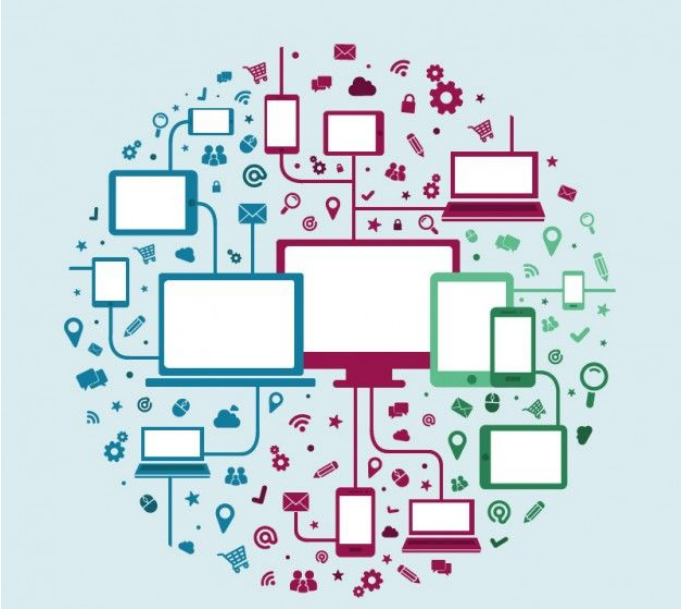
Компьютерные сети

Урок 6

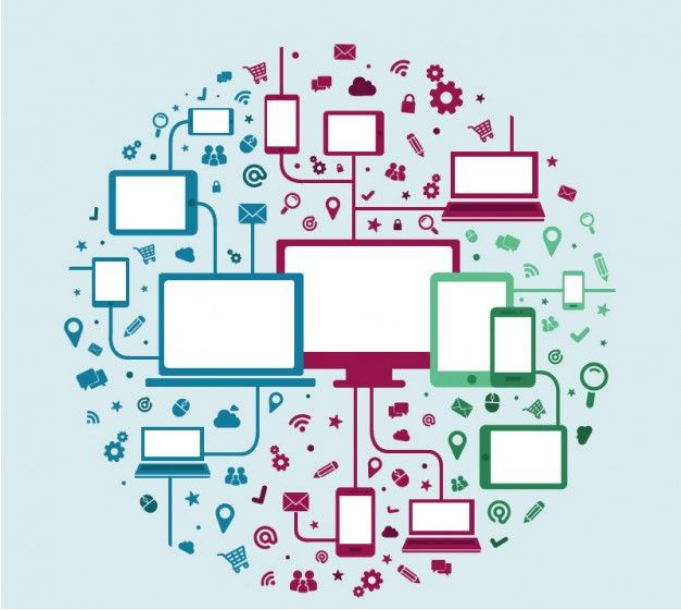
Углубленное изучение сетевых технологий. Часть 1

