

24

Стек PPP

Стек протоколов PPP (Point-to-Point Protocol) кроме протокола PPP включает перечисленные ниже протоколы:

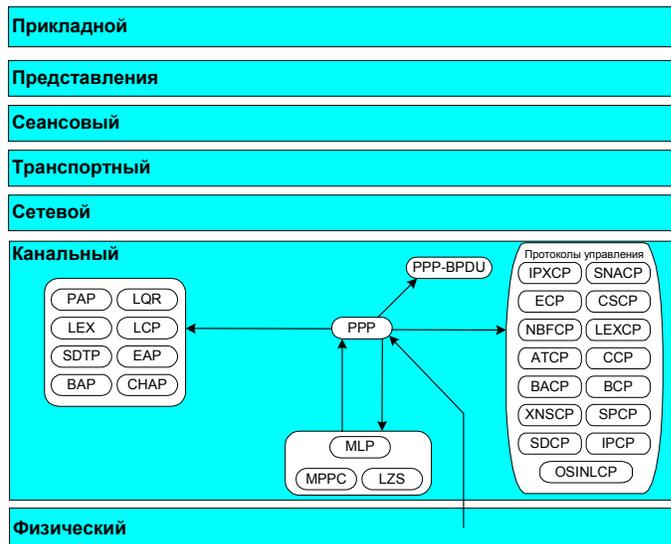
- MLP - Multilink PPP
- PPP-BPDU - PPP Bridge Protocol Data Unit
- PPPoE - PPP over Ethernet
- BAP - Bandwidth Allocation Protocol
- BSD - UNIX Compress Command source
- CHAP - Challenge Handshake Authentication Protocol
- DESE - DES Encryption Algorithm
- EAP - Extensible Authentication Protocol
- LCP - Link Control Protocol
- LEX - LAN Extension Interface Protocol
- LQR - Link Quality Report
- PAP - Password Authentication Protocol

© RADCOM, Ltd., 1999, Перевод на русский язык. © BiLiM Systems Ltd., 2000. <http://www.bilim.com>

Управляющие протоколы PPP

- ATCP - AppleTalk Control Protocol
- BACP - Bandwidth Allocation Control Protocol
- BCP - Bridging Control Protocol
- BVCP - PPP Banyan Vines Control Protocol
- CCP - Compression Control Protocol
- DNCP - PPP DECnet Phase IV Control Protocol
- ECP - Encryption Control Protocol
- IPCP - IP Control Protocol
- IPv6CP - IPv6 Control Protocol
- IPXCP - IPX Control Protocol
- LEXCP - LAN Extension Interface Control Protocol
- NBFCP - PPP NetBIOS Frames Control Protocol
- OSINLCP - OSI Network Layer Control Protocol
- SDCP - Serial Data Control Protocol
- SNACP - SNA PPP Control Protocol

На рисунке показано расположение протоколов стека PPP в эталонной модели OSI.



Положение стека протоколов PPP в эталонной модели OSI

PPP

RFC1548 <http://www.cis.ohio-state.edu/htbin/rfc/rfc1548.html>

RFC1661 <http://www.cis.ohio-state.edu/htbin/rfc/rfc1661.html>

RFC1662 <http://www.cis.ohio-state.edu/htbin/rfc/rfc1662.html>

Протокол PPP (Point-to-Point Protocol) предназначен для организации простых каналов, которые позволяют передавать пакеты между узлами одного уровня (peer). Эти каналы обеспечивают полнодуплексную связь (передача в обоих направлениях одновременно). Предполагается, что порядок следования пакетов при доставке через каналы PPP не нарушается. PPP обеспечивает простое решение для соединения различных хостов, мостов и маршрутизаторов.

Структура заголовков PPP показана на рисунке.

Адрес	Управление	Протокол	Информация	FCS
1 байт	1 байт	2 байта	переменный	2 байта

Структура заголовка PPP

Адрес

Широковещательный адрес HDLC. PPP не использует индивидуальных адресов для станций. Поле адреса в заголовке пакетов PPP всегда должно иметь значение FF

Управление

Команда HDLC для нумерованной информации (Unnumbered Information или UI) с нулевым значением бита Poll/Final. Кадры, содержащие в этом поле любое другое значение, будут отбрасываться.

Протокол

Идентификатор протокола, инкапсулированного в информационном поле кадра.

Информация

Данные протоколов вышележащих уровней.

FCS

Контрольная сумма кадра. Протокол PPP проверяет значение контрольной суммы после доставки пакета.

MLP (Multilink PPP)

RFC1717 <http://www.ietf.org/rfc/rfc1717.txt>

RFC1990 <http://www.ietf.org/rfc/rfc1990.txt>

Поддержка мультиканального режима Multilink основана на опции согласования параметров LCP, позволяющей станции сообщить станции-партнеру о возможности объединения нескольких физических каналов передачи данных в один логический канал. Одно "пакета" физических каналов достаточно практически для любых условий связи между парой станций.

Согласование параметров выполняется на начальной фазе согласования опций LCP. Система показывает своему партнеру того же уровня (peer) намерение использовать мультиканальный режим путем передачи мультиканальной опции на начальной фазе согласования параметров LCP. Согласование параметров показывает следующие возможности:

1. Система, предлагающая мультиканальный режим, может объединять несколько физических каналов в одно логическое соединение.
2. Система способна принимать фрагментированные PDU вышележащих уровней с использованием мультиканального заголовка и собирать фрагменты в исходный модуль данных PDU.
3. Система может принимать PDU размером N октетов, где N задается как часть опций согласования даже в тех случаях, когда N превышает значение MRU (максимальный размер принимаемого пакета) для одного физического канала.

При использовании протокола Multilink PPP пакеты сначала инкапсулируются (но не кадрируются) в соответствии с обычными процедурами PPP - большие пакеты разбиваются на фрагменты меньших размеров, приемлемых для физических каналов. Перед каждой секцией пакета вставляется новый PPP заголовок, содержащий идентификатор протокола Multilink PPP и заголовок Multilink.. Таким образом, первый фрагмент мультиканального пакета PPP будет содержать два заголовка - заголовок фрагмента и заголовок пакета.

Фрагменты Multilink PPP инкапсулируются с использованием идентификатора протокола 0x00 - 0x3d. Вслед за идентификатором протокола размещается четырехбайтовый заголовок, содержащий порядковый номер, и 2 однобайтовых поля, показывающие первый и последний фрагмент пакета. После согласования дополнительных опций PPP LCP четырехбайтовый заголовок может быть заменен двухбайтовым заголовком, после которого размещаются 12 последовательных нулей. Поля Адрес/Управление и Идентификатор протокола сохраняют свое назначение.

На рисунке показан формат пакетов с длинным порядковым номером фрагмента.

