Network Working Group
Request for Comments: 2516
Category: Informational

L. Mamakos
K. Lidl
J. Evarts
UUNET Technologies, Inc.
D. Carrel
D. Simone
RedBack Networks, Inc.
R. Wheeler
RouterWare, Inc.

February 1999

Метод передачи PPP через Ethernet (PPPoE)

A Method for Transmitting PPP Over Ethernet (PPPoE)

Статус документа

В этом документе содержится информация для сообщества Internet. Документ не задаёт каких-либо стандартов Internet и может распространяться без ограничений.

Авторские права

Аннотация

Протокол PPP[1] [1] обеспечивает стандартный метод передачи дейтаграмм различных протоколов через соединения «точка-точка». В этом документе описано как создавать сессии PPP и инкапсулировать пакеты PPP в сетях Ethernet.

Применимость

Назначением этой спецификации является задание таких, определённых для PPP функций, как протокол управления каналом LCP[2], протоколы управления на сетевом уровне NLCP[3], аутентификация и т. п. Поддержка этих функций требуют создания парных отношений между партнёрами и не предназначена для групповых взаимодействий, которые возможны в сетях Ethernet и других средах с множественным доступом.

Данная спецификация может использоваться множеством хостов разделяемой среды Ethernet для создания сессий PPP с многочисленными адресатами через один или множество модемов со встроенными мостами. Спецификация предназначена для использования с широкополосными технологиями удалённого доступа, создающими топологию Ethernet с соединениями на основе мостов[4], когда поставщики услуг доступа хотят поддерживать абстракции сессий, связанные с PPP.

Документ описывает инкапсуляцию PPPoE[5], которая развёрнута в сетях RedBack Networks, RouterWare, UUNET и других операторов.

1. Введение

Требования к современным технологиям доступа в некоторой степени противоречивы. Желательно подключить множество хостов удалённого сайта через одно устройство доступа, находящееся на этом сайте. Желательно также обеспечить контроль доступа и функциональность, подобные предоставлению услуг по коммутируемым каналам на базе PPP. В большинстве вариантов наиболее эффективным экономически является метод подключения множества хостов к одному устройству доступа на стороне абонента через сеть Ethernet. Весьма желательно также обеспечить невысокую цену для устройства доступа, вкупе с простотой настройки или возможностью обойтись вообще без настройки конфигурации этого устройства.

PPPoE обеспечивает возможность подключения сети хостов через одно простое устройство доступа, обеспечивающее функции моста, к удалённому концентратору доступа[6]. В этой модели каждый хост использует свой стек PPP и пользователь представляется с обычным интерфейсом. Контроль доступа, учёт работы (billing) и тип обслуживания могут осуществляться для отдельных пользователей, а не для сайта в целом.

Для обеспечения соединений «точка-точка» через сеть Ethernet каждая сессия PPP должна узнать Ethernet-адрес удалённого партнёра, а также создать уникальный идентификатор сессии. PPPoE включает протокол обнаружения для решения этих задач[7].

---

[1]Point-to-Point Protocol.
[2]Link Control Protocol.
[3]Network-layer Control Protocols.
[4]Bridged Ethernet topology.
[5]PPP Over Ethernet.
[6]Access Concentrator.
[7]Discovery protocol.

2. 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 интерпретируются в соответствии с [2].

3. Обзор протокола

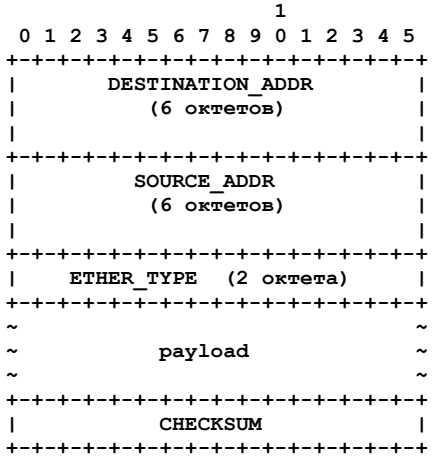
Работа PPPoE включает два разных этапа - обнаружение[1] и сеанс PPP[2]. Хост, желающий организовать сеанс PPPoE, должен выполнить этап Discovery для определения MAC-адреса партнёра и создания идентификатора сеанса PPPoE SESSION_ID. Хотя PPP определяет равноправное взаимодействие, этап Discovery использует отношения «клиент-сервер». В процессе обнаружения хост (клиент) отыскивает концентратор доступа (сервер). В зависимости от топологии сети в ней может присутствовать более одного концентратора доступа, с которым может взаимодействовать хост. Этап Discovery позволяет хосту обнаружить концентраторы доступа и выбрать один из них. После успешного завершения этапа Discovery хост и выбранный им концентратор доступа имеют информацию, которая требуется для организации соединения «точка-точка» через сеть Ethernet.

