Voice vlan, приоритизация трафика в локальных сетях (L2) и как с этим жить на оборудовании MikroTik

ASTERCONF
– 2020

ОБО МНЕ

ФИО	Козлов Роман
Контакты	t.me/soriel
Возраст	32
Сертификаты Mikrotik	MTCNA, MTCRE, MTCWE, MTCTCE, MTCUME, MTCINE, MTCIPv6E, MTCSE, MTCSWE, Trainer
Компания	IntegraSky
Должность	Технический директор
Технологии и профессиональные интересы	Сети, wifi, виртуализация, сервера, linux, безопасность, windows и etc
Дополнительно	Участвую в подкасте linkmeup, веду курсы MikroTik, видел некоторое количества дер*ma

00 Состав презентации

Состав презентации

- VLAN общие сведения
- Способы назначения VLAN на телефоны
  - Access
  - Tag
  - Mac based vlan
  - LLDP-Med
  - DHCP 132 / 66
  - 802.1x
- QoS в l2
  - best effor
  - На коммутаторах mikrotik CRS3xx
  - Wifi – WMM 802.11e

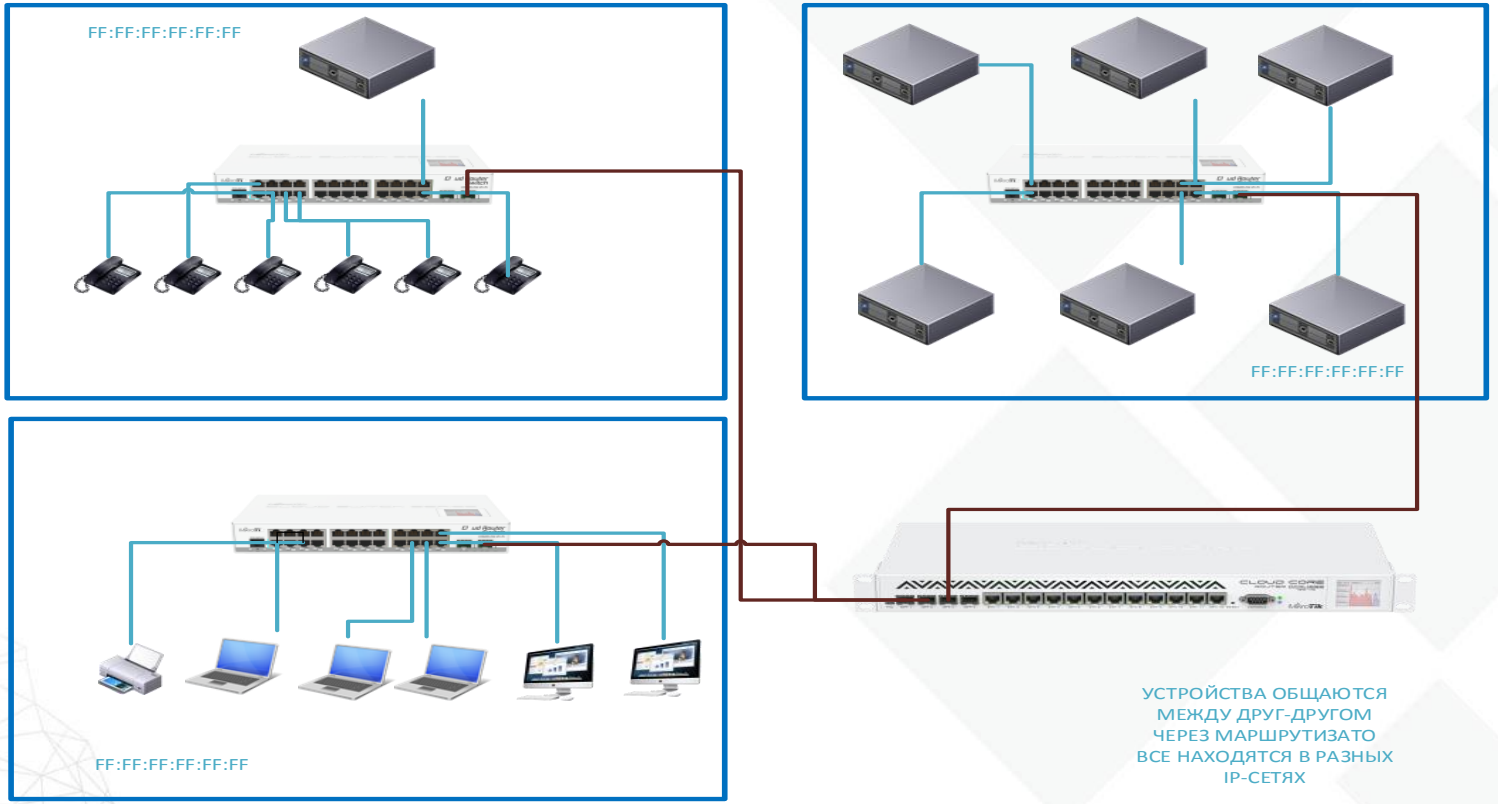
01

VLAN общие сведения

В сетях принято уменьшать размеры широковещательного домена

- Это позволяет:
  - Быстрее найти проблемное оборудование или петлю
  - Увеличить безопасность сети – firewall или acl между сетями и снижать риск различных атак на l2 (например: arp spoofing, dhcp starvation, dhcp rogue или атака на устройства)
  - Разделить сети на функциональные зоны (телефонам нужно ходить на asterisk и ntp, ПК в интернет и на сервера, камеры только в сервер видеонаблюдения и тд)
  - Удобно раздавать настройки на разные группы устройств (телефонам 66, пк dns ad)
  - Разделять на логические группы устройства (например – отдел ИТ, отдел бухгалтерии и тд)
  - Немного увеличивать производительность сети за счет уменьшения служебного l2 трафика

Разделение на физическом уровне

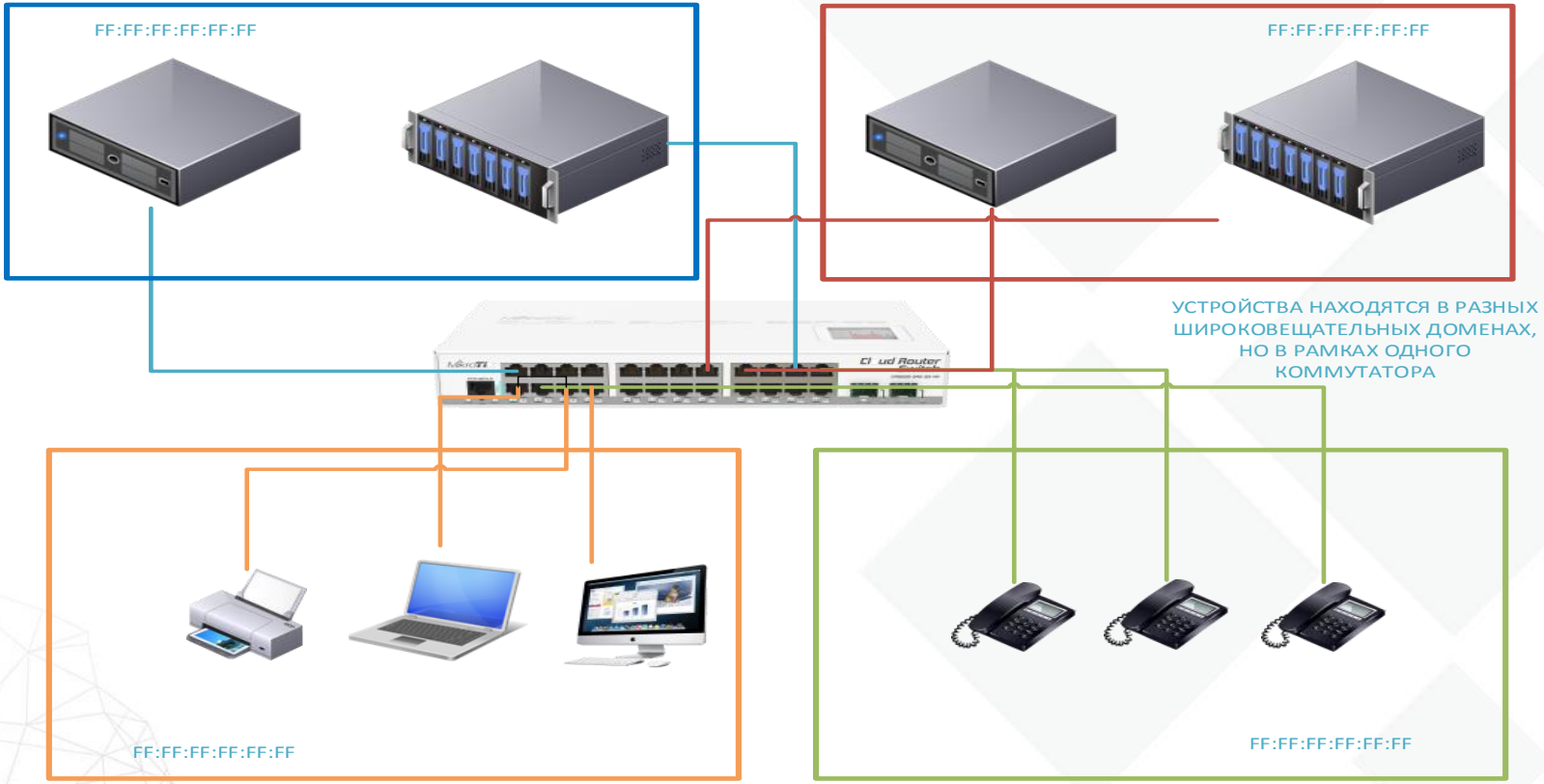


УСТРОЙСТВА ОБЩАЮТСЯ МЕЖДУ ДРУГ-ДРУГОМ ЧЕРЕЗ МАРШРУТИЗАТО ВСЕ НАХОДЯТСЯ В РАЗНЫХ IP-СЕТЯХ

Разделение на физическом уровне

- Плюсы:
  - Минимальное количество логики и настроек – нет настроек нет проблем
  - Максимальная производительность
  - Можно использовать неуправляемые коммутаторы
- Минусы:
  - При переезде начинаем заниматься монтажом
  - Дополнительные группы требуют дополнительного оборудования
  - Скорость перенастройки сети низкая
  - Большие расходы на монтаж СКС

