voxlink

MikroTik - TRAINING.RU

Аппаратная маршрутизация в коммутаторах crs3xx на RouterOS 7 и построение локальных сетей

MUoM

Mikrotik User Online Meeting

ОБО МНЕ

ФИО	Козлов Роман
Контакты	t.me/soriel
Возраст	34
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

О ЧЕМ Я РАССКАЖУ В ДОКЛАДЕ

- Общий подход
- Построение локальных сетей на RouterOS 6
    1. Устройство маленькой локальной сети
    2. Router-on-a-stick
    3. Упрощенная Двухуровневая модель локальной сети ROS6
    4. Двухуровневая модель локальной сети ROS6
    5. Трехуровневая модель локальной сети ROS6
- Немного о Железе
- Подход к построению локальных сетей в RouterOS 7
    - Основные улучшения в RouterOS 7
    - Устройство маленькой локальной сети ROS7
    - Двухуровневая модель локальной сети ROS6
    - Трехуровневая модель локальной сети ROS7
- Итоги

01

Общий подход

Классические локальные сети

MUoM
Mikrotik User Online Meeting

Общий подход

Построение локальной сети в предприятии зависит от нескольких параметров и предъявляет определенные требования

- Размер организации / Количество устройств / Портов
- Теоретическое время простоя и отказоустойчивость
- Стоимость внедрения / Стоимость обслуживания

Требования:

- Отказоустойчивость
- Производительность
- Удобство
- Масштабирование

Размер организации

Обоснование того или иного варианта построения локальной сети должен рассматривать не просто теоретическую модель того как должно быть, а отталкиваться от реальной ситуации:

- Не имеет смысла строить сложные сети на маленькие организации или филиалы, которые легко помещаются в один коммутатор/роутер
- С другой стороны крупные компании имеют высокие денежные потери в случае простоя
- Чем больше сервисов, рабочих групп, оборудования тем больше у вас будет индивидуальных схем для каждого из этих классов

Время простоя

- Время от начала инцидента до полного его устранения
- Обычно можно оценить в уе:
  - Прямые потери
  - Недополученная прибыль
  - Косвенные потери - например репутация
  - Потери оплаченного рабочего времени
- Критичность к времени простоя серьезно зависит от профиля работы компании, конкурентов, схемы работы и тд. – зачастую индивидуальный параметр, который лучше всего обсуждать с руководством
- В некоторых случаях при обсуждении выясняется, что время простоя может длиться без серьезных последствий для компании до нескольких суток
- Если устройство одно стоит ориентироваться на 6-8 часов временя простоя – время закупки, диагностики, доставки, настройки и тд
- Часто малые организации не имеют штатного технического специалиста который может незамедлительно начать решать проблему

Стоимость внедрения

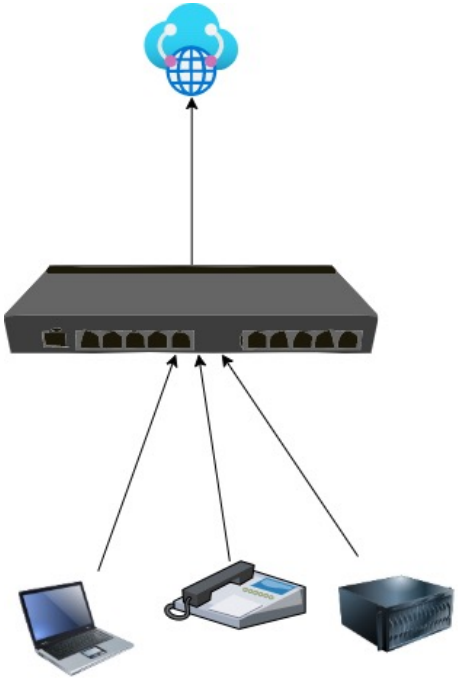
- Учитывать ЗИП при покупке и его возможный поиск
- Наличие специалистов и их квалификация (40 van, mstp, acl на компанию из 15 человек)
- Гарантийный срок и срок модернизации
- Стоимость и необходимость обслуживания
- Стоимость модернизации (css vs crs)

