rule

General Advanced Extra Action Statistics

Action: fasttrack connection

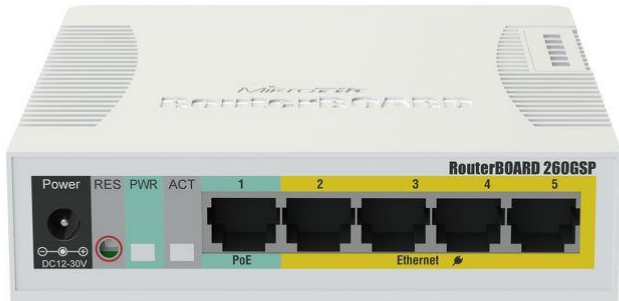
☐ Log

Log Prefix:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

QoS в SwOS



QoS в SwOS

Ingress Shaping (ограничение входящей скорости на порту) делается через ACL

MikroTik SwOS Logout

Link SFP Forwarding Statistics VLAN VLANs Static Hosts Hosts SNMP ACL System

From: ☐1☐2☐3☒4☐5 SFP

MAC Src:

VLAN:

IP Src:

MAC Dst:

VLAN ID:

IP Dst:

Условия

Ethertype: hex

Priority:

Protocol:

DSCP:

☐ Redirect To ☐1☐2☐3☐4☐5 SFP

☐ Mirror

Rate:

Действия

Set VLAN ID:

Priority:

From: ☐1☐2☐3☒4☐5 SFP

MAC Src:

VLAN:

IP Src:

MAC Dst:

VLAN ID:

IP Dst:

Ethertype: hex

Priority:

Protocol:

DSCP:

☐ Redirect To ☐1☐2☐3☐4☐5 SFP

☐ Mirror

Rate:

Set VLAN ID:

Priority:

Порядок следования правил имеет значение!

QoS в SwOS

	Port1	Port2
Forwarding		
From Port 1	☐	☒
From Port 2	☒	☐
From Port 3	☒	☒
From Port 4	☒	☒
From Port 5	☒	☒
From SFP	☒	☒
Port Lock		
Port Lock	☐	☐
Lock On First	☐	☐
Port Mirroring		
Mirror Ingress	☐	☐
Mirror Egress	☐	☐
Mirror To	☒	☐
Bandwidth Limit		
Egress Rate		30m

Чтобы ограничить скорость исходящего (egress) трафика, заходим на закладку Forwarding

Тем самым можно делать простые политики QoS средствами коммутатора, не нагружая маршрутизатор очередями simple queue или queue tree!

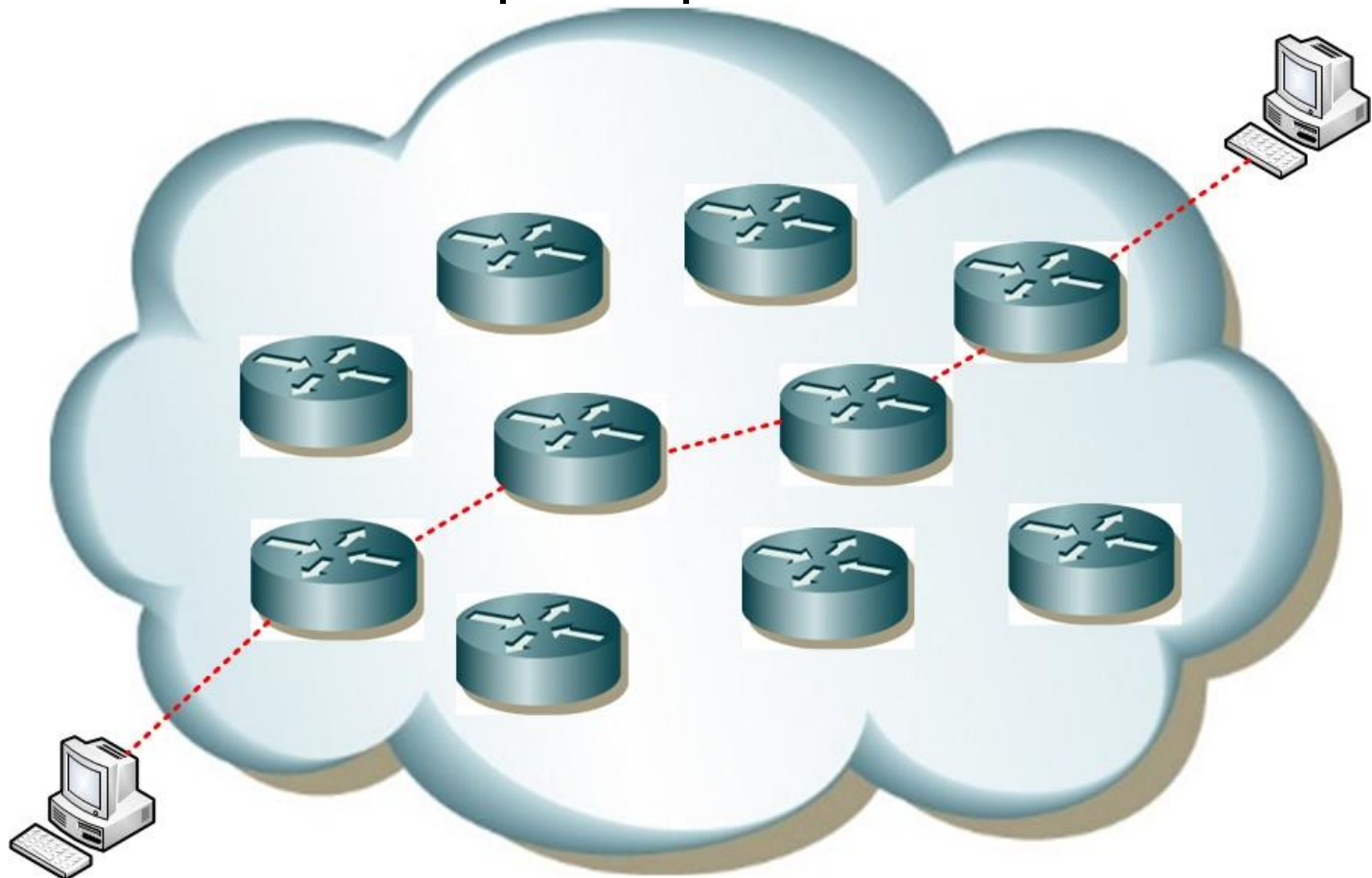
Еще один плюс использования ACL на коммутаторе – коммутатор применяет политики к трафику на скорости порта!

VLAN Priority и поле DSCP

- Как приоритезировать трафик в сети? На основании каких параметров?
- На 2-м уровне в Ethernet-кадре может присутствовать VLAN tag, а в этом tag'е, помимо VLAN ID, есть поле Priority (0-7). Обработывается данное поле коммутаторами
- На 3-м уровне в заголовках IP-пакета есть поле DSCP (0-63), обрабатывается преимущественно маршрутизаторами, но и коммутаторы тоже могут его считывать