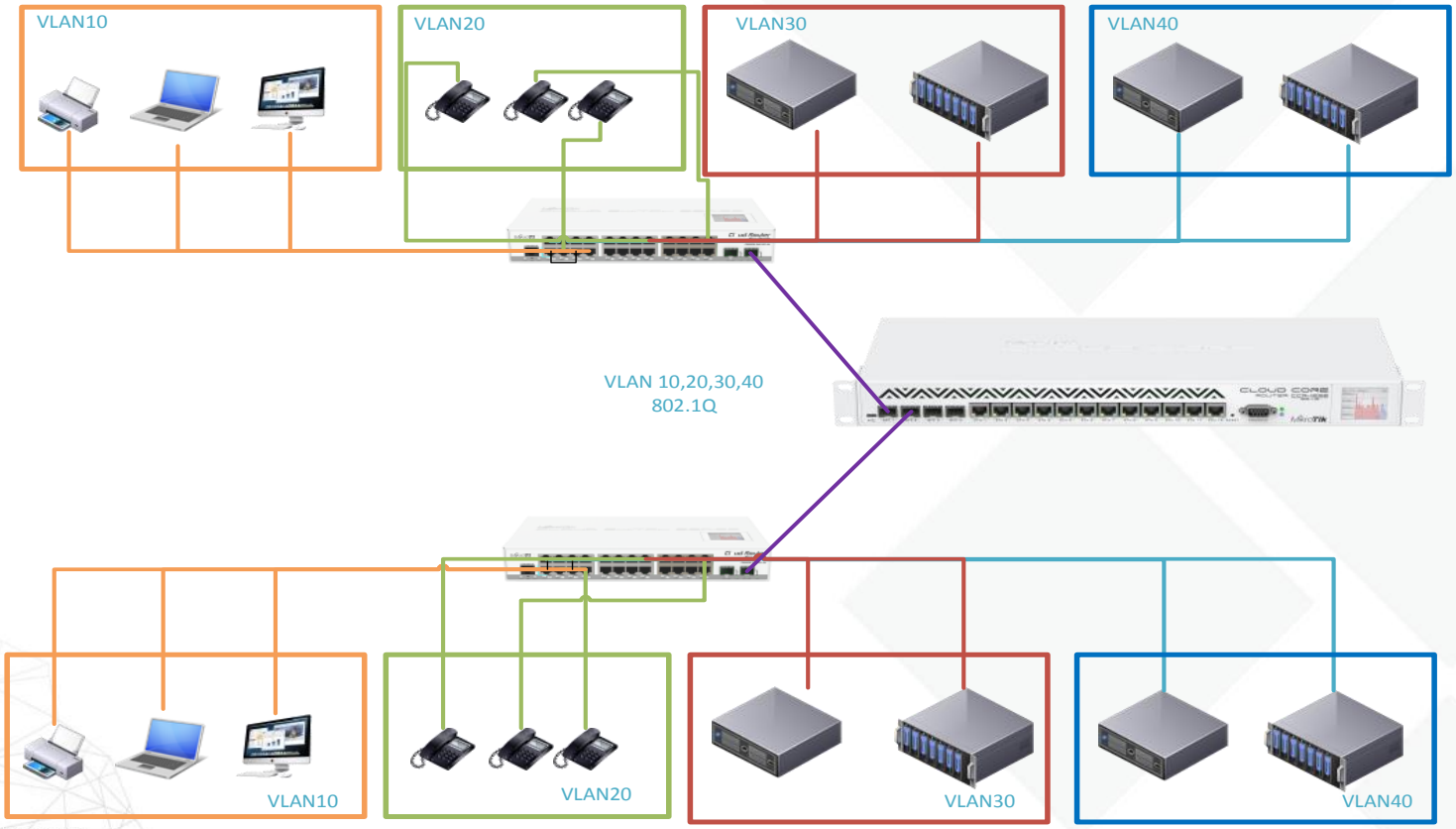
Разделение на уровне коммутатора



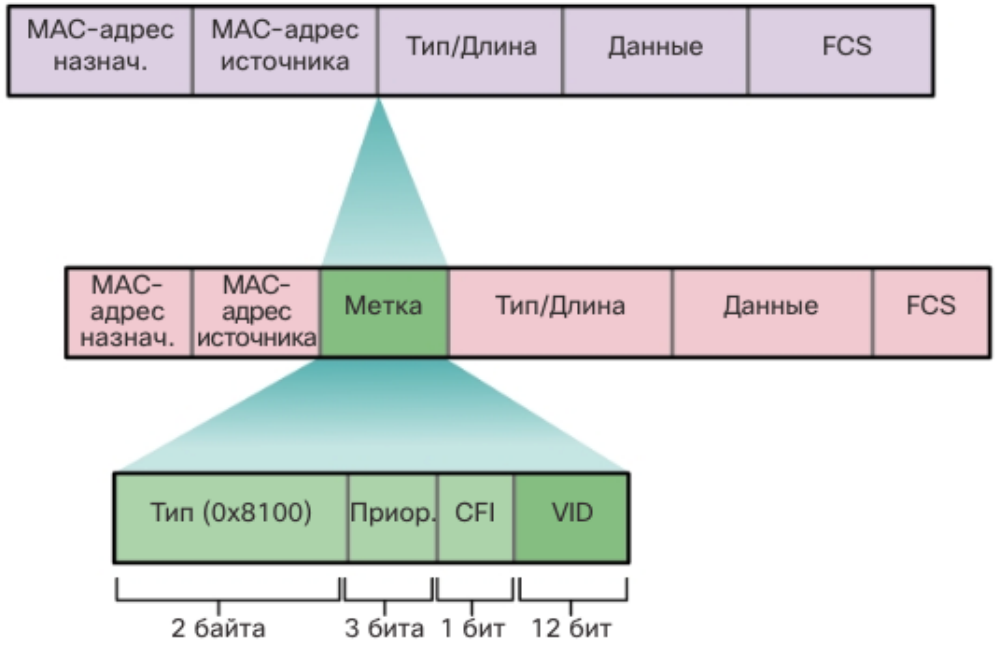
Разделение на уровне коммутатора

- Плюсы:
  - Разные широковещательные домены
  - Высокий уровень безопасности
  - Высокая производительность при использовании аппаратной реализации
  - Простота
- Минусы:
  - Соединения по группам – дополнительные проводные подключения
  - Подходит только для небольших организаций
  - Дополнительные настройки на коммутаторах
  - Требует управляемых устройств

Использование 802.1q



VLAN IEEE 802.1q



Технология 802.1q модифицирует исходный заголовок кадра и добавляет дополнительные 4 байта информации

Использование 802.1q

- Плюсы:
  - Высокая гибкость
  - Экономия на проводных подключениях
  - Высокий уровень безопасности
- Минусы:
  - Более сложные настройки
  - Дополнительные настройки на коммутаторах
  - Требует управляемых устройств
  - Нужно не забывать о производительности на соединениях с 802.1q

02

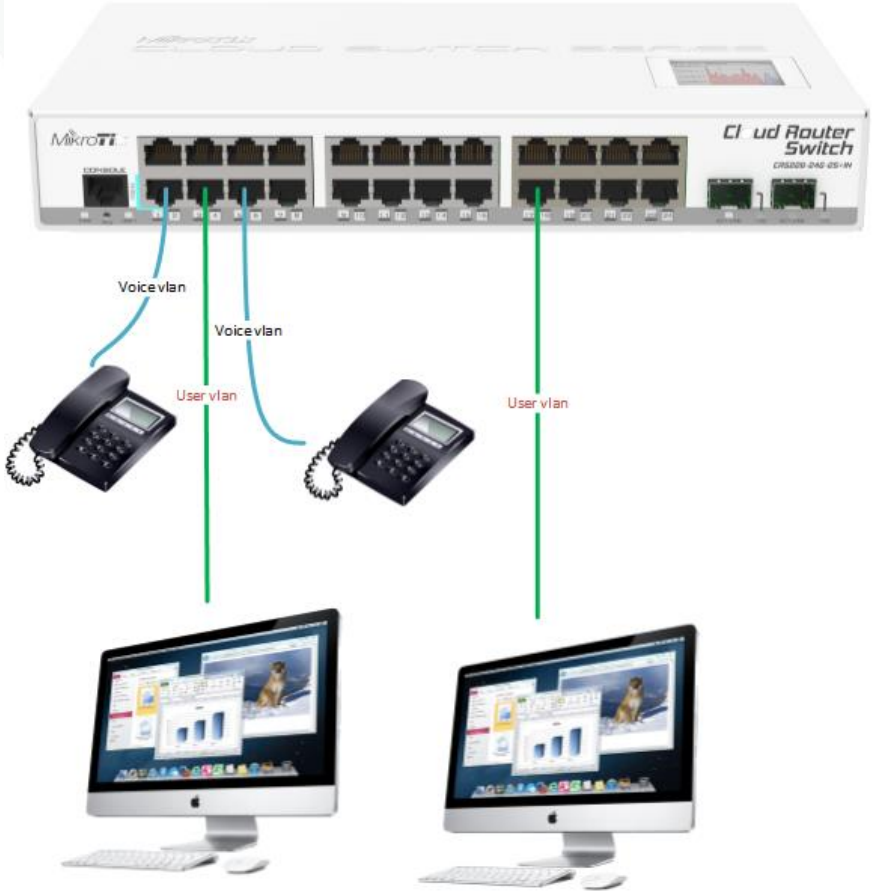
Способы назначения VLAN на телефоны

Способы подключения телефонов и PC

- Телефон подключается напрямую в коммутатор, PC так же напрямую в коммутатор
- Телефон подключается напрямую в коммутатор, PC подключается через порт телефона

