

Реализация Policy Routing (PBR) на оборудовании MikroTik

Алексей Чудин
Москва, МУМ 2016



Обо мне

Алексей Чудин

Сертифицированный тренер MikroTik с 2014 г.

Сертификаты:

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

Microsoft: MCP, MCSA

Cisco: CCNA, CCNP (R&S)

www.mikrotik-courses.ru

[Расписание тренингов](#) | [F.A.Q.](#) | [О тренере](#) | [Программа обучения](#) | [Контакты](#)



Официальный тренинг-партнер

MikroTik-Courses.ru — быстрый и эффективный способ изучить возможности MikroTik RouterOS.

[Оставить заявку на обучение](#)



426
специалистов
обучено

663
сертификата
выдано

79%
средний
балл

18
городов
посетили

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

За 2,5 года работы:

- обучено **426** специалистов
- выдано **663** сертификата
(МТСНА, МТСРЕ, МТСВЕ, МТСТСЕ, МТСИНЕ)
- в среднем проводится 1 тренинг в неделю

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

За 2,5 года работы:

- 4 страны СНГ (РФ, РБ, РК, Кыргызстан)
- 18 городов
- География от Калининграда до Владивостока
- **Новые города 2016**: Бишкек, Краснодар, Красноярск, Симферополь, Казань, Пермь, Екатеринбург
- планируется тренинг в Хабаровске (7-9 ноября)

Цель презентации

Рассказать про возможности MikroTik RouterOS в области маршрутизации на основе политик (Policy Routing). Будут рассмотрены такие инструменты как **routing mark**, **VRF**, **route rules**, их применение для работы с несколькими провайдерами, а также будет предложена схема простой реализации IP-VPN в сети провайдера, использующего в своей сети протокол OSPF без использования связки MPLS+BGP

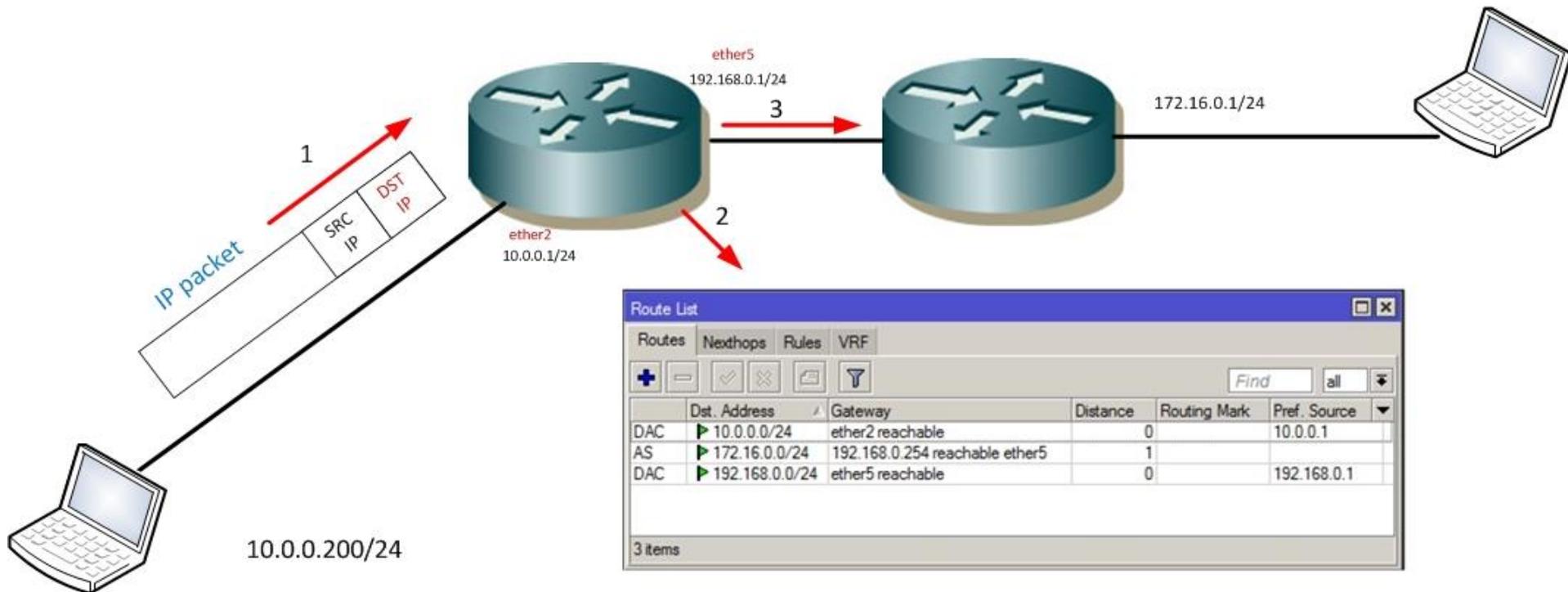
Классическая маршрутизация

Классическая маршрутизация

Как работает маршрутизатор?

Когда на него приходит IP-пакет, то решение о его дальнейшей маршрутизации принимается на основании только заголовка DST IP

Классическая маршрутизация



Policy Routing

(Policy Based Routing, PBR)

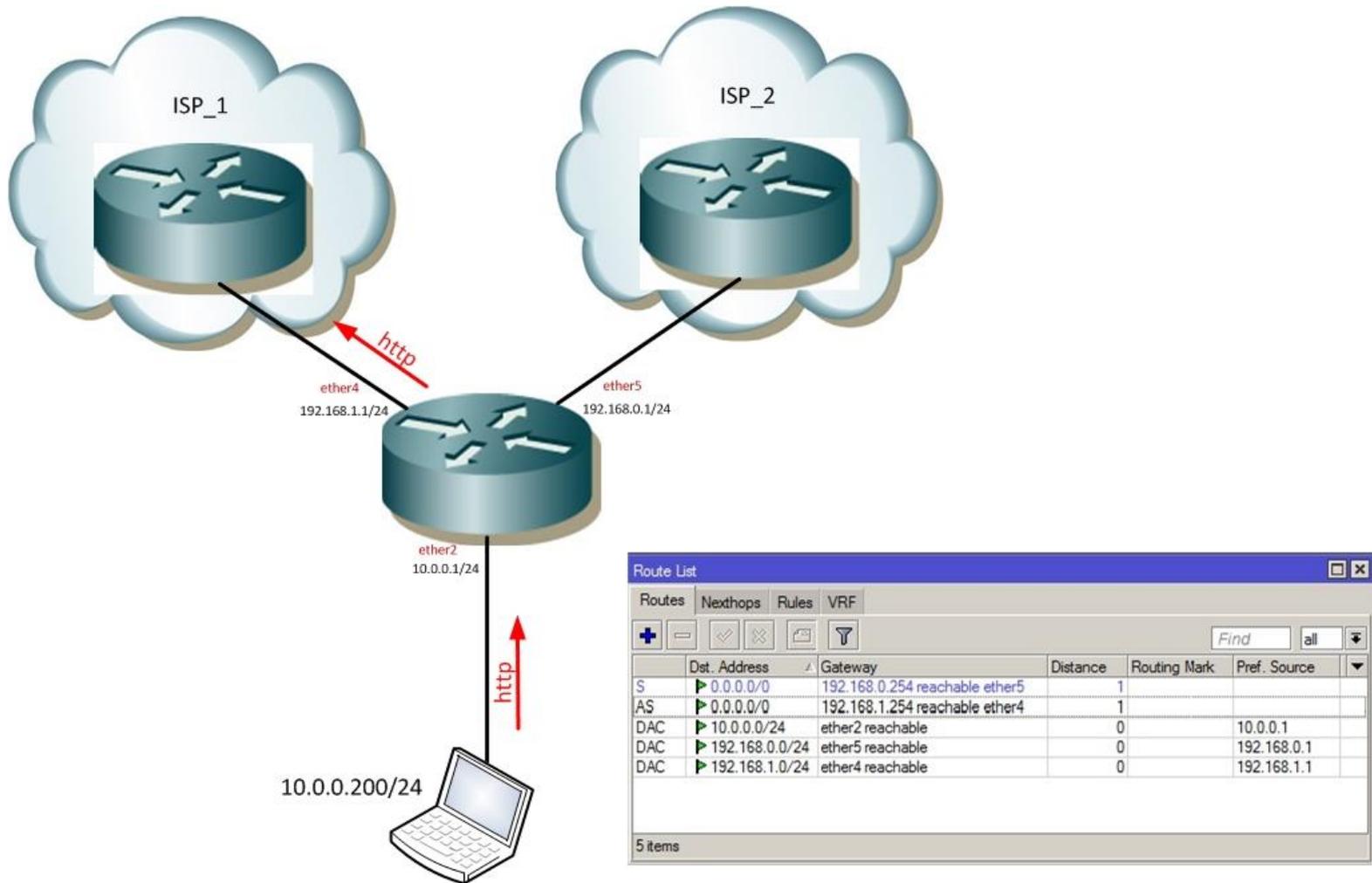
Policy Routing

- Маршрутизатор принимает решение о том, куда слать пакет, на основании каких-то еще параметров, а не DST IP.
- Например, на основании протокола, порта, метки DSCP, SRC IP и т.д., а также многочисленных комбинаций этих параметров

