VPN

Виртуальные частные сети

Защита сетевого трафика. Сервис защищенного канала и виртуальных частных сетей.

IPSec - протокол защиты сетевого трафика на IP-уровне.

Виртуальные частные сети: **IPSec**

IPSec (Internet Protocol Security) – это не столько протокол, сколько целая система открытых стандартов и протоколов, призванная чтобы обеспечить решение по безопасной передачи данных через публичные сети – т.е. для организации VPN. Система IPSec использует следующие протоколы для своей работы:

- **Протокол AH** (Authentication Header) - обеспечивает целостность и аутентификацию источника данных в передаваемых пакетах, а также защиту от ложного воспроизведения пакетов;
- **Протокол ESP** (Encapsulation Security Payload) - обеспечивает не только целостность и аутентификацию передаваемых данных, но еще и шифрование данных, а также защиту от ложного воспроизведения пакетов;
- **Протокол IKE** (Internet Key Exchange - обеспечивает способ инициализации защищенного канала, а также процедуры обмена и управления секретными ключами;

Стек протоколов IPSec

Internet Key Management - Управление ключами пользователя на прикладном уровне

Два протокола:
AH: аутентификация, гарантия целостности данных
ESP: аутентификация и шифрование

В случае использования IPSec в заголовке IP в поле «протокол верхнего уровня» (IPv4) или «следующий заголовок» (IPv6) помечается «IPSec»

Виртуальные частные сети: **IPSec**

Для **шифрования** данных в IPSec может быть применен любой симметричный алгоритм шифрования, использующий секретные ключи.

Взаимодействие протоколов IPSec происходит следующим образом:

С помощью протокола **IKE** между двумя точками устанавливается защищенный канал, называемый «безопасной ассоциацией» - **Security Association, SA**.

При этом выполняется следующие действия:

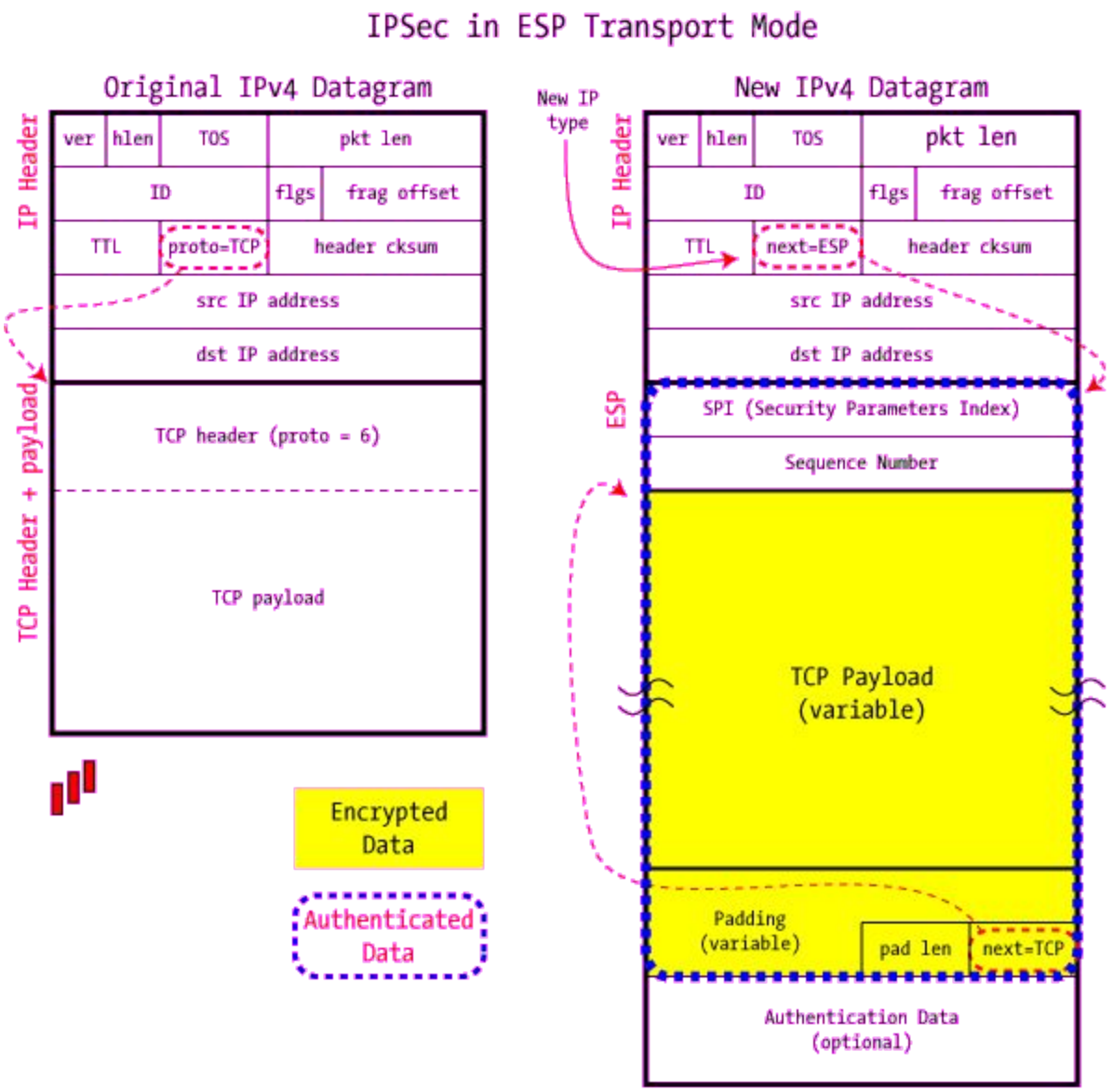
- аутентификация конечных точек канала
- выбираются параметры защиты данных (алгоритм шифрования, сессионный ключ и др.)
- согласование объединяемых подсетей