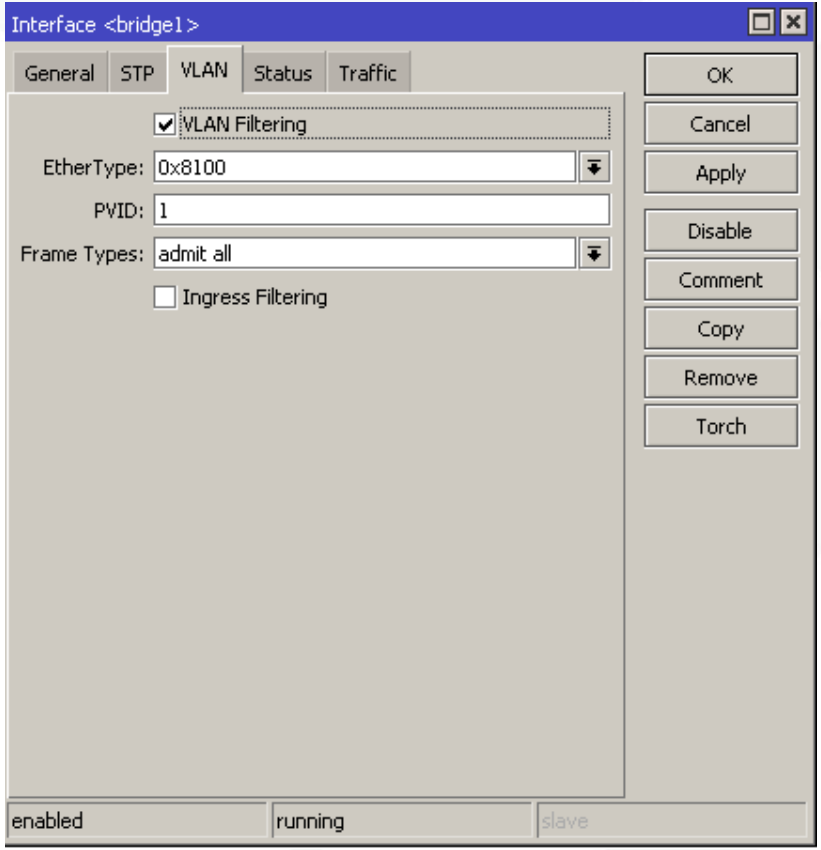
Способы подключения телефонов access VLAN

- Устройства подключаются в отдельный порт
- Плюсы
  - Максимальная скорость
  - Нет ограничений
  - Нет необходимости использовать vlan на телефоне
- Минусы
  - Ручное назначение портов коммутатора в нужный vlan
  - Неэкономное использование портов
  - Пользователь может подключиться в телефон и попасть в телефонную сеть



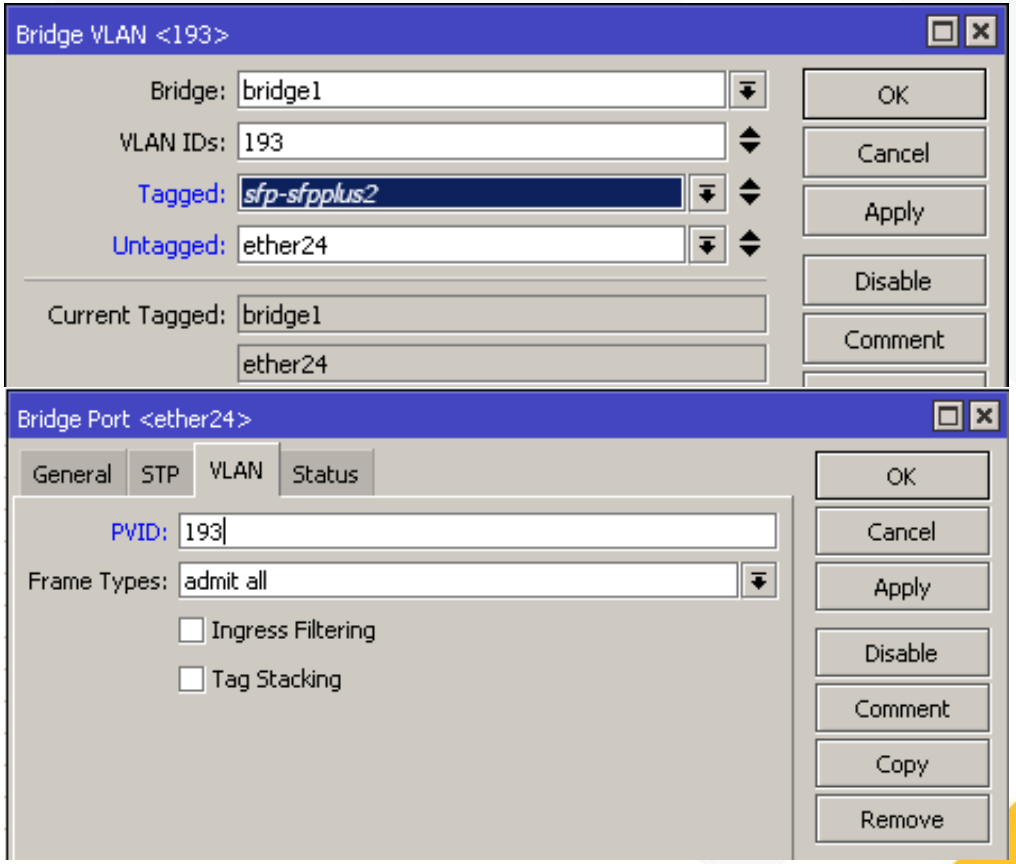
Способы подключения телефонов access VLAN

- Включаем vlan filtering
- /interface bridge set vlan-filtering=yes bridge1



Способы подключения телефонов access VLAN

- Добавляем порты в vlan untagged
- /interface bridge vlan set vlan-ids=193 bridge=bridge1 tagged=sfp-sfpplus1 untagged=ether24
- Добавляем PVID на нужный порт
- /interface bridge port set pvid=193 interface=ether24

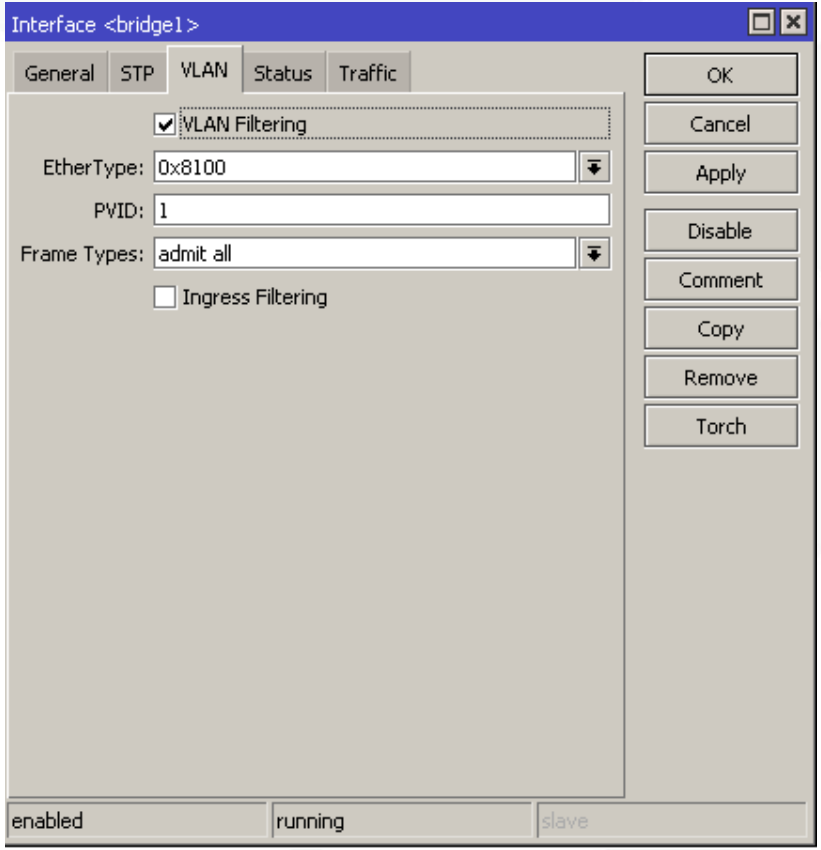


Способы подключения телефонов tag

- PC подключается в телефон, телефон работает с tag кадрами
- Плюсы
  - Экономное использование портов коммутатора
- Минусы
  - Снижение скорости на порту PC
  - PC видит тегированный трафик
  - Ручные настройки телефонов / config + tag
  - Ручные настройки коммутаторов