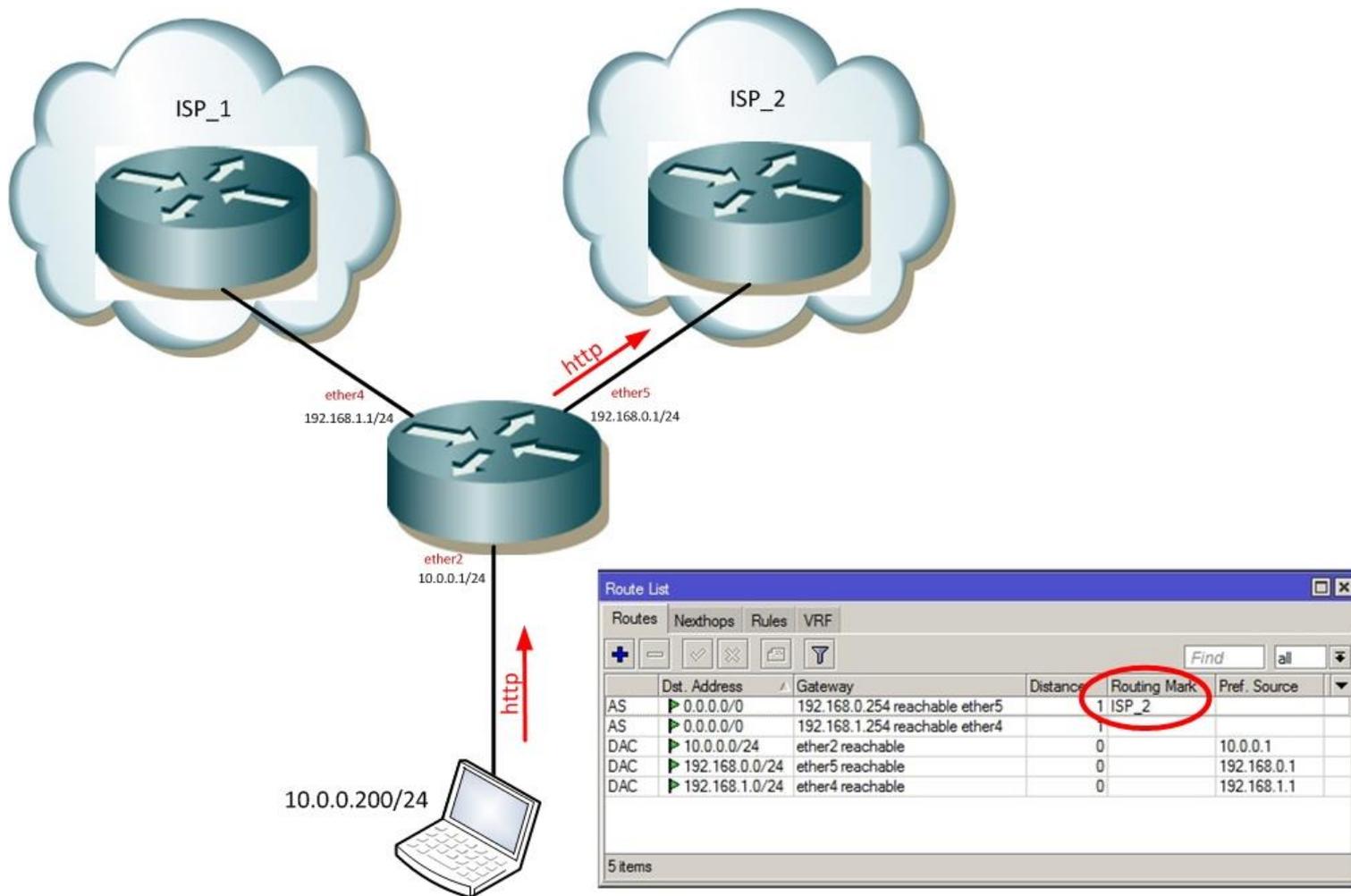
Как работает Policy Routing

- Нам нужны следующие инструменты:
 - Отдельная таблица маршрутизации (**routing mark**)
 - Трафик, помеченный специальным образом, чтобы решение о его маршрутизации принималось на основе этой отдельной таблицы, а не таблицы main (**/ip firewall mangle**)

Как работает Policy Routing



Как работает Policy Routing



Как работает Policy Routing

The screenshot displays the Mikrotik WinBox interface for configuring a Firewall Mangle Rule. The main window shows a list of rules with the following data:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	mar...	prerouting			6 (tcp)		80	ether2		0 B	0

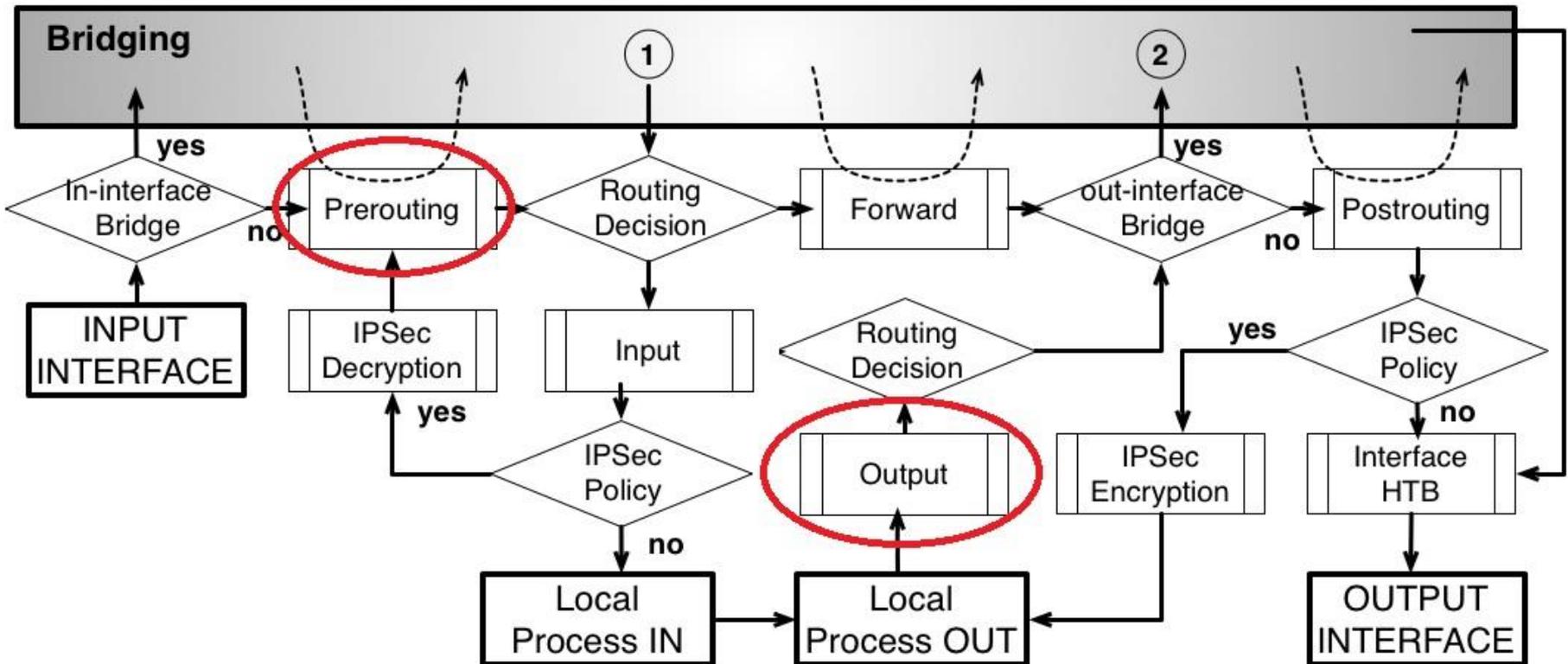
Below the table, two configuration windows are open:

- New Mangle Rule:** Shows the configuration for a new rule. The Chain is set to 'prerouting', Protocol to '6 (tcp)', Dst. Port to '80', and In. Interface to 'ether2'. The Action tab is selected, showing 'mark routing' as the action.
- Mangle Rule <80>:** Shows the configuration for the selected rule. The Action is 'mark routing' and the New Routing Mark is 'ISP_2'. Both the 'Action' and 'New Routing Mark' fields are circled in red.

Как работает Policy Routing

- В каких цепочках мы можем помечать пакеты при помощи **mark routing**?
- Только в **prerouting** и **output** таблицы /ip firewall mangle
- В цепочке **prerouting** мы помечаем трафик, проходящий через маршрутизатор
- В цепочке **output** мы помечаем локальный трафик, выходящий с самого маршрутизатора

