Основы компьютерных сетей. 6. Углубленное изучение сетевых технологий.

DNS. Сетевая безопасность. Шифрование. VPN

План занятия:

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

Domain Name Service

п·о·р	Основные протоколы TCP/IP по уровням модели OSI [скрыть]	
Прикладной	BGP • HTTP • DHCP • IRC • SNMP DNS NNTP • XMPP • SIP • BitTorrent • IPP • NTP • SNTP • RDP	
	Электронная почта	SMTP • POP3 • IMAP4
	Передача файлов	FTP • TFTP • SFTP
	Удалённый доступ	rlogin • Telnet
Представления	XDR • SSL	
Сеансовый	ADSP • H.245 • iSNS • NetBIOS • PAP • RPC • L2TP • PPTP • RTCP • SMPP • SCP • SSH • ZIP • SDP	
Транспортный	TCP • UDP • SCTP • DCCP • RUDP • RTP	
Сетевой	IPv4 • IPv6 • IPsec • ICMP • IGMP • ARP • RARP • RIP2 • OSPF	
Канальный	Ethernet • PPPoE • PPP • L2F • 802.11 Wi-Fi • 802.16 WiMax • Token ring • ARCNET • FDDI • HDLC • SLIP • ATM • DTM • X.25 • Frame relay • SMDS • STP	
Физический	Ethernet • RS-232 • EIA-422 • RS-449 • RS-485	

Domain Name System (DNS, система доменных имен) – определение IP-адреса компьютера по его доменному имени

- www.yandex.ru -> 77.88.55.66

DNS – распределенная система:

- Доменные зоны (корневой, верхний уровень, и т.д.)
- Серверы DNS

Распределение доменных имен

- Корневой регистратор ICANN
- Один или несколько аккредитованных регистраторов для зон верхнего уровня

Зачем нужен DNS?

Что это за сервер?

- 77.88.55.66
- 2a02:6b8:a::a
- www.yandex.ru

Система DNS позволяет преобразовывать имена компьютеров в IP-адреса

- www.yandex.ru -> 77.88.55.66

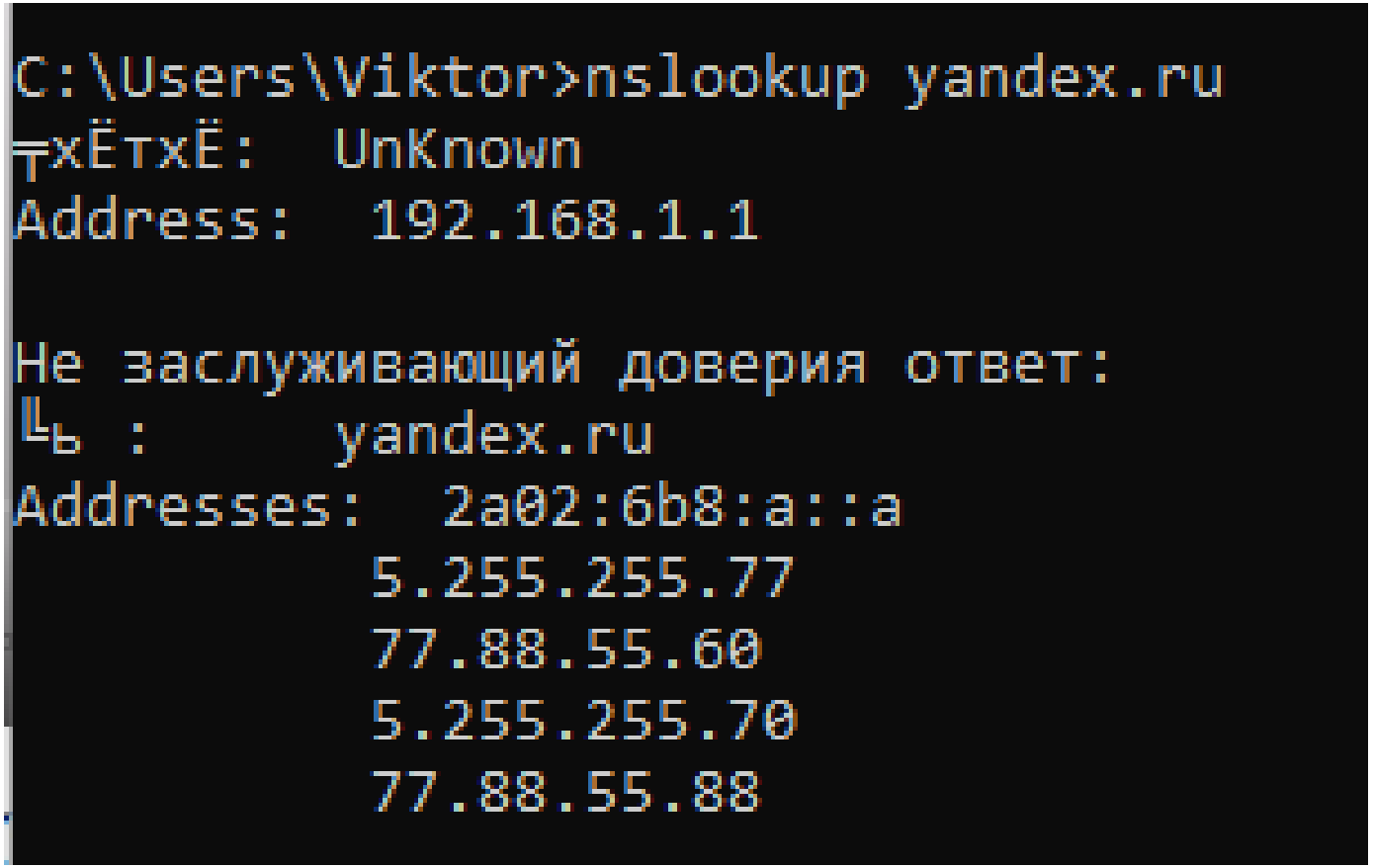
Преимущества DNS

- Понятные человеку имена
- Возможность менять сетевую инфраструктуру

DNS выполняет две основные задачи.

- Отвечает на запросы вида «какой IP принадлежит компьютеру с таким именем».
- Решает обратную задачу: «какое доменное имя принадлежит такому IP адресу».

nslookup



Linux: host, dig

Файл hosts

Файл содержит имена компьютеров их адреса

- Linux/Unix: /etc/hosts
- Windows: C:\Windows\System32\drivers\etc\hosts

Пример

```
102.54.94.97     server
38.25.63.10      my-client
```

Недостатки

- Быстро увеличивается размер
- Сложно вносить изменения
- Возможны конфликты имен

