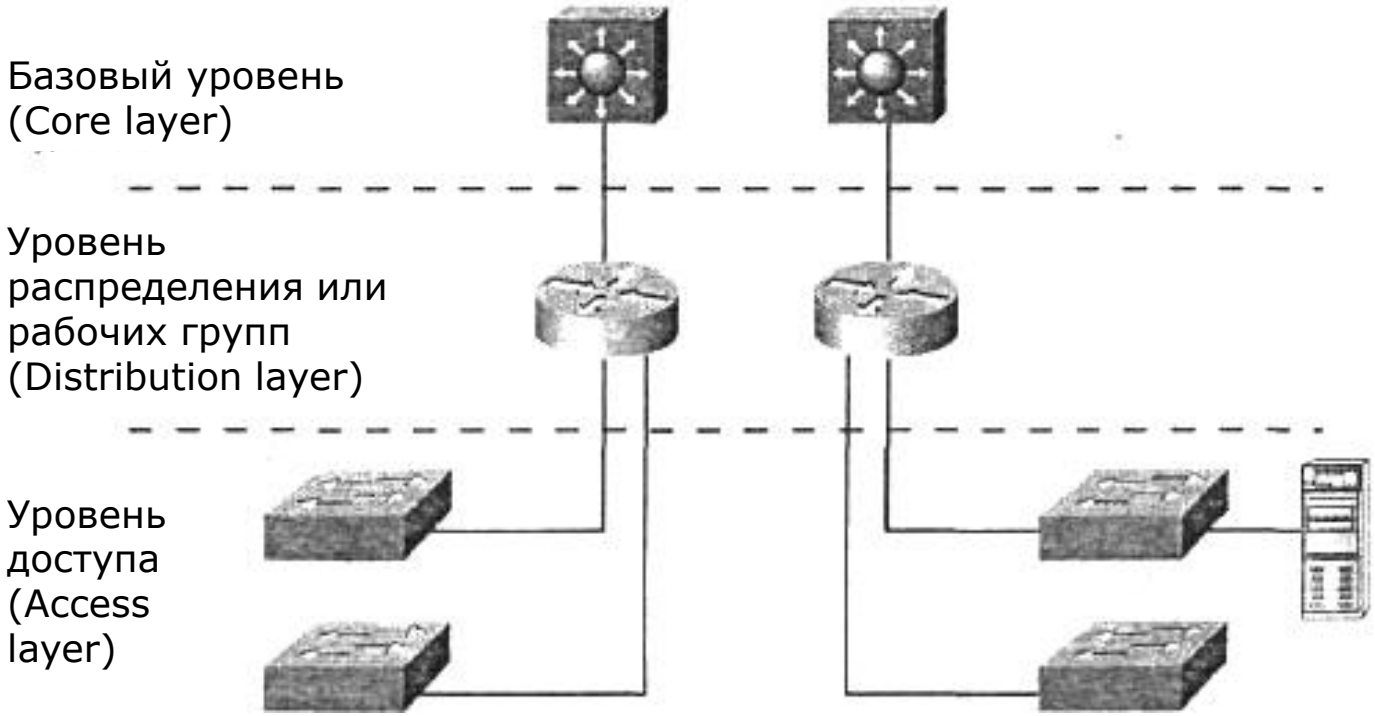
Иерархическая модель CISCO



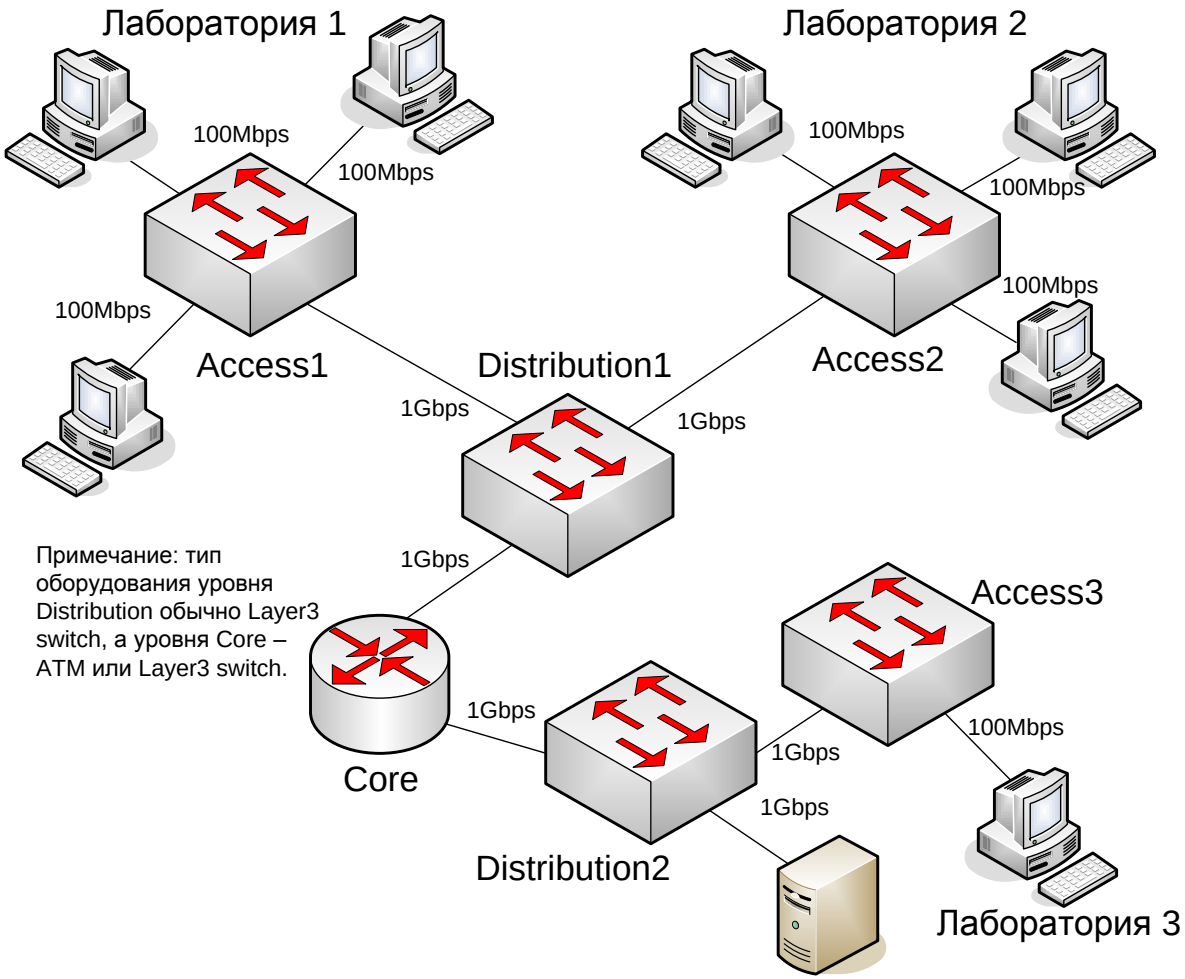
Функции уровней: базового, распределения, доступа

- Быстрая коммутация трафика

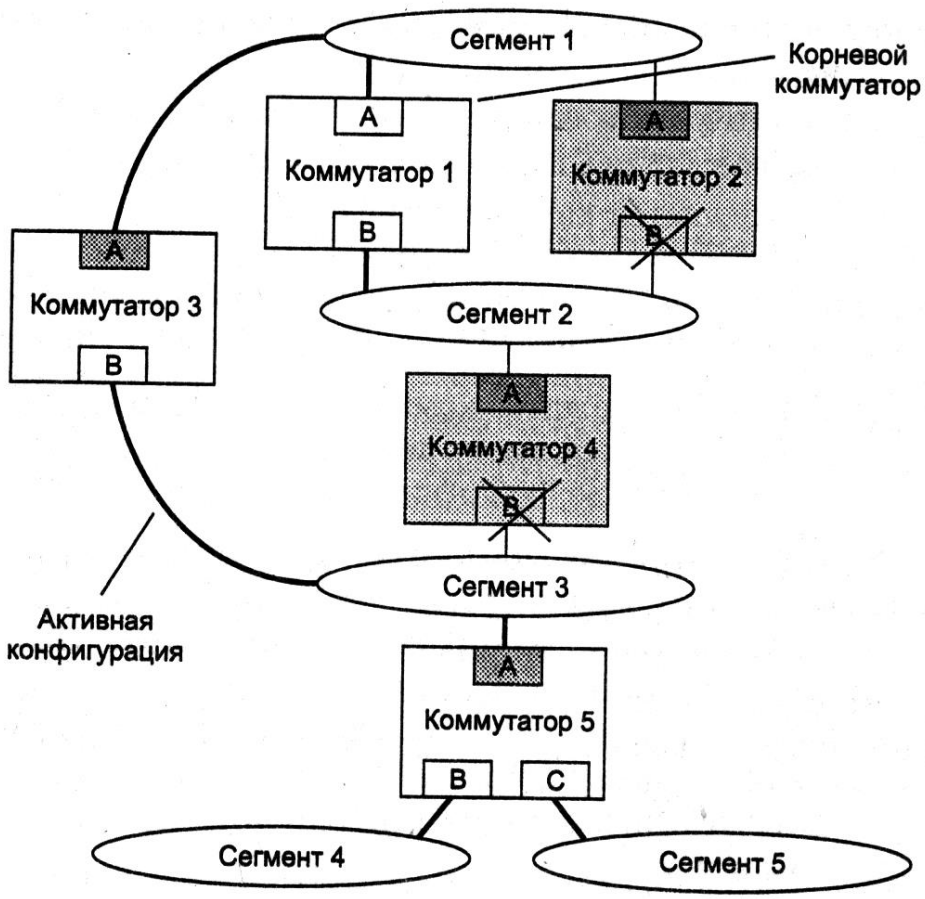
- Реализация инструментов, подобных спискам доступа, фильтрации пакетов или механизму запросов.
- Реализация системы безопасности и сетевых политик, включая трансляцию адресов и установку брандмауэров.
- Перераспределение между протоколами маршрутизации, включая использование статических путей.
- Маршрутизация между сетями VLAN и другие функции поддержки рабочих групп.
- Определение доменов широковещательных и многоадресных рассылок.

- Постоянный контроль (из уровня распределения) за доступом и политиками
- Формирование независимых доменов конфликтов/коллизий (сегментация)
- Соединение рабочих групп с уровнем распределения

Иерархическая модель CISCO



Spanning Tree Algorithm/Protocol, IEEE802.1D



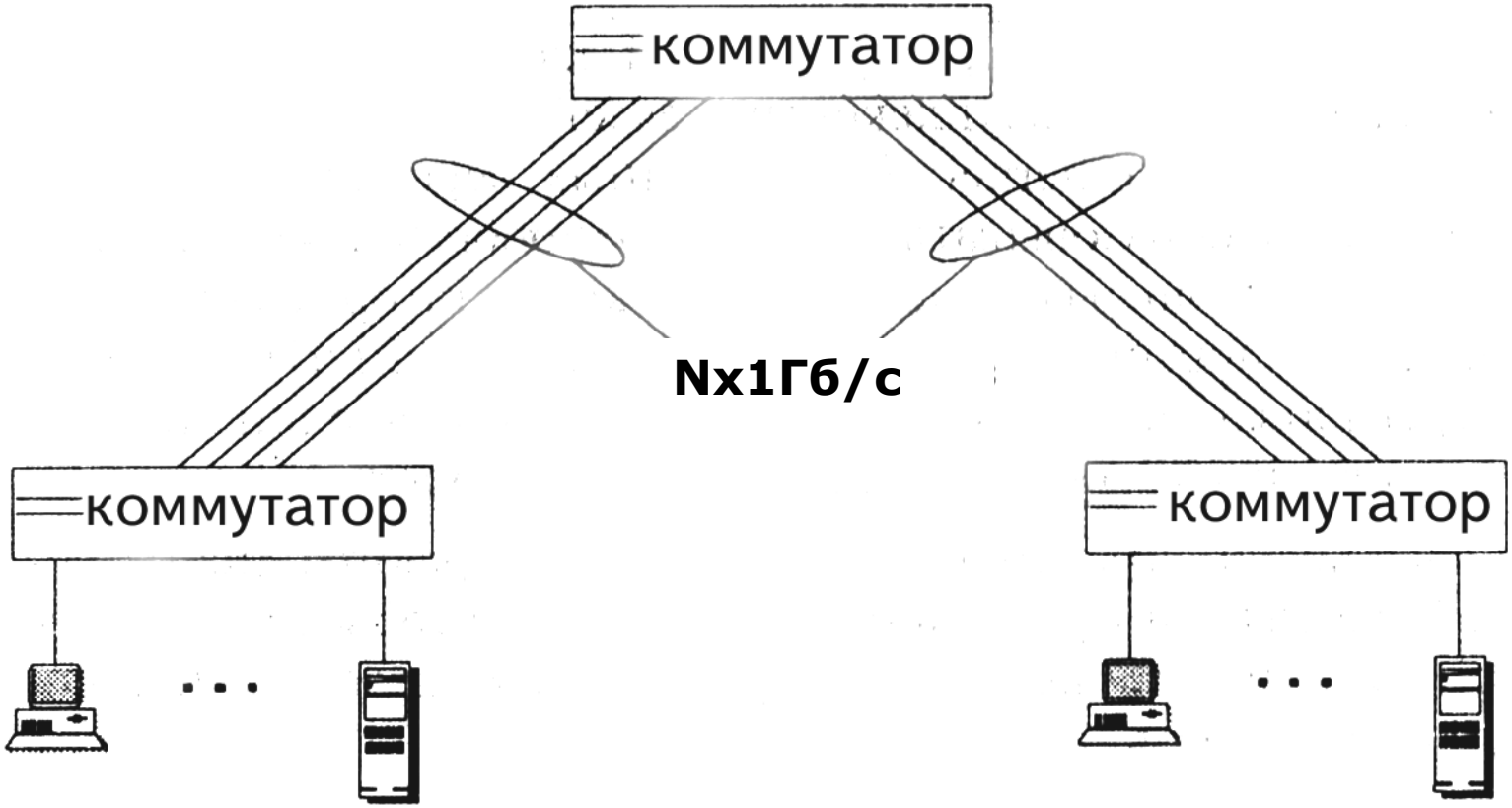
Корневой коммутатор (в начальным момент каждый) передает BPDU (Bridge Protocol Data Unit) сообщения по которым происходит:

•определение корневого коммутатора «root switch» автоматически (мин. MAC-адрес) или администратором

•определение корневого порта «root port» для каждого коммутатора (мин. расстояние до root)

•определение назначенного порта для каждого сегмента «designated port» (мин. расстояние до root)

Агрегирование каналов, trunking

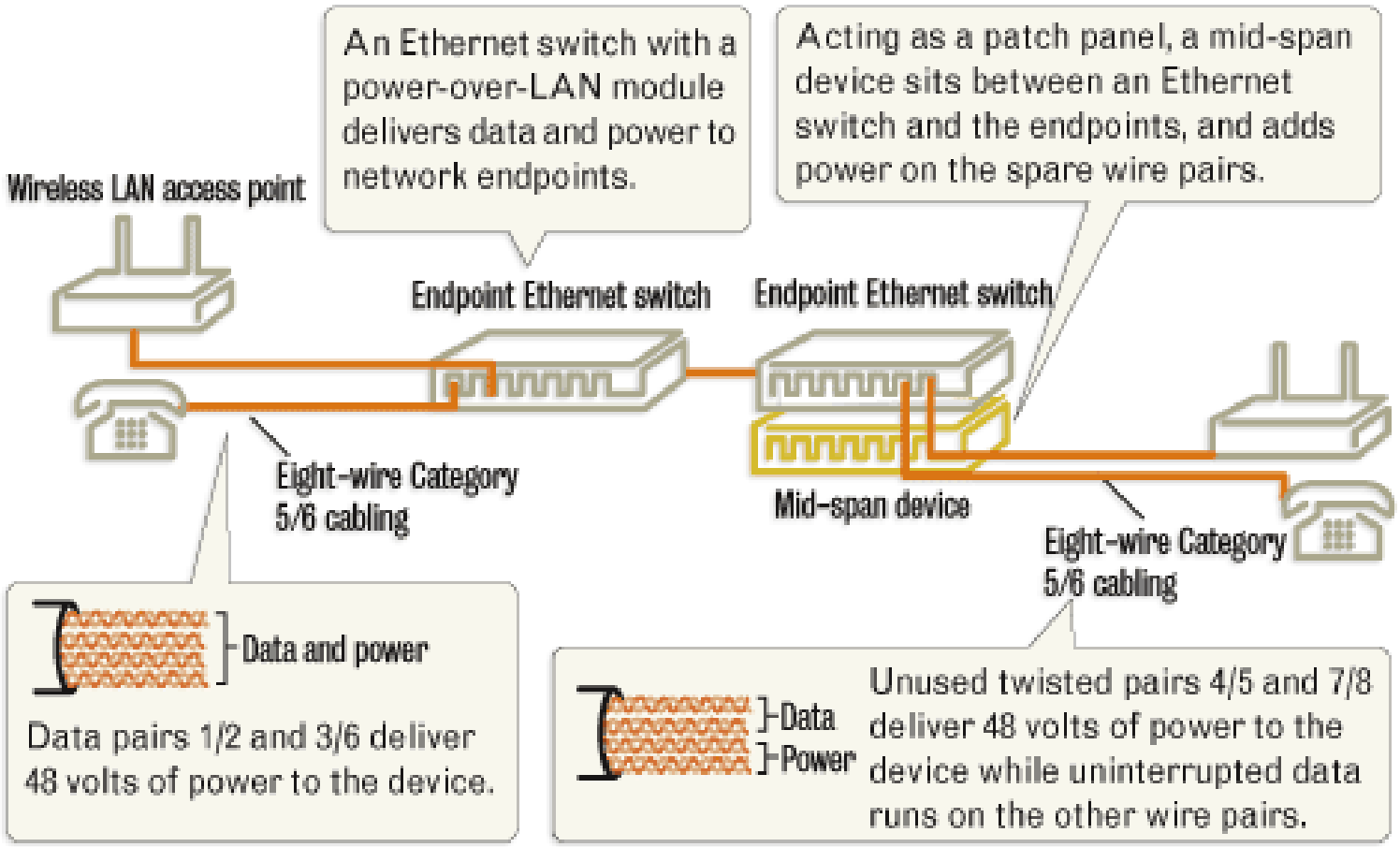


IEEE 802.3ad, Link Aggregation Control Protocol (LACP) позволяет создавать и динамический транк на оборудовании разных производителей

Стандарт 802.3af (питание через Ethernet, Power over Ethernet PoE)

- Два способа инжекции питания:
  - с оконечного оборудования (endspan)
  - с промежуточного (midspan)
  - питание подается после процедуры запроса
- Питание подается через UTP5, 5e, 6 по:
  - сигнальным линиям (10/100/1000Base-T, mode A)
  - неиспользуемым линиям (10/100 Base-T , mode B)
  - 48В постоянный ток, мощность 15.4 Вт
  - стадии питания: детектирование, клас-я, питание
  - развитие – стандарт IEEE 802.3at (PoE+)

