Network Working Group
Request for Comments: 2661
Category: Standards Track

W. Townsley
A. Valencia
cisco Systems
A. Rubens
Ascend Communications
G. Pall
G. Zorn
Microsoft Corporation
B. Palter
Redback Networks

August 1999

Протокол туннелирования на уровне 2 - L2TP

Layer Two Tunneling Protocol "L2TP"

Статус документа

Этот документ задаёт проект стандартного протокола Internet для сообщества Internet и служит приглашением к дискуссии в целях развития и совершенствования. Текущее состояние стандартизации и статус протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Авторские права

Аннотация

В этом документе описан протокол туннелирования на уровне 2 (L2TP[1]). Документ STD 51, RFC 1661 определяет мультипротокольный доступ по протоколу PPP [RFC1661]. L2TP обеспечивает возможности туннелирования пакетов PPP через промежуточную сеть максимально прозрачным для приложений и конечных пользователей способом.

Оглавление

1.0 Введение....2
1.1 Уровни требований....3
1.2 Термины....3
2.0 Топология....4
3.0 Обзор протокола....4
3.1 Формат заголовка L2TP....4
3.2 Типы управляющих сообщений....5
4.0 AVP для управляющих сообщений....6
4.1 Формат AVP....6
4.2 Обязательные AVP....6
4.3 Сокрытие значений атрибутов AVP....7
4.4 Описание AVP....8
4.4.1 AVP, применимые для всех управляющих сообщений....8
4.4.2 Коды результатов и ошибок....8
4.4.3 AVP для контроля управляющих сообщений....9
4.4.4 AVP для управления вызовами....12
4.4.5 AVP для Proxy LCP и аутентификации....15
4.4.6 AVP для статуса вызовов....17
5.0 Работа протокола....18
5.1 Организация управляющего соединения....18
5.1.1 Аутентификация туннеля....18
5.2 Организация сессии....18
5.2.1 Организация входящего вызова....19
5.2.2 Организация исходящего вызова....19
5.3 Пересылка кадров PPP....19
5.4 Использование порядковых номеров в канале данных....19
5.5 Keepalive (Hello)....19
5.6 Разрыв сессии....20
5.7 Разрыв управляющего соединения....20
5.8 Гарантированная доставка управляющих сообщений....20
6.0 Спецификация протокола управляющего соединения....21
6.1 Запрос SCCRQ....21
6.2 Отклик SCCRP....21
6.3 Отклик SCCCN....22
6.4 Уведомление StopCCN....22
6.5 Сообщение HELLO....22

[1]Layer Two Tunneling Protocol.

6.6 Запрос для входящего вызова (ICRQ)....22
6.7 Ответ на входящий вызов (ICRP)....23
6.8 Входящий вызов принят (ICCN)....23
6.9 Запрос для исходящего вызова (OCRQ)....23
6.10 Отклик для исходящего вызова (OCRP)....23
6.11 Исходящее соединение организовано (OCCN)....24
6.12 Уведомление о разрыве соединения (CDN)....24
6.13 Уведомление об ошибке в сети WAN (WEN)....24
6.14 Установка параметров канала (SLI)....24
7.0 Машина состояний управляющего соединения....24
7.1 Операции протокола управляющего соединения....25
7.2 Состояния управляющего соединения....25
7.2.1 Организация управляющего соединения....25
7.3 Синхронизация....26
7.4 Входящие вызовы....26
7.4.1 Состояния LAC для входящих вызовов....26
7.4.2 Состояния LNS для входящих вызовов....27
7.5 Исходящие вызовы....27
7.5.1 Состояния LAC для исходящих вызовов....27
7.5.2 Состояния LNS для исходящих вызовов....28
7.6 Разрыв туннеля....28
8.0 L2TP в разных средах....28
8.1 L2TP через UDP/IP....28
8.2 IP....29
9.0 Вопросы безопасности....29
9.1 Безопасность конечных точек туннеля....29
9.2 Защита на уровне пакетов....29
9.3 Сквозная защита....30
9.4 L2TP и IPsec....30
9.5 Аутентификация PPP....30
10.0 Взаимодействие с IANA....30
10.1 Атрибуты AVP....30
10.2 Значения Message Type AVP....30
10.3 Значения Result Code AVP....30
10.3.1 Значения поля Result Code....30
10.3.2 Значения поля Error Code....30
10.4 Framing Capabilities и Bearer Capabilities....30
10.5 Значения Proxy Authen Type AVP....31
10.6 Биты заголовка AVP....31
11.0 Литература....31
12.0 Благодарности....31
13.0 Адреса авторов....31
Приложение A. Slow Start и Congestion Avoidance на канале управления....32
Приложение B. Примеры управляющих сообщений....32
B.1. Этапы организации туннеля....32
B.2. Потеря пакета с повторной передачей....33
Приложение C. Интеллектуальная собственность....33
Полное заявление авторских прав....33

1.0 Введение

PPP [RFC1661] определяет механизм инкапсуляции для доставки пакетов разных протоколов через соединения уровня 2 (L2) типа «точка-точка». Обычно пользователь организует соединение L2 с сервером доступа (NAS[1]), используя подходящий метод связи (например, модемное соединение через телефонную линию, ISDN, ADSL и т. п.) и протокол PPP «поверх» физического соединения. В такой конфигурации терминальные точки L2 и PPP размещаются на одном физическом устройстве (т. е., NAS).

L2TP расширяет модель PPP, позволяя разносить терминальные точки L2 и PPP на разные устройства, соединённые через сеть с коммутацией пакетов. С помощью L2TP пользователь организует соединение L2 с концентратором доступа (например, модемный пул, ADSL DSLAM и т. п.), а концентратор туннелирует кадры PPP в NAS. Это позволяет перенести реальную обработку пакетов PPP с терминального устройства L2.

Одним из очевидных преимуществ такого разделения является то, что взамен требования завершать соединения L2 на NAS (это может потребовать оплаты междугородных соединений) они могут заканчиваться на (локальном) концентраторе, который распространит сессию PPP через сетевую инфраструктуру совместного использования (например, Frame Relay или Internet). С точки зрения пользователя функциональных различий между этими вариантами просто не будет.

L2TP позволяет также решить проблему расщепления групп (multilink hunt-group splitting). Расширение Multilink PPP [RFC1990] требует, чтобы все каналы, образующие композитное соединение, были связаны с одним сервером NAS. Благодаря возможности расширения сессий PPP за пределы точки физического завершения, протокол L2TP может использоваться для организации завершения всех каналов на одном устройстве NAS. Это позволяет организовать многоканальные соединения даже в тех случаях, когда используется множество физических устройств NAS.

В этом документе определён протокол управления для создания по запросам туннелей между парами узлов и выполнения связанной с этим инкапсуляции для мультиплексирования множества туннелируемых сессий PPP.

[1] Network Access Server - сервер доступа в сеть.

1.1 Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с [RFC2119].

1.2 Термины

Analog Channel - аналоговый канал
Коммутируемый коммуникационный путь, предназначенный для передачи звука с полосой частот 3,1 КГц в каждом направлении.

Attribute Value Pair (AVP) - пара «атрибут-значение»
Объединение переменного размера с уникальным атрибутом (Attribute), представленным целым числом и значением (Value), содержащим реальные данные, идентифицируемые атрибутом. Множество AVP образуют управляющие сообщения (Control Message), служащие для организации, поддержки и удаления туннелей.

Call - вызов
Соединение (или попытка такового) между удалённой системой (Remote System) и LAC. Примером может служить телефонный звонок через сеть PSTN. Соединение (входящее или исходящее) между Remote System и LAC приводит к созданию сессии L2TP в ранее созданном туннеле между LAC и LNS. (см. также Session, Incoming Call, Outgoing Call).

Called Number - вызываемый номер
Индикация принимающей вызов стороны (например, телефонный номер).

Calling Number - вызывающий номер
Индикация вызывающей стороны на приёмной стороне (например, телефонный номер).

CHAP
Challenge Handshake Authentication Protocol [RFC1994] - протокол криптографически защищённой аутентификации PPP, в котором по линии не передаётся паролей в открытом виде.

Control Connection - управляющее соединение
Управляющее соединение существует в основной полосе туннеля и служит для организации, поддержки и разрыва сессий или самого туннеля.

Control Messages - управляющие сообщения
Управляющими сообщениями обмениваются между собой пары устройств LAC и LNS через существующий между ними туннель. Управляющие сообщения относятся к сессиям в данном туннеле и самому туннелю.

Digital Channel - цифровой канал
Коммутируемый коммуникационный путь предназначенный для передачи в обоих направлениях цифровой информации.

DSLAM
Модуль доступа по цифровым абонентским линиям (DSL[1]) - сетевое устройство, используемое для реализации сервиса DSL. Обычно представляет собой концентратор линий DSL в центральном офисе (CO) или местной станции.

Incoming Call - входящий вызов
Вызов, полученный LAC и туннелируемый на LNS (см. Call, Outgoing Call).

L2TP Access Concentrator (LAC) - концентратор доступа L2TP
Узел, который на одной стороне имеет конечные точки туннелей L2TP, а на другой стороне является партнёром сетевого сервера L2TP (LNS). LAC размещается между LNS и удалённой системой, пересылая пакеты между ними. Пакеты от LAC к LNS требуют туннелирования L2TP в соответствии с данным документом. Соединение LAC с удалённой системой является локальным (см. Client LAC) или PPP-каналом.

L2TP Network Server (LNS) - сетевой сервер L2TP
Узел, который является конечной точкой туннеля L2TP и партнёром LAC. LNS является логической точкой завершения сессии PPP, которая будет туннелироваться от удалённой системы через LAC.

Management Domain (MD) - домен управления
Сеть или сети, находящиеся под единым администрированием. Например, доменом управления для LNS может быть обслуживаемая им корпоративная сеть, а доменом управления LAC - ISP, который владеет управляет им.

Network Access Server (NAS) - сервер доступа в сеть
Устройство, обеспечивающее локальный сетевой доступ для пользователей через сеть удалённого доступа (например, PSTN). NAS может также служить в качестве LAC и/или LNS.

Outgoing Call - исходящий вызов
Вызов, организуемый LAC от имени LNS (см. Call, Incoming Call).

Peer - партнёр
В контексте L2TP партнёрами являются LAC или LNS. Партнёром LAC является LNS и наоборот. В контексте PPP партнёрами являются обе стороны соединения PPP.

POTS - телефонная сеть
Телефонная сеть общего пользования.

Remote System - удалённая система
Конечная система или маршрутизатор, подключенный к удалённой сети доступа (например, PSTN) и являющийся инициатором или адресатом вызова. Для обозначения удалённой системы используются также термины dial-up client или virtual dial-up client.

Session - сессия
Протокол L2TP ориентирован на соединения. LNS и LAC поддерживают состояние для каждого инициированного или принятого LAC вызова (Call). Сессия L2TP создаётся между LAC и LNS при организации сквозного соединения PPP между удалённой системой и LNS. Дейтаграммы, относящиеся к соединению PPP, передаются через туннель между LAC и LNS. Организованные сессии L2TP однозначно связаны с соответствующими вызовами (см. Call).

Tunnel - туннель
Туннели организуются между LAC и LNS. Туннель включает управляющее соединение и может также включать одну или множество сессий L2TP. Через туннель между LAC и LNS передаются инкапсулированные дейтаграммы PPP и управляющие сообщения.

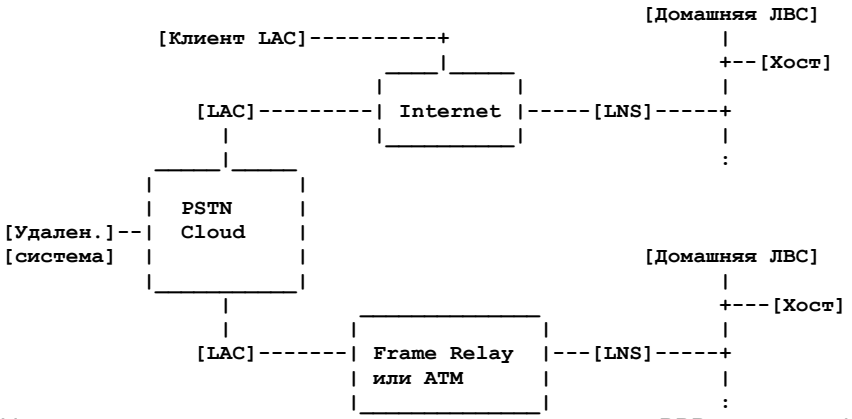
[1]Digital Subscriber Line.

Zero-Length Body (ZLB) Message - сообщение нулевого размера

Управляющий пакет, состоящий лишь из заголовка L2TP. Сообщения ZLB служат для явного подтверждения пакетов на каналах с гарантированной доставкой.

2.0 Топология

На рисунке показан типовой случай использования L2TP. Целью является организация туннеля для кадров PPP между удалённой системой или клиентом LAC и LNS в домашней ЛВС.



Удалённая система инициирует организацию соединения PPP через телефонную сеть (PSTN Cloud) с LAC. После этого LAC туннелирует соединение PPP через Internet, Frame Relay или ATM Cloud до LNS, что обеспечивает доступ в домашнюю ЛВС. Удалённой системе предоставляется адрес из домашней ЛВС в результате согласования PPP NCP. Процедуры AAA[1] доменом управления домашней ЛВС как для случая прямого подключения клиента к серверу доступа NAS.

Клиент LAC (хост с поддержкой L2TP) может также участвовать в создании туннеля в домашнюю ЛВС без привлечения отдельного LAC. В этом случае хост с программным клиентом LAC уже имеет соединение с публичной сетью Internet. Создаётся «виртуальное» соединение PPP и локальный клиент L2TP LAC создаёт туннель до LNS. Как и в предыдущем случае функции AAA будут обеспечиваться доменом управления домашней ЛВС.

3.0 Обзор протокола

L2TP использует два типа сообщений - управление и данные. Управляющие сообщения служат для организации, поддержки и удаления туннелей и вызовов. Сообщения с данными служат для инкапсуляции кадров PPP, передаваемых через туннель. Для управляющих сообщений используется надёжный канал управления (Control Channel) в L2TP, обеспечивающий гарантированную доставку (см. параграф 5.1). При возникновении потери пакетов повторной передачи пакетов данных не производится.

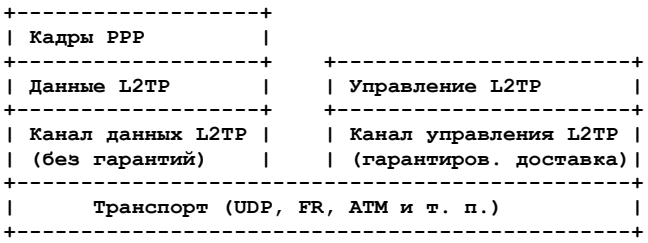


Рисунок 3.0. Структура протокола L2TP.

На рисунке 3.0 показана передача кадров PPP и управляющих сообщений через каналы данных и управления L2TP. Кадры PPP передаются без гарантий доставки через канал данных с инкапсуляций сначала в L2TP, а затем в пакетный транспорт (UDP, Frame Relay, ATM и т. п.) Управляющие сообщения передаются через надёжный канал управления L2TP в основной полосе того же пакетного транспорта.

Для всех управляющих сообщений требуется указывать порядковые номера, используемые для обеспечения гарантий доставки. Порядковые номера в пакетах данных могут использоваться для обеспечения порядка доставки и обнаружения потерь.

Все значения помещаются в соответствующие поля и передаются в сетевом порядке (сначала старшие октеты).

3.1 Формат заголовка L2TP

Пакеты L2TP для управления и данных используют общий формат заголовков. Для необязательных полей пространство в пакете не используется при отсутствии поля. Отметим, что необязательные для пакетов данных поля Length, Ns и Nr являются обязательными в управляющих сообщениях.

Формат заголовков показан на рисунке.

[1]Authentication, Authorization and Accounting - аутентификация, проверка полномочий и учёт.

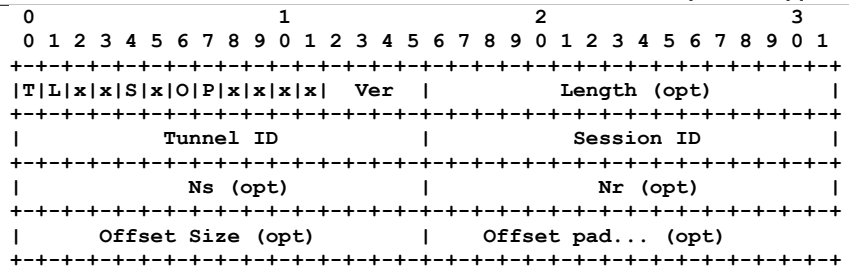


Рисунок 3.1. Формат заголовков L2TP.

Флаг типа (T) указывает тип сообщения (0 для данных, 1 для управляющих сообщений).

Установленный флаг размера (L) говорит о присутствии поля Length. В управляющих сообщениях этот бит **должен** быть установлен.

Флаги x зарезервированы для будущих расширений. Соответствующие биты **должны** устанавливаться в 0 при передаче и игнорироваться на приёмной стороне.

