

VPN с компьютера в корпоративную сеть

Алексей Чудин
Москва, МУМ 2018



Обо мне

Алексей Чудин

Сертифицированный тренер MikroTik с 2014 г.

Сертификаты:

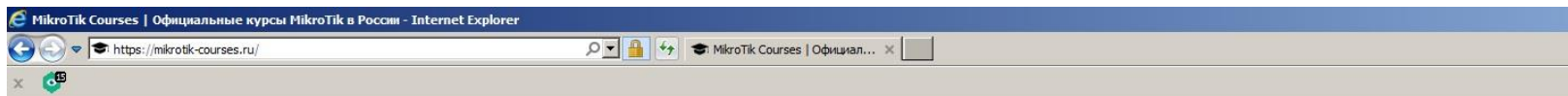
MikroTik: MTCNA, MTCRE, MTCWE, MTCTSE,
MTCUME, MTCINE, MTCIPv6E,

MikroTik Trainer №0246

Microsoft: MCP, MCSA

Cisco: CCNA, CCNP (R&S)

www.mikrotik-courses.ru



[Обучение](#) [Поддержка](#) [Контакты](#)



Официальный тренинг-партнер

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

[Оставить заявку на обучение](#)



1671

2549

82%

50

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

За 4,5 года работы:

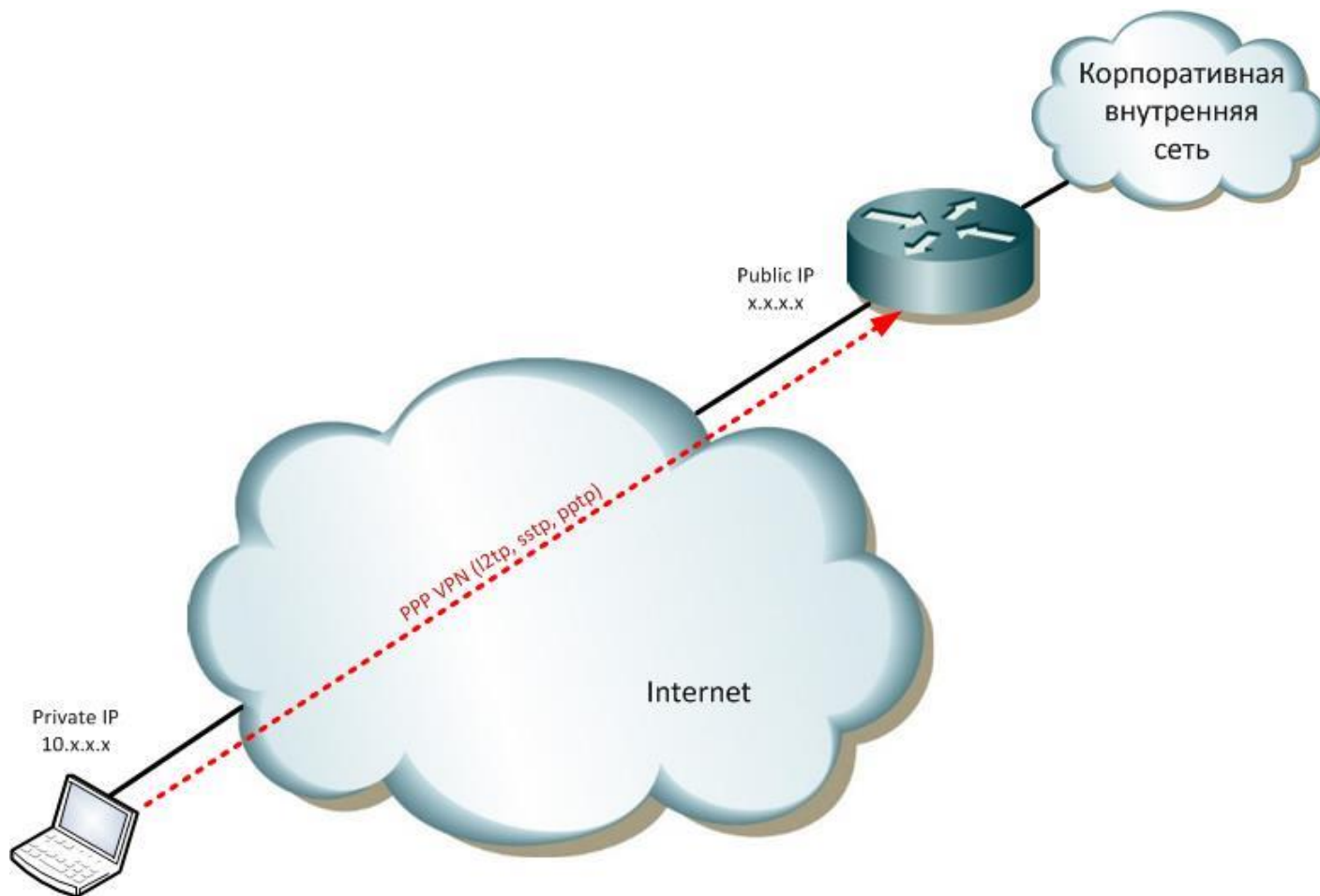
- Обучен **1671** специалист
- выдано **2549** сертификатов
(MTCNA, MTCRE, MTCWE, MTCTSE, MTCINE, MTCIPv6E)
- в среднем проводится 2 тренинга в неделю
- 4 тренера:
 - Алексей Чудин
 - Александр Романов
 - Николай Кузнецов
 - Максим Бусов

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

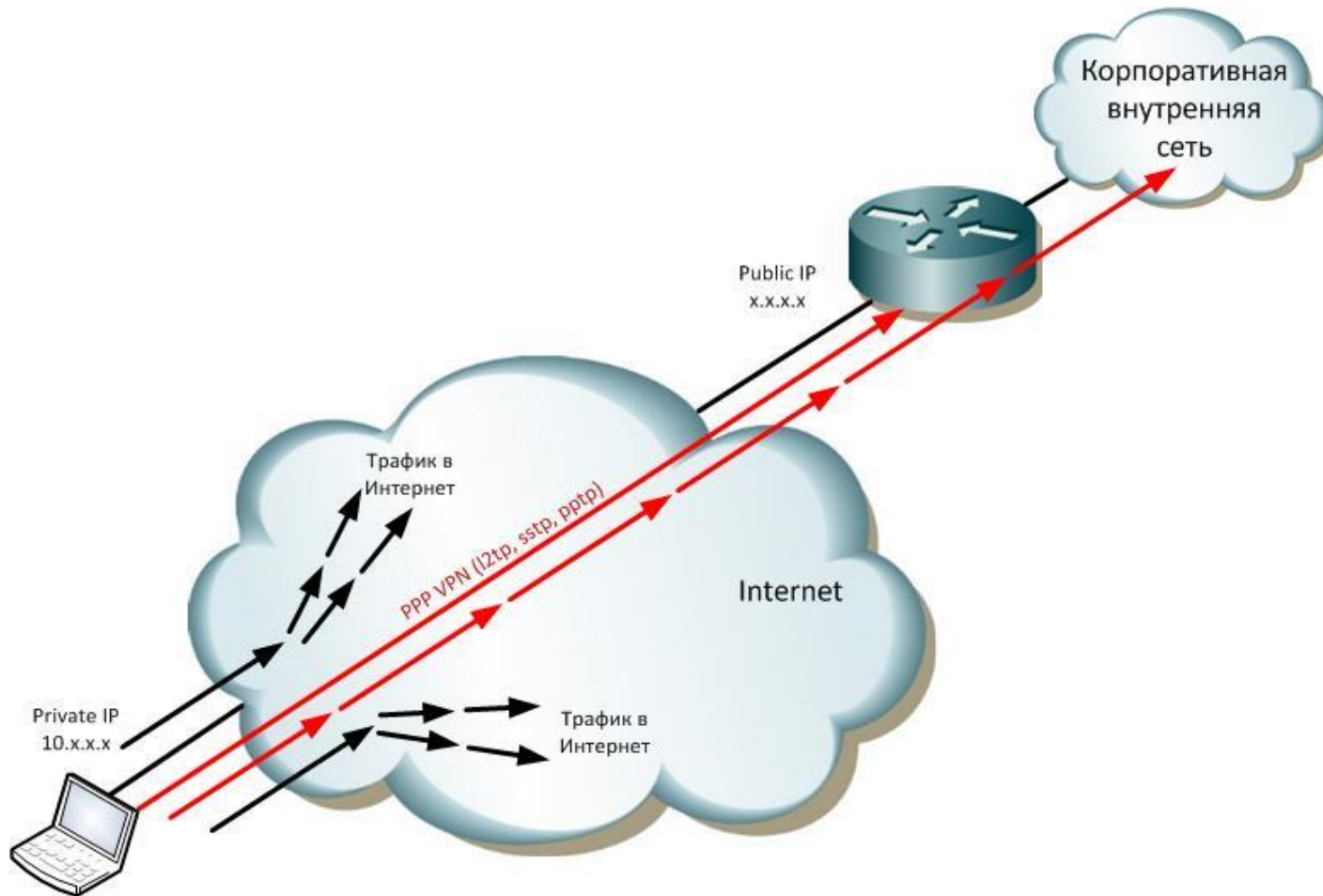
За 4,5 года работы:

- 5 стран (РФ, РБ, Казахстан, Кыргызстан, Индия)
- 50 городов
- География от Калининграда до Владивостока и от Архангельска до Калькутты
- Тренинги в Риге в собственном тренинг-центре компании **MikroTik** (октябрь)

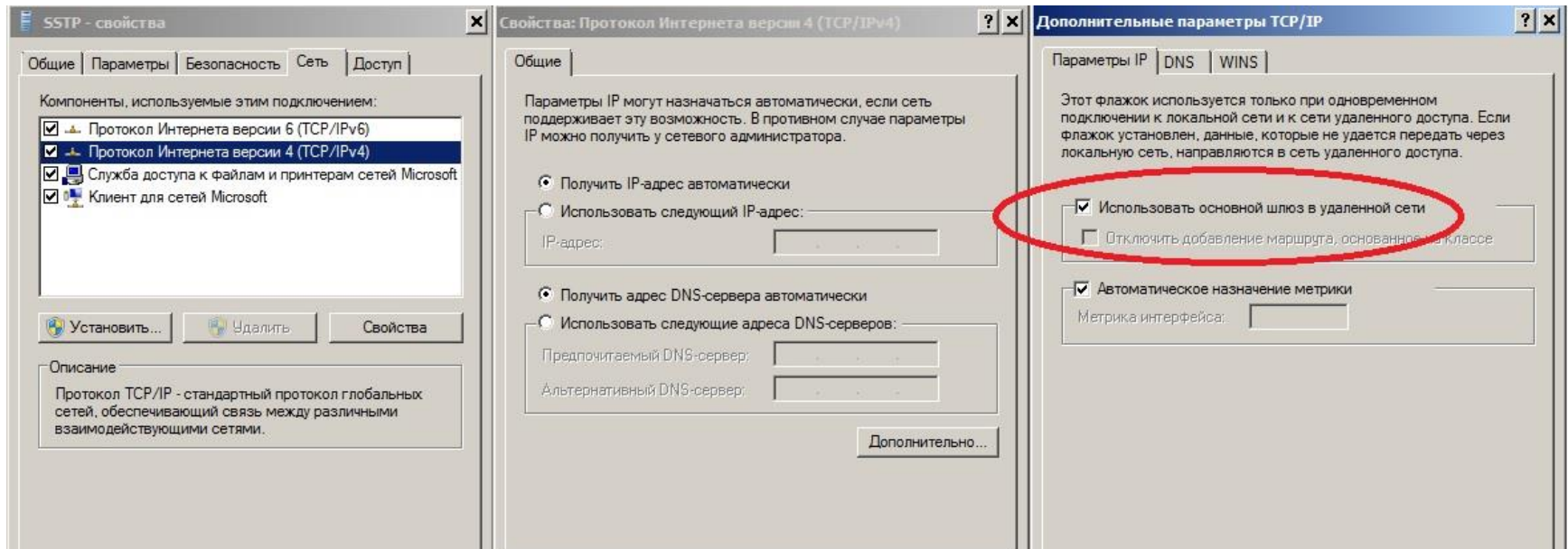
Постановка задачи



Постановка задачи



Постановка задачи



Постановка задачи

- Снимаем галочку
- Теперь все маршруты в рабочую сеть придется писать руками...
- А если сетей много?
- И они постоянно добавляются (сеть растет)?