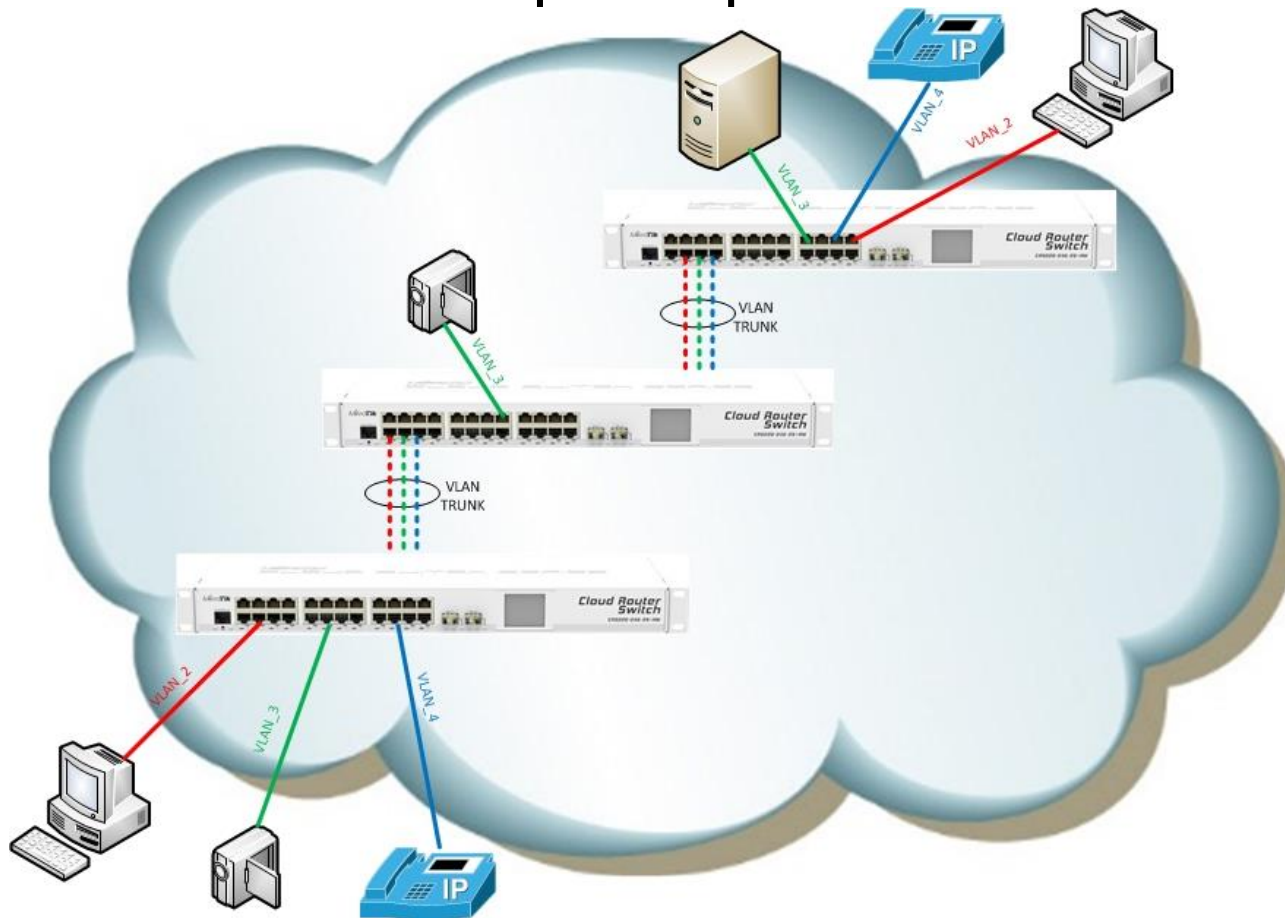
Приоритизация трафика End-to-end

- Как приоритизировать трафик через всю сеть? На основании каких параметров?



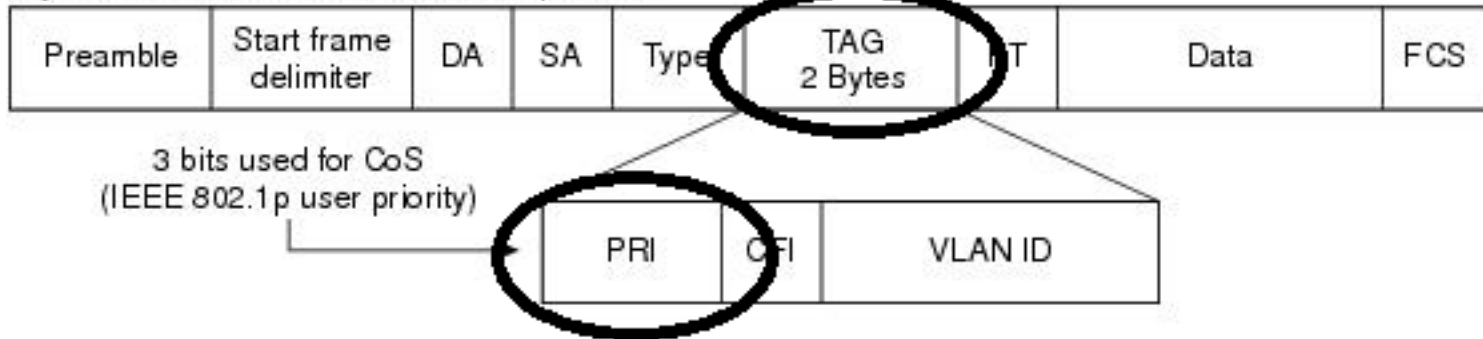
Приоритизация трафика End-to-end

- Как приоритизировать трафик через всю сеть? На основании каких параметров?

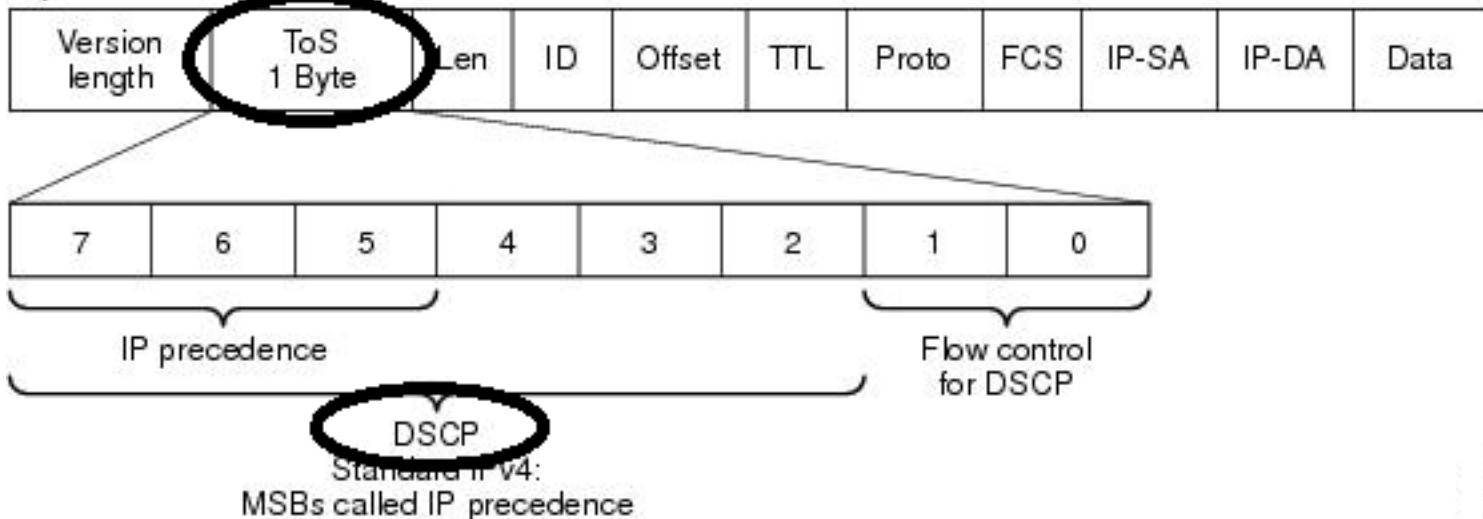


VLAN Priority и поле DSCP

Layer 2 IEEE 802.1Q and IEEE 802.1p Frame



Layer 3 IPv4 Packet

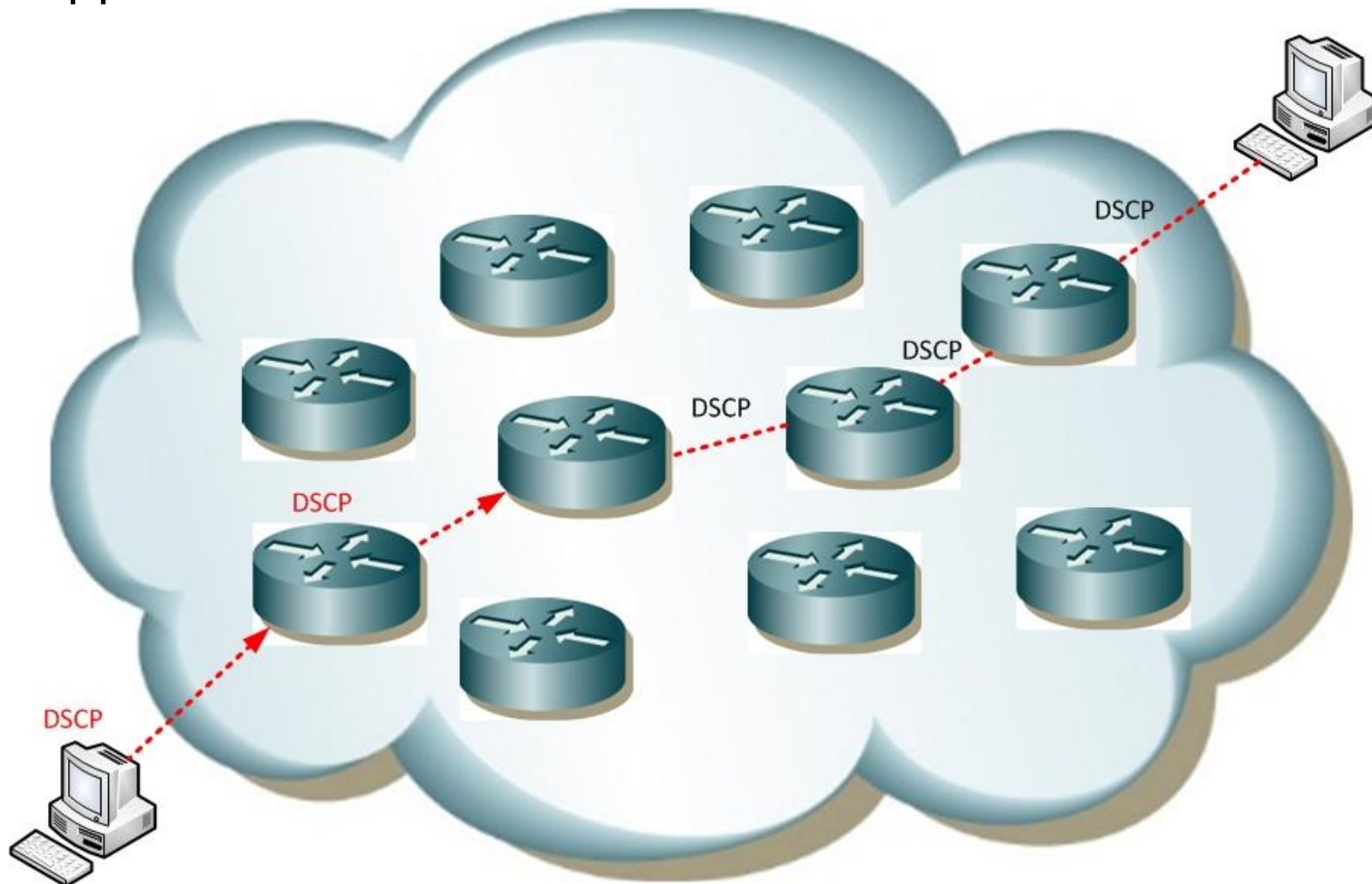


VLAN Priority и поле DSCP

- Как помечать (“красить”) трафик, подлежащий приоритизации? Ближе к источнику.
- На 2-м уровне мы можем на коммутаторе изменить VLAN Priority для трафика, входящего в порт, дальше этот трафик пойдет по сети тэгированным (это надо учитывать)
- На 3-м уровне можно изменить поле DSCP, в MS Windows это делается гибко через “QoS на основе политик” (если компьютер не в домене, то нужно править реестр ☺)