Установленный флаг S говорит о наличии полей Ns и Nr. В управляющих сообщениях этот бит **должен** быть установлен.

Установленный флаг смещения (O) говорит о наличии поля Offset Size. В управляющих сообщениях этот бит **должен** быть сброшен (0).

Установленный флаг приоритета (P) означает, что этому сообщению с данными следует предоставить преимущество в локальных очередях и при передаче. Например, эхо-запросы LCP, используемые для сохранения живучести канала, следует передавать с установленным флагом приоритета. Если флаг не используется то при наличии локальной перегрузки сообщения keepalive могут теряться. Этот флаг используется только для сообщений с данными, а в управляющих сообщениях **должно** устанавливаться P = 0.

Поле Ver **должно** иметь значение 2, соответствующее версии сообщений с данными протокола L2TP, описанных в этом документе. Значение 1 зарезервировано для возможности детектирования пакетов L2F [RFC2341], которые могут приходить вперемешку с пакетами L2TP. Пакеты с неизвестным значением поля Ver **должны** отбрасываться.

Поле Length показывает общий размер сообщения в октетах.

Поле Tunnel ID служит идентификатором управляющего соединения. Туннели L2TP обозначаются идентификаторы с локальной значимостью. По этой причине один и тот же туннель может иметь на каждой стороне разные значения Tunnel ID. Поле Tunnel ID в сообщении предназначено для получателя, а не для отправителя. Значения Tunnel ID выбираются и информация о них передаётся в Assigned Tunnel ID AVP при создании туннеля.

Поле Session ID указывает идентификатор сессии в туннеле. Сессии L2TP обозначаются идентификаторами локальной значимости. Это означает, что одна и та же сессия может иметь разные значения Session ID на разных концах. Значение Session ID в каждом сообщении предназначено для получателя, а не отправителя. Значения Session ID выбираются и передаются в Assigned Session ID AVP при организации сессии.

Ns указывает порядковый номер передаваемого сообщения. Отсчёт начинается с 0 и номер увеличивается на 1 для каждого последующего сообщения (модуль для нумерации 2^{16}). Дополнительная информация об использовании этого поля приводится в параграфах 5.8 и 5.4.

Nr показывает порядковый номер, который ожидается в следующем принятом управляющем сообщении. Таким образом, Nr представляет собой значение Ns из принятого последним без нарушения порядка сообщения плюс 1 (модуль для нумерации 2^{16}). В сообщениях с данными поле Nr является резервным и, при его использовании (как указано флагом S), **должно** игнорироваться на приёмной стороне. Дополнительная информация об использовании этого поля приводится в параграфе 5.8.

Поле Offset Size (при его наличии) указывает число октетов в заголовке L2TP, после которого ожидается наличие данных. Реальное заполнение спецификацией не задаётся. При наличии поля смещения заголовок L2TP завершается последним байтом этого заполнения.

3.2 Типы управляющих сообщений

Message Type AVP (см. параграф 4.4.1) определяет конкретный тип передаваемого сообщения. Напомним (параграф 3.1), что это относится только к управляющим сообщениям (сообщениям с T = 1).

Данный документ определяет перечисленные ниже типы сообщений (описание и применение сообщений в параграфах 6.1 - 6.14).

Поддержка управляющих соединений

0 (резерв)

1 (SCCRQ) Start-Control-Connection-Request

2 (SCCRP) Start-Control-Connection-Reply

3 (SCCCN) Start-Control-Connection-Connected

4 (StopCCN) Stop-Control-Connection-Notification

5 (резерв)

6 (HELLO) Hello

Управление соединениями

7 (OCRQ) Outgoing-Call-Request

8 (OCRP) Outgoing-Call-Reply

9 (OCCN) Outgoing-Call-Connected

10 (ICRQ) Incoming-Call-Request

11 (ICRP) Incoming-Call-Reply

12 (ICCN) Incoming-Call-Connected

13 (резерв)

14 (CDN) Call-Disconnect-Notify

Сообщения об ошибках

15 (WEN) WAN-Error-Notify

Управление сеансами PPP

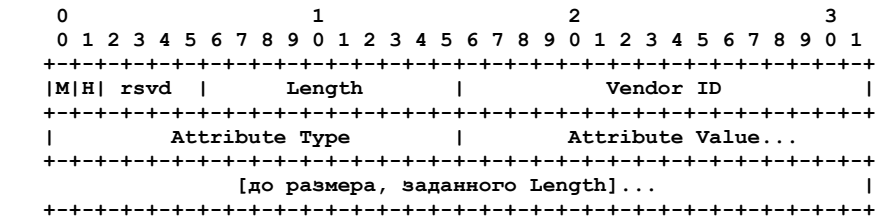
16 (SLI) Set-Link-Info

4.0 AVP для управляющих сообщений

Для обеспечения максимальной расширяемости с сохранением интероперабельности в L2TP используется однотипное представление типов и сообщений. Это представление называется AVP[1] и используется в оставшейся части документа.

4.1 Формат AVP

Каждая пара AVP представляется в виде:



Первые 6 битов задают маску, описывающую общие атрибуты AVP.

В этом документе определены два бита маски, а прочие оставлены для будущих расширений. Резервные биты **должны** устанавливаться в 0. AVP, полученные с установленными в 1 резервными битами маски, **должны** трактоваться, как нераспознанные AVP.

Бит M[2]. Определяет поведение, требуемое от реализации, принявшей AVP, которую не удалось распознать. При установленном флаге M приём нераспознанной AVP в сообщении, связанном с конкретной сессией, такая сессия **должна** прерываться. Если бит M установлен и AVP не удалось распознать в сообщении, связанном с туннелем, этот туннель (и все сессии в нем) **должен** быть разорван. При сброшенном флаге M нераспознанные AVP **должны** игнорироваться. Обработка управляющего сообщения в этом случае продолжается.

Бит H[3]. Указывает на сокрытие данных в поле Attribute Value пары AVP. Это свойство может использоваться для предотвращения данных, которые не следует раскрывать (например, пользовательских паролей) в открытом виде внутри AVP. Процедура сокрытия AVP описана в параграфе 4.3.

Length. Задаёт число октетов (включая поле Overall Length и маску) в данной AVP. Значение Length можно рассчитать, добавив 6 к размеру поля Attribute Value в октетах. Само поле имеет размер 10 битов, что позволяет представлять поля размером до 1023 октетов в одной AVP. Минимальное значение поля Length для AVP составляет 6. В этом случае поле Attribute Value отсутствует.

Vendor ID. Значение из выделенного агентством IANA реестра SMI Network Management Private Enterprise Codes [RFC1700]. Значение 0, соответствующее принятым IETF атрибутам, используется для всех AVP, определённых в данном документе. Любой производитель, желающий реализовать свои расширения L2TP, может использовать своё значение Vendor ID вместе с приватными значениями Attribute, что гарантирует отсутствие конфликтов с расширениями других производителей и будущими расширениями IETF. Отметим, что 16 битов поля Vendor ID ограничивают число идентификаторов значением 65 535.

Attribute Type. Двухоктетное значение с уникальной интерпретацией среди всех AVP для данного Vendor ID.

Attribute Value. Реальное значение атрибута, заданного полями Vendor ID и Attribute Type. Это поле следует непосредственно за полем Attribute Type и включает число октетов до смещения, заданного полем Length (т. е., Length - 6 октетов заголовка). При Length = 6 это поле отсутствует.

4.2 Обязательные AVP

Получение неизвестной AVP с установленным битом M является катастрофой для сессии или связанного с ней туннеля. По этой причине флаг M следует задавать лишь для AVP, которые критически важны для работы сессии или туннеля. Кроме того, в случае получения устройством LAC или LNS неизвестной AVP с установленным битом M и последующего отключения сессии или туннеля, отправившая такую (обязательную) AVP сторона должна быть готова к

[1] Attribute-Value Pair - пара «атрибут-значение».
[2] Mandatory - обязательный.
[3] Hidden - скрытый.

возникновению проблем взаимодействия. При определении AVP с установленным битом M (особенно для фирменных AVP) следует принимать во внимание возможные последствия.

Если имеется адекватная альтернатива установке бита M, следует ею воспользоваться. Например, вместо отправки AVP с установленным битом M для проверки наличия соответствующего расширения можно можно передать AVP в запросе с ожиданием получить соответствующую AVP в ответном сообщении.

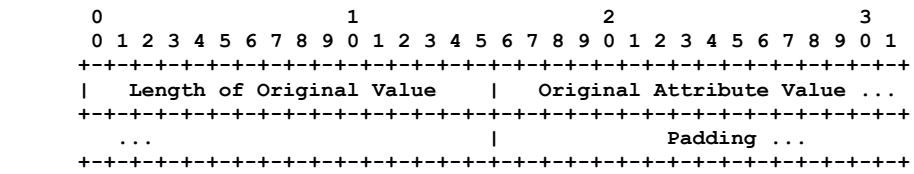
При использовании бита M в новых AVP (не определённых в данном документе) **должна** обеспечиваться возможность отключения соответствующей функции, чтобы такие AVP не передавались или бит M не устанавливался.

4.3 Сокрытие значений атрибутов AVP

Бит H в заголовке каждого AVP обеспечивает механизм индикации принимающей стороне сокрытия содержимого AVP или его присутствия в открытом виде. Это свойство помогает предотвратить раскрытие конфиденциальной информации типа паролей или имён пользователей.

Флаг H **должен** устанавливаться только в тех случаях, когда LAC и LNS известен общий секрет. Это тот же секрет, который служит для аутентификации туннеля (параграф 5.1.1). Если бит H установлен в любом из AVP данного управляющего сообщения, в этом сообщении должна также присутствовать Random Vector AVP и эта пара **должна** размещаться перед первым AVP с H = 1.

Сокрытие значение AVP выполняется в несколько этапов. Сначала берутся исходные размер и значение AVP, которые затем кодируются в субформат Hidden AVP, показанный ниже.



Length of Original Attribute Value - это поле указывает размер исходного значения скрываемого атрибута в октетах. Это значение требуется сохранять, поскольку размер меняется в результате заполнения Padding.

Original Attribute Value - исходное значение скрываемого атрибута.

Padding - дополнительные октеты со случайными значениями, используемые для сокрытия размера исходного значения атрибута.

Для маскировки размера скрываемых данных в субформате **может** использоваться показанное выше заполнение. Поле Padding **не** учитывается в Length of Original Attribute Value, но меняет размер получаемой в результате AVP. Например, если скрывается 4-октетное значение атрибута, поле размера нескрытой AVP будет иметь значение 10 (6 + 4). После сокрытия размер AVP будет равен 6 + размер Attribute Value + размер Length of Original Attribute Value + Padding. Таким образом при 12 октетах заполнения размер AVP будет 6 + 4 + 2 + 12 = 24 октета.

После этого определяется хэш MD5 для конкатенации:

2 октета номера атрибута из AVP;

разделяемый секрет;

случайный вектор произвольной длины.

Используемый в этом хэше случайный вектор передаётся в поле Random Vector AVP. Эта пара Random Vector AVP должна помещаться отправителем в сообщение впереди всех скрываемых AVP. Один и тот же случайный вектор может использоваться для множества AVP в одном сообщении. При использовании разных векторов для сокрытия последовательных AVP новый Random Vector AVP должен помещаться перед первой AVP, к которой он будет применяться.

Хэш MD5 используется в операции XOR применительно к первым 16 (или меньше) октетам Hidden AVP Subformat и результат помещается в поле Attribute Value скрываемой пары Hidden AVP. Если размер Hidden AVP Subformat меньше 16 октетов, субформат преобразуется, как будто поле Attribute Value дополнено до 16 октетов перед операцией XOR, но меняются только октеты, реально присутствующие в Subformat , а размер AVP не меняется.

Если размер Subformat превышает 16 октетов, рассчитывается второе значение MD5 для потока октетов, состоящего из разделяемого секрета, за которым следует результат первой операции XOR. Полученное значение используется для операции XOR с вторым сегментом из 16 (или меньше) октетов Subformat и помещается в соответствующие октеты поля Value пары Hidden AVP.

При необходимости эта операция повторяется с использованием разделяемого секрета с каждым результатом XOR для генерации следующего хэш-значения, применяемого в операции XOR со следующим сегментом значения.

Метод сокрытия был взят из RFC 2138 [RFC2138], заимствовавшего его, в свою очередь из раздела Mixing in the Plaintext книги Network Security, авторами которой являются Kaufman, Perlman и Speciner [KPS]. Ниже приведено подробное разъяснение этого метода.

Возьмём разделяемый секрет S, случайный вектор RV и значение атрибута AV. Разделим поле значения на 16-октетные блоки p1, p2 и т. д., дополнив при необходимости последний блок случайными данными до размера 16 октетов. Возьмём шифрованные блоки c(1), c(2) и т. д. Определим также промежуточные значения b1, b2 и т. д.

```
b1 = MD5(AV + S + RV)    c(1) = p1 xor b1
b2 = MD5(S  + c(1))      c(2) = p2 xor b2
                .                .
                .                .
                .                .
bi = MD5(S  + c(i-1))    c(i) = pi xor bi
```

String будет содержать c(1)+c(2)+...+c(i), где + обозначает конкатенацию.

При получении случайный вектор берётся из последней пары Random Vector AVP в сообщении, расположенной перед раскрываемой AVP. Описанная выше процедура выполняется в обратном направлении для восстановления исходного значения.

4.4 Описание AVP

В последующих параграфах рассматриваются все L2TP AVP, определяемые в данном документе.

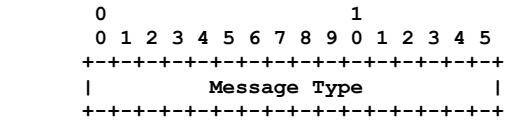
После имени AVP указывается список типов сообщений, в которых может применяться данная AVP. Указывается также назначение AVP и приводится подробное описание формата для Attribute Value и дополнительная информация, которая может потребоваться для корректного применения AVP.

4.4.1 AVP, применимые для всех управляющих сообщений

Message Type (все сообщения)

Message Type AVP (Attribute Type 0) идентифицирует управляющее сообщение и определяет контекст, в котором будет определяться точный смысл последующих AVP.

Формат поля Attribute Value для данной AVP показан ниже.



Message Type представляет собой 2-октетное целое число без знака.

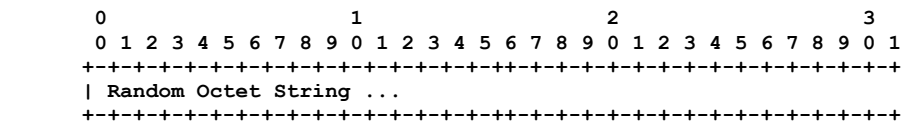
Message Type AVP **должна** быть первой AVP в сообщении, следуя непосредственно после заголовка управляющего сообщения (определен в параграфе 3.1). Список определённых типов управляющих сообщений и их идентификаторы приведены в параграфе 3.2.

Бит обязательности (M) в Message Type AVP имеет специальное значение. Он относится не к данной AVP, как обычно, а ко всему управляющему сообщению. Таким образом, если в Message Type AVP установлен бит M а тип сообщения не известен реализации, туннель **должен** закрываться. Если бит M сброшен, реализация может игнорировать сообщение неизвестного типа. Флаг M **должен** устанавливаться для всех типов сообщений, определённых в этом документе. Эта AVP не может быть скрыта (бит H **должен** быть сброшен). Поле Length для этой AVP имеет значение 8.

Random Vector (все сообщения)

Random Vector AVP (Attribute Type 36) используется для того, чтобы разрешить сокрытие Attribute Value в AVP.

Формат поля Attribute Value для данной AVP показан ниже.



Random Octet String может иметь произвольный размер, хотя рекомендуется использовать случайные векторы не короче 16 октетов. Строка содержит случайный вектор, используемый при расчёте значения MD5 для извлечения или сокрытия значения Attribute Value в AVP (см. параграф 4.2).

В сообщении может присутствовать несколько Random Vector AVP. В этом случае для скрытых AVP используется ближайшая предшествующая пара Random Vector AVP. Данная AVP **должна** предшествовать первой AVP с установленным битом H.

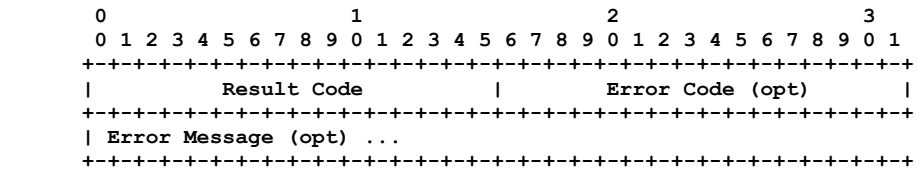
Бит M для данной AVP **должен** иметь значение 1. Такую AVP **недопустимо** скрывать (бит H должен иметь значение 0). Поле Length в данной AVP имеет значение размера Random Octet String + 6.

4.4.2 Коды результатов и ошибок

Result Code (CDN, StopCCN)

Result Code AVP (Attribute Type 1) указывает причину разрыва управляющего канала или сессии.

Формат поля Attribute Value для данной AVP показан ниже.