Заголовок PPP	Адрес 0xff						Управление 0x03	
	PID (H) 0x00						PID (L) 0x3d	
Заголовок MP	B	E	O	O	O	O	Порядковый номер	
	Порядковый номер (L)							
PPP FCS	Фрагмент данных							
	.							
	.							
FCS								

Фрагмент Multilink PPP с длинным порядковым номером

На следующем рисунке показан формат фрагмента с коротким порядковым номером.

Заголовок PPP	Адрес 0xff						Управление 0x03	
	PID (H) 0x00						PID (L) 0x3d	
Заголовок MP	B	E	O	O	Порядковый номер			
	Фрагмент данных							
PPP FCS	.							
	.							
	FCS							

Фрагмент Multilink PPP с коротким порядковым номером

PID

Идентификатор протокола.

B

Флаг начального (первого) фрагмента. Нулевое значение этого поля указывает, что фрагмент не является первым фрагментом пакета PPP, а 1 указывает первый фрагмент. Таким образом, для последовательности фрагментов этот бит устанавливается только в заголовке первого фрагмента.

E

Флаг конечного (последнего) фрагмента. Нулевое значение этого поля указывает, что фрагмент не является последним фрагментом пакета PPP, а 1 указывает последний фрагмент. Это поле имеет нулевое значение для всех фрагментов пакета PPP, кроме последнего.

Порядковый номер

24-х или 12-битовый номер фрагмента. Фрагменты нумеруются по порядку с увеличением номера на 1. По умолчанию используются 24-битовые (длинные) номера, но при согласовании опций конфигурации LCP можно договориться об использовании 12-битовых (коротких) номеров.

О

Зарезервированные поля между флагом последнего фрагмента и порядковым номером. Эти поля в настоящее время не используются и должны иметь нулевые значения. В пакетах с длинным порядковым номером используется 6 полей О, в пакетах с коротким номером - 2.

FCS

Контрольная сумма. Значение контрольной суммы наследуется от обычного механизма кадрирования для канала, по которому передается пакет.

Тип MAC

Это поле может принимать следующие значения:

- 1 Bridge-Identification (идентификация моста)
- 2 Line-Identification (идентификация линии)
- 3 MAC-Support (поддержка MAC)
- 4 Tinygram-Compression (компрессия Tinygram)
- 5 LAN-Identification (идентификация ЛВС)
- 6 MAC-Address (MAC-адрес)
- 7 Spanning-Tree-Protocol (протокол Spanning Tree).

Идентификатор ЛВС

Необязательное 32-битовое поле, идентифицирующее сообщество ЛВС (Community of LAN), заинтересованных в получении данного кадра. Если флаг LAN ID (идентификатор ЛВС) не установлен, это поле отсутствует, делая PDU на 4 октета короче.

Управление кадром

В ЛВС 802.4, 802.5 и FDDI перед MAC-адресом получателя имеется несколько октетов, один из которых защищен FCS. Поле "Тип MAC" задает содержимое поля управления кадром. Для выравнивания по 32-битовой границе используется октет заполнения.

MAC-адрес получателя

Адрес получателя в соответствии со спецификацией IEEE. Порядок битов адреса определяется значением поля "Тип MAC."

MAC-адрес отправителя

Адрес отправителя в соответствии со спецификацией IEEE. Порядок битов адреса определяется значением поля "Тип MAC."

Данные LLC

Данные уровня управления логическим каналом (LLC) составляют остальную часть кадра MAC и (если они присутствуют) учитываются при расчете контрольной суммы LAN FCS.

PPPoE

RFC 2516 <http://www.ietf.org/rfc/rfc2516.txt>

PPPoE представляет собой метод передачи PPP в сетях Ethernet. Этот метод обеспечивает возможность соединить сеть хостов с концентратором удаленного доступа через простой мост. При использовании такой модели каждый хост использует свой стек PPP и пользователю предоставляется привычный интерфейс. Управление доступом, учет использования сервиса и тип обслуживания можно задавать отдельно для каждого пользователя или (в более редких случаях) для всего сайта.

Для обеспечения парных (точка-точка) соединений через сеть Ethernet, каждая сессия PPP должна знать Ethernet-адрес удаленной станции того же уровня. Кроме того, для каждой сессии нужен уникальный идентификатор. Протокол PPPoE включает механизм обнаружения (discovery protocol), который решает эти задачи.

PPPoE имеет две различных стадии - обнаружение и сеанс PPP. Когда хост намеревается инициировать сеанс PPPoE, он должен сначала провести обнаружение для определения MAC-адреса Ethernet партнера, а потом организовать PPPoE SESSION_ID. В протоколе PPP используются между узлами одного уровня (peer), а процесс обнаружения использует модель "клиент-сервер". В процессе обнаружения хост (клиент) находит концентратор доступа (сервер). В зависимости от топологии сети может использоваться один или несколько концентраторов доступа, с которыми может работать каждый хост. При успешном завершении этапа обнаружения хост и выбранный концентратор доступа имеют информацию, требуемую для организации соединения "точка-точка" через сеть Ethernet.

Этап обнаружения продолжается до тех пор, пока не будет организована сессия PPP. После организации сеанса PPP хост и концентратор доступа должны предоставить свои ресурсы для виртуального интерфейса PPP.

Поле EtherType в кадрах Ethernet имеет значение 0x8863 на этапе обнаружения и 0x8864 - на этапе сеанса PPP.

Формат данных Ethernet для PPPoE показан на рисунке.

4	8	16
Версия	Тип	Код
Идентификатор сессии		
Размер		
Содержимое (payload)		

Формат содержимого Ethernet для PPPoE

Версия

Задаёт номер версии и имеет значение 0x1 для текущей версии PPPoE (RFC 2516).

Тип

Имеет значение 0x1 для текущей версии PPPoE (RFC 2516).

Код

Значение кода зависит от переданного пакета:

<i>Пакет</i>	<i>Код</i>
Этап обнаружения	
Active Discovery Initiation (PADI)	0x09
Active Discovery Offer (PADO)	0x07
Active Discovery Request (PADR)	0x19
Active Discovery Session-confirmation (PADS)	0x65
Active Discovery Terminate (PADT)	0xa7
Этап сеанса PPP	0x00

Идентификатор сессии

Беззнаковое целое число, которое вместе с адресами отправителя и получателя идентифицирует сеанс PPP. Значение 0xffff зарезервировано для использования в будущем.

Размер

Размер поля содержимого пакета PPPoE без учёта заголовков Ethernet и PPPoE.

ВАР

RFC 2125 <http://www.ietf.org/rfc/rfc2125.txt>

Протокол выделения полосы ВАР (Bandwidth Allocation Protocol) можно использовать для управления числом каналов в мультисканальном потоке. ВАР определяет дейтаграммы для координации процессов добавления или отключения отдельных каналов мультисканального потока. Эти же дейтаграммы используются для задания узла, ответственного за различные решения, связанные с управлением полосой мультисканального потока.