DNS. Сетевая безопасность. Шифрование. VPN

Вопросы к аудитории



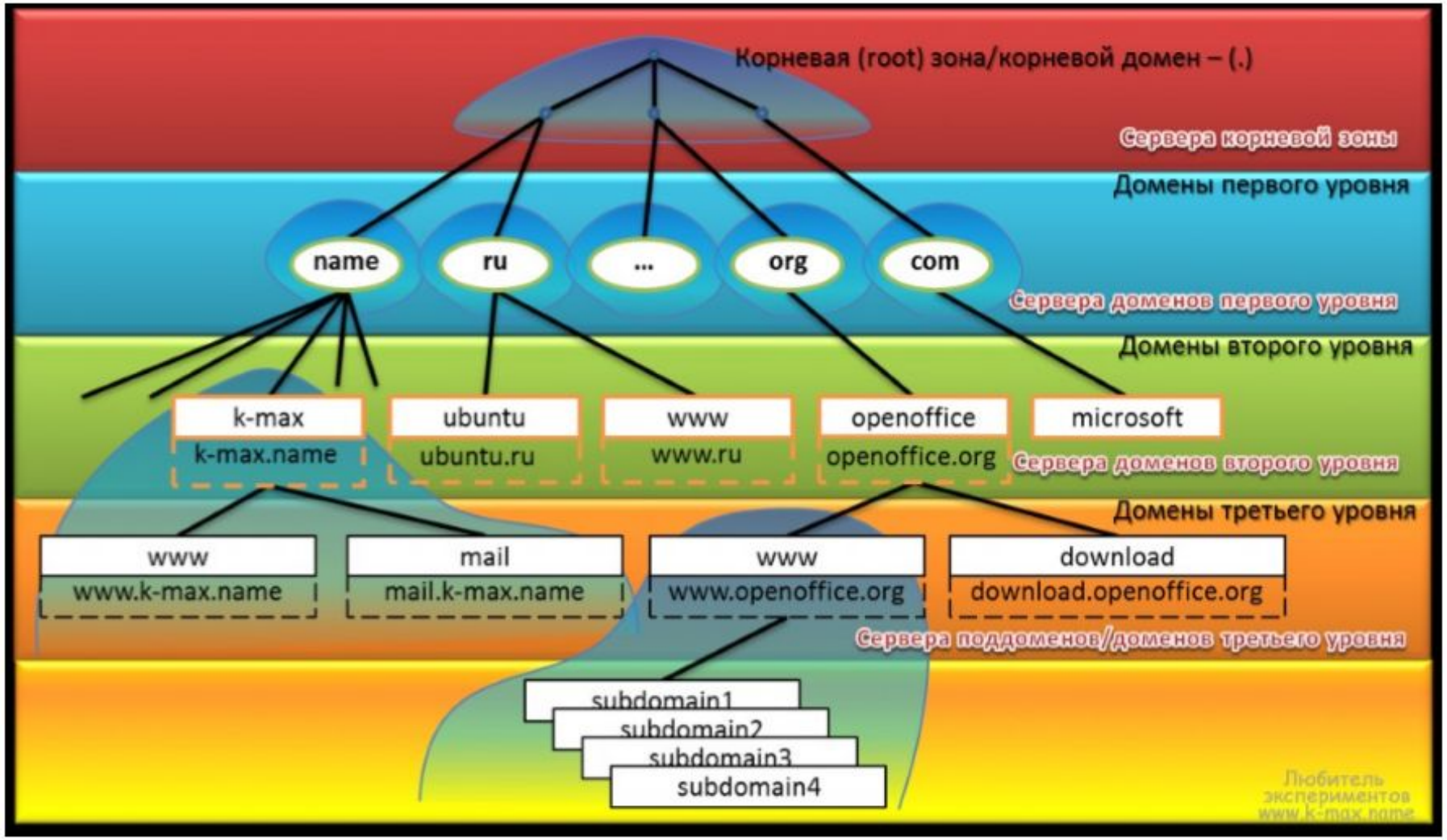
План урока



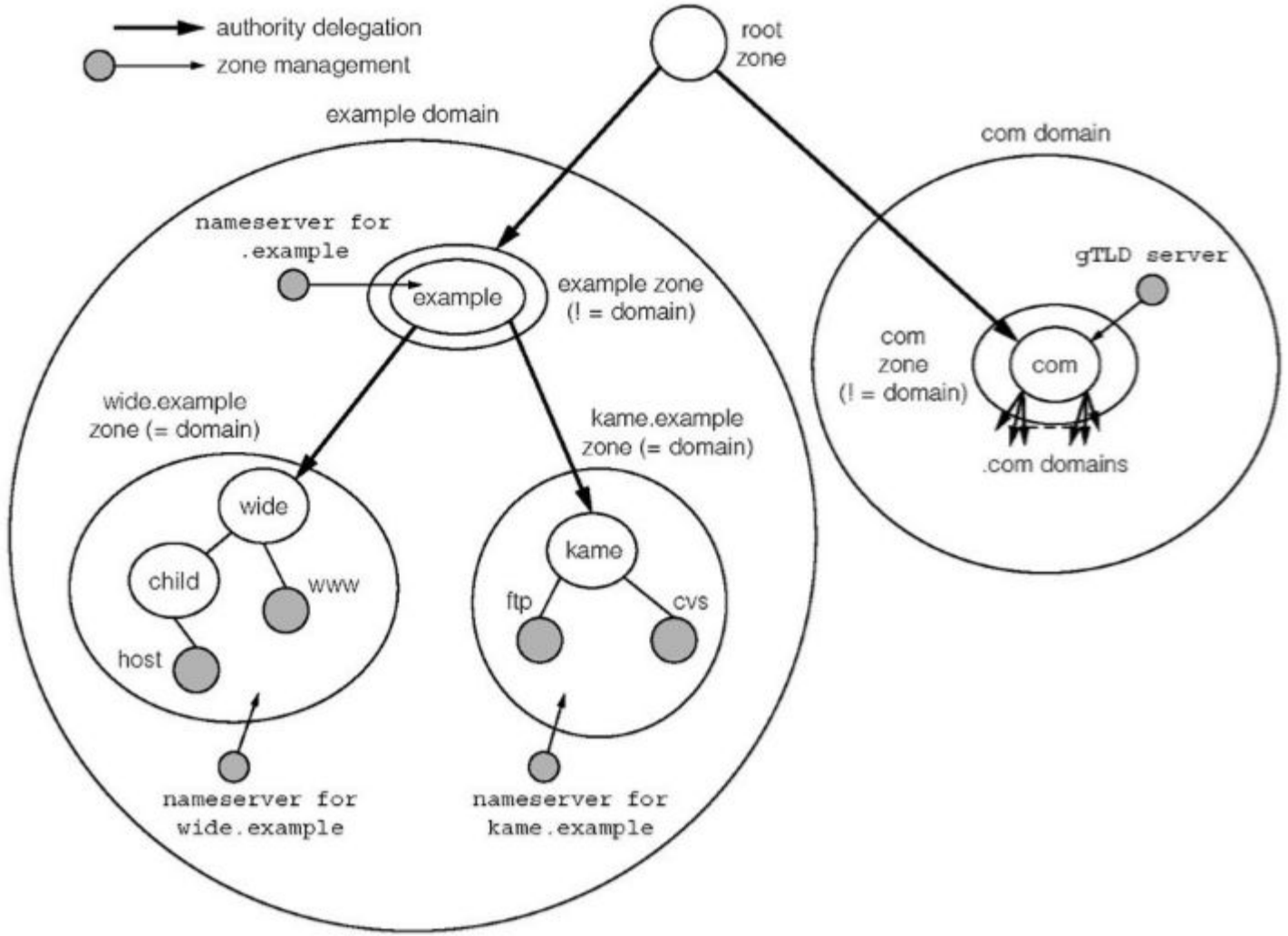
- DNS.
- Асимметричное и симметричное шифрование.
- Протоколы и методы шифрования.
- VPN и их назначение.

Domain Name Service

Иерархическая структура DNS



Домены и зоны



Ресурсные записи

name. TTL CLASS TYPE DATA

где

- name — доменное имя
- TTL — срок хранения записи в кэше
- CLASS — всегда IN (INternet)
- TYPE — тип записи (A/CNAME/MX/PTR...)
- DATA — данные (зависит от TYPE)

