МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 621.391

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ VPLS НА БАЗЕ СЕТИ MPLS

Р.А. Бельфер[1], **И.С. Петрухин**[2], **А.П. Тепикин**[1]

[1]МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: a.belfer@yandex.ru; tepandrew@gmail.com

[2]"INLINE Technologies", Москва, Российская Федерация
e-mail: ispetrukhin@gmail.com

Проанализированы угрозы информационной безопасности виртуальной частной сети (VPN), которая называется услугой виртуальной частной локальной сети VPLS. Рассмотрены два типа угроз информационной безопасности этой VPLS: 1) угрозы абонентского доступа между граничными маршрутизаторами пользователей LAN и MPLS; 2) угрозы, аналогичные угрозам в виртуальной локальной вычислительной сети VLAN. Предложен алгоритм обеспечения шифрования на участке абонентского доступа в транзитную сеть MPLS. В основу положен алгоритм, принятый для сети ISDN и рекомендованный Международным союзом электросвязи ITU-T. Для некоторых угроз безопасности, аналогичных угрозам в сети VLAN, предложены реализуемые при конфигурировании сети VPLS механизмы защиты. К таким угрозам относятся DoS-атака на протокол связующего дерева STP, угроза вставки фиктивной метки в структуру кадра стандарта 802.1q, угроза подмены DHCP-сервера, угроза переполнения таблицы памяти адресов CAM и др. Согласно имеющимся отечественным и зарубежным материалам (включая документы некоторых зарубежных фирм, по которым осуществляется проектирование сети VPLS на сетях связи России), защита от таких угроз информационной безопасности не предусмотрена. Предложен реализованный на некоторых корпоративных сетях VPLS механизм защиты от перечисленных угроз.

***Ключевые слова*:** виртуальная частная сеть, информационная безопасность, услуга частной виртуальной сети локальной вычислительной сети, многопротокольная коммутация по меткам, граничный маршрутизатор клиента, граничный маршрутизатор провайдера, псевдоканал, маршрутизатор провайдера.

ANALYSIS OF INFORMATION SECURITY THREATS FOR VIRTUAL PRIVATE NETWORKS VPLS BASED ON NETWORK MPLS

R.A. Bel'fer[1], **I.S. Petrukhin**[2], **A.P. Tepikin**[1]

[1]Bauman Moscow State Technical University, Moscow, Russian Federation
e-mail: a.belfer@yandex.ru; tepandrew@gmail.com

[2]"INLINE Technologies", Moscow, Russian Federation
e-mail: ispetrukhin@gmail.com

The authors have analyzed information security threats for virtual private network (VPN), which is called a virtual private area network (LAN) service (VPLS). Two types of security threats of VPLS were considered: 1) threats of subscriber access between border routers of users LAN and MPLS; 2) threats, similar threats in

a virtual local area network VLAN. Our research proposes to provide encryption algorithm on the site user's access into a transit network MPLS. It is based on the algorithm adopted for the ISDN network and recommended by the International Telecommunication Union ITU-T. For some security threats (similar threats in the VLAN) protection mechanisms (implemented at configuring of network VPLS) are offered. These threats include: DoS-attacks on the spanning tree protocol STP, fictitious label insert in a frame structure of standard 802.1q, spoofing DHCP-server, table overflow of memory address CAM and other. But protection against such information security threats have not been supported according to the available domestic and foreign publications and manuals (including some foreign firms documents, on which VPLS network design have performed using communication networks of Russia). The authors suggest mechanism of protection against such threats implemented on some corporate networks VPLS.

***Keywords*:** virtual private network (VPN), information security, virtual private local area network (VLAN) service (VPLS), multiple protocol label switching (MPLS), customer edge router (CE), provider edge router (PE), pseudowire (PW), provider router (P).

Введение. Многопротокольная коммутация по меткам (Multiple Protocol Label Switching, MPLS), выполняя функцию транзитной сети связи, в зависимости от технологии поступающего в нее трафика позволяет создать виртуальные частные сети (VPN) двух различных типов [1, 2]. При поступлении в коммутацию MPLS пакетов третьего уровня (IP-пакетов) создаются сети VPN третьего уровня, называемые виртуальными частными маршрутизируемыми сетями (Virtual Private Routed Network, VPRN). В работах [3, 4] проанализированы угрозы информационной безопасности (ИБ) и механизмы защиты от них. Настоящая работа посвящена аналогичным вопросам одних из сетей VPN, создаваемых на базе коммутации MPLS при поступлении в нее пользовательских кадров второго уровня. В данном случае рассмотрено поступление кадров локальной вычислительной сети (LAN) Ethernet. Такие VPN называются услугой виртуальной частной локальной сети (Virtual Private LAN Service, VPLS), которая объединяет несколько дистанционно разбросанных сетей LAN, превращая их в единую сеть LAN, доставка трафика от пользователя до граничного маршрутизатора MPLS осуществляется с помощью кадра Ethernet.

