Технологии защищенного канала

Основные функции защищенного канала

:

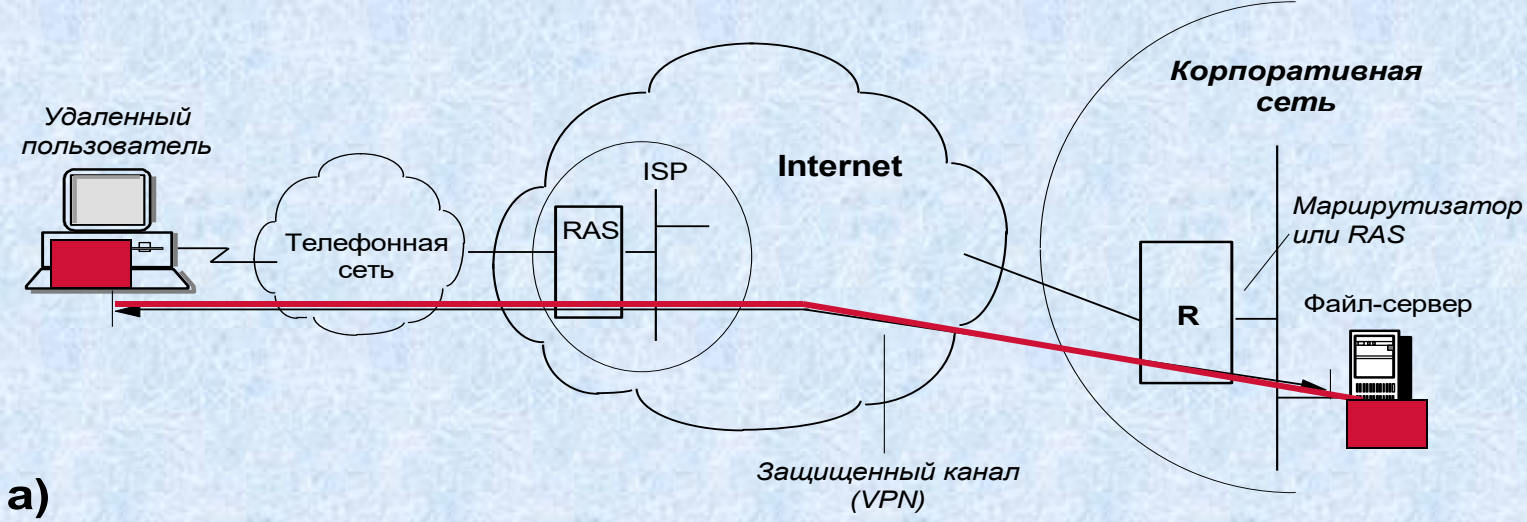
- взаимная аутентификация абонентов,
- защита передаваемых по каналу сообщений от несанкционированного доступа,
- подтверждение целостности поступающих по каналу сообщений

Протоколы, формирующие защищенный канал на разных уровнях

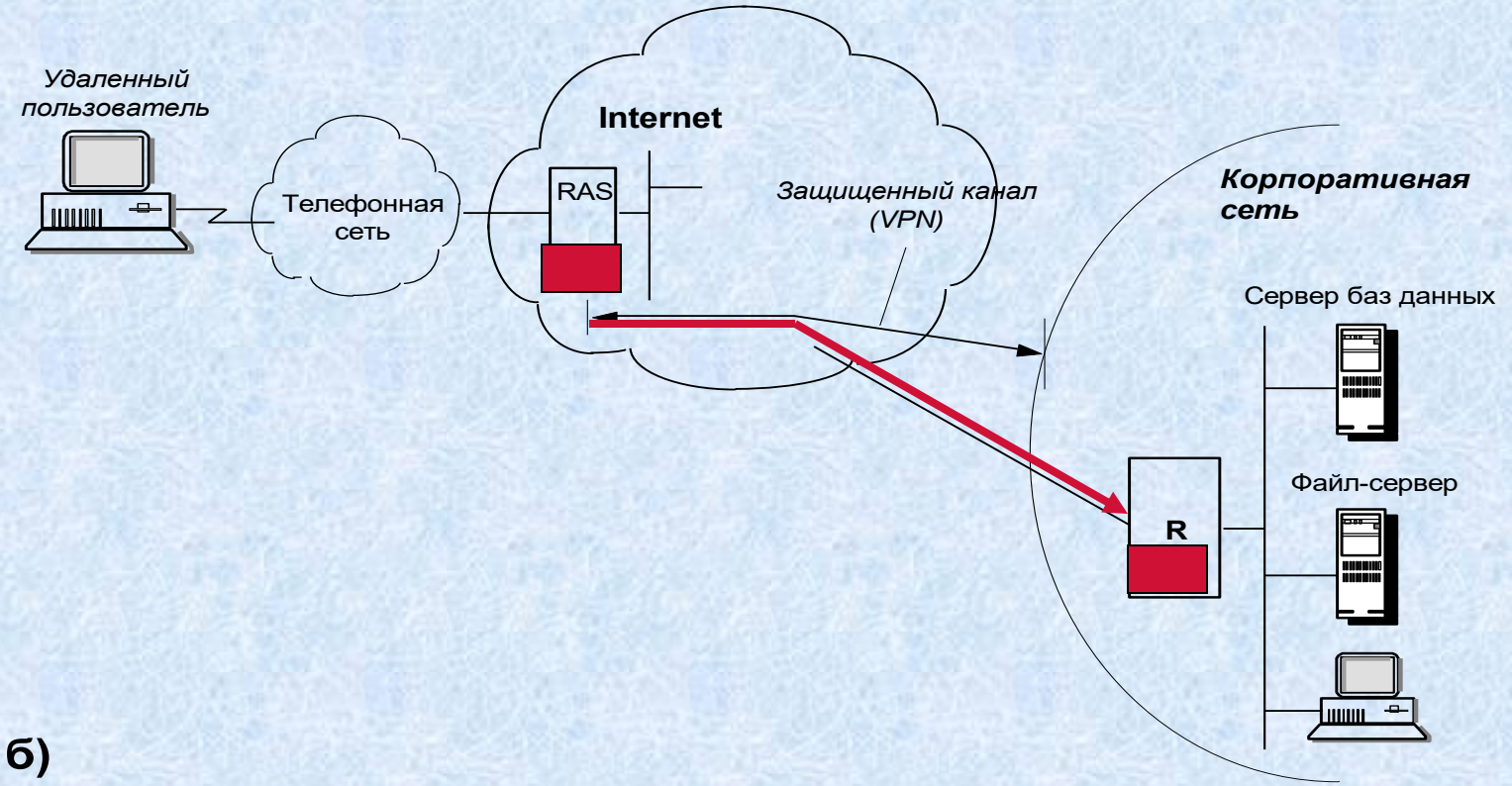
Прикладной	HTTP/S, S/MIME	Непрозрачны для приложений, не зависят от транспортной инфраструктуры
Презентационный	SSL	
Сеансовый		
Транспортный		
Сетевой	IPSec, SKIP	Прозрачны для приложений, зависят от транспортной инфраструктуры
Канальный	PPTP	
Физический		