Корневые серверы

a.root-servers.net

b.root-servers.net

c.root-servers.net

d.root-servers.net

e.root-servers.net

f.root-servers.net

g.root-servers.net

h.root-servers.net

i.root-servers.net

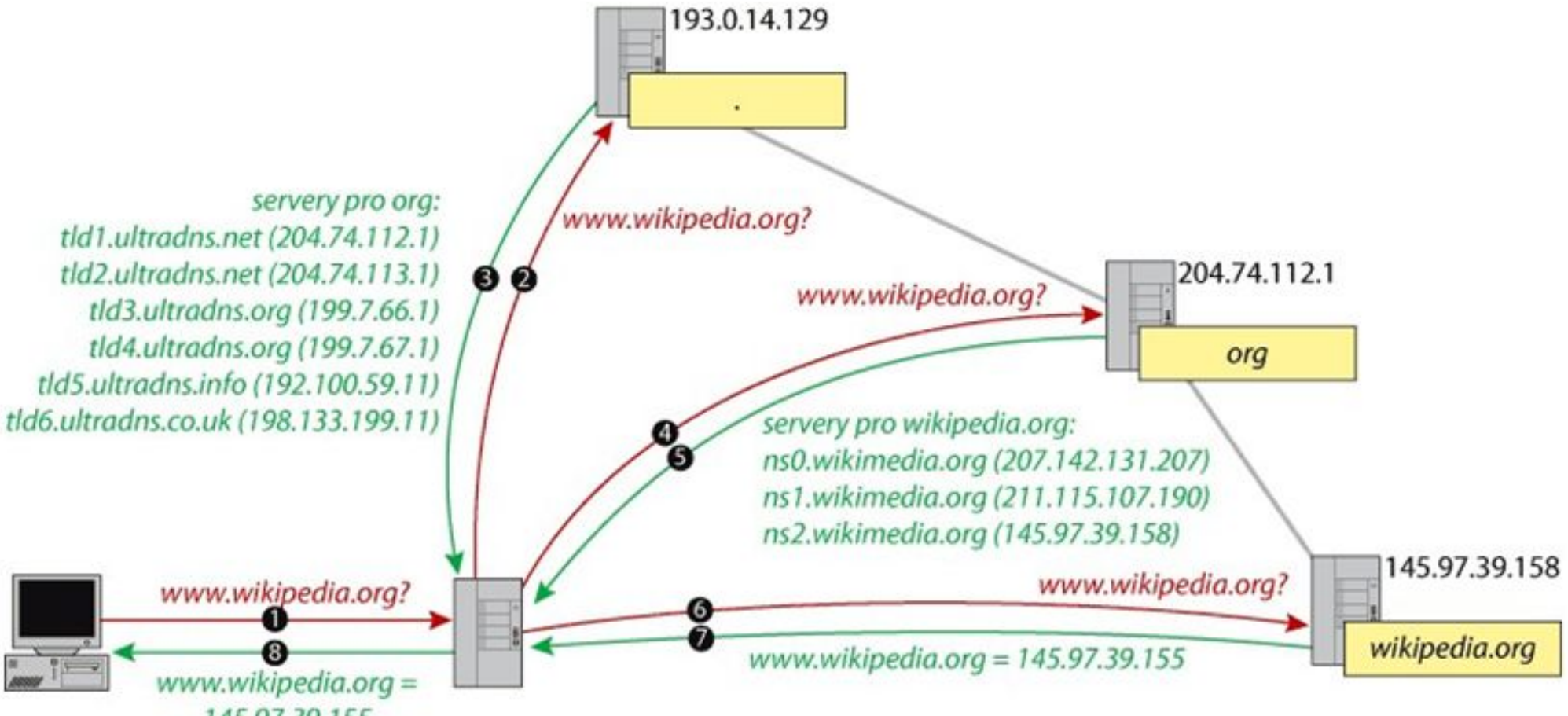
j.root-servers.net

k.root-servers.net

l.root-servers.net

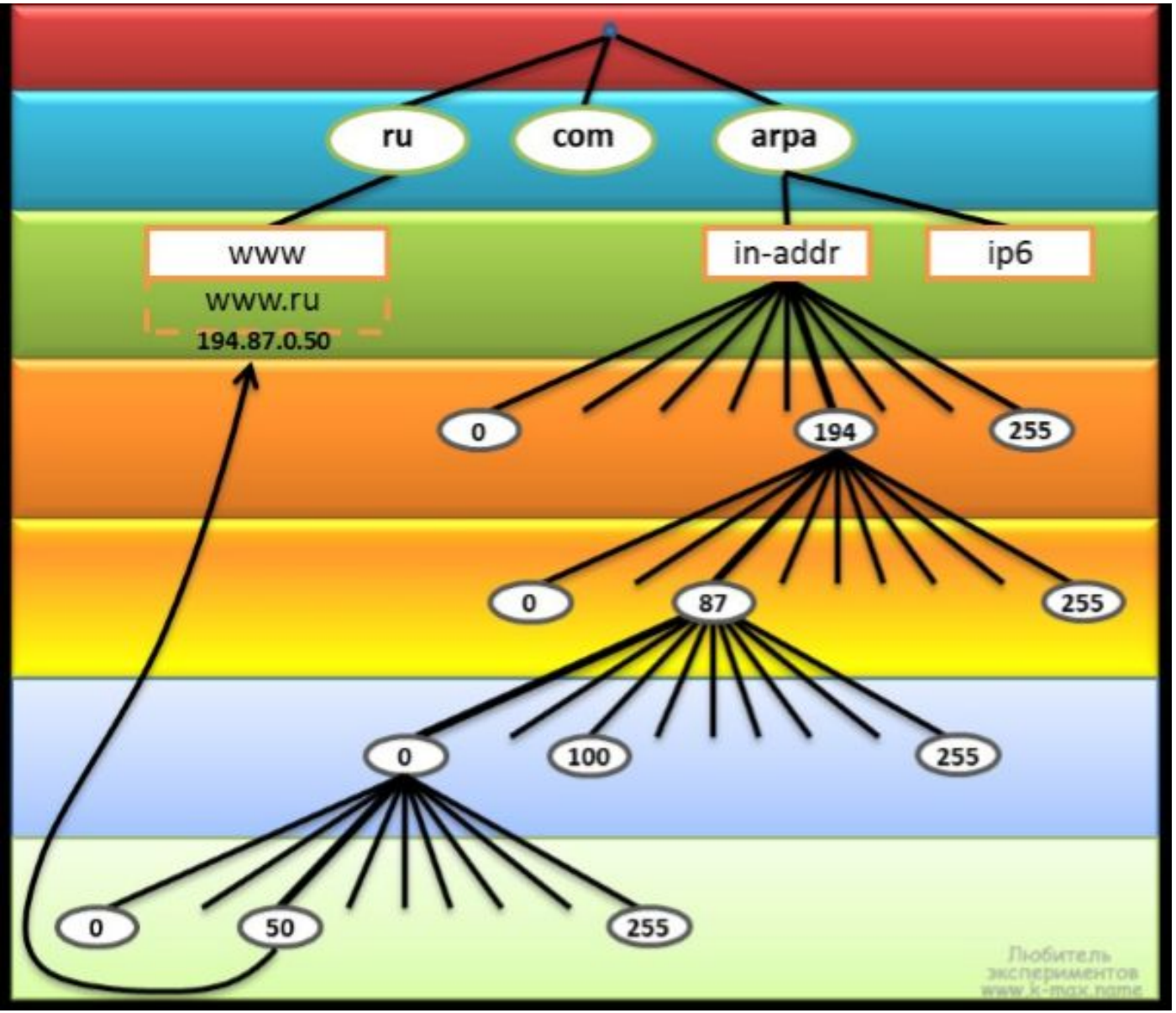
m.root-servers.net

Разрешение доменного имени



Некоторые типы записей

- A — доменному имени сопоставить IPv4
- CNAME — доменному имени сопоставить каноническое доменное имя
- NS — доменному имени сопоставить DNS-сервер
- MX — доменному имени сопоставить доменное имя почтового сервера и приоритет
- PTR — IP-адресу, записанному в виде доменного имени (в in-addr.arpa) сопоставить каноническое доменное имя



Записи PTR

Запись 50.0.87.194.in-addr.arpa. IN PTR www.ru означает, что IP-адресу 194.87.0.5 соответствует каноническое доменное имя www.ru

Запись должна быть добавлена провайдером, предоставившим IP-адрес.

Запись используется SMTP-службами для проверки возможности отправить почту от вашего домена.

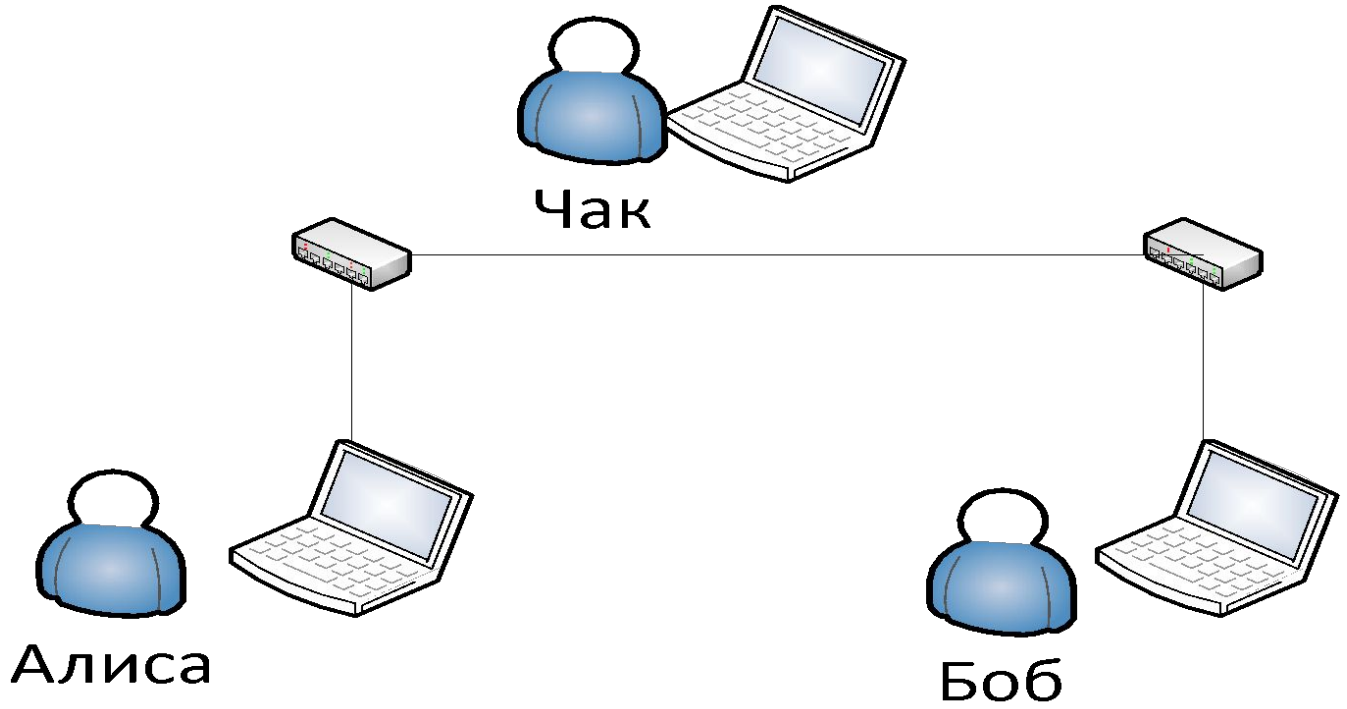
Сетевая безопасность

Сетевая безопасность — раздел прикладной научной дисциплины, называемый информационной безопасностью.