Общая модель услуги VPLS. Пример структуры, состоящей из трех VPLS (A, B, C, т.е. из трех виртуальных частных сетей VPN), приведен на рис. 1. Магистральная транзитная сеть (Backbone Network) MPLS включает в себя граничные маршрутизаторы провайдера PE (Provider Edge router) и не показанного для упрощения внутренних маршрутизаторов провайдера P (Provider router). Каждая VPLS содержит несколько территориально обособленных сетей LAN Ethernet, которые принято называть сайтами. Например, сети VPLS с центральным отделением и тремя удаленными филиалами включают в себя четыре сайта. Маршрутизатор, с помощью которого сайт клиента подключается к граничному маршрутизатору провайдера PE, называется граничным маршрутизатором пользователя (Counter Edge router, CE).

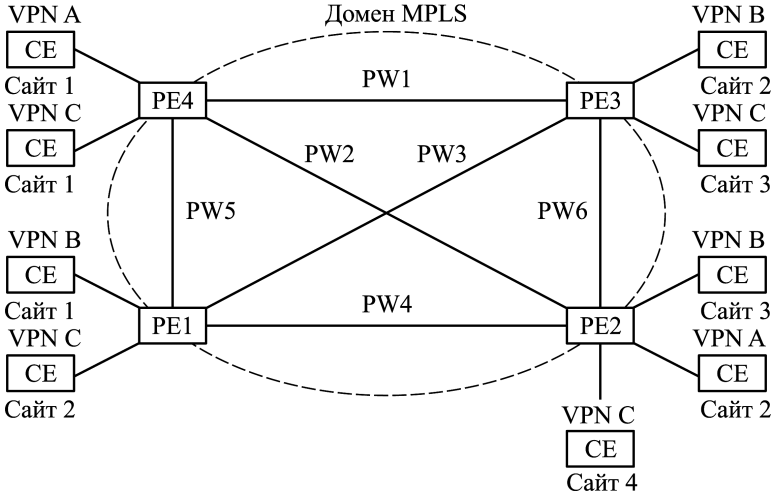

Рис. 1. Пример структуры, состоящей из трех VPLS

Показаны VPLS A с двумя сайтами, VPLS B с тремя сайтами и VPLS C с четырьмя сайтами. Пограничные маршрутизаторы PE соединены с помощью шести так называемых псевдоканалов PW (pseudowire), позволяющих объединить сайты одной сети VPLS (PW1–PW6). Псевдоканалы представляют собой туннели второго уровня иерархии (называемого внутренним уровнем), проложенным внутри первого (внешнего) уровня. При передаче кадра по псевдоканалу MPLS кадр данных в псевдоканале пользователя содержит два уровня меток стека. Верхняя транспортная метка направляет кадр через внутренние маршрутизаторы P к требуемому маршрутизатору PE, а вторая нижняя метка указывает на сайт, принадлежащий данной сети VPLS. На выходном маршрутизаторе PE верхняя метка удаляется и анализируется нижняя, указывающая требуемый маршрутизатор CE.

Угрозы безопасности сети VPLS, аналогичные угрозам в сетях VLAN. Для анализа угроз безопасности, возникающих в сетях VPLS, необходимо учесть принципы построения виртуальных локальных сетей VLAN (Vitrual LAN) [5]. На основе их строится и сеть VPLS. Виртуальной локальной сетью называется группа узлов сети, трафик которых, в том числе и широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети. В сети VPLS существуют реализуемые угрозы (атаки), которые похожи на угрозы в сети VLAN. Рассмотрим некоторые из угроз и предложения по защите от них.

