D-Link®

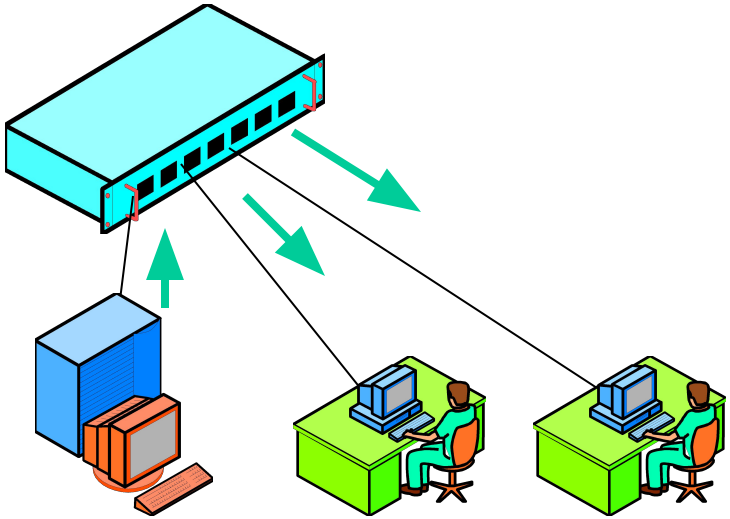
Интернет шлюзы

D-Link®

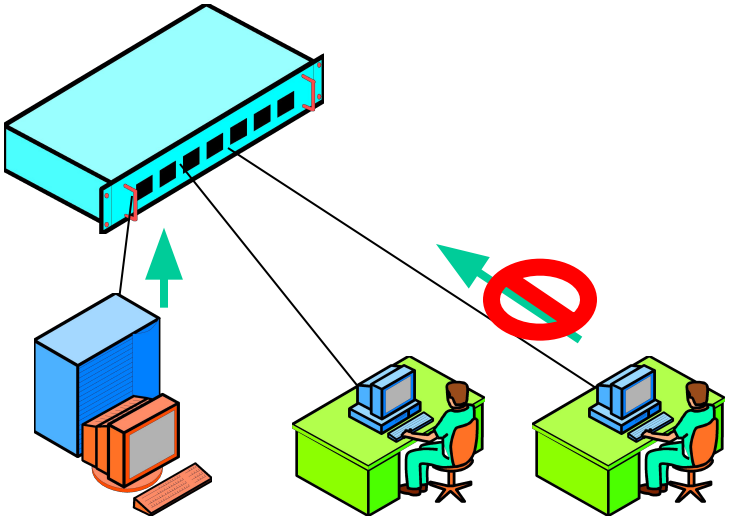
Building Networks for People

Работа концентраторов

Концентратор



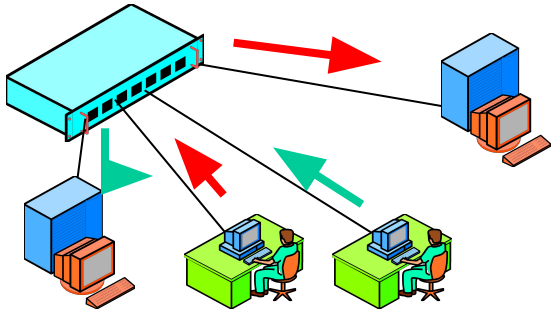
Концентратор

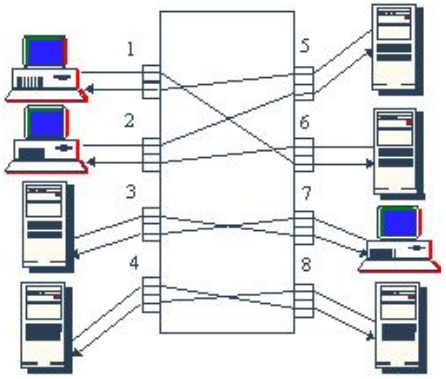


Работают на физическом уровне.
Выполняют передачу пакетов на все порты.
Производится усиление электрического сигнала.

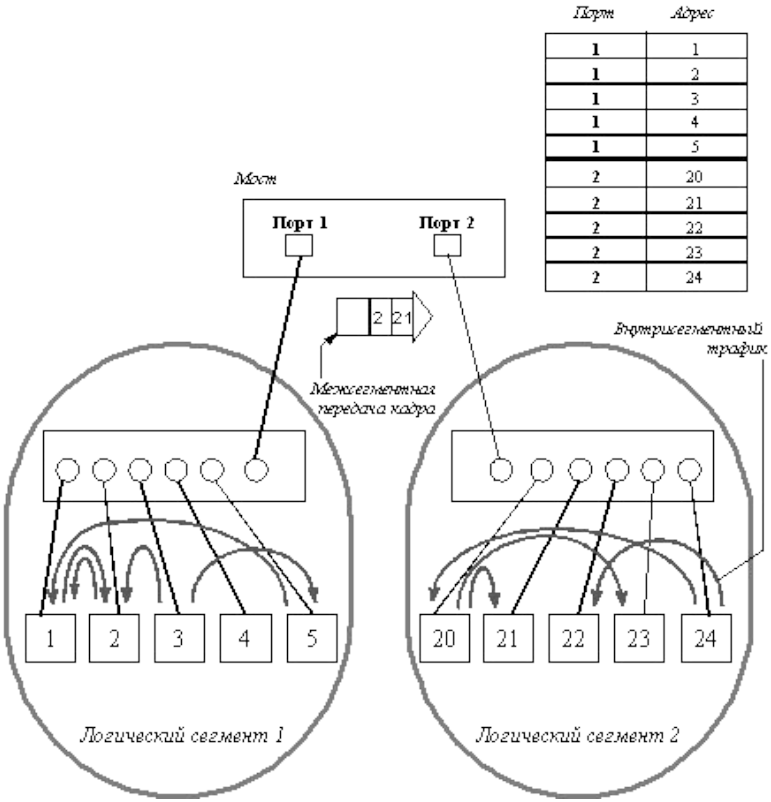
Работа коммутаторов

Коммутатор





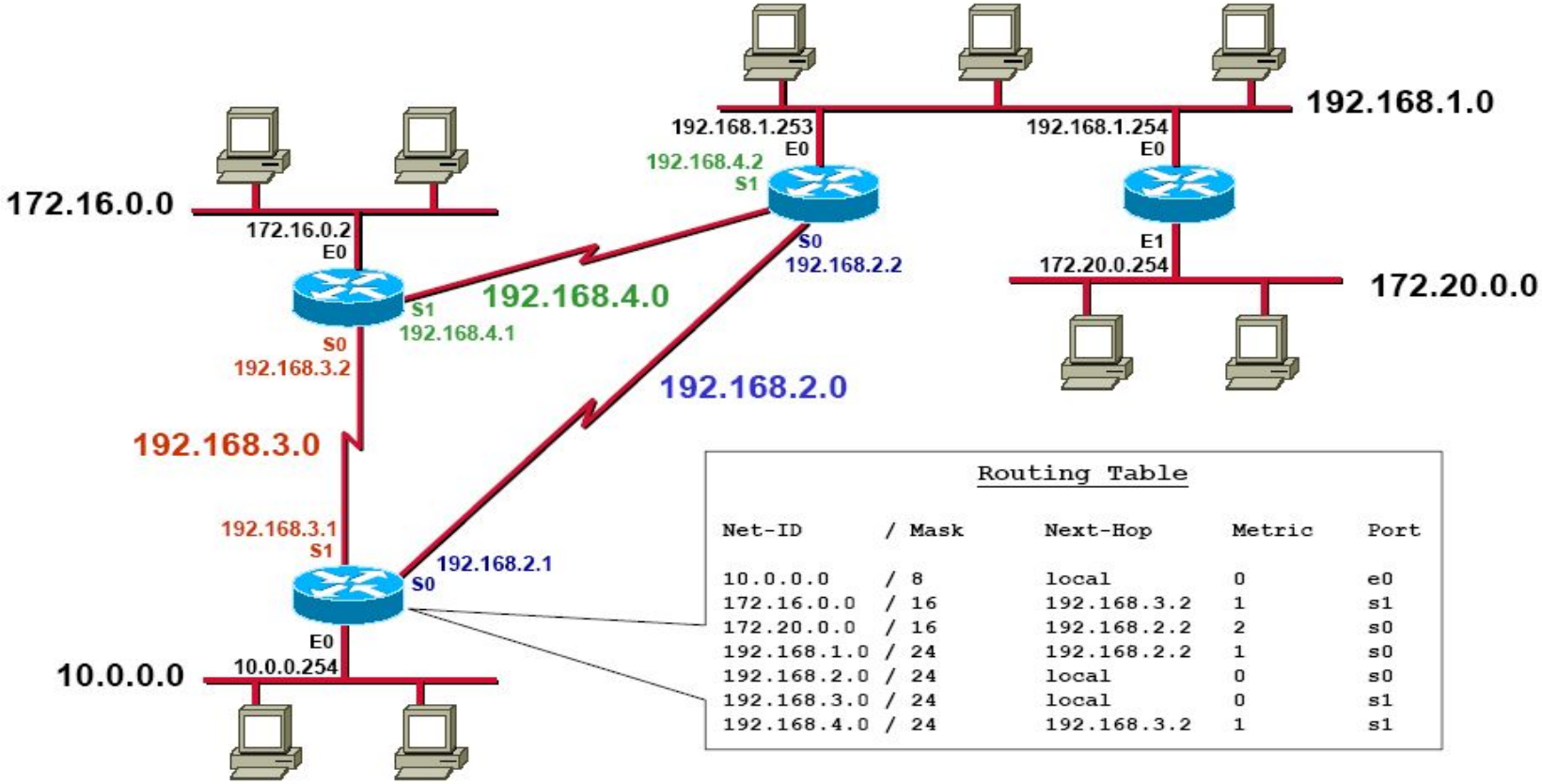
Общая пропускная способность сегмента равна 8 x 10 = 80 Мб/с



Порт	Адрес
1	1
1	2
1	3
1	4
1	5
2	20
2	21
2	22
2	23
2	24

Работают на канальном уровне.
Строят таблицу коммутации. Выполняют передачу пакетов на требуемый порт.
Производится регенерация пакета перед передачей.