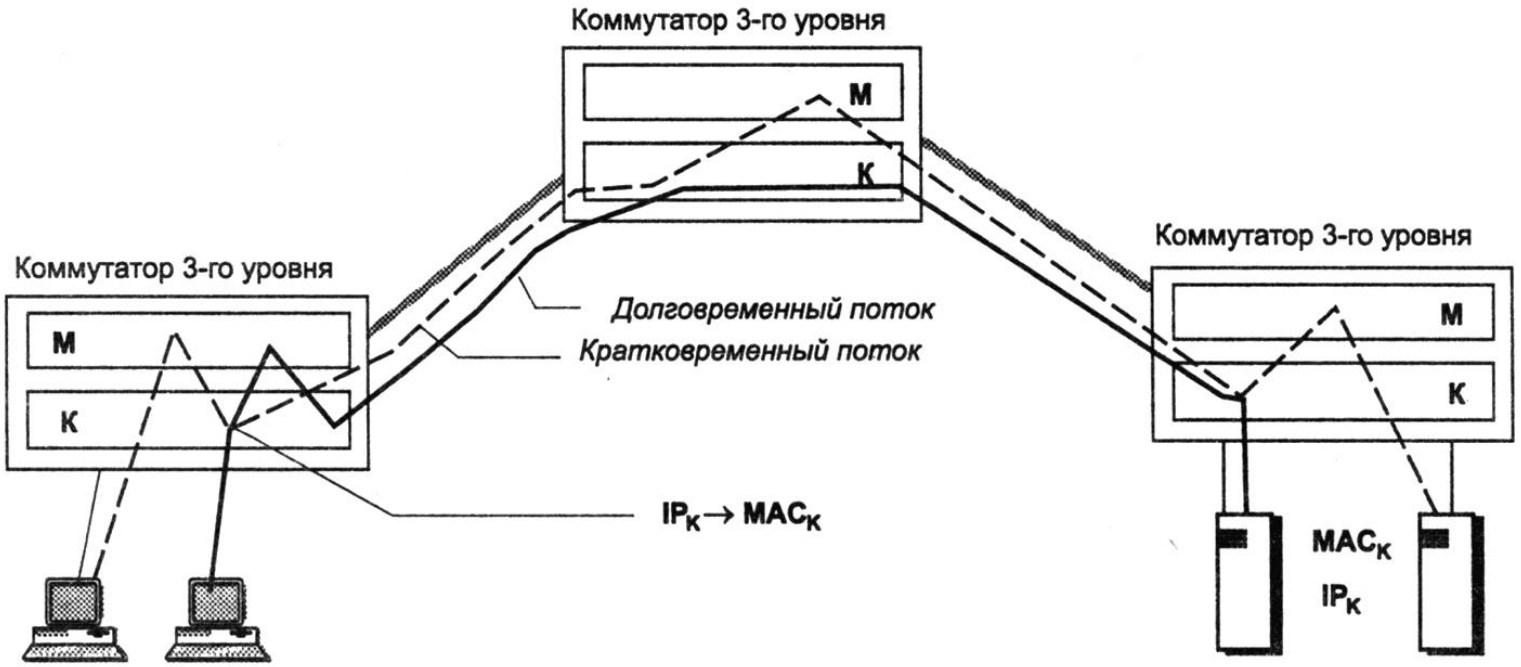
Стандарт 802.3af (питание через Ethernet, Power over Ethernet PoE)



Стандарт 802.3af (питание через Ethernet, Power over Ethernet PoE)

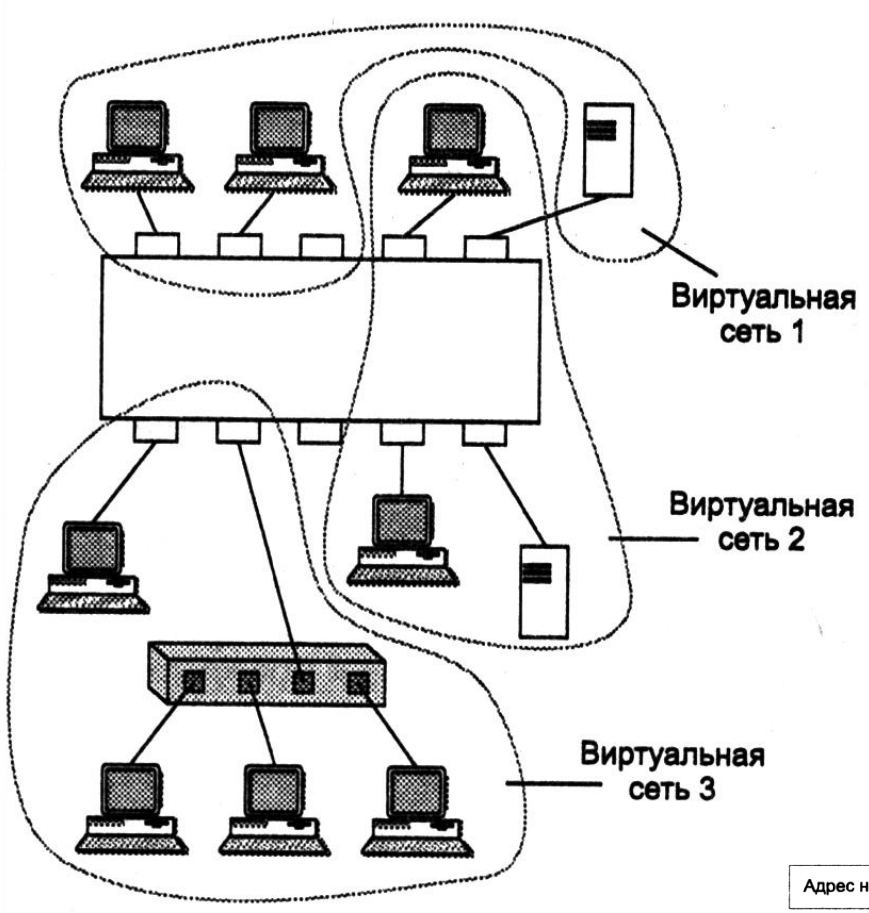
Инжекторы и сплиттеры PoE

Коммутаторы 3 уровня (Layer3)



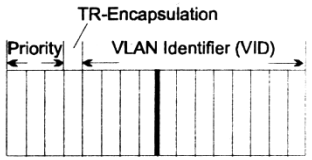
Первый коммутатор помещает в кадр Ethernet не MAC-адрес порта следующего маршрутизатора, а MAC-адрес узла назначения (MACk)

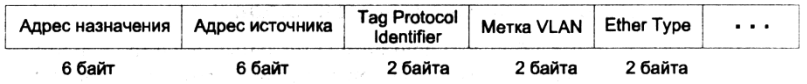
Виртуальные сети (VLAN)



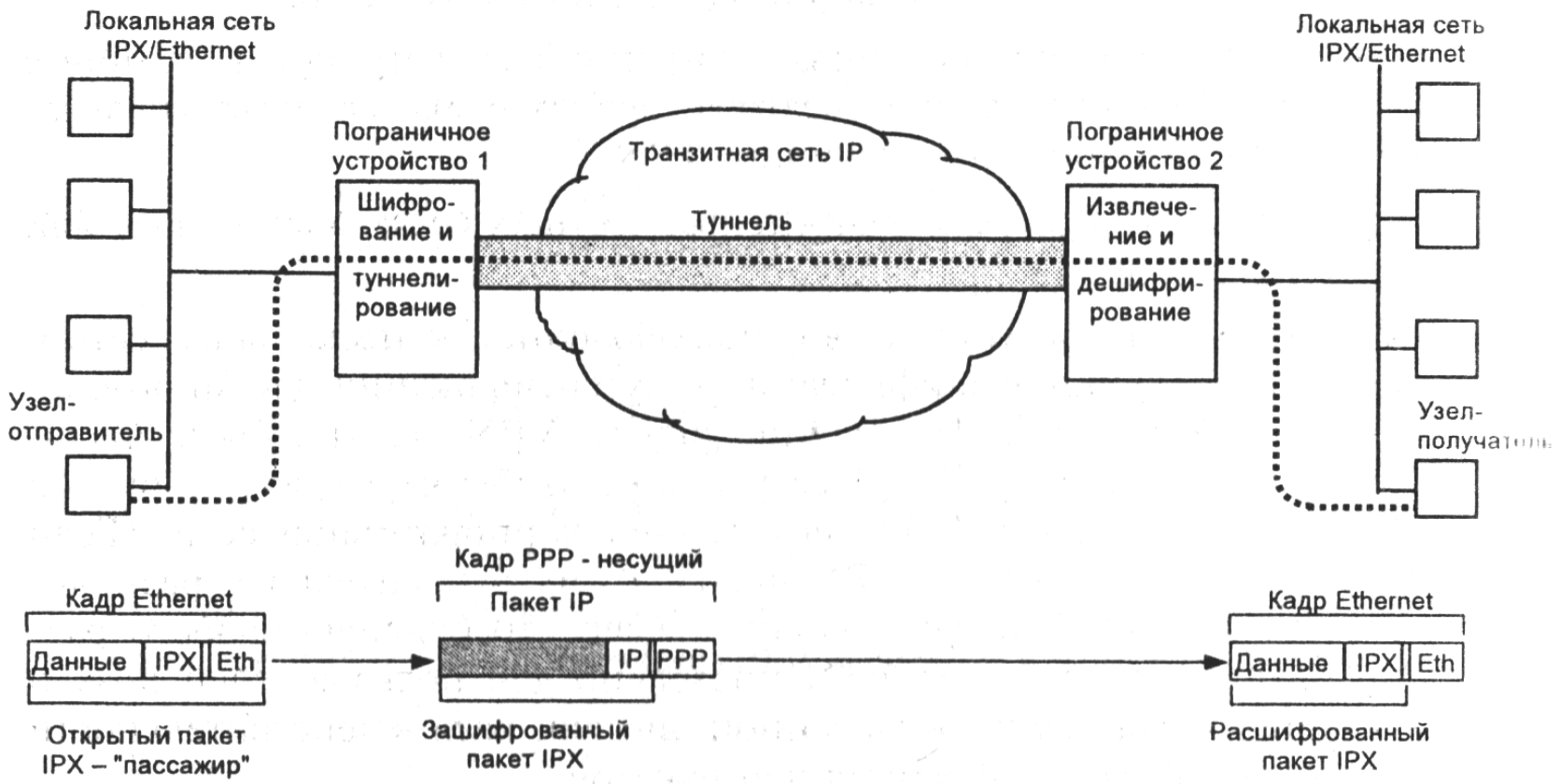
IEEE802.1p/Q определяет формат инкапсуляции дополнительного поля для номера VLAN (12 бит) и номера приоритета (3 бита)

Кроме того, в коммутируемой сети возможно создавать multicast-группы





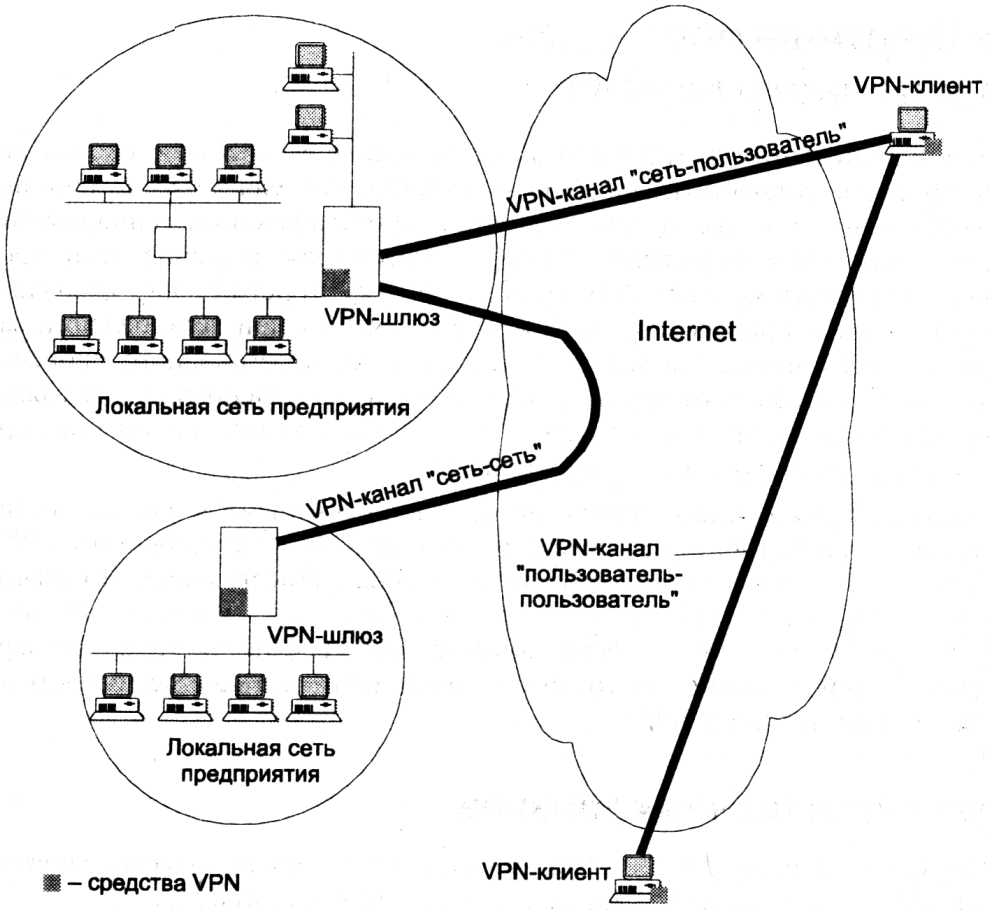
Инкапсуляция, туннелирование

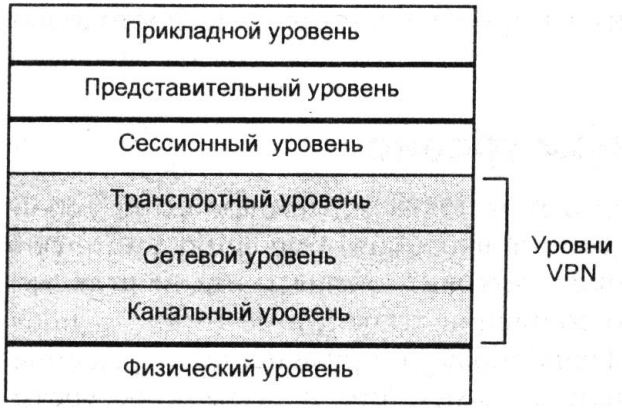


Виртуальные частные сети, VPN

- 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

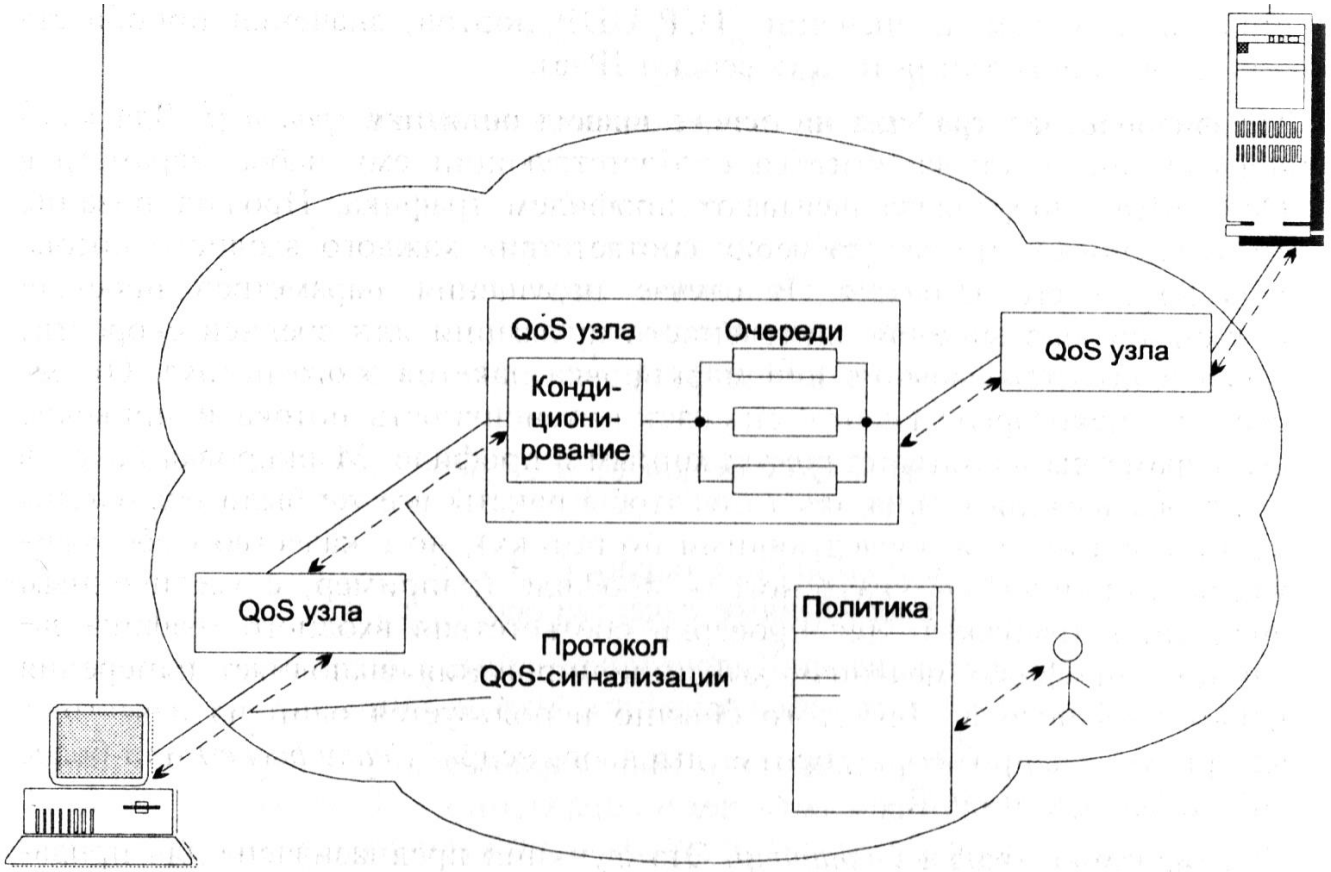
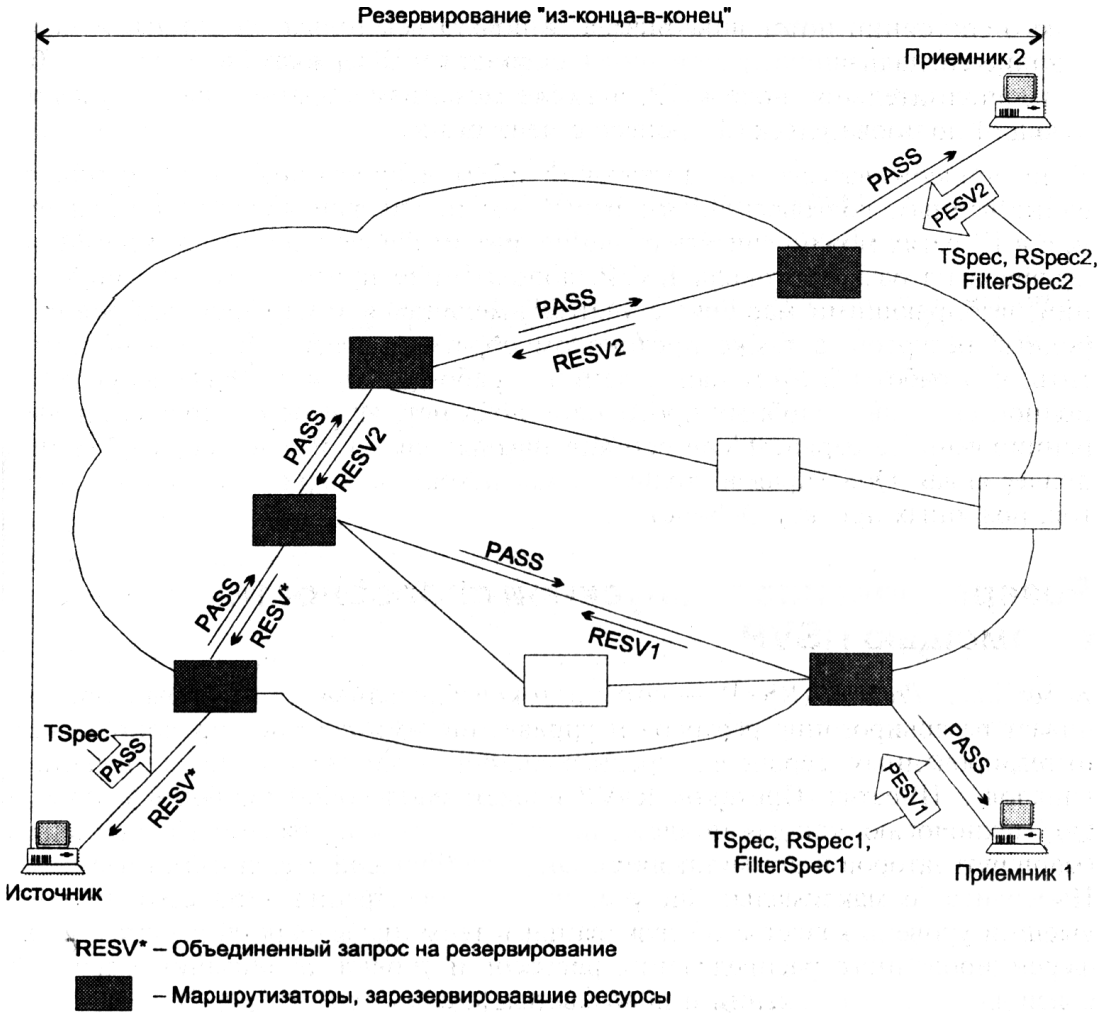
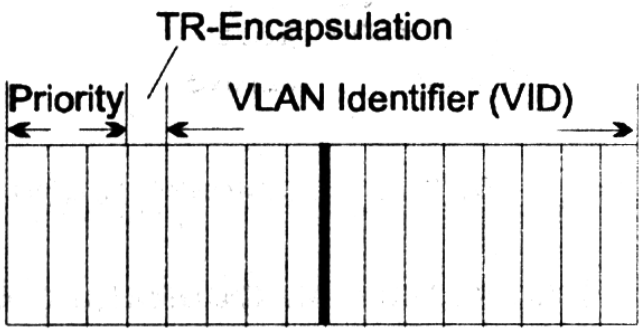


