Правильная настройка VPN для доступа к корпоративной сети

Доступ из windows без костылей

Almaty - 2018

MikroTik Courses

Обо мне

- ✓Руководитель ИТ-службы торговой компании
- ✓MikroTik certified engineer, consultant
- ✓MikroTik Trainer с 2015 года
- ✓Сертификаты: ccna, mtcna, mtcre, mtcwe, Eltex-коммутация, ФЗ-152, ubuquiti ubwa
- ✓Работаю с микротик с 2008

telegram: @Nick_The_First

Обо мне

Провожу учебные курсы в России и Казахстане с компанией «MikroTik-Courses»

MikroTik Courses

1671

Специалистов обучено

2549

Сертификатов выдано

82%

Средний балл

50

Городов посетили

Сеть 192.168.x.0/24

Не годится для корпоративной работы

Имеет пересечения с домашними сетями

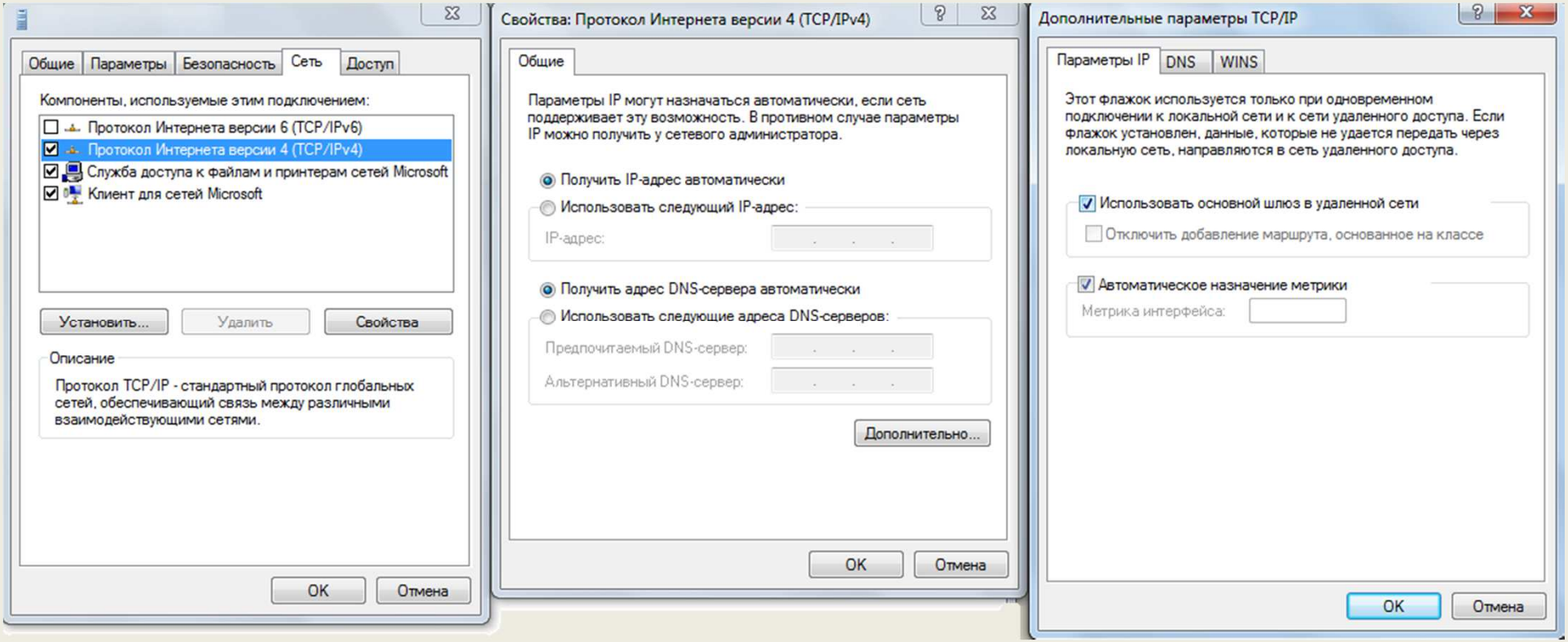
Содержит всего 254 адреса

Не дает удобно расширяться

Альтернатива: сети **172.16.0.0/12 и 10.0.0.0/8** для средних и больших предприятий. Имеют запас для роста.