02

Построение локальных сетей на RouterOS 6

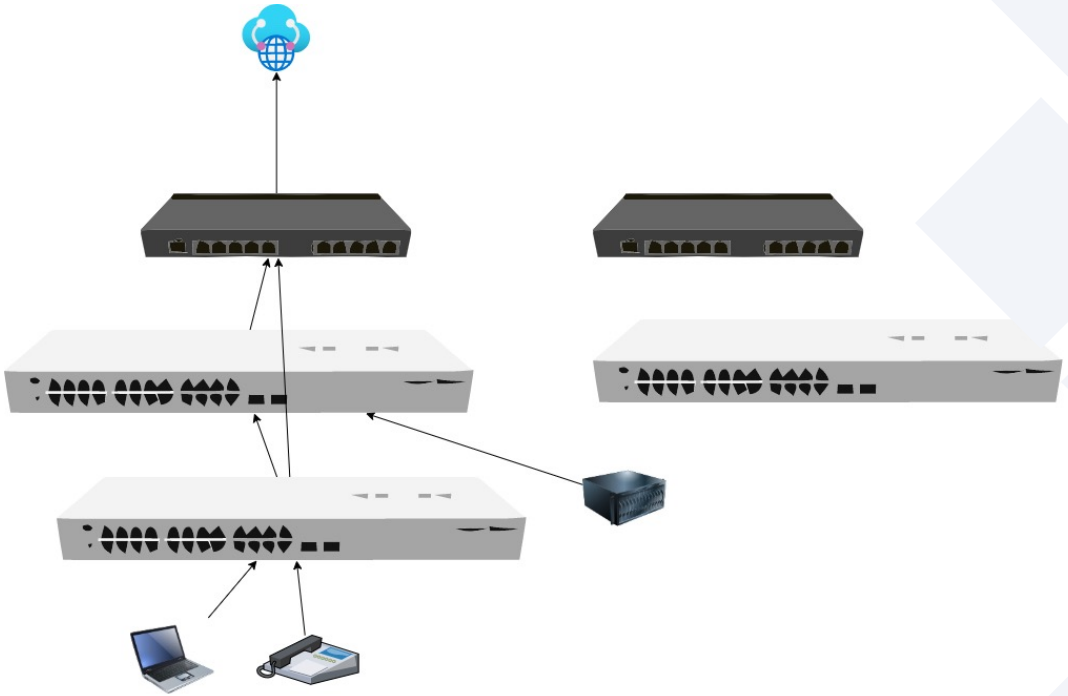
Router-on-a-stick

Устройство маленькой локальной сети



- Все устройства помещаются в одно устройство
- Выбор из устройств rb3011/4011/5009/CRS3xx/RB750GR3/ HAPAC3/HAPAC2/CCR/etc
- Возможен холодный резерв
- **Плюсы:**
  - Дешево
  - Просто
  - Мало места/Электроэнергии
  - Можно использовать конфигурации по-умолчанию

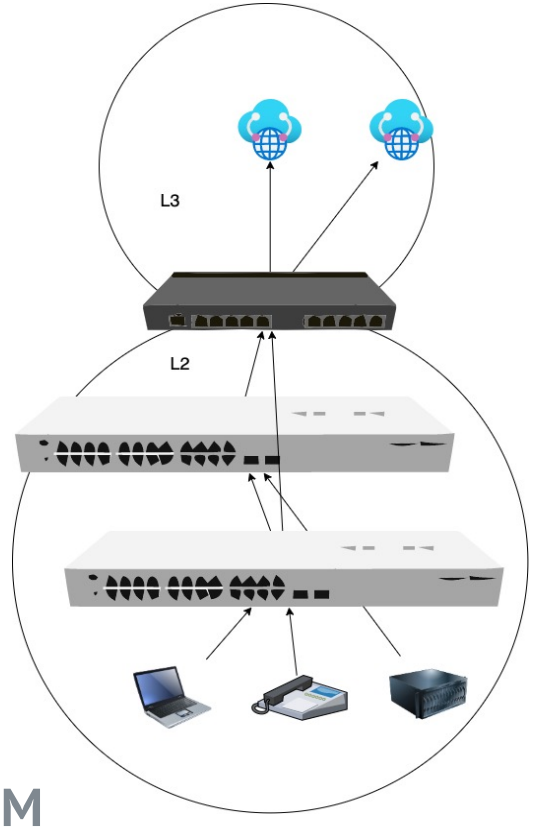
Устройство маленькой локальной сети ROS6



Минусы:

- Минусы – без ЗИП можно попасть на длительный простой
- Производительность маршрутизации зависит от CPU роутера
- Масштабирование не линейное и стихийное(свитч в свитч)
- Производительность l2 не всегда удовлетворительная – 24Gb в 1Gb
- Низкий уровень маштабирования

Устройство маленькой локальной сети ROS6



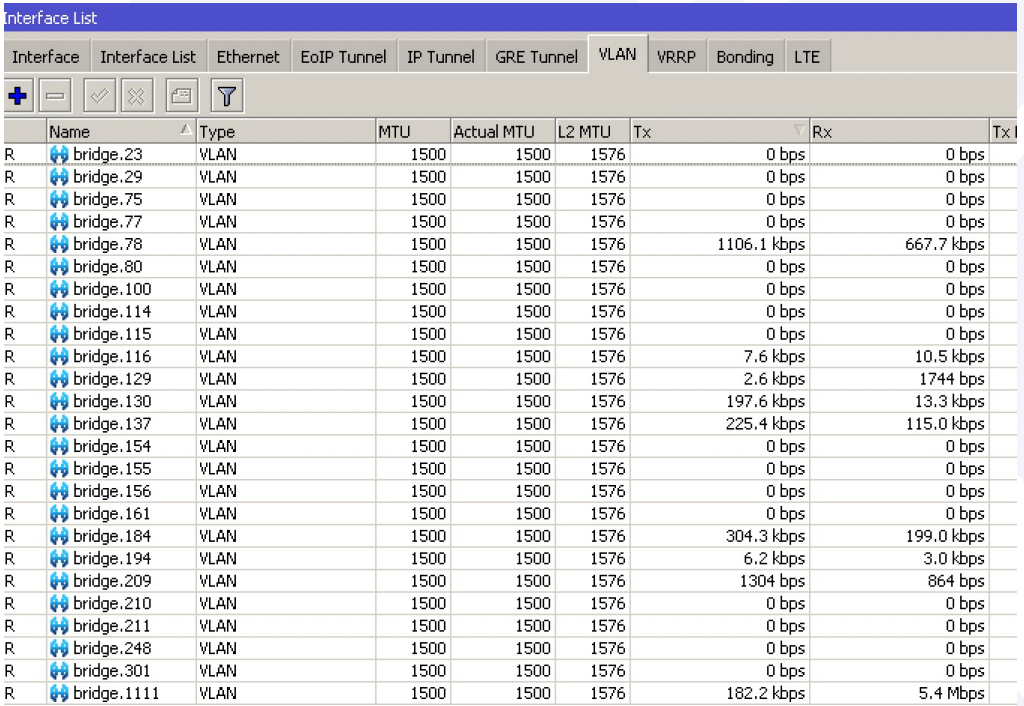
Протоколы и технологии

- Bonding
- STP/RSTP/MSTP
- VLAN
- Граница L2 сети проходит на роутере
- При наличии VLAN маршрутизация между VLAN осуществляется на роутере
- Схема router-on-a-stick
- QoS (shaper) на switch rules
- Большая часть настроек безопасности на router
- Возможно использовать switch rules