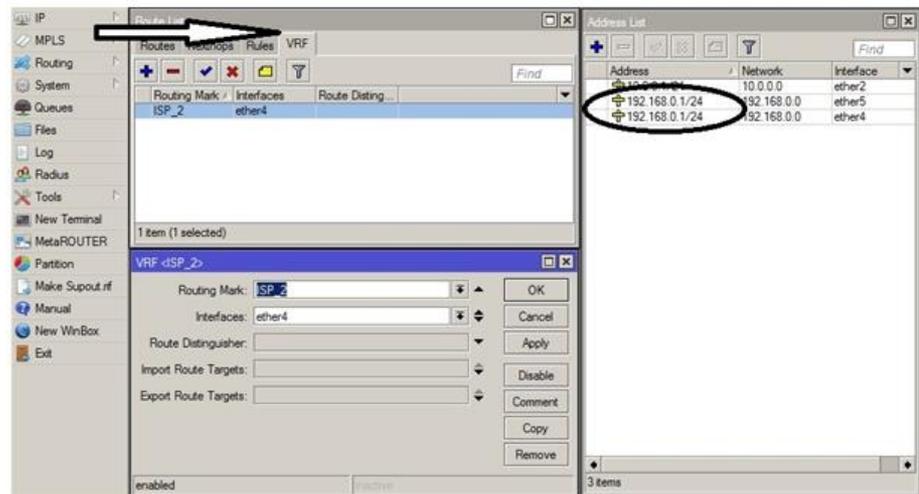
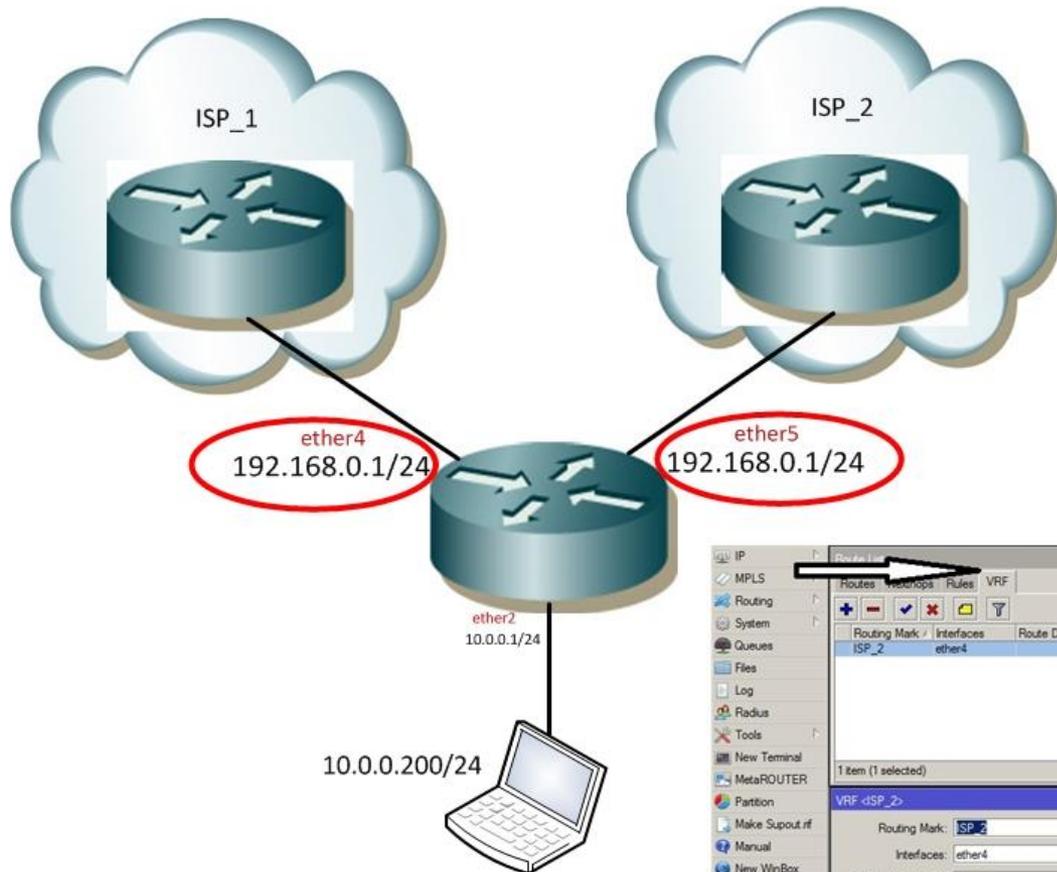
Как работает Policy Routing



Как работает Policy Routing

- Что делать, если оба провайдера имеют одну подсеть?
- Использовать **VRF**
(Virtual Routing & Forwarding)
- Это позволяет нам два одинаковых **Connected** маршрута поместить в изолированные друг от друга таблицы маршрутизации

Как работает Policy Routing



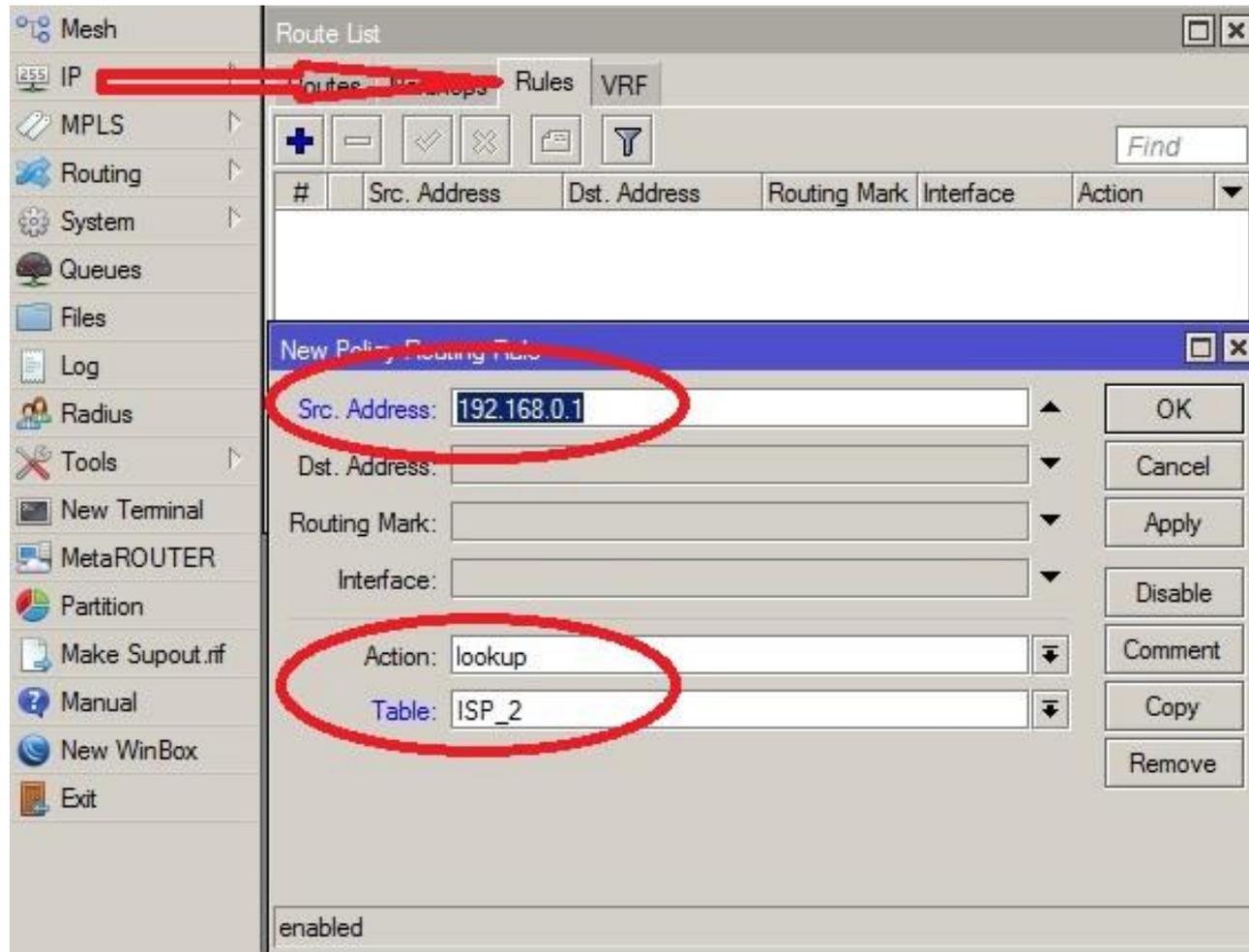
Как работает Policy Routing

	Dest. Address	Gateway	Distance	Routing Mark
AS	0.0.0.0/0	192.168.0.254 on ISP_2 reachab...	1	ISP_2
AS	0.0.0.0/0	192.168.0.254 reachable ether5	1	
DAC	10.0.0.0/24	ether2 reachable	0	
DAC	192.168.0.0/24	ether4 reachable	0	ISP_2
DAC	192.168.0.0/24	ether5 reachable	0	

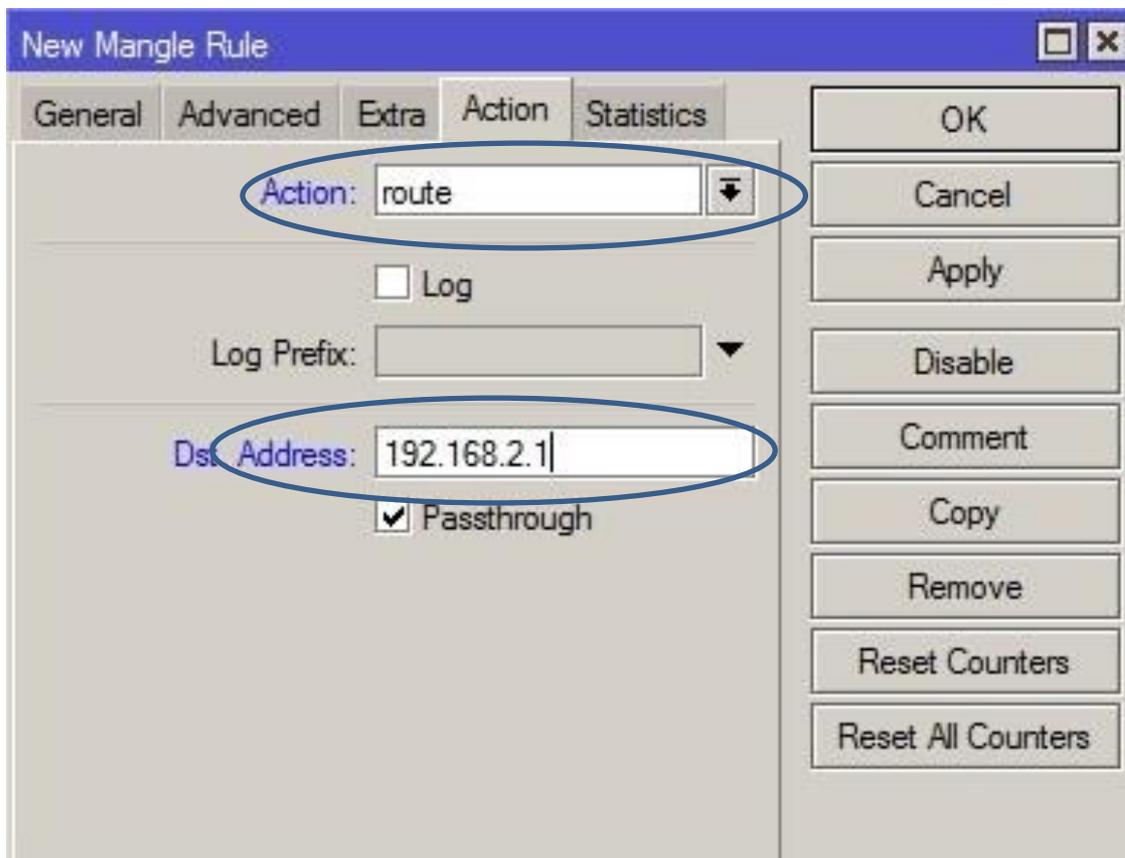
Как работает Policy Routing

- Существует еще один инструмент Policy Routing'a: **/ip route rules**
- Позволяет, например, осуществлять **source routing**, то есть трафик с определенных IP-адресов направлять в отдельную таблицу маршрутизации
- Таким образом, позволяет в ряде случаев упростить настройку и снизить нагрузку на firewall (не нужно использовать маркировку в **/ip firewall mangle**)
- Для примера можно почитать [мою презентацию](#) с МУМа 2014.

