

RSTP/VLAN/CRS3xx

Вопросы вебинара

- STP/RSTP
- VLAN в crs3xx
 - Tag/untag/management
 - Mac on vlan / Mask Mac on VLAN
- Port base security в CRS3xx
- DHCP snooping в CRS3xx



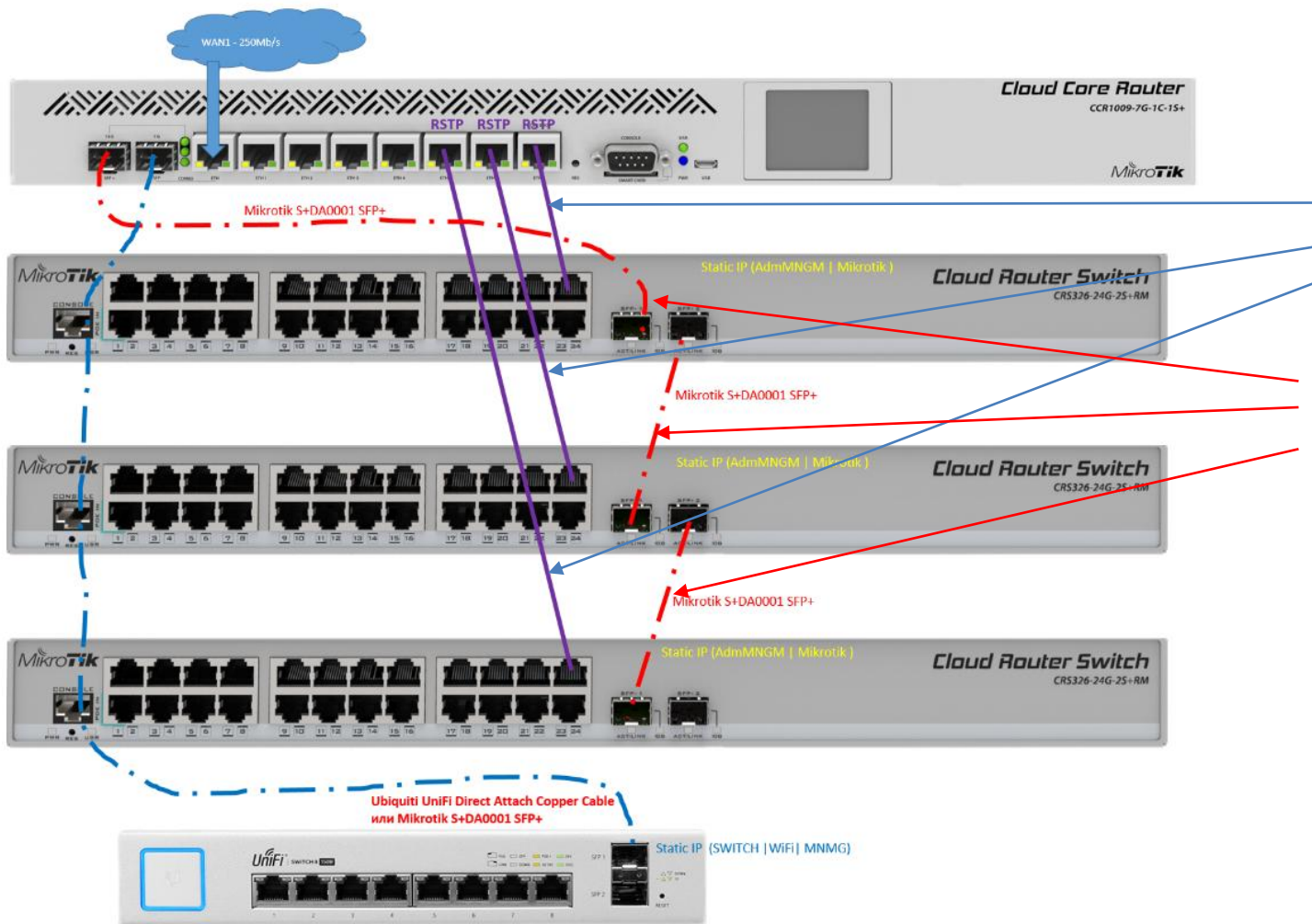
STP/RSTP

- Часто, для обеспечения стабильности работы сети в случае проблем со связью между свичами (выход порта из строя, обрыв провода), используют избыточные линки (redundant links) — дополнительные соединения.
- Если между свичами по какой-то причине не работает один линк, используем запасной. Вроде все правильно, но представим себе такую ситуацию: два свича соединены двумя проводами
- В Ethernet кадре 802.3 в отличие от пакета нет поля TTL – поэтому срок жизни кадров не ограничен и при возникновении петель коммутации вся пропускная полоса будет заполнена широковещательными кадрами

IEEE 802.3						
7	1	6	6	2	46 - 1500	4
Преамбула	Начало Разделителя Кадра	Адрес Назначения	Адрес Источника	Длина	802.2 Заголовок и Данные	Проверочная Последовательность Кадра

STP/RSTP

- (R) STP исключает возможность просмотра одних и тех же MAC-адресов на нескольких bridge портах путем отключения дополнительных портов до этого MAC-адреса
- Каждые 2 секунды коммутаторы рассылают BPDU сообщения в которых сообщают mac адрес корневого bridge, приоритет
- Первый (R) STP будет выбирать корневой мост на основе наименьшего идентификатора bridge
- Затем (R) STP будет использовать алгоритм поиска по ширине, принимая корневой мост в качестве отправной точки
- Если алгоритм достигает MAC-адреса в первый раз - он оставляет активный link
- Если алгоритм достигает MAC-адреса во второй раз - он отключает link



Отключенные
линки
Alternative port
Активные
линки
Root port

Настройка корневого bridge

Interface <bridge-local>

General STP VLAN Status Traffic

Protocol Mode: ☐ none ☐ STP ☒ RSTP ☐ MSTP

Priority: 0 hex

Region Name:

Region Revision: 0

Max Message Age: 00:00:20

Forward Delay: 00:00:15

Transmit Hold Count: 6

Max Hops: 20

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

- Настройка сводится к включению RSTP и к выбору root bridge
- По умолчанию у mikrotik значение priority = 8000(hex) = 32768
- Другие устройства могут не понимать значения с шагом отличным от 4096 (IEEE 802.1W) 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Настройка корневого bridge