Два способа образования защищенного канала

1. Средствами конечных узлов
   - $\Rightarrow$ полная защищенность канала вдоль всего пути следования
   - $\Rightarrow$ возможность использования любых протоколов создания защищенных каналов
   - $\Rightarrow$ избыточность и децентрализованность решения
   - $\Rightarrow$ необходимость отдельного администрирования каждого сервера и каждого клиентского компьютера
2. Средствами шлюзов, стоящих на границе между частной и публичной сетями


Удаленный пользователь
Телефонная сеть
ISP
RAS
Internet
Корпоративная сеть
Маршрутизатор или RAS
R
Файл-сервер
Защищенный канал (VPN)

а)


Удаленный пользователь
Телефонная сеть
RAS
Internet
Защищенный канал (VPN)
Корпоративная сеть
Сервер баз данных
Файл-сервер
R

б)

Internet Protocol Security (IPSec)

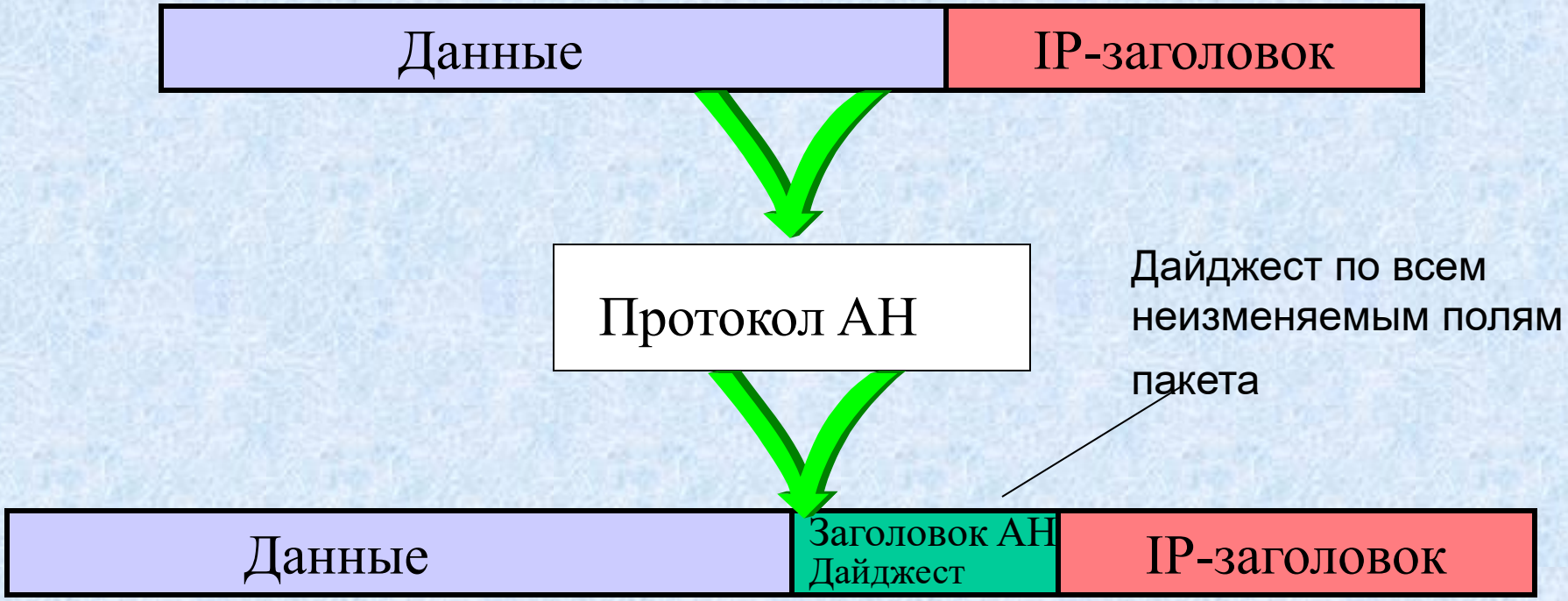
- система протоколов для защиты трафика IP-сетей
- ядро стандартизовано в конце 1998 года. Стандарт на архитектуру - RFC2401
- поддерживается IPv6

<table>
<tr><th>Решаемые задачи</th><th colspan="2">Протокол</th></tr>
<tr><td>Целостность</td><td rowspan="3">ESP</td><td rowspan="2">AH</td></tr>
<tr><td>Аутентификация</td></tr>
<tr><td>Шифрование</td><td></td></tr>
<tr><td>Распределение секретных ключей</td><td colspan="2">IKE</td></tr>
</table>

Протокол Autentication Header (AH)

обеспечивает:

- целостность
- аутентификацию передаваемых данных
- защиту от дубликатов (опционально)



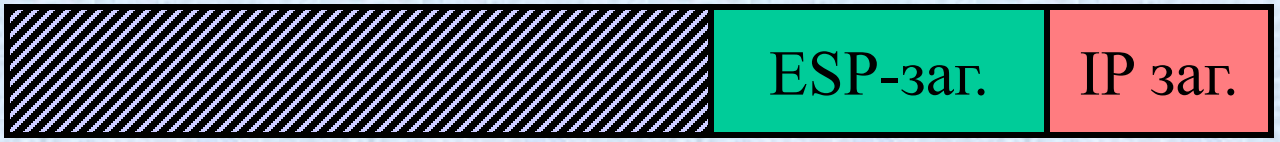
Encapsulation Security Payload (ESP)

обеспечивает:

- целостность
- аутентификацию передаваемых данных
- защиту от дубликатов (опционально)
- ***шифрование трафика***

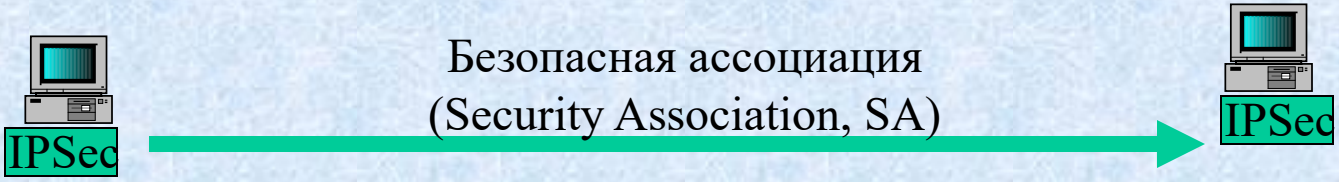
Целостность - дайджест для поля данных

Шифрование - по симметричному принципу



Internet Key Exchange (IKE)

- протокол распределения ключей



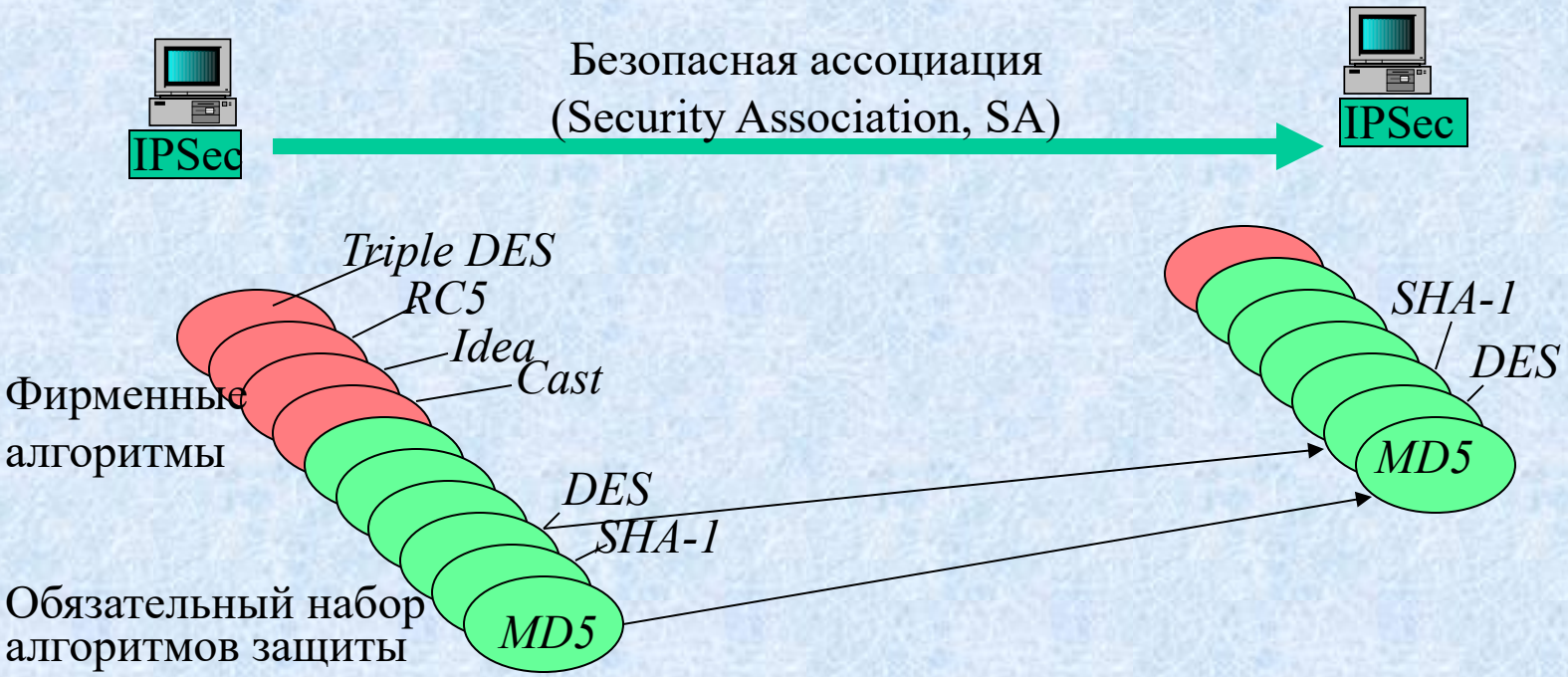
Установить SA -

(1) аутентифицировать стороны

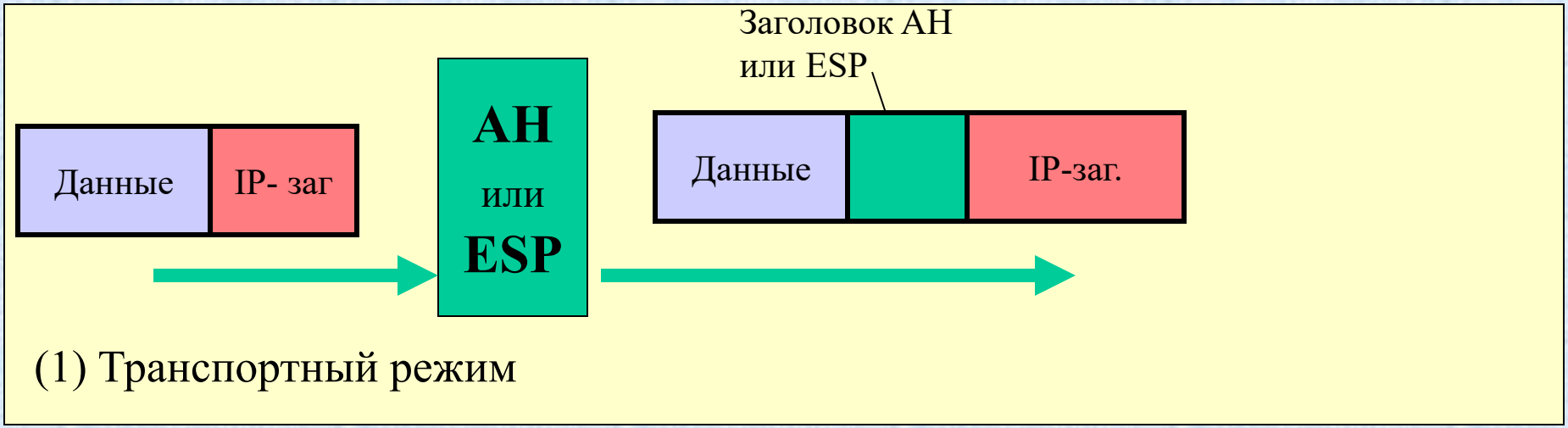
(2) согласовать параметры защиты

- SA - однонаправленное (симплексное) логическое соединение
- Между узлами устанавливается произвольное количество SA
- В рамках одной SA нельзя использовать одновременно AH и ESP

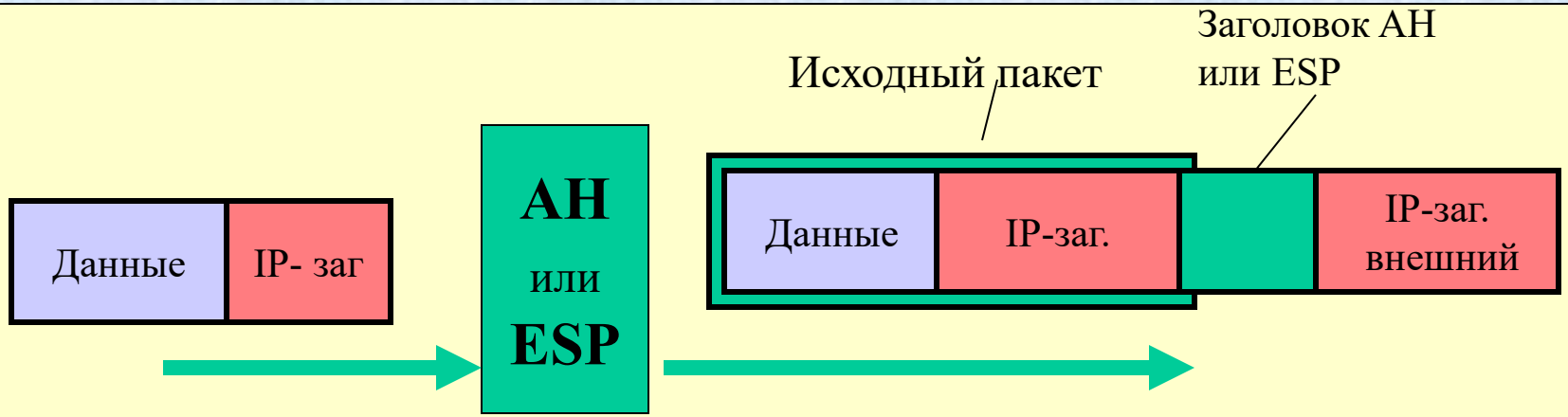
Согласование параметров в протоколе ESP



Два режима работы протоколов AH и ESP



(1) Транспортный режим



(2) Туннельный режим

Режим работы в одном направлении не зависит от режима работы в другом направлении

3 схемы установления SA

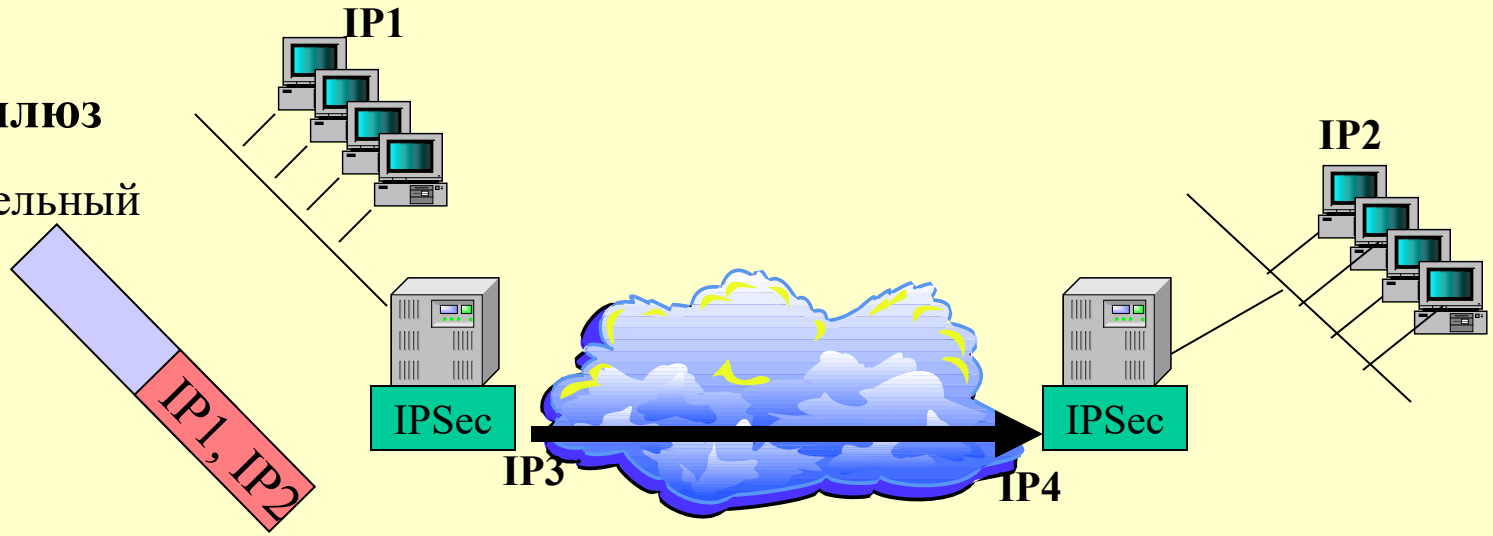
(1) хост-хост

режимы:

- транспортный
- туннельный

(2) шлюз-шлюз

режим: туннельный

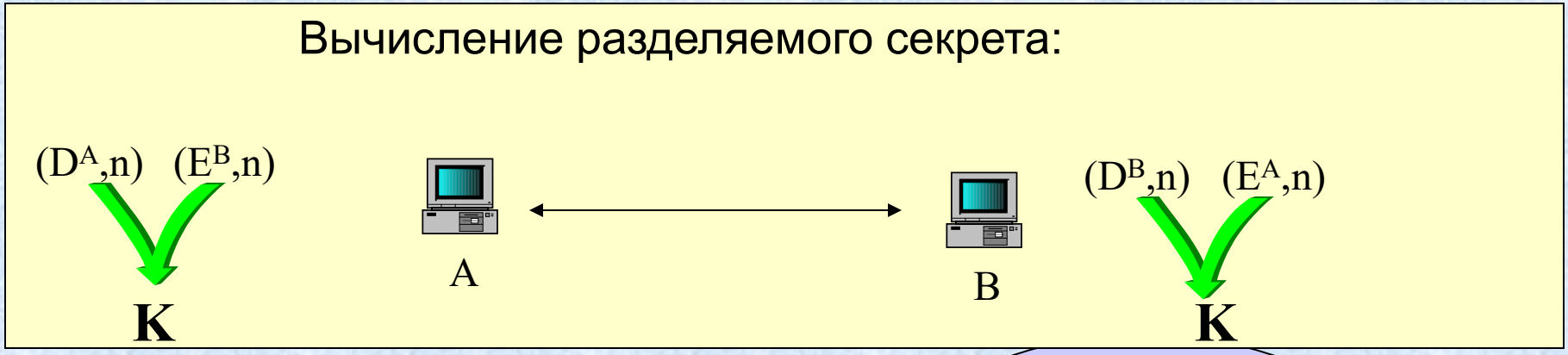


(3) хост-шлюз

Протокол IKE

(1) Проверка аутентичности сторон

- аналогично протоколу CHAP
- обмен сертификатами



(2) Согласование параметров защиты

способы:

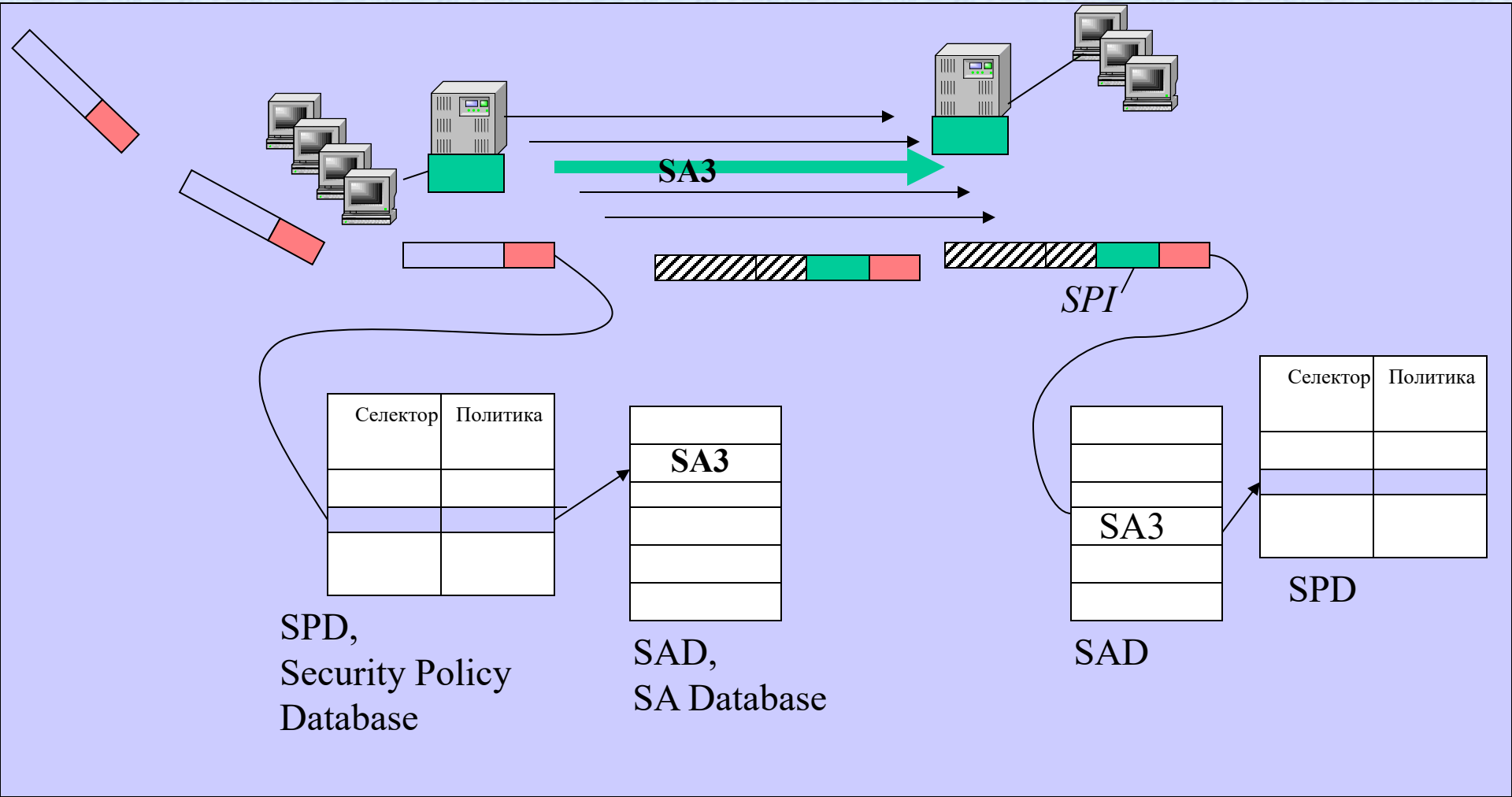
- ручной
- автоматический

Параметры:

- **протокол**
- **опция дубликатов**
- **режим**
- **используемые алгоритмы**
- **секретные ключи**

Механизм распознавания пакетов, относящихся к разным безопасным ассоциациям

- на узле-отправителе - ***селектор***
- на узле-получателе - ***SPI (Security Parameters Index)***



Механизм распознавания пакетов, относящихся к разным ассоциациям SA

Security Polisy Database (SPD)

Селектор						Политика			
IP-адрес назначения	IP-адрес источника	DNS-имя пользователя	DNS-имя узла	Тип протокола	Порт TCP, UDP	Прото-кол защиты	Режим	Опция дублей	Указа-тель на SA

В каждом узле должно быть 2 SPD - для входящих и исходящих пакетов

База данных параметров безопасных ассоциаций
Security Association Database (SAD)

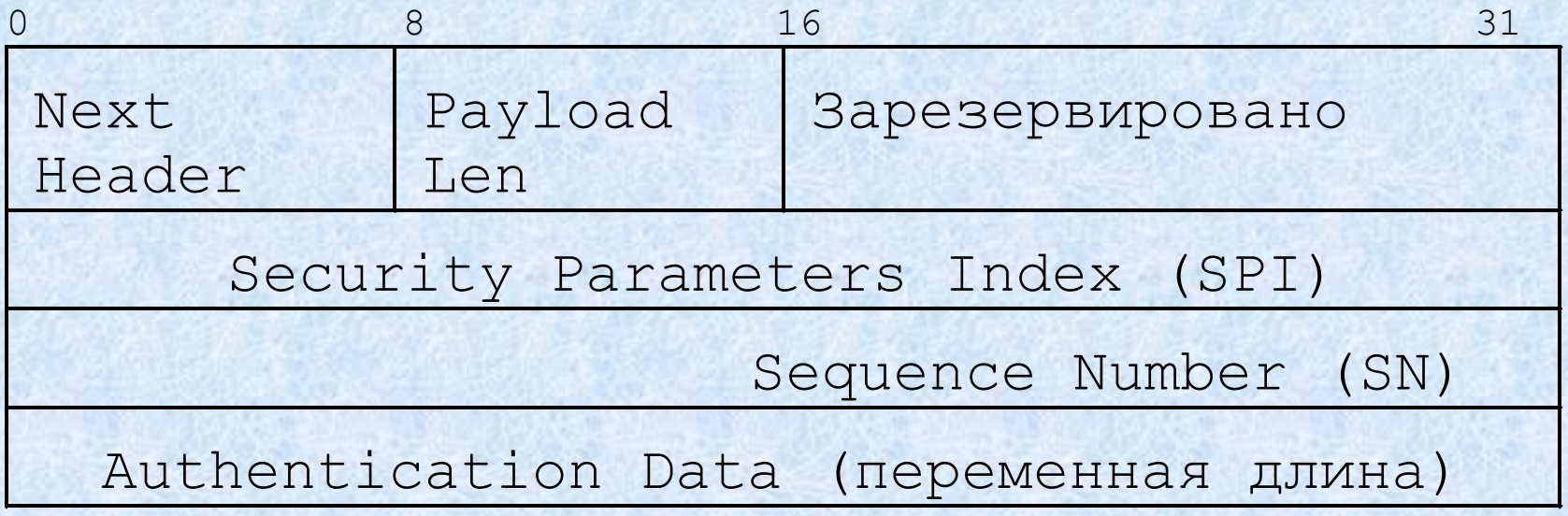
	Текущие параметры SA		
	Ключ	Номер пакета	…
SA1			
SA2			
SA3			
SA4			

Защита данных с помощью протокола AH

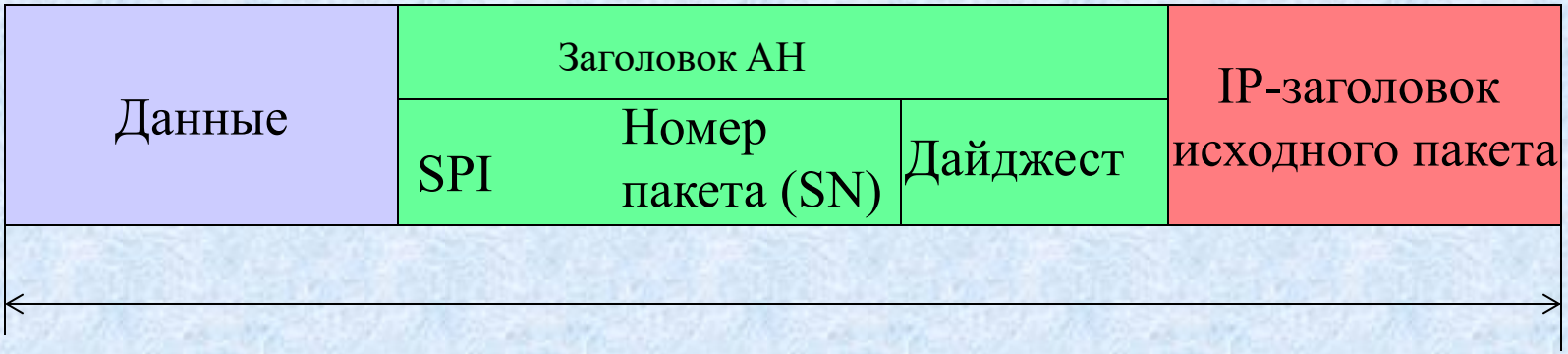
Проверка условий:

- пакет был отправлен стороной, с которой была установлена данная ассоциация,
- содержимое пакета не было искажено в процессе передачи его по сети,
- пакет не является дубликатом некоторого пакета, полученного ранее.

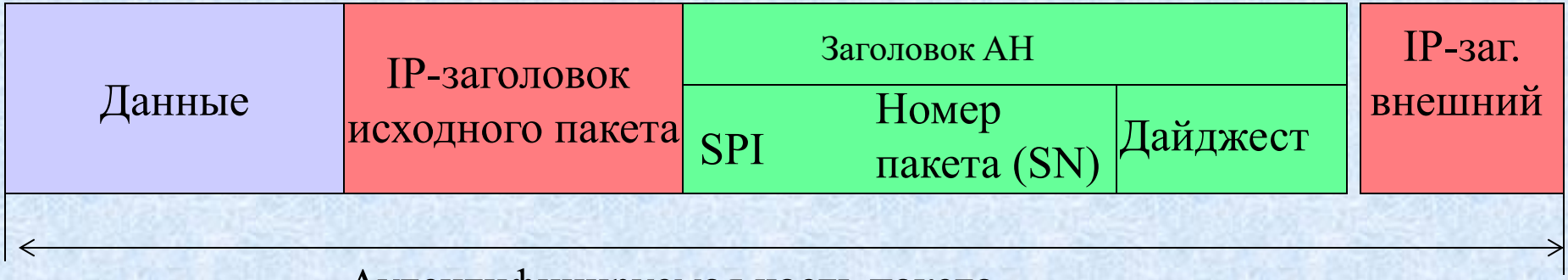
Структура заголовка протокола AH



А) транспортный режим

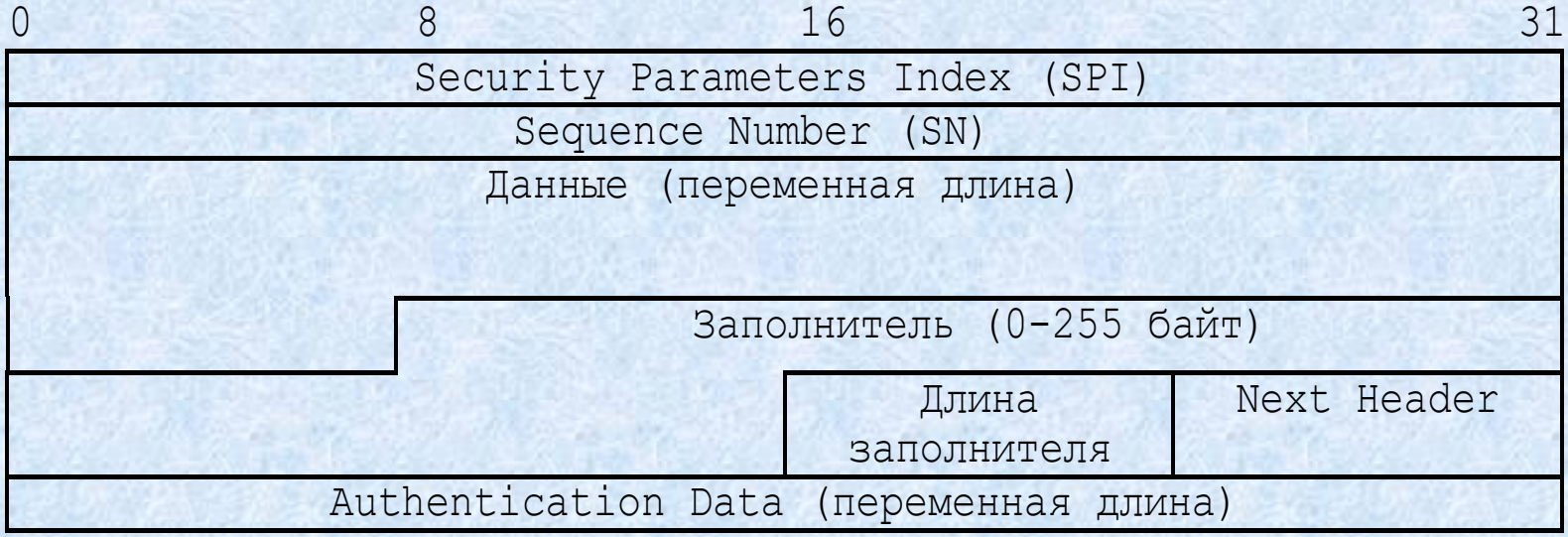


Б) туннельный режим



Протокол защиты данных ESP

Структура заголовка

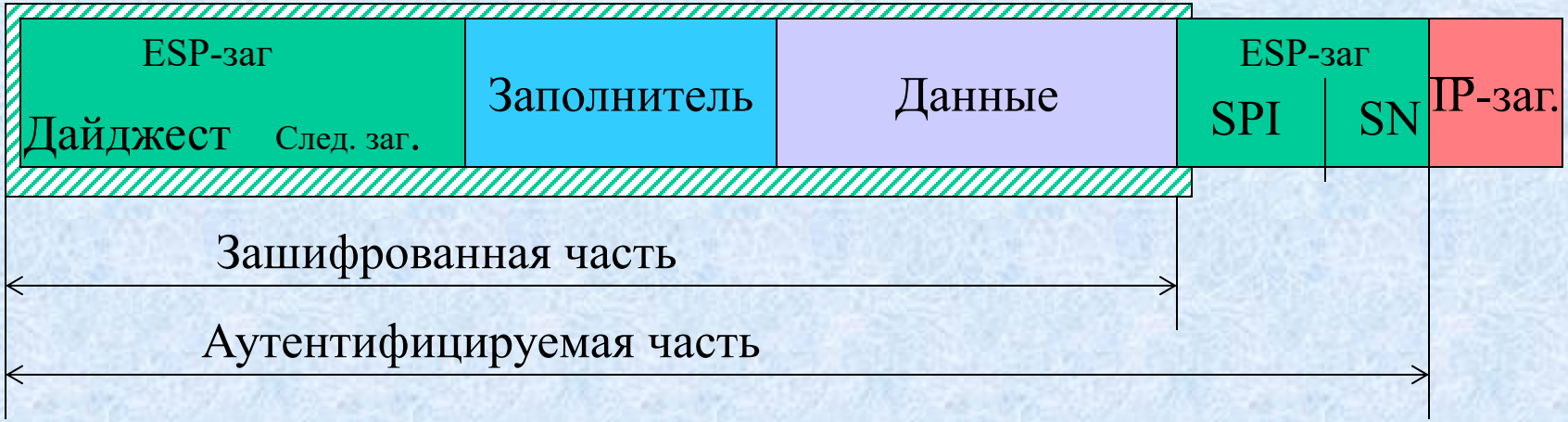


Заполнитель:

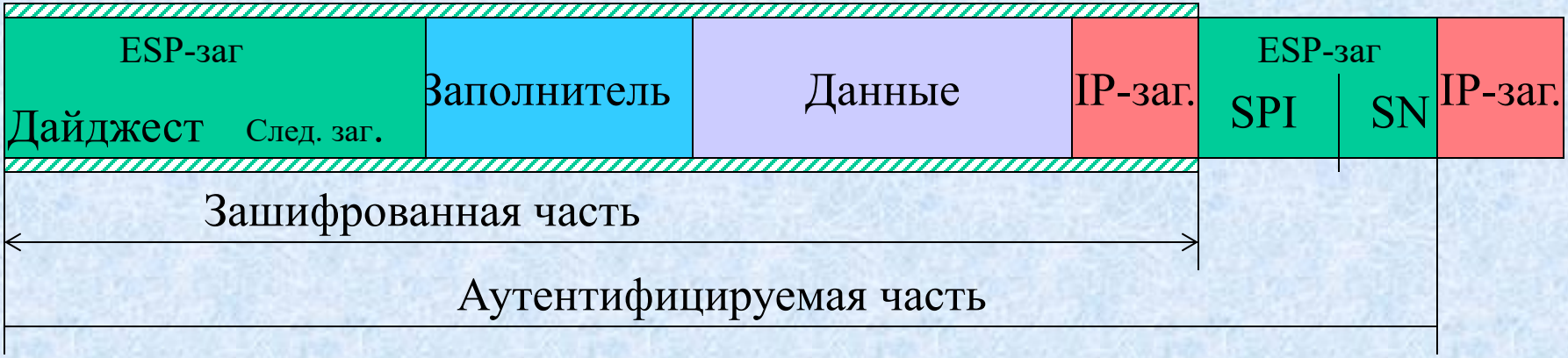
(1) требования методов шифрации

(2) формат заголовка ESP

(3) частичная конфиденциальность трафика



А) транспортный режим



б) туннельный режим

Протокол PPTP (Point-to-Point-Tunneling Protocol)

- протокол создания защищенного канала при доступе удаленных пользователей через публичные сети к корпоративным сетям
- разработан компанией Microsoft совместно с Ascend Communications, 3Com/Primary Access, ECI-Telematics и US Robotics
- был представлен в IETF в качестве претендента на стандарт, однако не был утвержден
- в качестве стандарта был принят L2TP (Layer 2 Tunneling Protocol), который объединяет черты протоколов PPTP и L2F (Layer 2 Forwarding)
- протокол инкапсуляции кадров канального уровня PPP в сетевой протокол IP
  - *многопротокольность*
  - *прозрачность для протоколов прикладного и сетевого уровней*

Защищенный канал PPTP

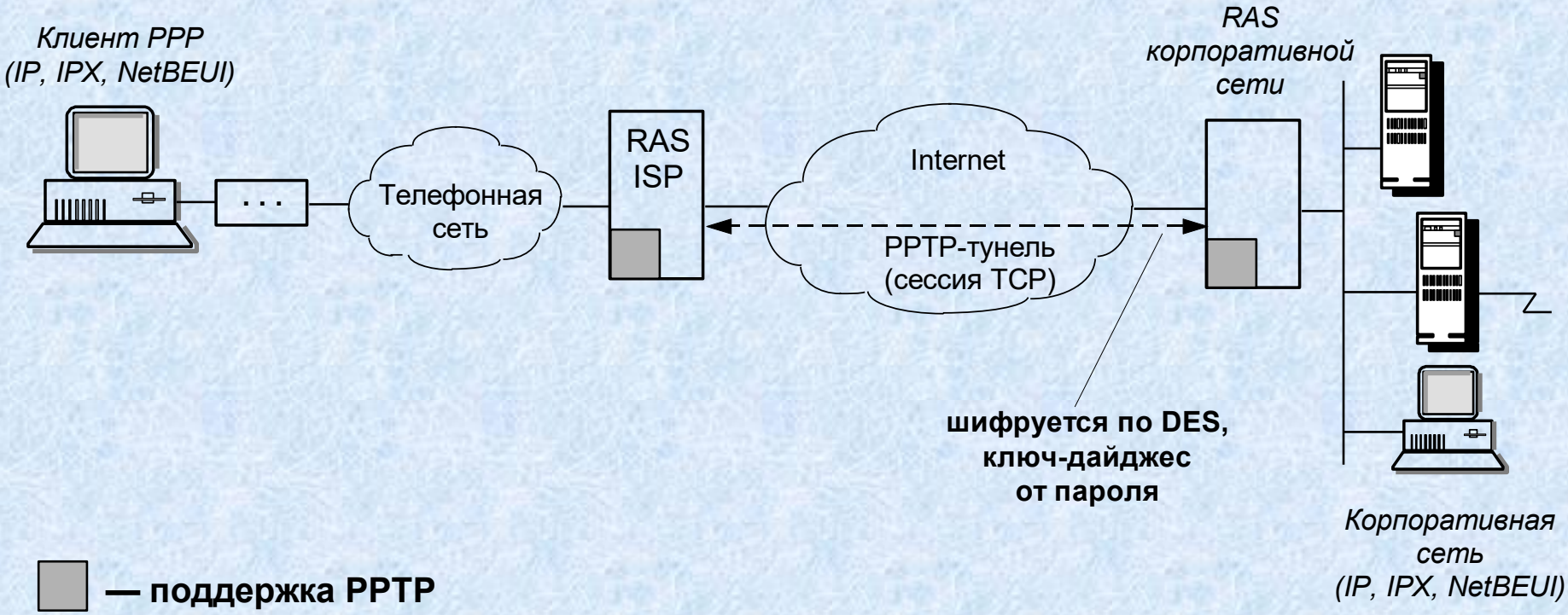
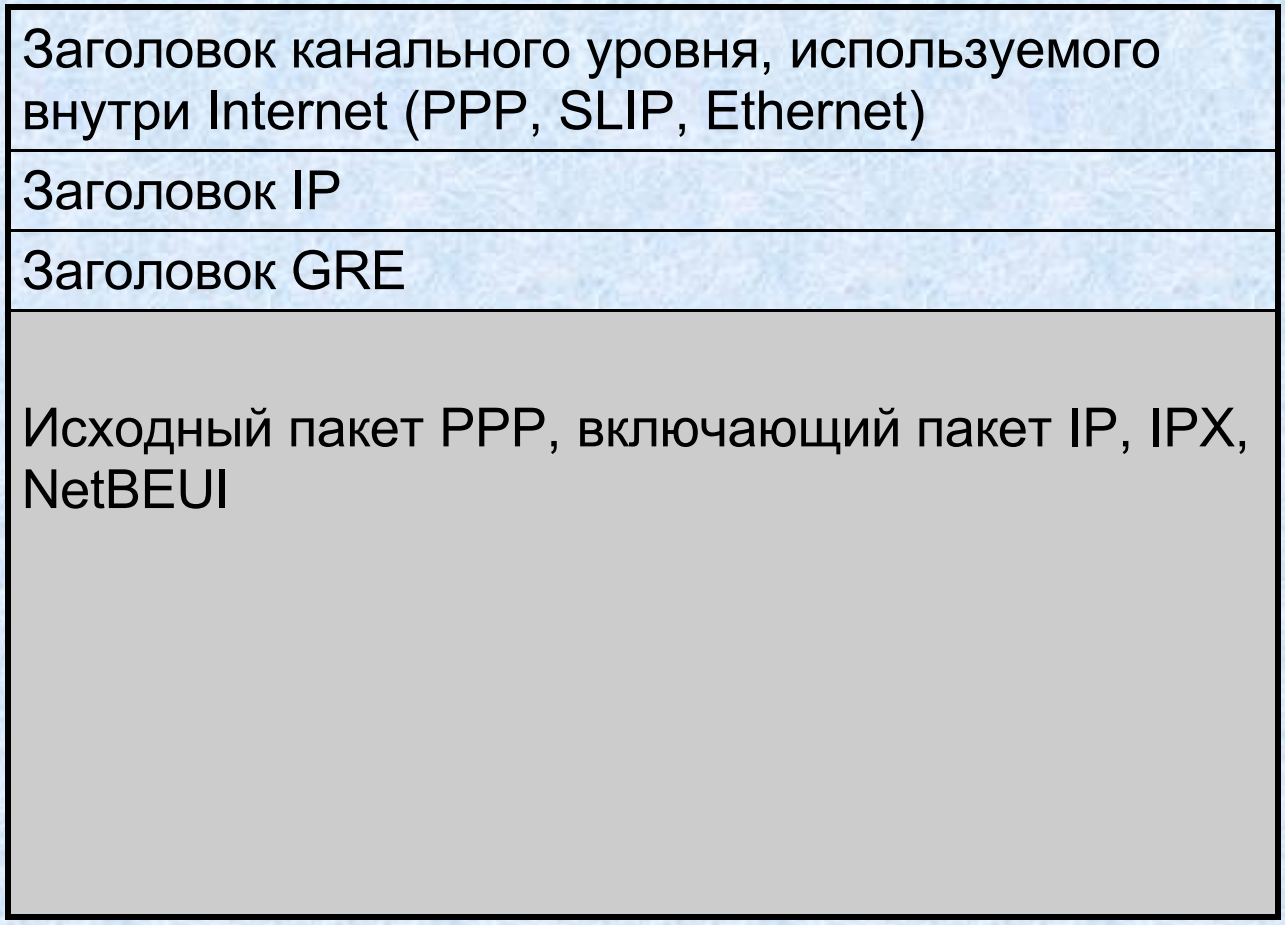
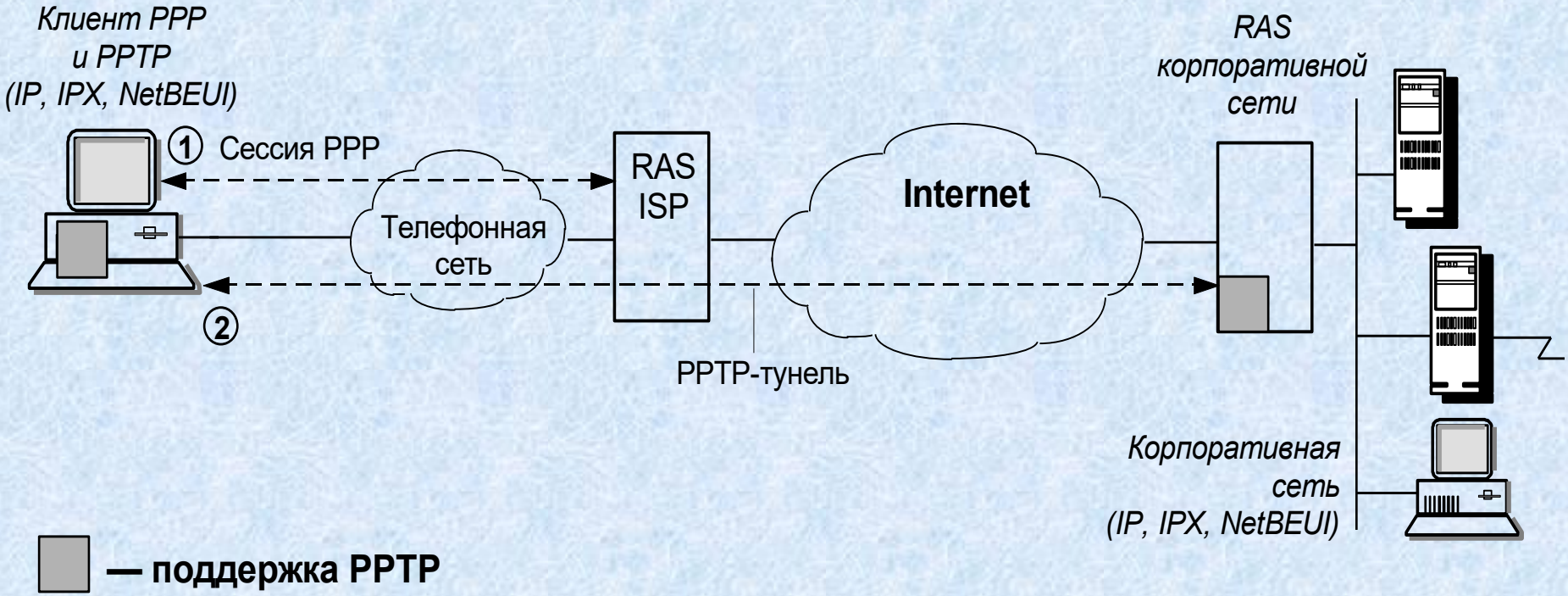


Схема инкапсуляции протокола PPTP



Реализация Microsoft



Протокол Secure Socket Layer (SSL)

- разработан компанией Netscape Communications для защиты данных, передаваемых между Web-сервером и Web-браузером
- работает на представительном уровне
- создает защищенный канал между конечными узлами
- может использоваться для защиты данных любых приложений

⇒ **Взаимная аутентификация** выполняется путем обмена сертификатами (стандарт X.509)

⇒ **Секретность** обеспечивается шифрацией с использованием симметричных сессионных ключей

⇒ **Целостность** путем добавления дайджеста