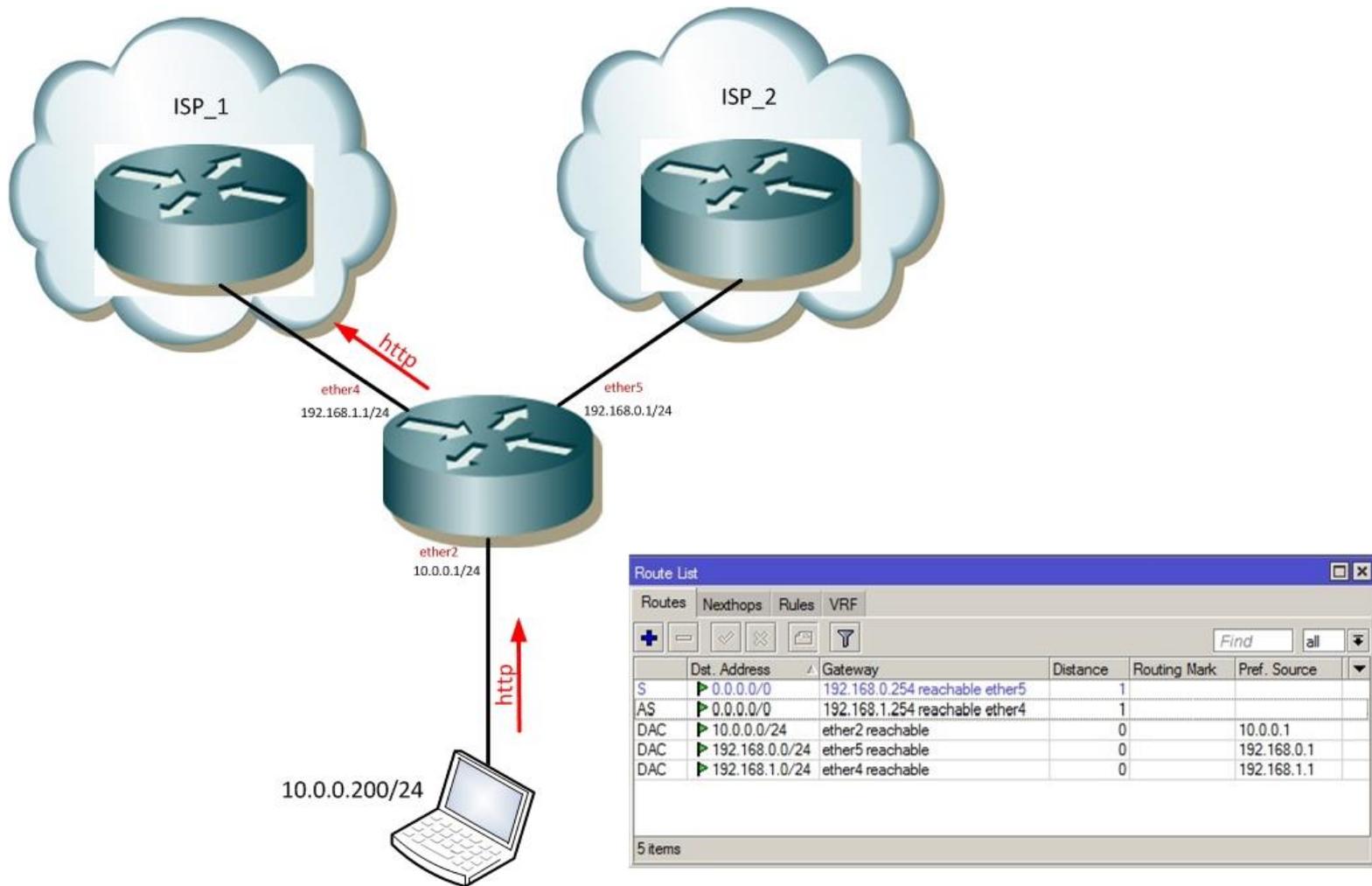
Как работает Policy Routing



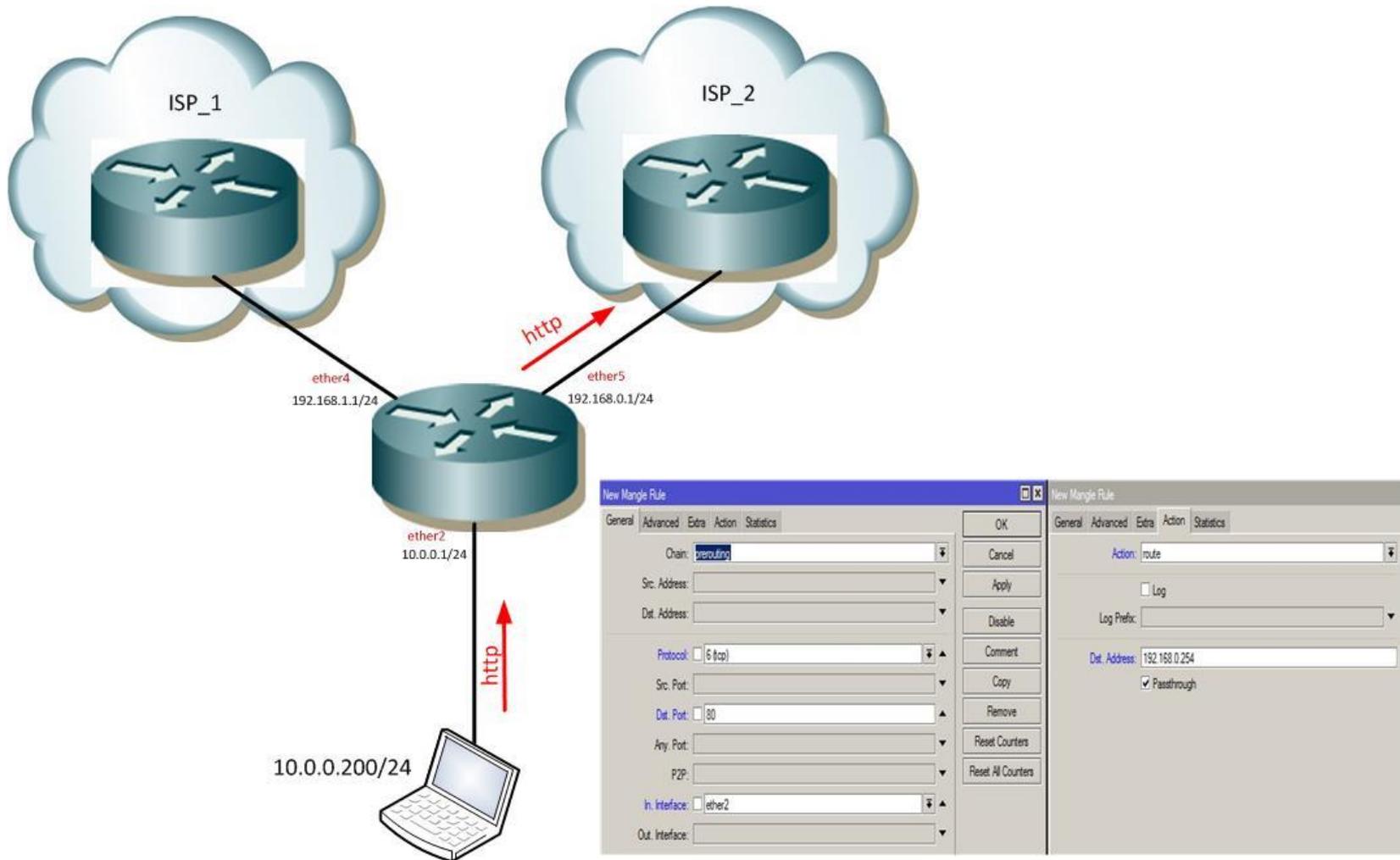
Что нового в Policy Routing



Что нового в Policy Routing



Что нового в Policy Routing



L3 VPN (IP-VPN)