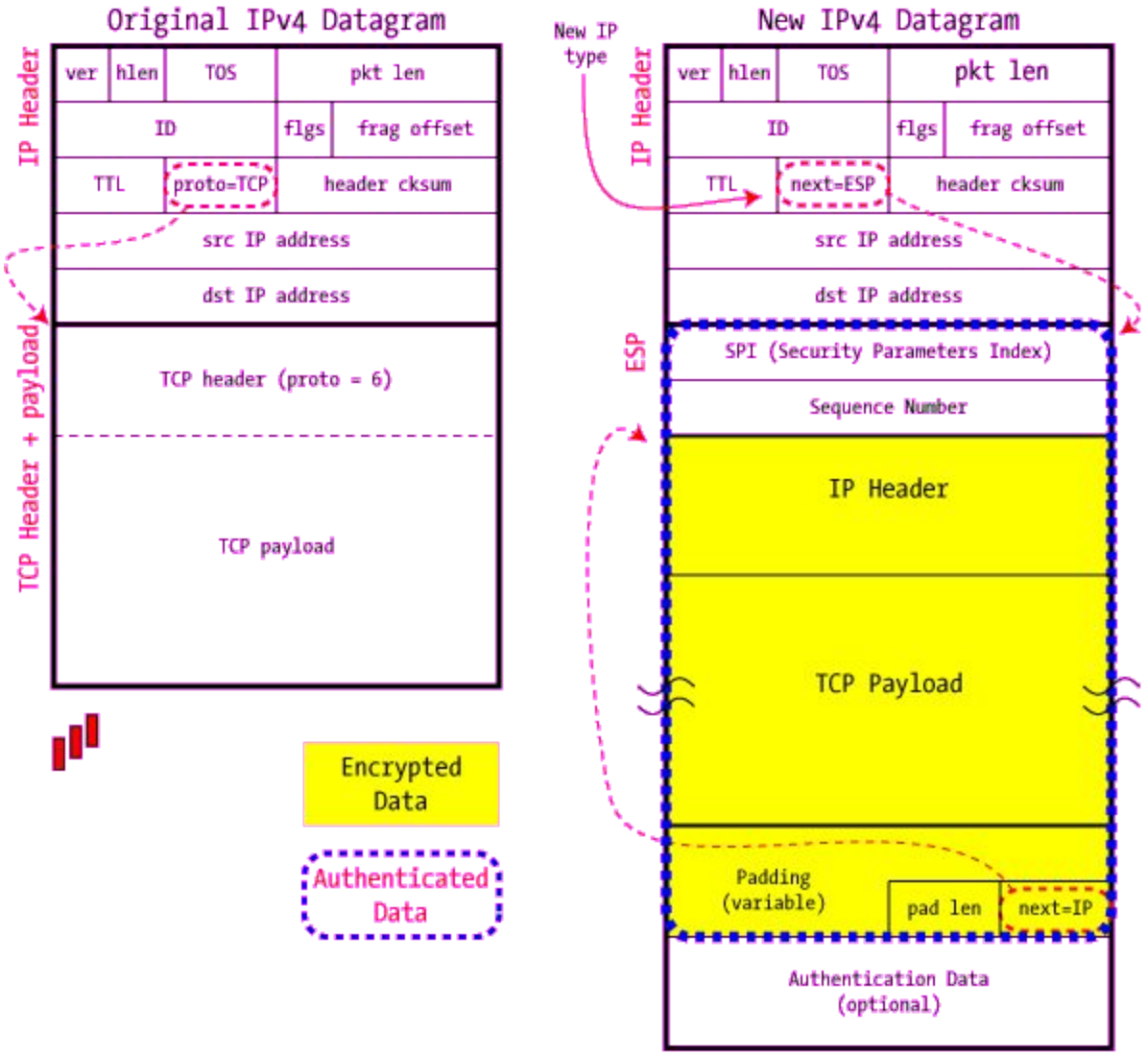
Виртуальные частные сети: **IPSec**

Протоколы AH и ESP могут работать в двух режимах: **транспортном** и **тоннельном**.

В транспортном режиме передача IP-пакета через сеть выполняется с помощью оригинального заголовка этого пакета. При этом не все поля исходного пакета защищаются. Протокол ESP аутентифицирует, проверяет целостность и шифрует только поле данных пакета IP. Протокол AH защищает больше полей: кроме поля данных еще и некоторые поля заголовка, за исключением изменяемых при передаче полей, например, поля TTL.

В тоннельном режиме исходный пакет помещается в новый IP-пакет и передача данных выполняется на основании заголовка нового IP-пакета.

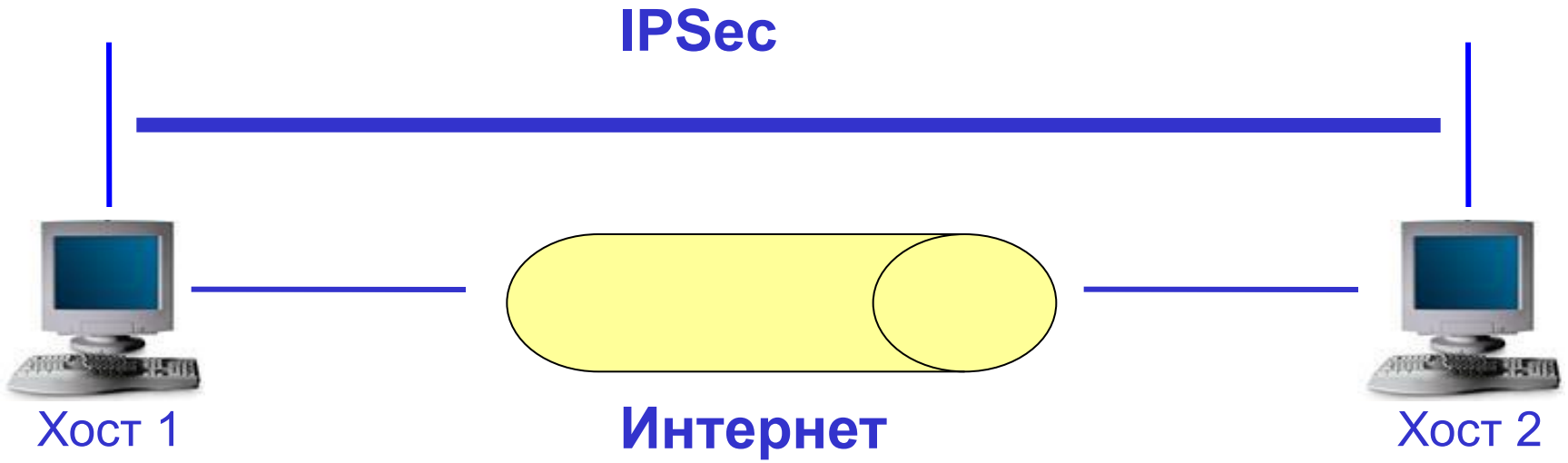

IPSec in ESP Transport Mode
Original IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
TCP Header + payload
TCP header (proto = 6)
TCP payload
Encrypted Data
Authenticated Data
New IPv4 Datagram
New IP type
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
next=ESP
header cksum
src IP address
dst IP address
ESP
SPI (Security Parameters Index)
Sequence Number
TCP Payload (variable)
Padding (variable)
pad len
next=TCP
Authentication Data (optional)


IPSec in ESP Tunnel Mode
Original IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
TCP Header + payload
TCP header (proto = 6)
TCP payload
Encrypted Data
Authenticated Data
New IPv4 Datagram
New IP type
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
next=ESP
header cksum
src IP address
dst IP address
ESP
SPI (Security Parameters Index)
Sequence Number
IP Header
TCP Payload
Padding (variable)
pad len
next=IP
Authentication Data (optional)

Виртуальные частные сети: **IPSec**

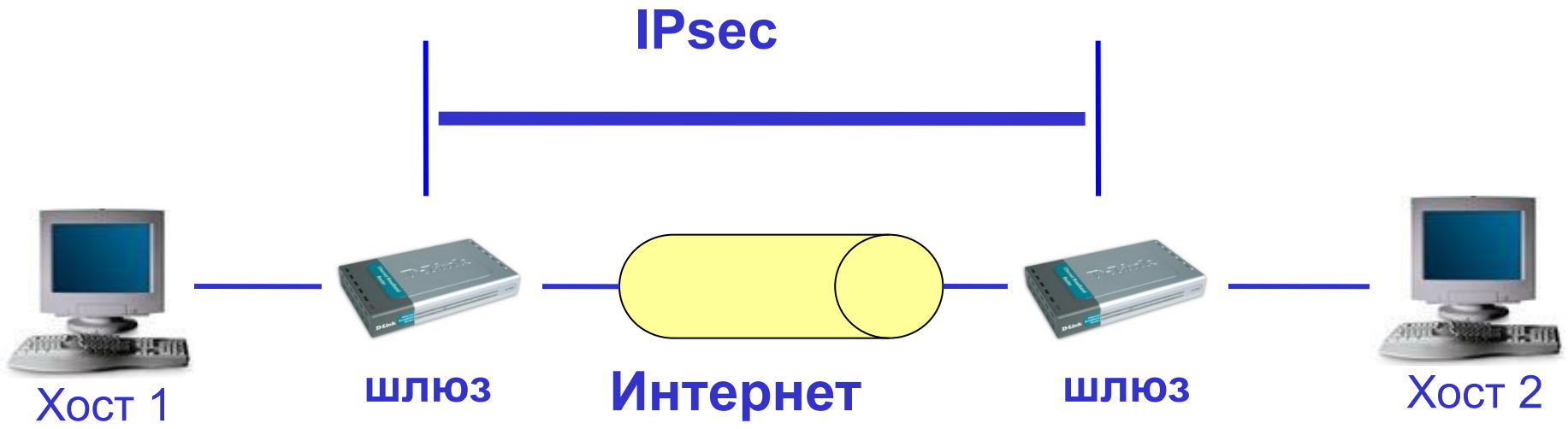
Существуют две основные схемы применения IPSec, отличающиеся ролью узлов, образующих защищенный канал.