Linux: /etc/hosts

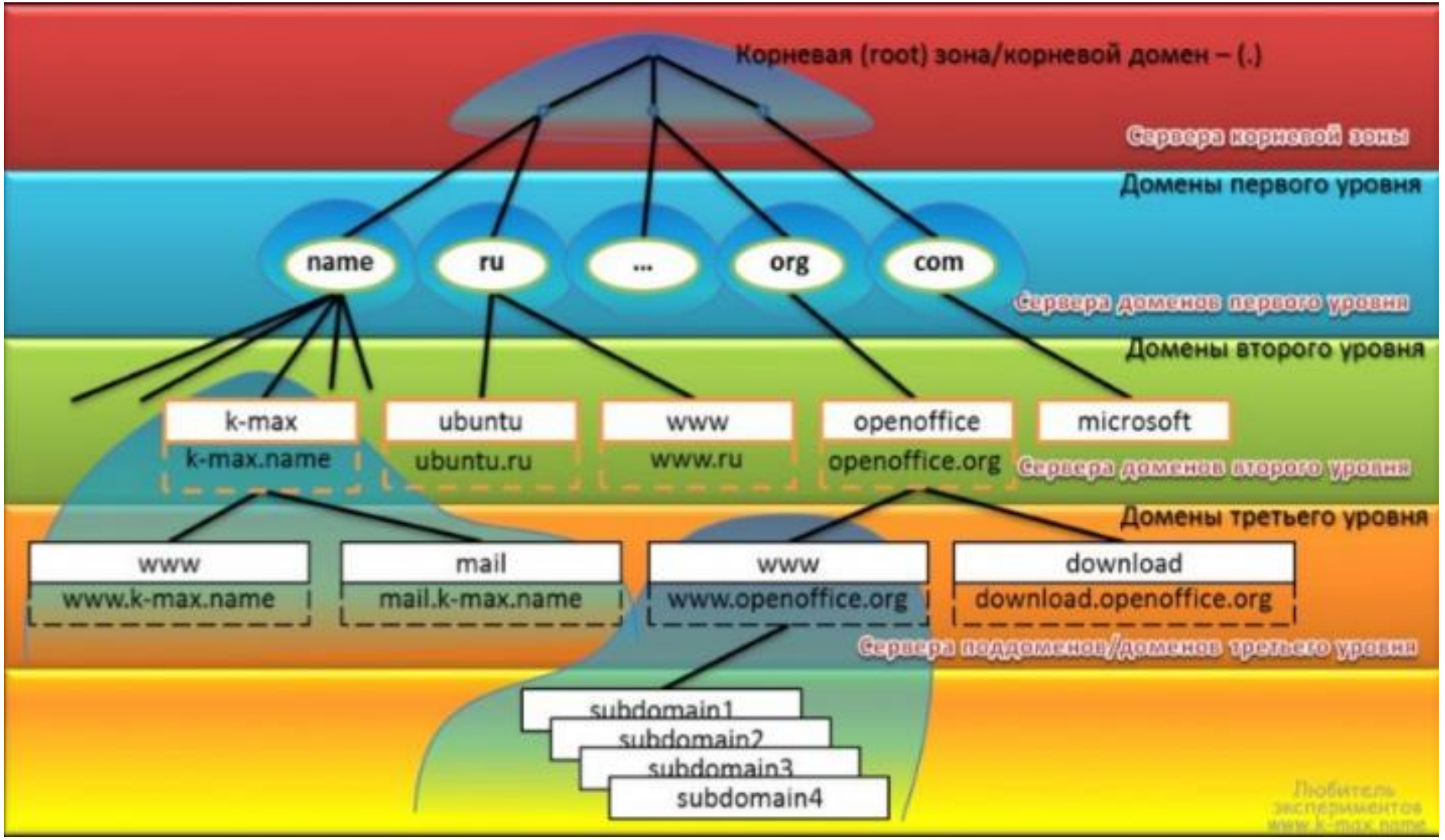
Структура доменного имени

Соглашение о доменах 1 уровня:

страна, тип организации

com – компании, edu – образование, org – организации, net – сетевые, gov – правительственные, mil – военные, arpa –выходит из употребления, сеть arpa
ru –Россия, ca – Канада, uk – Великобритания, au – Австралия и т.д.

Иерархическая структура DNS



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

Доменная зона

Доменное имя читается справа налево, начиная от корня.

Рассмотрим для примера доменное имя www.example.com.

Комментируем имя справа налево.

- . - корневой домен. Список из 13 серверов корневой зоны с их IP, есть на любом сервере DNS.
- .com — домен 1-го уровня (TLD Top Level Domain). Есть TLD общего пользования типа com и национальные домены по странам.
- example — домен 2-го уровня. Обычно это как раз то, что вы можете зарегистрировать и самостоятельно поддерживать.
- www — домен 3-го уровня или имя компьютера.

Доменная зона

Доменная зона — совокупность доменных имён определённого уровня, входящих в конкретный домен.

Корневая доменная зона содержит записи всех доменов 1-го уровня.

Доменная зона KZ содержит записи всех доменов 2-го уровня.

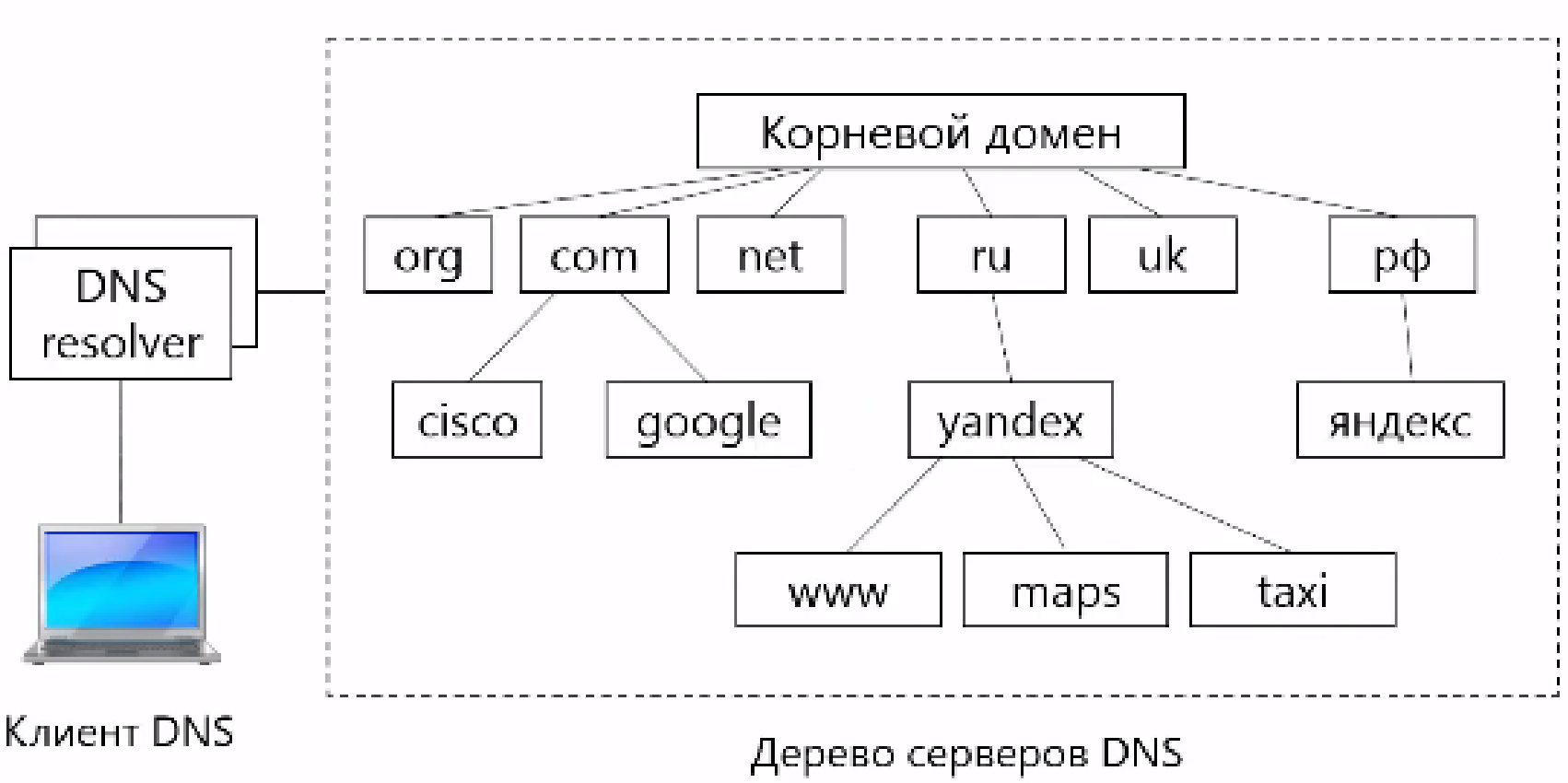
Доменная зона Yandex сдержит записи о поддоменах www, maps, taxi

И т.д.