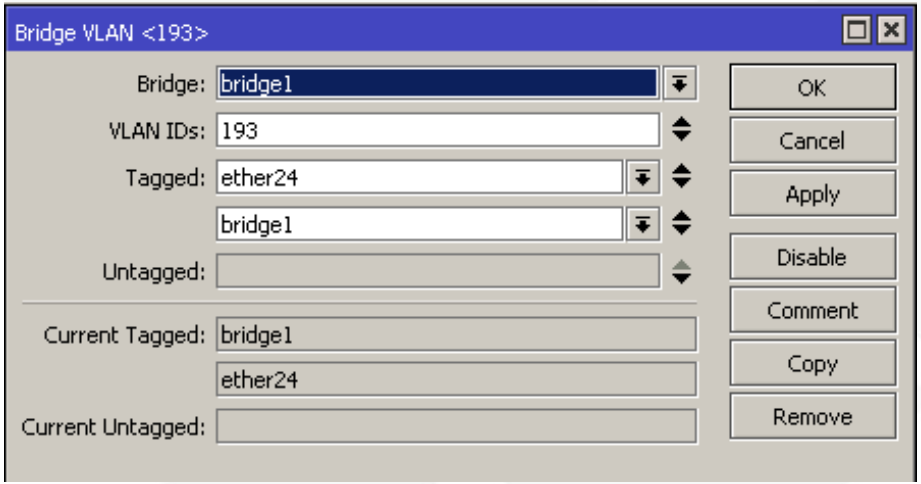
Способы подключения телефонов tag

- Включаем vlan filtering
- /interface bridge set vlan-filtering=yes bridge1



Способы подключения телефонов tag VLAN

- Добавляем порты в vlan tagget
- /interface bridge vlan set vlan-ids=193 bridge=bridge1 tagged=sfp-sfpplus1, ether24
- Не меняем PVID
- Настраиваем телефоны на работу с tag = 193

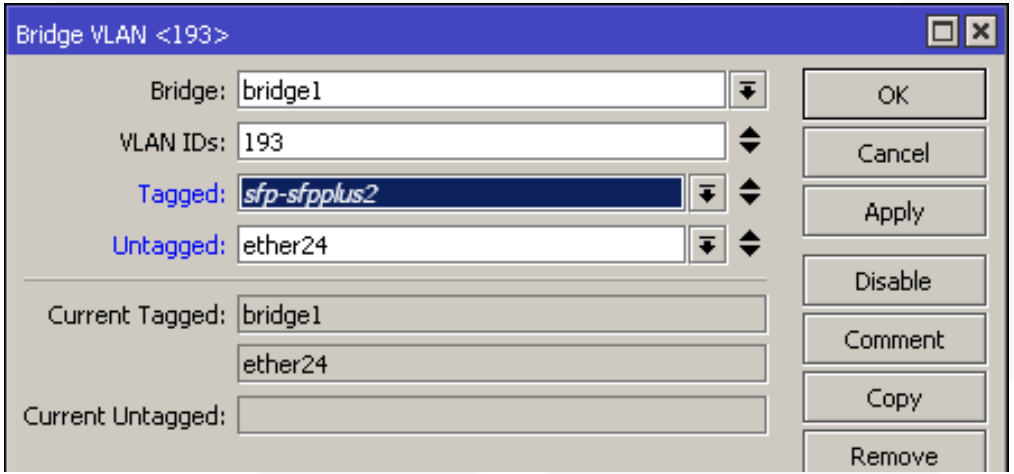


Способы подключения телефонов mac based vlan

- Коммутатор назначает необходимый vlan на на кадры согласно MAC-адресам
- Плюсы
  - Автоматическое назначение vlan на mac телефона
- Минусы
  - Снижение скорости на порту PC
  - Более сложные настройки коммутатора
  - Требуется поддержка от коммутатора

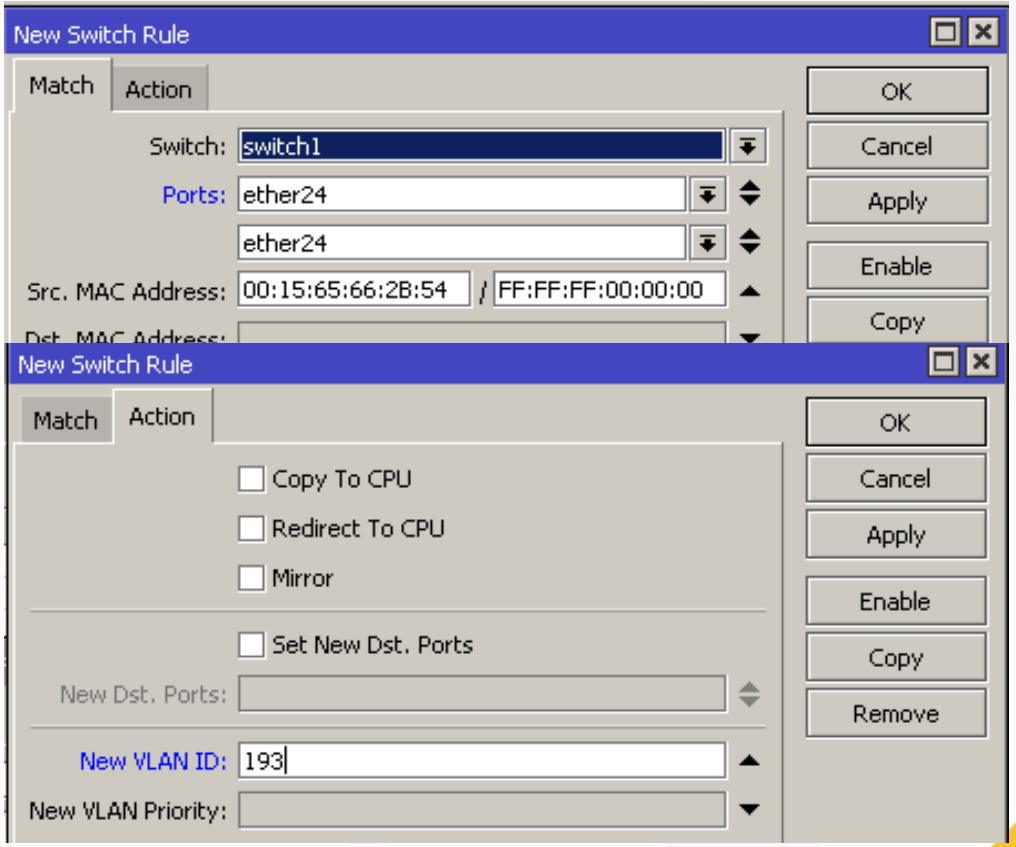
Способы подключения телефонов mac based vlan

- Добавляем порты в vlan untagged
- /interface bridge vlan set vlan-ids=193 bridge=bridge1 tagged=sfp-sfpplus1 untagged=ether24



Способы подключения телефонов mac based vlan

- Добавьте правила коммутатора, которые назначают идентификатор VLAN на основе MAC-адреса.
- /interface ethernet switch rule add new-vlan-id=193 ports=ether24 src-mac-address=00:15:65:66:2B:54/FF:FF:FF:00:00:00 switch=switch1

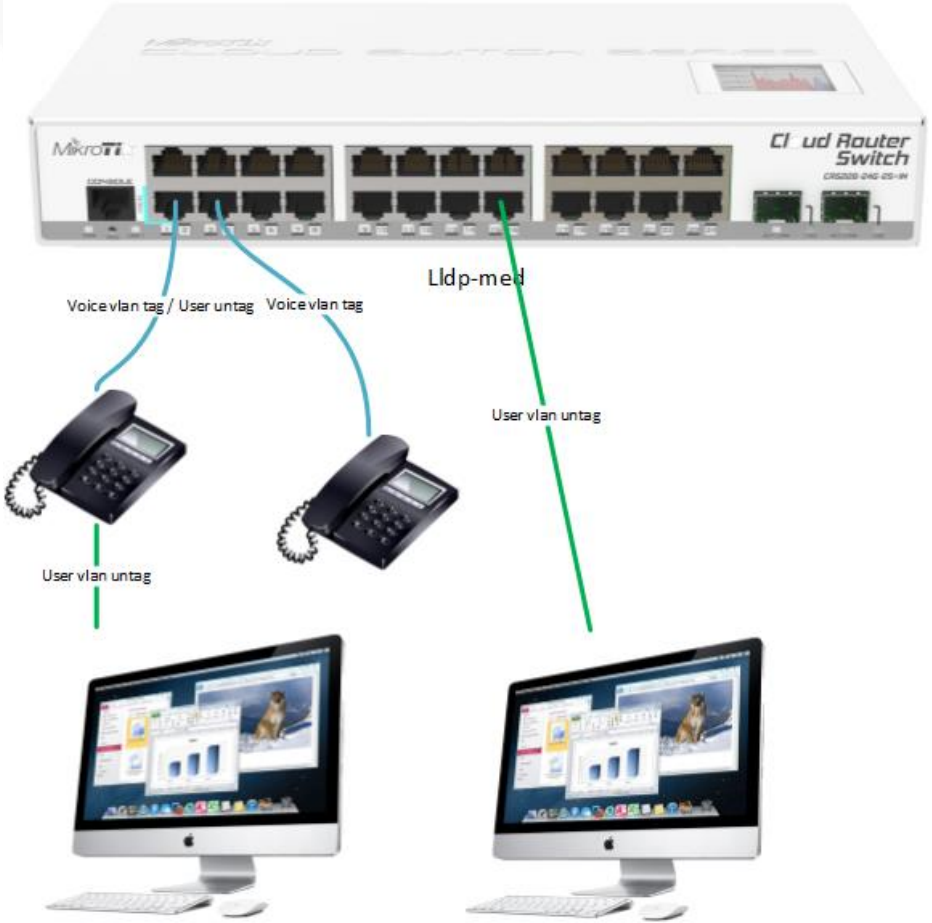


lldp-med

- Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) — расширение стандарта LLDP, которое позволяет:
  - **Автоматически обнаруживать сетевые политики (VLAN, 802.1p, DSCP),**
  - Использовать более расширенное и автоматическое управление питанием на PoE хостах,
  - Отслеживать местоположения устройств и топологию, в том числе таких устройств как IP-телефоны,
  - Выполнять инвентаризацию устройств в сети и определение их характеристик
  - Отслеживать перемещения устройств и отправлять SNMP-сообщения на соответствующий управляющий хост.
  - Для того чтобы LLDP-MED анонсировал информацию о VLAN, должен быть создан voice VLAN и порт, на котором находится IP-телефон должен быть тегированным в этом VLAN.

