Дисциплина «Технологии обеспечения информационной безопасности»

Лекция 6.1. «Технологии виртуальных частных сетей»

доцент кафедры КБ-4

кандидат педагогических наук, доцент

Пимонов Роман Владимирович

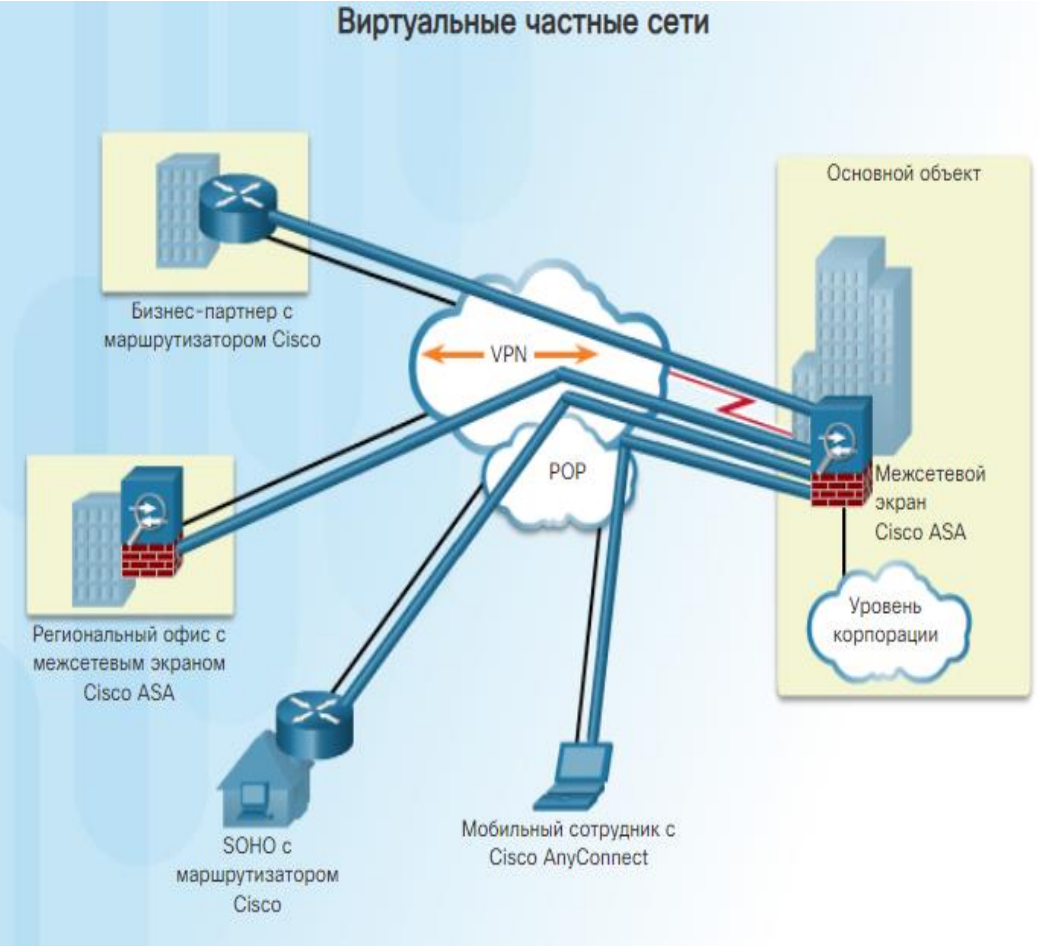
Внедрение системы предотвращения вторжений

Учебные вопросы:

1. Сети VPN.
2. Протокол IPSec.
3. Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Первый учебный вопрос.
Сети VPN.

Первый учебный вопрос.
Сети VPN.



VPN – это частная сеть, которая создана через сеть общего пользования, обычно через Интернет. Вместо применения выделенных физических подключений, в VPN используются виртуальные подключения, маршрутизируемые через Интернет из организации на удаленную площадку. Первыми сетями VPN фактически были обычные IP-туннели, в которых не выполнялись операции аутентификации или шифрования данных.

Первый учебный вопрос.
Сети VPN.

Преимущества сети VPN

Типы сетей VPN:

- Site-to-site (межузловые или межфилиальные)
- Remote access (удалённого доступа)

Второй учебный вопрос.
Протокол IPSec.

Технология IPsec

IPsec – это стандарт IETF (RFC 2401-2412), который определяет способ защиты сетей VPN в IP-сетях. Протокол IPsec обеспечивает защиту и аутентификацию IP-пакетов между источником и местом назначения. IPsec может защищать практически весь трафик от уровня 4 до уровня 7.

Основные функции обеспечения безопасности:

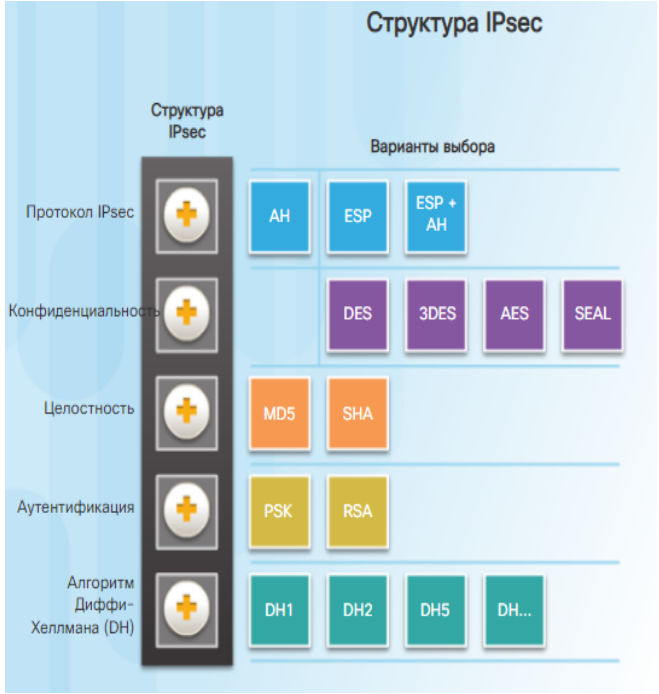
- конфиденциальность с помощью шифрования,
- целостность с помощью алгоритмов хеширования,
- аутентификация с помощью протокола Internet Key Exchange (IKE),
- безопасный обмен ключами с помощью алгоритма Диффи-Хеллмана (DH).

Второй учебный вопрос.
Протокол IPSec.

IPsec представляет собой структуру открытых стандартов, определяющую правила для организации защищённой связи.

Основные особенности протокола IPsec:

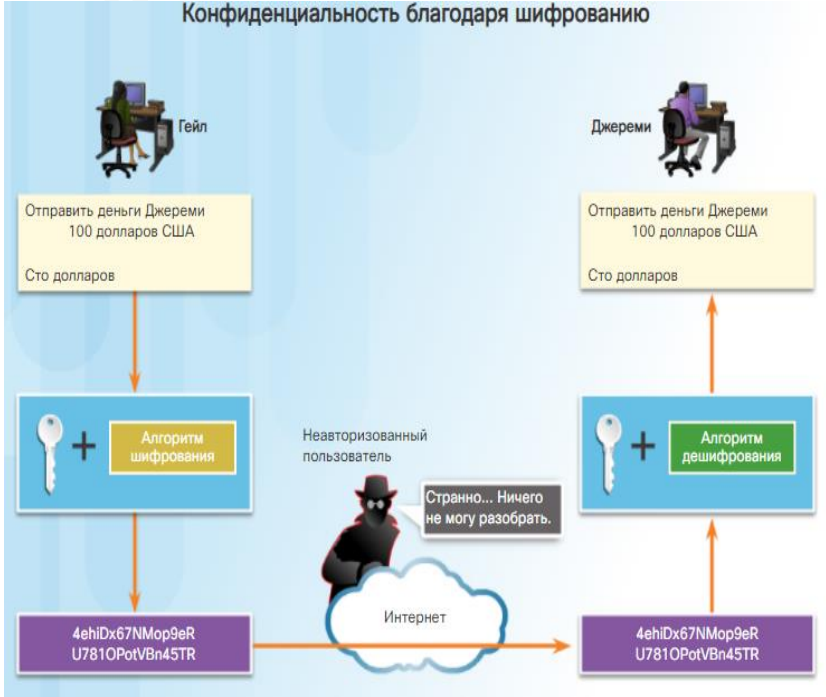
- IPsec – это структура открытых стандартов, независимая от алгоритмов.
- IPsec обеспечивает конфиденциальность и целостность данных, а также аутентификацию источника.
- IPsec действует как протокол сетевого уровня, защищая пакеты IP и проверяя их подлинность.