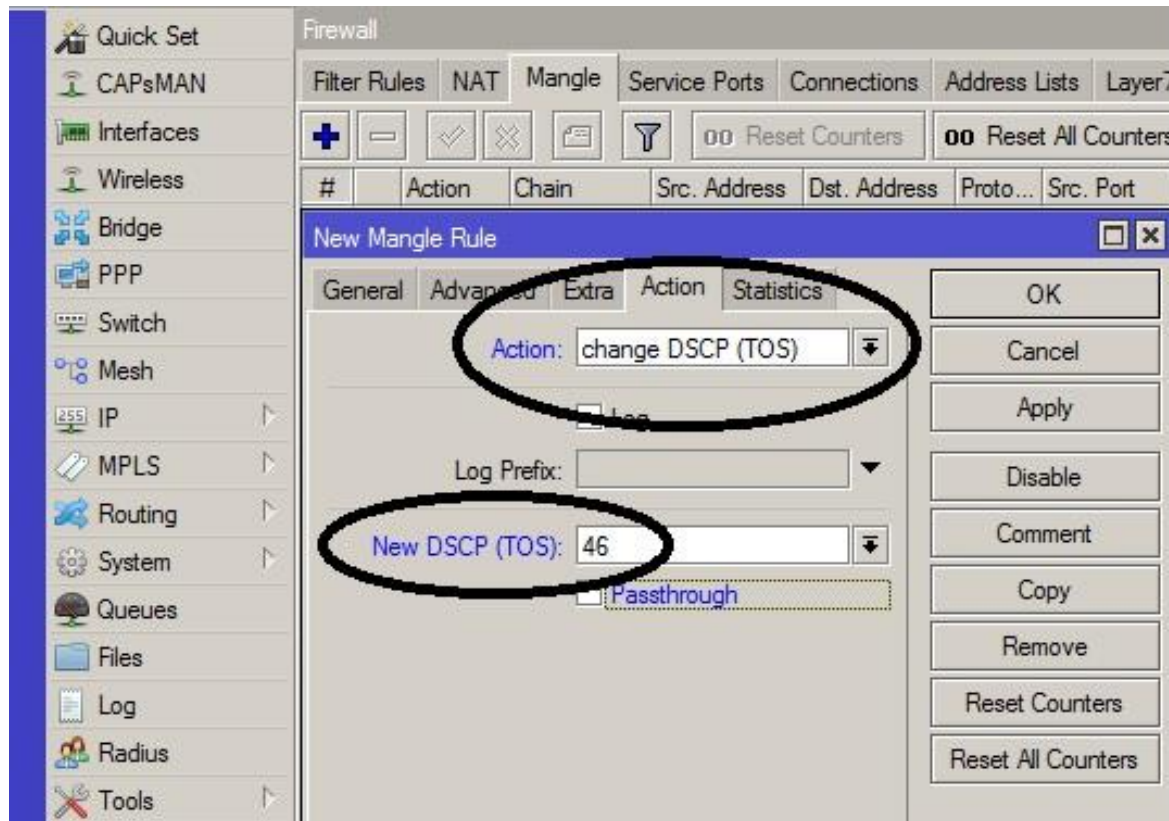
VLAN Priority и поле DSCP

- Где можно изменить поле DSCP в пакете?

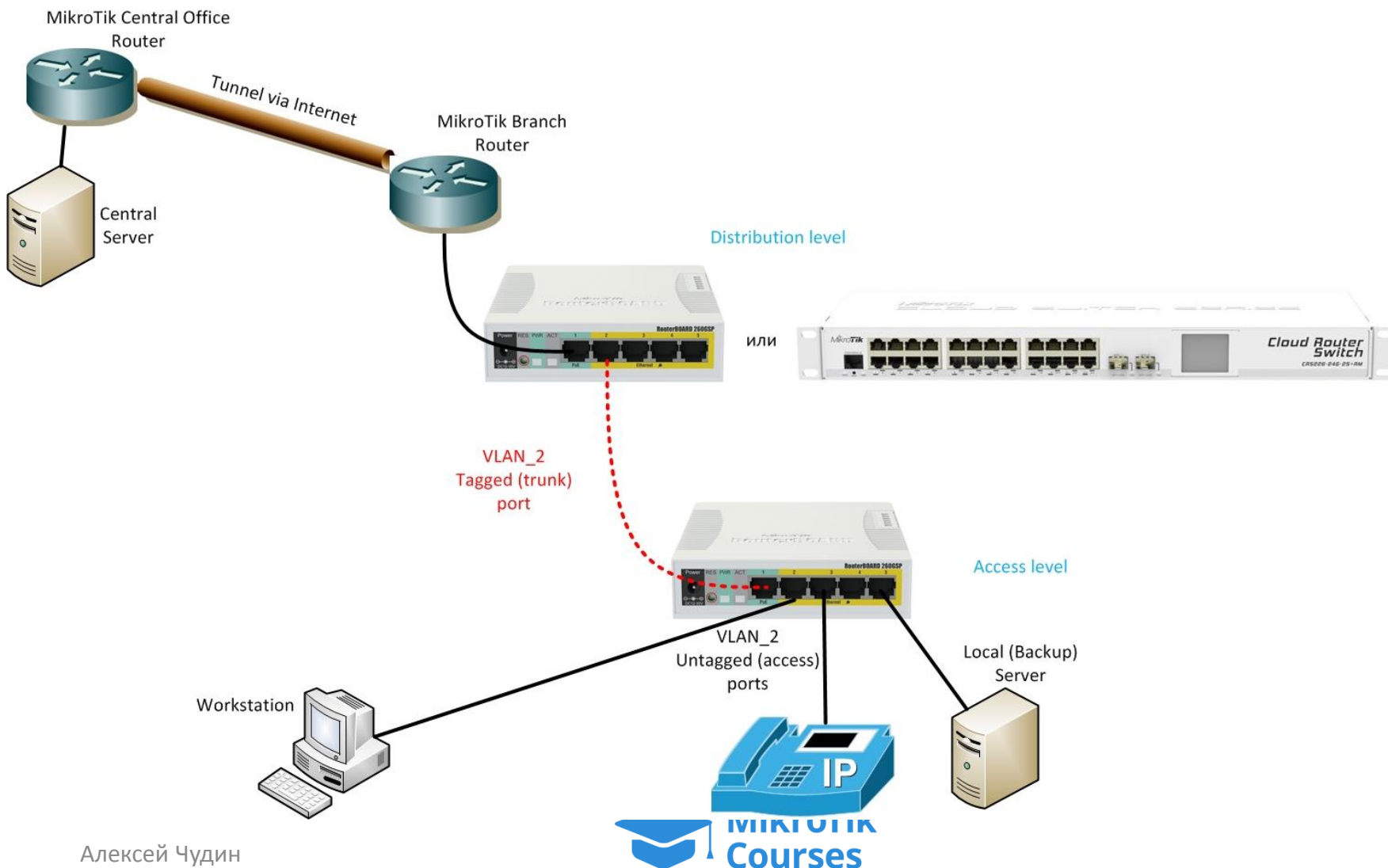


VLAN Priority и поле DSCP

- Где можно изменить поле DSCP в пакете?
- В таблице **/ip firewall mangle**:



VLAN Priority и поле DSCP



Коммутаторы серии CRS



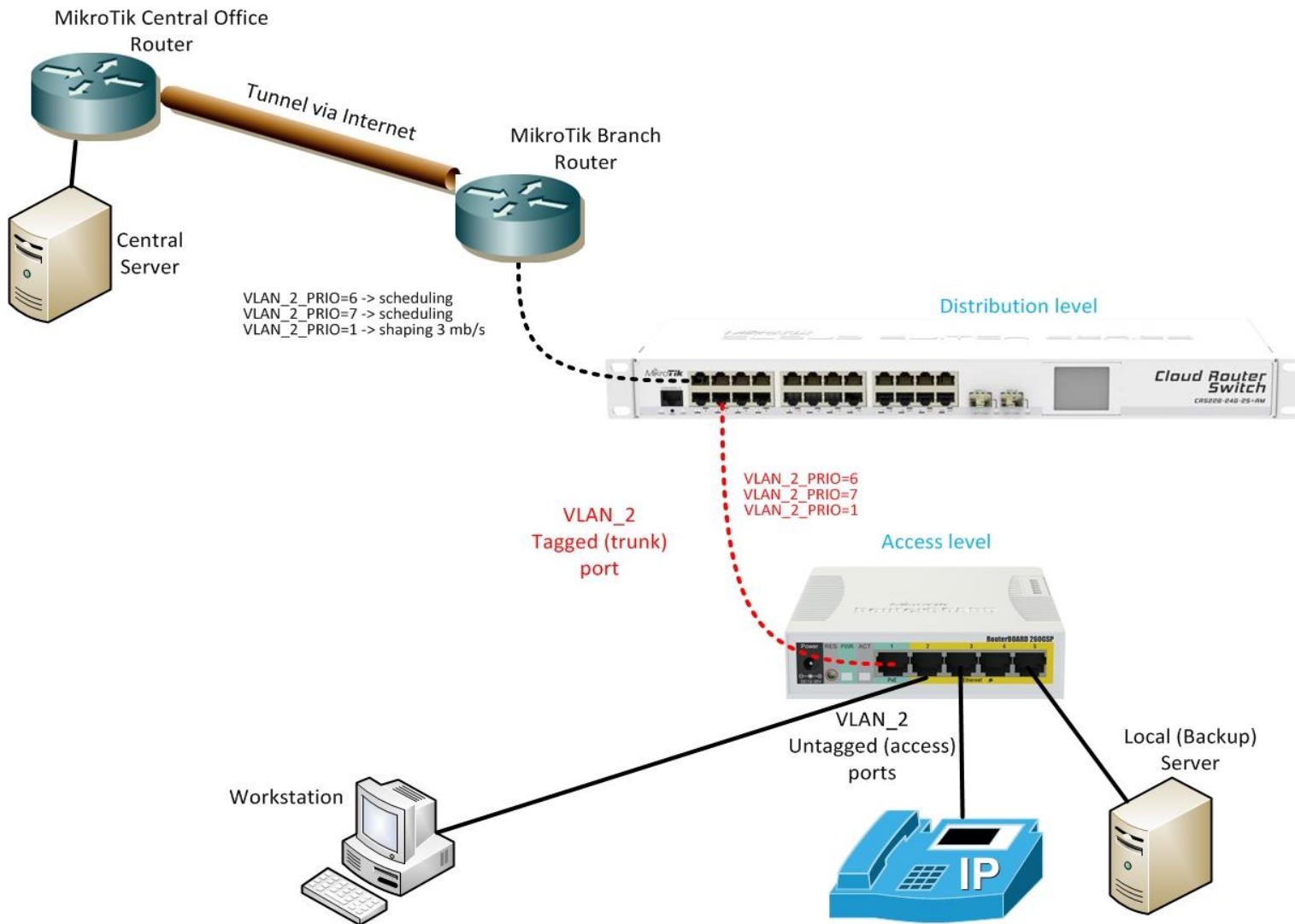
QoS на коммутаторах серии CRS

- Коммутаторы серии CRS обладают огромными возможностями и работают под управлением RouterOS
- Каждый порт можно отвязать от switch-chip'а и сделать независимым (маршрутизирующим)
- Доступны разные модели для разных задач (только с SFP-портами, комбинированные SFP/Gigabit Ethernet, с WLAN)
- В плане QoS коммутаторы CRS позволяют делать политики более гибкими, чем в SwOS

QoS на коммутаторах серии CRS

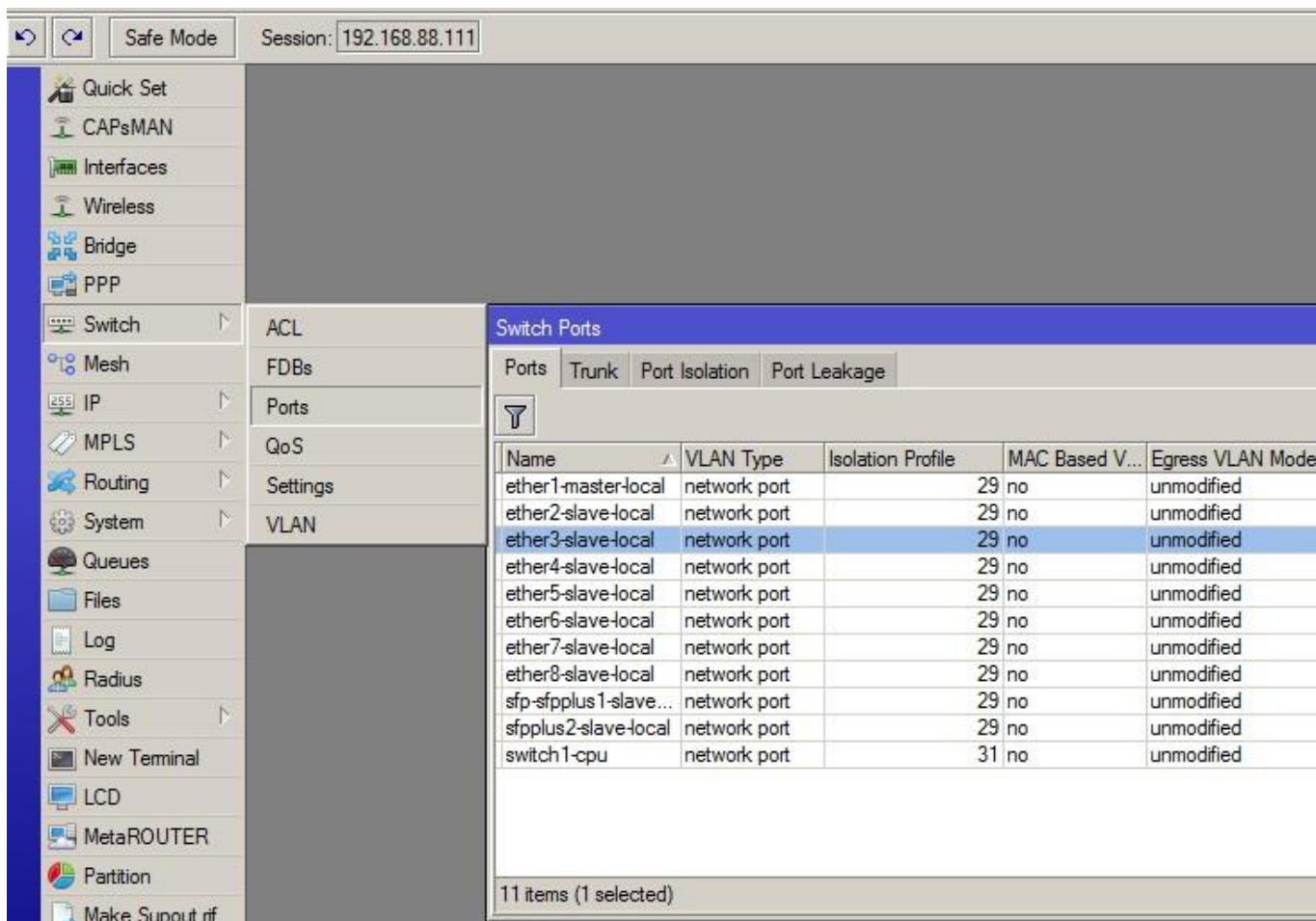
- На каждом порту коммутатора есть 8 очередей: queue7 имеет высший приоритет, queue0 – низший. Очереди применяются к трафику, выходящему из порта (egress).
- Как уже говорилось выше, существует 2 подхода к QoS: shaping и scheduling. Shaping жестко ограничивает скорость трафика, Scheduling приоритизирует трафик

QoS на коммутаторах серии CRS



QoS на коммутаторах серии CRS

Настройка ingress-порта (опускаем настройку VLAN 😊):



The screenshot shows the Mikrotik WinBox interface. The left sidebar contains a tree view with categories like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, LCD, MetaROUTER, Partition, and Make Supout.rif. The 'Switch' category is expanded, showing sub-items: ACL, FDBs, Ports, QoS, Settings, and VLAN. The 'Ports' sub-item is selected, and the 'Switch Ports' tab is active. The table below shows the configuration for 11 ports, with 'ether3-slave-local' selected.

