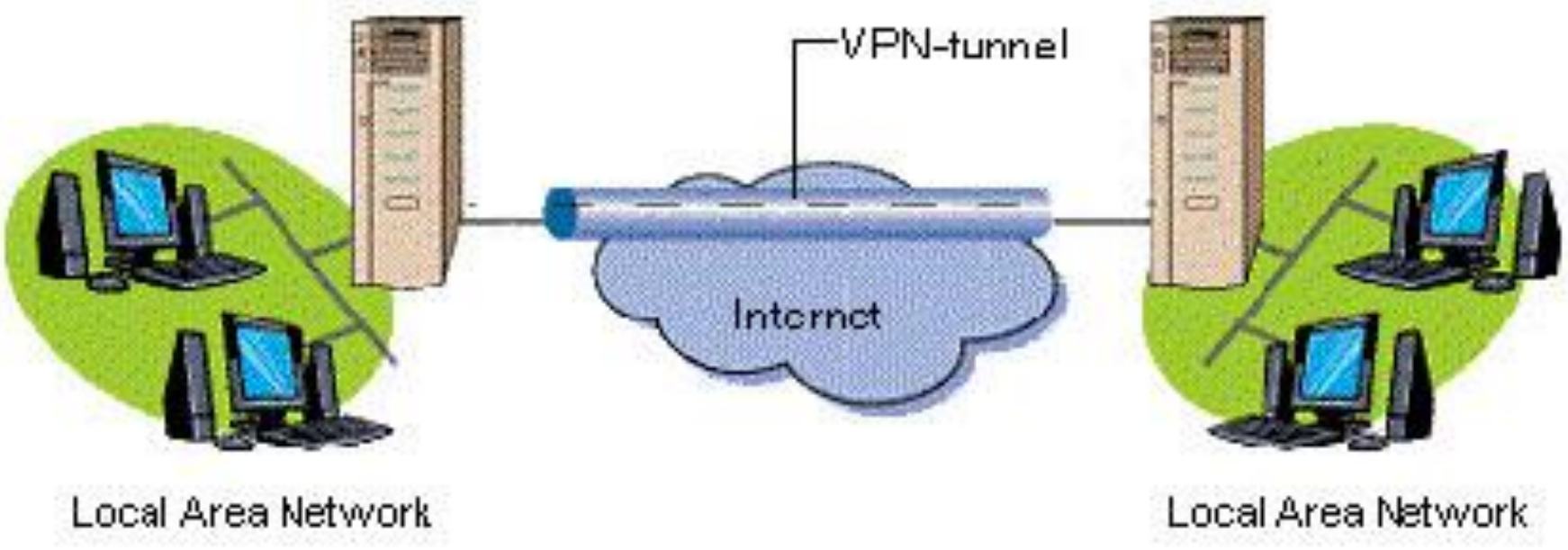
VPN

Виртуальные частные сети

Виртуальные частные сети - VPN

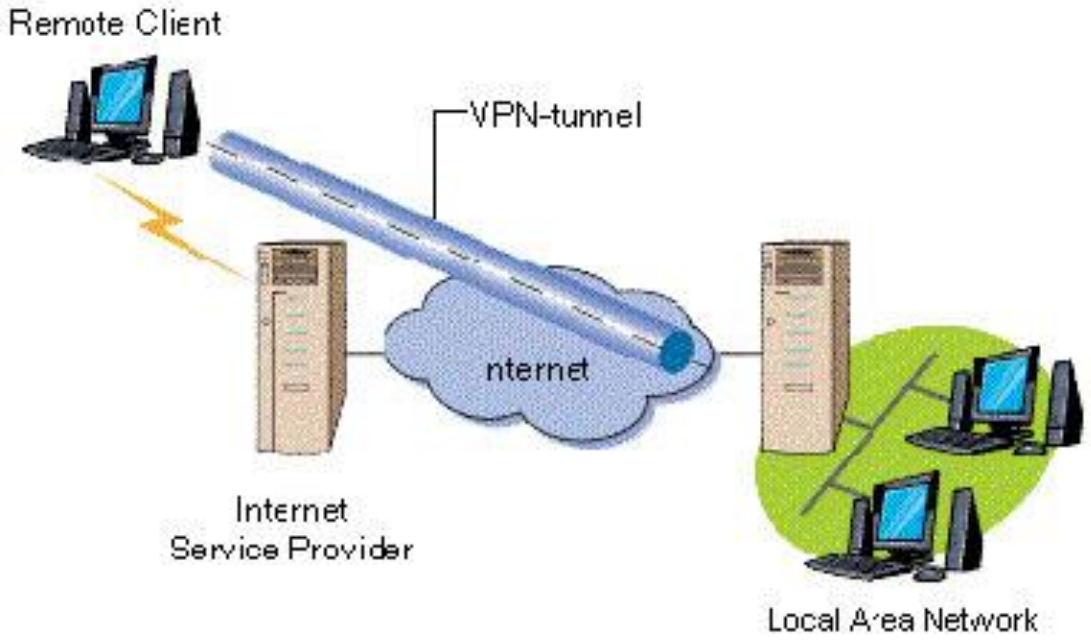
VPN представляет собой объединение отдельных машин или локальных сетей в единую виртуальную сеть, которая обеспечивает целостность и безопасность передаваемых данных. Она обладает свойствами выделенной частной сети и позволяет передавать данные через промежуточную сеть например Интернет. VPN позволяет отказаться от использования выделенных линий.



- 1998 год – разработка приложений VPN, позволяющих осуществлять централизованный контроль со стороны пользователей.
- 1999 год – модель аутентификации, дополнительные средства для конфигурирования клиентов
- 2000 год – включение средств VPN в Windows2000
- В настоящее время технология вошла в фазу расцвета. Используются различные технологии и архитектуры с учетом потребностей конкретной сети.
- Использование общедоступной IP-сети для предоставления удаленного доступа к информации может (!) являться безопасным.

Виртуальные частные сети - VPN

Имея доступ в Интернет, любой пользователь может без проблем подключиться к сети офиса своей фирмы. Общедоступность данных совсем не означает их незащищенность. Система безопасности VPN - защищает всю информацию от несанкционированного доступа: информация передается в зашифрованном виде. Прочитать полученные данные может лишь обладатель ключа к шифру.



Виртуальные частные сети - VPN

Средства VPN должны решать как минимум следующие задачи:

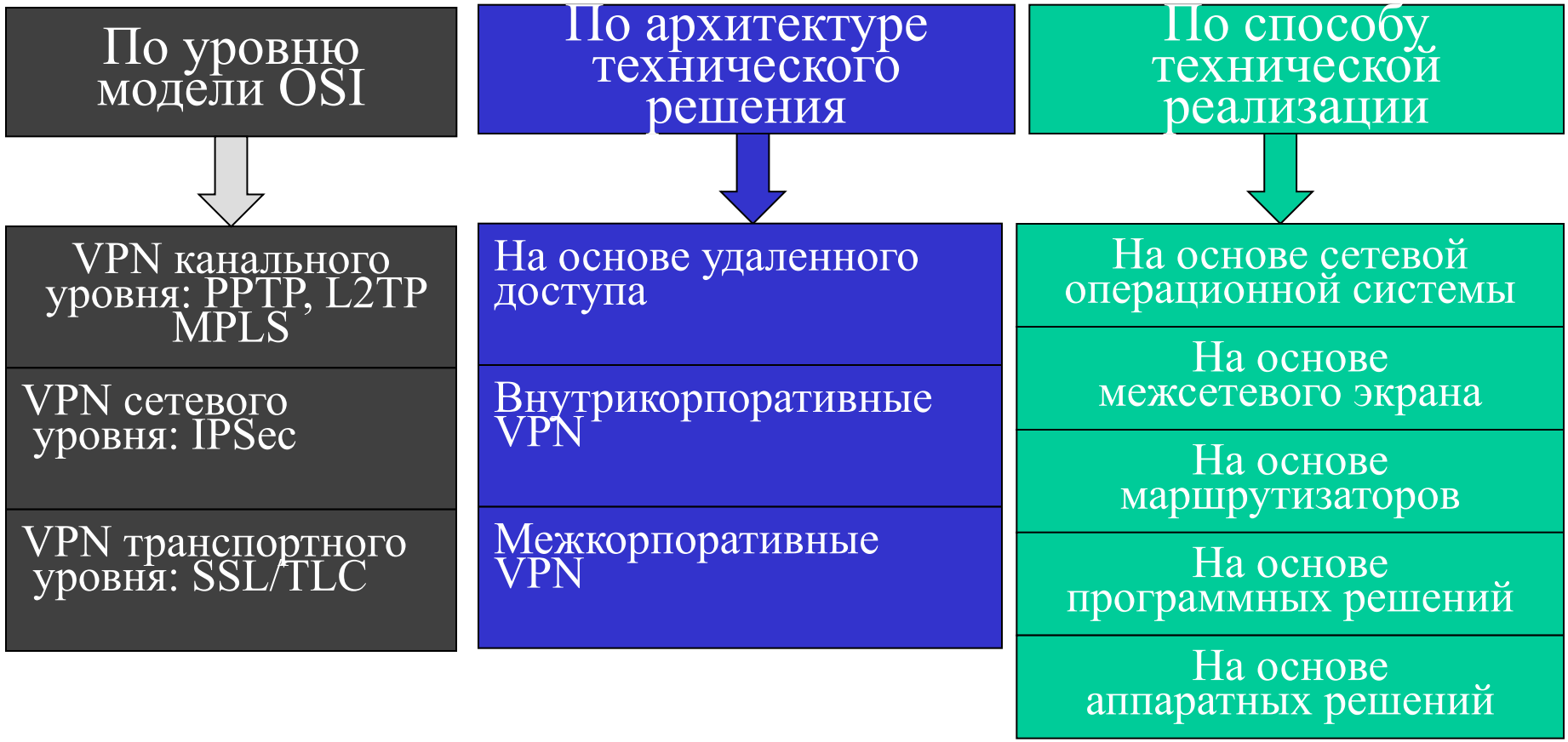
Конфиденциальность – это гарантия того, что в процессе передачи данных по каналам VPN эти данные не будут просмотрены посторонними лицами.

Целостность – гарантия сохранности передаваемых данных. Никому не разрешается менять, модифицировать, разрушать или создавать новые данные при передаче по каналам VPN.

Доступность – гарантия того, что средства VPN постоянно доступны легальным пользователям.

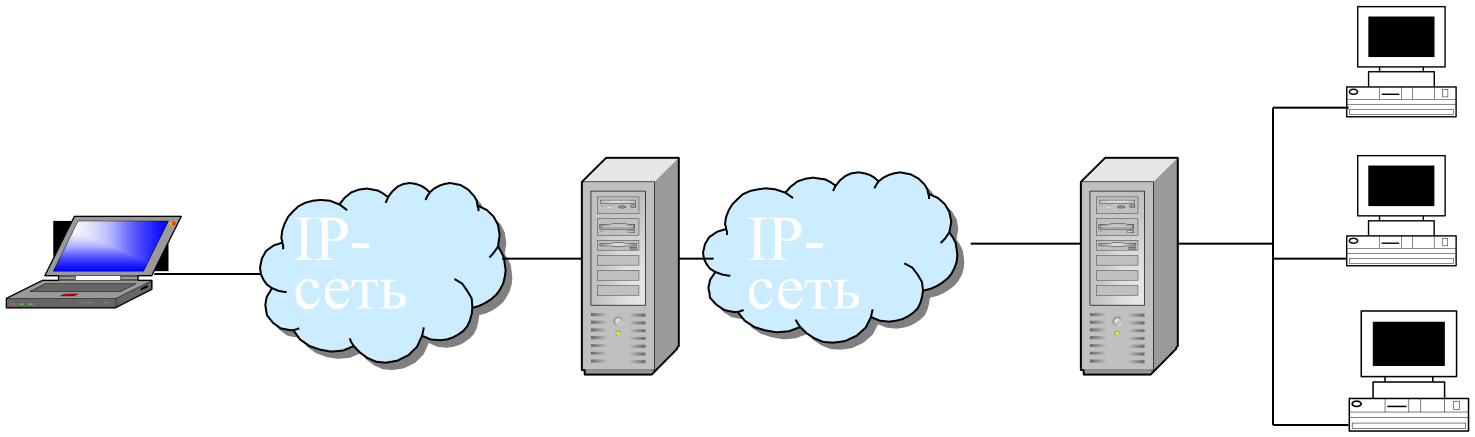
Для решения этих задач в решениях VPN используются такие средства как шифрование данных для обеспечения целостности и конфиденциальности, аутентификация и авторизации для проверки прав пользователя и разрешения доступа к сети VPN.

Классификация VPN



Базовые архитектуры VPN

- Шлюз-шлюз
- Шлюз-хост
- Хост-хост
- Комбинированная – через промежуточный шлюз (IPSG)



Основные компоненты VPN

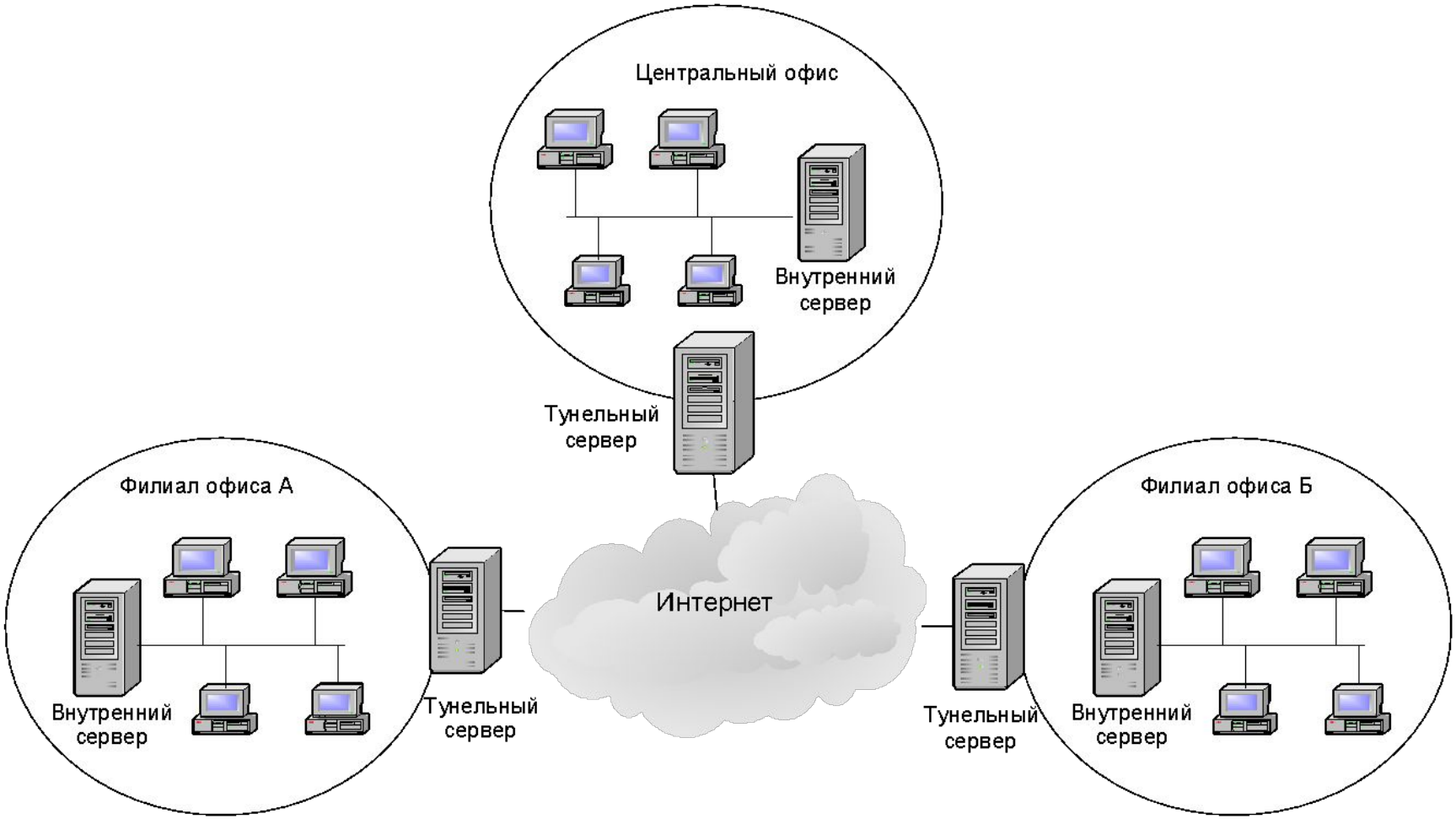
- **VPN-шлюз** – сетевое устройство, подключенное к нескольким сетям, выполняет функции шифрования, идентификации, аутентификации, авторизации и туннелирования. Может быть решен как программно, так и аппаратно.
- **VPN-клиент (хост)** решается программно. Выполняет функции шифрования и аутентификации. Сеть может быть построена без использования VPN-клиентов.

- **Туннель** – логическая связь между клиентом и сервером. В процессе реализации туннеля используются методы защиты информации.
- **Граничный сервер** – это сервер, являющийся внешним для корпоративной сети. В качестве такого сервера может выступать, например, брендмауэр или система NAT.
- **Обеспечение безопасности информации VPN** – ряд мероприятий по защите трафика корпоративной сети при прохождении по туннелю от внешних и внутренних угроз.

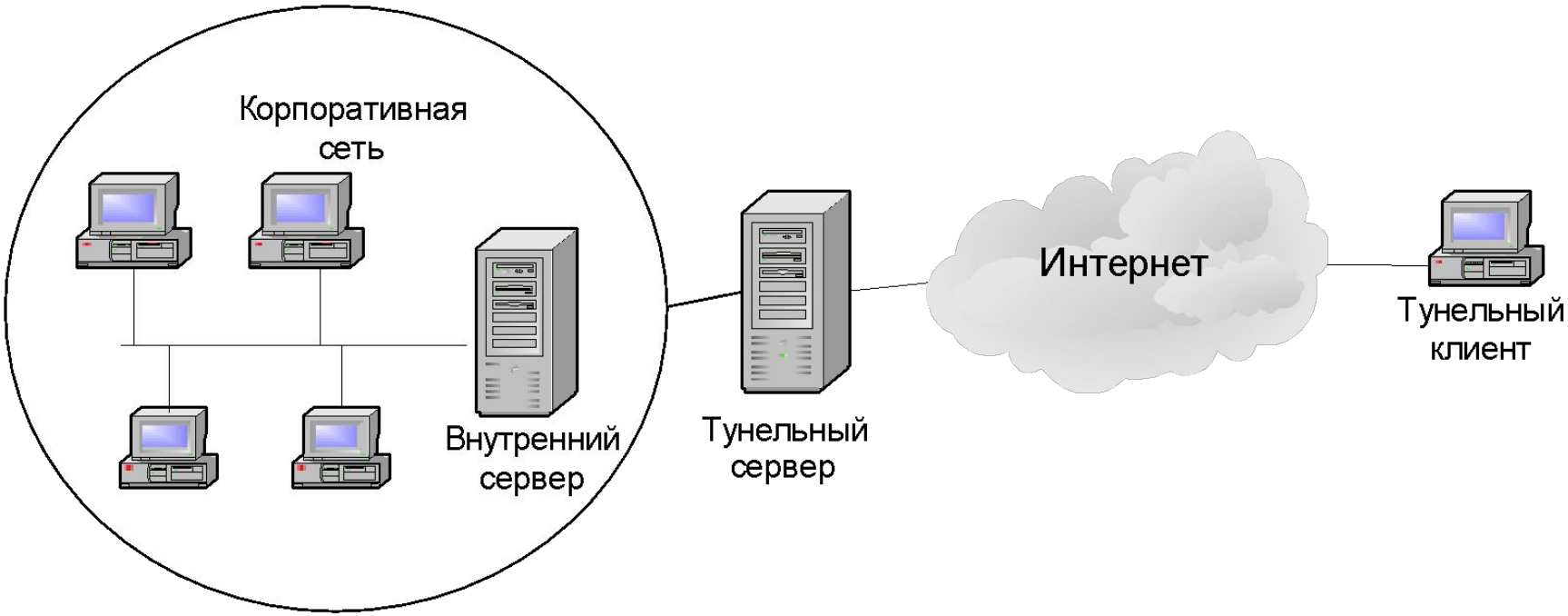
Схемы взаимодействия провайдера и клиента

- **Пользовательская схема** – оборудование размещается на территории клиента, методы защиты информации и обеспечения QoS организуются самостоятельно.
- **Провайдерская схема** – средства VPN размещаются в сети провайдера, методы защиты информации и обеспечения QoS организуются провайдером.
- **Смешанная схема** – используется при взаимодействии клиента с несколькими провайдерами.

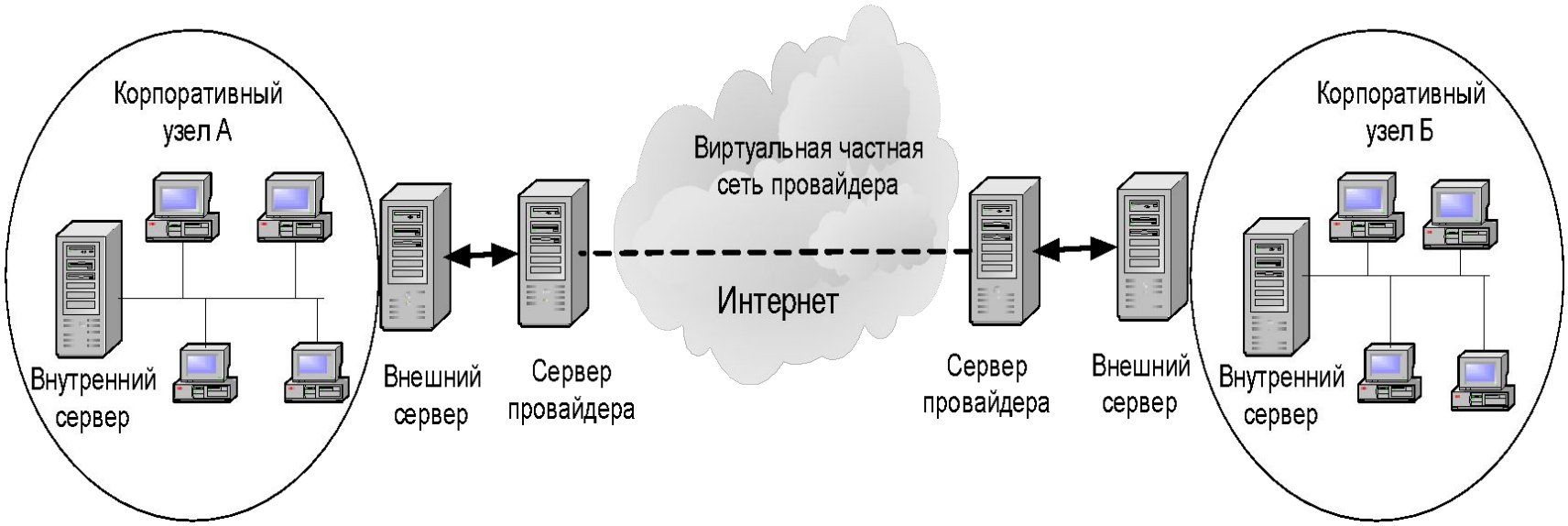
Схема соединения филиалов с центральным офисом



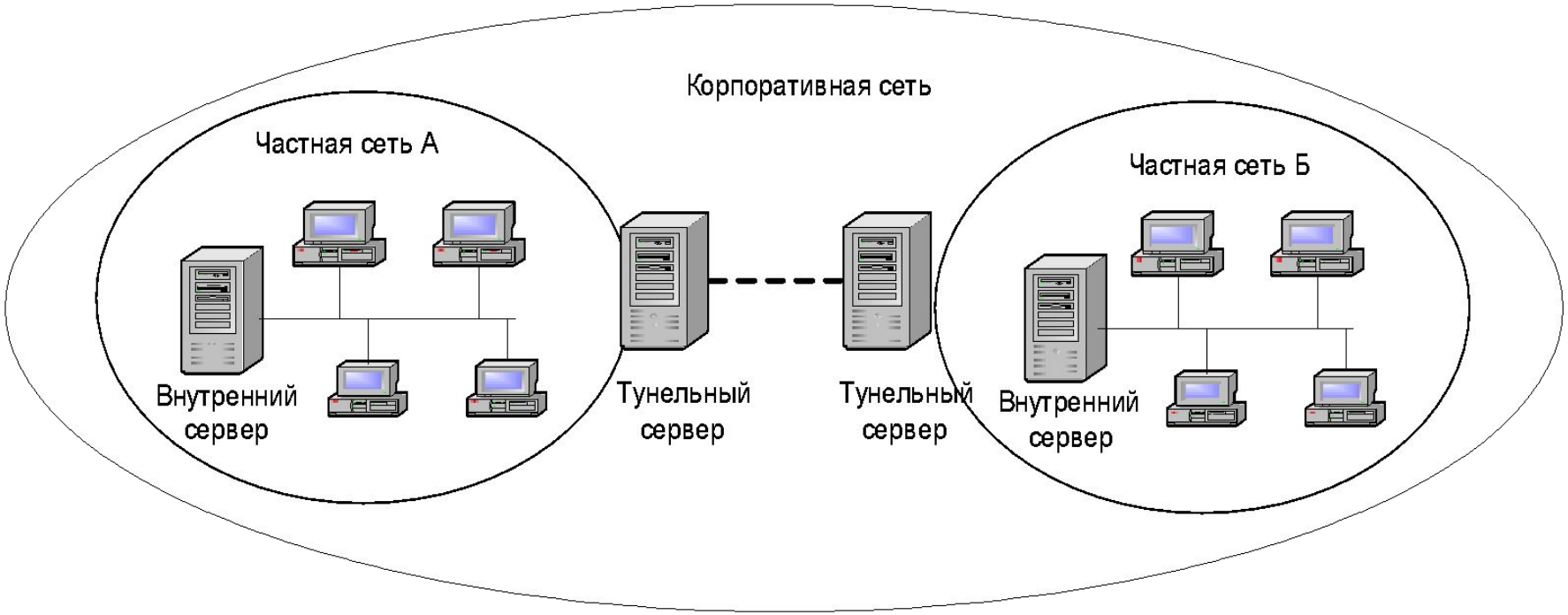
Связь удаленного пользователя с корпоративной сетью



Организация туннеля через провайдера Internet, поддерживающего службу VPN



VPN-соединение защищенных сетей внутри корпоративной сети



VPN-соединение корпоративного клиента с защищенной сетью внутри корпоративной сети

Виртуальные частные сети - VPN

Часто в своей работе решения VPN используют **туннелирование** (или **инкапсуляцию**).

Туннелирование или инкапсуляция - это способ передачи полезной информации через промежуточную сеть. Такой информацией могут быть кадры (или пакеты) другого протокола. При инкапсуляции кадр не передается в сгенерированном узлом-отправителем виде, а снабжается **дополнительным заголовком**, содержащим информацию о маршруте, позволяющую инкапсулированным пакетам проходить через промежуточную сеть (Интернет). На конце туннеля кадры **деинкапсулируются** и передаются получателю.

Одним из явных достоинств туннелирования является то, что данная технология позволяет зашифровать исходный пакет целиком, включая заголовок, в котором могут находится данные, содержащие информацию, полезную для взлома сети, например, IP- адреса, количество подсетей и т.д.

Защита данных в VPN

Требования к защищенному каналу:

- Конфиденциальность
- Целостность
- Доступность легальным пользователям (аутентификация)

Методы организации защищенного канала:

- Шифрование.
- Аутентификация – позволяет организовать доступ к сети только легальных пользователей.
- Авторизация – контролирует доступ легальных пользователей к ресурсам в объемах, соответствующих предоставленными им правами.
- Туннелирование – позволяет зашифровать пакет вместе со служебной информацией.

Поддержка VPN на различных уровнях модели OSI

- Канальный уровень:
  - L2TP, PPTP и др. (авторизация и аутентификация)
  - Технология MPLS (установление туннеля)
- Сетевой уровень:
  - IPSec (архитектура «хост-шлюз» и «шлюз-шлюз», поддержка шифрования, авторизации и аутентификации, проблемы с реализацией NAT)
- Транспортный уровень:
  - SSL/TLS (архитектура «хост-хост» соединение из конца в конец, поддержка шифрования и аутентификации, реализован только для поддержки TCP-трафика)

Протоколы канального уровня:

- **PPTP** (Point-to-Point-Tunneling Protocol). Шифрует кадры PPP и инкапсулирует их в IP пакеты (1996 год, разработка Microsoft, Ascend, 3Con и US Robotics)
- **L2F** (Layer to Forwarding). Прототип L2TP (1996 год, разработка Cisco)
- **L2TP** (Layer to Tunneling Protocol). Инкапсулирует кадры PPP в протокол сетевого уровня, предварительно проведя аутентификацию пользователя (1997 год, разработка Cisco и IETF)

Виртуальные частные сети - VPN

Существует множество различных решений для построения виртуальных частных сетей. Наиболее известные и широко используемые это:

- **PPTP** (Point-to-Point Tunneling Protocol). Этот протокол стал достаточно популярен благодаря его включению в операционные системы фирмы Microsoft.
- **PPPoE** (PPP over Ethernet) — разработка RedBack Networks, RouterWare, UUNET и другие.
- **IPSec** (Internet Protocol Security) — официальный стандарт Интернет.

Эти протоколы поддерживаются в Интернет-шлюзах **D-Link**, в зависимости от модели все или часть из них.

Виртуальные частные сети: **PPTP**

- **PPTP** дает возможность пользователям устанавливать коммутируемые соединения с Internet-провайдерами для получения доступа в интернет. И подключать удаленных пользователей к ресурсам защищенной сети

- В отличие от IPSec, протокол PPTP изначально не предназначался для организации туннелей между локальными сетями. **PPTP расширяет возможности PPP** — протокола, который специфицирует соединения типа **точка-точка** в IP-сетях.

- PPTP позволяет создавать защищенные каналы для обмена данными по протоколам – **IP, IPX, NetBEUI** и др.

Виртуальные частные сети: **PPTP**

- **Как происходит установление соединения PPTP**: пользователь «звонит» на сервер корпоративной сети или провайдера, где установлен протокол PPTP. Этот «звонок» отличается от обычного тем, что вместо телефонного номера указывается адрес сервера PPTP. После аутификации (согласовения управляющих пакетов и проверки пароля) устанавливается туннель для передачи данных

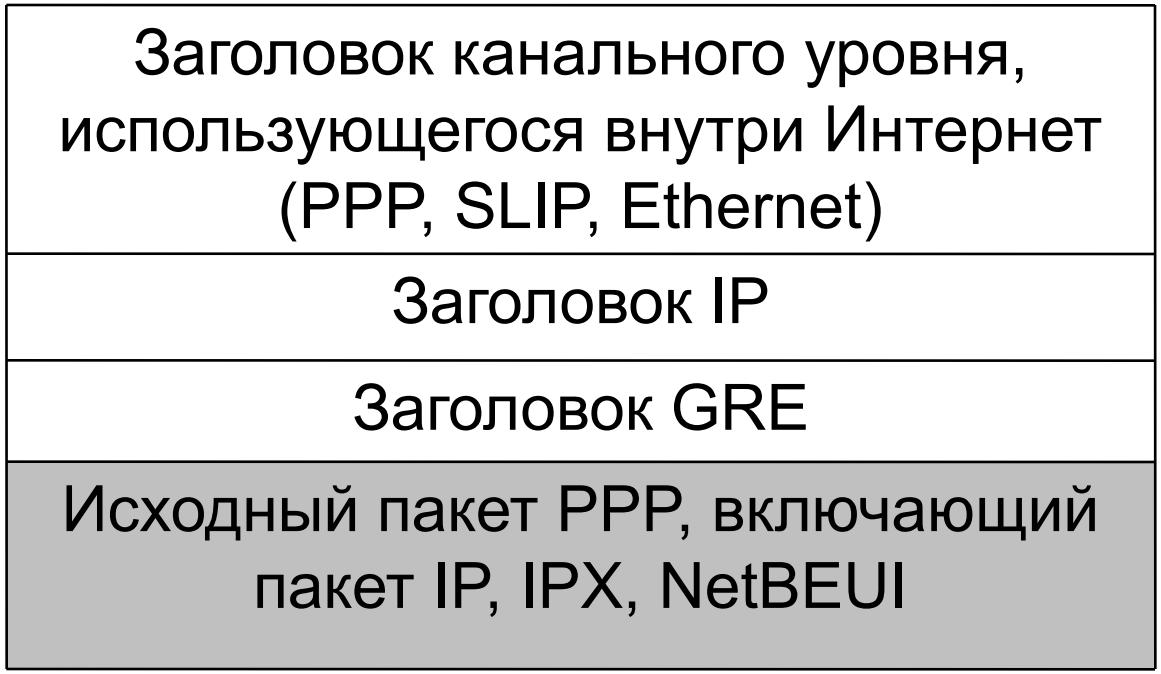
- **Метод шифрования**, применяемый в PPTP, специфицируется на уровне PPP. Обычно в качестве клиента PPP выступает настольный компьютер с операционной системой Microsoft, а в качестве протокола шифрования используется Microsoft Point-to-Point Encryption (MPPE). Данный протокол основывается на стандарте RSA RC4 и поддерживает 40- или 128-разрядное шифрование.

Виртуальные частные сети: **PPTP**

Как происходит передача: На выходе от источника сигнала, данные поступают в туннель в начальном виде, т. е. согласно стеку протоколов TCP/IP. Полученный пакет икапсулируется в PPP пакет, затем в GRE протокол, который лежит в основе PPTP, к сформированному пакету присваивается IP адрес отправителя(WAN-IP) и адрес назначения IP (PPTP)
За счёт такой инкапсуляции с помощью протокола PPTP можно работать не только с IP, но и с IPX NetBEUI и др.

Виртуальные частные сети: **PPTP**

- Пакеты, переносящие пользовательские данные в рамках сессии PPTP, инкапсулируются непосредственно в пакеты IP с помощью заголовка Generic Routing Protocol (GRE). Пакет, полученный в результате инкапсуляции, показан на рисунке:



Виртуальные частные сети: **PPTP**

Для организации VPN на основе **PPTP** не требуется больших затрат и сложных настроек: достаточно установить в центральном офисе сервер PPTP, а на клиентских компьютерах выполнить необходимые настройки
Для объединения филиалов вместо настройки PPTP на всех клиентских станциях лучше выполнить настройки только на пограничном маршрутизаторе филиала, подключенном к Интернет, для пользователей все абсолютно прозрачно.

Примером таких устройств могут служить многофункциональные Интернет-маршрутизаторы и шлюзы **D-Link**: **DI-524***,**DI-604****, **DI-624****,**DI-634, DI-804V**, **DI-824vup+**
*,** с суффиксом IP
*** с суфиксом S

Виртуальные частные сети: **PPPoE**

Технология **PPPoE** сегодня является одной из самых дешевых при предоставлении пользователям доступа к услугам Интернет на базе Ethernet и при использовании технологии DSL.

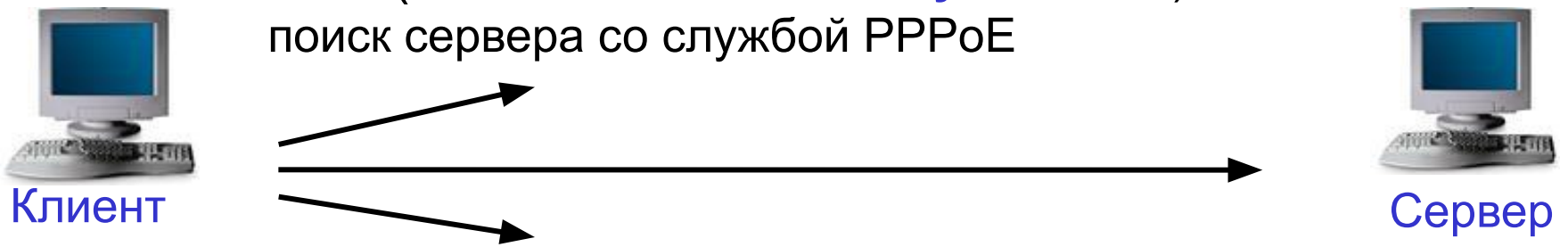
PPPoE запускает сессию PPP поверх сети Ethernet. При этом будет поддерживаться аутентификация пользователей по протоколам PAP и CHAP, динамическое выделение IP-адресов пользователям, назначение адреса шлюза, DNS-сервера и т.д.

Принципом работы **PPPoE** является установление соединения **"точка-точка" поверх общей среды Ethernet**, поэтому процесс функционирования PPPoE разделен на две стадии. И ограничена одним доменом коллизий

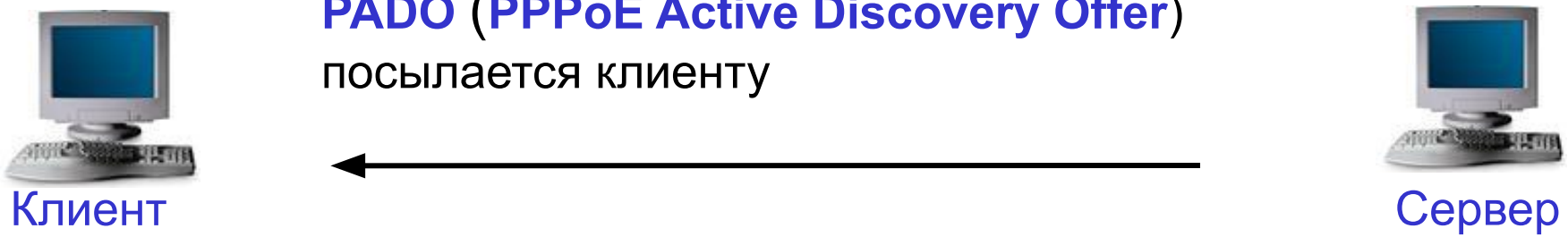
Виртуальные частные сети: **PPPoE**

Стадия установления соединения

клиент посылает широковещательный запрос **PADI** (**PPPoE Active Discovery Initiation**) на поиск сервера со службой PPPoE



Ответный пакет от сервера доступа **PADO** (**PPPoE Active Discovery Offer**) посылается клиенту



Виртуальные частные сети: **PPPoE**

Стадия установления соединения (продолжение)

Клиент

клиент выбирает нужный ему сервер доступа и посылает пакет **PADR** (**PPPoE Active Discovery Request**) с информацией о требуемой службе, имя провайдера и т.д.

Сервер

сервер доступа подготавливается к началу PPP сессии и посылает клиенту пакет PADS (**PPPoE Active Discovery Session-confirmation**).

Клиент

Сервер

Стадия установленной сессии

Если все запрашиваемые клиентом службы доступны, то начинается второй этап - стадия установленной сессии. Если требуемые клиентом услуги не могут быть предоставлены, клиент получает пакет PADS с указанием ошибки в запросе услуги.

Клиенту можно назначить динамический IP- адрес из пула адресов сервера, установить настройки шлюза и DNS-сервера. При этом на сервере доступа клиенту соответственно ставится виртуальный интерфейс.

Завершение соединения PPPoE происходит по инициативе клиента или концентратора доступа при помощи посылки пакета PADT (PPPoE Active Discovery Terminate).

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:

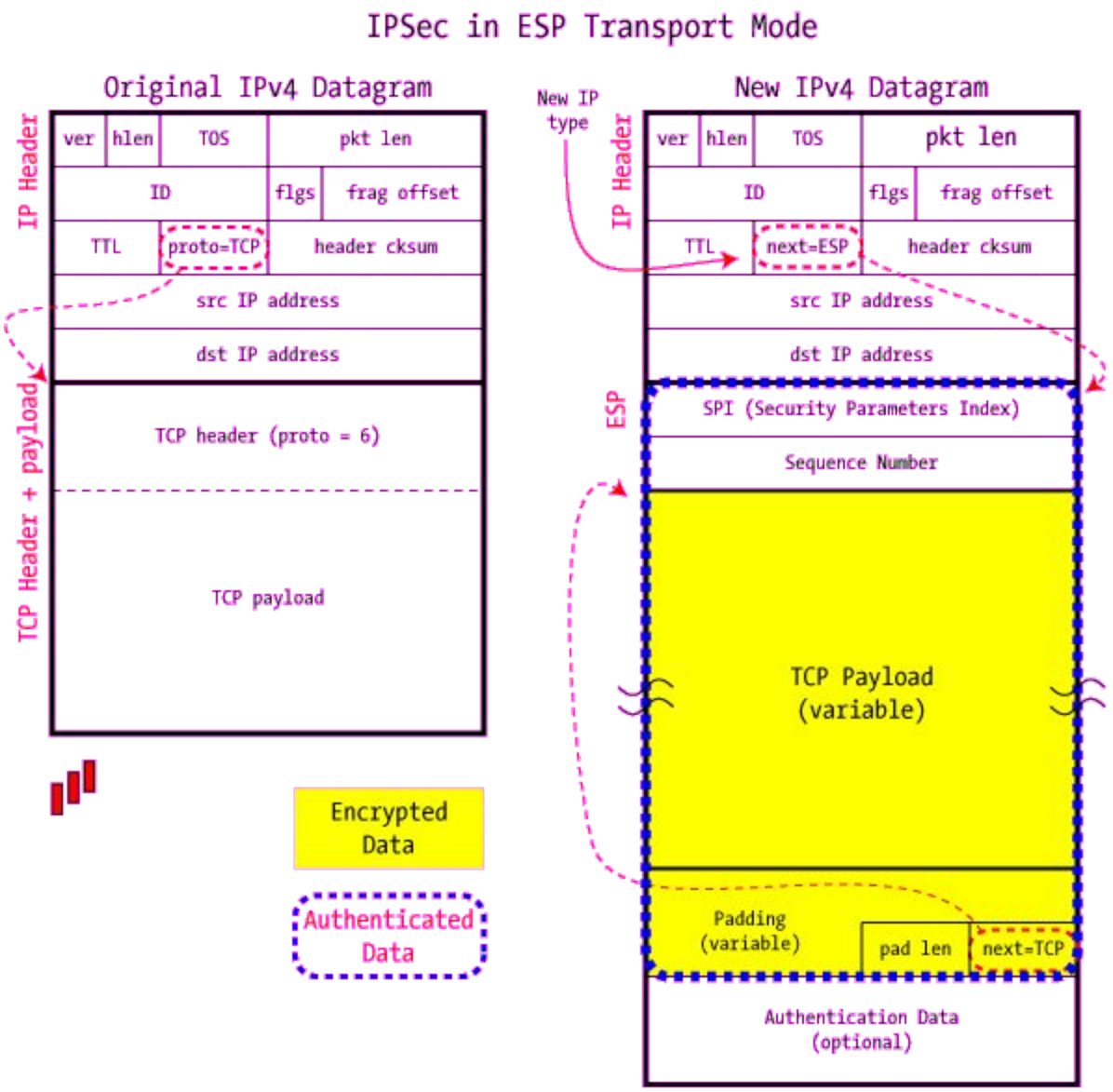
- аутентификация конечных точек канала
- выбираются параметры защиты данных (алгоритм шифрования, сессионный ключ и др.)
- согласование объединяемых подсетей

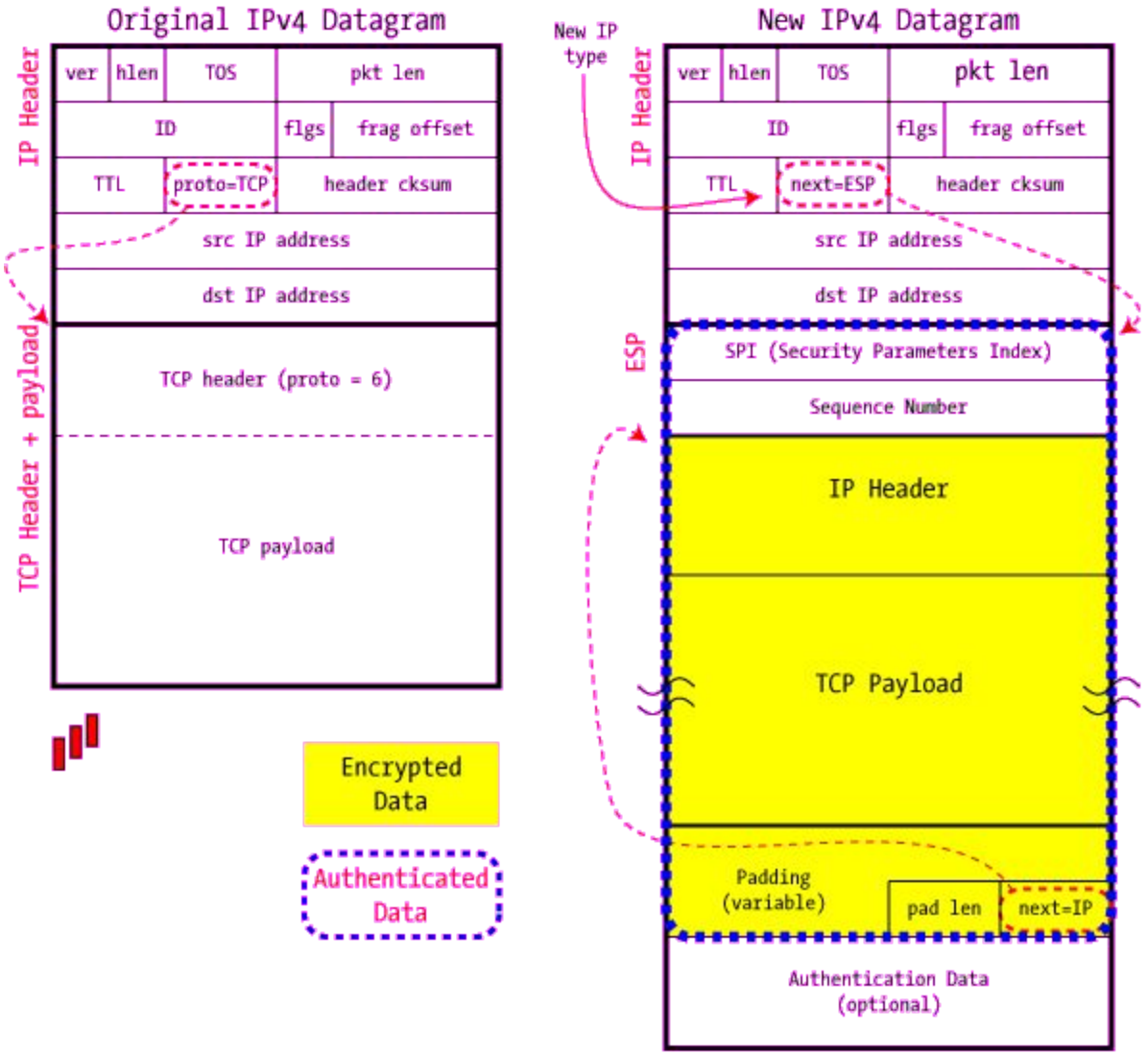
Виртуальные частные сети: **IPSec**

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.

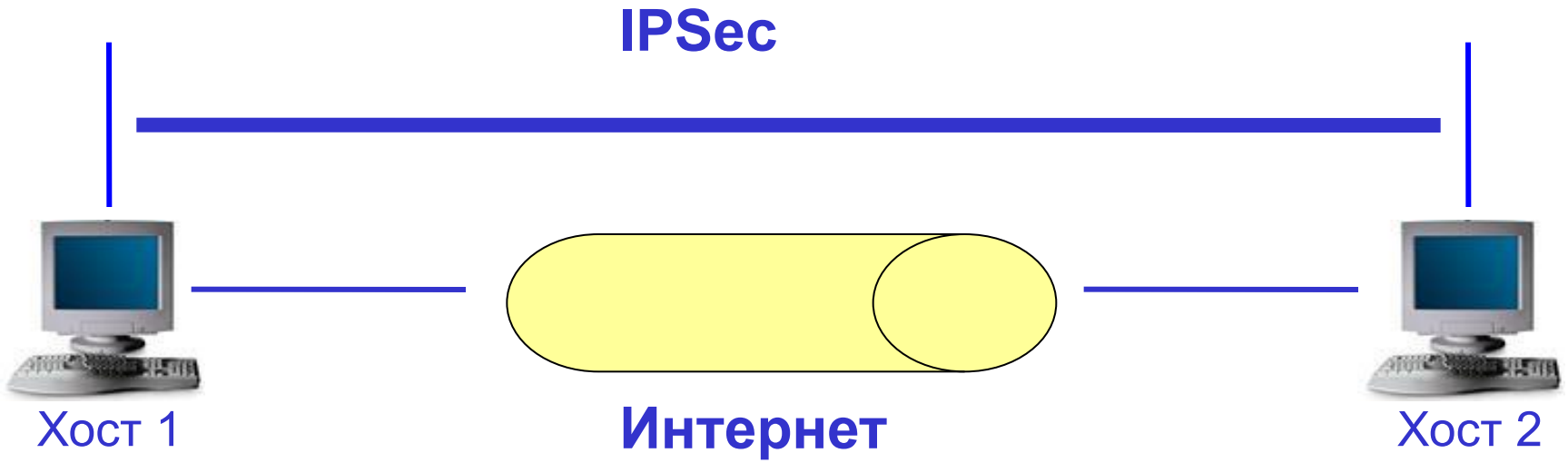

IPSec in ESP Transport Mode
Original IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
TCP Header + payload
TCP header (proto = 6)
TCP payload
Encrypted Data
Authenticated Data
New IPv4 Datagram
New IP type
IP Header
ver
hlen
TOS
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**

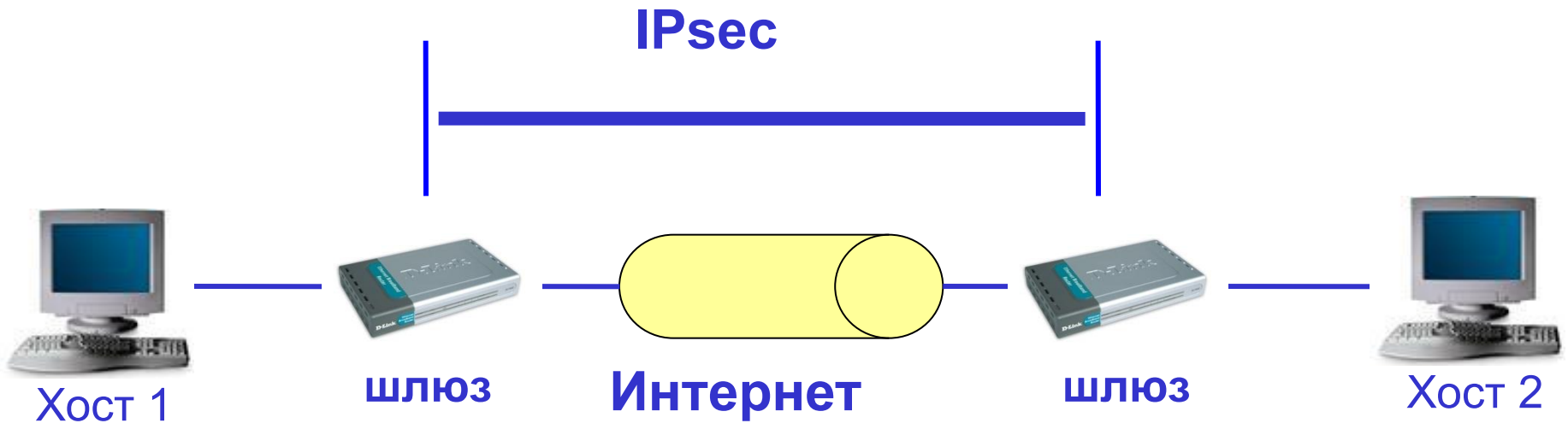
Существуют две основные схемы применения IPSec, отличающиеся ролью узлов, образующих защищенный канал.

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



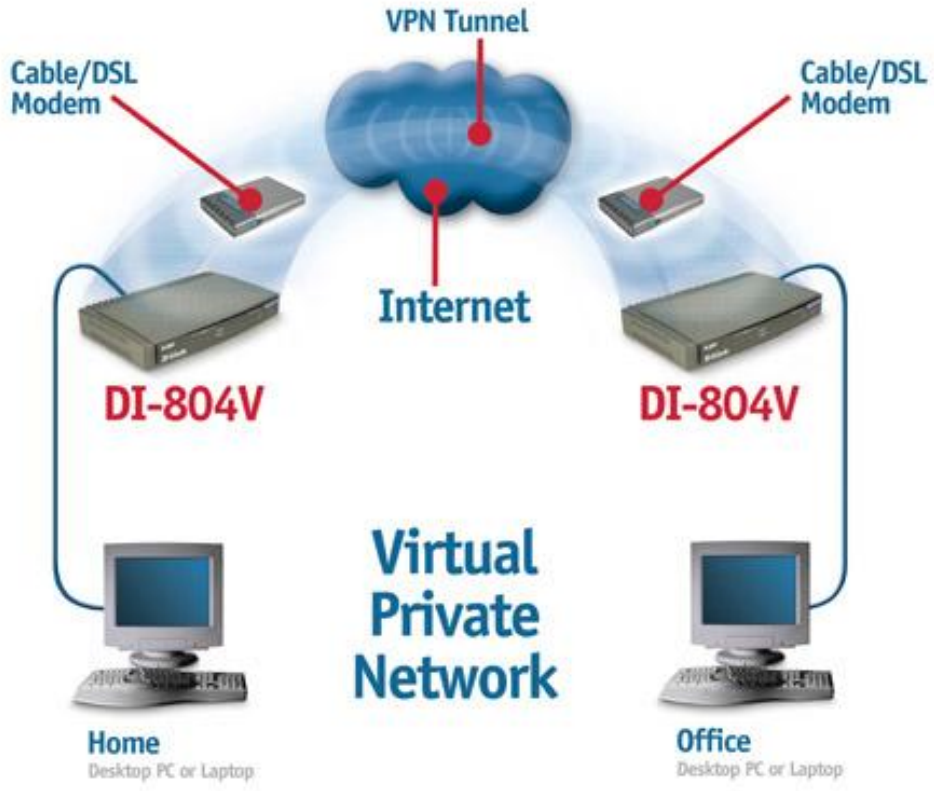
Виртуальные частные сети: **IPSec**

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.

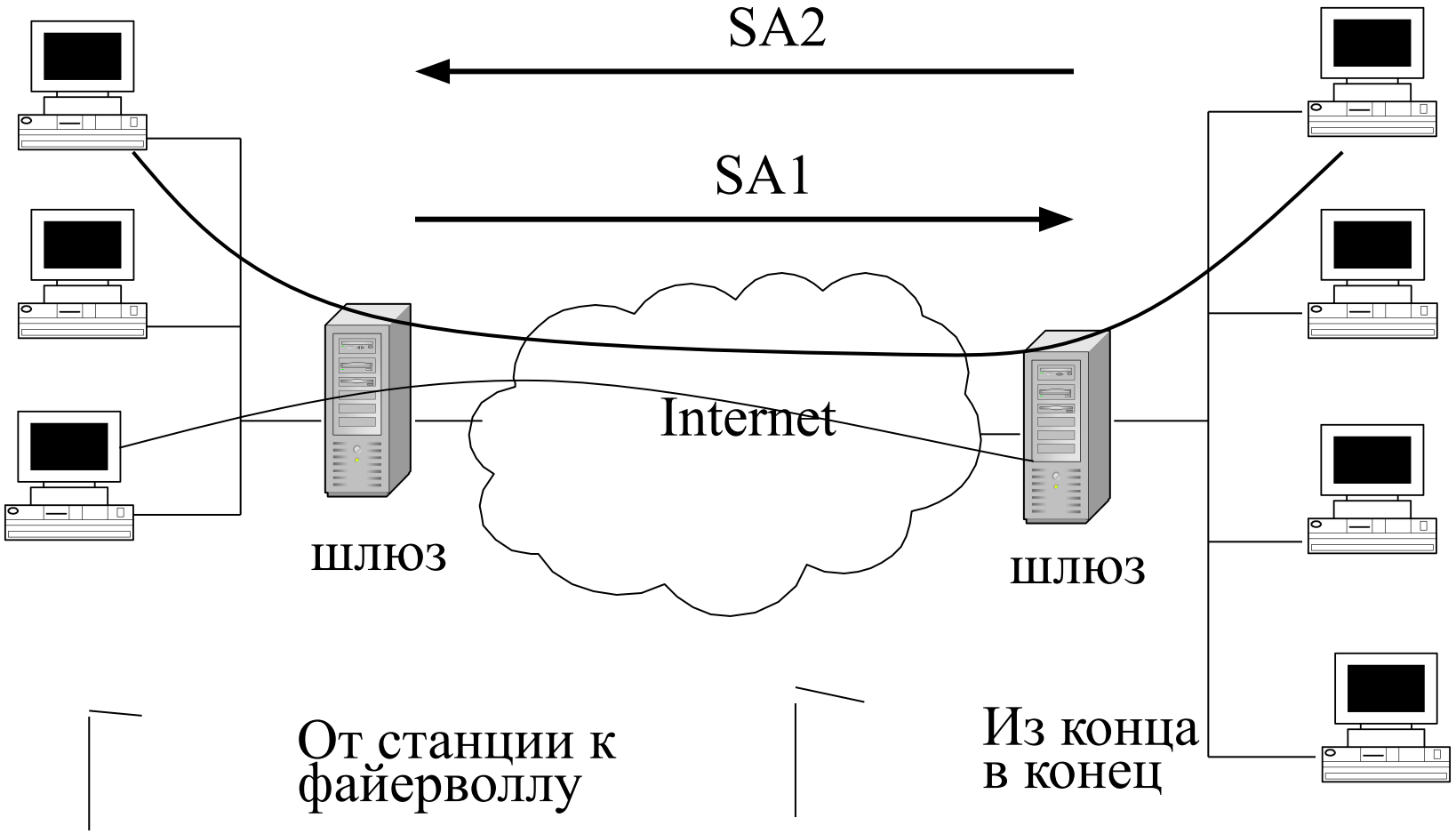


Виртуальные частные сети: **IPSec**

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**.



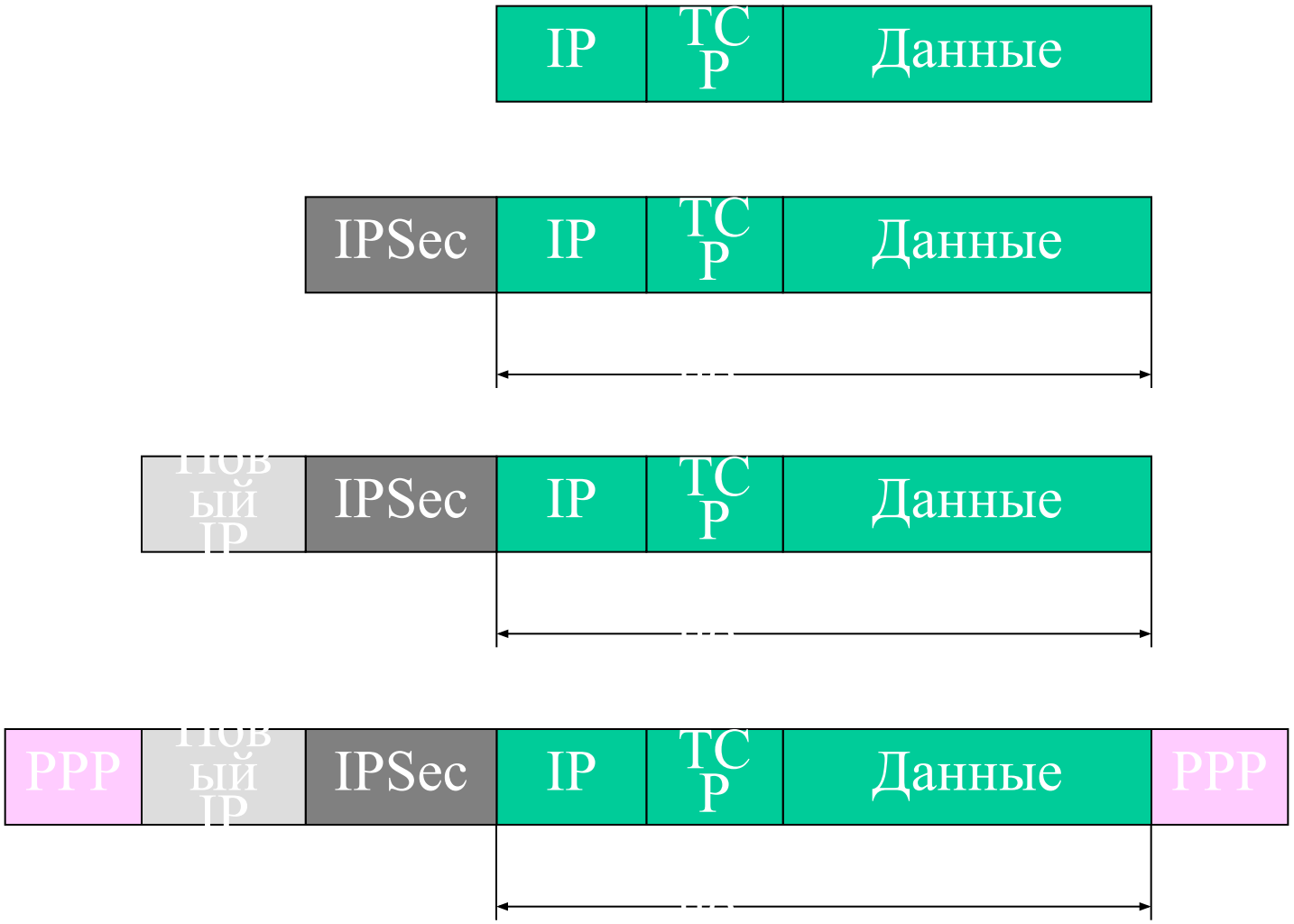
Определение SA



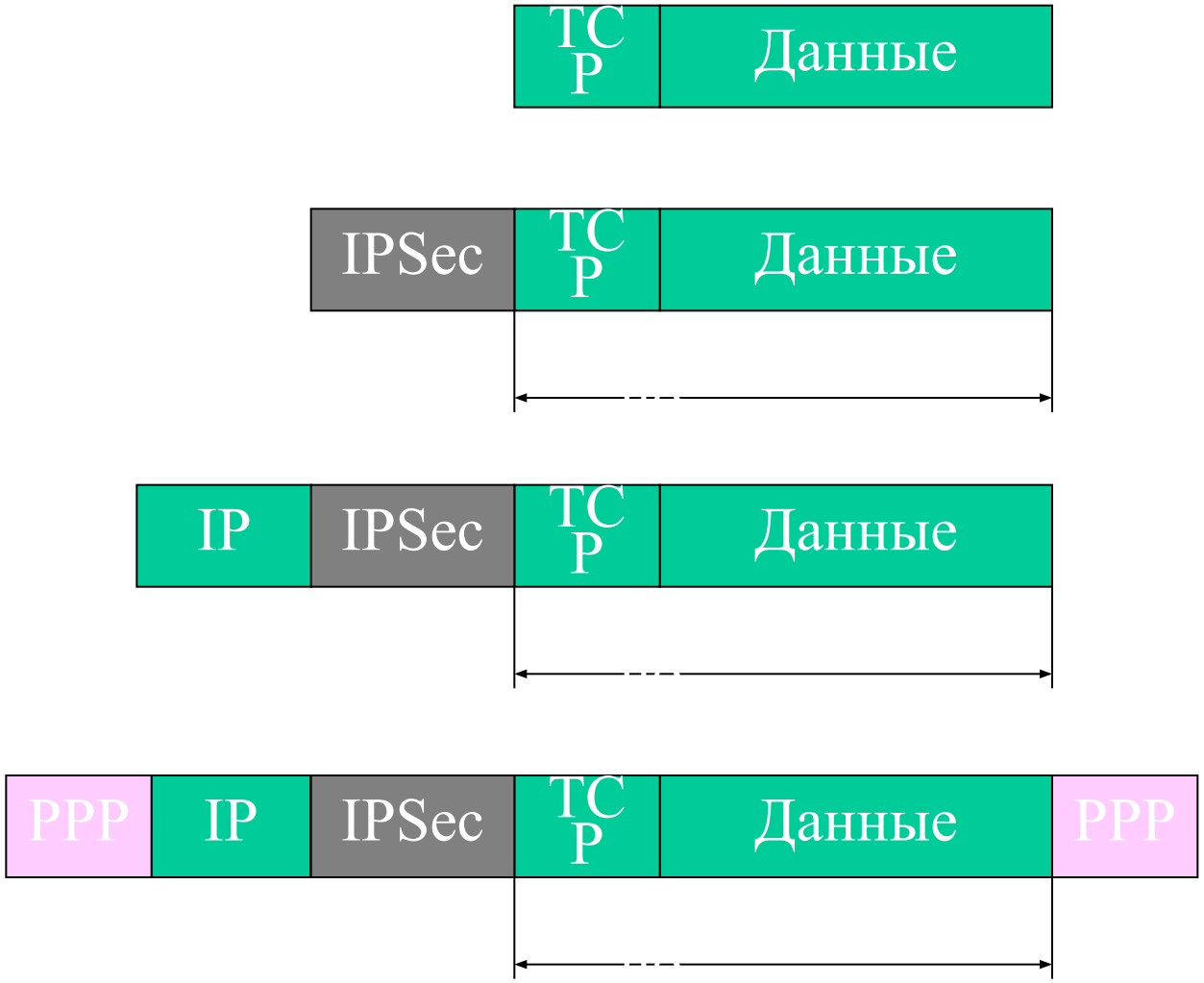
Режимы IPSec

- 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

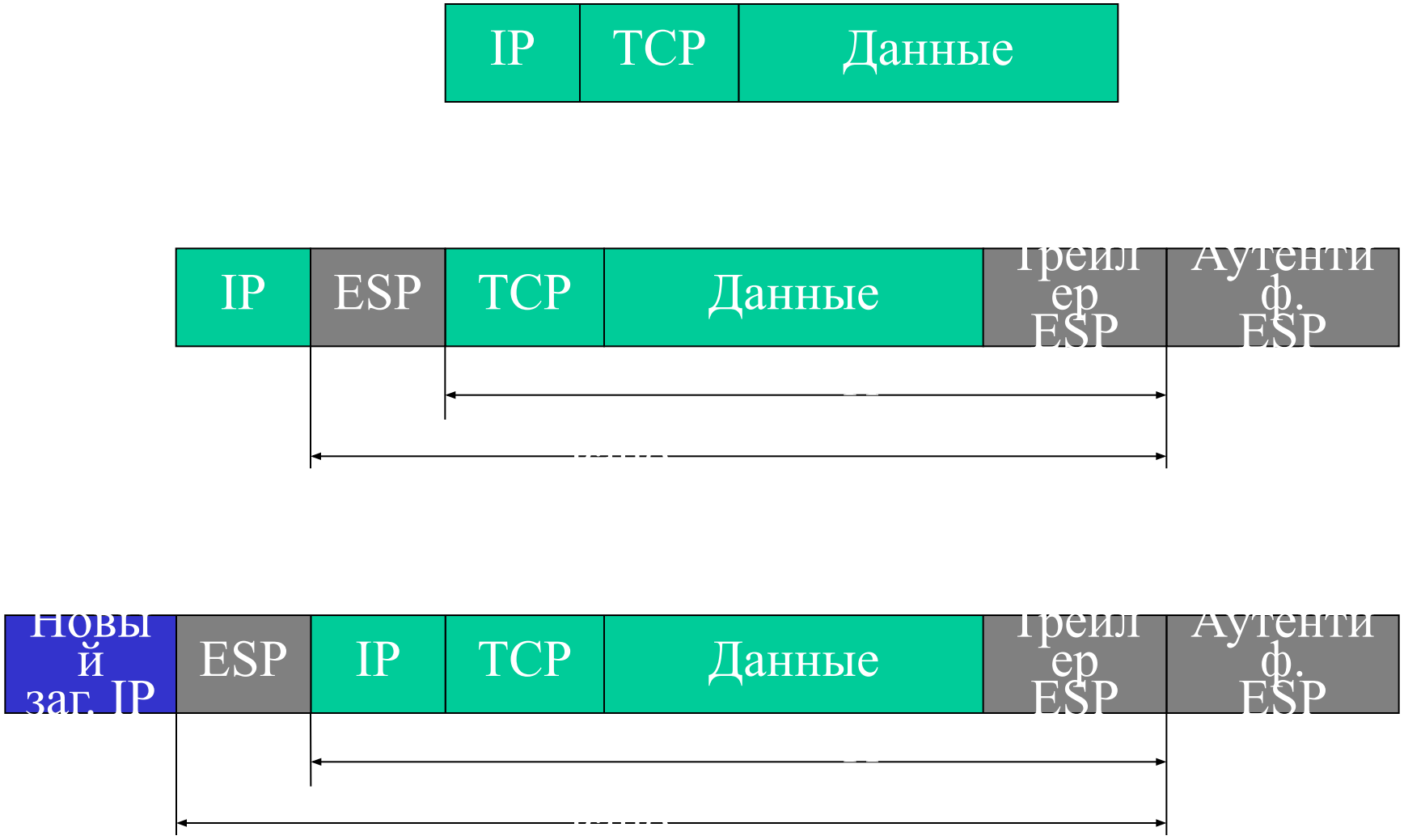
Инкапсуляция IPSec для туннельного режима



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.

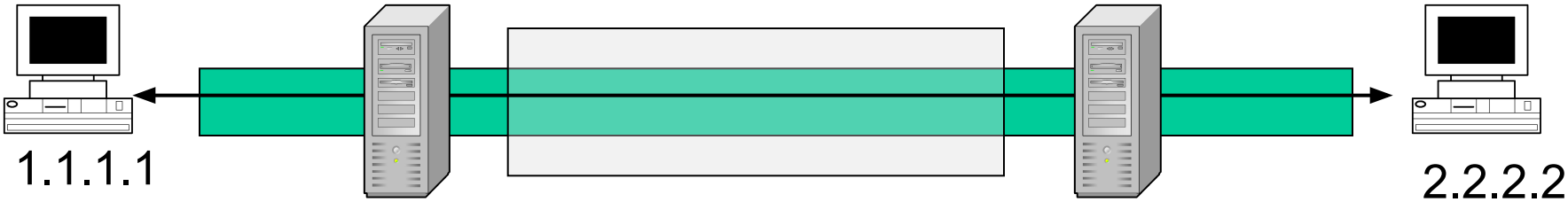
Правила безопасности

- 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

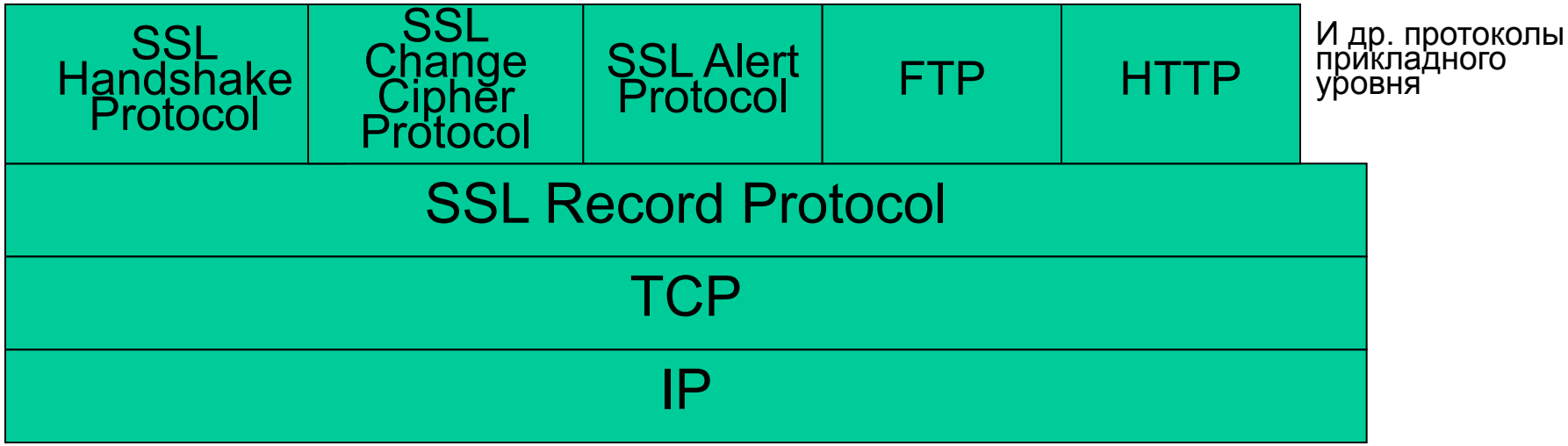
TCP 2.2.*.*: any 1.1.*.*: any protect
TCP 2.2.2.2: any 1.1.1.1: any AH transport

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)

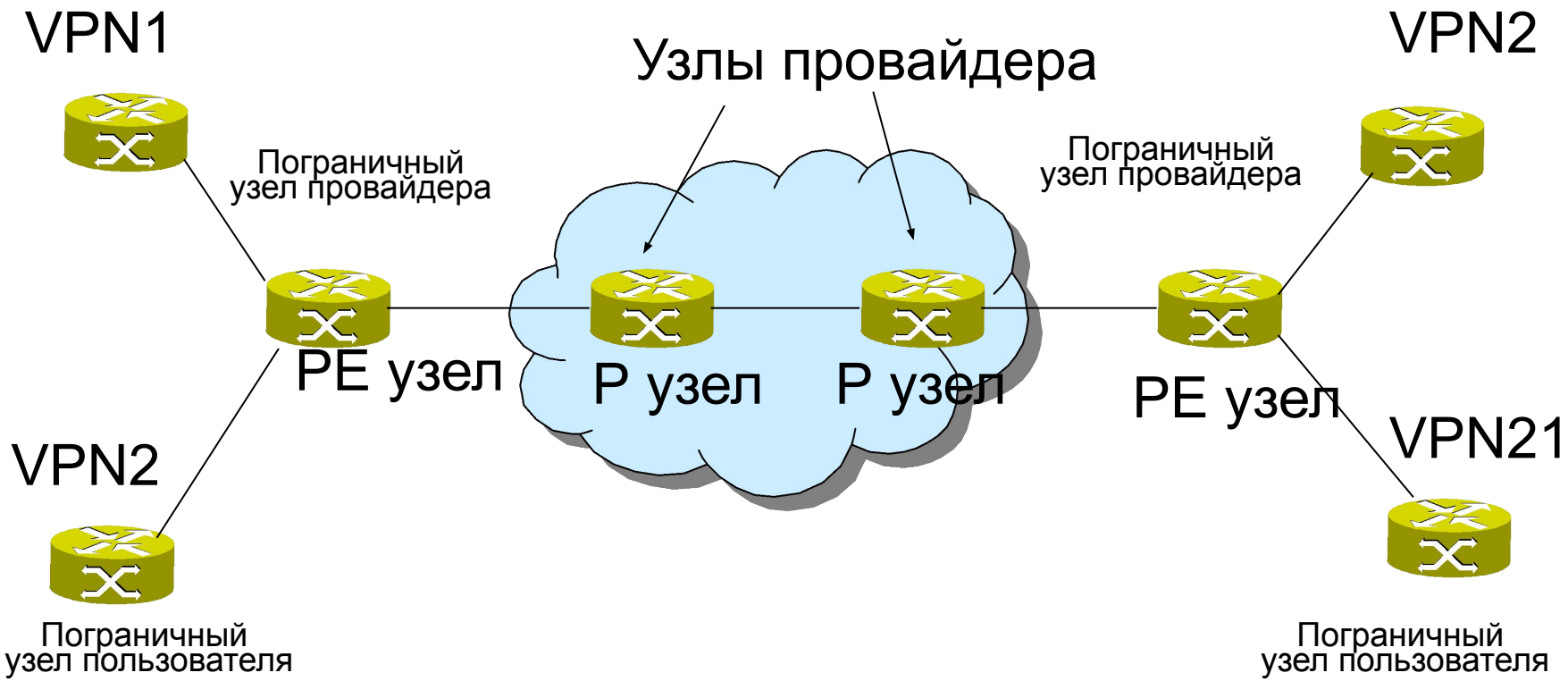
Организация VPN/MPLS

VPN/MPLS – хорошо масштабируемое решение.

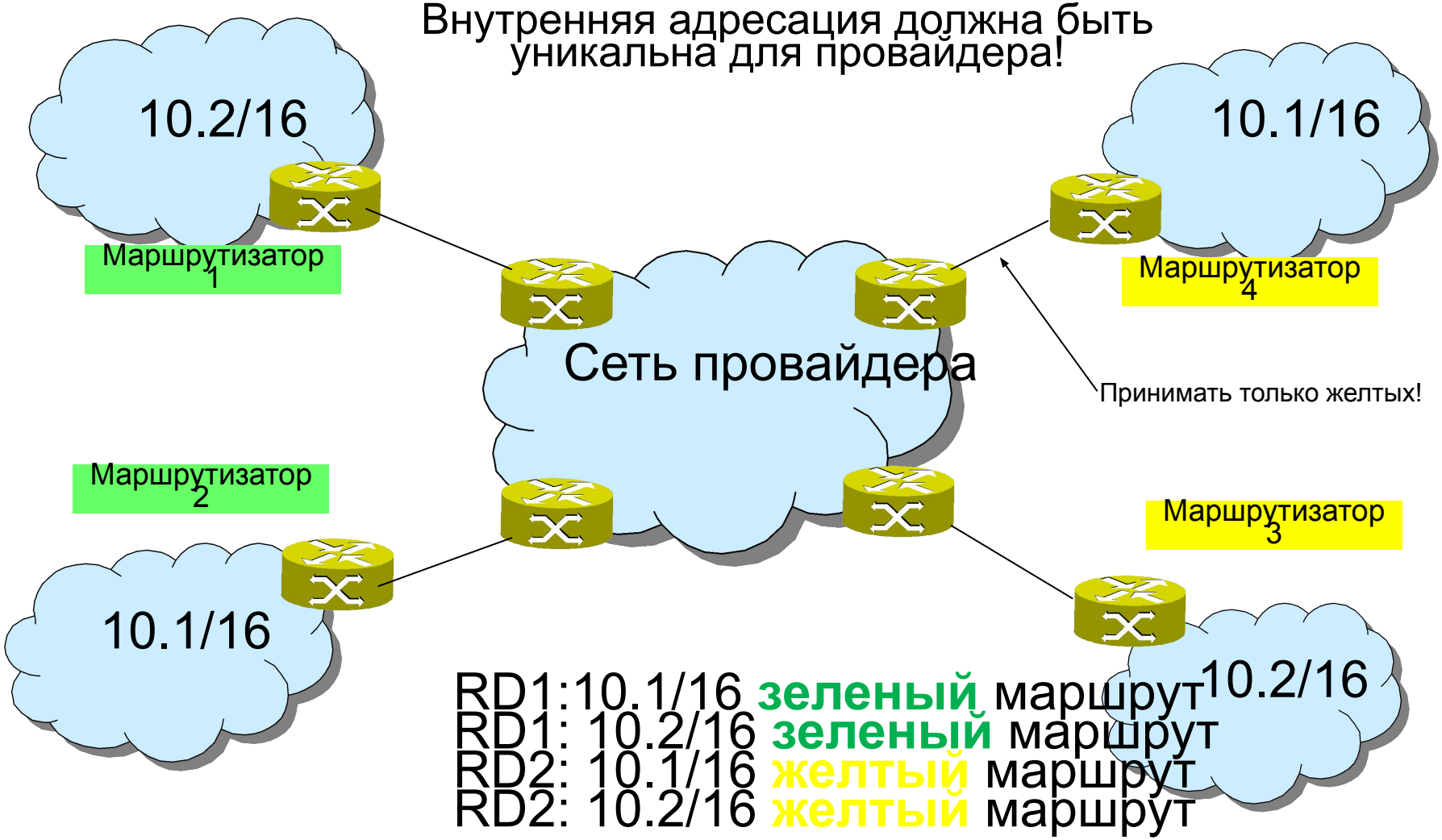
Рекомендация RFC 2547bis (модель IETF):

- 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

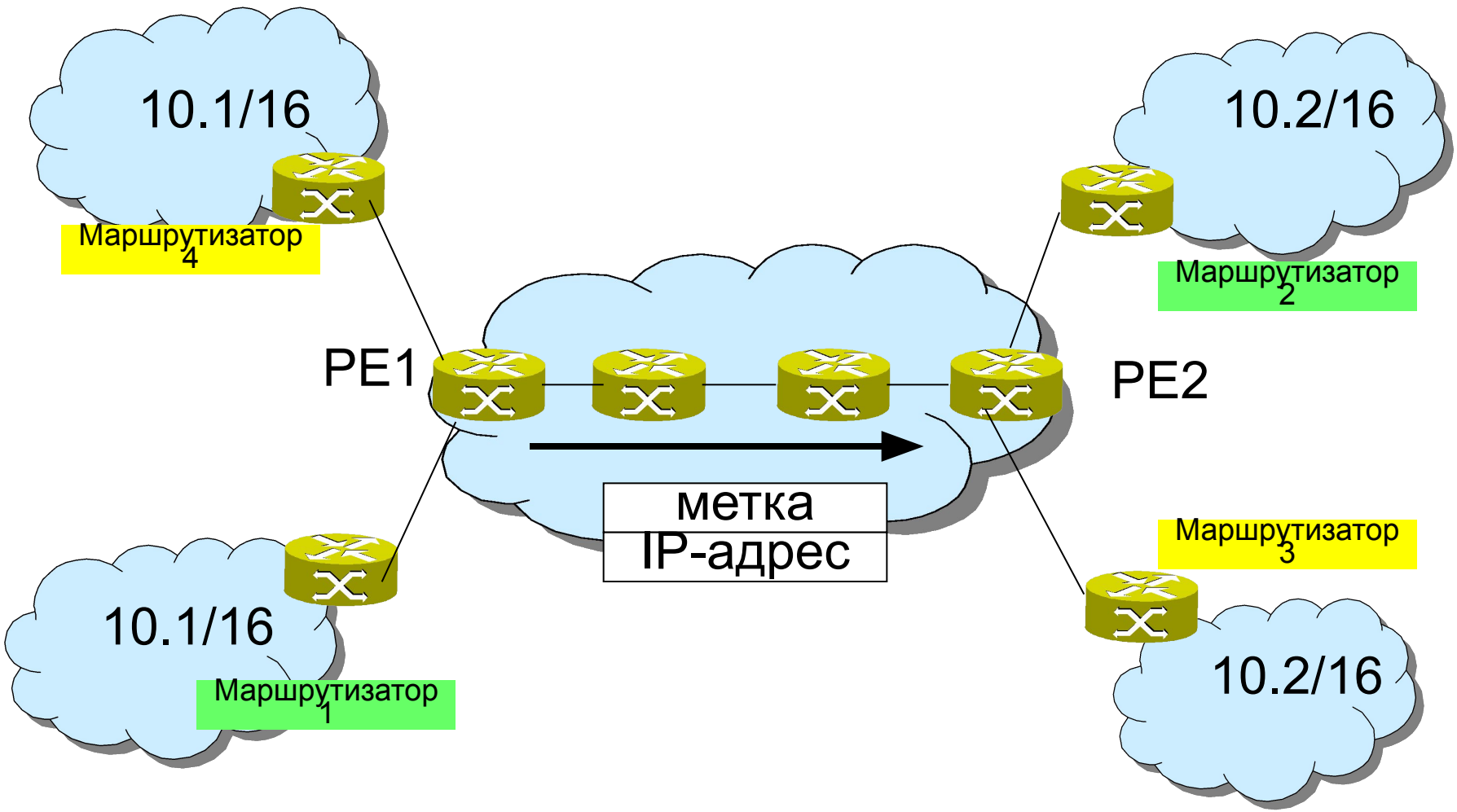


Адресация VPN

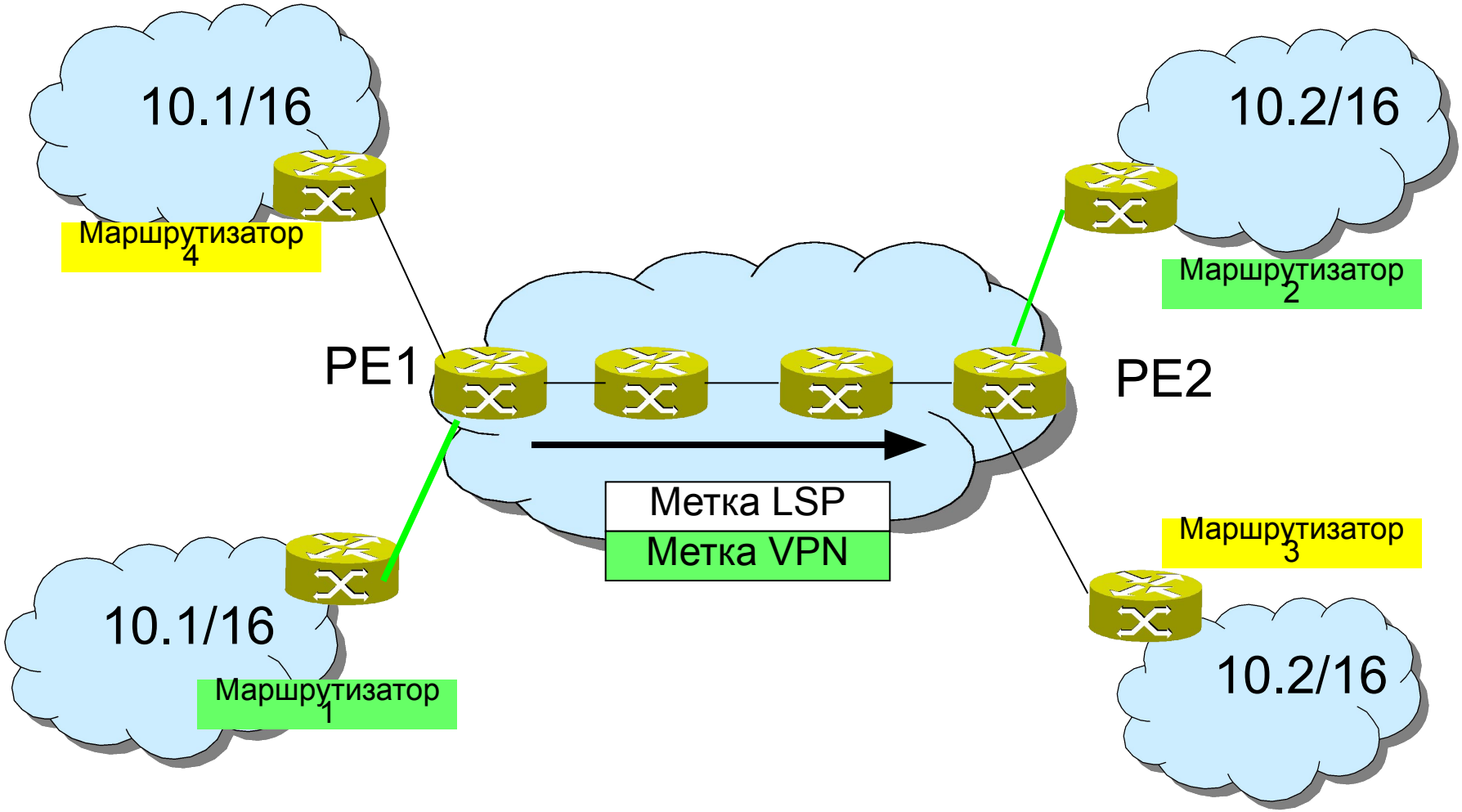


- **RD – Route Distinguisher** – признак маршрута. Используется для определения конкретных маршрутов. Это новый тип адреса.
- Основная идея – сделать неуникальные адреса уникальными, заменив группы IP-адресов на RD.
- Способ: совмещение IP-адреса и некоторого уникального идентификатора. Таким образом, 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



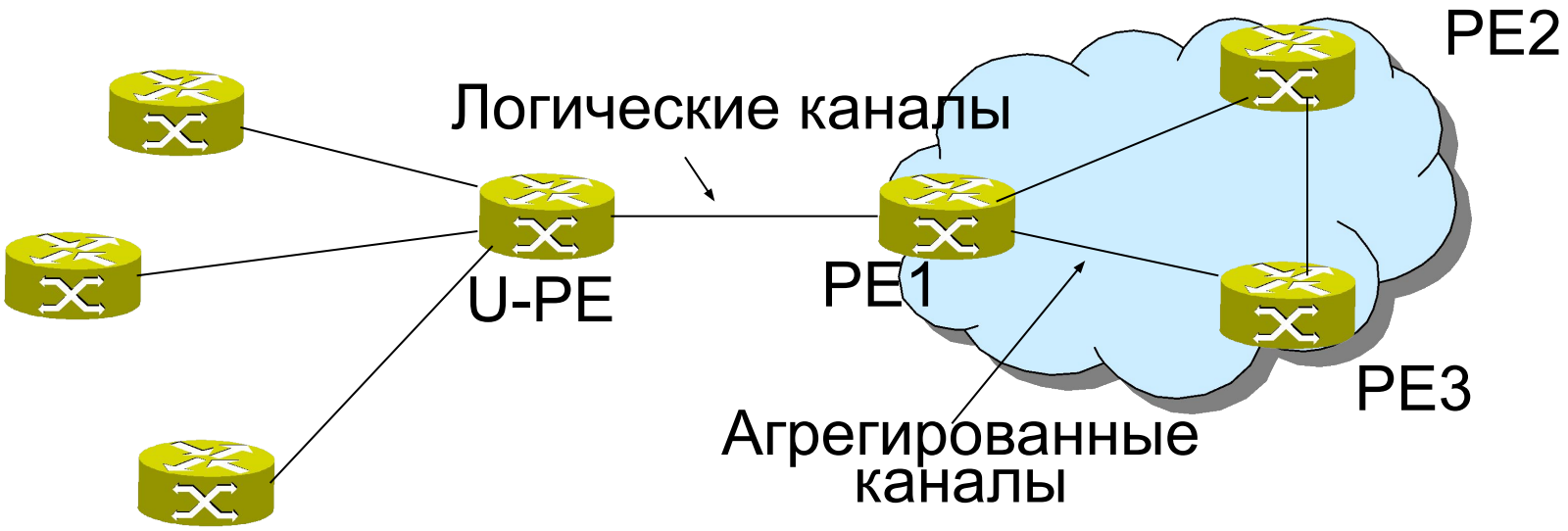
Использование метки VPN



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.



Интернет-маршрутизаторы D-Link

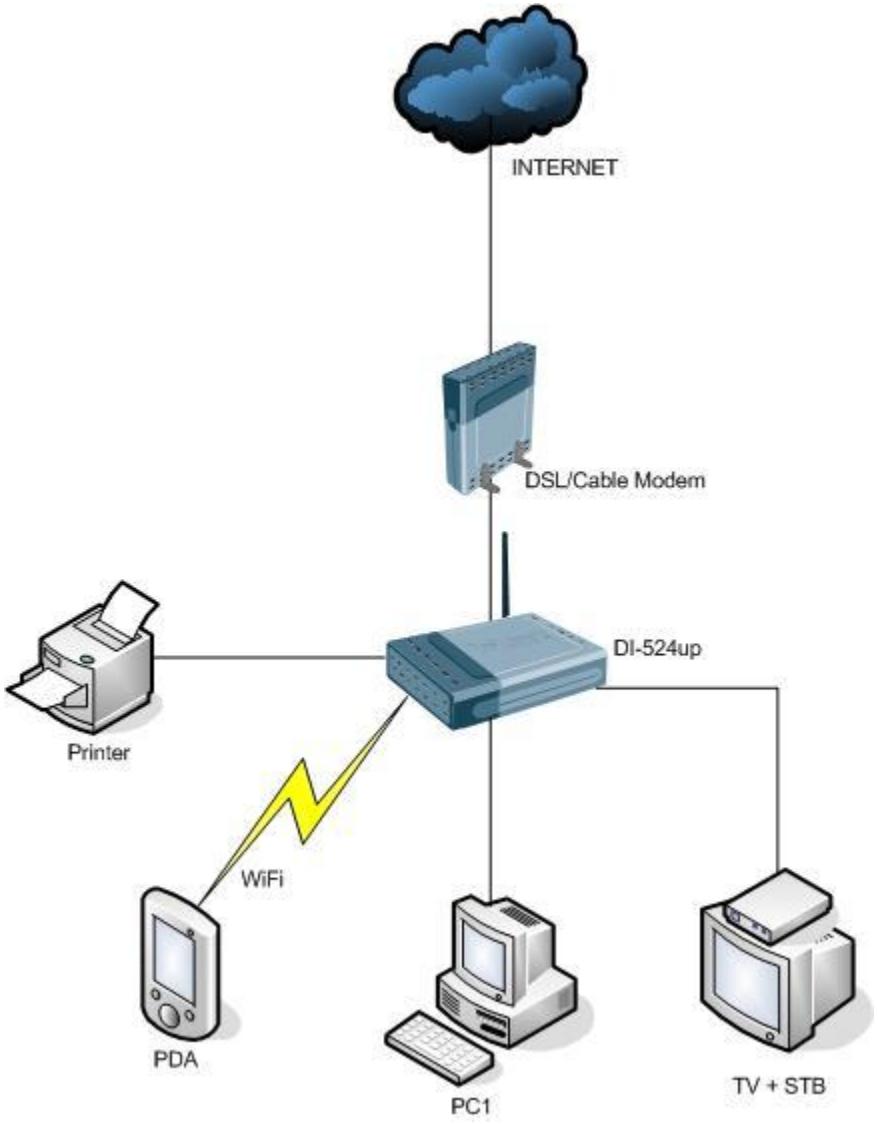
Модель	WAN	LAN	ADSL	Дополнительные функции
DI-524up	1 Fast Ethernet	4 FastEthernet	+	USB принт сервер, беспроводная точка доступа, работа с Multicast
DI-604	1 Fast Ethernet	4 FastEthernet	+	Internet Gateway
DI-624	1 Fast Ethernet	4 FastEthernet	+	Беспроводная точка доступа
DI-624s	1 Fast Ethernet	4 FastEthernet	+	Беспроводная точка доступа, WebServer, FTPServer, SMBServer(FAT32 lim)
DI-634m	1 Fast Ethernet	4 FastEthernet	+	Беспроводная точка доступа с технологией MIMO
DI-804hv	1 Fast Ethernet	4 FastEthernet	+	PPTP/L2TP Server, IPSec, DynIPSec, возможность резервирования/предоставления аналогового модема или мобильного телефона
DI-824vup+	1 Fast Ethernet	4 FastEthernet	+	резервирования/предоставления аналогового модема или мобильного телефона, беспроводная точка доступа, принт серверс с USB или LTP

Широкополосный шлюз: DI-524up

- 1 порт WAN – 10/100 Base-T для подключения к DSL или кабельному модему
- 4 порта LAN 10/100 Мбит/с
- 1 USB порт для принтера
- Беспроводная точка доступа

Применение DI-524up

Устройство позволяет осуществлять Одновременный выход в Интернет небольшой локальной сети.
Благодаря наличию функции Multicast и IGMP
Proxy устройство может быть использовано для просмотра IP TV
Наличие беспроводного клиента позволяет Подключать устройства без дополнительной прокладки проводов



Характеристики DI-524up

- Обеспечение доступа в интернет всем компьютерам сети
- Оборудован 4-портовым коммутатором Fast Ethernet
- Поддержка VPN в режиме Path Trough: PPTP, L2TP, IPSec
- Встроенный клиент PPTP и PPPoE для установления VPN-тоннеля с провайдером иди центральным офисом
- Встроенный принт-сервер
- Межсетевой экран
- Беспроводная точка доступа
- Поддержка виртуального сервера с демилитаризованной зоной – DMZ
- Удобное управление через Web-интерфейс
- Поддержка Multicast

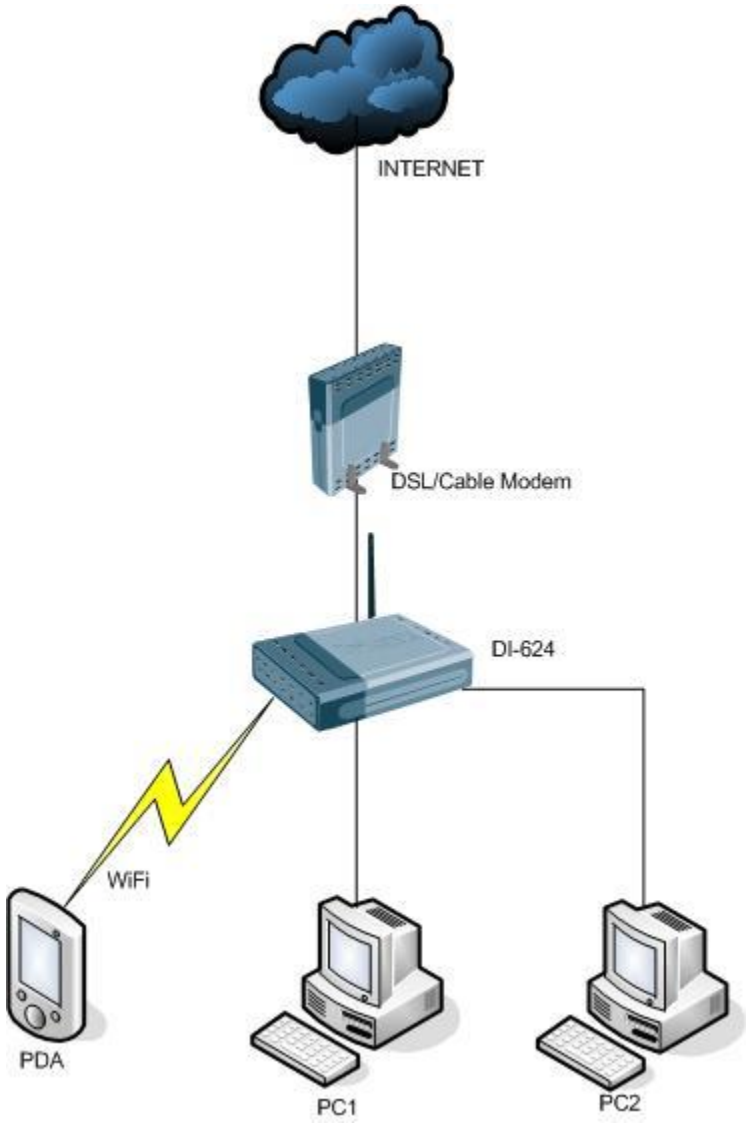
Широкополосный шлюз: DI-624

- 1 порт WAN – 10/100 Base-T для подключения к DSL или кабельному модему
- 4 порта LAN 10/100 Мбит/с
- Беспроводная точка доступа

Применение DI-624

Устройство может быть использовано для предоставления доступа в Интернет небольшой локальной сети

Наличие беспроводной точки доступа обеспечивает подключение клиентов без дополнительной прокладки проводов



Возможности DI-624

- Обеспечение доступа в интернет всем компьютерам сети
- Оборудован 4- х портовым коммутатором Fast Ethernet
- Поддержка VPN в режиме Path Trough: PPTP, L2TP, IPSec
- Встроенный принт-сервер
- Межсетевой экран
- Беспроводная точка доступа
- Поддержка контроля доступа
- Поддержка виртуального сервера с демилитаризованной зоной – DMZ
- Удобное управление через Web-интерфейс

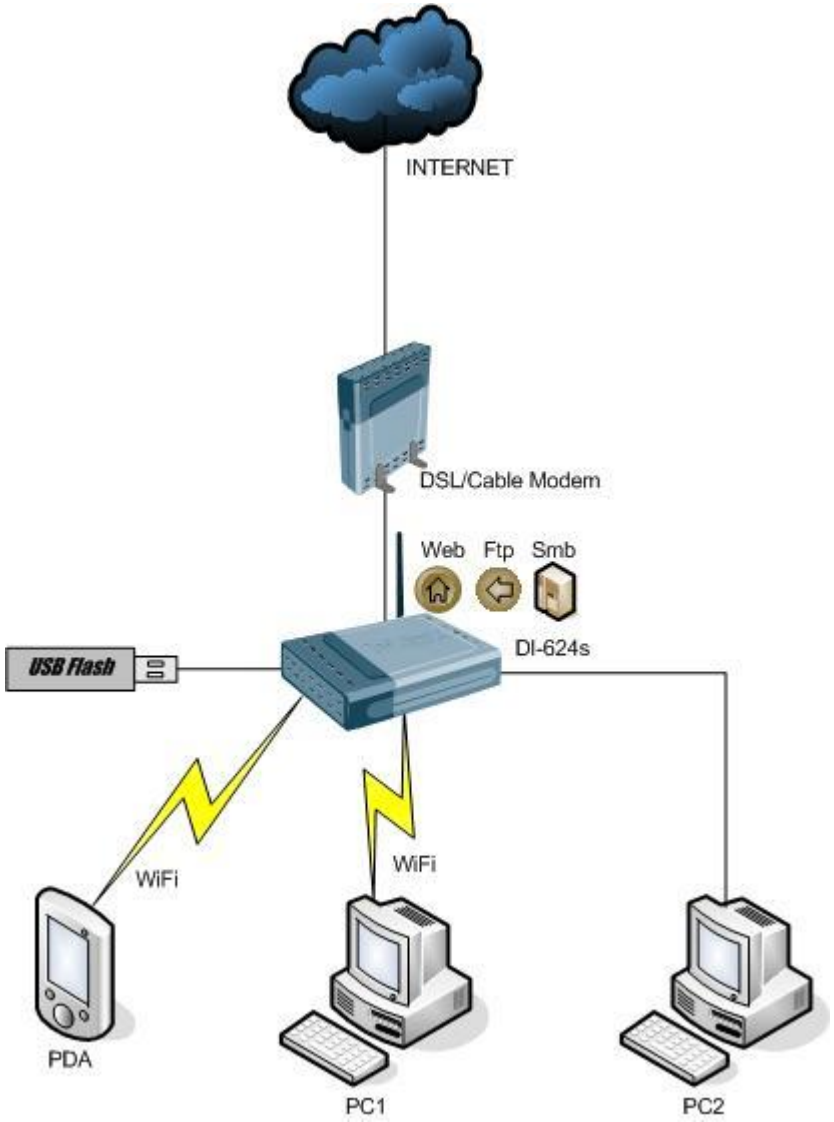
Широкополосный шлюз: DI-624s

- 1 порт WAN – 10/100 Base-T для подключения к DSL или кабельному модему
- 4 порта LAN 10/100 Мбит/с
- Беспроводная точка доступа
- USB порт для подключения внешнего носителя

Применение DI-624s

Устройство может быть использовано для предоставления выхода в Интернет небольшой локальной сети. Наличие Беспроводной точки доступа обеспечивает подключение клиентов без дополнительной прокладки кабелей.

Возможность подключения внешнего источника хранения информации(USB) позволяет создавать собственные Web Сервера,FTP Сервера и Файл серверы. Что даёт возможность не привязывать работу сервисов к определенному компьютеру



Возможности DI-624s

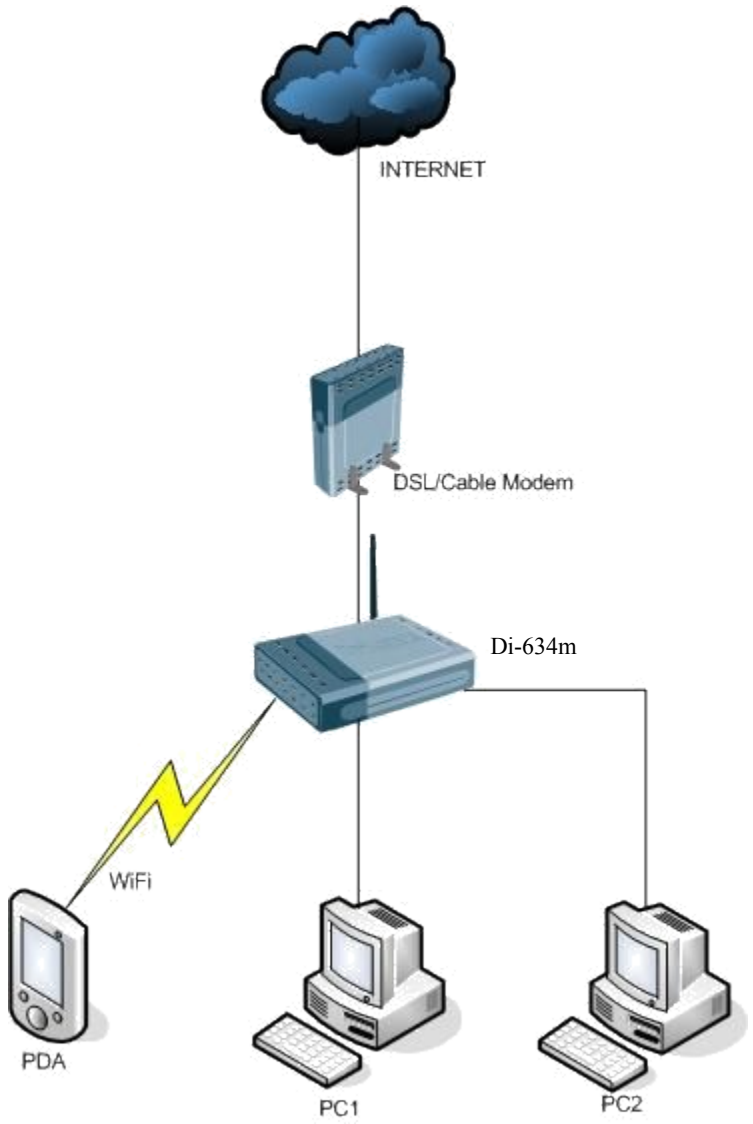
- Доступ в Интернет как для проводных, так и для беспроводных клиентов
- Встроенный 4- х портовый коммутатор Fast Ethernet
- Поддержка VPN-клиентов(PPTP/PPPoE/L2TP)
- Межсетевой экран
- Беспроводная точка доступа
- Поддержка контроля доступа с возможностью задания расписания действия правил доступа
- Поддержка виртуального сервера с демилитаризованной зоной – DMZ
- WebServer,FTPServer,SMBServer – FAT32
- Удобное управление через Web-интерфейс

Интернет маршрутизатор: DI-634M

- 1 порт WAN – 10/100 Base-T для подключения к DSL, кабельному модему и Ethernet
- 4 порта LAN 10/100 Мбит/с
- Беспроводная точка доступа IEEE-802.11b MIMO с повышенной зоной покрытия

Применение DI-634m

Устройство предназначено для предоставления доступа в Интернет небольшой локальной сети состоящий как из проводных, так и беспроводных клиентов. Благодаря технологии MIMO устройство покрывает большую территорию, обеспечивая связь на скоростях до 108Мбит/с



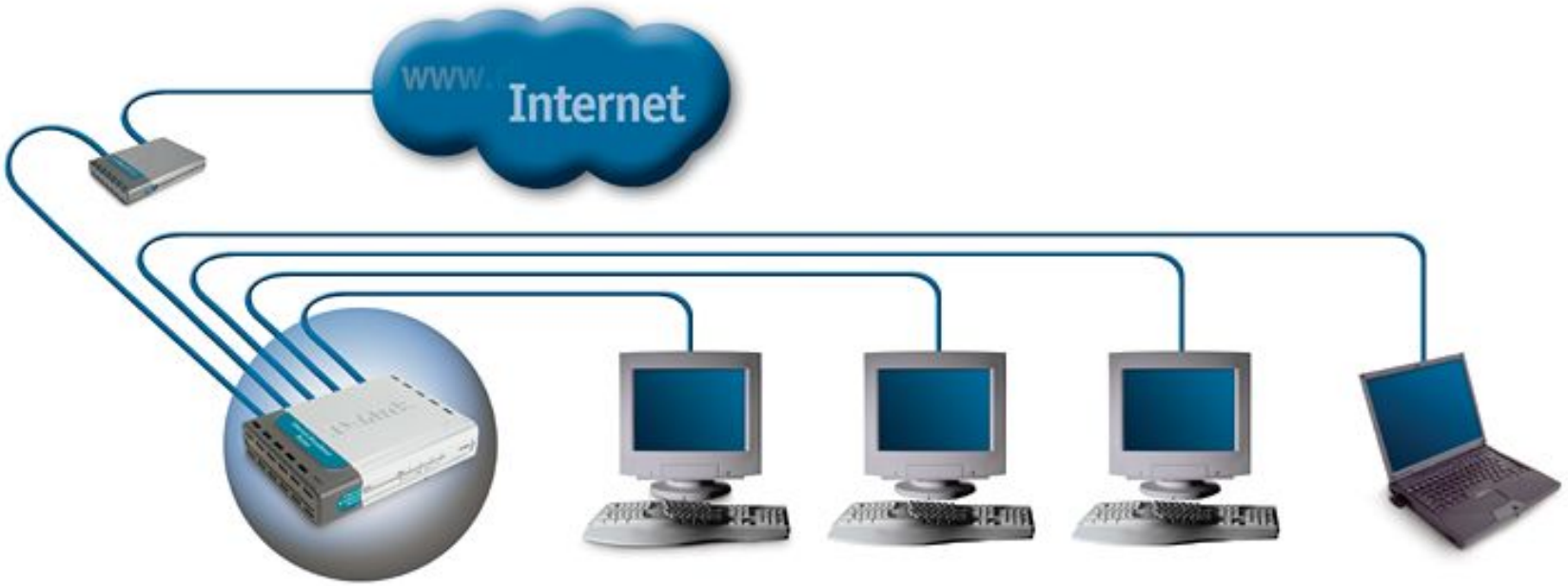
Возможности DI-634m

- Обеспечение доступа в интернет всем компьютерам сети
- Оборудован 4-х портовым коммутатором Fast Ethernet
- Поддержка VPN в режиме Path Trough: PPTP, L2TP, IPSec
- Межсетевой экран
- Имеет встроенную беспроводную точку доступа по технологии MIMO
- Поддержка виртуального сервера с демилитаризованной зоной – DMZ
- Удобное управление через Web-интерфейс

Интернет маршрутизатор: DI-604

- 1 порт WAN – 10/100 Base-T для подключения к DSL или кабельному модему
- 4 порта LAN 10/100 Мбит/с
- Расширенные функции межсетевого экрана
- Управление через Web-интерфейс

Применение DI-604

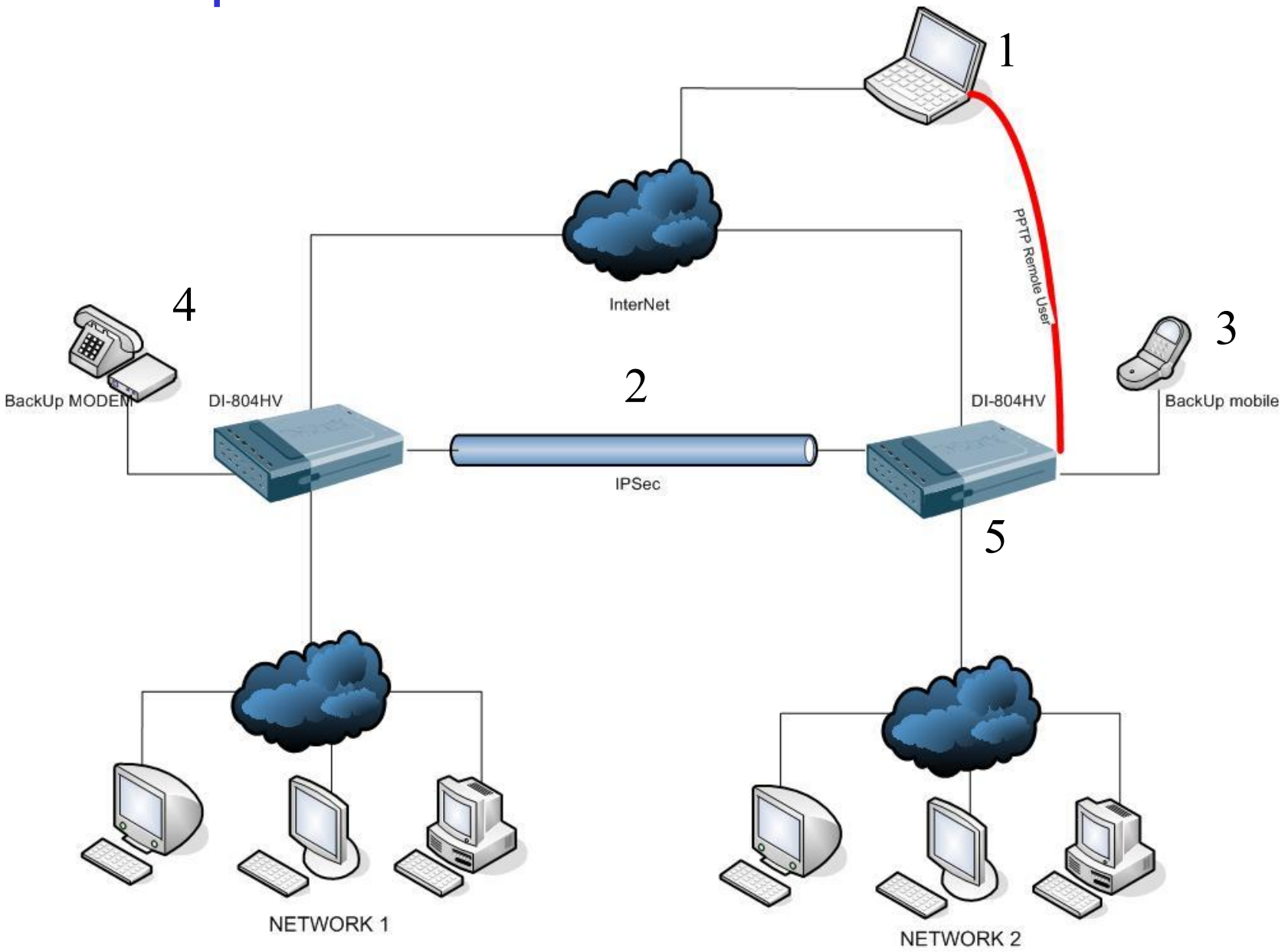


Разработанный специально для использования дома или в малом офисе, DI-604 позволяет быстро и легко подключиться к Интернет посредством DSL или кабельного модема

Интернет - маршрутизатор: DI-804HV

- 1 порт WAN – 10/100 Base-T для подключения к DSL,кабельному модему или Ethernet
- 4 порта LAN 10/100 Мбит/с
- Управление через Web-интерфейс
- Поддержка VPN: **до 40 туннелей IPSec**
- **PPTP/L2TP Сервер**

Применение DI-804V / DI-804HV



Многофункциональное устройство DI-804HV позволяет

1 Подключать к локальной сети удалённых пользователей

2 Объединять в единую сеть с использованием IPSec несколько филиалов

3-4 Резервировать или предоставлять доступ к интернет с помощью аналогового модема или сотового телефона (AT команды)

5 Обеспечивать доступ небольшой локальной сети к Интернет

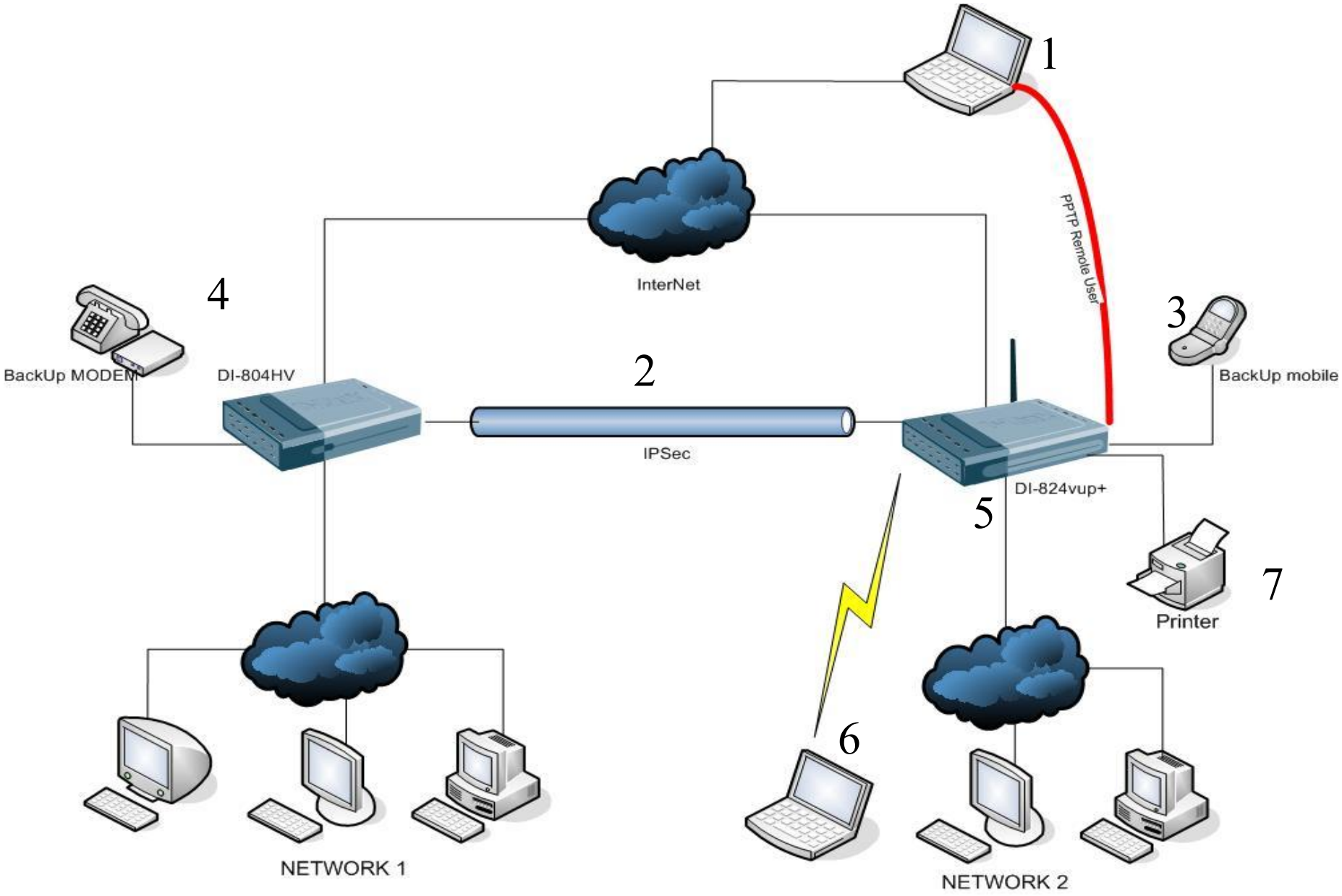
Характеристики DI-804HV

- WAN - порт 10/100 Мбит/с для подключения к глобальной сети посредством кабельного или ADSL-модема
- 4-портовый коммутатор 10/100Мбит/с Fast Ethernet для подключения к локальной сети
- PPTP/L2TP Сервер
- Встроенный межсетевой экран
- Встроенный клиент PPTP и PPPoE для установления VPN-тоннеля с провайдером иди центральным офисом
- Поддержка IPSec: до 40 туннелей
- Встроенный DHCP-сервер
- Порт RS-232 для подключения внешнего аналогового модема или мобильного телефона(AT comp.)
- Управление посредством Web-браузера

Интернет - маршрутизатор: DI-824vup+

- 1 порт WAN - 10/100Base-T для подключения к DSL, кабельному модему или Ethernet
- 4 порта LAN 10/100 Мбит/с
- Управление через Web-интерфейс
- Поддержка VPN: до 40 туннелей IPSec
- Беспроводная точка доступа
- Встроенный USB/LTP принт сервер
- Порт для подключения аналогового модема

Применение DI-824vup+



Многофункциональное устройство DI-824vup+ позволяет

1 Подключать к локальной сети удалённых пользователей

2 Объединять в единую сеть с использованием IPSec несколько филиалов

3-4 Резервировать или предоставлять доступ к Интернет с помощью аналогового модема или сотового телефона (AT команды)

5 Обеспечивать доступ небольшой локальной сети к Интернет

6 Подключать беспроводных клиентов

7 Использовать принт сервер для клиентов локальной сети

Характеристики DI-824vup+

- WAN - порт 10/100 Мбит/с для подключения к глобальной сети посредством кабельного, ADSL-модема или Ethernet
- 4-портовый коммутатор 10/100Мбит/с Fast Ethernet для подключения к локальной сети
- Беспроводная точка доступа
- Встроенный межсетевой экран
- Встроенный клиент PPTP и PPPoE для установления VPN-тоннеля с провайдером иди центральным офисом
- Поддержка IPSec: до 40 туннелей
- Встроенный PrintServer(USB/LTP)
- Встроенный DHCP-сервер
- Порт RS-232 для подключения внешнего аналогового модема
- Управление посредством Web-браузера

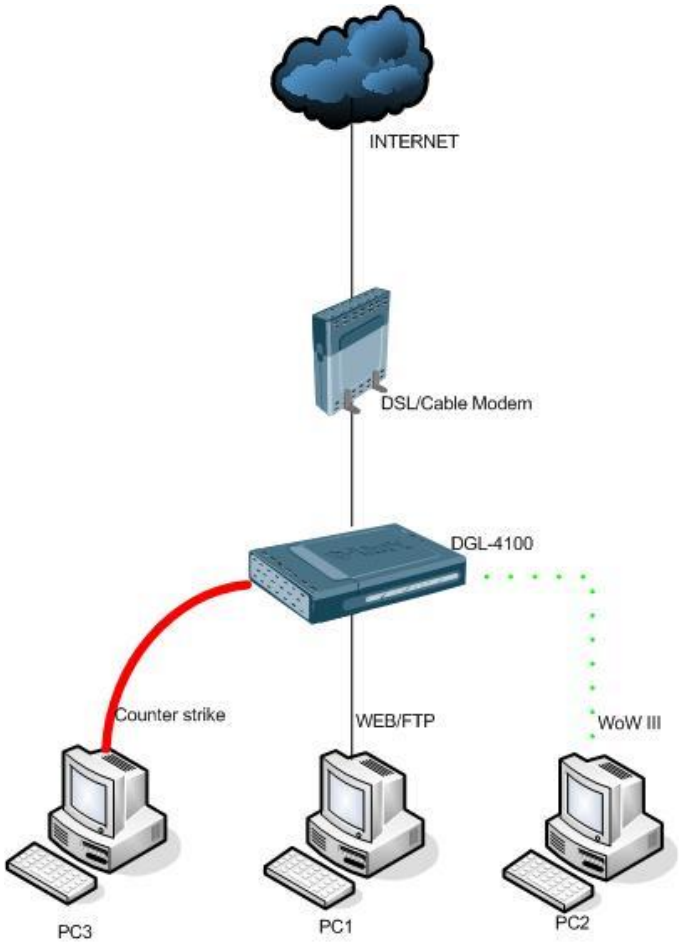
Маршрутизаторы для сетевых игр GamerLounge с технологией GameFuel

Игровой маршрутизатор DGL-4100

- 4 GigabitEthernet порта
- 1 Порт WAN 10/100
- Уникальная система приоритезации трафика, для выскоропроизводительных игр.
- Поддержка p2p клиентов
- Технология GameFuel, позволяющая выделять приложениям необходимую полосу пропускания
- 40 предустановленных настроек для игр

Применение DGL-4100

Использование уникальной технологии GameFuel, позволяет выделять определенным приложениям, например играм гарантированную полосу пропускания, что даёт возможность играть без разделения скорости с другими приложениями. 1Гб порты позволяют обменивается данными со скоростями до 125Мб/с



Характеристики DGL-4100

- WAN - порт 10/100 Мбит/с для подключения к глобальной сети посредством кабельного, ADSL-модема или Ethernet
- 4-портовый коммутатор 10/100/1000Мбит/с для подключения локальной сети
- Встроенный межсетевой экран
- Приоритизация трафика по приложению с помощью технологии GameFuel
- Встроенный firewall
- Встроенный DHCP-сервер
- Удобный интерфейс и помощник установки соединения
- Уникальная технология просмотра контента для ограничения просмотра данных по этическим соображениям
- Технология контроля трафика, обнаруживающая вторжения и вирусную активность

Игровой маршрутизатор DGL-4300

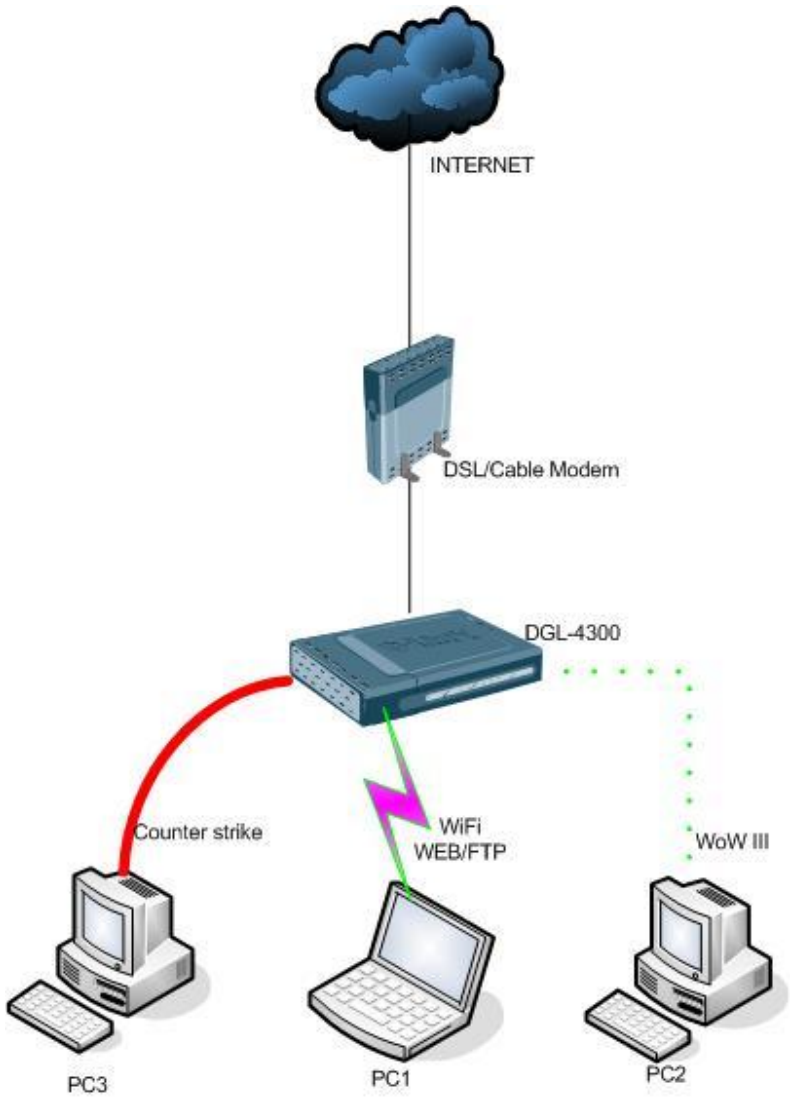
GAMEFUEL
PRIORITY

GAMERLOUNGE Wireless 108G
Gaming Router™

- 4 GigabitEthernet порта
- 1 Порт WAN 10/100
- Беспроводная точка доступа 108Мбит/с
- Поддержка p2p клиентов
- Технология GameFuel, позволяющая выделять приложениям необходимую полосу пропускания
- 40 предустановленных настроек для игр

Применение DGL-4300

Использование уникальной технологии GameFuel, позволяет выделять определенным приложениям, например играм гарантированную полосу пропускания, что даёт возможность играть без разделения скорости с другими приложениями. 1Гб порты позволяют обменивается данными со скоростями до 125Мб/с. Беспроводные клиенты работают на скоростях до 108Мбит/с



Характеристики DGL-4300

- WAN - порт 10/100 Мбит/с для подключения к глобальной сети посредством кабельного, ADSL-модема или Ethernet
- 4-портовый коммутатор 10/100/1000Мбит/с для подключения локальной сети
- Встроенный межсетевой экран
- Приоритизация трафика по приложению с помощью технологии GameFuel
- Встроенный firewall
- Беспроводная точка доступа 108Мбит/с
- Удобный интерфейс и помощник установки соединения
- Уникальная технология просмотра контента для ограничения просмотра данных по этическим соображениям
- Технология контроля трафика, обнаруживающая вторжения и вирусную активность

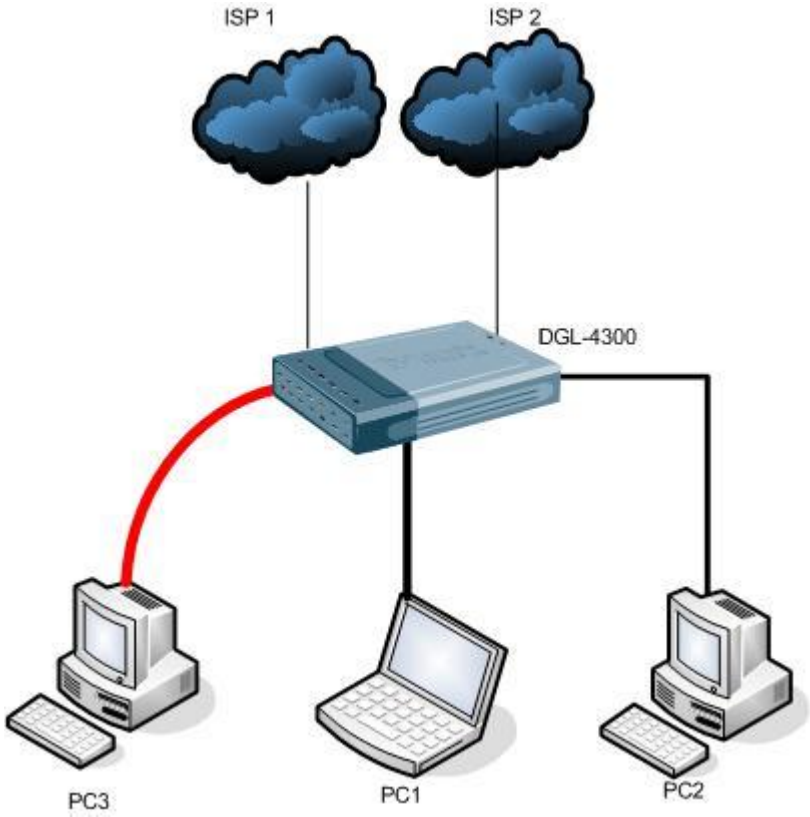
Баласировщик нагрузки DI-LB604

- 2 Wan 10/100 Ethernet
- Коммутатор на 4 порта 10/100 Мбит/с
- Встроенный firewall
- Резервирование канала
- Встроенный firewall
- Отключаемый NAT

Применение DI-LB604

Устройство позволяет использовать одновременно двух в провайдеров динамически разделяя нагрузку или использовать второй канал как резервный, обеспечивая отказоустойчивость системы.

Использование статического NAT позволяет выделить для сервера отдельный IP



Характеристики DI-LB604

- 2 WAN - порта 10/100 Мбит/с для подключения к глобальной сети посредством кабельного, ADSL-модема или Ethernet
- 4-портовый коммутатор 10/100/100Мбит/с для подключения локальной сети
- Встроенный межсетевой экран
- Использование одновременно двух провайдеров
- Использование второго провайдера как резервного, автоматическое переключение
- Встроенный firewall
- Статический NAT
- Подключение к провайдеру VPN или PPPoE
- 3 логических уровня приоритета
- Расширенные настройка NAT

Интернет маршрутизато DI-704GU

- 4 Порта GigabitEthernet(LAN)
- 1 Порт Fast Ethernet(WAN)
- Встроенный PrintServer для работы с USB принеторм
- Уникальная система динамической приоритизации траффика StreamEngine™
- Встроенный Firewall
- Виртуальные сервера