Работа маршрутизаторов

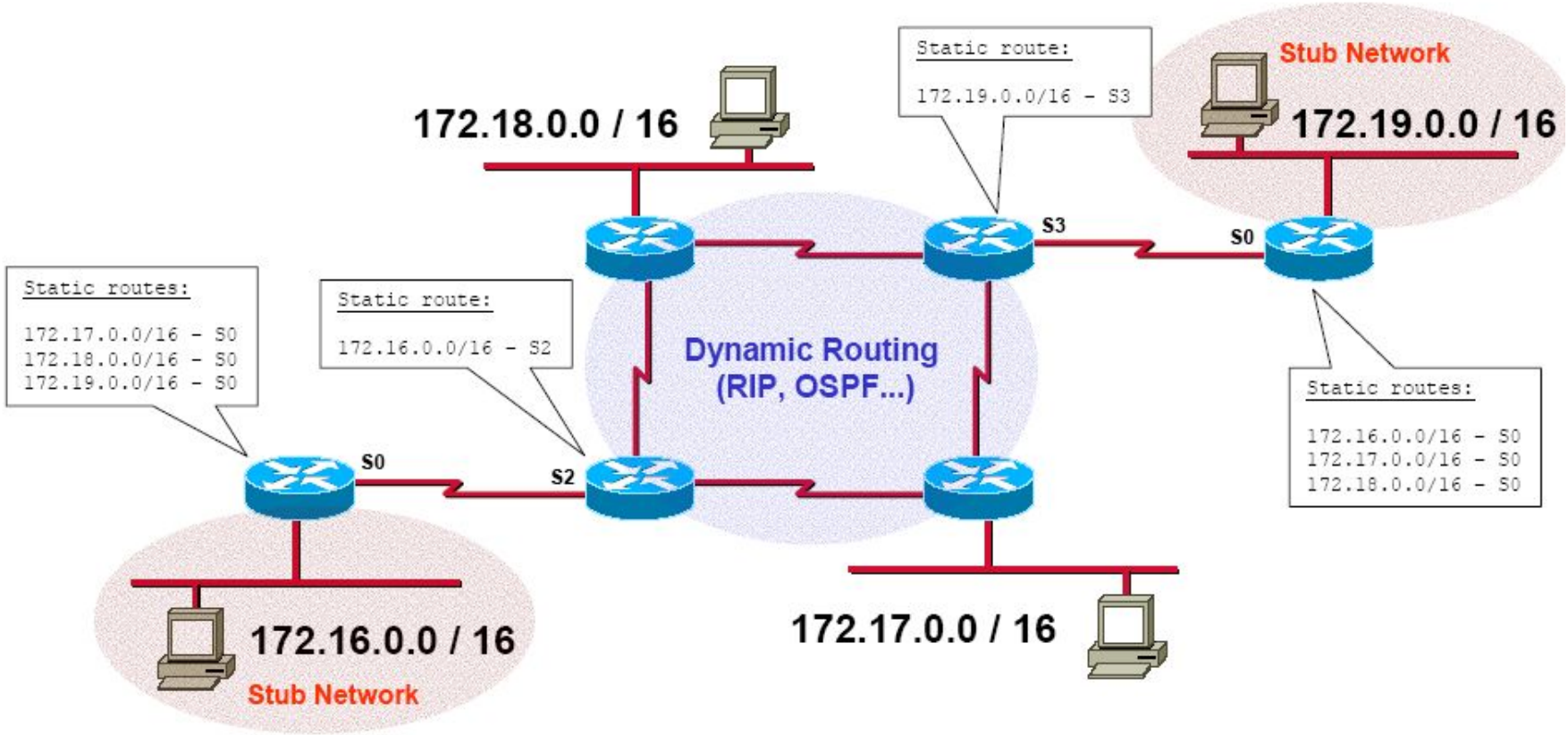


Routing Table

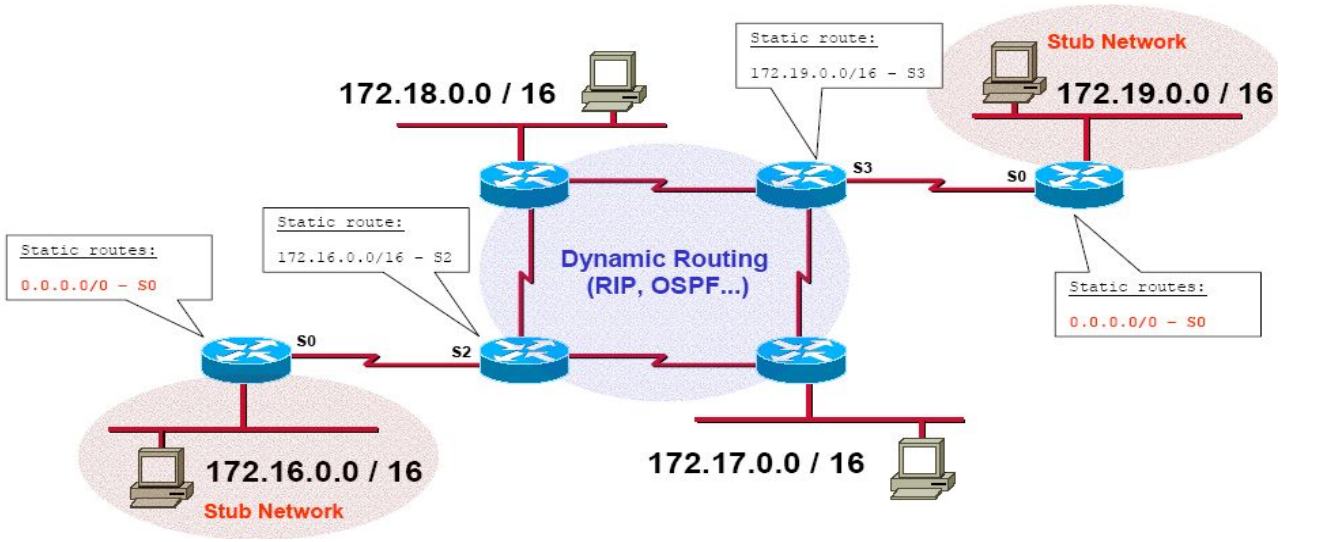
Net-ID	/ Mask	Next-Hop	Metric	Port
10.0.0.0	/ 8	local	0	e0
172.16.0.0	/ 16	192.168.3.2	1	s1
172.20.0.0	/ 16	192.168.2.2	2	s0
192.168.1.0	/ 24	192.168.2.2	1	s0
192.168.2.0	/ 24	local	0	s0
192.168.3.0	/ 24	local	0	s1
192.168.4.0	/ 24	192.168.3.2	1	s1

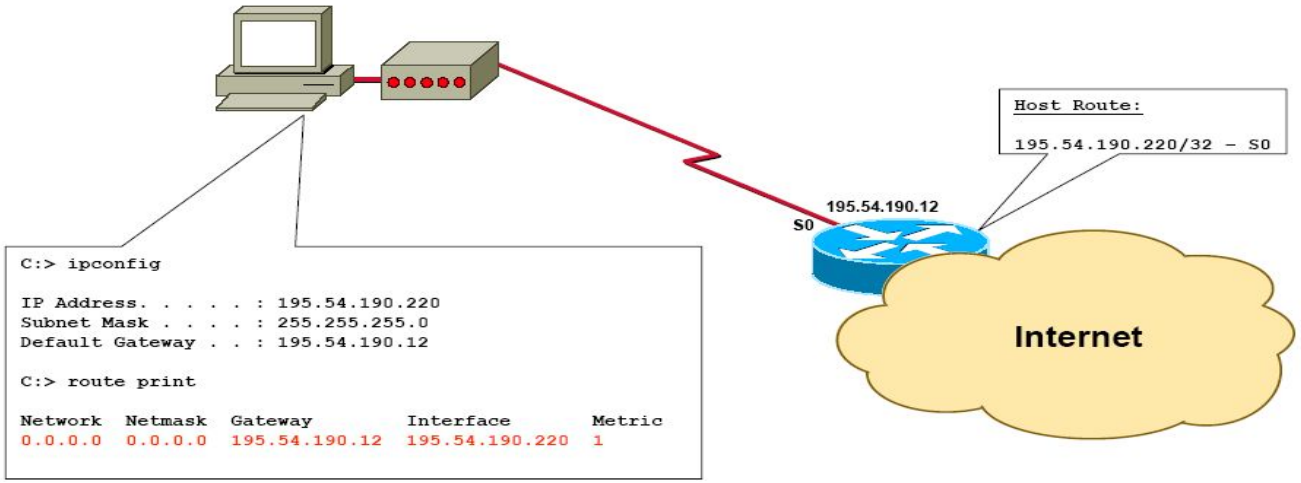
Работают на сетевом уровне. Оперируют сетями.
Строят таблицу маршрутизации. Выполняют передачу пакетов на требуемый порт.
Умеют выбирать лучший маршрут.

Статическая и динамическая маршрутизация



Маршрут по умолчанию





Динамическая маршрутизация

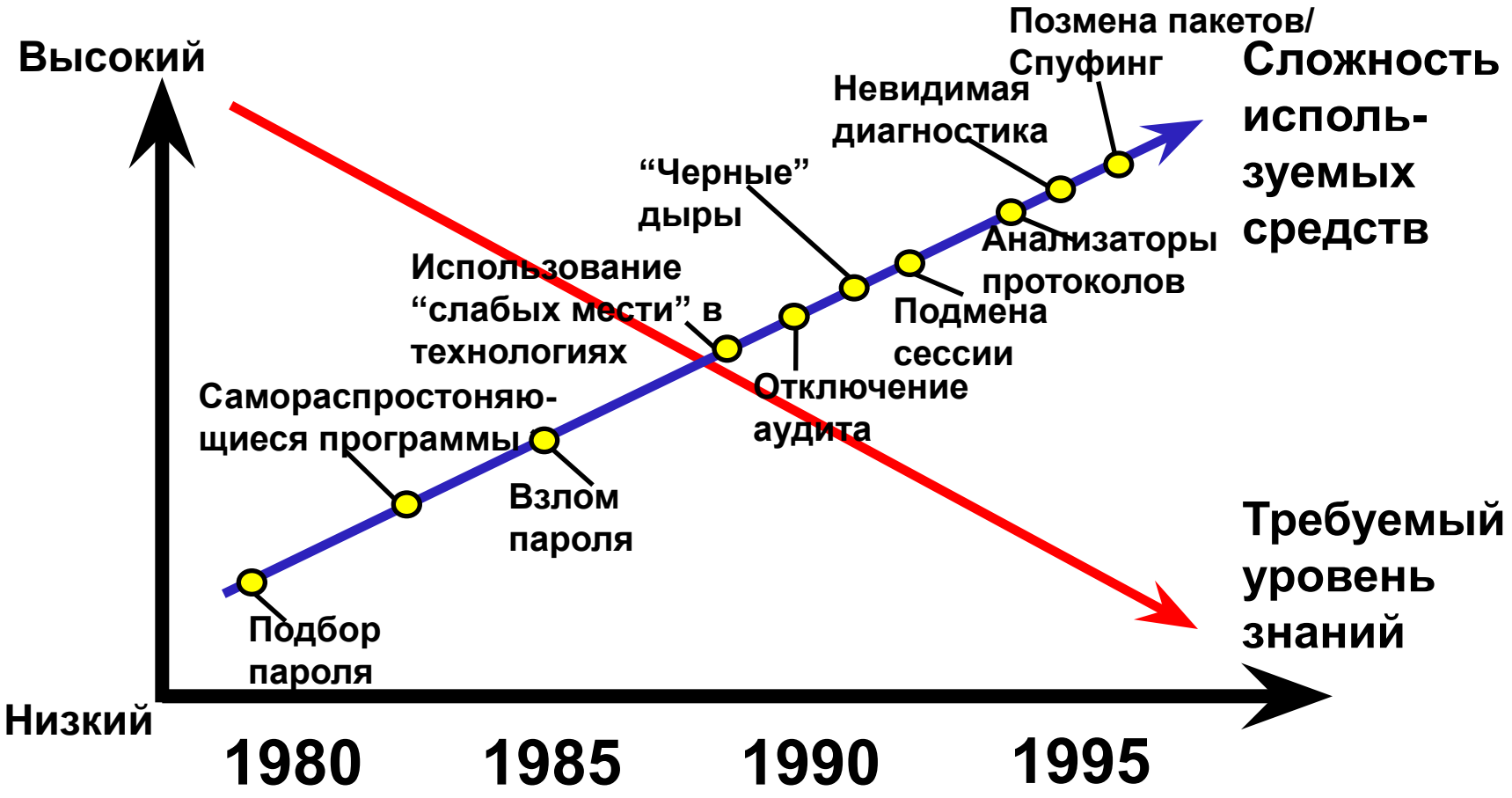
Unknown	255
I-BGP	200
E-EIGRP	170
EGP	140
RIP	120
IS-IS	115
OSPF	110
IGRP	100
I-EIGRP	90
E-BGP	20
EIGRP Summary Route	5
Static route to next hop	1
Static route through interface	0
Directly Connected	0

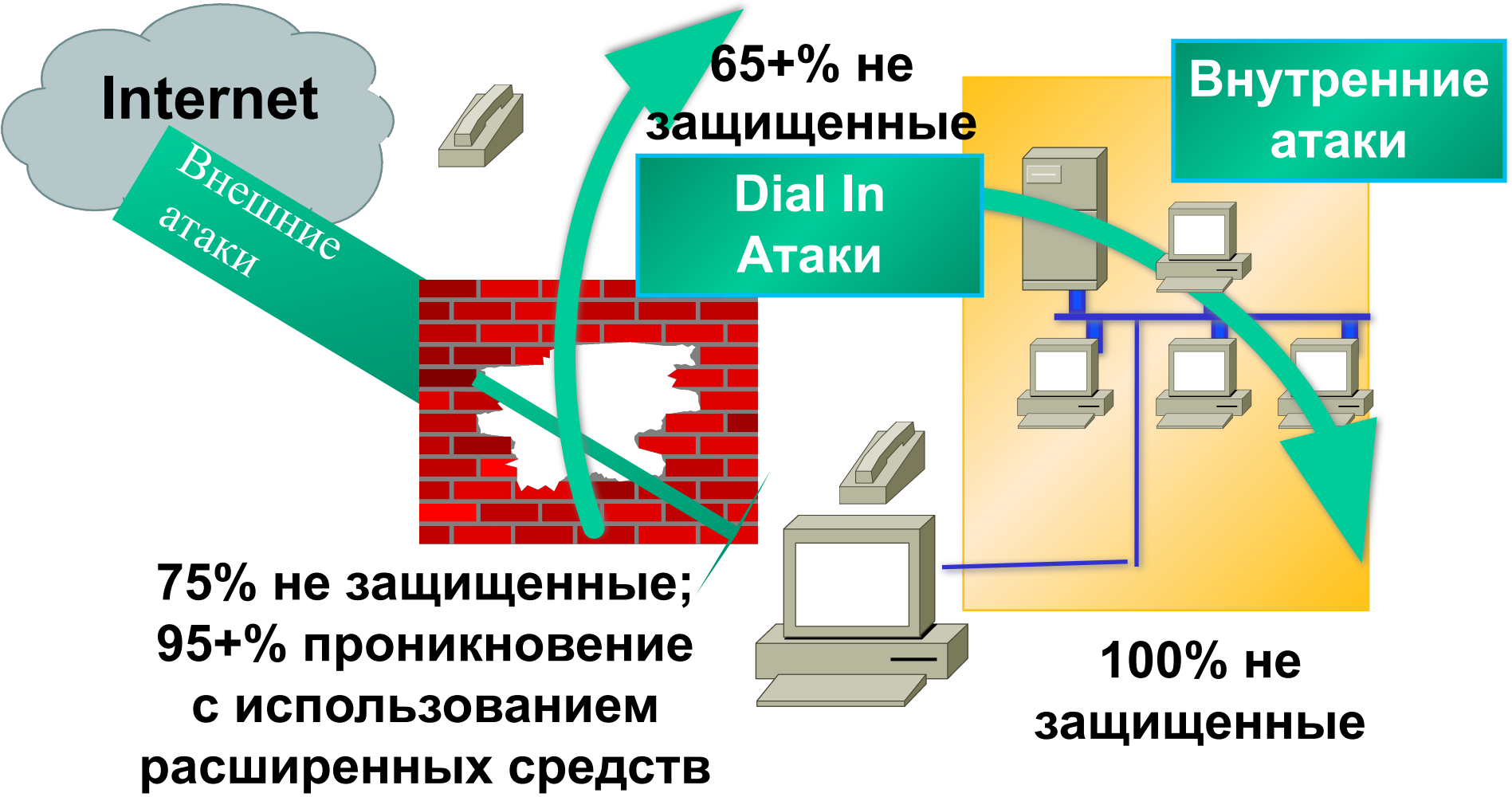
Протокол маршрутизации	Сложность	Максимальный размер сети	Сходимость
RIP	Очень простой	16 хопов	Медленный
IGRP	Простой	255 хопов	Средний
EIGRP	Сложный	255 хопов	Средний
OSPF	Очень сложный	Тысячи маршрутизаторов	Быстрый
IS-IS	Сложный	Тысячи маршрутизаторов	Быстрый
BGP	Сложный	Сотни тысяч маршрутизаторов	Быстрый

```
Gateway of last resort is 175.18.1.2 to network 0.0.0.0

     10.0.0.0 255.255.0.0 is subnetted, 4 subnets
C       10.1.0.0 is directly connected, Ethernet1
R       10.2.0.0  [120/1] via 10.4.0.1, 00:00:05, Ethernet0
R       10.3.0.0  [120/5] via 10.4.0.1, 00:00:05, Ethernet0
C       10.4.0.0 is directly connected, Ethernet0
R    192.168.12.0  [120/3] via 10.1.0.5, 00:00:08, Ethernet1
S    194.30.222.0 [1/0] via 10.4.0.1
S    194.30.223.0 [1/0] via 10.1.0.5
C    175.18.1.0 255.255.255.0 is directly connected, Serial0
S*   0.0.0.0 0.0.0.0 [1/0] via 175.18.1.2
```