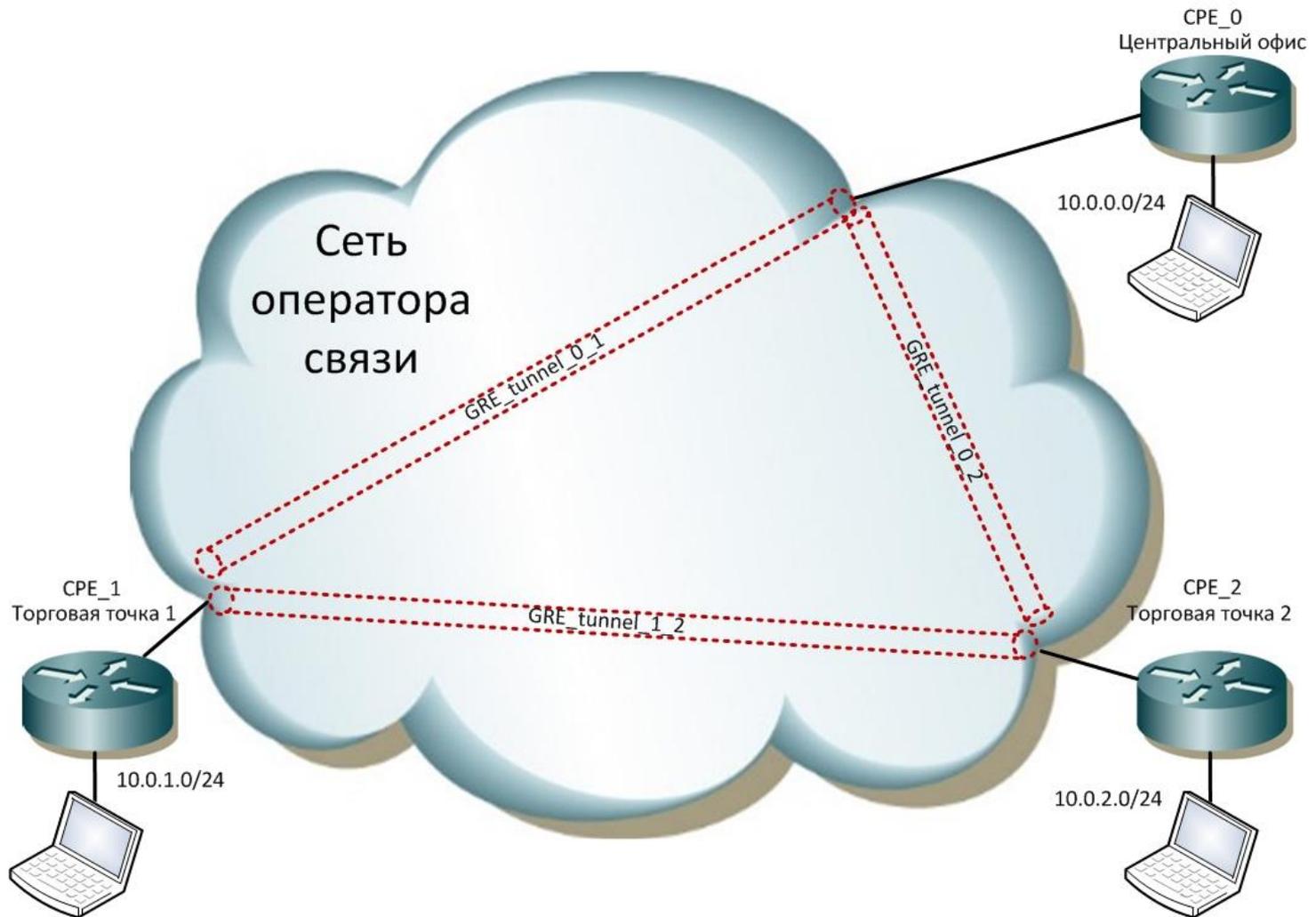
L3 VPN

- Часто бывает ситуация, когда корпоративному клиенту нужно сделать VPNы внутри сети одного провайдера, с определенным в договоре уровнем сервиса (SLA), а также чтобы ответственность за работу этих VPN-ов нес сам провайдер
- Это могут быть VPN-ы между центральным офисом и многочисленными торговыми точками, филиалами, складами, в том числе в других городах (если это крупный провайдер)
- Адресацию сетей назначает сам клиент
- Зачастую выход в Интернет на удаленных объектах не нужен, либо он организуется через центральный офис

L3 VPN



L3 VPN



L3 VPN

- Настройка GRE-туннеля очень проста:

	Routes	Nexthops	Rules	VRF
AS	0.0.0.0/0	192.168.0.254 reachable ether5		
DAC	10.0.0.0/24	ether5 reachable		
AS	10.0.1.0/24	gre-tunnel1 reachable		
DAC	192.168.0.0/24	ether5 reachable		

4 items

Interface

Name: gre-tunnel1

Type: GRE Tunnel

MTU: []

Actual MTU: []

L2 MTU: []

Local Address: []

Remote Address: 172.16.16.2

IPsec Secret: []

Keepalive: []

DSCP: inherit

Dont Fragment: no

Clamp TCP MSS

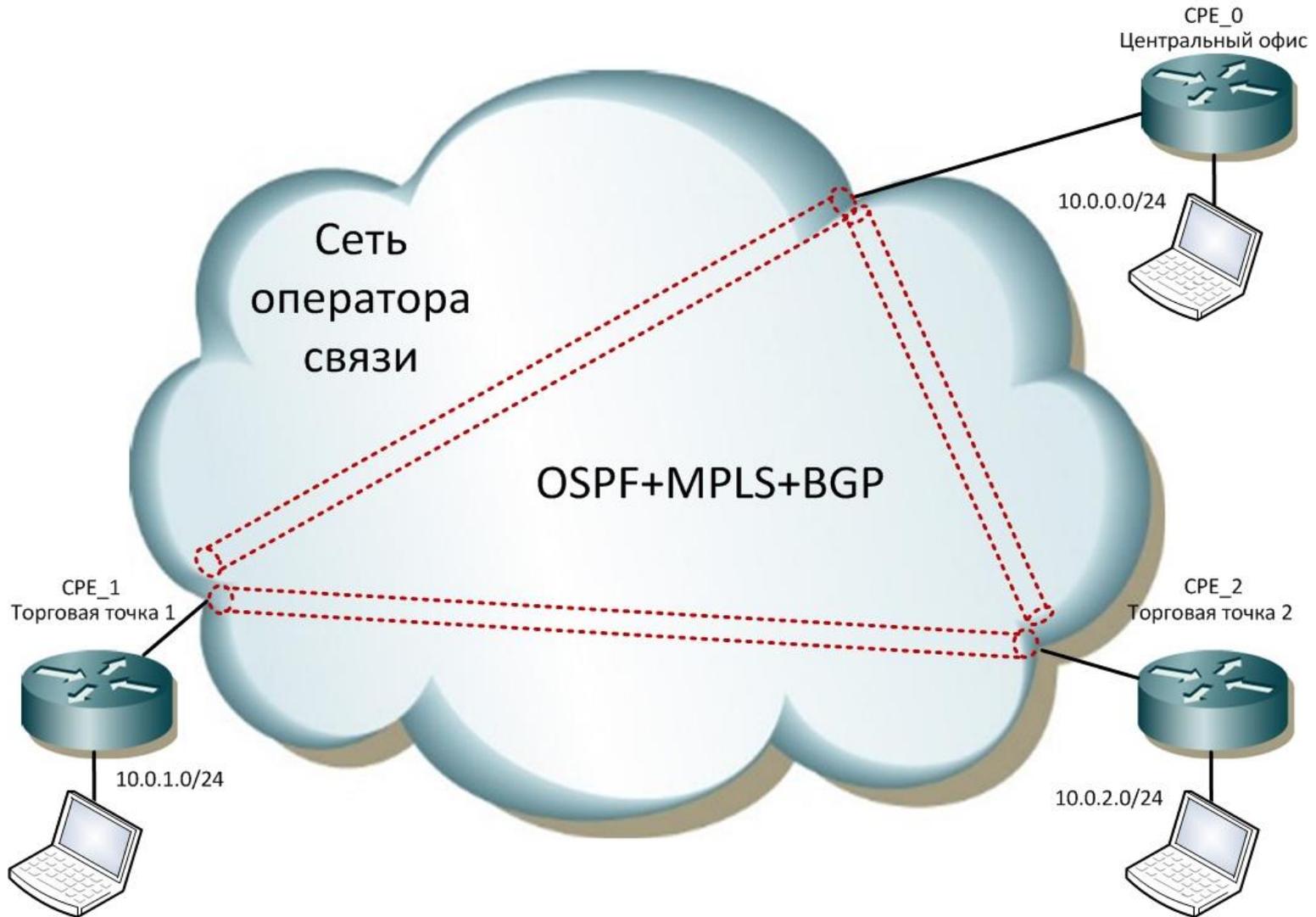
Allow Fast Path

enabled running slave

L3 VPN

- К плюсам такого подхода можно отнести:
 - простоту конфигурации
 - низкую нагрузку на CPU
 - большую пропускную способность из-за отсутствия шифрования по умолчанию
- К минусам:
 - большое количество статических маршрутов, если делаем туннели между всеми объектами
 - в случае переезда объекта придется перенастраивать все туннели

L3 VPN



L3 VPN

- К плюсам такого подхода можно отнести:
 - универсальность

- К минусам:
 - уровень знаний и навыков сетевого администратора, потому что в случае поиска и устранения неисправностей искать их придется на всех уровнях: в MPLS, BGP, OSPF

L3 VPN

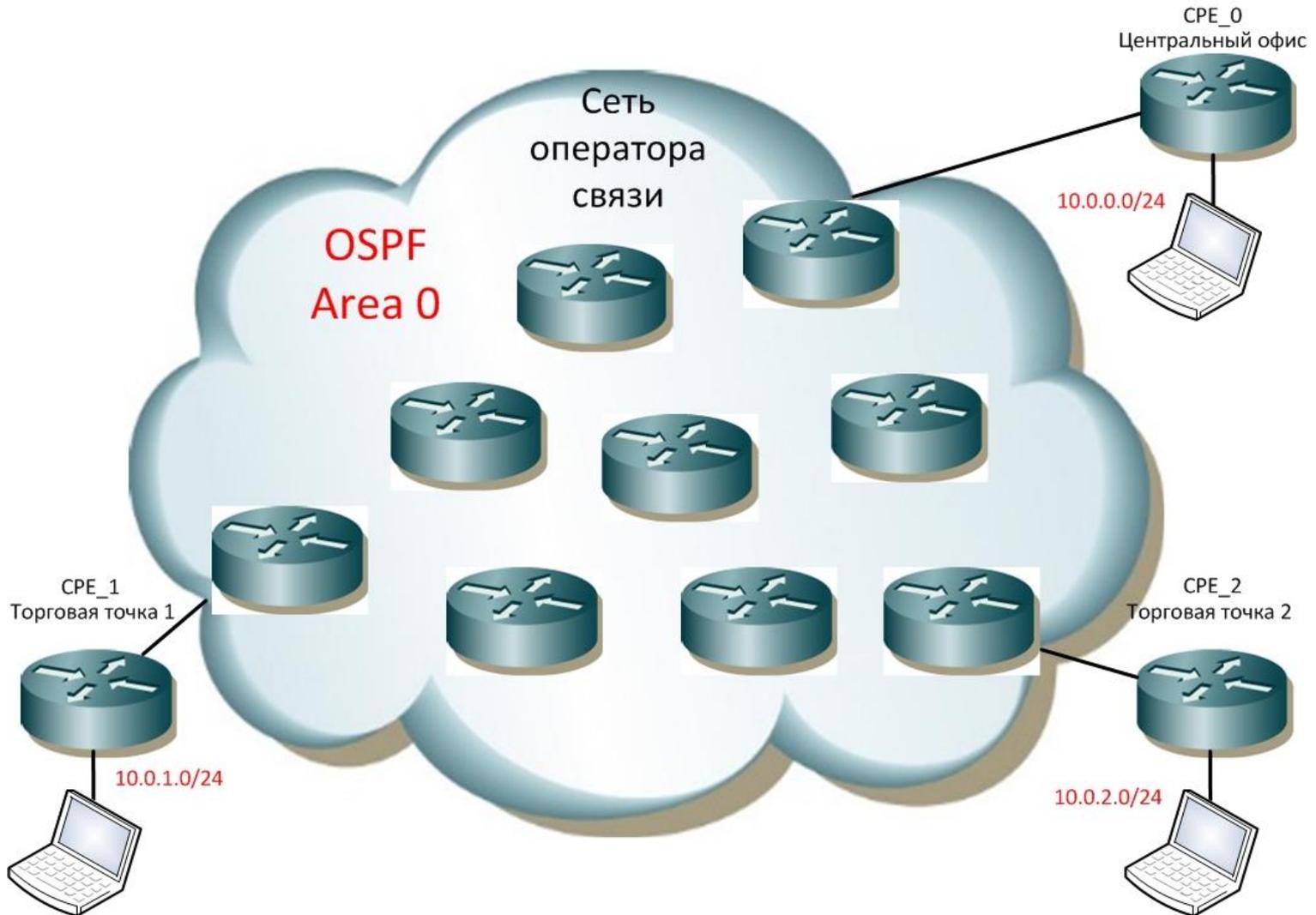
- Вариант L3 VPN, который я хочу предложить, основан на использовании протокола OSPF и Policy Routing без туннелей и связки OSPF+BGP+MPLS