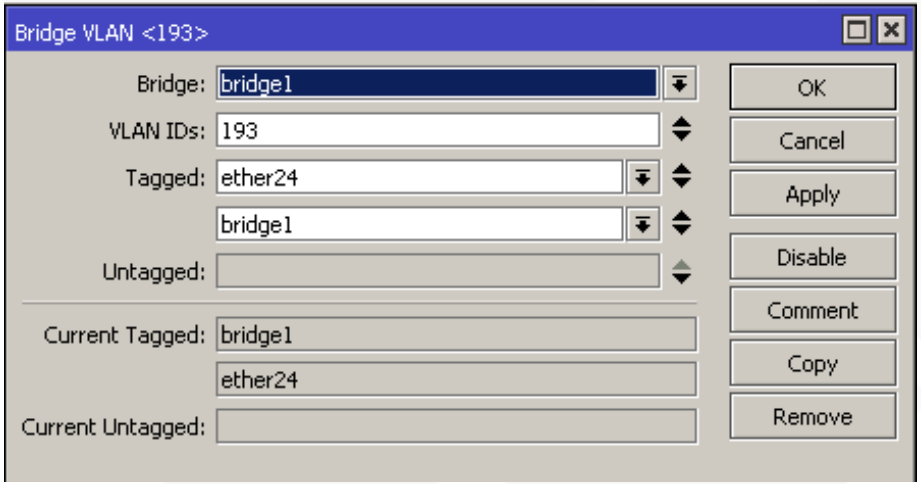
Способы подключения телефонов lldp-med

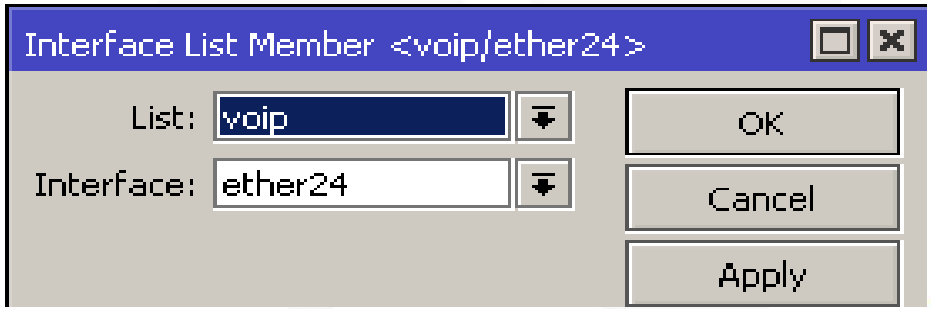
- Рассылка lldp сообщений в которых содержится информация о необходимом vlan для телефонов
- Плюсы
  - Автоматическое назначение vlan на телефон
- Минусы
  - Необходима поддержка от телефонов
  - Снижение уровня безопасности
  - Дополнительные настройки



Способы подключения телефонов lldp-med

- Добавляем порты в vlan tagget
- /interface bridge vlan set vlan-ids=193 bridge=bridge1 tagged=sfp-sfpplus1, ether24
- Добавляем порты в интерфейс лист
- /interface list member add list=voip interface=ether24
- Добавляем правило на расслылку lldp сообщений (6.48beta40)
- /ip neighbor discovery-settings set lldp-med-net-policy-vlan=193 protocol=lldp discover-interface-list=voip



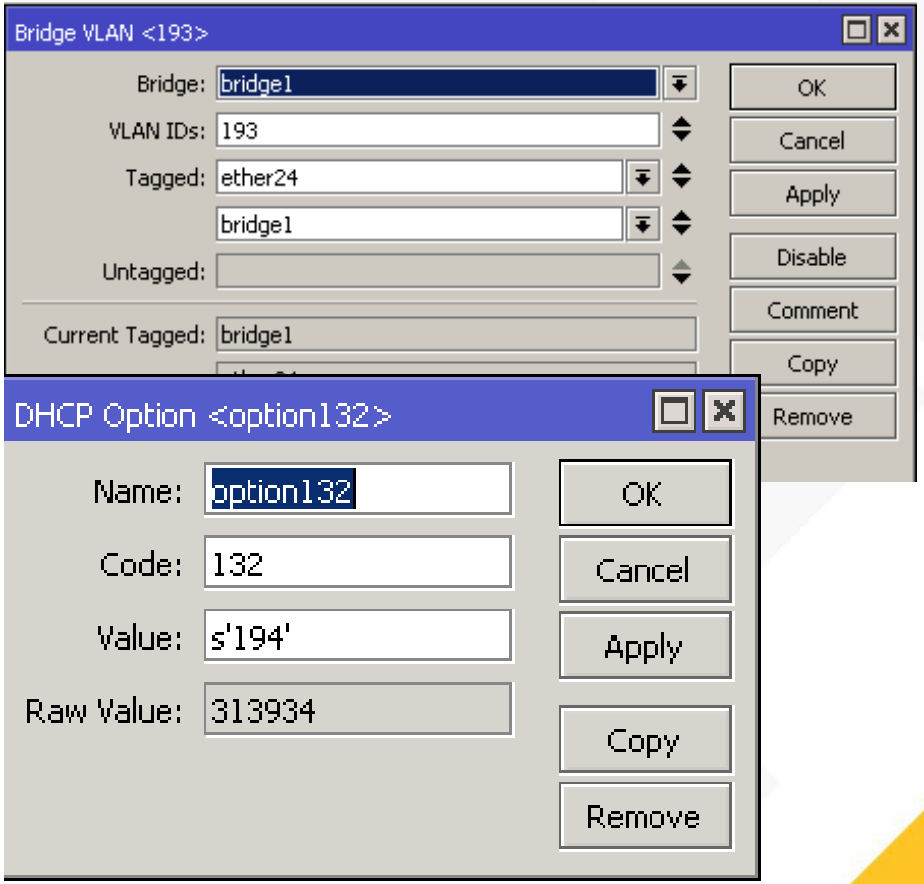


Способы подключения телефонов DHCP 132

- DHCP сервер отправляет опцию 132 в которой указан VLAN id
- Устройства понимающие опцию – настраивают tag VLAN
- Плюсы
  - Автоматическое назначение vlan на телефон через dhcp
- Минусы
  - Необходима поддержка от телефонов
  - Снижение уровня безопасности
  - Дополнительные настройки

Способы подключения телефонов DHCP 132

- Добавляем порты в vlan tagget
- /interface bridge vlan set vlan-ids=193 bridge=bridge1 tagged=sfp-sfpplus1, ether24
- Добавляем опцию в DHCP
- /ip dhcp-server option add code=132 name=option132 value="s'194'"
- /ip dhcp-server network add address=192.168.193.0/24 dhcp-option=option132 dns-server=192.168.193.1 gateway=192.168.193.

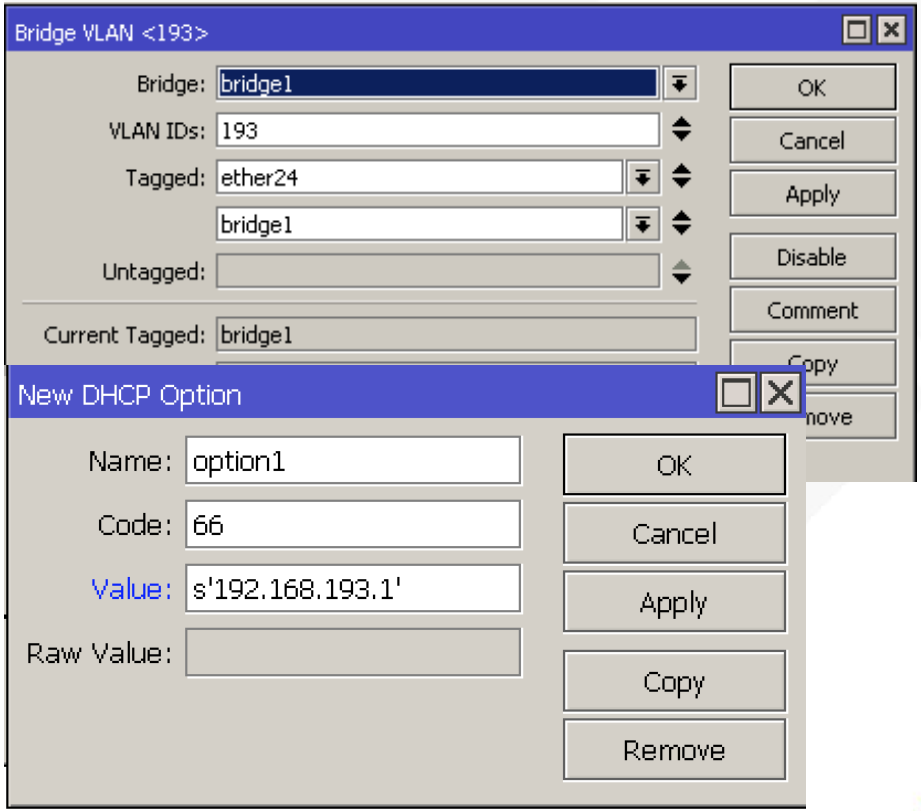


Способы подключения телефонов DHCP 66

- DHCP сервер отправляет опцию 66 на сервер tftp загрузки
- Устройства понимающие опцию – загружают конфигурацию в которой прописан vlan id
- Плюсы
  - Автоматическое назначение vlan на телефон через dhcp
- Минусы
  - Необходима поддержка от телефонов
  - Снижение уровня безопасности
  - Дополнительные настройки
  - TFP и разбор файла конфигов телефонов