Этап Discovery не задаёт какого-либо состояния, пока не будет организован сеанс PPP. После организации сеанса PPP хост и концентратор доступа **должны** выделить ресурсы для виртуального интерфейса PPP.

4. Информационное поле пакетов

В этом параграфе определён формат пакетов. Содержимое информационного поля определено ниже при описании этапов Discovery и PPP.

Формат кадра Ethernet показан на рисунке.

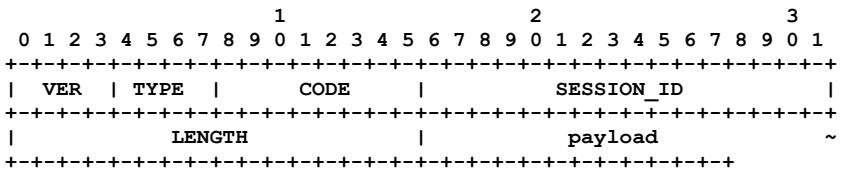


Поле DESTINATION_ADDR содержит индивидуальный Ethernet-адрес[3] получателя или широковещательный адрес Ethernet (0xffffffff). Для пакетов Discovery адрес может быть индивидуальным или широковещательным, как описано в параграфе 5. Этап Discovery. Для трафика сеансов PPP это поле **должно** содержать индивидуальный адрес партнёра, определённый на этапе Discovery.

Поле SOURCE_ADDR **должно** содержать MAC-адрес отправителя.

Поле ETHER_TYPE имеет значение 0x8863 (Discovery) или 0x8864 (PPP Session).

Данные кадра Ethernet для PPPoE имеют следующий формат:



Поле VER имеет размер 4 бита и **должно** иметь значение 0x1 для данной версии спецификации PPPoE.

4-битовое поле TYPE **должно** иметь значение 0x1 для данной версии спецификации PPPoE.

8-битовое поле CODE определено ниже при описании этапов Discovery и PPP Session.

Поле SESSION_ID имеет размер 16 битов и трактуется как целое число без знака с сетевым порядком байтов. Значения поля для этапа Discovery определены ниже. Значение этого поля фиксируется для данной сессии PPP и, фактически, определяет связь пакета с сессией PPP вместе с полями SOURCE_ADDR и DESTINATION_ADDR кадра Ethernet. Значение 0xffff зарезервировано и его использование **недопустимо**.

Поле LENGTH имеет размер 16 битов. Значение этого поля (сетевой порядок байтов) определяет размер информационного поля PPPoE. Значение поля не учитывает размер заголовков Ethernet и PPPoE.

5. Этап Discovery

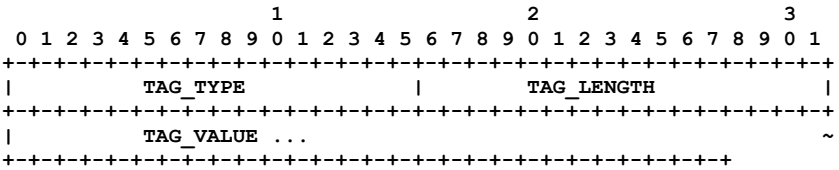
Этап обнаружения (Discovery) состоит из 4 частей. По завершении этого этапа оба партнёра получает значение идентификатора сессии PPPoE (SESSION_ID) и Ethernet-адрес своего партнёра, которые совместно обеспечивают уникальную идентификацию сеансов PPPoE. Процесс обнаружения включает широковещательную передачу хостом

[1]Discovery stage.
[2]PPP Session stage.
[3]MAC-адрес. *Прим. перев.*

пакета Initiation, передачу одним или несколькими концентраторами доступа пакетов Offer, передачу хостом пакета Session Request по индивидуальному адресу и передачу выбранным концентратором доступа пакета Confirmation (подтверждение). Когда хост получает пакет Confirmation, он может переходить к этапу PPP Session. Концентратор доступа, передав пакет Confirmation, может переходить к этапу PPP Session.