Bridge Port <sfp-sfpplus2>

General STP VLAN Status

Priority: 80 hex

Path Cost: 30

Internal Path Cost: 10

Edge: auto

Point To Point: auto

☐ Auto Isolate

☐ Restricted Role

☐ Restricted TCN

☐ BPDU Guard

OK

Cancel

Apply

Disable

Comment

Copy

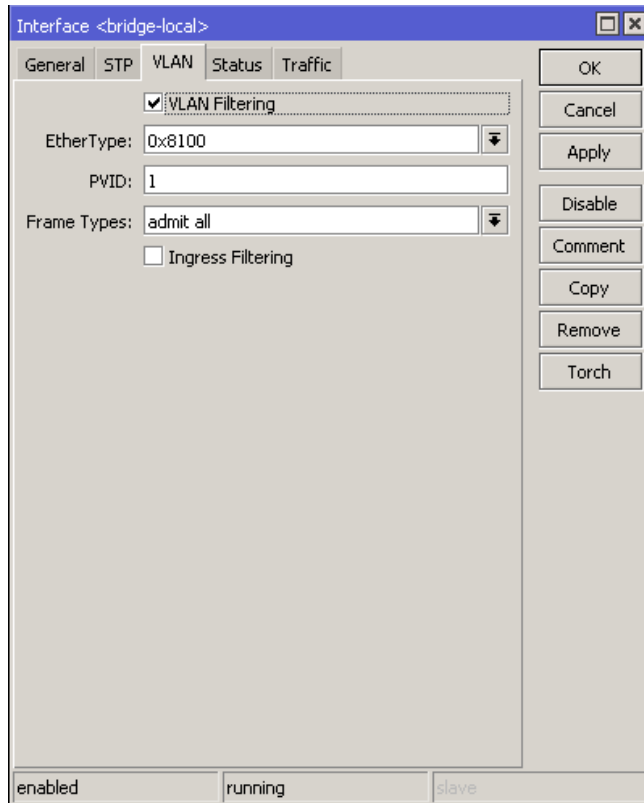
Remove

enabled inactive Hw. Offload

В RouterOS root port выбираются на основе самой низкой стоимости пути порта, самого низкого приоритета порта и самого низкого идентификатора порта моста в этом конкретном порядке:

- Port path cost (lowest)
- Port priority (lowest)
- Bridge port ID (lowest)

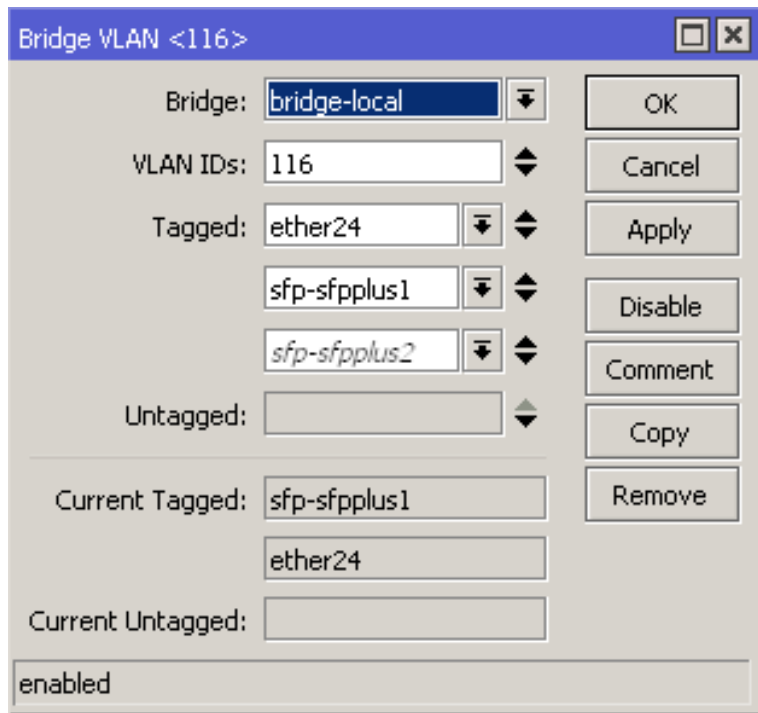
VLAN в crs3xx



- На crs3xx аппаратно можно разбирать кадры VLAN в bridge
- Для включения достаточно выбрать пункт VLAN filtering
- PVID – native vlan

VLAN в crs3xx

- Настройка тегированных vlan
- Настройка access (PVID)



Bridge VLAN <116>

Bridge:

VLAN IDs:

Tagged:

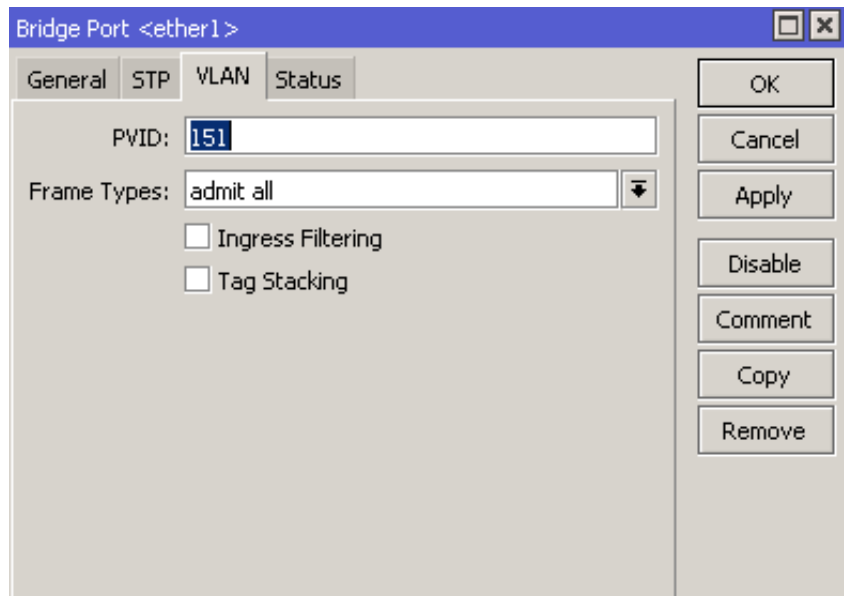
Untagged:

Current Tagged:

Current Untagged:

enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove



Bridge Port <ether1>

General STP VLAN Status

PVID:

Frame Types:

☐ Ingress Filtering

☐ Tag Stacking

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

Management VLAN в crs3xx

- Создаем VLAN интерфейс на bridge
- Добавляем bridge в vlan tagget
- Вешаем ip address на vlan интерфейс

Interface <bridge-local.17>

General Loop Protect Status Traffic

Name: bridge-local.17

Type: VLAN

MTU: 1500

Actual MTU: 1500

L2 MTU: 1588

MAC Address: B8:69:F4:28:BB:45

ARP: enabled

ARP Timeout:

VLAN ID: 17

Interface: bridge-local

☐ Use Service Tag

OK Cancel Apply Disable Comment Copy Remove Torch

Bridge VLAN <17>

Bridge: bridge-local

VLAN IDs: 17

Tagged: bridge-local, ether24, sfp-sfpplus1, sfp-sfpplus2

Untagged:

Current Tagged: bridge-local, sfp-sfpplus1, ether24

Current Untagged:

enabled

OK Cancel Apply Disable Comment Copy Remove

Mac on VLAN в crs3xx

New Switch Rule

Match

Action

Switch: switch1

Ports: ether19 ether20 ether21 ether23 ether22 ether24 sfp-sfpplus1 sfp-sfpplus2

Src. MAC Address: 0C:38:3E:21:7D:B3 / FF:FF:FF:FF:FF:FF

Dst. MAC Address:

MAC Protocol:

VLAN

IP

IP 6

OK

Cancel

Apply

Enable

Copy

Remove

New Switch Rule

Match

Action

☐ Copy To CPU

☐ Redirect To CPU

☐ Mirror

☐ Set New Dst. Ports

New Dst. Ports:

New VLAN ID: 718

New VLAN Priority:

OK

Cancel

Apply

Enable

Copy

Remove

Mac mask on VLAN в crs3xx

New Switch Rule

Match	Action
Switch: switch1	
Ports: ether20	
ether21	
ether23	
ether22	
ether24	
sfp-sfpplus1	
sfp-sfpplus2	
Src. MAC Address: 0C:38:3E:00:00:0C / FF:FF:FF:00:00:0C	
Dst. MAC Address:	
MAC Protocol:	
VLAN	
IP	
IP 6	

