

Требования к сквозной эмуляции псевдопровода (PWE3)

Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)

Статус документа

Этот документ содержит информацию, предназначенную для сообщества Internet. В документе не содержится спецификаций каких-либо стандартов Internet. Документ можно распространять свободно.

Авторские права

Copyright (C) The Internet Society (2004).

Аннотация

В это документе описываются базовые требования для PWE3¹, разработанные группой PWE3 WG. Документ включает рекомендации для других рабочих групп, занимающихся определением механизмов эмуляции псевдопроводов для сетей Ethernet, ATM и Frame Relay. Требования к эмуляции псевдопроводов для (синхронных битовых потоков, определенный в спецификации ITU G.702) рассматриваются в отдельном документе². Следует отметить, что рабочая группа PWE3 занимается стандартизацией механизмов, которые могут использоваться для обеспечения сервиса PWE3, но не сервисом, как таковым.

Оглавление

1. Введение.....	2
1.1. Что такое псевдопровод?.....	2
1.2. Современная архитектура сетей.....	2
1.2.1. Множество разнотипных сетей.....	2
1.2.2. Переход к оптимизированным для передачи пакетов сетям.....	2
1.3. PWE3 как путь сближения.....	2
1.4. Приложения, подходящие для PWE3.....	2
1.5. Резюме.....	3
2. Терминология.....	3
3. Эталонная модель PWE3.....	3
4. Обработка пакетов.....	4
4.1. Инкапсуляция.....	4
4.1.1. Передача требуемой информации из заголовков канального уровня.....	4
4.1.2. Поддержка переменного размера PDU.....	4
4.1.3. Поддержка мультиплексирования и демультимплексирования.....	4
4.1.4. Проверка корректности PW-PDU.....	4
4.1.5. Доставка информации о типе данных.....	4
4.2. Порядок доставки кадров.....	4
4.3. Дублирование кадров.....	4
4.4. Фрагментация.....	4
4.5. Объединение PDU для снижения объема служебного трафика.....	5
5. Обслуживание эмулируемого сервиса.....	5
5.1. Организация и разрыв псевдопроводных соединений.....	5
5.2. Обработка управляющих сообщений исходного сервиса.....	5
5.3. Инициированные PE управляющие сообщения.....	5
6. Управление эмулируемыми службами.....	6
6.1. Базы MIB.....	6
6.2. Общие требования к MIB.....	6
6.3. Настройка и обслуживание.....	6
6.4. Мониторинг производительности.....	6
6.5. Контроль отказов и уведомления о них.....	6
6.6. Проверка и трассировка псевдопроводных соединений.....	7
7. Недостатки эмулируемых служб.....	7
7.1. Характеристики эмулируемого сервиса.....	7
7.2. Качество обслуживания для эмулируемого сервиса.....	7
8. Что не относится к числу требований.....	7
9. Качество обслуживания (QoS).....	7
10. Вопросы междоменного взаимодействия.....	8

¹Pseudo-Wire Emulation Edge to Edge - эмуляция сквозного псевдопровода.

²RFC 4197.

11. Вопросы безопасности.....	8
12. Благодарности.....	8
13. Литература.....	8
13.1. Нормативные документы.....	8
13.2. Ссылки.....	8
14. Адреса авторов.....	9
15. Полное заявление авторских прав.....	9

1. Введение

1.1. Что такое псевдопровод?

Эмуляция сквозного псевдопровода (PWE3) представляет собой механизм эмуляции существенных атрибутов различных типов сетевого сервиса (ATM, Frame Relay или Ethernet) через сети с коммутацией пакетов (PSN¹). Обязательные функции псевдопровода PW включают инкапсуляцию обусловленных типом сервиса PDU², получаемых входным портом и передачу их через путь или туннель с обеспечением синхронизации, порядка доставки и иных операций, требуемых для эмуляции поведения и характеристик сервиса с максимально возможной полнотой.

С точки зрения пользователя PW представляется как выделенное соединение или устройство выбранного типа сервиса. Однако эмуляции присущ ряд существенных ограничений, осложняющих использование PW для некоторых приложений. Такие ограничения должны быть подробно описаны в документации сервиса и заявлениях о применимости (Applicability Statement).

1.2. Современная архитектура сетей

В следующих параграфах кратко рассмотрены основы современных сетей и тенденции их изменения. Приведена также мотивация конвергенции сетей с продолжением поддержки существующих типов сервиса. И, наконец, рассматриваются варианты использования PW в этом контексте.