Все кадры Ethernet на этапе Discovery имеют значение ETHER_TYPE = 0x8863.

Информационное поле PPPoE может содержать теги, представляющие собой триплеты TLV[1], формат которых показан ниже.



16-битовое поле TAG_TYPE использует сетевой порядок байтов. Список значений полей TAG_TYPE и TAG_VALUE приведён в Приложении A.

Поле TAG_LENGTH имеет размер 16 битов. Это целое число без знака с сетевым порядком байтов показывает число октетов в поле TAG_VALUE.

Если на этапе обнаружения получен пакет с тегом неизвестного типа, данный тег **должен** игнорироваться, если в этом документе явно не указано иное. Такое поведение обеспечит обратную совместимость в случае добавления новых тегов. При добавлении новых тегов со статусом обязательных (mandatory) будет изменён номер версии.

Примеры пакетов Discovery приводятся в Приложении B.

5.1 Пакет PADI

Хост передаёт пакет PADI[2] с широковещательным адресом в поле DESTINATION_ADDR. Поле CODE имеет значение 0x09, а поле SESSION_ID **должно** иметь значение 0x0000.

Пакет PADI **должен** включать в точности единственный тег типа Service-Name, показывающий запрашиваемый хостом тип сервиса, и может также содержать произвольное число тегов иных типов. Размер пакета PADI в целом (включая заголовок PPPoE) **не может** превышать 1484 октетов, чтобы транслирующий пакет агент мог добавить тег Relay-Session-Id.

5.2 Пакет PADO

Когда концентратор доступа получает пакет PADI, который он может обслужить, этот концентратор передаёт в ответ пакет PADO[3]. Поле DESTINATION_ADDR в этом пакете содержит индивидуальный адрес хоста, передавшего пакет PADI. Поле CODE имеет значение 0x07, а поле SESSION_ID **должно** иметь значение 0x0000.

Пакет PADO **должен** содержать один тег AC-Name, указывающий имя концентратора доступа, и тег Service-Name из полученного пакета PADI, а также может включать произвольное число тегов Service-Name, показывающих другие типы сервиса, предоставляемого данным концентратором доступа. Если концентратор доступа не может обслужить пакет PADI, для него **недопустимо** передавать в ответ пакет PADO.

5.3 Пакет PADR

Поскольку пакет PADI передается с использованием широковещательного адреса, хост может получить в ответ более одного пакета PADO. Хост просматривает полученные пакеты PADO и выбирает один из них. Выбор может основываться на включённых в эти пакеты тегах AC-Name или предлагаемых концентратором услугах. После этого хост передаёт выбранному концентратору доступа один пакет PADR[4]. Поле DESTINATION_ADDR в этом пакете содержит индивидуальный Ethernet-адрес выбранного концентратора доступа из пакета PADO. Поле CODE имеет значение 0x19, а поле SESSION_ID **должно** иметь значение 0x0000.

Пакет PADR **должен** включать в точности один тег типа Service-Name, показывающий запрашиваемый хостом сервис, и может также включать произвольное число тегов иных типов.

5.4 Пакет PADS

Когда концентратор доступа получает пакет PADR, он готовится к началу сеанса PPP. Концентратор генерирует уникальное значение SESSION_ID для сеанса PPPoE и отвечает хосту пакетом PADS[5]. Поле DESTINATION_ADDR в этом пакете содержит индивидуальный Ethernet-адрес хоста из пакета PADR. Поле CODE имеет значение 0x65, а поле SESSION_ID **должно** содержать уникальный идентификатор, созданный для сеанса PPPoE.

Пакет PADS содержит единственный один тег типа Service-Name, показывающий тип сервиса, для которого концентратор доступа организовал сеанс PPPoE, и может также включать произвольное число тегов иных типов.

