электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 621.391

Обеспечение информационной безопасности услуги виртуальной частной сети VPLS на участке между граничными маршрутизаторами пользователей

Тепикин А.П., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Тарабрина О.В., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Бельфер Р.А. доцент, к.т.н., с.н.с.
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана.
bauman@bmstu.ru

Введение. Сети связи разделяются на локальные и глобальные. Локальные сети *LAN* (*Local Area Network*) - это объединение компьютеров, расположенных на небольшом расстоянии друг от друга в радиусе до нескольких километров или в некоторых случаях десятков километров. Глобальные сети *WAN* (*Wide Area Network*) объединяют территориально расположенные компьютеры, находящиеся на большом расстоянии, возможно в различных городах и странах.

Классическая технология *Ethernet* до недавнего времени применялась только в локальных сетях. Успех технологии *Ethernet* в *LAN*, где она вытеснила все остальные технологии, привел ее к идее использования в глобальных сетях. Одним из наиболее распространенных способов объединения нескольких территориально распределенных в разных местах *LAN Ethernet* является сеть многопротокольной коммутация по меткам *MPLS* (*Multiple Protocol Label Switching*) [1,2,3], выполняющая функцию транзитной сети связи. При этом создается услуга виртуальной частной локальной сети *VPLS* (*Virtual Private LAN Service*), которая объединяет вместе несколько дистанционно разбросанных *LAN*, превращая их в единую *LAN*, при которой доставка трафика от пользователя до граничного маршрутизатора *MPLS* осуществляется с помощью кадра *Ethernet*. Сервисы виртуальных частных сетей второго уровня (*VPLS*) описаны в спецификациях *RFC* 4761 [4] и *RFC* 4762 [5] в зависимости от протокола создания пути (*LDP* или *BGP*). Настоящая

работа посвящена обеспечению информационной безопасности *VPLS* и состоит из трех разделов:

1. Основные положения функционирования *MPLS* в создании услуги *VPLS* и угрозы ИБ на участке *CE-CE*.
2. Защита информационной безопасности *VPLS* с помощью туннелирования.
3. Обеспечение информационной безопасности *VPLS* с помощью шифрования.

1. Основные положения функционирования *MPLS* в создании услуги *VPLS* и угрозы ИБ на участке *CE-CE*

1.1. Основные положения функционирования сети *MPLS*. На рисунке 1 приведён пример общей модели услуги *VPLS*, состоящей из трёх услуг *VPLS*: *A*, *B*, *C* (т.е. из трех виртуальных частных сетей *VPN*).