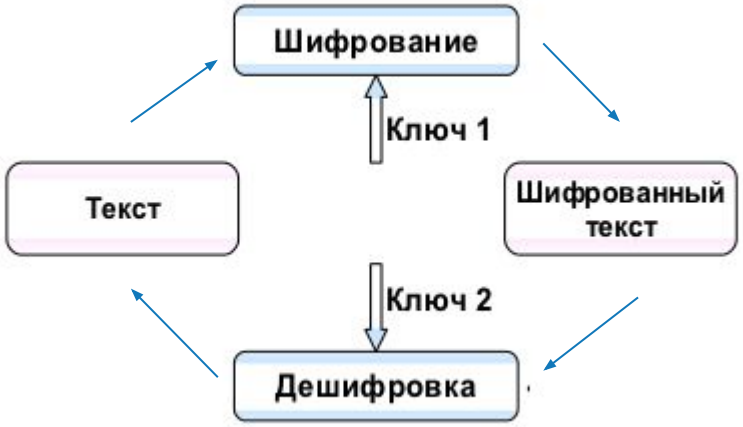
Сетевая безопасность включает в себя набор правил, методик и средств обеспечивающих: надежность и конфиденциальность передачи информации в сети.

Определения

- Аутентификация
- Авторизация
- Шифрование
- Конфиденциальность
- Целостность
- Доступность
- Несанкционированный доступ



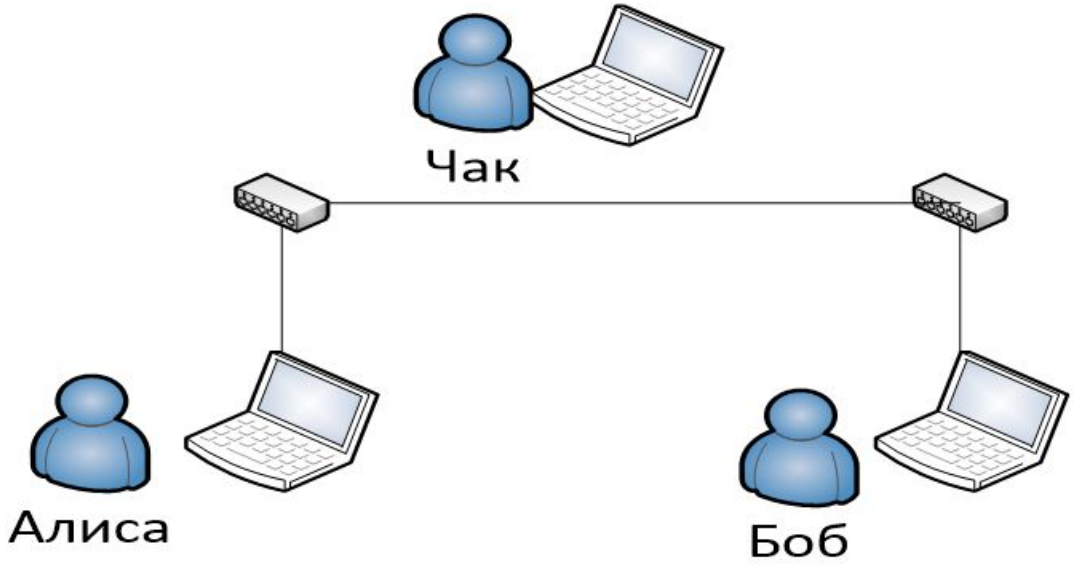
Шифрование



Существует два типа алгоритмов шифрования.

- Симметричный — такой тип шифрования при котором для шифровки и дешифровки используется один и тот же ключ.
- Асимметричный — такой тип шифрования, при котором для шифровки и дешифровки используются разные ключи.

Система криптографии с открытым ключом



Открытый ключ

Секретный ключ

Алгоритм генерации ключей

Цифровая подпись (электронная подпись)

Алгоритмы шифрование

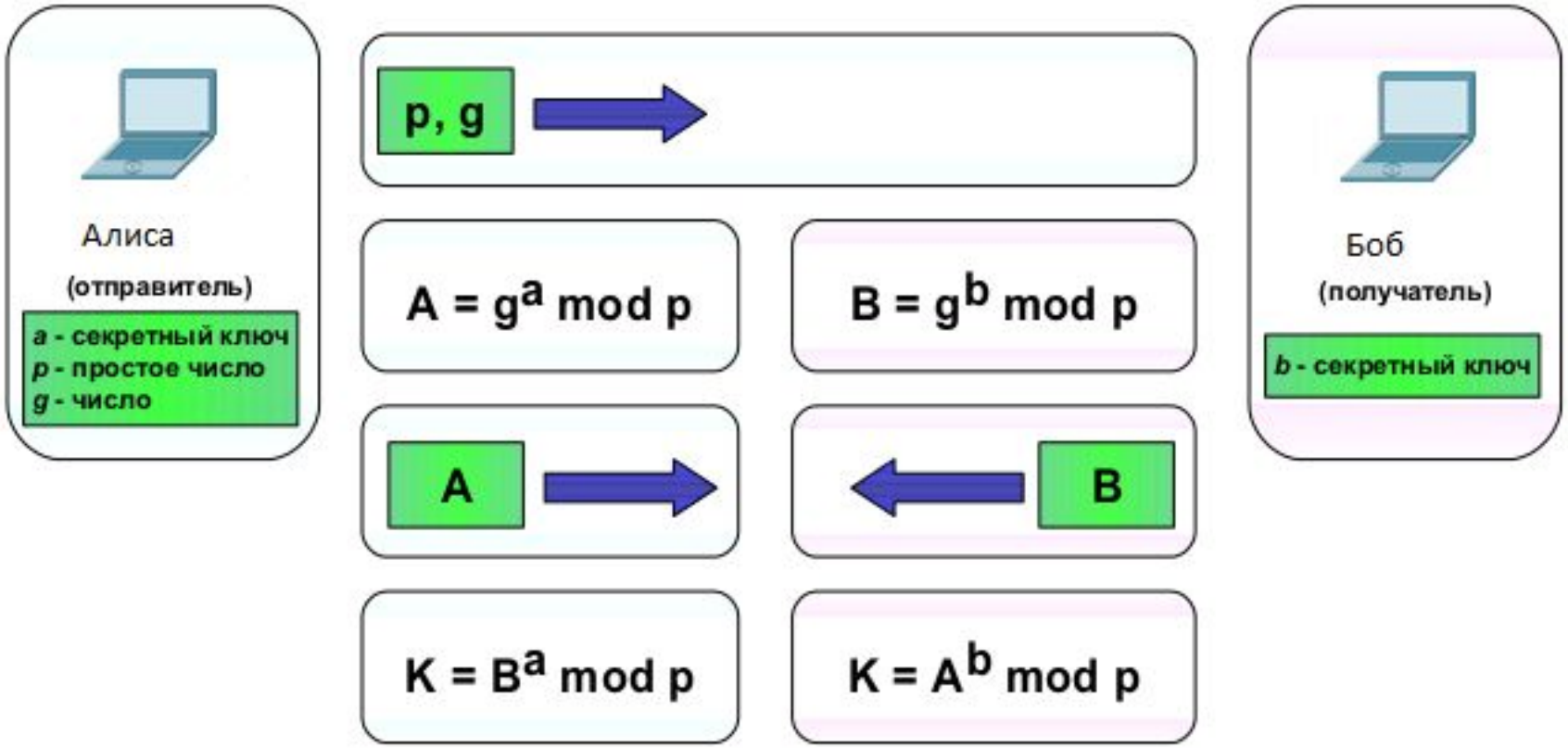
Ассиметричные алгоритмы шифрования:

- RSA
- DSA
- ГОСТ Р 34.10-2001

Симметричные алгоритмы шифрования:

- AES - американский стандарт шифрования
- ГОСТ 28147-89 — советский и российский стандарт шифрования, также является стандартом СНГ
- DES/3DES - стандарты шифрования данных в США

Алгоритм Диффи-Хелмана



$$B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p$$

RSA (Rivest, Shamir и Adleman)

Электронная подпись

ЭЦП или электронная цифровая подпись - это реквизит используемый для электронных документов, обеспечивающий защиту документов от подделки или изменения. ЭЦП получается путем применения криптографических преобразований данных с применением закрытого ключа шифрования для электронно-цифровой подписи выданной центром сертификации.

Сертификат

Цифровой сертификат — это специальный документ, который подтверждает соответствие открытого ключа и информации, которая идентифицирует хозяина ключа. Сертификат выдается центром сертификации или может быть сгенерирован самостоятельно и включает данные о владельце сертификата, открытый ключ, его сферы использования, адрес и название центра сертификации выдавшего данный сертификат, а также цифровую подпись центра и т.д.

SSL/TLS

Secure sockets layer - уровень защищённых сокетов, криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.

SSL

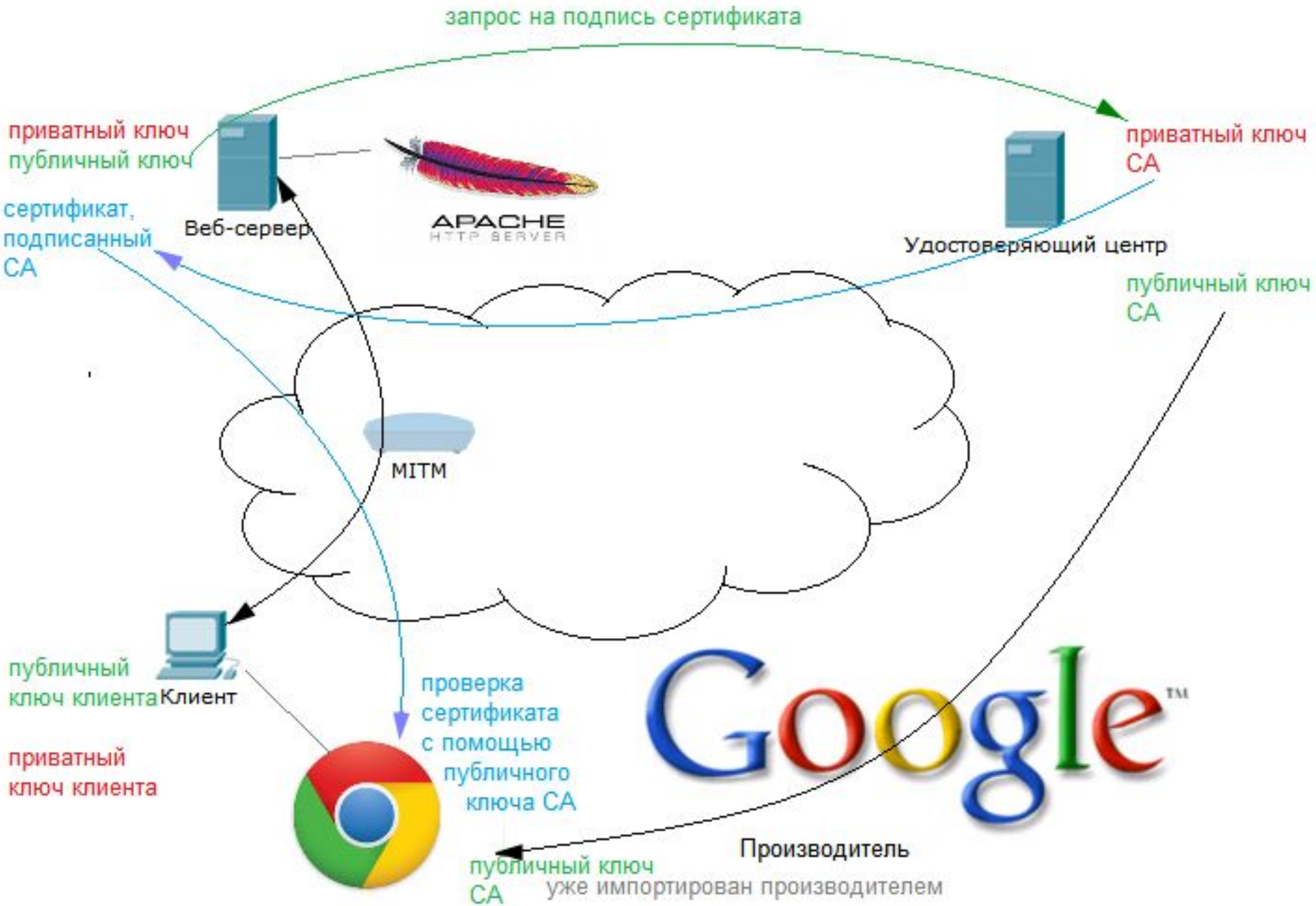
По материалам https://blog.jenrom.com/2014/09/07/internet-fundamentals-osi-модель-уровень-представления/

- **SSL (Secure Socket Layer)**
- **SSL** — протокол шифрования, который обеспечивает безопасное соединение между клиентом и сервером. Протокол **SSL** был разработан фирмой **Netscape**, достаточно давно. Версия **1.0** никогда не была обнародована. Версия **2.0**была выпущена в феврале **1995** года, но содержала много недостатков по безопасности, которые привели к разработке **SSL** версии **3.0**.

SSL

По материалам https://blog.jenrom.com/2014/09/07/internet-fundamentals-osi-модель-уровень-представления/

- **TLS (Transport Layer Security)**
- **TLS** — протокол шифрования, обеспечивающий защищённую передачу данных между узлами в сети Интернет. Он является следующим поколением протокола **SSL**.
- На данный момент есть три версии протокола **TLS**: **1.0**, **1.1** и **1.2**. Они, соответственно, имеют внутренние идентификаторы версии **3.1**, **3.2** и **3.3**, поэтому иногда называются **SSL 3.1**, **SSL 3.2** и **SSL 3.3**.
- **TLS** и **SSL** используют асимметричную криптографию для аутентификации и симметричное шифрование для передачи данных.
- Стоит отметить, что основная работа шифрования данных **TLS** и **SSL** проходит на **6** уровне модели **OSI** (уровень представления), **а аутентификация — на 5уровне модели OSI (сеансовый уровень)**
-


запрос на подпись сертификата
приватный ключ
публичный ключ
Веб-сервер
APACHE
HTTP SERVER
приватный ключ
CA
Удостоверяющий центр
сертификат,
подписанный
CA
публичный ключ
CA
MITM
публичный
ключ клиента
Клиент
проверка
сертификата
с помощью
публичного
ключа CA
приватный
ключ клиента
Google
Производитель
публичный ключ
CA
уже импортирован производителем

VPN

Виртуальная частная сеть – это сеть используемая для создания безопасного туннеля между компьютером и удаленной сетью через сеть Интернет. Частные сети создаются путем применения протоколов выполняющих следующие функции:

- Шифрование трафика
- Аутентификация источника и передатчика
- Проверка достоверности данных
- Защита от подмены данных путем повторной передачи