Доменные зоны распределены по серверам DNS. Одну зону может обслуживать несколько серверов содержащих одинаковые записи.

Делегирование домена — это передача контроля над частью доменной зоны другой ответственной стороне.

Инфраструктура DNS



DNS resolver - сервер разрешения имен

Распределение доменных имен

Распределением доменных имен занимаются регистраторы

Регистратор корневого домена один

- Internet Corporation for Assigned Names and Numbers (ICAN)

Регистраторы зон первого уровня:

- Необходима аккредитация в ICANN
- Один или несколько регистраторов для каждой зоны
- Регистрируют домены второго уровня

Регистрация домена – платная услуга.

Ресурсные записи

Важной особенностью DNS является возможность содержать в зонах различные записи о доменных именах и часто их называют ресурсными записями.

Общая форма ресурсной записи:

name. TTL CLASS TYPE DATA

где

- name — доменное имя, которому «принадлежит» данная ресурсная запись либо IP адрес.
- TTL — срок хранения записи в кэше, с
- CLASS — всегда IN (INternet)
- TYPE — тип записи (A/CNAME/MX/PTR...)
- DATA — данные (зависит от TYPE)

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

Наиболее часто применяемые ресурсные записи

Запись A (Address Record): Эта запись устанавливает соответствие между доменным именем и IPv4-адресом. Она используется для преобразования доменного имени в числовой IP-адрес. Например, запись A может указывать, что домен example.com соответствует IP-адресу 192.0.2.100.

example.com. IN A 192.0.2.100

www.example.com. IN A 192.0.2.100

Запись AAAA (IPv6 Address Record): Эта запись аналогична записи A, но используется для преобразования доменного имени в IPv6-адрес.

example.com. IN AAAA 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Запись CNAME (Canonical Name Record): Запись CNAME создает псевдоним для доменного имени. Она позволяет одному домену ссылаться на другой домен. Например, если у вас есть домен www.example.com и вы хотите, чтобы он указывал на example.com, вы можете создать запись CNAME, указывающую на example.com.

www.example.com. IN CNAME example.com.

Наиболее часто применяемые ресурсные записи

Запись MX (Mail Exchanger Record): Эта запись определяет почтовый сервер, который обрабатывает электронную почту для домена. Она указывает, где должна быть доставлена почта, отправленная на адреса с этим доменом.

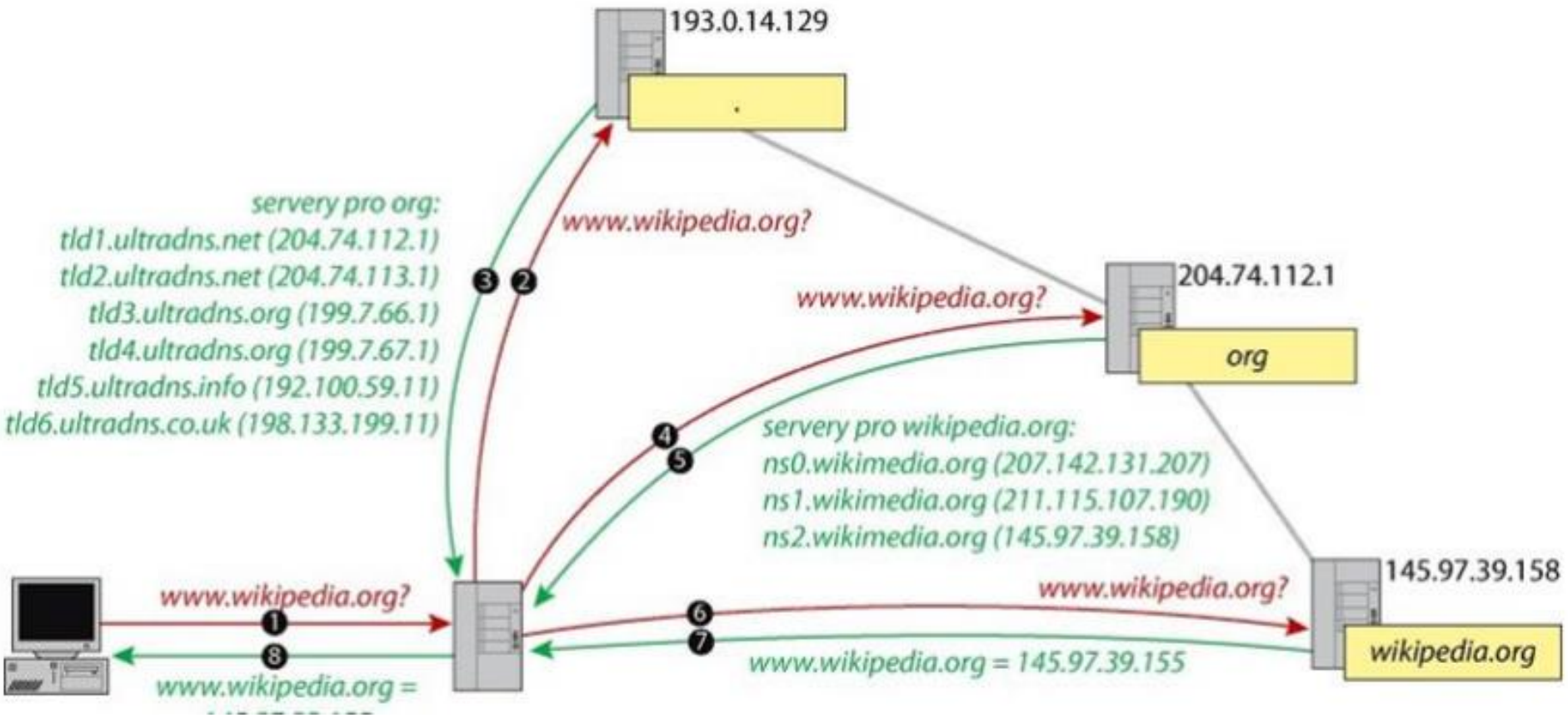
example.com. IN MX 10 mail.example.com.

Запись NS (Name Server Record): Запись NS указывает на DNS-серверы, ответственные за управление зоной домена. Она определяет авторитетные серверы, которые могут предоставлять информацию о домене.

example.com. IN NS ns1.example.com.

example.com. IN NS ns2.example.com.

Разрешение доменного имени



Процесс разрешения доменного имени

1.Клиентский компьютер обращается к локальному DNS-серверу с запросом: получить IP-адрес для доменного имени www.wikipedia.org.

2. Локальный DNS, не обнаружив данные по запросу в своем кеше, выполняет процедуру разрешения с одного из корневых серверов (193.0.14.129). Адрес корневого сервера берется из специального файла со списком корневых серверов. Итак, на корневой сервер также отправляется запрос ресурсной записи типа A для www.wikipedia.org.

3. Корневой DNS имеет только записи о делегировании доменов первого уровня, поэтому он в ответ на запрос выдает локальному DNS список DNS-серверов, отвечающих за домен .org.

4. Локальный DNS повторяет запрос на этот раз одному из DNS домена .org (204.74.112.1) из списка, который ему вернул корневой DNS.