Настройка клиента windows

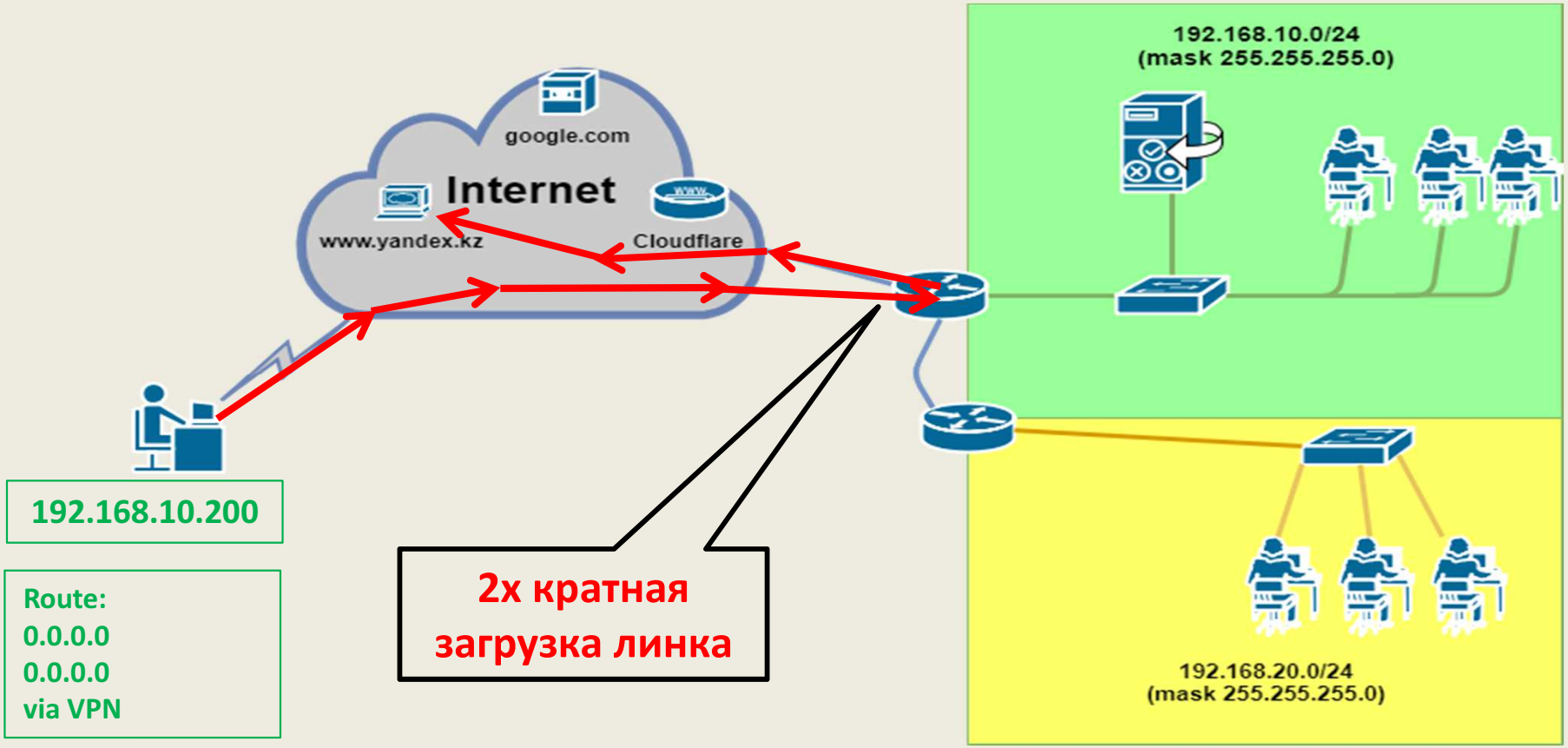
«Использовать основной шлюз в удаленной сети»



