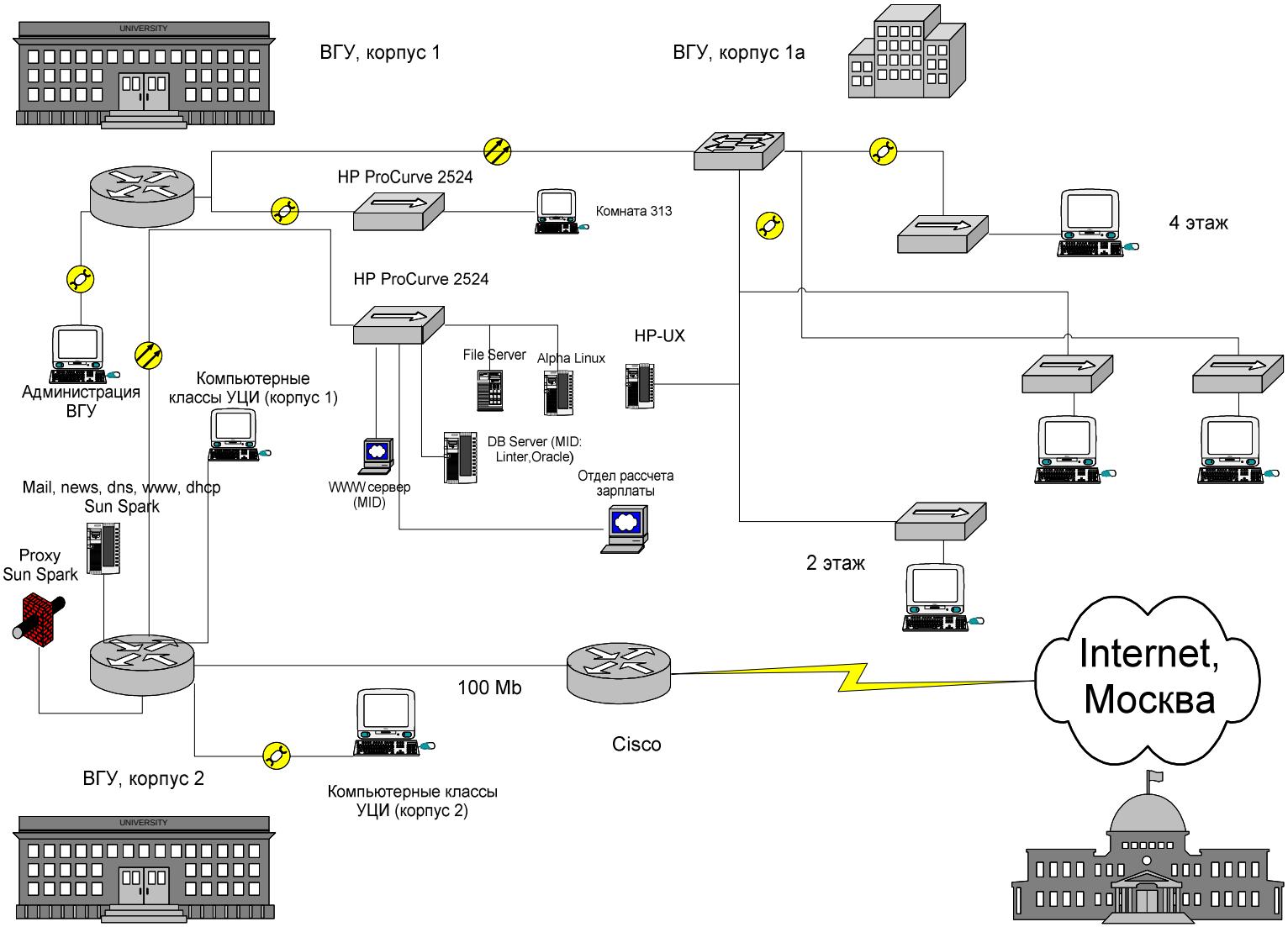
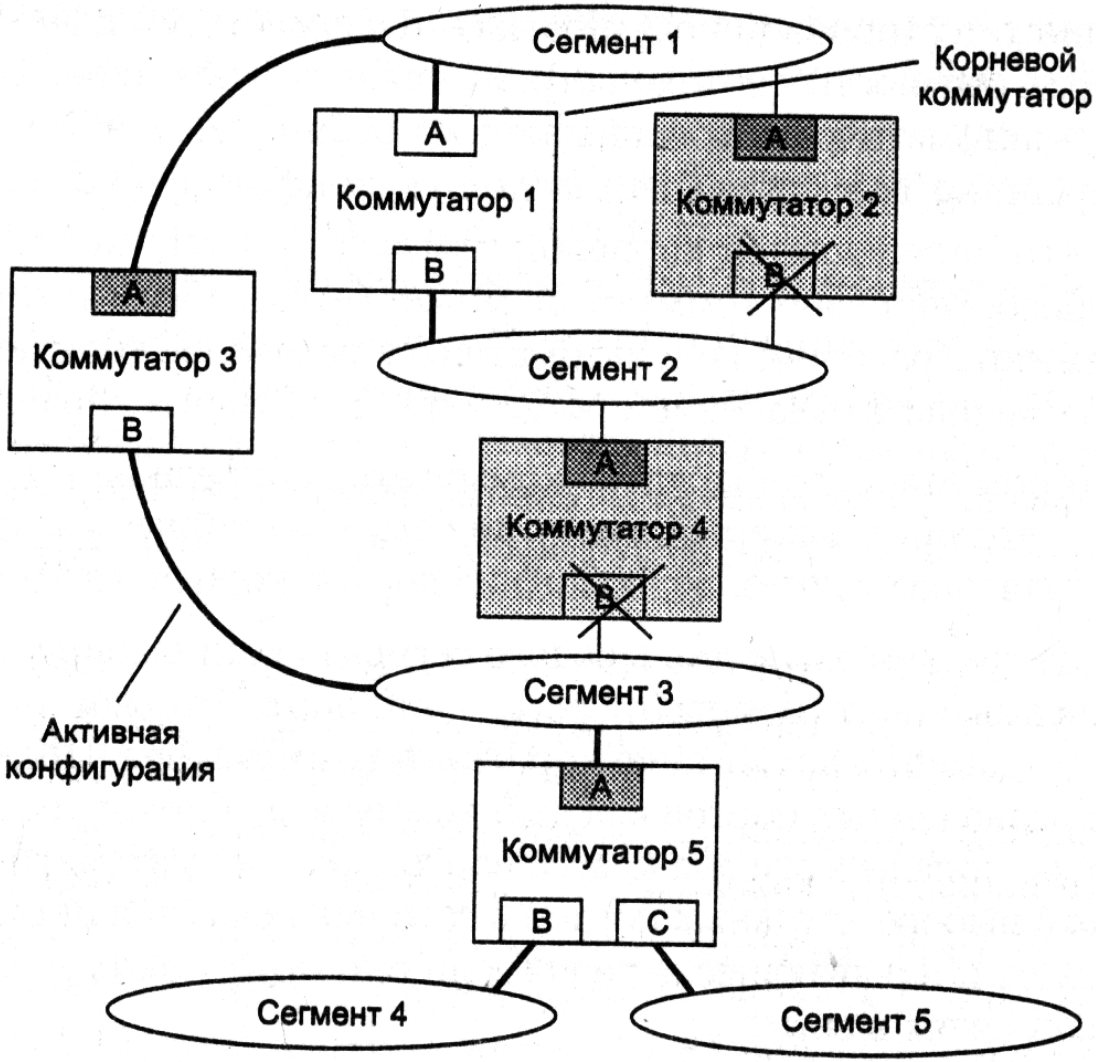
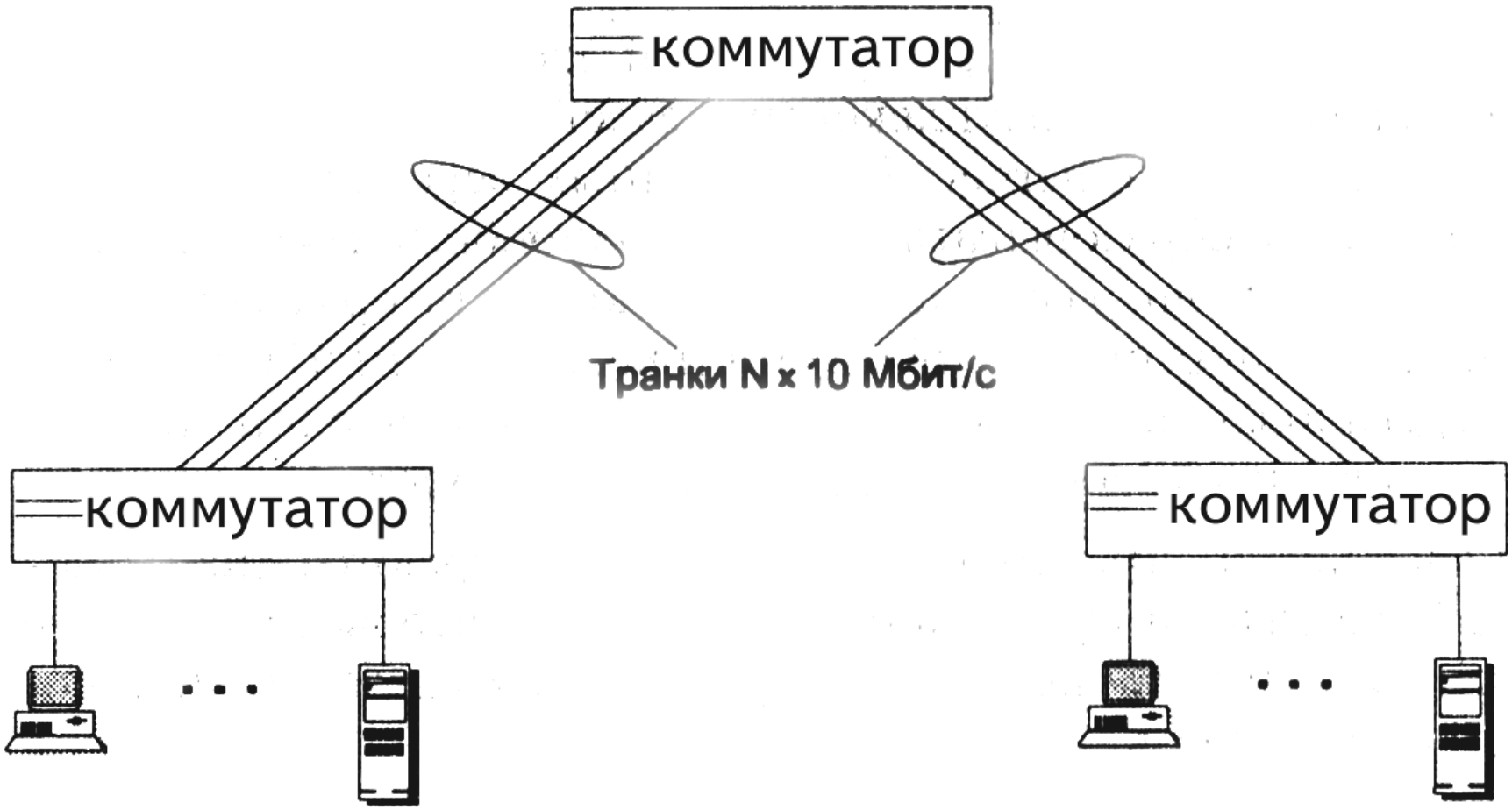
Современное оборудование интранет-сетей (сеть ВГУ)



Spanning Tree Algorithm/Protocol, IEEE802.1D



Агрегирование каналов, trunking

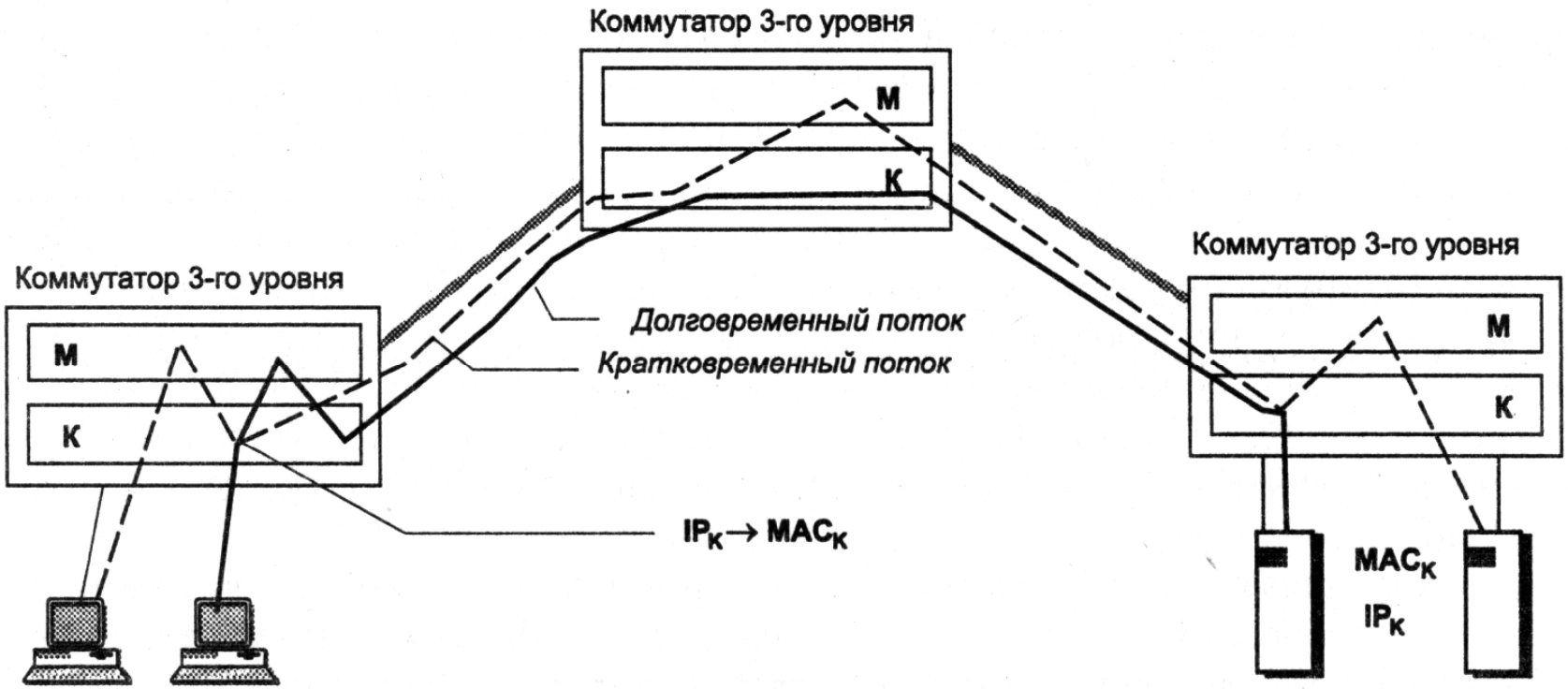


Агрегирование каналов, 802.3ad

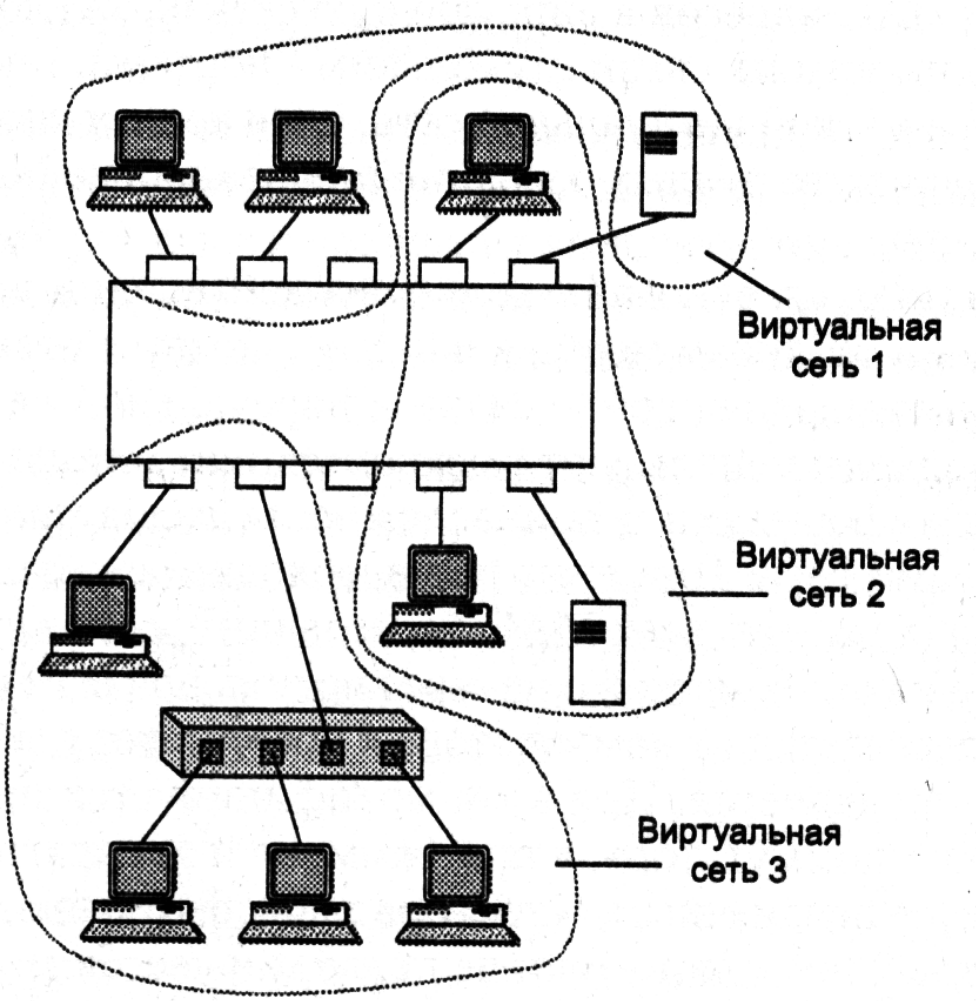
- 802.3ad Link Aggregation (LACP)
- …

Стандарт 802.3af (Питание через сеть Ethernet, PoE)

Коммутаторы 3 уровня (Layer3)



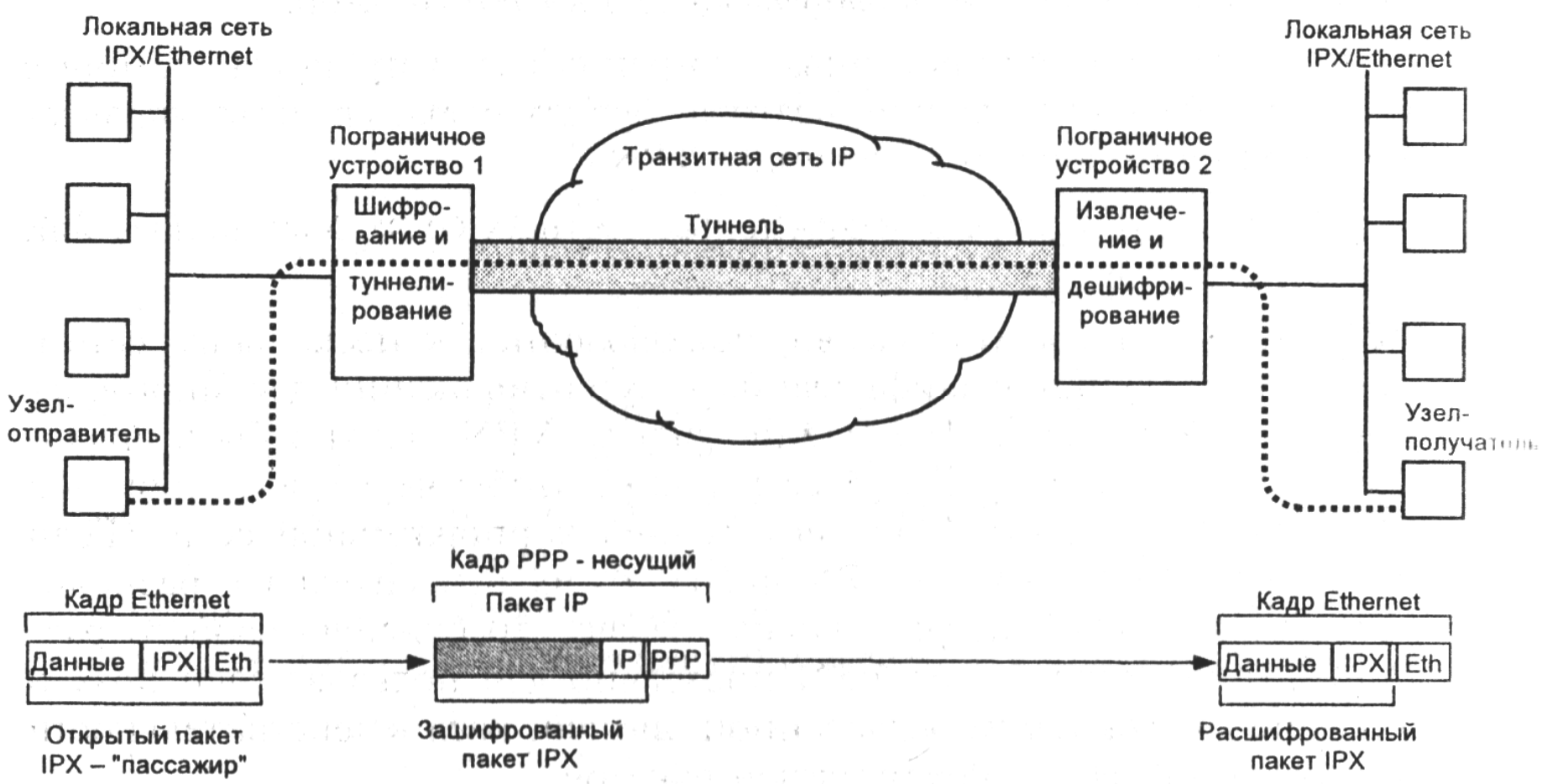
Виртуальные сети (VLAN)



IEEE802.1p/Q определяет формат инкапсуляции дополнительного поля для номера VLAN (12 бит) и номера приоритета (3 бита)

Кроме того, в коммутируемой сети возможно создавать multicast-группы

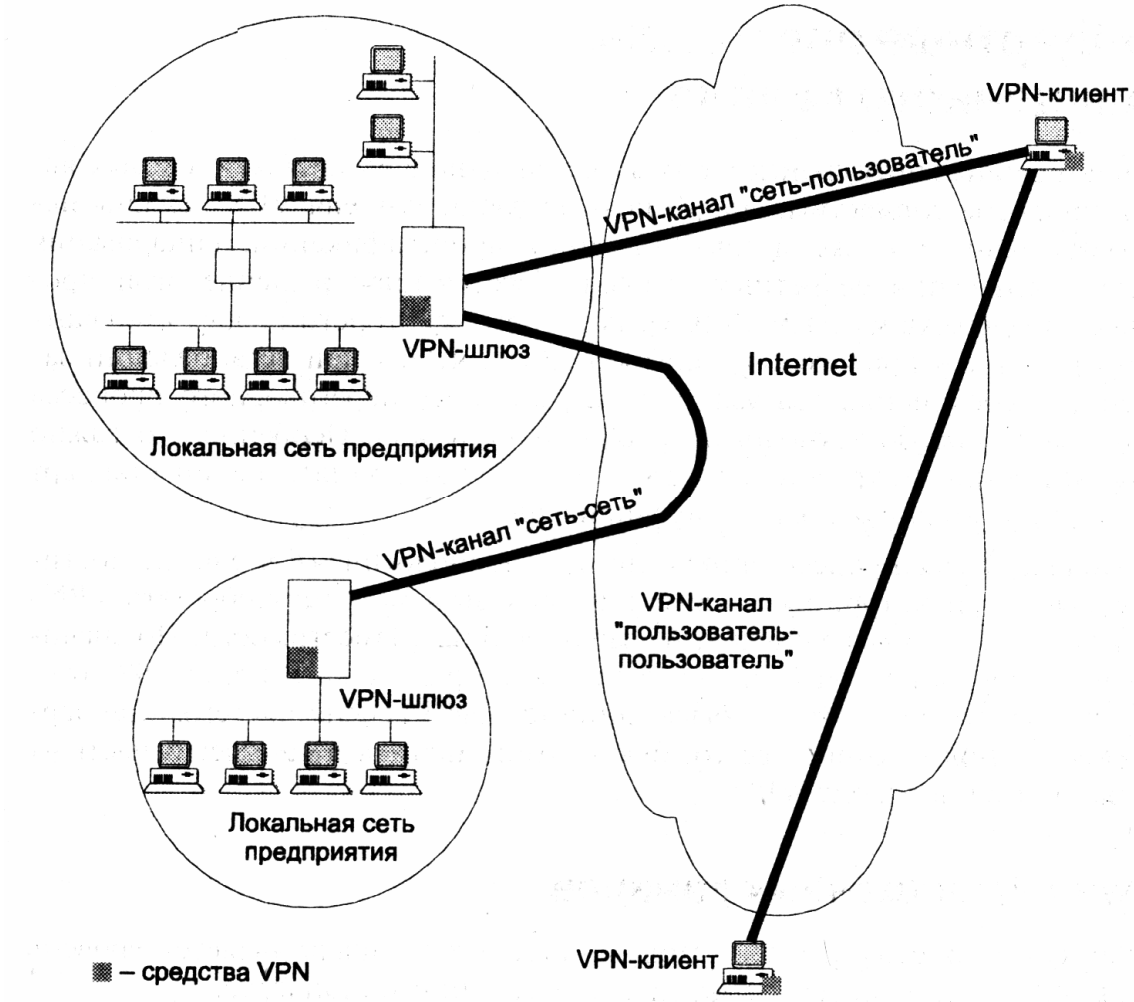
Инкапсуляция, туннелирование

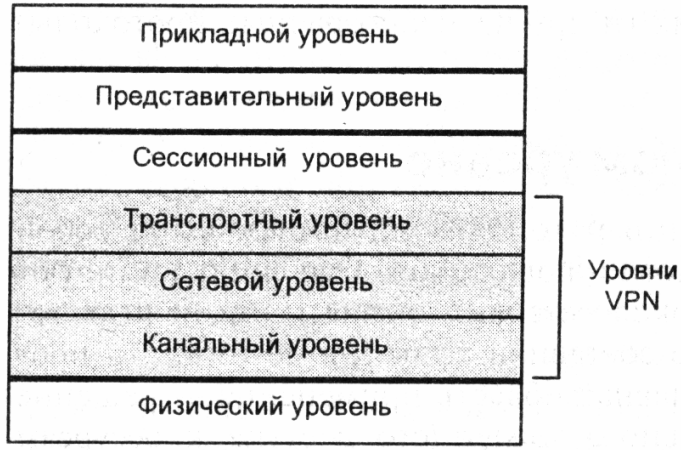


Виртуальные частные сети, VPN

- Применяются для:
  - организации глобальной связи между филиалами одной компании (интрасеть)
  - для соединения частной сети кампании с ее деловыми партнерами и клиентами (экстрасеть)
  - для взаимодействия с корпоративной сетью отдельных мобильных сотрудников и клиентов (удаленный доступ)
- Задачи VPN:
  - защита корпоративных данных от несанкционированного доступа и модификации
  - обеспечение гарантированного качества обслуживания

Шлюзы и клиенты VPN





Архитектура QoS. RSVP, 802.1p/Q

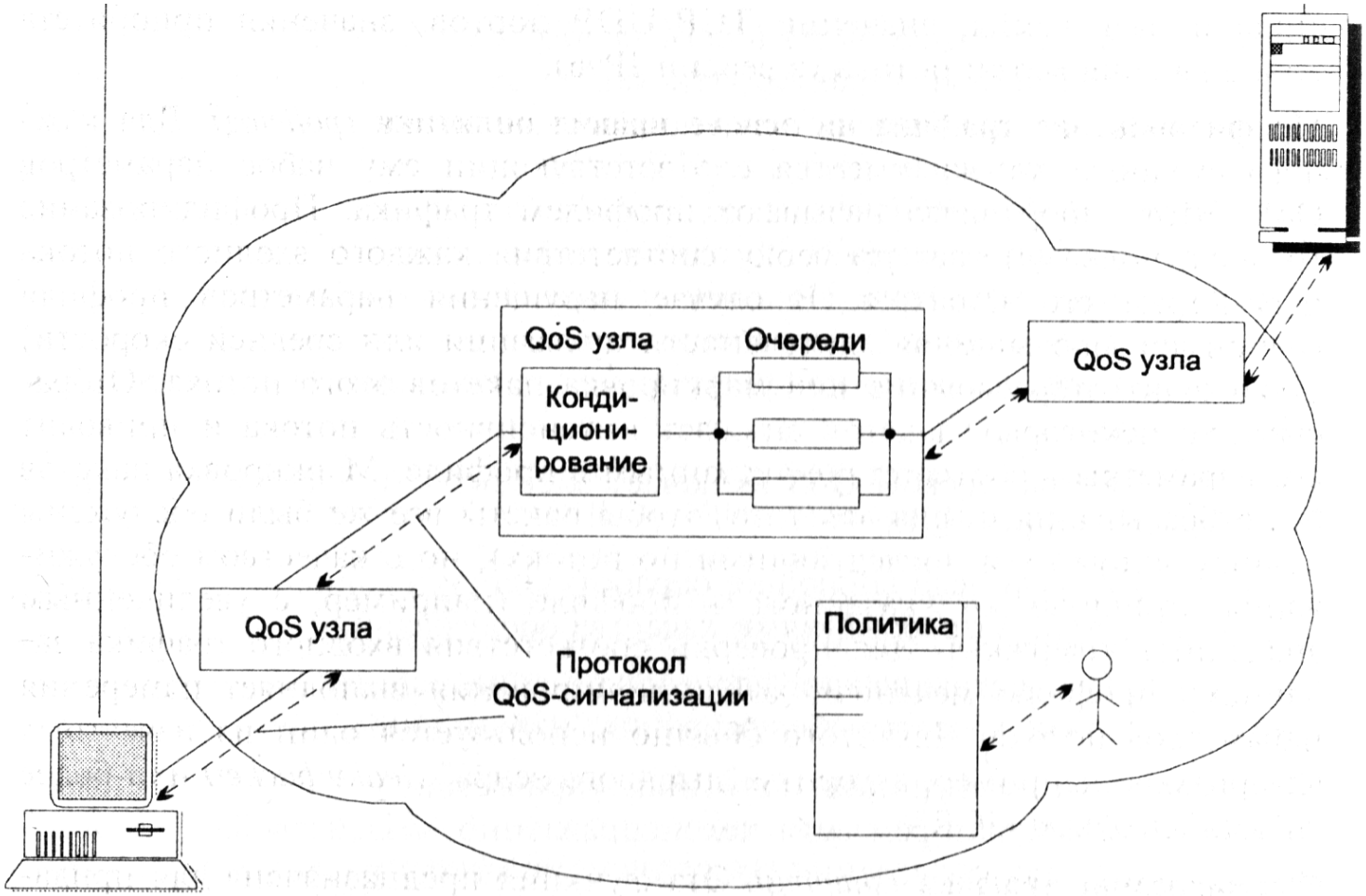
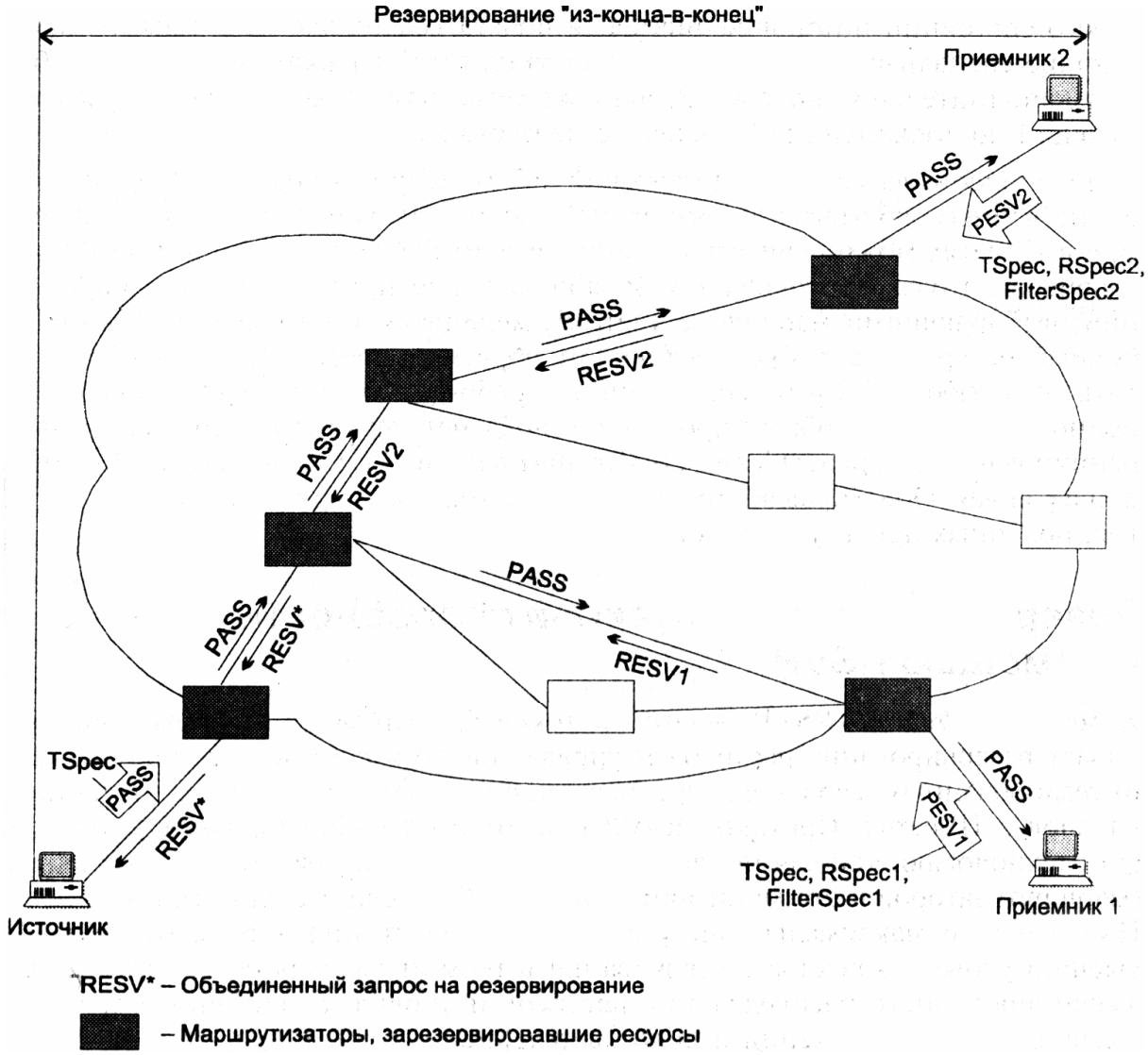
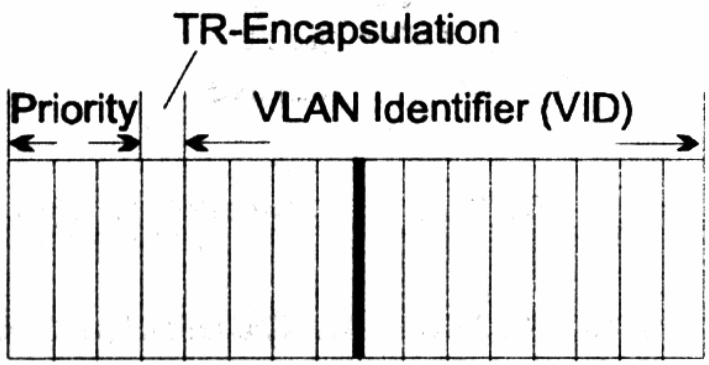


Рис. 2.18. Базовая архитектура средств QoS

Резервирование с помощью RSVP (ReSerVation Protocol)



Структура кадра Ethernet с полем 801.2Q



Адрес назначения	Адрес источника	Tag Protocol Identifier	Метка VLAN	Ether Type	. . .
6 байт	6 байт	2 байта	2 байта	2 байта	

Недостатки IPv4

- Низкая безопасность
  - возможность подмены IP;
  - отсутствие надежных схем аутентификации у многих распространенных приложений;
- Сложность организации группового вещания
  - маршрутизаторы должны хранить информацию о группах и источниках распространения информации.
- Отсутствие гарантий QoS
- Низкая пропускная способность маршрутизаторов из-за резкого увеличения объема выполняемых ими операций при росте сети:
  - сборка/разборка IP-пакетов;
  - работа с большим количеством подсетей.

Цели модернизации IPv4 (1994 – IPng, 1998 – IPv6)

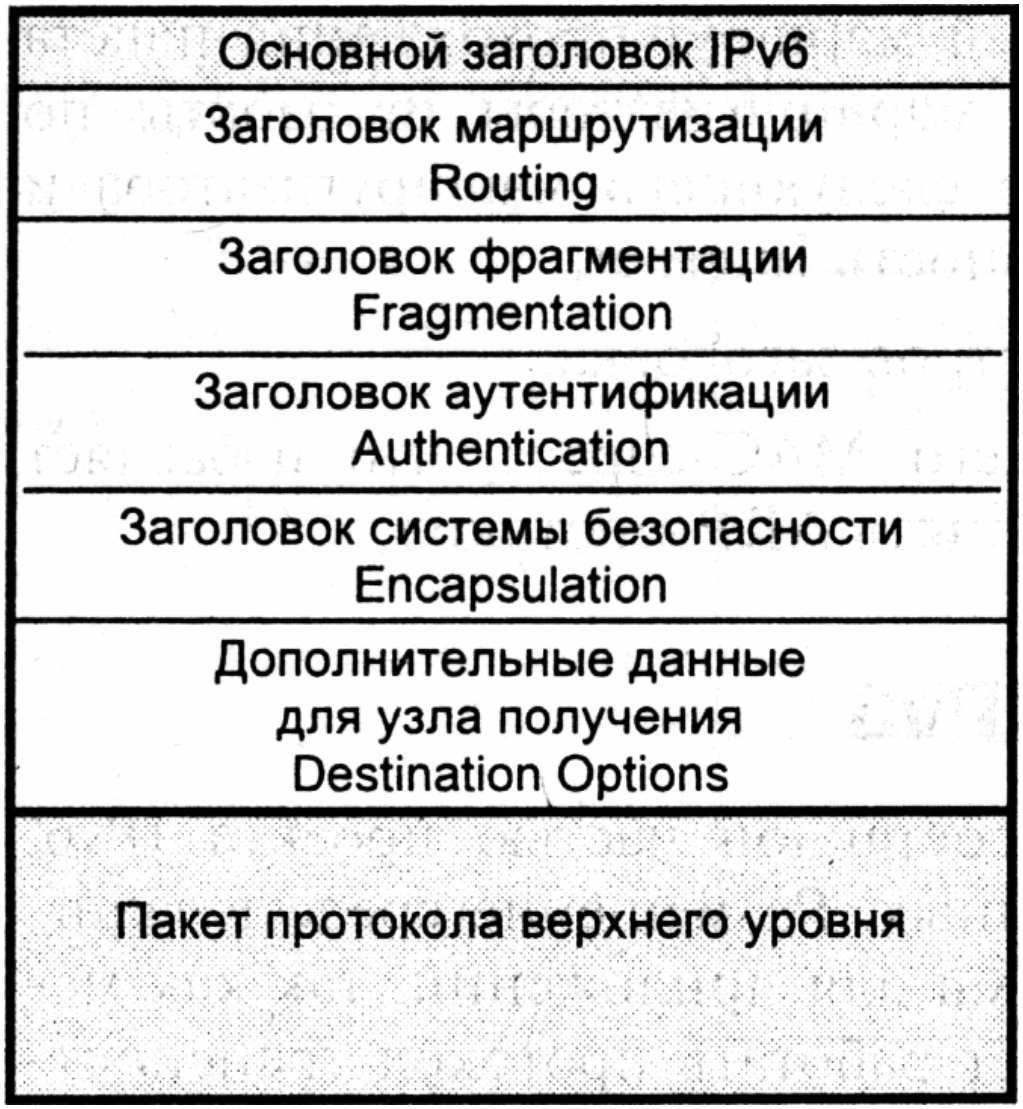
- создание масштабируемой схемы адресации;
- повышение пропускной способности за счет упрощения работы маршрутизаторов;
- предоставление гарантий QoS;
- обеспечение защиты данных.

Адрес IPv6

- длина – 16 байт;
- запись в 16-ричной системе, либо в режиме совместимости с – смешанная 16-ричная и 10-тичная:
  - FEDC:0A98:0:0:0:0:7654:3210
  - 0:0:0:0:FFFF:62.76.175.200
- Типы адресов (задается полем префикса формата - FP):
  - unicast
  - multicast
  - anycast

3	13	8	24	16	64
Префикс формата (FP)	Агрегирование верхнего уровня (TLA)		Агрегирование следующего уровня (NLA)	Агрегирование местного уровня (SLA)	Идентификатор интерфейса (Interface ID)

Структура пакета IPv6



Защита данных на 2 уровне

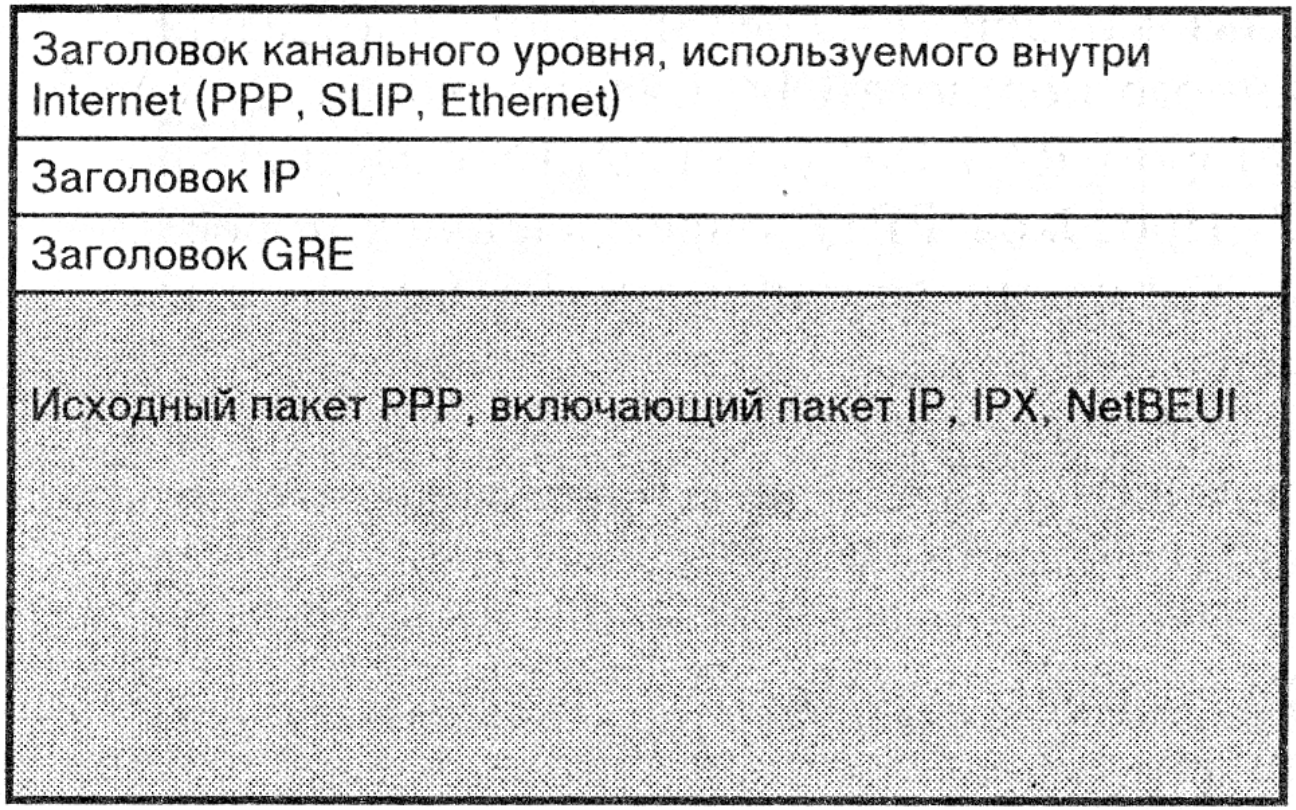
- PPTP - Point-to-Point Tunneling Protocol
  - Microsoft, 3COM, US Robotics
- L2F - Layer 2 Forwarding
  - Cisco Systems
- L2TP – Layer 2 Tunneling Protocol
  - PPP Extensions IETF

Point-to-Point Tunneling Protocol

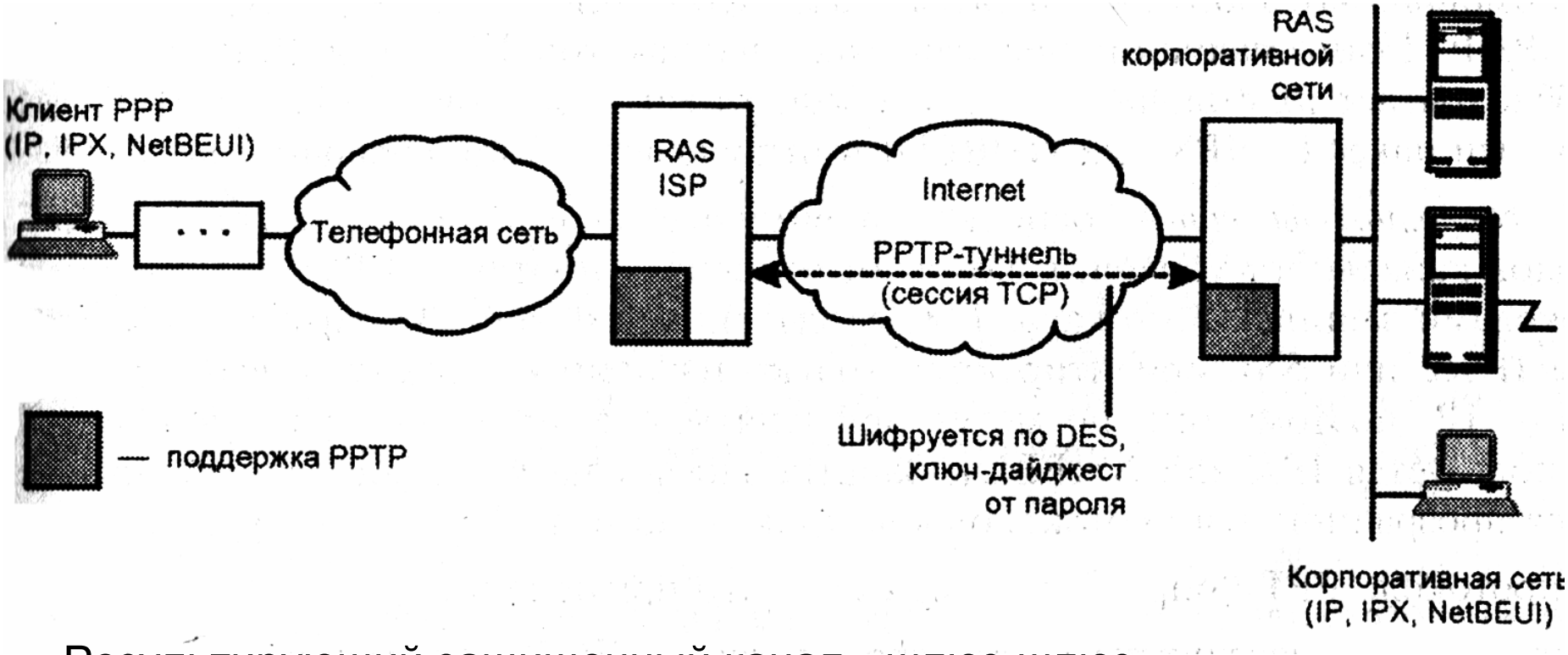
- Инкапсулирующий протокол 2 уровня
- Позволяет создавать защищенные каналы для работы по протоколам IP, IPX, NetBEUI (алгоритмы DES, RC-4)
- Существует две схемы применения:
  - RAS ISP – пограничный маршрутизатор КИС
  - пользователь – маршрутизатор КИС

Структура пакета PPTP

пакеты пользователя (IP, IPX, и т.п.) инкапсулируются в пакеты IP с помощью заголовка Generic Routing Encapsulation (GRE)



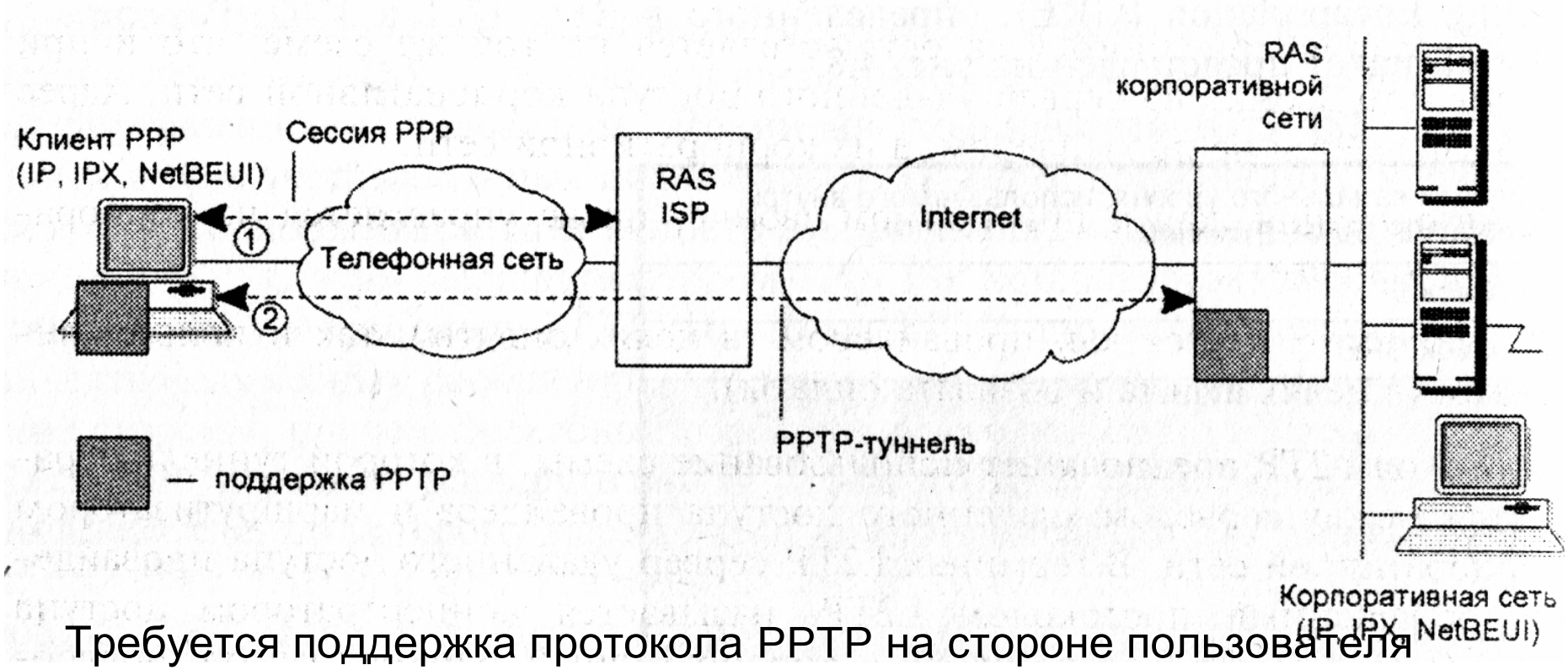
RAS ISP – пограничный маршрутизатор КИС



Результирующий защищенный канал - шлюз-шлюз

- Пользователь связывается с ISP и проходит аутентификацию
- По имени пользователя RAS ISP находит PPTP шлюз КС
- Шлюз PPTP аутентифицирует пользователя по CHAP или PAP

пользователь – маршрутизатор КИС



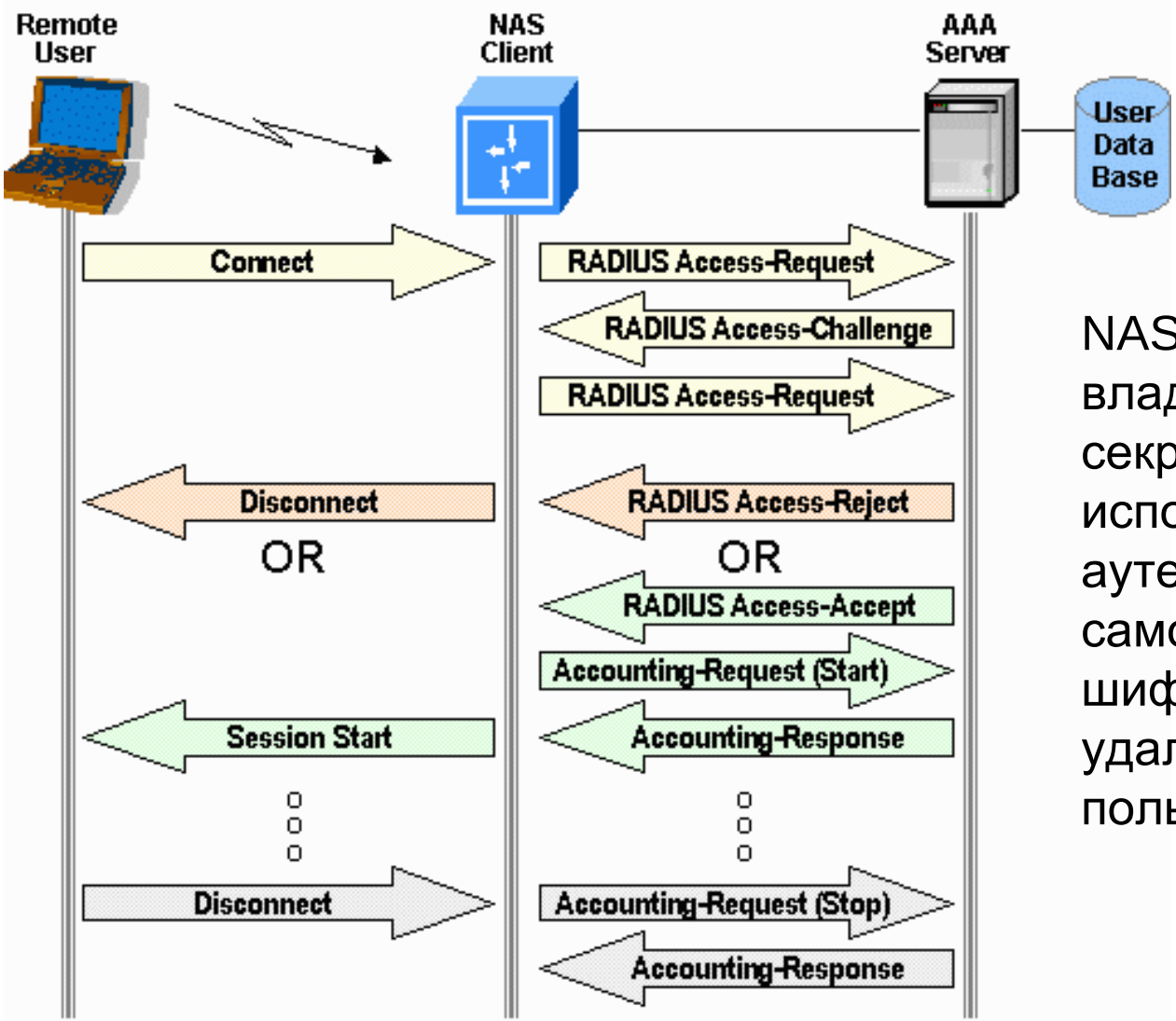
Требуется поддержка протокола PPTP на стороне пользователя

- Пользователь связывается с ISP по протоколу PPP и проходит у ISP аутентификацию по протоколу PAP, CHAP или в диалоге.
- Пользователь устанавливает соединение по протоколу PPTP и вторично аутентифицируется, теперь на сервере КС.

Элементы технологии IEEE802.1X

- Удаленный пользователь/клиент, например, компьютер с радиоинтерфейсом.
- Сервер доступа (NAS - Network Access Server), например, точка доступа IEEE802.11. По отношению к AAA – клиент.
- Сервер централизованной аутентификации (Authentication Server), или сервер AAA - authentication, authorization, and access control).
- RADIUS-служба (Remote Authentication Dial In User Service).

Инфраструктура RADIUS



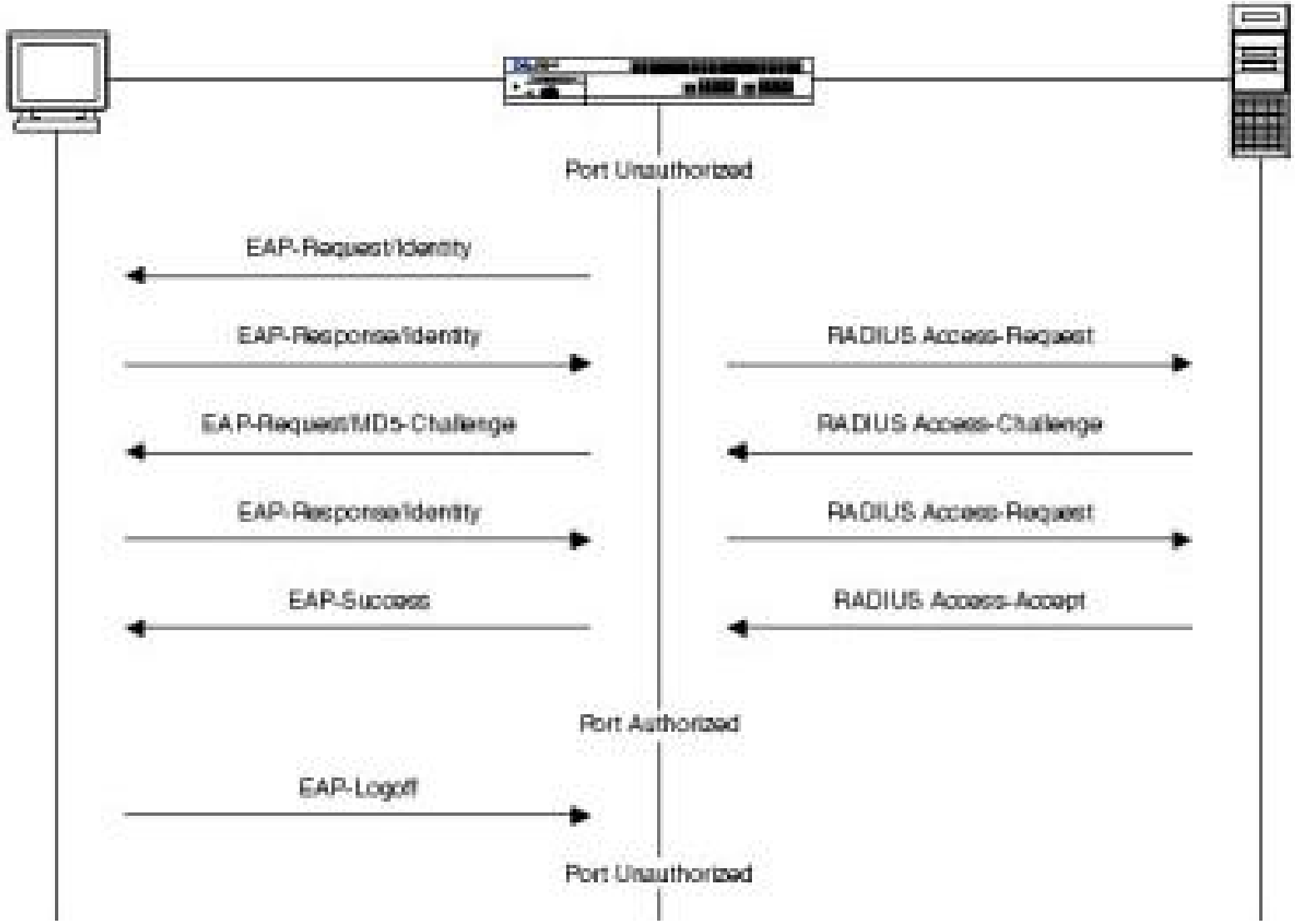
NAS и AAA-сервер владеют общим секретным ключом, использующимся для аутентификации самой NAS и шифрации запроса от удаленного пользователя.

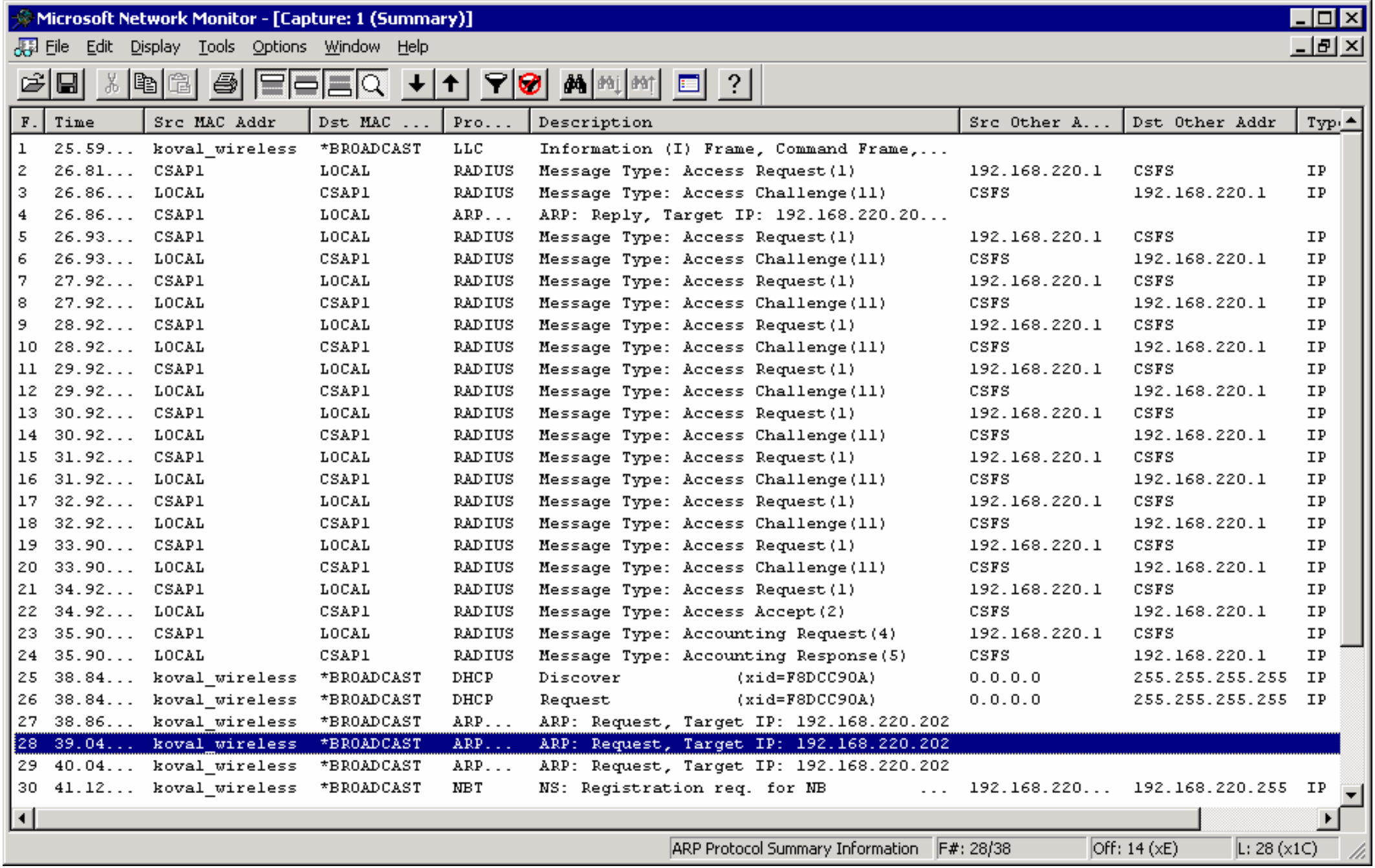
Последовательность аутентификации IEEE802.1x в сетях IEEE802.11

1. Клиент посылает сообщение точке доступа EAP-Start
2. Точка запрашивает имя клиента и включает его в в запрос для AAA-сервера «Access-Request» в виде значения атрибута «User-Name»
3. Клиент и AAA-сервер обмениваются через точку доступа сообщениями RADIUS-протокола «Access-Challenge» и «Access-Request». В зависимости от выбранного типа EAP, сообщения могут передаваться и в зашифрованном виде по TLS туннелю
4. Если AAA-сервер ответил сообщением «Access-Accept», клиент и точка генерируют сеансовые ключи TKIP или WEP. Затем точка разрешает использование порта клиентом для передачи данных.

Примечание: EAP - Extensible Authentication Protocol

Последовательность аутентификации IEEE802.1x





F.	Time	Src MAC Addr	Dst MAC ...	Pro...	Description	Src Other A...	Dst Other Addr	Typ
1	25.59...	koval_wireless	*BROADCAST	LLC	Information (I) Frame, Command Frame,...			
2	26.81...	CSAP1	LOCAL	RADIUS	Message Type: Access Request(1)	192.168.220.1	CSFS	IP
3	26.86...	LOCAL	CSAP1	RADIUS	Message Type: Access Challenge(11)	CSFS	192.168.220.1	IP
4	26.86...	CSAP1	LOCAL	ARP...	ARP: Reply, Target IP: 192.168.220.20...			
5	26.93...	CSAP1	LOCAL	RADIUS	Message Type: Access Request(1)	192.168.220.1	CSFS	IP
6	26.93...	LOCAL	CSAP1	RADIUS	Message Type: Access Challenge(11)	CSFS	192.168.220.1	IP
7	27.92...	CSAP1	LOCAL	RADIUS	Message Type: Access Request(1)	192.168.220.1	CSFS	IP
8	27.92...	LOCAL	CSAP1	RADIUS	Message Type: Access Challenge(11)	CSFS	192.168.220.1	IP
9	28.92...	CSAP1	LOCAL	RADIUS	Message Type: Access Request(1)	192.168.220.1	CSFS	IP
10	28.92...	LOCAL	CSAP1	RADIUS	Message Type: Access Challenge(11)	CSFS	192.168.220.1	IP
11	29.92...	CSAP1	LOCAL	RADIUS	Message Type: Access Request(1)	192.168.220.1	CSFS	IP
12	29.92...	LOCAL	CSAP1	RADIUS	Message Type: Access Challenge(11)	CSFS	192.168.220.1	IP
13	30.92...	CSAP1	LOCAL	RADIUS	Message Type: Access Request(1)	192.168.220.1	CSFS	IP
14	30.92...	LOCAL	CSAP1	RADIUS	Message Type: Access Challenge(11)	CSFS	192.168.220.1	IP
15	31.92...	CSAP1	LOCAL	RADIUS	Message Type: Access Request(1)	192.168.220.1	CSFS	IP
16	31.92...	LOCAL	CSAP1	RADIUS	Message Type: Access Challenge(11)	CSFS	192.168.220.1	IP
17	32.92...	CSAP1	LOCAL	RADIUS	Message Type: Access Request(1)	192.168.220.1	CSFS	IP
18	32.92...	LOCAL	CSAP1	RADIUS	Message Type: Access Challenge(11)	CSFS	192.168.220.1	IP
19	33.90...	CSAP1	LOCAL	RADIUS	Message Type: Access Request(1)	192.168.220.1	CSFS	IP
20	33.90...	LOCAL	CSAP1	RADIUS	Message Type: Access Challenge(11)	CSFS	192.168.220.1	IP
21	34.92...	CSAP1	LOCAL	RADIUS	Message Type: Access Request(1)	192.168.220.1	CSFS	IP
22	34.92...	LOCAL	CSAP1	RADIUS	Message Type: Access Accept(2)	CSFS	192.168.220.1	IP
23	35.90...	CSAP1	LOCAL	RADIUS	Message Type: Accounting Request(4)	192.168.220.1	CSFS	IP
24	35.90...	LOCAL	CSAP1	RADIUS	Message Type: Accounting Response(5)	CSFS	192.168.220.1	IP
25	38.84...	koval_wireless	*BROADCAST	DHCP	Discover (xid=F8DCC90A)	0.0.0.0	255.255.255.255	IP
26	38.84...	koval_wireless	*BROADCAST	DHCP	Request (xid=F8DCC90A)	0.0.0.0	255.255.255.255	IP
27	38.86...	koval_wireless	*BROADCAST	ARP...	ARP: Request, Target IP: 192.168.220.202			
28	39.04...	koval_wireless	*BROADCAST	ARP...	ARP: Request, Target IP: 192.168.220.202			
29	40.04...	koval_wireless	*BROADCAST	ARP...	ARP: Request, Target IP: 192.168.220.202			
30	41.12...	koval_wireless	*BROADCAST	NBT	NS: Registration req. for NB ...	192.168.220...	192.168.220.255	IP

Терминология и типы EAP

- Технология IEEE802.1X использует EAP (Extensible Authentication Protocol) для взаимодействия:
  - клиентов-станций (supplicants),
  - точек доступа (authenticators),
  - серверов RADIUS (authentication servers).
- Используются следующие типы EAP:
  - Cisco's Lightweight EAP (LEAP)
  - EAP with Transport Layer Security (EAP-TLS)
  - EAP with Tunneled TLS (EAP-TTLS)
  - Protected EAP (PEAP)

Сводная таблица типов EAP

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
аутентификация сервера	нет	хэш пароля	открытый ключ (сертификат)	открытый ключ (сертификат)	открытый ключ (сертификат)
аутентификация клиента	хэш пароля	хэш пароля	открытый ключ (сертификат или смарт-карта)	CHAP, PAP, MS-CHAP(v2), EAP	Любой EAP, напр. EAP-MS-CHAPv2, открытый ключ
динамический ключ, доставка	нет	да	да	да	да
угрозы безопасности	Identity видна, возможны атаки: по словарю, Man-in-the-Middle (MM), перехват сеанса	Identity видна, атака по словарю	Identity видна	атака на пользовательские реквизиты	Identity не видна в фазе 2, но потенциально доступна в фазе 1; аналогично TTLS

Защита на сетевом уровне

- IPSec (Internet Protocol Security) RFC 2401 «Security Architecture for the IP»)

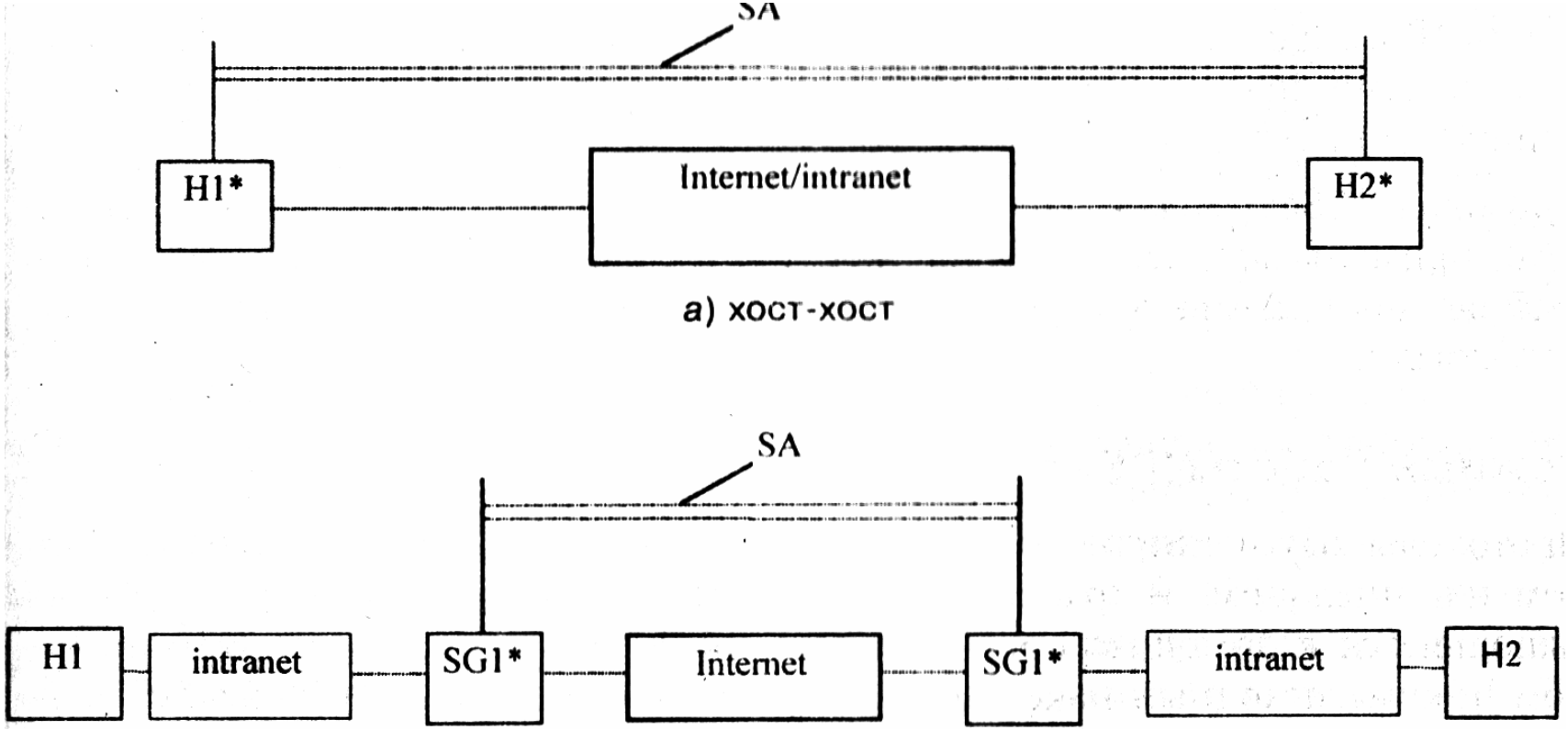
  Используются протоколы 3-х типов:

  - AH –Authentication Header
    - целостность данных и аутентификация источника
  - ESP – Encapsulation Security Payload
    - шифрование, аутентификацию и целостность
  - IKE – Internet Key Exchange
    - Security Association (SA)
    - инициализация защищенного канала
    - процедуры обмена и управления секретными ключами

Взаимодействие AH, ESP, IKE

- IKE инициализирует защищенный двухточечный канал – SA
  - аутентификация конечных точек
  - устанавливаются параметры защиты (алгоритм шифрования, сессионный ключ)
- В рамках SA начинает работу AH или ESP
- Существование 2-х протоколов AH ESP вызвано ограничением на экспорт средств шифрования

Установка SA

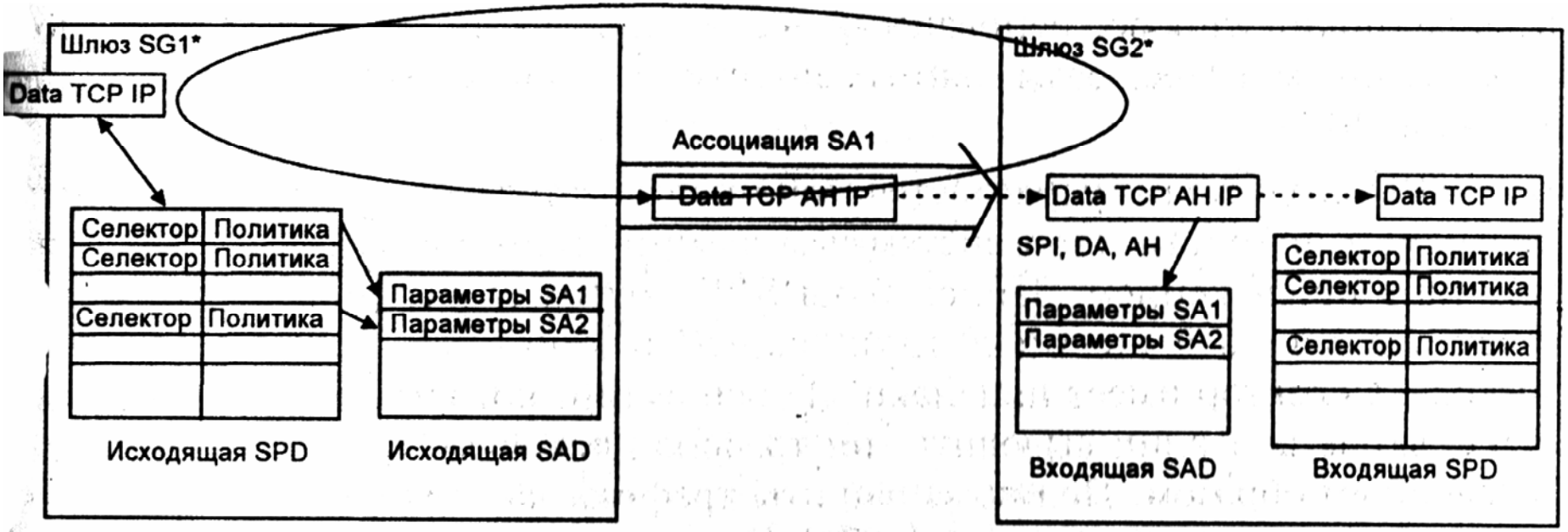


а) хост-хост

AH, ESP работают в 2-х режимах: транспортном (шифруется только поле данных, заголовок остается) и туннельном, причем AS –симплексное соединение.

Выбор режима зависит от выбора схемы: H1-H2 (см. рис а), или SG1-SG2 (см. рис б).

База данных политик безопасности



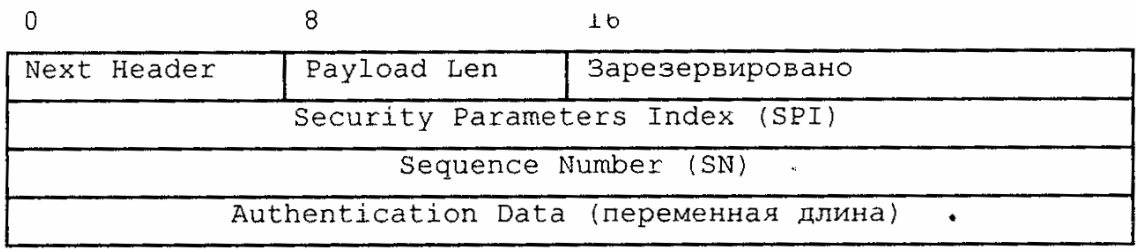
каждый узел/шлюз использует Security Policy Database (SPD)?

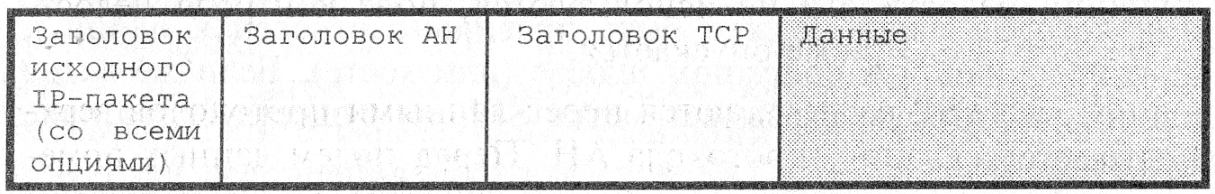
SPD создается локально, имеет 2 типа полей:

селектор пакета: IPv4,v6 адреса источника и назначения (маска); имя пользователя в формате DNS (user@cs.vsu.ru) или X.500; имя системы в формате DNS (srv3.cs.vsu.ru) или X.500; транспорт TCP или UDP, порт источника и порт назначения

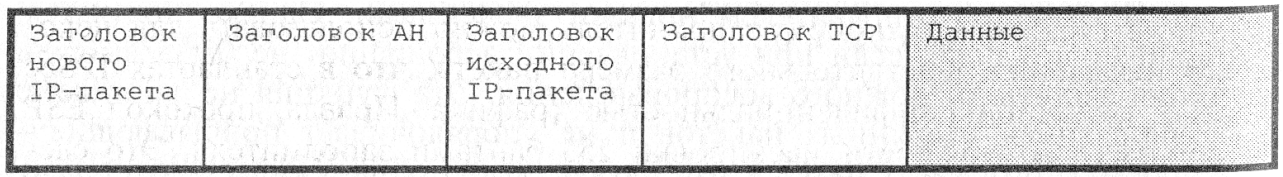
политика защиты пакета: пропустить, обработать, отвергнуть

Защита данных с помощью AH



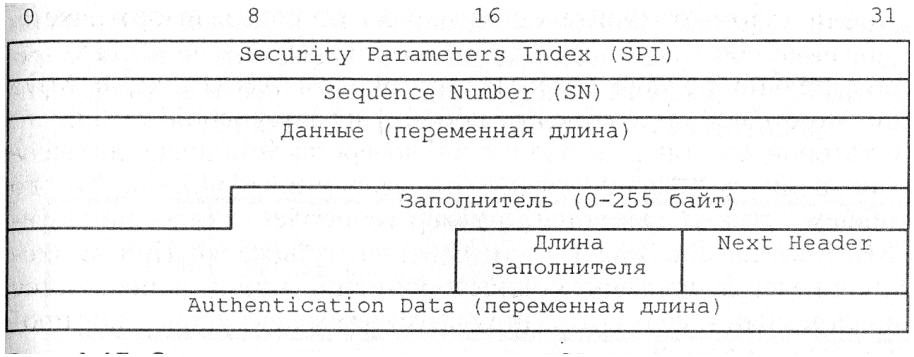


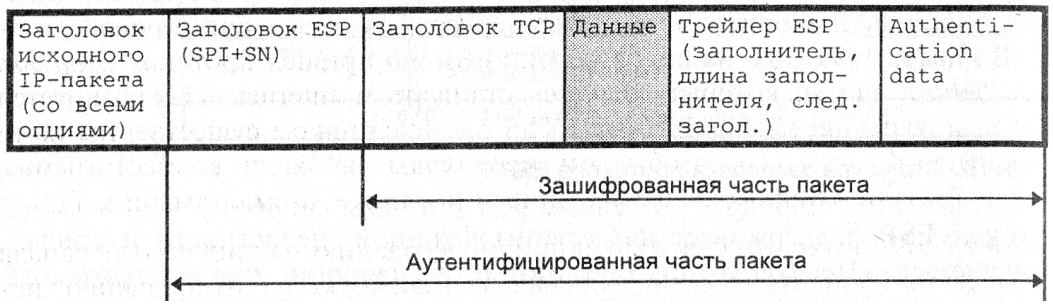
Аутентифицированная часть пакета (за исключением изменяющихся полей)

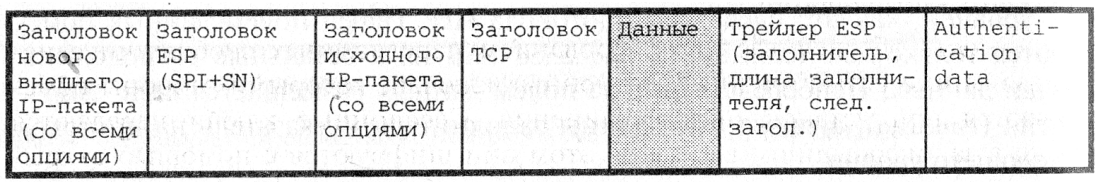


Аутентифицированная часть пакета (за исключением изменяющихся полей)

Защита данных с помощью ESP





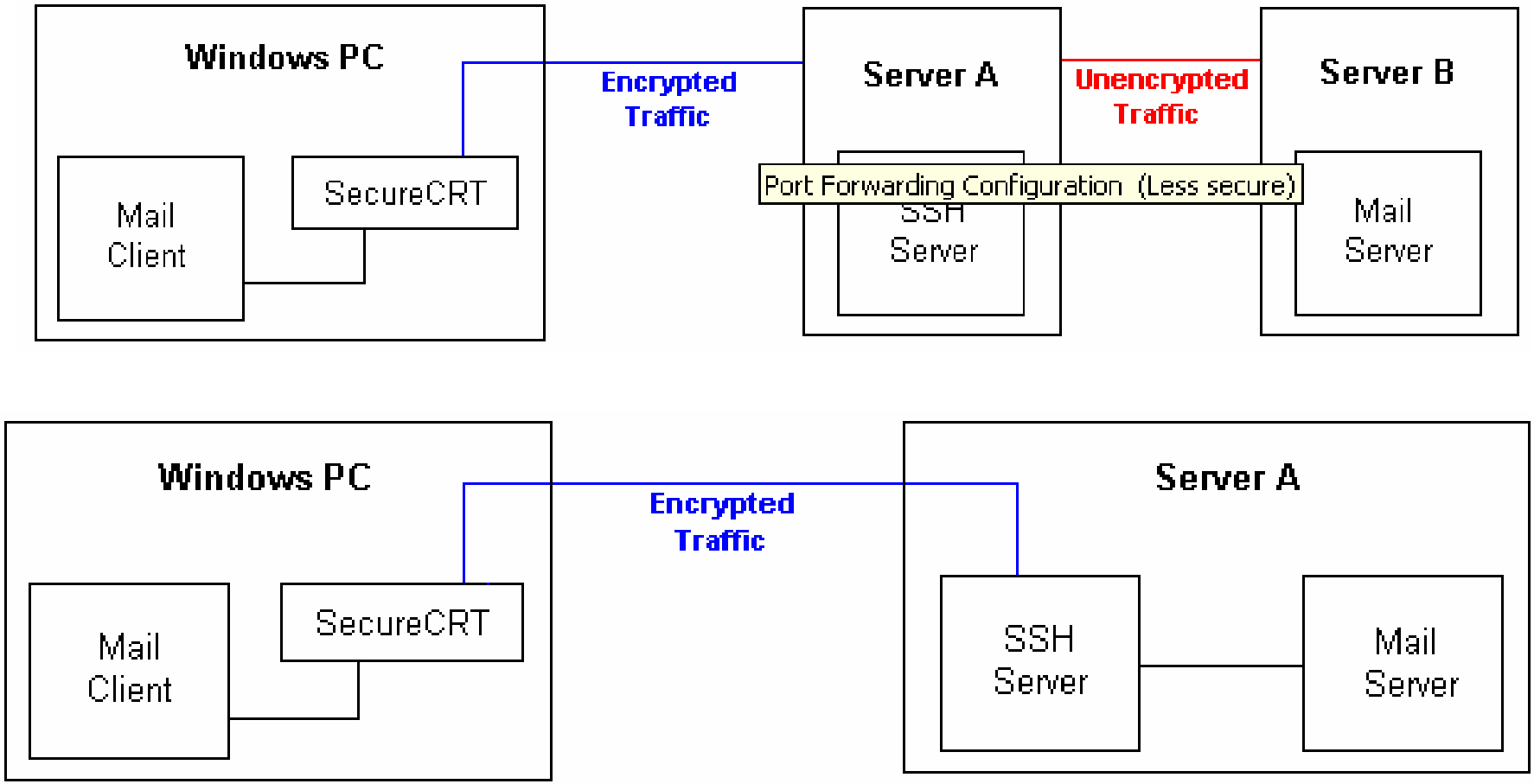


Защита на уровне представления

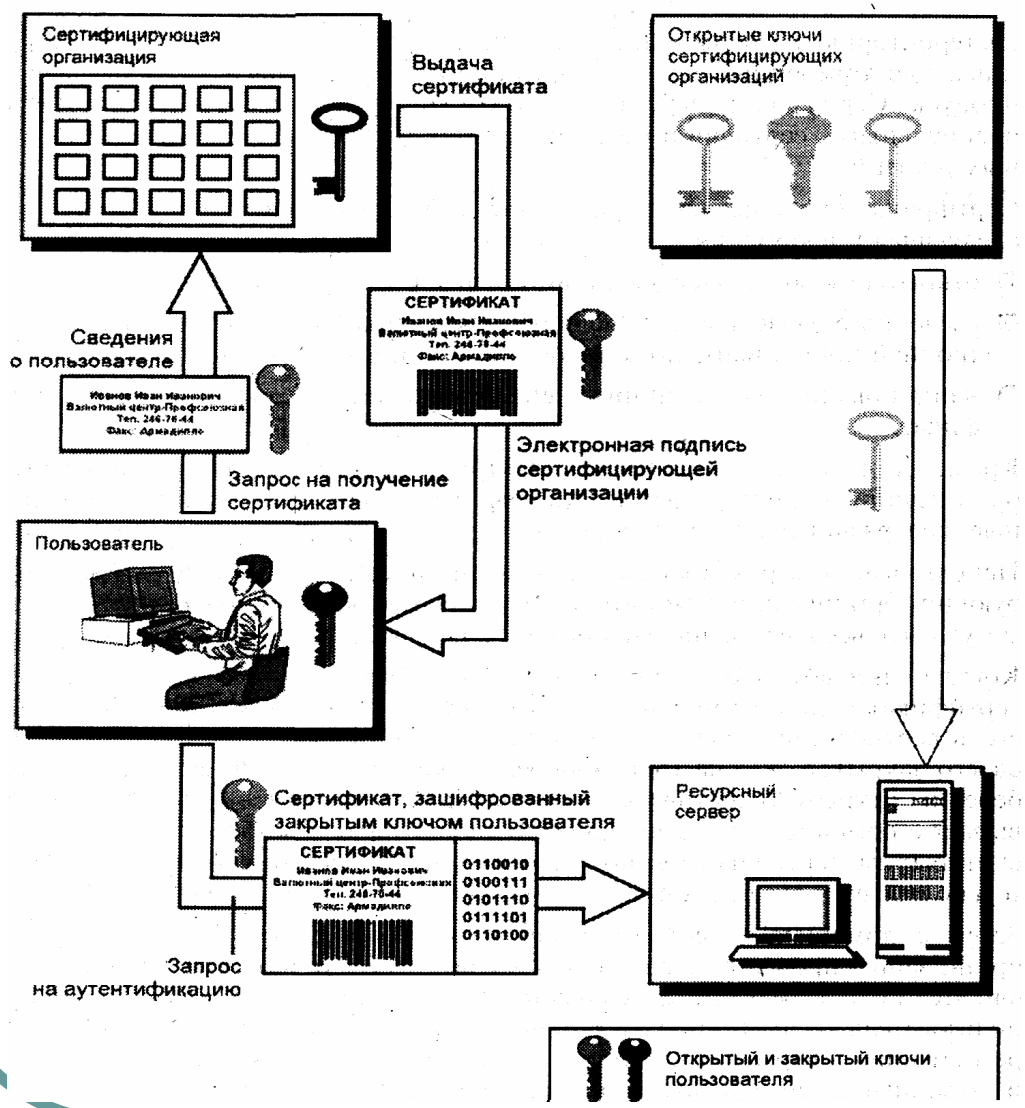
- Secure Socket Layer SSL (разработка фирмы Netscape)
- Transport Layer Security TLS (разработка комитета IETF)

PKI (Public Key Infrastructure) – инфраструктура открытых ключей

Secure Shell Protocol



Сертификационная аутентификация пользователей



Сертификат состоит из:

- открытого ключа
- информации о владельце
- одной и более подписей

Требуется PKI (Public Key Infrastructure) – инфраструктура открытых ключей

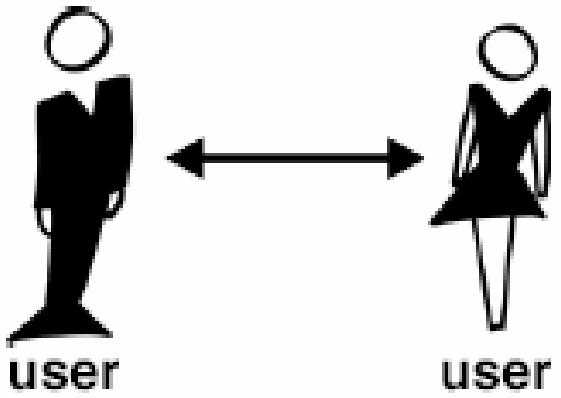
X.509v3 – стандарт ITU-T на формат сертификатов

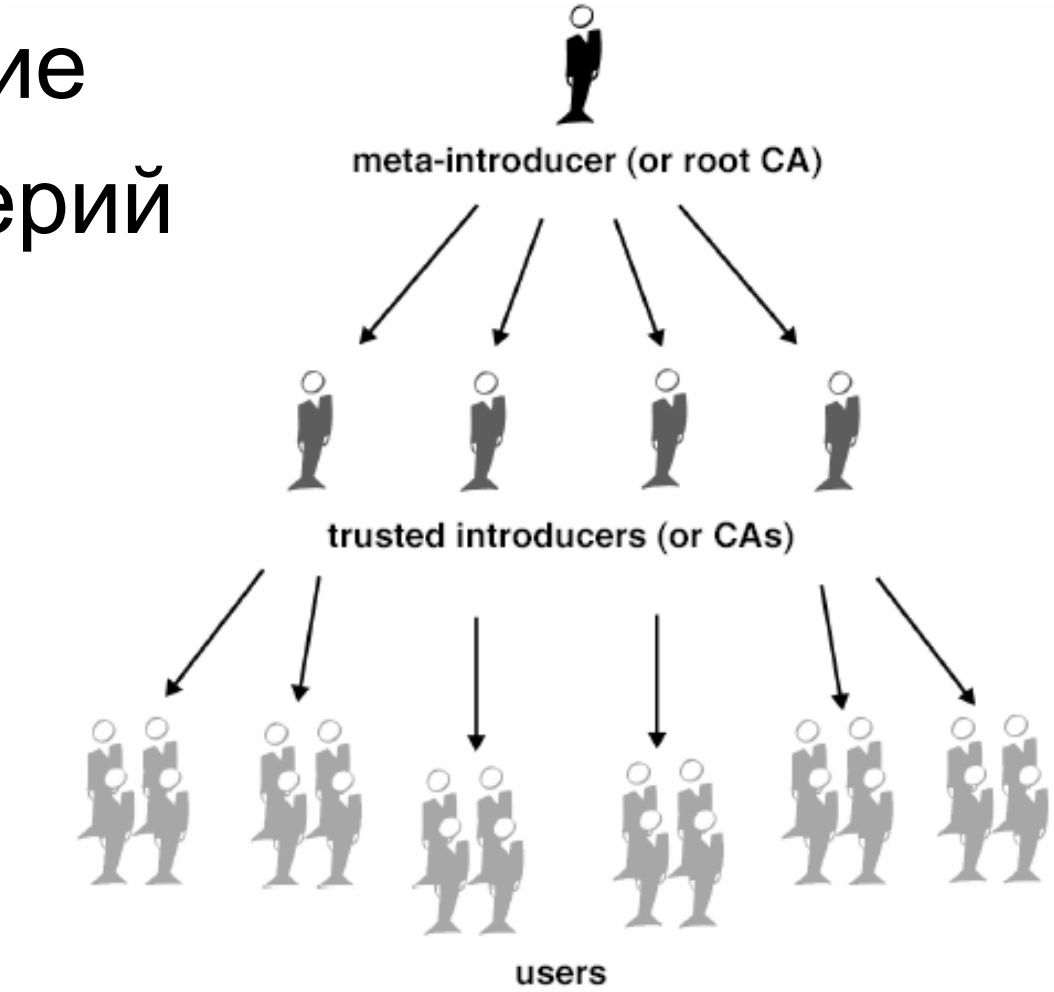
Инфраструктура открытых ключей

- При использовании сертификационной схемы аутентификации пользователей, очень важно быть уверенным в принадлежности открытых ключей.
- Эта проблема решается назначением центра доверия - Certification Authority (CA) и центра регистрации Registration Authority (RA), аналогично паспортному отделу (RA) и подразделениям печати и выдачи паспортов (CA).
- В PKI реалиуются функции хранения и управления открытыми ключами: выпуск, отзыв, подписывание.

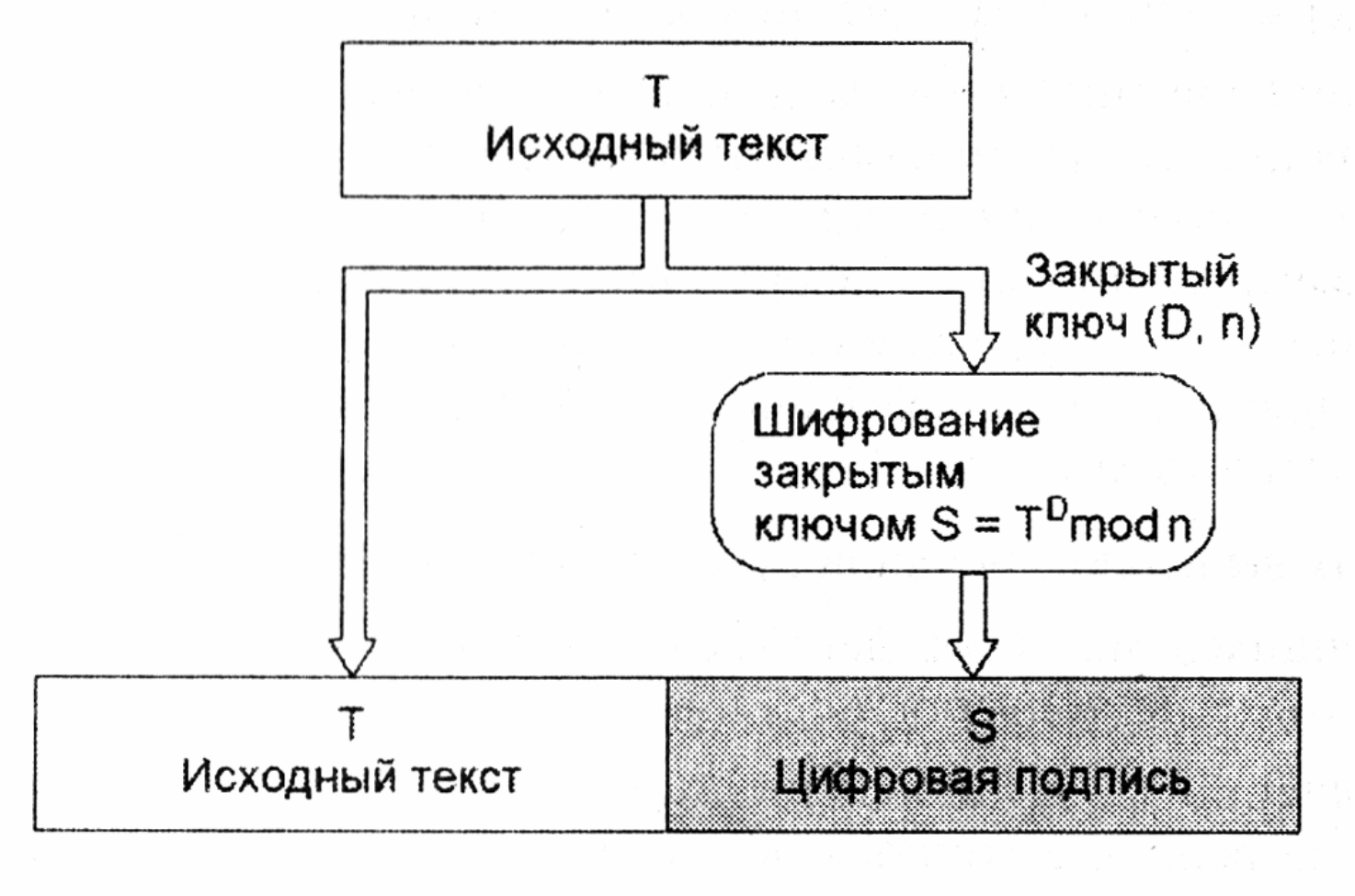
Модели доверия

- Прямое доверие
- Иерархия доверий
- Сеть доверий

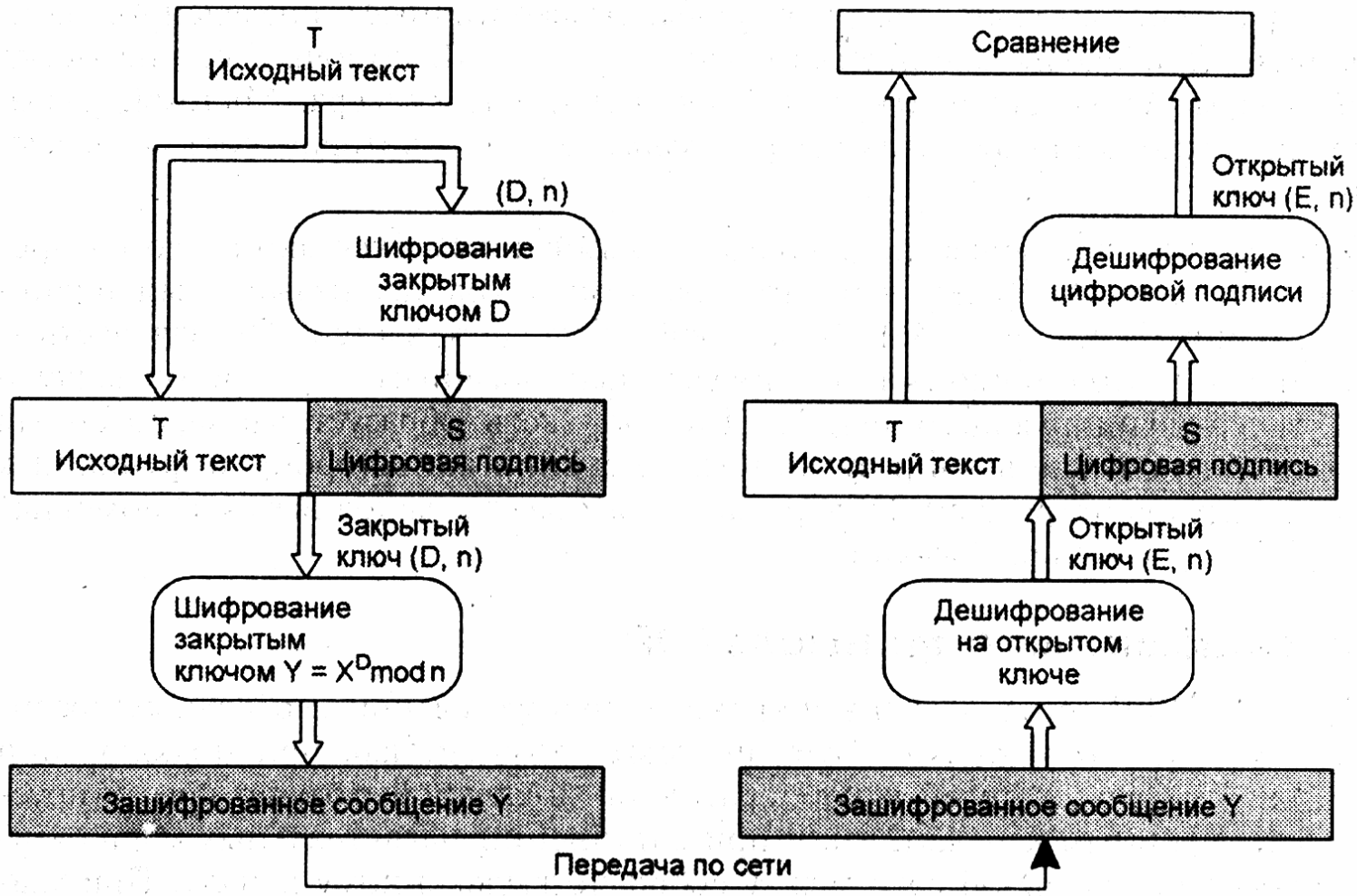




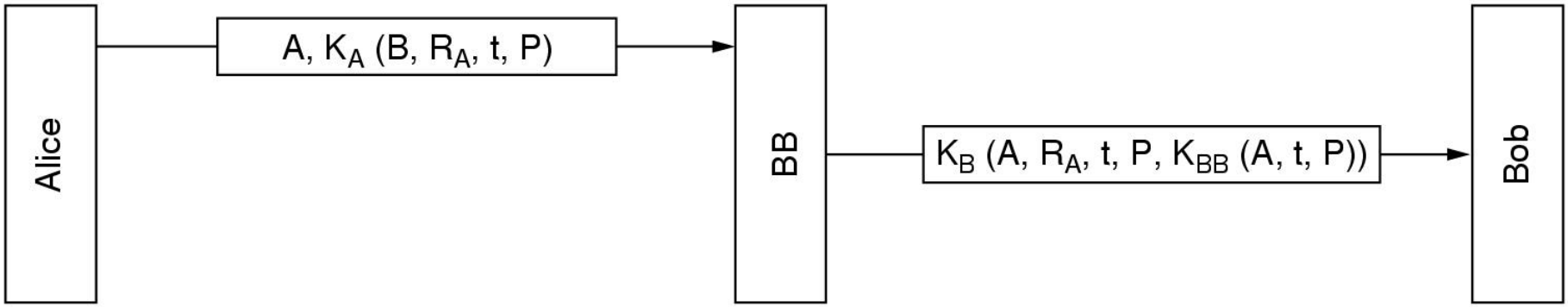
Цифровая подпись по RSA



Обеспечение конфиденциальности документов

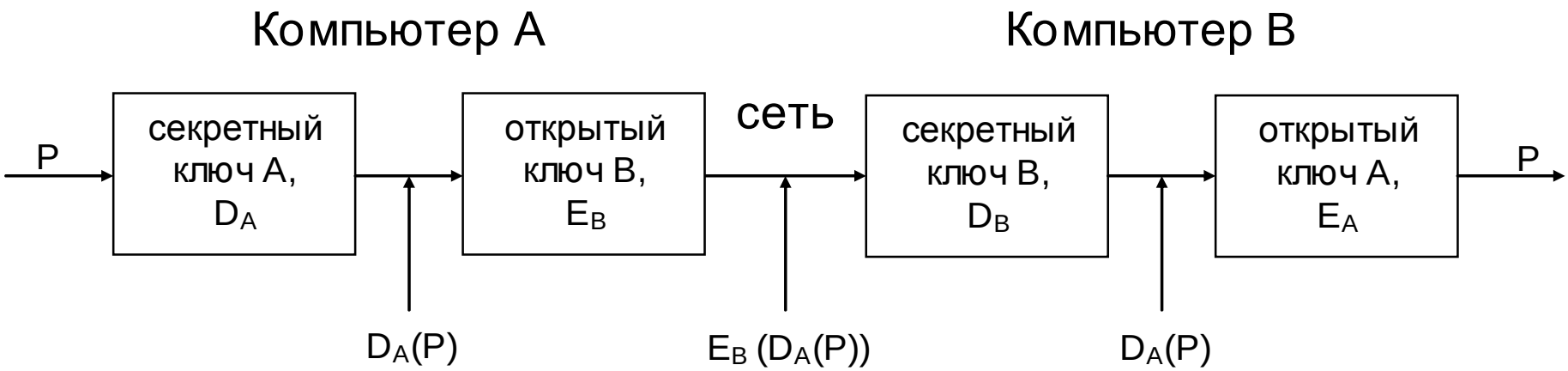


Подписи на основе секретного ключа



Примечание: BB – центр безусловного доверия

Подписи с использованием криптографии на основе открытых ключей



- Любой алгоритм на основе открытых ключей может быть использован для подписи
- Стандарт de facto - RSA
- Существует стандарт – Digital Signature Standard (США), 1991 на основе алгоритма Эль Гамаля. Критика:
  - Алгоритм Эль Гамаля довольно новый, недостаточно проверен
  - На порядок медленнее RSA (в 10 – 50 раз, в зависимости от реализации)
  - В стандарте определен небольшой 512-битный ключ

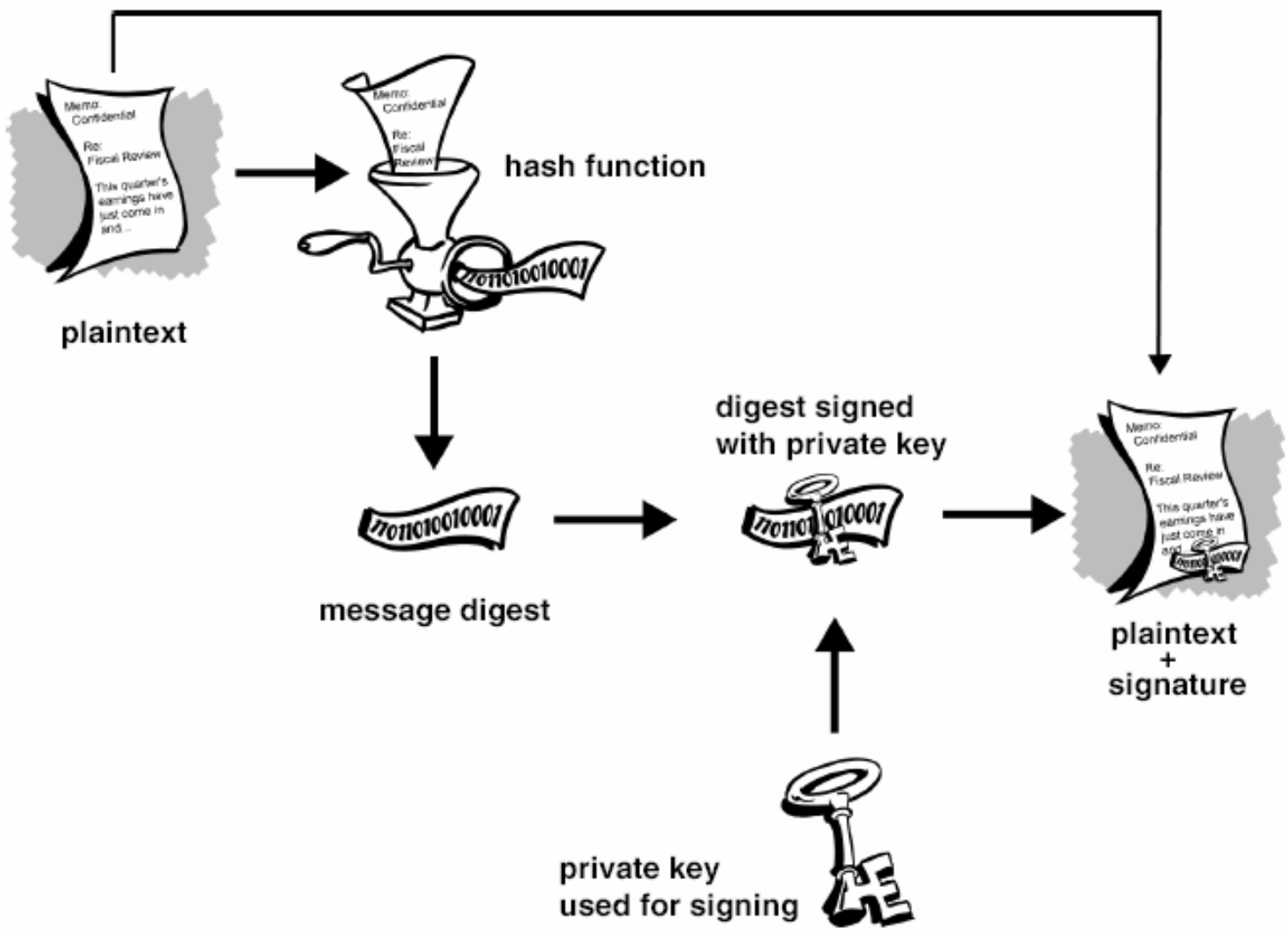
Вычисление дайджестов

•SHA-1 (Secure Hash Algorithm) - современный алгоритм вычисления дайджеста сообщения. Разработан National Security Agency (NSA) для института стандартов США - National Institute of Standards and Technology (NIST).

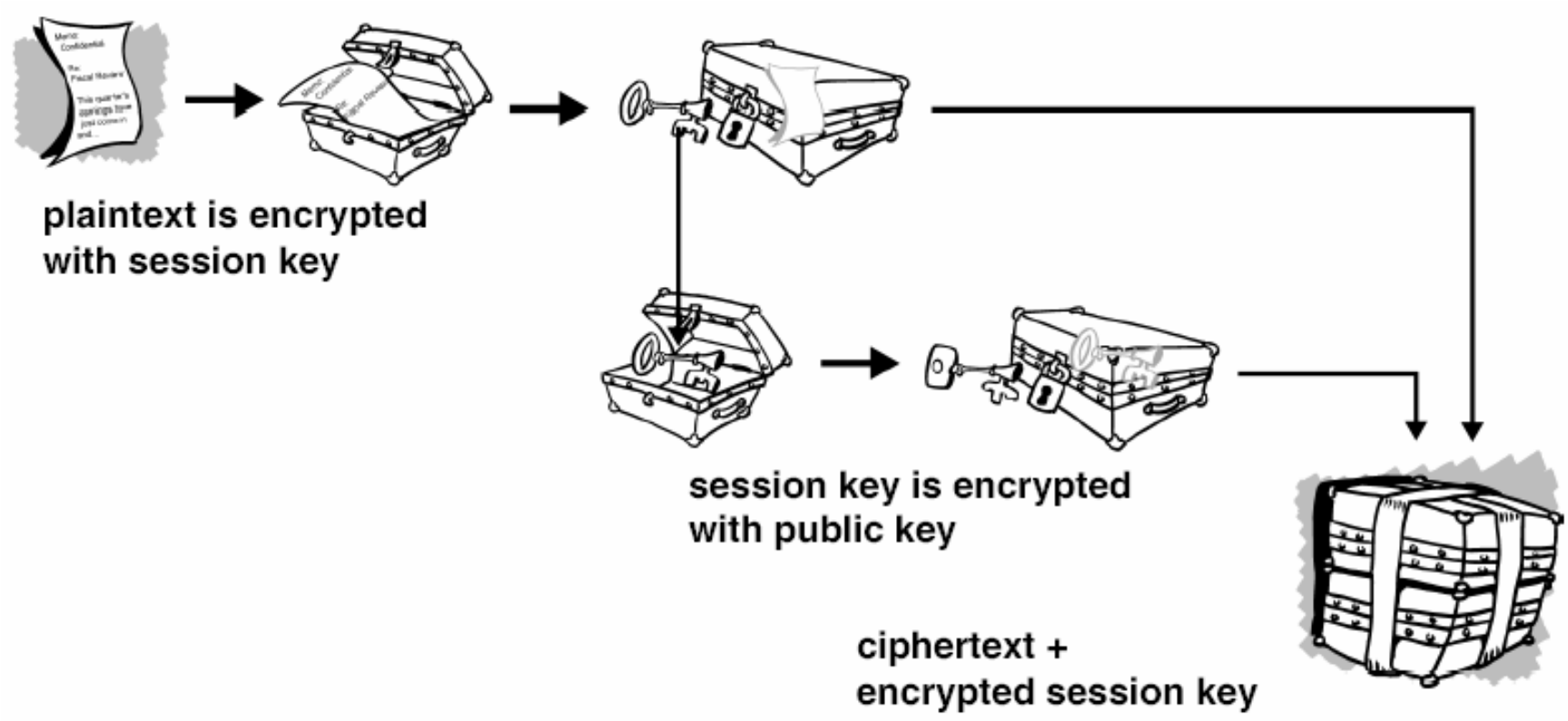
- •Используется в составе федерального стандарта США - DSS
- •Заменил MD5, уязвимость которого была обнаружена в 1996 году.

•MD2, MD4, MD5 (Message Digest) - хэш-функции для вычисления 128-битного дайджеста сообщения.

Подпись документа в PGP



Шифрация документа в PGP



Дешифрация документа в PGP