Способы подключения телефонов DHCP 132

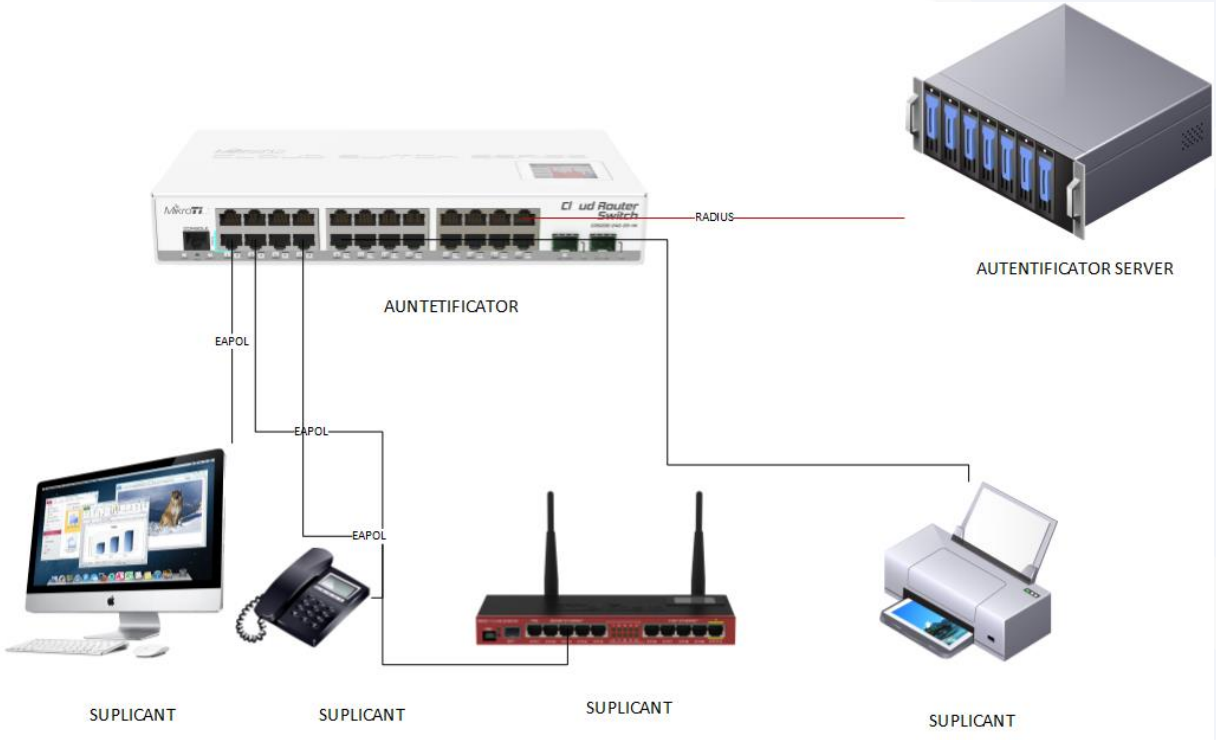
- Добавляем порты в vlan tagget
- /interface bridge vlan set vlan-ids=193 bridge=bridge1 tagged=sfp-sfpplus1, ether24
- Добавляем опцию в DHCP
- /ip dhcp-server option add code=66 name=option132 value="s’192.168.193.1’”
- /ip dhcp-server network add address=192.168.193.0/24 dhcp-option=option66 dns-server=192.168.193.1 gateway=192.168.193.



Введение в Dot1x

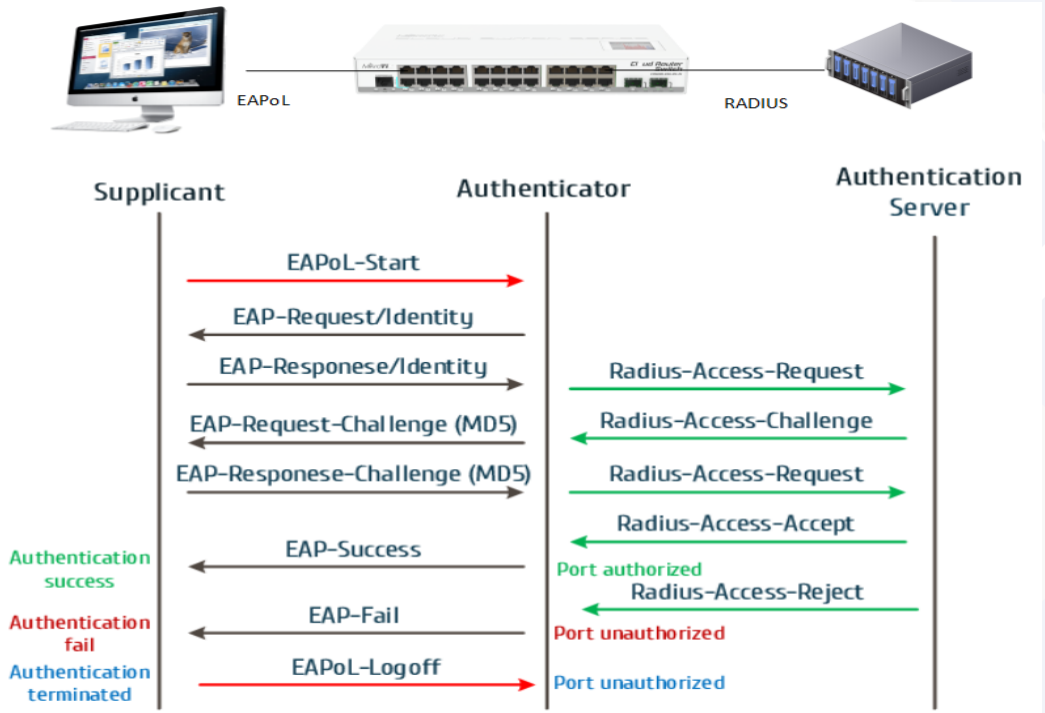
- 802.1X — это способ обеспечения безопасности портов.
- Устройство, подключенное к порту с поддержкой 802.1X, не может отправлять и получать пакеты в сети до тех пор, пока его идентификационные данные не будут проверены
- Эта функция называется в соответствии со спецификацией IEEE.
- 802.1X использует протокол EAP (Extensible Authentication Protocol) для передачи учетных данных устройства на сервер аутентификации (обычно RADIUS) с помощью обязательного промежуточного устройства сетевого доступа
- Устройство сетевого доступа служит для обмена данными между устройством конечного пользователя и сервером аутентификации, обеспечивая безопасность сети.
- Устройство сетевого доступа использует протокол EAP-over-Ethernet (EAPOL) для связи с устройством конечного пользователя и EAP-over-RADIUS для связи с сервером.

Схема работы Dot1x



- Suplicant – клиент(в нашем случае рабочая станция, телефон, принтер, камера, другой роутер
- Autentificator – коммутатор на порту которого осуществляется процесс проверки клиентов
- Autentifivator server - Radius server

Схема работы Dot1x



- Suplicant – обменивается с atentificator(в нашем случае mikrotik crs3xx) EAPoL сообщениями
- Autentificator транслирует сообщения RADIUS серверу
- В обратную сторону от сервера приходят ответы - либо разрешающие аутентификацию – либо нет
- При отсутствии разрешения – suplicant либо не получает доступа к сети, либо попадает в reject Vlan