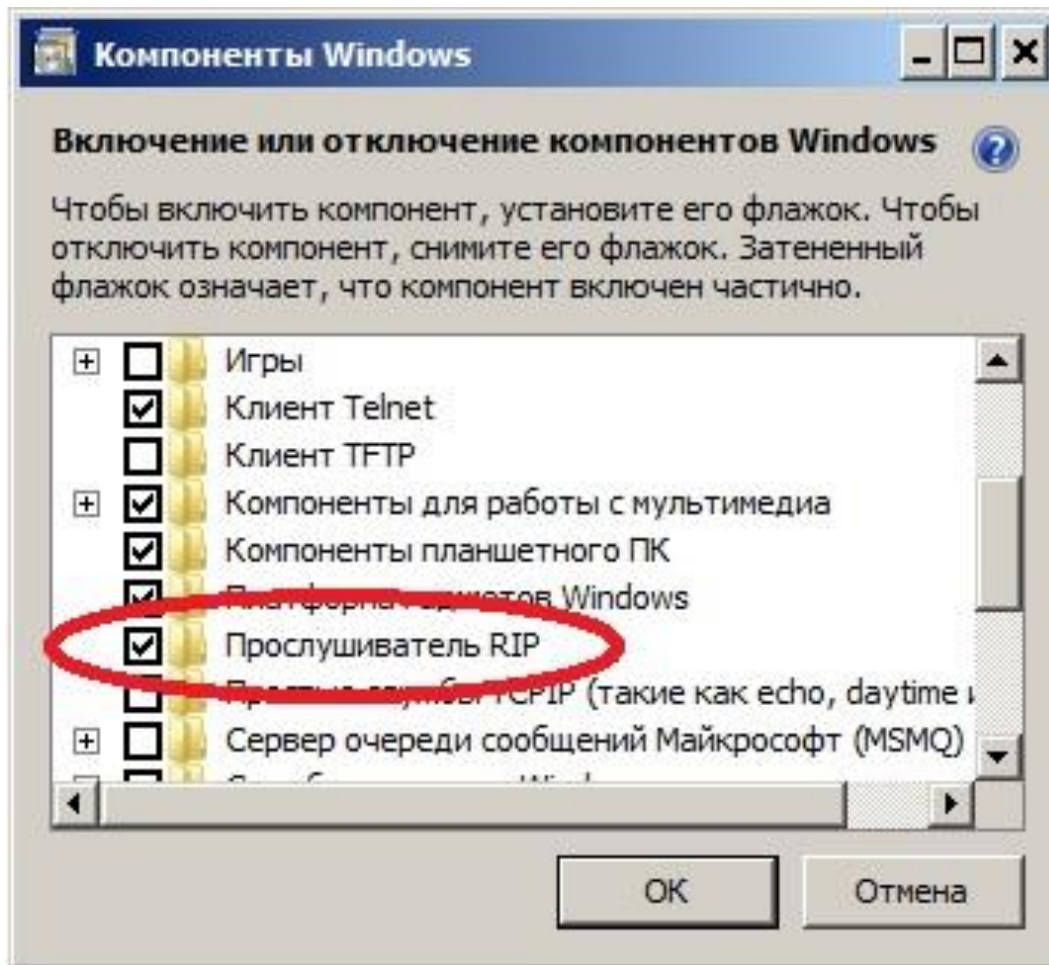
Постановка задачи

- VPN'ы не занимаются передачей маршрутов...
- Как насчет протоколов маршрутизации?
- OSPF, RIP, BGP?

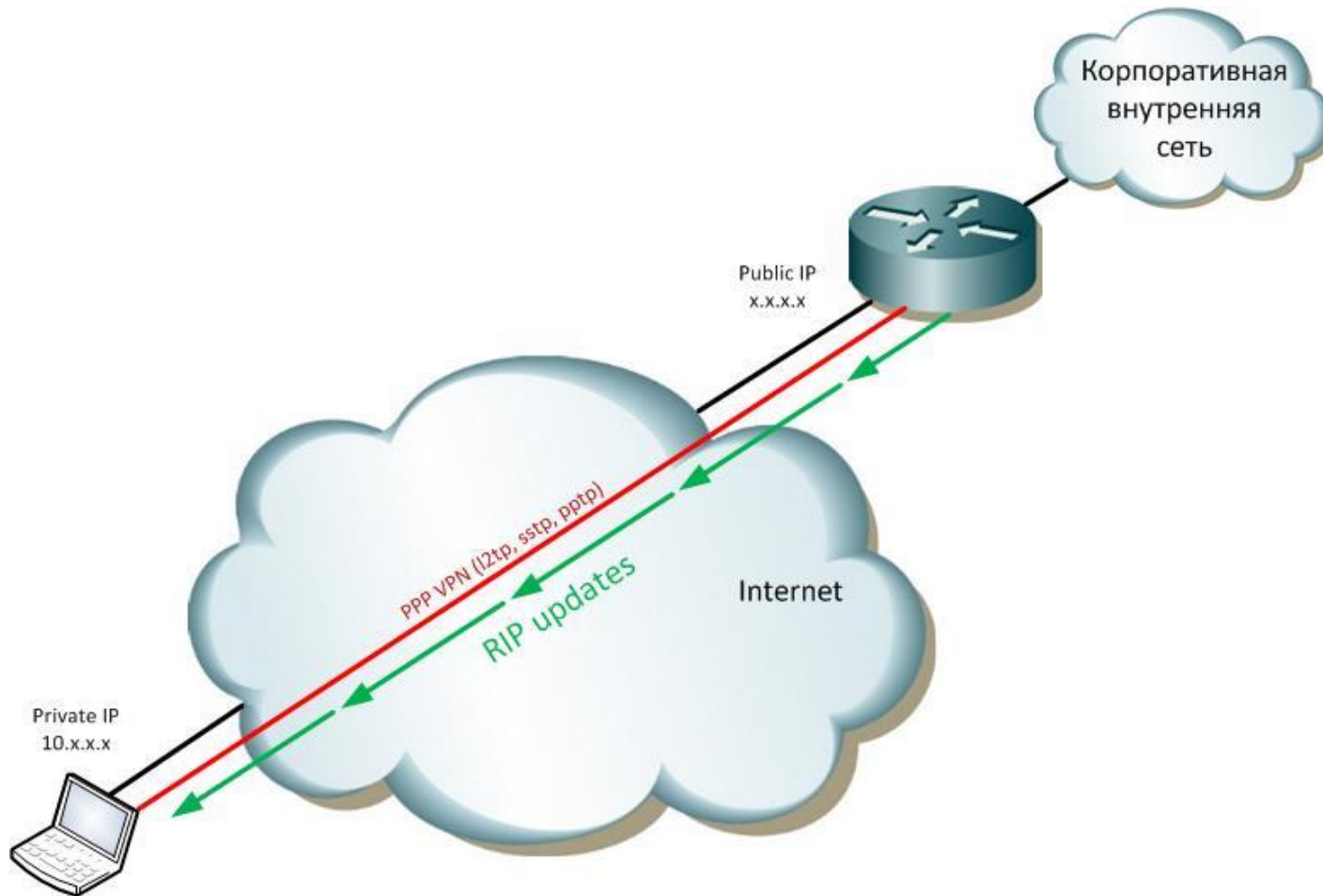
Решение задачи

RIP!

Решение задачи



Решение задачи



Решение задачи

1. Включаем PPP-сервер

The screenshot shows the MikroTik WinBox interface. On the left sidebar, the 'PPP' menu item is highlighted. A red arrow points from this menu item to the 'Active Connections' tab in the main window. The 'Active Connections' tab is also highlighted with a red circle. Below the tabs, there are four buttons: 'PPTP Server', 'SSTP Server', 'L2TP Server', and 'OVPN Server', all of which are circled in red. Below these buttons is a table with the following data:

	Name	Type	Actual MTU	L2 MTU	Tx	Rx
X	ztp-out1	L2TP Client			0 bps	0 bps
R	sstp-test_rip	SSTP Server Binding	1500		0 bps	624 bps

Решение задачи

2. Заводим юзера

The screenshot shows the MikroTik WinBox interface. In the left sidebar, the 'PPP' menu item is highlighted with a red arrow. The main window displays the 'PPP Authentication & Accounting' configuration page. A table lists the configured PPP secrets:

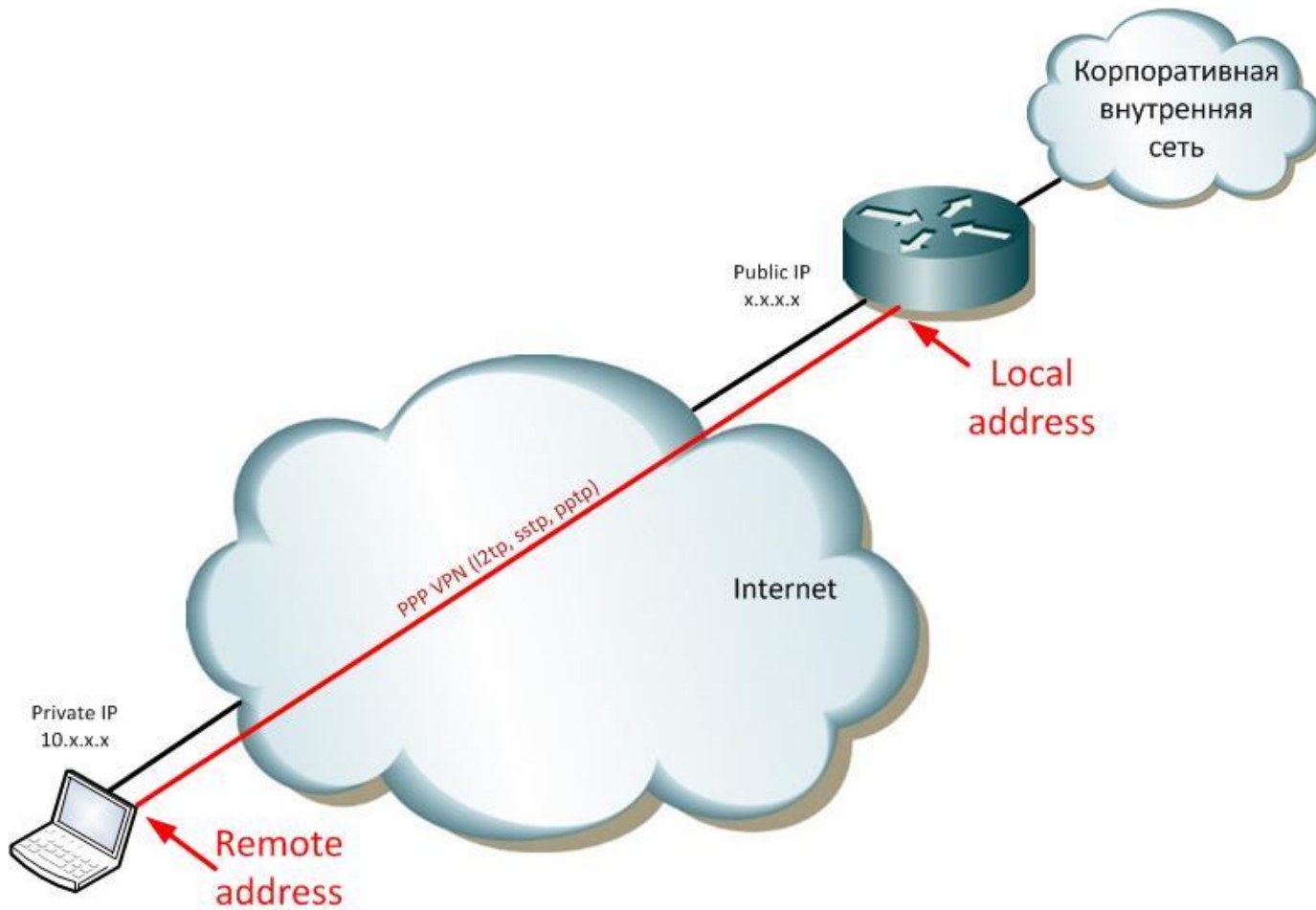
Name	Password	Service	Caller ID	Profile	Local Address	Remote
test_rip	*****	any		default	10.3.3.3	10.4.4.4

A dialog box titled 'PPP Secret <test_rip>' is open, showing the configuration for the 'test_rip' user. The 'Name' field is circled in blue. The dialog includes the following fields and buttons:

- Name: test_rip
- Password: *****
- Service: any
- Caller ID: (empty)
- Profile: default
- Local Address: 10.3.3.3
- Remote Address: 10.4.4.4
- Remote IPv6 Prefix: (empty)
- Routes: (empty)
- Limit Bytes In: (empty)
- Limit Bytes Out: (empty)
- Last Logged Out: Sep/16/2018 14:14:48
- enabled

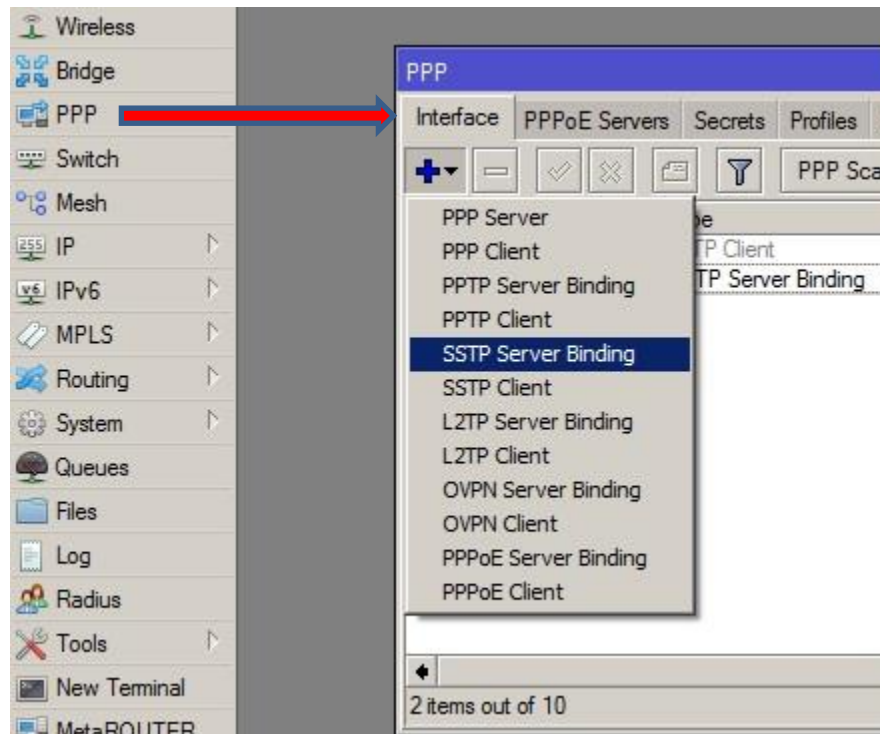
Buttons on the right side of the dialog include OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

