VPN с компьютера в корпоративную сеть

Алексей Чудин
Москва, МУМ 2018

MikroTik Courses

Обо мне

Алексей Чудин

Сертифицированный тренер MikroTik с 2014 г.

Сертификаты:

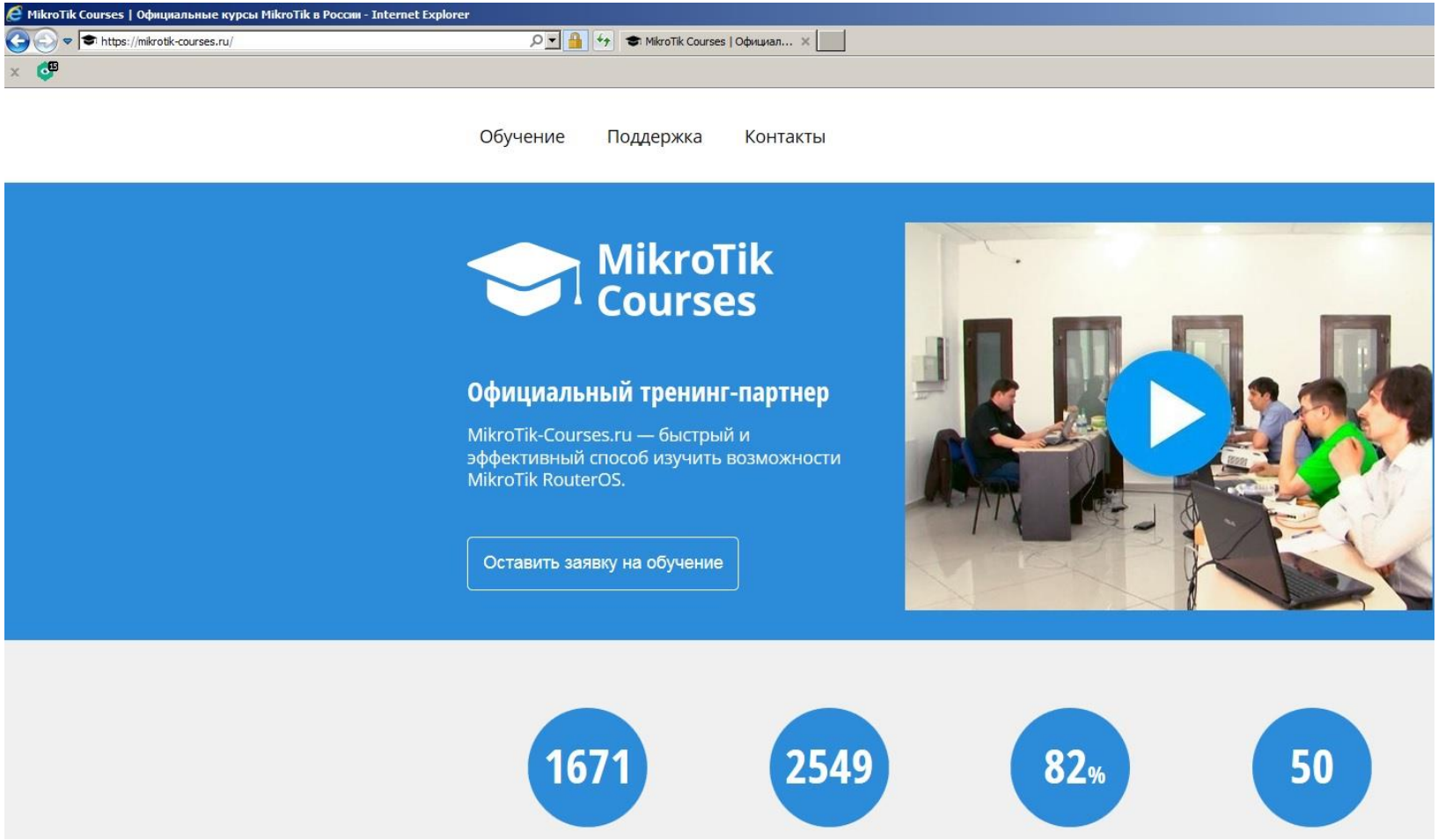
MikroTik: MTCNA, MTCRE, MTCWE, MTCTCE, MTCUME, MTCINE, MTCIPv6E,

MikroTik Trainer №0246

Microsoft: MCP, MCSA

Cisco: CCNA, CCNP (R&S)

www.mikrotik-courses.ru



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, MTCTCE, MTCINE, MTCIPv6E)

- в среднем проводится 2 тренинга в неделю
- 4 тренера:
- Алексей Чудин
- Александр Романов
- Николай Кузнецов
- Максим Бусов

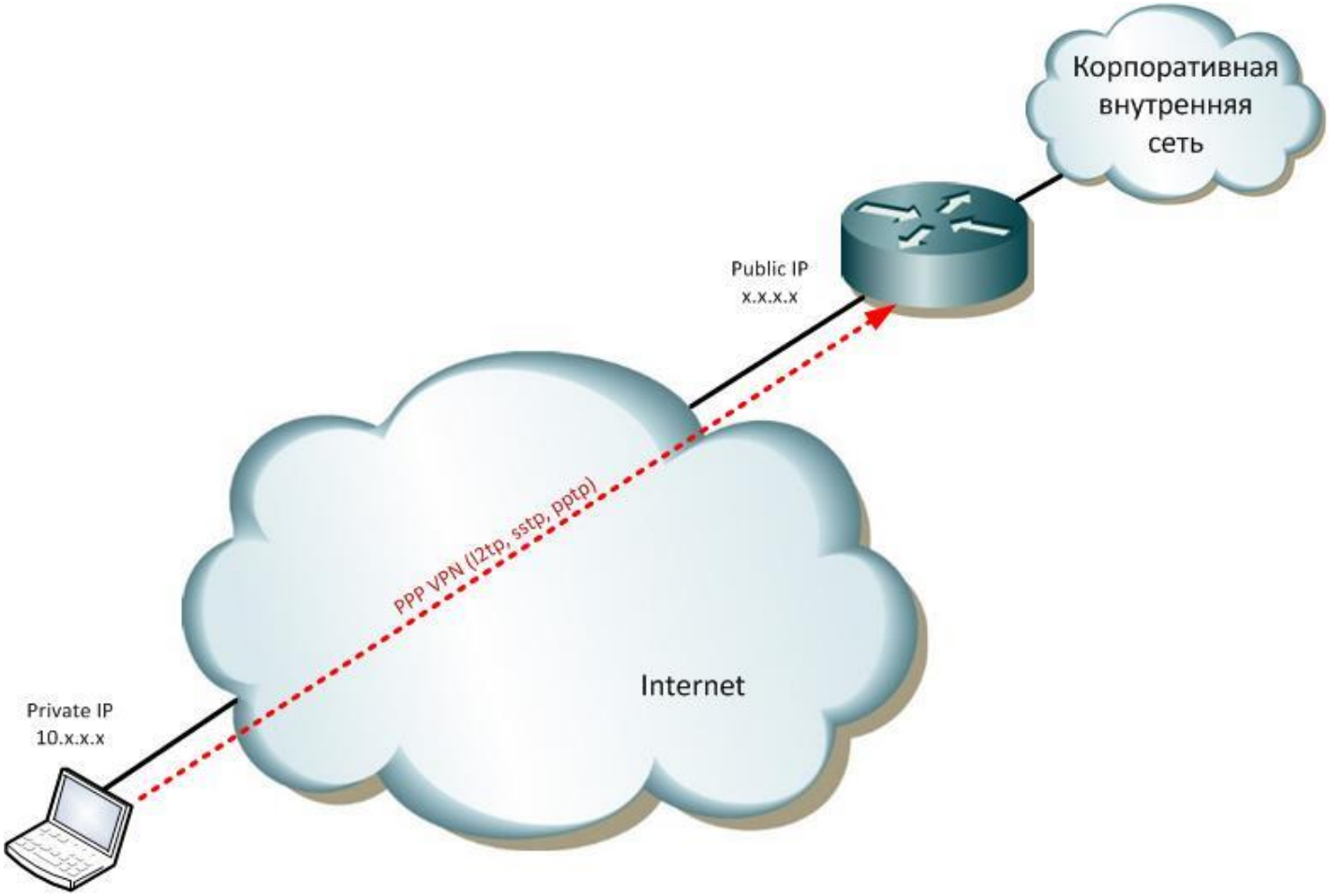
MikroTik-Courses.ru: ведущий тренинг-центр **MikroTik** в России и СНГ

За 4,5 года работы:

- 5 стран (РФ, РБ, Казахстан, Кыргызстан, Индия)
- 50 городов
- География от Калининграда до Владивостока и от Архангельска до Калькутты

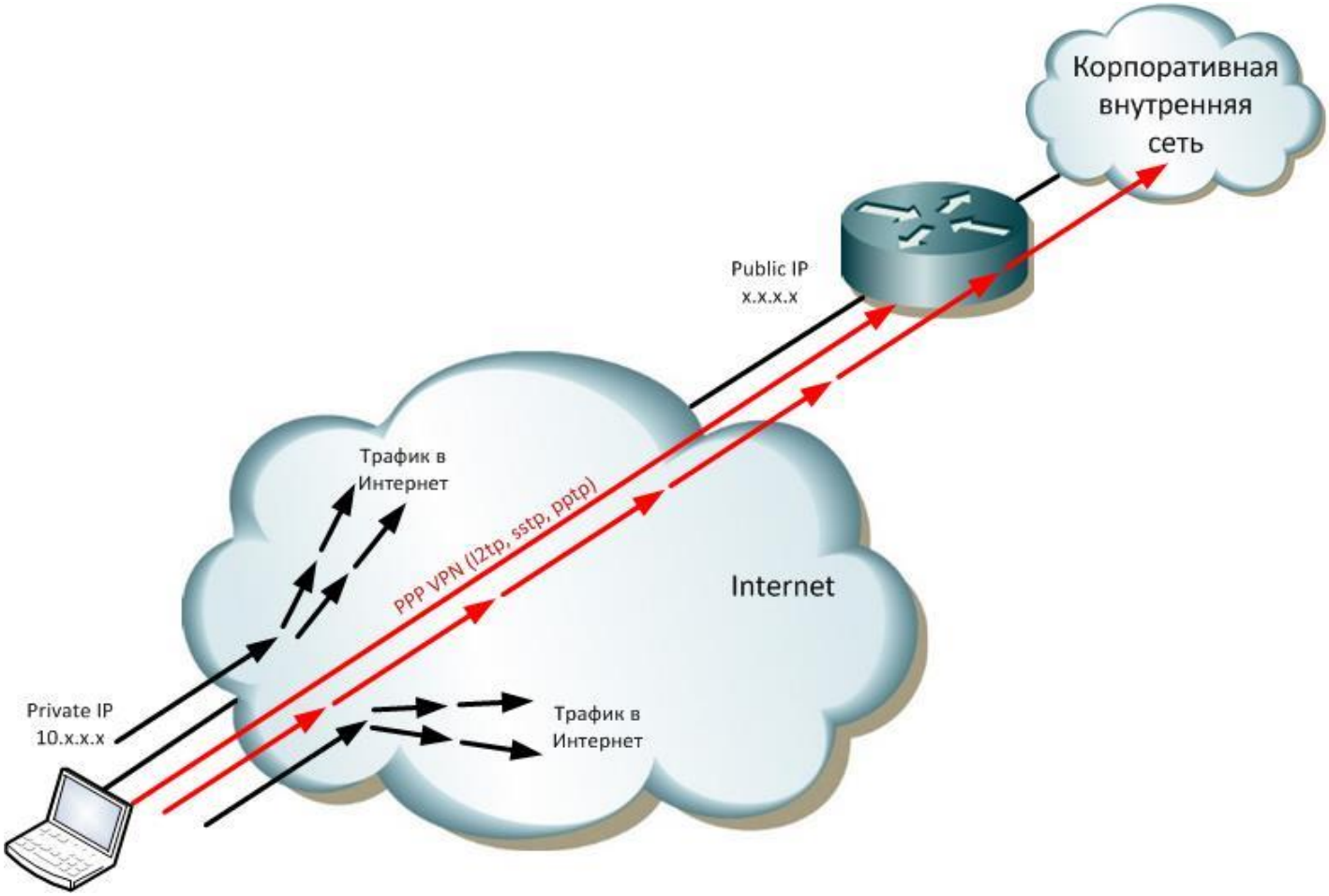
- Тренинги в Риге в собственном тренинг-центре компании **MikroTik** (октябрь)

Постановка задачи



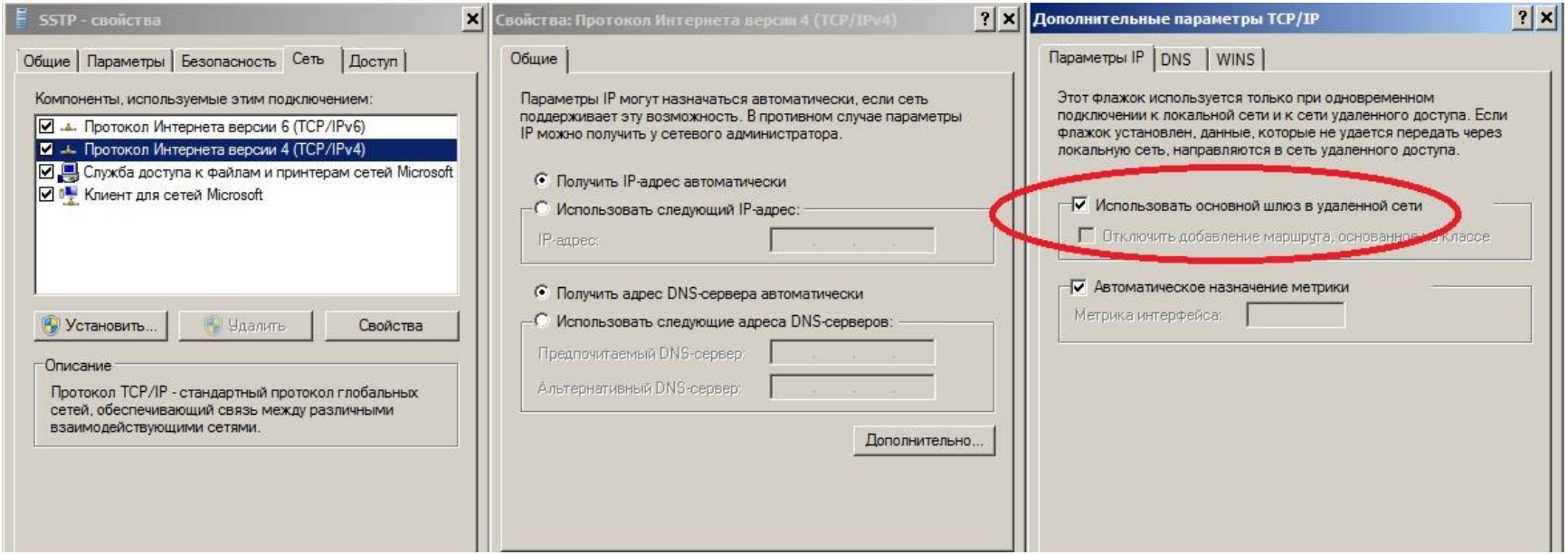
MikroTik Courses

Постановка задачи



MikroTik Courses

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)?

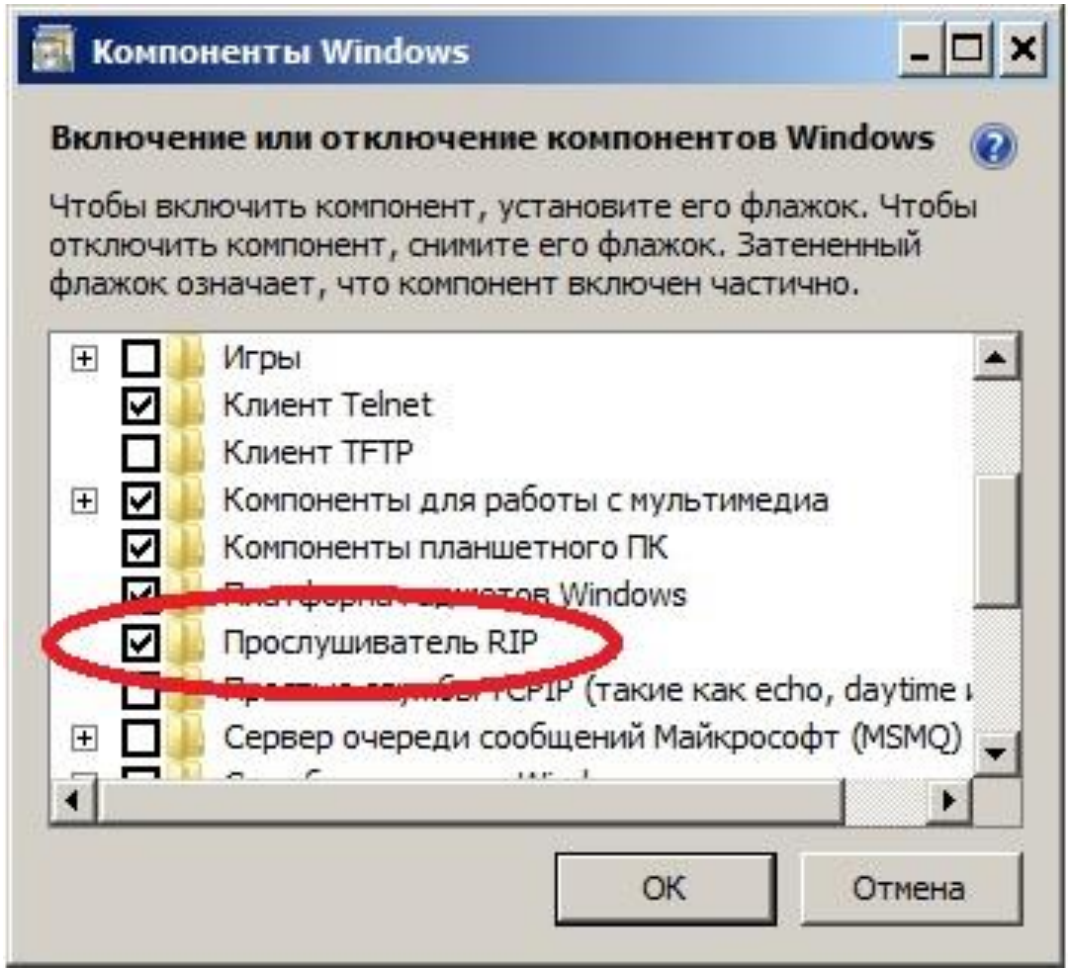
Постановка задачи

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

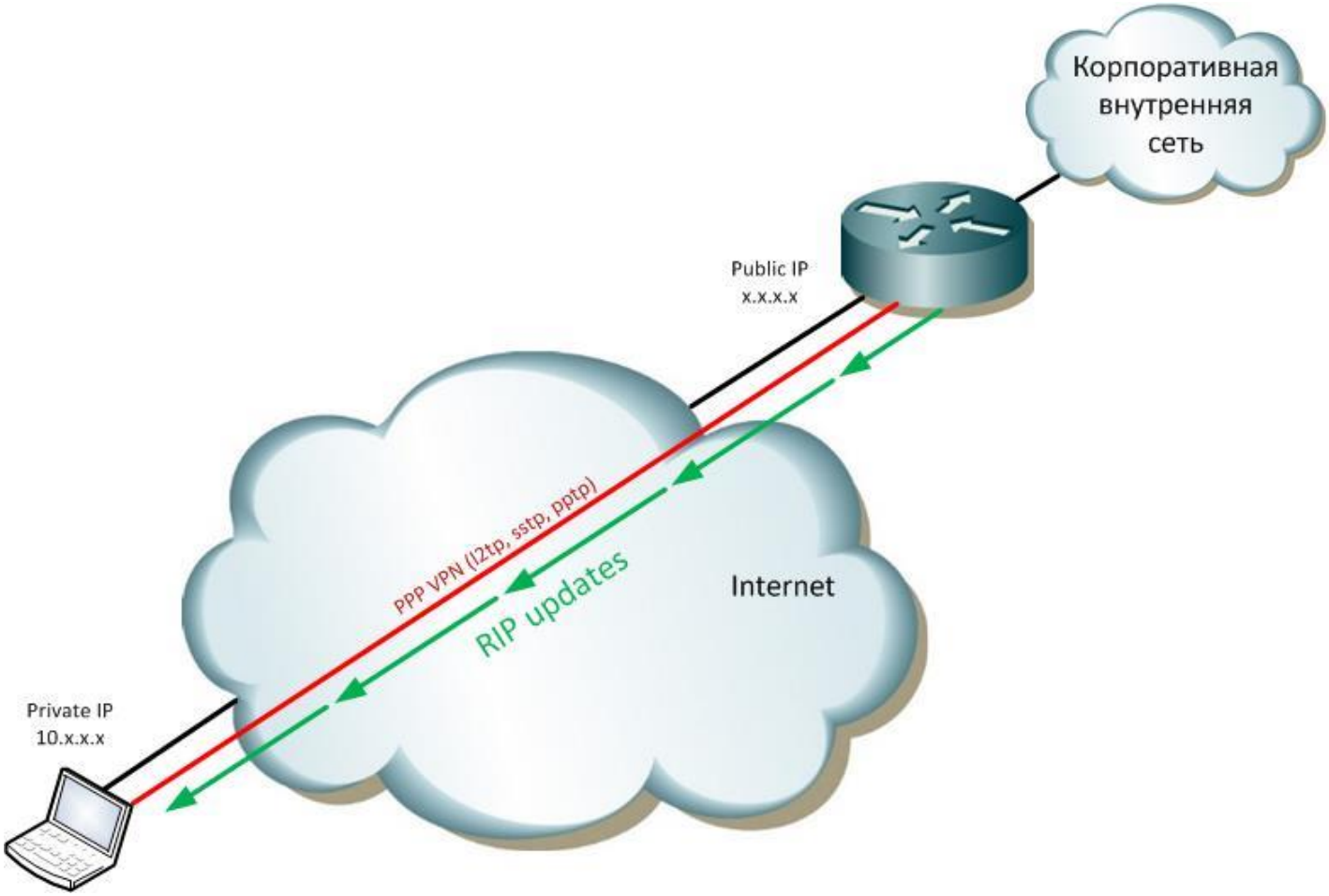
Решение задачи

RIP!

Решение задачи



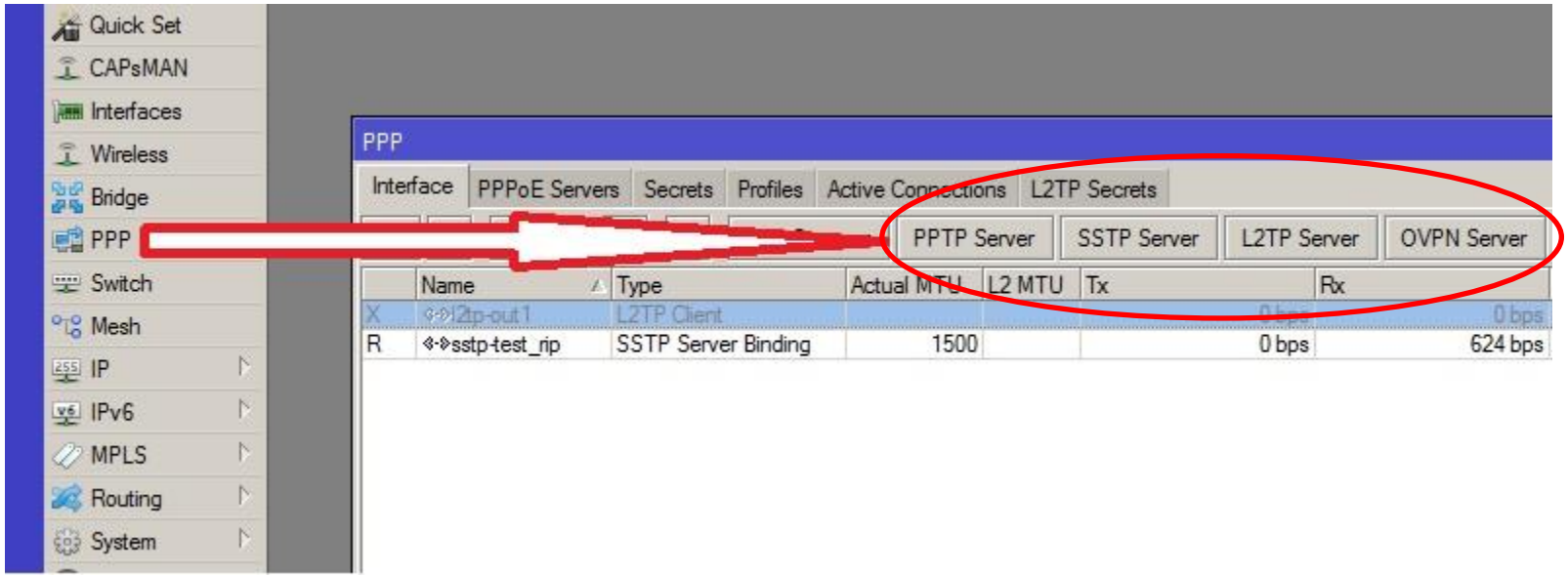
Решение задачи



MikroTik Courses

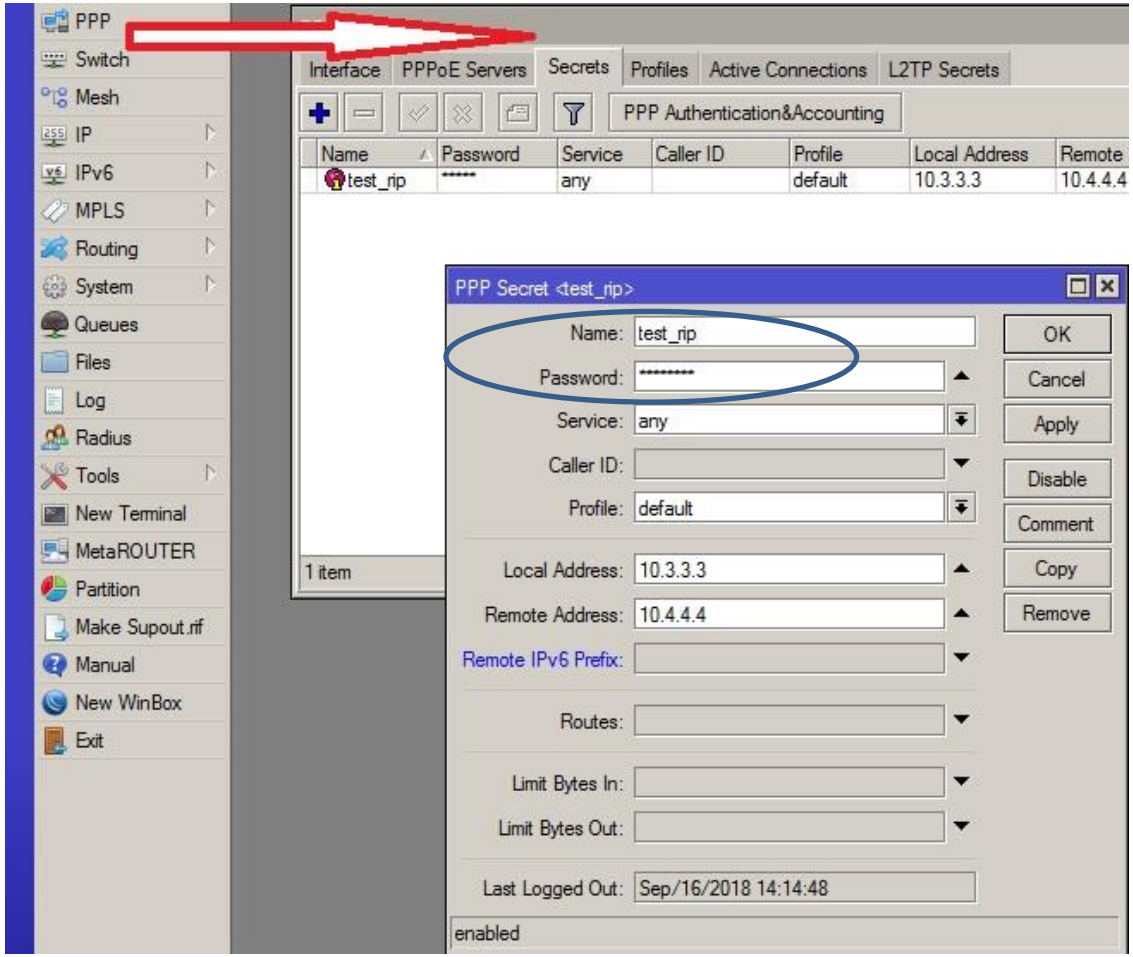
Решение задачи

1. Включаем PPP-сервер

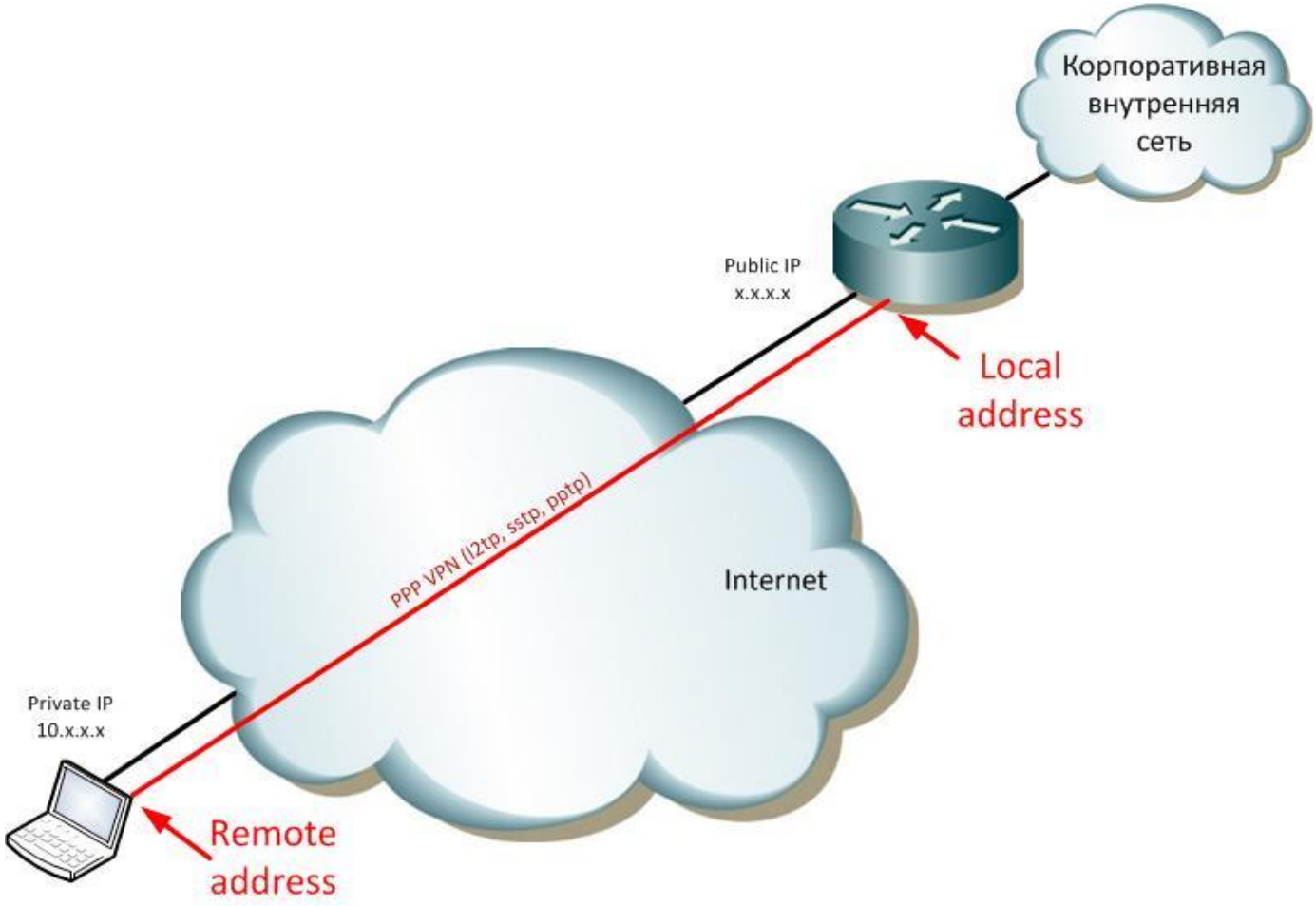


Решение задачи

2. Заводим юзера



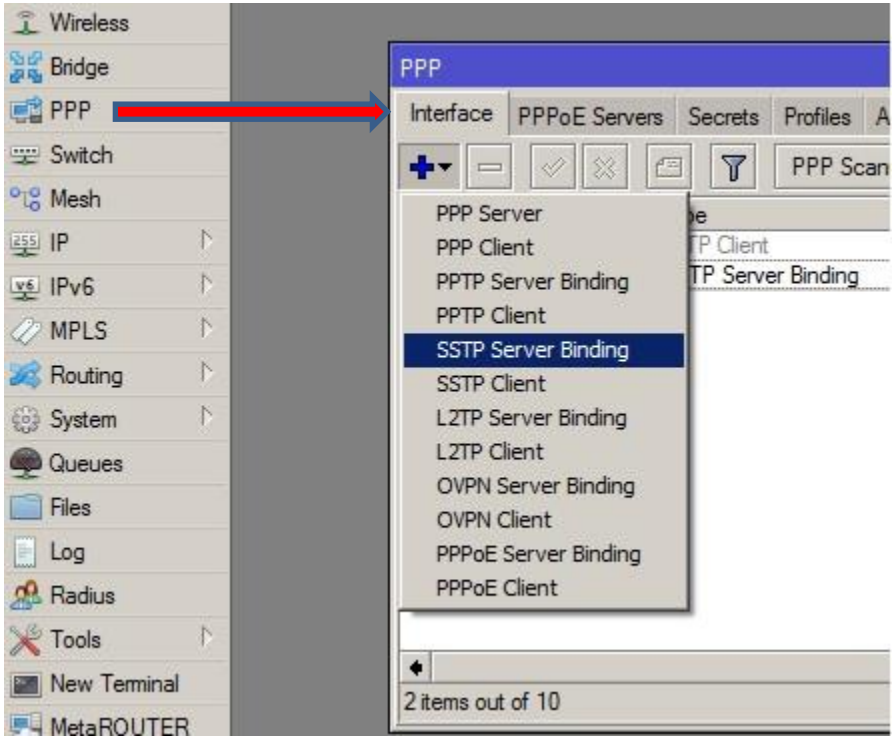
Решение задачи



MikroTik Courses

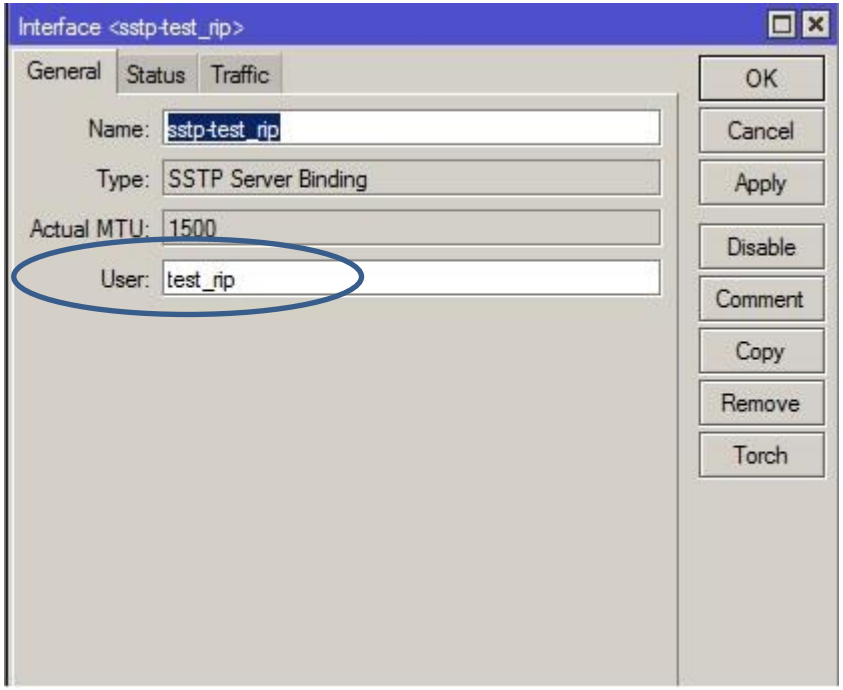
Решение задачи

3. Создаем server binding



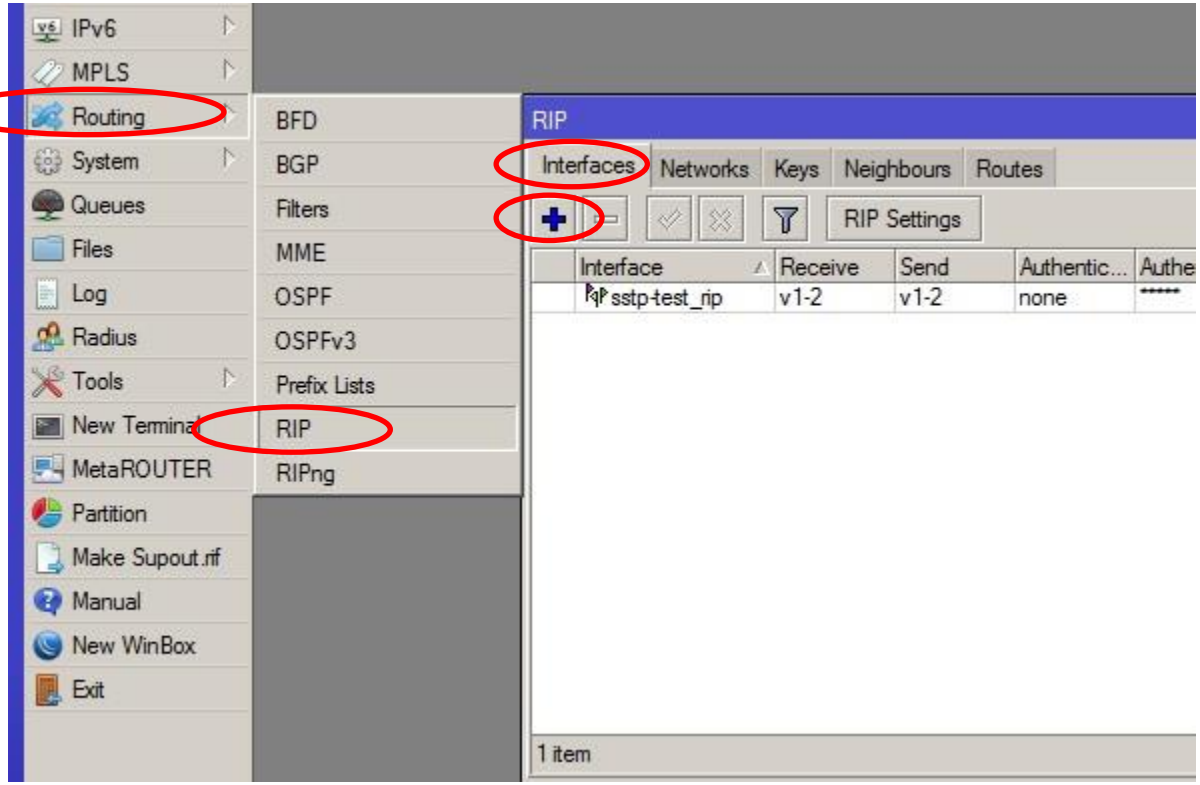
Решение задачи

3. Создаем server binding



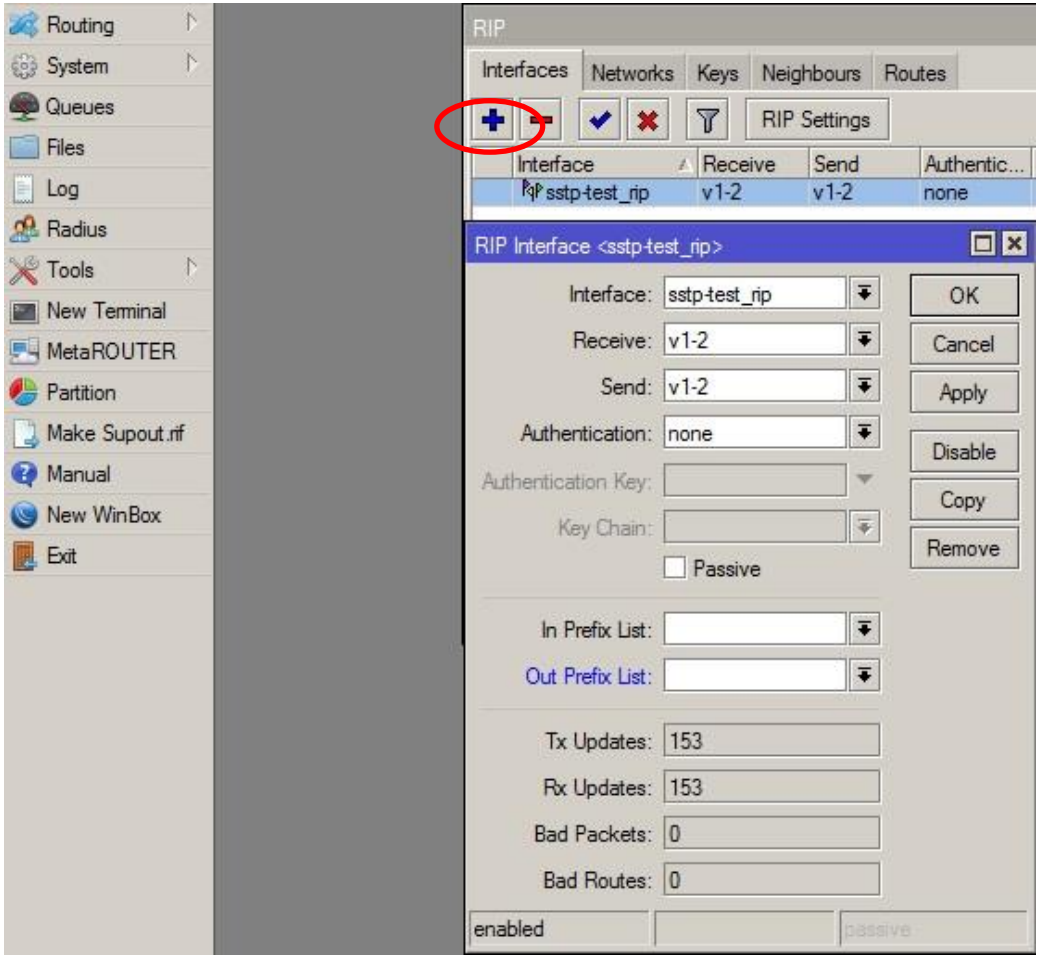
Решение задачи

4. Запускаем протокол RIP на роутере



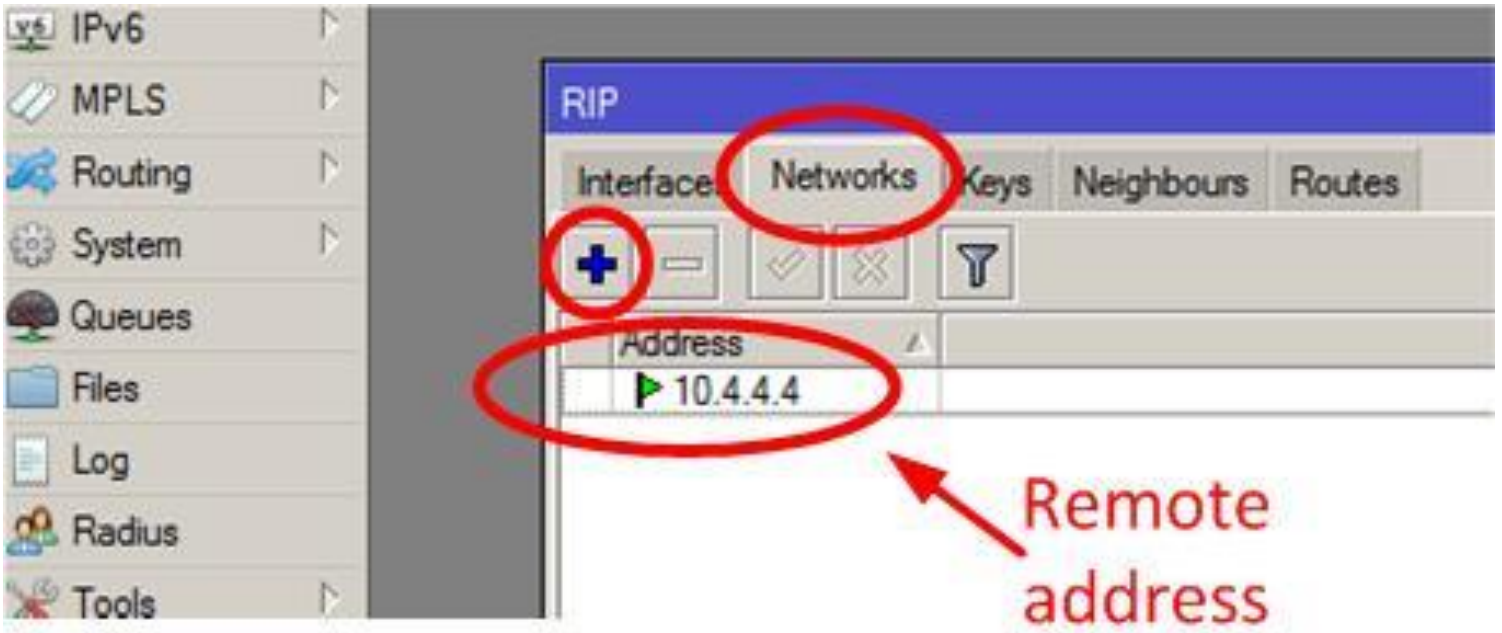
Решение задачи

4. Запускаем протокол RIP на роутере



Решение задачи

4. Запускаем протокол RIP на роутере



Remote address – это адрес нашего компьютера

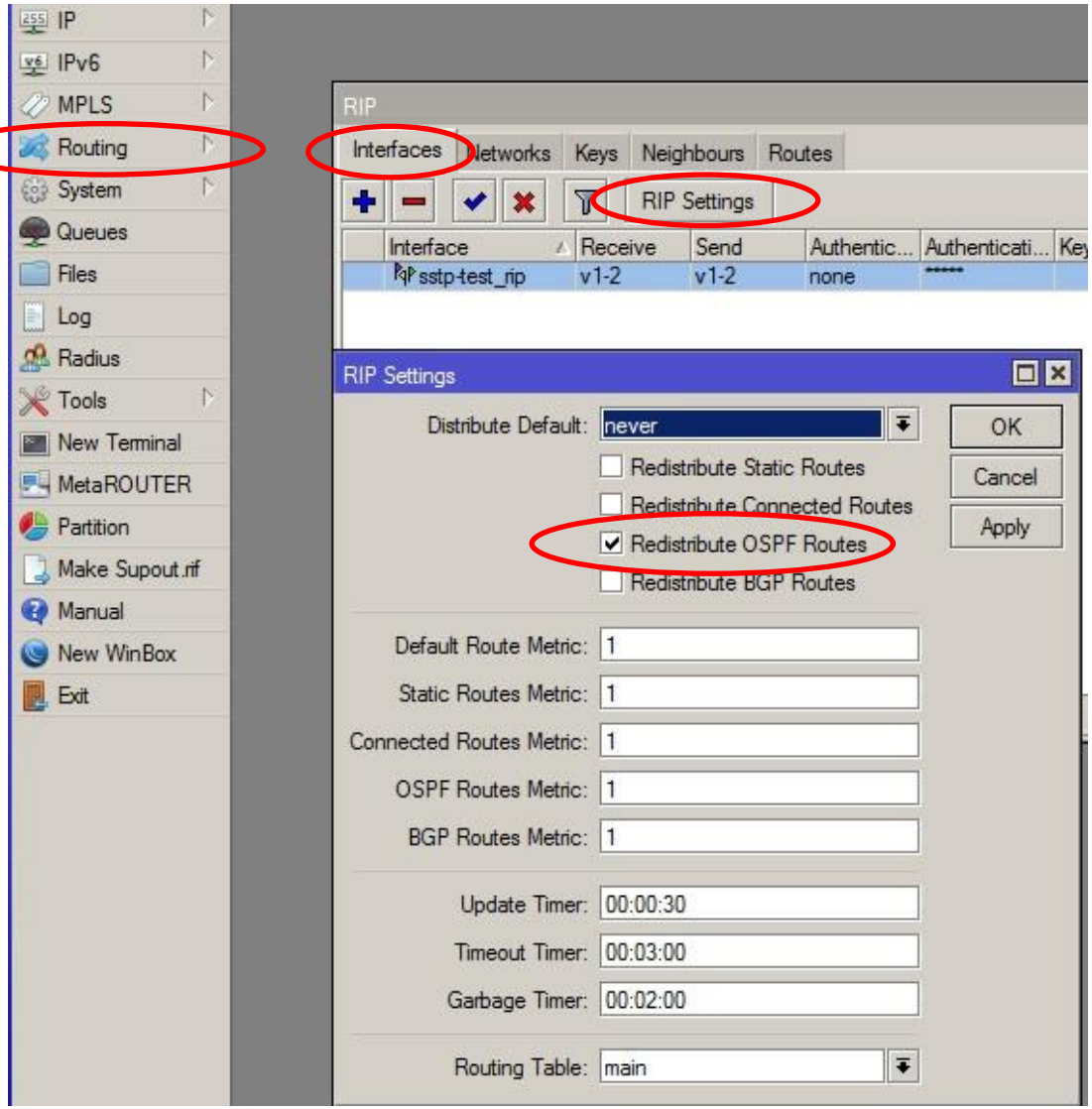
Решение задачи

- 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**

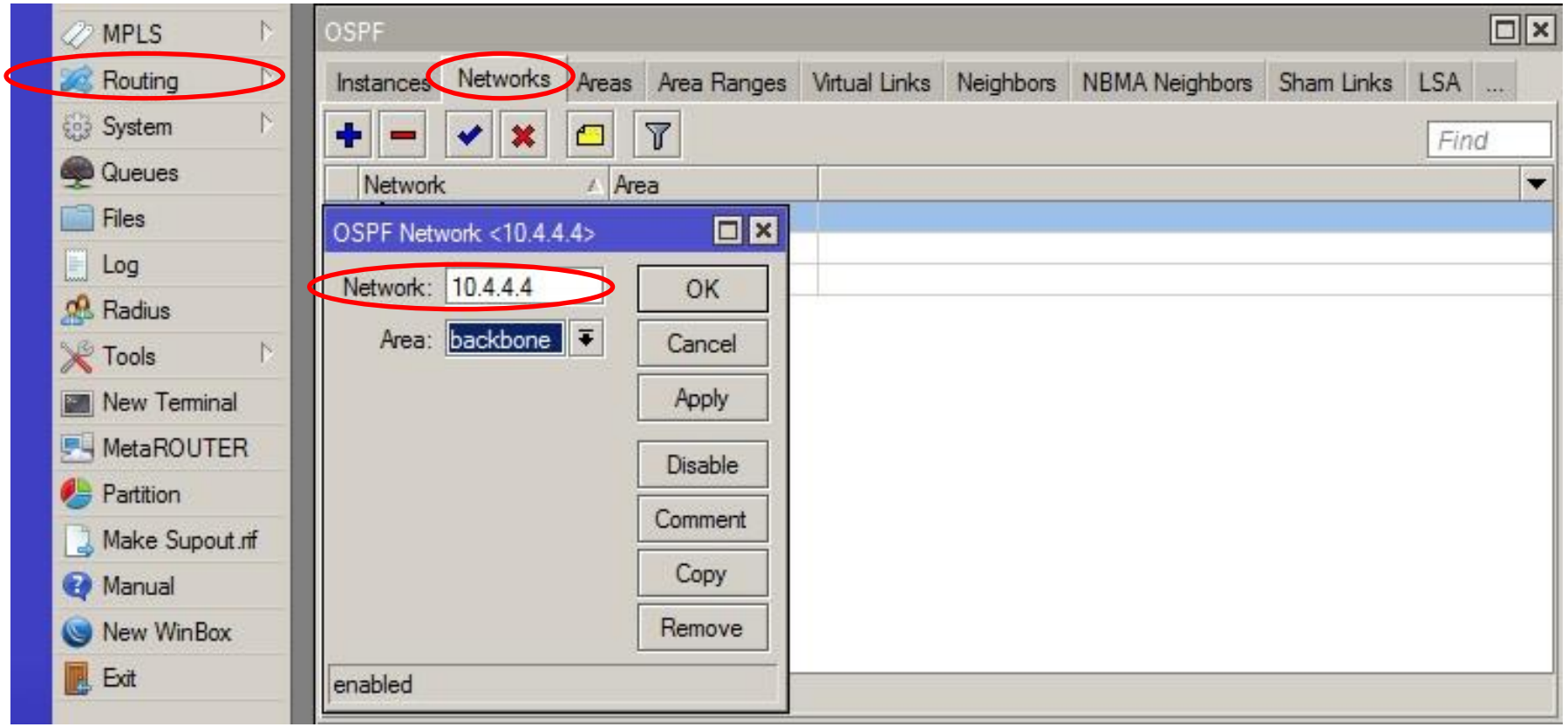
Решение задачи



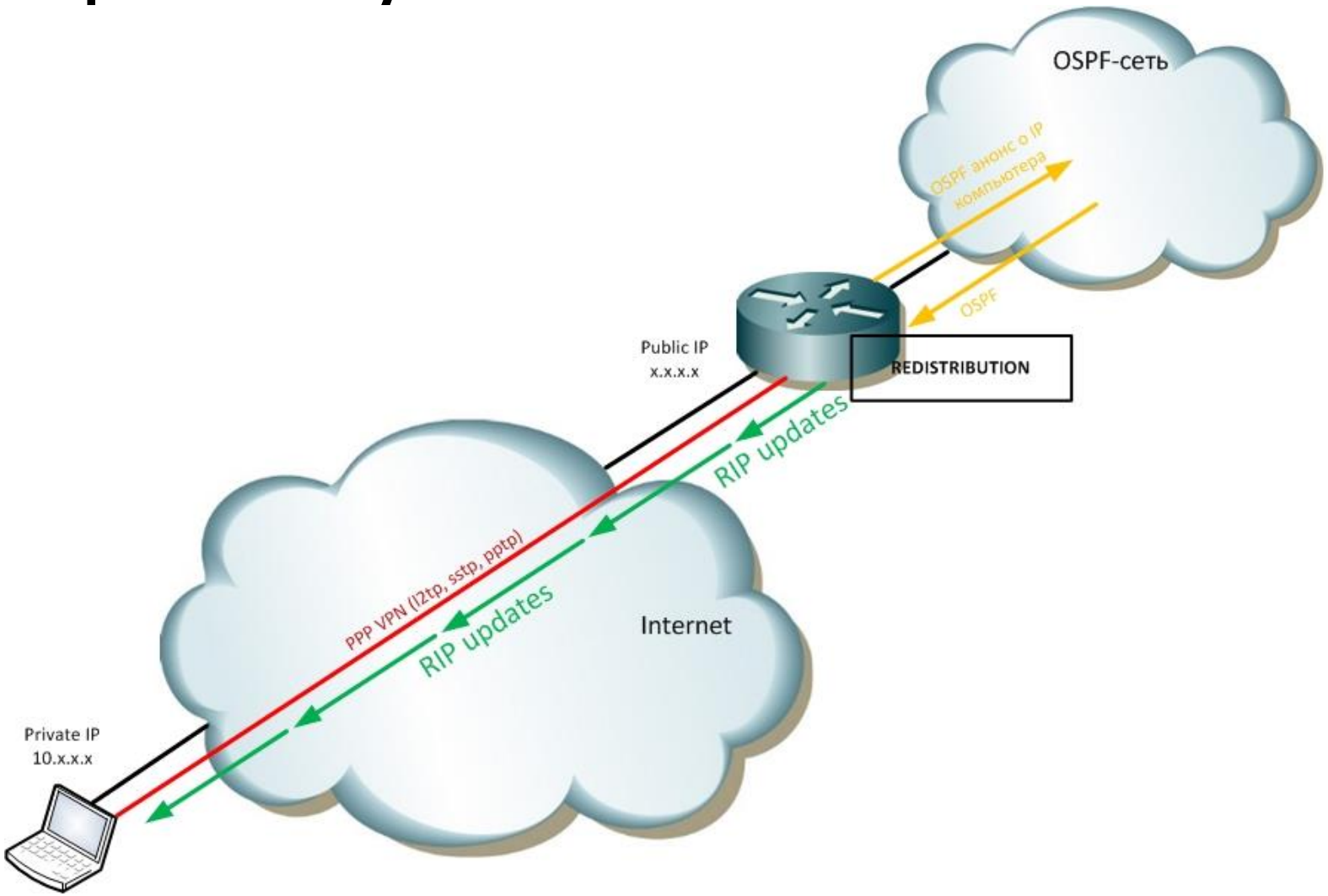
Решение задачи

- 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

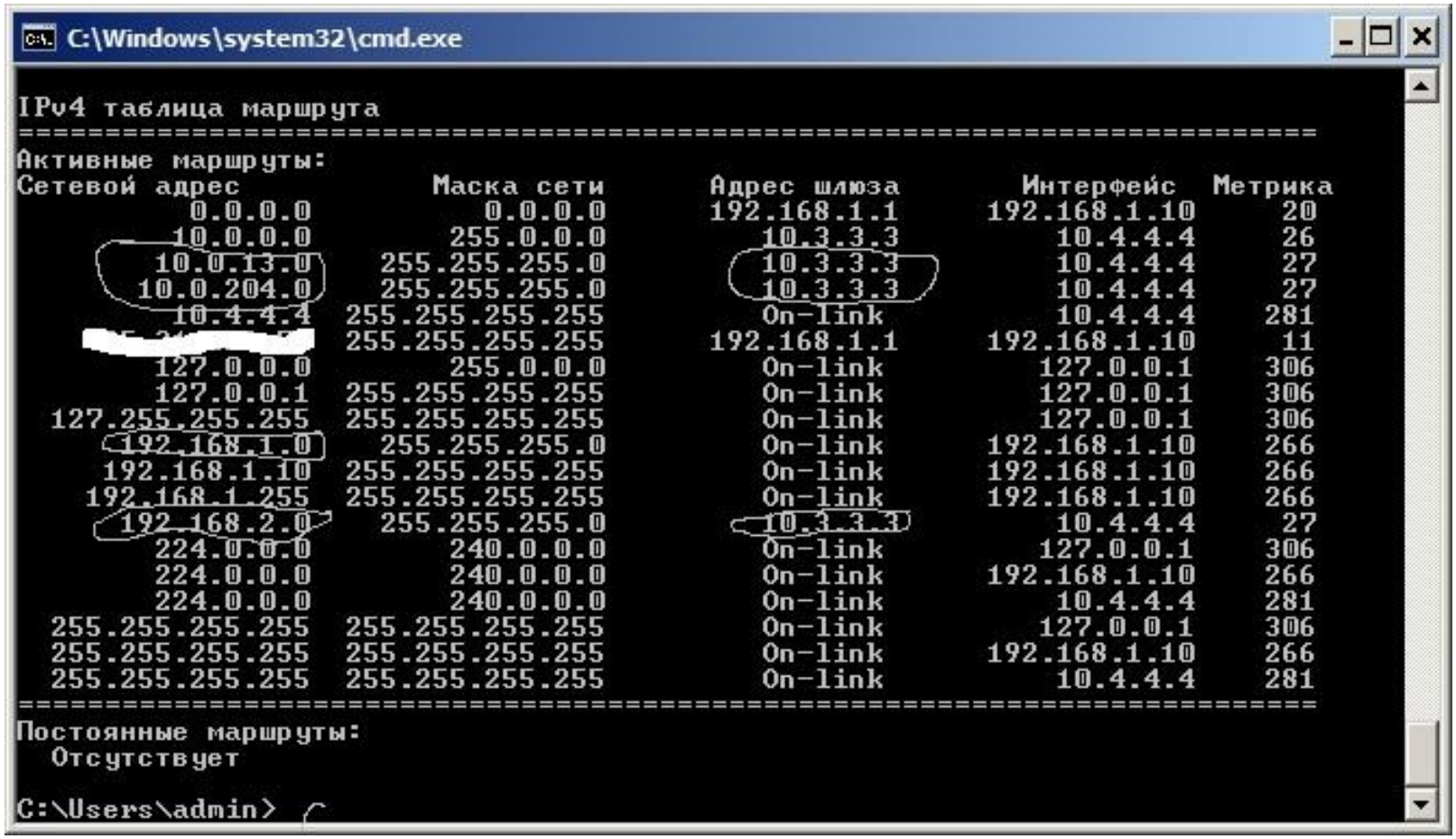
Решение задачи



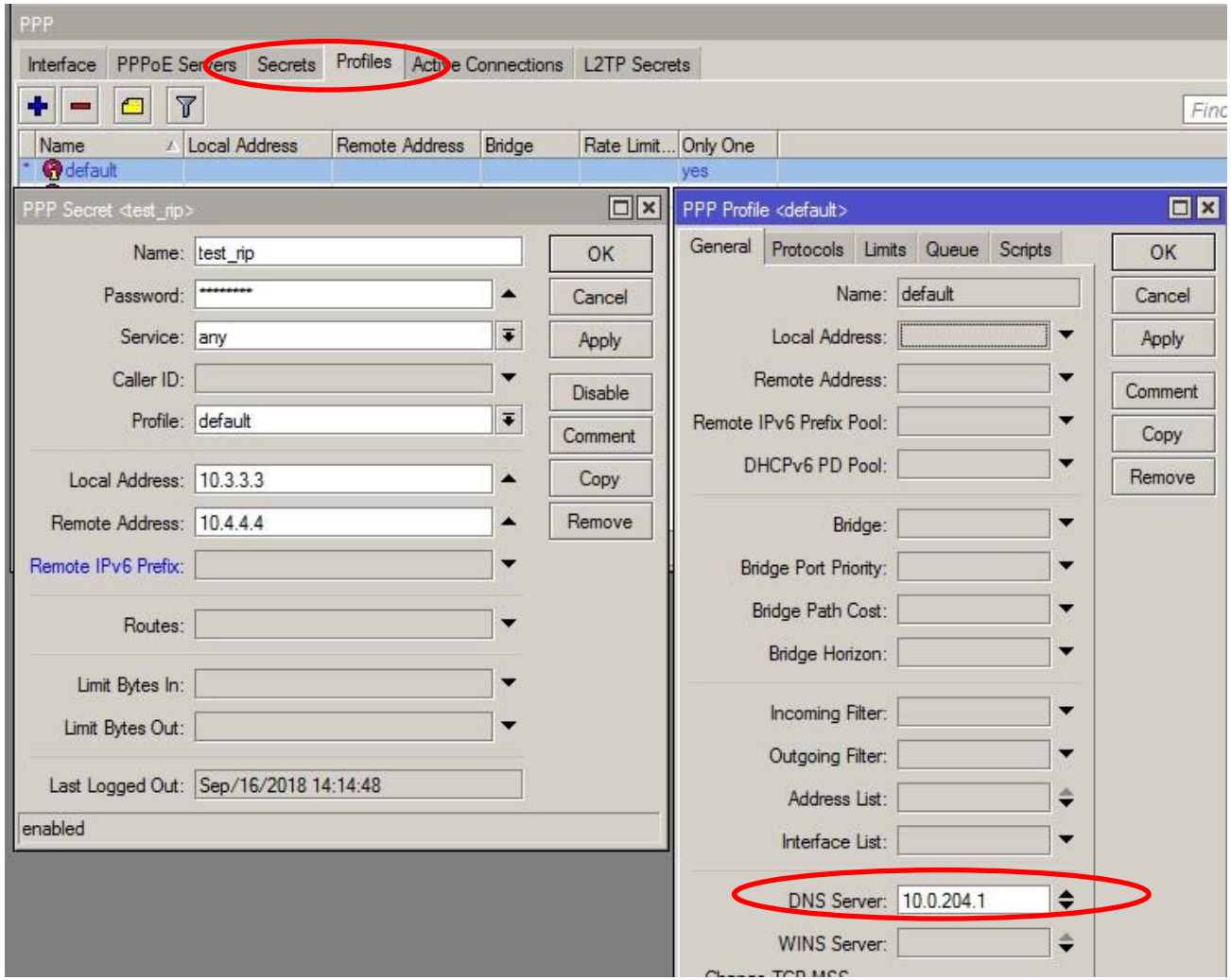
Промежуточный итог



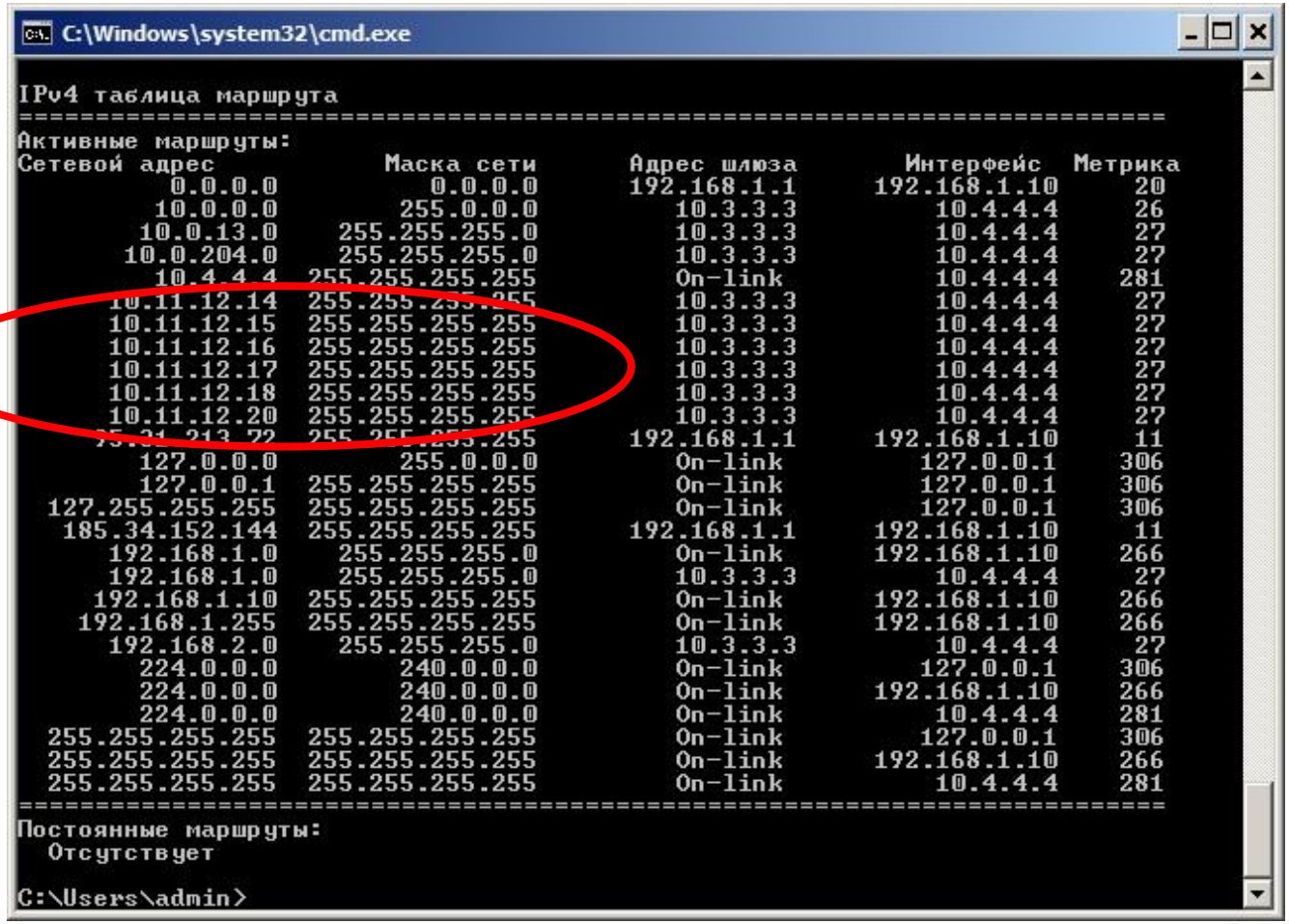
Промежуточный итог



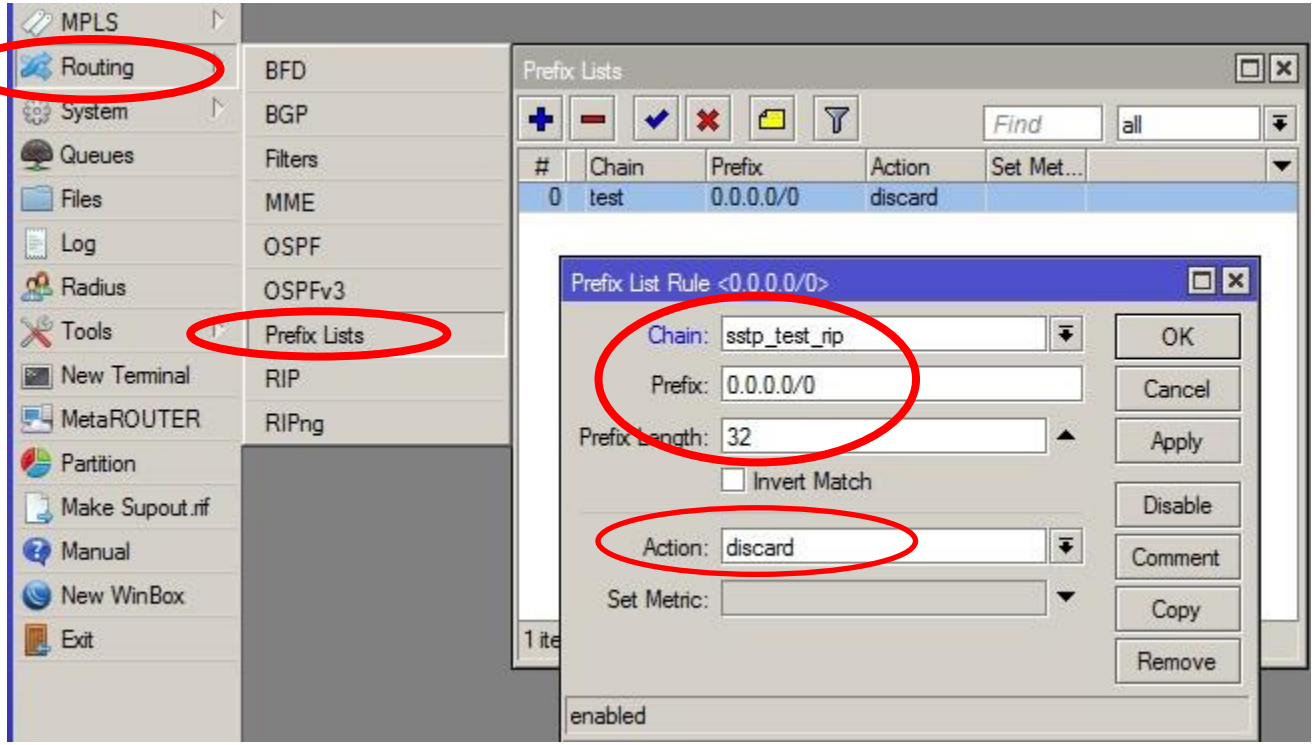
Приятные мелочи



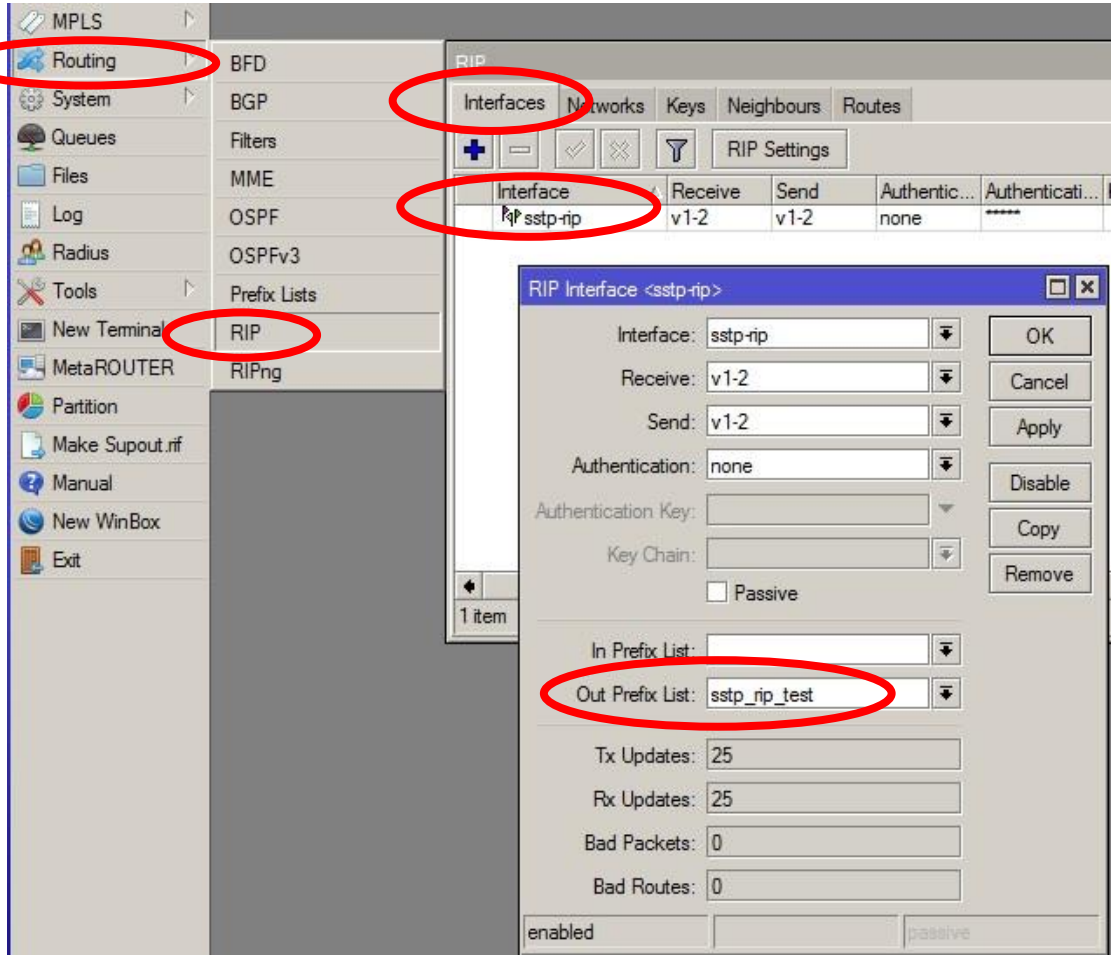
Приятные мелочи



Приятные мелочи

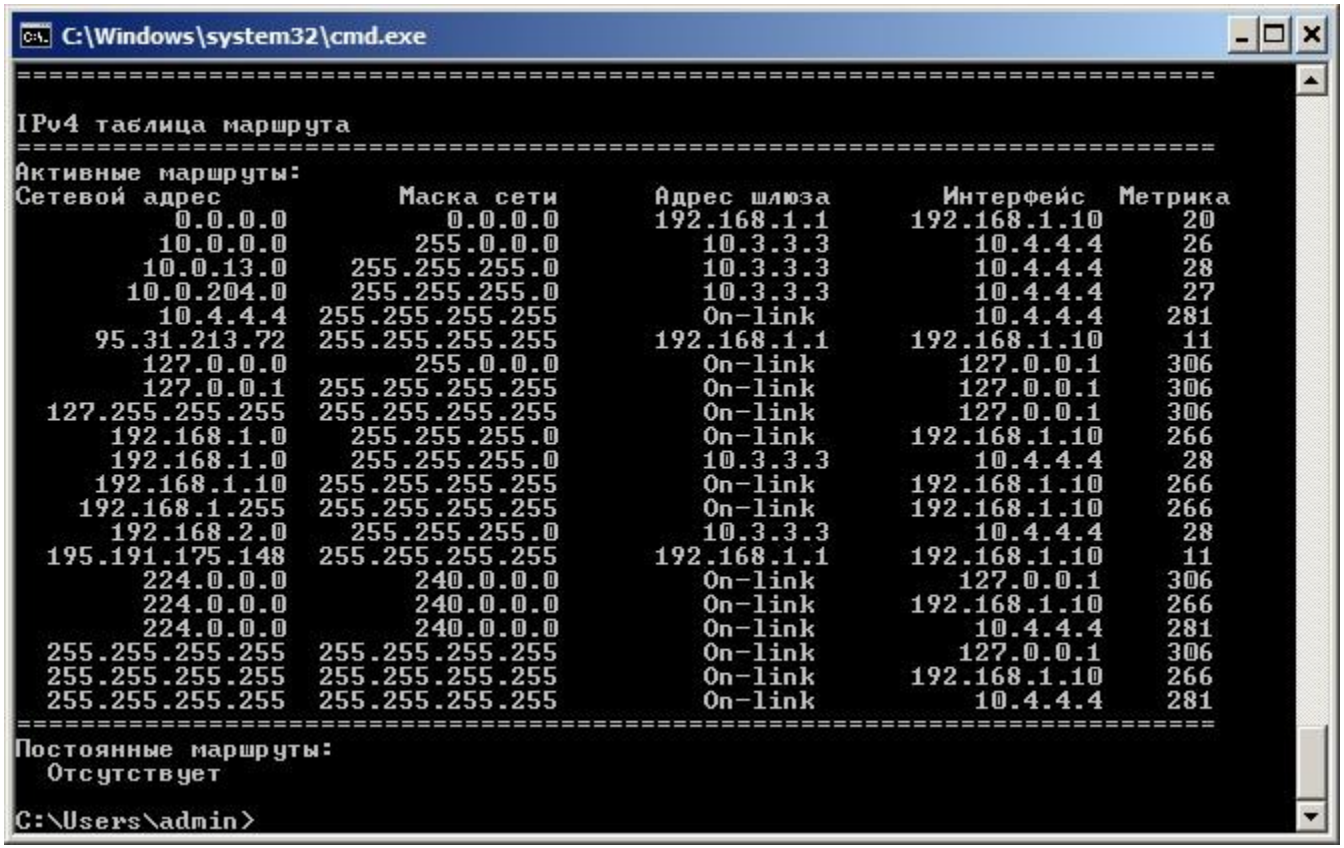


Приятные мелочи



MikroTik Courses

Приятные мелочи

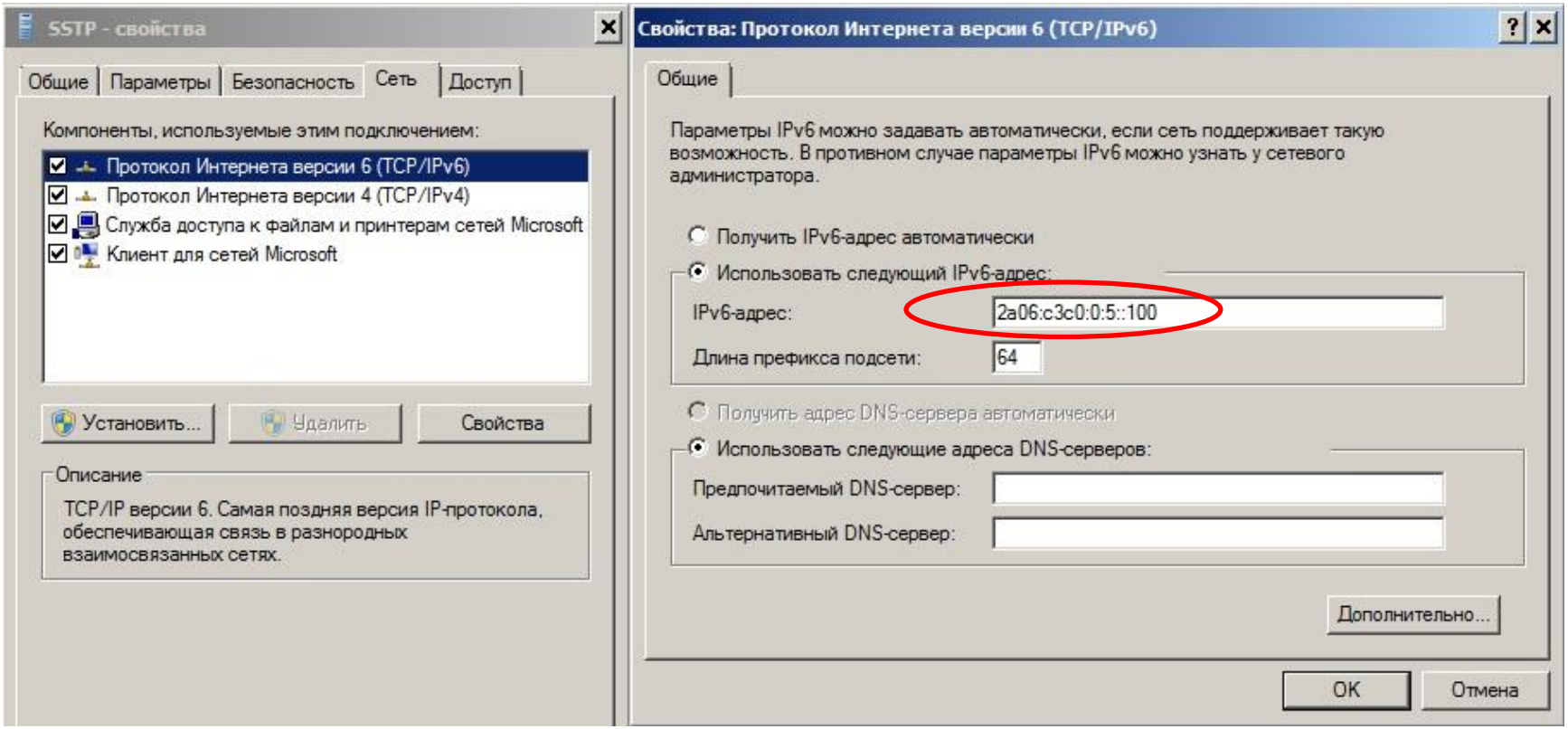


А как насчет IPv6? ☺

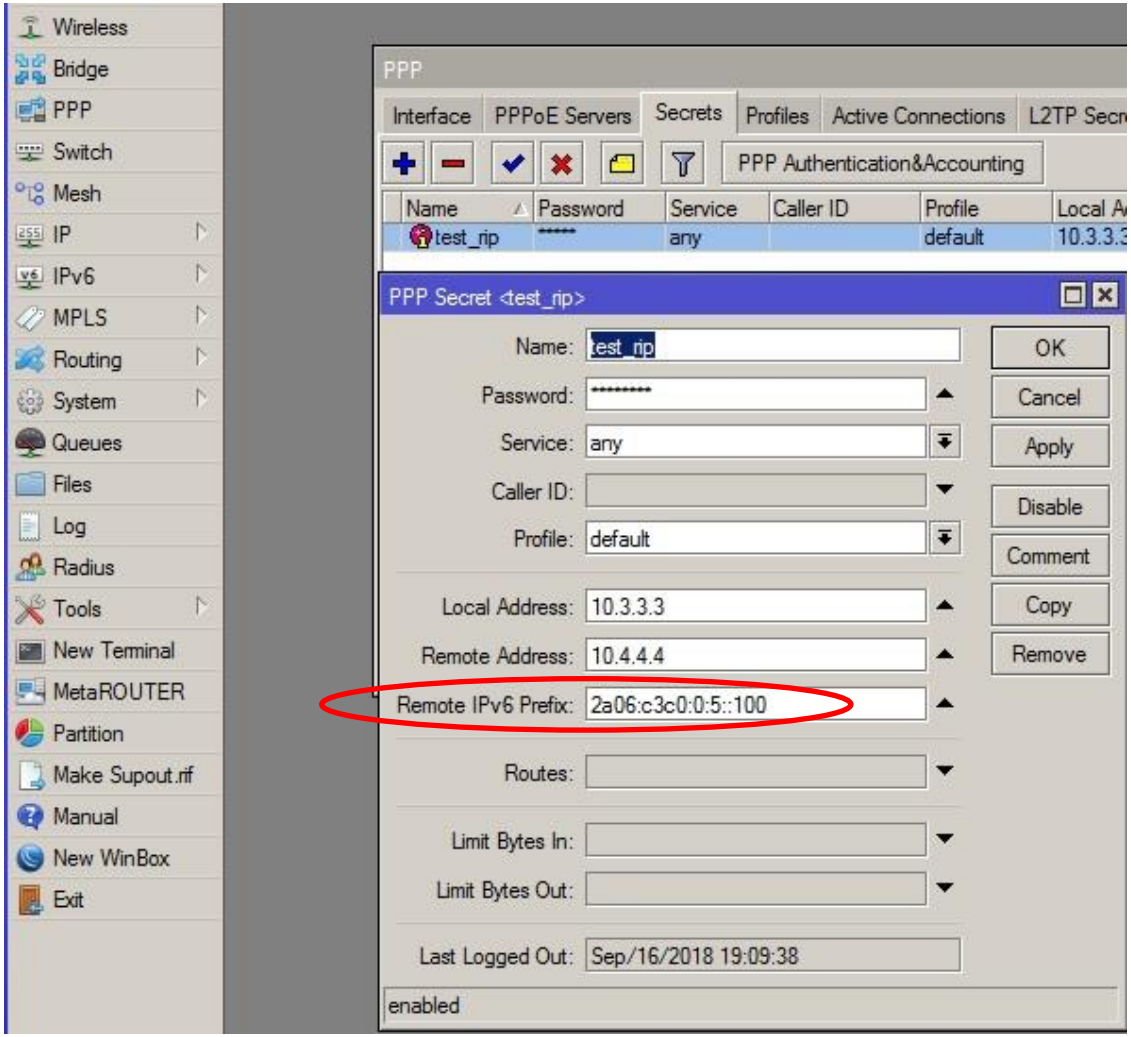
Доступ к IPv6

- 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

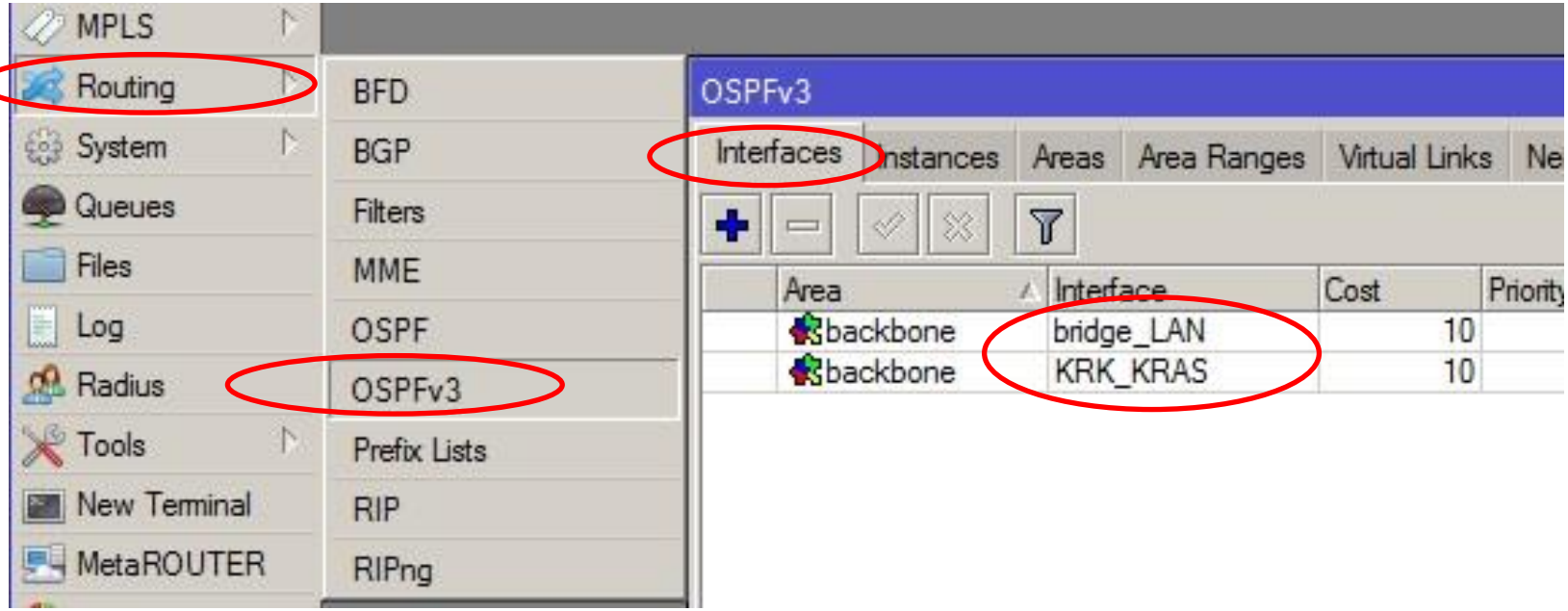


Доступ к IPv6

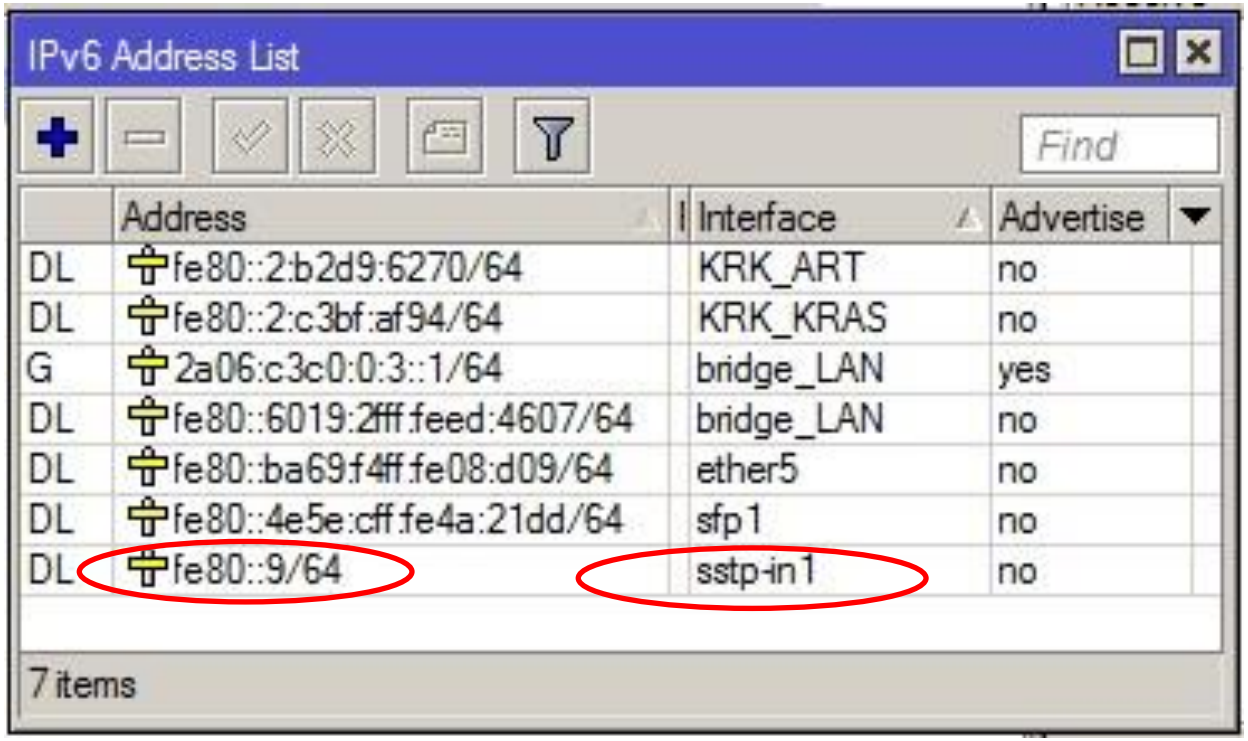


MikroTik Courses

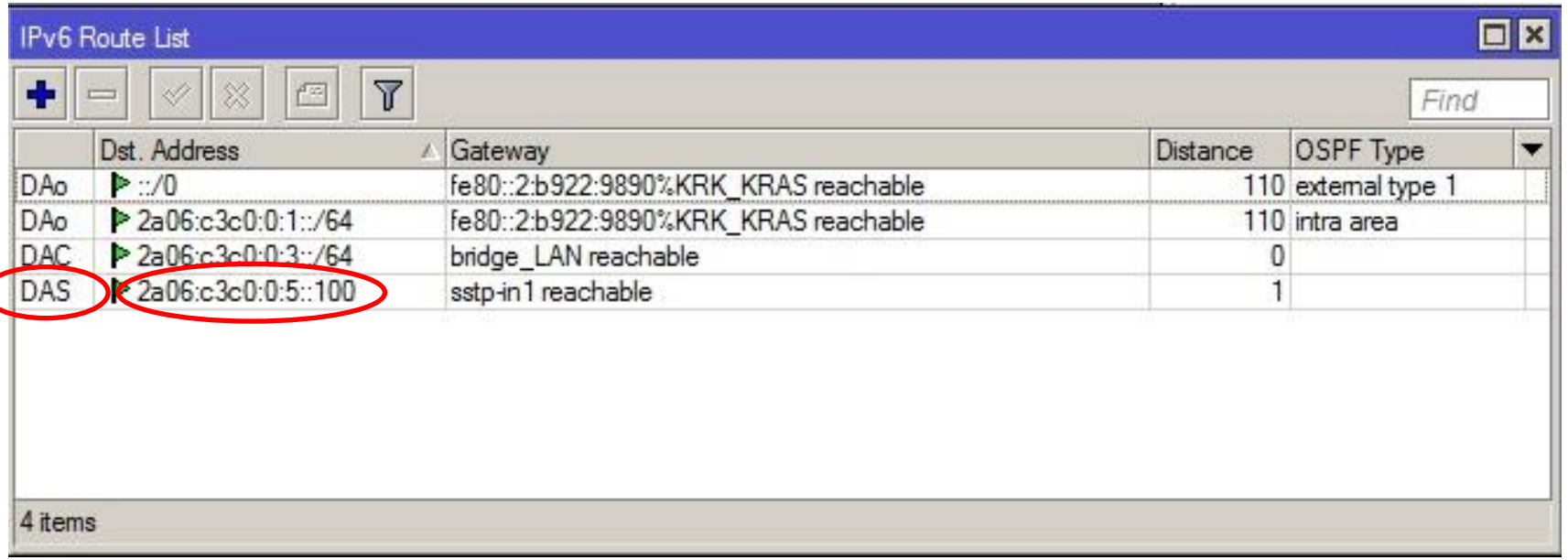
Доступ к IPv6



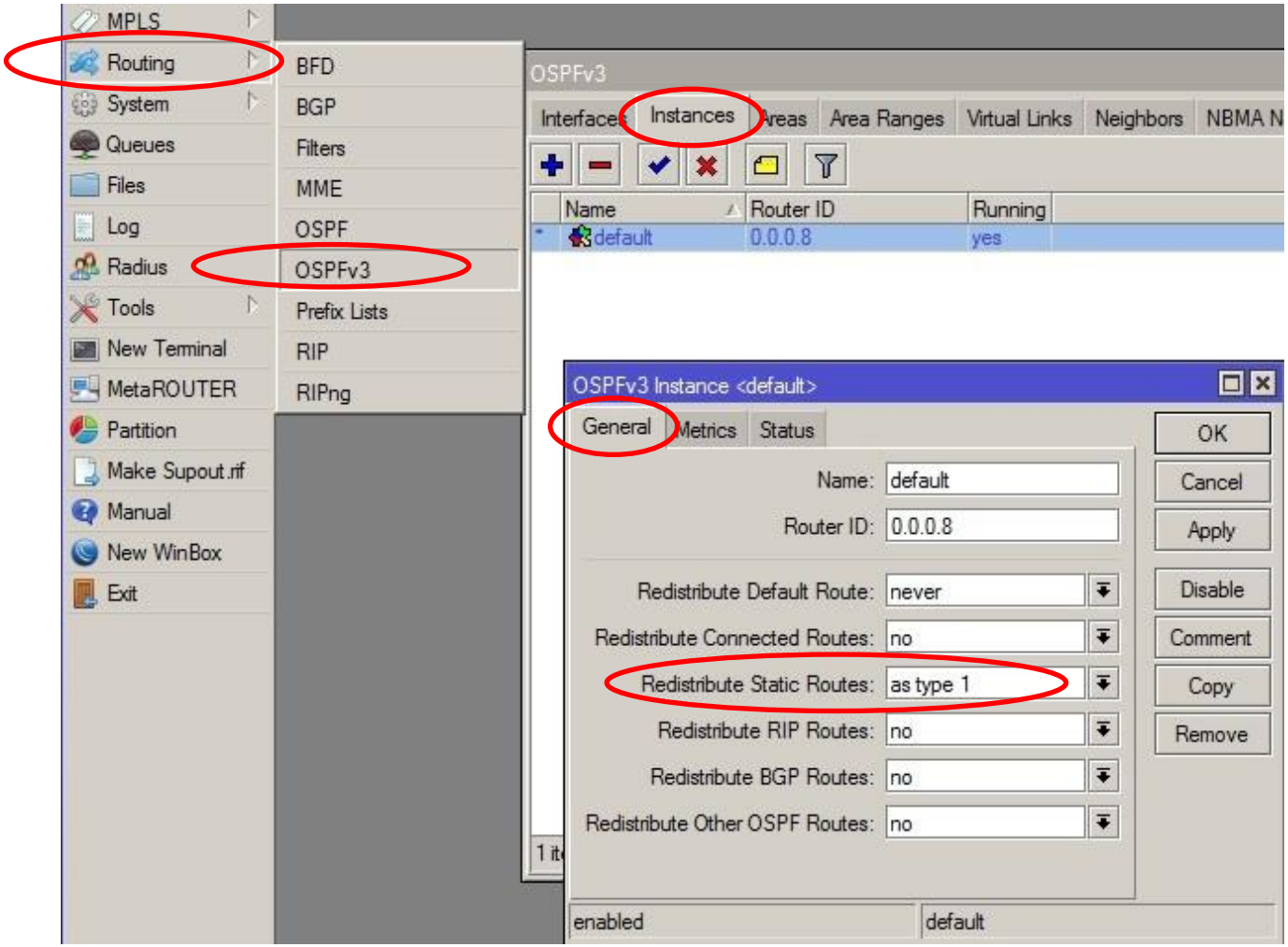
Доступ к IPv6



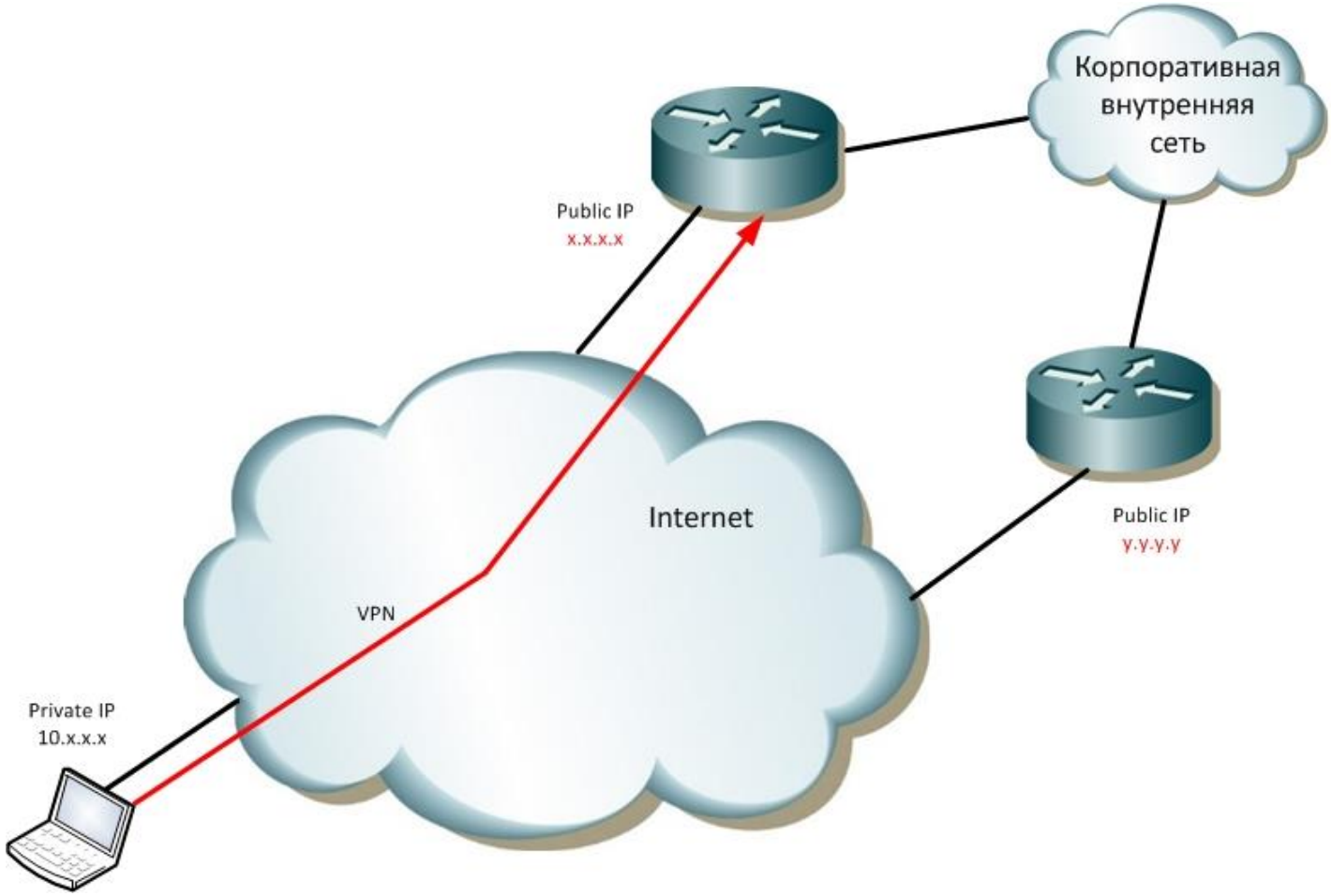
Доступ к IPv6



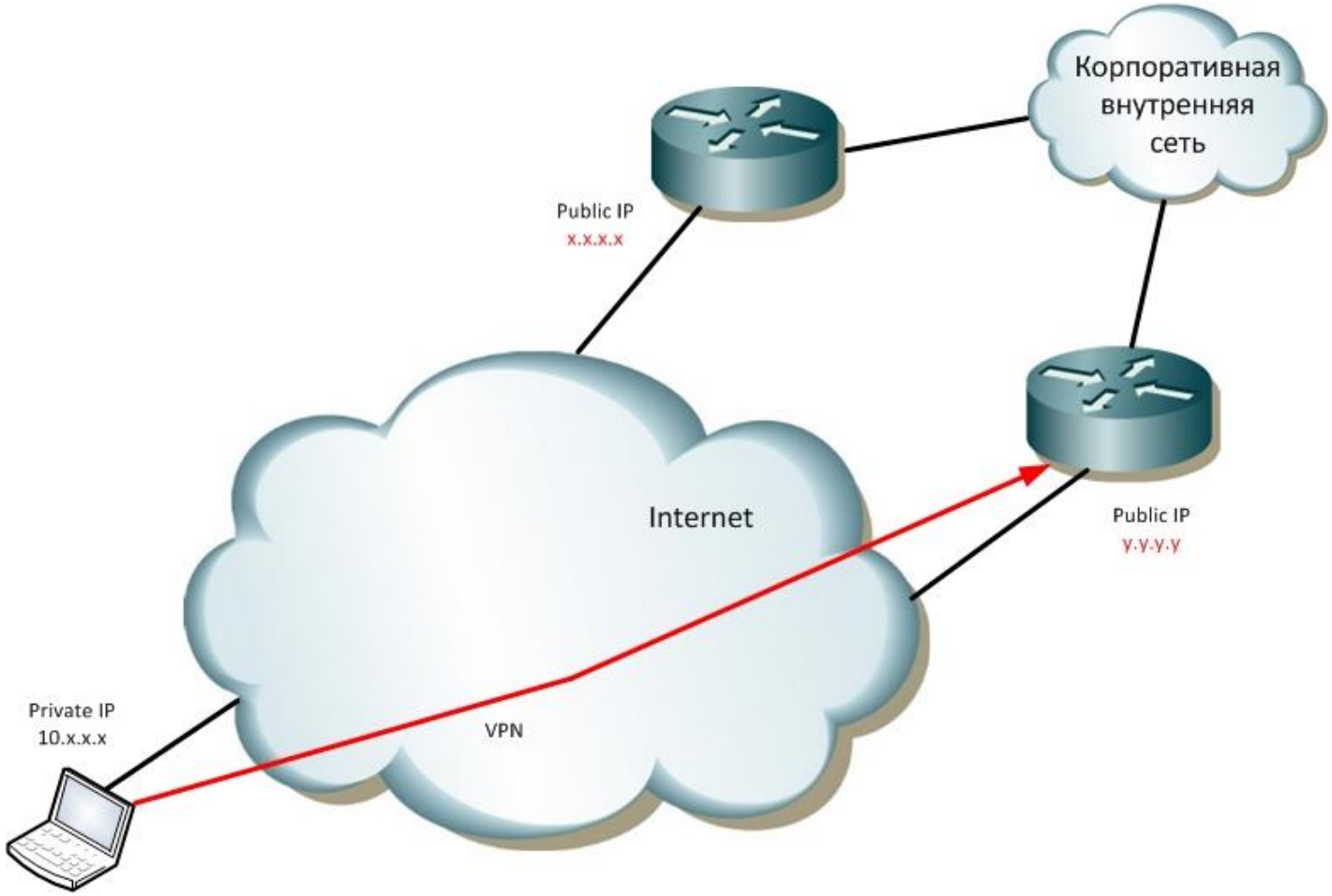
Доступ к IPv6



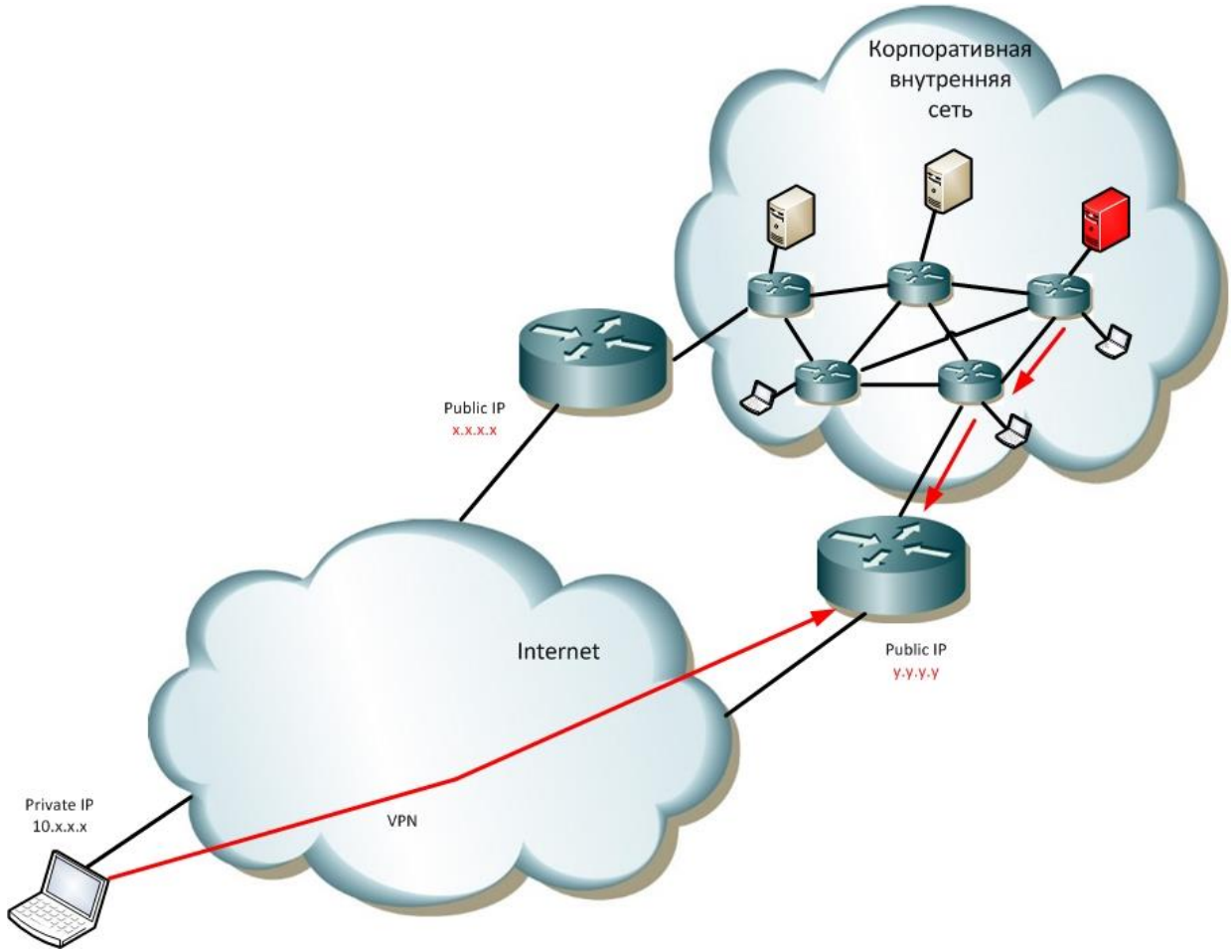
Отказоустойчивость VPN-сервера



Отказоустойчивость VPN-сервера

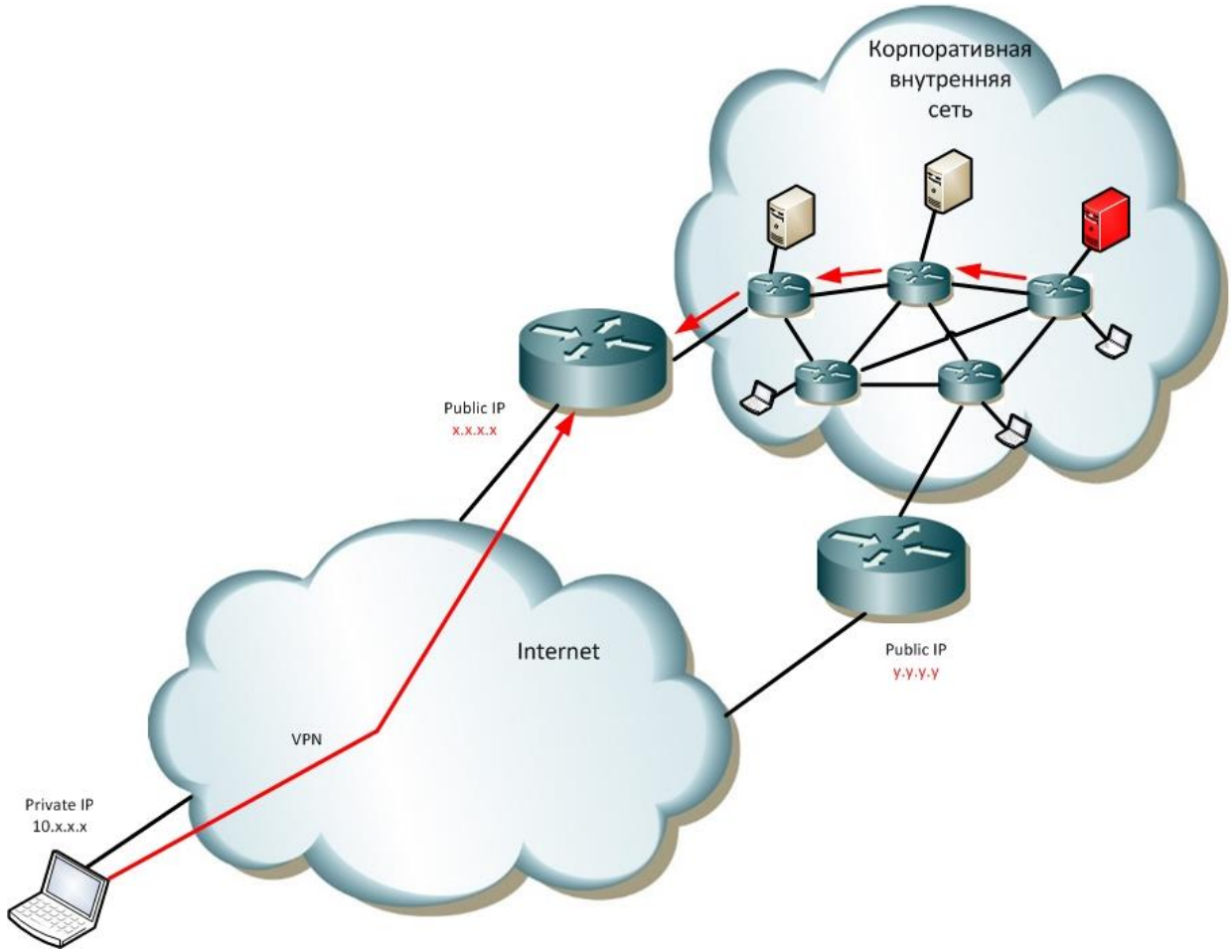


Отказоустойчивость VPN-сервера



MikroTik Courses

Отказоустойчивость VPN-сервера

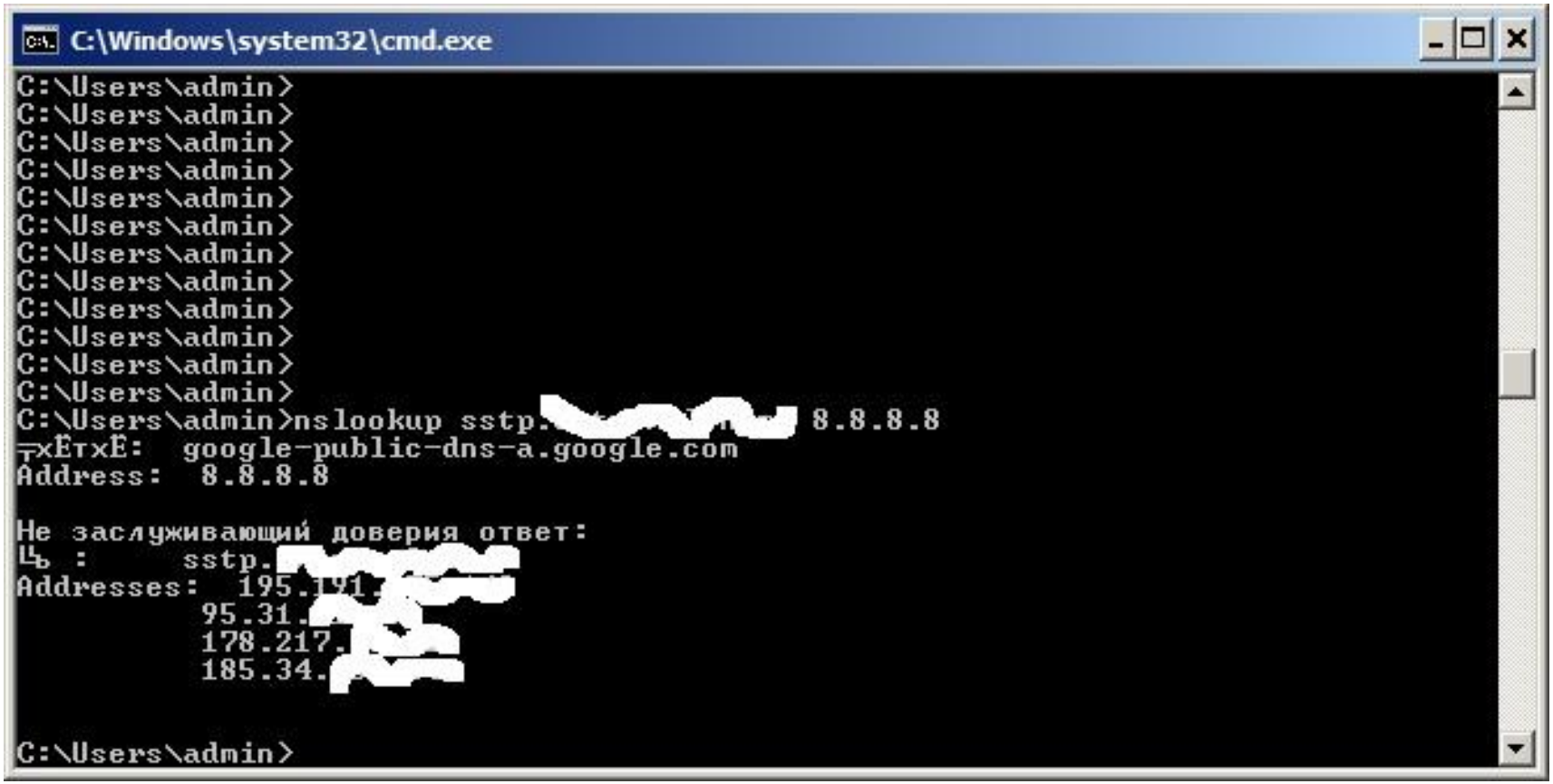


MikroTik Courses

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



Техника Apple?..

Техника Apple?..

Не, не слышал

Вопросы?

Пишите на

training@mikrotik-courses.ru

Хорошего дня!

Спасибо за ваше внимание!