L3 VPN

В чем суть проблемы, почему нужны такие сложные схемы ли с туннелями, либо через связку OSPF+BGP+MPLS?

Проблема в том, что подсети разных корпоративных клиентов могут быть одинаковыми

L3 VPN



L3 VPN

- Исходные данные: клиентские подсети для нас (провайдера) являются чужими и нет смысла их анонсировать по OSPF в общую сеть как свои, потому что другие клиенты не должны знать, как до этих сетей можно добраться
- Мы эти подсети считаем внешними (external) и соответствующим образом анонсируем в нашу сеть
- Внешние (external) маршруты обладают одной полезной для нас особенностью: их можно фильтровать, то есть не допускать их встраивания в основную (main) таблицу маршрутизации
- Либо их можно встроить их в другую таблицу!
- Для этого воспользуемся возможностями инструмента **/routing filter**

L3 VPN

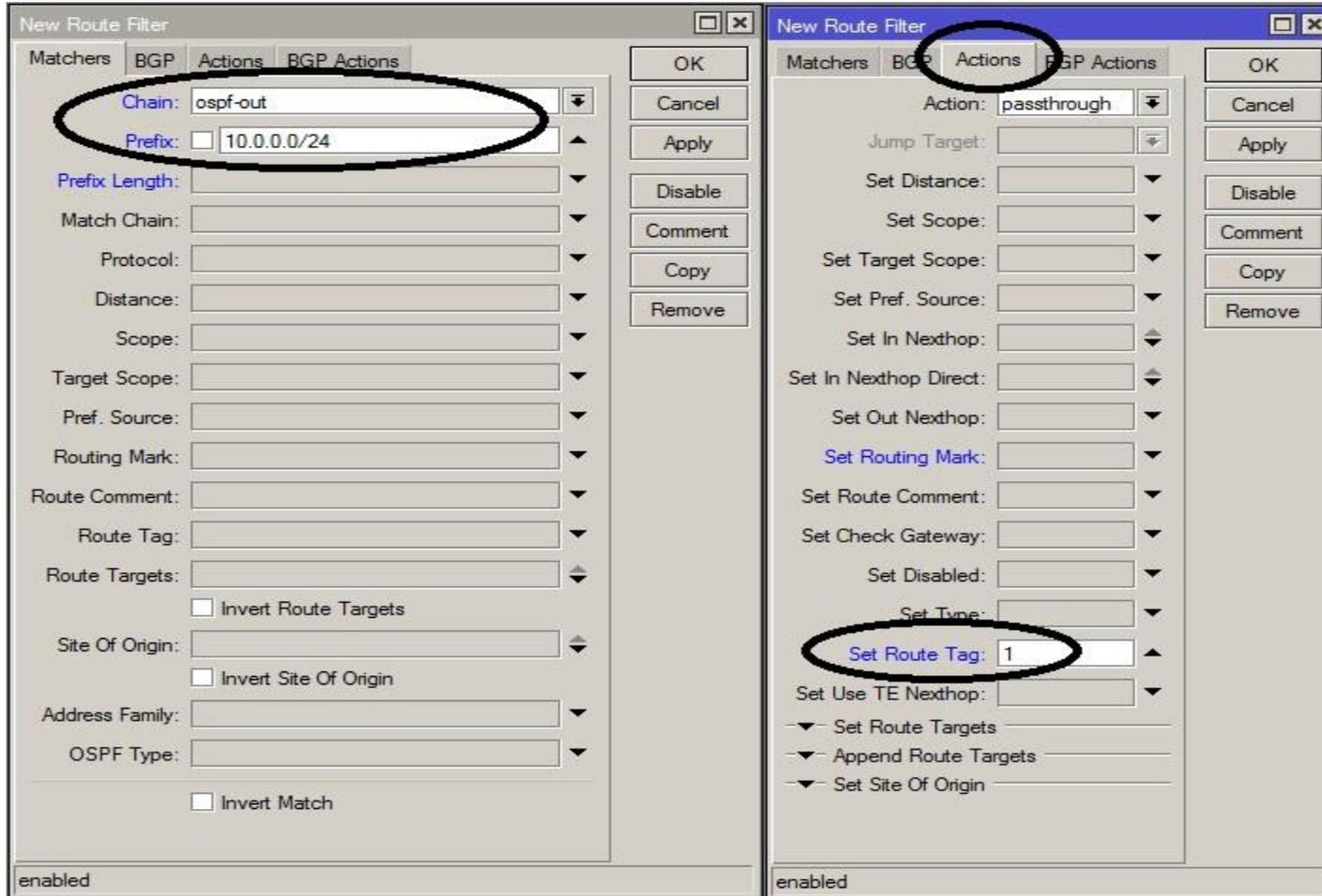
- Настройка OSPF нашего роутера у клиента (CPE)

The screenshot displays the Mikrotik WinBox interface. On the left is a sidebar menu with options like Routing, System, Queues, Files, Log, Radius, Tools, and New Terminal. The main window is divided into three panes:

- OSPF Instance:** Shows a table with columns for Network and Area. A row is visible for Network 192.168.0.0/24 in the backbone area. The 'Instance' and 'Networks' tabs are circled.
- OSPF Instance <default> Configuration:** Shows fields for Name (default), Router ID (0.0.0.1), and various redistribution options. The 'Redistribute Connected Routes' dropdown is set to 'as type 1' and is circled.
- Address List:** A table with columns for Address, Network, and Interface. Two entries are shown: 10.0.0.1/24 on ether2 and 192.168.0.1/24 on ether5. The first entry is circled.

L3 VPN

- Настройка /routing filter на CPE



L3 VPN

- Рассмотрим, что мы наконфигурили 😊
- Мы распространяем внутри сети OSPF топологическую информацию о том, как достичь сети 10.0.0.0/24
- Маршрут распространяется с **tag**'ом, который отвечает за идентификацию конкретного корпоративного клиента и его VPN-ов
- Зачем нам нужен этот **tag**?
- Чтобы эти маршруты, относящиеся только к одному клиенту, при помощи фильтра перевести в отдельную таблицу маршрутизации!
- Остается это настроить! Делаем это на каждом маршрутизаторе в нашей сети при помощи фильтров в направлении **in**

L3 VPN

- Для этого нужно набрать команду на каждом роутере в нашей OSPF-сети:

/routing filter

add chain=ospf-in route-tag=1 set-routing-mark=1

- Это если у нас один корпоративный клиент. Если много, то тиражируем эти правила следующим образом:

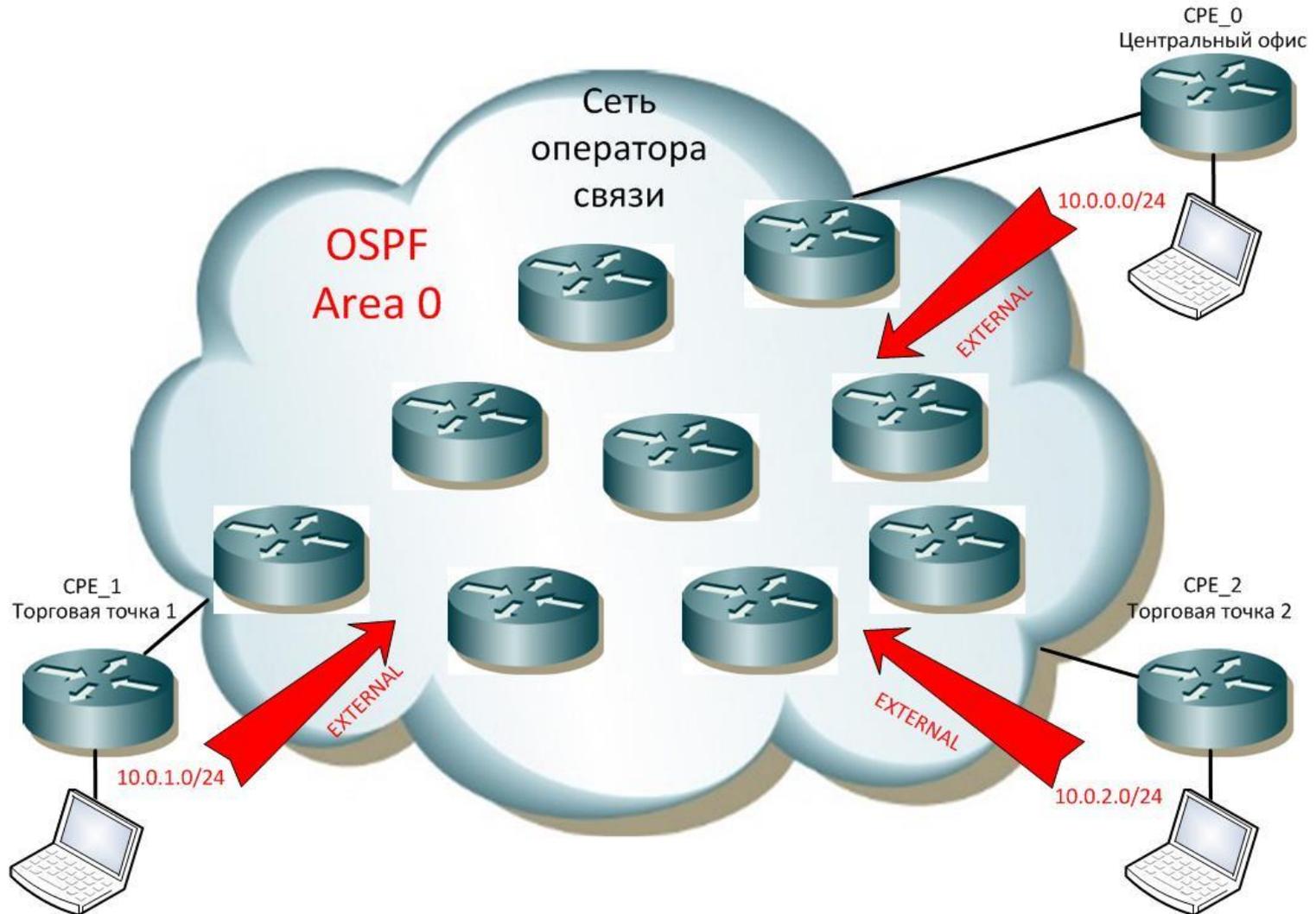
L3 VPN

A1 fx add

route_tag.txt

	A	B	C	D	E	F
1	add	chain=ospf-in	route-tag=1	set-routing-mark=1		
2	add	chain=ospf-in	route-tag=2	set-routing-mark=2		
3	add	chain=ospf-in	route-tag=3	set-routing-mark=3		
4	add	chain=ospf-in	route-tag=4	set-routing-mark=4		
5	add	chain=ospf-in	route-tag=5	set-routing-mark=5		
6	add	chain=ospf-in	route-tag=6	set-routing-mark=6		
7	add	chain=ospf-in	route-tag=7	set-routing-mark=7		
8	add	chain=ospf-in	route-tag=8	set-routing-mark=8		
9	add	chain=ospf-in	route-tag=9	set-routing-mark=9		
10	add	chain=ospf-in	route-tag=10	set-routing-mark=10		
11	add	chain=ospf-in	route-tag=11	set-routing-mark=11		
12	add	chain=ospf-in	route-tag=12	set-routing-mark=12		
13	add	chain=ospf-in	route-tag=13	set-routing-mark=13		
14	add	chain=ospf-in	route-tag=14	set-routing-mark=14		
15	add	chain=ospf-in	route-tag=15	set-routing-mark=15		
16	add	chain=ospf-in	route-tag=16	set-routing-mark=16		
17	add	chain=ospf-in	route-tag=17	set-routing-mark=17		
18	add	chain=ospf-in	route-tag=18	set-routing-mark=18		
19	add	chain=ospf-in	route-tag=19	set-routing-mark=19		
20	add	chain=ospf-in	route-tag=20	set-routing-mark=20		
21	add	chain=ospf-in	route-tag=21	set-routing-mark=21		
22	add	chain=ospf-in	route-tag=22	set-routing-mark=22		
23	add	chain=ospf-in	route-tag=23	set-routing-mark=23		
24	add	chain=ospf-in	route-tag=24	set-routing-mark=24		
25	add	chain=ospf-in	route-tag=25	set-routing-mark=25		
26	add	chain=ospf-in	route-tag=26	set-routing-mark=26		
27	add	chain=ospf-in	route-tag=27	set-routing-mark=27		
28	add	chain=ospf-in	route-tag=28	set-routing-mark=28		
29	add	chain=ospf-in	route-tag=29	set-routing-mark=29		
30						
31						

L3 VPN



L3 VPN

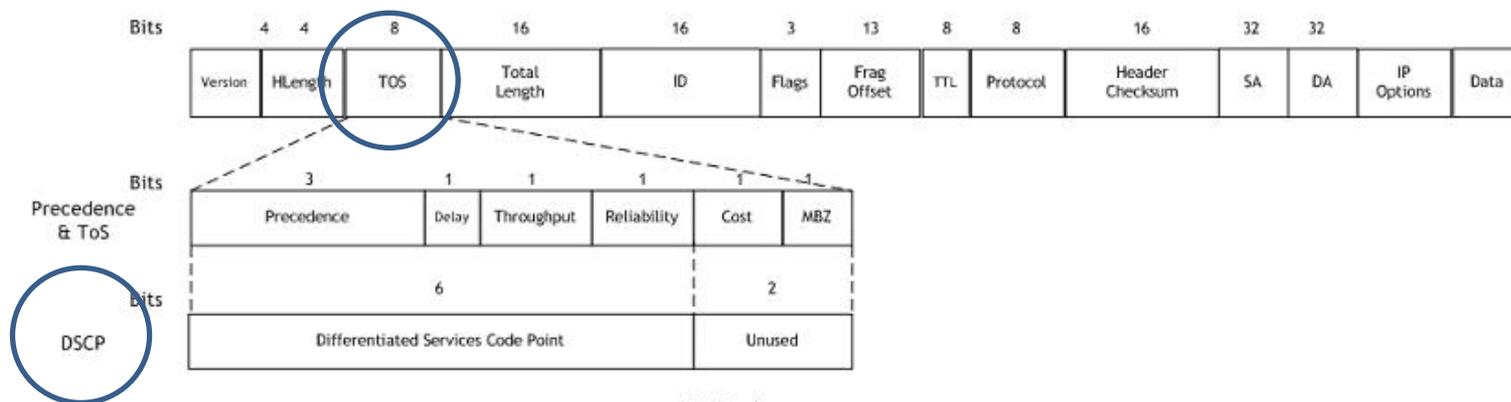
- Итого, что мы имеем на данный момент:
 1. На CPE-роутерах мы анонсируем подсеть клиента на внешнюю, причем с tag'ом
 2. Эти маршруты пытаются встроиться в таблицу **main** на каждом роутере в нашей OSPF-сети, но фильтры устанавливают их в свои отдельные таблицы маршрутизации, относящиеся только к конкретному корпоративному клиенту

L3 VPN

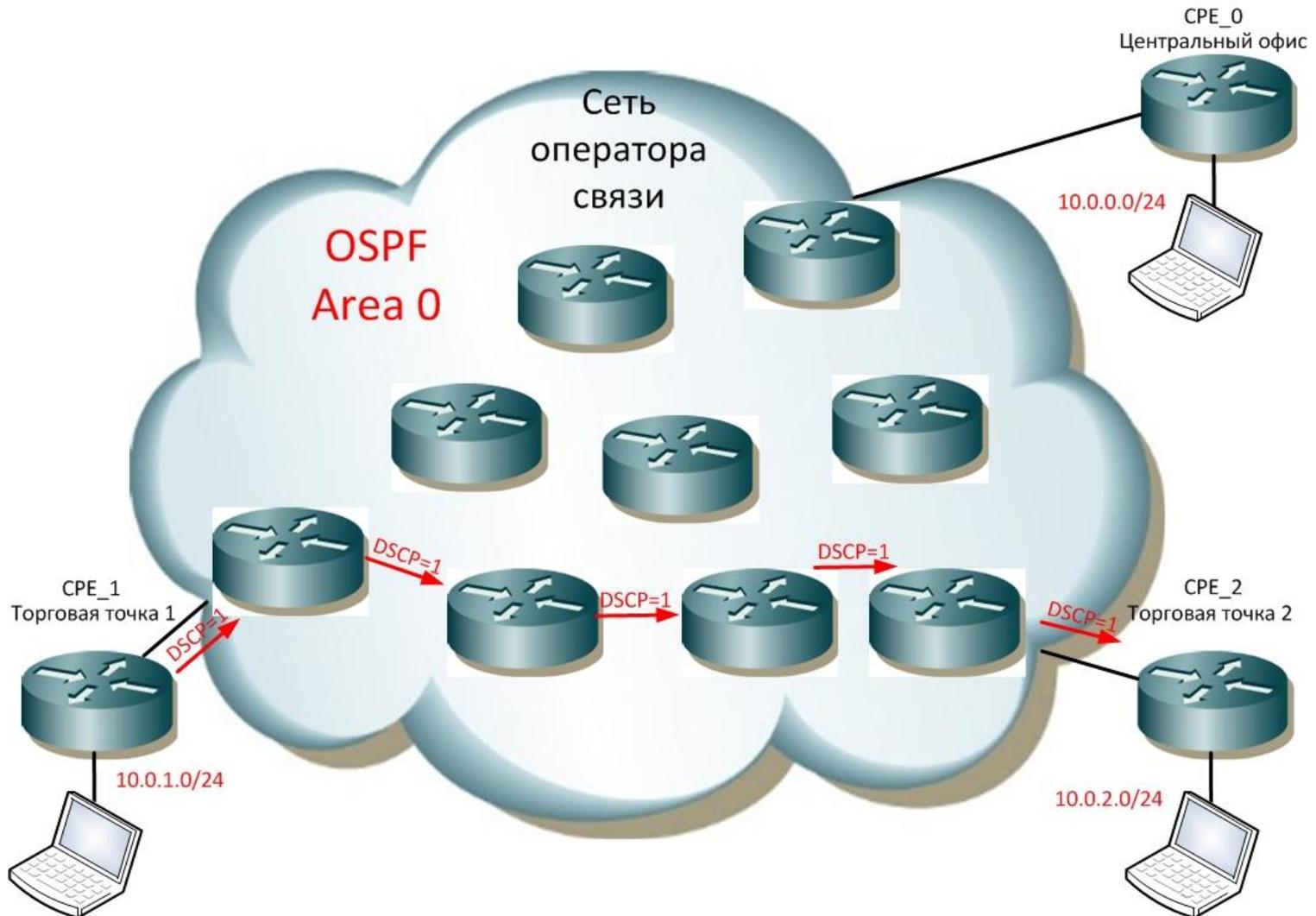
- Вопрос: какие же IP-пакеты будут искать свои маршруты в этих таблицах маршрутизации?
- По умолчанию все пакеты используют таблицу **main**
- Нам нужно отметить необходимые нам пакеты при помощи **mark routing**
- Но это уже на самом роутере мы используем помечаем трафик, а нам надо изначально как-то пометить трафик внутри VPN-ов одного корпоративного клиента и на основе этой метки (которая переносится в IP-пакете от роутера к роутеру) уже делать **action=mark routing**