DoS-атака на протокол связующего дерева STP. Рассмотрим потенциальную атаку злоумышленника на протокол связующего дерева IEEE 802.1d Spanning Tree Protocol (STP). Основная задача STP — устранение петель в топологии произвольной сети VLAN, в которой есть один или более сетевых мостов, связанных избыточными соеди-

нениями. Протокол STP решает эту задачу, автоматически блокируя соединения, которые являются избыточными, а также позволяет защитить сеть от широковещательных штормов и переполнения таблицы коммутации [6]. Сеть VPLS логически представляет собой коммутатор (мост), поэтому в нем существуют инстанции (инстанция — единичный экземпляр любого сетевого протокола; высокопроизводительное оборудование провайдера (P и PE) позволяет запускать по несколько экземпляров одного и того же протокола для различных целей) протокола STP, защита которых становится важной задачей.

После построения связующего дерева всем портам виртуального коммутатора назначаются следующие роли (в соответствии с терминологией STP): корневой порт (Root Port); выделенный порт (Designated Port); блокирующий порт (Blocking Port); альтернативный порт (Alternate Port); перенаправляющий порт (Forwarding Port).

Предположим, что другой виртуальный или физический коммутатор появился в сети VPLS с приоритетом моста меньшим, чем у конкретного корневого моста. Тогда новый коммутатор станет корневым мостом для этой услуги VPLS (так как по правилам STP коммутатор с наименьшим приоритетом становится корневым мостом). Начнется изменение всей топологии связующего дерева STP, при которой произойдет отказ в обслуживании услуги VPLS (DoS-атака). Защита от DoS-атаки при проектировании сети VPLS не предусмотрена.

Для защиты топологии STP в сервисе сети VPLS от указанной атаки необходимо использовать функцию Root Guard на всех интерфейсах (доступа абонента и туннельных), на которых не предполагается наличие корневого коммутатора. Эту функцию можно реализовать с помощью определенных команд конфигурации на граничном маршрутизаторе PE. Список команд так же, как и в последующих примерах, не приводится, поскольку зависит от конкретного производителя оборудования.

Угроза вставки фиктивной метки в структуру кадра стандарта 802.1q. Структура кадра Ethernet в соответствии со стандартом IEEE 802.1q приведена на рис. 2, *а* [7]. Основную функцию выполняет идентификатор сети VLAN.

Суть такой угрозы отражена на рис. 2, *б*. Автоматизированное рабочее место (АРМ) злоумышленника находится в сети VLAN 10 (первичная сеть VLAN для коммутатора A) и отправляет дважды промаркированные 802.1q метками пакеты в магистральный порт (порт коммутатора, через который может передаваться информация о нескольких сетях VLAN). На самом деле злоумышленник не подключен к магистральному порту, а пытается обмануть магистральную инкапсуляцию, чтобы попасть в другую сеть VLAN.

Когда коммутатор CE A получает дважды тегированный кадр, он принимает решение отправить его через магистральный интерфейс.

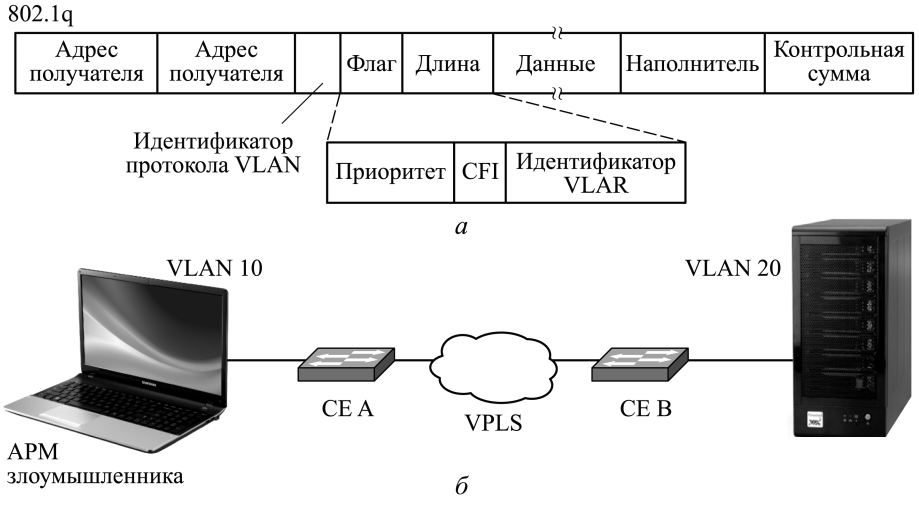

Рис. 2. Структура кадра Ethernet в соответствии со стандартом IEEE 802.1q (*а*) и пример связи сетей VLAN10 и VLAN20 (*б*)