Вопросы безопасности





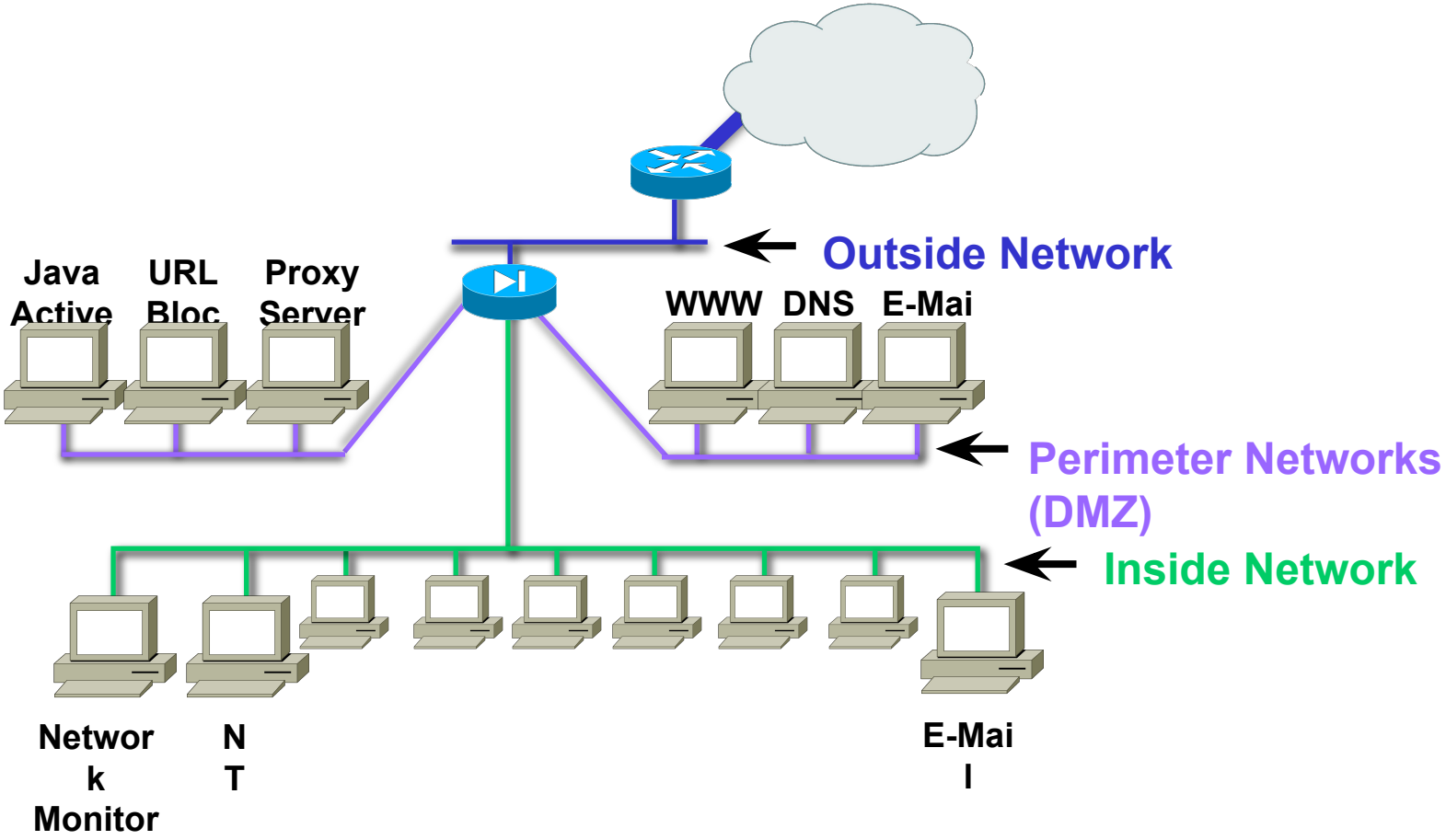
Source: Cisco Secure Consulting Engagements, 1996-1999

Основные задачи, выполняемые файрволами

- Разделение сети на зоны с различным уровнем доверия
- Пакетные фильтры – ограничение трафика на основании информации 3 и 4 уровней
- NAT – скрытие внутренних адресов
- Защита от DoS (Denial of Service, отказ в обслуживании) атак – ограничение на количество одновременных сессий, время жизни сессии и т.д.
- Statefull Packet Inspection – отслеживание корректности установленных сессий
- Отслеживание корректности работы протоколов более высоких уровней
- Защита от атак на основе базы сигнатур и эвристического анализа
- Защита от вирусов на основе базы сигнатур и эвристического анализа
- Ограничение доступа к URL ресурсам на основе базы, масок и анализа страниц
- Блокирование определённых Java и ActiveX аплетов.

Основные задачи, выполняемые файрволами

Разделение сети на зоны с различным уровнем доверия



Основные задачи, выполняемые файрволами

Пакетные фильтры – ограничение трафика на основании информации 3 и 4 уровней

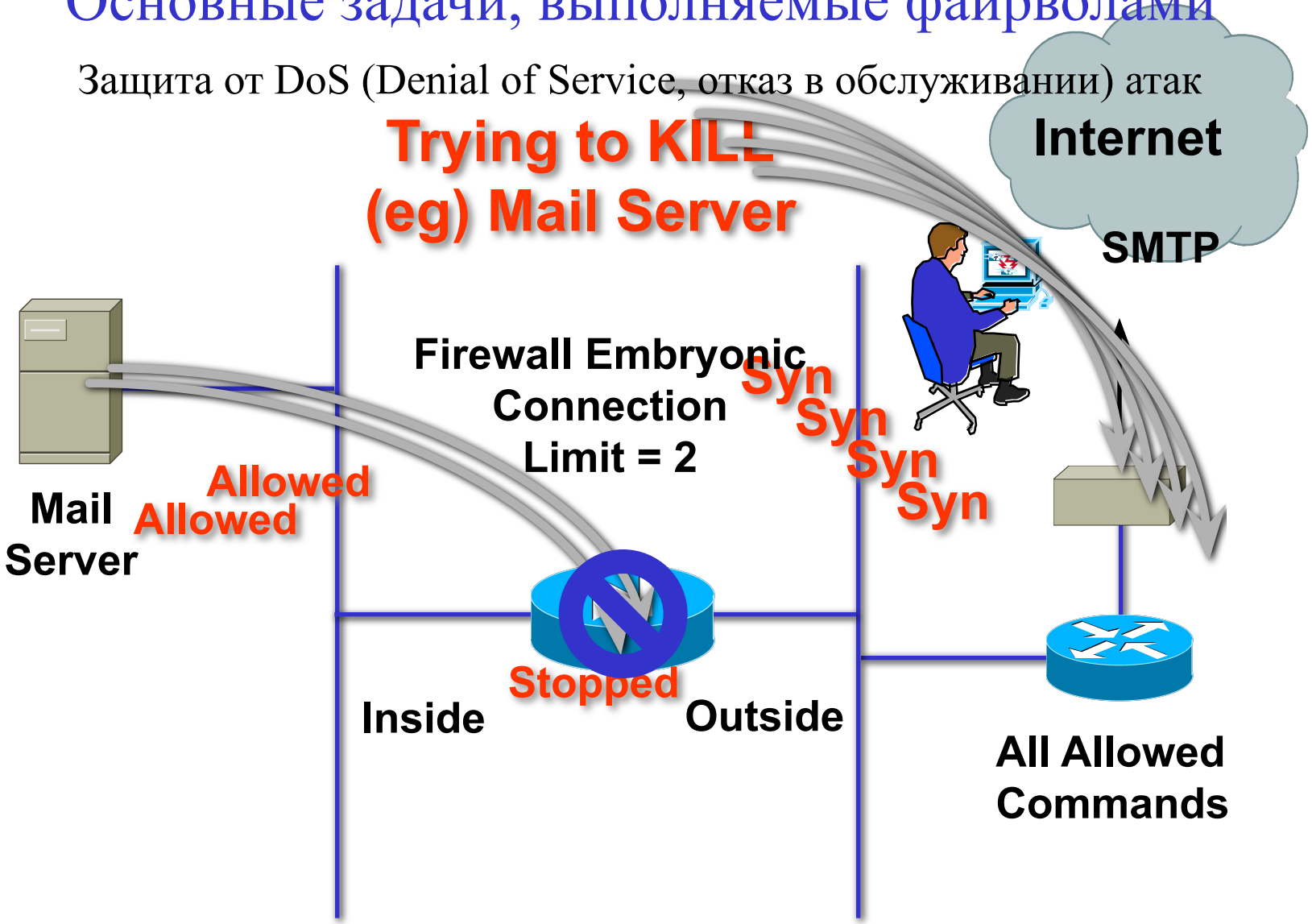
- If <test> then <action> (если <тест> тогда <действие>), где
- <test> is about layer 3/4 matches (<тест> на совпадения на уровнях 3/4
- <action> can be (<действия> могут быть следующими
  - ✔permit/deny (разрешить/запретить)
  - ✔prioritize (приоритизировать)
  - ✔trigger interface (запустить интерфейс)
  - ✔encrypt, etc... (зашифровать и др.)

Пример:

Если IP адрес источника 193.168.1.12, TCP порт источника 25, IP адрес назначения 194.129.8.5, TCP порт назначения 25, тогда прохождение пакета разрешить

Основные задачи, выполняемые файрволами

Защита от DoS (Denial of Service, отказ в обслуживании) атак

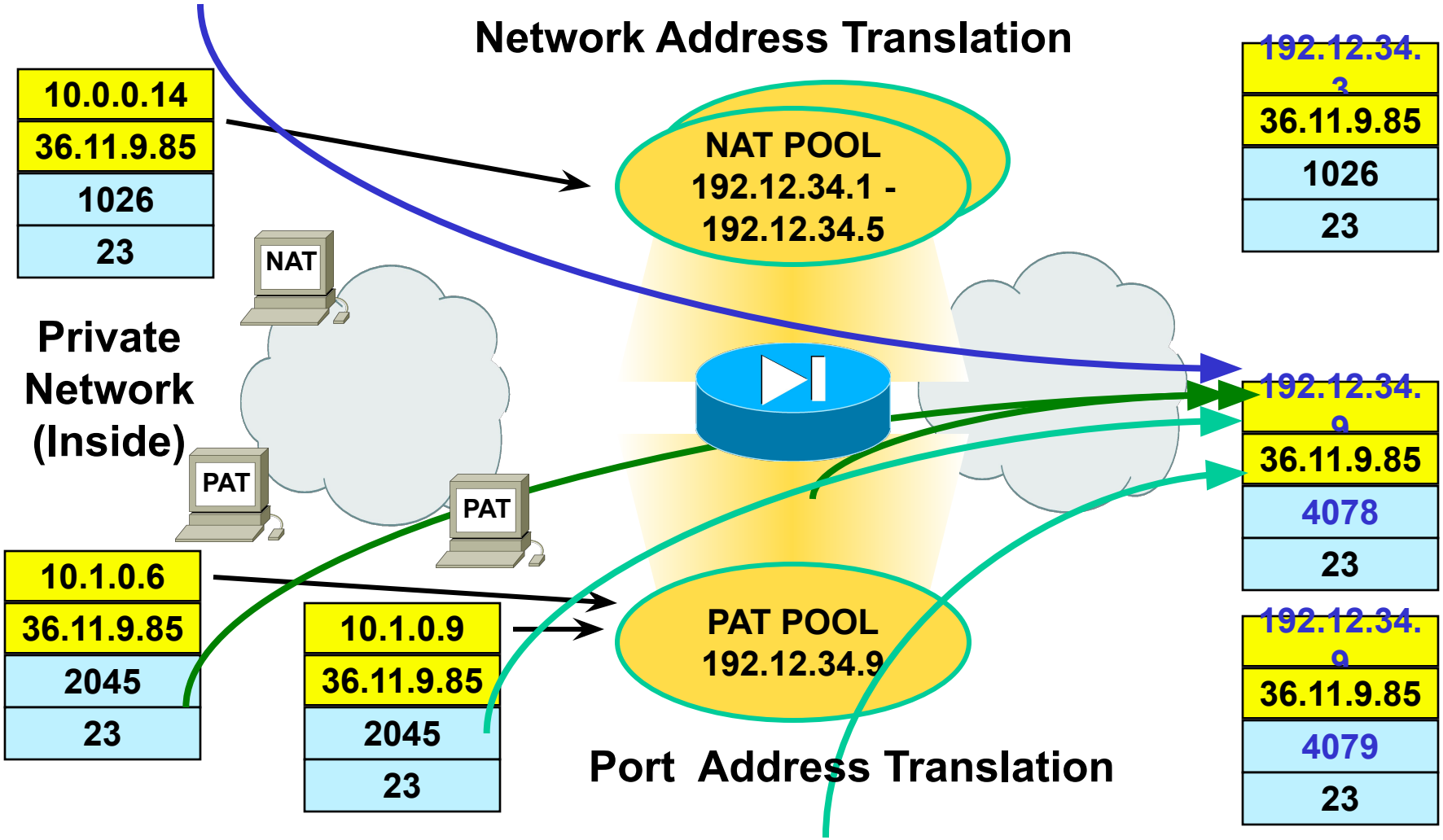


Основные задачи, выполняемые файрволами

NAT – Network address Translation

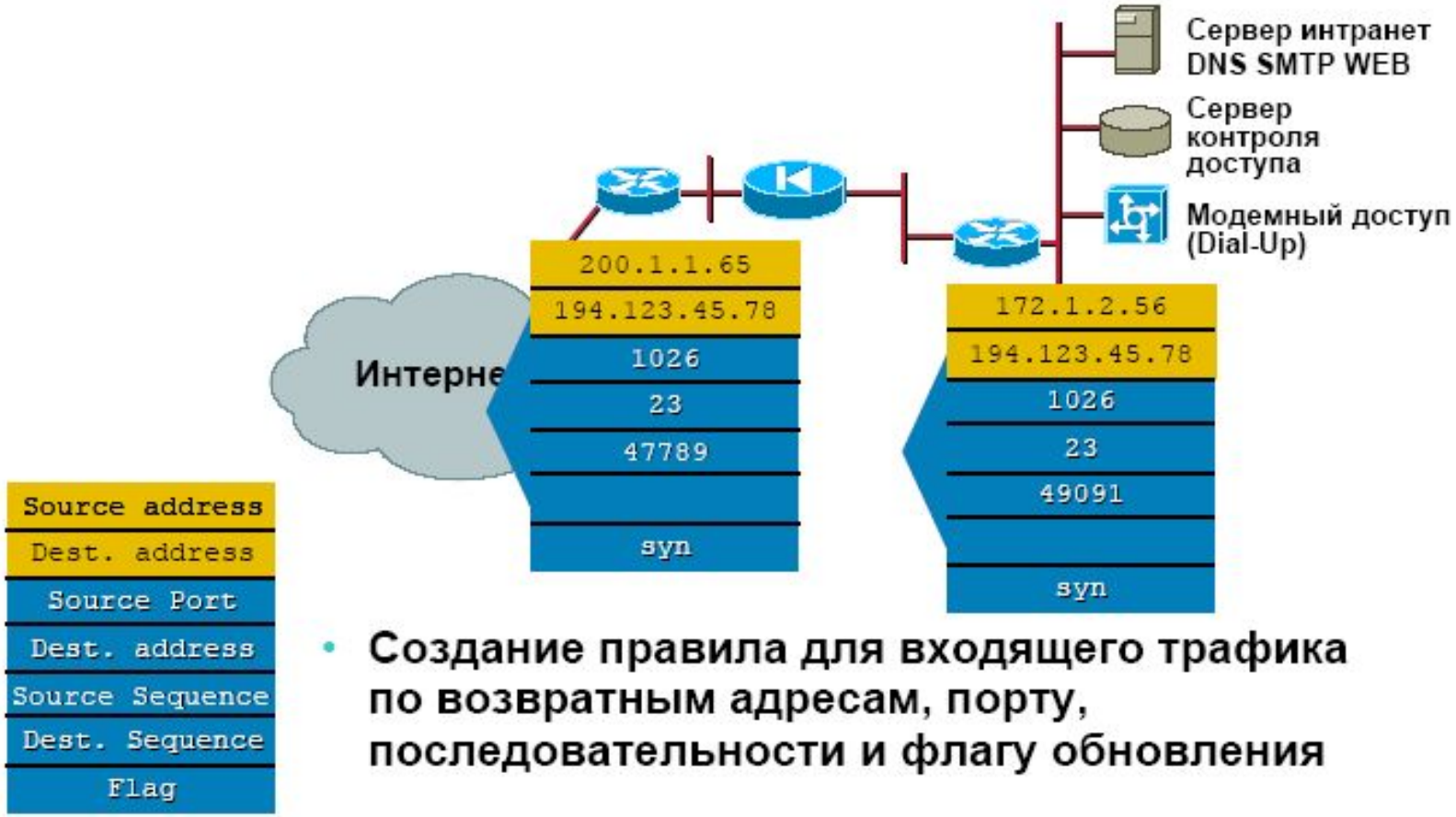
- Трансляция между внутренними (не зарегистрированными) и внешними (зарегистрированными) адресами
  - Безопасность: скрыты внутренние адреса
- Может быть статическим и динамическим
- PAT – вид NATа: использует номера портов, что бы ставить в соответствие множество внутренних адресов к одному или нескольким внешним адресам

Основные задачи, выполняемые файрволами



Основные задачи, выполняемые файрволами

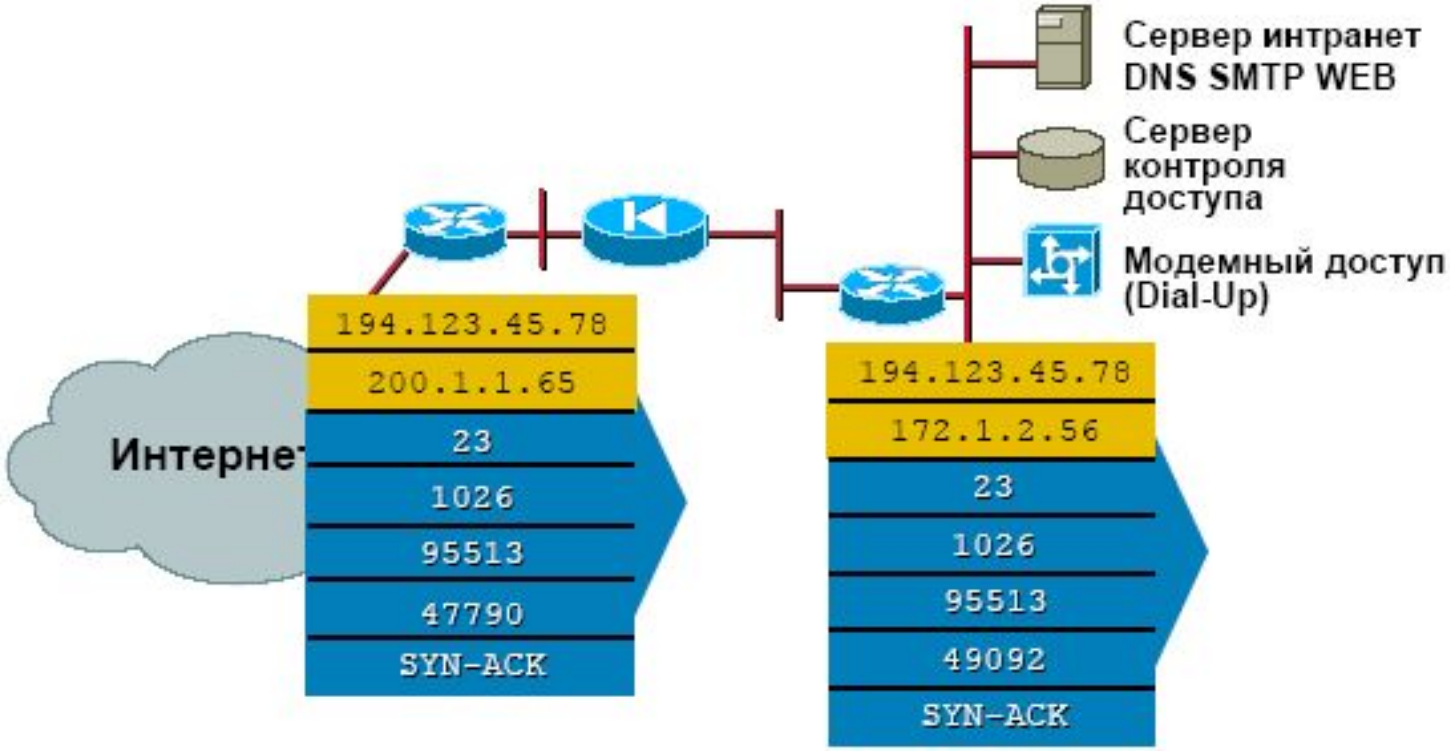
Statefull Packet Inspection – отслеживание корректности установленных сессий



- **Создание правила для входящего трафика по возвратным адресам, порту, последовательности и флагу обновления**

Основные задачи, выполняемые файрволами

Statefull Packet Inspection – отслеживание корректности установленных сессий



Проверка входящего пакета по динамическому правилу и удаление в случае несоответствия или истечения лимита времени

Основные задачи, выполняемые файрволами

- Отслеживание корректности работы протоколов более высоких уровней, например отслеживание команд протоколов FTP, SNMP, SMTP, HTTP и терминация сессии в случае неправильного порядка команд и др.
- Защита от атак на основе базы сигнатур и эвристического анализа
- Защита от вирусов на основе базы сигнатур и эвристического анализа
- Ограничение доступа к URL ресурсам на основе информационной базы, масок и анализа страниц
- Блокирование определённых Java и ActiveX аплетов.

Зачем нужен Интернет/широкополосный шлюз?

- Информация, свободно доступная из Интернет.
- Работа и конкуренция в информационно-богатом мире. Такая информация необходима для принятия быстрых и правильных решений.
- Многие компании хотят использовать интернет без больших затрат.
- Им не нужен дорогой маршрутизатор.
- Эффективное дешевое решение

Интернет шлюз или Широкополосный шлюз

Интернет - шлюз

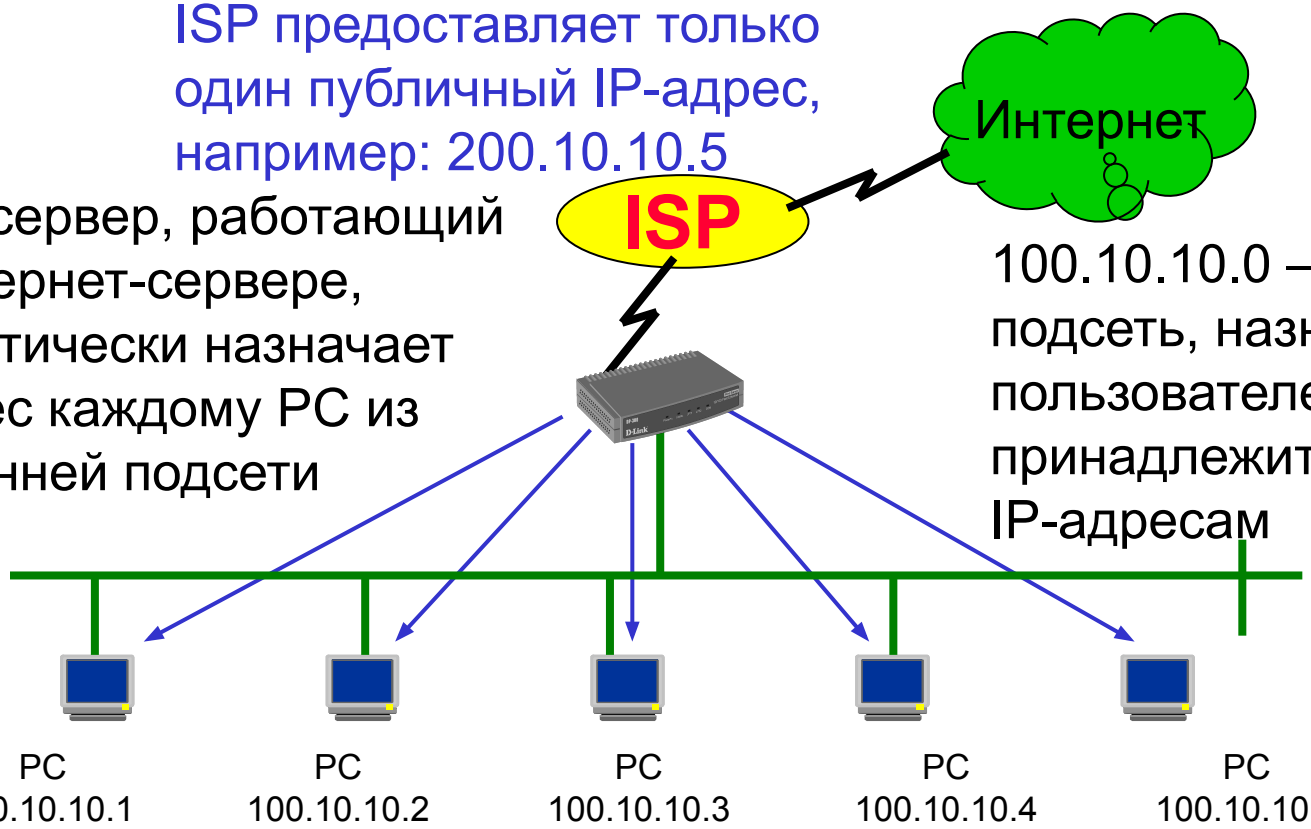
2 основные идеи в работе Интернет-шлюза :

- **Трансляция сетевых адресов - NAT**
  - Разделяет один общий IP адрес на много компьютеров
- **Разделение полосы пропускания**
  - Много пользователей получают доступ к интернет одновременно

NAT & DHCP Сервер

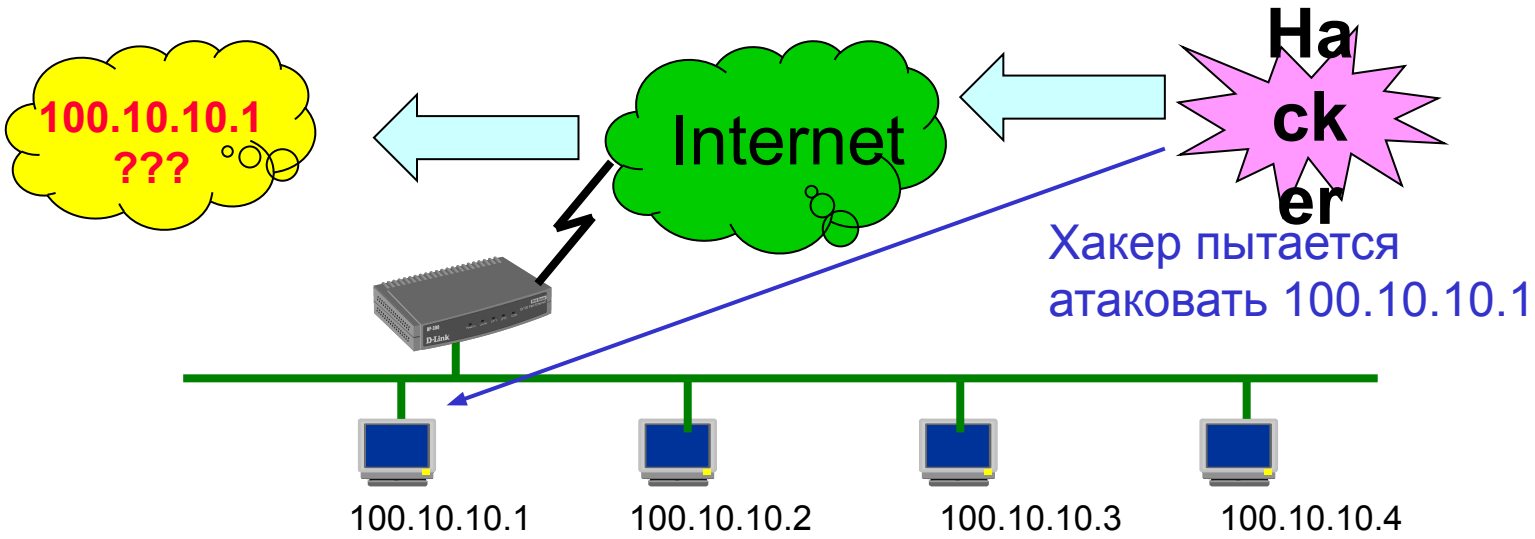
ISP предоставляет только один публичный IP-адрес, например: 200.10.10.5

DHCP сервер, работающий на Интернет-сервере, автоматически назначает IP адрес каждому PC из внутренней подсети



100.10.10.0 – внутренняя подсеть, назначенная пользователем, принадлежит к частным IP-адресам

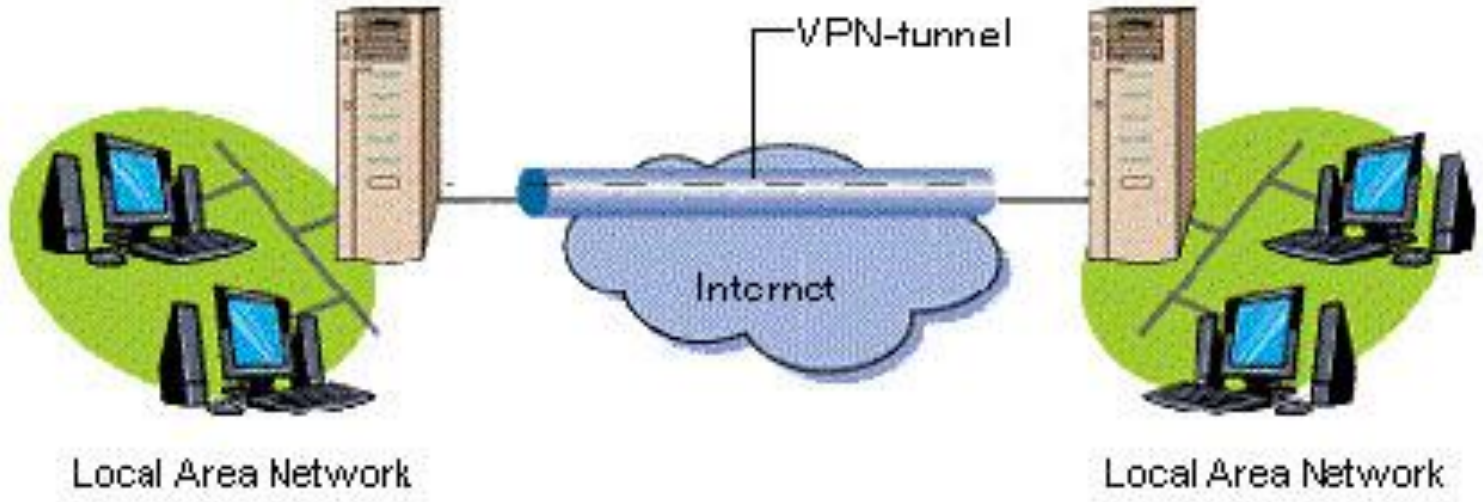
Firewall & NAT



- Только один публичный IP, все остальные адреса IP в LAN - частные IP адреса
- Хакер рыщет в Интернет в поисках общего IP, потому что LAN IP адреса “защищены”

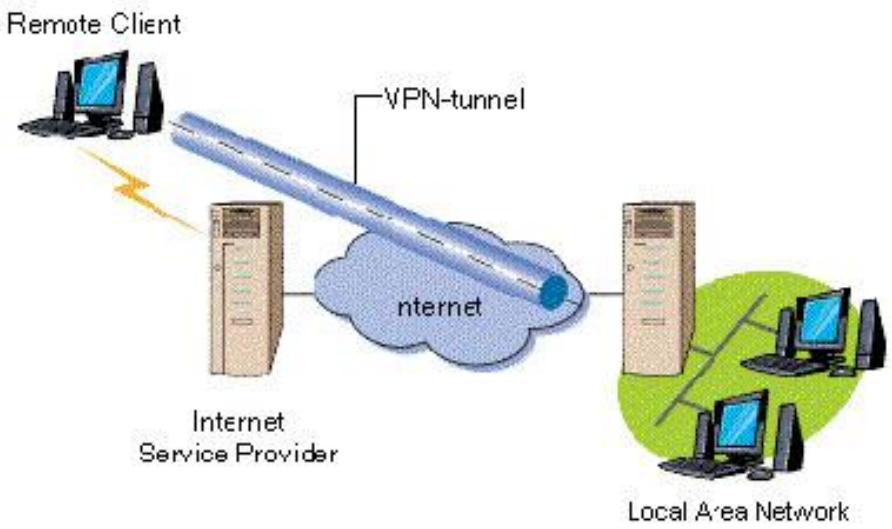
Виртуальные частные сети - VPN

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.



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.

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.

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), разработанный совместно Microsoft, 3Com и Ascend Communications. Этот протокол стал достаточно популярен благодаря его включению в операционные системы фирмы Microsoft.
- **PPPoE** (PPP over Ethernet) — разработка RedBack Networks, RouterWare, UUNET и другие.
- **L2TP** (Layer 2 Tunneling Protocol) - представляет собой дальнейшее развитие протокола L2F и объединяет технологии L2F и PPTP.
- **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 и создавать защищенный тоннель к своим корпоративным сетям.

- 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 IP-адрес сервера PPTP. При этом устанавливается сессия PPTP между клиентом и сервером, клиент аутентифицируется и дальше начинается передача 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: данные протоколов, использующихся внутри сети, поступают в глобальную сеть упакованными в кадры PPP, затем с помощью протокола PPTP инкапсулируются в пакеты протокола IP. Далее они переносятся с помощью IP в зашифрованном виде через любую сеть TCP/IP (например, Интернет). Принимающий узел извлекает из пакетов IP кадры PPP, а затем обрабатывает их стандартным способом, т.е. извлекает из кадра PPP пакет IP, IPX или NetBEUI и отправляет его по локальной сети. Таким образом, протокол PPTP создает соединение точка-точка в сети и по созданному защищенному каналу передает данные.

Виртуальные частные сети: **PPTP**

- PPTP шифрует поле полезной нагрузки пакета и берет на себя функции второго уровня, обычно принадлежащие PPP, т. е. добавляет к PPTP-пакету PPP-заголовок (header) и окончание (trailer). Далее, PPTP инкапсулирует PPP-кадр в пакет Generic Routing Encapsulation (GRE), который принадлежит сетевому уровню:

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-604**, **DI-714P+**, **DI-614+**, **DI-804HV**, **DI-754**

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.

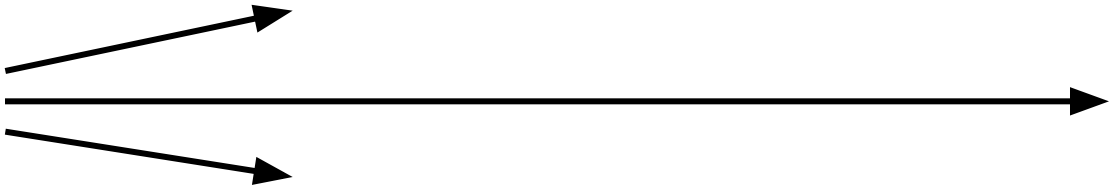
Принципом работы **PPPoE** является установление соединения **"точка-точка" поверх общей среды Ethernet**, поэтому процесс функционирования PPPoE разделен на две стадии.

Виртуальные частные сети: **PPPoE**

Стадия установления соединения

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

Клиент



Сервер

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

Клиент

Сервер

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.

Сессия начинается с использованием пакетов PPP. При установлении PPP-сессии клиент может быть аутентифицирован, например, при помощи RADIUS, и его трафик будет учитываться как при обычном модемном доступе.

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.

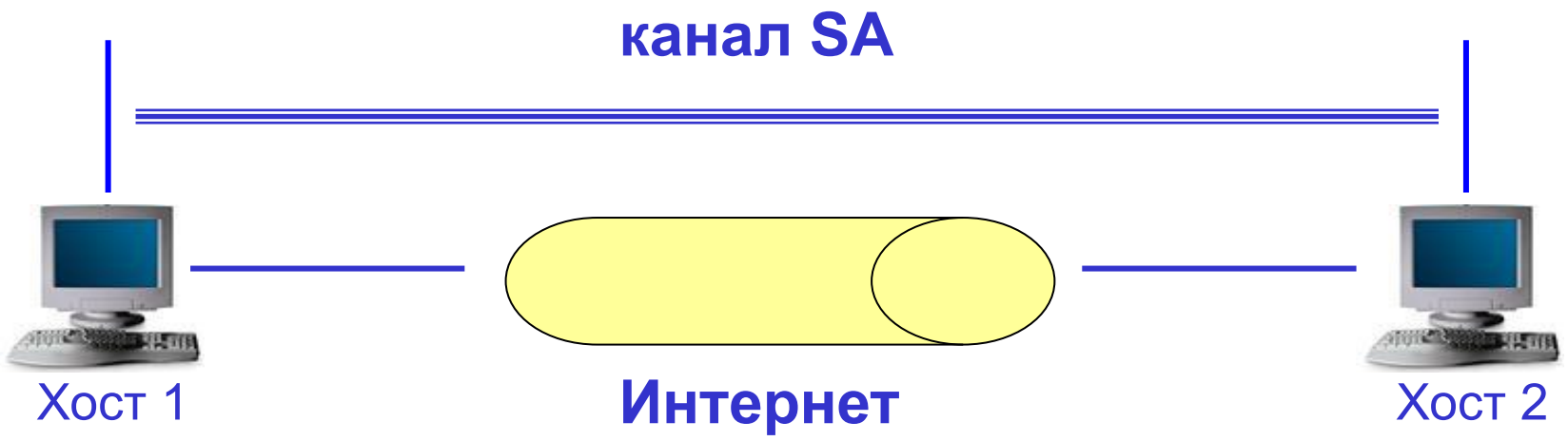
Система IPSec использует следующие протоколы для своей работы:

- **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;

Виртуальные частные сети: **IPSec**

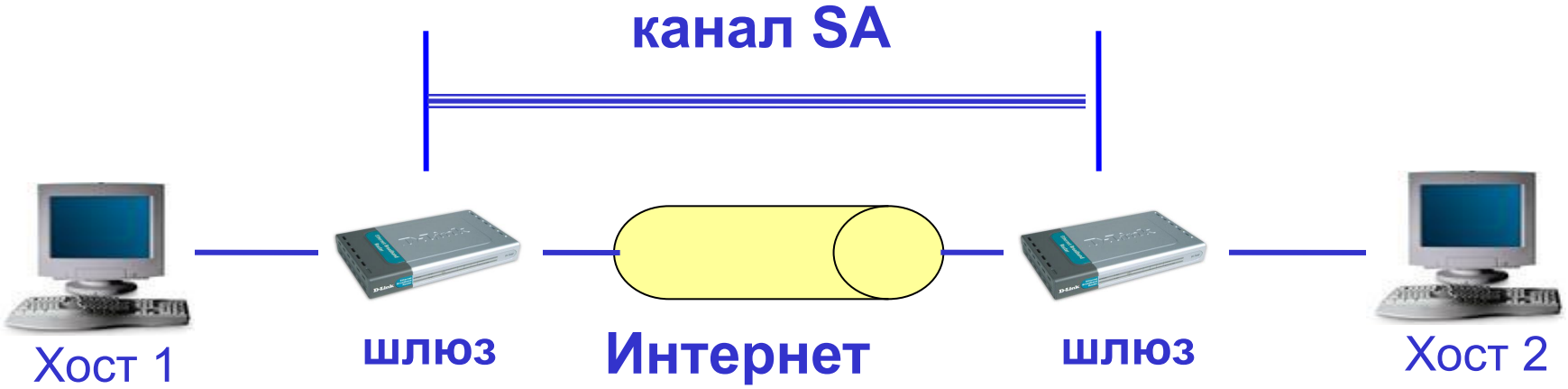
Существуют две основные схемы применения IPSec, отличающиеся ролью узлов, образующих защищенный канал.

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 **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.)

IPSec Security Association (SA)

Destination Address	192.168.2.1
Security Parameter Index (SPI)	7A390BC1
IPSec Transform	AH, HMAC-MD5
Key	7572CA49F7632946
Additional SA Attributes (for example, lifetime)	One Day or 100MB

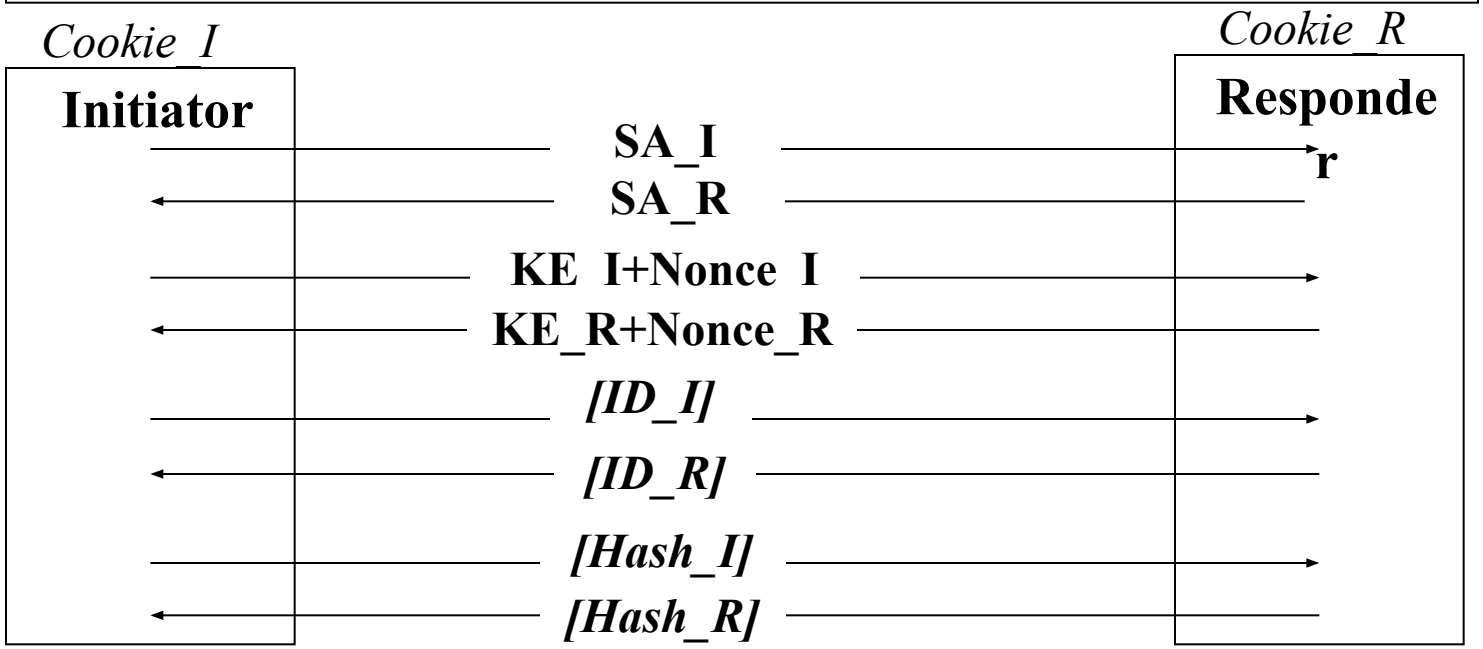
Затем в рамках установленного канала начинает действовать протокол **AH** или **ESP**, с помощью которого и выполняется требуемая защита передаваемых данных.

Виртуальные частные сети: **IPSec**

- Две фазы
  - Фаза 1 – Установление двухстороннего SA
    - Используются сертификаты или Pre-Shared ключи
    - Существует два режима: Main Mode или Aggressive Mode
  - Фаза 2 – Устанавливается IPSEC
    - Инициатор определяет какие записи в SPD для каждого SA будут посылаться респондеру
    - Ключи и SA атрибуты передаются из Фазы 1
    - Всегда используется Quick mode

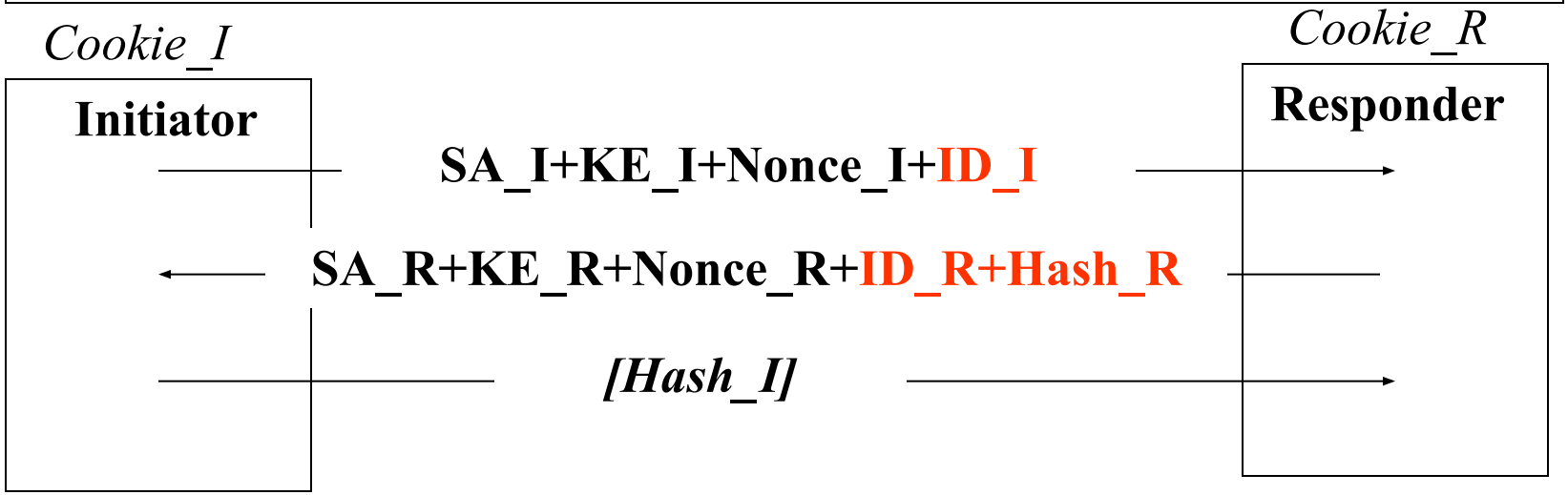
Виртуальные частные сети: **IPSec**

Main Mode IKE
Фаза 1



Виртуальные частные сети: **IPSec**

Aggressive Mode IKE
Фаза 1



Виртуальные частные сети: **IPSec**

IKE
Фаза 2

SPI_I | *SPI_R*

Initiator | **Responder**

SA_I+New_KE_I+Nonce_I
+ID_R+ID_I+Hash_I →

← **SA_R+New_KE_R+ Nonce_I**
ID_R+ID_I+Hash_R

[New_Hash_I] →

Виртуальные частные сети: **IPSec**

Security Association – SA

Логический канал между двумя точками, определяет правила обработки и шифрации/дешифрации трафика

Security Parameters Index – SPI

Уникальный идентификатор, который позволяет устройству назначения выбрать соответствующий SA

Как правило, SA= SPI + Dest IP address + IPSec Protocol (AH or ESP)

SA Database – SAD

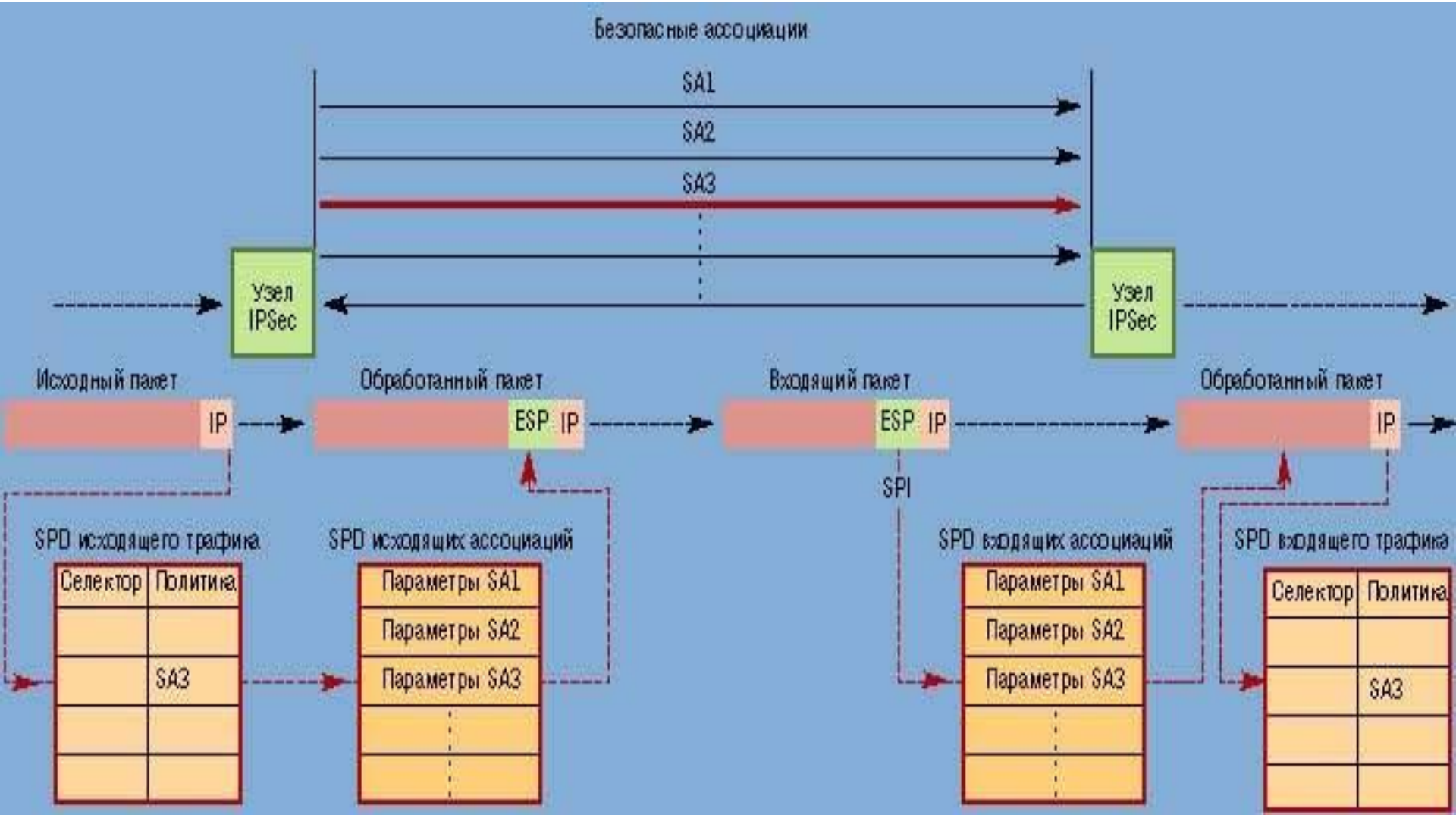
Содержит параметры для каждого SA:

- Время жизни SA
- AH и ESP информацию
- Туннельный или транспортный режим

Security Policy Database – SPD

Определяет какой трафик защищать, правильно ли защищён входящий трафик, какие SA применять к IP трафику

Виртуальные частные сети: **IPSec**



Установление соответствия между IP-пакетами и правилами их обработки

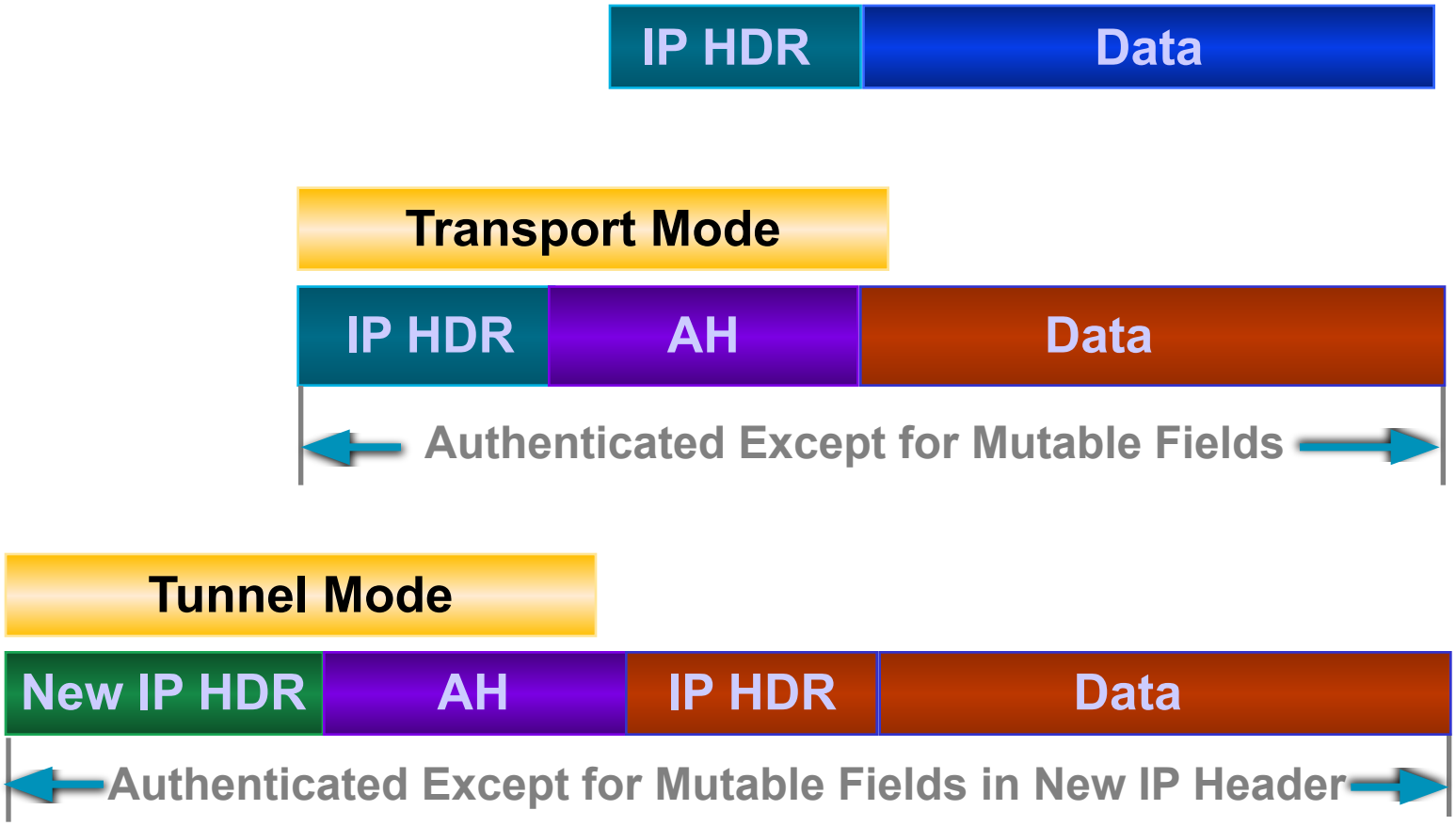
Виртуальные частные сети: **IPSec**

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

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.

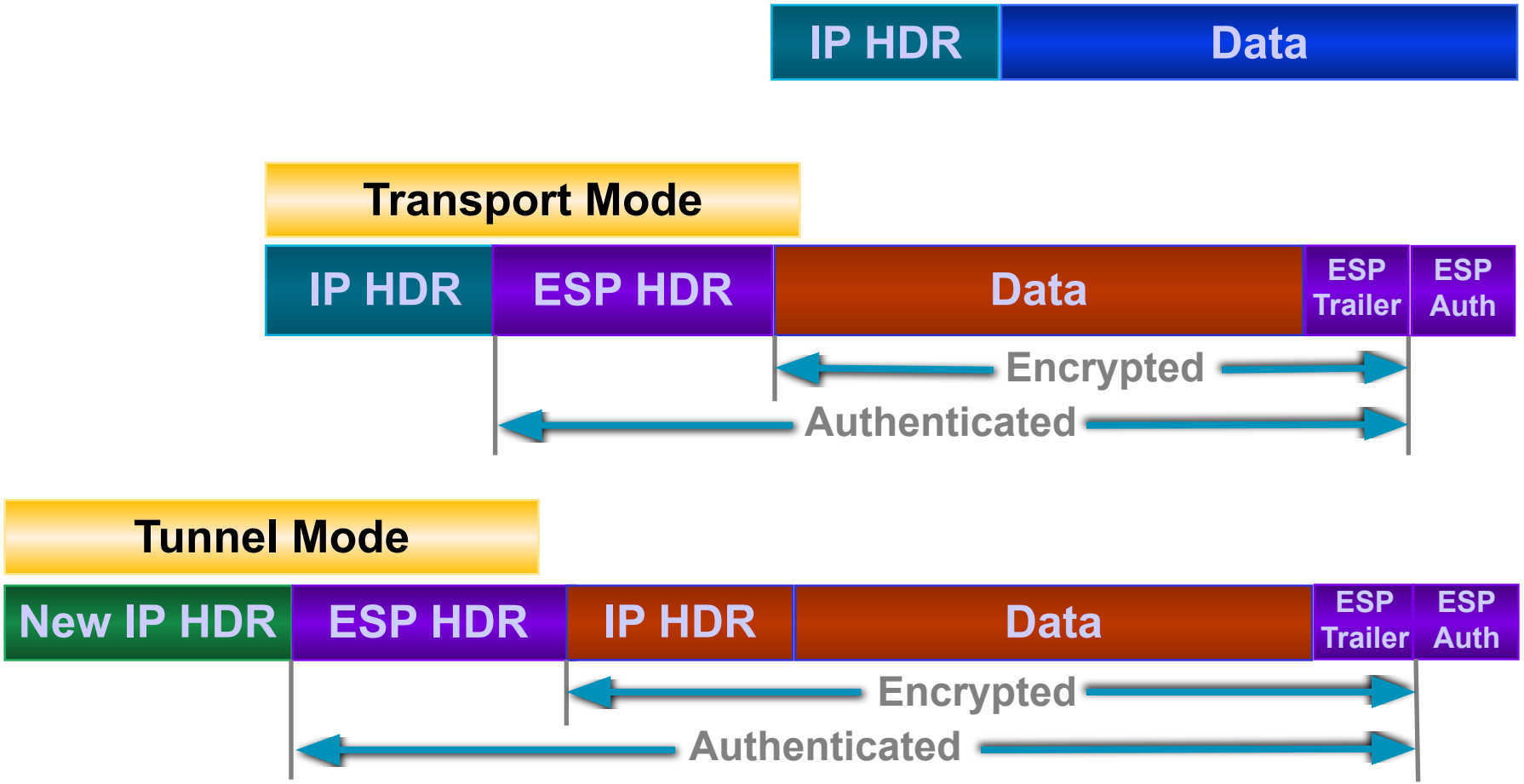
В туннельном режиме исходный пакет помещается в новый IP-пакет и передача данных выполняется на основании заголовка нового IP-пакета.

Виртуальные частные сети: **IPSec**



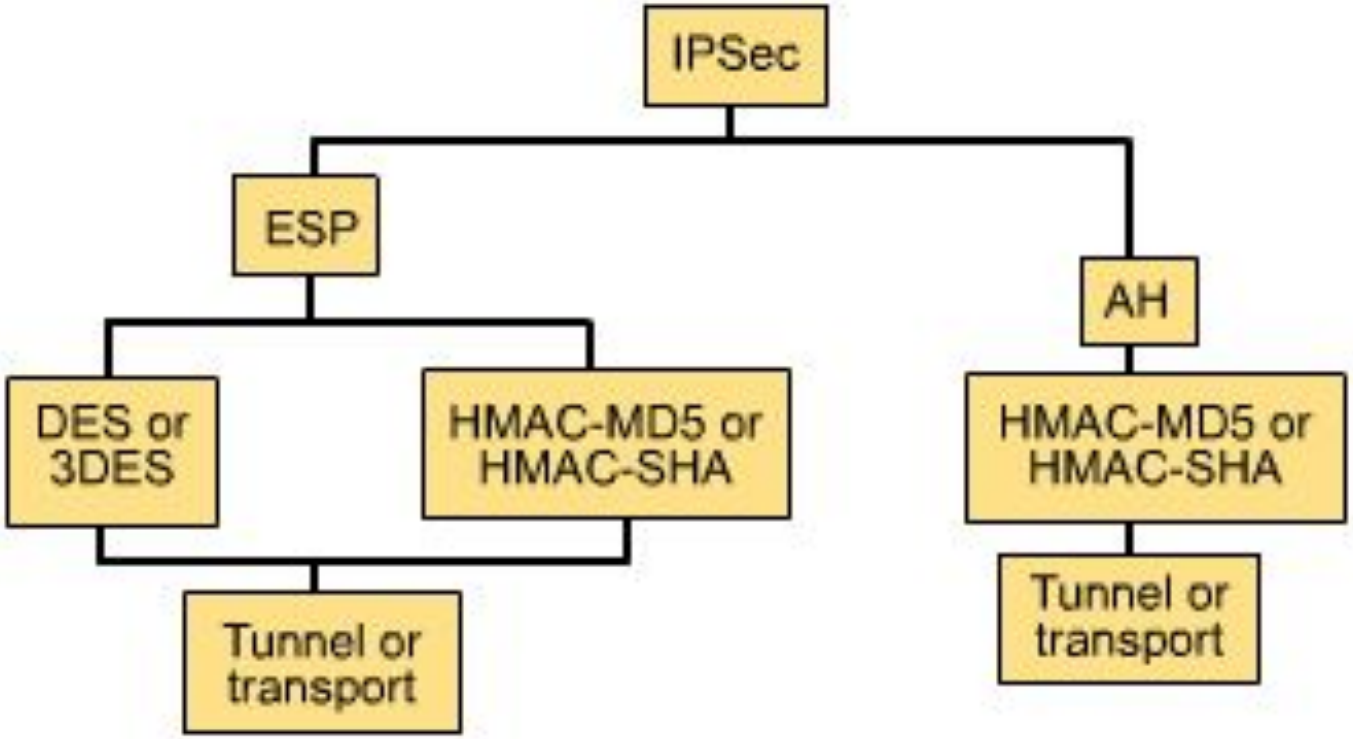
AH – туннельный и транспортный режимы работы

Виртуальные частные сети: **IPSec**



ESP – туннельный и транспортный режим

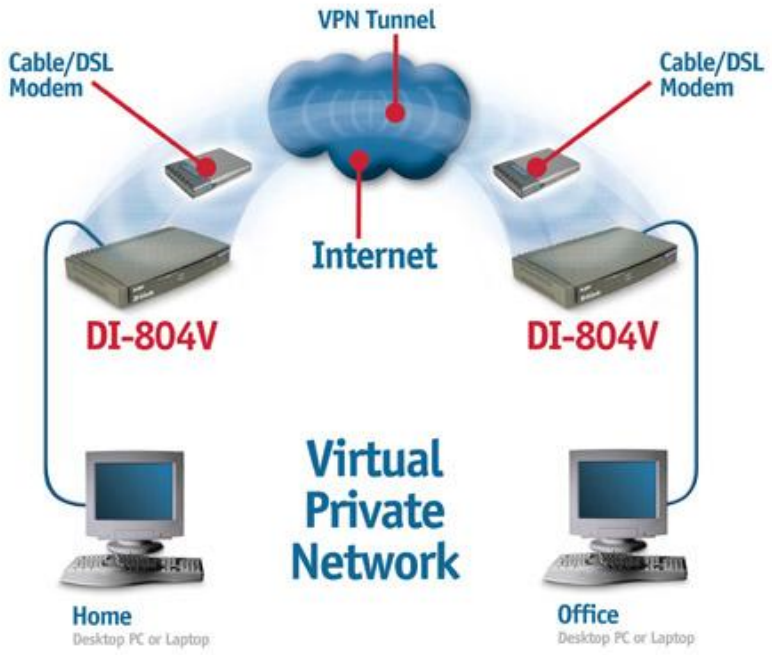
Виртуальные частные сети: **IPSec**



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-804HV**.



Резюме по применению режимов IPSec*

Протокол – ESP (AH)
Режим – туннельный (транспортный)
Способ обмена ключами – IKE (ручной)
Режим IKE – main (aggressive)
Ключ DH – group 5 (group 2, group 1)
Аутентификация – SHA1 (SHA, MD5)
Шифрование – AES (3DES, Blowfish, DES)

*Параметры указаны в порядке снижения уровня безопасности

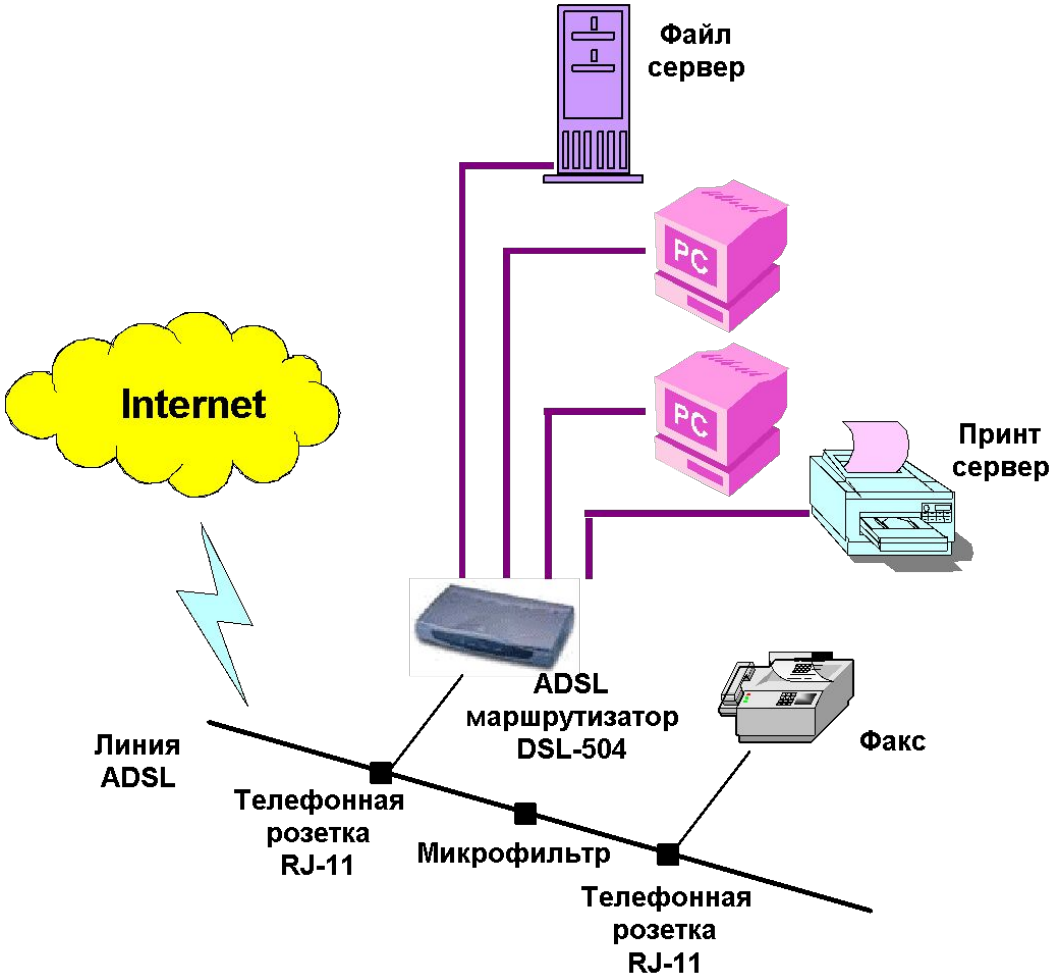
Интернет-маршрутизаторы D-Link

Модель	WAN Порты	LAN порты	Поддержка ADSL/ Кабельного модема	Дополнительные функции
DSL-504G	1 10/100 BASE-T	4 10/100 Мбит/с	Встроенный	-
DI-604	1 10/100 BASE-T	4 10/100 Мбит/с	√	Advanced Firewall
DI-704P	1 10 BASE-T	4 10/100 Мбит/с	√	Встроенный принт-сервер
DI-707P	1 10 BASE-T	7 10/100 Мбит/с	√	Встроенный принт-сервер
DI-614+	1 10/100 BASE-T	4 10/100 Мбит/с	√	Advanced Firewall, IEEE 802.11b+ Wireless LAN
DI-804HV	1 10/100 BASE-T 1 RS-232	4 10/100 Мбит/с	√	IPSec, PPTP, L2TP, Advanced Firewall Поддержка аналогового модема
DI-714P+	1 10 BASE-T	4 10/100 Мбит/с	√	IEEE 802.11b+ Wireless LAN, Встроенный принт-сервер
DI-764	1 10/100 BASE-T 1 RS-232	4 10/100 Мбит/с	√	IEEE 802.11a/ b + Wireless LAN,

ADSL - маршрутизатор DSL-504

- 4 порта 10/100 Мбит/с
- 1 порт ADSL
- 1 порт RS-232 (DB-9) для настройки
- Управление на основе Web-интерфейса

Использование DSL-504



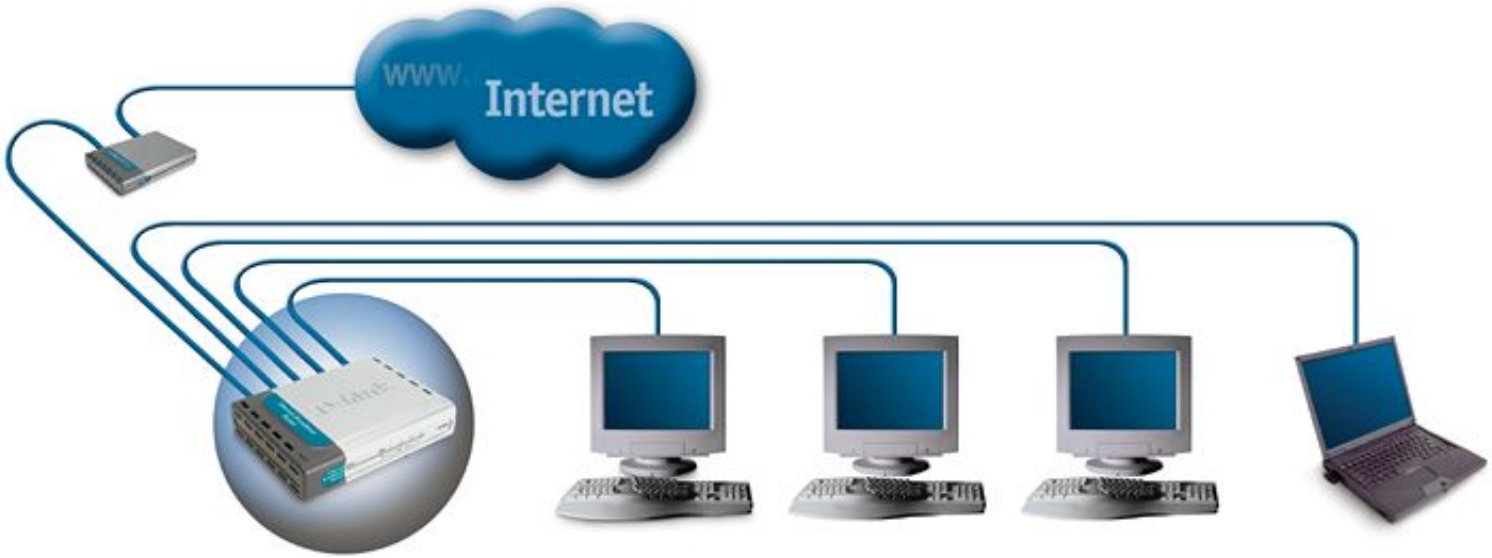
Характеристики DSL-504

- Маршрутизатор со встроенным ADSL-интерфейсом и 4-х портовым коммутатором
- 1 консольный порт (DB-9 RS-232) для настройки
- Высокоскоростное подключение к Интернет
- Стандарты G.dmt и G.lite, скорость нисходящего потока до 8 Мбит/с
- Ethernet over ATM, IP over ATM, PPPoE
- Встроенный NAT и DHCP сервер
- Протоколы маршрутизации RIP-1, RIP-2, Static routing
- Управление через web-интерфейс и консольный порт

Интернет маршрутизатор: DI-604

- 1 порт WAN - 10Base-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

Расширенные функции Firewall в DI-604

NAT с поддержкой VPN	√
Фильтрация на основе MAC адресов	√
Фильтрация на основе IP адресов	√
Фильтрация на основе URL	√
Блокирование определенных доменов	√

Интернет маршрутизатор: DI-614+

- 1 порт WAN – 10/100 Base-T для подключения к DSL или кабельному модему
- 4 порта LAN 10/100 Мбит/с
- Беспроводная точка доступа IEEE-802.11b+

Применение DI-614+

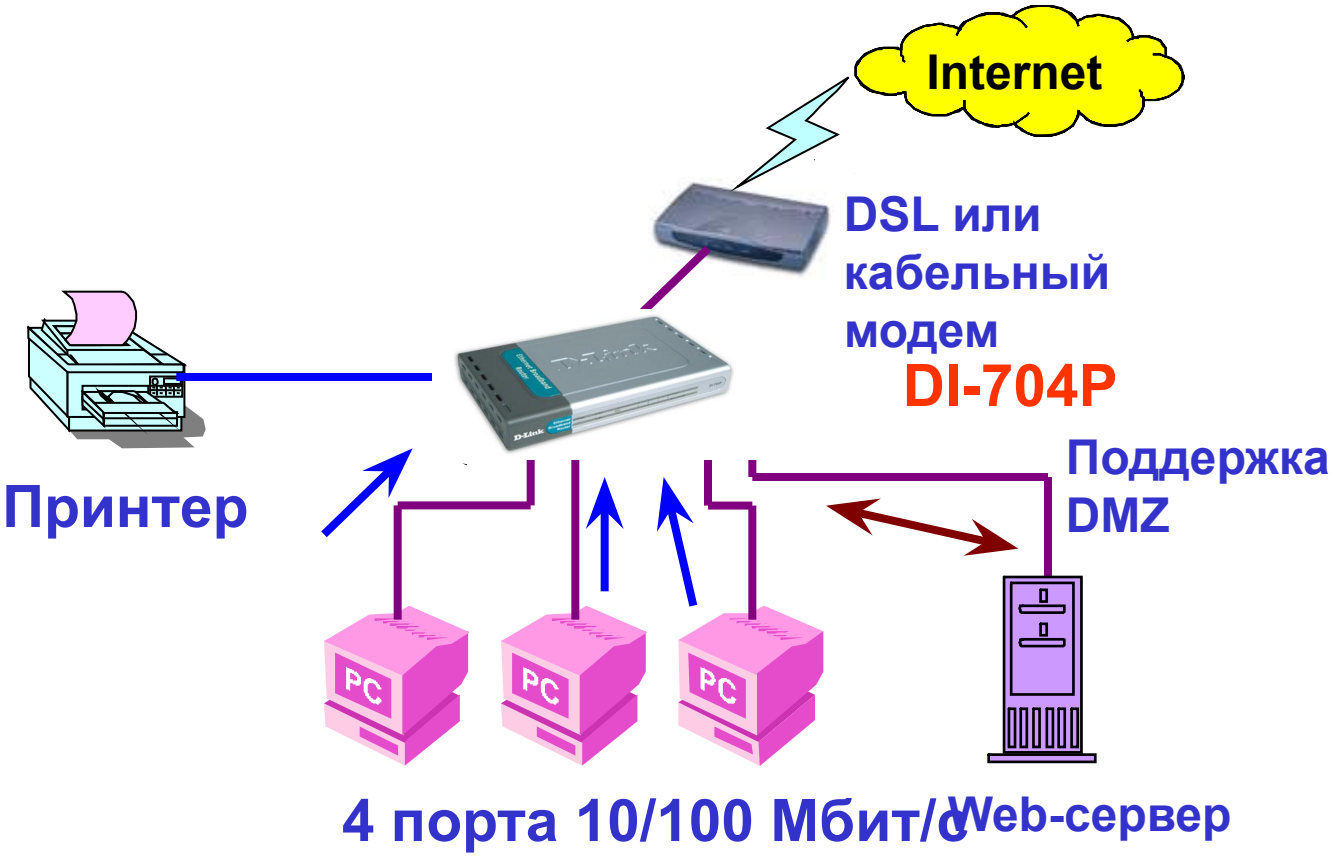
Возможности DI-614+

- 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
- Поддержка маршрутизации RIP 1, RIP 2, Static
- Имеет встроенную беспроводную точку доступа IEEE-802.11b+ - скорость соединения до 22 Мбит/с
- Поддержка виртуального сервера с демилитаризованной зоной – DMZ
- Удобное управление через Web-интерфейс

Широкополосный шлюз: DI-704P

- 1 порт WAN - 10Base-T для подключения к DSL или кабельному модему
- 4 порта LAN 10/100 Мбит/с
- 1 параллельный порт для принтера

Применение DI-704P



Характеристики DI-704P

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

Широкополосный шлюз: DI-714P+

- 1 порт WAN - 10Base-T для подключения к DSL или кабельному модему
- 4 порта LAN 10/100 Мбит/с
- 1 параллельный порт для принтера
- Беспроводная точка доступа IEEE-802.11b+

Применение DI-714P+

Возможности DI-714P+

- 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
- Имеет встроенную беспроводную точку доступа IEEE-802.11b+ - скорость соединения до 22 Мбит/с
- Поддержка контроля доступа
- Поддержка виртуального сервера с демилитаризованной зоной – DMZ
- Удобное управление через Web-интерфейс

Широкополосный шлюз: DI-764

- 1 порт WAN – 10/100 Base-T для подключения к DSL или кабельному модему
- 4 порта LAN 10/100 Мбит/с
- Двухдиапазонная беспроводная точка доступа 802.11a / 802.11b+

Применение DI-764

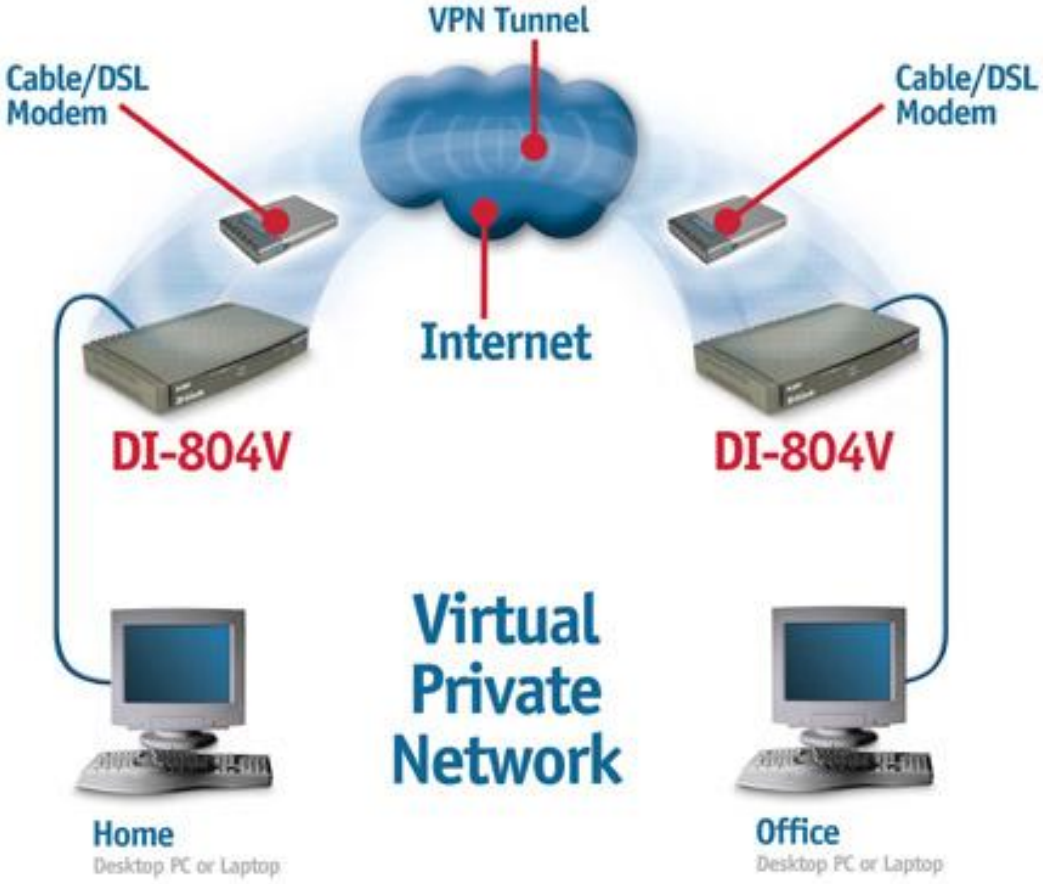
Возможности DI-764

- Доступ в Интернет как для проводных, так и для беспроводных клиентов
- Встроенный 4- х портовый коммутатор Fast Ethernet
- Поддержка VPN
- Межсетевой экран
- Двухдиапазонная беспроводная точка доступа стандартов 802.11a и 802.11b+ - скорость соединения до 54 Мбит/с
- Поддержка контроля доступа с возможностью задания расписания действия правил доступа
- Поддержка виртуального сервера с демилитаризованной зоной – DMZ
- Поддержка протокола NTP для синхронизации времени
- Удобное управление через Web-интерфейс

Интернет - маршрутизатор: DI-804HV

- 1 порт WAN - 10Base-T для подключения к DSL или кабельному модему
- 1 порт WAN – RS-232 для подключения к Dial-up модему
- 4 порта LAN 10/100 Мбит/с
- Управление через Web-интерфейс
- Поддержка VPN: до 40 туннелей IPSec

Применение DI-804V / DI-804HV



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
- Маршрутизация: RIP I, RIP II, Static
- Встроенный межсетевой экран
- Встроенный клиент PPTP и PPPoE для установления VPN-тоннеля с провайдером иди центральным офисом
- Встроенный PPTP и L2TP сервер
- Поддержка IPSec: до 40 туннелей
- Встроенный DHCP-сервер
- Порт RS-232 для подключения внешнего аналогового модема
- Управление посредством Web-браузера

Спасибо за внимание!

ftp://ftp.dlink.ru/pub/Training/presentations/

Иван Мартынюк
D-Link Украина
Консультант по проектам
Тел./Факс +380 (44) 216-91-51
IMartynyuk@Dlink.ru
www.D-Link.ua