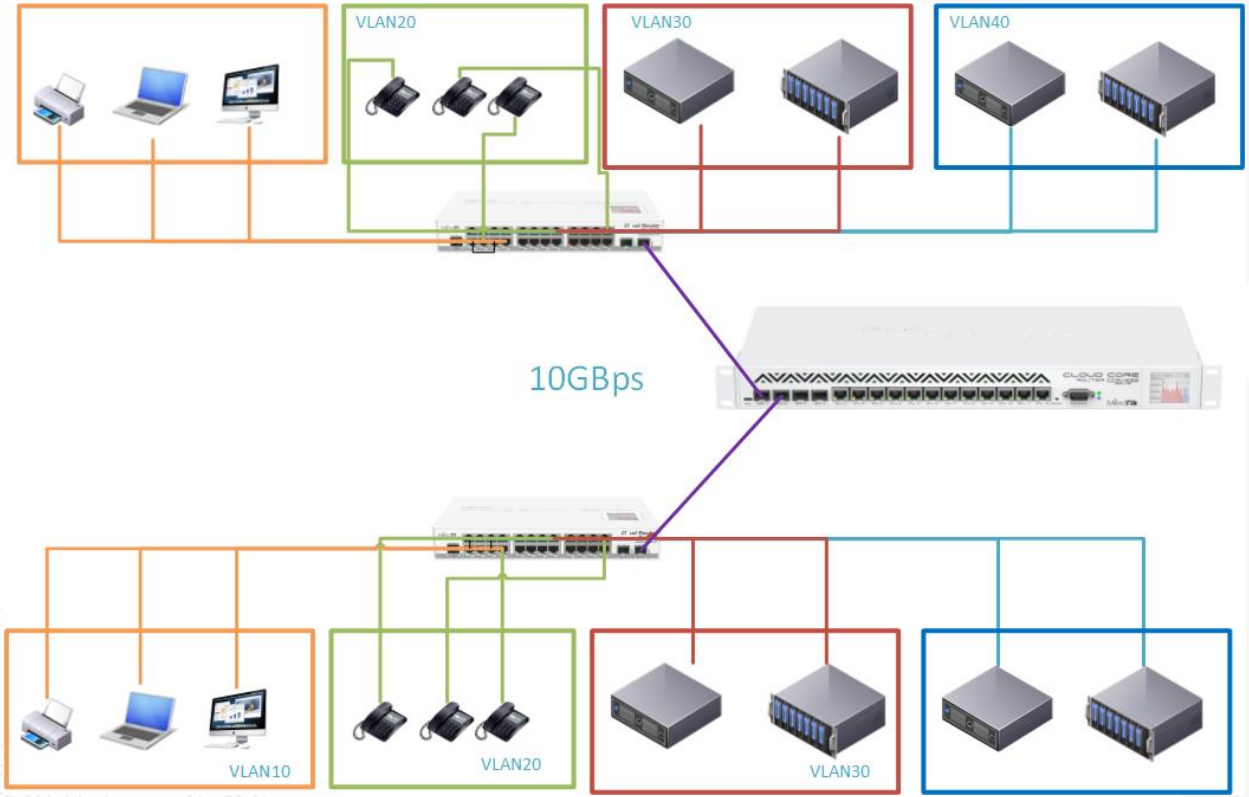
802.1x

- Какую пользу мы получаем от внедрения Dot1x
  - Повышение уровня безопасности в компании
  - Возможность установки VLAN на группу пользователей
  - Возможность настройки параметров switch rule для групп пользователей
  - Всегда знаешь где находится устройство и что это за устройство
  - Радость за себя, что ты это смог реализовать
- Минусы
  - Поддержка нескольких служб
  - Поддержка оборудования
  - Некоторое количество проблем

03

QoS в l2

Best Effort – никаких гарантий – все равны



Этот подход используется повсеместно:

В локальных сетях

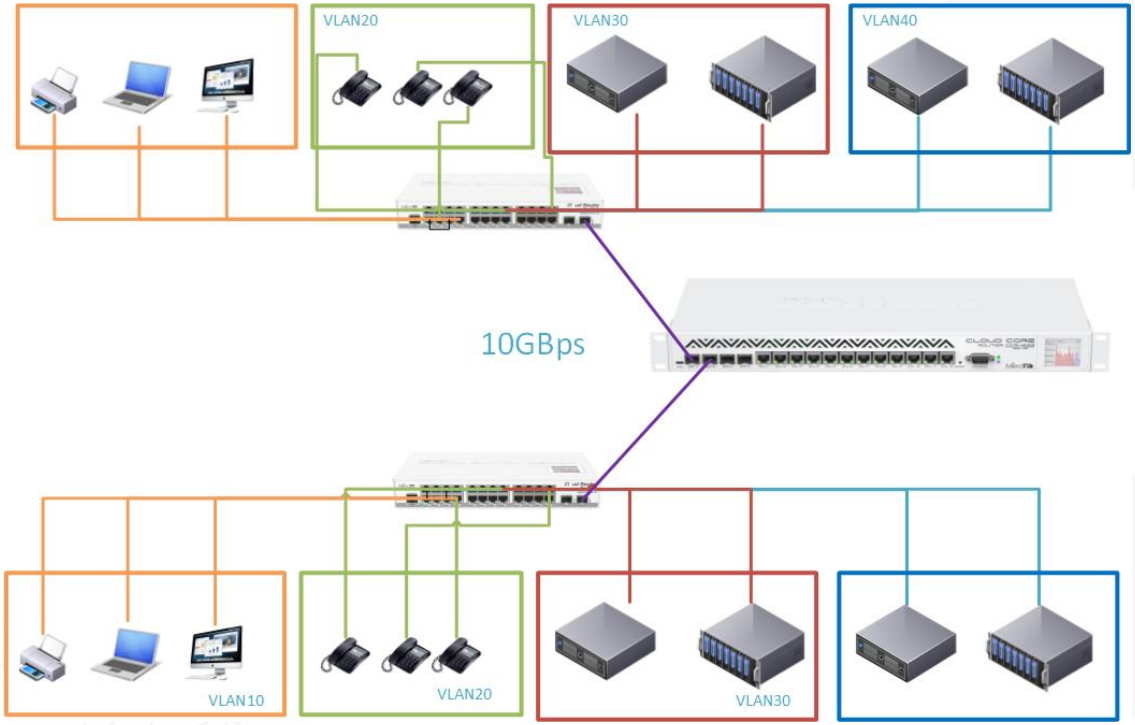
В беспроводных сетях

В домашних сетях

Дать возможность вашим устройствам максимально потреблять

Зачастую выгодно увеличить канал, чем усложнять конфигурацию

QoS на коммутаторах Crs3xx



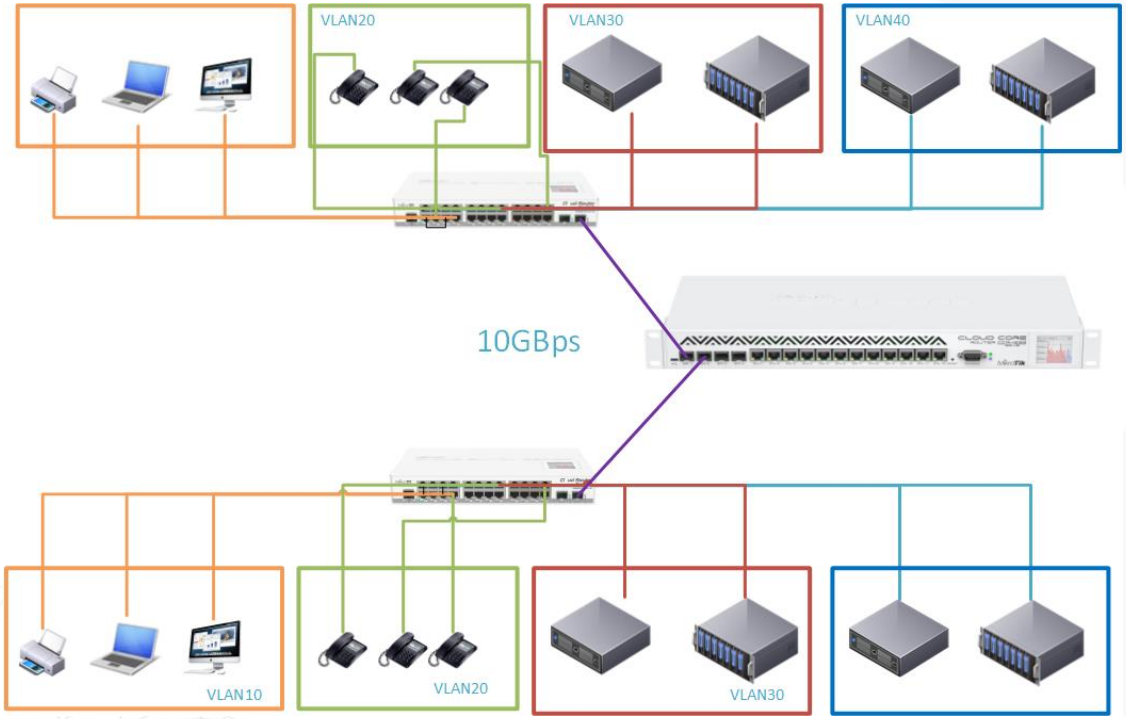
Можно ограничить определенные типы трафика с помощью правил ACL.

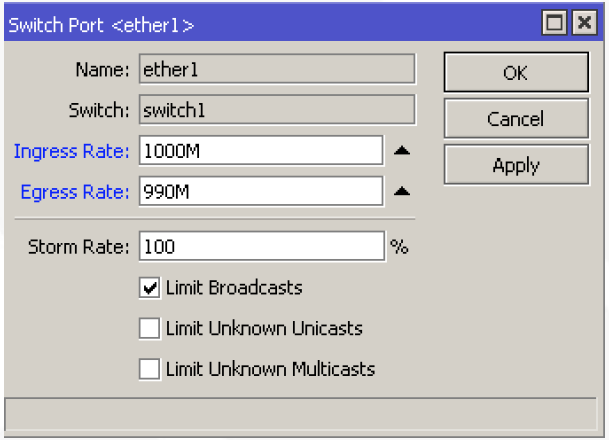
Для коммутаторов серии CRS3xx можно ограничить входящий трафик, который соответствует определенным параметрам, и можно ограничить входящий/ исходящий трафик для каждого интерфейса.