1.2.1. Множество разнотипных сетей

У любого, предоставляющего различные типы услуг сервис-провайдера, сетевая инфраструктура обычно включает "параллельные" или перекрывающиеся сети. Каждая из таких сетей поддерживает свой тип сервиса (например, Frame Relay, доступ в Internet и т. п.). Такое решение ведет к увеличению расходов как на приобретение оборудования, так и на его обслуживание. Кроме того, наличие множества разнотипных сетей усложняет планирование и управление. У сервис-провайдеров возникают естественные вопросы:

- Какую из сетей следует развивать?
- Какое количество оптических волокон требуется для каждой сети?
- Как эффективно управлять многочисленными сетями?

Конвергенция поможет сервис-провайдерам ответить на все эти вопросы и обеспечить согласованное и экономичное развитие сети.

1.2.2. Переход к оптимизированным для передачи пакетов сетям

Для повышения эффективности инвестиций и снижения эксплуатационных расходов сервис-провайдеры зачастую стараются использовать одну сетевую технологию для доставки различных типов сервиса.

Поскольку пакетный трафик занимает все большую часть доступной полосы сетей, растет целесообразность перевода сетей общего пользования на протоколы IP. Однако многие сервис-провайдеры сталкиваются с проблемами при развертывании оптимизированных для передачи пакетов сетей. Хотя трафик Internet и является наиболее быстро расширяющимся по объёму, на сегодняшний день он не является преобладающим. Например, трафик Frame Relay по-прежнему имеет суммарный объем, превышающий объем естественного трафика IP. А частные каналы TDM обеспечивают трафик, который по своему уровню превосходит трафик Frame Relay. Кроме того, в сетях общего пользования имеется огромное количество старого оборудования, которое не способно работать по протоколу IP. Сервис-провайдеры продолжают использовать не поддерживающее IP оборудование для различных типов сервиса и возникает необходимость сопряжения такого оборудования с оптимизированными для передачи трафика IP сетями.

1.3. PWE3 как путь сближения

Как сервис-провайдеры могут реализовать свои преимущества в новых инфраструктурах, оптимизированных для передачи пакетов, и продолжить использование установленного оборудования с сохранением трафика, передаваемого через это оборудование? Как они могут перейти от сетей Frame Relay или ATM, не нарушая работу существующих типов сервиса?

Одним из вариантов является эмуляция устройств или служб с использованием псевдопроводов (PW). Эмуляция устройств в сетях ATM и взаимодействие между сетями Frame Relay и ATM уже стандартизованы. Эмуляция позволяет передавать трафик существующих типов сервиса через новую инфраструктуру и, таким образом, обеспечивает возможность взаимодействия разнородных сетей.

При корректной реализации PWE3 может обеспечить возможность поддержки традиционного сервиса в новых сетях.

1.4. Приложения, подходящие для PWE3

Что делает приложение подходящим (или неподходящим) для использования с PWE3? При рассмотрении PW как основы для реализации приложений следует получить ответы на приведенные ниже вопросы:

- Достаточно ли широко распространено данное приложение?

¹Packet Switched Network.

²PDU - Protocols Data Unit - модуль данных протокола. *Прим. перев.*

передаются через PW удаленному PE, где восстанавливаются естественные для данного сервиса кадры и передаются в устройство CE. Детальное описание архитектуры PWE3 приведено в документе [PWE3_ARCH].

В этом документе не используется допущений о природе PW (например, сессия [L2TPv3], [MPLS] LSP) или PSN (например, IP или MPLS). Вместо этого описываются базовые требования, которые применимы ко всем типам PW и PSN для всех эмулируемых служб, включая Ethernet, ATM, Frame Relay и т. д.

4. Обработка пакетов

В этой главе описаны требования PWE3 в части данных.

4.1. Инкапсуляция

Каждое устройство PE **должно** обеспечивать механизм инкапсуляции PDU от AC. Следует отметить, что инкапсулируемые PDU могут включать или не включать заголовки канального уровня (L2) - это зависит от типа сервиса. Каждый сервис PWE3 **должен** указывать что собой представляет PDU.

Заголовок PW PDU содержит все поля, которые используются на выходе PW для определения механизмов обработки PDU. Заголовок туннеля PSN не рассматривается как часть заголовка PW.

Конкретные требования к инкапсуляции PDU рассматриваются ниже.

4.1.1. Передача требуемой информации из заголовков канального уровня

На выходной стороне PW требуется некая информация (например, тип естественного сервиса, к которому относятся PW PDU, а в некоторых случаях информация из заголовка L2) для определения способа обработки принятых PDU. Механизм инкапсуляции PWE3 **должен** обеспечивать тот или иной способ передачи такой информации со входной стороны PW на выходную. Следует отметить, что вся информация этого типа должна содержаться в PW-заголовке PW PDU. Часть информации (например, тип сервиса для PW) может сохраняться на выходной стороне как состояние в процессе организации PW.