Если концентратор доступа не устраивает значение Service-Name из пакета PADR, он **должен** ответить пакетом PADS, содержащим тег типа Service-Name-Error (и произвольное количество прочих тегов). В этом случае поле SESSION_ID **должно** иметь значение 0x0000.

5.5 Пакет PADT

Пакет этого типа может передаваться после организации сеанса PPPoE для индикации разрыва сессии. Такие пакеты могут передаваться как хостом, так и концентратором доступа. Поле DESTINATION_ADDR содержит индивидуальный

[1]Type-length-value - тип-размер-значение.
[2]PPPoE Active Discovery Initiation - инициирование процесса обнаружения PPPoE. *Прим. перев.*
[3]PPPoE Active Discovery Offer.
[4]PPPoE Active Discovery Request.
[5]PPPoE Active Discovery Session-confirmation.

адрес Ethernet, поле CODE имеет значение 0xa7, а поле SESSION_ID **должно** содержать идентификатор прерываемой сессии. Тегов для пакетов этого типа не требуется.

При получении пакета PADT[1] не допускается дальнейшая передача трафика PPP в данной сессии. Для нормального завершения сеанса PPP **недопустимо** использовать пакеты PADT. Узлу PPP **следует** использовать средства протокола PPP для завершения сессии PPPoE, однако пакеты PADT **могут** применяться в тех случаях, когда невозможно использовать средства протокола PPP.

6. Этап PPP Session

После организации сеанса PPPoE данные PPP передаются как обычно (инкапсуляция PPP). Все кадры Ethernet используют индивидуальные адреса. Для поля ETHER_TYPE устанавливается значение 0x8864. Поле CODE пакетов PPPoE **должно** иметь значение 0x00. Значение поля SESSION_ID **недопустимо** изменять с течение сеанса PPPoE и это значение должно совпадать с идентификатором, полученным на этапе Discovery. Информационное поле пакетов PPPoE содержит кадр PPP, начинающийся с идентификатора Protocol-ID. Примеры пакетов показаны в Приложении B.

7. Вопросы управления каналом (LCP)

Рекомендуется использовать конфигурационную опцию LCP Magic Number и **не рекомендуется** использовать опцию PFC[2]. Для реализаций **недопустимо** запрашивать любые из перечисленных ниже опций и **требуется** отвергать запросы на такие опции:

- FCS[3] Alternatives;
- ACFC[4];
- ACCM[5].

Для опции MRU[6] **недопустимо** согласовывать значения более 1492[7]. Поскольку кадр Ethernet может включать не более 1500 октетов полезной информации, заголовок PPPoE занимает 6 октетов, а поле PPP Protocol ID - 2 октета, значение PPP MTU **недопустимо** делать более 1492.

Концентраторам доступа **рекомендуется** время от времени передавать хосту пакеты Echo-Request для определения состояния сеанса. В противном случае, если хост прервал сессию без передачи пакета Terminate-Request, концентратор доступа не сможет определить, что сессия уже разорвана.

При прерывании LCP хост и концентратор доступа **должны** прекратить использование сессии PPPoE. Если хост желает организовать другой сеанс PPP, он **должен** вернуться к этапу PPPoE Discovery.

8. Прочие вопросы

Если хост не получает пакета PADO в течение заданного интервала времени, ему **следует** заново передать свой пакет PADI и удвоить период ожидания. Эта процедура может повторяться желаемое количество раз. При ожидании хостом пакета PADS **следует** применять аналогичную процедуру с повтором передачи пакета PADR. После заданного числа попыток хосту **следует** повторить передачу пакета PADI.

Значения ETHER_TYPE, используемые в данном документе (0x8863 и 0x8864), были выделены IEEE для использования с PPPoE. Эти значения в комбинации с полем PPPoE VER (версия) служат уникальным идентификатором протокола.

В данном документе используется кодировка UTF-8 [5] взамен ASCII. UTF-8 поддерживает весь набор символов ASCII, а также символы других языков. Дополнительную информацию об этой кодировке можно найти в документе [5].