OK
Cancel
Apply
Disable
Copy
Remove

New Switch Rule

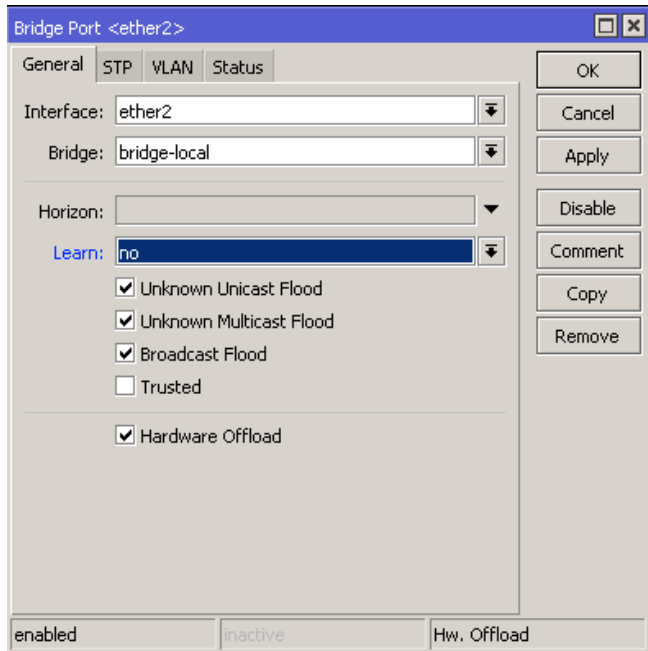
Match	Action
	<input type="checkbox"/> Copy To CPU
	<input type="checkbox"/> Redirect To CPU
	<input type="checkbox"/> Mirror
	<input type="checkbox"/> Set New Dst. Ports
New Dst. Ports:	
New VLAN ID: 718	
New VLAN Priority:	

OK
Cancel
Apply
Enable
Copy
Remove

Port base security

- Для использования порта только определенным mac address можно воспользоваться ограничением mac-адресов на порту

/interface bridge port



Bridge Port <ether2>

General STP VLAN Status

Interface: ether2

Bridge: bridge-local

Horizon:

Learn: no

☒ Unknown Unicast Flood

☒ Unknown Multicast Flood

☒ Broadcast Flood

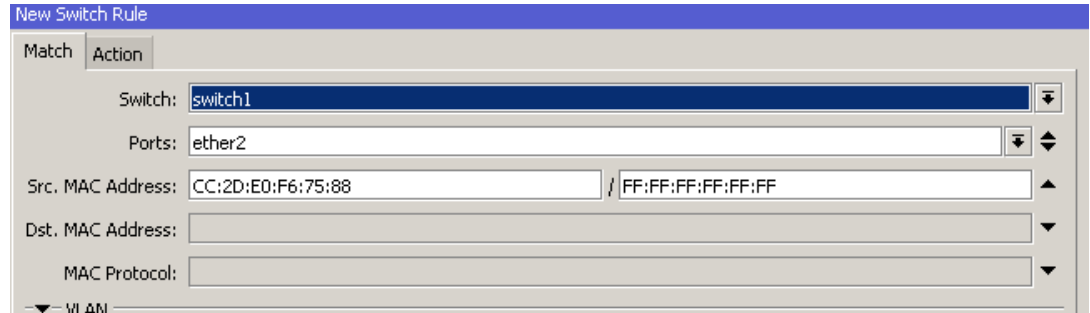
☐ Trusted

☒ Hardware Offload

OK Cancel Apply Disable Comment Copy Remove

enabled inactive Hw. Offload

/interface ethernet switch rule



New Switch Rule

Match Action

Switch: switch1

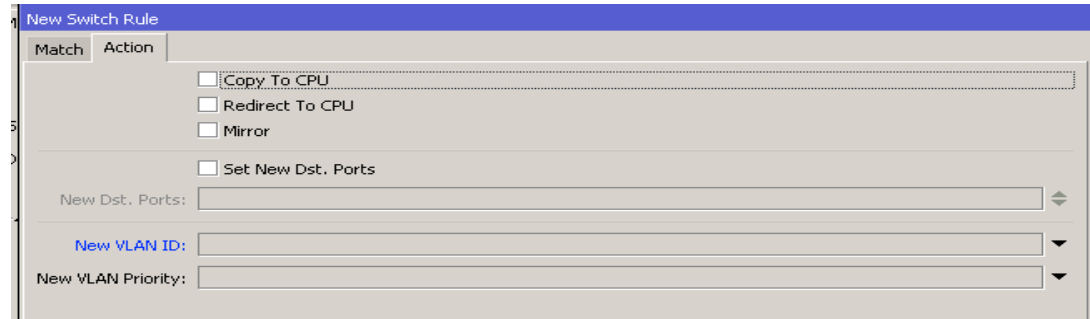
Ports: ether2

Src. MAC Address: CC:2D:E0:F6:75:88 / FF:FF:FF:FF:FF:FF

Dst. MAC Address:

MAC Protocol:

VLAN



New Switch Rule

Match Action

☐ Copy To CPU

☐ Redirect To CPU

☐ Mirror

☐ Set New Dst. Ports

New Dst. Ports:

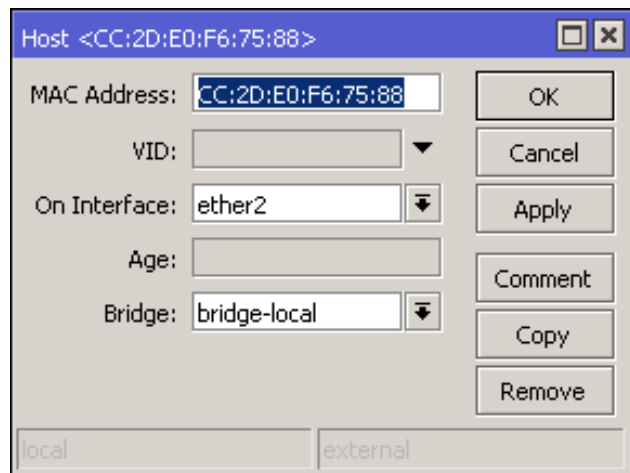
New VLAN ID:

New VLAN Priority:

Port base security

- Для использования порта только определенным mac address можно воспользоваться ограничением mac-адресов на порту

/interface bridge hosts



Host <CC:2D:E0:F6:75:88>

MAC Address: CC:2D:E0:F6:75:88

VID:

On Interface: ether2

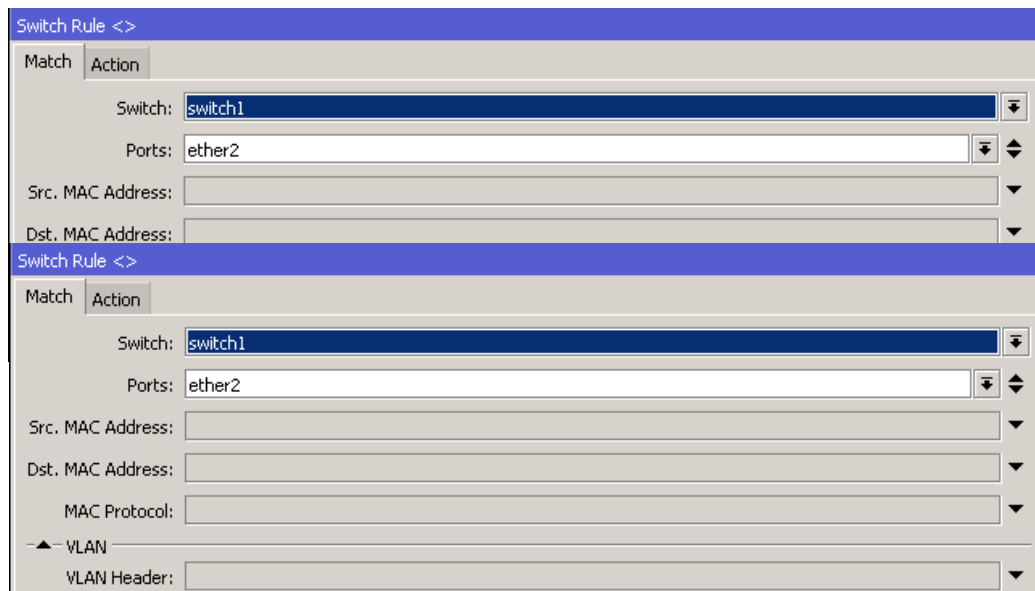
Age:

Bridge: bridge-local

local external

Buttons: OK, Cancel, Apply, Comment, Copy, Remove

/interface ethernet switch rule



Switch Rule <>

Match Action

Switch: switch1

Ports: ether2

Src. MAC Address:

Dst. MAC Address:

Switch Rule <>

Match Action

Switch: switch1

Ports: ether2

Src. MAC Address:

Dst. MAC Address:

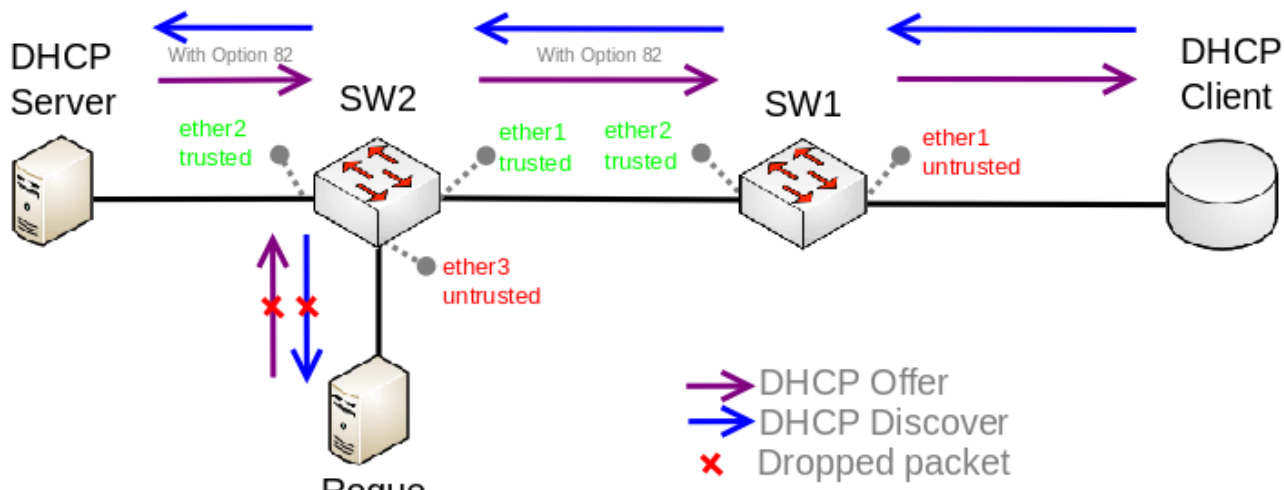
MAC Protocol:

VLAN

VLAN Header:

DHCP snooping в CRS3xx

- Защита от чужих DHCP серверов в локальной сети
- Начиная с версии RouterOS 6.43, мост поддерживает DHCP Snooping и опцию DHCP 82.
- DHCP Snooping - это функция безопасности L2, которая ограничивает несанкционированные DHCP-серверы
- В RouterOS вы можете указать, какие порты моста являются доверенными



DHCP snooping в CRS3xx

Interface <bridge-local>

General STP VLAN Status Traffic

Name:

Type:

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP:

ARP Timeout:

Admin. MAC Address:

Ageing Time:

☒ IGMP Snooping

☒ DHCP Snooping

☒ Add DHCP Option 82

OK Cancel Apply Disable Comment Copy Remove Torch

Bridge Port <sfp-sfpplus1>

General STP VLAN Status

Interface:

Bridge:

Horizon:

Learn:

☒ Unknown Unicast Flood

☒ Unknown Multicast Flood

☒ Broadcast Flood

☒ Trusted

☒ Hardware Offload

OK Cancel Apply Disable Comment Copy Remove

СПАСИБО ЗА ВНИМАНИЕ

Приходите на наши курсы по
Mikrotik и Asterisk