Формат пакетов ВАР показан на рисунке.

Тип	Размер	Данные
1 байт	1 байт	Переменный размер

Формат пакетов ВАР

Тип

Однооктетное поле, показывающее тип дейтаграммы ВАР. В приведенном ниже списке показаны возможные значения кодов в шестнадцатеричном формате.

- 1 Call-Request (запрос соединения)
- 2 Call-Response (отклик на запрос соединения)
- 3 Callback-Request (запрос обратного соединения)
- 4 Callback-Response (отклик на запрос обратного соединения)
- 5 Link-Drop-Query-Request (запрос сброса канала)
- 6 Link-Drop-Query-Response (отклик на запрос сброса канала)
- 7 Call-Status-Indication (индикация состояния соединения)
- 8 Call-Status-Response (запрос состояния соединения)

Размер

Однооктетное поле, показывающее размер опций ВАР с учетом полей типа, размера и данных.

Данные

Поле, содержащее информацию ВАР. Формат и размер поля данных определяются значениями предшествующих полей. Поле данных может иметь нулевой размер.

BSD

RFC 1977 <http://www.ietf.org/rfc/rfc1977.txt>

BSD представляет собой бесплатный и широко распространенный механизм компрессии данных UNIX. Основные особенности BSD перечислены ниже.

- Динамическая очистка таблиц в тех случаях, когда эффективность компрессии снижается.
- Автоматическое отключение компрессии в тех случаях, когда сжатые данные по размеру не меньше исходных.
- Динамический выбор размера кода в определенных пределах.
- Многолетняя практика использования протокола в сетях, на модемных линиях и других каналах "точка-точка."
- Эффективная ширина кода, требующая менее 64К памяти на приемной и передающей стороне.

До того, как какой-либо пакет BSD Compress будет передан, протокол PPP должен дойти до фазы сетевого уровня, а протокол управления CCP должен дойти до стадии открытия. В информационное поле пакетов PPP с полем протокола, имеющим значение 0xFD или 0xFB инкапсулируется единственная дейтаграмма BSD Compress. 0xFD используется вместе MLP для независимой компрессии на каждом физическом канале мультисканального потока. Максимальный размер дейтаграммы BSD Compress, передаваемой через канал PPP совпадает с максимальным размером информационного поля пакета инкапсулированного в PPP. Сжатие возможно только для пакетов с номерами от 0x0000 до 0x3FFF, исключая номера 0xFD и 0xFB. Остальные пакеты PPP передаются без сжатия. Пакеты управления достаточно редки и должны передаваться без компрессии.

CHAP

RFC 1334 <http://www.ietf.org/rfc/rfc1334.txt>

Протокол аутентификации CHAP (Challenge Handshake Authentication Protocol) используется для периодической проверки узлов одного уровня, использующих трехстороннюю процедуру согласования (handshake). Процедура проверки выполняется при организации соединения и может повторяться в любой момент в процессе использования канала.

В информационное поле пакетов PPP с полем протокола 0xc223 инкапсулируется единственный пакет CHAP. Структура пакетов CHAP показана на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов CHAP

Код

Код идентифицирует тип пакета CHAP и может принимать одно из перечисленных ниже значений:

- 1 Challenge (вызов, проверка)
- 2 Response (отклик)
- 3 Success (успех)
- 4 Failure (отказ)

Идентификатор

Дополнительная идентификация в зависимости от типа пакета.

Размер

Размер пакета CHAP с учетом всех полей.

Данные

Поле, содержащее данные в формате, определяемом полем кода. Формат данных для пакетов Challenge и Response показан ниже.

Размер значения	Значение	Имя
1 байт		1 байт

Структура поля данных для пакетов CHAP Challenge и Response

Размер значения

Это поле определяет размер поля значения.

Значение

Значение Challenge представляет собой поток октетов, который должен изменяться при каждом повторении вызова.

Значение Response представляет собой результат расчета на основе потока октетов, содержащего Идентификатор, "Секрет" и значение Challenge.

Имя

Идентификатор системы, передающей пакет.

Для пакетов Success и Failure поле данных имеет переменную длину, а содержащаяся в нем информация зависит от реализации протокола.

DESE

RFC 1969 <http://www.ietf.org/rfc/rfc1969.txt>

Алгоритм DES (Data Encryption Standard) Encryption является хорошо известной, понятной и широко распространенной реализацией алгоритма шифрования, предназначенной для эффективного шифрования на аппаратном уровне. DESE представляет опцию ECP, показывающую что предлагается использовать шифрование DES для коммуникационного канала.

Формат пакетов DESE показан на рисунке.

Адрес	Управление	0 0 0 0	Идентификатор протокола
Номер сегмента (старшая часть)	Номер сегмента (младшая часть)	Ciphertext (переменный размер)	

Формат пакетов DESE

Идентификатор протокола

Поле идентификатора протокола может иметь значение 0x53 или 0x55. Значение 0x55 говорит о том, что поле Ciphertext содержит заголовки для MLP и требует, чтобы протокол Individual Link Encryption Control Protocol находился в открытом состоянии. Нули перед полем идентификатора протокола могут отсутствовать, если опция PFC (PPP Protocol Field Compression) согласована.

Номер сегмента

Порядковые номера сегментов представляют собой 16-битовые числа, присваиваемые программой шифрования по порядку, начиная с нуля (для первого пакета, переданного после того, как ECP достигнет открытого состояния).

Ciphertext

Генерация зашифрованных данных описана в стандарте DESE.

EAP

RFC 2284 <ftp://ftp.isi.edu/in-notes/rfc2284.txt>

RFC 2716 <ftp://ftp.isi.edu/in-notes/rfc2716.txt>

Расширенный протокол аутентификации EAP (Extensible Authentication Protocol) представляет собой расширение PPP, обеспечивающее поддержку дополнительных методов аутентификации в PPP.

Формат заголовка пакетов EAP показан на рисунке.

Код	Идентификатор	Размер	Тип	Данные
1 байт	1 байт	2 байта	1 байт	Переменный размер

Формат заголовка EAP

Код

Десятичное значение, задающее тип пакета EAP:

- 1 Request
- 2 Responce
- 3 Success
- 4 Failure

Идентификатор

Дополнение к соответствующим откликам

Размер

Размер всех полей пакета в октетах. Октеты, выходящие за пределы указанного размера, трактуются как заполнение канального уровня и отбрасываются на приемной стороне.

Тип

Задаёт тип EAP. Поддерживаются следующие типы:

- KEA validate
- KEA public
- GTC
- OTP
- MD5
- NQK
- Notification
- Identify.