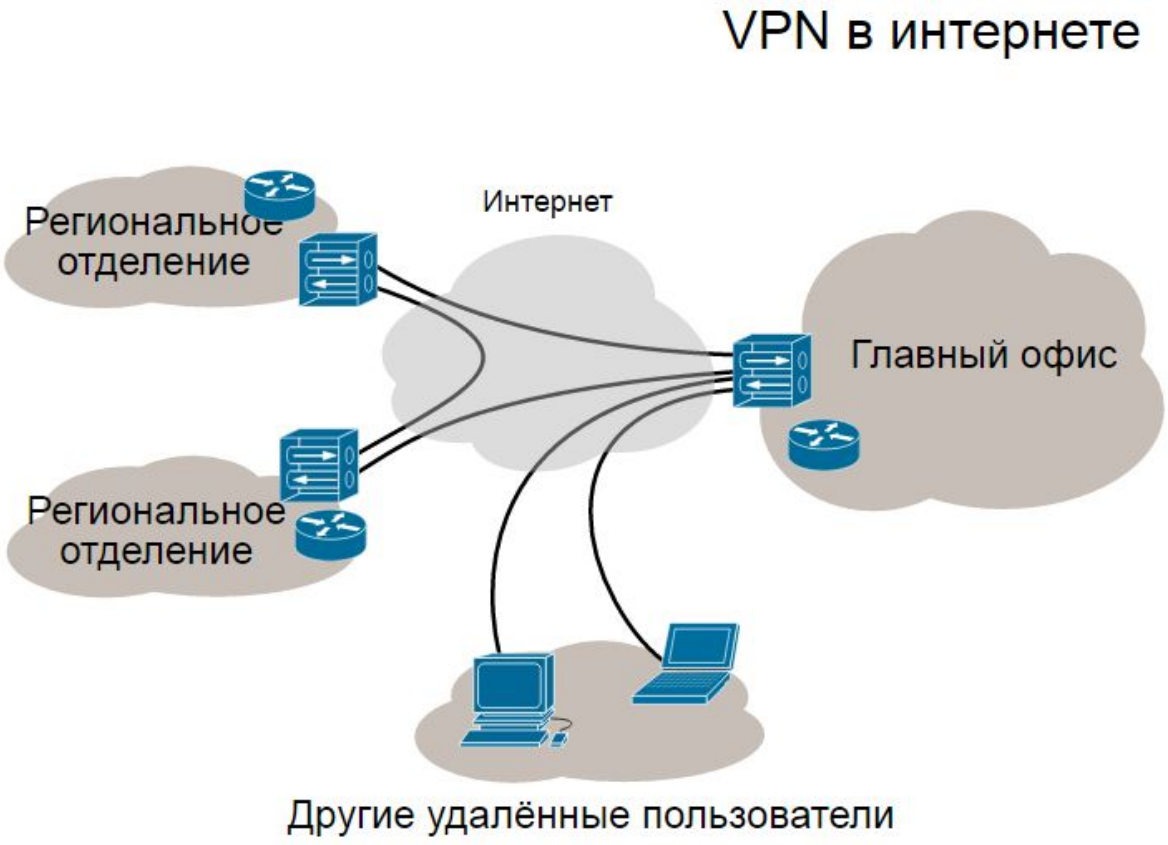
Классификация VPN

Основанная на сфере применения:

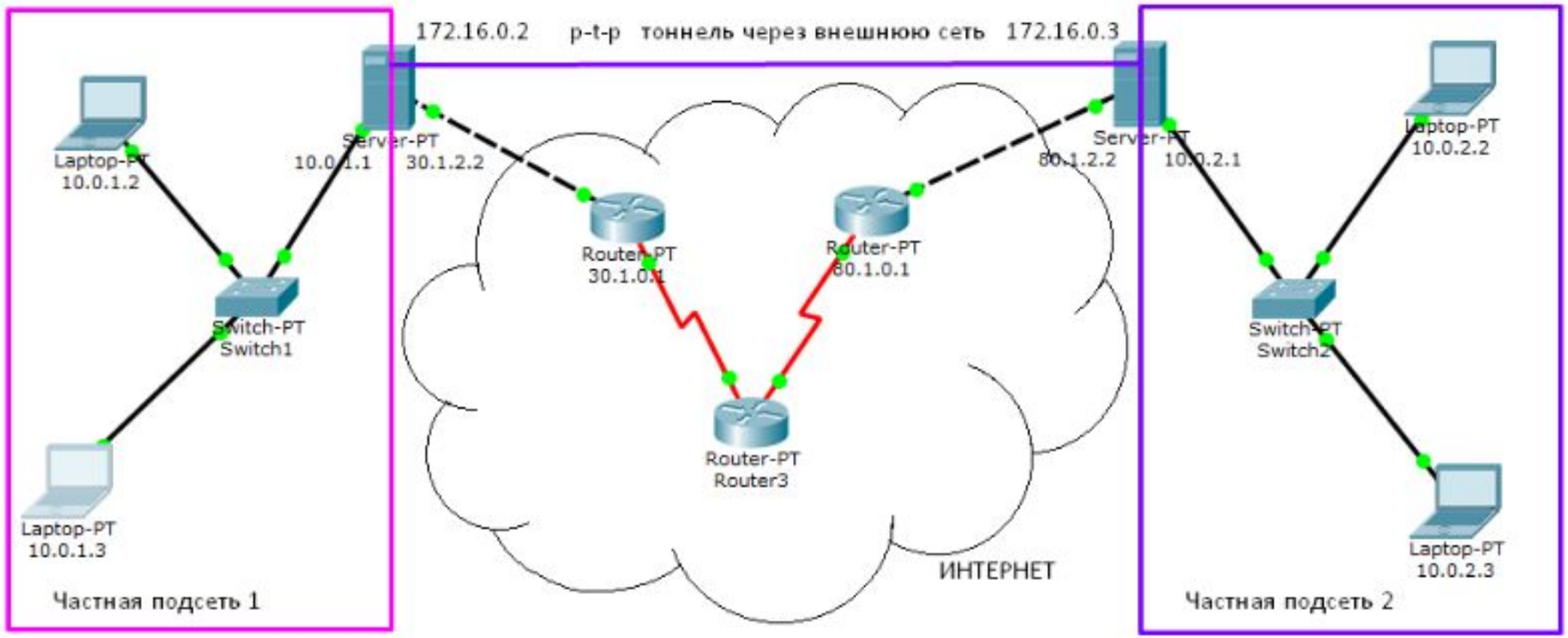
- Доступ в сеть (Access VPN)
- Соединение внутренних сетей (Intranet VPN)
- Подключение к внешним сетям (Extranet VPN)

Основная на уровне OSI:

- Уровень 2 VPN
- Уровень 3 VPN



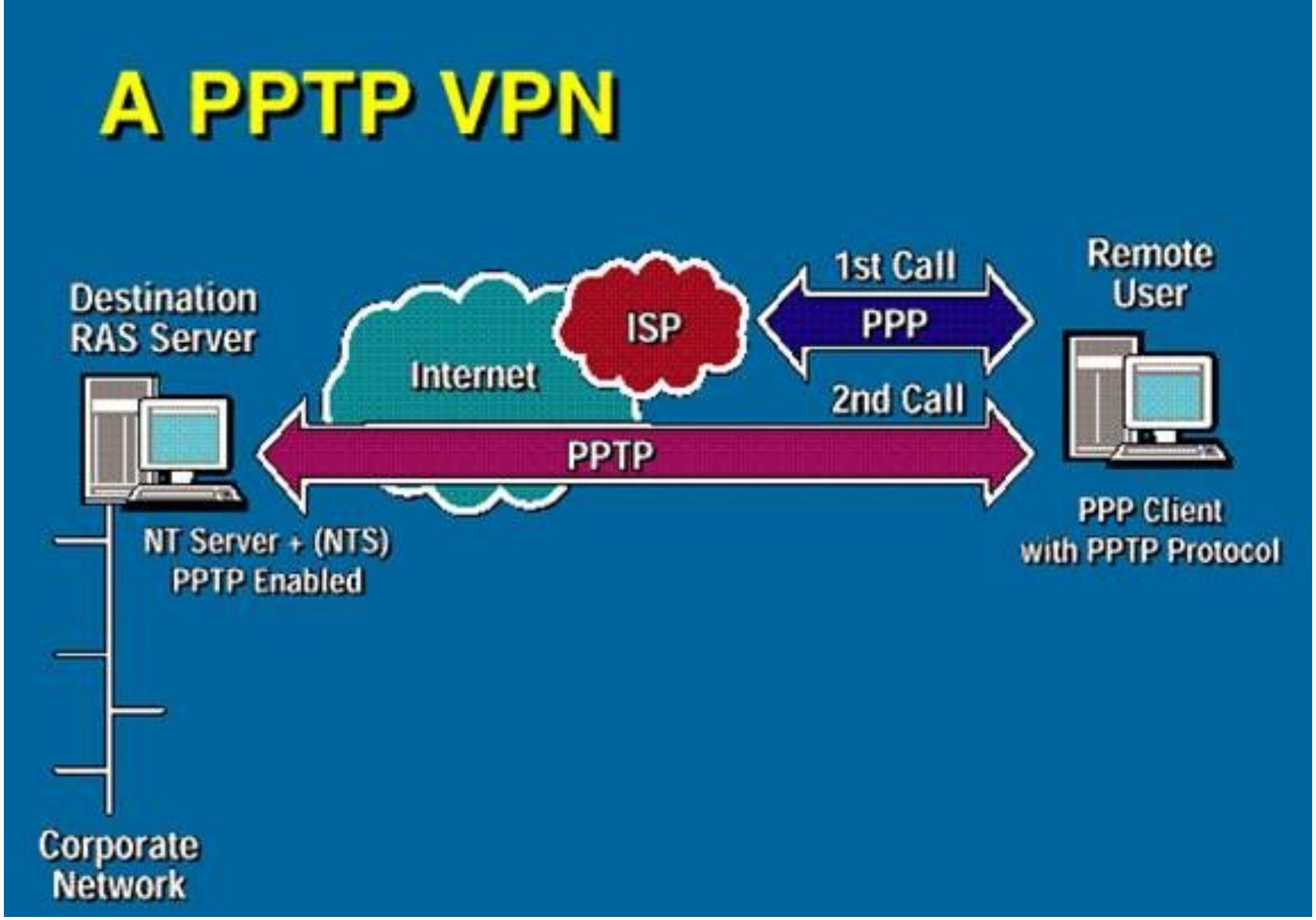
Тоннели


172.16.0.2
p-t-p
тоннель через внешнюю сеть
172.16.0.3
Laptop-PT
10.0.1.2
Server-PT
10.0.1.1
30.1.2.2
Router-PT
30.1.0.1
Router-PT
80.1.0.1
80.1.2.2
Server-PT
10.0.2.1
Laptop-PT
10.0.2.2
Switch-PT
Switch1
Switch-PT
Switch2
Router-PT
Router3
Laptop-PT
10.0.1.3
ИНТЕРНЕТ
Laptop-PT
10.0.2.3
Частная подсеть 1
Частная подсеть 2

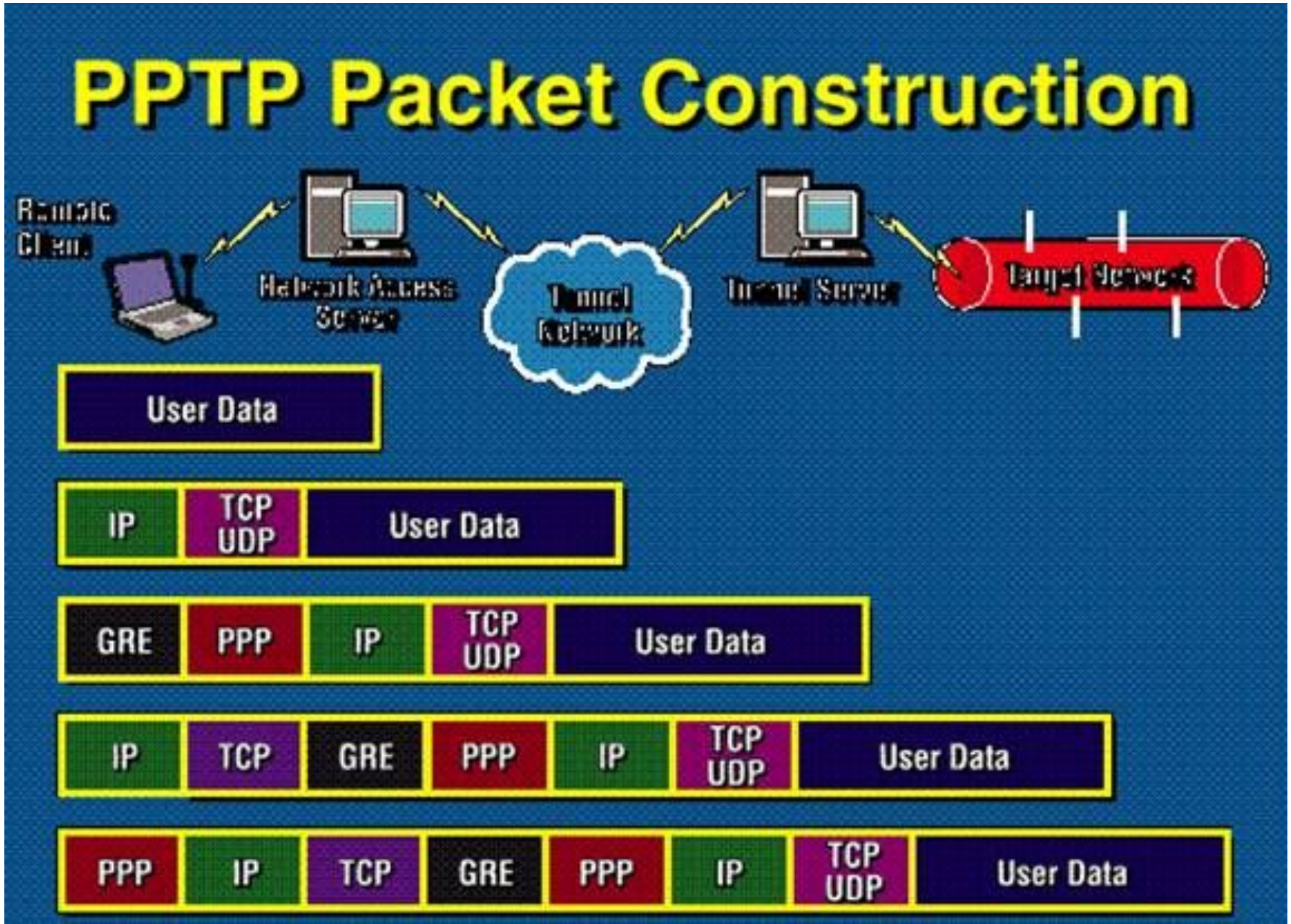
Основные протоколы используемые для построения сетевых туннелей:

- PPTP
- L2TP
- OpenVPN
- IPSec

PPTP



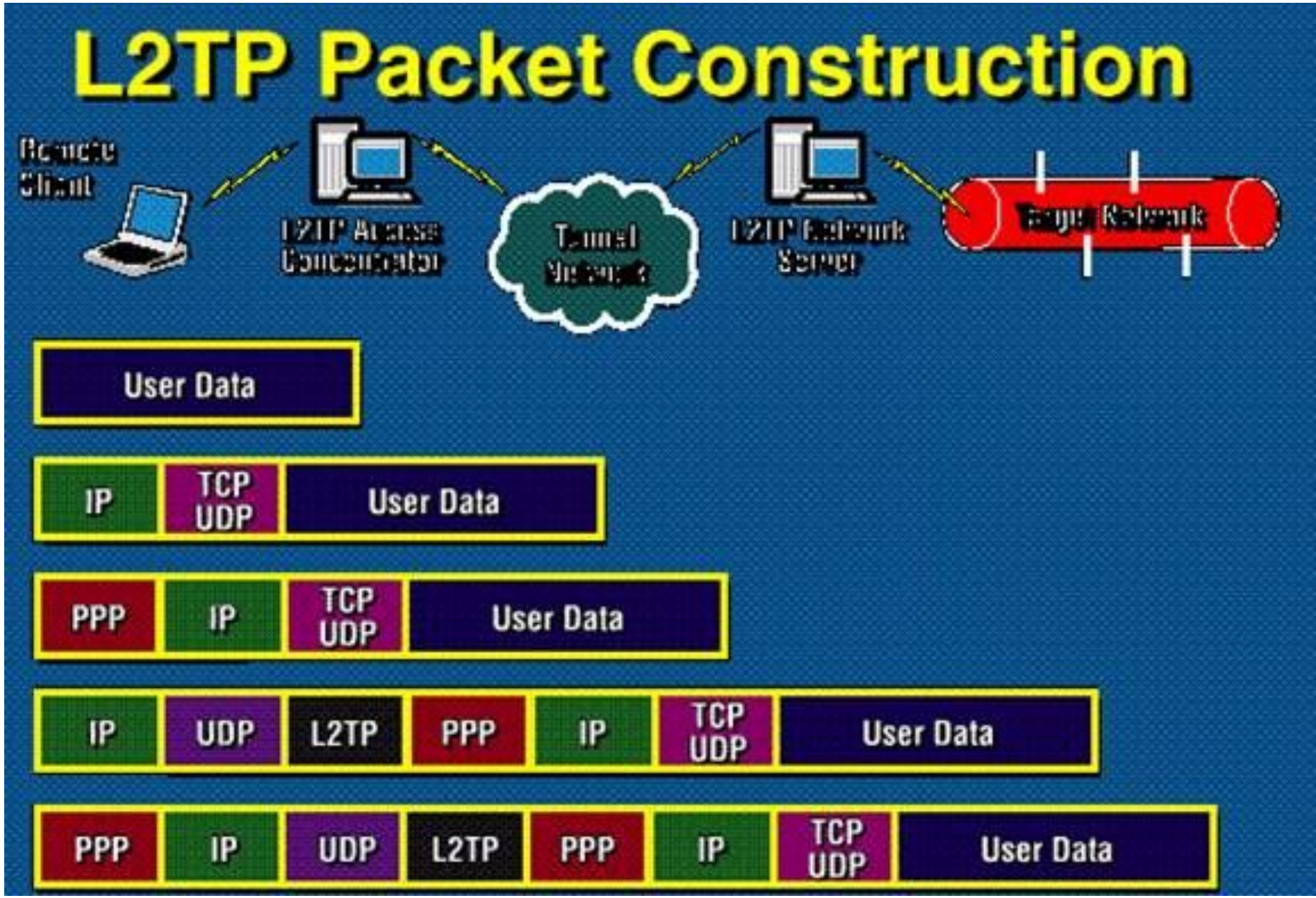
PPTP означает ‘Point-to-Point Tunneling Protocol’, протокол туннелирования "точка-точка".


PPTP Packet Construction
Remote Client
Network Access Server
Tunnel Network
Target Servers
User Data
IP
TCP UDP
User Data
GRE
PPP
IP
TCP UDP
User Data
IP
TCP
GRE
PPP
IP
TCP UDP
User Data
PPP
IP
TCP
GRE
PPP
IP
TCP UDP
User Data

OpenVPN

- Может использовать UDP или TCP для транспорта
- Может соединять сети на L2 (tap) и L3 (tun)
- Может управлять фрагментацией или использовать MTU для tun/tap
- Может использоваться для подключения офисов или удаленного доступа

L2TP


L2TP Packet Construction
User Data
IP
TCP
UDP
User Data
PPP
IP
TCP
UDP
User Data
IP
UDP
L2TP
PPP
IP
TCP
UDP
User Data
PPP
IP
UDP
L2TP
PPP
IP
TCP
UDP
User Data

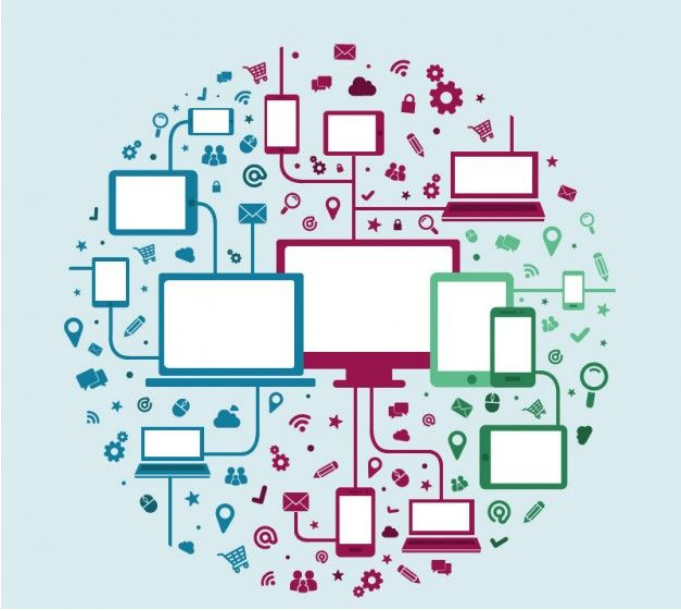
IPsec

IPsec sec наиболее широко используемый протокол для построения VPN.

IPsec является набором протоколов:

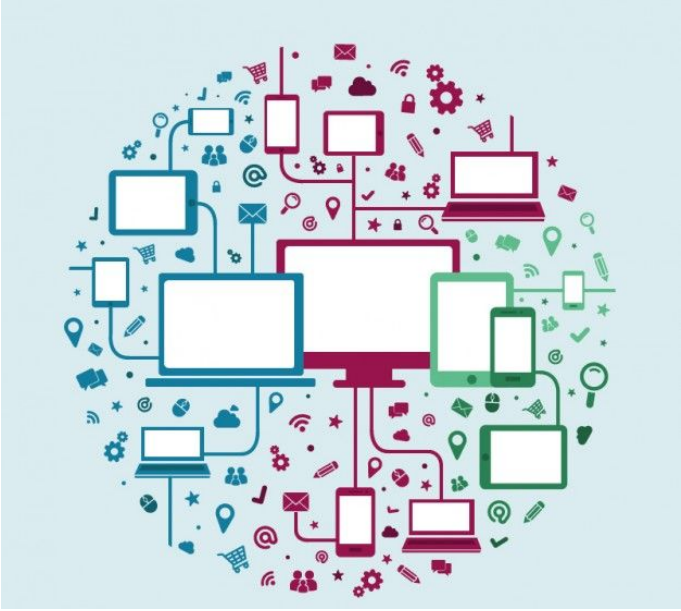
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Security Association and Key Management Protocol (ISAKMP)

Практическое задание



Работа в Wireshark и PT.

Вопросы



Не забудьте написать
отзыв о курсе и преподавателе