Решение задачи



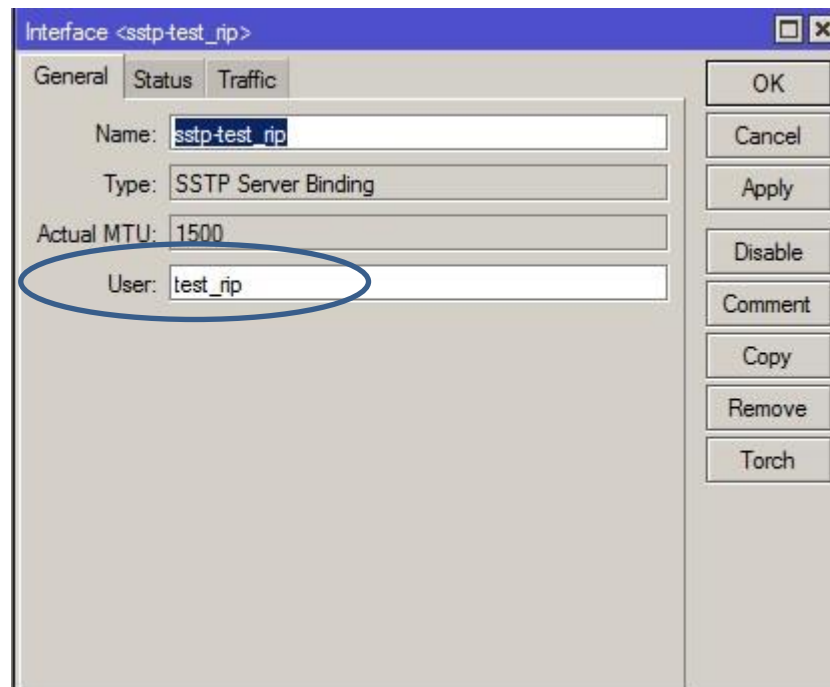
Решение задачи

3. Создаем server binding



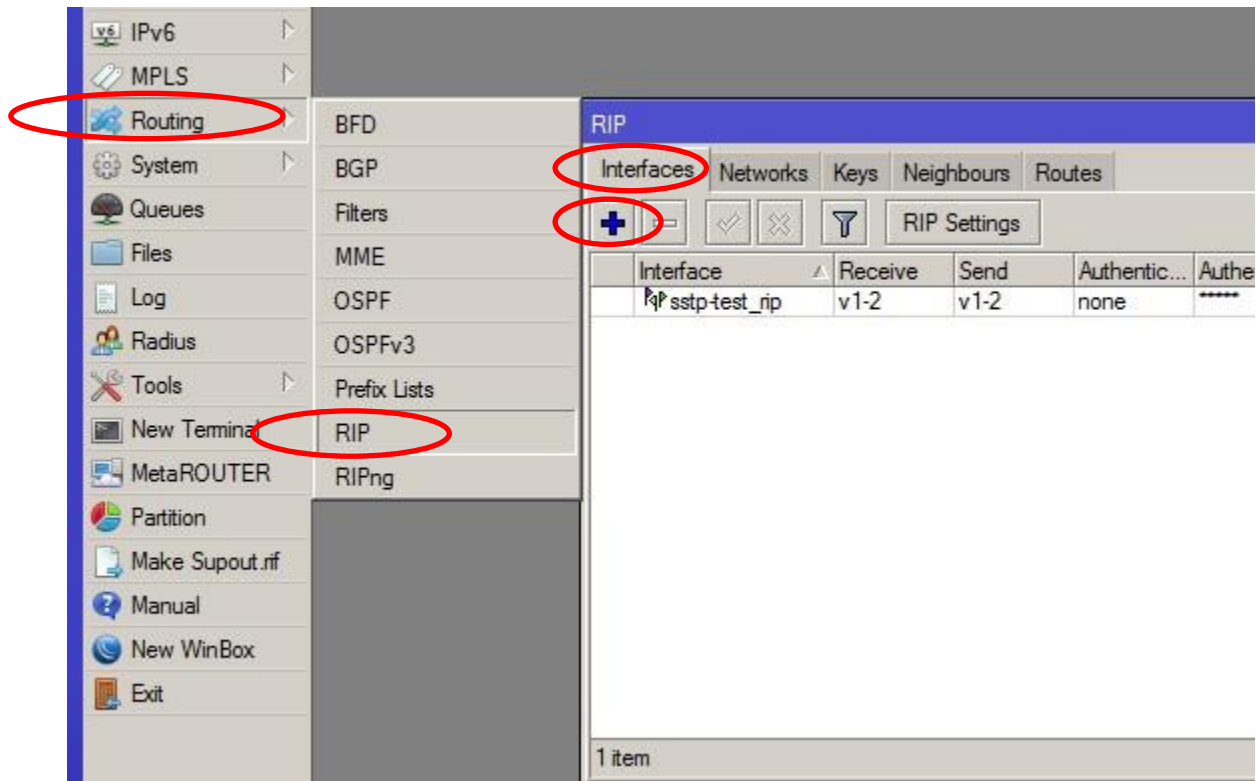
Решение задачи

3. Создаем server binding



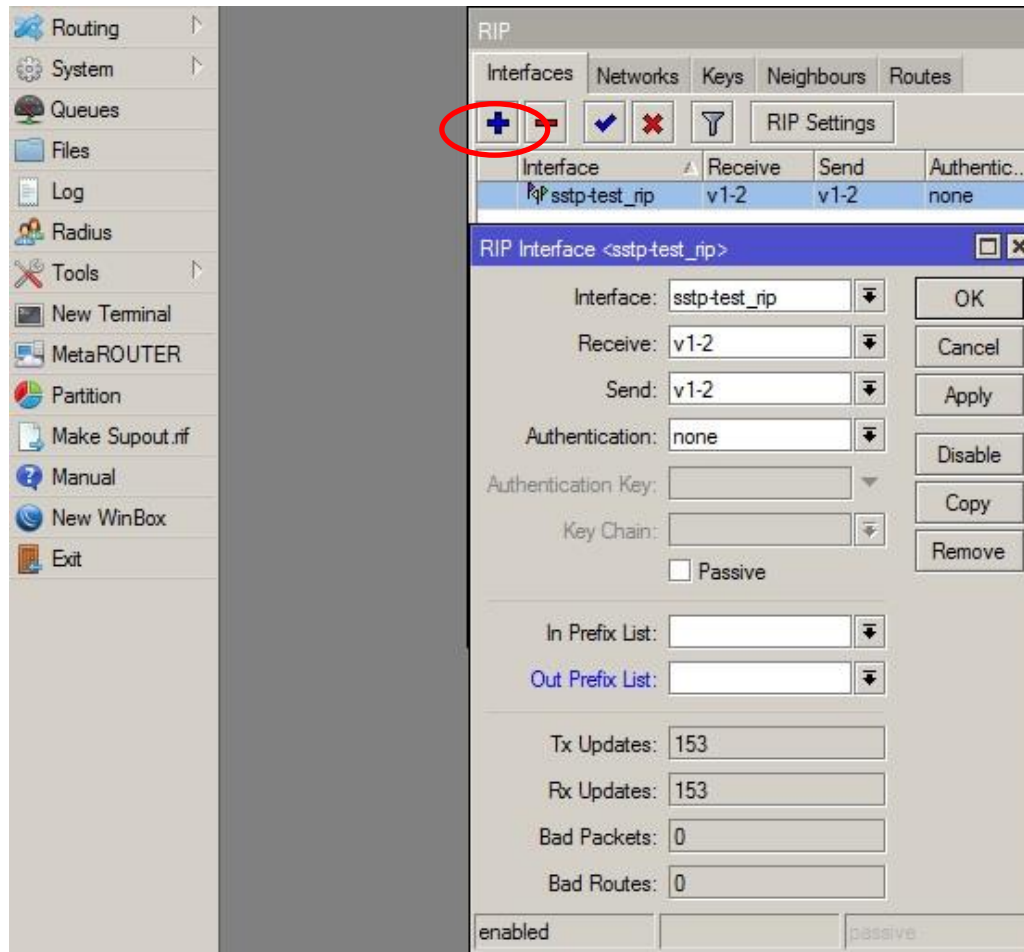
Решение задачи

4. Запускаем протокол RIP на роутере



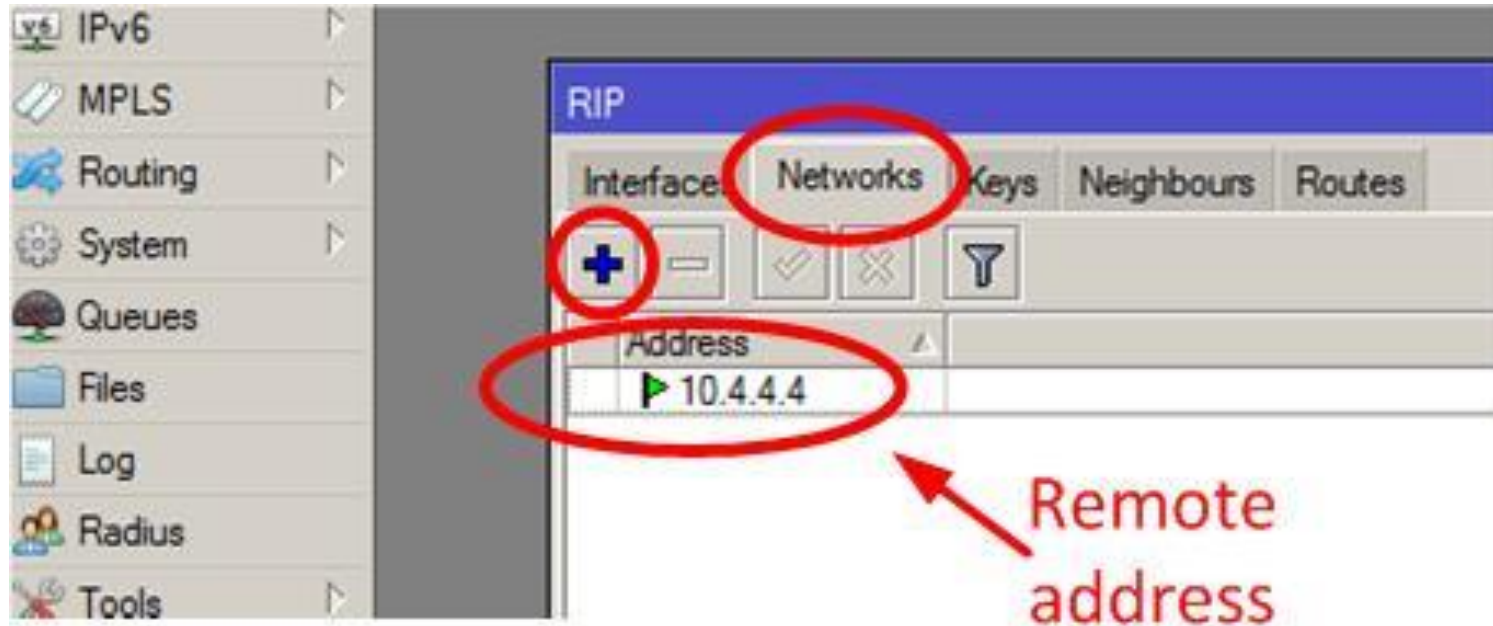
Решение задачи

4. Запускаем протокол RIP на роутере



Решение задачи

4. Запускаем протокол RIP на роутере



Remote address – это адрес нашего компьютера

Решение задачи

- Если строить сеть на основе протокола RIP, то update'ы будут прилетать на компьютер
- Вроде все работает?
 - Компьютер выходит в интернет не через VPN
 - а все маршруты из корпоративной сети приходят на компьютер...

Решение задачи

- Сеть строить есть смысл на протоколе OSPF 😊
- Осталось только передать маршруты из OSPF в RIP!
- Называется данный процесс **Redistribution**

Решение задачи

The screenshot shows the Mikrotik WinBox interface. On the left, the 'Routing' menu item is highlighted with a red oval. In the main window, the 'RIP' configuration page is active, with the 'Interfaces' tab selected. A table lists the configuration for the 'sstp-test_rip' interface:

Interface	Receive	Send	Authentic...	Authenticati...	Key
sstp-test_rip	v1-2	v1-2	none	*****	

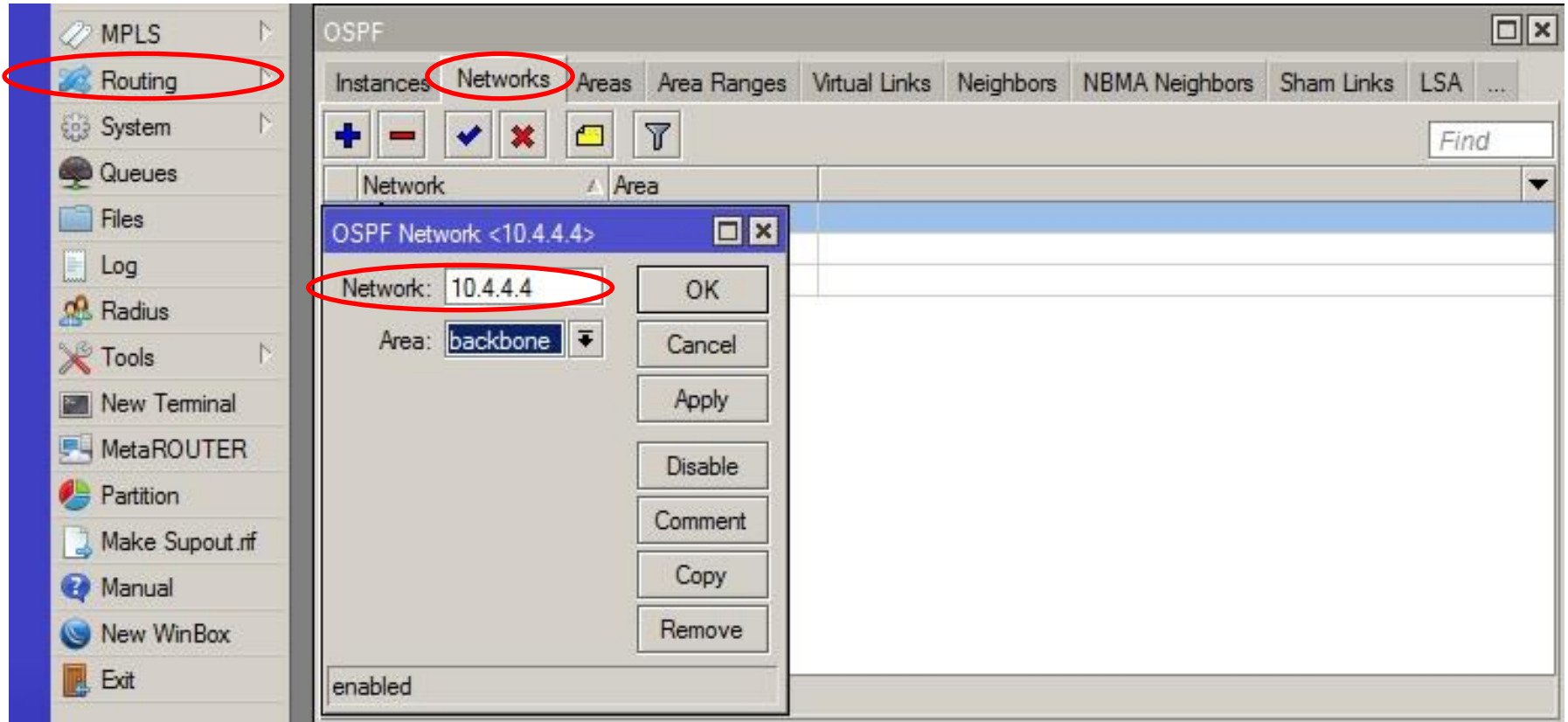
Below the table, the 'RIP Settings' dialog box is open. The 'Distribute Default' dropdown is set to 'never'. The 'Redistribute OSPF Routes' checkbox is checked and highlighted with a red oval. Other options include 'Redistribute Static Routes', 'Redistribute Connected Routes', and 'Redistribute BGP Routes', all of which are unchecked. The dialog also contains fields for metrics and timers:

- Default Route Metric: 1
- Static Routes Metric: 1
- Connected Routes Metric: 1
- OSPF Routes Metric: 1
- BGP Routes Metric: 1
- Update Timer: 00:00:30
- Timeout Timer: 00:03:00
- Garbage Timer: 00:02:00
- Routing Table: main

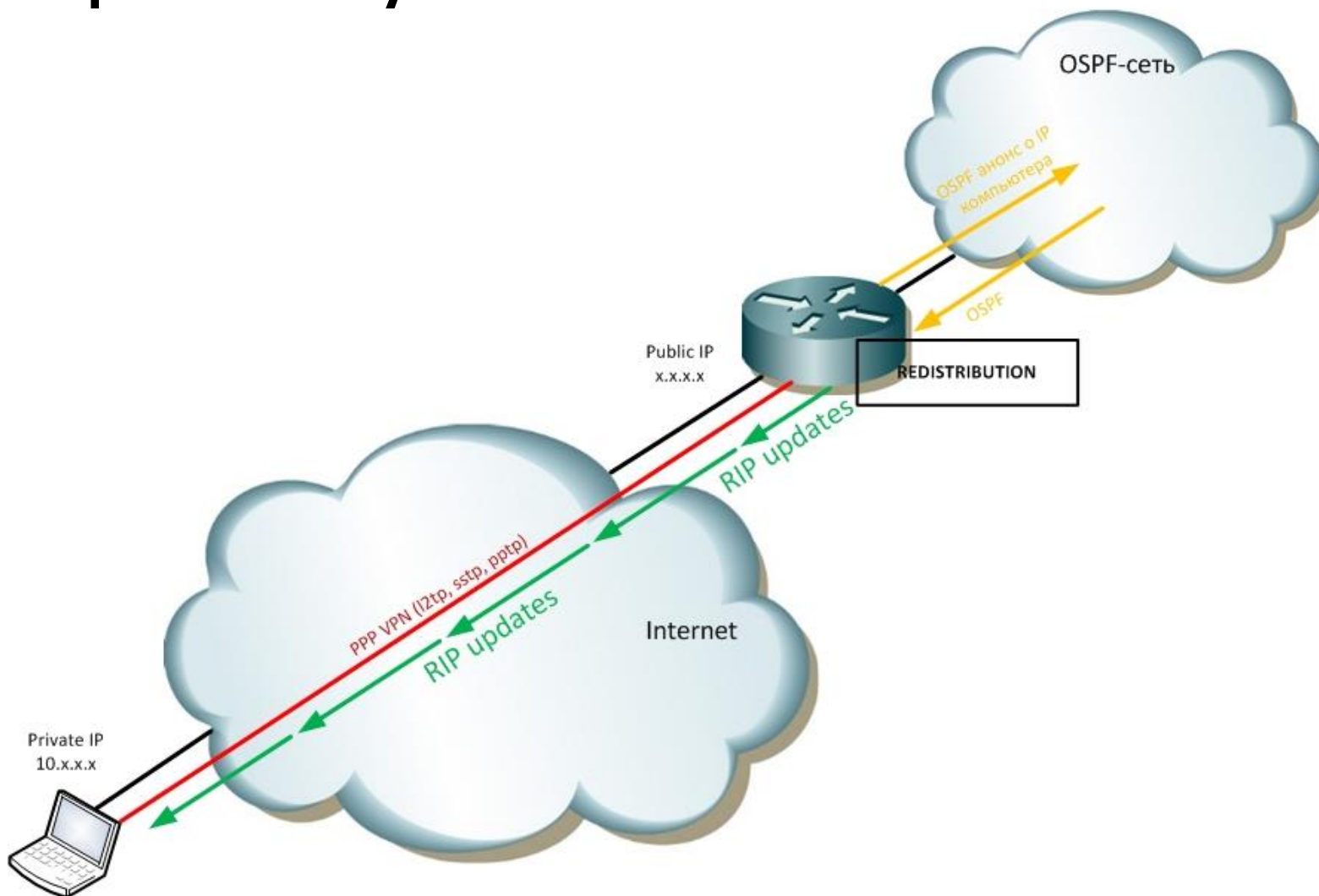
Решение задачи

- Остался последний шаг: анонсировать наш **Remote Address** (адрес компьютера на конце туннеля) в OSPF
- Это нужно, чтобы в корпоративной сети появился маршрут **/32** до самого компьютера

Решение задачи



Промежуточный итог



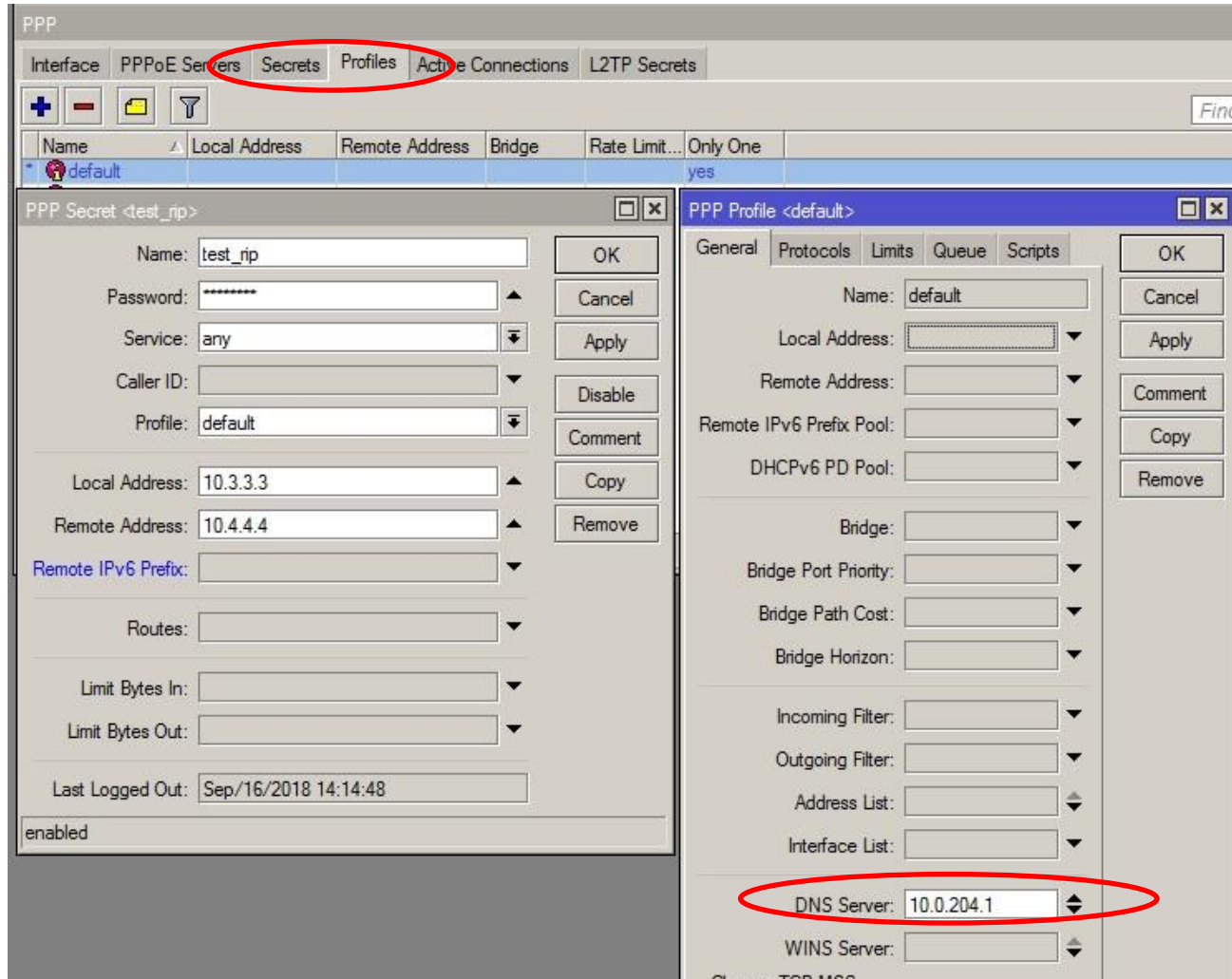
Промежуточный итог

```
C:\Windows\system32\cmd.exe

IPv4 таблица маршрута
-----
Активные маршруты:
Сетевой адрес          Маска сети            Адрес шлюза           Интерфейс             Метрика
-----
0.0.0.0                0.0.0.0              192.168.1.1          192.168.1.10         20
10.0.0.0               255.0.0.0            10.3.3.3             10.4.4.4             26
10.0.13.0              255.255.255.0        10.3.3.3             10.4.4.4             27
10.0.204.0             255.255.255.0        10.3.3.3             10.4.4.4             27
10.4.4.4               255.255.255.255     On-link              10.4.4.4             281
127.0.0.0              255.0.0.0            On-link              127.0.0.1            306
127.0.0.1              255.255.255.255     On-link              127.0.0.1            306
127.255.255.255        255.255.255.255     On-link              127.0.0.1            306
192.168.1.0            255.255.255.0        On-link              192.168.1.10         266
192.168.1.10          255.255.255.255     On-link              192.168.1.10         266
192.168.1.255         255.255.255.255     On-link              192.168.1.10         266
192.168.2.0            255.255.255.0        10.3.3.3             10.4.4.4             27
224.0.0.0              240.0.0.0            On-link              127.0.0.1            306
224.0.0.0              240.0.0.0            On-link              192.168.1.10         266
224.0.0.0              240.0.0.0            On-link              10.4.4.4             281
255.255.255.255        255.255.255.255     On-link              127.0.0.1            306
255.255.255.255        255.255.255.255     On-link              192.168.1.10         266
255.255.255.255        255.255.255.255     On-link              10.4.4.4             281
-----
Постоянные маршруты:
Отсутствует

C:\Users\admin>
```

Приятные мелочи



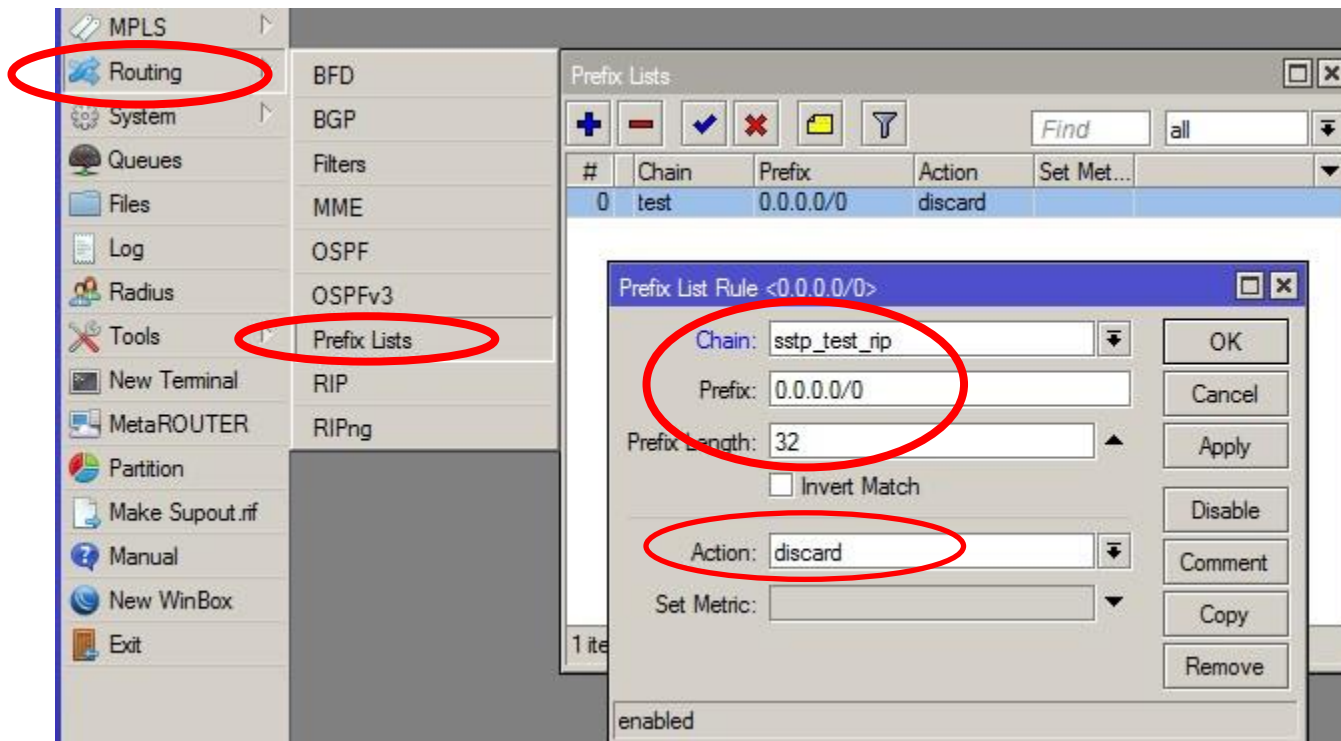
Приятные мелочи

```
C:\Windows\system32\cmd.exe

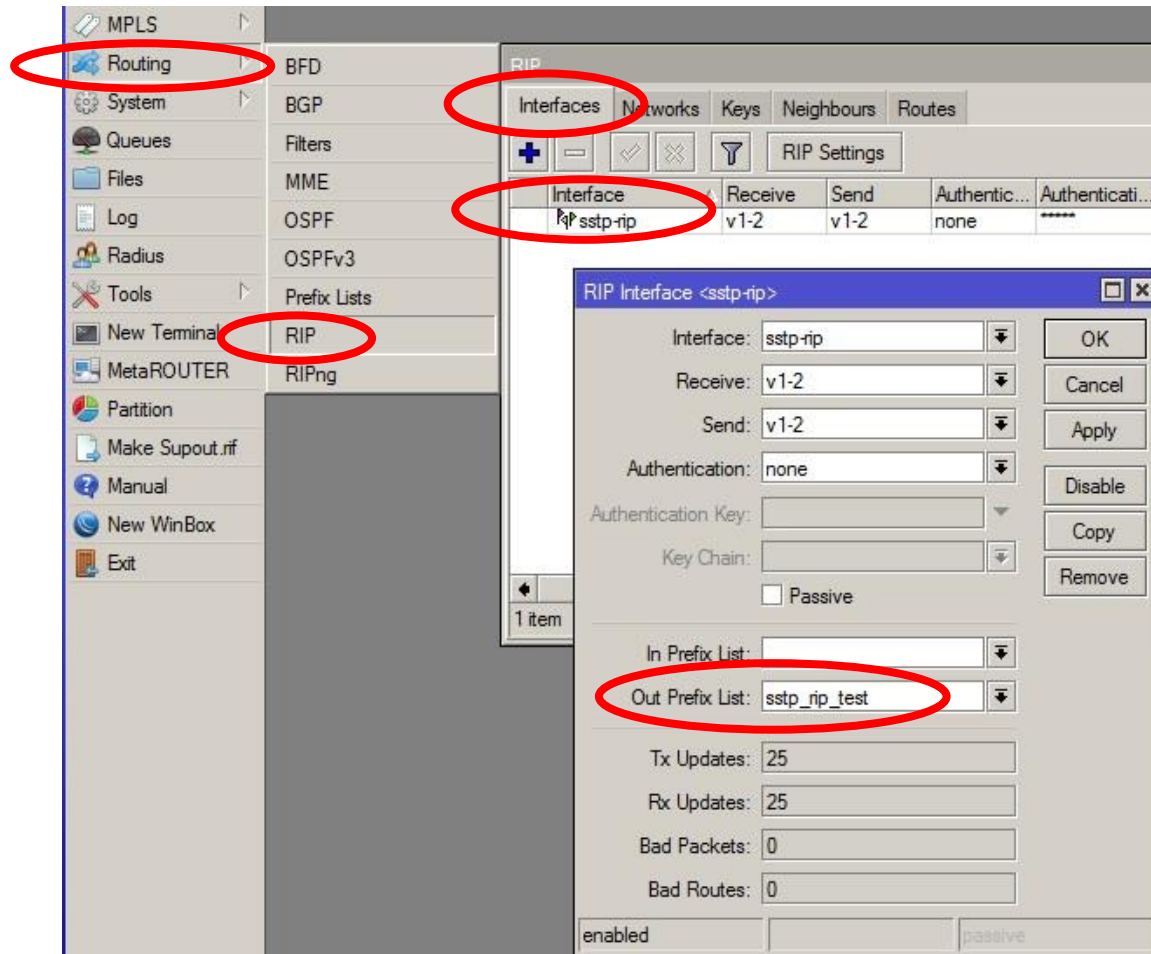
IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес          Маска сети            Адрес шлюза           Интерфейс             Метрика
0.0.0.0                0.0.0.0              192.168.1.1          192.168.1.10         20
10.0.0.0               255.0.0.0            10.3.3.3             10.4.4.4             26
10.0.13.0              255.255.255.0       10.3.3.3             10.4.4.4             27
10.0.204.0             255.255.255.0       10.3.3.3             10.4.4.4             27
10.4.4.4               255.255.255.255     On-link              10.4.4.4             281
10.11.12.14           255.255.255.255     10.3.3.3             10.4.4.4             27
10.11.12.15           255.255.255.255     10.3.3.3             10.4.4.4             27
10.11.12.16           255.255.255.255     10.3.3.3             10.4.4.4             27
10.11.12.17           255.255.255.255     10.3.3.3             10.4.4.4             27
10.11.12.18           255.255.255.255     10.3.3.3             10.4.4.4             27
10.11.12.20           255.255.255.255     10.3.3.3             10.4.4.4             27
15.31.213.22          255.255.255.255     192.168.1.1          192.168.1.10         11
127.0.0.0              255.0.0.0            On-link              127.0.0.1            306
127.0.0.1              255.255.255.255     On-link              127.0.0.1            306
127.255.255.255        255.255.255.255     On-link              127.0.0.1            306
185.34.152.144        255.255.255.255     192.168.1.1          192.168.1.10         11
192.168.1.0            255.255.255.0       On-link              192.168.1.10         266
192.168.1.0            255.255.255.0       10.3.3.3             10.4.4.4             27
192.168.1.10          255.255.255.255     On-link              192.168.1.10         266
192.168.1.255         255.255.255.255     On-link              192.168.1.10         266
192.168.2.0            255.255.255.0       10.3.3.3             10.4.4.4             27
224.0.0.0              240.0.0.0            On-link              127.0.0.1            306
224.0.0.0              240.0.0.0            On-link              192.168.1.10         266
224.0.0.0              240.0.0.0            On-link              10.4.4.4             281
255.255.255.255       255.255.255.255     On-link              127.0.0.1            306
255.255.255.255       255.255.255.255     On-link              192.168.1.10         266
255.255.255.255       255.255.255.255     On-link              10.4.4.4             281
=====
Постоянные маршруты:
Отсутствует

C:\Users\admin>
```

Приятные мелочи



Приятные мелочи



Приятные мелочи

```
C:\Windows\system32\cmd.exe

-----
IPv4 таблица маршрута
-----
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0         192.168.1.1      192.168.1.10   20
10.0.0.0           255.0.0.0       10.3.3.3         10.4.4.4       26
10.0.13.0          255.255.255.0   10.3.3.3         10.4.4.4       28
10.0.204.0         255.255.255.0   10.3.3.3         10.4.4.4       27
10.4.4.4           255.255.255.255 On-link          10.4.4.4       281
95.31.213.72      255.255.255.255 192.168.1.1      192.168.1.10   11
127.0.0.0          255.0.0.0       On-link          127.0.0.1      306
127.0.0.1          255.255.255.255 On-link          127.0.0.1      306
127.255.255.255    255.255.255.255 On-link          127.0.0.1      306
192.168.1.0        255.255.255.0   On-link          192.168.1.10   266
192.168.1.0        255.255.255.0   10.3.3.3         10.4.4.4       28
192.168.1.10      255.255.255.255 On-link          192.168.1.10   266
192.168.1.255     255.255.255.255 On-link          192.168.1.10   266
192.168.2.0        255.255.255.0   10.3.3.3         10.4.4.4       28
195.191.175.148   255.255.255.255 192.168.1.1      192.168.1.10   11
224.0.0.0          240.0.0.0       On-link          127.0.0.1      306
224.0.0.0          240.0.0.0       On-link          192.168.1.10   266
224.0.0.0          240.0.0.0       On-link          10.4.4.4       281
255.255.255.255    255.255.255.255 On-link          127.0.0.1      306
255.255.255.255    255.255.255.255 On-link          192.168.1.10   266
255.255.255.255    255.255.255.255 On-link          10.4.4.4       281
-----
Постоянные маршруты:
Отсутствует

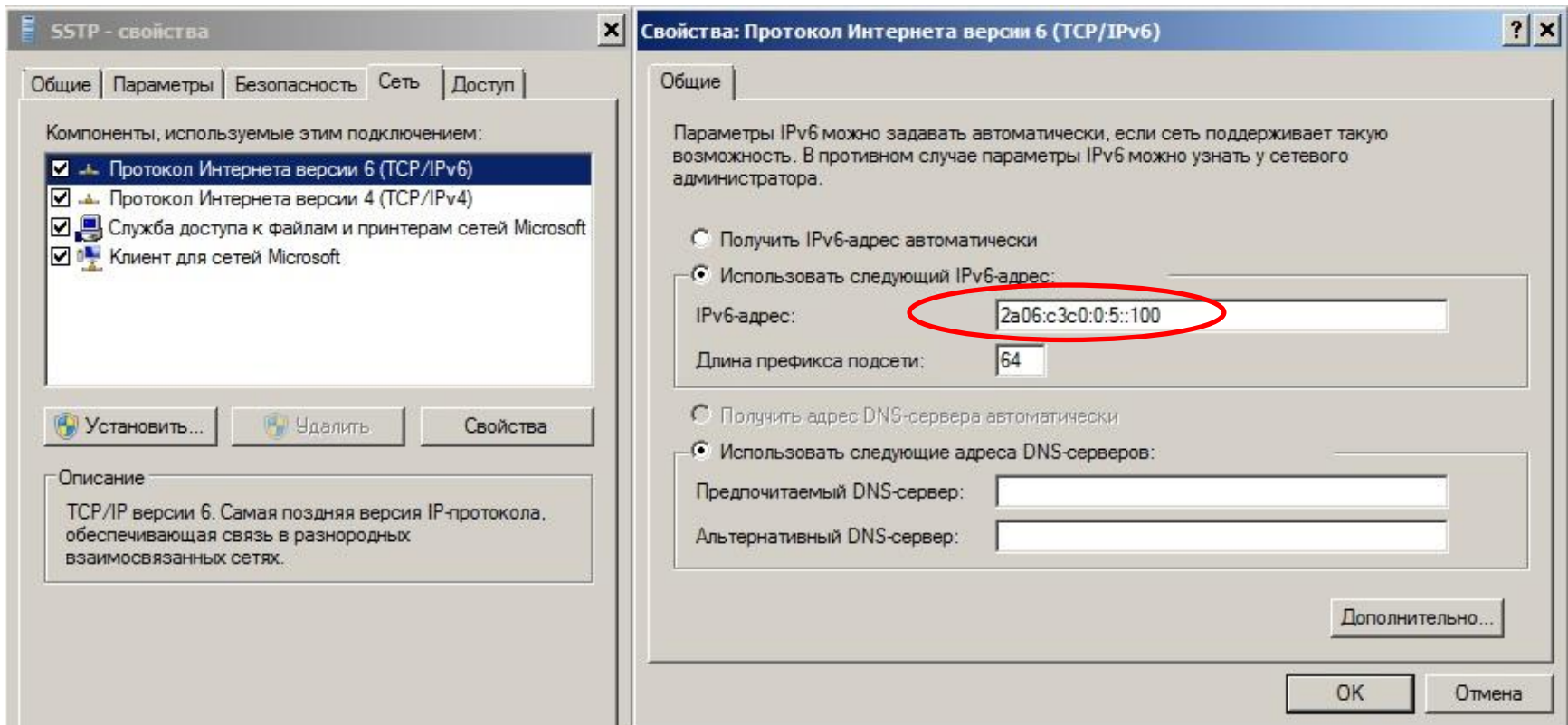
C:\Users\admin>
```