LCP

RFC 1570 <http://www.ietf.org/rfc/rfc1570.txt>

RFC 1661 <http://www.ietf.org/rfc/rfc1661.txt>

Для обеспечения возможности адаптации к различным средам протокол PPP использует специальный протокол управления каналом LCP (Link Control Protocol) для организации, настройки и проверки каналов связи. LCP служит для автоматического согласования опций инкапсуляции, размера пакетов, обнаружения возвратных (looped-back) каналов и других ошибок, а также для разрыва соединений. К дополнительным возможностям этого протокола относятся аутентификация участников соединения и проверка корректности работы канала с обнаружением сбоев.

Формат пакетов LCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов LCP

Код

Однооктетное поле, определяющее тип пакета LCP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject
- 8 Protocol-Reject
- 9 Echo-Request
- 10 Echo-Reply
- 11 Discard-Request
- 12 Link-Quality Report

Идентификатор

Десятичное значение, дополняющее соответствующий запрос или отклик

Размер

Размер всех полей пакета LCP.

Данные

Поле переменной длины, которое может содержать одну или несколько опций. Формат конфигурационных опций LCP показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Структура поля данных LCP

Тип

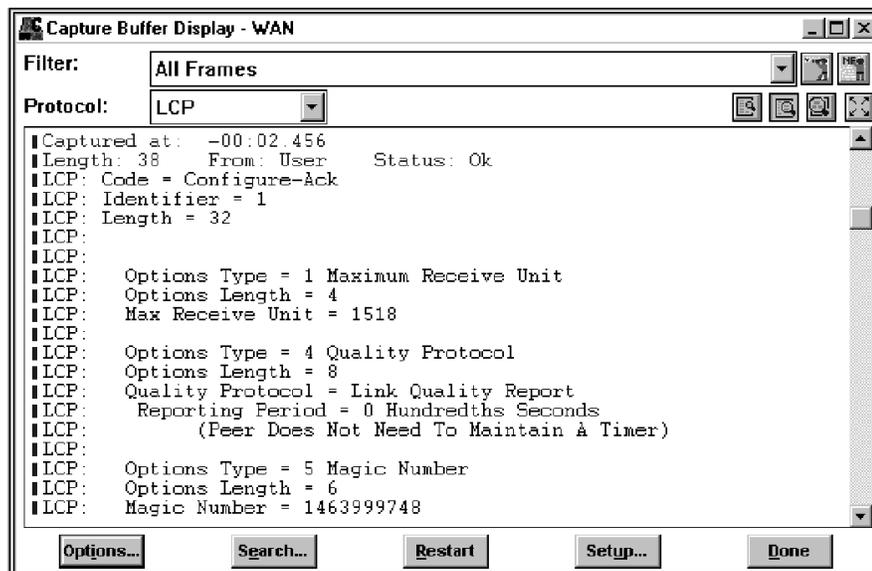
Однобайтовый идентификатор типа опций конфигурации.

Размер

Размер всех полей конфигурационных опций (тип, длина, данные).

Данные

Значение поля "Данные".



Декодирование протокола LCP

LEX

RFC 1841 <http://www.ietf.org/rfc/rfc1841.txt>

Интерфейс расширения ЛВС представляет собой аппаратный модуль, устанавливаемый на удаленных сайтах (например, дома или в филиале), подключенных к ЛВС через WAN-канал и центральный маршрутизатор. Для поддержки такой архитектуры были разработаны протоколы PPP NCP (Network Control Protocol) и PPP-LEX (LAN extension interface protocol). Назначением протокола LEX является инкапсуляция пакетов управления интерфейсом расширения ЛВС и пакетов данных. Последовательно передаваемые пакеты могут содержать данные или управляющую информацию. Пакеты управления описываются протоколом LEXCP.

Формат кадров показан PPP-LEX на приведенном ниже рисунке. Кадры MAC передаются с исключением поля FCS (контрольная сумма). Интерфейсные модули расширения ЛВС рассчитывают значение FCS для пакетов, передаваемых в локальную сеть, и вырезают значение FCS из пакетов, передаваемых маршрутизатору.

				4	8					16					24					32
Флаг HDLC																				
Адрес								Управление				Тип протокола								
F	I	Z	O	Заполн.				Тип MAC				MAC-адрес получателя								
MAC-адрес получателя																				
MAC-адрес отправителя																				
MAC-адрес отправителя								Размер/тип												
Данные LLC																				
HDLC CRC								Флаг HDLC												

Структура пакетов данных PPP-LEX

Флаг HDLC

Ограничитель кадра HDLC.

Адрес

Поле адреса содержит широковещательный адрес 0xFF.

Управление

Поле управления содержит нумерованную информацию (0x03).

Тип протокола

Идентификатор типа протокола, выделенный IETF (0x0041 - данные).

F

Этот флаг устанавливается при наличии поля LAN FCS. Пакеты данных PPP-LEX не содержат контрольной суммы LAN FCS и это поле всегда равно 0.

I

Флаг наличия поля LAN ID. Поскольку пакеты данных PPP-LEX не содержат идентификатора ЛВС, это поле всегда имеет нулевое значение.

Z

Этот флаг показывает, что нужно использовать заполнение IEEE 802.3.

O

Зарезервированное поле (0).

Заполнение

Любой кадр PPP может содержать байты заполнения в поле Optional Data Link Layer Padding. Значение данного поля говорит принимающей системе, какое количество октетов заполнения должно быть отброшено. Протокол расширения ЛВС не поддерживает заполнения и должно быть равно 0.

Тип MAC

Это поле может содержать значения типов MAC, перечисленные в последнем варианте Assigned Numbers RFC (в настоящее время - RFC). В соответствии с RFC 1841 это поле содержит идентификатор IEEE 802.3/Ethernet с канонической адресацией.

MAC-адрес получателя

6-октетное поле, содержащее MAC-адрес получателя в соответствии со спецификацией IEEE. Порядок битов адреса определяется полем Тип MAC.

MAC-адрес отправителя

6-октетное поле, содержащее MAC-адрес отправителя в соответствии со спецификацией IEEE. Порядок битов адреса определяется полем Тип MAC.

Размер/тип

Тип протокола Ethernet или размер пакета для кадров IEEE 802.3.

Данные LLC

Остальная часть кадра MAC, защищенная контрольной суммой LAN FCS.

HDLC CRC

16-битовая контрольная сумма.

LQR

RFC 1333 <http://www.ietf.org/rfc/rfc1333.txt>

Протокол LQR (Link Quality Report - отчет о качестве канала) описывает механизмы мониторинга каналов PPP. Пакеты могут отбрасываться или повреждаться в результате шумов в линии, сбоя оборудования, переполнения буферов и т.п. - зачастую важно определить, когда и при каких условиях повреждаются пакеты данных. Маршрутизаторы могут временно отдавать предпочтение другому маршруту или может быть реализовано переключение на альтернативный канал. Для решения связанных с такими ситуациями вопросов требуется механизм мониторинга качества каналов.

В информационное поле кадров канального уровня PPP с полем протокола c025 инкапсулируется один пакет LQR. Структура пакетов LQR показана на рисунке.