Router-on-a-stick

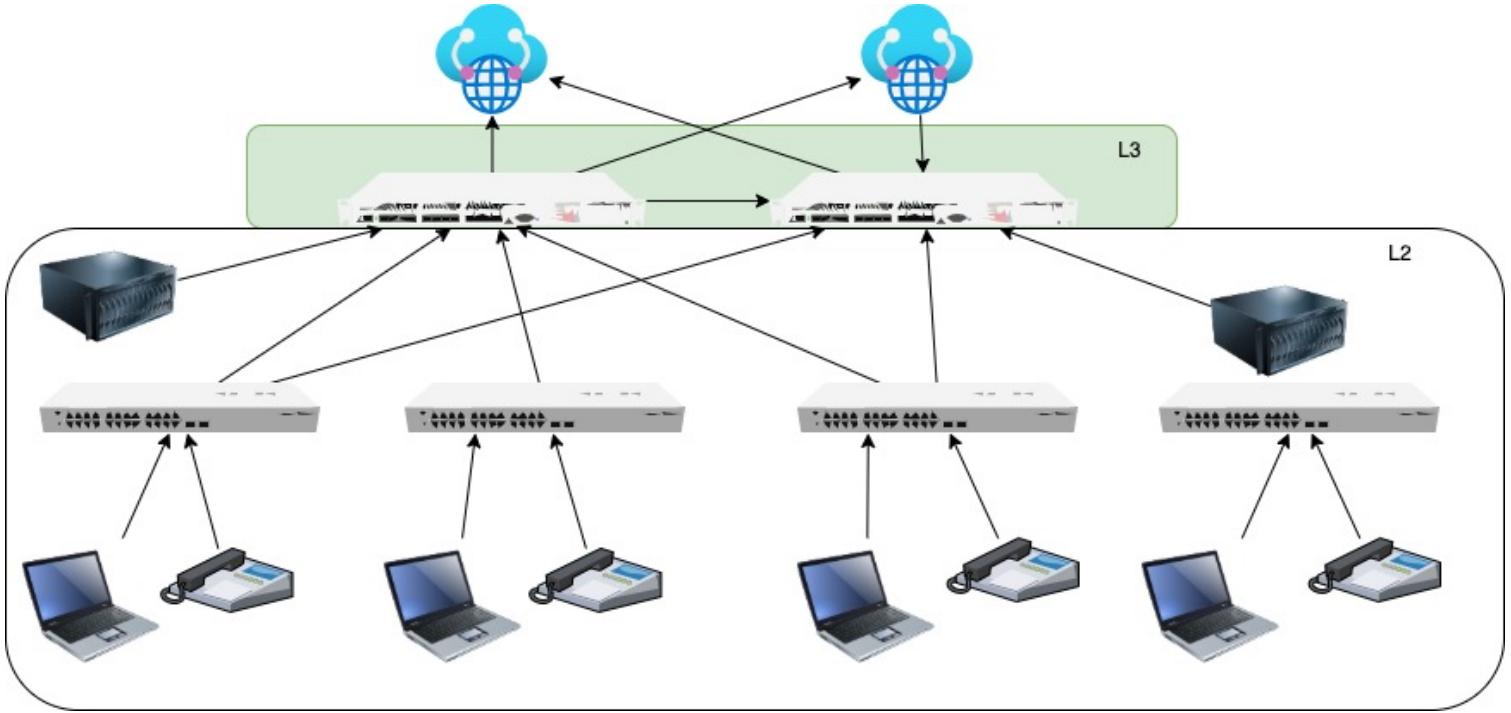
Router-on-a-stick

- Виртуальные интерфейсы создастся на основном роутере
- В качестве интерфейса указывается либо bridge, либо интерфейс(ы) уходящий(ие) в коммутатор
- В случае наличия bridge – используется bridge vlan filtering, а так же настройка STP/RSTP/MSTP



	Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx
R	bridge.23	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.29	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.75	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.77	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.78	VLAN	1500	1500	1576	1106.1 kbps	667.7 kbps	
R	bridge.80	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.100	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.114	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.115	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.116	VLAN	1500	1500	1576	7.6 kbps	10.5 kbps	
R	bridge.129	VLAN	1500	1500	1576	2.6 kbps	1744 bps	
R	bridge.130	VLAN	1500	1500	1576	197.6 kbps	13.3 kbps	
R	bridge.137	VLAN	1500	1500	1576	225.4 kbps	115.0 kbps	
R	bridge.154	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.155	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.156	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.161	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.184	VLAN	1500	1500	1576	304.3 kbps	199.0 kbps	
R	bridge.194	VLAN	1500	1500	1576	6.2 kbps	3.0 kbps	
R	bridge.209	VLAN	1500	1500	1576	1304 bps	864 bps	
R	bridge.210	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.211	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.248	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.301	VLAN	1500	1500	1576	0 bps	0 bps	
R	bridge.1111	VLAN	1500	1500	1576	182.2 kbps	5.4 Mbps	