Result Code представляет собой 2-октетное целое число без знака. Необязательное поле Error Code также является 2-октетным целым числом без знака. За полем Error Code может следовать необязательное поле Error Message. Присутствие полей Error Code и Error Message указывается полем AVP Length. Поле Error Message содержит произвольную строку, обеспечивающую дополнительный (понятный человеку) текст, связанный с ошибкой. Текст для человека во всех сообщениях об ошибках **должен** задаваться в кодировке UTF-8 с использованием принятого по умолчанию языка (Default Language) [RFC2277].

Такие AVP **недопустимо** скрывать (бит H **должен** иметь значение 0). Бит M для таких AVP **должен** иметь значение 1. Поле Length имеет значение 8 при отсутствии Error Code и Error Message, 10 при наличии Error Code без Error Message и 10 + размер Error Message, если присутствуют код и сообщение об ошибке.

Определённые для сообщений StopCCN значения Result Code включают:

0 - резерв

1 - запрос общего типа для сброса управляющего соединения;

2 - типовая ошибка, проблему указывает Error Code;

3 - управляющий канал уже существует;

4 - запрашивающий не имеет полномочий на организацию управляющего канала;

5 - версия протокола у запрашивающего не поддерживает значение Error Code более новой версии;

6 - запрашивающий будет отключён (shut down);

7 - ошибка машины конечных состояний.

Определённые для сообщений CDN значения Result Code включают:

0 - резерв

1 - соединение разорвано в результате потери несущей;

2 - соединение разорвано по причине, указанной кодом ошибки;

3 - соединение разорвано административными мерами;

4 - отказ при соединении по причине недоступности (временно);

5 - отказ при соединении по причине недоступности (постоянная ошибка);

6 - некорректный адресат;

7 - отказ в соединении по причине отсутствия несущей;

8 - отказ в соединении по причине занятости линии;

9 - отказ в соединении по причине слабого сигнала вызова (dial tone);

10 - соединение не было организовано в течение интервала, отведённого устройством LAC;

11 - соединение организовано, но не найдено подходящего кадрирования.

Значения Error Code, определённые ниже, относятся не к каким-либо ошибкам для конкретных запросов L2TP, а к ошибкам протокола или формата сообщений. Если отклик L2TP указывает в своём Result Code ошибку общего типа, следует проверить значение кода General Error для определения причины ошибки. Ниже перечислены определённые в настоящее время значения кодов General Error и краткие описания.

0 - нет ошибок;

1 - нет управляющего соединения для данной пары LAC - LNS;

2 - некорректный размер;

3 - значение одного из полей выходит за допустимые пределы или резервное поле отлично от нуля;

4 - в настоящее время недостаточно ресурсов для обработки операции;

5 - значение Session ID некорректно в данном контексте;

6 - ошибка общего типа, специфическая для производителя LAC;

7 - повторите попытку; если устройству LAC известны другие возможные адресаты LNS, ему следует пытаться использовать один из них; это может служить руководством для LAC, работающего на основе политики LNS (например, наличие множества групп multilink PPP);

8 - сессия или туннель разорваны по причине получения неизвестной AVP с установленным флагом M (см. параграф 4.2). В сообщение об ошибке **следует** включать атрибут вызвавшей проблему AVP в (понятном человеку) текстовом формате.

При использовании кода General Error 6 **следует** включать дополнительную информацию об ошибке в поле Error Message.

4.4.3 AVP для контроля управляющих сообщений

Protocol Version (SCCRP, SCCRQ)

Protocol Version AVP (Attribute Type 2) показывает версию протокола L2TP у отправителя.

Формат поля Attribute Value для данной AVP показан ниже.

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Ver      |     Rev       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

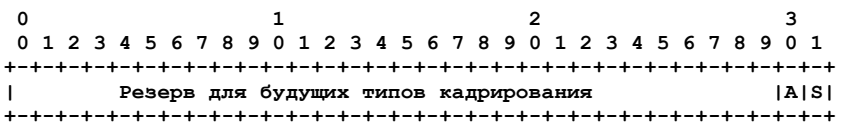
Поле Ver размером 1 октет содержит целое число без знака 1. Поле Rev имеет размер 1 октет и содержит целое число без знака 0. Это указывает протокол L2TP версии 1, вариант 0. Отметим, что это не то же самое, что номер версии, указываемый в заголовке каждого сообщения.

Данную AVP **недопустимо** скрывать (бит H **должен** иметь значение 0). Бит M для данной AVP **должен** иметь значение 1. Поле Length в данной AVP имеет значение 8.

Framing Capabilities (SCCRP, SCCRQ)

Framing Capabilities AVP (Attribute Type 3) показывает партнёру типы кадрирования, поддерживаемые или запрашиваемые отправителем.

Формат поля Attribute Value для данной AVP показан ниже.



Поле Attribute Value является 32-битовой маской, в которой определены 2 бита. Бит A указывает поддержку асинхронного кадрирования, бит S - поддержку синхронного.

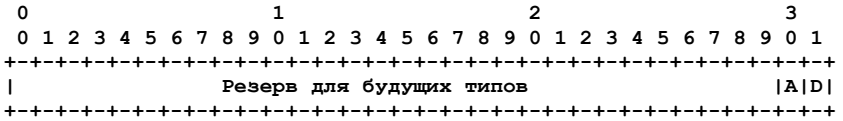
Партнёру **недопустимо** запрашивать входящий или исходящий вызов с Framing Type AVP, задающей значение, которое не было анонсировано в Framing Capabilities AVP, полученной в процессе организации управляющего соединения. При таких попытках вызовы будет отвергаться.

Данная AVP может быть скрытой (H = 1). Бит M в данной AVP **должен** быть установлен (1). Поле Length (без сокрытия) имеет значение 10.

Bearer Capabilities (SCCRP, SCCRQ)

Bearer Capabilities AVP (Attribute Type 4) показывает партнёру типы устройств, поддерживаемых аппаратными интерфейсами отправителя для исходящих вызовов.

Формат поля Attribute Value для данной AVP показан ниже.



Поле Attribute Value является 32-битовой маской, в которой определены 2 бита. Бит A указывает поддержку аналогового доступа, бит D - поддержку цифрового доступа.

Устройствам LNS не следует запрашивать исходящих вызовов, которые задают Bearer Type AVP для типов устройств, не анонсированных в Bearer Capabilities AVP, полученных от LAC при организации управляющего соединения. При возникновении такой попытки она будет завершаться отказом.

Данная AVP **должна** присутствовать, если отправитель может организовывать исходящие вызовы по запросам.

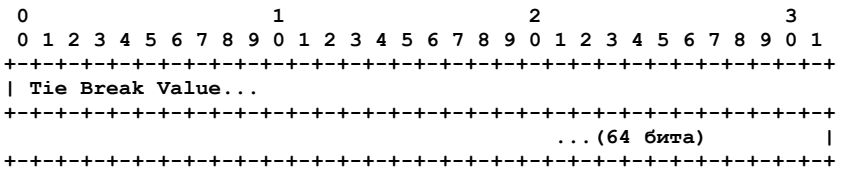
Отметим, что устройство LNS, которое не может работать в качестве LAC, не будет также поддерживать аппаратных компонент для обслуживания входящих или исходящих вызовов и ему следует устанавливать нулевые значения битов A и D в данной AVP или совсем не использовать таких AVP. Устройству LNS, которое может служить LAC и организовывать исходящие вызовы, следует устанавливать биты A и D по своим возможностям. Присутствие этого сообщения не гарантирует организации исходящего вызова по запросу отправителя, а лишь указывает на физическую возможность организации таких вызовов.

Данная AVP может быть скрытой (бит H может быть установлен). Бит M для этой AVP **должен** иметь значение 1. Поле Length (до сокрытия) имеет значение 10.

Tie Breaker (SCCRQ)

Tie Breaker AVP (Attribute Type 5) показывает желание отправителя использовать только один туннель между данными LAC и LNS.

Формат поля Attribute Value для данной AVP показан ниже.



Поле Tie Breaker Value представляет собой 8-октетное значение, которое служит для выбора одного туннеля, когда оба устройства LAC и LNS запрашивают туннельные соединения. Получатель SCCRQ должен проверить свою передачу SCCRQ отправителю и, при наличии таковой, сравнить значения Tie Breaker. По результатам сравнения выбирается меньшее из двух значений и соответствующий ему туннель **должен** быть сброшен без уведомления. Если значения совпадают, обе стороны **должны** сбросить свои туннели.

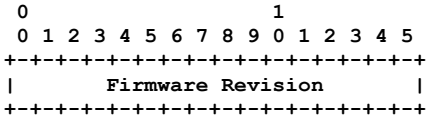
Если на получившей SCCRQ стороне нет значения Tie Breaker, «выигрывает» инициатор отправки Tie Breaker AVP. Если ни одна из сторон не использовала SCCRQ, организуются два раздельных туннеля.

Данную AVP **недопустимо** скрывать (бит H **должен** иметь значение 0). Бит M для данной AVP **должен** быть сброшен (0). Поле Length в данной AVP имеет значение 14.

Firmware Revision (SCCRP, SCCRQ)

Firmware Revision AVP (Attribute Type 6) показывает версию программного кода на устройстве.

Формат поля Attribute Value для данной AVP показан ниже.



Поле Firmware Revision представляет собой 2-октетное целое число без знака, формат представления версии определяется производителем.

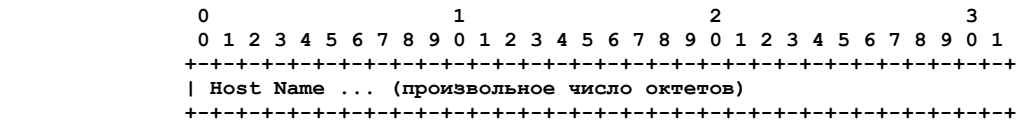
Для устройств без номера версии программного кода (например, компьютеры общего назначения с программными модулями L2TP) может указываться номер версии программ L2TP.

Данная AVP может быть скрытой (бит H может быть установлен). Бит M для этой AVP **должен** иметь значение 0. Поле Length (до сокрытия) имеет значение 8.

Host Name (SCCRP, SCCRQ)

Host Name AVP (Attribute Type 7) указывает имя передавшего атрибут устройства LAC или LNS.

Формат поля Attribute Value для данной AVP показан ниже.



Поле Host Name может иметь произвольный размер, но **должно** быть не короче 1 октета.

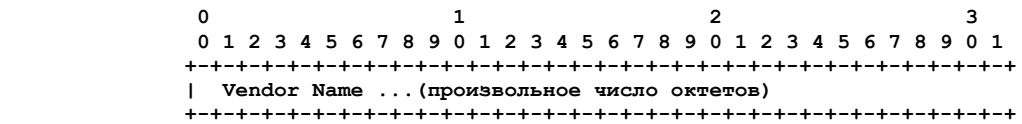
Следует использовать в этом поле по возможности уникальное имя. Для хостов, участвующих в DNS [RFC1034], подойдёт полное доменное имя хоста.

Эту AVP **недопустимо** скрывать (бит H **должен** иметь значение 0). Бит M для данной AVP **должен** быть установлен (1). Поле Length в этой AVP равно размеру Host Name + 6.

Vendor Name (SCCRP, SCCRQ)

Vendor Name AVP (Attribute Type 8) указывает имя производителя (возможно, для человека), описывающее тип используемого устройства LAC или LNS.

Формат поля Attribute Value для данной AVP показан ниже.



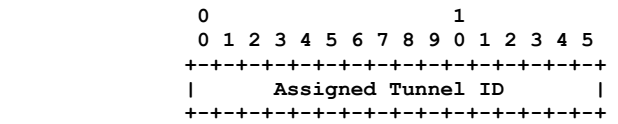
Поле Vendor Name представляет имя производителя в строке символов. Предназначенный для людей текст **должен** использовать кодировку UTF-8 для принятого по умолчанию языка (Default Language [RFC2277]).

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть сброшен (0). Поле Length в этой AVP равно размеру Vendor Name + 6.

Assigned Tunnel ID (SCCRP, SCCRQ, StopCCN)

Assigned Tunnel ID AVP (Attribute Type 9) представляет идентификатор, который будет присвоен данному туннелю отправителем.

Формат поля Attribute Value для данной AVP показан ниже.



Поле Assigned Tunnel ID представляет собой 2-октетное целое число без знака, отличное от 0.

Assigned Tunnel ID AVP организует значение, используемое для мультиплексирования и демультиплексирования туннелей между LNS и LAC. Партнёр L2TP **должен** помещать это значение в поле заголовка Tunnel ID всех сообщений, передаваемых через данный туннель. До получения от партнёра Assigned Tunnel ID AVP управляющие сообщения **должны** передаваться в туннель с Tunnel ID = 0 в заголовках.

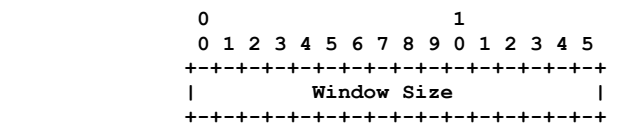
В управляющем сообщении StopCCN пара Assigned Tunnel ID AVP **должна** совпадать с Assigned Tunnel ID AVP, переданной изначально принимающему партнёру, что позволяет идентифицировать туннель даже при получении StopCCN раньше, чем Assigned Tunnel ID AVP.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length в этой AVP (до сокрытия) имеет значение 8.

Receive Window Size (SCCRQ, SCCRP)

Receive Window Size AVP (Attribute Type 10) указывает размер приёмного окна, предлагаемый удаленным партнёром.

Формат поля Attribute Value для данной AVP показан ниже.



Поле Window Size представляет собой 2-октетное целое число без знака.

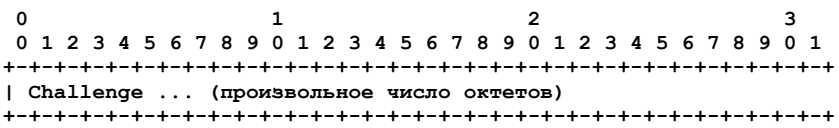
В отсутствии информации партнёр должен устанавливать Window Size = 4 для своего окна передачи. Удалённый партнёр может передать указанное размером окна число управляющих сообщений без ожидания подтверждений.

Эту AVP **недопустимо** скрывать (бит H **должен** иметь значение 0). Бит M для данной AVP **должен** быть установлен (1). Length = 8.

Challenge (SCCRP, SCCRQ)

Challenge AVP (Attribute Type 11) показывает желание партнёра аутентифицировать конечные точки туннеля с использованием механизма в стиле CHAP.

Формат поля Attribute Value для данной AVP показан ниже.



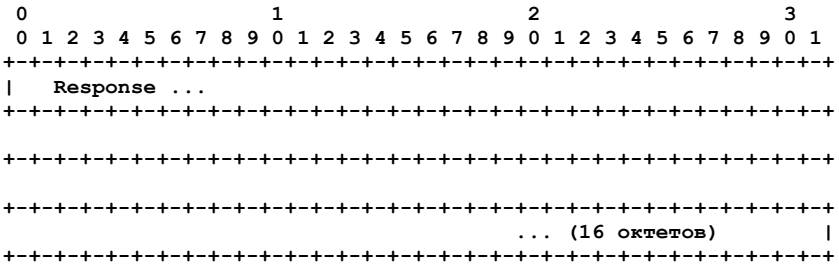
Поле Challenge представляет собой один или множество октетов случайных денных.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP равно размеру Challenge + 6.

Challenge Response (SCCCN, SCCRP)

Response AVP (Attribute Type 13) предоставляет отклик на полученный вызов.

Формат поля Attribute Value для данной AVP показан ниже.



Поле Response имеет размер 16 октетов и представляет собой отклик на вызов в стиле CHAP [RFC1994].

Данная AVP **должна** присутствовать в SCCRP или SCCCN, если в предшествующем SCCRQ или SCCRP был получен вызов. В качестве значения ID при расчёте отклика CHAP используется значение Message Type AVP для данного сообщения (2 для SCCRP или 3 для SCCCN).

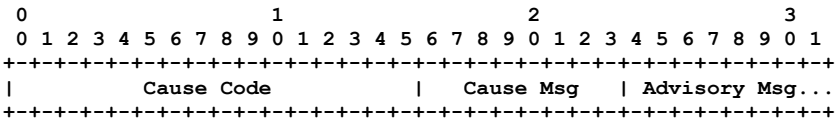
Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 22.

4.4.4 AVP для управления вызовами

Q.931 Cause Code (CDN)

Q.931 Cause Code AVP (Attribute Type 12) используется для предоставления дополнительной информации в случаях незапрошенного разрыва соединений.

Формат поля Attribute Value для данной AVP показан ниже.



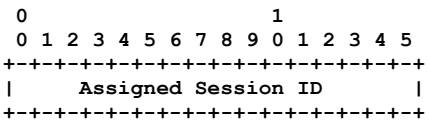
В поле Cause Code возвращается код Q.931 Cause, а в Cause Msg код сообщения Q.931 (например, DISCONNECT), связанного с Cause Code. Оба значения представляются в естественной кодировке ITU [DSS1]. Дополнительный ASCII-текст в поле Advisory Message (его присутствие указывается значением поля AVP Length) служит для дополнительного разъяснения причины разрыва соединения.

Эту AVP **недопустимо** скрывать (бит H **должен** иметь значение 0). Бит M для данной AVP **должен** быть установлен (1). Поле Length в этой AVP равно размеру Advisory Message + 9.

Assigned Session ID (CDN, ICRP, ICRQ, OCRP, OCRQ)

Assigned Session ID AVP (Attribute Type 14) представляет идентификатор, выделяемый для данной сессии отправителем.

Формат поля Attribute Value для данной AVP показан ниже.



Assigned Session ID представляет собой 2-октетное целое число без знака, отличное от 0.

Assigned Session ID AVP обеспечивает идентификатор, служащий для мультиплексирования и демультиплексирования данных, направляемых через туннель между LNS и LAC. Партнёр L2TP **должен** помещать это значение в поле заголовка Session ID всех сообщений, которые будут передаваться через туннель во время существования данной сессии. До получения от партнёра Assigned Session ID AVP, все управляющие сообщения **должны** передаваться ему с Session ID = 0 в заголовках.

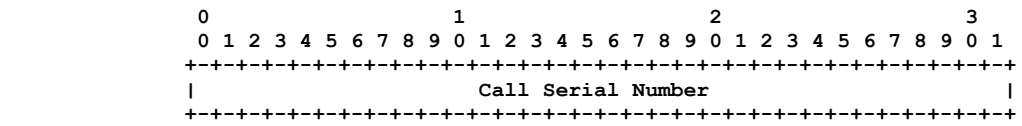
В управляющем сообщении CDN используется та же самая Assigned Session ID AVP, которая ранее была отправлена принимающему партнёру, что позволяет идентифицировать подходящий туннель даже в тех случаях, когда CDN передаётся до получения Assigned Session ID.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 8.

Call Serial Number (ICRQ, OCRQ)

Call Serial Number AVP (Attribute Type 15) показывает идентификатор, присвоенный соединению LAC или LNS.

Формат поля Attribute Value для данной AVP показан ниже.



Поле Call Serial Number имеет размер 32 бита.

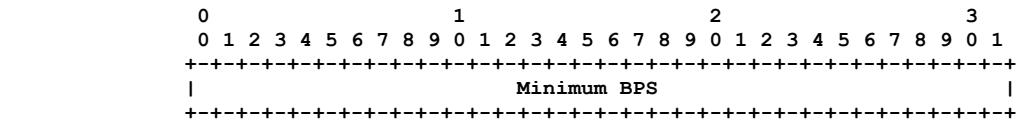
Значение Call Serial Number предназначено для администраторов на обеих сторонах туннеля и позволяет идентифицировать соединения при поиске неисправностей. Значения Call Serial Number следует устанавливать в порядке возрастания и обеспечивать долговременную уникальность нумерации для всех связанных между собой устройств LNS и LAC.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 10.

Minimum BPS (OCRQ)

Minimum BPS AVP (Attribute Type 16) показывает минимально допустимую скорость в линии для данного вызова.

Формат поля Attribute Value для данной AVP показан ниже.



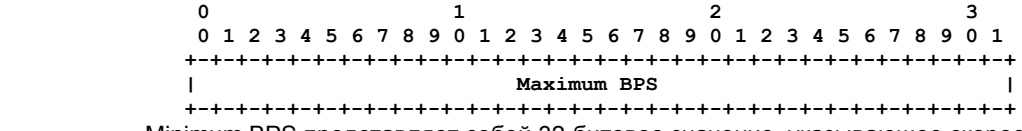
Minimum BPS представляет собой 32-битовое значение, указывающее скорость в бит/сек.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 10.

Maximum BPS (OCRQ)

Maximum BPS AVP (Attribute Type 17) показывает максимально допустимую скорость в линии для этого вызова.

Формат поля Attribute Value для данной AVP показан ниже.



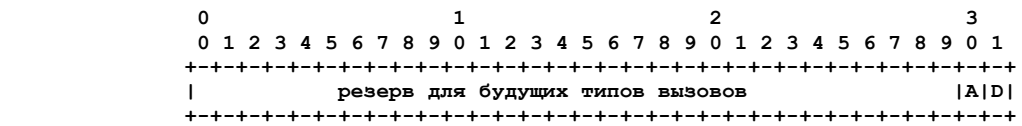
Minimum BPS представляет собой 32-битовое значение, указывающее скорость в бит/сек.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 10.

Bearer Type (ICRQ, OCRQ)

Bearer Type AVP (Attribute Type 18) представляет тип входящего или исходящего вызова.

Формат поля Attribute Value для данной AVP показан ниже.



Поле Bearer Type представляет собой 32-битовую маску, которая показывает свойства (ICRQ) или требования (OCRQ) для вызова. Установленный бит A показывает, что вызов относится к аналоговым каналам, бит D - к цифровым. Установка обоих флагов сразу показывает, что вызовы не различаются или могут размещаться на обоих типах каналов.

Биты поля Value данной AVP **должны** устанавливаться устройством LNS для OCRQ только в тех случаях, когда они были установлены в Bearer Capabilities AVP, полученной от LAC при организации управляющего соединения.

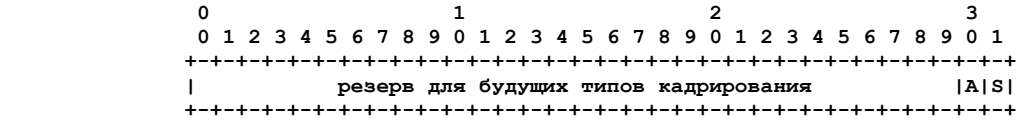
В ICRQ можно не устанавливать ни один из битов A и D. Это будет говорить о том, что вызов принимается не по физическому каналу (например, если LAC и PPP размещаются в одной подсистеме).

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 10.

Framing Type (ICCN, OCCN, OCRQ)

Framing Type AVP (Attribute Type 19) представляет тип кадрирования для входящих или исходящих вызовов.

Формат поля Attribute Value для данной AVP показан ниже.



Framing Type представляет собой 32-битовую маску, которая показывает тип кадрирования PPP, запрашиваемый для OCRQ, или согласованный тип кадрирования PPP для OCCN или ICCN. Тип кадрирования **может** служить модулю PPP на устройстве LNS индикацией опций для использования при согласовании LCP [RFC1662].

Бит A показывает асинхронное кадрирование, бит S - синхронное. Для OCRQ могут устанавливаться оба бита, указывая возможность использования любого типа кадрирования.

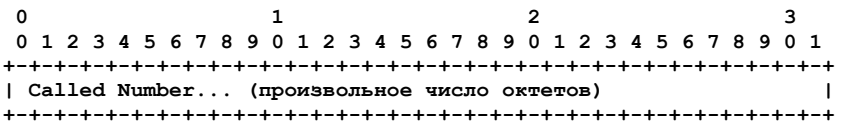
Биты поля Value данной AVP **должны** устанавливаться устройством LNS для OCRQ только в тех случаях, когда они были установлены в Framing Capabilities AVP, полученной от LAC при организации управляющего соединения.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 10.

Called Number (ICRQ, OCRQ)

Called Number AVP (Attribute Type 21) показывает телефонный номер для звонка в OCRQ или номер звонящего в ICRQ.

Формат поля Attribute Value для данной AVP показан ниже.



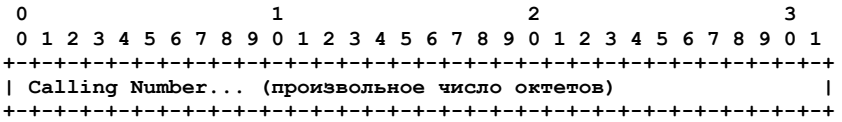
Поле Called Number представляет собой строку ASCII. Для согласования интерпретации значений может потребоваться контакт между администраторами LAC и LNS.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 6 + размер Called Number.

Calling Number (ICRQ)

Calling Number AVP (Attribute Type 22) показывает телефонный номер вызывающей стороны при входящем звонке.

Формат поля Attribute Value для данной AVP показан ниже.



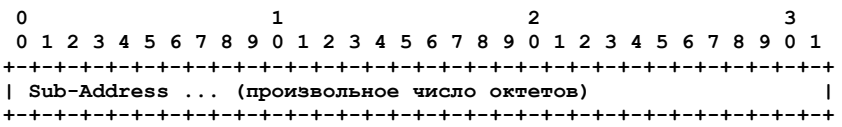
Поле Calling Number представляет собой строку ASCII. Для согласования интерпретации значений может потребоваться контакт между администраторами LAC и LNS.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 6 + размер Calling Number.

Sub-Address (ICRQ, OCRQ)

Sub-Address AVP (Attribute Type 23) представляет дополнительные сведения о звонящем.

Формат поля Attribute Value для данной AVP показан ниже.



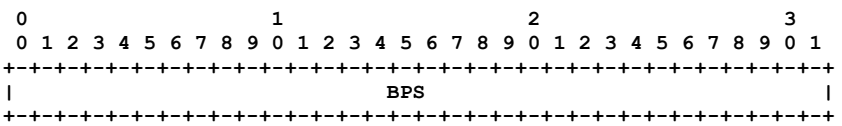
Поле Sub-Address представляет собой строку ASCII. Для согласования интерпретации значений может потребоваться контакт между администраторами LAC и LNS.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 6 + размер Sub-Address.

(Tx) Connect Speed (ICCN, OCCN)

(Tx) Connect Speed BPS AVP (Attribute Type 24) показывает скорость среды, выбранной для попытки соединения.

Формат поля Attribute Value для данной AVP показан ниже.



Поле BPS представляет собой 4-октетное значение, задающее скорость в бит/сек.

При наличии необязательной Rx Connect Speed AVP значение данной AVP представляет скорость передачи с точки зрения LAC (т. е.. потока данных от LAC к удалённой системе). При отсутствии Rx Connect Speed скорость соединения между удалённой системой и LAC предполагается одинаковой для обоих направлений и представленной данной AVP.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 10.

Rx Connect Speed (ICCN, OCCN)

Rx Connect Speed AVP (Attribute Type 38) представляет скорость соединения с точки зрения LAC (поток данных от удалённой системы к LAC).

Формат поля Attribute Value для данной AVP показан ниже.

Поле BPS представляет собой 4-октетное значение, задающее скорость в бит/сек.

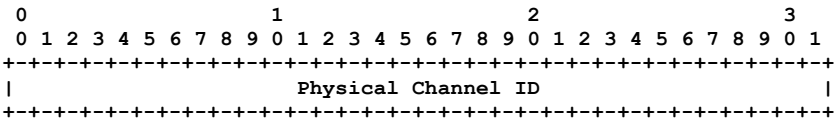
Наличие данной AVP предполагает возможную асимметрию соединения в части скорости.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 10.

Physical Channel ID (ICRQ, OCRP)

Physical Channel ID AVP (Attribute Type 25) представляет номер физического канала, используемого для вызова (зависит от производителя).

Формат поля Attribute Value для данной AVP показан ниже.



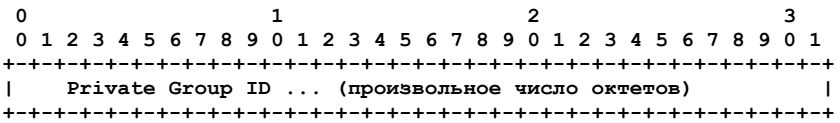
Поле Physical Channel ID представляет собой 4-октетное значение, которое может использоваться только в целях протоколирования.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 10.

Private Group ID (ICCN)

Private Group ID AVP (Attribute Type 37) используется LAC для индикации связи данного вызова с конкретной группой заказчиков.

Формат поля Attribute Value для данной AVP показан ниже.



Private Group ID представляет собой строку октетов произвольной длины.

LNS **может** использовать специальную трактовку сессии PPP и проходящего через неё трафика в соответствии с указаниями партнёра. Например, если устройство LNS имеет отдельные соединения с несколькими приватными сетями, использующими незарегистрированные адреса, данная AVP может указать LAC, что данный вызов связан с конкретной сетью из числа подключённых.

Private Group ID представляет собой строку, соответствующую таблице в LNS, определяющей характеристики указанной группы. LAC **может** определить Private Group ID из отклика RADIUS, локальной конфигурации или иных источников.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть сброшен (0). Поле Length (до сокрытия) в этой AVP имеет значение 6 + размер Private Group ID.

Sequencing Required (ICCN, OCCN)

Sequencing Required AVP (Attribute Type 39) показывает устройству LNS, что в канале данных всегда **должны** присутствовать порядковые номера.

Данная AVP не имеет поля Attribute Value.

Сокрытие данной AVP **недопустимо** (H = 0). Бит M для данной AVP **должен** быть установлен (1), Length = 6.

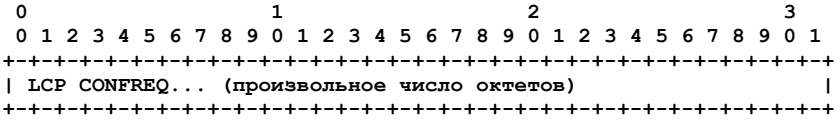
4.4.5 AVP для Proxy LCP и аутентификации

LAC может иметь отвеченные вызовы и согласованные LCP с удалённой системой, которые могут служить для её идентификации. В этом случае могут использоваться рассмотренные ниже AVP, служащие для индикации свойств соединения, запрошенных изначально удалённой системой, свойств, согласованных удалённой системой и LAC, а также аутентификационной информации PPP, переданной и полученной LAC. Эта информация может использоваться для инициирования PPP LCP и аутентификации на LNS, позволяющей PPP продолжить работу без повторного согласования LCP. Отметим, что политика LNS может требовать дополнительного согласования LCP и/или аутентификации, если LAC не является доверенным.

Initial Received LCP CONFREQ (ICCN)

Initial Received LCP CONFREQ AVP (Attribute Type 26) предоставляет LNS значение Initial CONFREQ, полученное LAC от партнёра PPP.

Формат поля Attribute Value для данной AVP показан ниже.



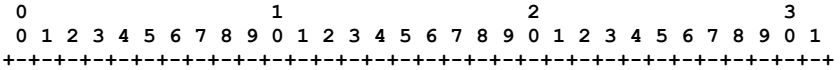
Поле LCP CONFREQ содержит копию тела первого CONFREQ, начиная с первой опции в теле сообщения LCP.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть сброшен (0). Поле Length (до сокрытия) в этой AVP имеет значение 6 + размер CONFREQ.

Last Sent LCP CONFREQ (ICCN)

Last Sent LCP CONFREQ AVP (Attribute Type 27) предоставляет LNS значение Last CONFREQ, переданное LAC партнёру PPP.

Формат поля Attribute Value для данной AVP показан ниже.



```
   | LCP CONFREQ... (произвольное число октетов)                   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Поле LCP CONFREQ содержит копию тела последнего CONFREQ, переданного клиенту для завершения согласования LCP, начиная с первой опции в теле сообщения LCP.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть сброшен (0). Поле Length (до сокрытия) в этой AVP имеет значение 6 + размер CONFREQ.

Last Received LCP CONFREQ (ICCN)

Last Received LCP CONFREQ AVP (Attribute Type 28) предоставляет LNS значение Last CONFREQ, полученное LAC от партнёра PPP.

Формат поля Attribute Value для данной AVP показан ниже.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | LCP CONFREQ... (произвольное число октетов)                   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Поле LCP CONFREQ содержит копию тела последнего CONFREQ, полученного от клиента для завершения согласования LCP, начиная с первой опции в теле сообщения LCP.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть сброшен (0). Поле Length (до сокрытия) в этой AVP имеет значение 6 + размер CONFREQ.

Proxy Authen Type (ICCN)

Proxy Authen Type AVP (Attribute Type 29) определяет, следует ли пользоваться прокси-аутентификацией.

Формат поля Attribute Value для данной AVP показан ниже.

```
    0                   1
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Authen Type          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Поле Authen Type представляет собой 2-октетное целое число без знака.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть сброшен (0). Поле Length (до сокрытия) в этой AVP имеет значение 8.

Определены следующие значения Authen Type:

0 - резерв;

1 - обмен username/password в форме текста;

2 - PPP CHAP;

3 - PPP PAP;

4 - без аутентификации;

5 - Microsoft CHAP версии 1 (MSCHAPv1).

Данная AVP **должна** присутствовать, если используется прокси-аутентификация. При отсутствии данной пары предполагается, что данный партнёр не может выполнять прокси-аутентификацию - это требует перезапуска фазы аутентификации на устройстве LNS, если клиент уже вошёл в эту фазу взаимодействия с LAC (может определяться Proxy LCP AVP при её наличии).

Для каждого типа аутентификации далее следуют соответствующие AVP.

Proxy Authen Name (ICCN)

Proxy Authen Name AVP (Attribute Type 30) указывает имя аутентифицирующего клиента при использовании прокси-аутентификации.

Формат поля Attribute Value для данной AVP показан ниже.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Authen Name... (произвольное число октетов)                   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Authen Name представляет собой строку октетов произвольного размера, содержащую имя, которое указывается в аутентификационном отклике клиента.

Данная AVP **должна** присутствовать в сообщениях, включающих Proxy Authen Type AVP со значениями 1, 2, 3, 5. Может оказаться желательным сокрытие данной AVP, поскольку имя указывается открытым текстом.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть сброшен (0). Поле Length (до сокрытия) в этой AVP имеет значение 6 + размер текстовой строки с именем.

Proxy Authen Challenge (ICCN)

Proxy Authen Challenge AVP (Attribute Type 31) указывает запрос (challenge), переданный LAC партнёру PPP при использовании прокси-аутентификации.

Формат поля Attribute Value для данной AVP показан ниже.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
| Challenge... (произвольное число октетов)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Поле Challenge представляет собой строку из одного или множества октетов.

Данная AVP **должна** присутствовать для Proxy Authen типов 2 и 5. Поле Challenge содержит значение CHAP challenge, представленное клиенту устройством LAC.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть сброшен (0). Поле Length (до сокрытия) в этой AVP имеет значение 6 + размер Challenge.

Proxy Authen ID (ICCN)

Proxy Authen ID AVP (Attribute Type 32) указывает идентификатор для аутентификации PPP, которая была начата между LAC и партнёром. PPP при использовании прокси-аутентификации.

Формат поля Attribute Value для данной AVP показан ниже.

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    резерв     |       ID      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ID представляет собой 2-октетное целое число без знака; старший октет **должен** иметь значение 0.

Proxy Authen ID AVP **должна** присутствовать для Proxy Authen типов 2, 3 и 5. Для типов 2 и 5 поле ID содержит значение ID, представленное клиенту LAC в своём Challenge, для типа 3 - значение Identifier в Authenticate-Request.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть сброшен (0).

Proxy Authen Response (ICCN)

Proxy Authen Response AVP (Attribute Type 33) указывает отклик PPP Authentication, полученный LAC от партнёра PPP при использовании прокси-аутентификации.

Формат поля Attribute Value для данной AVP показан ниже.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Response... (произвольное число октетов)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Поле Response представляет собой строку октетов.

Данная AVP **должна** присутствовать для Proxy Authen типов 1, 2, 3, 5. Поле Response содержит клиентский отклик на вызов (challenge). Для типов 2 и 5 это поле указывает значение отклика, полученное LAC, для типов 1 и 3 - пароль (в открытом виде), полученный LAC от клиента. При использовании текстовых паролей рекомендуется скрывать данную AVP.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть сброшен (0). Поле Length (до сокрытия) в этой AVP имеет значение 6 + размер Response.

4.4.6 AVP для статуса вызовов

Call Errors (WEN)

Call Errors AVP (Attribute Type 34) используется LAC для передачи информации об ошибках устройству LNS.

Формат поля Attribute Value для данной AVP показан ниже.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Reserved              |        CRC Errors (H)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         CRC Errors (L)        |        Framing Errors (H)     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Framing Errors (L)    |        Hardware Overruns (H)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Hardware Overruns (L) |        Buffer Overruns (H)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Buffer Overruns  (L)  |        Time-out Errors (H)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Time-out Errors (L)   |        Alignment Errors (H)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Alignment Errors (L)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Ниже перечислены определённые к настоящему моменту поля.

Reserved - не используется и должно иметь значение 0;

CRC Errors - число кадров PPP с ошибками CRC, принятых с момента организации соединения;

Framing Errors - число принятых пакетов PPP с недопустимым кадрированием;

Hardware Overruns - число фактов переполнения приёмного буфера с момента организации соединения;

Buffer Overruns - число фактов переполнения буфера с момента организации соединения;

Time-out Errors - число тайм-аутов с момента организации соединения;

Alignment Errors - число ошибок выравнивания с момента организации соединения.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 32.

ACCM (SLI)

ACCM AVP (Attribute Type 35) используется LNS для информирования LAC о параметрах ACCM согласованных с партнёром. PPP.

Формат поля Attribute Value для данной AVP показан ниже.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Reserved             |    Send ACCM (H)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Send ACCM   (L)      |    Receive ACCM (H)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Receive ACCM  (L)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Поля Send ACCM и Receive ACCM имеют размер 4 октета каждое, а перед ними размещается 2-октетное резервное поле. Значение Send ACCM устройству LAC следует использовать для обработки пакетов, передаваемых в соединение. Значение Receive ACCM устройству LAC следует использовать для обработки пакетов, принимаемых из соединения. По умолчанию LAC для обоих полей использует значение 0xFFFFFFFF. Устройствам LAC следует пользоваться значениями этих полей, если у них нет конкретной конфигурационной информации, указывающей, что запрошенную маску требуется изменить для выполнения операции.

Эта AVP **может** быть скрытой (бит H может быть установлен). Бит M для данной AVP **должен** быть установлен (1). Поле Length (до сокрытия) в этой AVP имеет значение 16.

5.0 Работа протокола

Действия по организации туннелирования сессии PPP с использованием L2TP включают два этапа: (1) организация управляющего соединения (Control Connection) для туннеля и (2) организация сессии по входящему или исходящему запросу на соединение. Туннель и соответствующее управляющее соединение **должны** быть организованы до того, как будет инициирован входящий или исходящий вызов. Сессия L2TP **должна** быть организована до того, как L2TP начнёт туннелировать кадры PP. В одном туннеле может быть организовано множество сессий, а между парой LAC и LNS может существовать множество туннелей.

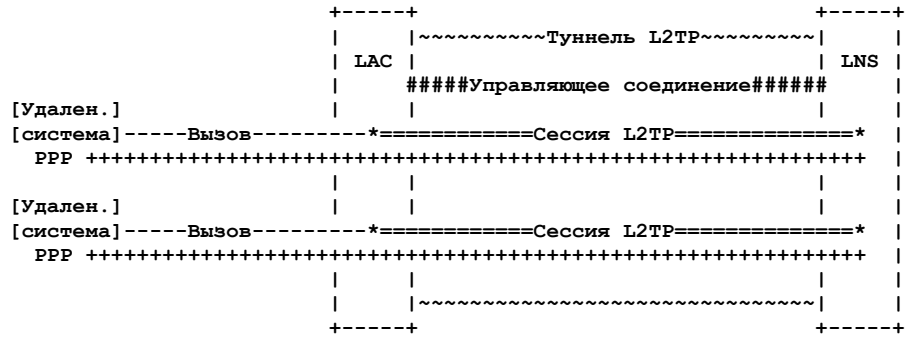


Рисунок 5.1. Туннелирование PPP.

5.1 Организация управляющего соединения

Control Connection представляет собой начальное соединение, которое должно быть организовано между LAC и LNS до того, как можно будет организовать какие-либо сессии. Организация управляющего соединения включает обеспечение идентификации партнёра, определение версии L2TP у него, кадрирование, согласование возможностей и т. п.

Для организации управляющего соединения используется обмен тремя сообщениями, показанный ниже.

```
LAC или LNS  LAC или LNS
-----------  ----------
SCCRQ ->
             <- SCCRP
SCCCN ->
             <- ZLB ACK
```

Сообщение ZLB ACK передаётся в тех случаях, когда в очереди для данного партнёра нет других сообщений.

5.1.1 Аутентификация туннеля

L2TP включает простой, необязательный механизм (похожий на CHAP [RFC1994]) аутентификации туннеля в процессе организации управляющего соединения. Если LAC или LNS желает проверить идентичность контактирующего с ним партнёра в сообщение SCCRQ или SCCRP включается Challenge AVP. При получении Challenge AVP в SCCRQ или SCCRP, **должна** быть передана Challenge Response AVP в SCCRP или SCCCN, соответственно. Если полученный отклик не соответствует ожидаемому от партнёра, организация туннеля **должна** блокироваться.

Для участия в аутентификации туннеля устройства LAC и LNS должны знать общий секрет. Это тот же секрет, который применяется для сокрытия AVP (см. параграф 4.3). Описание AVP для запросов и откликов дано в параграфе 4.4.3.

5.2 Организация сессии

После организации управляющего соединения могут создаваться отдельные сессии, каждая из которых соответствует одному потоку PPP между LAC и LNS. В отличие от управляющего соединения организация сессии имеет направления

относительно LAC и LNS. Устройство LAC запрашивает у LNS восприятие сессии для входящих вызовов, а LNS запрашивает у LAC восприятие сессии для исходящих вызовов.

5.2.1 Организация входящего вызова
Организация сессии состоит из обмена тремя сообщениями, как показано ниже.

```
LAC          LNS
---          ---
(Обнаружен вызов)

ICRQ ->
          <- ICRP
ICCN ->
          <- ZLB ACK
```

Сообщение ZLB ACK передаётся в тех случаях, когда в очереди для данного партнёра нет других сообщений.

5.2.2 Организация исходящего вызова
Организация сессии состоит из обмена тремя сообщениями, как показано ниже.

```
LAC          LNS
---          ---
          <- OCRQ
OCRP ->

(Выполнена обработка вызова)

OCCN ->
          <- ZLB ACK
```

Сообщение ZLB ACK передаётся в тех случаях, когда в очереди для данного партнёра нет других сообщений.

5.3 Пересылка кадров PPP
По завершении организации туннеля из кадров PPP от удалённой системы, принимаемых LAC, вырезается CRC, байты канального кадрирования и «прозрачности», после чего выполняется инкапсуляция в L2TP и пересылка через подходящий туннель. LNS получает пакеты L2TP и обрабатывает инкапсулированные кадры PPP, как будто они были получены от локального интерфейса PPP.

Отправитель сообщения, связанного с конкретной сессией и туннелем, помещает идентификаторы Session ID и Tunnel ID (задаётся его партнёром.) в одноимённые поля заголовков всех исходящих сообщений. С помощью этих полей кадры PPP мультиплексируются и демультиплексируются через один туннель между парой устройств LNS и LAC. Между конкретной парой устройств LNS и LAC может существовать множество туннелей, в каждом из которых быть организовано множество сессий.

Нулевые значения идентификаторов сессии и туннеля имеют специальное значение и **недопустимо** применять их в качестве Assigned Session ID или Assigned Tunnel ID. Для случаев когда значение Session ID ещё не присвоено партнёром. (т. е., в процессе организации новой сессии или туннеля), в поле Session ID **должно** помещаться значение 0, а в сообщении **должна** использоваться Assigned Session ID AVP для идентификации сессии. Аналогично, для случаев когда значение Tunnel ID ещё не было присвоено партнёром., в поле Tunnel ID **должно** помещаться значение 0 с использованием для идентификации туннеля Assigned Tunnel ID AVP.

5.4 Использование порядковых номеров в канале данных
Порядковые номера указываются в заголовках управляющих сообщений L2TP и могут использоваться также в сообщениях с данными (см. параграф 3.1). Номера служат для обеспечения гарантий доставки управляющих сообщений (см. параграф 5.8) и могут применяться для упорядочения сообщений с данными. Каждый из партнёров поддерживает раздельную нумерацию для управляющего соединения и каждой сессии с данными в туннеле.

В отличии от канала управления L2TP, канал данных не использует порядковые номера для повтора передачи утерянных сообщений с данными. Порядковые номера в сообщениях с данными могут использоваться для обнаружения потери пактов и/или восстановления порядка, нарушенного при транспортировке. LAC может запросить включение порядковых номеров в сообщения сданными с помощью Sequencing Required AVP (см. параграф 4.4.6). Если данная AVP присутствует при организации сессии, порядковые номера **должны** включаться во все кадры. При отсутствии данной AVP использование порядковых номеров определяет LNS. Устройство LNS может включить или отключить использование порядковых номеров в сообщениях в любой момент, просто добавляя или исключая эти номера для передаваемых им пакетов. Таким образом, если устройство LAC получает сообщение с данными, включающее порядковый номер, оно **должно** начать использование порядковых номеров в передаваемых после этого сообщениях с данными. Если LNS возобновляет использование порядковых номеров после отказа, нумерация продолжается с того значения, на котором она была прервана ранее.

LNS может инициировать отказ от использования порядковых номеров в любой момент (включая передачу первого сообщения с данными). Для соединений, на которых могут происходить потери или нарушение порядка доставки, рекомендуется включать использование порядковых номеров на этапах согласования PPP и отключать использование нумерации только в тех случаях, когда риск потери или нарушения порядка становится приемлемым. Например, если туннелируемая сессия PPP не использует протоколов компрессии или шифрования с учётом состояний и служить для передачи только пакетов IP (как указано в организованном NCP), LNS может принять решение об отказе от использования порядковых номеров, поскольку протокол IP устойчив к потере и нарушению порядка дейтаграмм.

5.5 Keepalive (Hello)
Механизм keepalive используется в L2TP для того, чтобы отличить отказы в туннеле от продолжительных интервалов бездействия. Для этого используются управляющие сообщения Hello (см. параграф 6.5), передаваемые по истечении

заданного интервала с момента приёма последнего сообщения (данные или управление) из туннеля. Как и для прочих управляющих сообщений, если сообщение Hello не было доставлено, считается, что туннель не работоспособен и выполняется его сброс. Механизм сброса на транспортном уровне вкупе с сообщениями Hello обеспечивает обнаружение отказов в туннеле между LNS и LAC с любой стороны туннеля.

5.6 Разрыв сессии

Разрыв сессии может быть инициирован LAC или LNS и реализуется путём отправки управляющего сообщения CDN. После завершения последней сессии **может** быть разорвано и управляющее соединение (обычно так и происходит). Ниже приведён пример обмена управляющими соединениями для этого случая:

```
LAC или LNS   LAC или LNS

CDN ->
(Очистка)

              <- ZLB ACK
                 (Очистка)
```

5.7 Разрыв управляющего соединения

Разрыв управляющего соединения может быть инициирован LAC или LNS и выполняется путём передачи одного управляющего сообщения StopCCN. Получатель сообщения StopCCN **должен** передать ZLB ACK для подтверждения приёма и поддерживать состояние управляющего соединения для корректного восприятия повторов StopCCN в течение по крайней мере интервала полного цикла повтора передачи (на случай потери ZLB). Рекомендуемая продолжительность полного цикла повтора передачи составляет 31 сек. (см. параграф 5.8). Ниже приведён пример обмена управляющими сообщениями.

```
LAC или LNS   LAC или LNS

StopCCN ->
(Очистка)

              <- ZLB ACK
                 (Ожидание)
                 (Очистка)
```

Реализация может «погасить» туннель целиком вместе с организованными в нем сессиями, передав StopCCN. Таким образом, не требуется разрывать каждую сессию отдельно при полном разрыве туннеля.

5.8 Гарантированная доставка управляющих сообщений

L2TP обеспечивает гарантированный транспорт для всех управляющих сообщений. Поля Nr и Ns в заголовке управляющего сообщения (см. параграф 3.1) относятся к этому транспорту. Функции верхнего уровня L2TP не связаны с повтором передачи и соблюдением порядка доставки управляющих сообщений. Использование скользящего окна порядковых номеров обеспечивает контроль перегрузок и повтор передачи управляющих сообщений. Каждый из партнёров поддерживает своё состояние для порядковых номеров передаваемых через туннель сообщений.

Порядковые номера передаваемых сообщений Ns начинаются с 0. В каждом следующем передаваемом сообщении порядковый номер увеличивается на 1. Модуль счётчика порядковых номеров составляет 65536. Порядковый номер в заголовке принятого сообщения рассматривается, как не превышающий последний принятый номер, если его значение попадает в диапазон, включающий 32767 предшествующих номеров и последний принятый номер. Например, если последний принятый номер равен 15, сообщения с номерами от 0 до 15 и от 32784 до 65535 будут рассматриваться, как сообщения с номерами меньше последнего. Такие сообщения трактуются, как дубликаты ранее принятых сообщений и при обработке игнорируются. Однако для обеспечения корректного подтверждения всех сообщений (на случай потери ZLB ACK) полученные дубликаты **должны** подтверждаться с применением надёжного транспорта. Для этого подтверждение может «прицепляться» к сообщению из очереди или передаваться в виде отдельного ZLB ACK.

Передача всех сообщений, кроме подтверждений ZLB, увеличивает порядковый на 1. После передачи сообщения ZLB порядковый номер Ns не увеличивается.

Номер последнего принятого сообщения Nr используется для подтверждения полученных партнёром. L2TP сообщений. Это поле указывает порядковый номер, который партнёр ожидает получить в следующем сообщении (например, Ns из последнего сообщения не ZLB + 1 по модулю 65536). Хотя значение Nr из полученного сообщения ZLB применяется для исключения сообщений из локальной очереди на повторную передачу (см. ниже), значение Nr для следующего сообщения не обновляется значением Ns из принятого ZLB.

Гарантированный транспорт на приёмной стороне отвечает за упорядоченную доставку сообщений без их дублирования на вышележащий уровень. Прибывающие с нарушением порядка сообщения могут помещаться в очередь для упорядочения (ожидание приёма недостающих сообщений) или отбрасываться (потребуется повторная передача со стороны партнёра).

Для каждого туннеля поддерживается очередь сообщений, которые будут передаваться партнёру. Находящееся первым в очереди управляющее сообщение с порядковым номером Ns будет сохраняться в очереди, пока от партнёра не будет принято управляющее сообщение с полем Nr, показывающим получение партнёром. данного сообщения. По истечении некого периода (рекомендуется использовать по умолчанию 1 секунду) ожидания приёма подтверждения передача сообщения из очереди повторяется. При передаче повтора используется прежнее значение Ns, а значение Nr в заголовке **должно** обновляться в соответствии с порядковым номером следующего ожидаемого сообщения.

При передаче каждого последующего сообщения интервал **должен** экспоненциально возрастать. Таким образом, если первый повтор был сделан через 1 секунду, второй следует делать по истечении 2 секунд, третий - после 4 и т. д. Реализация **может** ограничивать максимальный интервал между повторами. Это ограничение **должно** быть не меньше 8 секунд. Если после нескольких (по умолчанию рекомендуется 5, но это значение **следует** делать настраиваемым) повторов отклик от партнёра не был получен, туннель и все сессии в нем **должны** быть сброшены.

Когда туннель закрывается по причинам, не связанным с потерей соединения, **должно** сохраняться состояние и механизмы гарантированной доставки в течение полного интервала повторов после завершения финального обмена сообщениями.

Для управления передачей сообщений используется механизм скользящего окна. Рассмотрим двух партнёров - A и B. Предположим, что A задаёт Receive Window Size AVP со значением N в сообщении SCCRQ или SCCRP. Это позволяет B передать до N управляющих сообщений, не получив подтверждения доставки. После передачи N сообщений требуется ждать подтверждения, которое позволит сдвинуть окно и передать новое управляющее сообщение. Реализация может поддерживать приёмное окно размером 1 (передав Receive Window Size AVP со значением 1), но **должна** воспринимать от партнёра окна размером до 4 (т. е., возможность отправить до 4 сообщений без ожидания подтверждений). Значение 0 для Receive Window Size AVP является неприемлемым.

При повторе передачи управляющих **следует** применять сообщений механизмы замедленного старта и предотвращения перегрузок для подстройки размера окна. Рекомендуемые процедуры описаны в Приложении A.

Партнёру **недопустимо** применять удержание подтверждений в качестве метода контроля потока управляющих сообщений. Предполагается, что реализации L2TP могут сохранять входящие управляющие сообщения, возможно отвечая на некоторые из них сообщениями об ошибках, которые показывают невозможность выполнения запрашиваемого действия.

В Приложении B приведены примеры передачи, подтверждения и повтора управляющих сообщений.

6.0 Спецификация протокола управляющего соединения

Описанные ниже управляющие сообщения служат для организации, поддержки и удаления туннелей L2TP. Все данные передаются в сетевом порядке байтов (сначала старший октет). Для всех резервных и пустых полей **должны** устанавливаться значения 0, для обеспечения возможности расширения протокола.

6.1 Запрос SCCRQ

Управляющее сообщение SCCRQ[1] служит для инициализации туннеля между LNS и LAC. Сообщение передаётся устройством LAC или LNS для инициирования процесса организации туннеля.

В сообщении SCCRQ **должны** присутствовать перечисленные ниже AVP:

Message Type AVP;

Protocol Version;

Host Name;

Framing Capabilities;

Assigned Tunnel ID.

Перечисленные ниже AVP также **могут** присутствовать в сообщениях SCCRQ:

Bearer Capabilities;

Receive Window Size;

Challenge;

Tie Breaker;

Firmware Revision;

Vendor Name.

6.2 Отклик SCCRP

Управляющие сообщения SCCRP[2] передаются в ответ на получение сообщения SCCRQ. Отклик SCCRP служит для индикации восприятия запроса SCCRQ и показывает, что организацию туннеля следует продолжать.

В сообщении SCCRP **должны** присутствовать перечисленные ниже AVP:

Message Type;

Protocol Version;

Framing Capabilities;

Host Name;

Assigned Tunnel ID.

Перечисленные ниже AVP также **могут** присутствовать в сообщениях SCCRP:

Bearer Capabilities;

Firmware Revision;

Vendor Name;

Receive Window Size;

Challenge;

[1]Start-Control-Connection-Request - запрос на организацию управляющего соединения.
[2]Start-Control-Connection-Reply - отклик на запрос организации управляющего соединения.

Challenge Response.

6.3 Отклик SCCCN

Сообщения SCCCN[1] передаются в ответ на SCCRP. Сообщение SCCCN показывает завершение процесса организации туннеля.

В сообщении SCCCN **должна** присутствовать Message Type AVP.

Кроме того, в SCCCN **может** включаться Challenge Response AVP.

6.4 Уведомление StopCCN

Уведомление о разрыве управляющего соединения (StopCCN[2]) представляет собой управляющее сообщение, передаваемое LAC или LNS для информирования своего партнёра о предстоящем разрыве туннеля и необходимости закрытия управляющего соединения. Кроме управляющего соединения неявно (без передачи каких-либо явных уведомлений) завершаются все активные сессии через этот туннель. Причина отправки такого запроса указывается в Result Code AVP. На это сообщение нет явного отклика и используется только неявное подтверждение ACK, передаваемое через гарантированный транспорт управляющих сообщений.

В StopCCN **должны** присутствовать следующие AVP:

Message Type;

Assigned Tunnel ID;

Result Code.

6.5 Сообщение HELLO

Управляющие сообщения HELLO в протоколе L2TP могут передаваться любым из партнёров в соединении LAC-LNS и служат для сохранения жизнеспособности туннеля (keepalive).

Передача сообщений HELLO и её правила определяются реализацией. Партнёру **недопустимо** ожидать получения HELLO в какой-либо момент или интервал. Как и все сообщения через управляющий канал, приветствия подтверждаются получателем с помощью сообщения ZLB ACK или путём добавки данных подтверждения в обычное сообщение.

Поскольку сообщения HELLO являются управляющими и для них должна обеспечиваться гарантированная доставка на нижележащем транспортном уровне, функция keepalive заставляет транспортный уровень обеспечивать такие гарантии. При обрыве в среде передачи транспорт не сможет обеспечить доставку сообщений HELLO и туннель будет разорван.

Сохранение жизнеспособности **может** быть реализовано путём передачи сообщения HELLO, если в течение заданного времени (по умолчанию рекомендуется использовать 60 секунд, это время **следует** делать настраиваемым) от партнёра не было получено ни одного сообщения (данные или управление).

Сообщения HELLO являются «глобальными» для туннеля. Поле Session ID в сообщении HELLO **должно** иметь значение 0.

В сообщении HELLO **должна** присутствовать Message Type AVP.

6.6 Запрос для входящего вызова (ICRQ)

Управляющее сообщение ICRQ[3] передаётся LAC для LNS при обнаружении входящего вызова. Оно является первым из трёх сообщений, используемых для организации сессии в туннеле L2TP.

ICRQ служит для индикации того, что для этого вызова будет организована сессия между LAC и LNS, а также предоставления устройству LNS информации о параметра сессии. LAC может задержать ответ на вызов, пока не получит от LNS сообщения ICRP, показывающего, что сессию следует организовать. Это механизм позволяет LNS получить информацию, позволяющую принять об ответе на вызов или отказе от него. Кроме того, LAC может ответить на вызов, согласовать LCP и аутентификацию PPP, а потом использовать полученную информацию для выбора LNS. В этом случае на момент получения ICRP ответ на вызов уже произошёл и LAC просто имитирует этапы «индикация вызова» и «ответ на вызов»..

В сообщении ICRQ **должны** присутствовать перечисленные ниже AVP:

Message Type;

Assigned Session ID;

Call Serial Number.

Перечисленные ниже AVP также **могут** присутствовать в сообщениях ICRQ:

Bearer Type;

Physical Channel ID;

Calling Number;

Called Number;

Sub-Address.

[1] Start-Control-Connection-Connected - управляющее соединение организовано.
[2] Stop-Control-Connection-Notification.
[3] Incoming-Call-Request.

6.7 Ответ на входящий вызов (ICRP)

Управляющее сообщение ICRP[1] передаётся LNS устройству LAC в ответ на принятое от того сообщение ICRQ. Это второе из трёх сообщений, используемых для организации сессии в туннеле L2TP.

ICRP служит для индикации получения и обработки ICRQ, указывая устройству LAC, что следует ответить на вызов, если это не было сделано ранее. Сообщение также позволяет указать параметры, требуемые для сессии L2TP.

В сообщениях ICRP **должны** присутствовать AVP Message Type и Assigned Session ID.

6.8 Входящий вызов принят (ICCN)

Управляющее сообщение ICCN[2] передаются LAC устройству LNS в ответ на получение ICRP. Это сообщение является последним из трёх сообщений, используемых для организации сессии в туннеле L2TP.

ICCN служит для индикации восприятия ICRP и ответа на входящий вызов, а также говорит о том, что сессию L2TP следует перевести в состояние established (организована). Сообщение также включает дополнительную информацию для LNS о параметрах, использованных при ответе на вызов (они не всегда доступны в момент передачи ICRQ).

В сообщении ICCN **должны** присутствовать перечисленные ниже AVP.

Message Type;

(Tx) Connect Speed;

Framing Type.

Перечисленные ниже AVP также **могут** присутствовать в сообщениях ICCN.

Initial Received LCP CONFREQ;

Last Sent LCP CONFREQ;

Last Received LCP CONFREQ;

Proxy Authen Type;

Proxy Authen Name;

Proxy Authen Challenge;

Proxy Authen ID;

Proxy Authen Response;

Private Group ID;

Rx Connect Speed;

Sequencing Required.

6.9 Запрос для исходящего вызова (OCRQ)

Управляющее сообщение OCRQ[3] передаются от LNS устройству LAC для индикации исходящего вызова со стороны LAC. Это первое из трёх сообщений при организации сессии в туннеле L2TP.

OCRQ показывает, что между LNS и LAC для этого вызова будет организована сессия и предоставляет устройству LAC информацию о параметрах для сессии L2TP и организованного соединения.

Устройство LNS **должно** иметь Bearer Capabilities AVP, принятую от LAC в процессе организации туннеля, для запроса исходящего вызова у этого устройства LAC.

В сообщении OCRQ **должны** присутствовать перечисленные ниже AVP.

Message Type;

Assigned Session ID;

Call Serial Number;

Minimum BPS;

Maximum BPS;

Bearer Type;

Framing Type;

Called Number.

Кроме того, в OCRQ **может** включаться Sub-Address AVP.

6.10 Отклик для исходящего вызова (OCRP)

Управляющее сообщение OCRP[4] передаётся от LAC к устройству LNS в ответ на полученное сообщение OCRQ. Это второе из трёх сообщений, используемых для организации сессии в туннеле L2TP.

[1] Incoming-Call-Reply.
[2] Incoming-Call-Connected.
[3] Outgoing-Call-Request.
[4] Outgoing-Call-Reply

OCRP показывает, что устройство LAC способно попытаться организовать исходящее соединение и возвратить некоторые параметры, относящиеся к такой попытке.

В сообщении OCRP **должны** присутствовать перечисленные ниже AVP.

Message Type;

Assigned Session ID.

Кроме того, в OCRP **может** включаться Physical Channel ID AVP.

6.11 Исходящее соединение организовано (OCCN)

Управляющее сообщение OCCN[1] передаётся LAC устройству LNS вслед за сообщением OCRP после организации исходящего соединения. Это сообщение является последним из трёх сообщений, используемых для организации сессии в туннеле L2TP.

OCCN служит для индикации успешной организации запрошенного исходящего соединения. Сообщение также предоставляет LNS информацию о параметрах, полученную после организации соединения.

В сообщении OCCN **должны** присутствовать перечисленные ниже AVP.

Message Type;

(Tx) Connect Speed;

Framing Type.

Перечисленные ниже AVP также **могут** присутствовать в сообщениях OCCN.

Rx Connect Speed;

Sequencing Required.

6.12 Уведомление о разрыве соединения (CDN)

Управляющее сообщение CDN[2] передаётся устройством LAC или LNS для запроса разрыва указанного соединения в туннеле. Цель этого сообщения заключается в информировании партнёра о разрыве соединения с указанием причины такого разрыва. Партнёр **должен** освободить все связанные с соединением ресурсы, не передавая отправителю никакой индикации результата очистки.

В сообщении CDN **должны** присутствовать перечисленные ниже AVP.

Message Type;

Result Code;

Assigned Session ID.

Кроме того, в CDN **может** включаться Q.931 Cause Code AVP.

6.13 Уведомление об ошибке в сети WAN (WEN)

Управляющее сообщение WEN[3] передаётся LAC устройству LNS для индикации ошибки в сети WAN (ошибка на интерфейсе, поддерживающем PPP). Счётчики для таких сообщений являются кумулятивными. Сообщения этого типа следует передавать лишь при возникновении ошибок, но не чаще 1 раза в течение 60 секунд. При организации нового соединения счётчики ошибок сбрасываются.

В сообщении WEN **должны** присутствовать перечисленные ниже AVP.

Message Type;

Call Errors.

6.14 Установка параметров канала (SLI)

Управляющее сообщение SLI[4] передаётся LNS устройству LAC для установки опций, согласуемых PPP. Эти опции могут меняться в течение действия соединения и устройство LAC **должно** обеспечивать возможность изменения своей внутренней информации о соединении и поведения для активной сессии PPP.

В сообщении SLI **должны** присутствовать перечисленные ниже AVP.

Message Type;

ACCM.

7.0 Машина состояний управляющего соединения

Обмен управляющими сообщениями, описанными в разделе 6, осуществляется в соответствии с таблицами состояний, рассмотренными ниже. Таблицы приведены для входящих и исходящих вызовов, а также для организации самого туннеля. В таблицах состояний не приводятся тайм-ауты и повторы передач, которые определяются семантикой, рассмотренной в параграфе 5.8.

[1] Outgoing-Call-Connected.
[2] Call-Disconnect-Notify.
[3] WAN-Error-Notify.
[4] Set-Link-Info.

7.1 Операции протокола управляющего соединения

В этом параграфе рассмотрены действия различных функций управляющих соединений L2TP и сообщений Control Connection, используемые для поддержки этих функций.

Получение недопустимого или необратимо испорченного управляющего сообщения следует соответствующим образом протоколировать, сбрасывая управляющее соединение для восстановления известного состояния. Управляющее соединение может быть перезапущено организовано его инициатором.

Неприемлемым считается управляющее сообщение, которое относится к обязательным типам (см. параграф 4.4.1), но этот тип не известен реализации, или получено с нарушением порядка (например, SCCCN в ответ на SCCRQ).

Примерами некорректно сформированных управляющих сообщений могут служить сообщения с недопустимыми значениями в заголовках, AVP с некорректным форматом или недопустимым значением, сообщения, где отсутствуют требуемые AVP. Управляющие сообщения с некорректным форматом заголовков следует отбрасывать. В сообщениях с недопустимыми AVP следует проверять флаг M для данной AVP, чтобы определить возможность исправления ошибки.

AVP с исправимыми ошибками (без флага M) в управляющем сообщении следует трактовать аналогично не распознанным необязательным AVP. Таким образом, при получении некорректно сформированной AVP с установленным флагом M сессию или туннель следует разрывать с возвратом подходящего кода результата или ошибки. Если флаг M не установлен, данную AVP следует игнорировать (но при этом делать запись о событии в системный журнал), воспринимая сообщение в целом.

Недопустимо рассматривать сказанное выше, как разрешение на отправку некорректно сформированных AVP, это лишь рекомендации по обработке полученных сообщений с некорректным форматом. Невозможно перечислить все возможные ошибки формата того или иного сообщения и дать рекомендации на каждый случай. Тем не менее, рассмотрим один из примеров искажённой, но исправимой AVP, когда Rx Connect Speed AVP (атрибут 38) принимается со значением поля размера 8 вместо 10, а BPS указана в двух октетах вместо четырёх. Поскольку Rx Connect Speed AVP не является обязательной, описанную ситуацию не следует считать критической. В этом случае управляющее сообщение следует воспринять, как будто данная AVP отсутствует (тем не менее, протоколируя этот факт).

В некоторых случаях, приведённых далее в таблицах, передаётся протокольное сообщение, а затем происходит «очистка». Отметим, что независимо от того, кто является инициатором разрыва туннеля, механизм гарантированной доставки должен иметь возможность работы (см. параграф 5.8) вплоть до разрушения туннеля. Это позволяет обеспечить партнёру надёжную доставку сообщений управления туннелем.

Этапы организации туннеля рассмотрены в Приложении B.1.

7.2 Состояния управляющего соединения

Протокол управляющих соединений L2TP не различается для LNS и LAC, но различается для инициатора и получателя. Инициатором считается тот партнёр, который начал организацию туннеля (при возникновении конфликта - победитель). Поскольку LAC и LNS могут быть инициаторами, возможно возникновение конфликтов. Для разрешения конфликтов используется Tie Breaker AVP, описанная в параграфе 4.4.3.

7.2.1 Организация управляющего соединения

Состояние	Событие	Действие	Новое состояние
idle	Локальный запрос Open	Передача SCCRQ	wait-ctl-reply
idle	Получение приемлемого SCCRQ	Передача SCCRP	wait-ctl-conn
idle	Получение неприемлемого SCCRQ	Очистка	idle
idle	Получение SCCRP	Передача StopCCN, очистка	idle
idle	Получение SCCCN	Очистка	idle
wait-ctl-reply	Получение приемлемого SCCRP	Передача SCCCN и события tunnel-open для ожидания сессий	established
wait-ctl-reply	Получение неприемлемого SCCRP	Передача StopCCN, очистка	idle
wait-ctl-reply	Получение SCCRQ, потеря tie-breaker	Очистка, переустановка SCCRQ в очередь для состояния idle	idle
wait-ctl-reply	Получение SCCCN	Передача StopCCN, очистка	idle
wait-ctl-conn	Получение приемлемого SCCCN	Передача события tunnel-open для ожидания сессий	established
wait-ctl-conn	Получение неприемлемого SCCCN	Передача StopCCN, очистка	idle
wait-ctl-conn	Получение SCCRP, SCCRQ	Передача StopCCN, очистка	idle
established	Локальный запрос Open (новый вызов)	Передача события tunnel-open для ожидания сессий	established
established	Административное закрытие туннеля	Передача StopCCN, очистка	idle
established	Получение SCCRQ, SCCRP, SCCCN	Передача StopCCN, очистка	idle
Idle, wait-ctl-reply, wait-ctl-conn, established	Получение StopCCN	Очистка	idle

Состояния, связанные с LNS и LAC при организации управляющего соединения перечислены ниже.

idle

Как инициатор, так и получатель начинают с этого состояния. Инициатор передаёт сообщение SCCRQ из этого состояния, а получатель сохраняет такое состояние до получения SCCRQ.

wait-ctl-reply

Инициатор проверяет не было ли запроса на организацию соединения от того же партнёра и при обнаружении такого запроса начинает обработку конфликтной ситуации, как описано в параграфе 5.8.

При получении SCCRP проверяется совместимость версий. Если номер версии в ответе меньше номера версии в запросе следует использовать младшую (с меньшим номером) из поддерживаемых обеими сторонами версий. Если предложенная в отклике версия поддерживается инициатором, он переходит в состояние established. Если предложенная в ответе версия не поддерживается, инициатор **должен** партнёру сообщение StopCCN, очистить и разорвать туннель.

wait-ctl-conn

Состояние ожидания SCCCN. При получении отклик проверяется. Туннель организуется или разрывается, если произошёл отказ при проверке полномочий.

established

Организованное соединение может быть разорвано по местным условиям или в ответ на получение Stop-Control-Connection-Notification. При разрыве соединения по местным условиям инициатор **должен** передать Stop-Control-Connection-Notification и очистить туннель.

Если инициатор получает Stop-Control-Connection-Notification, он также должен очистить туннель.

7.3 Синхронизация

Поскольку телефонная сигнализация работает в реальном масштабе времени, на устройствах LNS и LAC следует реализовать многопотоковую архитектуру, чтобы сообщения, относящиеся к множеству вызовов не выстраивались в очередь и не блокировались. Вызовы и состояния не задают исключений, причиняемых таймерами (см. параграф 5.8).

7.4 Входящие вызовы

Сообщение Incoming-Call-Request генерируется LAC при обнаружении входящего вызова (например, звонок по телефонной линии). LAC выбирает Session ID и порядковый номер, а также указывает тип подателя вызова. Для модемов всегда следует указывать аналоговый тип. Для вызовов ISDN следует указывать цифровой тип, если используется неограниченное цифровое обслуживание или адаптация скорости, и аналоговый тип при вовлечении модемов. Параметры Calling Number, Called Number и Subaddress могут включаться в сообщение, если они доступны из телефонной сети.

После того, как устройство LAC передаст Incoming-Call-Request, оно ждёт отклика от LNS, но это не обязательно будет вызов из телефонной сети. LNS может отвергнуть вызов по причине:

- отсутствия ресурсов для обслуживания дополнительной сессии;
- поля dialed, dialing или subaddress не соответствуют имеющему полномочия пользователю;
- тип вызова не поддерживается или для него нет разрешения.

Если устройство LNS воспринимает вызов, оно возвращает сообщение Incoming-Call-Reply. Получив такое сообщение, LAC пытается организовать соединение. Финальное при организации соединения сообщение от LAC к LNS показывает, что на обеих сторонах следует установить для вызова состояние established (соединение организовано). Если вызов был прерван до того, как устройство LNS восприняло его, LAC будет предавать сообщение Call-Disconnect-Notify для индикации этого.

Когда телефонный клиент «кладёт трубку» соединение разрывается обычным способом и LAC передаёт сообщение Call-Disconnect-Notify. Если устройство LNS хочет сбросить (очистить) соединение, оно передаёт сообщение Call-Disconnect-Notify и сбрасывает свою сессию.

7.4.1 Состояния LAC для входящих вызовов

Состояние	Событие	Действие	Новое состояние
idle	Звонок или Ready с индикацией входящего вызова	Инициирование локального создания туннеля	wait-tunnel
idle	Получение ICCN, ICRP, CDN	Очистка	idle
wait-tunnel	Отключение со стороны вызывающего или локальный запрос на закрытие	Очистка	idle
wait-tunnel	Создание туннеля	Передача ICRQ	wait-reply
wait-reply	Получение приемлемого ICRP	Передача ICCN	established
wait-reply	Получение неприемлемого ICRP	Передача CDN, очистка	idle
wait-reply	Получение ICRQ	Передача CDN, очистка	idle
wait-reply	Получение CDN, ICCN	Очистка	idle
wait-reply	Отключение со стороны вызывающего или локальный запрос на закрытие	Передача CDN, очистка	idle
established	Получение CDN	Очистка	idle
established	Получение ICRQ, ICRP, ICCN	Передача CDN, очистка	idle
established	Отключение со стороны вызывающего или локальный запрос на закрытие	Передача CDN, очистка	idle

Состояния LAC для входящих вызовов перечислены ниже.

idle

Устройство LAC обнаружило входящий вызов на одном из своих интерфейсов. Обычно это звонок по аналоговой линии или входящее сообщение Q.931 SETUP, полученное ISDN TE. LAC инициирует свою машину организации туннеля и переходит в состояние ожидания подтверждения существования туннеля.

wait-tunnel

В этом состоянии сессия ожидает открытия управляющего соединения или проверки факта существования туннеля. После того, как туннель создан/обнаружен может быть выполнен обмен управляющими сессией сообщениями, первым из которых является Incoming-Call-Request.

wait-reply

Устройство LAC получило сообщение CDN, показывающее, что LNS не желает принимать вызов (общая ошибка или отказ в восприятии), и возвращается в состояние idle или получило сообщение Incoming-Call-Reply, показывающее, что вызов воспринят, после чего LAC передаёт сообщение Incoming-Call-Connected и переходит в состояние established.

established

Обмен данными через туннель. Соединение может быть разорвано несколькими способами:

- событие на связанном с соединением интерфейсе - LAC передаёт сообщение Call-Disconnect-Notify;
- приём сообщения Call-Disconnect-Notify - LAC очищает состояние и разрывает соединение;
- локальная причина - LAC передаёт сообщение Call-Disconnect-Notify.

7.4.2 Состояния LNS для входящих вызовов

Состояние	Событие	Действие	Новое состояние
idle	Получение приемлемого ICRQ	Передача ICRP	wait-connect
idle	Получение неприемлемого ICRQ	Передача CDN, очистка	idle
idle	Получение ICRP	Передача CDN, очистка	idle
idle	Получение ICCN	Очистка	idle
wait-connect	Получение приемлемого ICCN	Подготовка для данных	established
wait-connect	Получение неприемлемого ICCN	Передача CDN, очистка	idle
wait-connect	Получение ICRQ, ICRP	Передача CDN, очистка	idle
idle, wait-connect, established	Получение CDN	Очистка	idle
wait-connect, established	Локальный запрос закрытия	Передача CDN, очистка	idle
established	Получение ICRQ, ICRP, ICCN	Передача CDN, очистка	idle

Состояния LNS для входящих вызовов перечислены ниже.

idle

Принято сообщение Incoming-Call-Request. Если запрос не воспринимается, в ответ передаётся сообщение Call-Disconnect-Notify и устройство LNS сохраняет состояние idle. Если сообщение Incoming-Call-Request воспринято, в ответ передаётся Incoming-Call-Reply и сессия переводится в состояние wait-connect.

wait-connect

Если соединение на устройстве LAC продолжает существовать, LAC передаёт сообщение Incoming-Call-Connected устройству LNS, которое после этого переходит в состояние established. LAC может передать сообщение Call-Disconnect-Notify для индикации того, что для исходящего вызова соединение не организовано. Это может происходить, например, в тех случаях, когда инициатор звонка случайно соединился с LAC вместо номера для голосовой связи и модем не смог согласовать соединение.

established

Сессия может быть прервана по приёму сообщения Call-Disconnect-Notify от LAC или передачей тому сообщения Call-Disconnect-Notify. Далее происходит сброс соединения на обеих сторонах независимо от того, кто был инициатором разрыва.

7.5 Исходящие вызовы

Исходящие соединения инициируются устройством LNS, которое инструктирует LAC по организации вызова. С исходящими вызовами используются три соединения: Outgoing-Call-Request, Outgoing-Call-Reply и Outgoing-Call-Connected. LNS передаёт сообщение Outgoing-Call-Request, указывающее телефонный номер вызываемого, субадрес и другие параметры. Устройство LAC **должно** ответить на Outgoing-Call-Request сообщением Outgoing-Call-Reply после того, как определит наличие требуемых для вызова компонент и административного разрешения на вызов (например, разрешение данному LNS использовать международные звонки). После организации исходящего соединения LAC передаёт LNS сообщение Outgoing-Call-Connected с результатом организации соединения.

7.5.1 Состояния LAC для исходящих вызовов

Состояние	Событие	Действие	Новое состояние
idle	Получение приемлемого ICRQ	Передача OCRP, звонок	wait-cs-answer
idle	Получение неприемлемого ICRQ	Передача CDN, очистка	idle
idle	Получение OCRP	Передача CDN, очистка	idle
idle	Получение OCCN, CDN	Очистка	idle
wait-cs-answer	Ответ, обнаружено кадрирование	Передача OCCN	established
wait-cs-answer	Отказ	Передача CDN, очистка	idle
wait-cs-answer	Получение OCRQ, OCRP, OCCN	Передача CDN, очистка	idle
established	Получение OCRQ, OCRP, OCCN	Передача CDN, очистка	idle
wait-cs-answer, established	Получение CDN	Очистка	idle
established	Разрыв соединения, локальный запрос закрытия	Передача CDN, очистка	idle

Состояния LAC для исходящих вызовов перечислены ниже.

idle

Если сообщение Outgoing-Call-Request принято с ошибкой, следует ответить сообщением Call-Disconnect-Notify. В остальных случаях выделяется физический канал и передаётся сообщение Outgoing-Call-Reply. Организуется исходящее соединение и выполняется переход в состояние wait-cs-answer.

wait-cs-answer

Если вызов не был завершён или закончился отсчёт таймера ожидания завершения соединения, передаётся сообщение Call-Disconnect-Notify с подходящим кодом ошибки и происходит переход в состояние idle. Если коммутируемое соединение организовано и обнаружено кадрирование, передаётся сообщение Outgoing-Call-Connected, показывающее успех, и выполняется переход в состояние established.

established

Если устройство LAC получает сообщение Call-Disconnect-Notify, телефонное соединение **должно** быть разорвано с использованием подходящего механизма, а сессия сброшена (очищена). Если соединение было разорвано клиентом или вызываемым интерфейсом, устройству LNS **должно** быть передано сообщение Call-Disconnect-Notify. Отправитель Call-Disconnect-Notify возвращается в состояние idle после завершения отправки сообщения.

7.5.2 Состояния LNS для исходящих вызовов

Состояние	Событие	Действие	Новое состояние
idle	Локальный запрос	Инициирование локального tunnel-open	wait-tunnel
idle	Получение OCCN, OCRP, CDN	Очистка	idle
wait-tunnel	tunnel-open	Передача OCRQ	wait-reply
wait-reply	Получение приемлемого OCRP	нет	wait-connect
wait-reply	Получение неприемлемого OCRP	Передача CDN, очистка	idle
wait-reply	Получение OCCN, OCRQ	Передача CDN, очистка	idle
wait-connect	Получение OCCN	нет	established
wait-connect	Получение OCRQ, OCRP	Передача CDN, очистка	idle
idle, wait-reply, wait-connect, established	Получение CDN	Очистка	idle
established	Получение OCRQ, OCRP, OCCN	Передача CDN, очистка	idle
wait-reply, wait-connect, established	Локальный запрос на разрыв	Передача CDN, очистка	idle
wait-tunnel	Локальный запрос на разрыв	Очистка	idle

Состояния LNS для исходящих вызовов перечислены ниже.

idle, wait-tunnel

При инициировании исходящего соединения сначала организуется туннель, как в состояниях idle и wait-tunnel для входящего вызова на LAC. После организации туннеля устройству LAC передаётся сообщение Outgoing-Call-Request и сессия переходит в состояние wait-reply.

wait-reply

При получении сообщения Call-Disconnect-Notify это рассматривается, как ошибка, сессия очищается и возвращается в состояние idle. При получении Outgoing-Call-Reply вызов обрабатывается и сессия переходит в состояние wait-connect.

wait-connect

При получении сообщения Call-Disconnect-Notify это рассматривается, как ошибка, сессия очищается и возвращается в состояние idle. При получении Outgoing-Call-Connected организация соединения завершается и через него может начинаться передача данных.

established

При получении сообщения Call-Disconnect-Notify соединение разрывается по причине, указанной в Result и Cause Code; сессия переходит в состояние idle. Если устройство LNS решает прервать сессию, оно передаёт Call-Disconnect-Notify устройству LAC, после чего очищает сессию и переводит её в состояние idle.

7.6 Разрыв туннеля

Разрыв туннеля может быть инициирован любым из партнёров путём передачи сообщения Stop-Control-Connection-Notification. Отправителю этого уведомления следует дождаться (ограниченное время) получения подтверждения доставки данного сообщения прежде, чем сбрасывать связанные с туннелем данные управления. Получателю такого уведомления следует отправить подтверждение приёма отправителю и после этого сбросить связанные с туннелем данные управления.

Обстоятельства разрыва туннеля определяются реализацией и не задаются в данном документе. Конкретная реализация может использовать ту или иную политику для решения вопроса о необходимости разрыва туннеля. Некоторые реализации могут оставлять открытый туннель на некий период времени (иногда неограниченный) после завершения в этом туннеле последней сессии. Другие могут разрывать туннель сразу же после разрыва последнего пользовательского соединения через этот туннель.

8.0 L2TP в разных средах

Протокол L2TP является самодостаточным и работает просто «поверх» среды передачи. Тем не менее, некоторые детали взаимодействия со средой нужно знать для обеспечения взаимодействия реализаций. В последующих параграфах описаны детали, требуемые для обеспечения взаимодействия через различные среды.

8.1 L2TP через UDP/IP

L2TP использует зарегистрированный порт UDP 1701 [RFC1700]. Весь пакет L2TP, включая данные и заголовок L2TP, передаётся в виде дейтаграммы UDP. Инициатор туннеля L2TP выбирает доступный выходной порт UDP (не обязательно 1701) и передаёт пакет в порт 1701 по желаемому адресу. Получатель этого пакета выделяет доступный порт в своей системе (не обязательно 1701) и передаёт через него отклик, используя номер порта UDP и адрес инициатора, указывая в качестве порта отправителя выбранный в своей системе свободный порт. После выбора

портов для отправки и получения пакетов, номера этих портов **должны** сохраняться в течение срока использования туннеля.

Высказывалось предположение, что выбор получателем произвольного порта-источника (вместо использованного для приёма порта 1701) может осложнить прохождение пакетов L2TP через некоторые устройства NAT. Разработчикам следует принимать во внимание этот аспект при выборе порта для отправки отклика.

При прохождении пакетов L2TP через инфраструктуру IP возможна их фрагментация. В L2TP не используется специальных мер оптимизации для таких случаев. Реализация LAC **может** заставить свой LCP согласовать конкретное значение MRU, оптимизированное для среды LAC, в которой MTU на пути прохождения пакетов L2TP можно предположить согласованным.

По умолчанию для любой реализации L2TP контрольные суммы UDP **должны** включаться в заголовки как управляющих пакетов, так и пакетов с данными. Реализация L2TP **может** поддерживать опцию для запрета использования контрольных сумм UDP в пакетах данных. В пакетах управления рекомендуется использовать контрольные суммы UDP во всех случаях.

Порт 1701 применяется как для пакетов L2F [RFC2341], так и для пакетов L2TP. Поле Version в заголовке может применяться для того, чтобы различать эти два типа пакетов (L2F использует значение 1, а L2TP, описанный в данном документе, - 2). Реализации L2TP в системах, не поддерживающих L2F, **должны** отбрасывать пакеты L2F без уведомления.

Для клиентов PPP, использующих L2TP через туннель UDP/IP, канальные характеристики PPP могут приводить к смене порядка и отбрасыванию пакетов без уведомления. Изменение порядка может нарушать работу не относящихся к IP протоколов, передаваемых через PPP, особенно протоколов ЛВС (например, протоколов мостов). Отбрасывание пакетов может нарушать работу протоколов, которые используют попакетную индикацию ошибок (например, протоколы сжатия заголовков TCP). Сохранение порядка можно обеспечить с помощью порядковых номеров в пакетах данных L2TP, если передаваемые через PPP чувствительны к нарушению порядка доставки. Требования отдельных протоколов к упорядоченной доставке выходят за рамки данного документа.

Вопрос с отбрасыванием пакетов без уведомления более сложен для некоторых протоколов. Если включена гарантированная доставка PPP [RFC1663], протокол не будет сталкиваться с потерей пакетов. При использовании порядковых номеров L2TP сам протокол L2TP сможет обнаруживать потерю пакетов. Для случая LNS в устройстве присутствуют стеки протоколов PPP и L2TP, поэтому сигнализация о потере пакетов может быть очень точной, как при получении пакетов с ошибками CRC. Если LAC и стек PPP используются совместно, этот метод также можно применить. Если же LAC и клиент PPP физически разделены, похожую сигнализацию **можно** обеспечить путём передачи клиенту PPP пакетов с ошибкой CRC. Отметим, что это будет сильно осложнять решение клиентских проблем с линией, поскольку статистика клиента не сможет различить ошибки в среде от имитированных устройством LAC ошибок. Кроме того, использование этого метода возможно не на всем оборудовании.

При использовании компрессии VJ и отсутствии гарантированной доставки PPP и порядковых номеров каждая потеря пакета будет приводить к вероятности пересылки сегмента TCP с некорректным содержимым 2^{-16} [RFC1144]. В тех случаях, когда комбинация частоты потери пакетов с указанной вероятностью некорректной пересылки не приемлема, сжатие заголовков TCP **не следует** использовать.

В общем случае следует помнить, что транспорт L2TP/UDP/IP не является надёжным. Как и для любой среды PPP с возможными потерями следует принимать соответствующие меры для протоколов, чувствительных к потерям. К таким протоколам относятся протоколы сжатия заголовков и шифрования, которые в своей работе опираются на предыдущие пакеты.

8.2 IP

При работе в средах IP протокол L2TP **должен** по умолчанию предлагать инкапсуляцию UDP, описанную в параграфе 8.1. В качестве дополнительных вариантов **могут** предлагаться иные конфигурации (возможно, соответствующие формату сжатых заголовков).

9.0 Вопросы безопасности

При работе L2TP возникает несколько связанных с безопасностью вопросов, которые в общем виде рассмотрены ниже.

9.1 Безопасность конечных точек туннеля

Конечные точки туннеля могут выполнять процедуры аутентификации другой стороны туннеля в процессе его организации. Такая аутентификация использует те же атрибуты безопасности, что и протокол CHAP и является разумной мерой защиты от повторно используемых и обманных пакетов при организации туннелей. Этот механизм не предназначен для какой-либо аутентификации сверх процедуры организации туннеля и злоумышленник может достаточно легко перехватывать поток данных через туннель после того, как процедура организации туннеля с использованием аутентификации будет завершена.

Для выполнения аутентификации устройства LAC и LNS **должны** использовать общий секрет. Каждая из сторон туннеля использует один и тот же секрет, выступая как в качестве аутентифицируемой, так и в качестве аутентифицирующей стороны. По причине использования одного секрета AVP для аутентификации туннеля включают дифференцирующие значения в полях CHAP ID для каждого расчёта цифровой подписи сообщения (с целью предотвращения повторного использования перехваченных пакетов).

Значения Assigned Tunnel ID и Assigned Session ID (см. параграф 4.4.3) **следует** выбирать непредсказуемым способом, а не перебирать последовательно или по иному алгоритму. Это поможет предотвратить захват сессии злоумышленниками, не имеющими доступа к пакетам между устройствами LAC и LNS.

9.2 Защита на уровне пакетов

Для защиты L2TP требуется поддержка нижележащим транспортом услуг шифрования, аутентификации и контроля целостности для всего трафика L2TP. Защищённый транспорт работает на уровне пакетов L2TP в целом и его

функциональность не зависит от PPP и протоколов, передаваемых через PPP. Сам по себе L2TP обеспечивает лишь целостность, конфиденциальность и аутентификацию для пакетов L2TP между конечными точками туннеля (LAC и LNS), тогда как шифрование канального уровня обеспечивает лишь защиту конфиденциальности для трафика между физическими точками.

9.3 Сквозная защита

Защита потока пакетов L2TP на уровне транспорта обеспечивает и защиту данных в туннелируемых пакетах PPP при их транспортировке от LAC к LNS. Такую защиту не следует рассматривать, как замену сквозной защиты между взаимодействующими хостами или приложениями.

9.4 L2TP и IPsec

При работе с IP протокол IPsec обеспечивает защиту на уровне пакетов с использованием ESP и/или AH. Все пакеты управления и данных L2TP для конкретного туннеля воспринимаются системой IPsec, как однотипные пакеты данных UDP/IP.

В дополнение к транспортно защите IP, протокол IPsec поддерживает режим работы, позволяющий туннелировать пакеты IP. Туннельный режим IPsec обеспечивает шифрование и аутентификацию на уровне пакетов, что обеспечивает протоколу L2TP с защитой IPsec требуемый уровень безопасности.

IPsec также поддерживает функции контроля доступа, которые являются обязательными для реализаций IPsec. Эти функции позволяют фильтровать пакеты по параметрам сетевого и транспортного уровня (таким, как адреса IP, номера портов и т. п.). В модели туннелирования L2TP аналогичные функции выполняются на уровне PPP или сетевом уровне над L2TP. Эти функции контроля доступа на сетевом уровне могут реализоваться на LNS с помощью фирменных функций проверки полномочий на базе аутентификации пользователей PPP или непосредственно на сетевом уровне при сквозном использовании транспортного режима IPsec между взаимодействующими хостами. Требования к механизмам контроля доступа не являются частью спецификации L2TP и выходят за рамки этого документа.

9.5 Аутентификация PPP

L2TP определяет AVP, которые **могут** передаваться в процессе организации сеанса для обеспечения пересылки управляющей информации PPP, имеющейся на LAC устройству LNS для её проверки (см. параграф 4.4.5). Это предполагает доверительные отношения на устройстве LAC от имени LNS. Если устройство LNS использует proxy-аутентификацию, оно **должно** обеспечивать возможность её отключения для выполнения нового раунда аутентификации PPP по инициативе LNS (может включать новый раунд согласования LCP).

10.0 Взаимодействие с IANA

В этом документе определено множество значений, распределение которых осуществляется через агентство IANA. В данном разделе описаны критерии, которыми IANA будет руководствоваться при выделении новых значений. Описана также политика распределения для определённых в этом документе пространств имён.

10.1 Атрибуты AVP

Как указано в параграфе 4.1, AVP включают поля Vendor ID, Attribute и Value. Для Vendor ID = 0 IANA будет поддерживать реестр выделенных значений Attribute, а в некоторых случаях и сами значения. Распределение атрибутов 0 - 39 описано в параграфе 4.4. Остальные значения доступны для распределения через процедуру IETF Consensus [RFC 2434].

10.2 Значения Message Type AVP

Как указано в параграфе 4.4.1, Message Type AVP (Attribute Type 0) имеет значение, распределяемое IANA. Значения 0 - 16 описаны в параграфе 3.2, остальные значения доступны для распределения по процедуре IETF Consensus [RFC 2434]

10.3 Значения Result Code AVP

Как указано в параграфе 4.4.2, Result Code AVP (Attribute Type 1) содержит три поля. Два из этих полей (Result Code и Error Code) используют значения, распределяемые IANA.

10.3.1 Значения поля Result Code

Result Code AVP может включаться в сообщения CDN и StopCCN. Допустимые значения поля Result Code данной AVP зависят от Message Type AVP. Для сообщений StopCCN значения 0 - 7 определены в параграфе 4.4.2; для сообщений StopCCN в том же параграфе определены значения 0 - 11. Остальные значения поля Result Code для обоих типов сообщений доступны для распределения по процедуре IETF Consensus [RFC 2434].

10.3.2 Значения поля Error Code

Значения 0 - 7 определены в параграфе 4.4.2. Значения 8 - 32767 доступны для распределения по процедуре IETF Consensus [RFC 2434]. Оставшиеся значения поля Error Code доступны для распределения по процедуре First Come First Served [RFC 2434].

10.4 Framing Capabilities и Bearer Capabilities

Framing Capabilities AVP и Bearer Capabilities AVP (см. параграф 4.4.3) содержат 32-битовые маски. Использование битов этих масок определяется по процедуре Standards Action [RFC 2434].

10.5 Значения Proxy Authen Type AVP

Proxy Authen Type AVP (Attribute Type 29) использует значения, распределяемые IANA. Значения 0 - 5 определены в параграфе 4.4.5, оставшиеся значения доступны для распределения по процедуре First Come First Served [RFC 2434].

10.6 Биты заголовка AVP

В заголовке AVP имеется четыре резервных поля. Использование этих полей возможно только в соответствии с процедурой Standards Action [RFC 2434].

11.0 Литература

[DSS1] ITU-T Recommendation, "Digital subscriber Signaling System No. 1 (DSS 1) - ISDN user-network interface layer 3 specification for basic call control", Rec. Q.931(I.451), May 1998

[KPS] Kaufman, C., Perlman, R., and Speciner, M., "Network Security: Private Communications in a Public World", Prentice Hall, March 1995, ISBN 0-13-061466-1

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

[RFC1144] Jacobson, V., "Compressing TCP/IP Headers for Low-Speed Serial Links", RFC 1144, February 1990.

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RFC1662] Simpson, W., "PPP in HDLC-like Framing", STD 51, RFC 1662, July 1994.

[RFC1663] Rand, D., "PPP Reliable Transmission", RFC 1663, July 1994.

[RFC1700] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700[1], October 1994. См. также: http://www.iana.org/numbers.html

[RFC1990] Sklower, K., Lloyd, B., McGregor, G., Carr, D. and T. Coradetti, "The PPP Multilink Protocol (MP)", RFC 1990, August 1996.

[RFC1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2138] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, January 1998.

[RFC2341] Valencia, A., Littlewood, M. and T. Kolar, "Cisco Layer Two Forwarding (Protocol) L2F", RFC 2341, May 1998.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC2637] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.

[STEVENS] Stevens, W. Richard, "TCP/IP Illustrated, Volume I The Protocols", Addison-Wesley Publishing Company, Inc., March 1996, ISBN 0-201-63346-9

12.0 Благодарности

Базовые концепции и многие из протокольных конструкций L2TP заимствованы из L2F [RFC2341] и PPTP [PPTP], авторами которых являются A. Valencia, M. Littlewood, T. Kolar, K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn.

Dory Leifer внёс важные уточнения в определения для протокола L2TP и существенный вклад в редактирование документа.

Steve Cobb и Evan Caves переработали таблицы машины состояний.

Barney Wolff внёс много предложений по механизму аутентификации конечных точек.

John Bray, Greg Burns, Rich Garrett, Don Grosser, Matt Holdrege, Terry Johnson, Dory Leifer и Rich Shea внесли существенные предложения и сделали обзор на 43-й конференции IETF в Orlando, FL, что существенно повысило уровень ясности данного документа и сделало его более читаемым.

13.0 Адреса авторов

Gurdeep Singh Pall
Microsoft Corporation
Redmond, WA
EMail: gurdeep@microsoft.com

Bill Palter
RedBack Networks, Inc

[1] В соответствии с RFC 3232 этот документ утратил силу. Данные доступны по ссылке. *Прим. перев.*

1389 Moffett Park Drive
Sunnyvale, CA 94089
EMail: palter@zev.net

Allan Rubens
Ascend Communications
1701 Harbor Bay Parkway
Alameda, CA 94502
EMail: acr@del.com

W. Mark Townsley
cisco Systems
7025 Kit Creek Road
PO Box 14987
Research Triangle Park, NC 27709
EMail: townsley@cisco.com

Andrew J. Valencia
cisco Systems
170 West Tasman Drive
San Jose CA 95134-1706
EMail: vandys@cisco.com

Glen Zorn
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
EMail: gwz@acm.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Приложение A. Slow Start и Congestion Avoidance на канале управления

Хотя каждая из сторон указывает максимальный размер приёмного окна, рекомендуется использовать для передачи пакетов управления механизмы замедленного старта и предотвращения перегрузок. Описанные здесь методы основаны на алгоритме предотвращения перегрузок TCP, описанном в параграфе 21.6 книги W. Richard Stevens TCP/IP Illustrated, Volume I [STEVENS].

Упомянутые механизмы используют несколько переменных. Размер окна насыщения (CWND) определяет число пакетов, которые отправитель может предать до получения подтверждения. Значение CWND может изменяться, как описано ниже. Однако следует отметить, что CWND ни в коем случае не может превосходить размер анонсируемый окна, полученный из Receive Window AVP (в последующем тексте предполагается, что увеличение ограничено значением Receive Window Size). Переменная SSTHRESH[1] определяет переключение из режима замедленного старта в режим предотвращения перегрузки. Механизм замедленного старта используется до тех пор, пока CWND < SSTHRESH.

Отправитель начинает с фазы замедленного старта. Для CWND устанавливается начальное значение в 1 пакет, а для SSTHRESH - размер анонсированного окна (берётся из Receive Window AVP). После этого отправитель передаёт один пакет и ждёт подтверждения его доставки (явного или прицепленного к данным). При получении подтверждения размер окна насыщения увеличивается с 1 до 2. В процессе замедленного старта значение CWND увеличивается на 1 при получении каждого ACK (явно в ZLB или с данными). Увеличение CWND на 1 при каждом ACK ведёт к удвоению CWND за каждый период кругового обхода, что ведёт к экспоненциальному росту размера окна. Когда значение CWND достигает SSTHRESH, фаза замедленного старта завершается и начинается фаза предотвращения перегрузок.

В фазе предотвращения перегрузок рост CWND замедляется. Более конкретно, размер окна увеличивается на 1/CWND при получении каждого нового ACK. Т. е., значение CWND увеличивается не 1 после приёма CWND новых пакетов ACK. Увеличение размера окна в фазе предотвращения перегрузок эффективно является линейным - CWND увеличивается на 1 за каждый период кругового обхода.

При возникновении перегрузки (указывается включением повтора передачи) для SSTHRESH устанавливается значение ½ CWND, а для окна насыщения (CWND) устанавливается значение 1. После этого отправитель возвращается в фазу замедленного старта.

Приложение B. Примеры управляющих сообщений

B.1. Этапы организации туннеля

В этом примере LAC организует туннель, при организации которого обе стороны поочерёдно передают сообщения. Этот пример показывает финальное подтверждение, явно передаваемое в сообщении ZLB ACK. Другим вариантом может служить добавление подтверждения в сообщение, передаваемое в ответ на ICRQ или OCRQ, которое явно передаст сторона-инициатор.

```
LAC или LNS                LNS или LAC
-----------                -----------
SCCRQ      ->
```

[1] В оригинале ошибочно указано SSHTRESH. См. https://www.rfc-editor.org/errata_search.php?eid=401. *Прим. перев.*

```
        Nr: 0, Ns: 0
                                  <-      SCCRP
                                  Nr: 1, Ns: 0
        SCCCN     ->
        Nr: 1, Ns: 1
                                  <-       ZLB
                                  Nr: 2, Ns: 1
```

B.2. Потеря пакета с повторной передачей

В существующем туннеле имеется новая сессия, запрошенная LAC. Сообщение ICRP теряется и должно быть передано повторно устройством LNS. Отметим, что потеря ICRP имеет двойное влияние, не только затормаживая обработку состояний верхнего уровня, но и останавливая на устройстве LAC поиск подтверждения отправленного им сообщения ICRQ.

```
          LAC                              LNS
          ---                              ---
       ICRQ      ->
       Nr: 1, Ns: 2

                        (потеря пакета) <-      ICRP
                                        Nr: 3, Ns: 1

    (пауза; таймер LAC запускается первым и первым завершает отсчёт)

       ICRQ      ->
       Nr: 1, Ns: 2

       (Понимая, что этот пакет уже был передан, LNS отбрасывает его и передаёт ZLB)
                                        <-       ZLB
                                        Nr: 3, Ns: 2

                      (завершается отсчёт таймера повтора передачи в LNS)

                                        <-      ICRP
                                        Nr: 3, Ns: 1
       ICCN      ->
       Nr: 2, Ns: 3

                                        <-       ZLB
                                        Nr: 4, Ns: 2
```

Приложение C. Интеллектуальная собственность

IETF не занимает какой-либо позиции в отношении действительности или объёма каких-либо прав интеллектуальной собственности или иных прав, которые могут быть заявлены как относящиеся к реализации или применению технологии, описанной в этом документе, или степени, в которой любая лицензия, по которой права могут или не могут быть доступны, не заявляется также применение каких-либо усилий для определения таких прав. Сведения о процедурах IETF в отношении прав в документах, связанных со стандартами, можно найти в BCP-11. Копии раскрытия IPR, предоставленные секретариату IETF, и любые гарантии доступности лицензий, а также результаты попыток получить общую лицензию или право на использование таких прав собственности разработчиками или пользователями этой спецификации, можно получить в IETF Secretariat.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Эту информацию следует направлять исполнительному директоу IETF (Executive Director).

IETF имеет сведения о правах интеллектуальной собственности, заявленных в отношении некоторых или всех спецификаций, содержащихся в документе. Для получения дополнительных сведений следует обращаться к online-списку заявленных прав.

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.