8	16	24	32
Магическое число			
Last out LQRs			
Last out Packets			
Last out octets			
Peer in LQRs			
Peer in packets			
Peer in discards			
Peer in errors			
Peer in octets			
Peer out LQRs			
Peer out packets			
Peer out octets			
Save in LQRs			
Save in packets			
Save in discards			
Save in errors			
Save in octets			

Структура пакета LQR

Магическое число

Вспомогательное поле для детектирующих каналов при наличии условий возврата (looped-back condition)

Last out LQRs

Значение этого поля копируется из последнего Peer Out LQR на передаче.

Last out Packets

Значение этого поля копируется из последнего Peer Out Packets на передаче.

Last out octets

Значение этого поля копируется из последнего Peer Out Octets на передаче.

Peer in LQRs

Значение этого поля копируется из последнего Save in LQRs на передаче. Если поле Peer in LQRs имеет нулевое значение, поля Last Out не определены, а поля Peer In содержат изначальные значения.

Peer in packets

Значение этого поля копируется из последнего Save in packets на передаче.

Peer in discards

Значение этого поля копируется из последнего Save in discards на передаче.

Peer in errors

Значение этого поля копируется из последнего Save in errors на передаче.

Peer in octets

Значение этого поля копируется из последнего Save in octets на передаче.

Peer out LQRs

Значение этого поля копируется из Out LQRs на передаче. Это число должно включать LQR.

Peer out packets

Значение этого поля копируется из текущего MIB ifOutUniPackets и ifOutNUniPackets на передаче. Это число должно включать LQR.

Peer out octets

Значение этого поля копируется из текущего MIB ifOutOctets на передаче. Это число должно включать LQR.

Перечисленные ниже поля реально не передаются через входящий канал. Вместо этого они логически присоединяются к пакету процессом Rx.

Save in LQRs

Значение этого поля копируется из In LQRs на приеме. Это число должно включать LQR.

Save in packets

Значение этого поля копируется из текущего MIB ifInUniPackets и ifInNUniPackets на приеме. Это число должно включать LQR.

Save in discards

Значение этого поля копируется из ifInDiscards на приеме. Это число должно включать LQR.

Save in errors

Значение этого поля копируется из ifInErrors на приеме. Это число должно включать LQR.

Save in octets

Значение этого поля копируется из InGoodOctets на приеме. Это число должно включать LQR.

PAP

RFC 1334 <http://www.ietf.org/rfc/rfc1334.txt>

Протокол PAP (Password Authentication Protocol - аутентификация по паролю) обеспечивает узлам одного уровня простой способ идентификации друг друга путем двухстороннего согласования (handshake).

Пакеты PAP инкапсулируются в информационное поле кадров канального уровня PPP с полем протокола с023. Структура пакетов PAP показана на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов PAP

Код

Однооктетное поле, определяющее тип пакета PAP.

- 1 Authenticate-Request
- 2 Authenticate-Ack
- 3 Authenticate-Nak

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета PAP.

Данные

Формат поля данных определяется значением кода. Поле данных пакетов PAP может иметь нулевой размер.

Формат запросов аутентификации (Authenticate-Request) показан на рисунке.

Размер Peer-ID	Peer-ID	Размер пароля	Пароль
1 байт	Переменный размер	1 байт	Переменный размер

Структура запросов аутентификации (Authenticate-Request)

Размер Peer-ID

Размер поля Peer-ID в октетах.

Peer-ID

Указывает имя узла для аутентификации.

Размер пароля

Указывает размер пароля в октетах.

Пароль

Содержит пароль, используемый для аутентификации.

Формат пакетов Authenticate -Ack и Authenticate-Nak показан на следующем рисунке.



Структура пакетов Authenticate -Ack и Authenticate-Nak

Размер сообщения

Размер поля Сообщение.

Сообщение

Содержание сообщения зависит от реализации.

ATCP

RFC 1378 <http://www.ietf.org/rfc/rfc1378.txt>

Протокол ATCP (AppleTalk Control Protocol) отвечает за настройку параметров AppleTalk на обеих сторонах соединения "точка-точка". ATCP использует такой же механизм обмена пакетами, как в протоколе управления каналом LCP. Обмен ATCP-пакетами невозможен до тех пор, пока PPP не достигнет фазы протокола сетевого уровня. Полученные до этого момента пакеты ATCP отбрасываются.

Формат заголовка пакетов ATCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов ATCP

Код

Однобайтное поле, определяющее тип пакета ATCP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета ATCP.

Данные

Поле данных переменной длины может содержать конфигурационные опции. Длина этого поля может быть равна 0. Формат конфигурационных опций ATCP показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Конфигурационные опции ATCP

Тип

Однobaйтовый идентификатор типа конфигурационных опций, который может принимать следующие значения:

- 1 AppleTalk-Address
- 2 Routing-Protocol
- 3 Suppress-Broadcasts
- 4 AT-Compression Protocol
- 6 Server-Information
- 7 Zone-Information
- 8 Default-Router Address

Размер

Размер всех полей конфигурационных опций (тип, размер, данные).

Данные

Значение поля данных.

ВАСР

RFC 2125 <http://www.ietf.org/rfc/rfc2125.txt>

Протокол управления полосой ВАСР (Bandwidth Allocation Control Protocol) связан с протоколом ВАР, который можно использовать для управления мультиканальными потоками на основе множества физических соединений. ВАР определяет дейтаграммы, используемые для добавления и удаления отдельных каналов, а также для определения стороны, отвечающей за принятие решений о полосе для мультиканального потока. Протокол ВАСР определяет параметры управления протоколом ВАР.

Формат пакетов ВАСР показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов ВАСР

Код

Однооктетное поле, определяющее тип пакета ВАСР.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета ВАСР.

Данные

Поле данных переменной длины может содержать конфигурационные опции. Длина этого поля может быть равна 0. Формат конфигурационных опций ВАСР показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Конфигурационные опции ВАСР

Тип

Однобайтовый идентификатор типа конфигурационных опций, который может принимать следующие значения:

- 1 Favored-Peer

Размер

Размер всех полей конфигурационных опций (тип, размер, данные).

Данные

Значение поля данных.

BCP

RFC 1638 <http://www.ietf.org/rfc/rfc1638.txt>

Протокол управления мостами BCP (Bridge Control Protocol) отвечает за настройку конфигурационных параметров протокола мостов на обеих сторонах соединения "точка-точка". BCP использует такой же механизм обмена пакетами, как в протоколе управления каналом LCP. Обмен BCP-пакетами невозможен до тех пор, пока PPP не достигнет фазы протокола сетевого уровня. Полученные до этого момента пакеты BCP отбрасываются.

Формат пакетов BCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов BCP

Код

Однобайтное поле, определяющее тип пакета BCP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета BCP.

Данные

Поле данных переменной длины может содержать конфигурационные опции. Длина этого поля может быть равна 0. Формат конфигурационных опций BCP показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Конфигурационные опции BCP

Тип

Однobaйтoвый идентификатор типа конфигурационных опций, который может принимать следующие значения:

- 1 Bridge-Identification
- 2 Line-Identification
- 3 MAC-Support
- 4 Tinygram-Compression
- 5 LAN-Identification
- 6 MAC-Address
- 7 Spanning-Tree-Protocol

Размер

Размер всех полей конфигурационных опций (тип, размер, данные).

Данные

Значение поля данных.

BVCP

RFC 1763 <http://www.ietf.org/rfc/rfc1763.txt>

Протокол BVCP (PPP Banyan VINES Control Protocol) отвечает за настройку, разрешение и запрещение протокольных модулей VINES на обеих сторонах соединения "точка-точка". BVCP использует такой же механизм обмена пакетами, как в протоколе управления каналом LCP.

Формат пакетов BVCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов BVCP

Код

Однооктетное поле, определяющее тип пакета BVCP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета BVCP.

Данные

Поле данных переменной длины может содержать конфигурационные опции. Длина этого поля может быть равна 0. Формат конфигурационных опций BVCP показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Конфигурационные опции BVCP

Тип

Однобайтовый идентификатор типа конфигурационных опций, который может принимать следующие значения:

- 1 BV-NS-RTP-Link-Type
- 2 BV-FRP (протокол фрагментации)
- 3 BV-RTP
- 4 BV-Suppress-Broadcast

Размер

Размер всех полей конфигурационных опций (тип, размер, данные).

Данные

Значение поля данных.

CCP

RFC 1962 <http://www.ietf.org/rfc/rfc1962.txt>

Протокол управления компрессией CCP (Compression Control Protocol) отвечает за настройку алгоритма компрессии данных на обеих сторонах канала "точка-точка". Этот протокол используется также для сигнализации о сбоях при компрессии или декомпрессии. CCP использует такой же механизм обмена пакетами, как в протоколе управления каналом LCP. Обмен CCP - пакетами невозможен до тех пор, пока PPP не достигнет фазы протокола сетевого уровня. Полученные до этого момента пакеты CCP отбрасываются.

Формат пакетов CCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов CCP

Код

Однооктетное поле, определяющее тип пакета CCP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета CCP.

Данные

Поле данных переменной длины может содержать конфигурационные опции. Длина этого поля может быть равна 0. Формат конфигурационных опций CCP показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Конфигурационные опции BVCP

Тип

Однобайтовый идентификатор типа конфигурационных опций, который может принимать следующие значения:

- 0 OUI
- 1 Predictor Type 1
- 2 Predictor Type 2
- 3 Puddle Jumper
- 16 Hewlett-Packard-PPC
- 17 Stac Electronics LZS
- 18 Microsoft PPC
- 19 Gandalf FZA
- 20 V.42bis Compression
- 21 BSD LZW Compression
- 23 LZS-DCP

Размер

Размер всех полей конфигурационных опций (тип, размер, данные).

Данные

Значение поля данных.

DNCP

RFC 1376 <http://www.ietf.org/rfc/rfc1376.txt>

Протокол управления PPP DECnet Phase IV отвечает за организацию и настройку протокола маршрутизации DNA Phase IV через PPP. Этот протокол применим только к сообщениям маршрутизации Digital DNA Phase IV и не может использоваться с другими протоколами DNA Phase IV (MOP, LAT и т.д.).

Формат пакетов DNCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов DNCP

Код

Однооктетное поле, определяющее тип пакета DNCP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета DNCP.

Данные

Поле данных пакетов DNCP не содержит конфигурационных опций. Длина этого поля может быть равна 0.

ECP

RFC 1968 <http://www.ietf.org/rfc/rfc1968.txt>

Протокол управления шифрованием (Encryption Control Protocol или ECP) отвечает за настройку и разрешение алгоритма шифрования данных на обеих сторонах канала "точка-точка". ECP использует такой же механизм обмена пакетами, как протокол LCP (Link Control Protocol). Обмен ECP-пакетами невозможен до тех пор, пока PPP не достигнет фазы протокола сетевого уровня. Полученные до этого момента пакеты ECP отбрасываются.

Формат заголовка пакетов ECP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов ECP

Код

Однооктетное поле, определяющее тип пакета ECP. В случае приема пакета с неизвестным значением кода генерируется пакет Code-Reject.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject
- 14 Reset-Request
- 15 Reset-Ack

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик

Размер

Размер всех полей пакета ECP.

IPv6CP

RFC 2023 <http://www.ietf.org/rfc/rfc2023.txt>

Протокол управления PPP IPv6CP отвечает за настройку, разрешение и запрещение протокольных модулей IPv6 на обеих сторонах соединений "точка-точка".

Формат пакетов IPv6CP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов IPv6CP

Код

Однооктетное поле, определяющее тип пакета IPv6CP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик

Размер

Размер всех полей пакета IPv6CP.

Данные

Поле данных переменной длины может содержать конфигурационные опции. Длина этого поля может быть равна 0. Формат конфигурационных опций IPv6CP показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Конфигурационные опции IPv6CP

Тип

Однобайтовый идентификатор типа конфигурационных опций, который может принимать следующие значения:

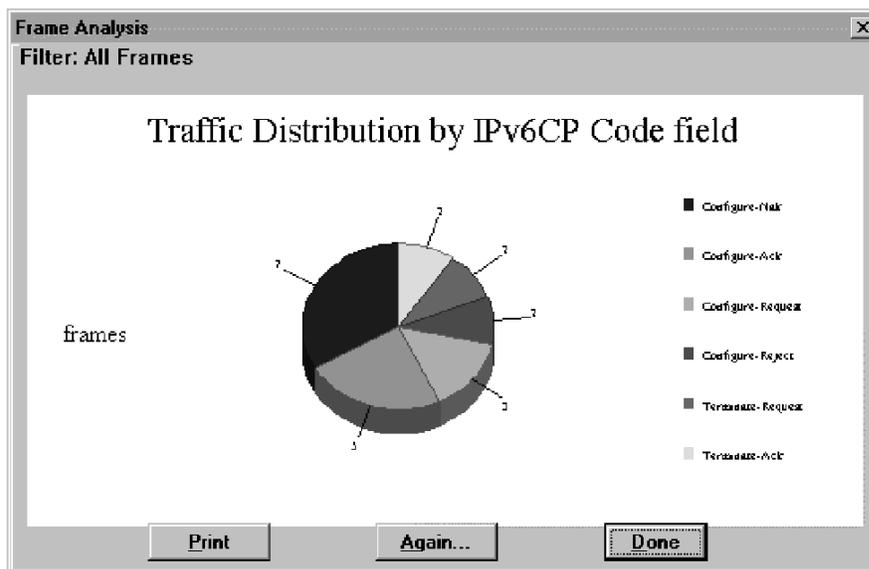
- 1 Interface Token
- 2 IPv6-Compression-Protocol

Размер

Размер всех полей конфигурационных опций (тип, размер, данные).

Данные

Значение поля данных.



Распределение трафика по кодам IPv6CP

IPCP

RFC 1332 <http://www.ietf.org/rfc/rfc1332.txt>

Протокол управления IP (IP Control Protocol или IPCP) отвечает за настройку протокольных параметров IP на обеих сторонах соединений "точка-точка".

Формат пакетов IPCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов IPCP

Код

Однооктетное поле, определяющее тип пакета IPCP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик

Размер

Размер всех полей пакета IPCP.

Данные

Поле данных переменной длины может содержать конфигурационные опции. Длина этого поля может быть равна 0. Формат конфигурационных опций IPCP показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Конфигурационные опции IPCP

Тип

Однобайтовый идентификатор типа конфигурационных опций, который может принимать следующие значения:

- 1 IP Address (использование этого кода не рекомендуется, лучше использовать код 3)
- 2 IP Compression Protocol
- 3 IP Address (способ согласования IP-адреса, который будет использоваться на локальной стороне канала).

Размер

Размер всех полей конфигурационных опций (тип, размер, данные).

Данные

Значение поля данных.

IPXCP

RFC 1552 <http://www.ietf.org/rfc/rfc1552.txt>

Для организации связи по каналу "точка-точка" каждая из сторон соединения PPP должна сначала передать пакеты LCP для настройки и тестирования канала данных. После организации канала и согласования дополнительных параметров, требуемых протоколом LCP, протокол PPP может передавать пакеты для выбора и настройки протокола сетевого уровня IPX. После того, как протокол IPXCP достигнет открытого состояния (Opened state), дейтаграммы IPX можно будет передавать через канал.

Формат пакетов IPXCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов IPXCP

Код

Однооктетное поле, определяющее тип пакета IPXCP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета IPXCP.

Данные

Поле данных переменной длины может содержать конфигурационные опции. Длина этого поля может быть равна 0. Формат конфигурационных опций IPXCP показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Конфигурационные опции IPXCP

Тип

Однобайтовый идентификатор типа конфигурационных опций, который может принимать следующие значения:

- 1 IPX Network number
- 2 IPX Node number
- 3 IPX Compression Protocol
- 1 IPX Routing Protocol
- 2 IPX Router name
- 3 IPX Configuration complete.

Размер

Размер всех полей конфигурационных опций (тип, размер, данные).

Данные

Значение поля данных.

LEXCP

RFC 1841 <http://www.ietf.org/rfc/rfc1841.txt>

Интерфейсные модули расширения ЛВС представляют собой устройства, установленные на удаленных сайтах (дома или в филиалах) и подключенные к маршрутизатору центрального сайта через WAN-каналы. Для поддержки такой архитектуры были разработаны протокол PPP NCP (Network Control Protocol - протокол управления сетью) и протокол PPP-LEX (LAN extension interface protocol). Основными функциями протокола LEX является инкапсуляция пакетов управления интерфейсом расширения ЛВС и пакетов данных. Последовательно передаваемые пакеты могут содержать данные или управляющую информацию. Пакеты данных описываются протоколом LEX.

Существует два типа пакетов LEXCP:

- пакеты стартовых опций;
- пакеты опций удаленных команд.

Пакет стартовых опций является первым пакетом LEX NCP, который интерфейсный модуль расширения ЛВС посылает центральному маршрутизатору после того, как LCP достигнет открытого состояния. Этот обязательный пакет настраивает протокол для интерфейса расширения ЛВС и переводит в открытое состояние LEX NCP.

Формат пакетов LEXCP показан на рисунке.

Адрес	Управление	Тип протокола
Код	Идентификатор	Размер
Опции		
1 байт	1 байт	2 байта

Заголовок протокола PPP + LEX

Тип опции	Размер опции	Данные
1 байт	1 байт	2 байта

Стартовые опции LEX

Тип опции	Флаги опции	Размер опции	Данные
1 байт	1 байт	2 байта	

Опции удаленных команд LEX

Адрес

Адрес всех станций - однооктетное поле, содержащее двоичную последовательность 11111111 (0xFF). Протокол PPP не использует для станций индивидуальных адресов. Адрес всех станций (широковещательный) должен распознаваться и приниматься всеми станциями.

Управление

Команда нумерованной информации (UI) с нулевым значением бита P/F - однооктетное поле, содержащее специфическое для PPP значение 00000011 (0x03).

Тип протокола

Выделенное IETF значение идентификатора протокола. Для пакетов управления значение этого поля составляет 0x8041.

Код

Идентифицирует тип пакета LLC, передаваемого интерфейсом расширения ЛВС. Корректные значения идентификаторов перечислены ниже:

Стартовые опции:

- 0x01 Configure-Request
- 0x02 Configure-Ack
- 0x03 Configure-Nak
- 0x04 Configure-Rej

Опции удаленных команд:

- 0x40 LEX_RCMD_REQUEST
- 0x41 LEX_RCMD_ACK
- 0x42 LEX_RCMD_NAK
- 0x43 LEX_RCMD_REJ

Идентификатор

Случайное число, позволяющее идентифицировать запрос или отклик. Рекомендуется использовать для идентификатора ненулевые значения. В будущих версиях 0 может использоваться для обозначения незапрошенных сообщений от интерфейса расширения ЛВС. Допустимые значения этого поля лежат в диапазоне от 0x01 до 0xFF.

Размер

Размер пакета в октетах с учетом полей Код, Идентификатор, Размер и Опции.

Тип опции

Идентифицирует стартовую опцию или опцию удаленной команды. Возможные значения идентификаторов перечислены ниже.

Стартовые опции:

0x01 MAC Type
0x03 MAC Address
0x05 LAN Extension

Опции удаленных команд:

0x01 Filter Protocol Type
0x02 Filter MAC Address
0x03 Set priority
0x04 Disable LAN Extension Ethernet Interface
0x05 Enable LAN Extension Ethernet Interface
0x06 Reboot LAN Extension Ethernet Unit
0x07 Request Statistics
0x08 Download Request
0x09 Download Data
0x0A Download Status
0x0B Inventory Request

Размер опции

Задаёт размер поля опций (тип, данные, размер, флаги для опций удаленных команд).

Данные

Данные, относящиеся к значению, указанному в поле типа опции. Ниже приведены варианты данных для стартовых опций.

<i>Тип опции</i>	<i>Данные</i>
0x01 MAC Type	Современное значение типа MAC (в настоящее время 0x001 для IEEE 802.3/Ethernet с канонической адресацией).
0x03 MAC Address	Актуальный MAC-адрес в каноническом формате IEEE 802.3
0x05 LAN Extension	Программная информация об интерфейсе расширения ЛВС. В настоящее время - 0x01.