5. 204.74.112.1 также не имеет в своих зональных файлах ресурсной записи для имени www.wikipedia.org, поскольку домен wikipedia.org делегирован. Поэтому в ответ на запрос сервер выдает список серверов, отвечающих за зону wikipedia.org, в которой находится запрашиваемое имя.

6. Локальный DNS вновь повторяет запрос для имени www.wikipedia.org одному из DNS (145.97.39.158), отвечающих за wikipedia.org из списка, полученного на предудущем шаге. © geekbrains.ru 62

7. 145.97.39.158 находит адрес для www.wikipedia.org в своем зональном файле и возвращает его нашему локальному DNS.

8. Локальный DNS возвращает клиенту адрес 145.97.39.155 для имени www.wikipedia.org.

Обратное разрешение.

Обратное разрешение (Reverse DNS) - это процесс преобразования IP-адреса обратно в доменное имя. В отличие от прямого разрешения, которое преобразует доменное имя в IP-адрес, обратное разрешение выполняет обратную операцию.

Обратное разрешение основано на специальной зоне домена, называемой обратной зоной (reverse zone) или зоной PTR (Pointer Record). В этой зоне содержатся записи PTR, которые связывают IP-адреса с соответствующими доменными именами.

Обратное разрешение.

Процесс обратного разрешения обычно используется для различных целей, включая:

Проверка подлинности: Обратное разрешение может использоваться для проверки подлинности отправителя электронной почты. При получении сообщения почтовый сервер может выполнить обратное разрешение IP-адреса отправителя и проверить, соответствует ли полученное доменное имя ожидаемому имени сервера.

Безопасность и отладка: Обратное разрешение может помочь в идентификации и отслеживании сетевых проблем или потенциальных угроз. Например, при анализе логов сетевых устройств или при обнаружении подозрительной активности можно использовать обратное разрешение для определения доменных имен, связанных с конкретными IP-адресами.

Обратное разрешение.

Пример записи в обратной зоне (зоне PTR).

В данном примере IP-адрес 192.0.2.100 связан с доменным именем example.com. При выполнении обратного разрешения для этого IP-адреса будет возвращено доменное имя example.com.

```
100.2.0.192.in-addr.arpa. IN PTR example.com.
```

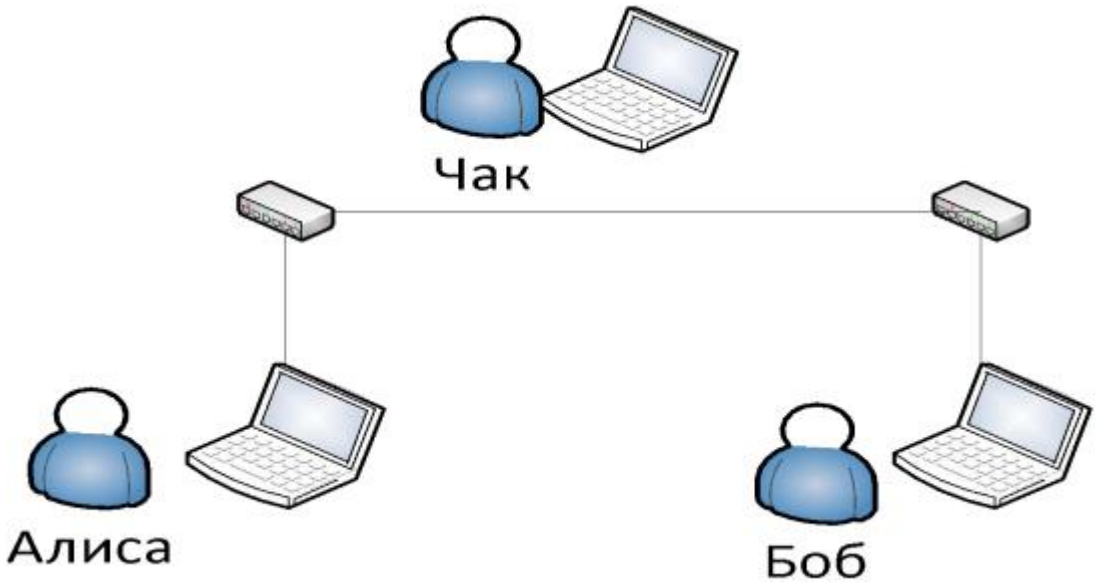
Сетевая безопасность

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



Определения

Аутентификация - это процесс проверки подлинности идентификационных данных пользователя или системы, чтобы убедиться, что представленные данные соответствуют ожидаемым или разрешенным учетным данным.

Авторизация - это процесс проверки прав доступа пользователя или системы к определенным ресурсам, функциям или операциям.

Шифрование - это процесс преобразования данных с использованием алгоритма шифрования, чтобы сделать их непонятными или недоступными для неавторизованных лиц.

Конфиденциальность - это принцип и состояние информации, которое означает, что доступ к этой информации ограничен только авторизованным пользователям или системам, которым разрешен доступ.

Определения

Целостность - это свойство данных или системы, которое обеспечивает их неприкосновенность, точность и непротиворечивость. Целостность данных означает, что данные не были изменены незаконно, случайно или неправильно во время хранения, передачи или обработки.

Доступность - это состояние, в котором информационные ресурсы или системы доступны и функционируют в течение необходимого времени и с необходимой производительностью для авторизованных пользователей.

Несанкционированный доступ, также известный как неавторизованный доступ или хакерский доступ, означает получение доступа к информационной системе, данным или ресурсам без разрешения или авторизации со стороны владельца или уполномоченного лица.

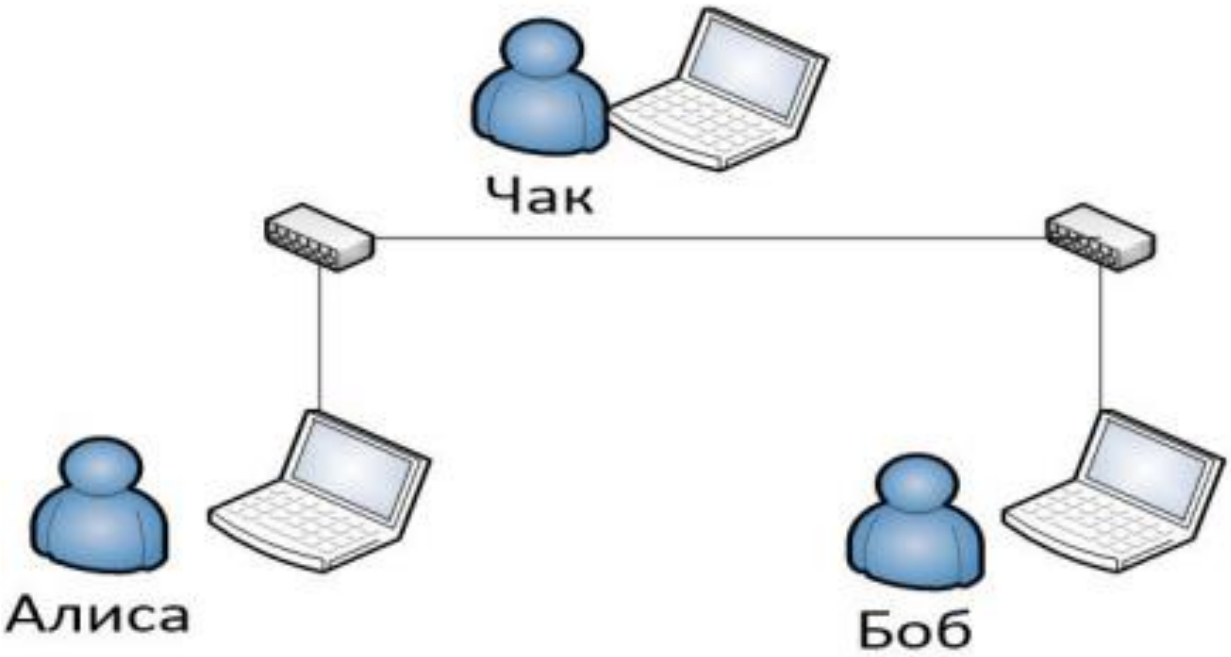
Шифрование

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

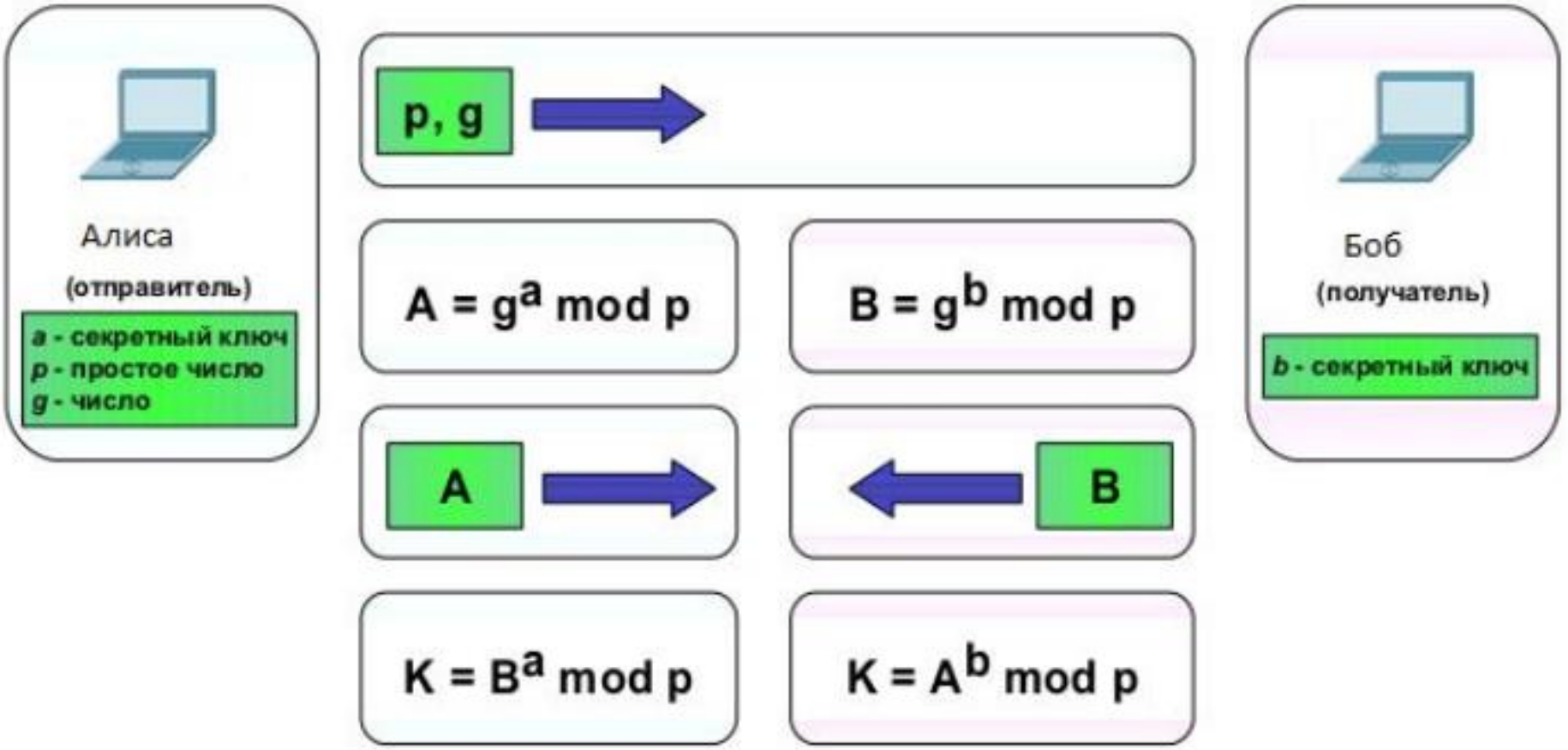
Ассиметричные алгоритмы шифрования:

- RSA
- DSA
- ГОСТ Р 34.10-2001

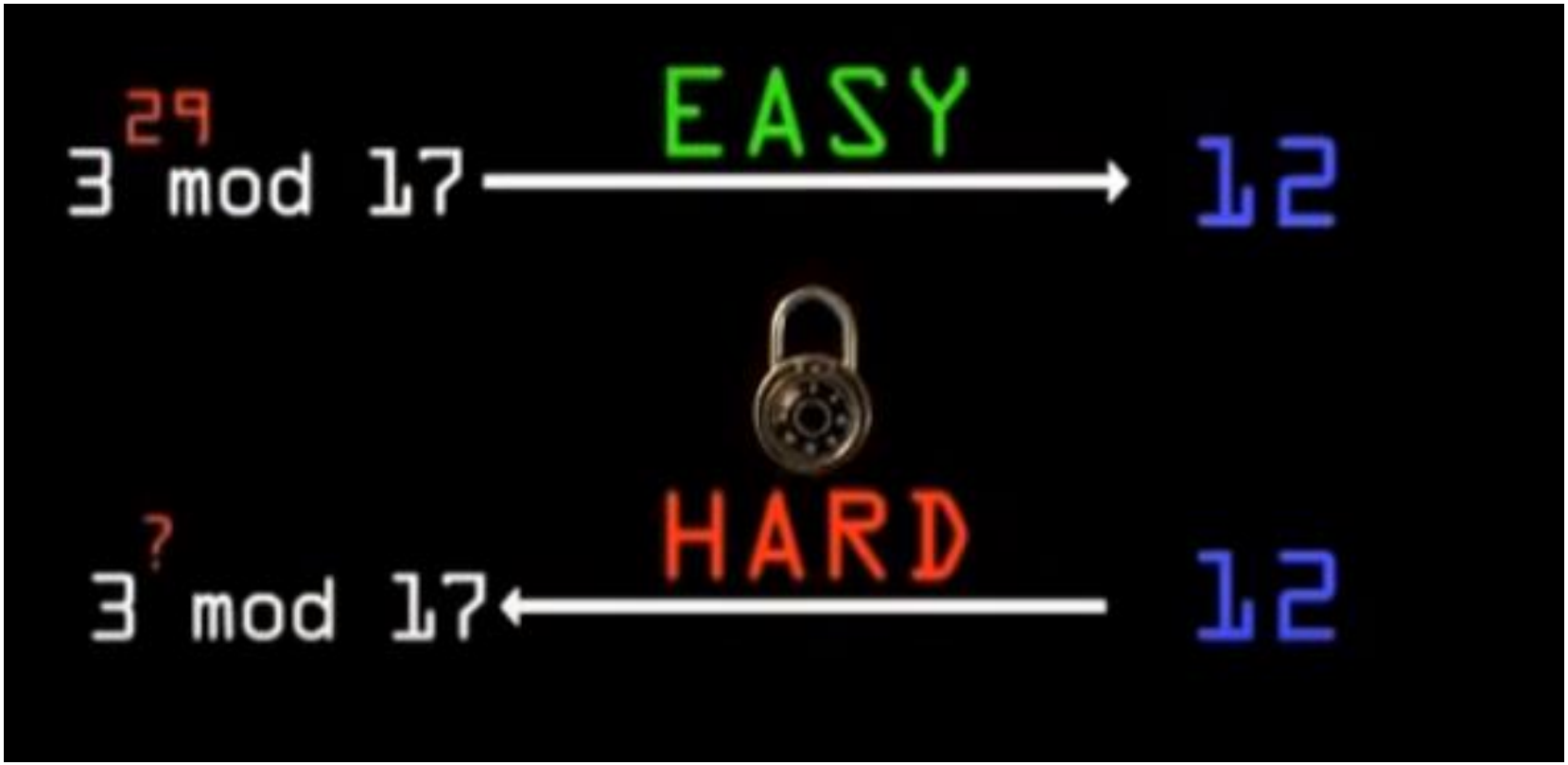
Симметричные алгоритмы шифрования:

- 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



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


29
3 mod 17
EASY
12
HARD
?
3 mod 17
12

RSA (Rivest, Shamir и Adleman)

RSA использует пару ключей - открытый ключ и секретный ключ.

Открытый ключ используется для шифрования данных, а секретный ключ используется для расшифровки зашифрованных данных.

При этом обеспечивается свойство неразрывности: данные, зашифрованные с использованием открытого ключа, могут быть расшифрованы только с помощью соответствующего секретного ключа.

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

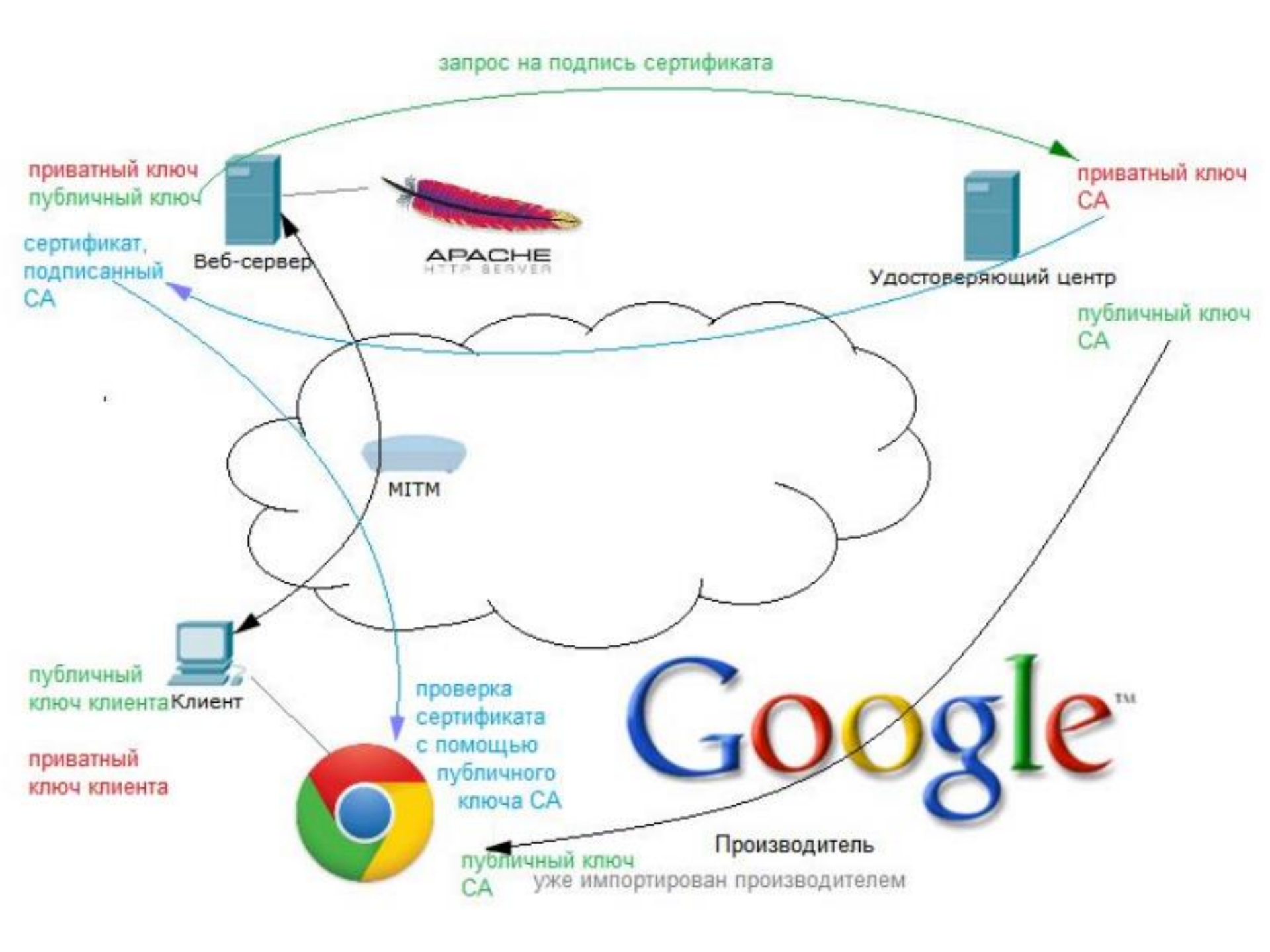
SSL (Secure Socket Layer)

- 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 2.0была выпущена в феврале 1995 года, но содержала много недостатков по безопасности, которые привели к разработке SSL версии 3.0.

TLS

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

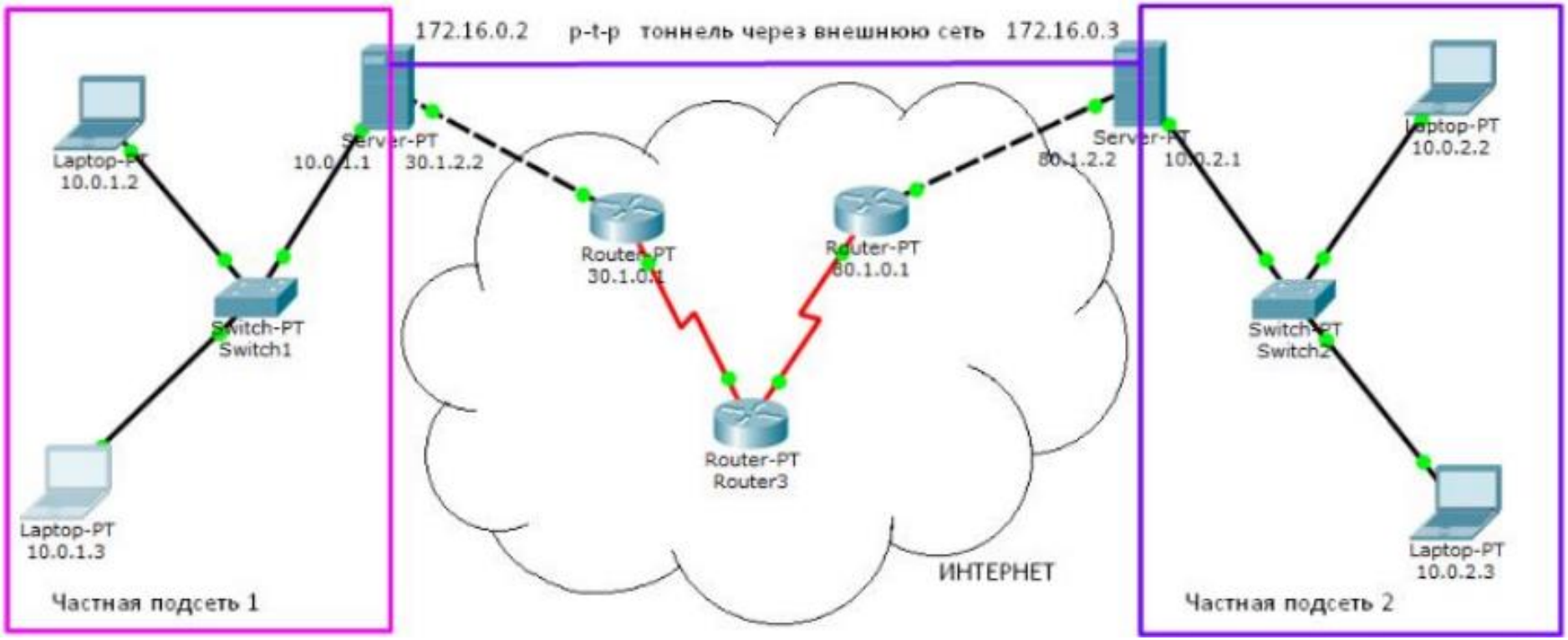
Основанная на сфере применения：

- 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

Сетевой туннель - это механизм, который позволяет создать виртуальный приватный канал внутри уже существующей сети или по сети, чтобы обеспечить безопасную и зашифрованную передачу данных между двумя узлами или сетями.

Туннельные протоколы используются для создания и управления сетевыми туннелями.

Когда данные проходят через сетевой туннель, они обертываются (или "запаковываются") в дополнительный слой протокола, который обеспечивает безопасность, шифрование и целостность данных.

Это позволяет передавать данные через незащищенные или неприемлемые сети, такие как общедоступный интернет, с минимальным риском их перехвата, изменения или несанкционированного доступа.

Основные протоколы используемые для построения сетевых туннелей:

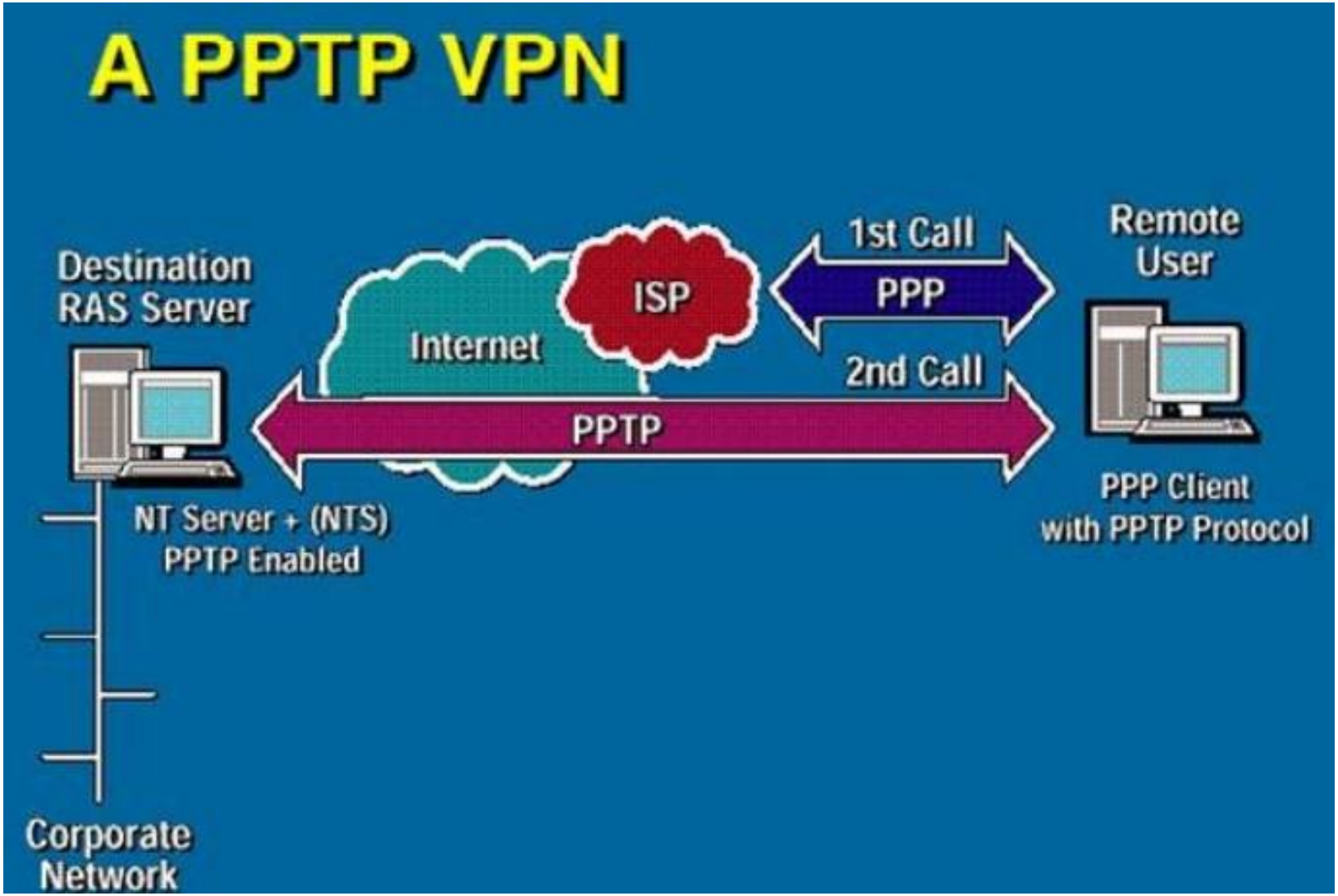
- PPTP
- L2TP
- OpenVPN
- IPSec
- GRE

GRE (Generic Routing Encapsulation) - это протокол сетевого туннелирования, который используется для создания виртуальных частных сетей (VPN) или для установления соединений между удаленными сетями через общедоступные сети, такие как интернет.

Протокол GRE добавляет дополнительный заголовок к оригинальному IP-пакету, оборачивая его в новый пакет. Это позволяет передавать пакеты через сеть, которая не распознает или не поддерживает протокол GRE, так как оригинальный IP-пакет остается неприкосновенным внутри обертки GRE.

Протокол GRE является простым и гибким, и он широко поддерживается различными устройствами и операционными системами. Однако он не обеспечивает нативное шифрование или проверку подлинности данных.

PPTP



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

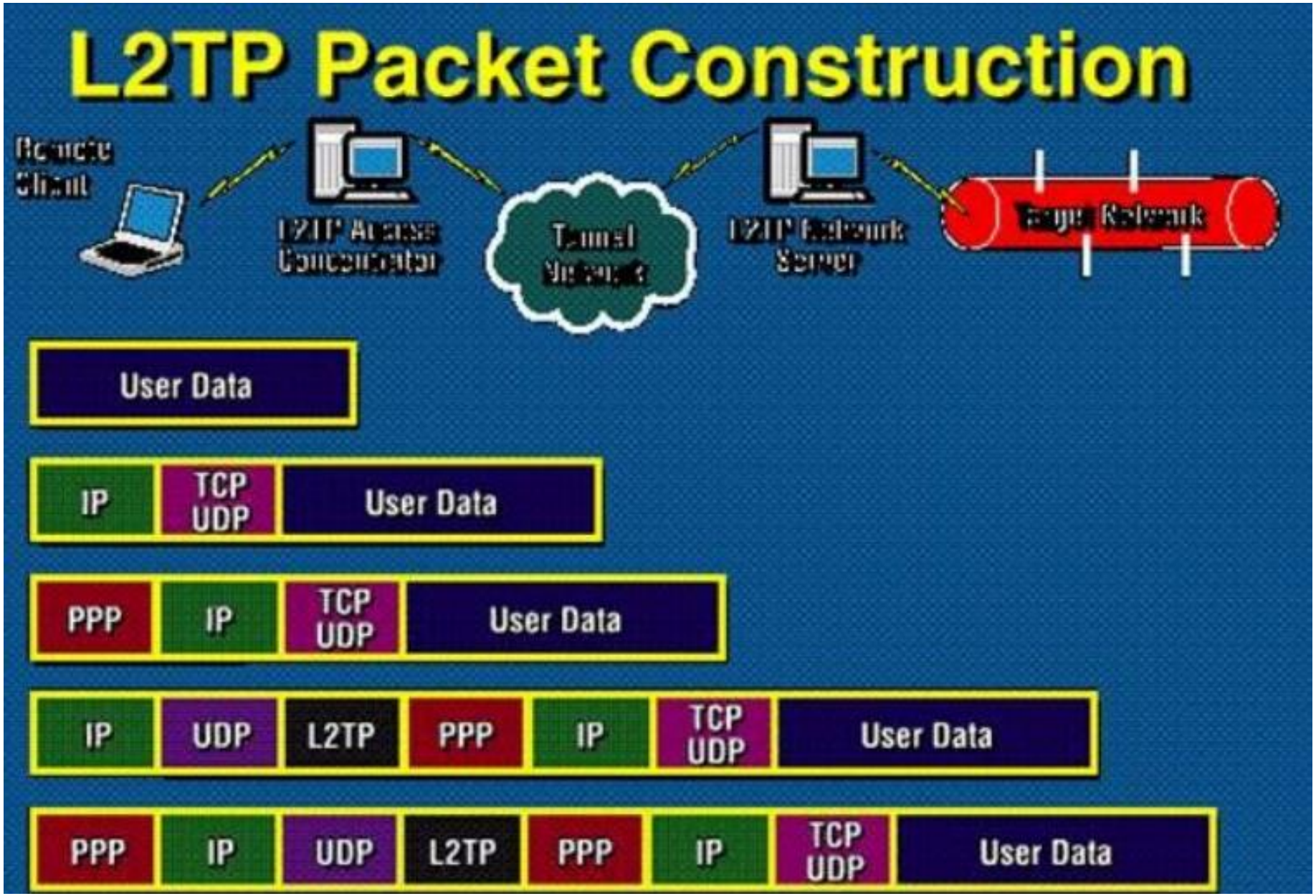
PPTP Packet Construction

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

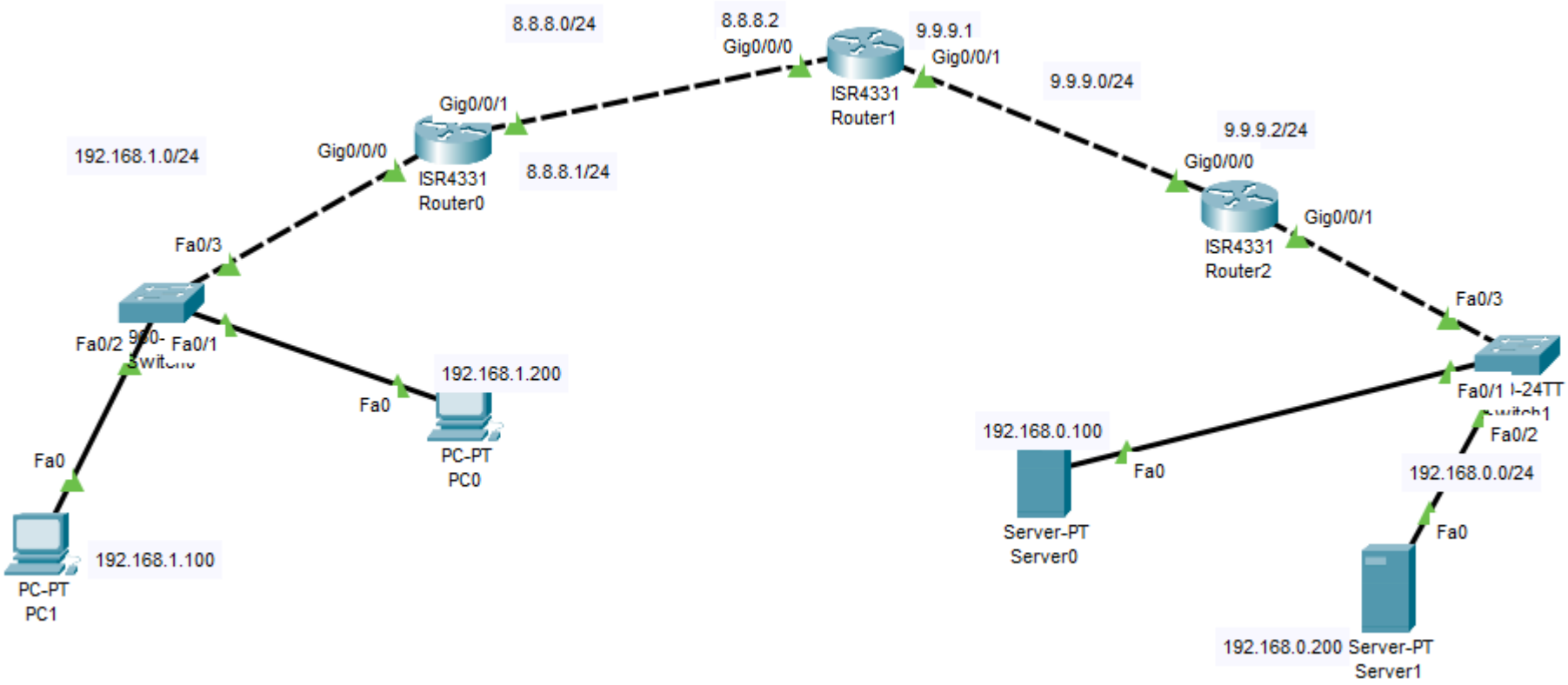
IPsec

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)

Практика. Туннели.



TUNNEL

```
//router0
Router#conf t
Router(config)#interface tunnel 0  // интерфейс – туннель №0
Router(config-if)#tunnel ?
  destination  destination of tunnel
  mode         tunnel encapsulation method
  source       source of tunnel packets
Router(config-if)#tunnel source gigabitEthernet 0/0/1  // начало туннеля
Router(config-if)#tunnel destination 9.9.9.2  // конечная точка туннеля
Router(config-if)#tunnel mode gre ip  // протокол
Router(config-if)#ip address 172.16.0.1 255.255.255.252  //ip-адрес интерфейса
Router#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
…
Tunnel0                172.16.0.1      YES manual up                    up
Router#
```

TUNNEL

//router2

Router>en

Router#conf t

Router(config)#int tunnel 0

Router(config-if)#tunnel source gigabitEthernet 0/0/0

Router(config-if)#tunnel destination 8.8.8.1

Router(config-if)#tunnel mode gre ip

Router(config-if)#ip address 172.16.0.2 255.255.255.252

Router#show ip int br

Interface IP-Address OK? Method Status Protocol

…

Tunnel0 172.16.0.2 YES manual up up

Router#ping 172.16.0.1

..!!!

TUNNEL

// Настраиваем маршрут через туннель

//router0

Router(config)#ip route 192.168.0.0 255.255.255.0 172.16.0.2

Router#show ip route

…

S 192.168.0.0/24 [1/0] via 172.16.0.2

//router2

Router(config)#ip route 192.168.1.0 255.255.255.0 172.16.0.1

Router#show ip route

…

S 192.168.1.0/24 [1/0] via 172.16.0.1

TUNNEL

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.100: bytes=32 time=1ms TTL=126
Reply from 192.168.0.100: bytes=32 time=12ms TTL=126
Reply from 192.168.0.100: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 8ms

C:\>
```