4.1.2. Поддержка переменного размера PDU

Реализации PWE3 **должны** поддерживать PDU переменной длины, если такие PDU поддерживаются исходным сервисом. Например, от PWE3 для Frame Relay **требуется** поддержка переменного размера кадров.

4.1.3. Поддержка мультиплексирования и демultipлексирования

Если исходный сервис может группировать множество устройств (соединений) в "транк" (например, объединение ATM VCC в VPC или поддержка на одном порту множества интерфейсов Ethernet 802.1Q), **следует** обеспечивать какие-либо механизмы, позволяющие использовать один PW для соединения двух транковых устройств. С точки зрения инкапсуляции **должна** передаваться информация, достаточная для того, чтобы PW на приемной стороне мог демultipлексировать отдельные устройства (соединения).

4.1.4. Проверка корректности PW-PDU

Большинство кадров L2 имеют поле контрольной суммы для проверки целостности кадра. Каждый сервис PWE3 **должен** указывать требуется ли сохранение контрольных сумм кадров при передаче через PW или контрольные суммы могут исключаться на входном PE и заново рассчитываться на выходном PE. Для протоколов типа ATM и FR контрольные суммы включают данные канального уровня (идентификаторы устройств - FR DLCI или ATM VPI/VCI). Следовательно, такие контрольные суммы **должны** исключаться на входном PE и заново рассчитываться на выходе.

4.1.5. Доставка информации о типе данных

В некоторых случаях желательно отличать трафик PW от других типов трафика (например, IPv4, IPv6 или OAM). В частности, при использовании ECMP¹ в сети PSN такое различие может использоваться для снижения вероятности нарушения порядка доставки пакетов PW при использовании механизмов распределения нагрузки. При необходимости **следует** обеспечивать какой-либо механизм поддержки таких различий. Такие механизмы **могут** определены рабочей группой PWE3 или другими группами.

4.2. Порядок доставки кадров

Когда пакеты, содержащие PW PDU проходят через PW, порядок их доставки может нарушаться. Для некоторых типов сервиса требуется сохранение порядка доставки кадров (это может относиться только к кадрам управления или ко всем кадрам). В таких случаях **должен** обеспечиваться тот или иной механизм обеспечения упорядоченной доставки. Одним из вариантов решения этой задачи может служить включение порядковых номеров в заголовки PW, что позволит детектировать нарушение порядка на приемной стороне. Механизм восстановления нарушенного порядка может обеспечиваться NSP-обработкой² [PWE3_ARCH], но этот вопрос выходит за рамки PWE3.

4.3. Дублирование кадров

В редких случаях пакеты при прохождении через PW могут дублироваться. Для некоторых типов сервиса дублирование кадров недопустимо. В таких случаях **должен** обеспечиваться механизм предотвращения доставки дубликатов. Этот механизм может быть самостоятельным или служить частью механизма обеспечения корректного порядка доставки.

4.4. Фрагментация

Если суммарный размер данных L2 и связанных с ними заголовков PWE3 и PSN превосходит значение MTU на пути через PSN, может возникнуть необходимость фрагментации данных L2 (в противном случае кадр L2 может быть

¹Equal Cost Multi-Path - множество равноценных путей.

²Native Service Processing - естественная обработка для сервиса.

отброшен на пути). Для некоторых типов сервиса фрагментация может потребоваться также для сохранения относительной позиции управляющего кадра среди кадров данных (например, относительное положение ячеек ATM PM). В общем случае фрагментация оказывает влияние на производительность и, следовательно, фрагментации следует избегать по возможности. Однако для отдельных типов сервиса требования фрагментации могут быть иными. Для случаев, когда фрагментация необходима, документ PWE3 для соответствующего типа сервиса **должен** указывать следует ли отбрасывать кадр или фрагментировать его. Если эмулируемый сервис выбирает для кадра отбрасывание, это **должно** быть указано в заявлении о применимости.

4.5. Объединение PDU для снижения объема служебного трафика

Когда размер L2 PDU мал, для снижения загрузки туннеля PSN **можно** объединять множество PDU перед тем, как в пакет будет добавлен заголовок туннеля PSN. Каждый инкапсулированный PDU по-прежнему содержит свой заголовок PW, поэтому PE на выходе знает как обрабатывать данные. Однако при объединении PDU следует принимать во внимание рост задержек и их флуктуаций (jitter), а также влияние потери пакетов.