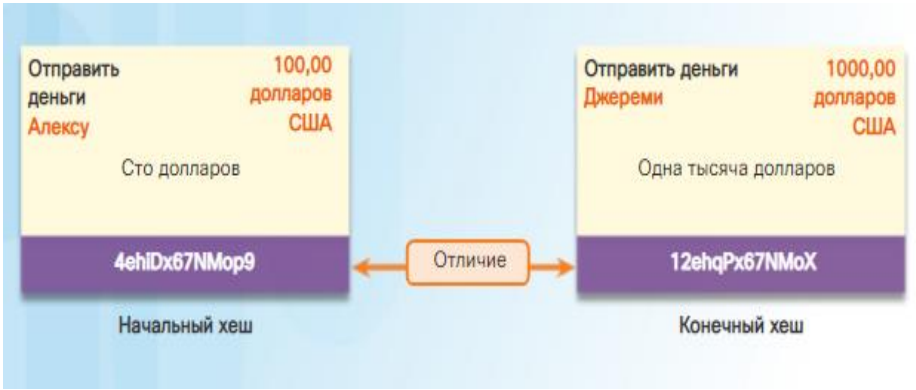
Второй учебный вопрос.
Протокол IPSec.

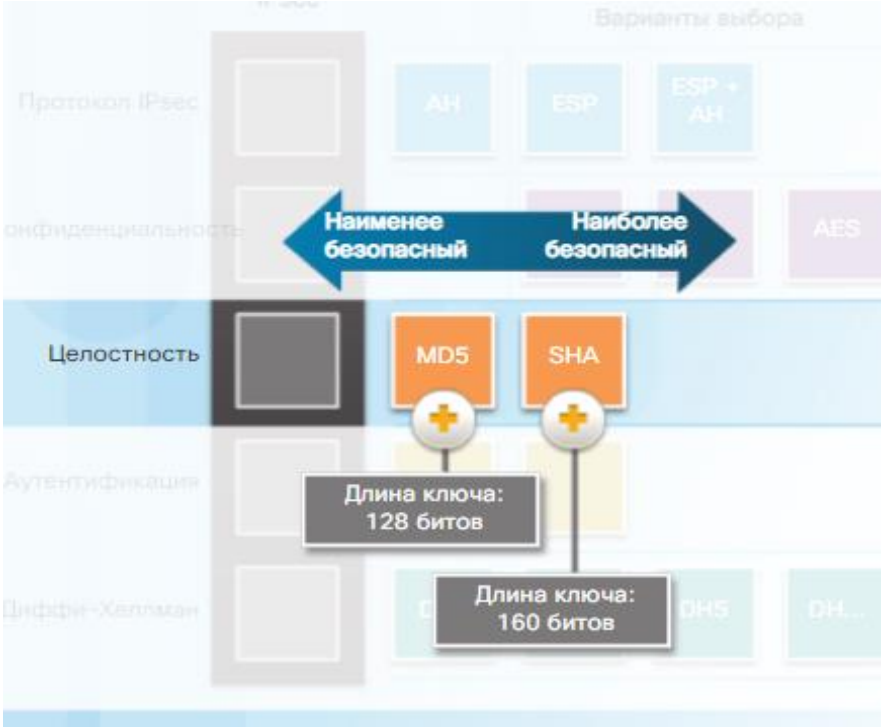
Сервисы безопасности IPsec:

1. Конфиденциальность (шифрование)



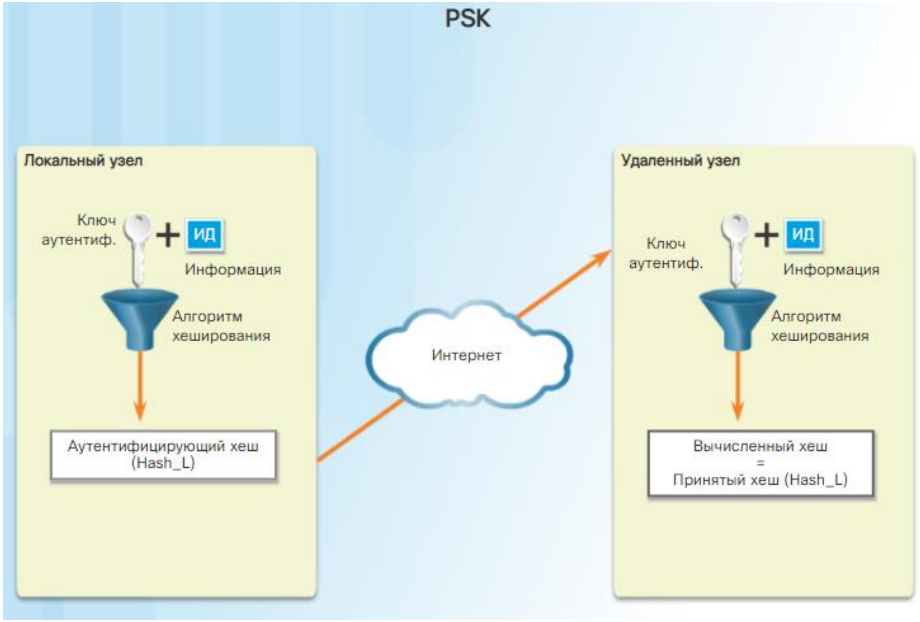
Сервисы безопасности IPsec:
2. Целостность данных

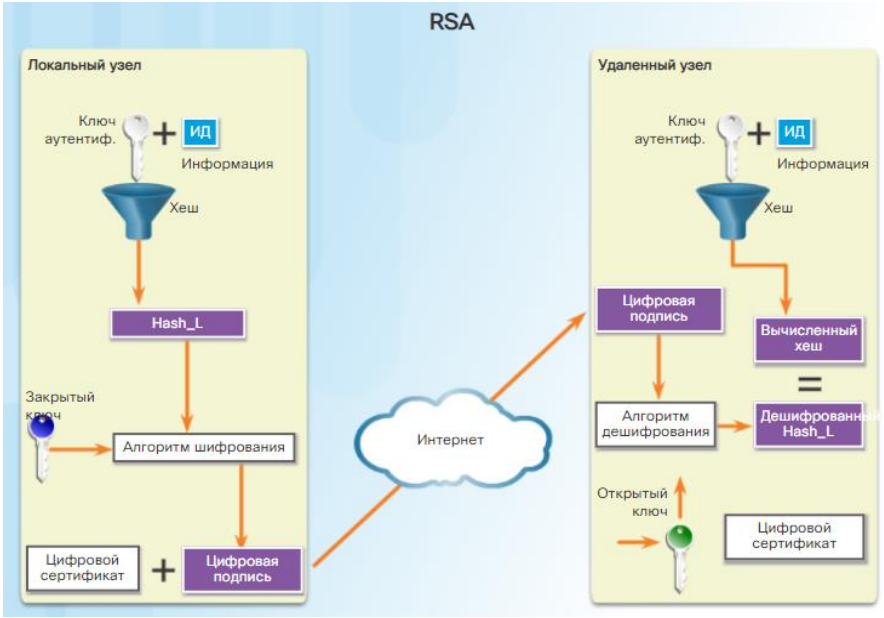




Сервисы безопасности IPsec:

3. Аутентификация





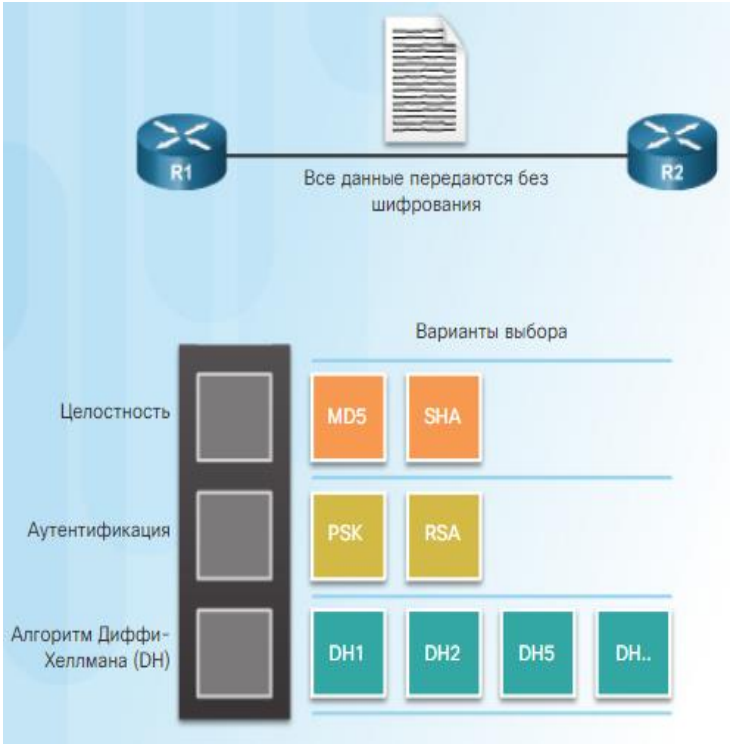
Сервисы безопасности IPsec:

4. Безопасный обмен ключами

- Группы DH 1, 2 и 5 поддерживают возведение в степень по простому модулю с размером ключа 768, 1024 и 1 536 битов соответственно. В настоящее время (после 2012 г.) эти группы использовать не рекомендуется.
- Группы DH 14, 15 и 16 используют ключи большего размера, а именно 2048, 3072 и 4096 битов соответственно, и рекомендуются для использования до 2030 г.
- Группы DH 19, 20, 21 и 24 с соответствующими размерами ключа 256, 384, 521 и 2048 битов поддерживают метод криптографии Elliptical Curve Cryptography (ECC), который уменьшает время, необходимое для генерирования ключей.
- Группа DH 24 является предпочтительным методом шифрования следующего поколения.

Набор протоколов IPsec

Аутентифицирующий заголовок (Authentication Header, AH) - AH обеспечивает подлинность путем применения однонаправленной функции хеширования на основе ключа к пакету для создания хеша или дайджеста сообщения. Хеш объединяется с текстом и передается в открытом виде.



Второй учебный вопрос.
Протокол IPSec.

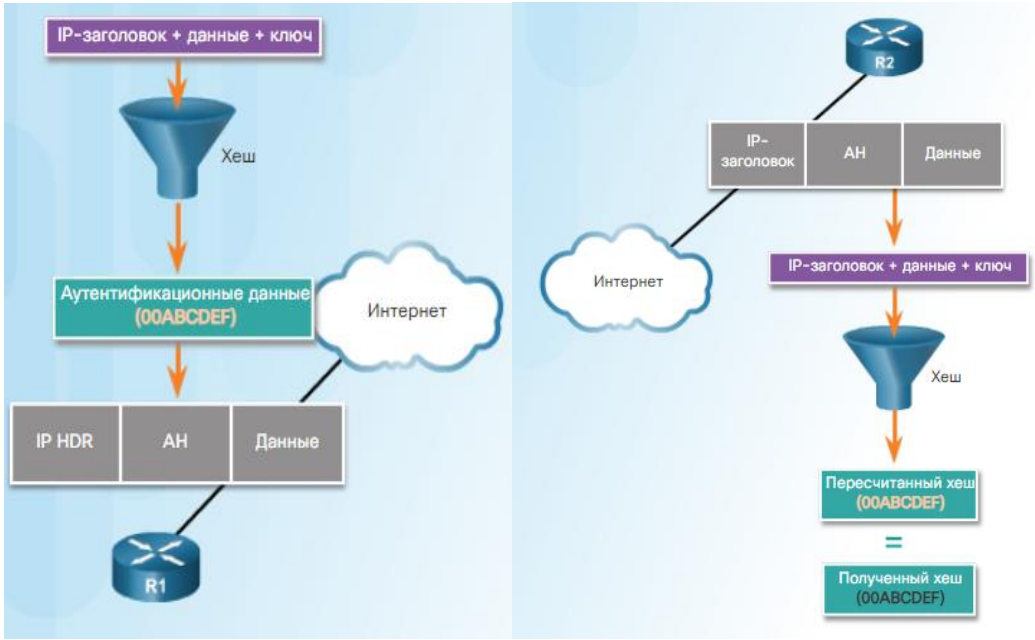
Аутентифицирующий заголовок (Authentication Header, AH)

Порядок выполнения процесса AH :

1. IP-заголовок и полезная нагрузка хешируются с помощью общего секретного ключа.
2. Хеш формирует новый заголовок AH, который вставляется в исходный пакет.
3. Новый пакет передается на маршрутизатор другого узла IPsec.
4. Другой маршрутизатор хеширует IP-заголовок и полезную нагрузку, используя общий секретный ключ, извлекает переданный хеш из заголовка AH и сравнивает два хеша.

Хеши должны полностью совпасть друг с другом.

- AH поддерживает алгоритмы MD5 и SHA.
- Процесс AH может не работать, если в среде используется NAT.



Набор протоколов Ipsec

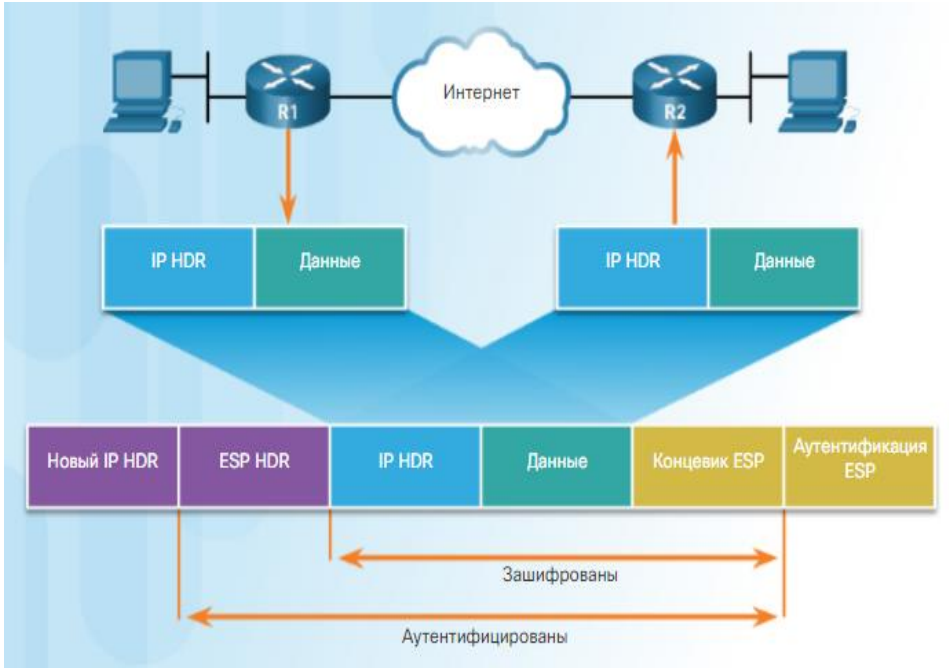
Протокол шифрования полезной нагрузки (Encapsulating Security Payload, ESP) – это протокол безопасности, который обеспечивает конфиденциальность и аутентификацию путем шифрования пакета IP.

В процессе шифрования пакета IP скрываются данные и идентификаторы источника и назначения.

В ESP проверяется подлинность внутреннего пакета IP и заголовка ESP.

Набор протоколов Ipsec

ESP позволяет защищать исходные данные, так как полностью шифруются исходная IP-датаграмма и концевик ESP. В случае аутентификации ESP шифрованные IP-датаграмма и концевик и заголовок ESP применяются в процессе хеширования. Затем новый IP-заголовок добавляется к аутентифицированной полезной нагрузке. Для маршрутизации пакета через Интернет используется новый IP-адрес.



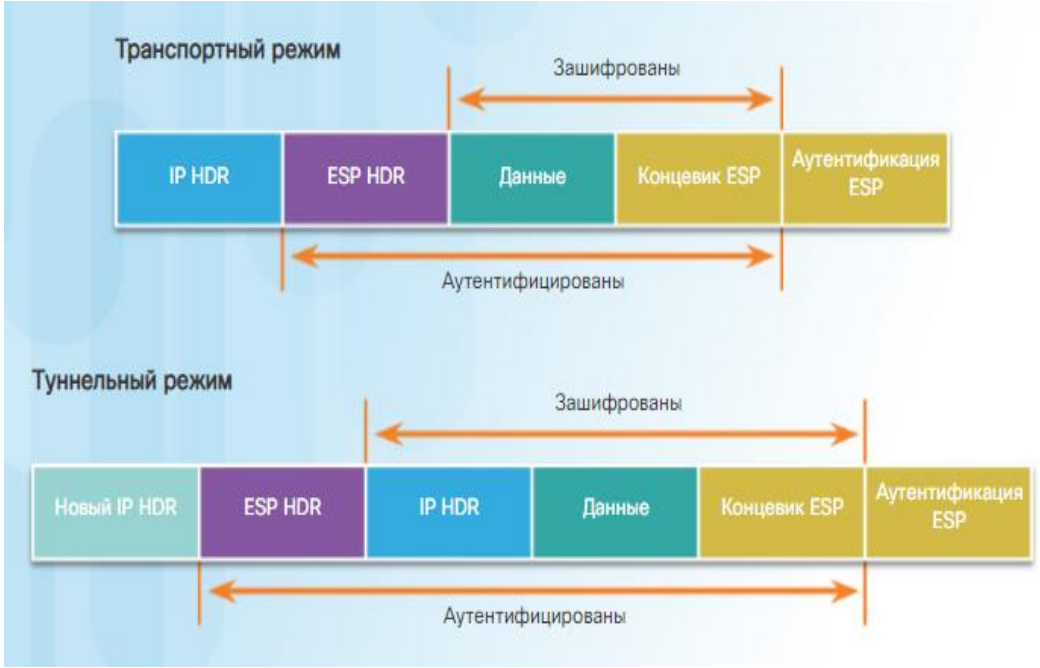
Режимы применения протокола ESP:

1. Транспортный режим

Безопасность обеспечивается только для транспортного уровня модели OSI и более высоких уровней. Транспортный режим защищает полезную нагрузку пакета, но оставляет исходный IP-адрес в открытом виде.

2. Туннельный режим

режим обеспечивает безопасность для всего исходного IP-пакета. Исходный IP-пакет шифруется, а затем инкапсулируется в другом IP-пакете. Такой метод называется шифрованием IP-в-IP.



Набор протоколов Ipsec - Протокол IKE

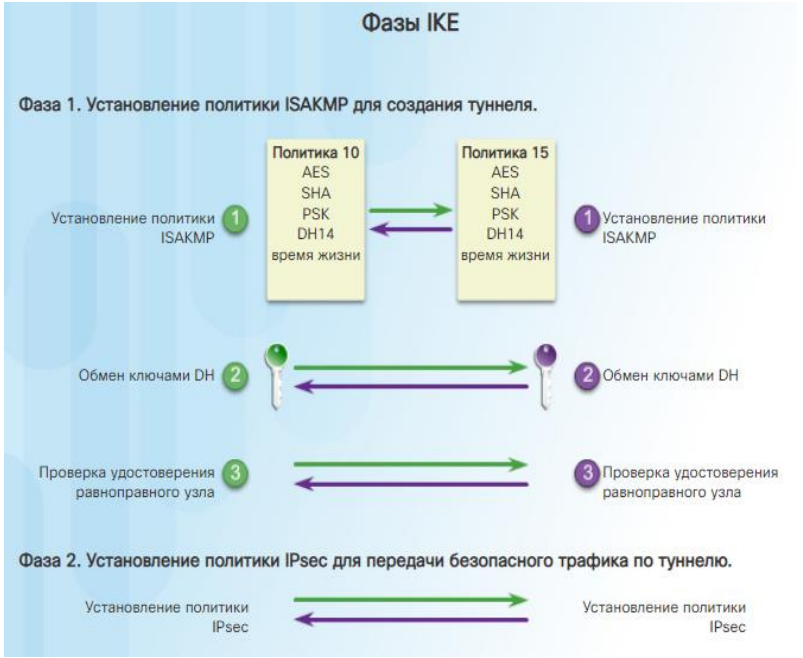
Протокол Internet Key Exchange (IKE) представляет собой стандарт протокола управления ключами. IKE используется вместе со стандартом IPsec. Для обмена информацией IKE между шлюзами безопасности протокол IKE использует UDP-порт 500.

Протокол IKE включает в себя две фазы:

1.Фаза 1 (Phase 1 - Main Mode). В этой фазе устанавливаются параметры безопасности для последующего обмена ключами. Происходит аутентификация сторон и установление общего секретного ключа (shared secret key), который будет использоваться для шифрования фазы 2.

2.Фаза 2 (Phase 2 - Quick Mode). После завершения фазы 1, в фазе 2 происходит установление параметров безопасности для сессии передачи данных, таких как шифрование, метод аутентификации, и др. В этой фазе создается защищенный туннель для безопасной передачи фактических данных между узлами.

Эти две фазы обеспечивают установку безопасного соединения и обмен ключами для последующей защищенной передачи данных через VPN (Virtual Private Network).



Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Протокол GRE

Обобщенная маршрутная инкапсуляция (Generic Routing Encapsulation, GRE) - один из примеров базового, незащищённого протокола создания туннелей для site-to-site VPN.

GRE предназначен для управления процессом передачи многопротокольного и группового IP-трафика между двумя и более площадками, между которыми связь может обеспечиваться только по IP. Он может инкапсулировать пакеты протоколов различного типа в IP-туннеле.

Сейчас GRE является стандартным методом инкапсуляции, описанным в стандартах IETF:
RFC 1701 и **RFC 2784** – основное назначение GRE.
RFC 1702 – описывает, как GRE может использоваться для транспорта L3 данных через IP сеть.
RFC 3147 – GRE через Connectionless Network Service (CLNS) networks.
RFC 4023 – описывает инкапсуляцию MPLS в GRE.

Протокол GRE

Мультипротокольная функциональность достигается добавлением дополнительного GRE заголовка между туннельным IP заголовком и инкапсулированными данными, как показано на схеме:

IP заголовок 20 байт	GRE заголовок 4 или больше байт	IP заголовок инкапсулированного IP пакета	TCP	DATA

Таким образом использование GRE создает дополнительные накладные расходы в размере 24 байт или больше – 20 байт IP заголовок и как минимум 4 байта GRE заголовок.

Формат заголовка GRE

бит	значение	Описание
0	Checksum Present	Если бит Checksum Present имеет значение 1, поле Checksum должно присутствовать в заголовке и содержать корректную информацию. Если установлен любой из битов Checksum Present или Routing Present, оба поля Checksum и Offset присутствуют в заголовке пакета GRE.
1	Routing Present	Если бит Routing Present имеет значение 1, это говорит о том, что поля Offset и Routing присутствуют в заголовке и содержат корректную информацию. Если установлен любой из битов Checksum Present или Routing Present, оба поля Checksum и Offset присутствуют в заголовке пакета GRE.
2	Key Present	Если бит Key Present имеет значение 1, это говорит о присутствии поля Key в заголовке GRE. В противном случае поле Key в заголовок GRE не включается.
3	Sequence Number Present	Если бит Sequence Number Present имеет значение 1, это говорит о присутствии поля Sequence Number. В противном случае поле Sequence Number в заголовок GRE не включается.

Формат заголовка GRE

4	**Strict Source Route**	**Значение бита Strict Source Route определено в других документах. Рекомендуется устанавливать для этого бита значение 1 только в тех случаях, когда вся маршрутная информация (Routing Information) состоит из маршрутов Strict Source Route**
5-7	Recursion Control	Поле Recursion Control содержит трехбитовое целое число без знака, указывающее допустимое количество дополнительных инкапсуляций. По умолчанию для этого поля следует устанавливать значение 0.
8-12	00000	зарезервированы
13-15	Version Number	Поле Version Number должно содержать значение 0. Другие значения этого поля выходят за пределы рассмотрения данного документа.
2 байта	Protocol Type	Поле Protocol Type указывает тип протокола во вложенном пакете. В общем случае это поле будет содержать значение поля типа протокола Ethernet для пакета. Определенные в настоящее время значения типов перечислены ниже. Дополнительные значения поля типа могут быть определены в других документах.

Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Формат заголовка GRE

2 байта	**Offset**	**Поле Offset показывает смещение в октетах от начала поля Routing до первого октета активной записи Source Route Entry, которая будет проверяться. Это поле присутствует в заголовке, если хотя бы один из битов Routing Present и Checksum Present имеет значение 1; поле содержит корректную информацию лишь при условии Routing Present = 1.**
2 байта	Checksum	Поле Checksum содержит контрольную сумму IP (дополнение до единицы) заголовка GRE и вложенного пакета. Это поле присутствует лишь в тех случаях, когда хотя бы один из битов Routing Present и Checksum Present имеет значение 1; поле содержит корректную информацию лишь при условии Checksum Present = 1.
4 байта	Key	Поле Key содержит 4-октетное число, которое включается при инкапсуляции. Это поле может использоваться получателем для аутентификации источника пакета. Методы такой аутентификации выходят за пределы настоящего документа. Поле Key присутствует в заголовке лишь при условии Key Present = 1.
4 байта	Sequence Number	Поле Sequence Number содержит 32-битовое целое число без знака, добавляемое при инкапсуляции. Это значение может использоваться получателем для отслеживания порядка передачи пакетов со стороны инкапсулятора. Точный алгоритм генерации значений поля Sequence Number и семантика порядковых номеров для получателя выходят за пределы настоящего документа.
--	Routing	Поле Routing является необязательным и присутствует лишь при условии Routing Present = 1. Поле Routing представляет собой список записей SRE (Source Route Entries)

Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

RFC 2784 Generic Routing Encapsulation (GRE)

1бит	12 бит	3 бита	16 бит
C	Reserved0	Ver	Protocol Type

16 бит	16 бит
Checksumm	Reserved1

Checksum Present (бит 0)
Если флаг Checksum Present (контрольная сумма присутствует) установлен, поля Checksum и Reserved1 присутствуют в заголовке и поле Checksum содержит корректную информацию.
Reserved0 (биты 1-12)
Получатель **должен** отбрасывать пакеты, в которых биты 1-5 отличны от нуля, если этот получатель не реализует RFC 1701. Биты 6-12 зарезервированы – они **должны** устанавливаться в 0 при передаче и игнорироваться на приеме.

Version Number (биты 13-15)
Поле номера версии **должно** иметь нулевое значение.
Protocol Type (2 октета)
Поле Protocol Type указывает тип протокола для вложенного пакета. **2.5. Checksum (2 октета)**
Поле Checksum содержит контрольную сумму IP (дополнение до единицы) для всех 16-битовых слов заголовка GRE и вложенного пакета. При расчете контрольной суммы значение данного поля принимается нулевым. Это поле присутствует только при установленном флаге Checksum Present.
Reserved1 (2 октета)
Поле Reserved1 зарезервировано и при его наличии **должно** содержать нулевое значение. Поле Reserved1 присутствует только при наличии поля контрольной суммы (т. е., при установленном флаге Checksum Present).

Последовательность настройки туннеля GRE

Шаг 1. Создать интерфейс туннеля
Шаг 2. Указать IP-адрес источника туннеля.
Шаг 3. Указать IP-адрес назначения туннеля.
Шаг 4. Указать IP-адрес для интерфейса туннеля.
Шаг 5. (Дополнительно) Указать на интерфейсе туннеля в качестве используемого режима режим GRE. Режим GRE является режимом по умолчанию для интерфейса туннеля в программном обеспечении Cisco IOS.

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Протокол туннелирования точка-точка (Point-to-Point Tunneling Protocol) – предназначен для создания защищённых виртуальных каналов при доступе удалённых пользователей к локальным сетям и для безопасной передачи данных между ними.

Протокол PPTP предполагает создание криптозащищённого туннеля на канальном уровне ЭМВОС в ДВУХ вариантах:

1) при прямом соединении удалённого компьютера с сетью,

2) при подсоединении его к сети по телефонной линии через провайдера.

PPTP работает, устанавливая обычную PPP сессию с противоположной стороной с помощью протокола GRE. Второе соединение на TCP-порту 1723 используется для инициации и управления GRE-соединением.

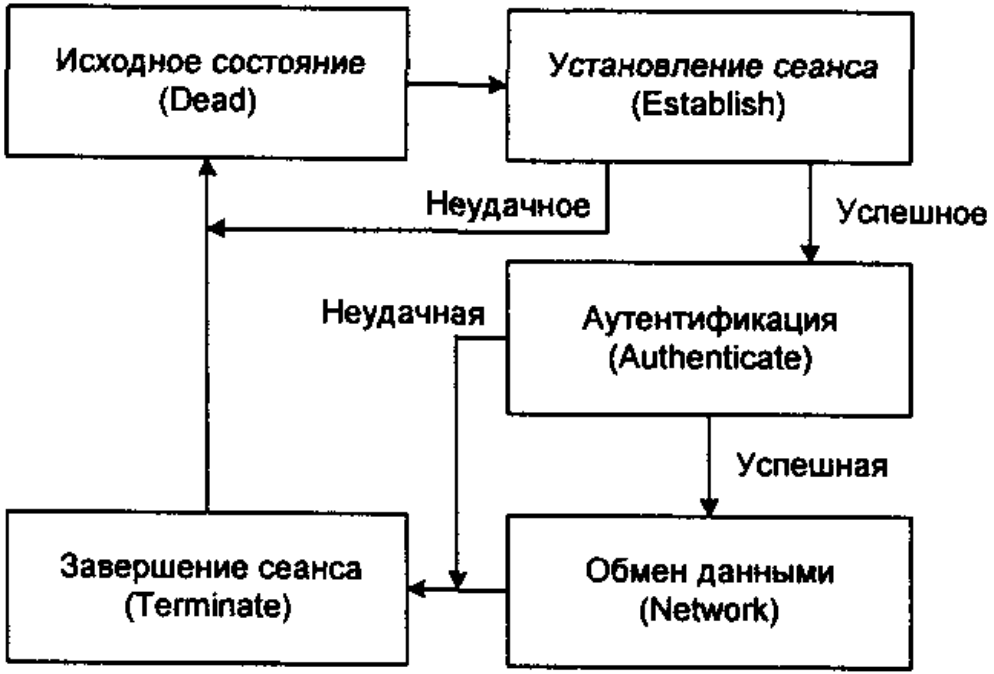
Структура кадров PPTP

Заголовок кадра передачи	IP-заголовок	GRE-заголовок	PPP-заголовок	Зашифрованные данные PPP	Окончание кадра передачи

Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

В основе обмена данными по протоколу PPTP лежит управляющее соединение PPTP — последовательность управляющих сообщений, которые устанавливают и обслуживают туннель.

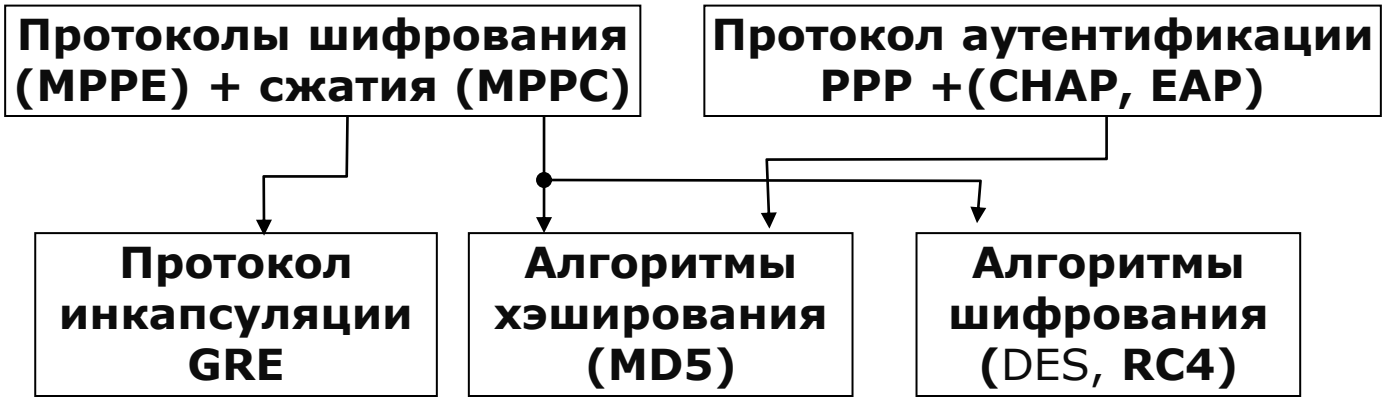
Управляющее сообщение	Функция
Start-Control-Connection-Request	Запрос на установление управляющего соединения
Start-Control-Connection-Replay	Ответ на сообщение Start-Control-Connection-Request
Echo-Request	Сообщение "Keep-alive" ("все живы") для управляющего соединения
Echo-Replay	Ответ на сообщение Echo-Request
Set-Link-Info	Посылается сервером сети для задания PPP-параметров переговоров
Stop-Control-Connection-Request	Команда завершить управляющее соединение
Stop-Control-Connection-Replay	Ответ на сообщение Stop-Control-Connection-Request



Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Для шифрования данных при организации туннеля по протоколу PPTP применяется протокол MPPE – Microsoft Point-to-Point Encryption с длиной ключа 40, 56 или 128 бит

Протокол GRE (Generic Routing Encapsulation) используется для управления данными, передаваемыми в инкапсулированных дейтаграммах, и контроля плотности потока.



Плюсы:

- клиент PPTP встроен почти во все операционные системы
- очень прост в настройке
- работает быстро

Недостатки протокола PPTP:

1. Протокол считается менее безопасным, чем IPSec.
2. PPTP сложно перенаправлять за сетевой экран, так как он требует одновременного установления двух сетевых сессий.

Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Протокол L2TP (Layer-2 Tunneling Protocol) [RFC 2661] – протокол туннелирования второго уровня.

Протокол L2TP предназначен:
- для согласования адресов сеанса, а также параметров шифрования и сжатия данных работает на канальном уровне ЭМВОС;
- в качестве транспортного протокола L2TP использует протокол UDP, что позволяет передавать данные по сетям IP, Frame Relay, X.25 и ATM;
- в качестве порта отправителя и получателя протокол L2TP использует UDP-порт 1701.

Типы сообщений протокола L2TP:
- Управляющие - пересылаются по надёжно защищённым каналам;
- Данные – пересылаться как по защищённым так и по открытым каналам.

Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Сокращения

LAN — локальные сети, к которым подключаются через L2TP;

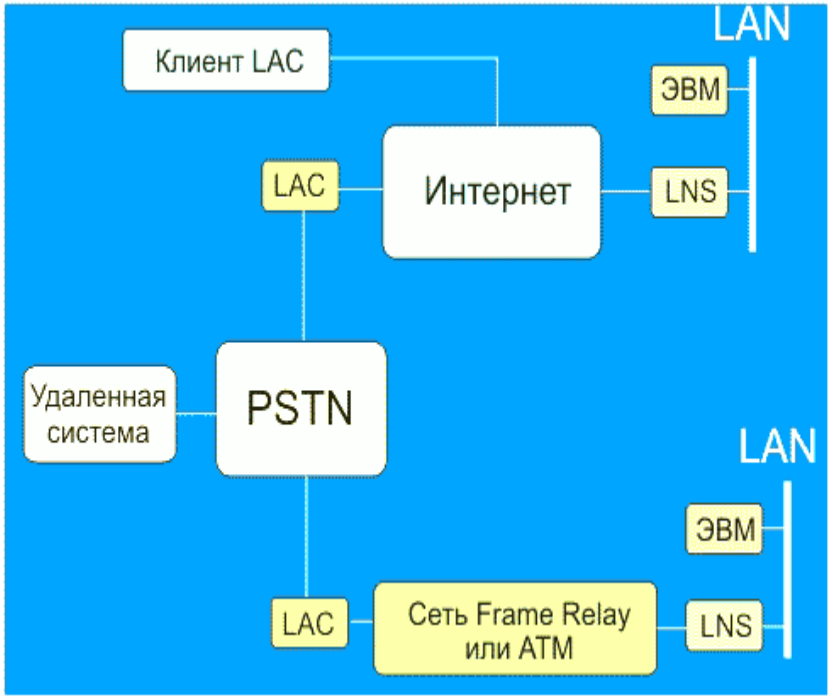
ЭВМ — компьютер(ы), подключённые к локальной сети напрямую

LNS — L2TP Network Server, сервер доступа к локальной сети по L2TP;

LAC — L2TP Access Concentrator, устройство для прозрачного подключения своих пользователей к LNS через сеть той или иной архитектуры;

Удалённая система — система, желающая подключиться к LAN через L2TP;

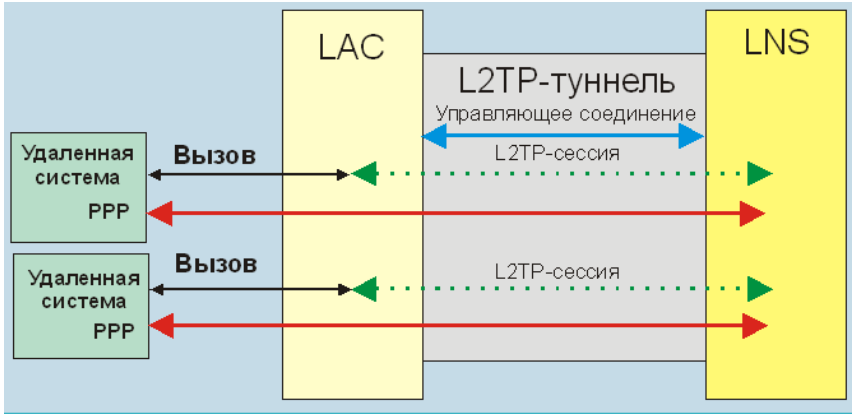
Клиент LAC — ЭВМ, которая сама для себя исполняет роль LAC для подключения к LNS;



Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Процедура установления PPP-сессии туннелирования L2TP включает в себя два этапа:

1. Установление управляющего канала для туннеля,
2. Формирование сессии в соответствии с запросом входящего или исходящего вызова.



