TLS/SSL

1. СЪЩНОСТ

- Предоставя сигурност в комуникацията в незащитена инфраструктура
- Надгражда TCP
- TLS (transport layer security)
- SSL (secure socket layer)
- HTTPS
- TLS 1.2
- Цели:
  - Сигурност
  - Оперативна съвместимост
  - Възможност за разширение
  - Работоспособност

1. СЪЩНОСТ

- Дели се на 4 под-протокола
- Всеки под-протокол си има специфични задължения
  - Протокол запис
  - Протокол за ръкостискане (handshake protocol)
  - Шифърни спецификации проткол (cipher spec protocol)
  - Протокол на приложението (application data protocol)
  - Протокол при тревога.

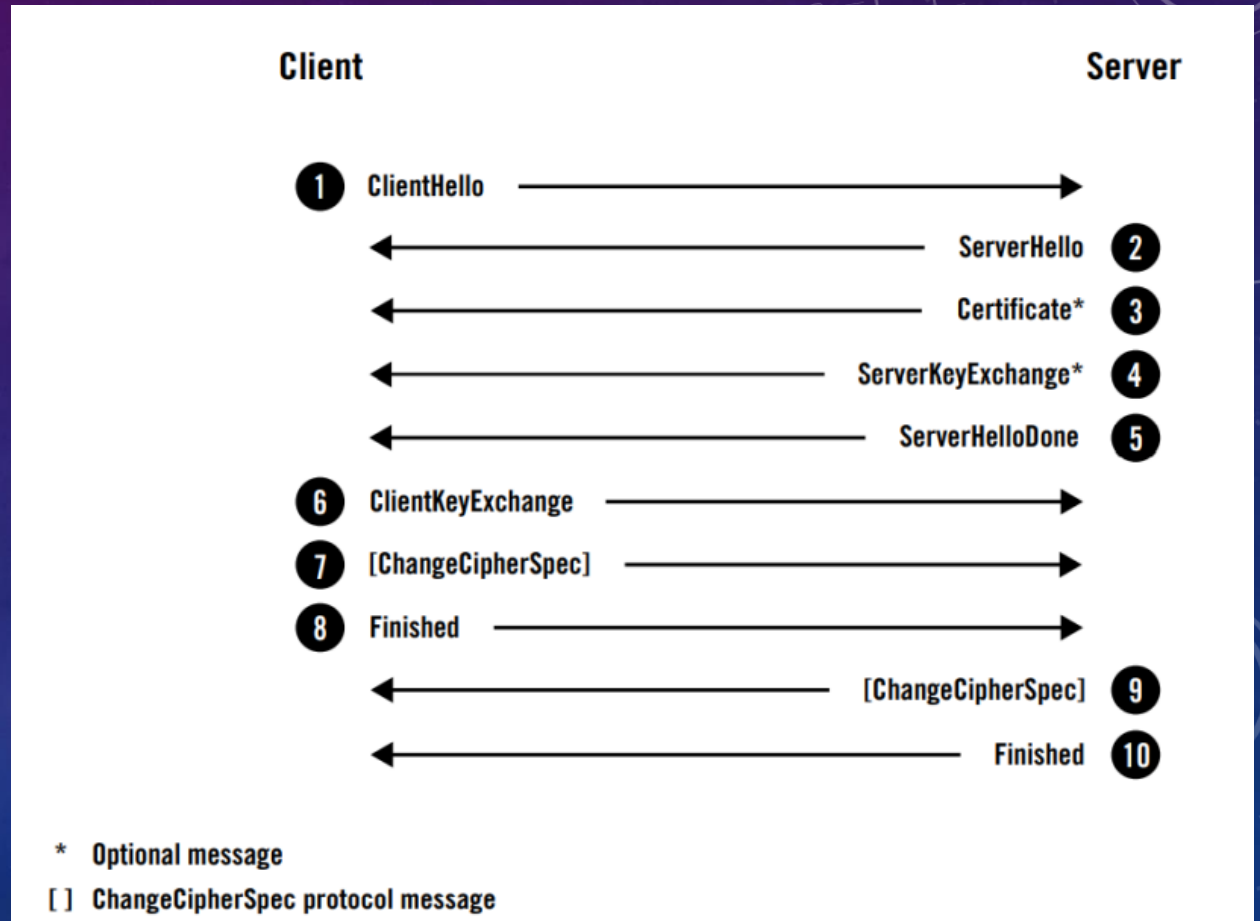
2. ПРОТОКОЛ ЗАПИС

- Криптиране
- Компресия
- Възможност за разширяване

Фиг. 1 – структура на Record съобщението

3. ПРОТОКОЛ ЗА РЪКОСТИСКАНЕ

- Четири стъпки
  - Размяна на възможностите и определяне на параметрите на връзката
  - Валидация на представеният сертификат или друг метод на автентикация
  - Съгласие да се ползва тайна (secret) за защита на сесията
  - Проверка че съобщенията за ръкостискане не са били променени от 3та страна



Фиг. 4 – пълно ръкостискане с автентикация на сървъра

3. ПРОТОКОЛ ЗА РЪКОСТИСКАНЕ

```
Handshake protocol: ClientHello
    Version: TLS 1.2
    Random
        Client time: May 22, 2030 02:43:46 GMT
        Random bytes: b76b0e61829557eb4c611adfd2d36eb232dc1332fe29802e321ee871
    Session ID: (empty)
    Cipher Suites
        Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
        Suite: TLS_RSA_WITH_AES_128_GCM_SHA256
        Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
        Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
        Suite: TLS_RSA_WITH_AES_128_CBC_SHA
        Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA
        Suite: TLS_RSA_WITH_RC4_128_SHA
    Compression methods
        Method: null
    Extensions
        Extension: server_name
            Hostname: www.feistyduck.com
        Extension: renegotiation_info
        Extension: elliptic_curves
            Named curve: secp256r1
            Named curve: secp384r1
        Extension: signature_algorithms
            Algorithm: sha1/rsa
            Algorithm: sha256/rsa
            Algorithm: sha1/ecdsa
            Algorithm: sha256/ecdsa
```

```
Handshake protocol: ServerHello
        Version: TLS 1.2
        Random
                Server time: Mar 10, 2059 02:35:57 GMT
                Random bytes: 8469b09b480c1978182ce1b59290487609f41132312ca22aacaf5012
        Session ID: 4cae75c91cf5adf55f93c9fb5dd36d19903b1182029af3d527b7a42ef1c32c80
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        Compression method: null
        Extensions
                Extension: server_name
                Extension: renegotiation_info
```

4. ОБМЕН НА КЛЮЧОВЕ

- 48 битов споделен ключ наречен главна тайна (master secret)
- Цел: Генериране основна тайна (premaster secret)
- ServerKeyExchange, ClientKeyExchange
- Изпращат се параметри
- Оционална сигнатура

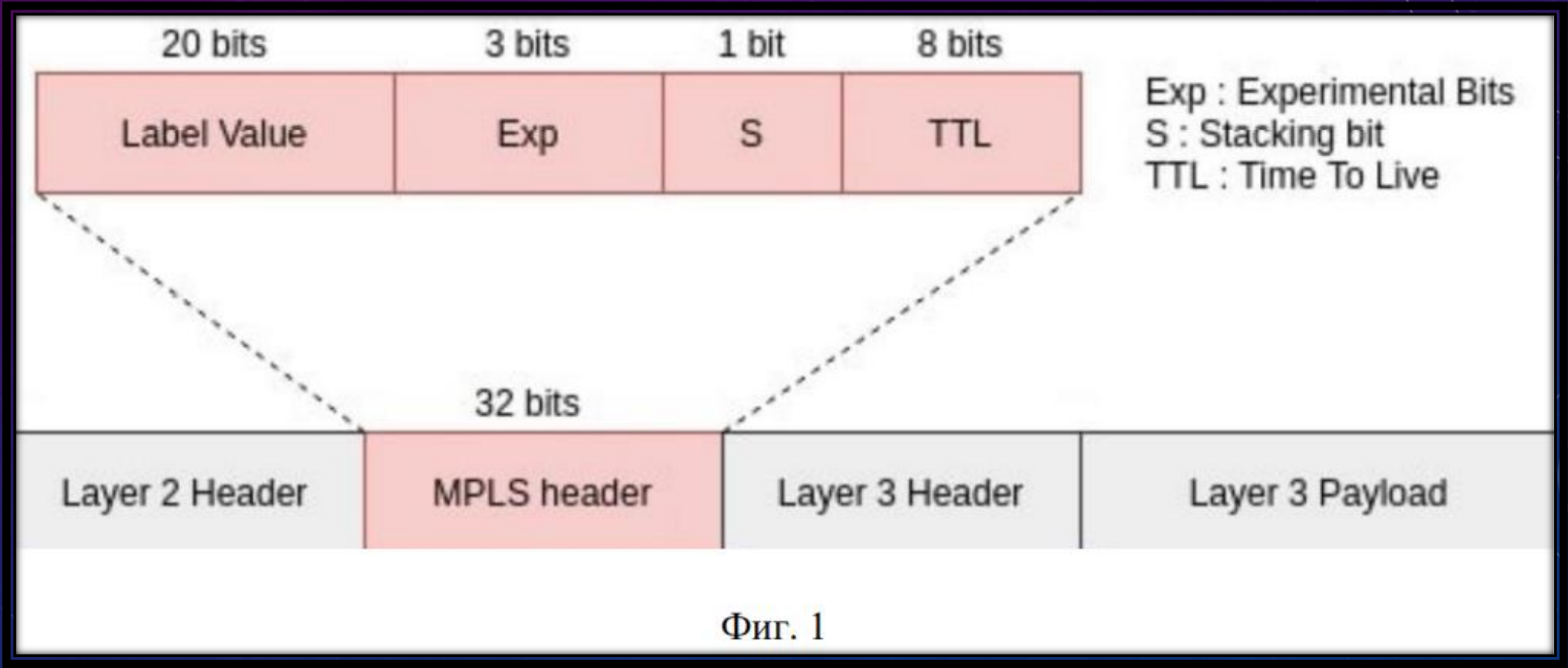
4. ОБМЕН НА КЛЮЧОВЕ

- RSA алгоритъм за обмен на ключове
  - 46 байтово произволно число
  - ClientKeyExchange
- Diffie-Hellman алгоритъм за обмен на ключове
  - математическа функция която не може да се обърне
  - Използват се двете KeyExchange съобщения
- Автентикация
  - Implicit
  - Сигнатура в ServerKeyExchange

5. КРИПТИРАНЕ

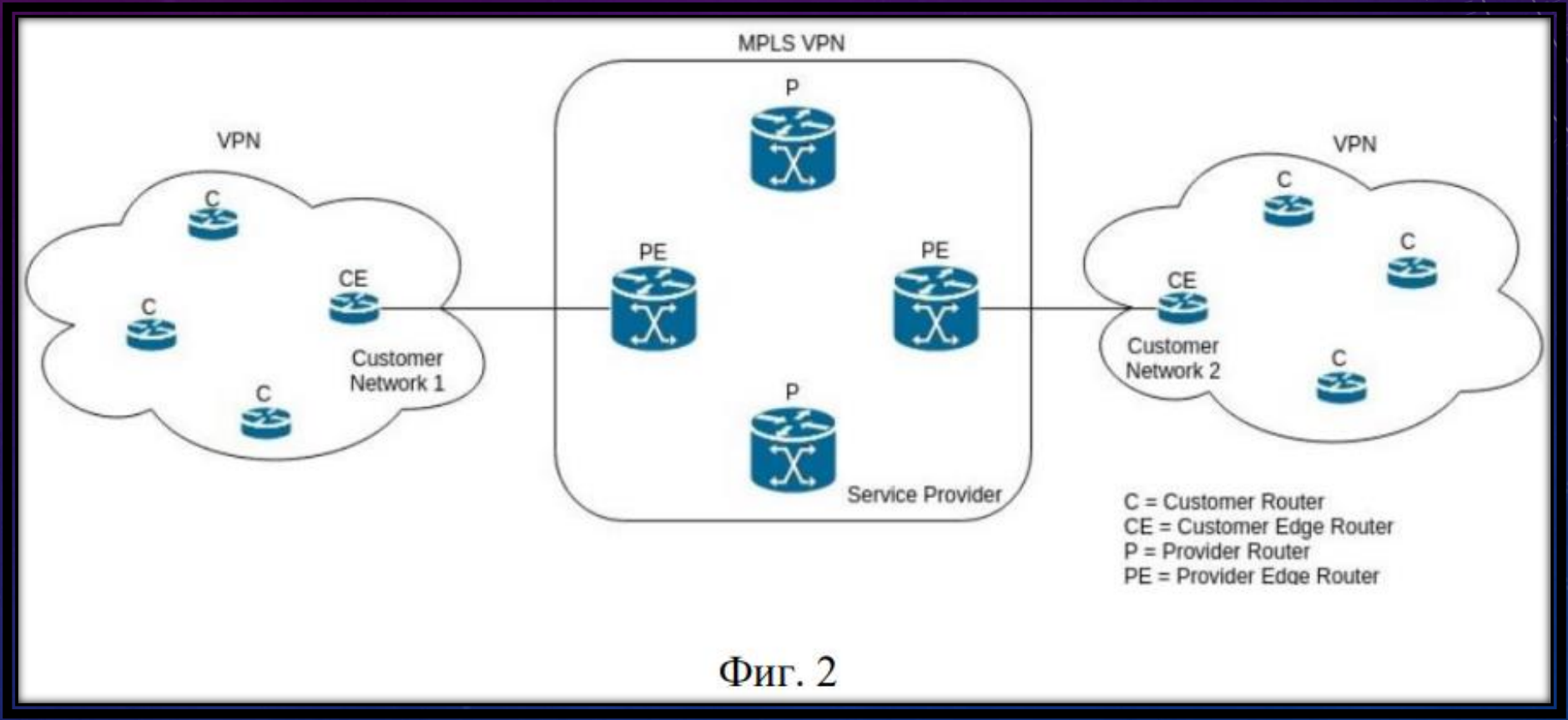
- поддържа много алгоритми и методи да криптиране на информация
- Поточно криптиране
- Боково криптиране

2. MPLS L3VPN



Фиг. 1

2. MPLS L3VPN

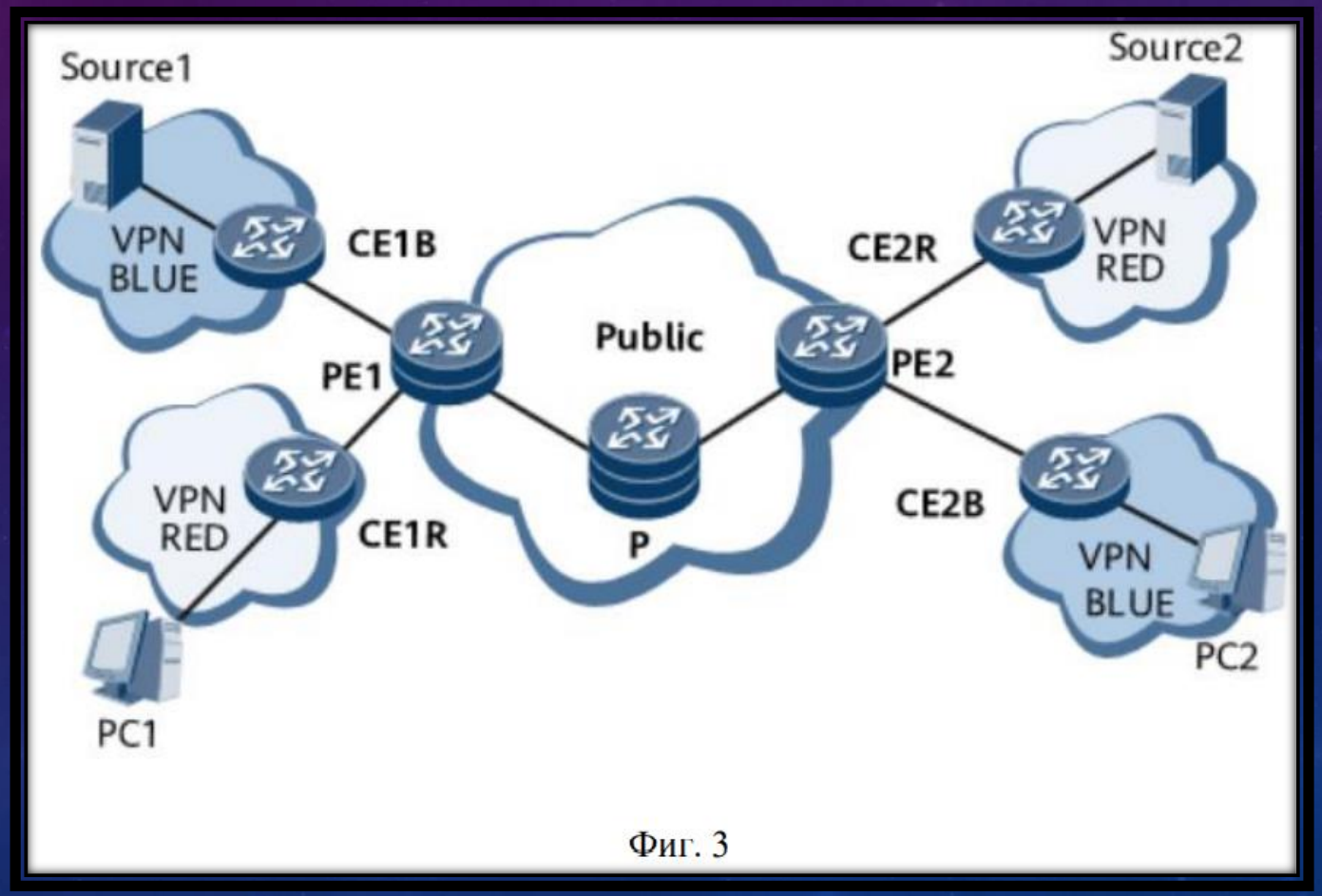


Фиг. 2

3. Rosen MVPN

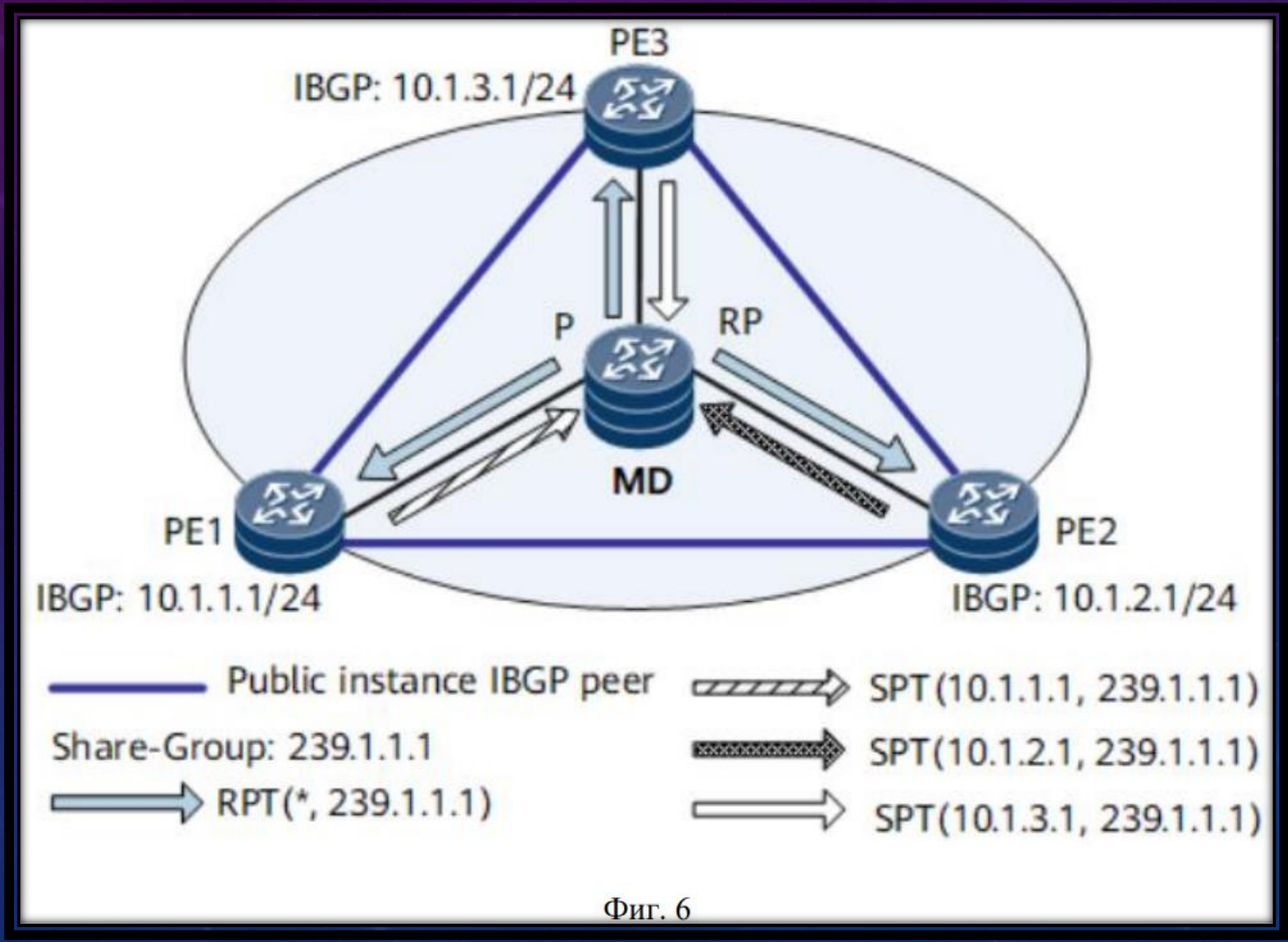
- Мултикаст домейн MD (multicast domain)
- Обща-група
- мултикаст тунел MT (Multicast Tunnel)
- Интерфейс на мултикаст тунела MTI (Multicast Tunnel Interface)
- VPN инстанции
- P-PIM (Provider PIM) и C-PIM (Customer PIM)
- Multicast Distribution Tree MDT
- share-MDT (shared Multicast Distribution Tree)

3. Rosen MVPN



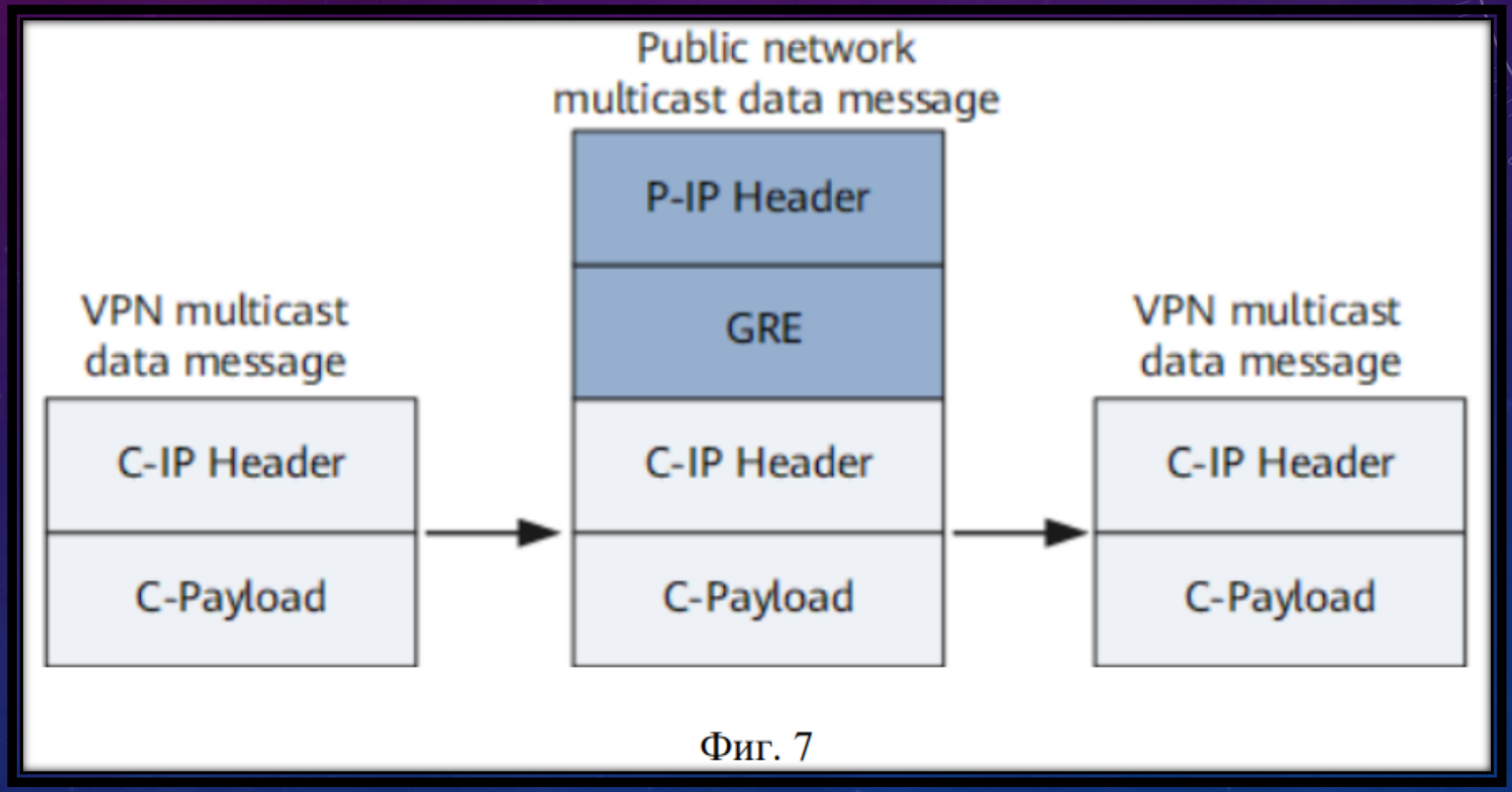
Фиг. 3

3. Rosen MVPN



Фиг. 6

3. Rosen MVPN



Фиг. 7

БЛАГОДАРЯ ЗА ВНИМАНИЕТО