9. Вопросы безопасности

Для защиты от DoS-атак[8] концентраторы доступа могут использовать тег AC-Cookie. Концентраторам **следует** обеспечивать возможность повторной генерации уникальных значений поля TAG_VALUE на основе значения поля SOURCE_ADDR в пакете PADR. Такой подход обеспечивает гарантию того, что поле SOURCE_ADDR в пакете PADI содержит доступный адрес, и позволяет ограничить число одновременных сессий для этого адреса. Выбор алгоритма не задаётся спецификацией и остаётся за разработчиками. Примером алгоритма может служить использование HMAC [3] применительно к MAC-адресу хоста с ключом, который известен лишь концентратору доступа. Тег AC-Cookie помогает предотвратить некоторые типы DoS-атак, но он не может защитить от всех атак на службы и концентраторы доступа **могут** применять также другие механизмы защиты.

Многие концентраторы доступа не захотят сообщать информацию о поддерживаемых услугах непроверенным хостам. В таких случаях концентратору следует реализовать один из двух вариантов политики:

- концентратору ни в коем случае **не следует** отвергать запросы на основании тега Service-Name и всегда **следует** возвращать значение TAG_VALUE, которое было передано концентратору;
- концентратору **следует** принимать только запросы, в которых тег Service-Name имеет поле TAG_LENGTH=0 (любой сервис).

Рекомендуется использовать второй вариант.

---

[1] PPPoE Active Discovery Terminate.
[2] Protocol Field Compression - сжатие полей протокола.
[3] Field Check Sequence - контрольная сумма поля.
[4] Address-and-Control-Field-Compression - сжатие адресных и управляющих полей.
[5] Asynchronous-Control-Character-Map - отображение символов асинхронного управления.
[6] Maximum-Receive-Unit - максимальный размер принимаемого пакета.
[7] В RFC 4638 внесены коррективы в это требование. *Прим. перев.*
[8] Denial of Service - атака, направленная на отказ служб.

10. Благодарности

Этот документ основан на результатах дискуссий в нескольких форумах, включая ADSL forum.

Часть текста документа была заимствована из RFC 1661, RFC 1662 и RFC 2364.

11. Литература

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

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

[3] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1998.

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

[5] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

Приложение A

Типы и значения тегов

0x0000 End-Of-List

Этот тег показывает завершение списка имеющихся тегов. Поле TAG_LENGTH для этого тега всегда **должно** иметь нулевое значение. Использование этого тега не обязательно, но рекомендуется с точки зрения совместимости со старыми версиями.

0x0101 Service-Name

Этот тег показывает, что далее следует имя сервиса. Поле TAG_VALUE представляет собой строку символов UTF-8 без завершающего NULL-символа. Нулевое значение поля TAG_LENGTH служит для индикации приемлемости любого сервиса. Примером использования тега Service-Name может служить индикация имени ISP[2], класса или качества обслуживания.

0x0102 AC-Name

Этот тег показывает, что далее следует строка, являющаяся уникальным идентификатором данного концентратора доступа. Эта строка может представлять собой, например, комбинацию торговой марки, модели и серийного номера устройства или просто задавать MAC-адрес концентратора в кодировке UTF-8. Строка не завершается NULL-символом.

0x0103 Host-Uniq

Этот тег используется хостом для того, чтобы однозначно (уникально) связать отклик концентратора доступа (PADO или PADS) с определенным запросом хоста (PADI или PADR). Значение TAG_VALUE представляет собой бинарные данные произвольного размера, выбранные хостом. Значение этого поля не интерпретируется концентратором доступа. Хост **может** включать тег Host-Uniq в пакеты PADI или PADR. Если концентратор доступа получает такой тег, он **должен** без изменений скопировать его в соответствующий отклик PADO или PADS.

0x0104 AC-Cookie

Этот тег используется концентраторами доступа для защиты от атак на службы (см. параграф 9. Вопросы безопасности). Концентратор **может** включать этот тег в пакет PADO. Если хост получает пакет с таким тегом, он **должен** без изменений скопировать тег в соответствующий пакет PADR. Поле TAG_VALUE представляет собой бинарные данные произвольной длины, которые не интерпретируются хостом.