Рис. 2.18. Базовая архитектура средств QoS

Резервирование с помощью RSVP (ReSerVation Protocol)



Структура кадра Ethernet с полем 802.1Q

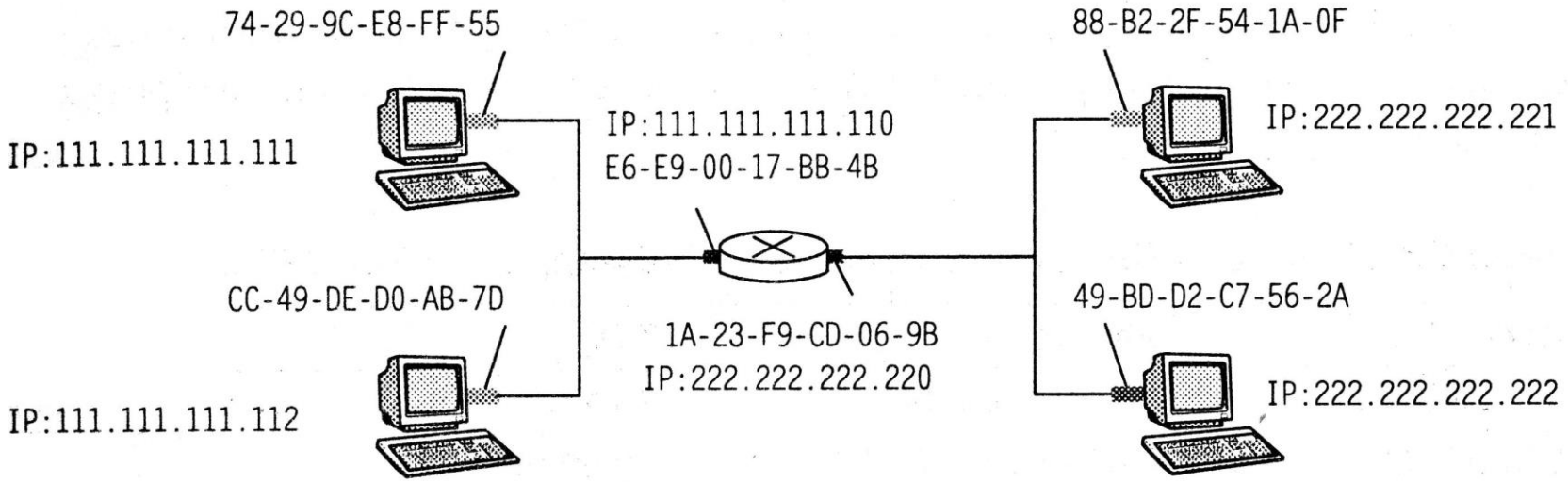


Адрес назначения	Адрес источника	Tag Protocol Identifier	Метка VLAN	Ether Type	. . .
6 байт	6 байт	2 байта	2 байта	2 байта	

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.

Пример уязвимости IP- протокол ARP



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

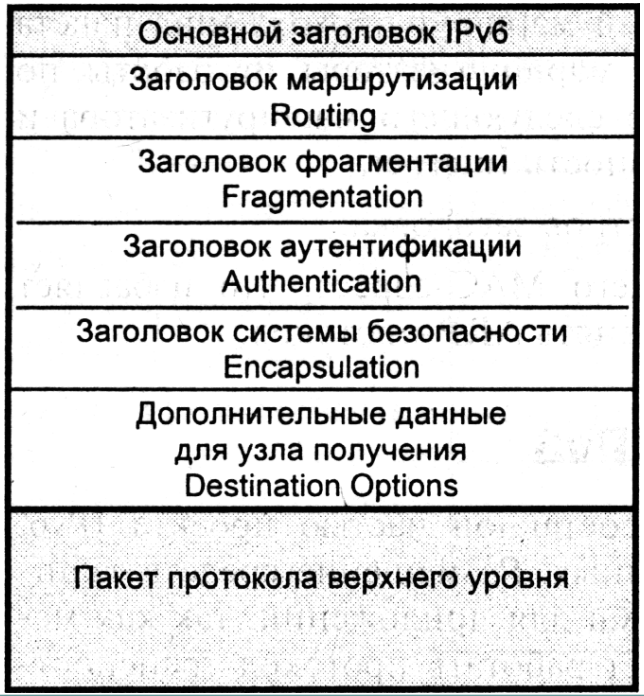
- длина – 16 байт;
- запись в 16-ричной системе, либо в режиме совместимости с – смешанная 16-ричная и 10-тичная:
  - FEDC:0A98:0:0:0:0:7654:3210
  - 0:0:0:0:FFFF:62.76.175.200

- Пока нет устоявшейся терминологии IPv6 на русском, используются «кальки» и термины на английском.

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)

Основной заголовок и структура пакета IPv6

4	8	16	24	31
Версия	Приоритет	Метка потока		
Размер поля данных		Следующий заголовок	Максим. количество хопов	
Адрес источника (128 бит)				
Адрес назначения (128 бит)				



IPv6 адресация

- IPv6 addresses 128-битные
  - 2^{128} возможных адресов
  - 340,282,366,920,938,463,463,374,607,431, 768,211,456 адресов
- 6.6 x 10^{23} адресов на 1м^2 поверхности планеты Земля
- ~ 5x 10^{28} адресов на жителя Земли

Представление IPv6 адресов

- Примеры:
  - FE80:0:0:0:2AA:FF:FE9A:4CA2 становится FE80::2AA:FF:FE9A:4CA2
  - FF02:0:0:0:0:0:0:2 становится FF02::2
- Часть 16-bit блока не сжимается:
  - FF02:30:0:0:0:0:0:5 не становится FF02:3::5, а записывается как FF02:30::5
- Использование префиксов:
  - 2001:DB8:0:2F3B::/64 -- subnet prefix
  - 2001:DB8::/48 -- route prefix
  - FF00::/8 диапазон адресов

Типы адресов IPv6

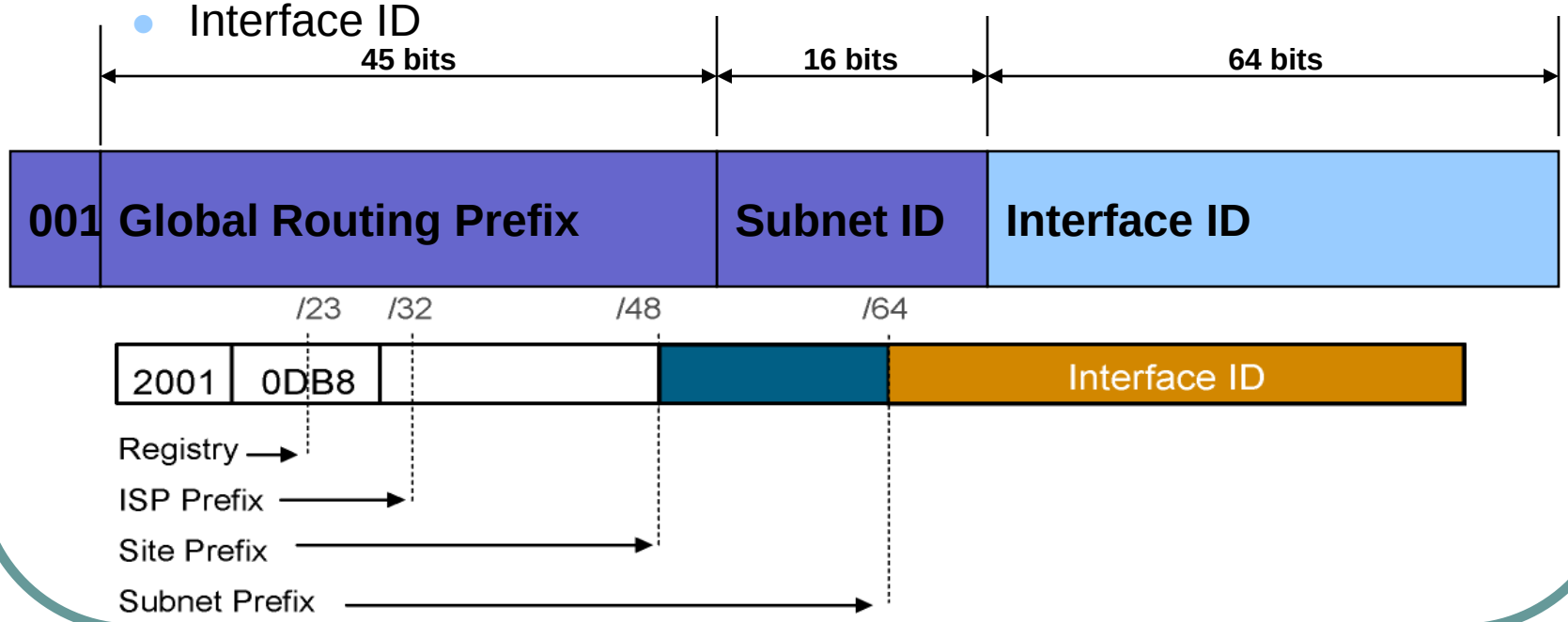
- Типы адресов (задается полем префикса формата - FP):
  - unicast
  - multicast
  - anycast

Unicast адреса IPv6

- Global unicast addresses
- Local-use addresses
  - Link-local addresses
  - Site-local addresses
- Unique local addresses
- Special addresses

Глобальные адреса IPv6

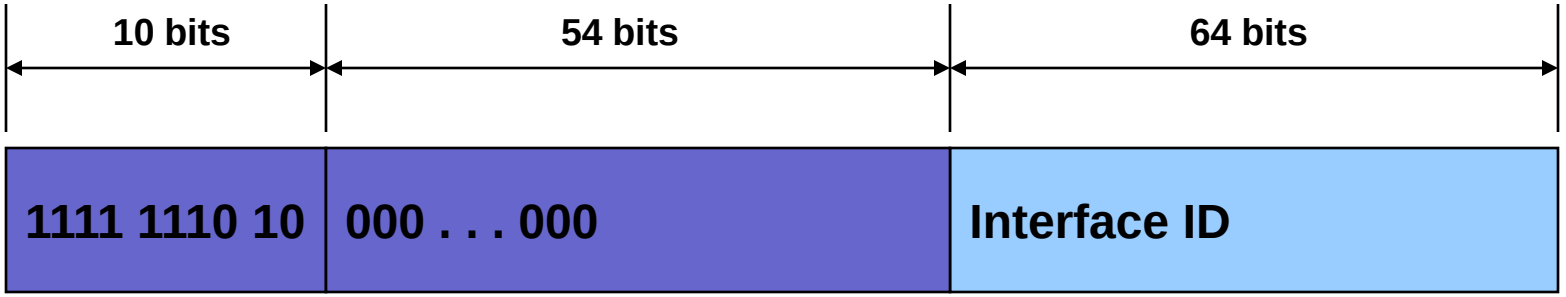
- Область -- IPv6 Internet
  - Эквивалентно public IPv4 адресам
- Структура
  - Global Routing Prefix
  - Subnet ID
  - Interface ID



"IPv6 Implementation Guide, Cisco IOS Release 15.2" (http://www.cisco.com)

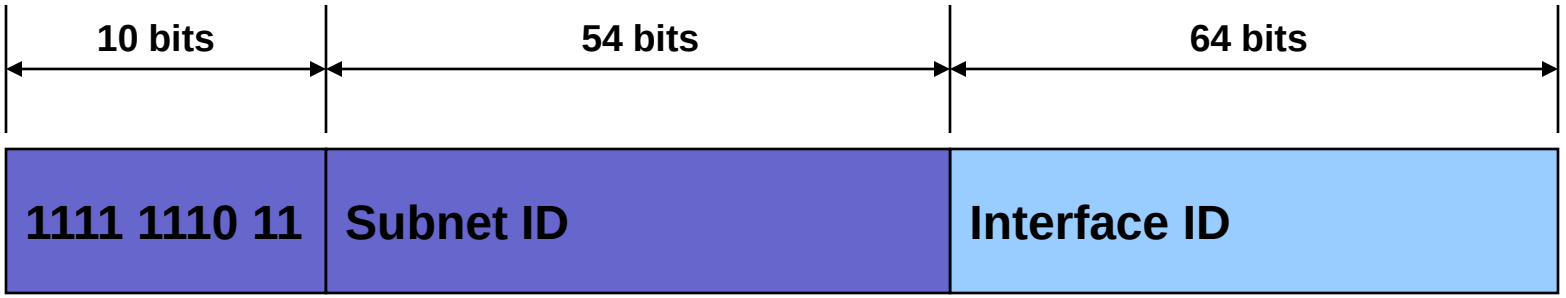
Link-Local адреса

- Область – локальное соединение
  - Эквивалентно APIPA IPv4
- FE80::/10 prefix
- Нужно указывать выходной интерфейс, т.к. все интерфейсы ведут в FE80::/10
- Применяется для:
  - Одной сети, в немаршрутизируемых сетях
  - Neighbor Discovery processes



Site-Local адреса

- Область – частная сеть
  - Эквивалентно private IPv4
- FEC0::/10 prefix
- Применяется для интранет сетей прямо не соединенных с IPv6 Internet
- Уже устарело, но пока поддерживается



Zone ID для Link-Local и Site-Local адресов

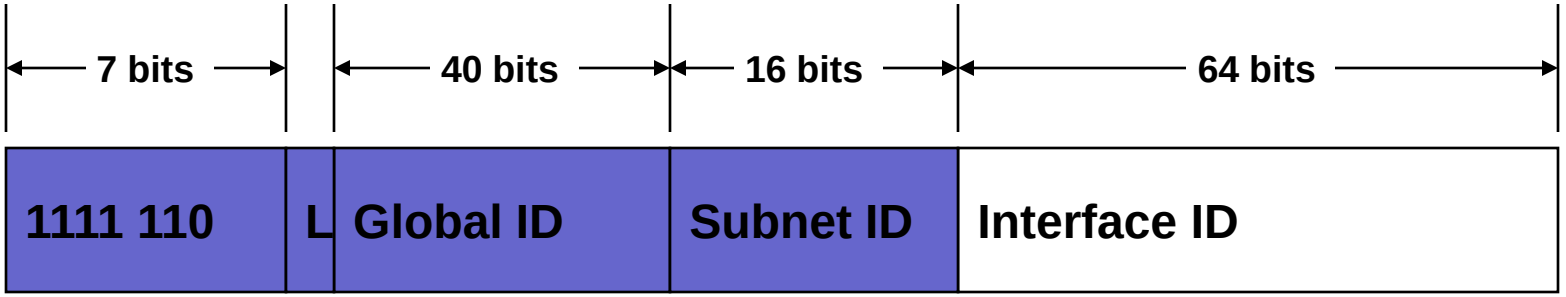
- Link-local и site-local адреса могут быть не уникальны
- Zone ID используется для идентификации конкретного линка или внутренней сети
  - Link-local адреса

    Zone ID обычно представляет собой номер интерфейса
  - Site-local адреса

    Zone ID обычно = 1, если внутренняя сеть одна
- Примеры:
  - **ping fe80::2b0:d0ff:fee9:4143%3**
  - **tracert fec0::f282:2b0:d0ff:fee9:4143%2**

Unique Local адреса

- Внутренние для организации, уникальные для все подсетей организации
- FD00::/8 prefix
- Это – замена site-local адресам
- Не требуется zone ID



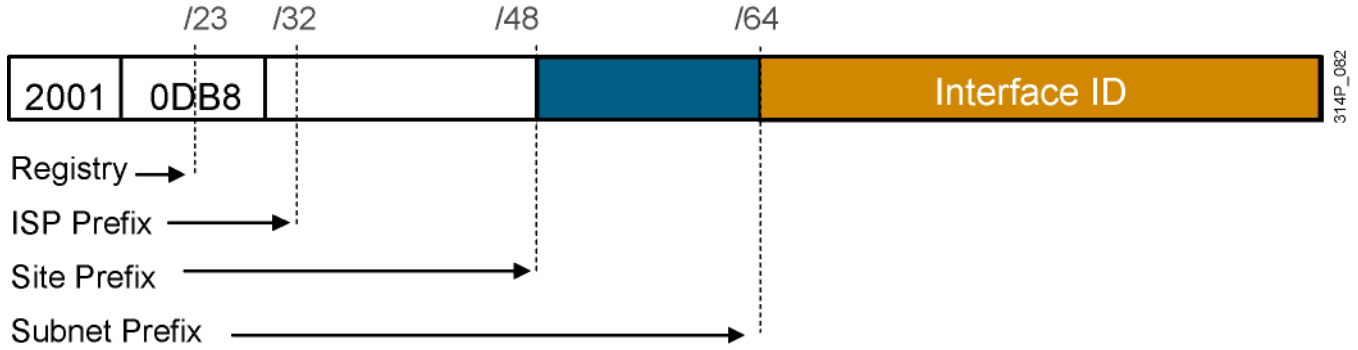
Специальные и multicast IPv6 адреса

- Unspecified Address
  - 0:0:0:0:0:0:0:0 ➔::
- Loopback Address
  - 0:0:0:0:0:0:0:1 ➔::1
- Multicast
  - FFxx::

Совместимые адреса

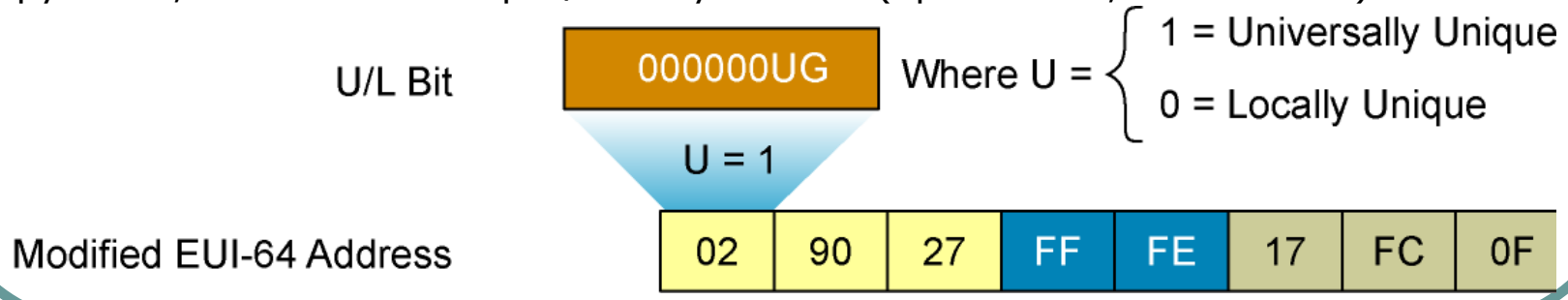
- IPv4-совместимые адреса
  - 0:0:0:0:0:0:*w.x.y.z* or ::*w.x.y.z*
- IPv4-отображенные адреса
  - 0:0:0:0:0:FFFF:*w.x.y.z* or ::FFFF:*w.x.y.z*
- 6to4 адреса
  - 2002::/16 address prefix
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) адреса
  - *interface ID*::0:5EFE:*w.x.y.z*