Поскольку первая метка 802.1q имеет значение первичной сети VLAN, она удаляется и кадр пересылается по магистральному интерфейсу. Когда коммутатор CE B получает кадр, то обнаруживает вторую метку 802.1q, которая отбрасывается и кадр нелегитимно попадает в сеть VLAN 20 путем коммутации. Таким образом, злоумышленник может осуществить вторжения на оборудование, находящееся в сети VLAN 20. Для того чтобы убрать уязвимость с повторным тегированием 802.1q, необходимо просто исключить первичную сеть VLAN со всех магистральных каналов сети VPLS. Это выполняется при конфигурации.

Угроза подмены DHCP-сервера и защита от DoS-атаки. Рассмотрим случай, когда злоумышленник смог подменить DHCP-сервер в услуге VPLS. Теперь любой компьютер в сети VPLS отправляет широковещательный DHCP-запрос, тогда нелегитимный DHCP-сервер может отправить ложный DHCP-ответ, в котором будет указан IP-адрес устройства злоумышленника вместо адреса шлюза по умолчанию. После получения компьютером DHCP-ответа он начнет использовать устройство злоумышленника как шлюз по умолчанию и пакеты, предназначенные для других подсетей, будут отправлены злоумышленнику.

Для предотвращения DoS-атаки предлагается использовать функцию DHCP Snooping, которая позволяет составить список всех легитимных DHCP-серверов в услуге VPLS [8]. Это выполняется при конфигурации.

Защита от широковещательных штормов. Производители оборудования компании Cisco предусмотрели конфигурирование так, чтобы ограничивалась сумма загрузки широковещательного трафика на входе интерфейса [9].

Прозрачная работа VTP (VLAN trunking protocol). Чтобы передать через порт трафик нескольких сетей VLAN, порт переводится в режим транка. По умолчанию в транке разрешены все сети VLAN. Для передачи данных через соответствующую сеть VLAN в транке необходимо, чтобы сеть VLAN была активной. Активной сеть VLAN становится тогда, когда она создана на коммутаторе. В то время как использование VLAN транкингового протокола может быть выгодным в корпоративной среде, это создает угрозы ИБ для поставщиков услуг, потому что протокол VTP допускает динамическое определение сети VLAN. Эту функцию необходимо отключить на сетевом оборудовании для большей безопасности. Протокол VTP является проприетарным протоколом компании Cisco, в связи с чем он реализуется на оборудовании только этой компании [9].

Ограничение MAC-адресов и безопасность портов. Оборудование может быть сконфигурировано так, чтобы разрешить доступ для предопределенного максимального количества MAC-адресов. Это помогает предотвратить переполнение таблицы памяти CAM-адресов (Content Addressable Memory Table). Коммутатор имеет CAM-таблицу (в ней содержится "привязка", какие MAC-адреса на каком порту принимаются), обычно связанной с атаками переполнения. Оборудование должно выполнять операции по определению допустимого максимума следующим образом:

- защищенный режим — отбрасывание пакетов от неизвестных исходных адресов, пока администратор не удалит достаточное число безопасных MAC-адресов и их число станет ниже максимального значения;
- режим ограничения — отбрасывание пакетов от неизвестных исходных адресов, пока администратор не удалит достаточное число безопасных MAC-адресов, чтобы их число стало ниже максимального значения, и вызывает операцию Security Violation вместо инкремента;
- режим завершения работы — отключение незаконного порта и генерация SNMP-прерывания, однако это требует ручное вмешательство администратора для восстановления работы [9].

Угрозы безопасности сети VPLS на абонентском участке CE–PE и механизм его защиты. Источниками угроз ИБ на этом участке является возможность пользователя VPLS обманным способом получить легитимные адреса пользователей других сетей VPLS. Еще один источник — угроза "человек посередине" для открытых данных кадров Ethernet. При реализации этих угроз на абонентском участке между граничными маршрутизаторами пользователя и провайдера CE–PE возможны следующие последствия: передача кадра пользователю перехваченного адреса; прием кадра пользователя перехваченного

адреса; вставка фиктивных кадров; изменение содержания кадра; незаконный повтор кадра; использование нелегитимных и легитимных маршрутизаторов CE при реализации угроз.