MikroTik Courses

Use Default Gateway

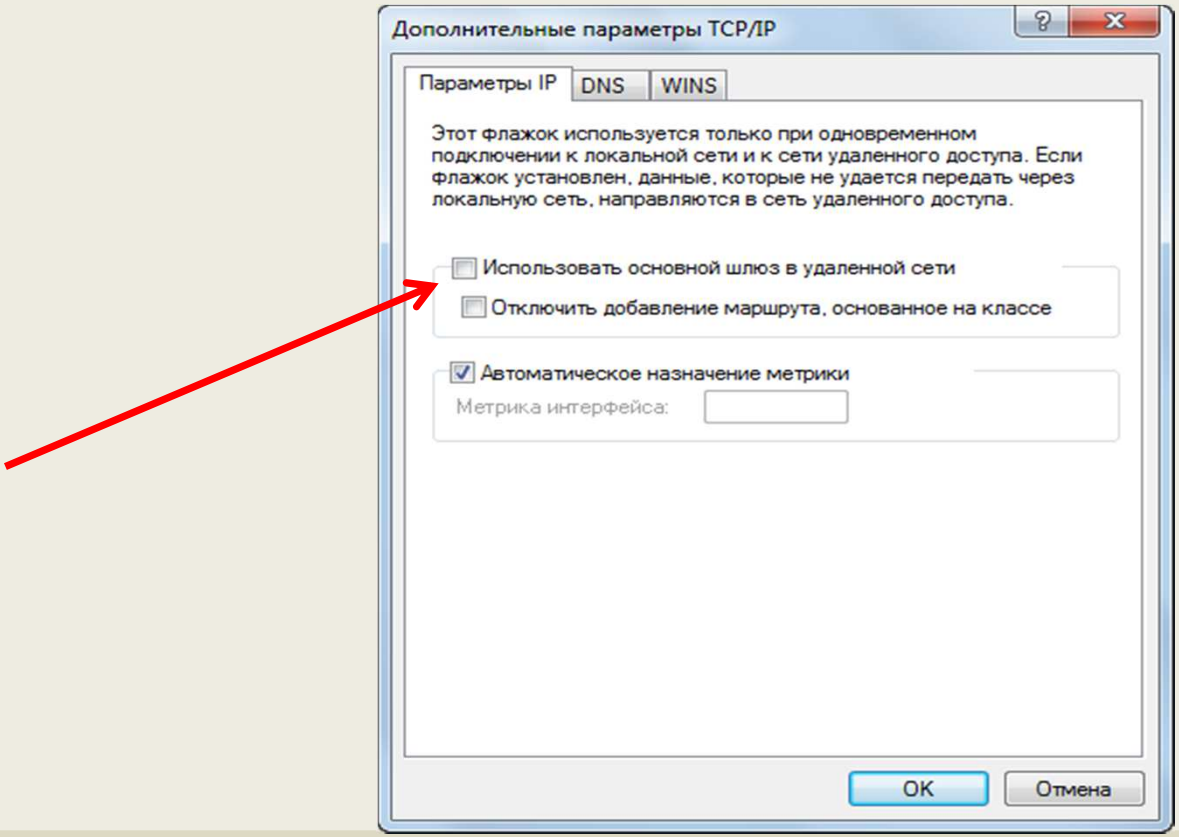
«Использовать основной шлюз в удаленной сети» отправляет **ВЕСЬ** трафик в туннель



MikroTik Courses

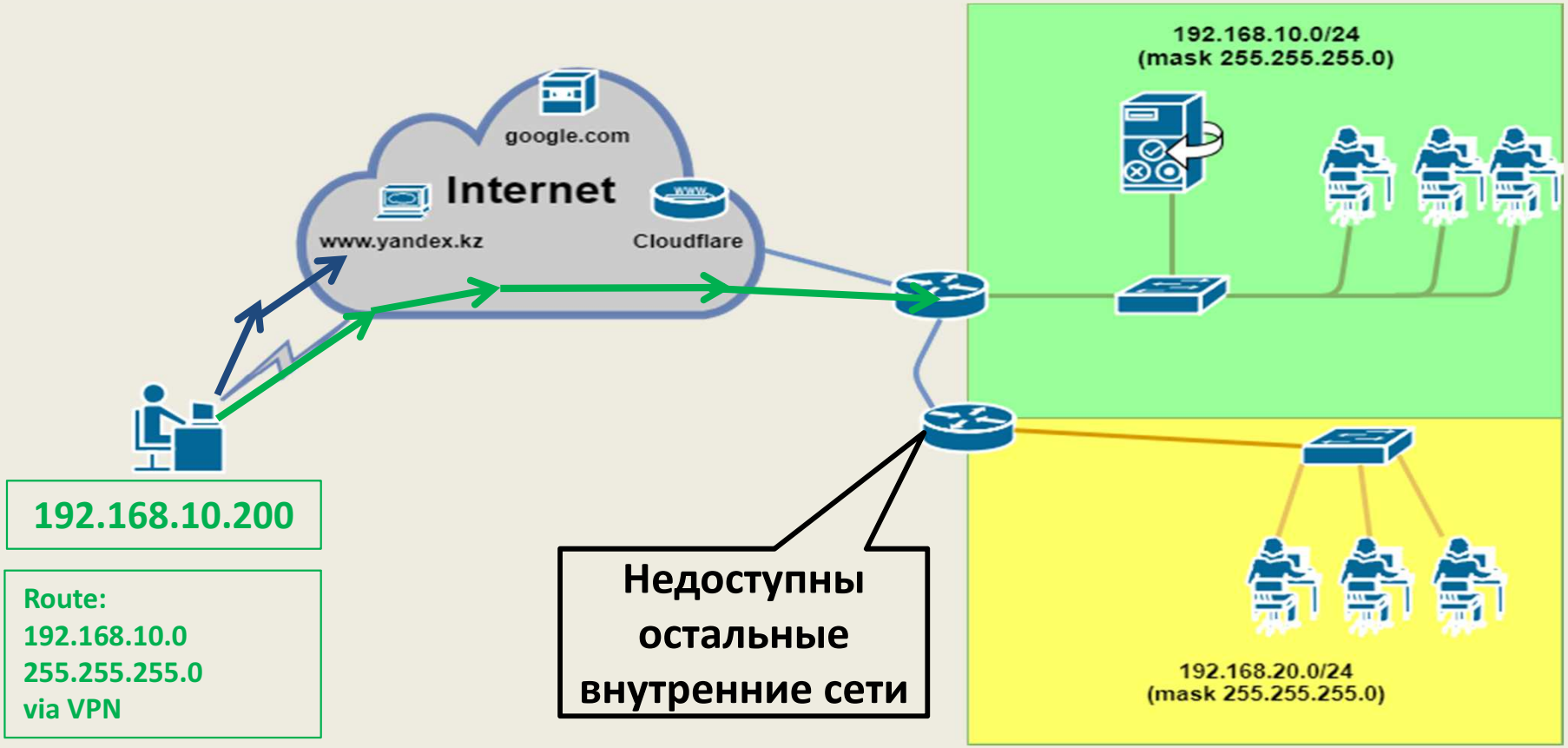
Отключаем удаленный шлюз

В туннель идёт трафик к подсети, к которой принадлежит адрес клиента



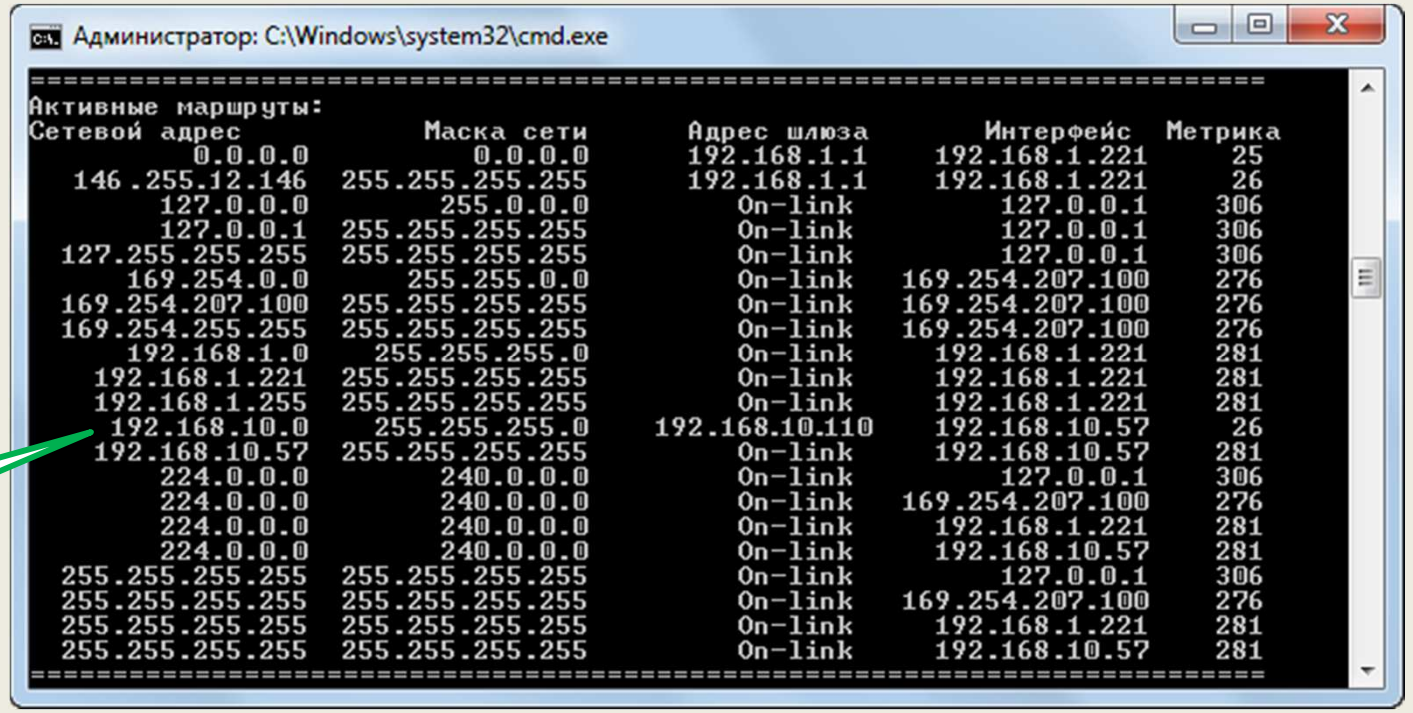
Выключен удаленный шлюз

В туннель идёт трафик к подсети, к которой принадлежит адрес клиента



Выключен удаленный шлюз

Строится один классовый маршрут, до одной подсети, которой принадлежит IP клиента



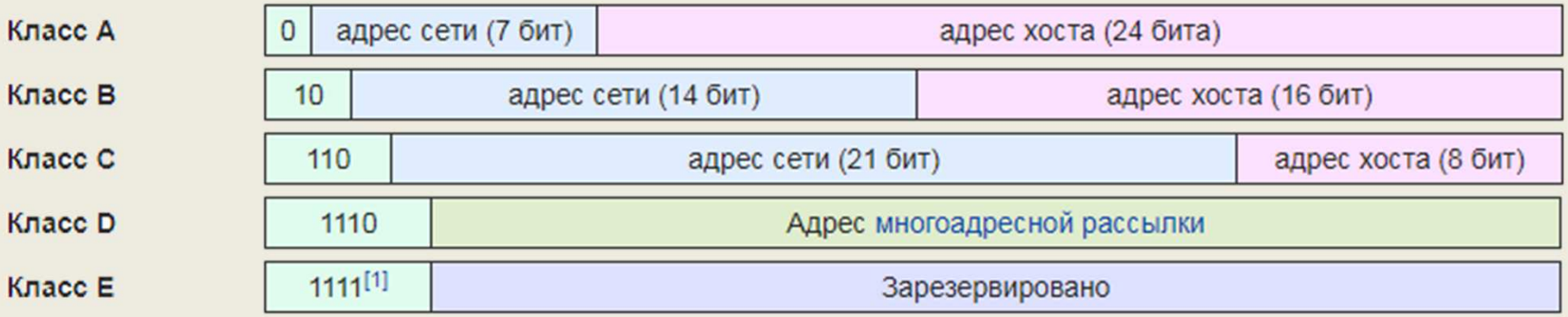
Маршрут в сеть 192.168.10.0/24 (mask 255.255.255.0)

Маршрута в 192.168.20.0/24 НЕТ. Остальной трафик идет на провайдера.

Что такое классовый маршрут

Каждая подсеть имеет параметр «Класс»

https://ru.wikipedia.org/wiki/Классовая_адресация



Чем выше класс, тем больше хостов или подсетей внутри.

Что такое классовый маршрут

Сколько подсетей /24 в каждом классе видит Windows

Класс сети	Пример адреса на клиенте	Маска маршрута windows VPN	Количество возможных подсетей /24
A	10.0.0.200	255.0.0.0	**65536** с 10.**0.0**.0 /24 по 10.**255.255**.0/24
B	172.16.0.200	255.255.0.0	**256** с 172.16.**0**.0 /24 по 172.16.**255**.0/24
C	192.168.10.200	255.255.255.0	**1** 192.168.10.0/24

Чем выше класс, тем больше хостов или подсетей внутри.

Что делать с доступом?

<u>Не использовать костыли:</u>

1. OVPN и Push Routes
2. Cmak
3. Скрипты .bat

В 99% случаев злоупортебление OpenVPN говорит о технической неграмотности админа и тупом копировании статей из Интернета.

Что делать с доступом?

Использовать:

1. Классовую маршрутизацию
2. Классовую маршрутизацию в сочетаниии в VLSM
3. Динамическую маршрутизацию RIP

Встроенные средства ОС, в большинстве случаев позволяют эффективно организовать доступ.
За вас давно всё придумали.

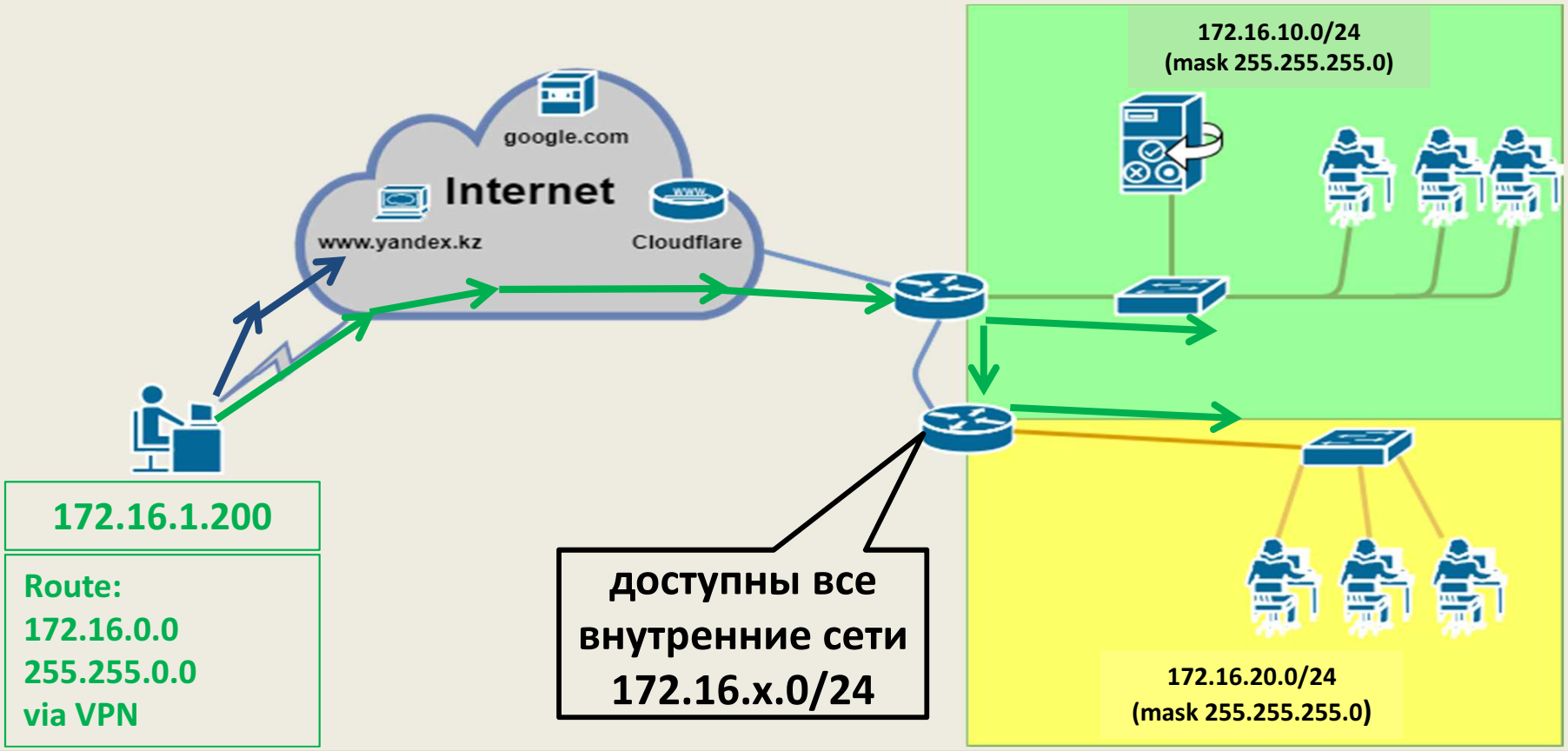
Классовая маршрутизация в VPN

Переводим адресацию сетей на диапазон **172.16.0.0/16** (mask 255.255.0.0). Получается сеть класса “B”. Внутри нее планируем подсети:

1. 172.16.1.0/24 (mask 255.255.255.0) – клиенты VPN
2. 172.16.10.0/24 (mask 255.255.255.0) – головной офис
3. 172.16.20.0/24 (mask 255.255.255.0) – сеть филиала
4. … и еще 253 подсети по /24 свободны

Классовая маршрутизация в VPN

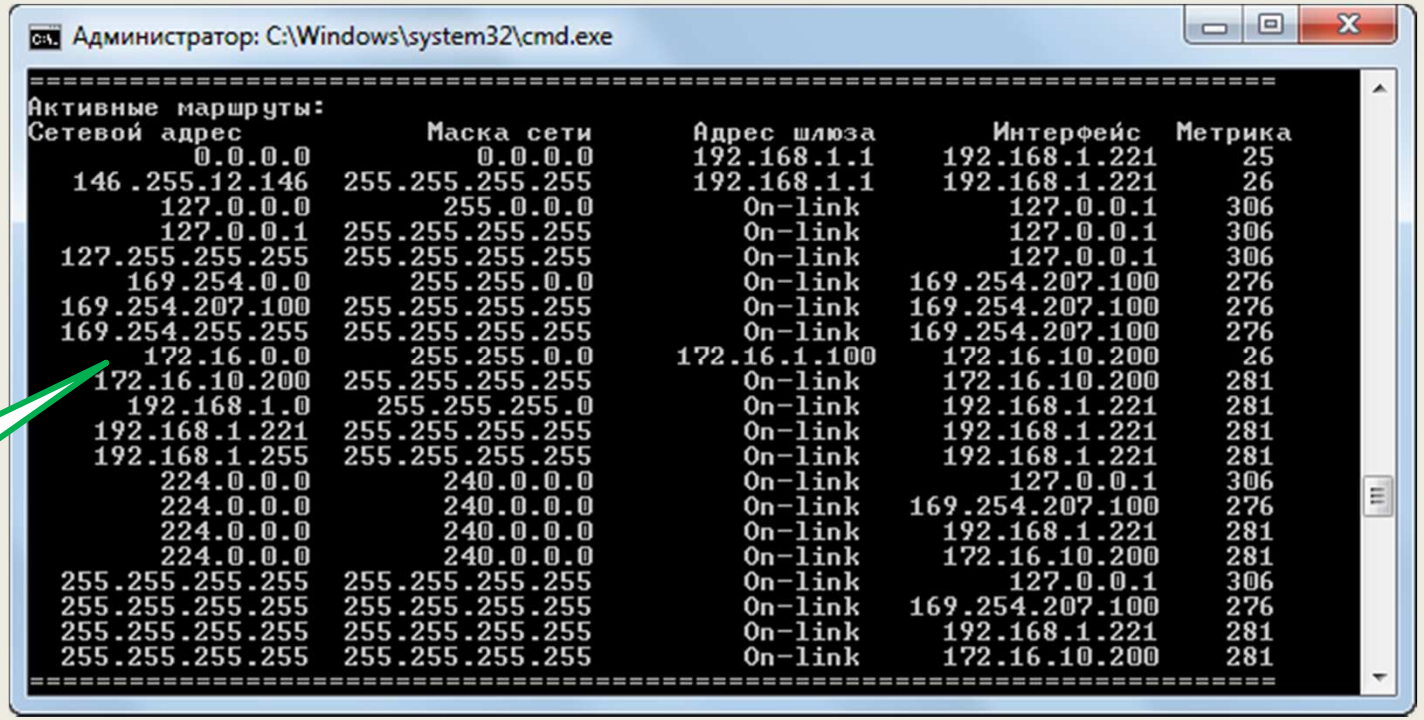
Объединяющая сеть предприятия
172.16.0.0/16 (mask 255.255.0.0)



MikroTik Courses

Классовая маршрутизация в VPN

Строится один классовый маршрут, до одной подсети, которой принадлежит IP клиента



Маршрут в сеть 172.16.0.0/16 (mask 255.255.0.0)

Маршрут в объединяющую сеть. Остальной трафик идет на провайдера.