L3 VPN

- В качестве такой метки нам подойдет поле **DSCP**, которое принимает значения от 0 до 63, и которое мы можем менять сами при помощи все того же инструмента **/ip firewall mangle**



L3 VPN



L3 VPN

A1 fx add

route_tag.txt

	A	B	C	D	E	F	G
1	add	action=mark-routing	chain=prerouting	dscp=1	new-routing-mark=DSCP1	passthrough=no	
2	add	action=mark-routing	chain=prerouting	dscp=2	new-routing-mark=DSCP2	passthrough=no	
3	add	action=mark-routing	chain=prerouting	dscp=3	new-routing-mark=DSCP3	passthrough=no	
4	add	action=mark-routing	chain=prerouting	dscp=4	new-routing-mark=DSCP4	passthrough=no	
5	add	action=mark-routing	chain=prerouting	dscp=5	new-routing-mark=DSCP5	passthrough=no	
6	add	action=mark-routing	chain=prerouting	dscp=6	new-routing-mark=DSCP6	passthrough=no	
7	add	action=mark-routing	chain=prerouting	dscp=7	new-routing-mark=DSCP7	passthrough=no	
8	add	action=mark-routing	chain=prerouting	dscp=8	new-routing-mark=DSCP8	passthrough=no	
9	add	action=mark-routing	chain=prerouting	dscp=9	new-routing-mark=DSCP9	passthrough=no	
10	add	action=mark-routing	chain=prerouting	dscp=10	new-routing-mark=DSCP10	passthrough=no	
11	add	action=mark-routing	chain=prerouting	dscp=11	new-routing-mark=DSCP11	passthrough=no	
12	add	action=mark-routing	chain=prerouting	dscp=12	new-routing-mark=DSCP12	passthrough=no	
13	add	action=mark-routing	chain=prerouting	dscp=13	new-routing-mark=DSCP13	passthrough=no	
14	add	action=mark-routing	chain=prerouting	dscp=14	new-routing-mark=DSCP14	passthrough=no	
15	add	action=mark-routing	chain=prerouting	dscp=15	new-routing-mark=DSCP15	passthrough=no	
16	add	action=mark-routing	chain=prerouting	dscp=16	new-routing-mark=DSCP16	passthrough=no	
17	add	action=mark-routing	chain=prerouting	dscp=17	new-routing-mark=DSCP17	passthrough=no	
18	add	action=mark-routing	chain=prerouting	dscp=18	new-routing-mark=DSCP18	passthrough=no	
19	add	action=mark-routing	chain=prerouting	dscp=19	new-routing-mark=DSCP19	passthrough=no	
20							

L3 VPN

- Насколько “тяжело” роутеру менять поле DSCP в каждом пакете?

L3 VPN

- На скорости 100 Мб/с: (тестировалось на RouterOS 6.34)
- hAP lite: **~30 %**
- RB850Gx2: **~16%**
- CCR1009-8G-1S-1S+: **0%**

- Как видим, не так уж и тяжело 😊

L3 VPN

- Исходя из того, что поле DSCP может принимать значения 0-63, можно сделать вывод, что в нашей сети может быть всего 64 корпоративных клиента с их L3 VPN-ами...
- Мало?

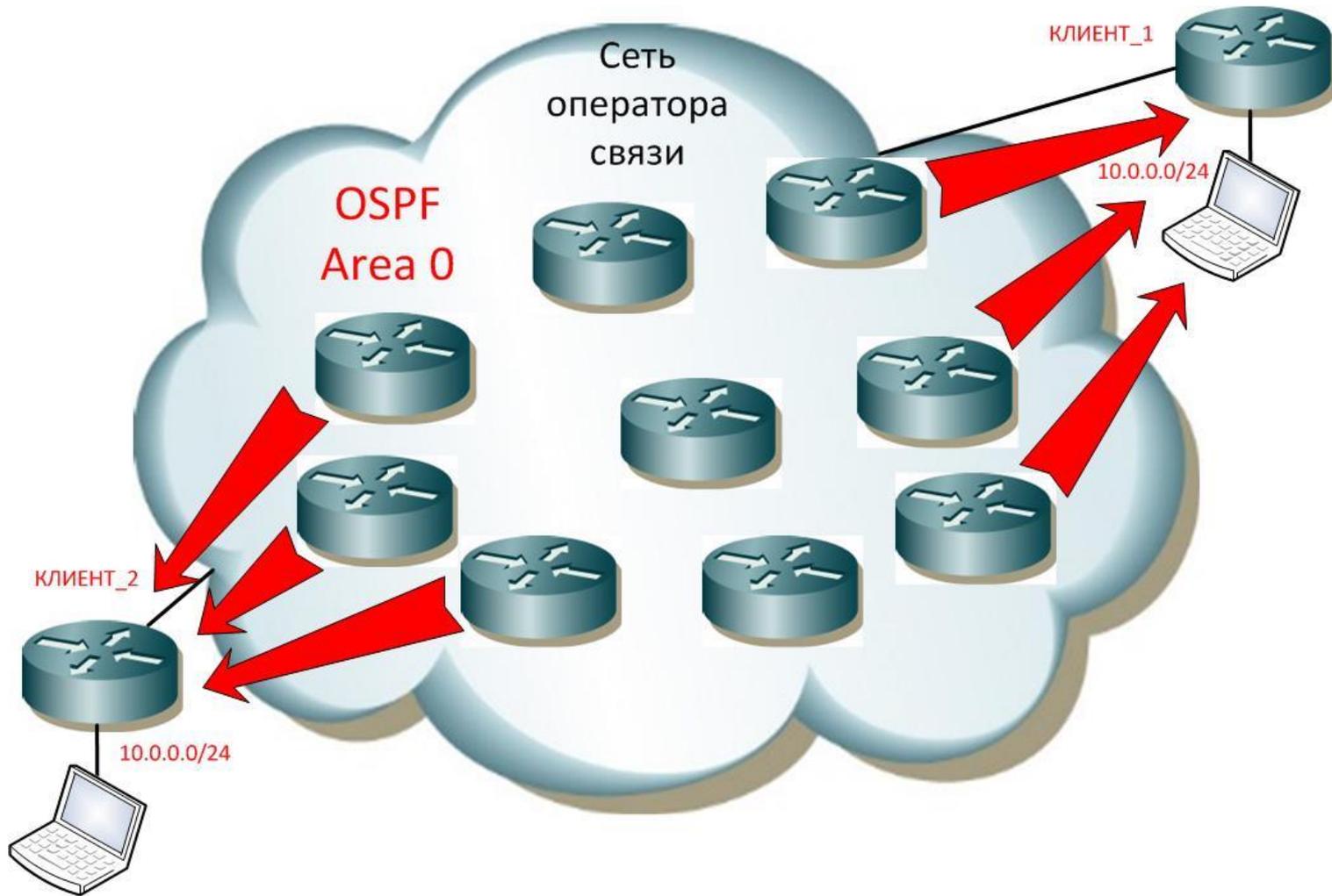
L3 VPN

- Кому мало, есть еще поле **TTL**, которое мы тоже можем менять и учитывать при проверке 😊 Количество только клиентов в этом случае возрастает до 16000 😊

L3 VPN

- Но проблему пересекающихся сетей мы еще пока не решили

L3 VPN



L3 VPN

- Выход есть: action=netmap в таблице NAT!
- /ip firewall nat
- add action=netmap chain=srcnat out-interface=ether4
- src-address=10.0.0.0/24 to-addresses=192.168.10.0/24
- add action=netmap chain=dstnat in-interface=ether1
- src-address=192.168.10.0/24 to-addresses=10.0.0.0/24

Знание – сила!

- Что нужно, чтобы уверенно ориентироваться в маршрутизации?
- Ответ очевиден: посетить тренинг MikroTik **MTCRE** по маршрутизации!

Расписание тренингов

Минск	MTCRE	3-6 октября	подробности	зарегистрироваться
Симферополь	MTCNA	11-13 октября	подробности	зарегистрироваться
	MTCRE	14-16 октября	подробности	зарегистрироваться
Новосибирск	MTCNA	24-26 октября	подробности	зарегистрироваться
	MTCRE	27-29 октября	подробности	зарегистрироваться
	MTCWE	31 октября – 2 ноября	подробности	зарегистрироваться
Хабаровск	MTCNA	7-9 ноября	подробности	зарегистрироваться
Владивосток	MTCNA	14-16 ноября	подробности	зарегистрироваться
	MTCRE	17-19 ноября	подробности	зарегистрироваться
	MTCWE	21-23 ноября	подробности	зарегистрироваться
Иркутск	MTCNA	28-30 ноября	подробности	зарегистрироваться
	MTCSTCE	1-3 декабря	подробности	зарегистрироваться
Москва	MTCNA	12-14 декабря	подробности	зарегистрироваться
	MTCRE	15-17 декабря	подробности	зарегистрироваться

Вопросы?

Пишите на

training@mikrotik-courses.ru

Хорошего дня!
Спасибо за ваше
внимание!