При установлении соединения для каждого вызова проводится взаимная аутентификация маршрутизаторов CE–PE и PE–CE. Одновременно с процедурой аутентификации выполняется функция создания общего секретного ключа шифрования сообщений этого соединения. С помощью секретного ключа осуществляется шифрование (дешифрование) кадра Ethernet. Рассмотрим пример такого шифрования с использованием сертификатов. При этом ограничимся процедурой взаимной аутентификации маршрутизаторов CE и PE, при которой создается общий секретный ключ шифрования. В приведенном ниже примере использована методика, основанная на рекомендации ETSI ITU-T X.509 [10] и используемая в рекомендации для обеспечения ИБ сети связи ISDN [11, 12].

Процедуру взаимной аутентификации маршрутизаторов CE и PE в соответствии с рекомендацией ITU-T рассмотрим на примере двухуровневой иерархии — цепочки удостоверяющих центров C_X и C_Y с общим центром (General Certification Authority, GCA) (рис. 3). Реально может быть больше уровней иерархии. Управление сертификации верхнего уровня (GCA) называют корневым, GCA сертифицирует управления второго уровня (на рис. 3 это удостоверяющие центры C_X и C_Y, создающие сертификаты соответствующих маршрутизаторов CE и PE). В общем случае может существовать не один корневой удостоверяющий центр, причем каждый из них имеет свою иерархию уровней. В современных машинах пользователей содержатся открытые ключи более 100 корневых уровней [5]. Согласно схеме, приведенной на рис. 3, при установлении вызова процедура аутентификации использует три сообщения: RSA.P1 — инициализация аутентификации; RSA.P2 — ответ на запрос аутентификации; RSA.P3 — успешное завершение аутентификации.

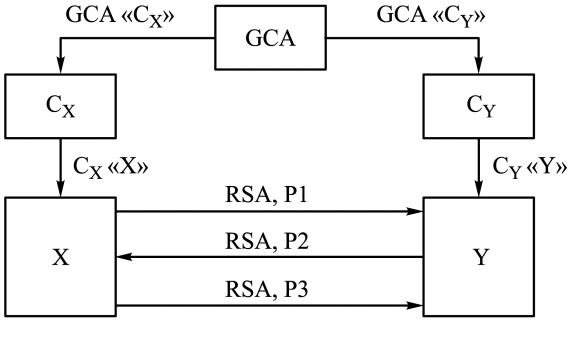

Рис. 3. Схема взаимной аутентификации CE и PE и передачи общих ключей симметричного шифрования

Рассмотрим случай, когда инициатором аутентификации является граничный маршрутизатор пользователя CE, который обозначим через X. Граничный маршрутизатор PE транзитной сети, вызываемый для проведения процедуры аутентификации, обозначим через Y. Удостоверяющие центры, в которых создаются сертификаты маршрутизаторов X и Y, обозначим через C_X ($C_X \ll X \gg$) и C_Y ($C_Y \ll Y \gg$). На первом шаге маршрутизатор X отправляет маршрутизатору Y сообщение RSA.P1. Содержание сообщения RSA.P1: GCA $\ll C_X \gg$, $C_X \ll X \gg$, Y, $X_s[h(Y)]$, где GCA$\ll C_X \gg$ — сертификат удостоверяющего центра (центра сертификации) C_X в общем удостоверяющем центре (центре сертификации) GCA; X_s — закрытый ключ объекта X. Маршрутизатор Y, получив сообщение RSA.P1, проверяет достоверность открытого ключа X_P маршрутизатора X, используя для этого принятые в сообщении два сертификата. Для упрощения изложения материала в открытой части сертификатов опущено много элементов. Сертификат GCA$\ll_X \gg$ включает в себя C_{XP}, $GCA_s[h(_{XP})]$, а сертификат — $C_X \ll X \gg$: X_P, $C_{xs}[h(_P)]$. Здесь GCA_s — закрытый ключ общего центра сертификации GCA; C_{XP} — открытый ключ центра сертификации C_X; C_{xs} — закрытый ключ центра сертификации C_X; X_P — открытый ключ объекта X. В объекте X записаны открытый ключ GCA_P общего сертификационного центра, сертификат центра сертификации C_X — GCA$\ll C_X \gg$ и сертификат маршрутизатора X ($C_X \ll X \gg$), а также закрытый ключ маршрутизатора X_s. Для этого вычисляется хеш-функция h (C_{XP}). С использованием ключа GCA_P проводится расшифровывание хеш-функции этой открытой части GCA_P $[GCA_s[h(C_{XP})]] = h(_{XP})$. Открытый ключ C_{XP} является достоверным, если две хеш-функции равны. Для проверки достоверности открытого ключа X_P маршрутизатора X рассчитывается хеш-функция открытой части сертификата маршрутизатора X – h(X_P). С помощью достоверного открытого ключа C_{XP} проводится расшифровывание хеш-функции открытой части сертификата маршрутизатора X — $C_{XP}[C_{xs}[h(_P)]] = h(_P)$. Открытый ключ X_P достоверен, если хеш-функции равны. Затем проверяется целостность сообщения Y. Для этого полученная хеш-функция h(Y) сравнивается с помощью расшифрованной — $X_P[X_s[h(Y)]]$. Оба значения должны быть равны.