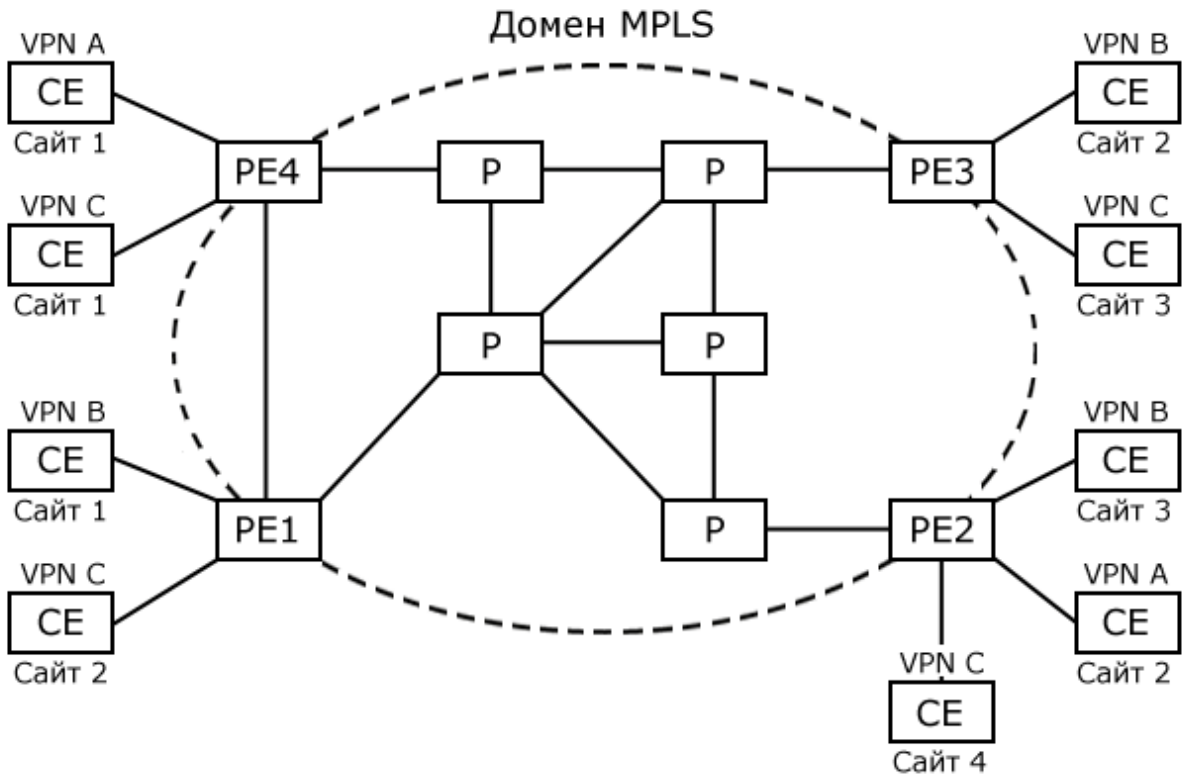

Рис. 1. Пример общей модели услуги *VPLS*

Магистральная транзитная сеть (*Backbone Network*) *MPLS* состоит из граничных маршрутизаторов провайдера *PE* (*Provider Edge router*) и не показанных для упрощения внутренних маршрутизаторов провайдера *P* (*Provider router*). Каждая *VPLS* состоит из нескольких территориально обособленных *LAN Ethernet*, которые принято называть

сайтами. Например, об услуге сети с центральным отделением и тремя удалёнными филиалами можно сказать, что они состоят из четырёх сайтов. Маршрутизатор, с помощью которого сайт клиента подключается к граничному маршрутизатору провайдера *PE*, называется граничным маршрутизатором клиента *CE* (*Customer Edge router*).

На рисунке 1 приведён пример *VPLS A* с двумя сайтами, *VPLS B* с тремя сайтами и *VPLS C* с четырьмя сайтами. Пограничные маршрутизаторы *PE* соединены с помощью так называемых псевдоканалов, позволяющие объединить сайты одной *VPLS* (*PW1-PW6*).

1.2. Принцип коммутации по меткам в сети *MPLS*. В технологии *MPLS* маршрутизация базируется не на адресе назначения, как в *IP*-сети, а на метках, которые вставляются в начало каждого пакета данных. Метод использования меток во многом близок к виртуальным каналам. Заголовок метки *MPLS*, состоящий из четырех байтов, предопределяет сетевой маршрут, который учитывает требуемый уровень *QoS*. Заголовок метки *MPLS* состоит из следующих полей (рис. 2):

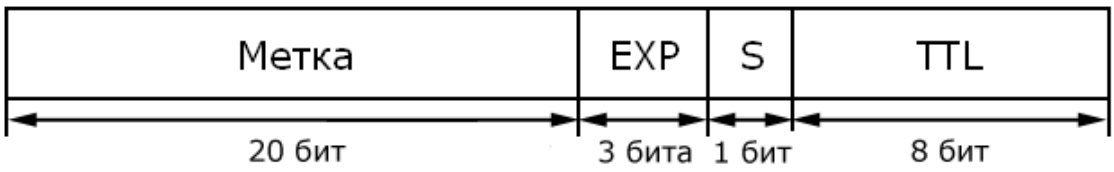

Рис. 2. Структура заголовка метки *MPLS*

– метка (20 бит) используется для выбора соответствующего пути коммутации по меткам;

– поле экспериментальных битов (*EXP*) содержит 3 бита, которые резервированы для дальнейших исследований и экспериментирования. В настоящее время проводится работа, направленная на создание согласованного стандарта использования этих битов для поддержания дифференцированного обслуживания разнотипного трафика и идентификации класса обслуживания. При предоставлении дифференцированных услуг *MPLS*-сети это поле может указывать определенный класс обслуживания, например, аналогичный классам *DiffServ*;

– поле *MPLS*-стека содержит 1 бит и является средством поддержки иерархической структуры стека меток *MPLS*. В заголовке последней метки бит равен 1, а во всех остальных - бит равен 0;

– время жизни *TTL* (8 бит) дублирует аналогичное поле *IP*-пакета, которое

является средством сброса пакетов в сети вследствие образования закольцованных маршрутов.

Заголовок *MPLS*-метки не образует полноценного уровня, а «вклинивается» в сеть *Ethernet* между вторым и третьим уровнями модели *OSI*, оставаясь независимым от этих уровней. На рис. 3. показан формат пакета *MPLS* с кадром *Ethernet* внутри.

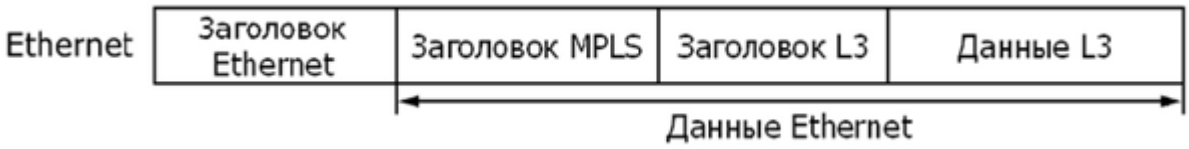

Рис. 3. Формат пакета MPLS с кадром Ethernet

В *MPLS*-сетях пересылка пакетов выполняется коммутаторами. Пакет перемещается в сети, основываясь только на содержании метки *MPLS*. Поэтому сеть *MPLS* можно рассматривать как один транзит. Маршрутизатор с поддержкой *MPLS* использует содержимое метки *MPLS* для указания маршрута, основываясь на *IP*-адресах граничных маршрутизаторов.

Приведенные на рис. 1 соединения между граничными маршрутизаторами показаны сплошными линиями для упрощения. В действительности, коммутацию в *MPLS* осуществляют маршрутизаторы провайдера коммутации меток *LP*. Граничный маршрутизатор выполняет функции назначения и удаления метки. *LER1* устанавливает метку для входящего кадра *Ethernet*. Получив кадр от *LER* маршрутизатор *LP* заменяет эту метку и отправляет этот кадр в следующий *LP* или *LER*.

Такой путь носит название коммутируемого по меткам пути *LSP* (*Label-Switched Path*) и идентифицируется набором меток во внутренних маршрутизаторах *LP*, расположенных на пути следования потока от отправителя к получателю. Внутренний маршрутизатор коммутирует пакет с меткой от одного интерфейса к другому интерфейсу с заменой метки. Продвижение кадра в *MPLS*-сети, обеспечивающей услугу *VPLS*, происходит на основе метки *MPLS* и техники коммутируемого по меткам тракта *LSP*, а не на основе адресной информации и технологии Ethernet. *MAC*-адреса источника и приемника, хотя и присутствуют в соответствующих полях Ethernet, но для продвижения кадра по *MPLS* не задействуются. Архитектура *MPLS* для создания позволяет использовать следующие протоколы распределения меток для создания пути *LSP*:

- специальный протокол распределения меток *LDP* (*Label Distribution Protocol*);
- расширение возможностей протокола *IP*-сети *BGP*.

1.3. Угрозы информационной безопасности *VPLS* на участке *CE-CE*. Приведем одни из основных видов угроз ИБ в *VPLS*.

Пользователь *VPLS* может обманным способом получить легитимные адреса других пользователей этой же *VPN* и применить их для передачи незашифрованных данных на участке абонентской линии между граничными маршрутизаторами пользователя и провайдера *CE–PE*. Шифрование/дешифрование данных пользователя обеспечивает также защиту от других К угрозам угроз ИБ на участках между *CE* относятся также:

- вставка фиктивных кадров в *VPLS*;
- изменение содержания пакета;
- незаконный повтор пакетов – механизм защиты предотвращает эту угрозу;
- вставка фиктивных *CE*;
- утечка трафика из защищенных *VPLS* в недоверенные *VPLS*, поскольку расшифровать трафик будет невозможно.

2. Защита информационной безопасности *VPLS* с помощью туннелирования

Защита информационной безопасности *VPLS* с помощью туннелирования и шифрования на участке *CE-CE*. Настоящий раздел посвящен туннелированию.

2.1. Структура услуги *VPLS*. Сервисы виртуальных частных сетей второго уровня (VPLS) описаны в спецификациях.

Сервис *VPLS* организован на базе псевдоканалов. Для каждого экземпляра *VPLS* используется собственный набор псевдоканалов. При этом каждый такой набор имеет полносвязную топологию, то есть все пограничные маршрутизаторы PE, участвующие в работе какого-то экземпляра *VPLS* связаны друг с другом. Псевдоканалы представляют собой пути *LSP* второго уровня иерархии (называемого так же внутренним уровнем), проложенным внутри *LSP* первого (внешнего) уровня.

На рисунке 4 показан пример сети провайдера, эмулирующей две услуги *VPLS*. Пользовательские сети *C1*, *C5* и *C8* относятся к «серому» сервису *VPLS*, а сети *C2*, *C3*, *C4*, *C6* и *C7* – к «белому». Соответственно, набор псевдоканалов *PW-B1*, *PW-B2* и *PW-B3* объединяет пограничные маршрутизаторы, к которым подключены сети услуги *VPLS* «серого» цвета, а набор псевдоканалов *PW-PW1*, *PW-W2* и *PW-W3* – маршрутизаторы, к которым подключены сети услуги «белого» *VPLS*.

Внутренняя организация пограничного маршрутизатора при оказании услуги *VPLS* показана на примере маршрутизатора *PE1*. Мы видим, что для поддержки каждого экземпляра сервиса *VPLS* пограничному маршрутизатору требуется отдельный виртуальный коммутатор, в данном случае это модули *VSB* и *VSW*. Модуль B выполняет стандартные функции моста и при этом формирует логический интерфейс с каждым из виртуальных коммутаторов.