Name	VLAN Type	Isolation Profile	MAC Based V...	Egress VLAN Mode
ether1-master-local	network port	29	no	unmodified
ether2-slave-local	network port	29	no	unmodified
ether3-slave-local	network port	29	no	unmodified
ether4-slave-local	network port	29	no	unmodified
ether5-slave-local	network port	29	no	unmodified
ether6-slave-local	network port	29	no	unmodified
ether7-slave-local	network port	29	no	unmodified
ether8-slave-local	network port	29	no	unmodified
sfp-sfpplus 1-slave...	network port	29	no	unmodified
sfpplus2-slave-local	network port	29	no	unmodified
switch1-cpu	network port	31	no	unmodified

11 items (1 selected)

QoS на коммутаторах серии CRS

Настройка ingress-порта:

Switch Port <ether3-slave-local>

Generic Ingress VLAN Egress VLAN Mirroring **QoS** Queues TPIDs Counters

QoS Scheme Precedence: **pcp based**

☐ Change DEI
☐ Change PCP
☐ Change DSCP

☒ DSCP Based DSCP to DSCP Mapping

PCP&DEI Map Drop Precedence: 0-15:green

PCP&DEI Map DSCP: 0-15:0

PCP&DEI Map Dei: 0-15:0

PCP&DEI Map PCP: 0-15:0

PCP&DEI Map Priority: 1:1
6:6
7:7

OK
Cancel
Apply

QoS на коммутаторах серии CRS

Настройка egress-порта (scheduling):

The screenshot shows the Mikrotik WinBox interface for configuring a switch port. The window title is 'Switch Port <ether2-slave-local>'. The 'Queues' tab is selected, showing the following configuration:

Priority To Queue:	1	6	7
1	1		
6		6	
7			7

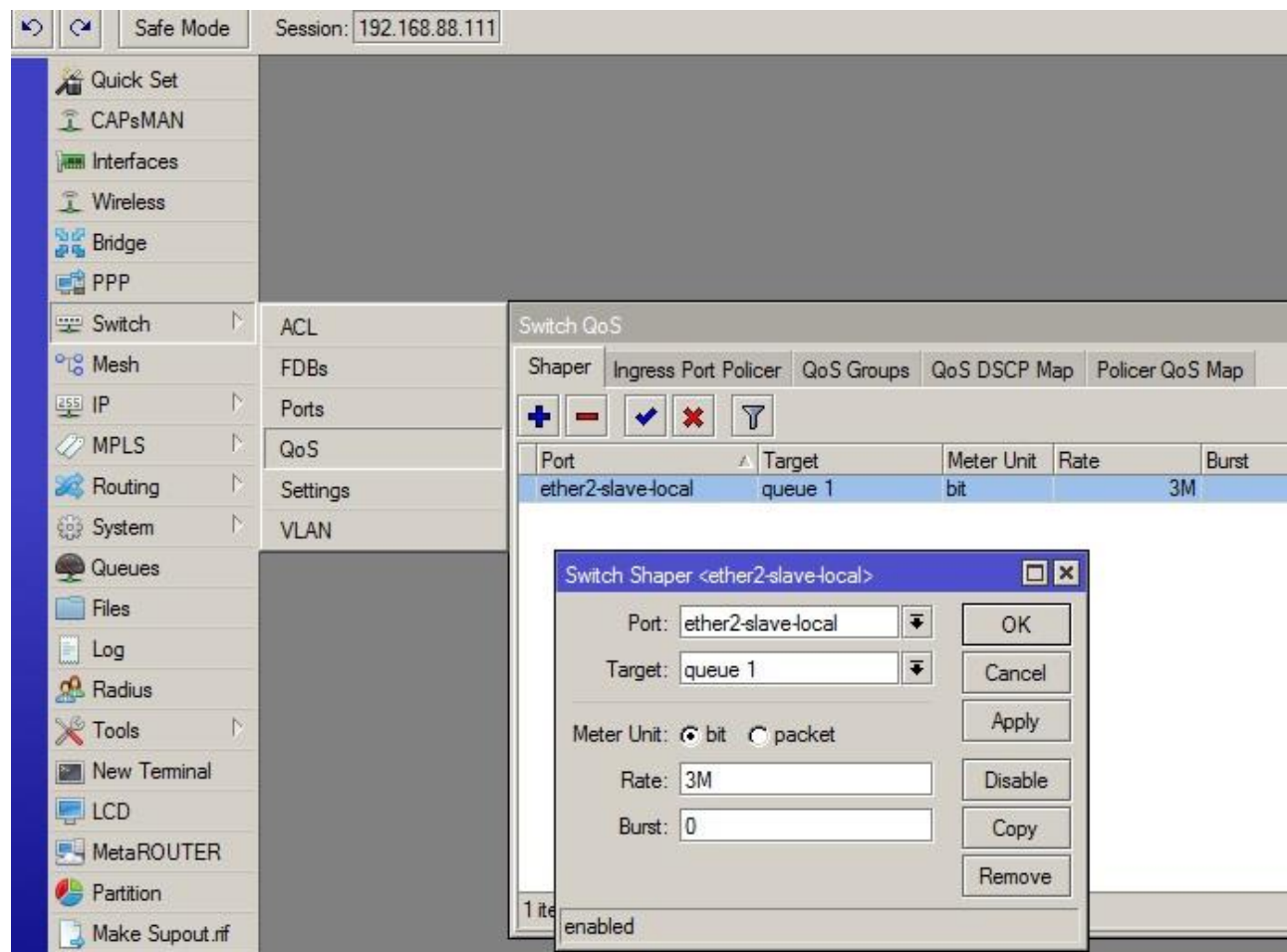
Per Queue Scheduling:

Queue	Scheduling	Priority	Weight
1	strict priority		
2	strict priority		
3	strict priority		
4	strict priority		
5	strict priority		
6	strict priority		
7	strict priority		
8	strict priority		

Buttons: OK, Cancel, Apply

QoS на коммутаторах серии CRS

Настройка shaper'a:



QoS на коммутаторах серии CRS

- На коммутаторах серии CRS2xx, а также в модели CRS112-8G-4S есть мощнейший инструмент: **ACL**, позволяющий, помимо прочего, более просто и гибко создавать политики QoS.

QoS на коммутаторах серии CRS:

Настройка ingress-порта

Switch Port <ether3-slave-local>

Generic Ingress VLAN Egress VLAN Mirroring **QoS** Queues TPIDs Counters

QoS Scheme Precedence: ingress acl based

☐ Change DEI

☐ Change PCP

☐ Change DSCP

☒ DSCP Based DSCP to DSCP Mapping

PCP&DEI Map Drop Precedence: 0-15:green

PCP&DEI Map DSCP: 0-15:0

PCP&DEI Map Dei: 0-15:0

PCP&DEI Map PCP: 0-15:0

PCP&DEI Map Priority:

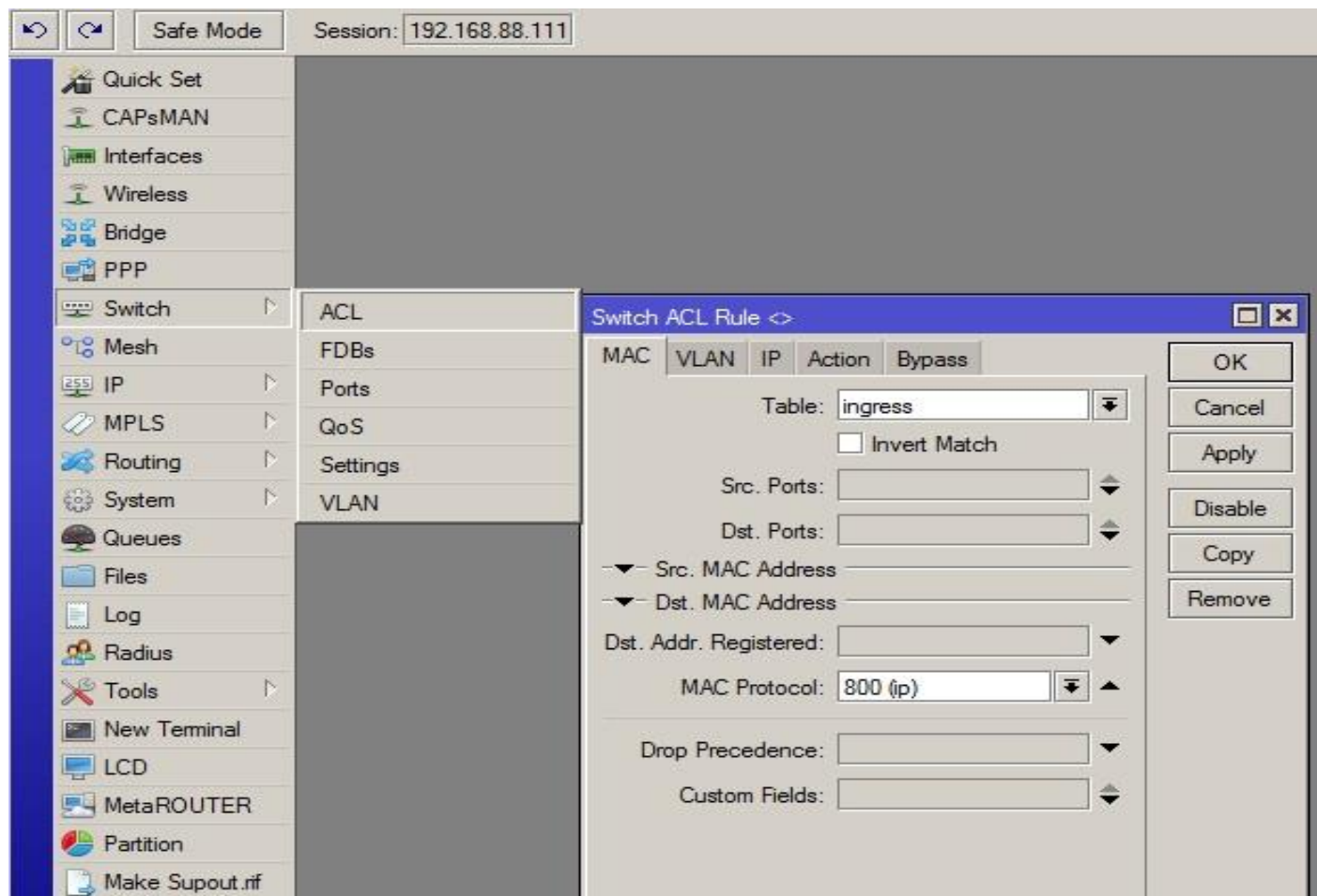
OK

Cancel

Apply

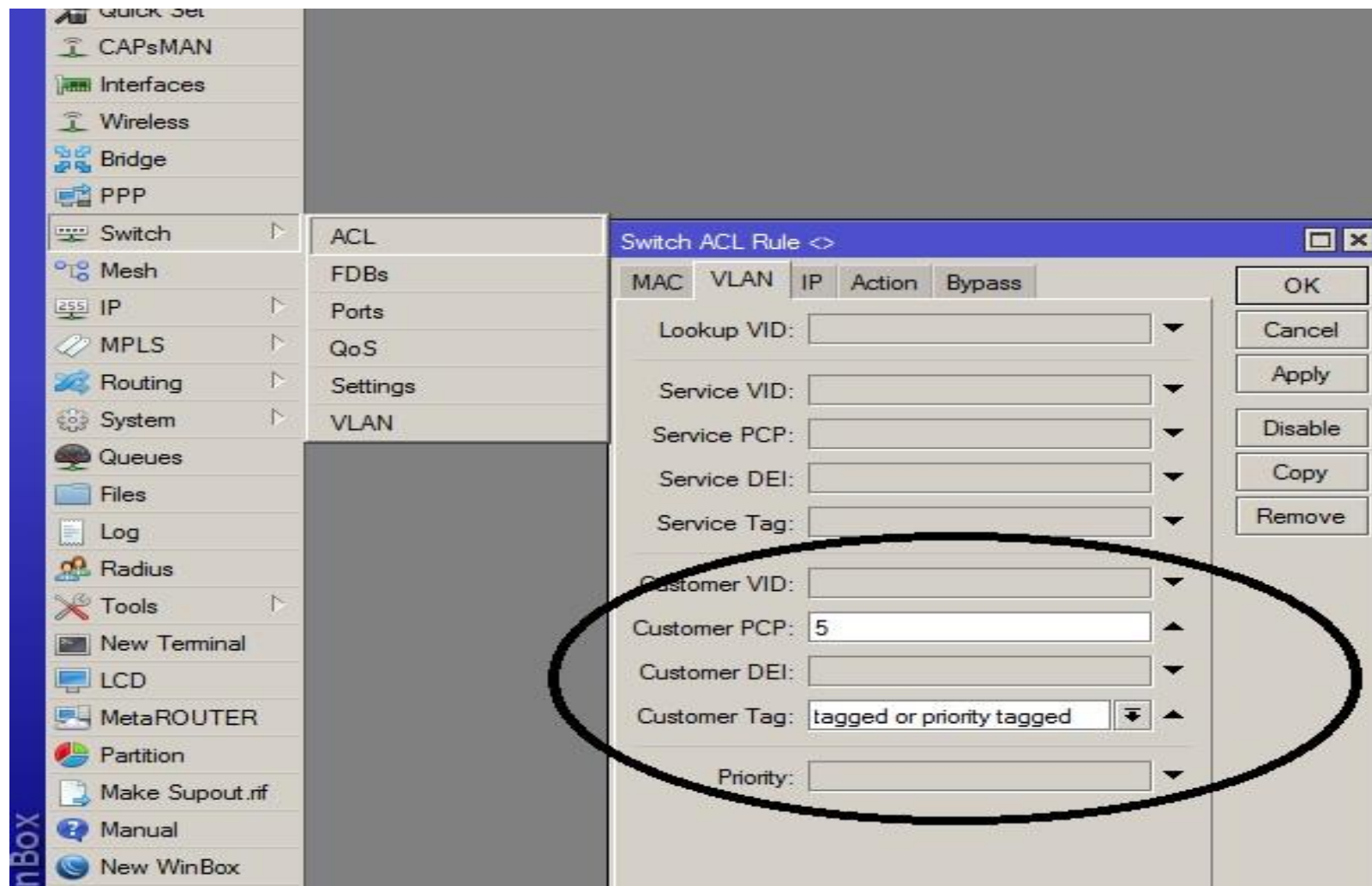
QoS на коммутаторах серии CRS:

Настройка ACL



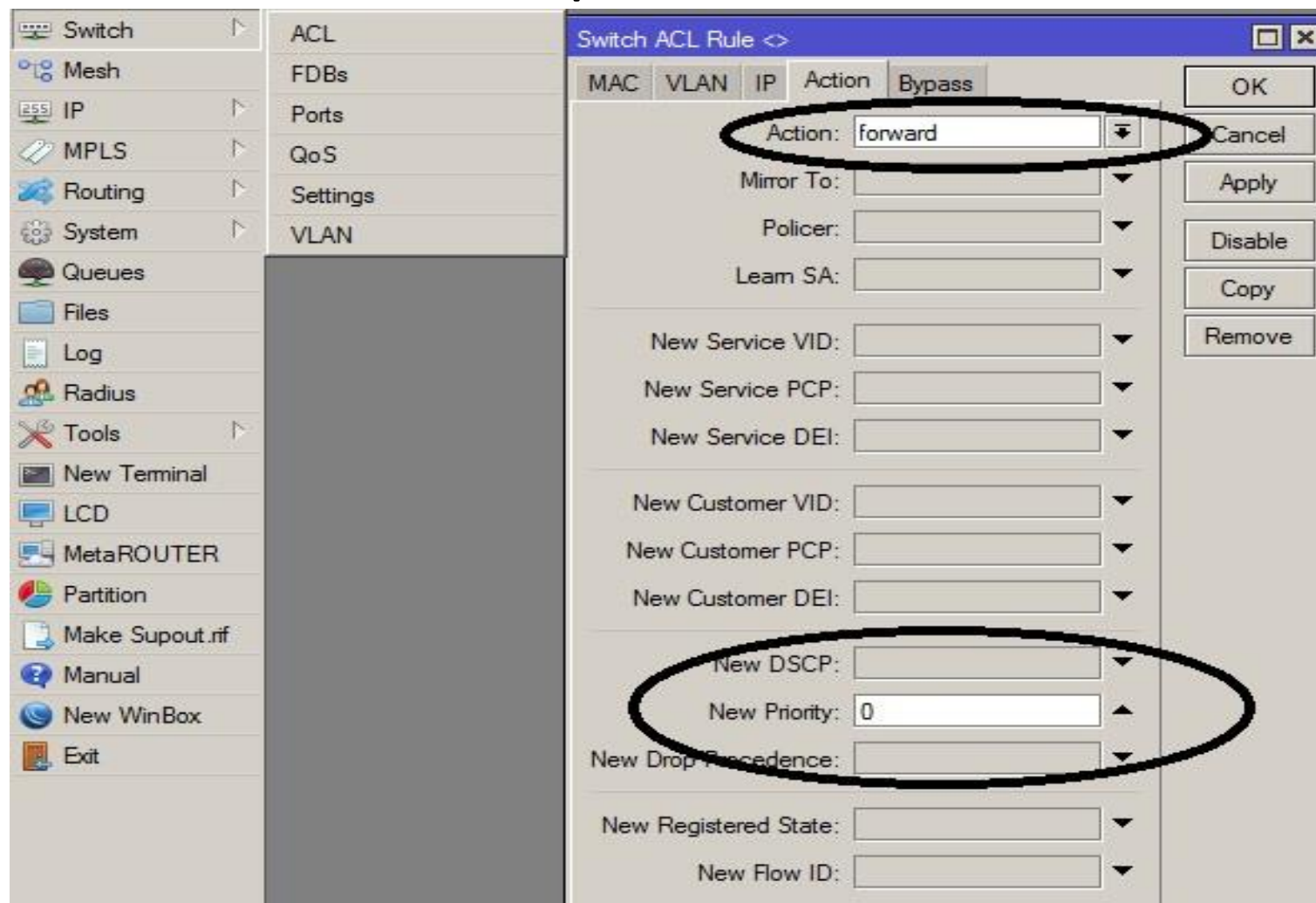
QoS на коммутаторах серии CRS:

Настройка ACL



QoS на коммутаторах серии CRS:

Настройка ACL



QoS на коммутаторах серии CRS:

Настройка ACL

The screenshot displays the MikroTik WinBox interface for configuring QoS on a CRS switch. The left sidebar shows the navigation tree with 'QoS' highlighted. The main window shows the 'Switch QoS' configuration for 'ether6-slave-local' with a target of 'queue 0', meter unit of 'bit', rate of '1M', and burst of '0'. A 'Switch Shaper' dialog box is open, showing the same configuration details.

Switch QoS Configuration:

Port	Target	Meter Unit	Rate	Burst
ether6-slave-local	queue 0	bit	1M	0

Switch Shaper Configuration:

Port: ether6-slave-local
Target: queue 0
Meter Unit: bit
Rate: 1M
Burst: 0

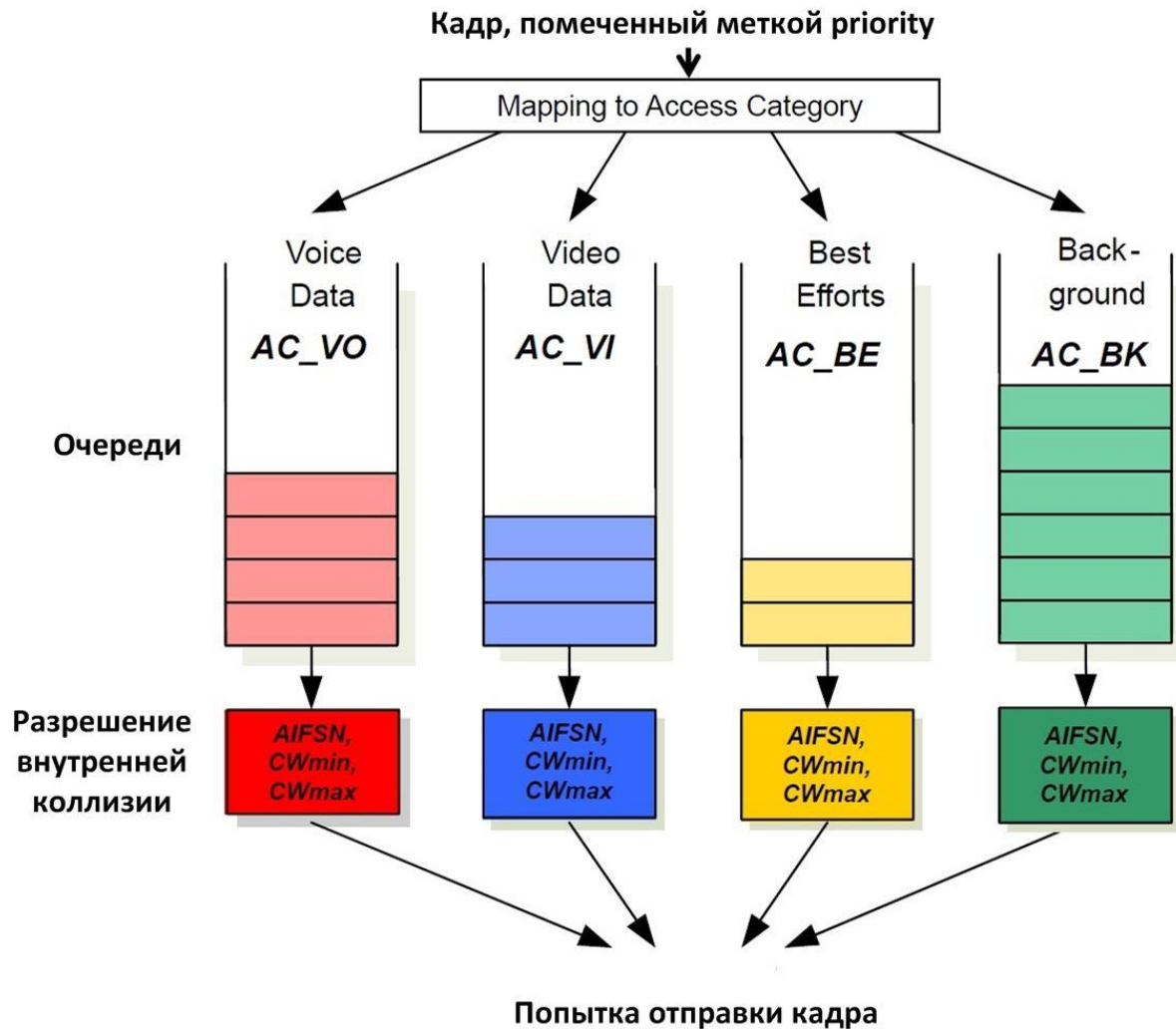
WMM (Wireless Multimedia)

- В беспроводных сетях возможна приоритизация на уровне самого протокола 802.11
- WMM позволяет разделить трафик на 4 группы, кадры из которых будут посылаться беспроводным интерфейсом с разными задержками, повышая вероятность того, что раньше с интерфейса в среду будут уходить кадры их группы с наивысшим приоритетом
- WMM не обеспечивает гарантированную полосу пропускания!

WMM (Wireless Multimedia)

Priority	User Priority (same as 802.1D user priority)	802.1D Designation	Access category (AC)	Designation (Informative)
Lowest  highest	1	BK	AC_BK	Background
	2	-	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
	7	NC	AC_VO	Voice

WMM (Wireless Multimedia)



WMM (Wireless Multimedia)

- Как включить WMM на MikroTik?

Interface: wlan1

General Wireless Data Rates Advanced HT HT MCS WDS ...

Mode: ap bridge

Band: 5GHz-A/N

Channel Width: 20/40MHz Ce

Frequency: auto MHz

SSID: MikroTik

Radio Name: 411U

Scan List: default

Wireless Protocol: any

Security Profile: profile1

Frequency Mode: regulatory-domain

Country: russia

Antenna Gain: 0 dBi

DFS Mode: none

Proprietary Extensions: post-2.9.25

WMM Support: enabled

Bridge Mode: enabled

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

☒ Default Authenticate

☒ Default Forward

☐ Hide SSID

Multicast Helper: default

☒ Multicast Buffering

☒ Keepalive Frames

enabled running slave running ap

WMM (Wireless Multimedia)

- Где мы ставим метку **Priority**?
- **/ip firewall mangle**
- **/interface bridge filter**
- Action в обоих случаях тот же: **set priority**

WMM (Wireless Multimedia)

Bridge Filter Rule <>

General Advanced ARP STP Action ...

Chain: forward

OK Cancel Apply Enable Comment Copy Remove Reset Counters Reset All Counters

Interfaces

In. Interface: ether1

Out. Interface: wlan1

Bridges

In. Bridge:

Out. Bridge:

Src. MAC Address

Dst. MAC Address

MAC Protocol

MAC Protocol-Num: 800 (ip) hex

IP

Src. Address:

Src. Port:

Dst. Address:

Dst. Port:

Protocol: 1 (icmp)

Packet Mark

Ingress Priority

disabled

Bridge Filter Rule <>

Advanced ARP STP Action Statistics ...

Action: set priority

Log

Log Prefix:

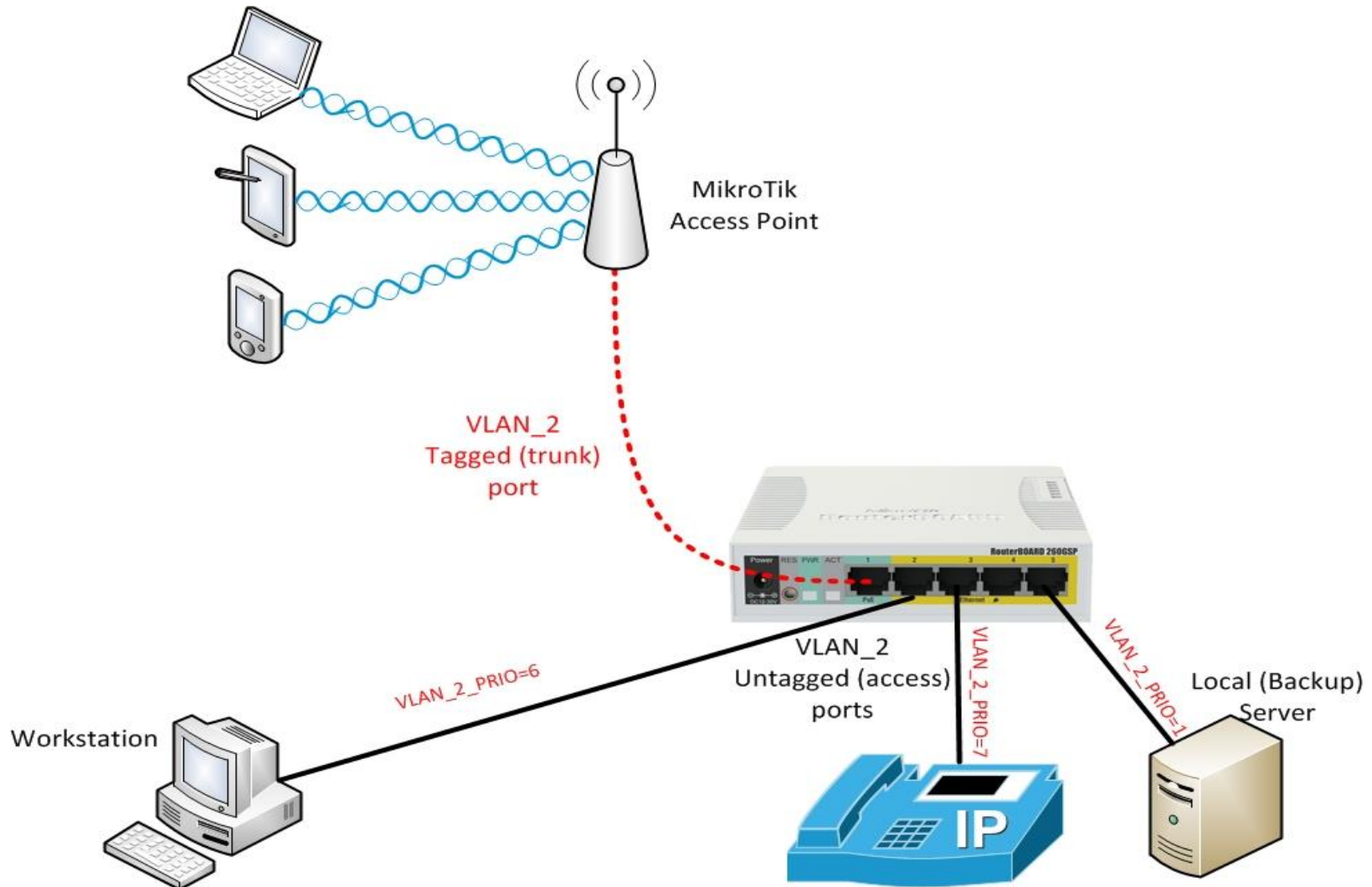
New Priority: 7

Passthrough

OK Cancel Apply Enable Comment Copy Remove Reset Counters Reset All Counters

disabled

VLAN Priority и Wireless Multimedia (WMM)



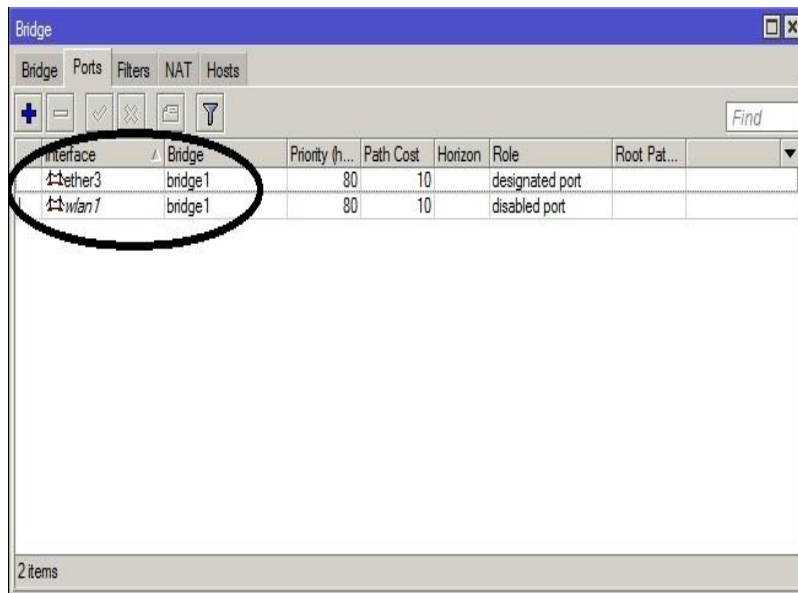
VLAN Priority и поле DSCP

From: ☐ 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 SFP	MAC Src:	MAC Dst:	Ethertype:	hex
VLAN: any	VLAN ID:	Priority:	DSCP: 45	
IP Src:	IP Dst:	Protocol:	Priority: 6	
☐ Redirect To ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 SFP	☐ Mirror	Rate:	Set VLAN ID:	

From: ☐ 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 SFP	MAC Src:	MAC Dst:	Ethertype:	hex
VLAN: any	VLAN ID:	Priority:	DSCP:	
IP Src:	IP Dst:	Protocol:	Priority: 7	
☐ Redirect To ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 SFP	☐ Mirror	Rate:	Set VLAN ID:	

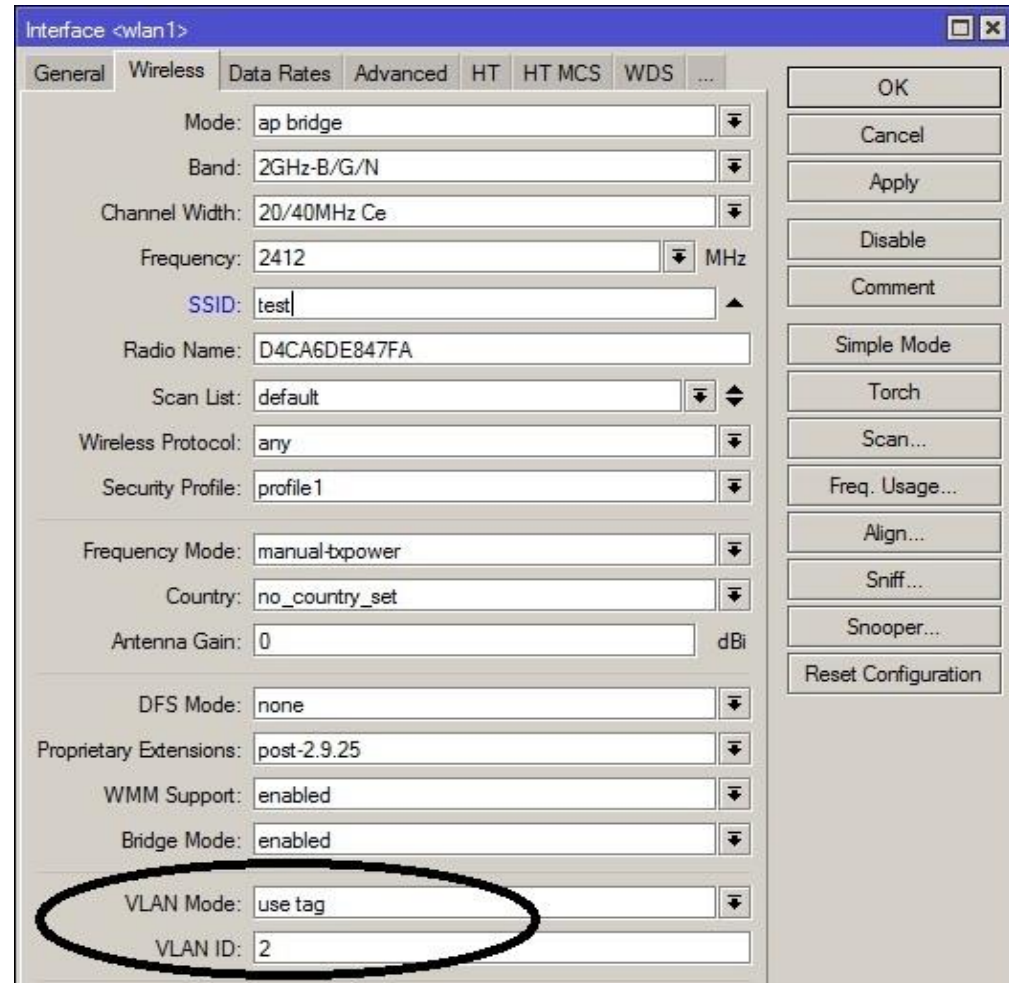
From: ☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5 SFP	MAC Src:	MAC Dst:	Ethertype:	hex
VLAN: any	VLAN ID:	Priority:	DSCP:	
IP Src:	IP Dst:	Protocol:	Priority: 1	
☐ Redirect To ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 SFP	☐ Mirror	Rate:	Set VLAN ID:	

VLAN Priority и Wireless Multimedia (WMM)



Interface	Bridge	Priority (h...)	Path Cost	Horizon	Role	Root Pat...
ether3	bridge1	80	10		designated port	
wlan1	bridge1	80	10		disabled port	

2 items



Interface <wlan1>

General Wireless Data Rates Advanced HT HT MCS WDS ...

Mode: ap bridge

Band: 2GHz-B/G/N

Channel Width: 20/40MHz Ce

Frequency: 2412 MHz

SSID: test

Radio Name: D4CA6DE847FA

Scan List: default

Wireless Protocol: any

Security Profile: profile1

Frequency Mode: manual-txpower

Country: no_country_set

Antenna Gain: 0 dBi

DFS Mode: none

Proprietary Extensions: post-2.9.25

WMM Support: enabled

Bridge Mode: enabled

VLAN Mode: use tag

VLAN ID: 2

OK Cancel Apply Disable Comment Simple Mode Torch Scan... Freq. Usage... Align... Sniff... Snooper... Reset Configuration

VLAN Priority и Wireless Multimedia (WMM)

Bridge Filter Rule <>

General Advanced ARP STP Action Statistics

Chain: **forward**

Interfaces

In. Interface:

Out. Interface:

Bridges

In. Bridge:

Out. Bridge:

Src. MAC Address

Dst. MAC Address

MAC Protocol

MAC Protocol-Num: **8100 (vlan)** hex

IP

Src. Address:

Src. Port:

Dst. Address:

Dst. Port:

Protocol:

Packet Mark

Ingress Priority

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

enabled

Bridge Filter Rule <>

General Advanced ARP STP Action Statistics

Action: **set priority**

Log

Log Prefix:

New Priority: **from ingress**

Bypass

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

enabled

Вопросы?

Пишите на

training@mikrotik-courses.ru

Приглашаю на тренинги MikroTik!

- **Иркутск:**
 - **МТСНА:** 28-30 марта
 - **МТСРЕ:** 31 марта-02 апреля

- **Владивосток:**
 - **МТСНА:** 06-08 апреля
 - **МТСТСЕ:** 11-13 апреля

<http://mikrotik-courses.ru>

Спасибо за ваше
внимание!