При успешном результате анализа принятого сообщения RSA.P1 маршрутизатор Y отправляет маршрутизатору X сообщение RSA.P2: GCA$\ll C_Y \gg$, $C_Y \ll Y \gg$, $X_P[K_Y]$, $Y_s[h(K_Y)]$. Здесь GCA$\ll C_Y \gg$ — сертификат удостоверяющего центра C_Y в общем удостоверяющем центре GCA; K_Y — случайное число, сгенерированное маршрутизатором Y, для создания ключа симметричного шифрования; Y_s — закрытый ключ объекта Y. Маршрутизатор X, получив сообщение RSA.P2, проверяет достоверность принятого открытого ключа Y_P маршрутизато-

ра Y, используя для этого принятые в сообщении сертификаты. Принцип работы алгоритма проверки аналогичен приведенному выше алгоритму при проверке достоверности принятого открытого ключа X_P в сообщении RSA.P1. Проводится расшифровывание числа K_Y, т.е. $K_Y = X_s[X_P[K_Y]]$, проверка целостности сообщений K_Y с помощью Y_P, проверка идентификатора маршрутизатора Y, полученного в составе сертификата $C_Y \ll Y \gg$. 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: Y, $Y_P[K_X]$, $X_s[h(Y, K_X)]$, где K_X — случайное число, сгенерированное маршрутизатором X для создания общего ключа симметричного шифрования. Объект Y, получив сообщение RSA.P3, расшифровывает число K_X, т.е. $K_X = Y_s[Y_P[K_X]]$, а затем проверяет целостность сообщений — Y, K_X. Для этого полученная хеш-функция $h(Y, K_X)$ сравнивается с расшифрованной — $X_P[X_s[h(Y, K_X)]]$. Значения должны быть равны. Успешный результат анализа принятого сообщения RSA.P3 свидетельствует об успешной аутентификации маршрутизатора X объектом Y, т.е. взаимной аутентификации. Из значений K_X и K_Y отбрасываются старшие и младшие 64 бит. Оставшиеся части K_X и K_Y складываются по модулю 2, образуя общий ключ симметричного шифрования (дешифрования) сообщений между маршрутизаторами X и Y (CE и PE) для устанавливаемого соединения.

Аналогично осуществляется взаимная аутентификация и создание общего ключа шифрования в том случае, когда инициатором аутентификации является не маршрутизатор CE, а PE.

Выводы. Проведенный в настоящей работе анализ угроз безопасности сети VPLS и предложения по ее защите могут быть учтены при проектировании таких сетей для операторов связи РФ.

ЛИТЕРАТУРА

1. *Гольдштейн Ф.Б.*, *Гольдштейн Б.С.* Технология и протоколы MPLS. СПб.: БХВ-Петербург, 2005. 304 с.
2. *Оливейн В.* Структура и реализация современной технологии MPLS. М.: Вильямс, 2004. 480 с.
3. *Бельфер Р.А.*, *Петрухин И.С.* Анализ источников угроз информационной безопасности виртуальных частных сетей VPRN на базе сети MPLS // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2013. № 4. С. 79–89.
4. *Бельфер Р.А.* Угрозы безопасности VPN MPLS на участке между соседними маршрутизаторами и защита с помощью IPSec // Электросвязь. 2013. № 4. С. 25–27.
5. *Таненбаум Э.*, *Уэзеролл Д.* Компьютерные сети. СПб.: Питер, 2012. 954 с.
6. *IEEE 802.1d.* Media Access Control Bridges. 2011.
7. *IEEE 802.1q.* Media Access Control Bridges and Virtual Bridged Local Area Networks. 2013.