По факту получается shaper:

Отрезаем большую часть для не приоритетного трафика и жестко ограничиваем трафик для приоритетного трафика

QoS на коммутаторах Crs3xx ingress rate / egress rate

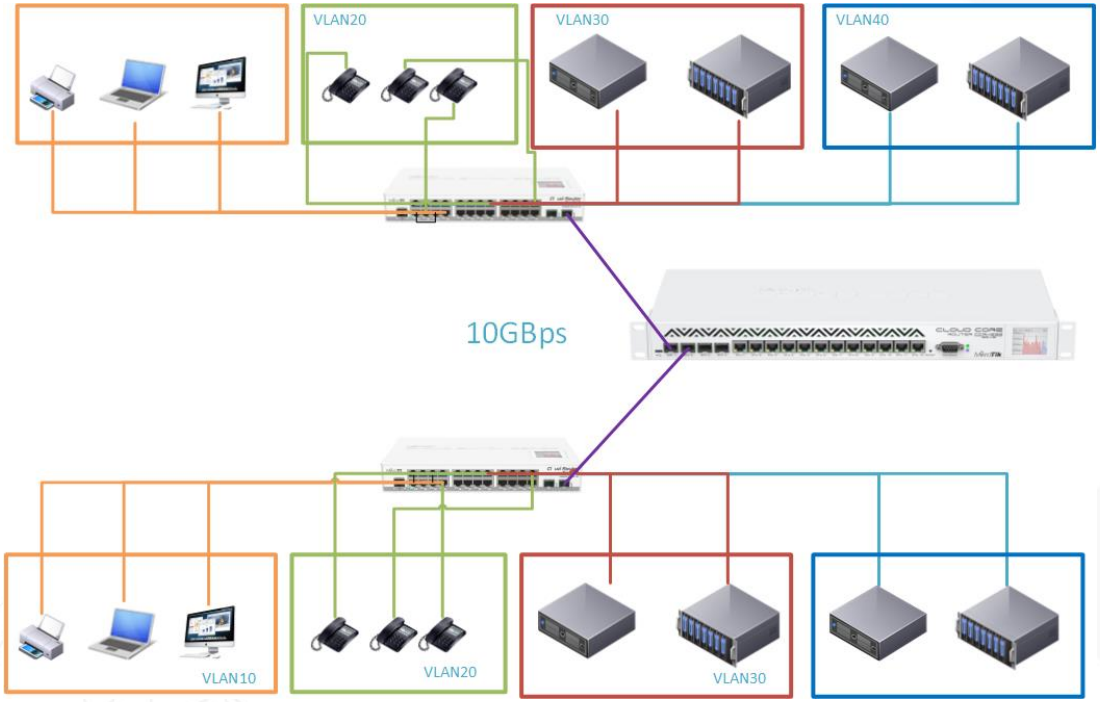


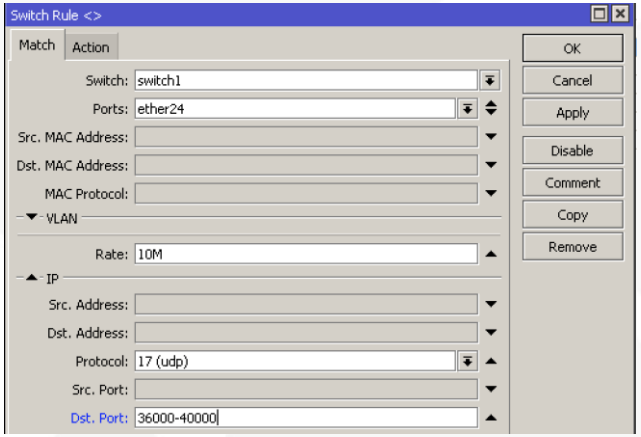


Ограничение скорости на порту

/interface ethernet switch port set ether1 ingress-rate=1000M egress-rate=990M

QoS на коммутаторах Crs3xx switch rules





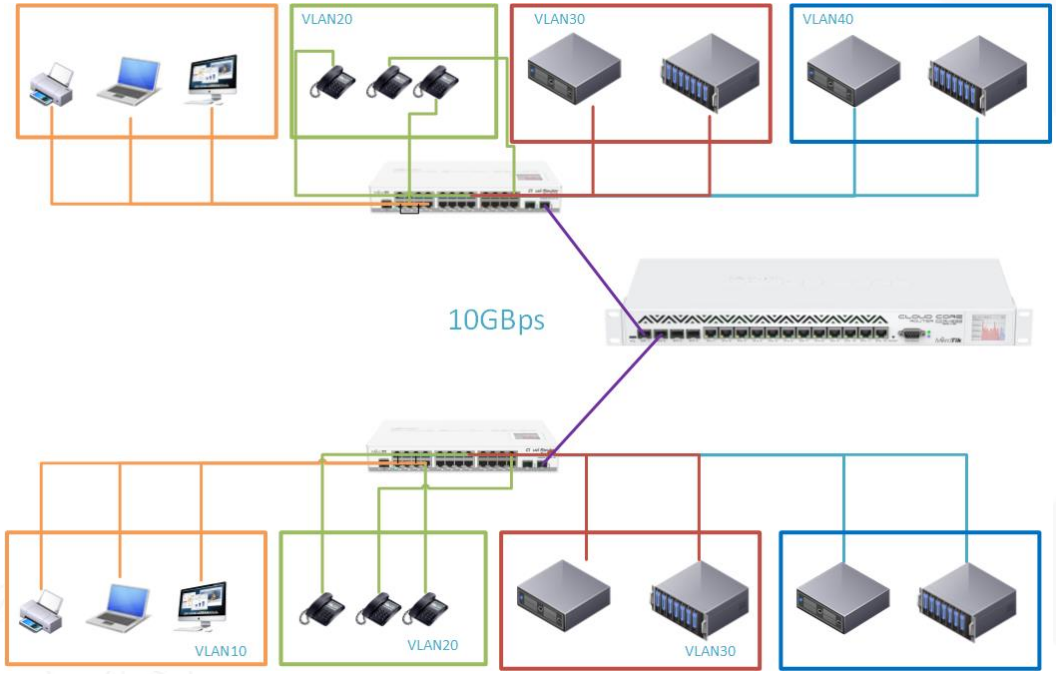
/interface bridge

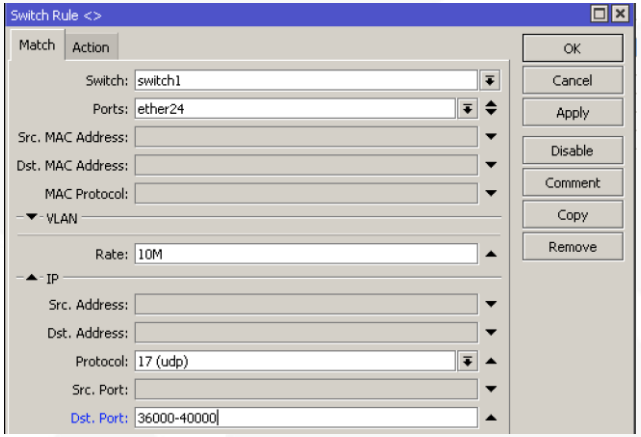
set bridge1 vlan-filtering=yes

/interface ethernet switch rule add ports=ether1

switch=switch1 vlan-id=11 rate=10M

QoS на коммутаторах Crs3xx switch rules





/interface bridge

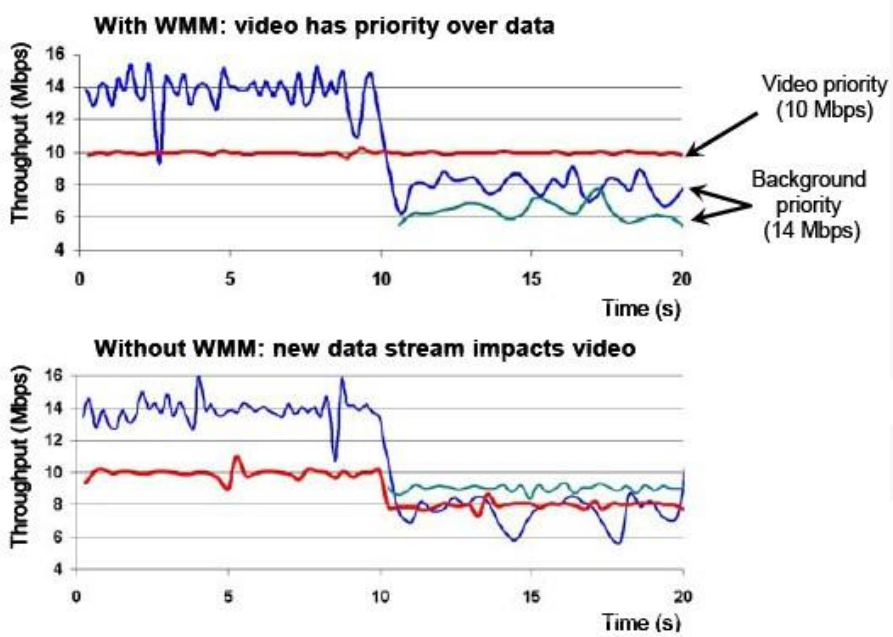
set bridge1 vlan-filtering=yes

/interface ethernet switch rule add ports=ether1

switch=switch1 vlan-id=11 rate=10M

Wifi – WMM 802.11e

- Если все-таки есть необходимость передавать голос через беспроводные сети, то ситуацию может немного исправить WMM:
- Wireless Multimedia Extensions - протокол, основанный на стандарте IEEE 802.11e, для обеспечения основных функций QoS для беспроводных сетей IEEE 802.11.
- WMM может использоваться для задания приоритета над «обычными данными» для голосового трафика (Voice over IP), видео-трафика, а также трафика негарантированной доставки от устройств, не имеющих механизма QoS.



Wifi – WMM 802.11e

- Приоритеты на L2 и их сопоставление с WMM.
- WMM устанавливает приоритет из поля priority в заголовке пакета
- Устанавливаются через опции
- /ip firewall mangle add chain=prerouting action=set-priority new-priority=0,1,2,3,4,5,6,7
- Может понадобиться использование
- /interface bridge settings set use-ip-firewall=yes
- /interface bridge filter add chain=forward action=set-priority new-priority=0,1,2,3,4,5,6,7

802.1p Priority	WMM Access Category
1	Background
2	
0	Best effort
3	
4	Video
5	
6	Voice
7	

WMM и DSCP

- WMM нужно настроить – нужно указать приоритеты
- WMM и DSCP
- /ip firewall mangle add action=set-priority chain=prerouting new-priority=from-dscp-high-3-bits passthrough=yes
- Можно использовать приоритеты из VLAN – ingress
- /interface bridge filter add action=set-priority chain=forward new-priority=from-ingress passthrough=yes

802.1p Priority	WMM Access Category
1	Background
2	
0	Best effort
3	
4	Video
5	
6	Voice
7	

СПАСИБО
ЗА ВНИМАНИЕ!

Роман Козлов

telegram @soriel
kozlov.r@integrasky.ru

ASTERCONF
– 2020