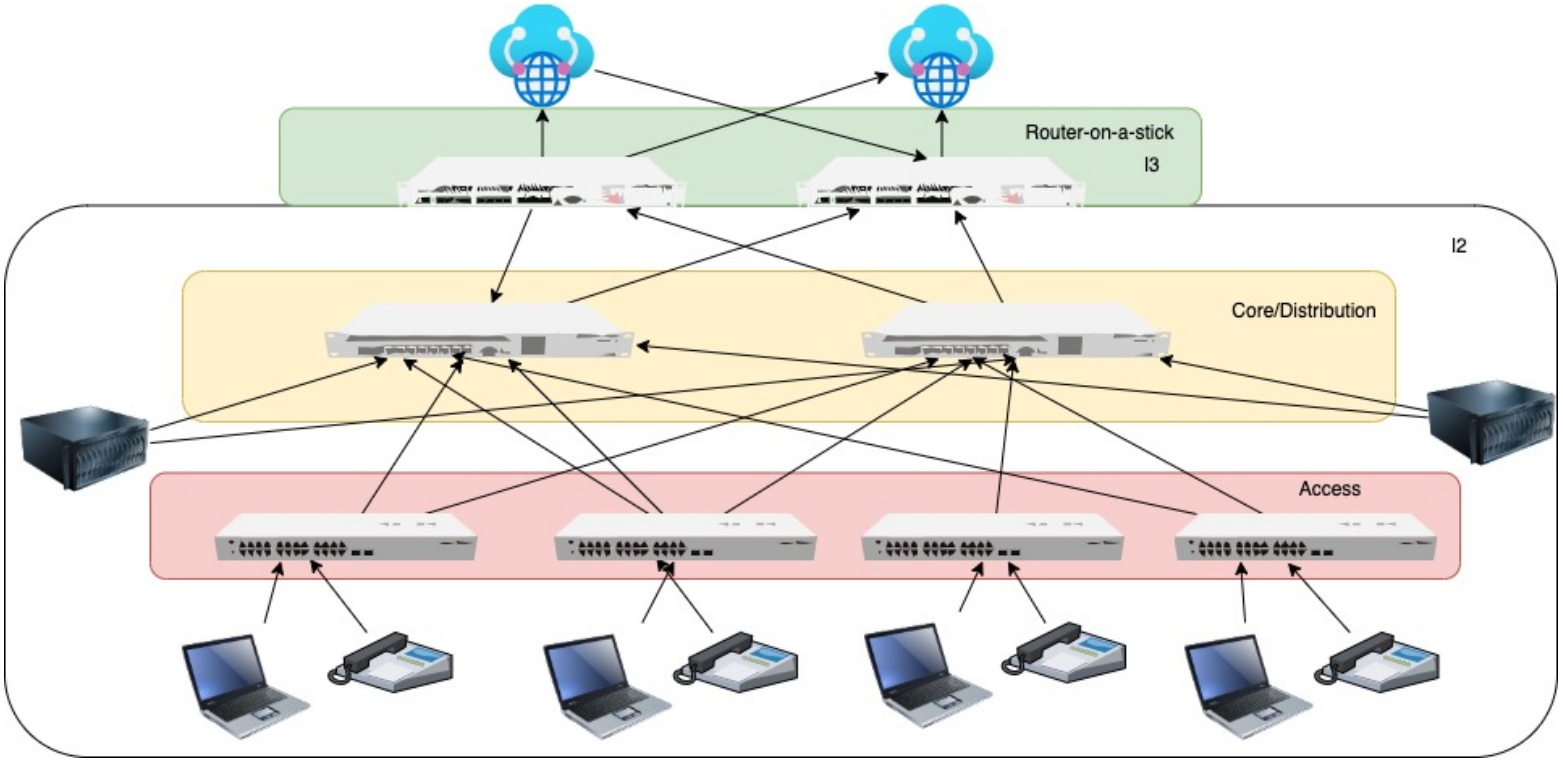
Упрощенная Двухуровневая модель локальной сети ROS6



Упрощенная Двухуровневая модель локальной сети ROS6

- Низкая производительность коммутации
- Посредственный уровень производительности внутренней маршрутизации
- Низкий уровень масштабирования
- На RouterOS 6 используется схема router-on-a-stick и все vlan, а так же маршрутизацию настраиваем на центральном роутере(ax)
- Требуется резервирование шлюза FHRP – в mikrotik VRRP
- Для резервирования подключения серверов используем STP/RSTP/MSTP или bonding, но тогда подключение к одному коммутатору
- Возможно использования объединения коммутаторов по протоколу IEEE 802.1BR но в данный момент без резервирования
- Отказ роутера повлечет сброс соединений
- Можно сделать схемы с активными VRRP интерфейсами в разных VLAN

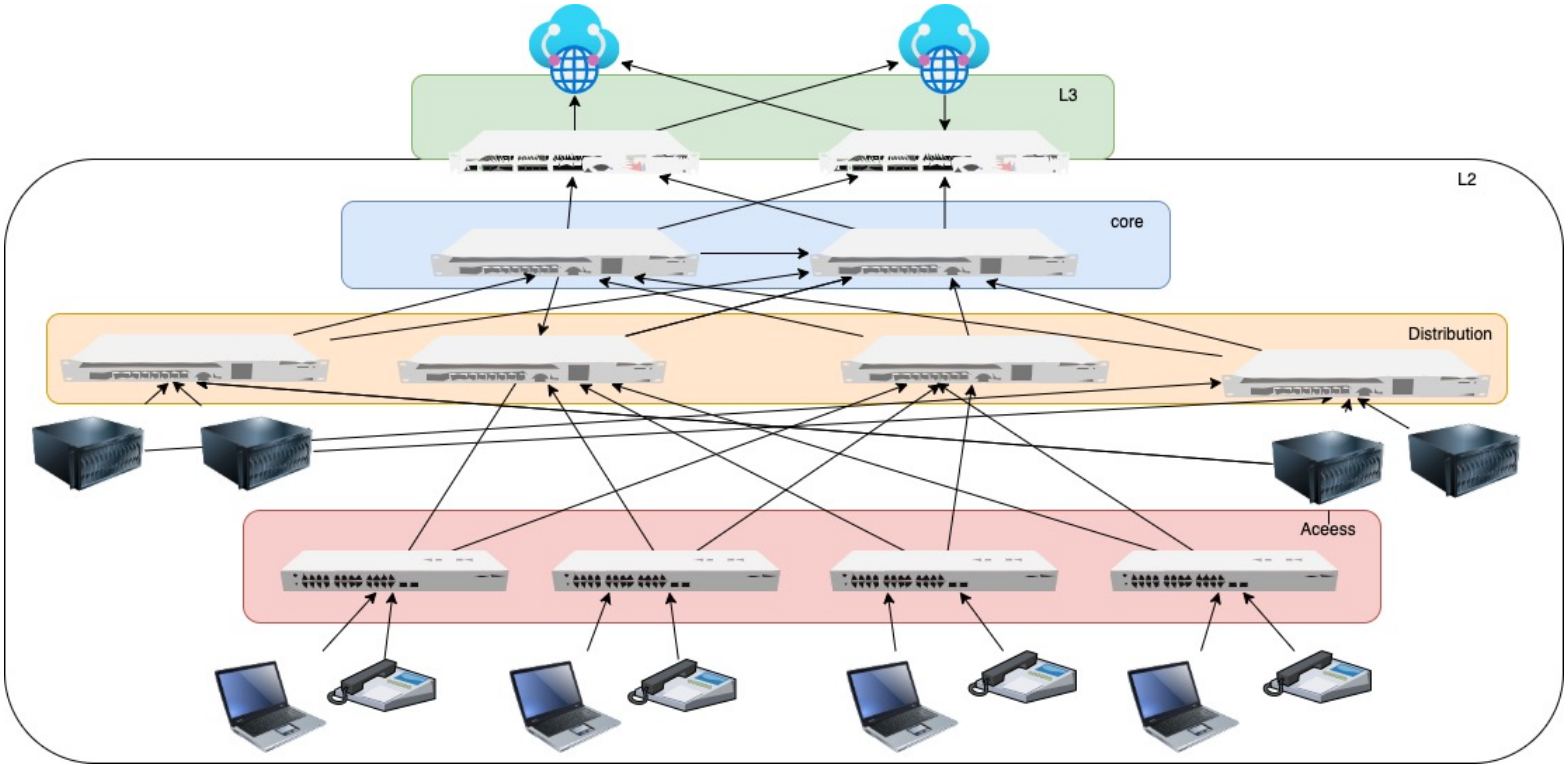
Двухуровневая модель локальной сети ROS6