8. http://xgu.ru/wiki/DHCP_snooping [Электронный ресурс].
9. *Michael H. Behringer*, *Monique J.* Morrow. MPLS VPN Security. Cisco Press, 2005. P. 312.
10. *ITU-T Recommendation X.509.* Information technology — Open Systems Interconnection. The Directory: Authentication framework (1993 edition — version 2, 1997 edition version 3).
11. *ETSI ETS 300 841.* Telecommunications Security; Integrated Services digital Network (ISDN); Encryption Key management system for audio-visual services, 1998.
12. *Бельфер Р.А.* Сети и системы связи (технологии, безопасность) [Электронное учебное издание]. М.: МГТУ им. Н.Э. Баумана, 2012. 738 с.

REFERENCES

[1] Gol'dshteyn F.B., Gol'dshteyn B.S. Tekhnologiya i protokoly MPLS [Technology and MPLS protocols]. SPb., BKhV-Peterburg Publ., 2005. 304 p.
[2] Alwayn V. Advanced MPLS design and implementation (CCIE professional development). Cisco Press, 2001. 496 p. (Russ. ed.: Oliveyn V. Struktura i realizatsiya sovremennoy tekhnologii MPLS [Design and implementation of modern technology MPLS]. Moscow, Vil'yams Publ., 2004. 480 p.).
[3] Bel'fer R.A., Petrukhin I.S. Analysis of sources of information security threats to MPLS-based VPRNs. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2013, no. 4, pp. 79–89 (in Russ.).
[4] Bel'fer R.A. VPN MPLS security threats in the area between neighboring routers and IPSec protection. *Elektrosvyaz'* [Telecommunications and Radio Engineering], 2013, no. 4, pp. 25–27 (in Russ.).
[5] Tanenbaum A., Wetherall D. Computer Networks. Prentice Hall, 5 Ed., 2010. 960 p. (Russ. ed.: Tanenbaum E., Uezeroll D. Komp'yuternye seti. SPb., Piter Publ., 2012. 954 p.).
[6] IEEE 802.1d. Media Access Control Bridges. IEEE, 2011.
[7] IEEE 802.1q. Media Access Control Bridges and Virtual Bridged Local Area Networks. IEEE, 2013.
[8] Samoylenko N. DHCP snooping. WIKI-site on UNIX / LINUX-systems and systems with open source software (in Russ.). Available at: http://xgu.ru/wiki/DHCP_snooping (accessed 01.11.2014).
[9] Behringer Michael H., Morrow Monique J. MPLS VPN Security. Cisco Press, 2005. 312 p.
[10] ITU-T Recommendation X.509. Information technology — Open Systems Interconnection. The Directory: Authentication framework. ITU, 1993 ed., ver. 2. ITU, 1997 ed., ver. 3.
[11] ETSI ETS 300 841. Telecommunications Security; Integrated Services digital Network (ISDN); Encryption Key management system for audio-visual services. ETSI, 1998. 30 p. Available at: http://www.etsi.org/deliver/etsi_i_ets/300800_300899/300841/01_30_9742/ets_300841e01v.pdf (accessed 01.11.2014).
[12] Bel'fer R.A. Seti i sistemy svyazi (tekhnologii, bezopasnost'). Elektronnoe uchebnoe izdanie na CD-ROOM [Network and communication system (technology, security). Electronic educational edition at CD-ROM]. Moscow, MGTU im. N.E. Baumana Publ., 2012. 738 p.

Статья поступила в редакцию 18.06.2014

Бельфер Рувим Абрамович — доцент кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор 97 научных работ в области информационных технологий.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Bel’fer R.A. — assoc. professor of “Information Security” department of the Bauman Moscow State Technical University. Author of 97 publications in the field of information technologies.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.

Петрухин Илья Сергеевич – системный инженер “INLINE Technologies”. Автор двух научных работ в области информационной безопасности.
“INLINE Technologies”, Российская Федерация, 125167, Москва, Ленинградский пр-т, д. 39, стр. 80.

Petrukhin I.S. — system engineer of “INLINE Technologies”. Author of two publications in the field of information security.
“INLINE Technologies”, Leninskiy pr. 39 (80), Moscow, 125167 Russian Federation.

Тепикин Андрей Павлович — студент кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор одной научной работы в области информационной безопасности.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Tepikin A.P. — student of “Information security” department of the Bauman Moscow State Technical University. Author of one publication in the field of information security.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.