0x0105 Vendor-Specific

Этот тег используется для передачи фирменной (proprietary) информации от производителя. Первые 4 октета поля TAG_VALUE содержат идентификатор производителя, а остальные могут быть произвольными (не задаются спецификацией). Старший октет идентификатора производителя имеет значение 0, а остальные 3 октета содержат значение SMI Network Management Private Enterprise Code для данного производителя с использованием сетевого порядка байтов. Коды определены в документе Assigned Numbers [4].

Использование этого тега **не рекомендуется**. В целях обеспечения взаимодействия реализация может игнорировать тег Vendor-Specific.

0x0110 Relay-Session-Id

Этот тег может добавляться к любым пакетам обнаружения на промежуточных агентах, транслирующих трафик. Поле TAG_VALUE не интерпретируется хостом и концентратором доступа. Если хост или концентратор получает пакет с таким тегом, он **должен** скопировать тег без изменений в передаваемый пакет отклика. Во всех пакетах PADI **должно** резервироваться место для добавления тега Relay-Session-Id TAG с полем TAG_VALUE размером 12 октетов.

Тег Relay-Session-Id **недопустимо** добавлять, если в пакете обнаружения уже имеется такой тег. В этом случае промежуточному транслятору **следует** использовать существующий тег Relay-Session-Id. Если существующий тег нельзя использовать или в пакете нет места для добавления тега Relay-Session-Id, отправителю пакета **следует** отправить пакет с тегом Generic-Error.

0x0201 Service-Name-Error

Этот тег TAG (обычно с полем данных нулевого размера) показывает, что по той или иной причине запрос Service-Name не может быть удовлетворён.

Если тег содержит данные и их первый октет отличается от нуля, эти данные **должны** представлять собой строку в кодировке UTF-8, которая объясняет причину отказа. Строка **может** не содержать завершающего NULL-символа.

0x0202 AC-System-Error

Этот тег показывает, что концентратор доступа столкнулся с той или иной ошибкой при выполнении запроса хоста (например, нехватка ресурсов для создания виртуального устройства). Тег **может** включаться в пакеты PADS.

Если тег включает данные, первый октет которых отличается от 0, эти данные **должны** представлять собой строку в кодировке UTF-8, объясняющую причину ошибки. Строка **может** не содержать завершающего NULL-символа.

---

[1] В соответствии с RFC 3232 документ RFC 1700 утратил статус стандарта. Выделенные значения доступны на сайте, указанном ссылкой. *Прим. перев.*

[2] Internet Service Provider - поставщик услуг Internet. *Прим. перев.*

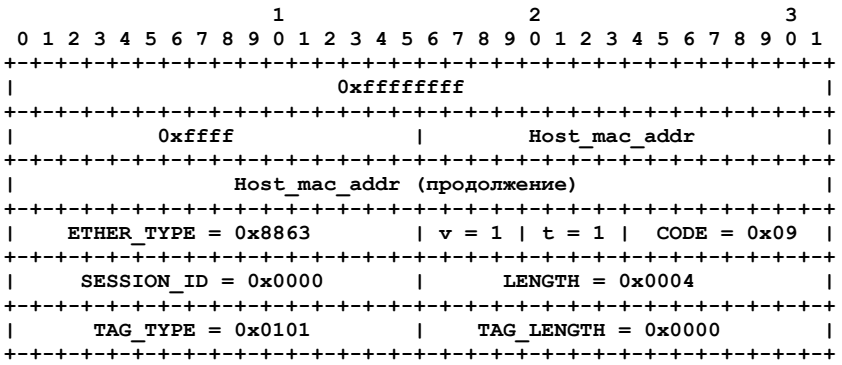
0x0203 Generic-Error

Этот тег указывает на наличие ошибки. Тег может включаться в пакеты PADO, PADR или PADS при возникновении неисправимой ошибки и отсутствии иных тегов, подходящих для объяснения причин ошибки. Если тег содержит данные, последние **должны** представлять собой строку в кодировке UTF-8, объясняющую причину ошибки. Строка **может** не содержать завершающего NULL-символа.