Двухуровневая модель локальной сети ROS6

- Высокая производительность коммутации
- Посредственный уровень производительности внутренней маршрутизации
- Масштабирование среднее
- Модель известна так же как collapse-core и подходит для не очень больших организаций
- На RouterOS 6 используется схема router-on-a-stick и все vlan, а так же маршрутизацию настраиваем на центральном роутере(ax)
- Требуется резервирование шлюза FHRP – в mikrotik VRRP
- Для резервирования подключения серверов используем STP/RSTP/MSTP или bonding, но тогда подключение к одному коммутатору
- Возможно использования объединения коммутаторов по протоколу IEEE 802.1BR но в данный момент без резервирования
- Отказ роутера повлечет сброс соединений
- Можно сделать схемы с активными VRRP интерфейсами в разных VLAN

Трехуровневая модель локальной сети ROS6



Трехуровневая модель локальной сети ROS6

- Высокая производительность коммутации
- Посредственный уровень производительности внутренней маршрутизации
- Высокий уровень масштабирования
- Модель известна так же как трех-уровневая модель и подходит для больших организаций
- На RouterOS 6 используется схема router-on-a-stick и все vlan, а так же маршрутизацию настраиваем на центральном роутере(ax)
- Требуется резервирование шлюза FHRP – в mikrotik VRRP
- Для резервирования подключения серверов используем STP/RSTP/MSTP или bonding, но тогда подключение к одному коммутатору
- Возможно использования объединения коммутаторов по протоколу IEEE 802.1BR но в данный момент без резервирования
- Отказ роутера повлечет сброс соединений
- Можно сделать схемы с активными VRRP интерфейсами в разных VLAN

03

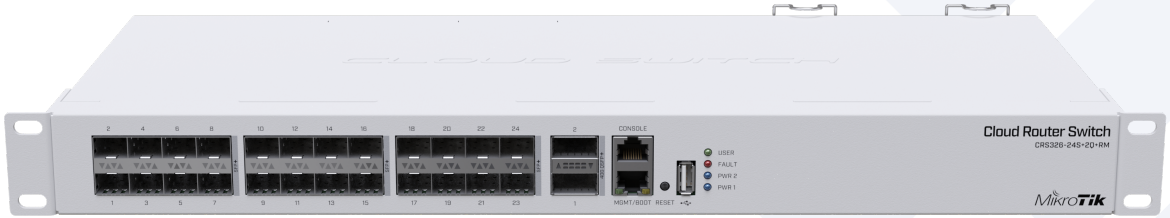
Подход к построению локальных сетей в RouterOS 7

Маршрутизация на аппаратной платформе

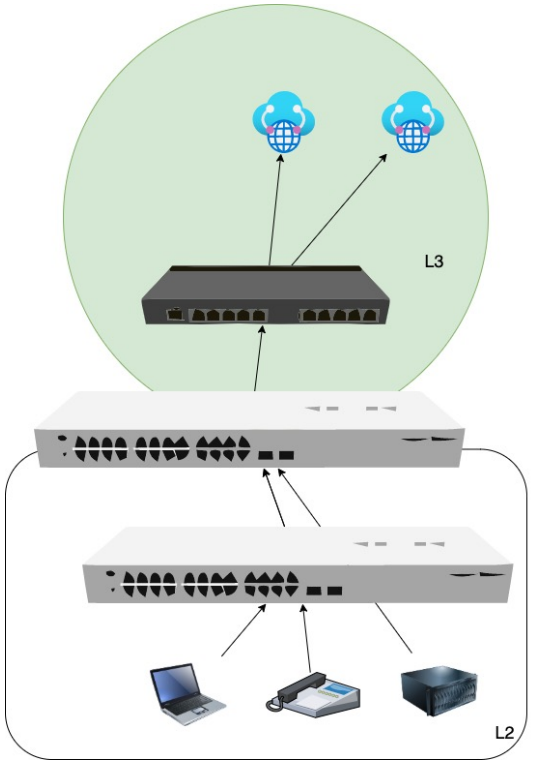
MUoM
Mikrotik User Online Meeting

Основные улучшения в RouterOS 7

- Наличие аппаратной маршрутизации на CRS3XX
- Появление MLAG в CRS3XX
- Аппаратный NAT на CRS317
- Синхронизация connection tracking в VRRP
- Ждем аппаратную маршрутизацию на ipv6
- Аппаратную поддержку VXLAN