В первой схеме защищенный канал образуется **между конечными узлами сети**. В этой схеме протокол IPSec защищает тот узел, на котором выполняется:



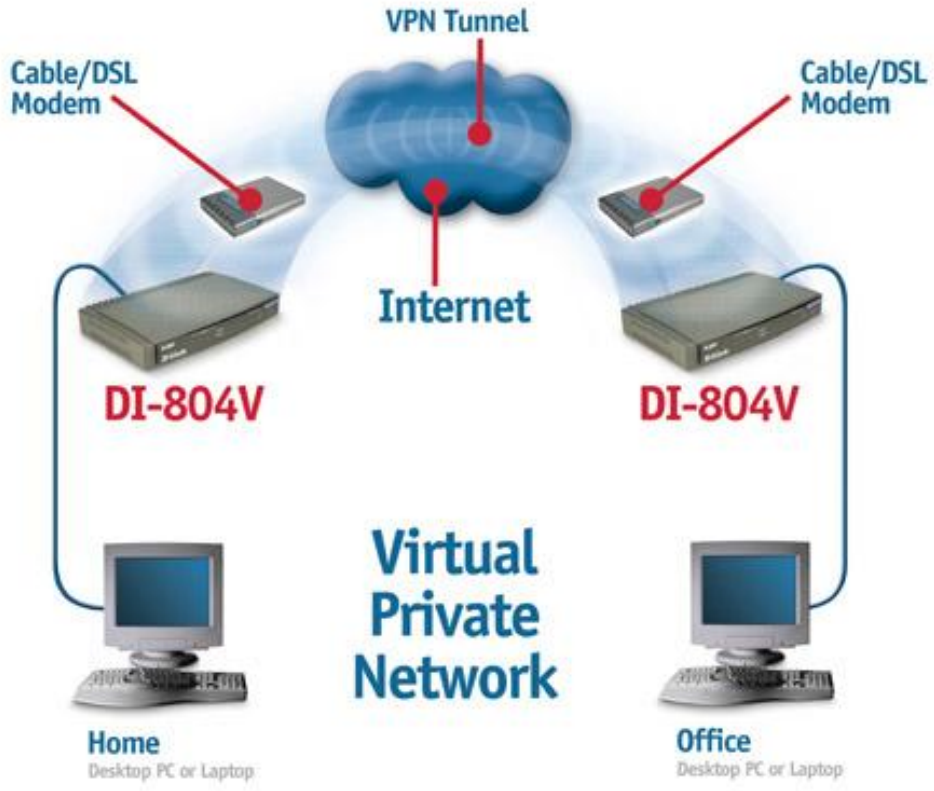
Виртуальные частные сети: **IPSec**

Во второй схеме защищенный канал устанавливается **между двумя шлюзами безопасности.** Эти шлюзы принимают данные от конечных узлов, подключенных к сетям, расположенным позади шлюзов. Конечные узлы в этом случае не поддерживают протокол IPSec, трафик, направляемый в публичную сеть проходит через шлюз безопасности, который выполняет защиту от своего имени.

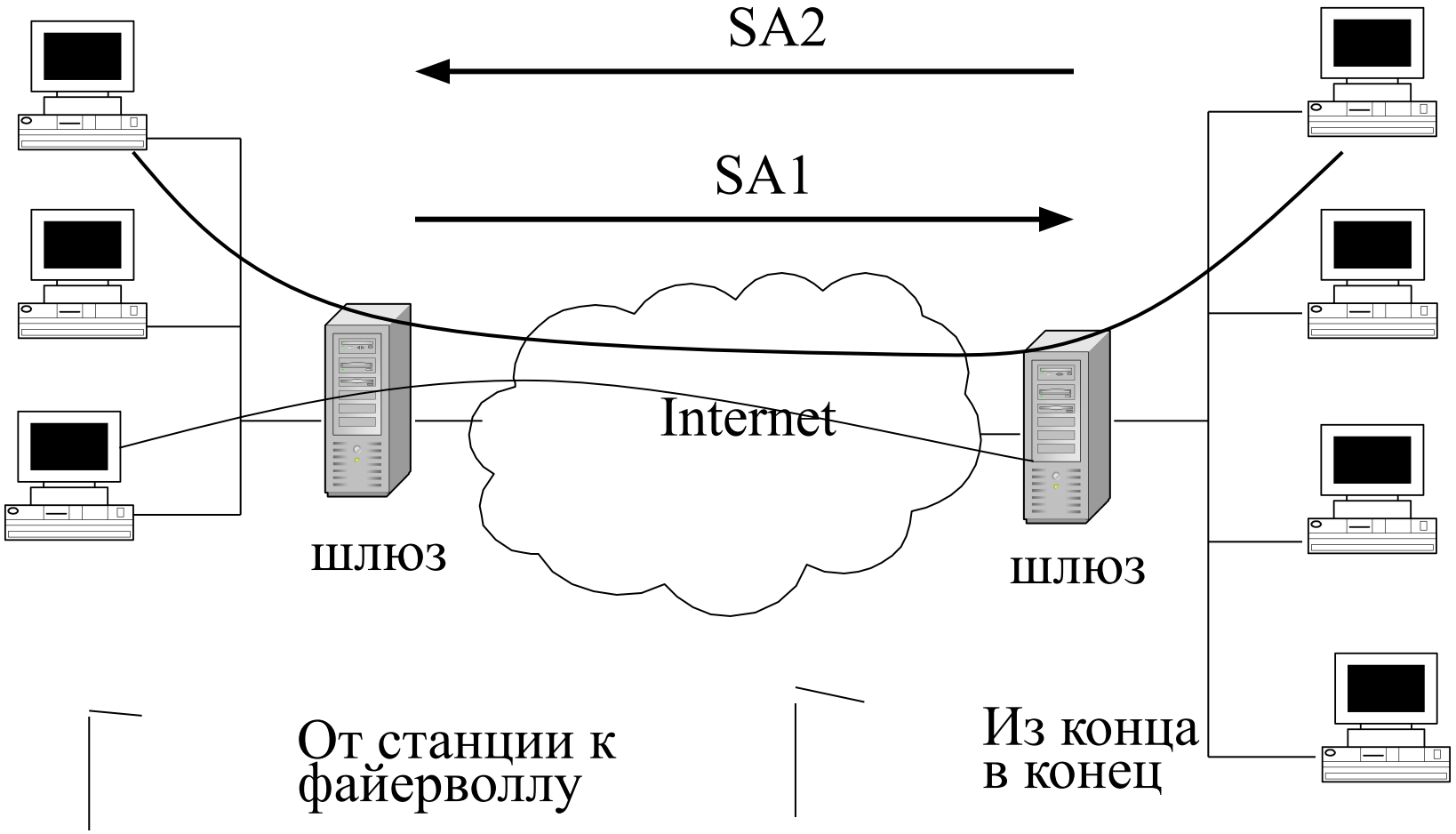


Виртуальные частные сети: **IPSec**

Для хостов, поддерживающих IPSec, разрешается использование как транспортного, так и тоннельного режимов. Для шлюзов разрешается использование только тоннельного режима.
В качестве устройств, работающих как шлюз IPSec, можно применять Интернет-маршрутизаторы **D-Link**, например, **DI-804V**.



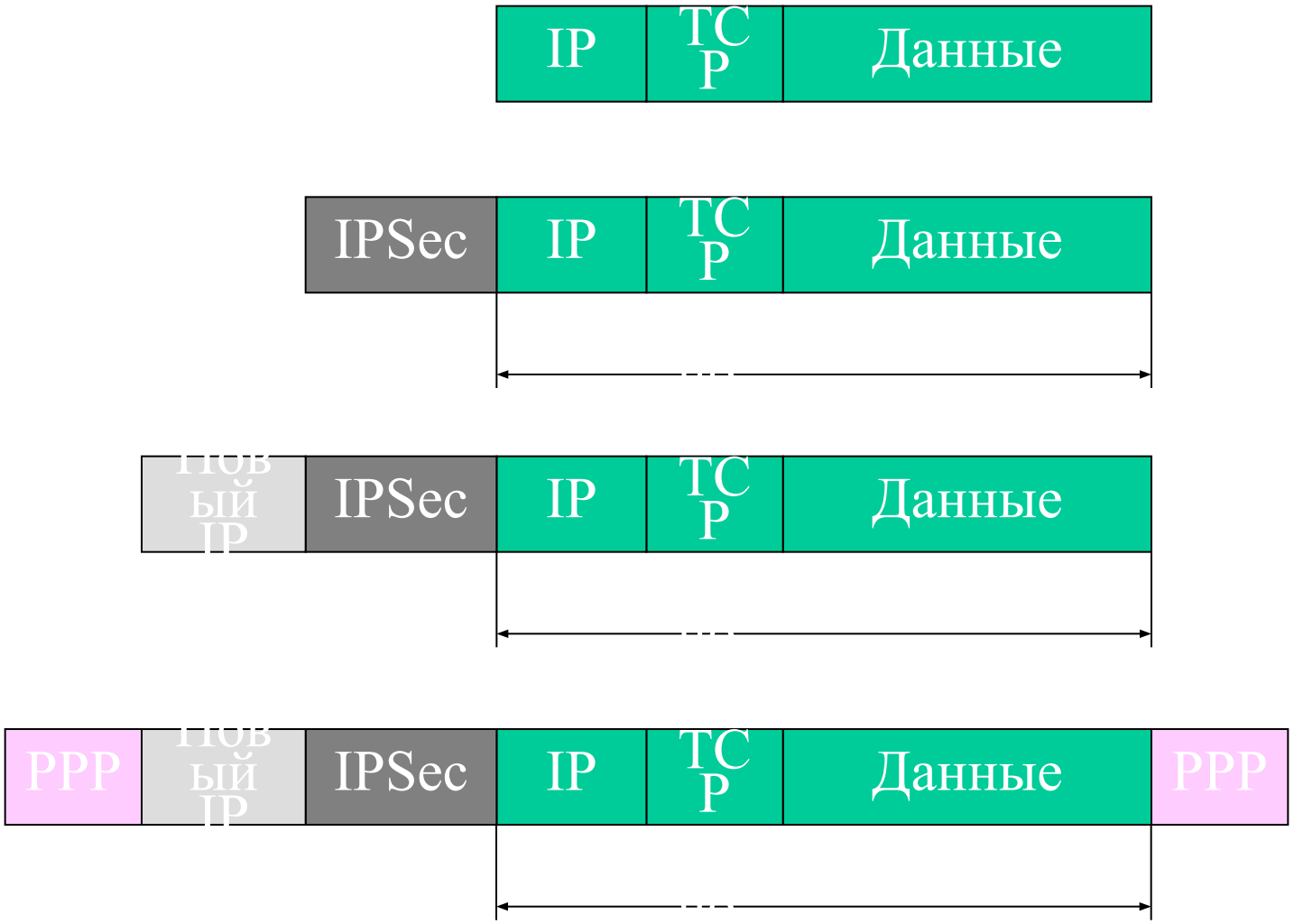
Определение SA



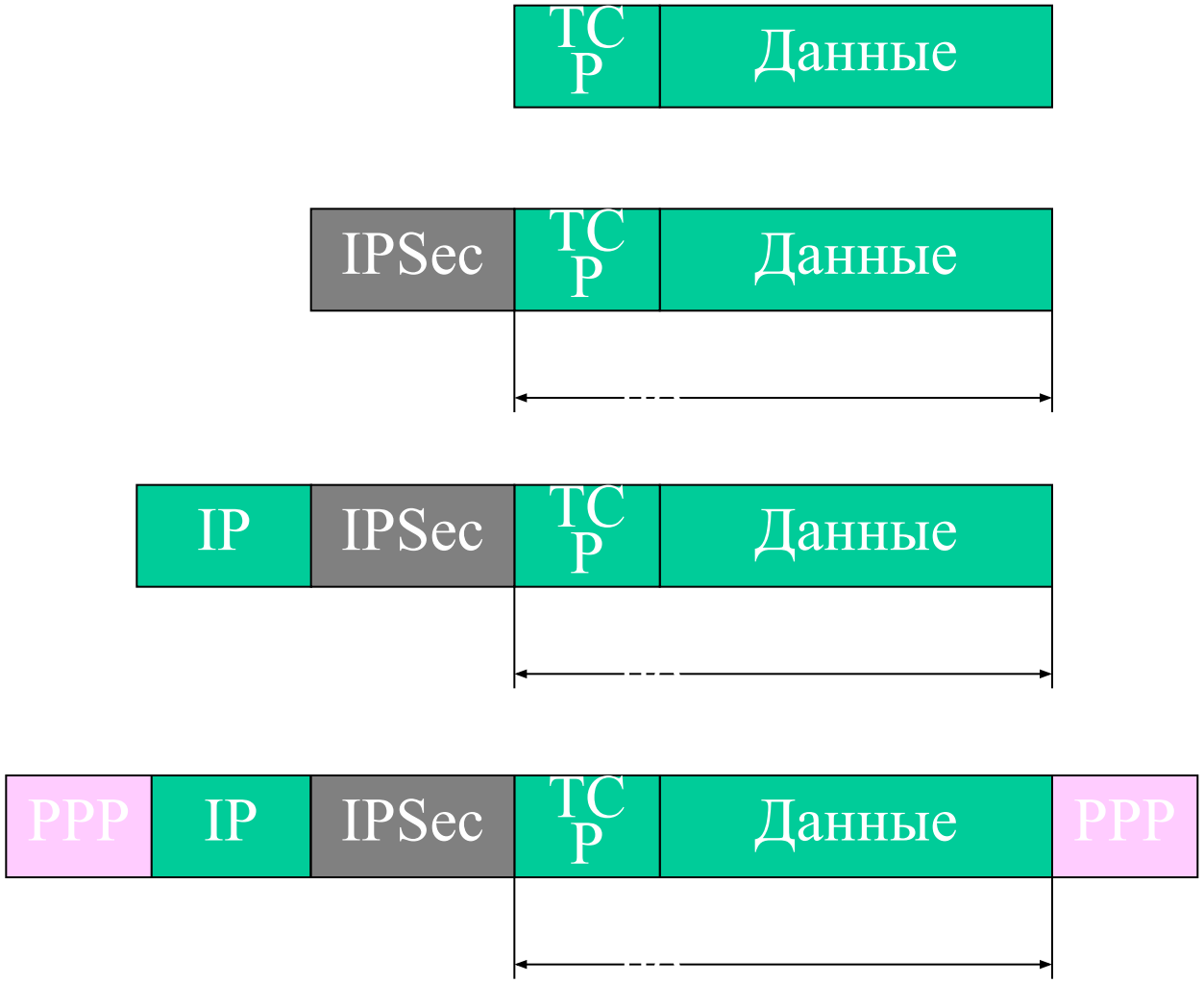
Режимы IPSec

- Туннельный режим:
  - Добавляется новый IP-заголовок
  - Исходный IP-заголовок инкапсулируется (предварительно шифруется).
  - Адрес приемника и передатчика может изменяться на адрес граничного шлюза
  - Инкапсуляция может производиться оконечной станцией или шлюзом VPN
- Транспортный режим:
  - Использует исходный IP-заголовок
  - Адреса оконечных устройств остаются без изменения
  - Инкапсуляция производится оконечными устройствами

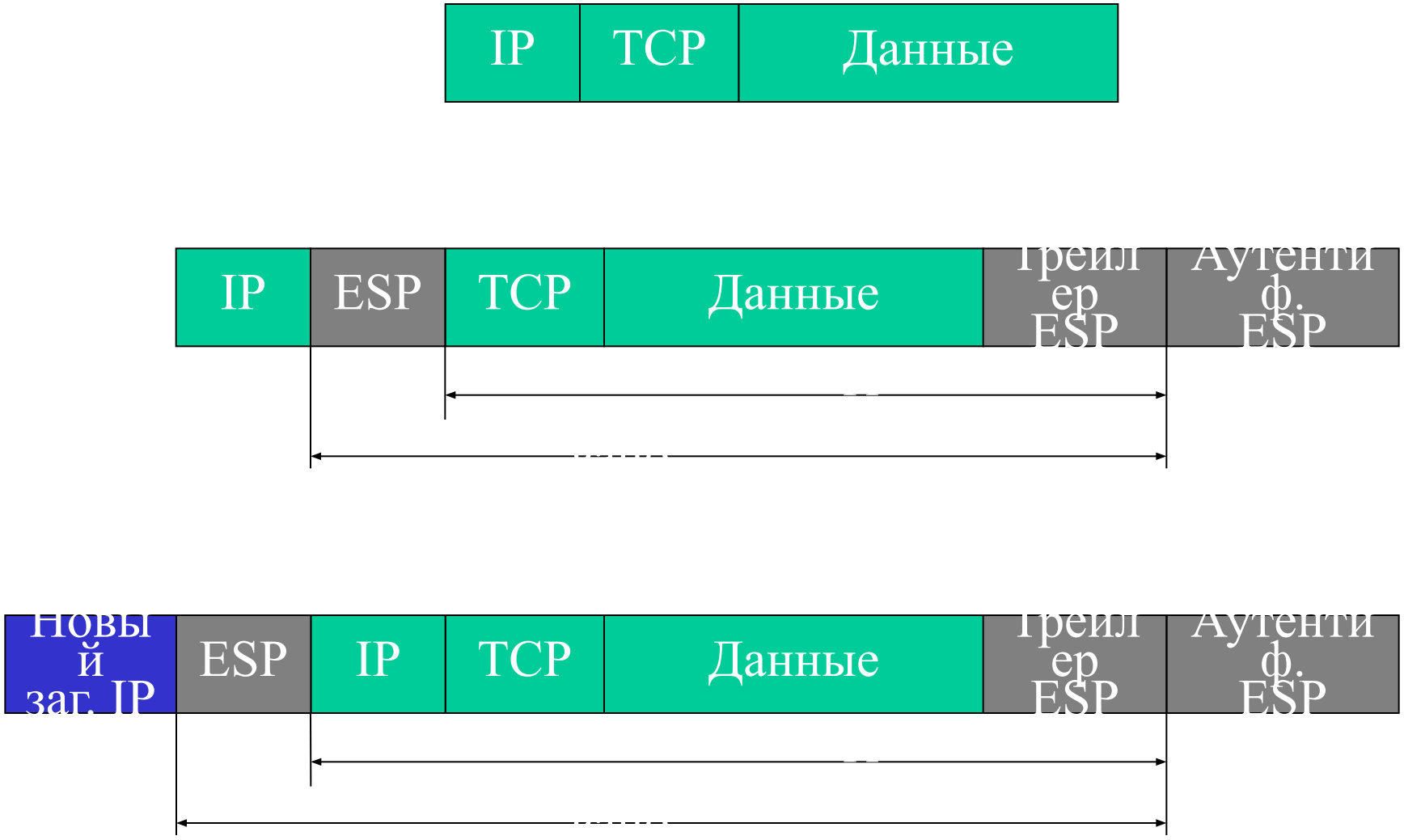
Инкапсуляция IPSec для туннельного режима



Инкапсуляция IPSec для транспортного режима



Инкапсуляция с аутентификацией (ESP)



Управление ключом IKE

- Функции IKE:
  - Установление SA (Security Association)
  - Определение параметров безопасности
  - Обмен ключами (UDP, порт 500)
- Фазы работы IKE:
  - Фаза I:
    - Аутентификация (из конца в конец, из конца к файерволлу)
    - Определение параметров безопасности для Фазы II
  - Фаза II:
    - Установление параметров безопасности для соединения
    - Выбор аутентификации (HMAC-MD5, HMAC-SHA)
    - Выбор алгоритма шифрования (DES, RC5, IDEA, Blowfish, CAST-128)

Общая процедура IPSec

- Фаза I для узла A, аутентификация
- Фаза II для узлов A и B, обмен ключами
- Установление туннеля
- Контроль состояния туннеля минимум каждые 10 с.

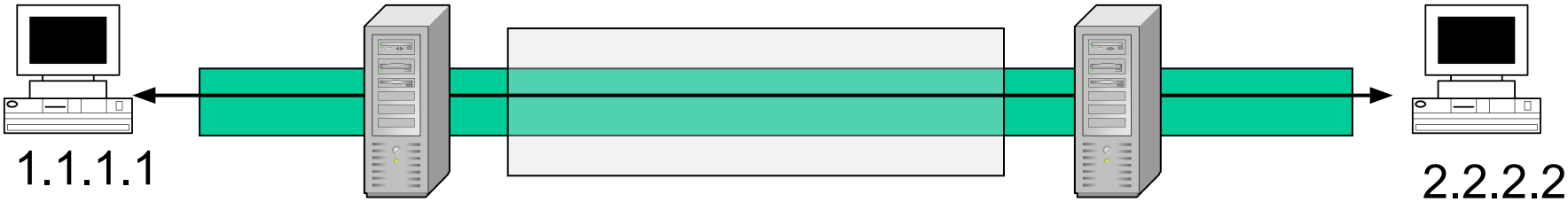
Правила безопасности

- Правила безопасности определяют способы защиты, пропуска и сброса трафика.
- Основным условием работы правил безопасности является зеркальность трафика в соединении
- В случае ошибочного прописывания правил безопасности могут возникать конфликты, приводящие к потере трафика:
  - Скрывание
  - Конфликт в типе туннелей
  - Зацикливание
  - Асимметрия

Пример реализации правил безопасности

TCP 1.1.*.*: any 2.2.*.*: any protect
TCP 1.1.1.1: any 2.2.2.2: any AH transport

TCP 1.1.*.*: any 2.2.*.*: any protect
TCP 1.1.1.*: any 2.2.2.*: any ESP tunnel 6.6.6.6



TCP 2.2.*.*: any 1.1.*.*: any protect
TCP 2.2.2.*: any 1.1.1.*: any ESP tunnel 5.5.5.5

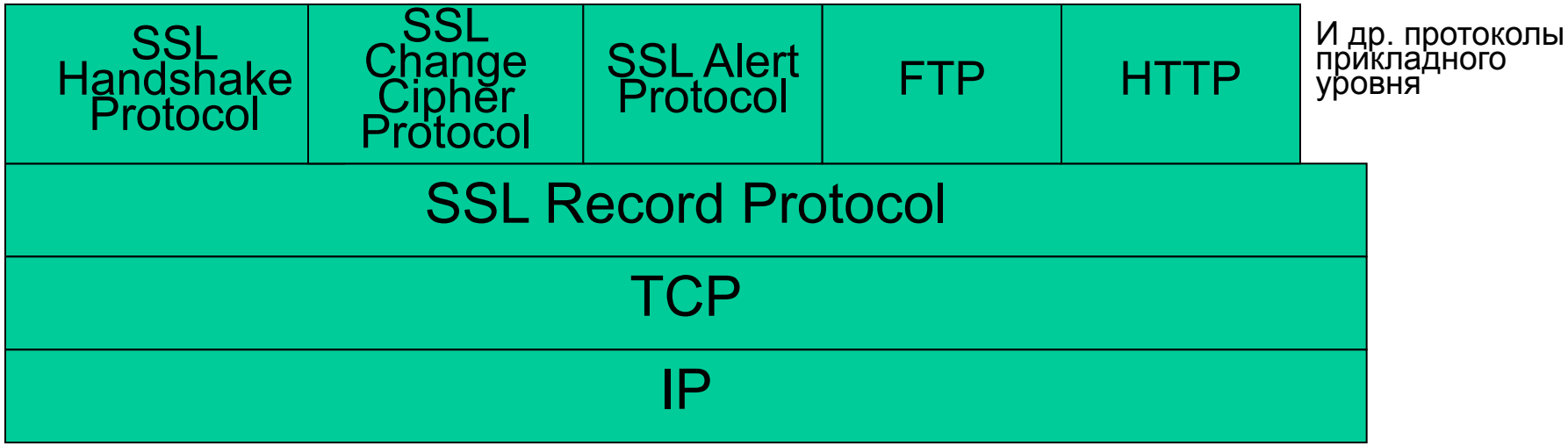
TCP 2.2.*.*: any 1.1.*.*: any protect
TCP 2.2.2.2: any 1.1.1.1: any AH transport

Протоколы транспортного уровня

- SSL – Secure Sockets Layer. SSLv3, 1996 год.
- TLS – Transport Layer Security. Стандарт IETF, RFC 2246.

  В настоящее время объединены в общий стек протоколов SSL/TLS

Стек протоколов SSL/TLS



- Все браузеры поддерживают SSL/TLC.
- SSL/TLS реализован поверх TCP (надежность доставки, квитирование), между транспортным и прикладным уровнем. Не поддерживает приложения UDP (отсутствует квитирование)
- Стек протоколов SSL/TLS:
  - SSL Record Protocol: защита передаваемых данных
  - SSL Handshake Protocol: установление сессии (соглашение о используемых алгоритмах, параметры безопасности)
  - SSL Change Cipher Protocol (смена шифра)
  - SSL Alert Protocol (сообщения об ошибках)

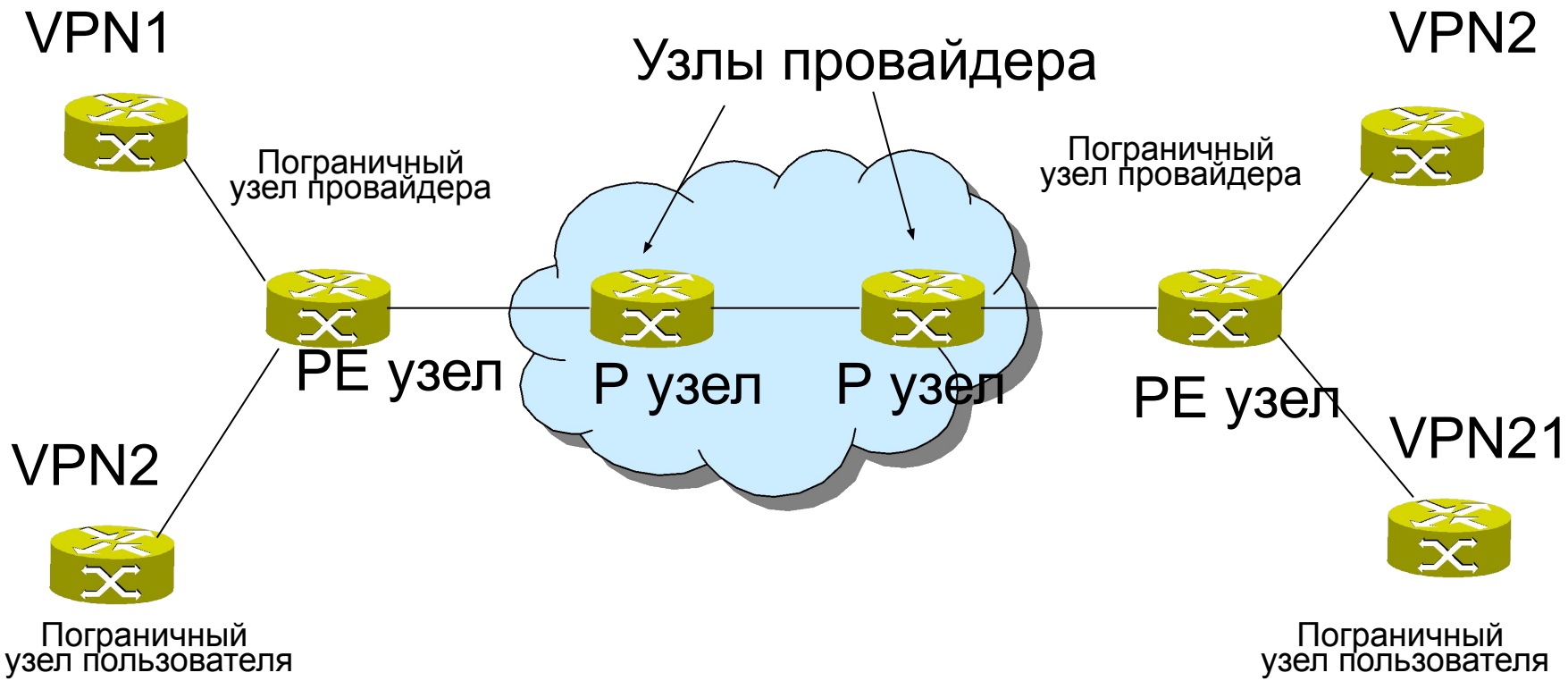
Организация VPN/MPLS

VPN/MPLS – хорошо масштабируемое решение.

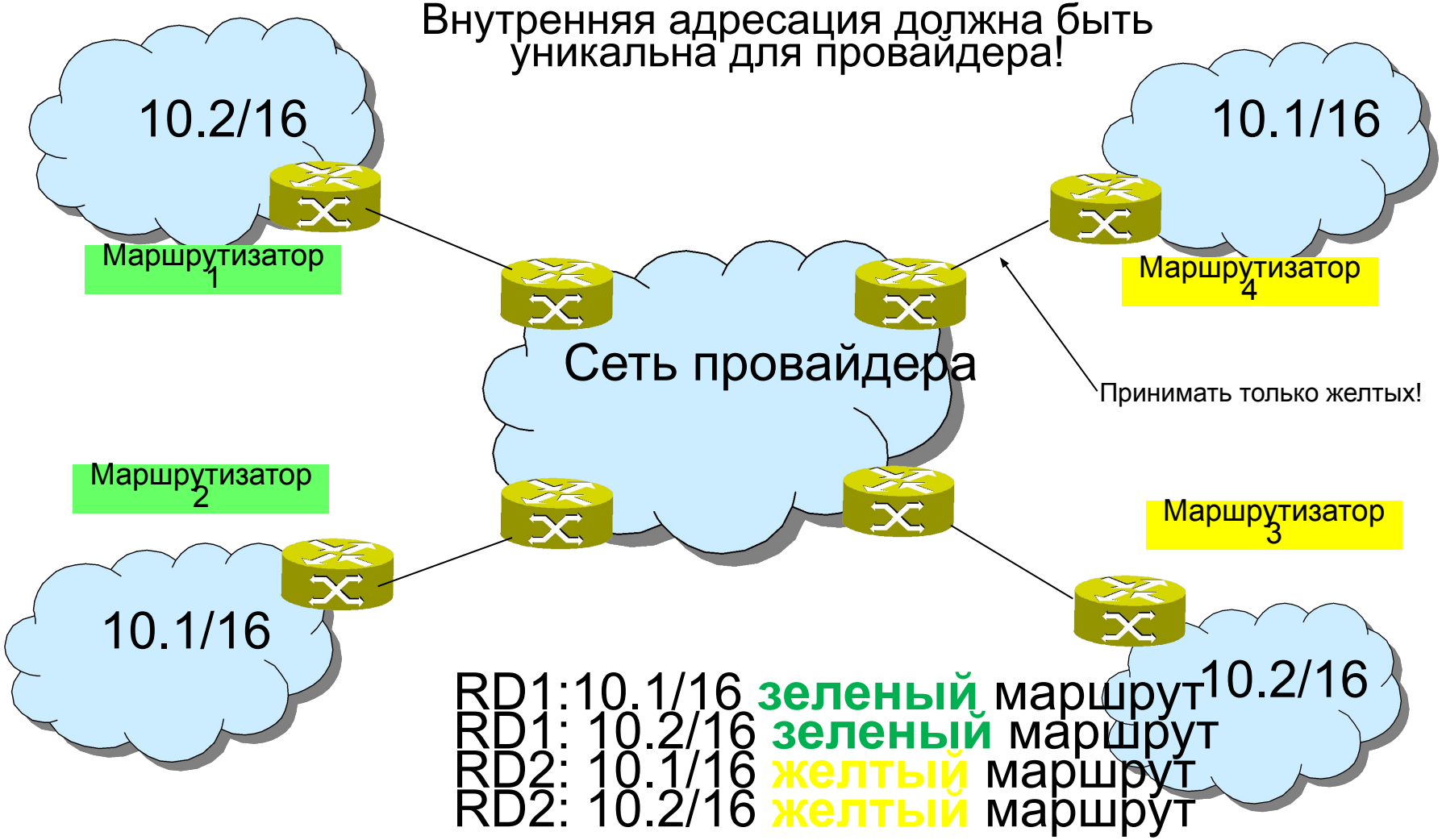
Рекомендация RFC 2547bis (модель IETF):

- P узлы: должны поддерживать маршруты к другим P и PE узлам, а не VPN-маршруты
- PE узлы: поддерживают только непосредственно подсоединенные VPN-маршруты
- VPN могут иметь перекрывающиеся адреса

Модель взаимодействия с сетью

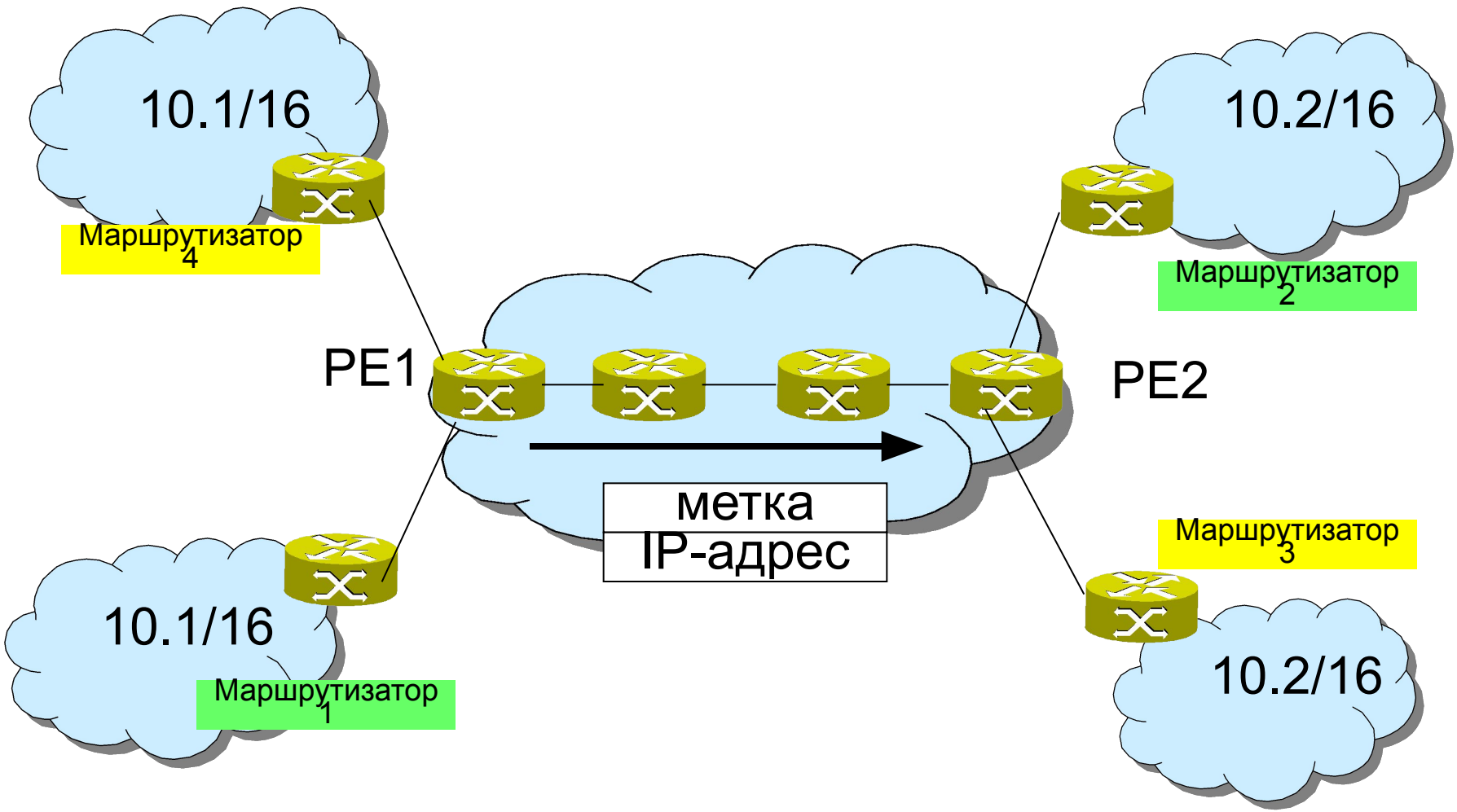


Адресация VPN

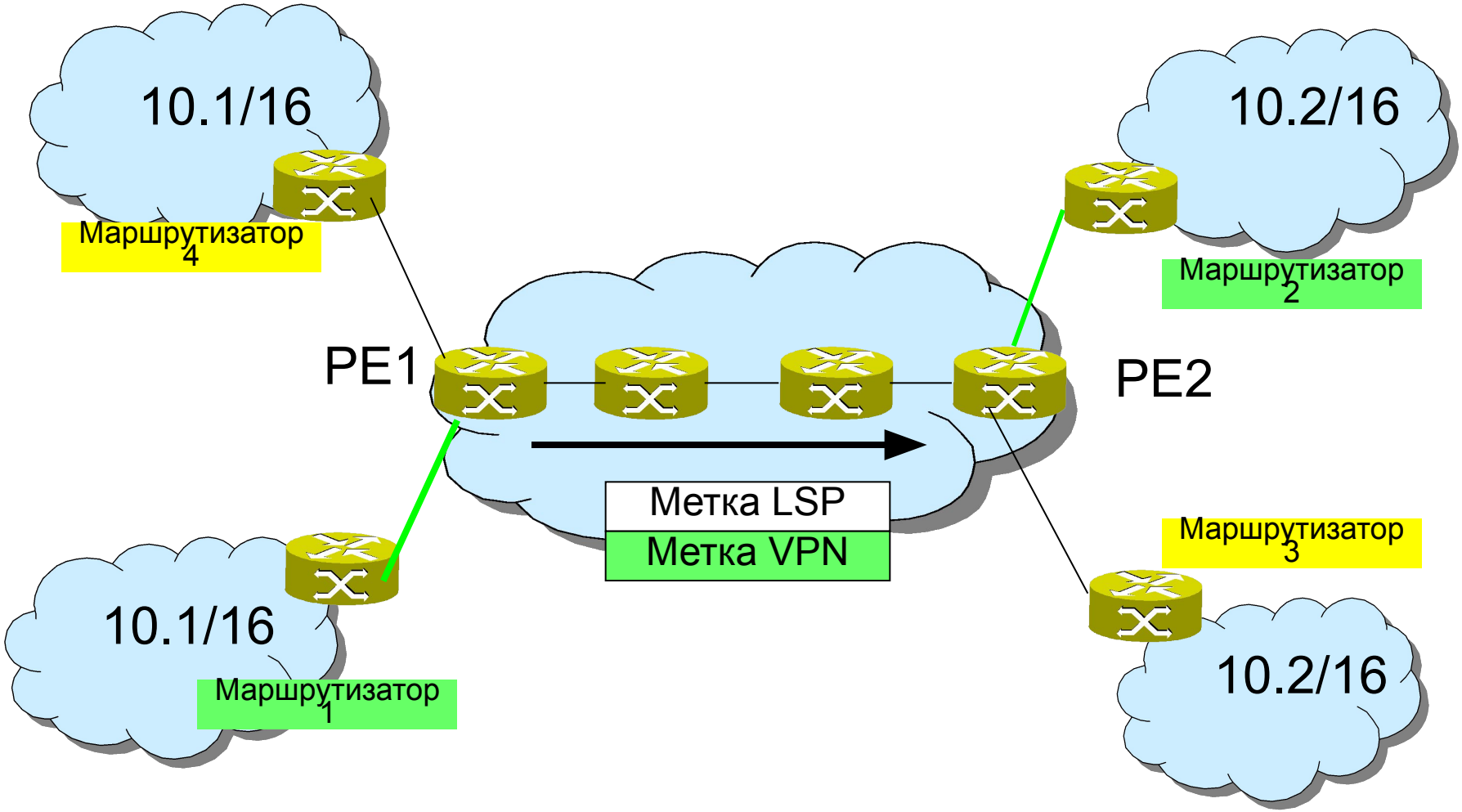


- **RD – Route Distinguisher** – признак маршрута. Используется для определения конкретных маршрутов. Это новый тип адреса.
- Основная идея – сделать неуникальные адреса уникальными, заменив группы IP-адресов на RD.
- Способ: совмещение IP-адреса и некоторого уникального идентификатора. Таким образом, для каждого маршрута в рамках одной VPN будут разные RD.
- **Комьюнити – сообщества** – используются для фильтрации трафика. Обозначаются «цветом».
- Трансляция комьюнити происходит только в узлах PE.
- Комьюнити используются только в сети провайдера и только для управления и трансляции.

Определение VPN



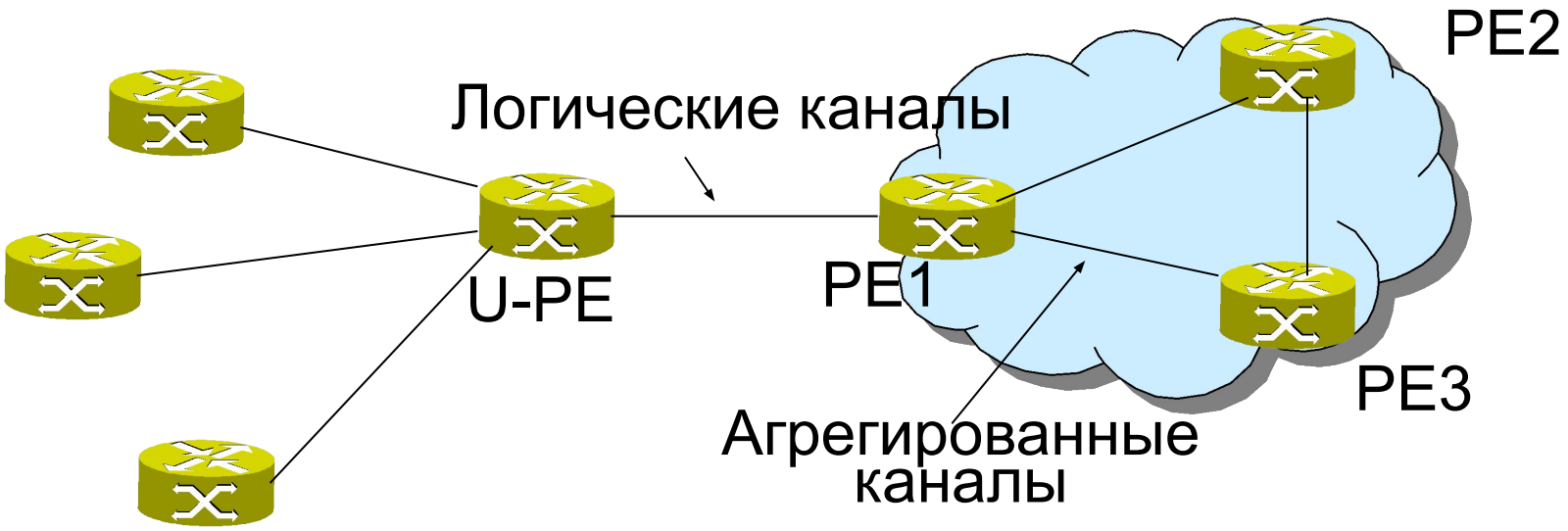
Использование метки VPN



Варианты решений:

- VPWS – для организации виртуальных частных каналов и решений точка-точка (все пакеты являются широковещательными). Самая примитивная версия. Легок в настройке и использовании (как односторонняя, так и двусторонняя конфигурация), поддерживает трафик альтернативных сетей, но недостаточно эффективно использует ресурс.
- VPLS – для организации виртуальных LAN и решений точка-многоточие (широковещательные пакеты отсылаются только на этапе установления соединения). Позволяет эмулировать VLAN на основе MPLS. Поддерживает интерфейсы Ethernet (низкая стоимость оконечного оборудования), эффективно управляет полосой пропускания. Существуют некоторые проблемы масштабирования.

- **HVPLS** – иерархический VPLS, поддерживает несколько уровней MPLS. Является следующей стадией развития VPLS. Решает проблему ограничения на количество узлов введением дополнительного пользовательского PE узла (U-PE). Для уменьшения таблицы коммутации передает часть функций U-PE узлам.



Применение DI-804V / DI-804HV