Если сеть небольшая

А) Её проще перевести на адреса классом выше
172.16.0.0/16 (mask 255.255.0.0)

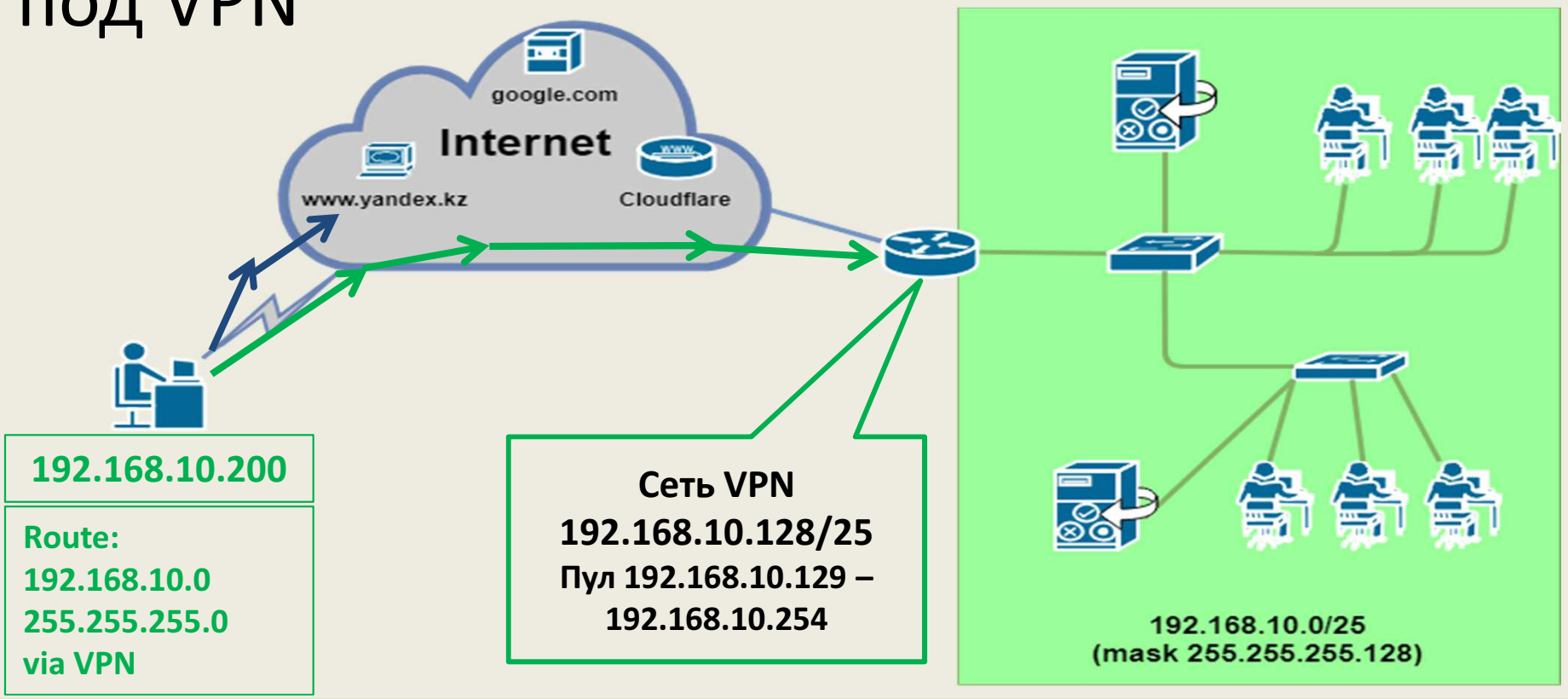
Б) Либо поделить на подсети с использованием VLSM

1. 192.168.10.0/25 (mask 255.255.255.128) – сеть офиса
2. 192.168.10.128/25 (mask 255.255.255.128) – клиенты VPN

Это позволяет отказаться от режима «Proxy-Arp»!

Если сеть небольшая –VLSM

До 125 узлов офиса объединяются в малую подсеть /25, оставляя адреса .129-.254 под VPN



Использование RIP

Это тема отдельной статьи и отдельного доклада.

Об использовании протокола RIP при подключении VPN-клиентов Windows рассказал Алексей Чудин в докладе на Московской конференции MUM – 2018 «VPN с компьютера в корпоративную сеть»

https://mum.mikrotik.com/2018/RUM/agenda/EN

Спасибо за внимание!

Приходите к нам на курсы
изучать MikroTik ☺

Наш сайт: www.mikrotik-courses.ru
Почта: manager@mikrotik-courses.ru