Назначение IPv6 адресов



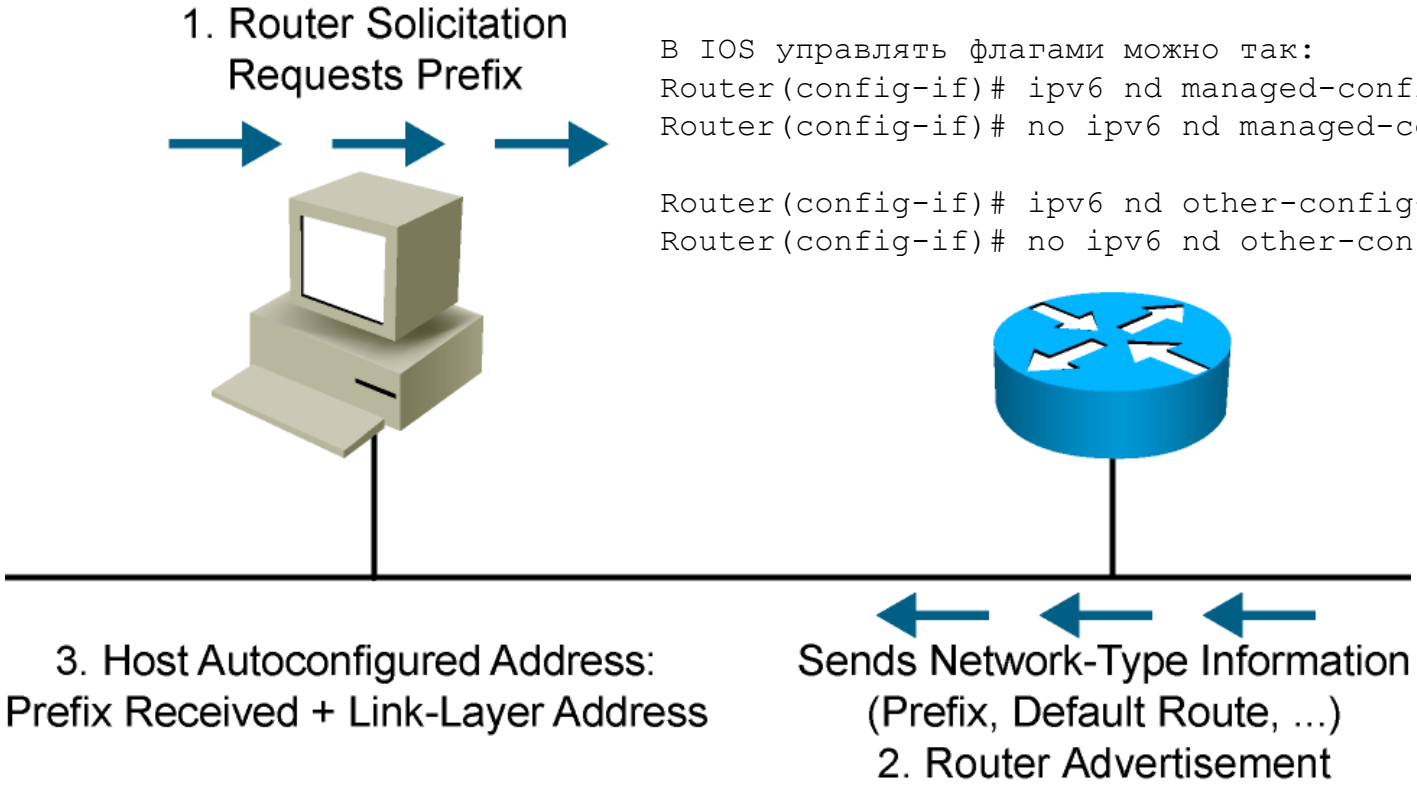
•Формирование полного 128-битного адреса (кроме «ручного» способа):
- Автоконфигурация, Stateless Address Auto-Configuration (SLAAC, по-умолч.)
- Автоконфигурация с добавление информации от DHCPv6 “Stateless”
- Автоконфигурация с использованием только DHCPv6 “Stateful”

•Определение младшей 64-битной части (Host ID, Interface ID) может быть: «ручное», EUI-64 или генерацией случайного (приватного, анонимного) ID.



Автоконфигурация без машины состояний (stateless)

- Stateless Address Auto-Configuration (SLAAC, RFC2462)
- На шаге 2, значения флагов O(ther) или M(anaged) определяет вид DHCPv6 участия: stateless или stateful

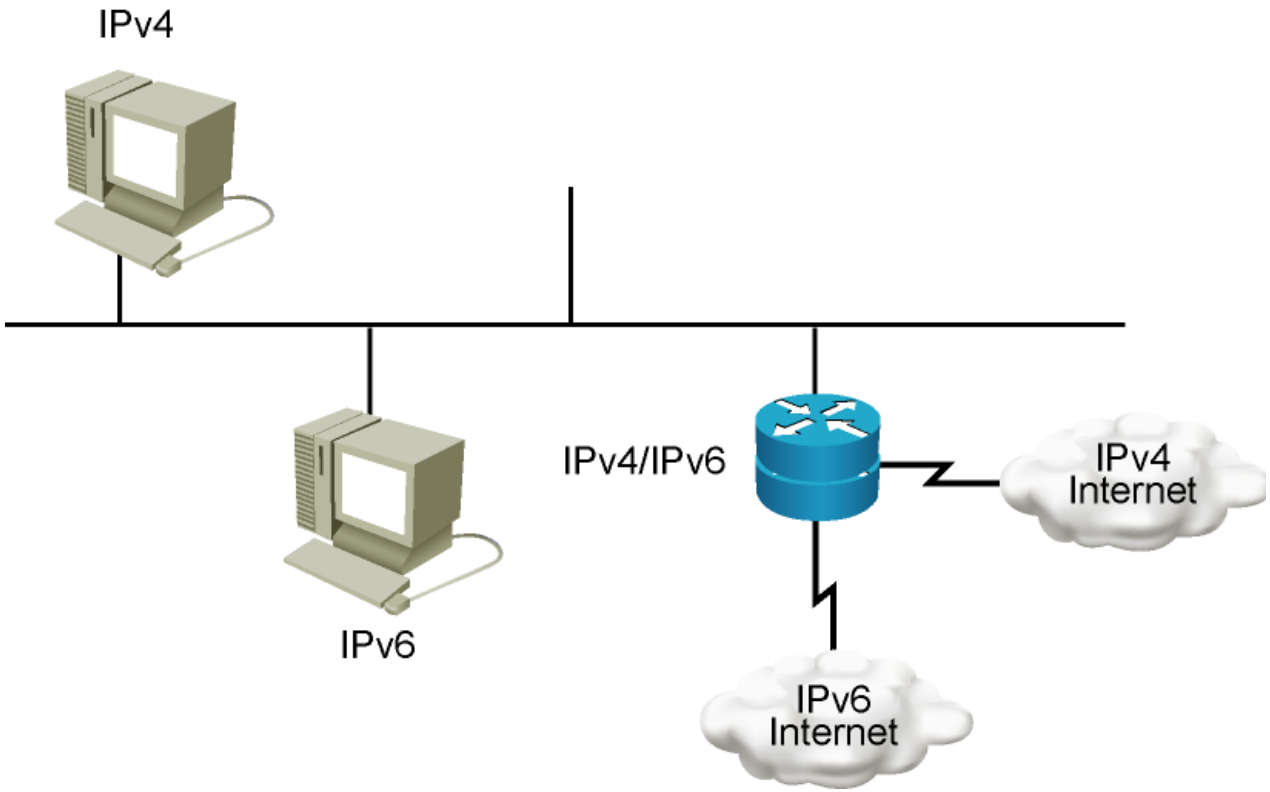



```
В IOS управлять флагами можно так:
Router(config-if)# ipv6 nd managed-config-flag
Router(config-if)# no ipv6 nd managed-config-flag

Router(config-if)# ipv6 nd other-config-flag
Router(config-if)# no ipv6 nd other-config-flag
```

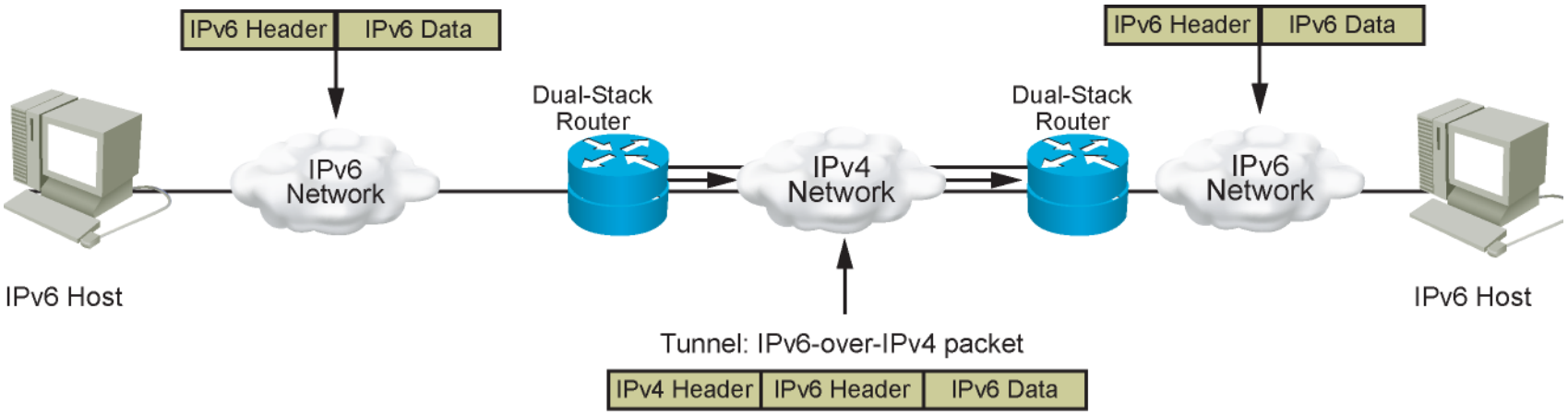
Dual Stack

Длительное время будут существовать и IPv4 и IPv6 сети
Нужны решения на этот период

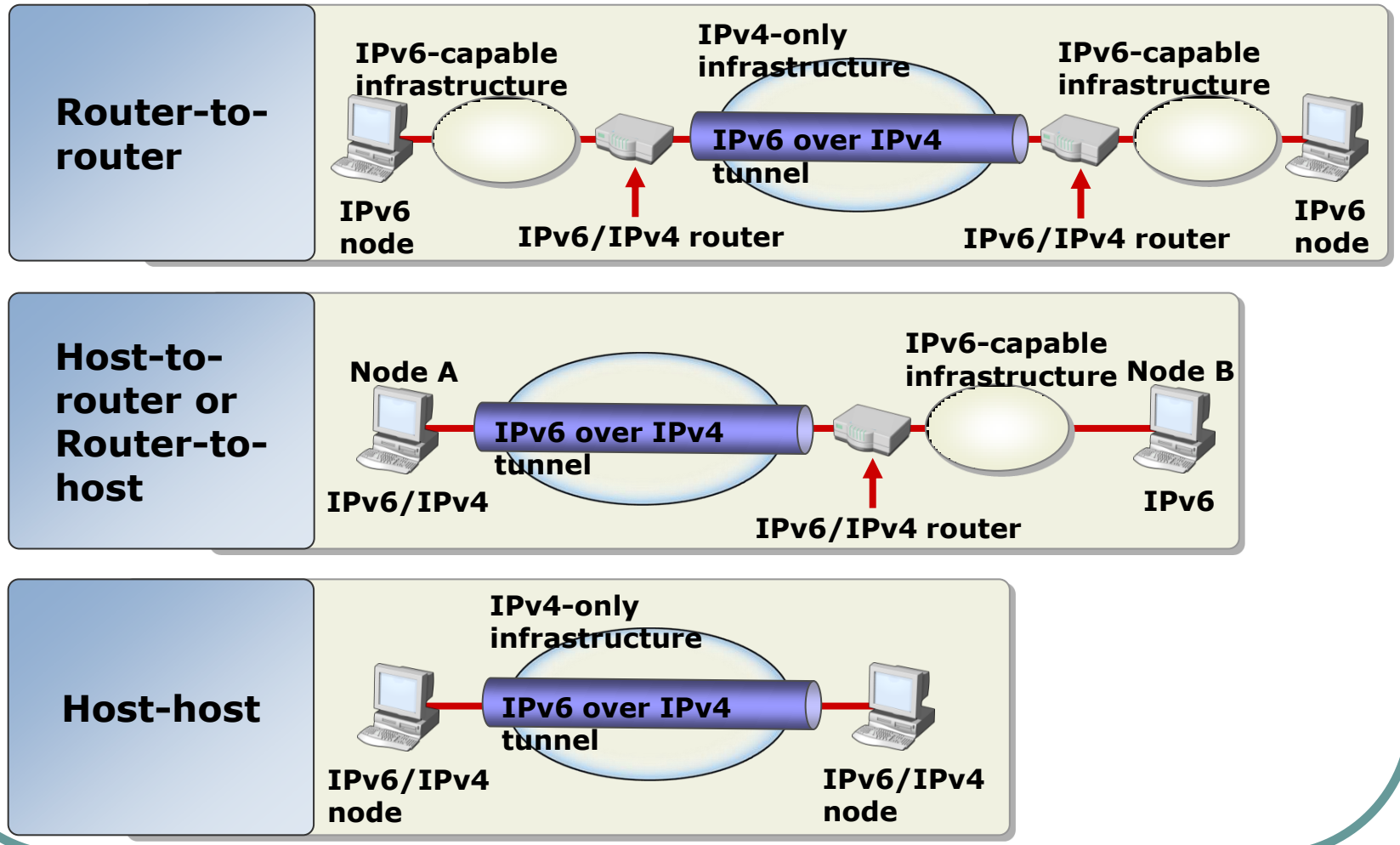


Туннелирование IPv6 over IPv4

Длительное время будут существовать и IPv4 и IPv6 сети
Нужны решения на этот период



Способы туннелирования



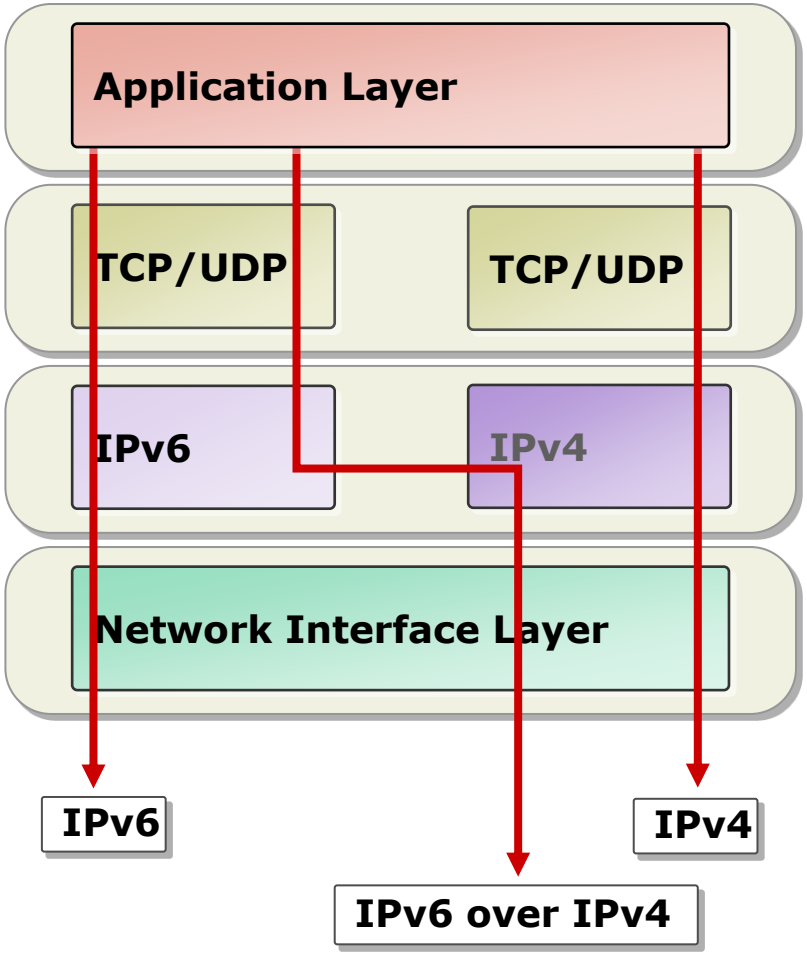
Технологии туннелирования

Технология	Особенности
ISATAP	• Для локальных интранет сетей • Автоматическая конфигурация конеч. систем • IPv6 узлы коммуницируют через IPv4 подсеть • По-умолчанию включена в W2K8, Vista, W7
6to4	• Взаимодействие IPv6 сетей через IPv4 Интернет • Автоматическая конфигурация конеч. систем • По-умолчанию включена в W2K8, Vista, W7
Teredo	• Взаимодействие IPv6 сетей через IPv4 NAT • По-умолчанию выключена

Dual stack (W2K3, XP)

Dual layer может создавать:

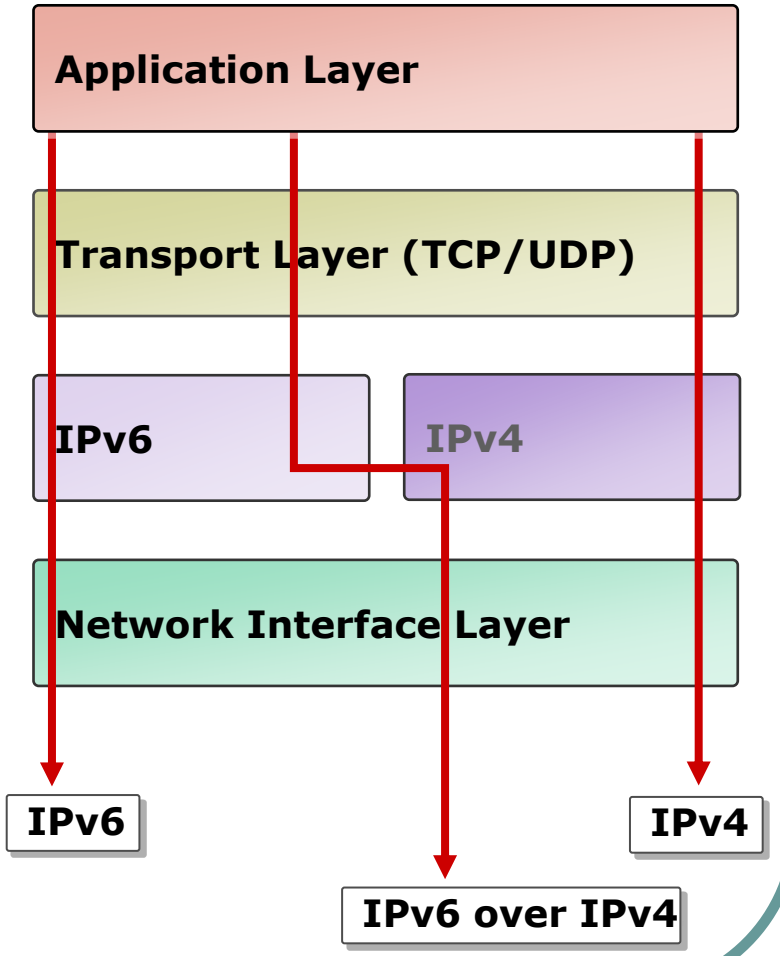
- **IPv4 packets**
- **IPv6 packets**
- **IPv6 over IPv4 packets**



Dual layer (W2K8, Vista, W7)

Dual layer может создавать:

- **IPv4 packets**
- **IPv6 packets**
- **IPv6 over IPv4 packets**



VPN - virtual private networks

- PPTP - Point-to-Point Tunneling Protocol
  - Microsoft, 3COM, US Robotics
  - GRE (IP протокол N47), PPTP 1723/TCP
- L2TP – Layer 2 Tunneling Protocol
  - IETF
  - IPSec: IKE, AH, ESP
  - AH (протокол N50), ESP (протокол N51)
  - IKE UDP/500

Совместная работа IPv4 и IPv6

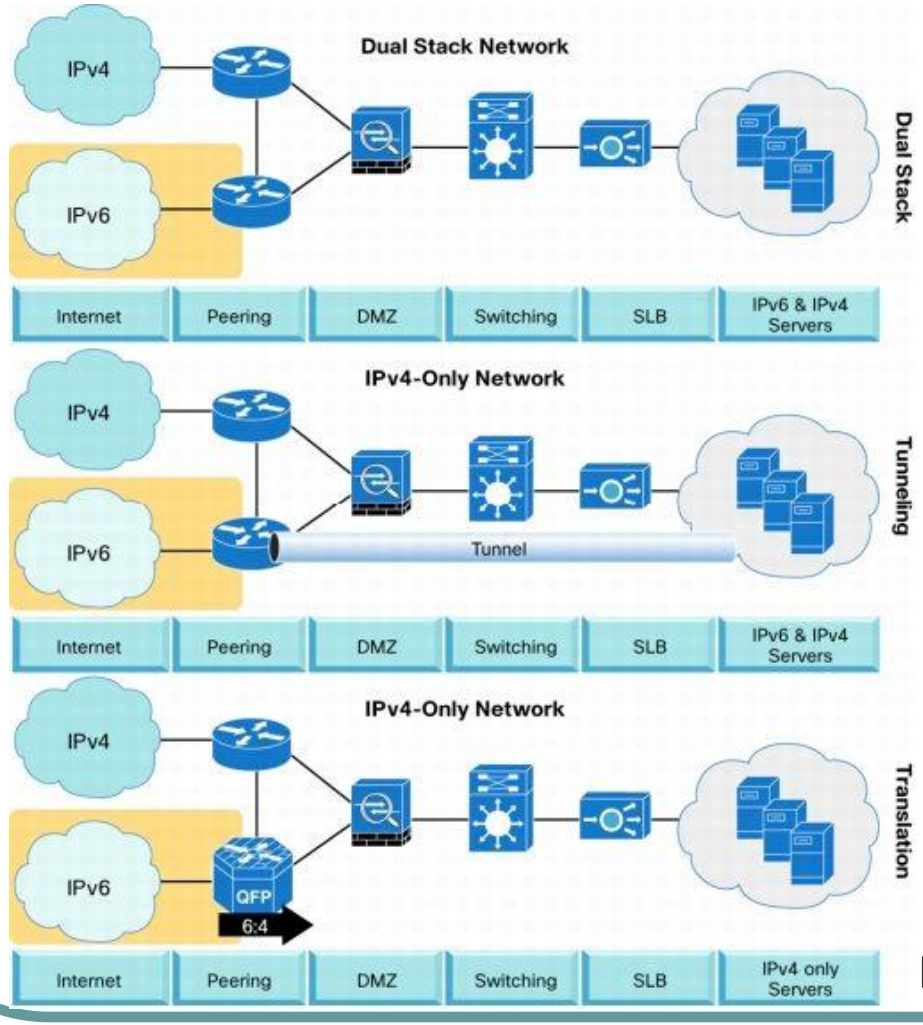


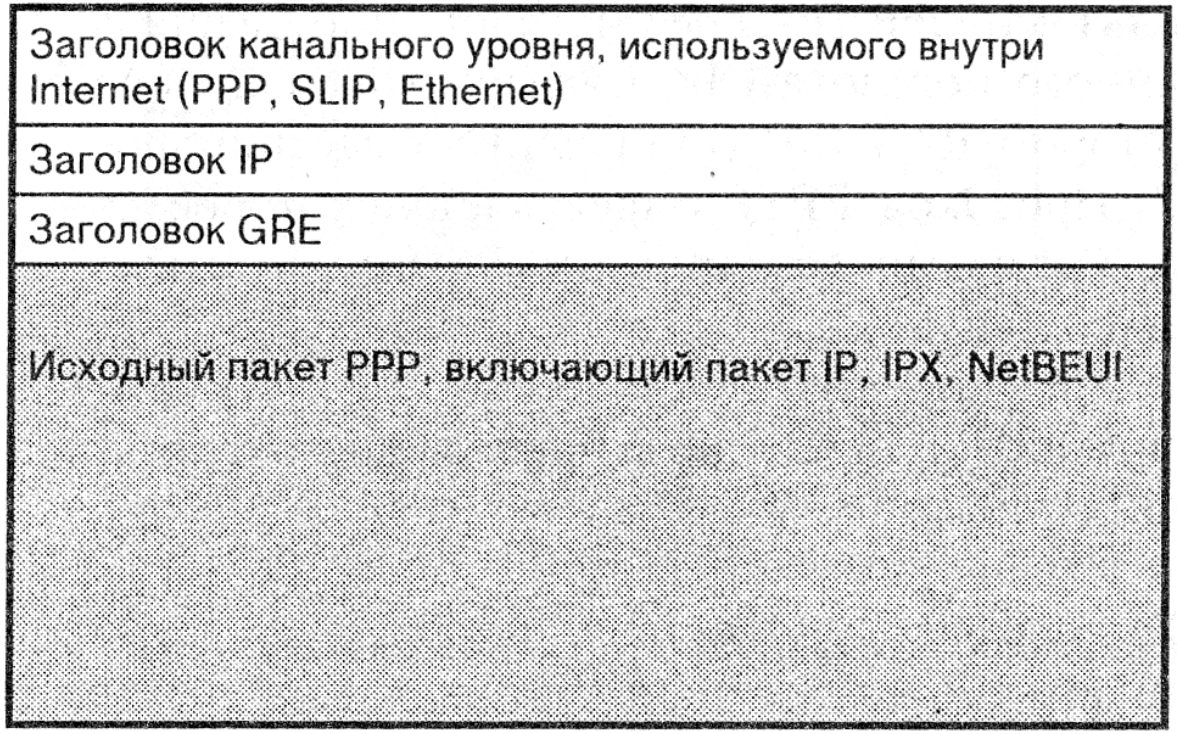
рисунок http://www.cisco.com

Point-to-Point Tunneling Protocol

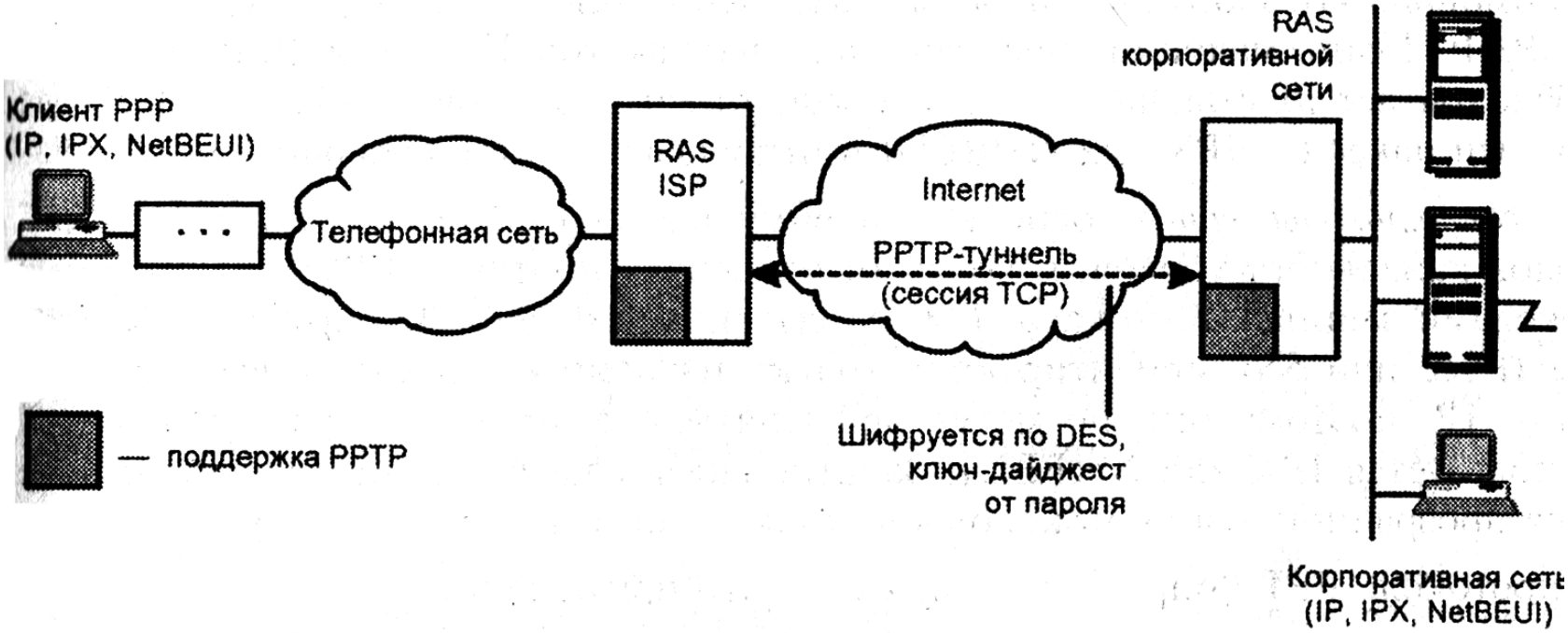
- Инкапсулирующий протокол 2 уровня
- Позволяет создавать защищенные каналы для работы по протоколам IP, IPX, NetBEUI (алгоритмы DES, RC-4)
- Существует две схемы применения:
  - RAS ISP – пограничный маршрутизатор КИС
  - пользователь – маршрутизатор КИС

Структура пакета PPTP

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



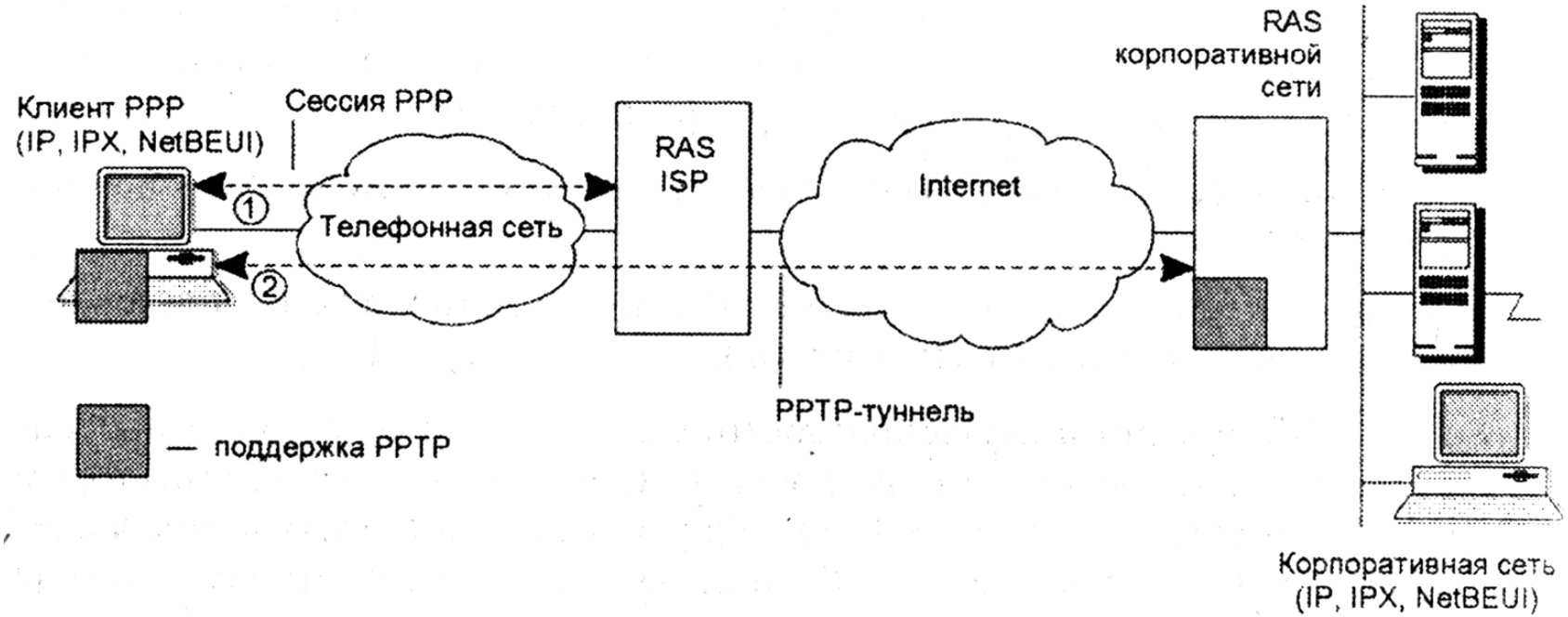
RAS ISP – пограничный маршрутизатор КИС



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



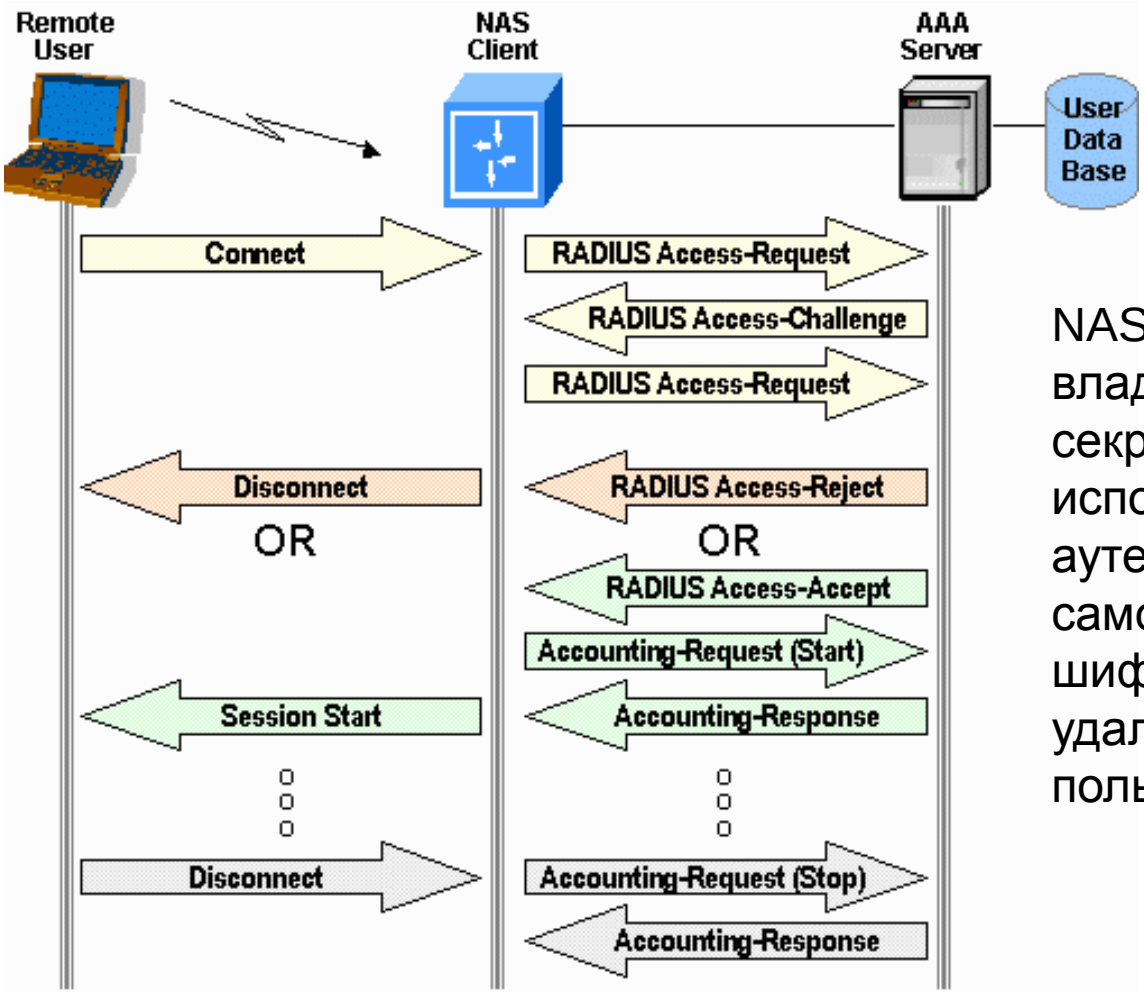
Требуется поддержка протокола PPTP на стороне пользователя

- 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 accounting).
- RADIUS-служба (Remote Authentication Dial In User Service).

Инфраструктура RADIUS



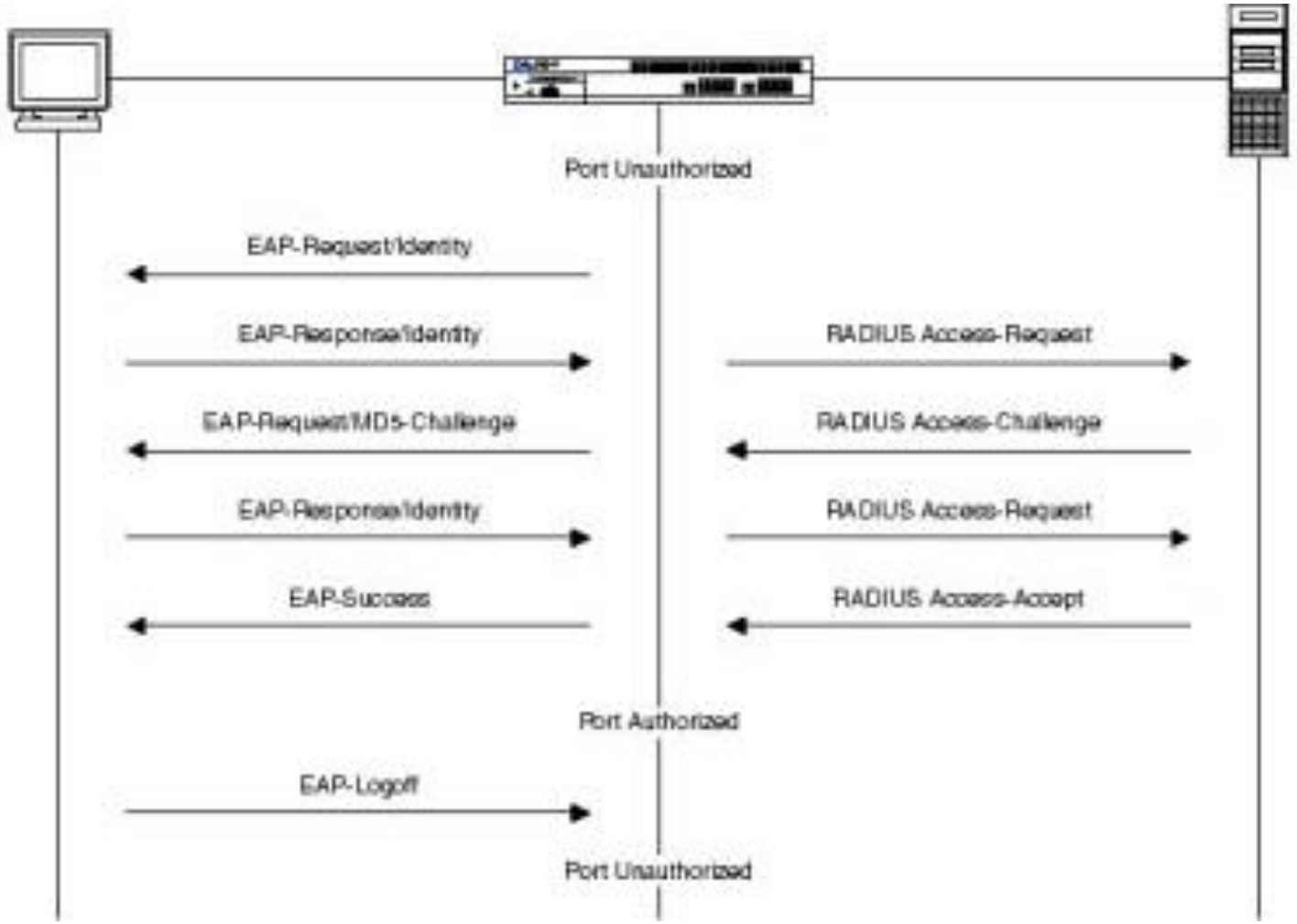
NAS и AAA-сервер владеют общим секретным ключом, использующимся для аутентификации самой NAS и шифрации запроса от удаленного пользователя.

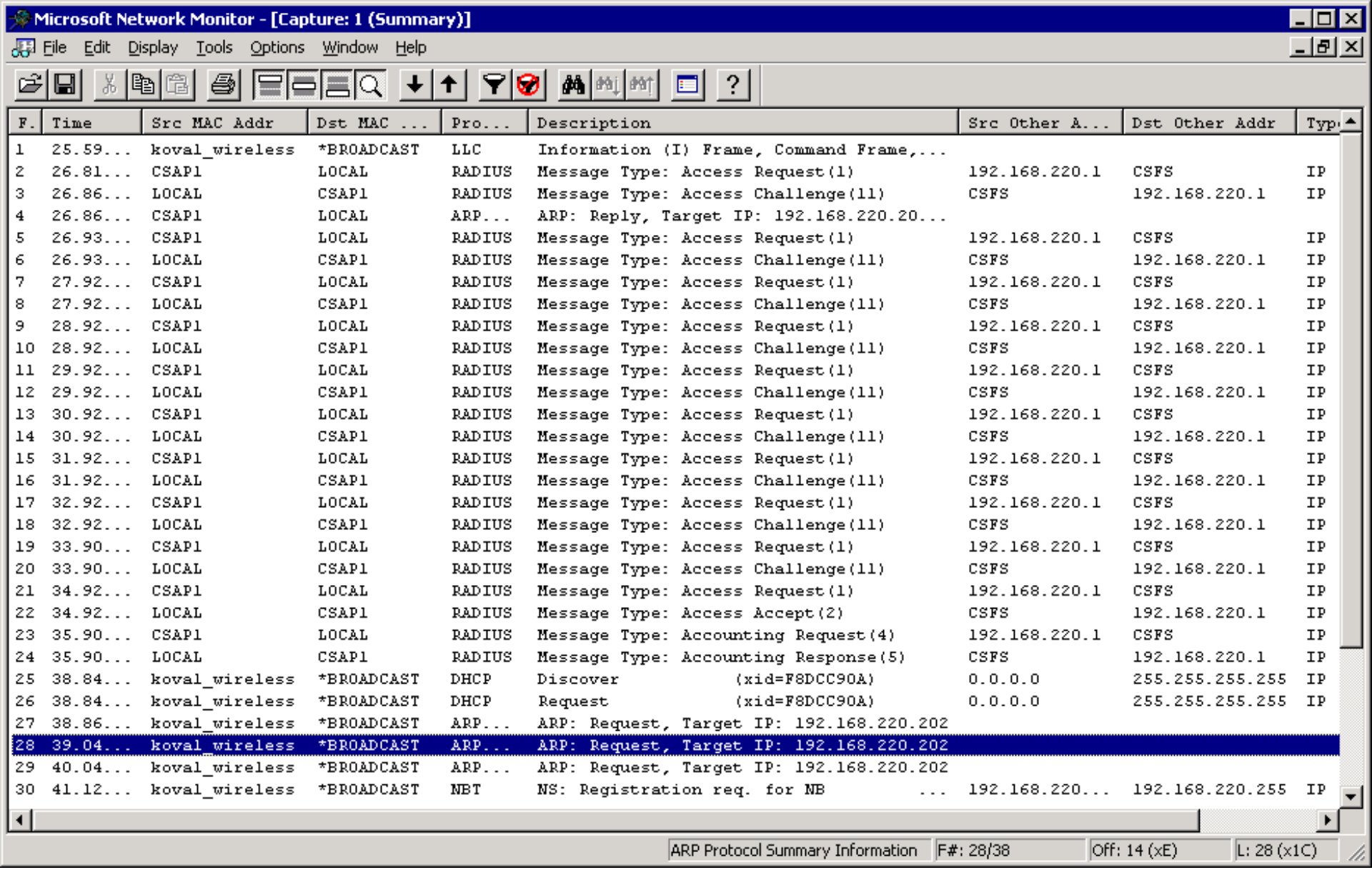
Последовательность аутентификации IEEE802.1x в сетях IEEE802.11

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




Microsoft Network Monitor - [Capture: 1 (Summary)]
File Edit Display Tools Options Window Help
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
ARP Protocol Summary Information
F#: 28/38
Off: 14 (xE)
L: 28 (x1C)

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»)

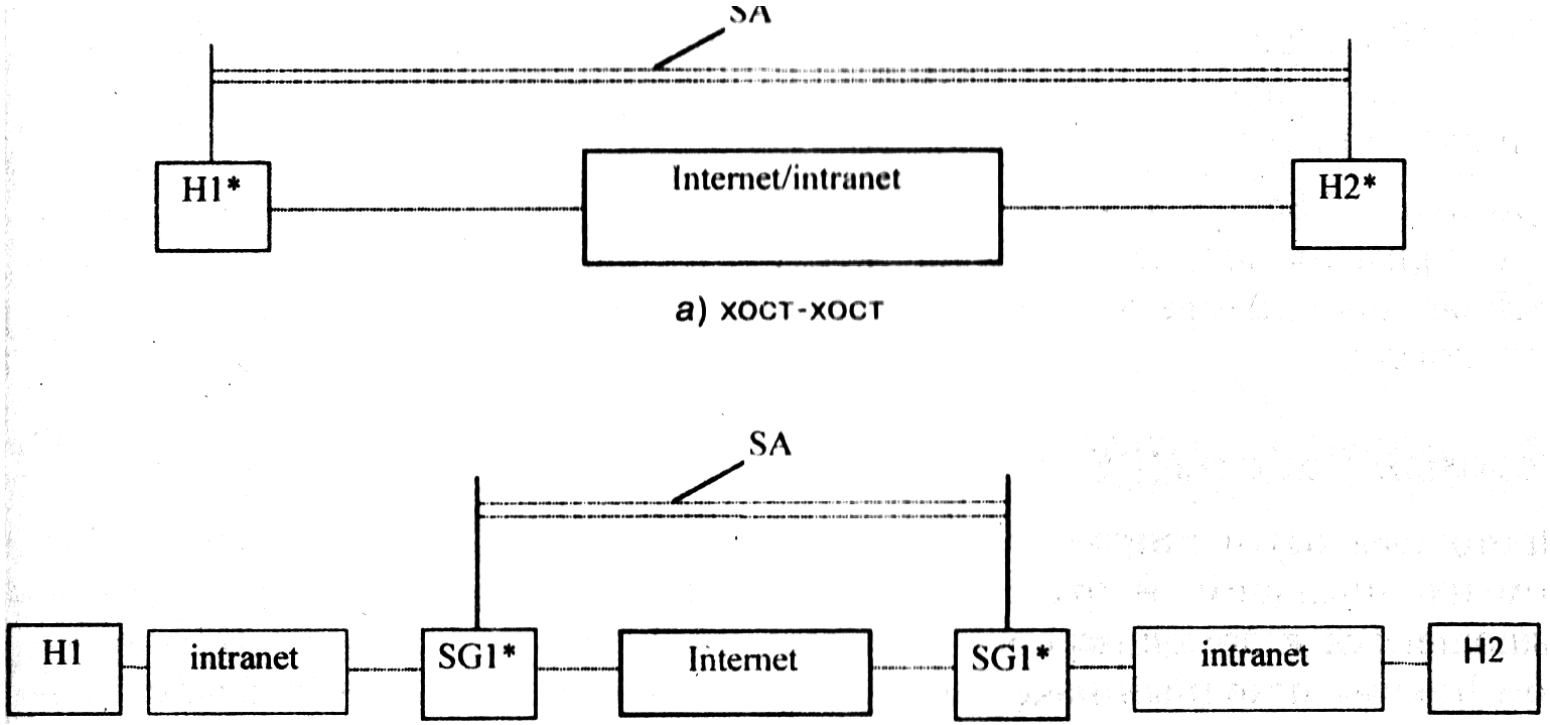
  Используются протоколы 3-х типов:

  - 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

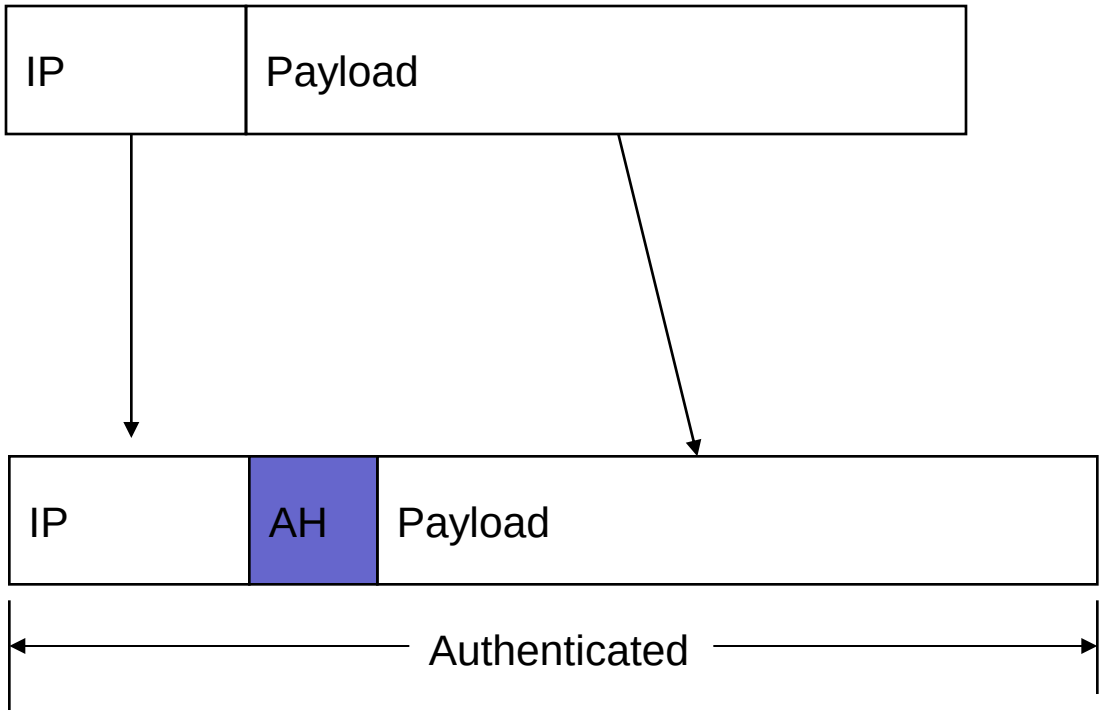


а) хост-хост

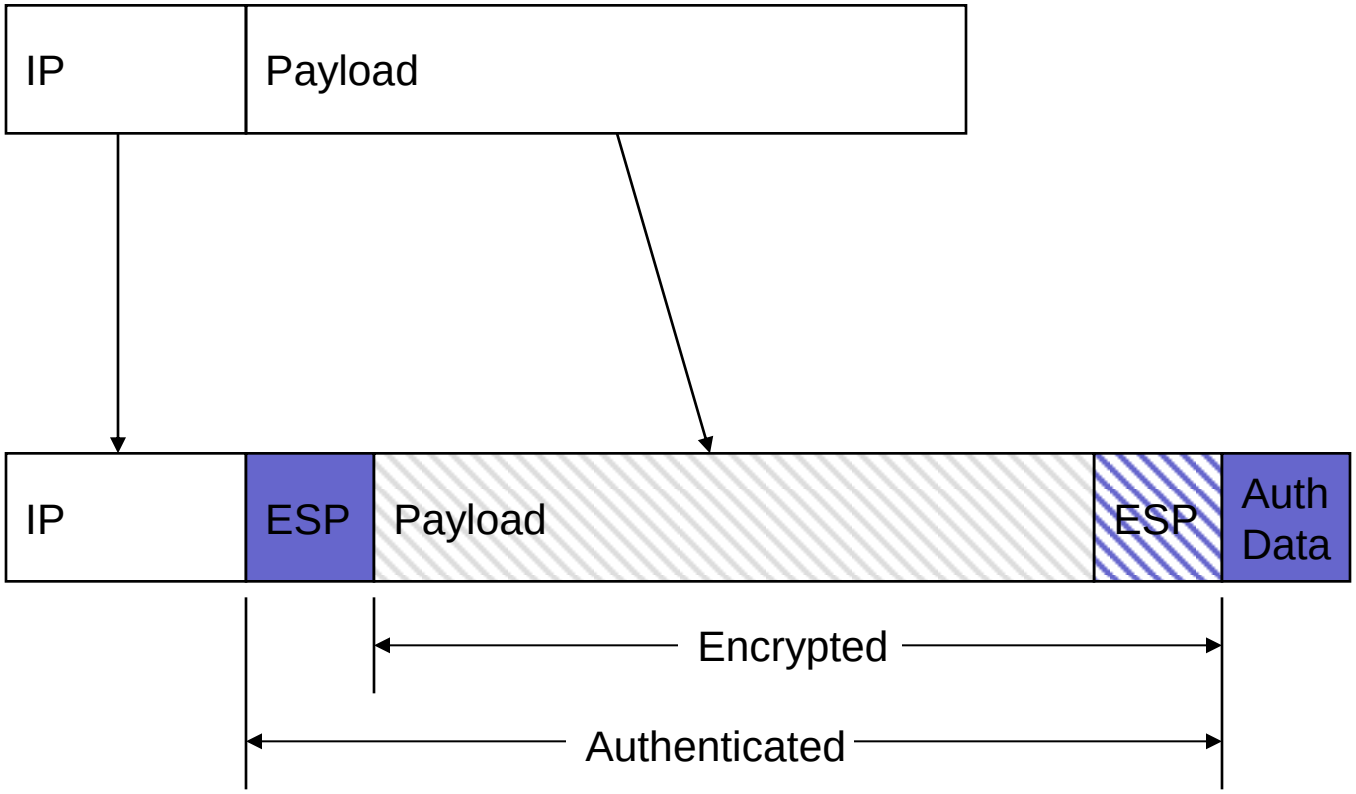
AH, ESP работают в 2-х режимах: транспортном (шифруется только поле данных, заголовок остается) и туннельном, причем AS –симплексное соединение.

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

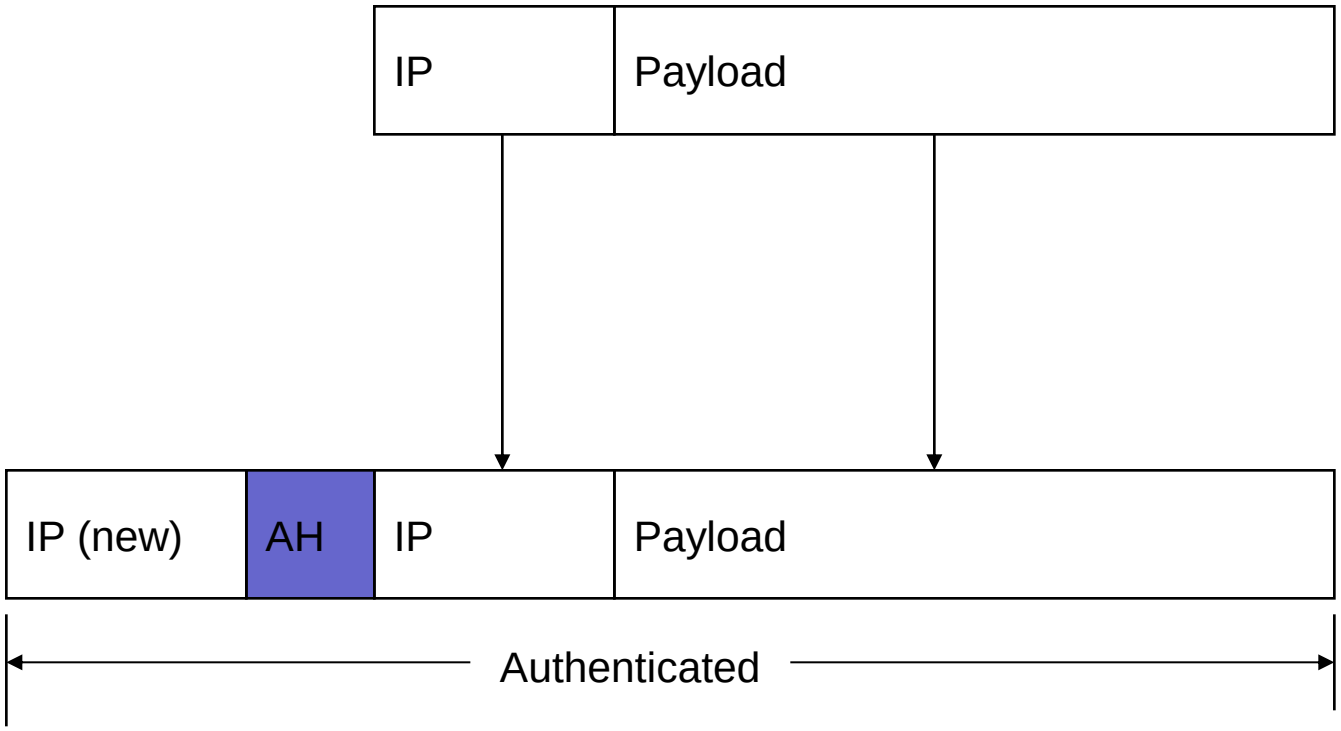
Пакет защищенный AH в транспортном режиме



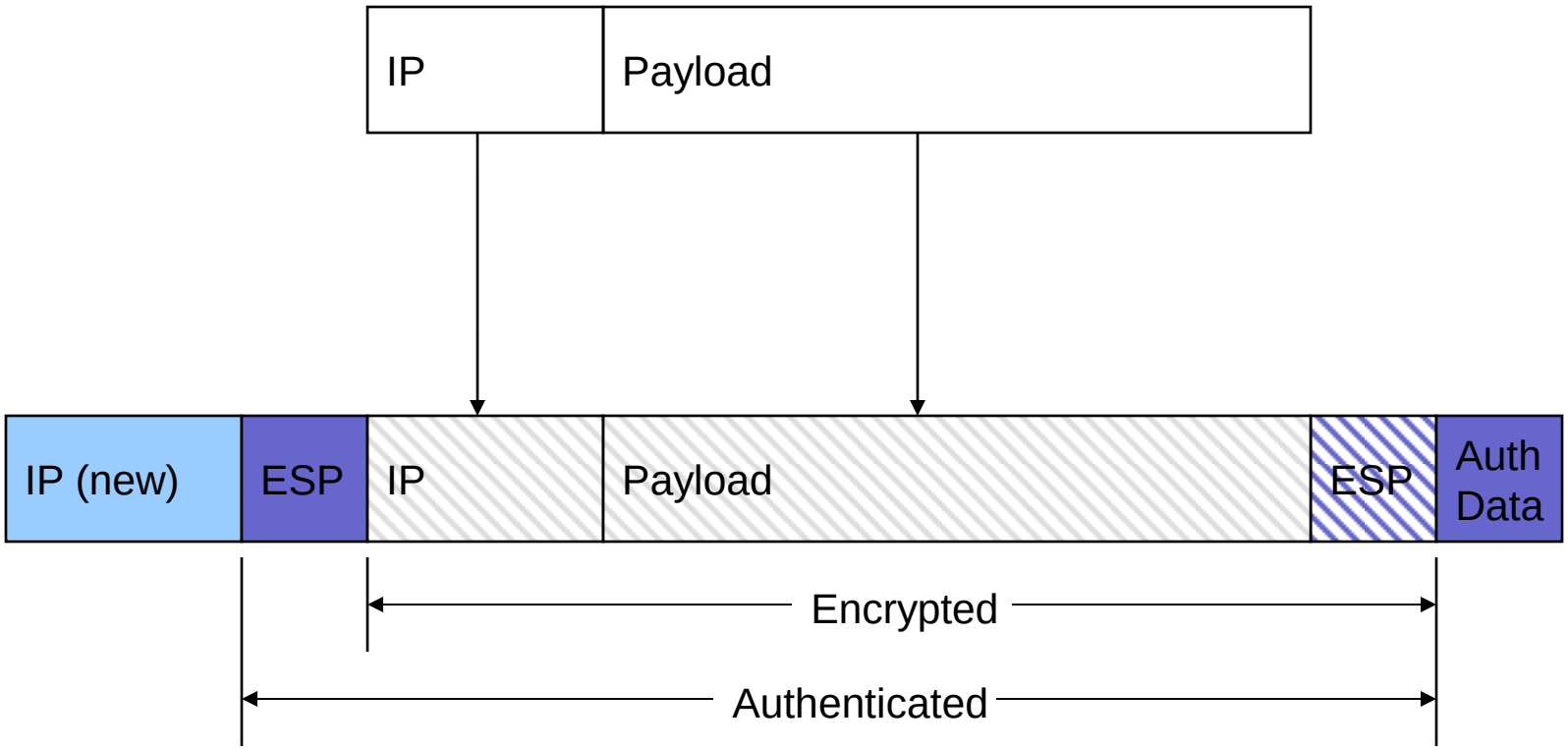
Пакет защищенный ESP в транспортном режиме



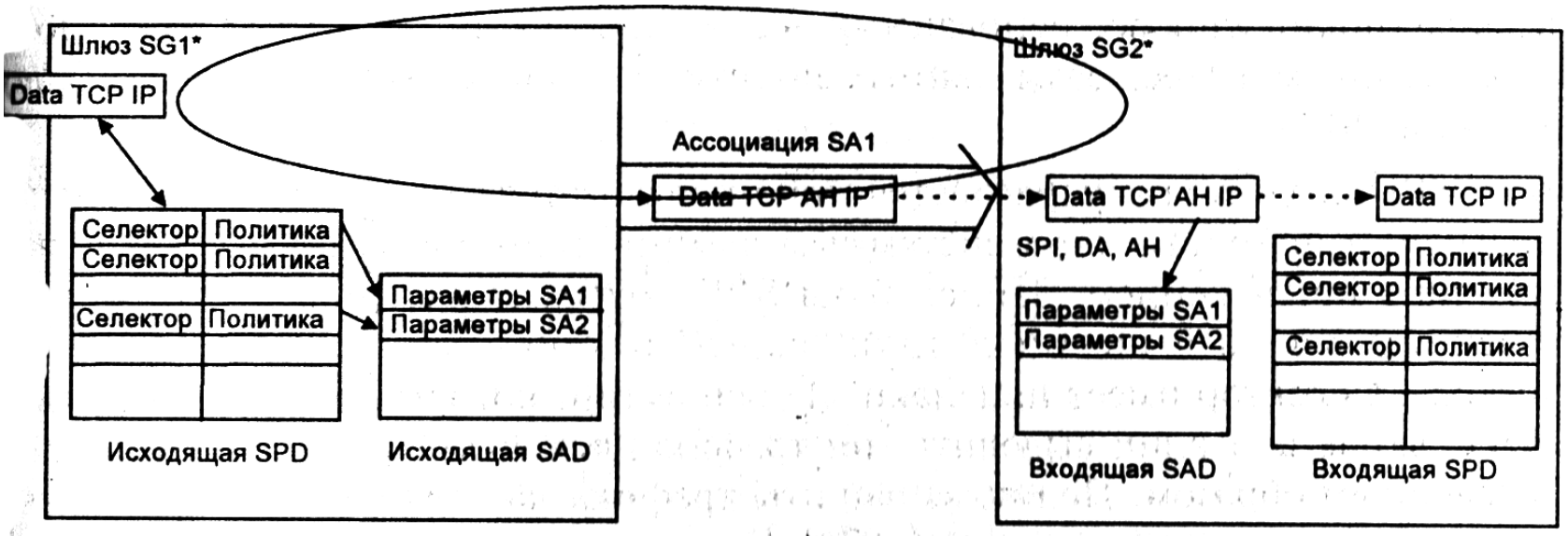
Пакет защищенный AH в туннельном режиме



Пакет защищенный ESP в туннельном режиме



База данных политик безопасности



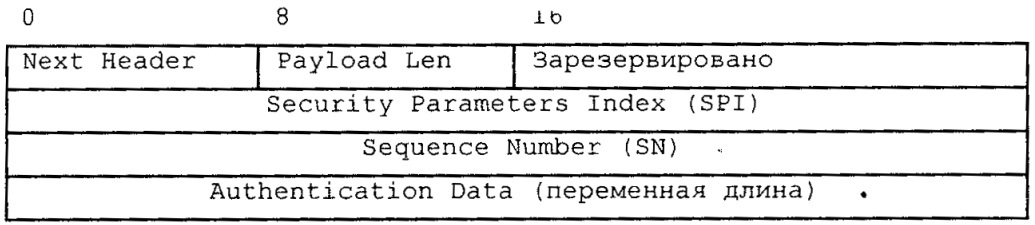
каждый узел/шлюз использует Security Policy Database (SPD)?

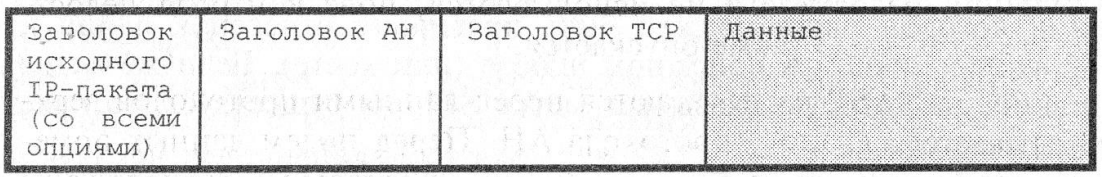
SPD создается локально, имеет 2 типа полей:

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

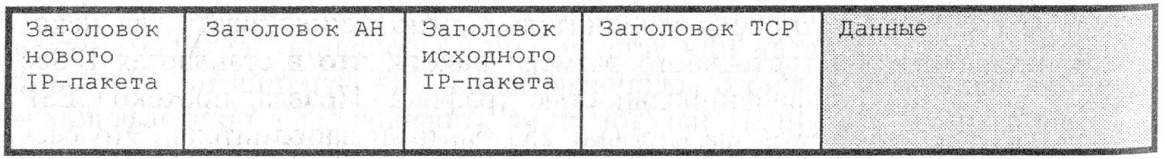
политика защиты пакета: пропустить, обработать, отвергнуть

Защита данных с помощью AH



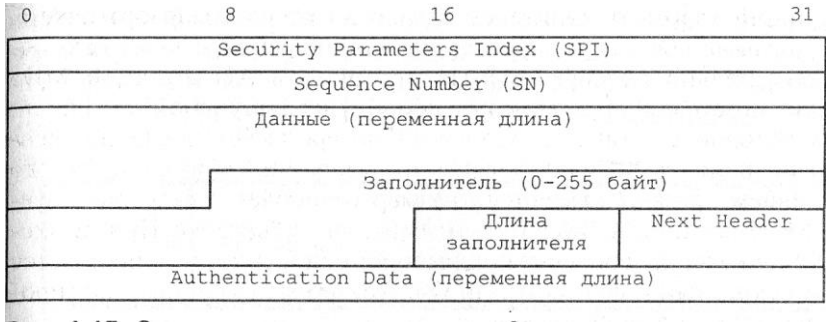


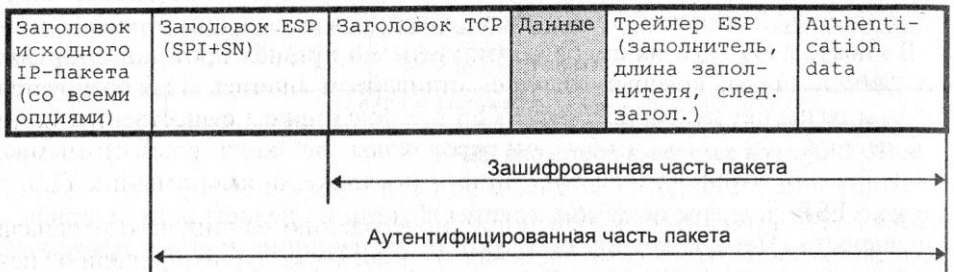
Аутентифицированная часть пакета (за исключением изменяющихся полей)

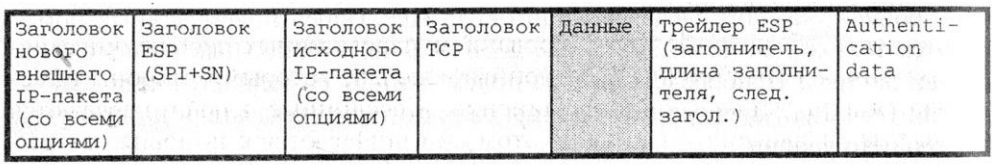


Аутентифицированная часть пакета (за исключением изменяющихся полей)

Защита данных с помощью ESP





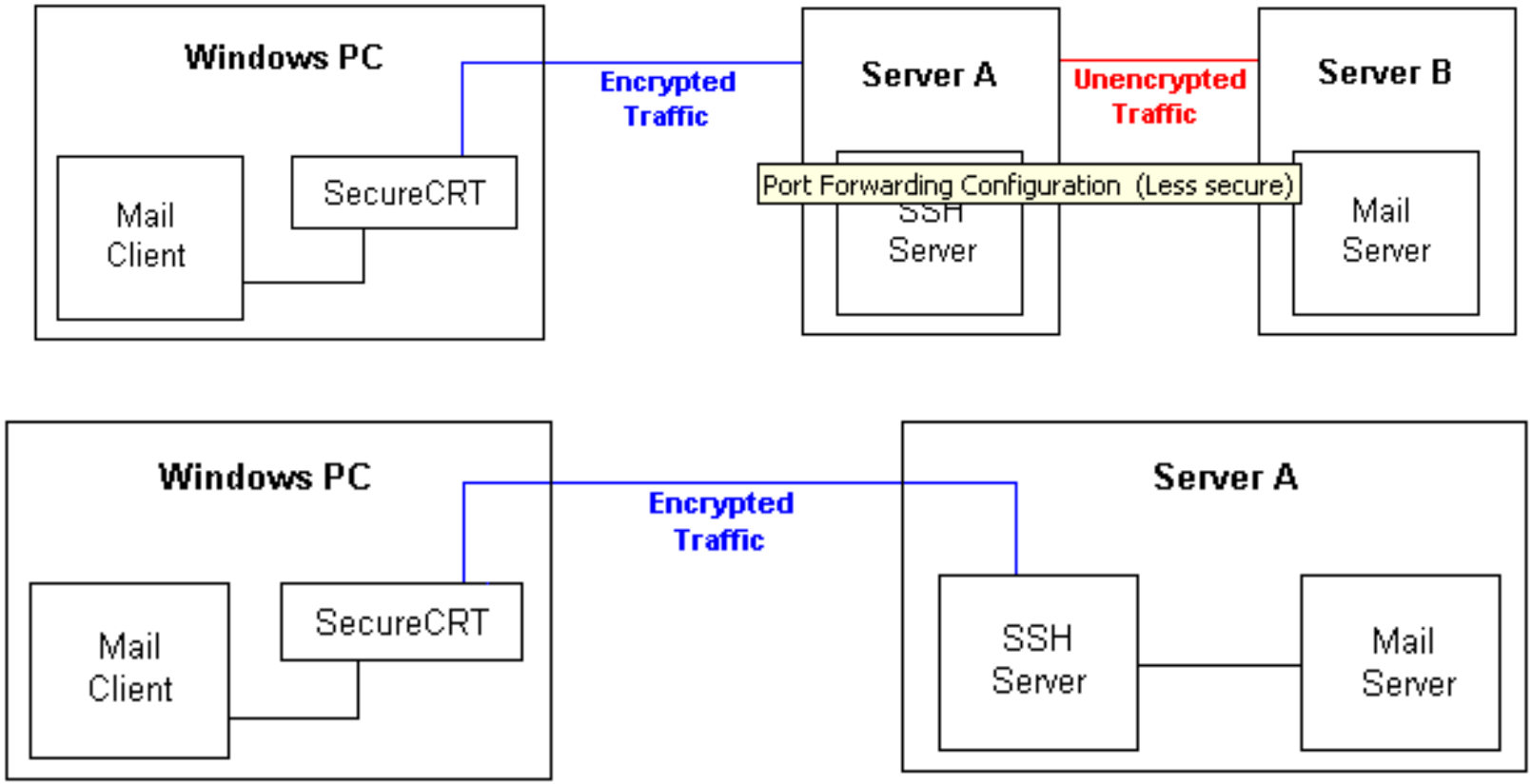


Защита на уровне представления

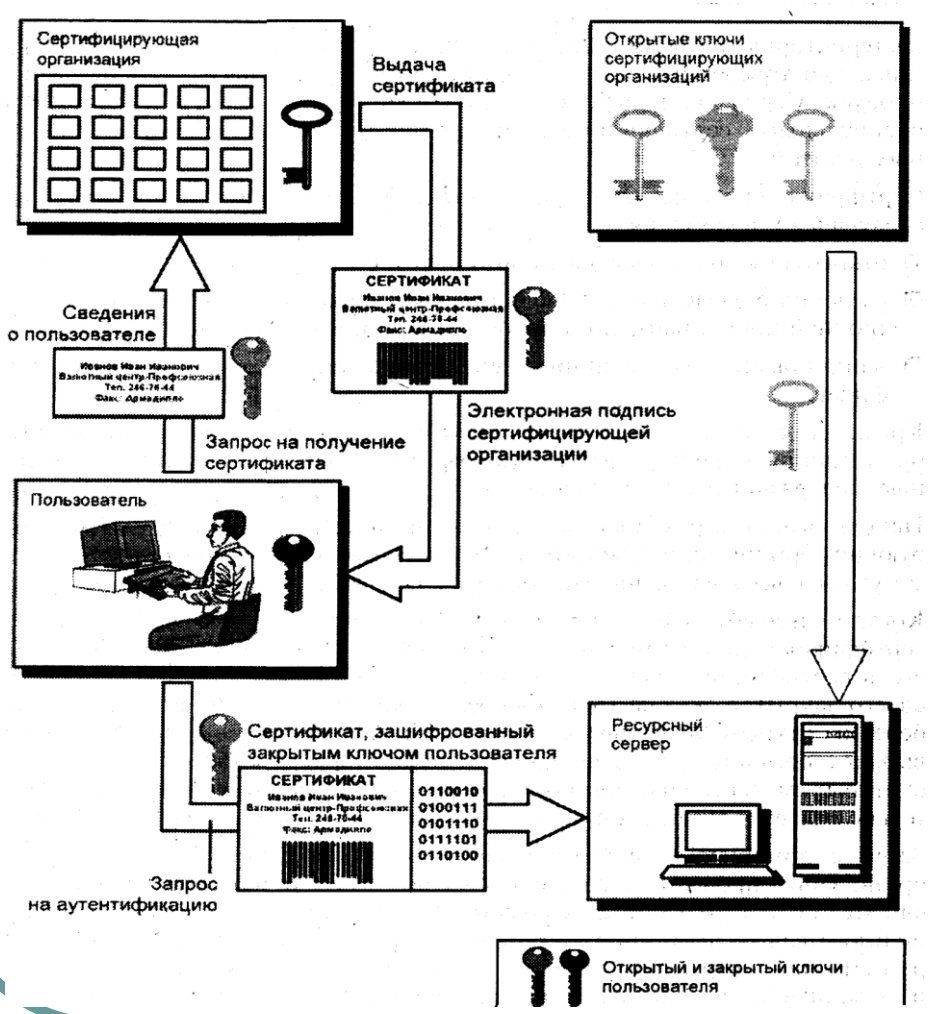
- Secure Socket Layer SSL (разработка фирмы Netscape)
- Transport Layer Security TLS (разработка комитета IETF)

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

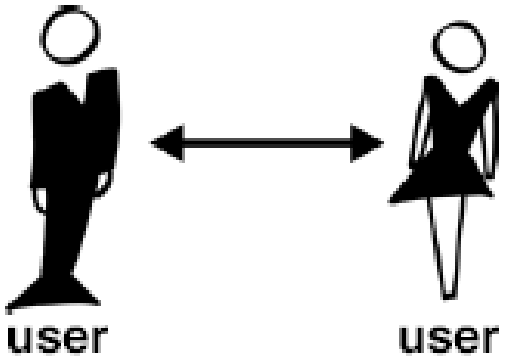
X.509v3 – стандарт ITU-T на формат сертификатов

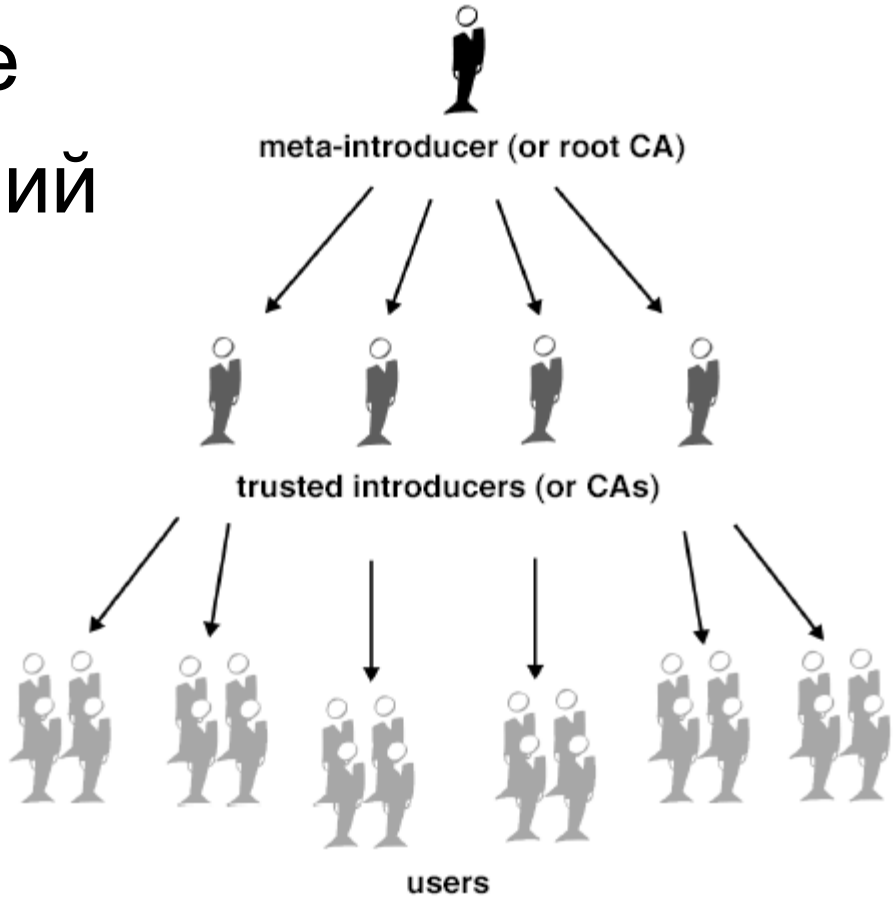
Инфраструктура открытых ключей

- 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.

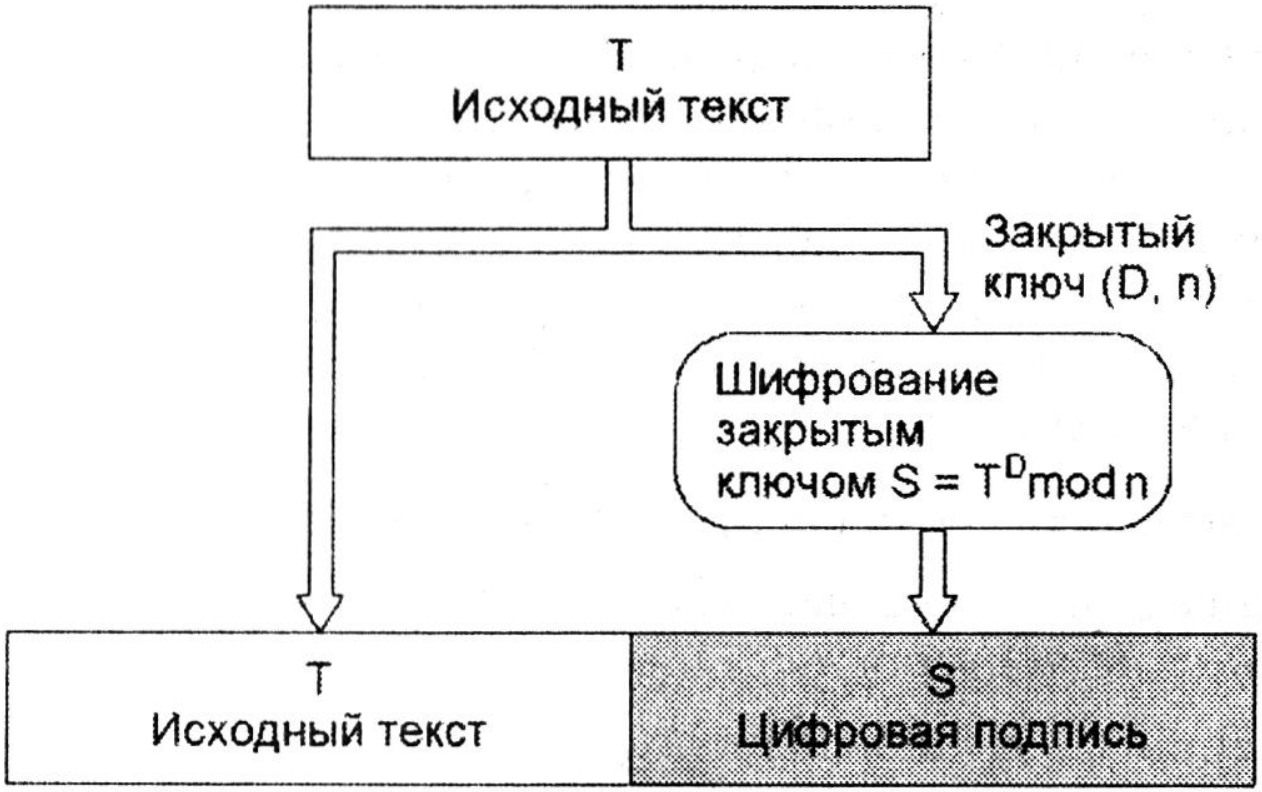
Модели доверия

- Прямое доверие
- Иерархия доверий
- Сеть доверий

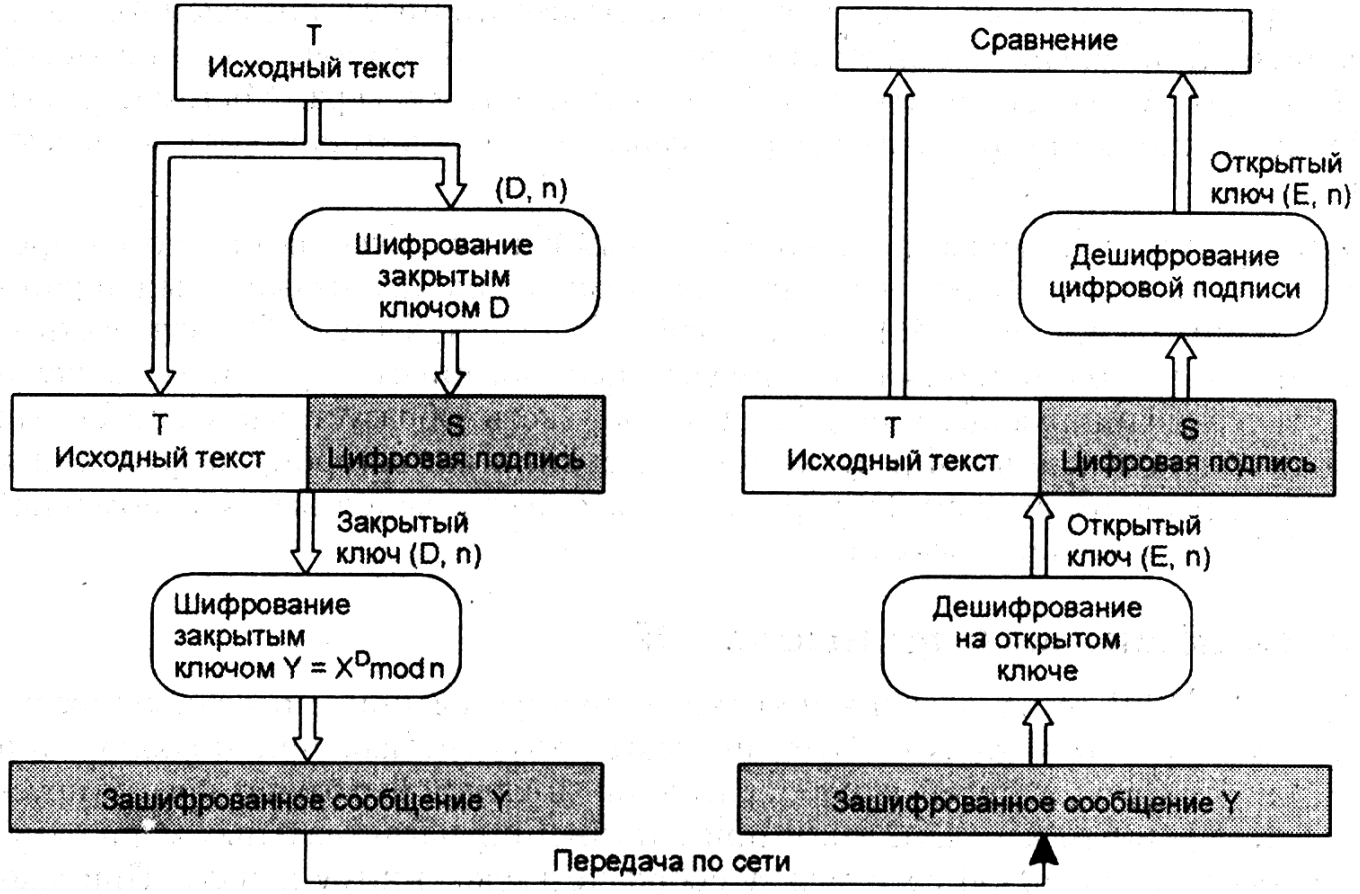




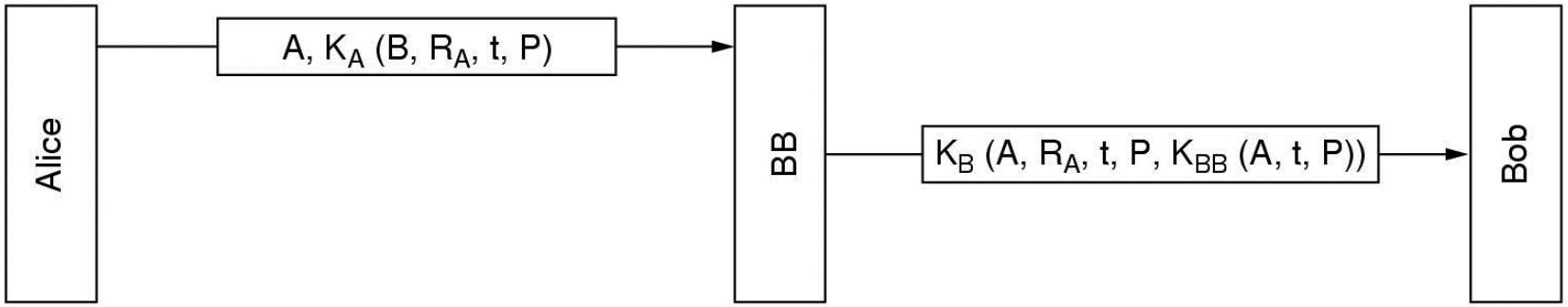
Цифровая подпись по RSA



Обеспечение конфиденциальности документов

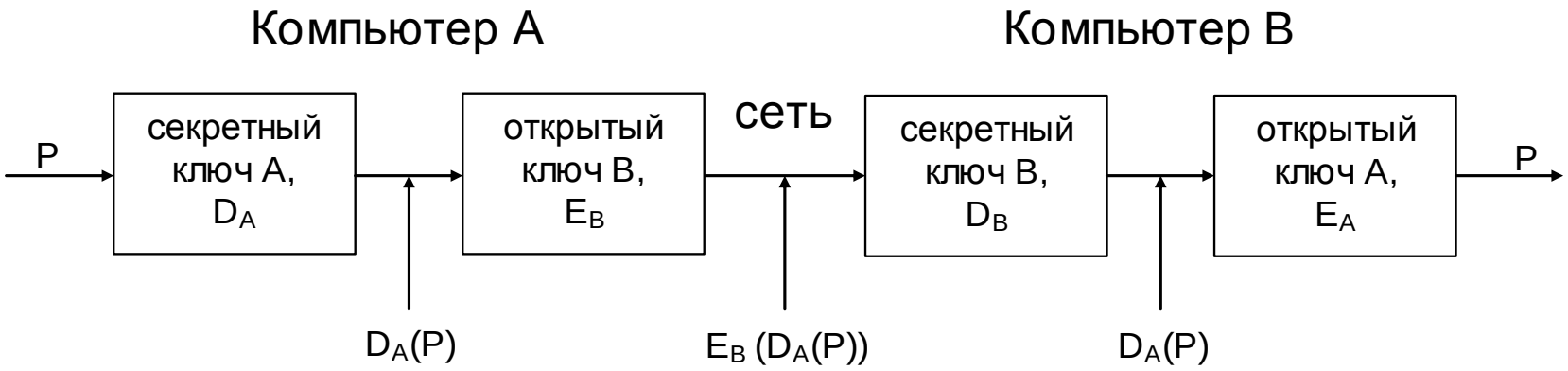


Подписи на основе секретного ключа



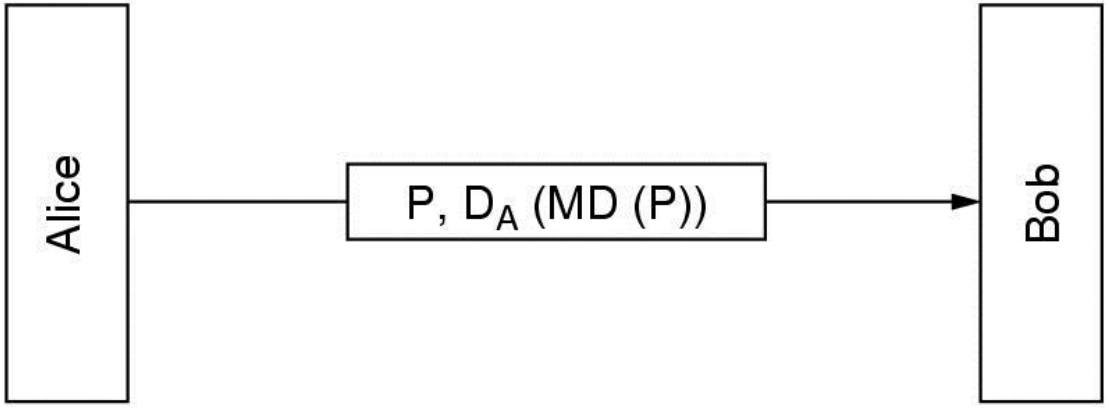
Примечание: BB – центр безусловного доверия

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

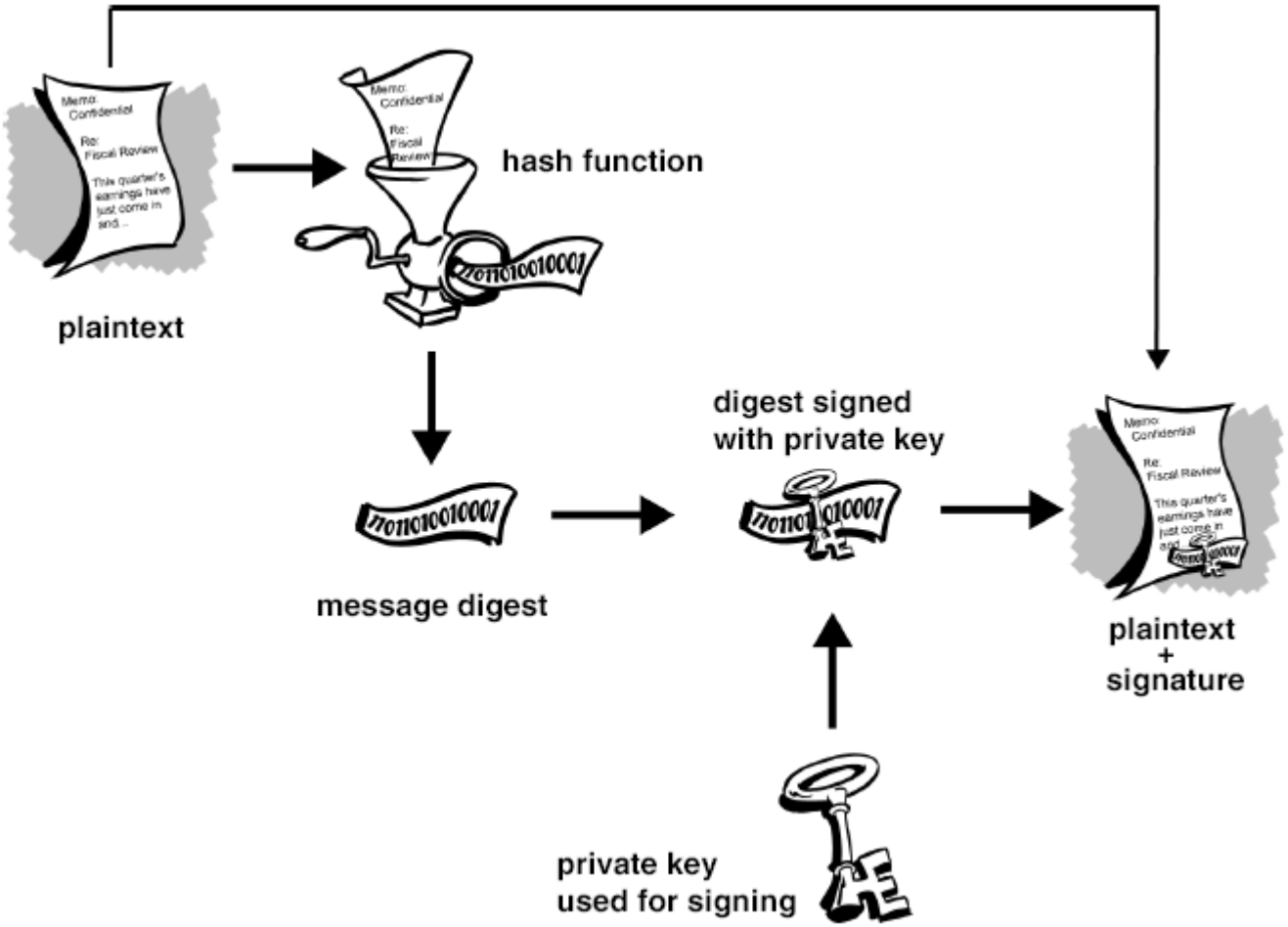


•SHA-1 (Secure Hash Algorithm) - современный алгоритм вычисления дайджеста сообщения. Разработан National Security Agency (NSA) для института стандартов США - National Institute of Standards and Technology (NIST).

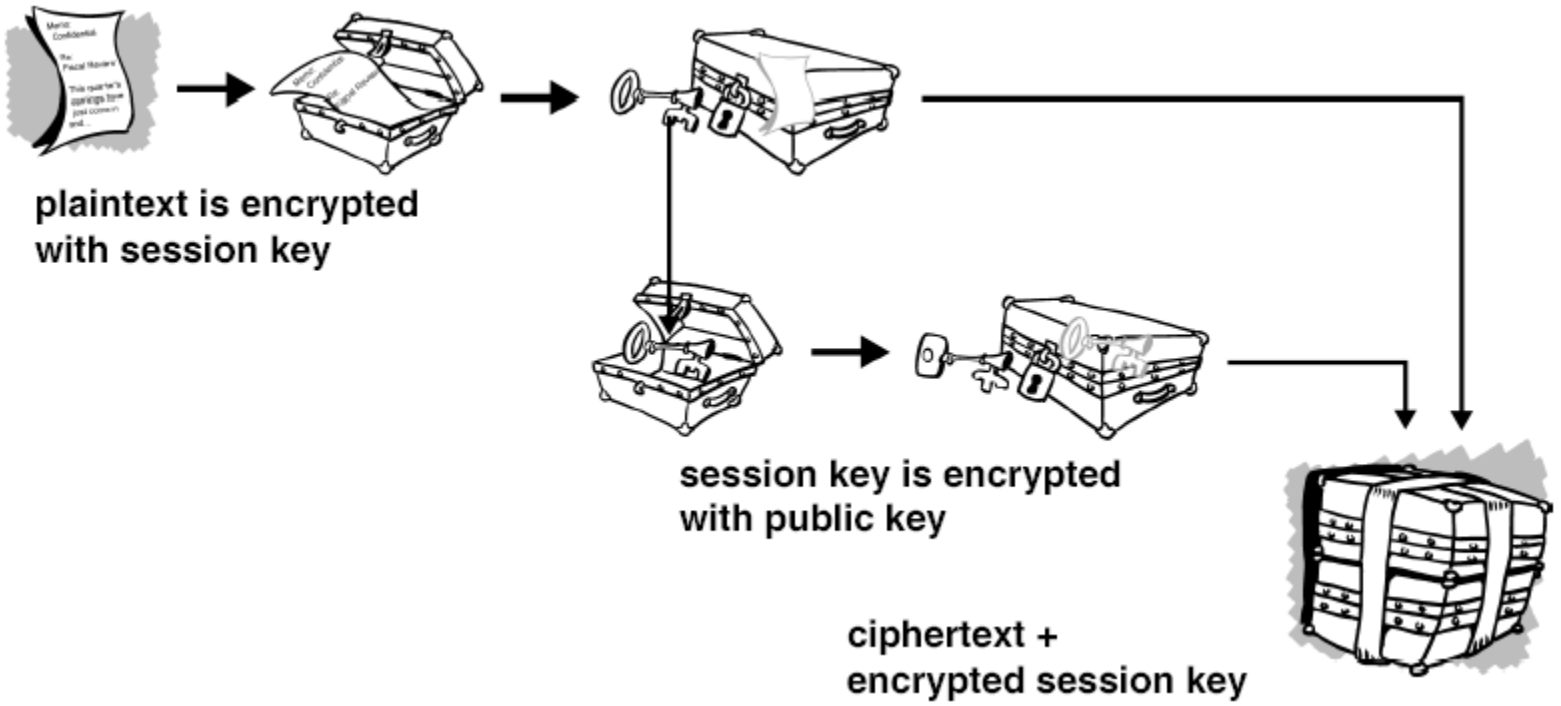
- •Используется в составе федерального стандарта США - DSS
- •Заменил MD5, уязвимость которого была обнаружена в 1996 году.

•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