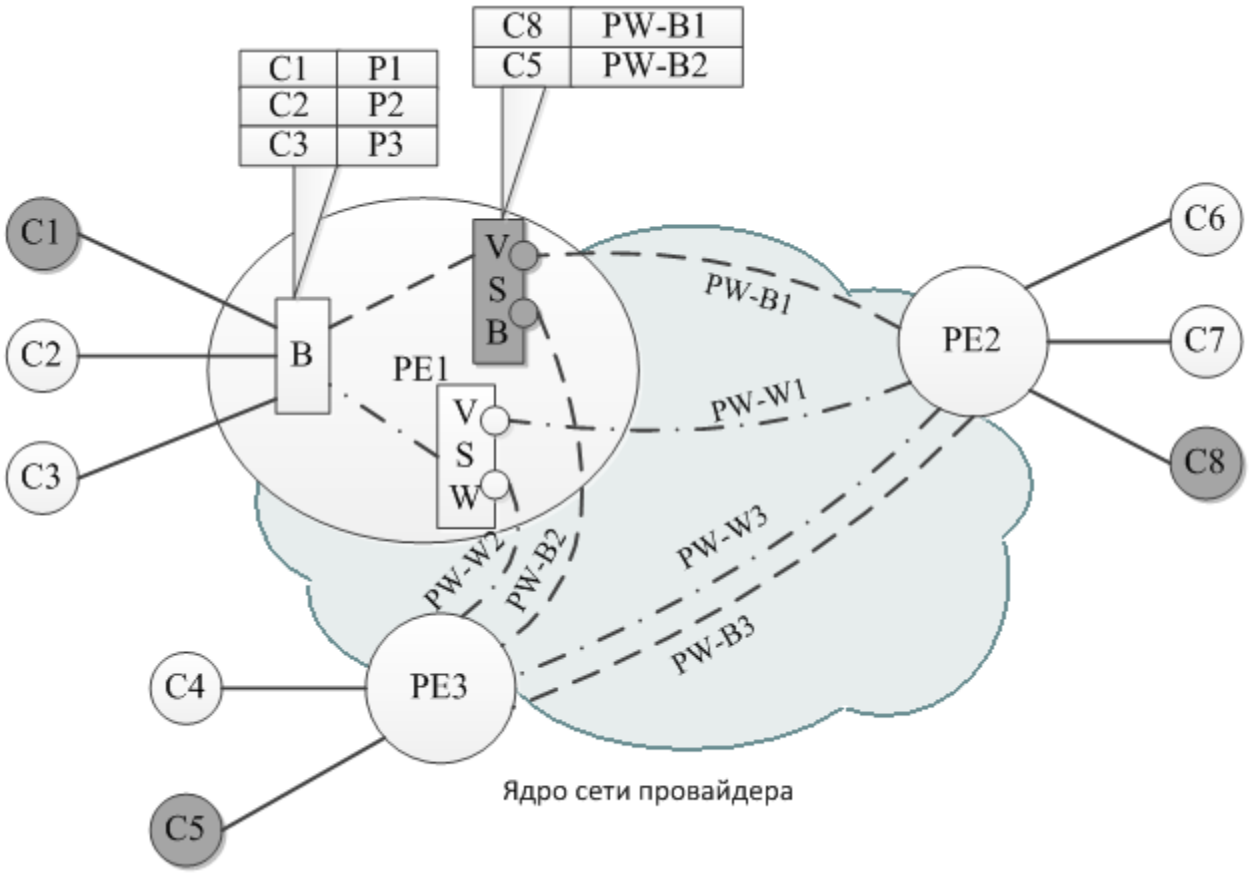

Рис. 4. Организация услуги VPLS

В сервисе *VPLS* виртуальный коммутатор функционирует по алгоритму стандартного коммутатора (моста). Для этого виртуальный коммутатор изучает *MAC*-адреса и строит свою таблицу коммутации, как и обычный коммутатор. На рисунке показан упрощенный вид таблицы коммутации *PE1*, состоящей из двух записей: одна запись связывает адрес *M8* сети *C8* с псевдоканалом *PW-B1*, другая – адрес *M5* сети *C5* с псевдоканалом *PW-B2*. Пользуясь такой таблицей, виртуальный коммутатор, получая кадры направляет их в псевдоканал, ведущий к пограничному коммутаторы, к которому подключены сеть с узлом назначения. Кадр, полученный виртуальным коммутаторам по псевдоканалу, всегда передается на логический интерфейс, соответствующий той услуги *VPLS*, к которой относится псевдоканал.

2.2. Защита ИБ *VPLS* в транзитной сети *MPLS* с помощью туннелирования.

В транзитной сети *MPLS* виртуальные частные локальные сети *VPLS* создаются с помощью туннелей. В отличие от *VPN IP*-сети в *MPLS* туннели создаются в результате использования стека меток.

Функциональные возможности стека *MPLS* позволяют реализовать несколько функций и, в частности, объединить (агрегировать) несколько LSP (псевдоканалов) в один. Каждый псевдоканал относится к определенной услуге *VPLS* (т.е. *VNN*). В случае услуги *VPLS* в одном *LSP* устанавливается псевдоканал со стеком из двух заголовков в кадре (рис.1). В *VPLS* Получив кадр от *CE* определенного сайта (сайта определенной *VPN*) в *PE* отправителя создается метка логически связанная с выходным *PE*-маршрутизатором. Эта метка является верхней и по ней производится доставка кадра *PE*, к которому может быть подключено несколько сайтов разных услуг *VPLS*. P-маршрутизаторы анализируют верхнюю транспортную метку и направляют кадр по сети к требуемому *PE*. На выходном *PE*-маршрутизаторе верхняя метка удаляется и исследуется нижняя Далее коммутация производится по нижней метке. Нижняя метка идентифицирует *CE* сайта той же услуги *VPLS*. Нижняя метка стека и является туннелем, обеспечивающим независимость разных услуг VPLS. *PE*-маршрутизатор помещает обе метки в стек меток *MPLS*.

3. Обеспечение информационной безопасности услуги *VPLS*

В настоящем разделе приводятся механизмы защиты ИБ от угроз услуги *VPLS*.

В случае высоких требований пользователей к ИБ от указанных (выше в разделе 1) угроз в *VPLS* на участке между граничными маршрутизаторами *PE* и *CE* необходимо шифровать кадры Ethernet. Для установления соединения для каждого вызова производится взаимная аутентификация *CE*-PE и *PE-CE*. Одновременно с процедурой аутентификации выполняется функция по созданию общего секретного ключа шифрования сообщений этого соединения. С помощью этого секретного ключа производится шифрование/дешифрование кадра *Ethernet*. При передаче кадра (участок *CE-PE*) на приеме в *PE* производится дешифрование этого кадра. Далее, как показано выше в разделе 2, этот кадр устанавливается в псевдоканал (туннель) на внутренний второй уровень стека сети *MPLS*. Выделение псевдоканала производится на основании *MAC* адресов в кадре Ethernet. Коммутация этого кадра в транзитной сети *MPLS* производится по внешнему первому уровню стека. При поступлении кадра на прием на

участке *PE-CE* производится аналогичная процедура взаимной аутентификации и создание общего секретного ключа. .С помощью этого секретного ключа производится шифрование этого кадра *Ethernet* в *PE* и дешифрование его в *CE*. Рассмотрим пример такого шифрования с использованием сертификатов. При этом ограничимся процедурой взаимной аутентификации CE и PE, при которой создается общий секретный ключ шифрования. В основу приведенного ниже примера положена методика, основанная на рекомендация *ETSI ITU-T X.509* [6] и используемая в рекомендации для обеспечения информационной безопасности сети связи *ISDN* [7].

Процедура взаимной аутентификации *CE* и *PE* в соответствии с рекомендацией *ITU-T* рассматривается на примере двухуровневой иерархии - цепочки удостоверяющих центров C_X и C_Y с общим центром *GCA, General Certification Authority* (рис. 5). Реально может быть больше уровней иерархии. Управление сертификации верхнего уровня (*GCA*) называют корневым. *GCA* сертифицирует управления второго уровня. На рис. 5 это удостоверяющие центры Cx и C_Y, которые создают сертификаты соответствующих *CE* и *PE*. В общем случае может иметь место не один корневой удостоверяющий центр, причем каждый из них свою иерархию уровней. В современных машинах пользователей содержатся открытые ключи более 100 корневых уровней [8].

При установлении вызова процедура аутентификации использует четыре сообщения: RSA.P1 – инициализация аутентификации; RSA.P2 – ответ на запрос аутентификации; RSA.P3 – успешное завершение аутентификации; RSA.P4 – безуспешное завершение аутентификации.

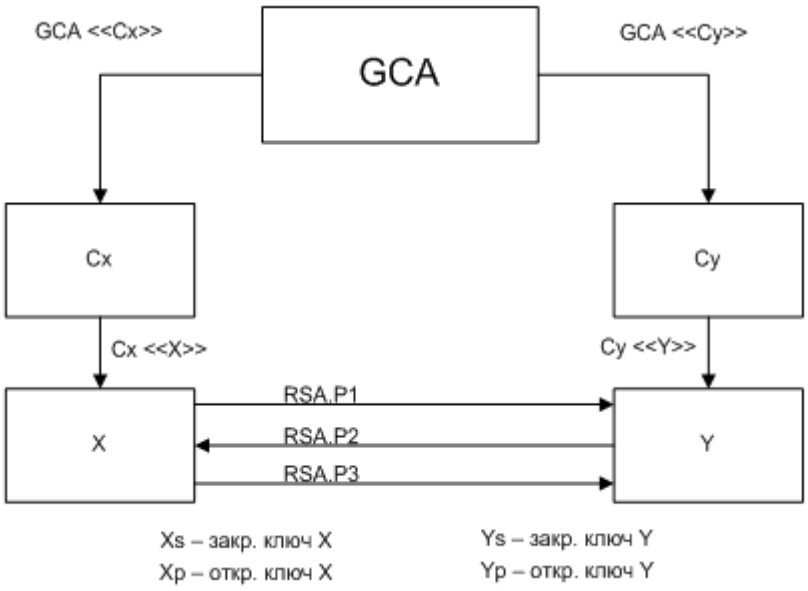

Рис. 5. Схема взаимной аутентификации CE и PE и передача общих ключей симметричного шифрования

Рассмотрим случай, когда инициатором аутентификации является *CE*, идентификатор которого обозначим через X. Идентификатор *PE*, вызываемого для проведения процедуры аутентификации, обозначим через Y. Маршрутизатор X отправляет сообщения RSA.P1 и RSA.P3. Маршрутизатор Y отправляет сообщение RSA.P2. Удостоверяющие центры, в которых создаются сертификаты маршрутизаторов X и Y, обозначим соответственно через Cx (Cx <<X>>) и C_Y (C_Y <<Y>>). На первом шаге маршрутизатор X отправляет маршрутизатору Y сообщение RSA.P1. Содержание сообщения RSA.P1: *GCA* <<Cx>>, Cx <<X>>, Rx, Y, Xs [h (Rx, Y)], где *GCA* <<Cx>> - сертификат удостоверяющего центра (центра сертификации) Cx в общем удостоверяющем центре (центре сертификации) *GCA*; Rx – случайное число, сгенерированное объектом X. Rx используется для защиты от угрозы «повтор аутентификации»; Xs – закрытый ключ объекта X; [h (Rx, Y)] - хеш-функция (Rx, Y).

Маршрутизатор Y, получив сообщение RSA.P1, выполняет следующую последовательность операций.

Производится проверка достоверности принятого открытого ключа Xp маршрутизатора X, используя для этого принятые в сообщении два сертификаты. Сертификат центра сертификации Cx, созданный в центре сертификации *GCA* обозначается *GCA*<<Cx >>.

Этот сертификат включает следующие данные: *GCA* <<Cx>>: *IGCA*, ICx, Cxp, *GCAs* [h (*IGCA*, ICx, Cxp)]. Здесь *IGCA* – идентификатор *GCA*; *GCAs* – закрытый ключ общего центра сертификации *GCA*; ICx – идентификатор центра сертификации Cx; Cxp – открытый ключ центра сертификации Cx; *GCAs* [*] – зашифрованная информация [*] с помощью ключа *GCAs*, где: [*] – хеш-функция открытой части сертификата.

Значение *GCAs* [*] является цифровой подписью открытой части сертификата. Для упрощения изложения материала в открытой части сертификата опущено много элементов.

Сертификат маршрутизатора X, созданный в центре сертификации Cx обозначается Cx <<X>>. Состав этого сертификата: Cx <<X>>: ICx, X, Xp , CXs [h (ICx, X, Xp)]. Здесь: ICx – идентификатор центра сертификации Cx; Cxs – закрытый ключ центра сертификации Cx; X – идентификатор объекта X; Xp – открытый ключ объекта X; Cxs [*] – зашифрованная информация [*] с помощью ключа Cxs.

В объекте X записаны открытый ключ *GCAp* общего сертификационного центра, сертификат центра сертификации Cx – *GCA* <<Cx>> и сертификат маршрутизатора

X (Cx <<X>>), а также закрытый ключ маршрутизатора Xs. Сначала производится проверка достоверности открытого ключа центра сертификации Cx (т.е. Cxp). Для этого производится вычисление хеш-функции h (IGCA, ICx, Cxp) открытой части сертификата этого центра сертификации Cx. Используя *GCAp*, производится расшифрование хеш-функции этой открытой части– *GCAp* [*GCAs* [h (IGCA, ICx, Cxp , T1)]] = h (*IGCA*, ICx, Cxp). Открытый ключ Cxp считается достоверным, если обе хеш-функции равны. Для проверки достоверности открытого ключа Xp маршрутизатора X производится вычисление хеш-функции открытой части сертификата маршрутизатора X - h (ICx, X, Xp). Используя достоверный открытый ключ Cxp производится расшифрование хеш-функции открытой части сертификата маршрутизатора X – Cxp [Cxs [h (ICx, X, Xp)]] = h (ICx, X, Xp). Открытый ключ Xp считается достоверным, если обе хеш-функции равны.

Производится проверка целостности сообщений – Rx, Y. Для этого полученная хеш-функция h (Rx,Y) сравнивается с помощью расшифрованной – Xp [Xs [h (Rx,Y)]]. Оба значения должны быть равны.

Производится проверка идентификатора маршрутизатора X, полученного в составе сертификата Cx <<X>>.

При успешном результате анализа принятого сообщения RSA.P1 маршрутизатор Y отправляет маршрутизатору X сообщение RSA.P2. Содержание сообщения RSA.P2: GCA <<C_Y>>, C_Y <<Y>>, R_Y, X, Rx, Xp [K_Y], Ys [h (R_Y, X, Rx, K_Y)] Здесь GCA <<C_Y>> - сертификат удостоверяющего центра C_Y в общем удостоверяющем центре *GCA*; R_Y – случайное число, сгенерированное объектом Y, R_Y используется для защиты от угрозы «повтор аутентификации»; K_Y – случайное число, сгенерированное маршрутизатором Y, для создания ключа симметричного шифрования; Ys – закрытый ключ объекта Y; [h (R_Y, X, Rx, K_Y)] - хеш-функция (R_Y, X, Rx, K_Y).

Маршрутизатор X, получив сообщение RSA.P2, выполняет следующую последовательность операций:

1. Производится проверка достоверности принятого открытого ключа Yp маршрутизатора Y, используя для этого принятые в сообщении сертификаты. Принцип работы алгоритма проверки аналогичен описанному выше при проверке достоверности принятого открытого ключа Xp в сообщении RSA.P1.

2. Производится расшифровывание K_Y, т.е. K_Y – Xs [Xp [K_Y]].

3. Производится проверка целостности сообщений – R_Y, X, Rx, K_Y. Для этого полученная хеш-функция h (R_Y, X, Rx, K_Y) сравнивается с расшифрованной – Yp [Ys [h(R_Y, X, Rx, K_Y)]]. Оба значения должны быть равны.

4. Производится проверка, является ли значение Rx тем же самым, что было отправлено в сообщении RSA.P1 (защита от угрозы «повтор аутентификации»).

5. Производится проверка идентификатора маршрутизатора Y, полученного в составе сертификата Cy <<Y>>.

При успешном результате анализа принятого сообщения RSA.P2 маршрутизатор X отправляет маршрутизатору Y сообщение RSA.P3 об успешном завершении аутентификации маршрутизатора Y.

Содержание сообщения RSA.P3: R_Y, Y, Yp [K_X], Xs [h (R_Y, Y, Kx)]. Здесь Kx – случайное число, сгенерированное маршрутизатором X, для создания общего ключа симметричного шифрования.

Объект Y, получив сообщение RSA.P3, выполняет следующую последовательность операций:

1. Производится расшифровывание Kx, т.е. Kx = Ys [Yp [Kx]].

2. Производится проверка целостности сообщений – R_Y, Y, Kx. Для этого полученная хеш-функция h (R_Y, Y, Kx) сравнивается с расшифрованной – Xp [Xs [h (R_Y, Y, Kx)]]. Оба значения должны быть равны.

3. Производится проверка, является ли значение R_Y тем же самым, что было отправлено в сообщении RSA.P3 (защита от угрозы «повтор аутентификации»).

Успешный результат анализа принятого сообщения RSA.P3 свидетельствует об успешной аутентификации маршрутизатора X объектом Y, т.е. взаимной аутентификации. Если проверка любого из сообщений RSA.P1, RSA.P2, RSA.P3 оказывается неуспешной, маршрутизатор X или Y отправляют сообщение RSA.P4 об отказе в аутентификации. При этом прекращается процедура установления соединения.

Из значений Kx и Ky отбрасываются старшие и младшие 64 бит. Оставшиеся части Kx и K_Y складываются по модулю 2, образуя общий ключ симметричного шифрования сообщений между маршрутизаторами X и Y (т.е. *CE* и *PE*) для устанавливаемого соединения.

Аналогичным образом осуществляется при взаимной аутентификация *PE* и *CE* создание общего ключа шифрования в том случае, когда инициатором аутентификации является *CE*, а *PE* вызывается для проведения процедуры аутентификации.

Выводы. Предлагаемый в работе механизм аутентификации и шифрования для защиты от угрозы ИБ на участке между граничным маршрутизатором пользователя услуги виртуальной частной локальной сети *VPLS* и граничным маршрутизатором *MPLS* может быть использован при проектировании на сетях связи России.

Список литературы

1. Бельфер Р.А. Сети и системы связи. М.: ФГУП НТЦ «Информрегистр», МГТУ им. Н.Э. Баумана, 2012 г. 723 с.
2. Гольдштейн Ф.Б., Гольдштейн Б.С. Технология и протоколы MPLS. СПб.: БХВ-Петербург, 2005. 304с.
3. Оливейн В. Структура и реализация современной технологии MPLS. М.:Вильямс, 2004. 480с.
4. Kompella K., Rekhter Y. Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling. Available at: https://tools.ietf.org/html/rfc4761, accessed 29.01.2014.
5. Kompella K., Lasserre M. Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling. Available at: https://tools.ietf.org/html/rfc4762 (дата обращения 29.01.2014).
6. ITU-T Recommendations – ITU-T X.509. Available at: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11735, accessed 12.02.2014.
7. ETSI TC-Security. Telecommunications Security; Integrated Services Digital Network (ISDN); Encryption key management and authentication system for audiovisual services. Available at: http://www.etsi.org/deliver/etsi_i_ets/300800_300899/300841/01_30_9742/ets_300841e01v.pdf, accessed 13.02.2014.
8. Таненбаум Э. Д. Уэзеролл. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 960с.