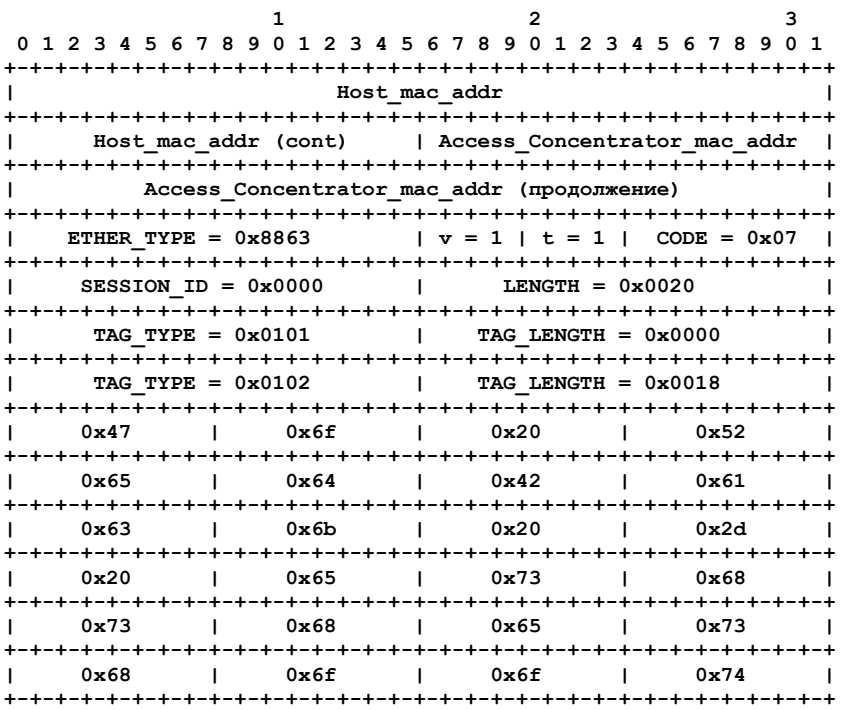
Приложение B

Ниже приводятся примеры некоторых пакетов.

Пакет PADI

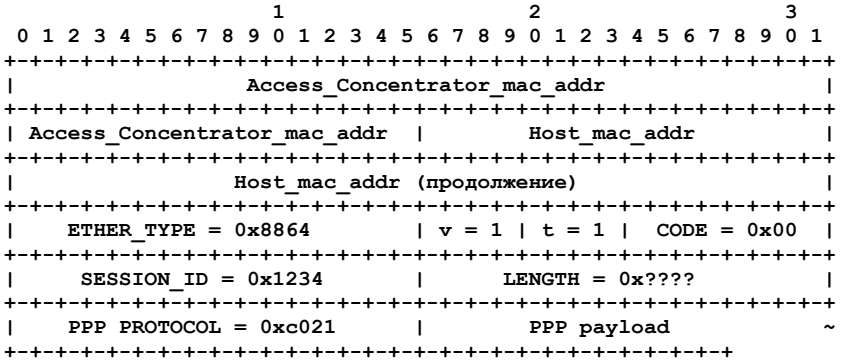


Пакет PADO



Пакет PPP LCP

В примере указан идентификатор протокола PPP (0xc021), но данные PPP (payload) не приводятся. Такие пакеты передаются от хоста концентратору доступа.



Адреса авторов

Louis Mamakos
UUNET Technologies, Inc.
3060 Williams Drive
Fairfax, VA 22031-4648
United States of America
EMail: louie@uu.net

Kurt Lidl
UUNET Technologies, Inc.
3060 Williams Drive
Fairfax, VA 22031-4648
United States of America
EMail: lidl@uu.net

Jeff Evarts
UUNET Technologies, Inc.
3060 Williams Drive
Fairfax, VA 22031-4648
United States of America
EMail: jde@uu.net

David Carrel
RedBack Networks, Inc.
1389 Moffett Park Drive
Sunnyvale, CA 94089-1134
United States of America
EMail: carrel@RedBack.net

Dan Simone
RedBack Networks, Inc.
1389 Moffett Park Drive
Sunnyvale, CA 94089-1134
United States of America
EMail:dan@RedBack.net

Ross Wheeler
RouterWare, Inc.
3961 MacArthur Blvd., Suite 212
Newport Beach, CA 92660
United States of America
EMail: ross@routerware.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав