



Онлайн-образование

Не забыть включить запись!





Меня хорошо видно && слышно?

Ставьте , если все хорошо
Напишите в чат, если есть проблемы

Правила вебинара



Активно участвуем



Задаем вопрос в чат или голосом



Off-topic обсуждаем в Slack #канал группы или #general



Вопросы вижу в чате, могу ответить не сразу



Мосты, туннели и VPN

Викирюк Павел

Системный инженер

Цели занятия | После занятия вы сможете

1 Понимать необходимость применения bridge-интерфейсов

2 Настроить bridge-интерфейс в Linux

3 Понимать принципы работы VPN

Цели занятия | После занятия вы сможете

4 Различать типы VPN-соединений

5 Понять как работает OpenVPN

6 Настроить свой OpenVPN-сервер

СМЫСЛ | Зачем вам это уметь

- 1 Чтобы уметь масштабировать и объединять сети на разных уровнях
- 2 Чтобы применять шифрование трафика при объединении сетей
- 3 Чтобы сделать правильный выбор технологии для решения рабочих задач

Маршрут вебинара

Bridge-интерфейсы



Туннели



OpenVPN



WireGuard



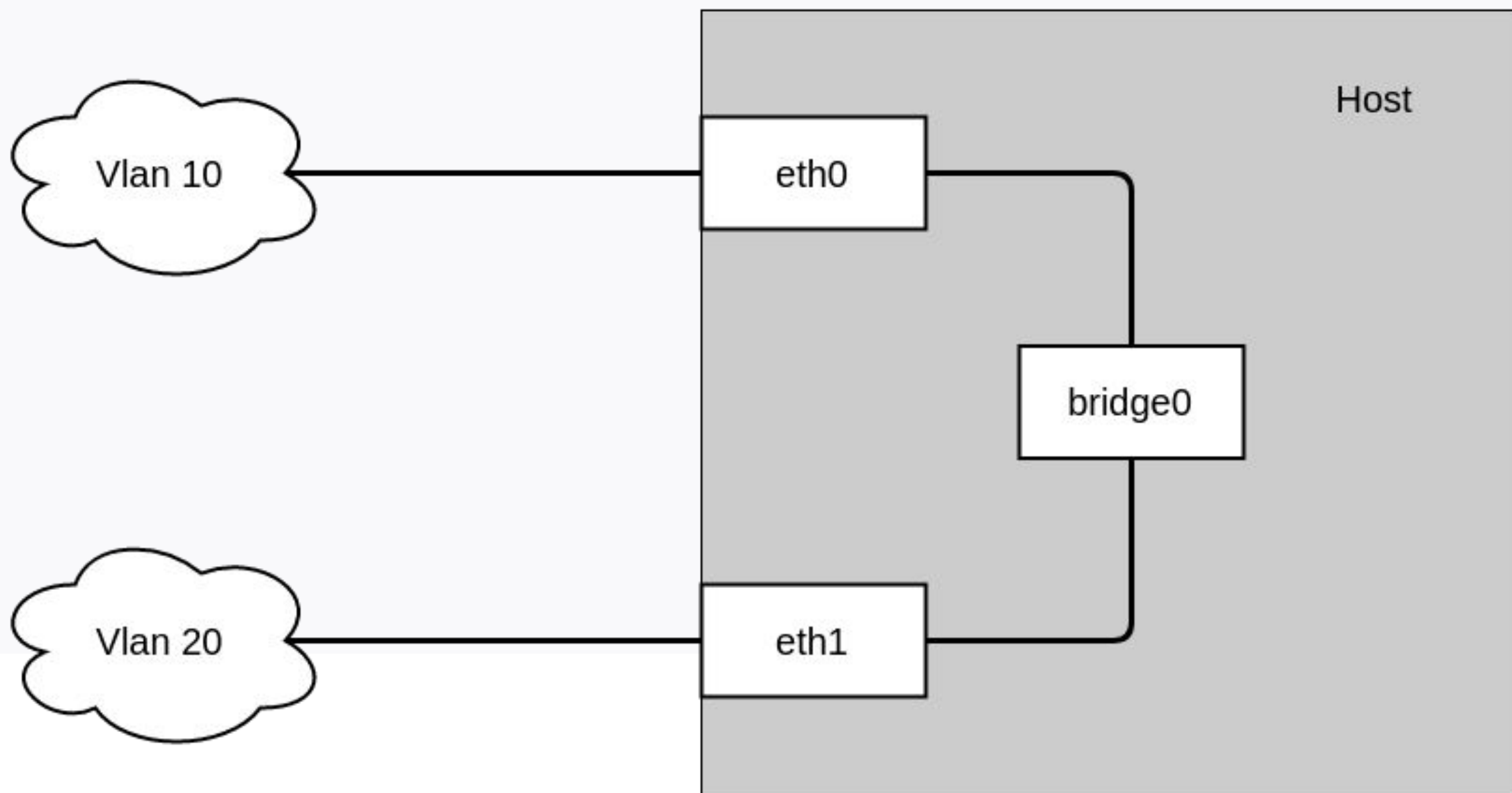
Bridge-интерфейс в Linux



Вопрос к аудитории:
Что такое bridge-интерфейс и
зачем он нужен?

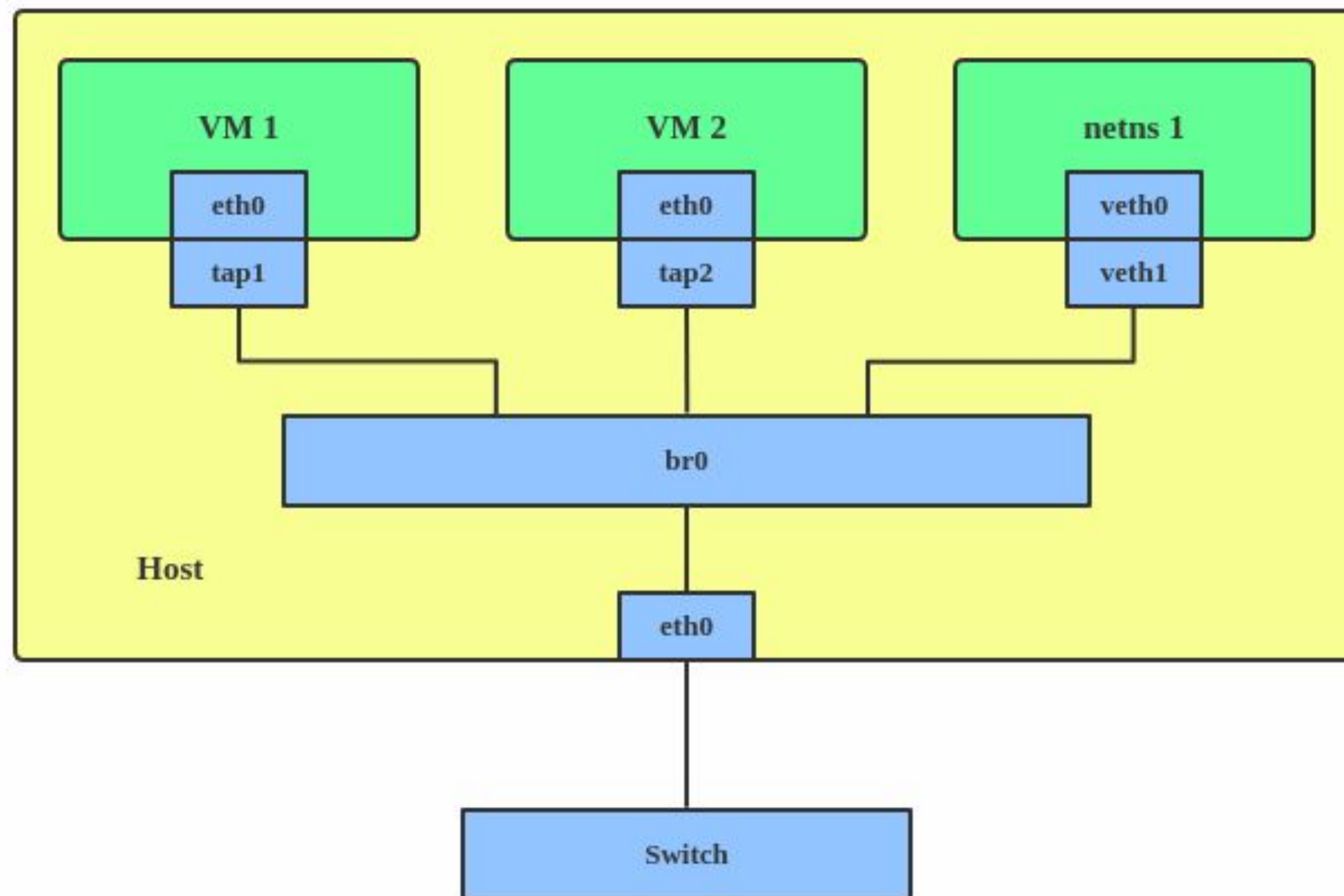
Bridge-интерфейс

Назначение bridge-интерфейса: способ объединения сегментов сети на канальном уровне модели OSI (т.е. L2) без использования протоколов более высокого уровня



Bridge-интерфейс

Назначение bridge-интерфейса: способ объединения сегментов сети на канальном уровне модели OSI (т.е. L2) без использования протоколов более высокого уровня



Bridge-интерфейс

Особенности:

- пакеты передаются на основе MAC, а не IP адресов
- настройка: утилиты `iproute2` (`ip link`) или `brctl` (`bridge-utils`)
- можно объединить: L2-интерфейсы (`eth`, `tap`, `wi-fi`)
- можно объединить до 1024 интерфейсов
- нельзя объединить: L3-интерфейсы (`tun`, `ppp`)

Важно!

- избегать создания петель с помощью bridge-интерфейсов
- использовать протокол STP

Bridge-интерфейс: настройка

Настройка с помощью утилит `iproute2`:

`ip link add name bridge0 type bridge` - создаем бридж-интерфейс `bridge0`

`ip link set bridge0 up` - включаем интерфейс `bridge0`

`ip link set eth0 up` - включаем интерфейс `eth0`

`ip link set eth0 master bridge0` - добавляем интерфейсу `eth0` мастер-интерфейс `bridge0` (то есть добавляем `eth0` в бридж)

`bridge link` - покажет информацию по бриджам

`ip link set eth0 nomaster` - удаляет `eth0` из бриджа (удаляет мастер-интерфейс)

`ip link set eth0 down` - выключаем интерфейс `eth0`

`ip link delete bridge0 type bridge` - удаляем бридж `bridge0`

Bridge-интерфейс: настройка

Настройка с помощью утилит **bridge-utils**:

`brctl addbr bridge0` - создаем интерфейс bridge0

`brctl addif bridge0 eth0` - добавляем интерфейс eth0 в бридж bridge0

`ip link set up dev bridge0` - включить интерфейс bridge0

`brctl show` - смотрим информацию по бриджам

`ip link set down dev bridge0` - выключить интерфейс bridge0

`brctl delif bridge0 eth0` - удалить интерфейс eth0 и бриджа bridge0

`brctl delbr bridge0` - удалить интерфейс bridge0

Bridge-интерфейс: настройка

Примеры конфигов в Centos:

```
cat /etc/sysconfig/network-scripts/ifcfg-bridge0  
DEVICE="bridge0"  
BOOTPROTO="static"  
ONBOOT="yes"  
TYPE="Bridge"  
IPADDR="172.16.0.2"  
NETMASK="255.255.255.0"  
GATEWAY="172.16.0.1"
```

```
cat /etc/sysconfig/network-scripts/ifcfg-eth0  
DEVICE="eth0"  
BOOTPROTO="none"  
ONBOOT="yes"  
TYPE="Ethernet"  
BRIDGE="bridge0"
```

```
cat /etc/sysconfig/network-scripts/ifcfg-eth1  
DEVICE="eth1"  
BOOTPROTO="none"  
ONBOOT="yes"  
TYPE="Ethernet"  
BRIDGE="bridge0"
```

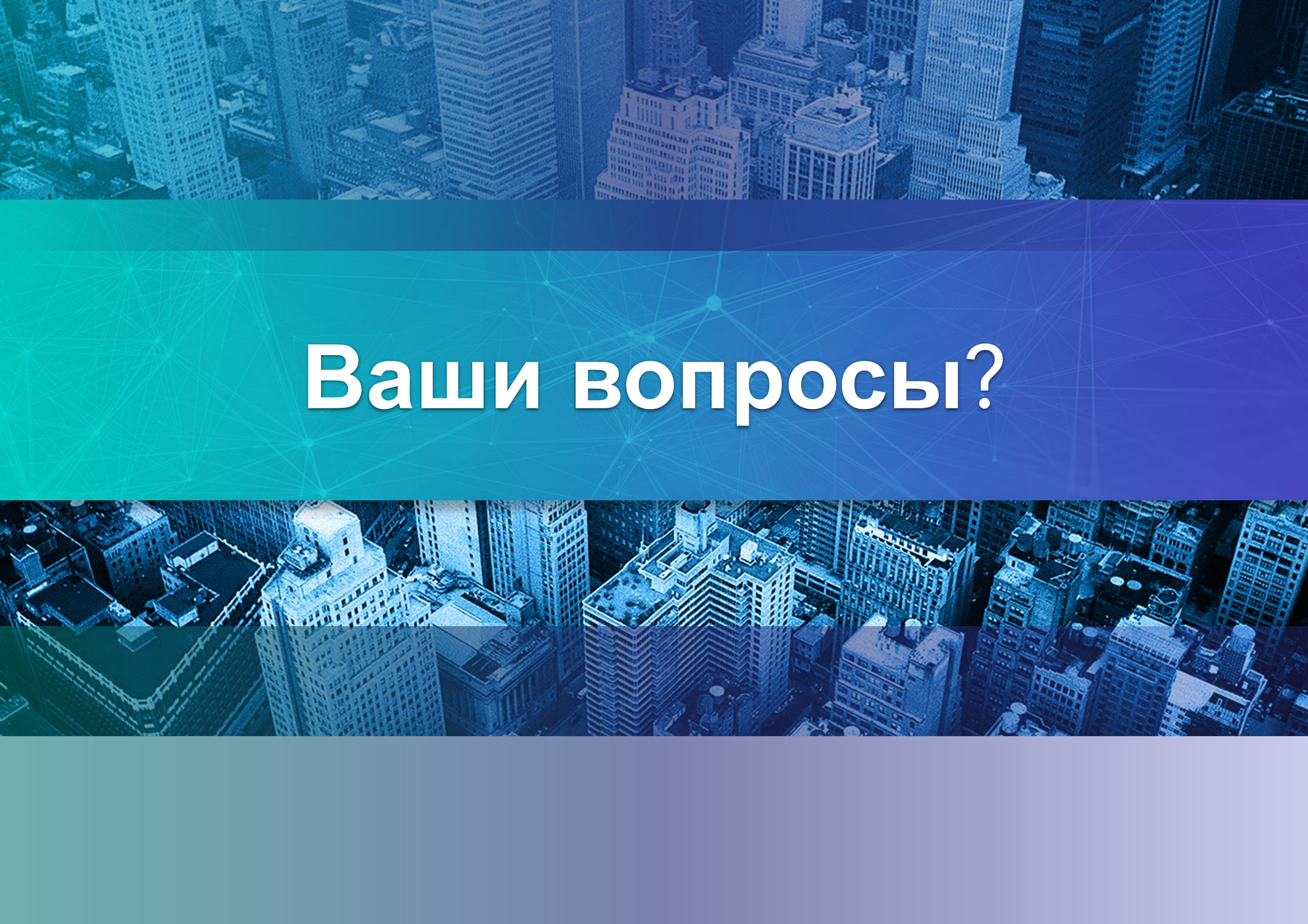

Bridge-интерфейс: настройка

Примеры конфигов в Ubuntu (Debian):

```
auto lo  
iface lo inet loopback
```

```
auto eth0  
auto eth1  
auto bridge1
```

```
iface bridge1 inet static  
    bridge_ports eth0 eth1  
    address 192.168.0.5  
    netmask 255.255.255.255
```

Ваши вопросы?

Маршрут вебинара

Bridge-интерфейсы



Туннели




OpenVPN



WireGuard



Туннели



Вопрос к аудитории:
**Что такое туннели и зачем они
нужны?**

The background of the slide is a composite image. The top half features a blue-tinted aerial view of a city skyline, with a network of white lines and dots overlaid, suggesting a digital or technological theme. The bottom half shows a similar aerial view of a city, but with a more pronounced blue overlay and a network pattern. The text "VPN технологии" is prominently displayed in the center, overlaid on the network pattern.

VPN технологии

VPN в интернете

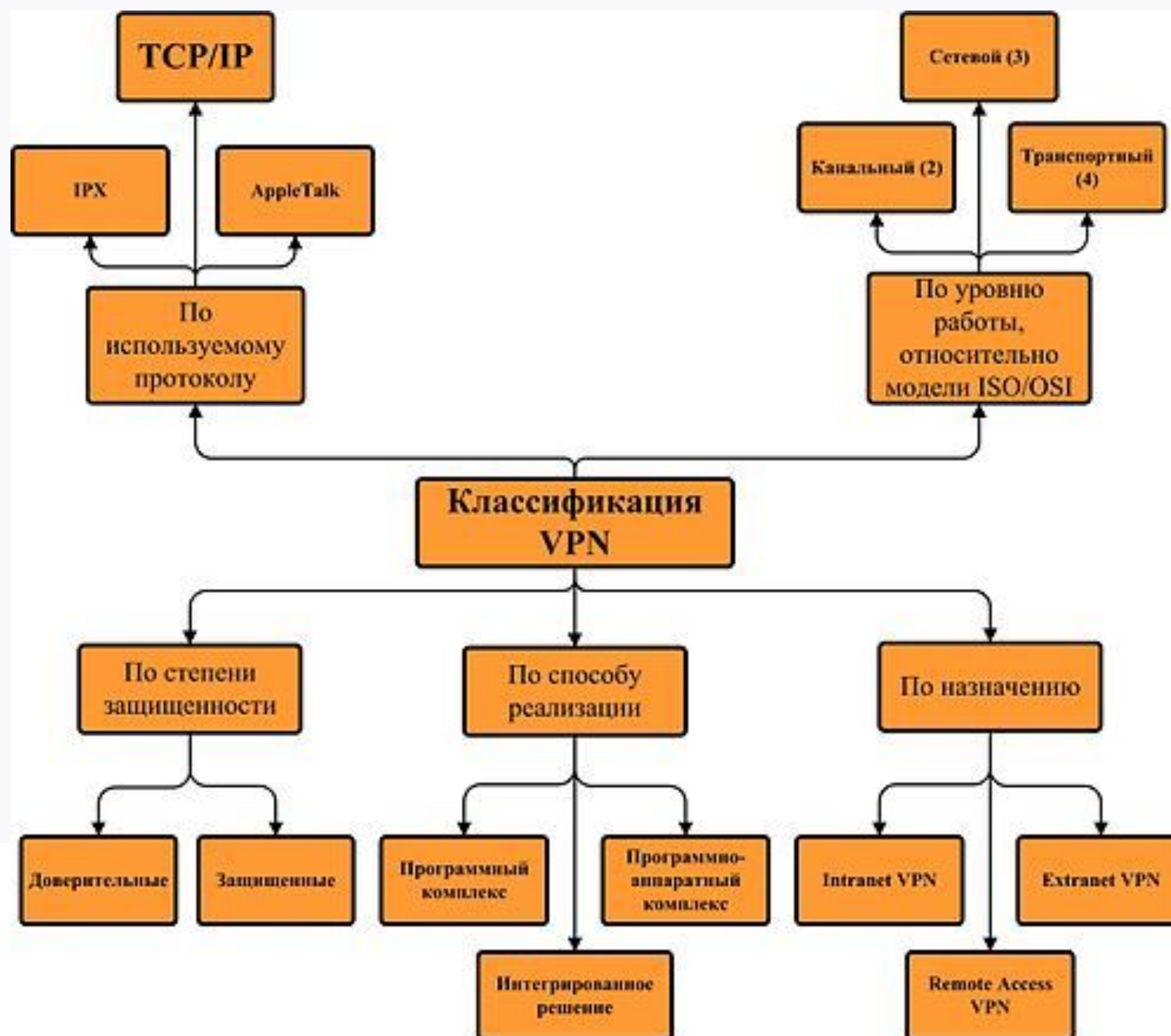


VPN: определение и особенности

VPN - Virtual Private Network (англ. виртуальные частные сети) - обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например Интернет) (<https://ru.wikipedia.org/wiki/VPN>)

- формируют логические связи независимо от физической среды
- позволяют обойтись без выделенных каналов
- позволяют защитить инфраструктуру

VPN: классификация





Вопрос:

**Про VPN понятно, так а что же
такое туннели?**

Туннели

Туннелирование - процесс, в ходе которого создаётся логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов
[https://ru.wikipedia.org/wiki/Туннелирование_\(компьютерные_сети\)](https://ru.wikipedia.org/wiki/Туннелирование_(компьютерные_сети))

Туннель - результат этого процесса

Особенности:

- используют **инкапсуляцию** протоколов
- протоколы, реализующие туннелирование могут работать на L4 и L7

Принцип:

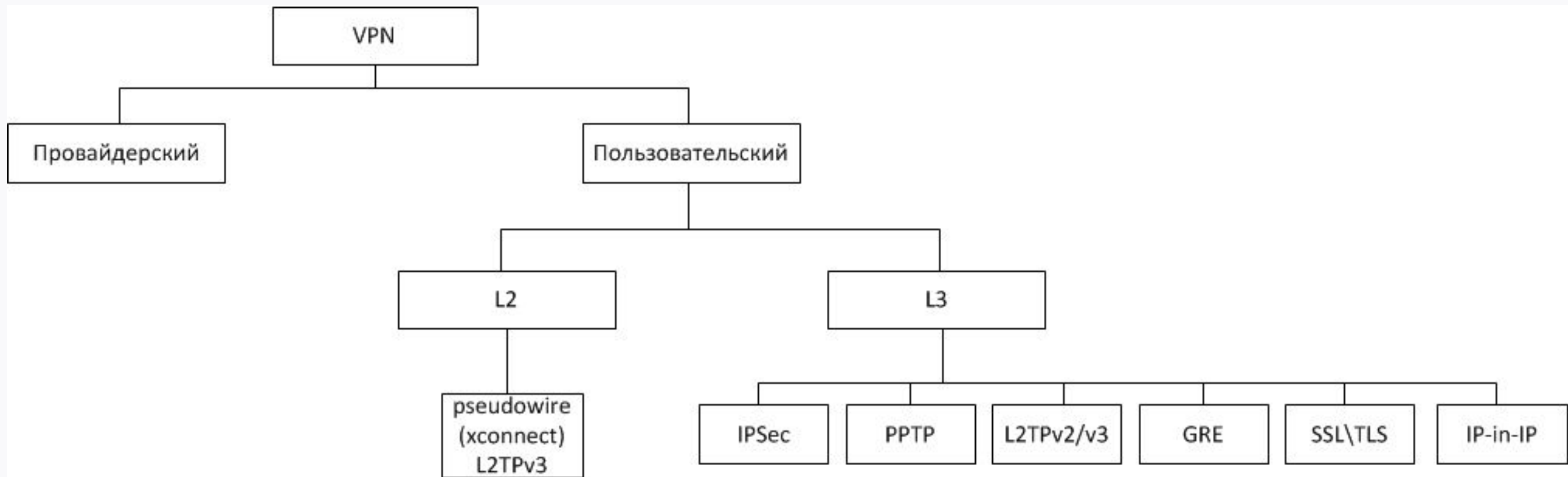
для создания туннелей применяются виртуальные интерфейсы, драйверы которых упаковывают (инкапсулируют) принятые данные в IP-пакет и отправляют снова на маршрутизацию, а также в обратном порядке



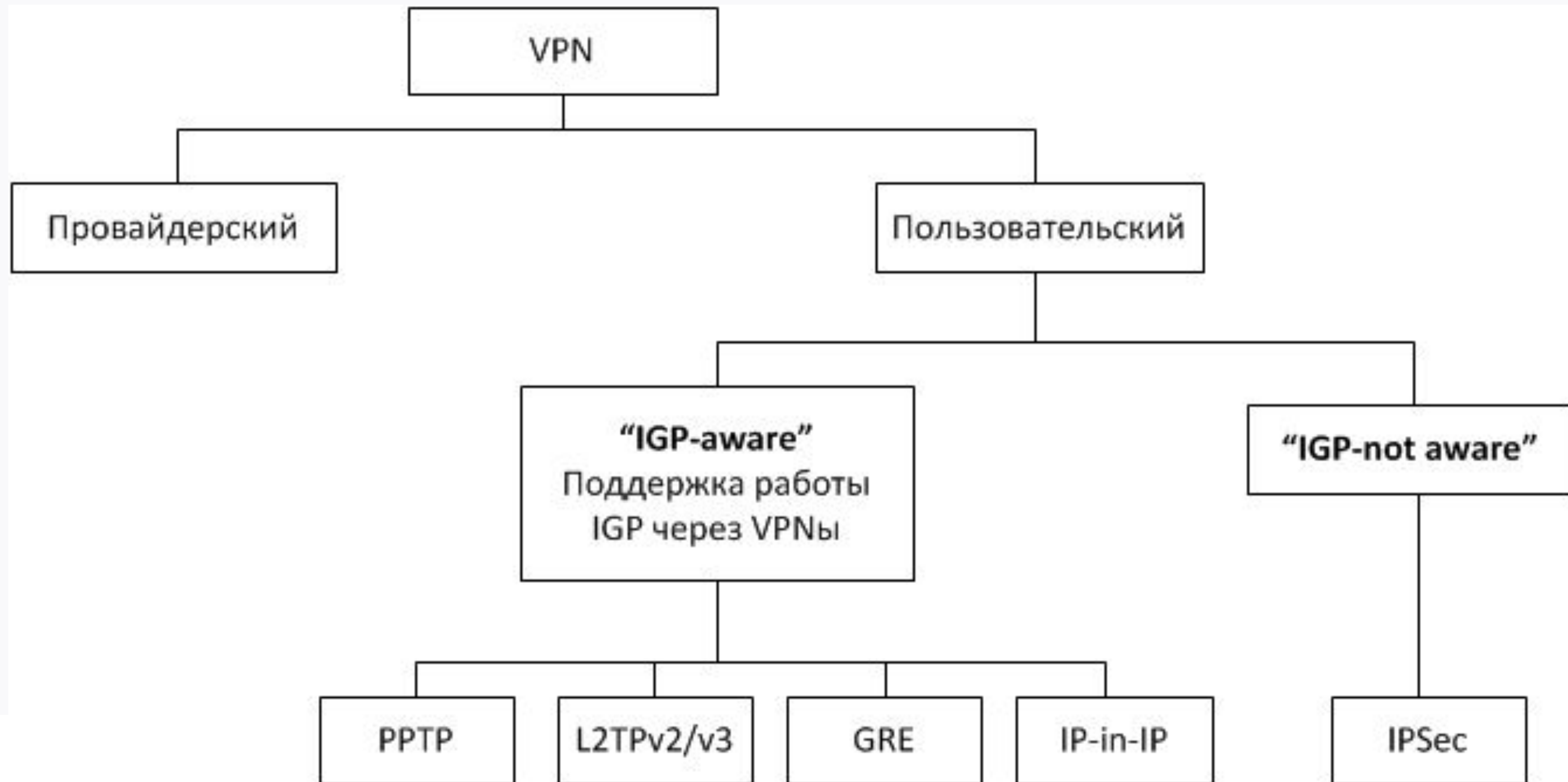
Вопрос к аудитории:

Какие типы туннелей вы знаете?

Типы VPN-соединений



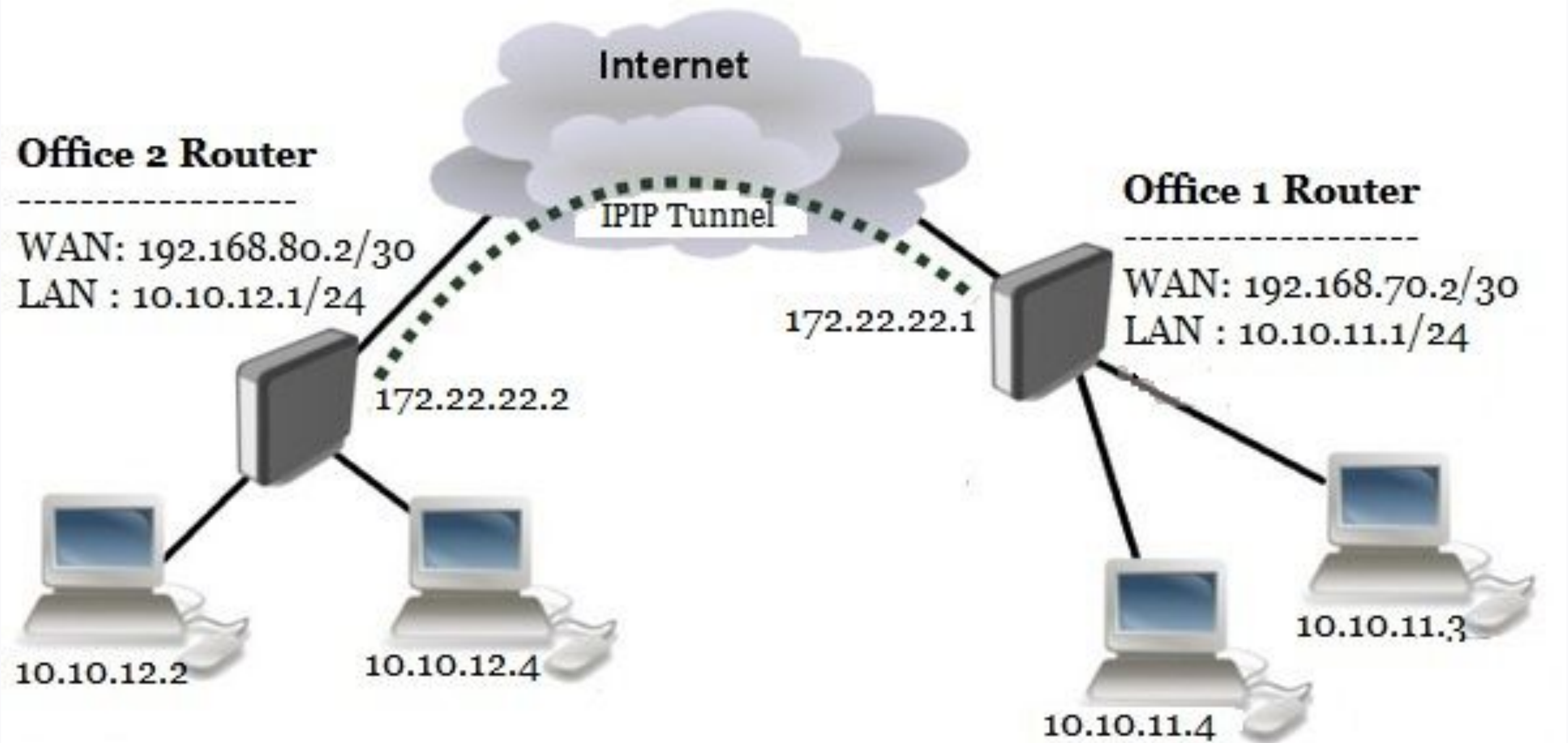
Типы VPN-соединений





IPIP

IPIP туннель



IPsec туннель

Особенности:

- инкапсулирует только unicast IPv4-трафик
- для работы требует внешние IP-адреса
- не имеет механизмов для работы через NAT
- так как не пропускает multicast - мешает работе VRRP и OSPF
- реализован в Linux и на оборудовании некоторых вендоров (Cisco, Mikrotik)
- не имеет собственных механизмов шифрования
- не требователен к ресурсам оборудования

IPIP туннель

Пример создания IPIP туннеля в Linux:

1. Создаем IPIP-туннельный интерфейс:

```
ip tunnel add tun0 mode ipip remote 200.200.200.200 local  
100.100.100.100 dev eth0
```

2. Добавляем IP-адрес на туннельный интерфейс:

```
ip address add 10.0.0.1 netmask 255.255.255.252 dev tun0
```

3. Устанавливаем MTU и поднимаем интерфейс:

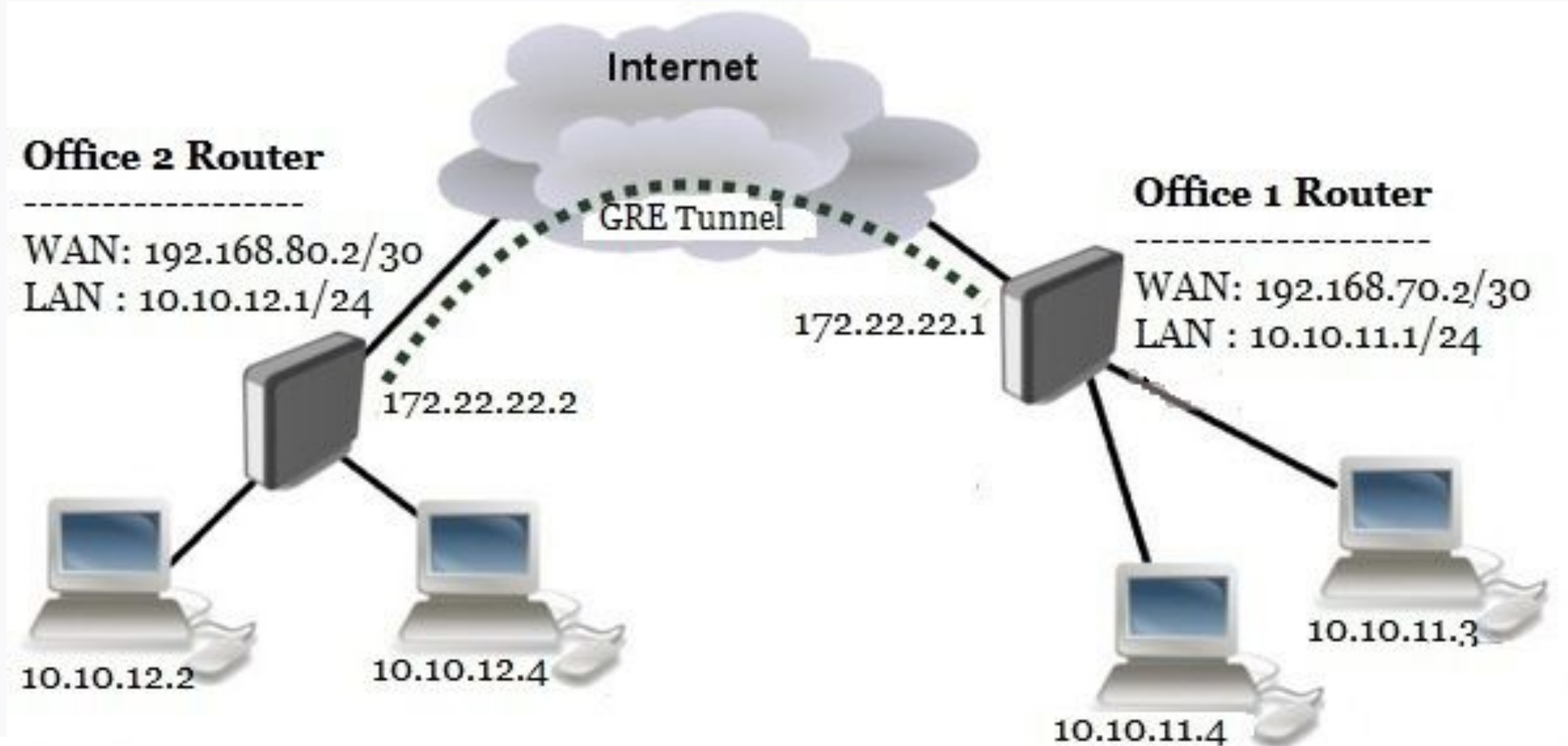
```
ifconfig tun0 mtu 1492 up
```




GRE



IP туннель



GRE туннель

Generic Routing Encapsulation — общая инкапсуляция маршрутов

Особенности:

- инкапсулирует практически любой IPv4-трафик (в том числе multicast)
- для работы требует внешние IP-адреса
- не имеет механизмов для работы через NAT
- реализован в Linux и на оборудовании **многих** вендоров
- не имеет собственных механизмов шифрования
- не требователен к ресурсам оборудования (работает в ядре)

GRE туннель

Пример создания IP/IP туннеля в Linux:

1. Загружаем модуль ядра:

```
modprobe ip_gre
```

2. Создаем GRE-интерфейс:

```
ip tunnel add tun0 mode gre remote 200.200.200.200 local  
100.100.100.100 dev eth0
```

3. Добавляем IP-адрес на туннельный интерфейс:

```
ip address add 10.0.0.1/30 dev tun0
```

4. Устанавливаем MTU и поднимаем интерфейс:

```
ifconfig tun0 mtu 1492 up
```

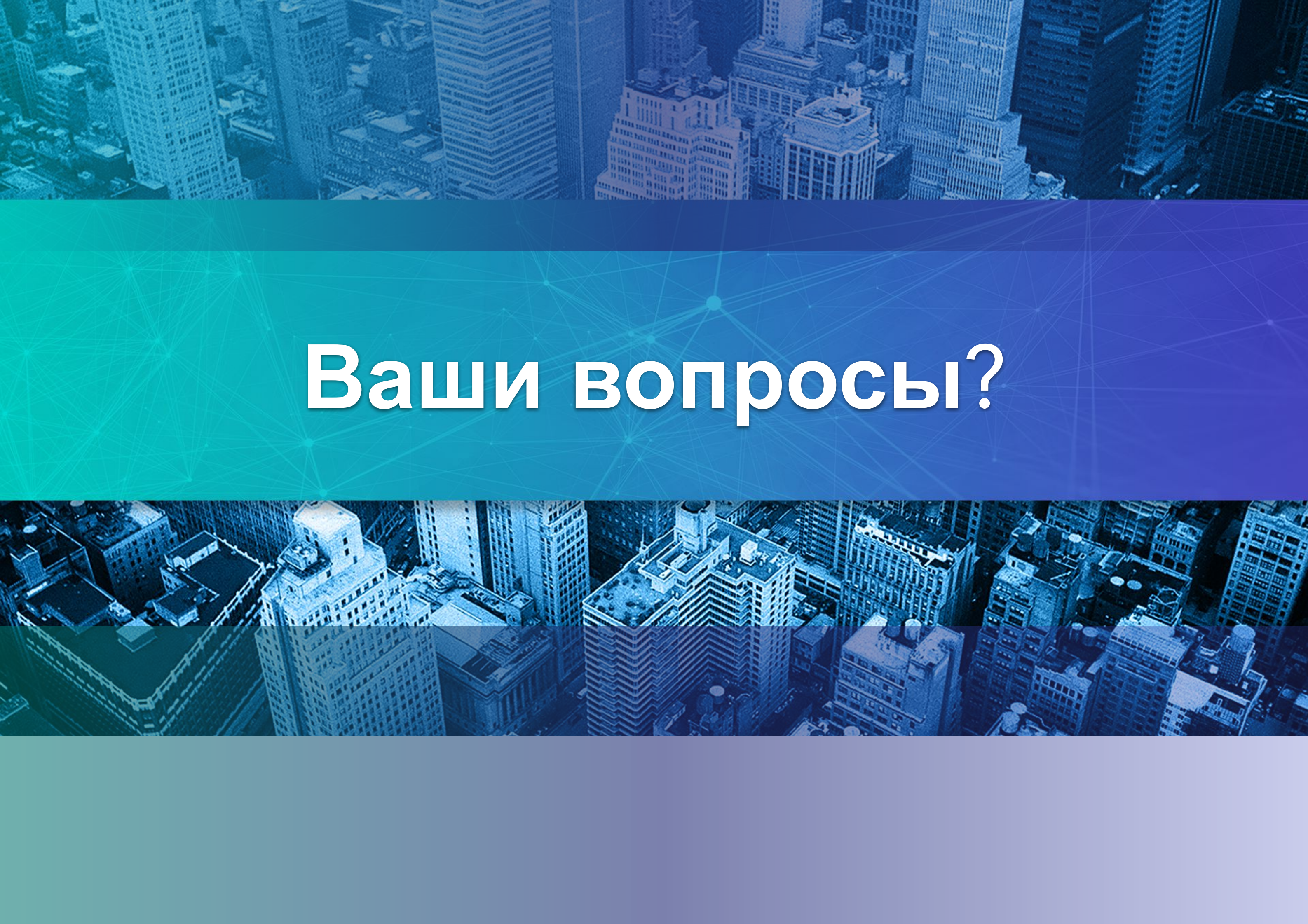



Недостатки Point to Point туннелей

Недостатки Point to Point туннелей

Недостатки:

- безопасность (решается применением например **IPsec**)
- сложность масштабирования
- ограничения в построении сложных топологий
- отсутствие отказоустойчивости (stateless или connectionless)



Ваши вопросы?

The background of the slide is a composite image. The top half features a teal-to-blue gradient with a white network diagram consisting of interconnected nodes and lines. The bottom half shows an aerial view of a dense city skyline, likely New York City, with numerous skyscrapers. The text 'IPsec' is overlaid on the left side of the network diagram.

IPsec



Вопрос к аудитории:

Что такое IPsec?

IPsec

IPsec (сокращение от **IP Security**) — набор протоколов для обеспечения защиты данных

<https://ru.wikipedia.org/wiki/IPsec>

Особенности:

- отсутствие виртуальных интерфейсов (если используется только IPsec в чистом виде)
- маршрутизация осуществляется с помощью ACL и Crypto map
- допускает применение протоколов динамической маршрутизации

Реализации в Linux:

- iproute2
- strongSwan: <https://www.strongswan.org>
- softether: <https://www.softether.org>

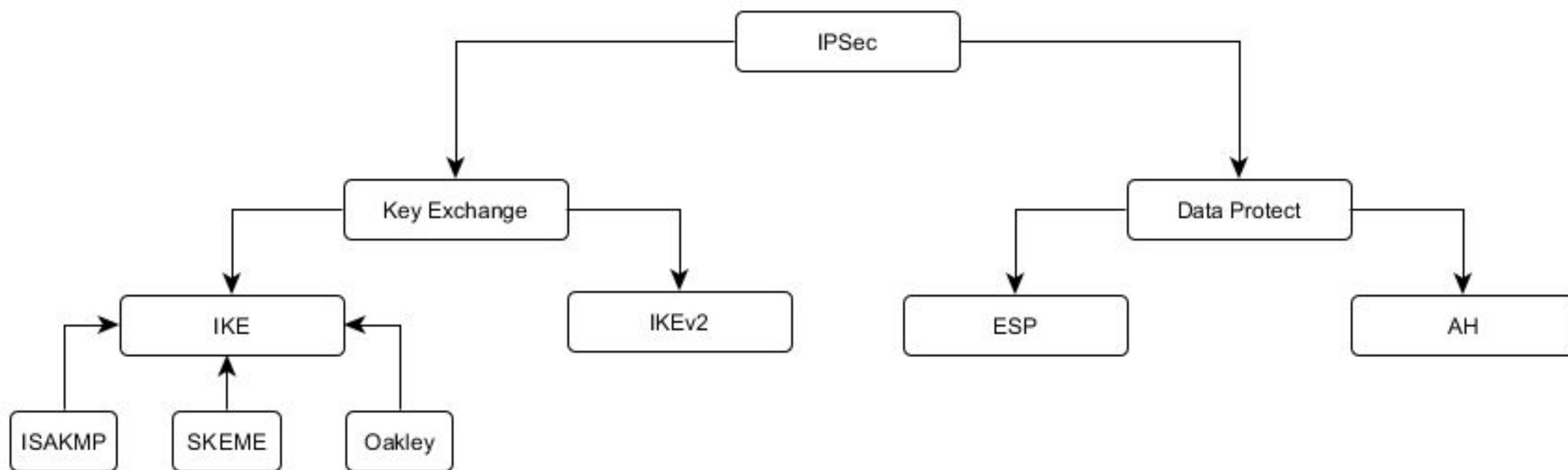
Преимущества:

- работает на сетевом уровне модели OSI
- может шифровать исходный пакет целиком либо от транспортного уровня и выше
- присутствует механизм преодоления NAT
- большой набор алгоритмов шифрования и хэширования трафика, на выбор

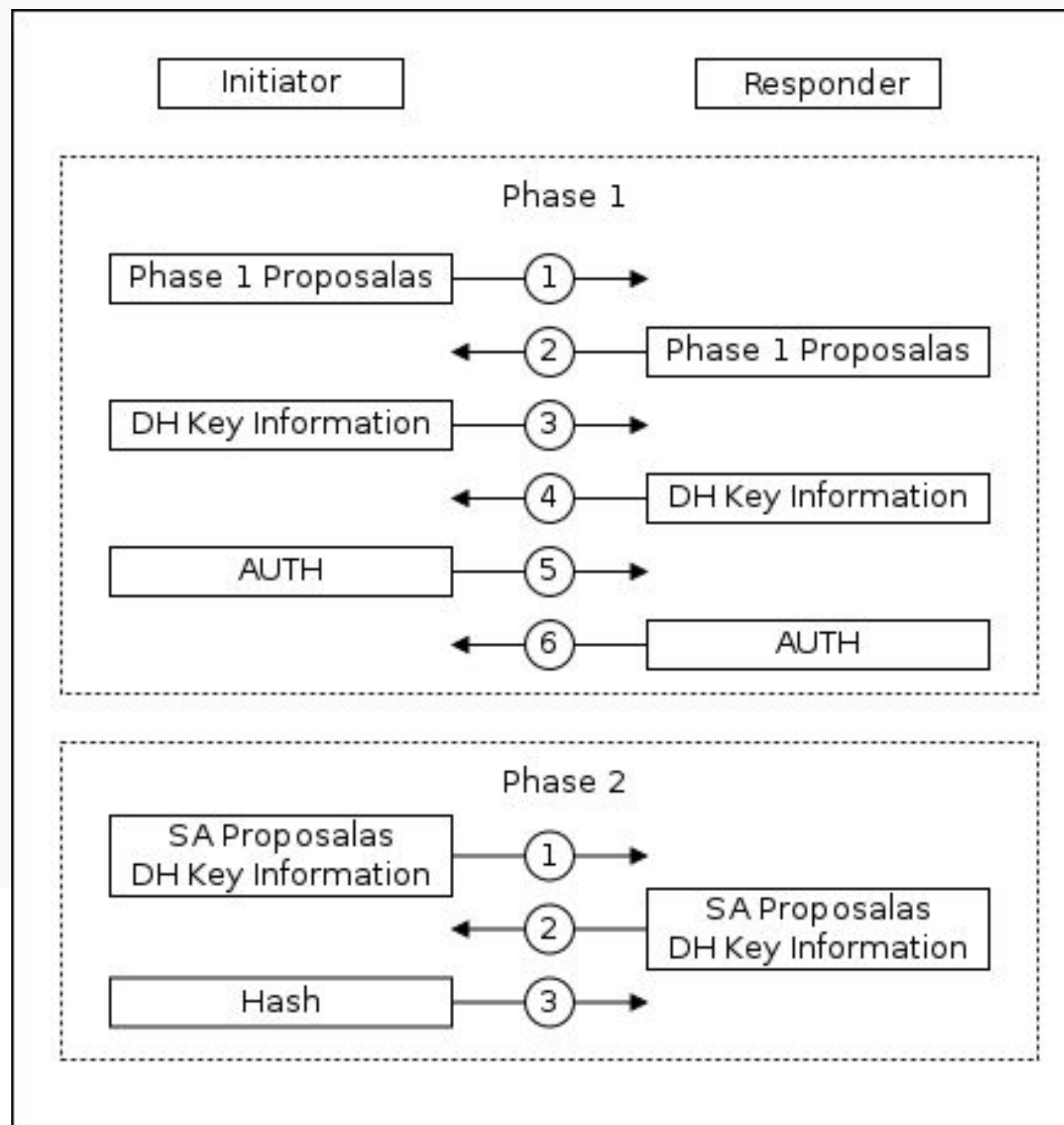
Недостатки:

- сложность
- различная терминология и инструменты конфигурации у различных вендоров
- использование сильных алгоритмов шифрования требует ресурсов
- легко обнаруживается DPI

Протоколы в составе IPSec



Примерный порядок установки соединения:



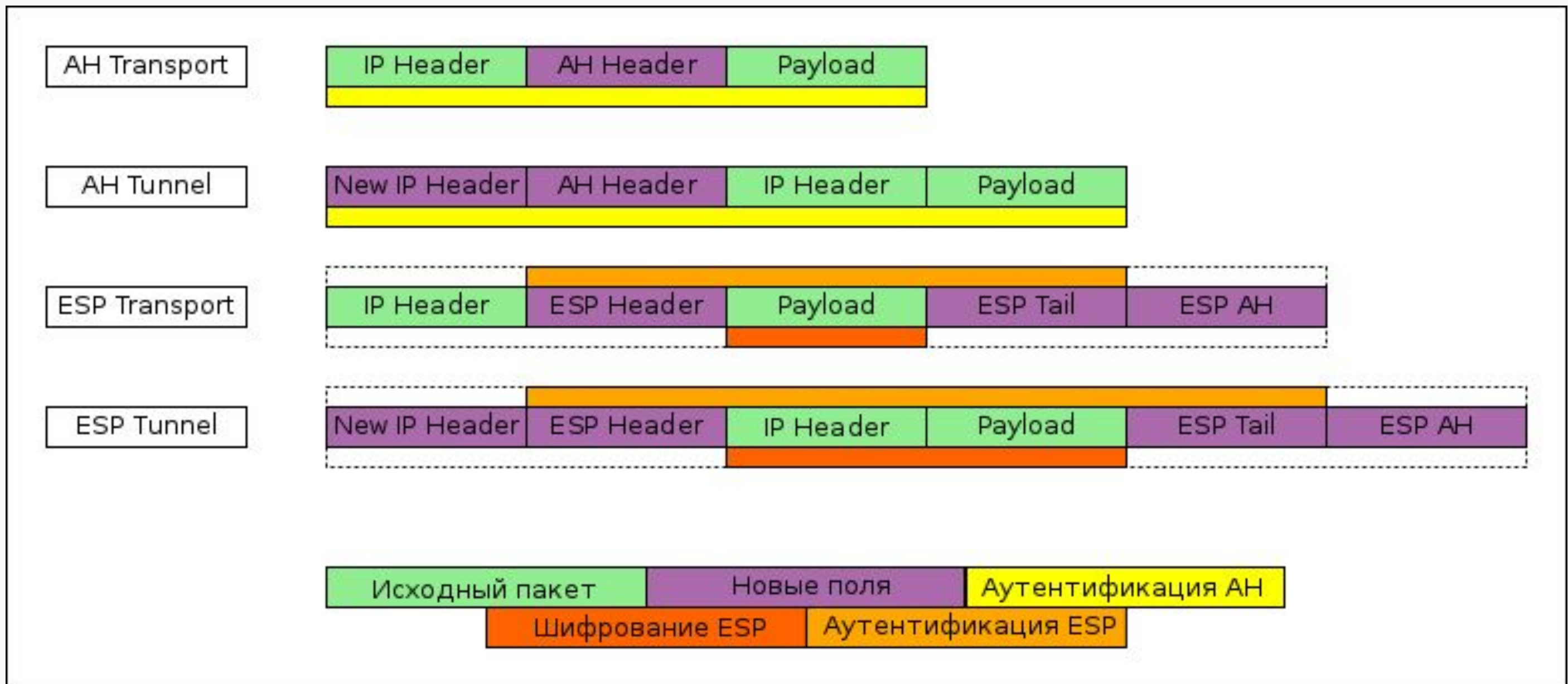
Примерный порядок установки соединения:

1. Один из пиров инициализирует соединение IPSec
2. Происходит обмен ключевой информацией, аутентификация пиров, согласование параметров подключения
3. На основе полученной ключевой информации формируется вспомогательный зашифрованный туннель
4. Используя зашифрованный туннель пиры определяют параметры шифрования данных и обмениваются информацией для генерации ключей
5. Результатом работы предыдущей фазы является набор правил и ключи для защиты данных (SA)
6. Периодически пиры производят обновление ключей шифрования

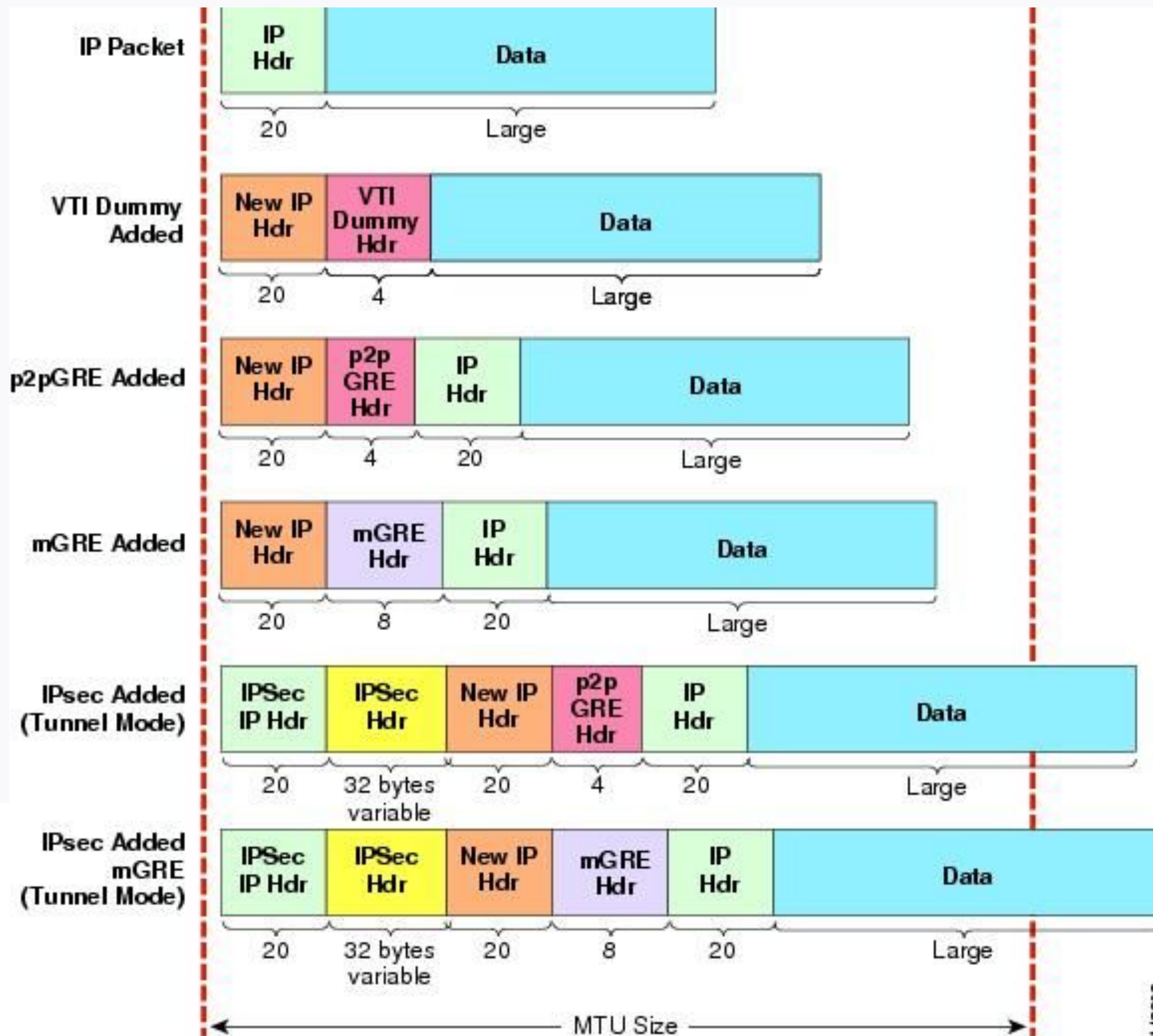
Транспортный режим — защищает только полезную нагрузку пакета, оставляя оригинальный заголовок. Для построения туннелей транспортный режим обычно используется в связке с IPsec или GRE, полезная нагрузка которых уже содержит весь исходный пакет

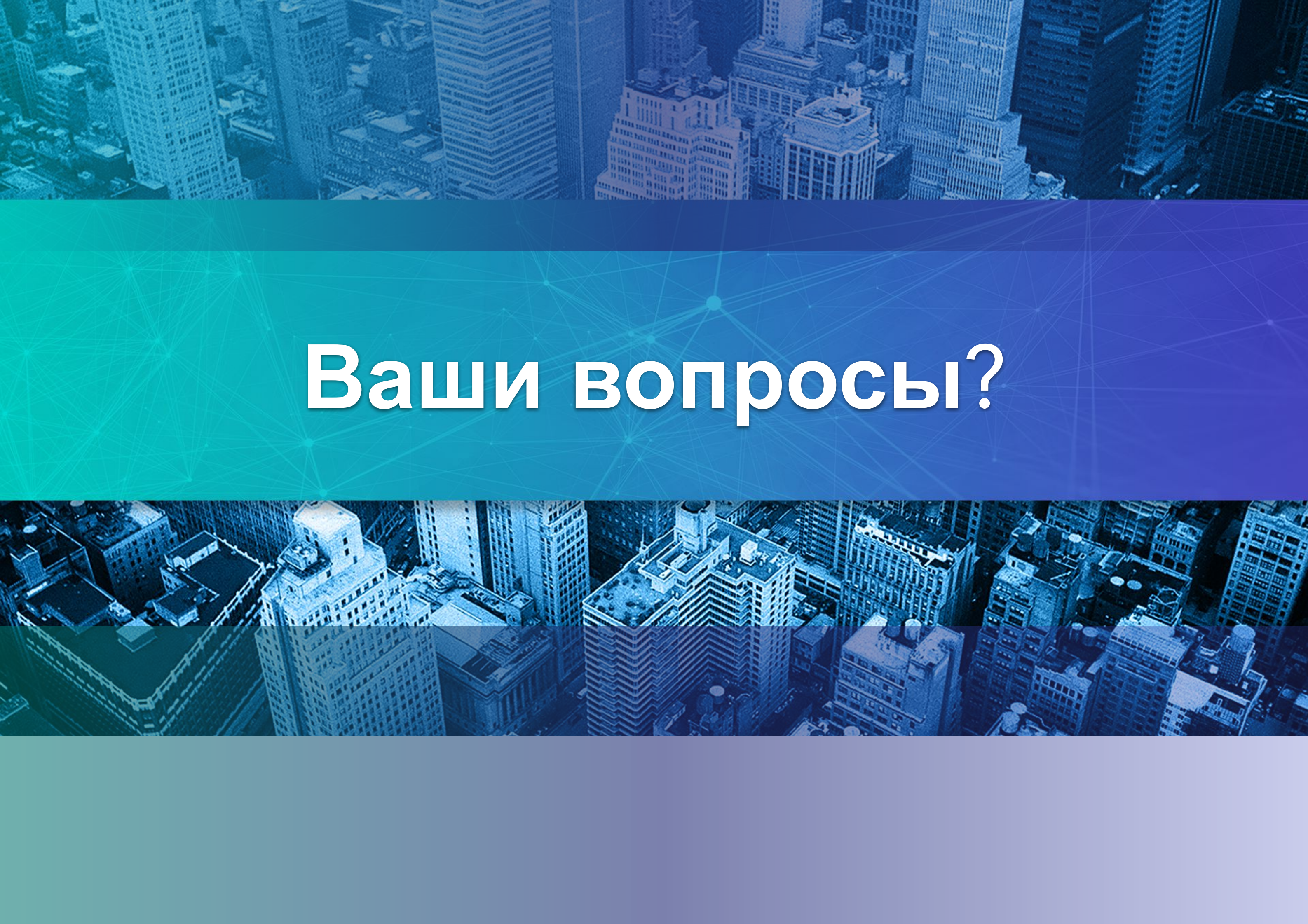
Туннельный режим — полностью инкапсулирует исходный пакет в новый (по аналогии с GRE или IPsec). Но для туннельного IPsec не создается явного интерфейса в системе, это может быть проблемой если используется динамическая или сложная статическая маршрутизация

Инкапсуляция IPsec



Инкапсуляция GRE + IPsec





Ваши вопросы?

Маршрут вебинара

Bridge-интерфейсы



Туннели




OpenVPN



WireGuard



OpenVPN



Вопрос к аудитории:
Кто-нибудь использовал
OpenVPN?

OpenVPN

Сайт проекта: <https://openvpn.net>

Wiki проекта: <https://community.openvpn.net/openvpn/wiki>

Особенности:

- реализует все типы защищенных каналов (client-to-server, server-to-server)
- TCP или UDP в качестве транспорта
- работает через NAT
- L2 и L3 туннели
- шифрование с использованием OpenSSL
- кроссплатформенный клиент

OpenVPN: аутентификация

Static key:

- простота настройки
- используется при **site-to-site** подключениях для создания full-mesh VPN-сетей
- нет необходимости в X.509 PKI инфраструктуре

Certificate-based:

- гибко настраивается
- требует выдачи сертификатов и приватных ключей клиентам
- требует развертывания X.509 PKI инфраструктуре
- удобно использовать в случае отсутствия доверия к клиентам

Авторизацию по логину-паролю:

- упрощает процесс подключения клиентов
- не требует ключей и сертификатов (кроме корневого)
- не так безопасно

OpenVPN: интерфейсы

tun-интерфейс:

- виртуальный интерфейс, работает на L3
- универсален с точки зрения типа и устройства подключения
- **не позволяет** использовать **link-state** протоколы динамической маршрутизации (например OSPF)
- для маршрутизации лучше использовать iBGP

tap-интерфейс:

- виртуальный интерфейс, работает на L2
- по сути представляет собой мост между роутерами
- подходит для проброса vlan`ов
- **позволяет** использовать link-state протоколы динамической маршрутизации

OpenVPN: режимы работы интерфейсов

Topology

P2P:

- каждое подключение имеет свой tun (tap) интерфейс
- маршрутизация и коммутация осуществляются на стороне ОС
- основной режим в **site-to-site** конфигурации

Subnet:

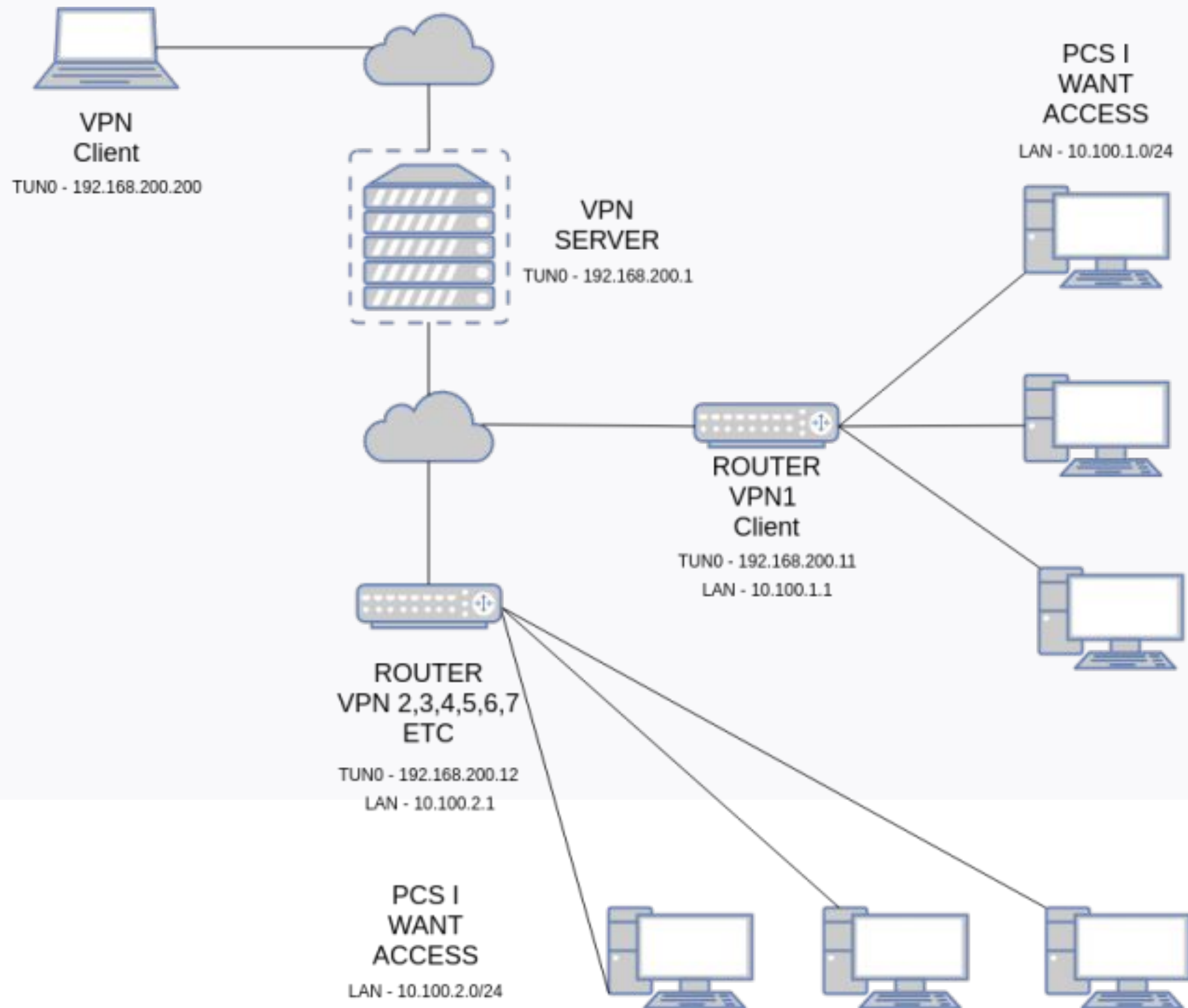
- реализует “традиционную” виртуальную подсеть на виртуальном интерфейсе (возможность все-таки использовать OSPF)
- маршрутизация осуществляется openvpn-сервером
- для общения openvpn-клиентов между собой нужно включать опцию **client-to-client**
- используется в **server-to-client** конфигурации

OpenVPN: примеры топологий

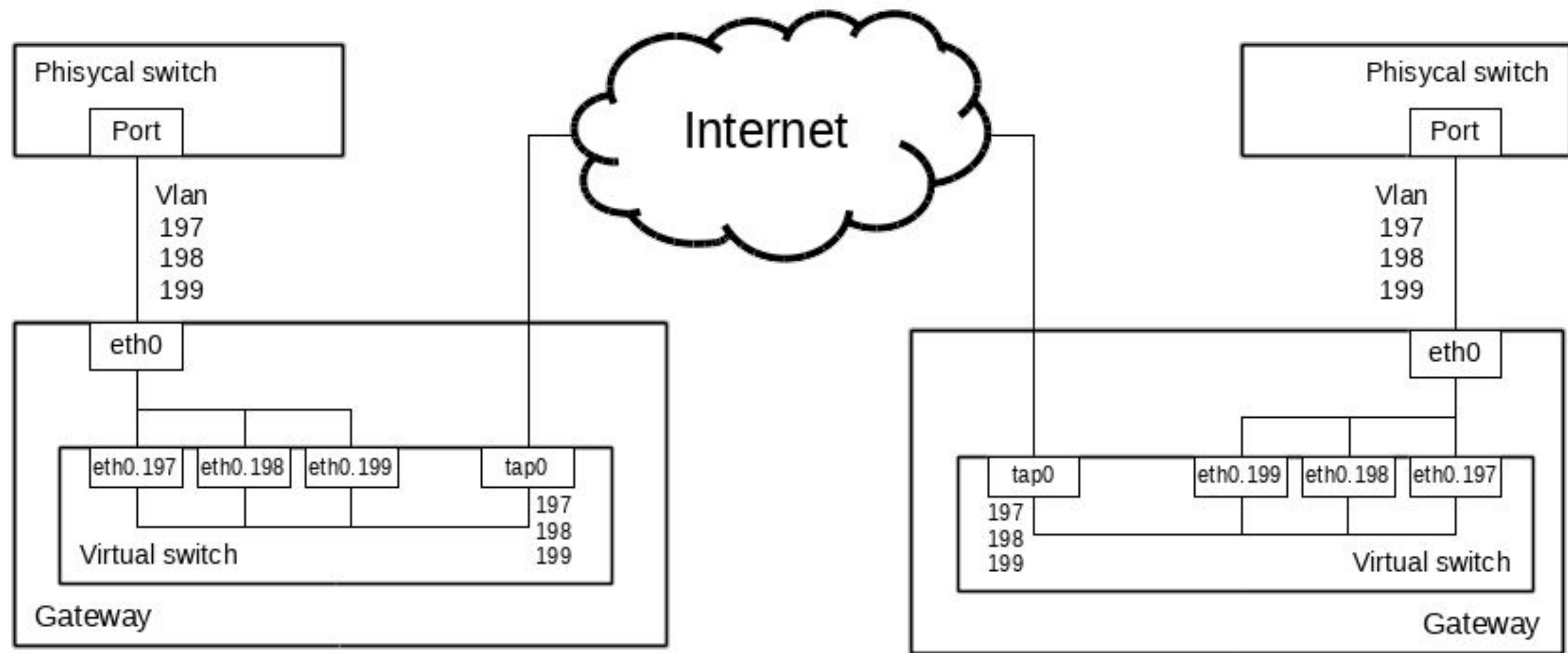
VPN в интернете

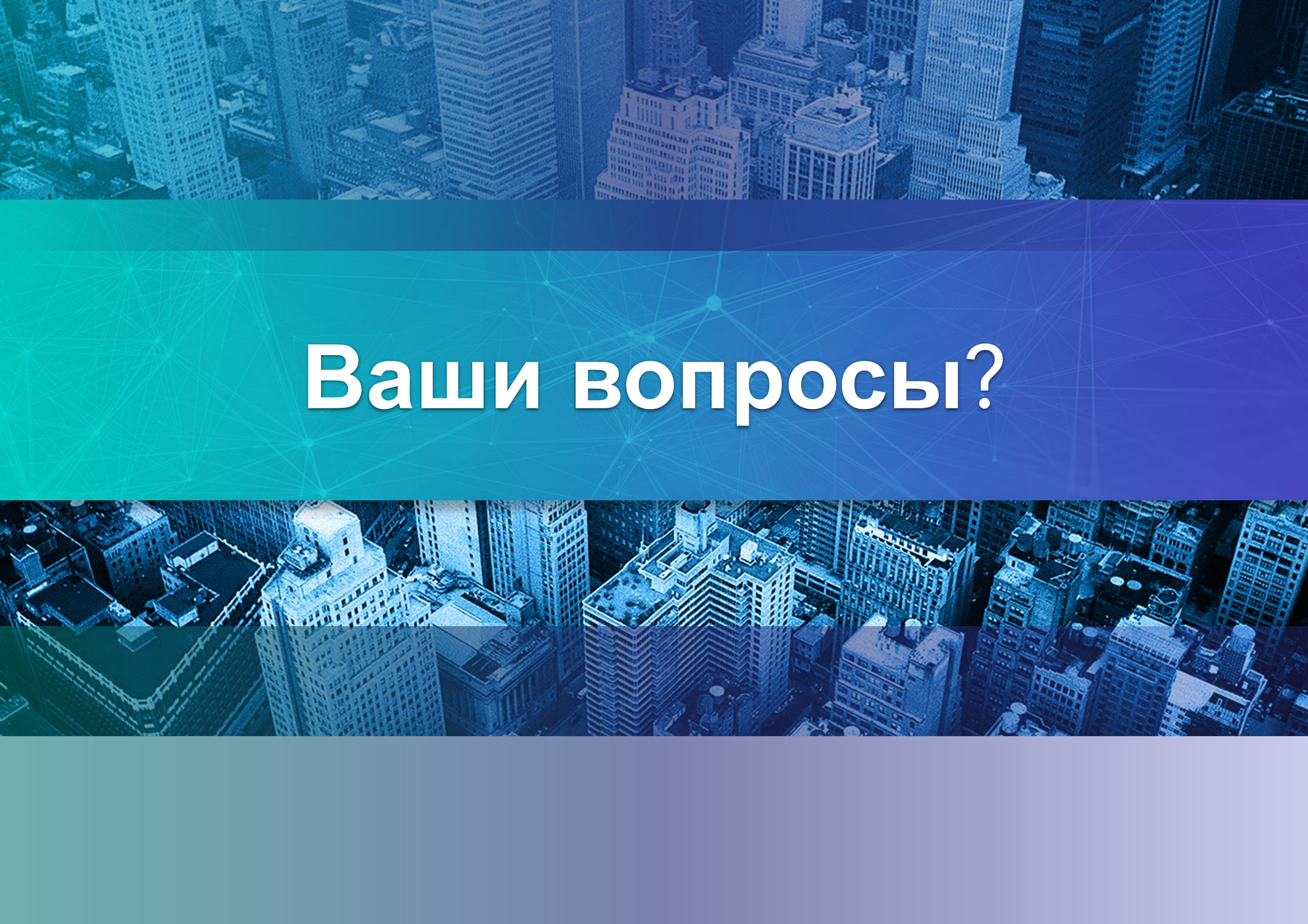


OpenVPN: примеры топологий



OpenVPN: примеры топологий



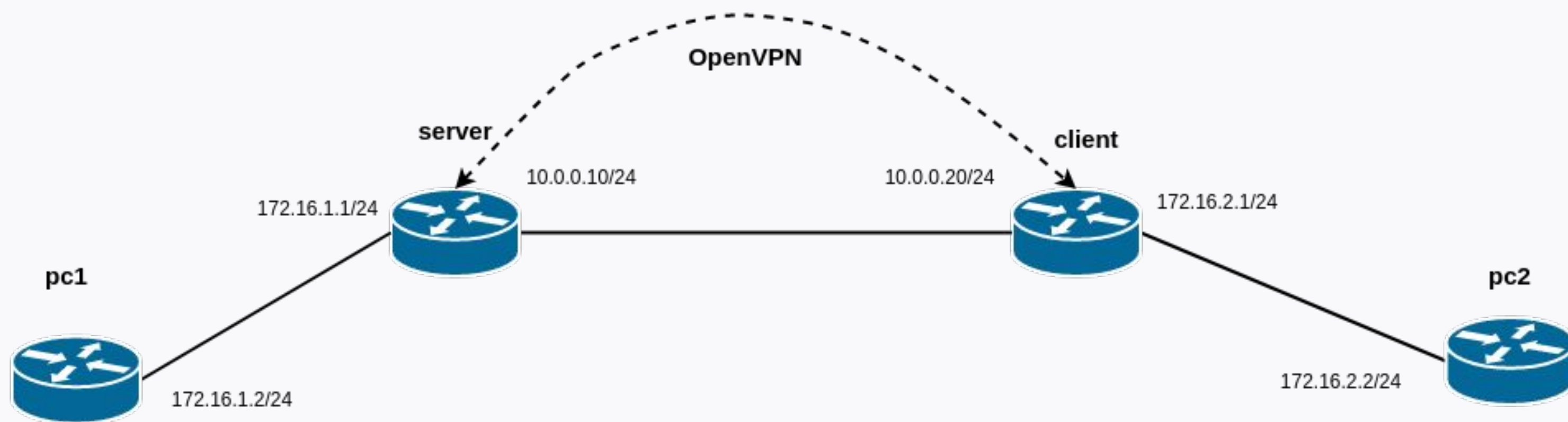


Ваши вопросы?

The background of the slide features an aerial view of a city skyline, likely New York City, with numerous skyscrapers. The image is overlaid with a semi-transparent blue layer that contains a white network pattern of interconnected dots and lines, suggesting a digital or technological theme. The text is centered horizontally across the middle of the slide.

Переходим от слов к делу

OpenVPN: схема тестового стенда





Ваши вопросы?

Маршрут вебинара

Bridge-интерфейсы



Туннели




OpenVPN



WireGuard

The background of the slide is a composite image. The top and bottom sections show an aerial view of a dense city skyline, likely New York City, with numerous skyscrapers. A semi-transparent blue overlay covers the entire image. Overlaid on this blue background is a network diagram consisting of numerous small dots connected by thin, light blue lines, creating a web-like pattern. The word "WireGuard" is written in a large, white, sans-serif font on the left side of the slide, positioned over the network diagram.

WireGuard



Вопрос к аудитории:
Кто-нибудь слышал про
WireGuard?

WireGuard

WireGuard - еще один opensource VPN, который однако получил одобрение Линуса Торвальдса и готовится быть официально включенным в состав ядра Linux. Автор - Jason A. Donenfeld, канадский специалист по информационной безопасности

Официальный сайт: <https://www.wireguard.com>

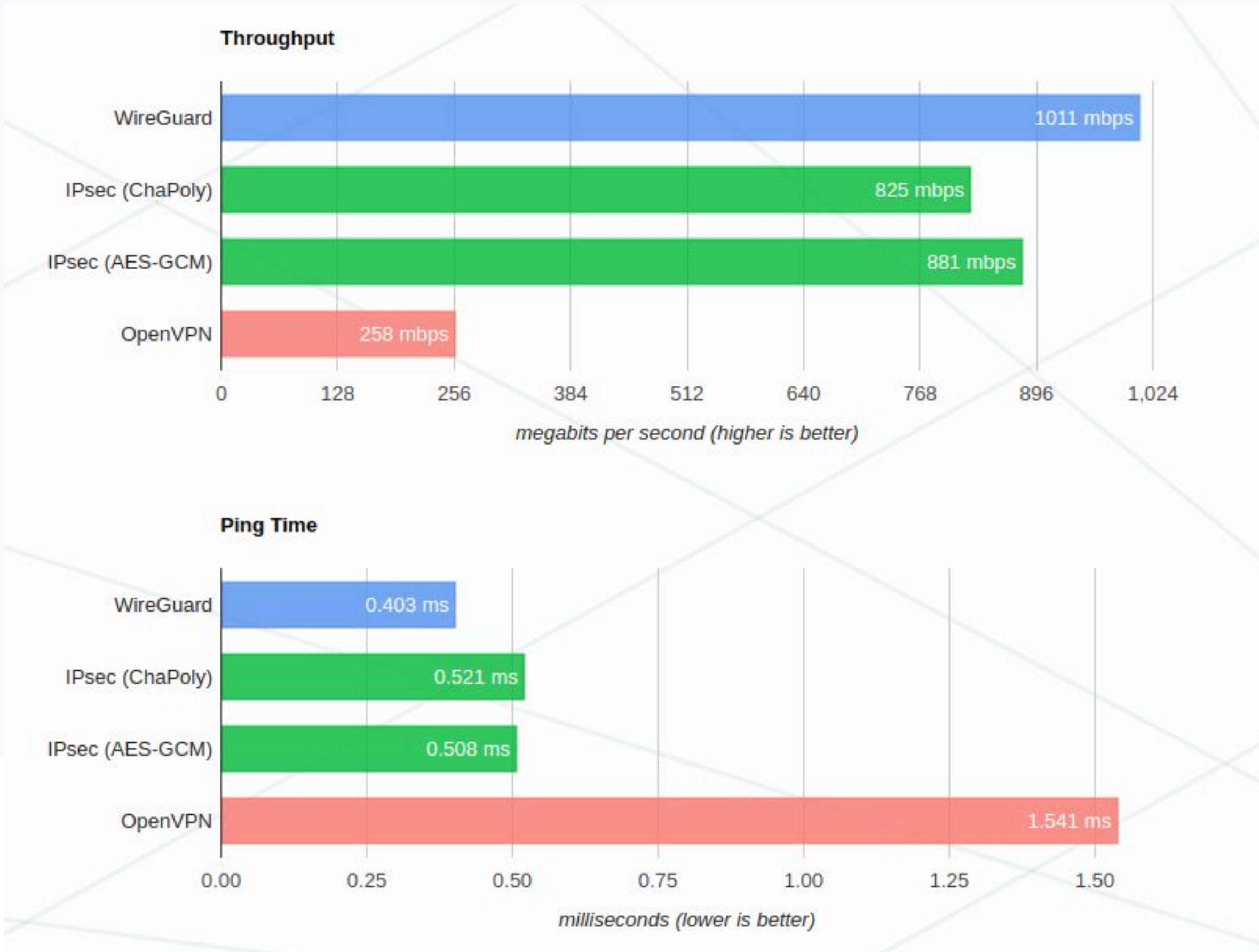
Преимущества:

- простой в использовании
- использует современную криптографию: Noise protocol framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF и вот это все
- компактный читаемый код (отсутствие legacy)

Производительность:

- высокая производительность на Linux, так как работает в виде модуля ядра

WireGuard



Недостатки:

- отсутствие формальной версии и никаких гарантий
- отсутствие поддержки устройствами различных вендоров
- сам продукт WireGuard не проходил аудит безопасности, аудит безопасности проходили используемые протоколы
- нет возможности менять используемые криптопримитивы и транспортный протокол

WireGuard

Установка в CentOS:

```
curl -Lo /etc/yum.repos.d/wireguard.repo  
https://copr.fedorainfracloud.org/coprs/jdoss/wireguard/repo/epel-7/jdoss-wireguard-epel-7.r  
epo  
yum makecache  
yum install epel-release  
yum install wireguard-dkms wireguard-tools
```

Генерация ключей:

```
umask 077  
wg genkey | tee privatekey | wg pubkey > publickey
```


WireGuard

Настройка сервера:

```
cat /etc/wireguard/wg0.conf
[Interface]
Address = 10.64.20.1/24
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o eth1 -j MASQUERADE
ListenPort = 51820
PrivateKey = <server private key>

[Peer]
PublicKey = <client public key>
Endpoint = 172.16.20.22:51821
AllowedIPs = 10.64.20.0/24
```


WireGuard

Настройка клиента:

```
cat /etc/wireguard/wg0.conf
[Interface]
PrivateKey = <client private key>
Address = 10.64.20.2/24
ListenPort = 51821

[Peer]
PublicKey = <server public key>
Endpoint = 172.16.20.21:51820
AllowedIPs = 10.64.20.0/24
PersistentKeepalive = 30
```

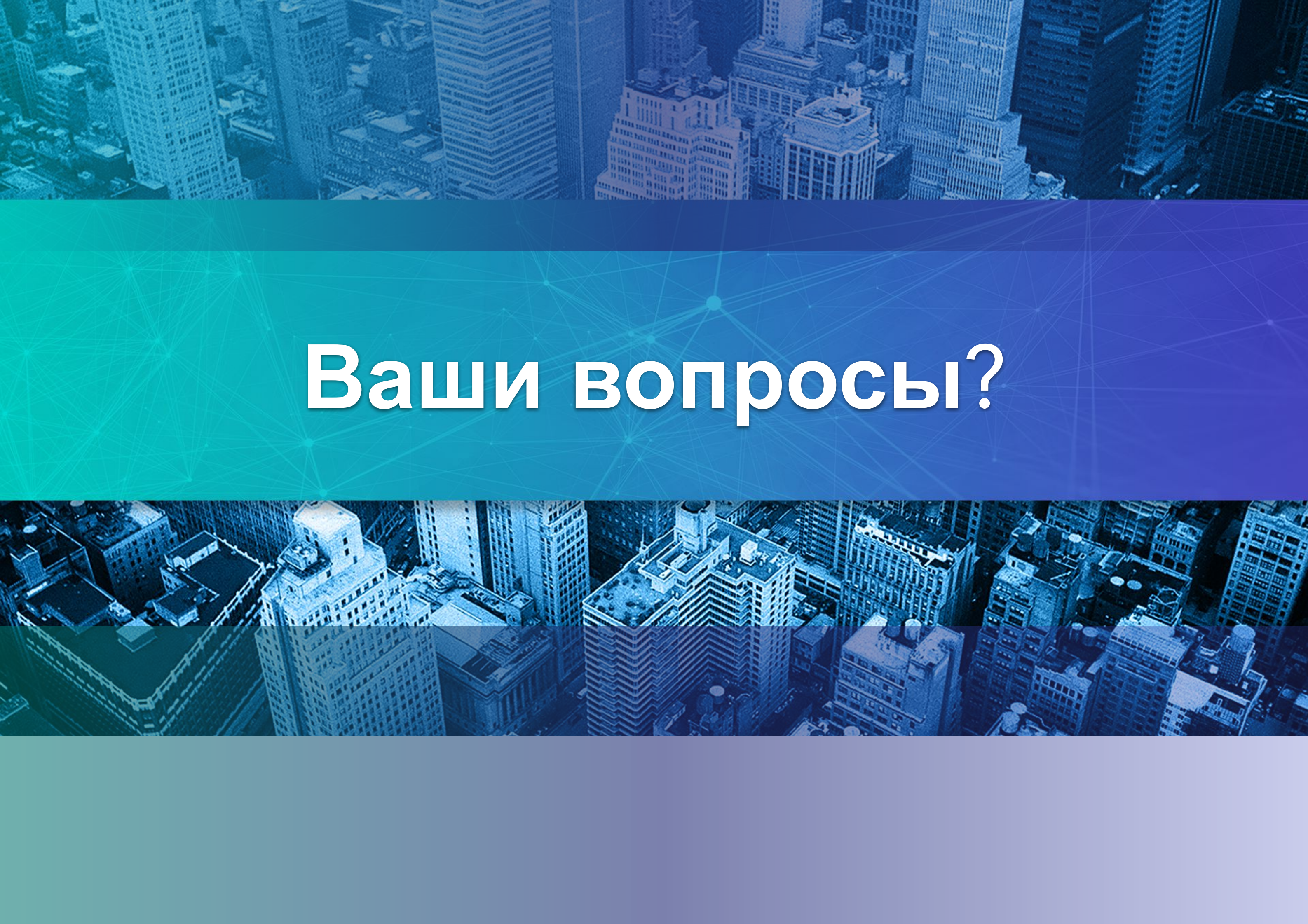

WireGuard

Запуск сервера:

```
wg-quick up wg0
```

Запуск клиента:

```
wg-quick up wg0
```

Ваши вопросы?

Домашнее задание

- 1 Между двумя виртуалками поднять vpn в режимах **tun** и **tap**. Прочувствовать разницу
- 2 Поднять RAS на базе OpenVPN с клиентскими сертификатами, подключиться с локальной машины на виртуалку
- 3 Самостоятельно изучить, поднять ocserv и подключиться с хоста к виртуалке

Рефлексия



Назовите 3 момента, которые вам запомнились в процессе занятия



Что вы будете применять в работе из сегодняшнего вебинара?

Следующий вебинар

Тема: Статическая и динамическая маршрутизация



11.02.20



Ссылка на вебинар будет в ЛК за 15 минут




Материалы к занятию в ЛК — можно изучать



Обязательный материал обозначен красной лентой

Список материалов для изучения

- Статья про IPsec: <https://asp24.ru/mikrotik/vpn/obzor-ipsec-v-mikrotik>
- Сети для самых маленьких. Часть 7. VPN: <https://habr.com/ru/post/170895/>
- Статья вообще про VPN: <http://xgu.ru/wiki/VPN>
- Статья по OpenVPN: <http://xgu.ru/wiki/OpenVPN>
- Установка и настройка WireGuard на CentOS: <https://sysadmin.pm/wireguard>



Заполните, пожалуйста,
опрос о занятии по ссылке в чате



Спасибо за внимание!
Приходите на следующие вебинары



Викирюк Павел

Системный инженер