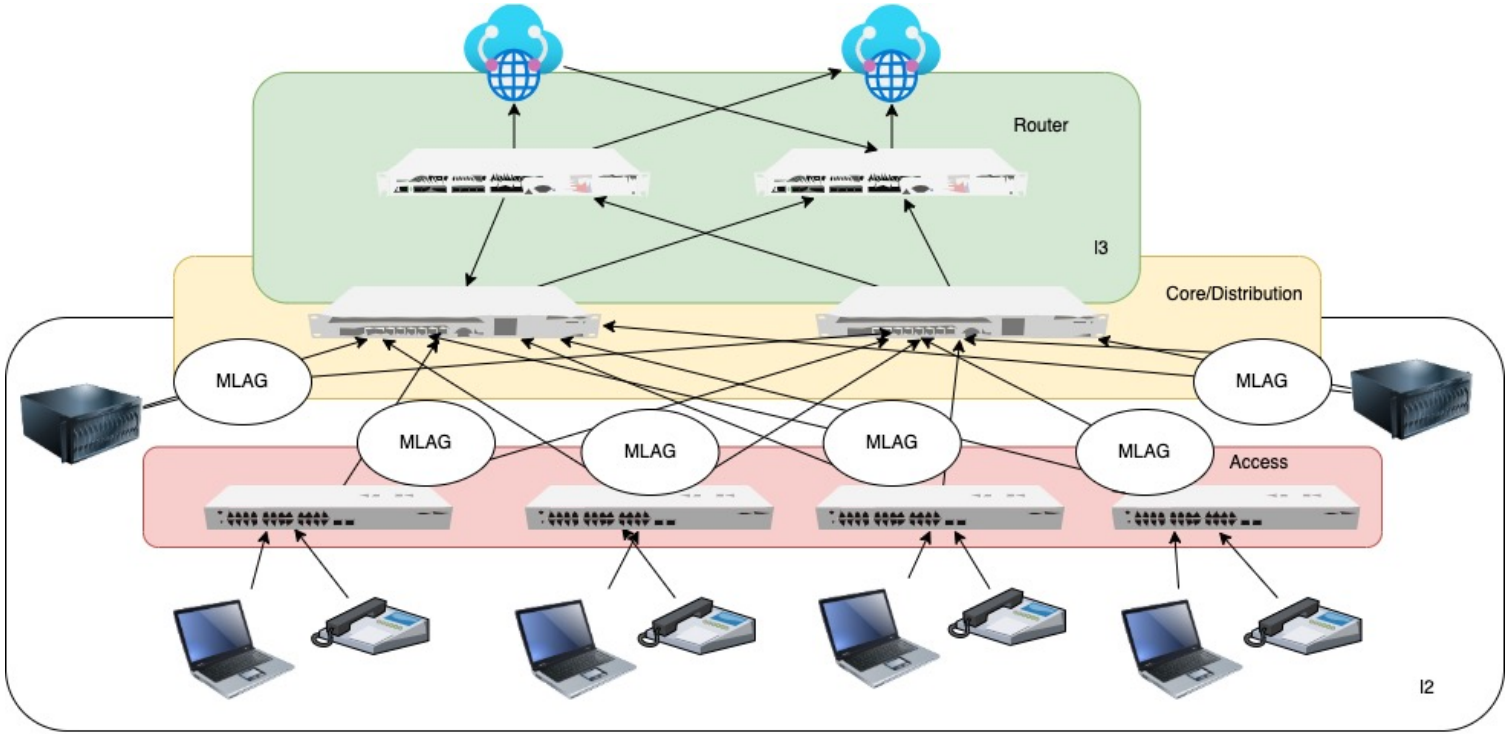
Устройство маленькой локальной сети ROS7



Протоколы и технологии

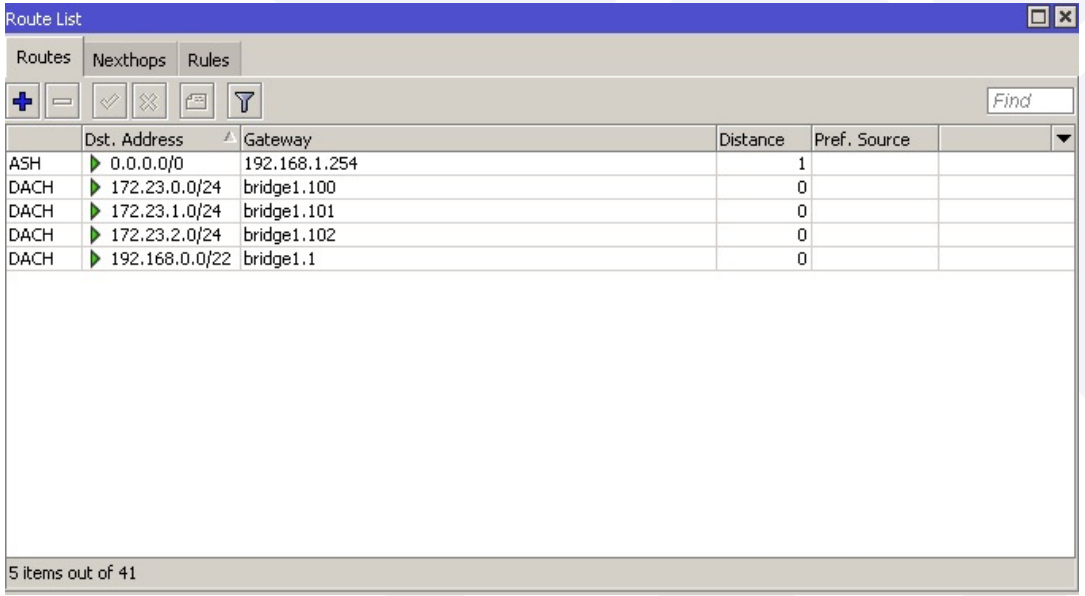
- STP/RSTP/MSTP
- VLAN на коммутаторе
- Граница L2 сети проходит на коммутаторе
- При наличии VLAN маршрутизация между VLAN осуществляется на коммутаторе
- QoS (shaper) на switch rules
- Возможно использовать switch rules
- Высокая скорость маршрутизации между сетями
- Роутер отвечает только за работу NAT, QoS, VPN и внешней защиты
- Низкий уровень масштабирования