Флаги опции

Задают опции удаленной команды, указывая конкретные действия, которые нужно выполнить (используется только в пакетах опций удаленных команд).

NBFCP

RFC 2097 <http://www.ietf.org/rfc/rfc2097.txt>

Протокол NBFCP (PPP NetBIOS Frames Control Protocol - протокол управления кадрами NetBIOS) отвечает за организацию и настройку протокола NBF для соединений PPP. Протокол применим только для оконечных систем, подключенных к системам того же ранга или локальным сетям.

Формат кадров NBFCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов NBFCP

Код

Однооктетное поле, определяющее тип пакета NBFCP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета NBFCP.

Данные

Поле данных переменной длины может содержать конфигурационные опции. Длина этого поля может быть равна 0. Формат конфигурационных опций NBFCP показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Конфигурационные опции NBFCP

Тип

Однобайтовый идентификатор типа конфигурационных опций, который может принимать следующие значения:

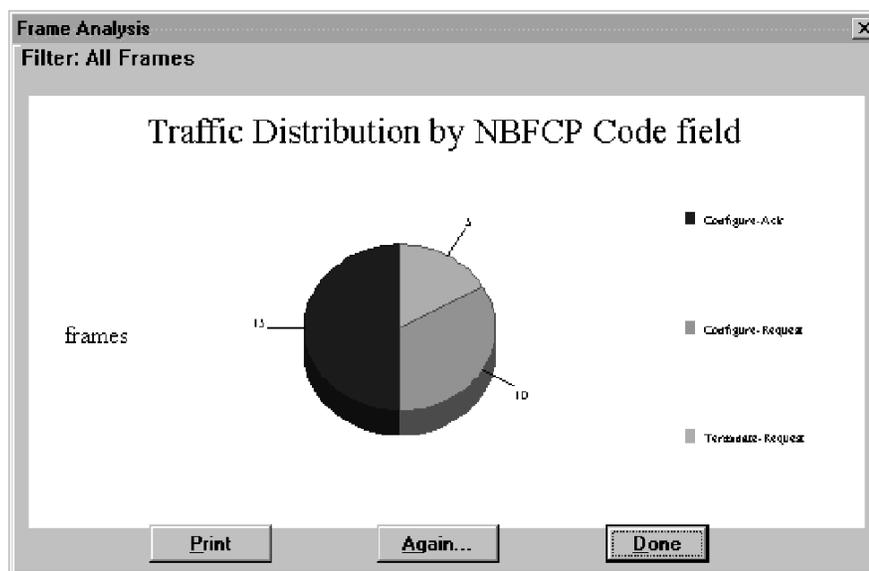
- 1 Name-Protection.
- 2 Peer-Information.
- 3 Multicast-Filtering.
- 4 IEEE-MAC-Address-Required.

Размер

Размер всех полей конфигурационных опций (тип, размер, данные).

Данные

Значение поля данных.



Распределение трафика по кодам NBFCEP

OSINLCP

RFC 1377 <http://www.ietf.org/rfc/rfc1377.txt>

Протокол OSINLCP (OSI Network Layer Control Protocol - протокол управления сетевого уровня OSI) отвечает за настройку, разрешение и запрещение протокольных модулей OSI на обеих сторонах соединений "точка-точка". OSINLCP использует такой же механизм обмена пакетами, как протокол LCP (Link Control Protocol). Обмен OSINLCP-пакетами невозможен до тех пор, пока PPP не достигнет фазы протокола сетевого уровня.

Формат кадров OSINLCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов OSINLCP

Код

Однооктетное поле, определяющее тип пакета OSINLCP. При получении пакетов с неизвестным кодом передается пакет Code Reject.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета OSINLCP.

Данные

Поле данных переменной длины может содержать конфигурационные опции.

SDCP

RFC 1963 <http://www.ietf.org/rfc/rfc1963.txt>

Протокол SDCP (PPP Serial Data Control Protocol - протокол управления последовательной передачей) отвечает за настройку, разрешение и запрещение протокола SDTP (Serial Data Transport Protocol) последовательный транспортный протокол) на обеих сторонах соединений "точка-точка". OSINLCP использует такой же механизм обмена пакетами, как протокол LCP (Link Control Protocol). Обмен SDCP-пакетами невозможен до тех пор, пока PPP не достигнет фазы протокола сетевого уровня.

Формат кадров OSINLCP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов SDCP

Код

Однооктетное поле, определяющее тип пакета SDCP. При получении пакетов с неизвестным кодом передается пакет Code Reject.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета SDCP.

Данные

Поле данных переменной длины может содержать конфигурационные опции. Формат конфигурационных опций SDCP показан на рисунке.

Тип	Размер	Данные
-----	--------	--------

Конфигурационные опции SDCP

Тип

Однобайтовый идентификатор типа конфигурационных опций, который может принимать следующие значения:

- 1 Packet-Format.
- 2 Header-Type.
- 3 Length-Field-Present.
- 4 Multi-Port.
- 5 Transport-Mode.
- 6 Maximum-Frame-Size.
- 7 Allow-Add-Frames.
- 8 FCS-Type.
- 9 Flow-Expiration-Time.

Размер

Размер всех полей конфигурационных опций (тип, размер, данные).

Данные

Значение поля данных.

SNACP

RFC 2043 <http://www.ietf.org/rfc/rfc2043.txt>

Протокол SNACP (SNA PPP Control Protocol - протокол управления SNA) отвечает за настройку, разрешение и запрещение протокола на обеих сторонах соединений "точка-точка". Отметим, что реально существует два протокола управления SNA - один протокол для LLC 802.2 и другой - для SNA без LLC 802.2. Эти протоколы согласуются независимо один от другого. Для организации соединения через канал "точка-точка" каждая из сторон канала PPP должна сначала передать пакеты LCP для организации и проверки соединения. После организации соединения и согласования его параметров в соответствии с требованиями LCP протокол PPP может передавать пакеты SNACP для выбора и настройки протокола сетевого уровня SNA. После того, как SNACP достигнет открытого состояния, через канал можно будет передавать дейтаграммы SNA.

Формат пакетов SNACP показан на рисунке.

Код	Идентификатор	Размер	Данные
1 байт	1 байт	2 байта	Переменный размер

Структура пакетов SNACP

Код

Однооктетное поле, определяющее тип пакета SNACP.

- 1 Configure-Request
- 2 Configure-Ack
- 3 Configure-Nak
- 4 Configure-Reject
- 5 Terminate-Request
- 6 Terminate-Ack
- 7 Code-Reject

Идентификатор

Десятичное значение, идентифицирующее соответствующий запрос или отклик.

Размер

Размер всех полей пакета SNACP.

Данные

Значение поля данных.