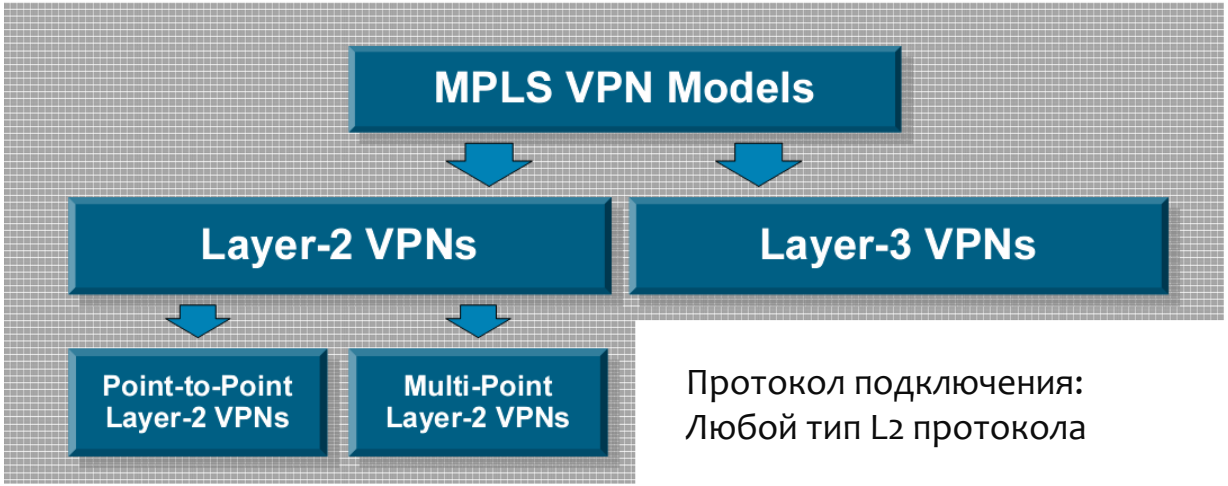
Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Недостатки протокола L2TP :

- для реализации протокола L2TP необходима поддержка провайдеров ISP;
- протокол L2TP ограничивает трафик рамками выбранного туннеля и лишает пользователей доступа к другим сегментам сети Internet;
- предложенная спецификация L2TP обеспечивает стандартное шифрование только в IP-сетях с помощью протокола IPSec.

Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Разновидности MPLS VPN



Протокол подключения:
Frame relay, ATM, Ethernet

Тип соединения:
Точка-точка

Маршрутизация:
Оборудование пользователя

Протокол подключения:
Ethernet

Тип соединения:
Точка-точка,
Многоточечное

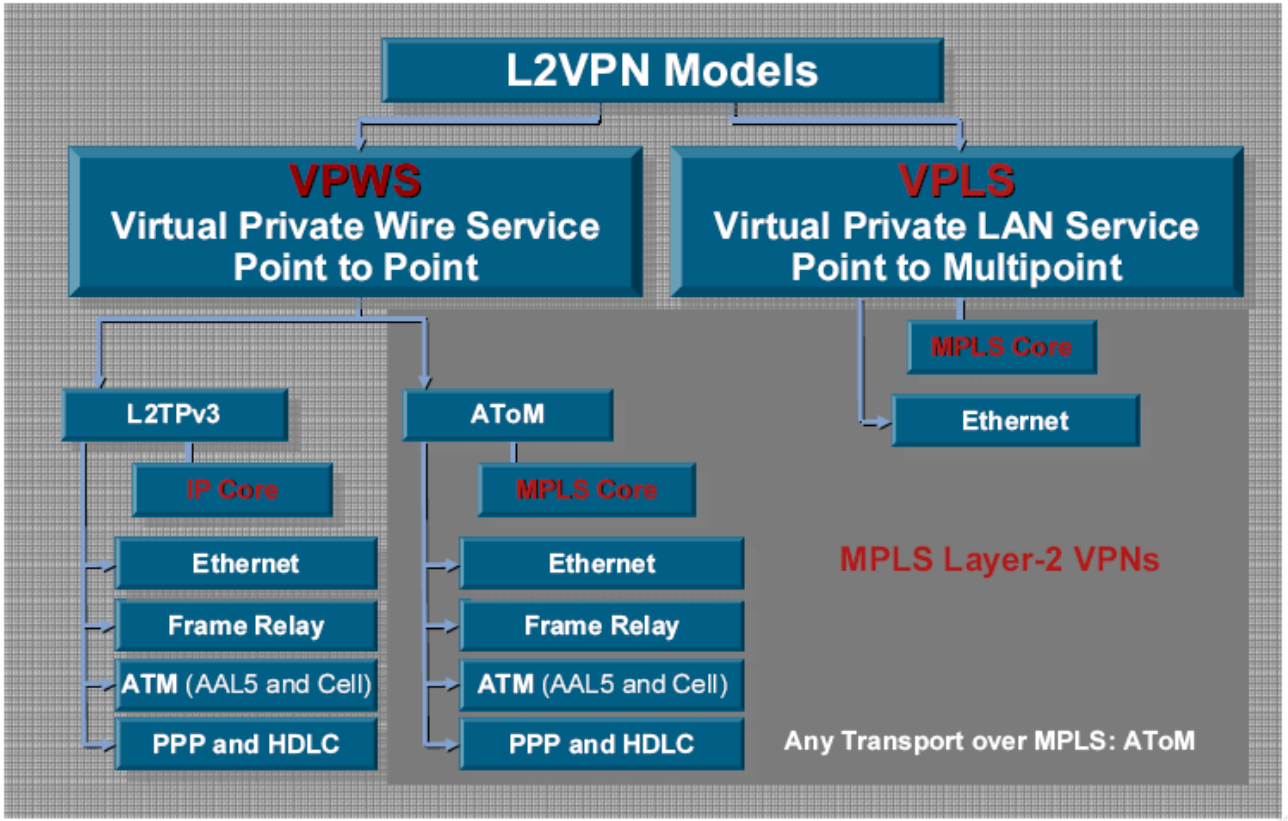
Маршрутизация:
Оборудование пользователя

Протокол подключения:
Любой тип L2 протокола

Тип соединения:
Точка-точка, многоточечное

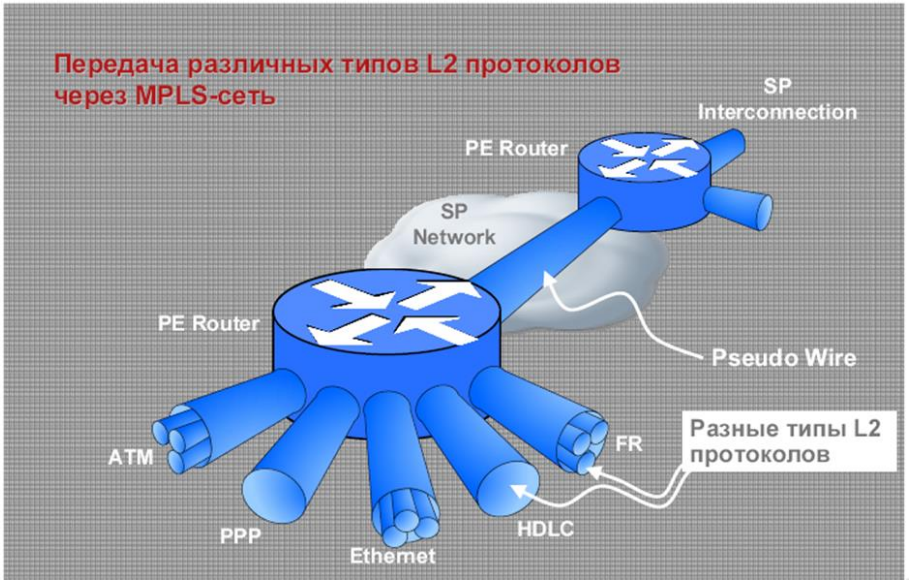
Маршрутизация:
Статическая маршрутизация;
Динамическая маршрутизация;
Оборудование провайдера участвует в маршрутизации данных пользователя

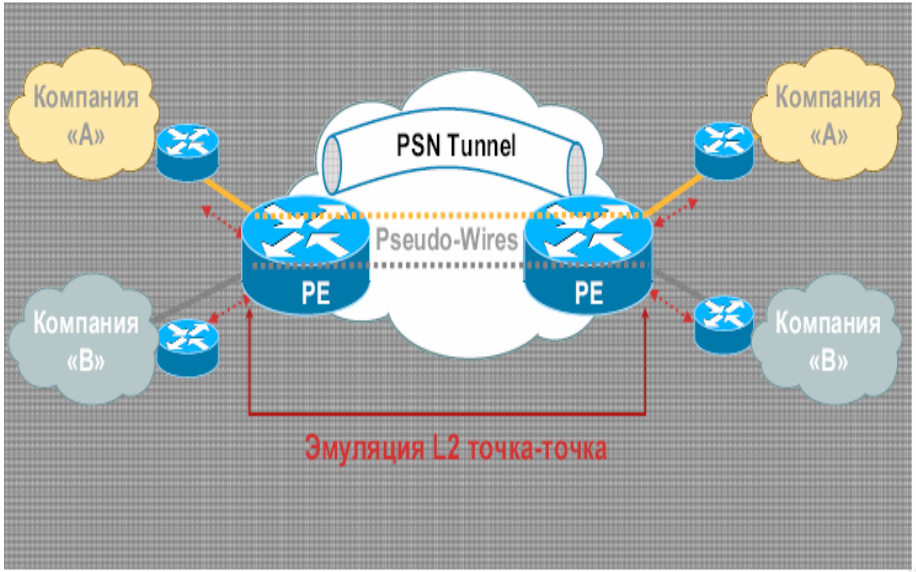
Существующие разновидности L2VPN



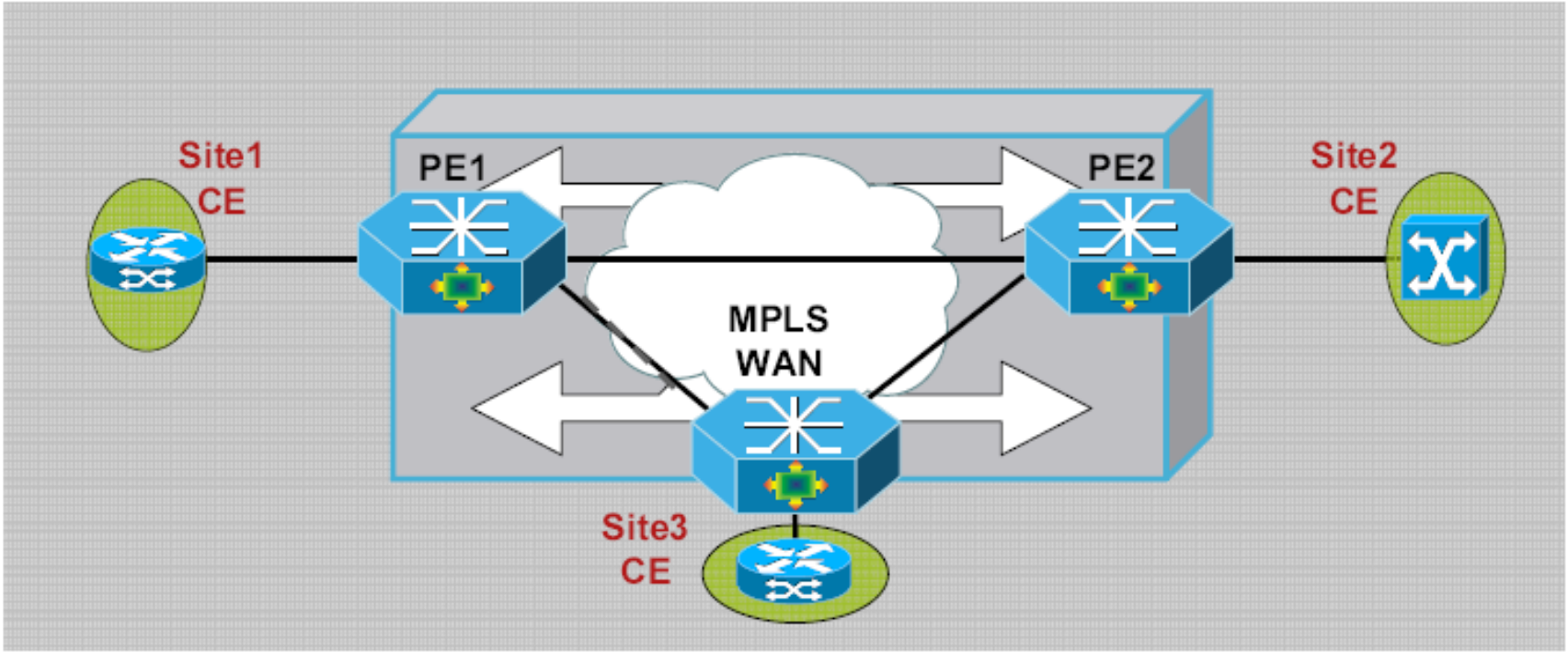
Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Технология Layer-2 VPN



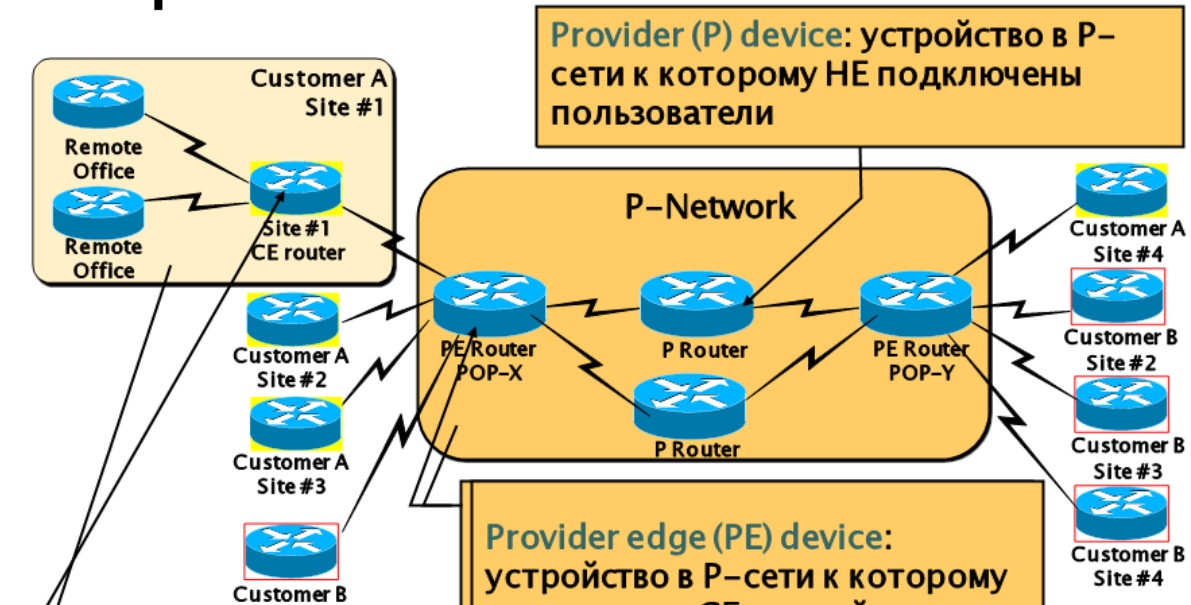


Технология Virtual Private LAN Service



Третий учебный вопрос.
Протоколы GRE, PPTP, L2TP, VPN на основе MPLS.

Терминология



- VPN – Виртуальная частная сеть

Дисциплина «Технологии обеспечения информационной безопасности»

Лекция 6.1. «Технологии виртуальных частных сетей»

доцент кафедры КБ-4

кандидат педагогических наук, доцент

Пимонов Роман Владимирович