Двухуровневая модель локальной сети ROS6



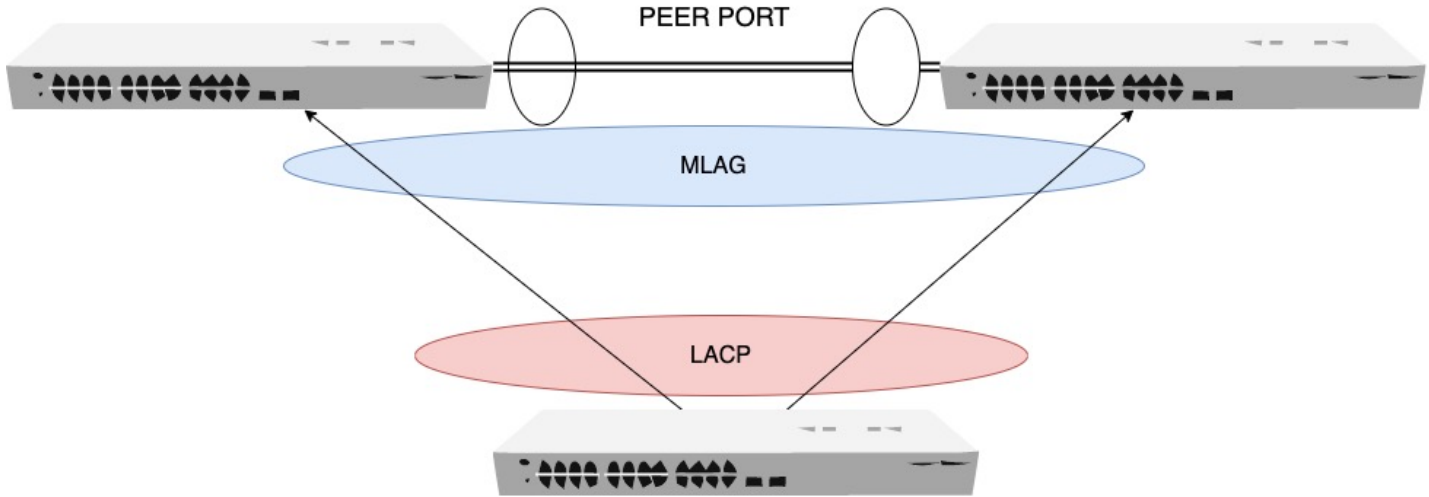
L3 hardware routing

- Виртуальные интерфейсы создастся на коммутаторе
- В качестве интерфейса указывается bridge
- В случае наличия bridge – используется bridge vlan filtering, а так же настройка STP/RSTP/MSTP
- Связь с нижними устройствами можно зарезервировать с использованием MLAG и сохранить



MLAG

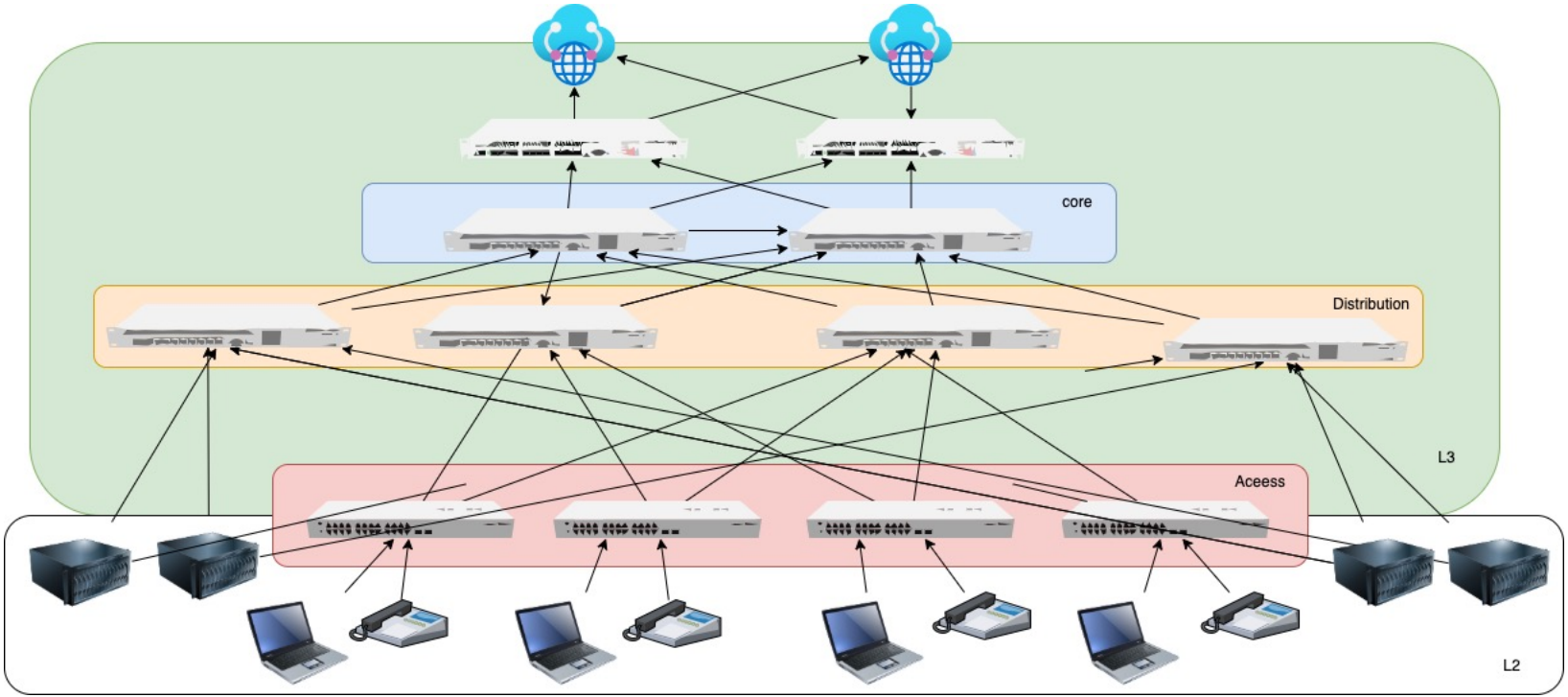
Реализация **MLAG (Multi-Chassis Link Aggregation Group)** в RouterOS 7 позволяет настраивать связи LACP(802.3ad) на двух отдельных устройствах, в то время как клиентское устройство полагает, что оно подключено к одной и той же машине.