А как насчет IPv6? 😊

Доступ к IPv6

- Имеем в сети предприятия постоянный пул шире чем /64 (/56, /48)
- Удаленные компьютеры получают доступ к IPv6 только через сеть предприятия
- Поэтому схема упрощается, галку “использовать основной шлюз в удаленной сети” оставляем

Доступ к IPv6



Доступ к IPv6

The screenshot displays the MikroTik WinBox interface. On the left is a sidebar menu with various system and network configuration options. The main window shows the 'PPP' configuration page, specifically the 'Secrets' tab. A table lists a secret named 'test_rip' with a password of '*****', service 'any', caller ID, profile 'default', and local address '10.3.3.3'. Below this, a 'PPP Secret <test_rip>' dialog box is open, showing configuration fields: Name (test_rip), Password (*****), Service (any), Caller ID, Profile (default), Local Address (10.3.3.3), Remote Address (10.4.4.4), and Remote IPv6 Prefix (2a06:c3c0:0:5::100). The 'Remote IPv6 Prefix' field is circled in red. Other fields include Routes, Limit Bytes In, Limit Bytes Out, and Last Logged Out (Sep/16/2018 19:09:38). The status at the bottom is 'enabled'.

Name	Password	Service	Caller ID	Profile	Local Address
test_rip	*****	any		default	10.3.3.3

PPP Secret <test_rip>

Name: test_rip
Password: *****
Service: any
Caller ID:
Profile: default
Local Address: 10.3.3.3
Remote Address: 10.4.4.4
Remote IPv6 Prefix: 2a06:c3c0:0:5::100
Routes:
Limit Bytes In:
Limit Bytes Out:
Last Logged Out: Sep/16/2018 19:09:38
enabled

Доступ к IPv6

The screenshot displays the Mikrotik WinBox interface. On the left sidebar, the 'Routing' menu item is circled in red. The main window shows the 'OSPFv3' configuration page, with the 'Interfaces' tab selected and circled in red. Below the tabs, there is a table with the following data:

Area	Interface	Cost	Priority
backbone	bridge_LAN	10	
backbone	KRK_KRAS	10	

Доступ к IPv6

	Address	Interface	Advertise
DL	✚ fe80::2:b2d9:6270/64	KRK_ART	no
DL	✚ fe80::2:c3bf:af94/64	KRK_KRAS	no
G	✚ 2a06:c3c0:0:3::1/64	bridge_LAN	yes
DL	✚ fe80::6019:2fff:feed:4607/64	bridge_LAN	no
DL	✚ fe80::ba69f4ff:fe08:d09/64	ether5	no
DL	✚ fe80::4e5e:cff:fe4a:21dd/64	sfp1	no
DL	✚ fe80::9/64	sstp-in1	no

7 items

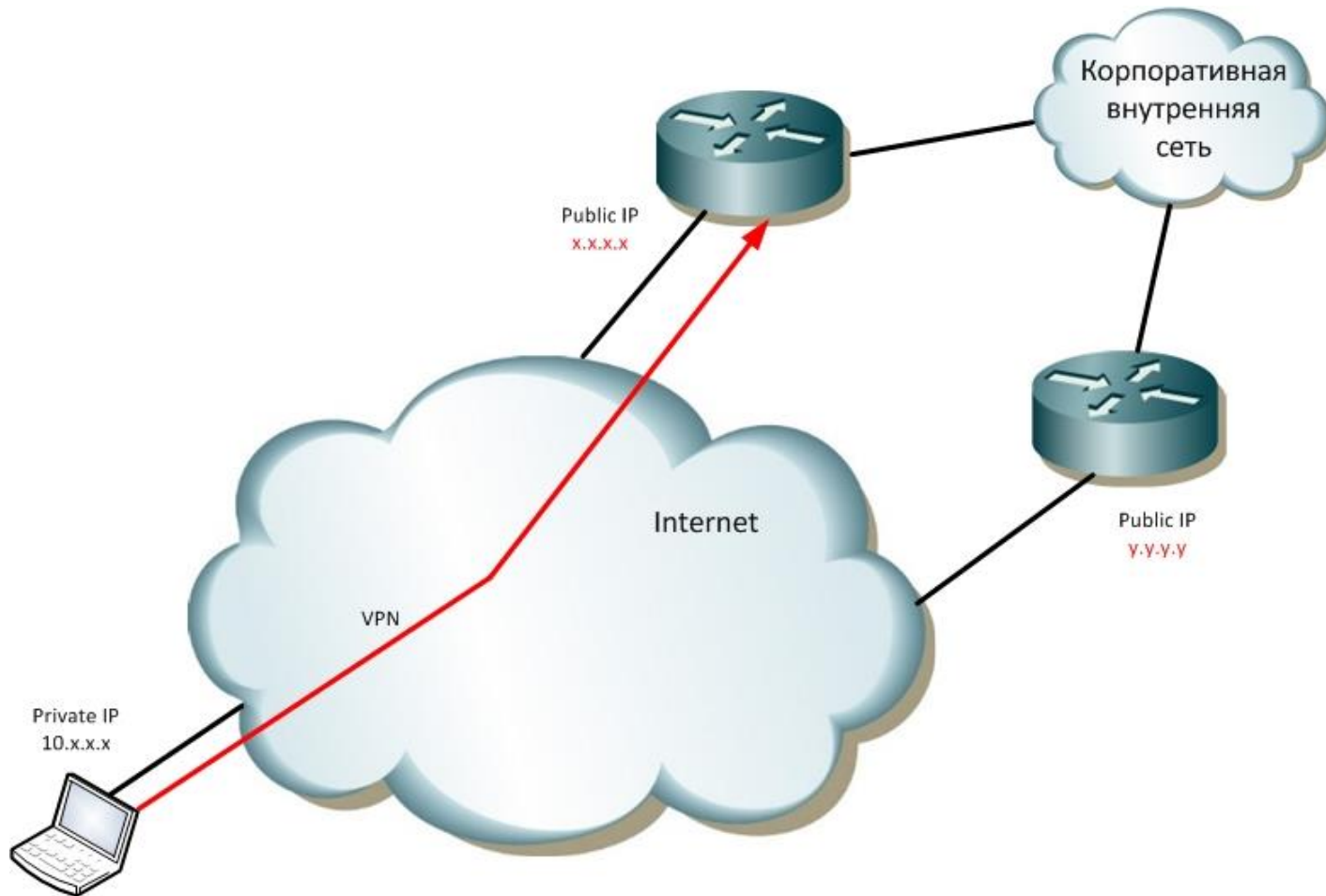
Доступ к IPv6

	Dst. Address ▲	Gateway	Distance	OSPF Type ▼
DAo	▶ ::/0	fe80::2:b922:9890%KRK_KRAS reachable	110	external type 1
DAo	▶ 2a06:c3c0:0:1::/64	fe80::2:b922:9890%KRK_KRAS reachable	110	intra area
DAC	▶ 2a06:c3c0:0:3::/64	bridge_LAN reachable	0	
DAS	▶ 2a06:c3c0:0:5::100	sstp-in1 reachable	1	

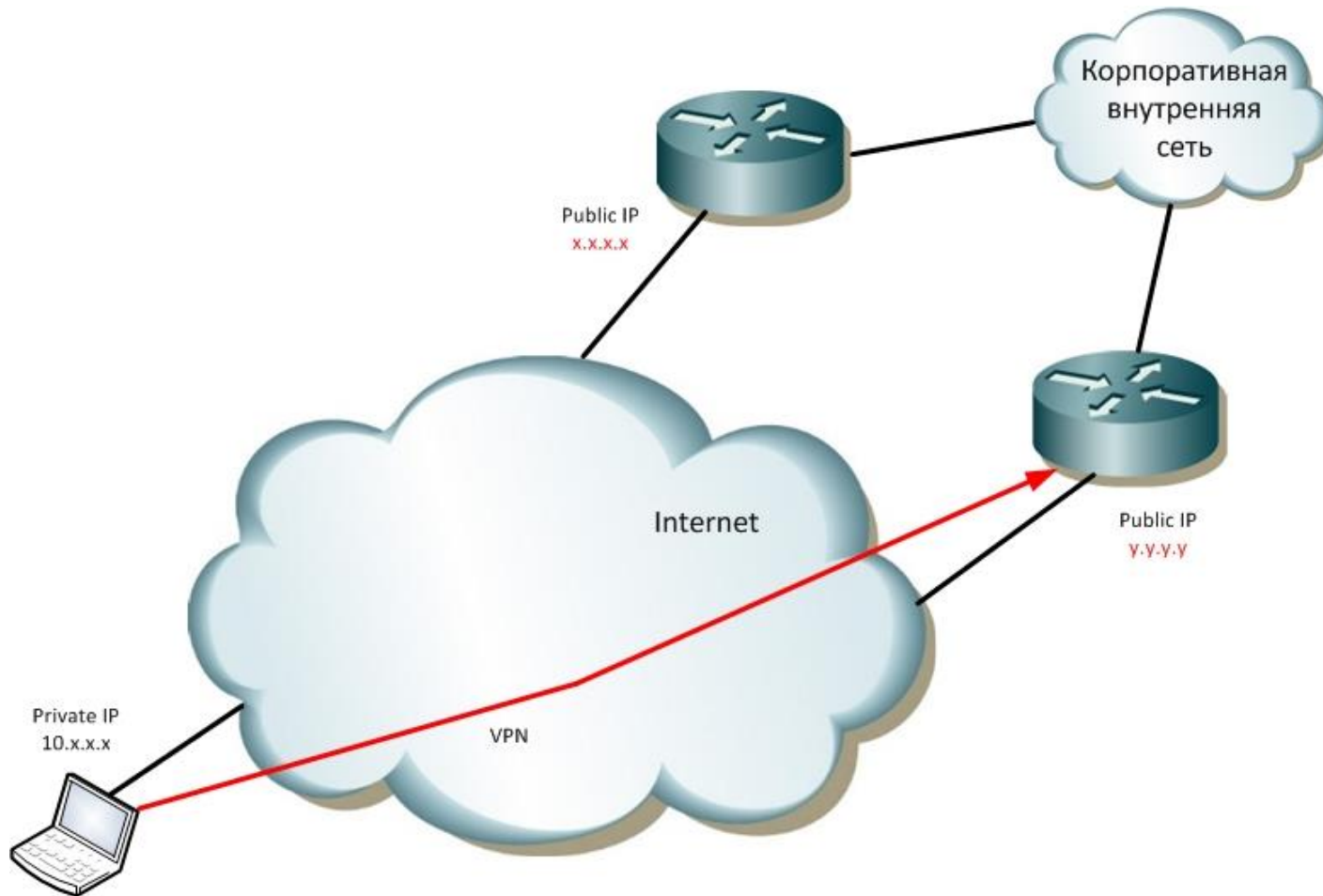
Доступ к IPv6

The screenshot displays the MikroTik WinBox interface. On the left, the 'Routing' menu is circled in red, and 'OSPFv3' is selected. The main window shows the 'OSPFv3' configuration page with the 'Instances' tab circled in red. Below this, a dialog box titled 'OSPFv3 Instance <default>' is open, showing the 'General' tab circled in red. The 'Redistribute Static Routes' option is set to 'as type 1' and is also circled in red. Other options include 'Redistribute Default Route' (never), 'Redistribute Connected Routes' (no), 'Redistribute RIP Routes' (no), 'Redistribute BGP Routes' (no), and 'Redistribute Other OSPF Routes' (no). The 'Name' is 'default' and 'Router ID' is '0.0.0.8'. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove' are visible on the right side of the dialog box.

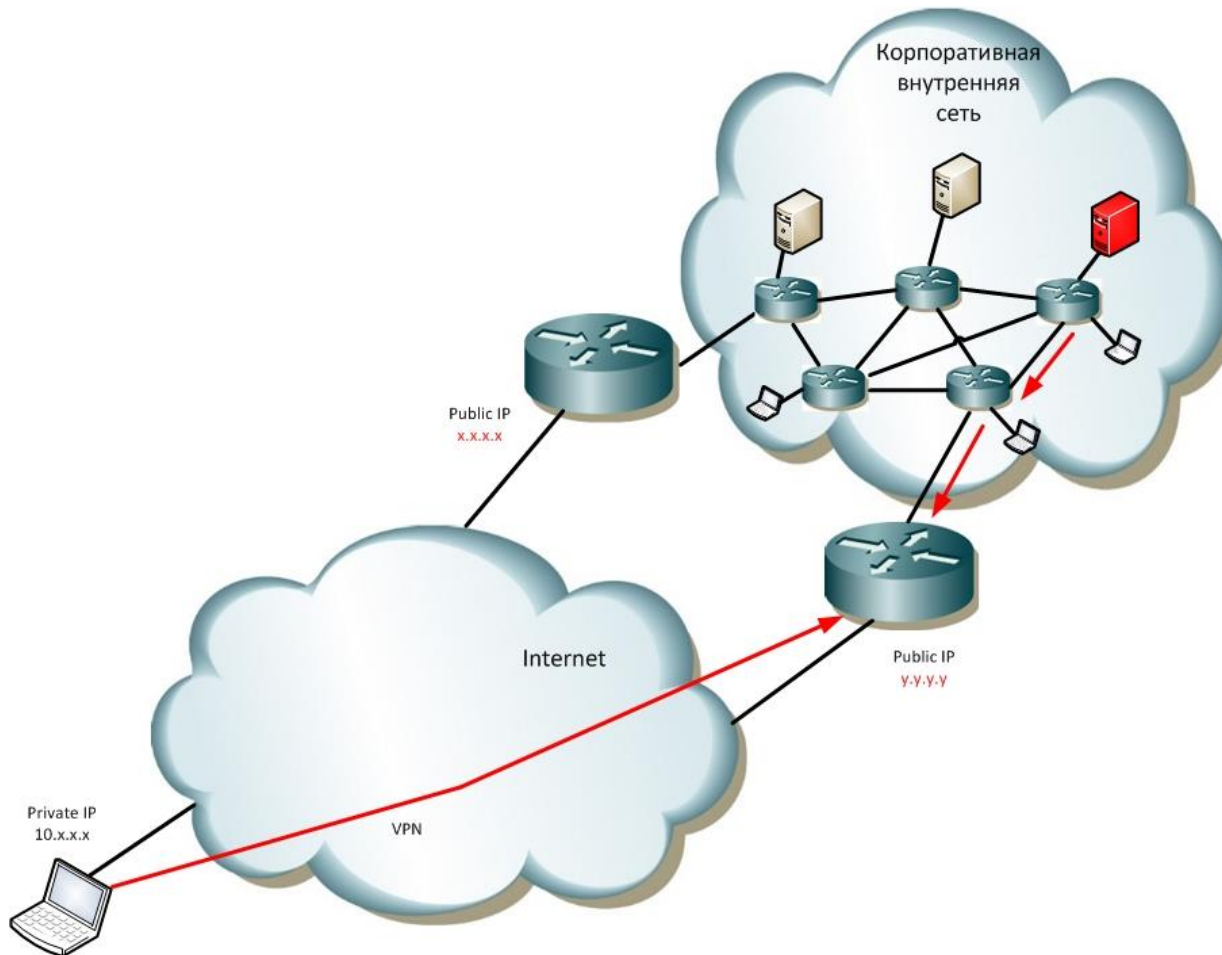
Отказоустойчивость VPN-сервера



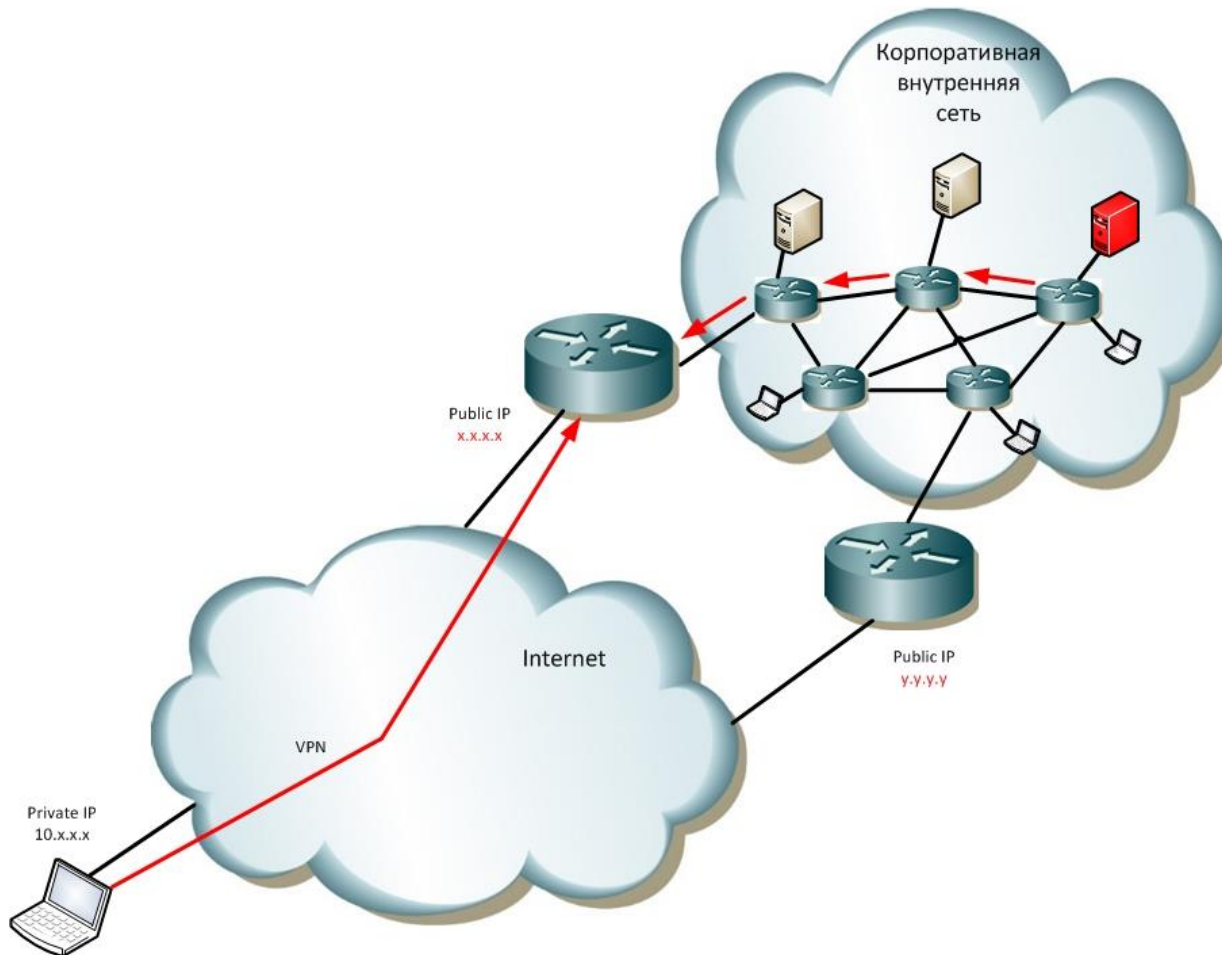
Отказоустойчивость VPN-сервера



Отказоустойчивость VPN-сервера



Отказоустойчивость VPN-сервера



Отказоустойчивость VPN-сервера

1. A-запись в DNS с несколькими IP-адресами
2. Костыль в MS Windows (правка реестра)
3. Копирование настроек PPP-secret, PPP-profile, RIP, OSPF на все пограничные маршрутизаторы (они же VPN-концентраторы)

Отказоустойчивость VPN-сервера

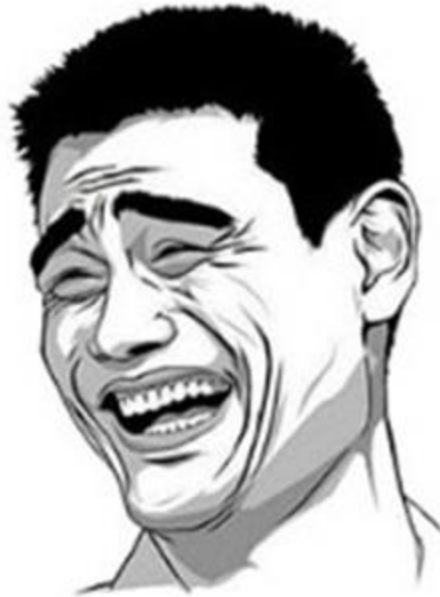
```
C:\Windows\system32\cmd.exe
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>nslookup sstp.[REDACTED] 8.8.8.8
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Не заслуживающий доверия ответ:
Цель: sstp.[REDACTED]
Addresses: 195.191.[REDACTED]
           95.31.[REDACTED]
           178.217.[REDACTED]
           185.34.[REDACTED]

C:\Users\admin>
```

Техника Apple?..

Техника Apple?..



Не, не слышал

Вопросы?

Пишите на

training@mikrotik-courses.ru

Хорошего дня!
Спасибо за ваше
внимание!