Двухуровневая модель локальной сети ROS7

- Высокая производительность коммутации и маршрутизации
- Масштабирование среднее
- Модель известна так же как collapse-core и подходит для не очень больших организаций
- Требуется резервирование шлюза FHRP – в mikrotik VRRP на коммутаторе
- Для резервирования подключения серверов и коммутаторов доступа используем STP/RSTP/MSTP или MLAG
- Возможно использования объединения коммутаторов по протоколу IEEE 802.1BR но в данный момент без резервирования
- Можно сделать схемы с активными VRRP интерфейсами в разных VLAN

Трехуровневая модель локальной сети ROS7



Трехуровневая модель локальной сети ROS7

- Высокая производительность коммутации и маршрутизации
- Высокий уровень масштабирования
- Модель известна так же как трех-уровневая модель и подходит для больших организаций
- Для резервирования подключения серверов используем STP/RSTP/MSTP или MLAG – в некоторых случаях возможен OSPF/BGP
- Можно сделать схемы с активными VRRP интерфейсами в разных VLAN
- Отличное использование резервных соединений с ECMP
- Для передачи маршрутной информации на коммутаторы полезно использовать отдельные OSPF Area NSSA
- Фильтрация на access уровне в switch rules – возможно автосоздание правил через dot1x

Трехуровневая модель локальной сети ROS7

- Стоимость решения
- Сложность внедрения
- Сложность обслуживания
- Более тонкая работа с локальными сетями и адресацией – необходимо планирование адресного пространства
- Пока нет аппаратной маршрутизации для ipv6

04

Немного о железе

Как можем жить с клиентами которые умеют и не умеют dot1x

Аппаратные возможности на MikroTik

Model	ROS	IPv4 Routes	Nexthops	Fasttrack Conn	NAT	ECMP
CRS309-1G-8S+	7.1	16K - 30K	8K	4.5K	8K	
CRS312-4C+8XG	7.1	16K - 30K	8K	2.25K	8K	
CRS317-1G-16S+	7.1	160K - 240K	8K	4.5K	8K [5]	
CRS326-24S+2Q+	7.1	16K - 30K	8K	2.25K	8K	
CRS354-48G-4S+2Q+	7.1	16K - 30K	8K	2.25K	8K	
CRS305-1G-4S+	7.1	13312	4K	-		8
CRS318-1Fi-15Fr-2S	7.1	13312	4K	-		8
CRS318-16P-2S+	7.1	13312	4K	-		8
CRS326-24G-2S+	7.1	13312	4K	-		8
CRS328-24P-4S+	7.1	13312	4K	-		8
CRS328-4C-20S-4S+	7.1	13312	4K	-		8
CCR2116-12G-4S+	7.1	16K - 30K	8K	2.25K	8K	

Количество правил на MikroTik CRS

- На CRS326/328 – примерно по 4 правила на порт
- Печалят crs354
- По большому счету придётся делать статические правила на коммутаторах

Model	Switch Chip	CPU	Cores	Wireless	SFP+ port	ACL rules	Unicast FDB entries	Jumbo Frame (Bytes)
CRS326-24G-2S+	Marvell-98DX3236	800MHz	1	-	+	128	16,000	10218
CRS328-24P-4S+	Marvell-98DX3236	800MHz	1	-	+	128	16,000	10218
CRS328-4C-20S-4S+	Marvell-98DX3236	800MHz	1	-	+	128	16,000	10218
CRS305-1G-4S+	Marvell-98DX3236	800MHz	1	-	+	128	16,000	10218
CRS309-1G-8S+	Marvell-98DX8208	800MHz	2	-	+	680	32 000	10218
CRS317-1G-16S+	Marvell-98DX8216	800MHz	2	-	+	680	128,000	10218
CRS312-4C+8XG	Marvell-98DX8212	650MHz	1	-	+	341	32,000	10218
CRS326-24S+2Q+	Marvell-98DX8332	650MHz	1	-	+	170	32,000	10218
CRS354-48G-4S+2Q+	Marvell-98DX3257	650MHz	1	-	+	170	32,000	10218
CRS354-48P-4S+2Q+	Marvell-98DX3257	650MHz	1	-	+	170	32,000	10218

05

Итоги

MUoM
Mikrotik User Online Meeting

Итоги

- Появление на рынке дешевых высокопроизводительных l3 коммутаторов от Mikrotik позволит строить более масштабные локальные сети
- В маленьких инсталляциях позволит разгрузить роутеры
- Единая операционная система позволяет подходить к автоматизации с единого ключа

Инфо

https://help.mikrotik.com/docs/display/ROS/L3+Hardware+Offloading

https://www.marvell.com/guide.html?type=Switching&psgtype=website

https://ru.wikipedia.org/wiki/%D0%98%D0%B5%D1%80%D0%B0%D1%80%D1%85%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_%D1%81%D0%B5%D1%82%D0%B8

https://help.mikrotik.com/docs/display/ROS/Multi-chassis+Link+Aggregation+Group

https://help.mikrotik.com/docs/display/ROS/CRS3xx+series+switches

https://help.mikrotik.com/docs/display/ROS/Spanning+Tree+Protocol

voxlink MikroTik - TRAINING.RU

Спасибо за внимание!

Пишите свои вопросы в чат Telegram:
@MikTrain

Мои контакты:
Роман Козлов
trainer@mikrotik-training.ru
+7 495 256-9-256
Telegram: @soriel

MUoM
Mikrotik User Online Meeting