5. Обслуживание эмулируемого сервиса

В этой главе рассматриваются требования по обслуживанию PWE3.

5.1. Организация и разрыв псевдопроводных соединений

Псевдопроводное соединение PW должно быть организовано до того, как будет использоваться эмулируемое устройство, и должно разрываться после того, как необходимость использования эмулируемого устройства отпадет. Организация и разрыв PW могут инициироваться командами из системы управления PE, командами Setup/Tearardown со стороны AC (например, ATM SVC) или с помощью механизмов автоматического детектирования.

В каждой реализации PWE3 **должен** быть определен тот или иной механизм организации PW. В процессе установки соединения PE требуется обмен той или иной информацией (например, определение возможностей удаленной стороны). Механизм организации соединения **должен** обеспечивать устройствам PE способ обмена всей необходимой информацией. Например, обе конечные точки должны согласовать методы инкапсуляции PDU и поддержки упорядоченной доставки кадров. Выбор сигнального протокола и передаваемой информации зависит от типа сервиса. Каждая реализация PWE3 **должна** указывать это. Ручная настройка PW может рассматриваться как специальный случай организации соединений.

Если в естественных условиях устройство является двунаправленным, соответствующее эмулируемое устройство может сигнализировать о своей готовности к работе (состояние "Up") только в том случае, когда связанные с ним PW и туннель PSN работают в обоих направлениях.

5.2. Обработка управляющих сообщений исходного сервиса

Некоторые типы сервиса в естественной форме поддерживают те или иные механизмы, используемые для обслуживания (например, ATM OAM или FR LMI). Служебные сообщения этих механизмов могут передаваться в основной полосе (т. е, помещаться вместе с данными в одном AC) или по отдельному каналу (например, с использованием выделенного для управления устройства). Для таких служб все передаваемые в основной полосе управляющие сообщения **следует** также передавать в основной полосе так же, как данные, с использованием соответствующего PW на удаленное устройство CE. Иными словами, для передаваемых в основной полосе управляющих сообщений не требуется трансляции в устройствах PE. Кроме того, **может** оказаться желательным обеспечения максимальной надежности доставки управляющих сообщений. Механизмы обеспечения высокой надежности доставки не определяются рабочей группой PWE3.

Управляющие сообщения, передаваемые по отдельному каналу между CE и PE могут относиться к различным AC между данной парой CE PE. Эти сообщения должны обрабатываться на локальном PE, а в некоторых случаях и на удаленном PE. Если в естественной форме сервиса используются те или иные управляющие сообщения, передаваемые по отдельному каналу, соответствующий эмулируемый сервис **должен** указать способы обработки таких сообщений в устройствах PE. В общем случае такие сообщения транслируются в in-band-сообщения естественного сервиса или определяемые PWE управляющие сообщения для каждого AC, связанного с данным сообщением, типа out-of-band. Для примера предположим, что некоторые AC между CE и PE используют ATM VCC в VPC. При получении F4 AIS [UNI3.0] от CE устройством PE следует транслировать F4 AIS с F5 AIS и передать сообщение удаленному CE для каждого VCC. В качестве альтернативного варианта PE следует генерировать определяемое PWE управляющее сообщение (например, аннулирование метки) удаленному PE для каждого VCC. Когда удаленное устройство PE получает такое сообщение может потребоваться генерация управляющего сообщения для естественного сервиса и передача этого сообщения подключенному CE.

5.3. Иницированные PE управляющие сообщения

От PE при некоторых обстоятельствах может потребоваться генерация служебных сообщений, которые не были вызваны тем или иным естественным управляющим сообщением от CE. Такие обстоятельства обычно связаны с отказами - например, отказ PW в PSN или повреждение канала между CE и PE.

Причина, по которой от PE требуется генерация сообщений при возникновении отказов, обусловлена тем, что наличие PW между парой CE будет существенно снижать возможности CE в части обслуживания. Пример подобной ситуации показан на рисунке. Если два CE соединены напрямую проводами, естественный сервис (например, ATM) может использовать уведомления от нижележащего уровня (например, уровня физического канала) для обслуживания. Например, ATM PVC может передавать сигнал Down при повреждении физического канала. Рассмотрим теперь несколько иную ситуацию.

```

+-----+ Phy-link +-----+           +-----+ Phy-link +-----+
| CE1 |-----| PE1 |.....PW.....| PE2 |-----| CE2 |
+-----+           +-----+           +-----+           +-----+

```

Если происходит отказ в PW между PE1 и PE2, устройства CE1 и CE2 не будут получать уведомлений о повреждении физического канала. В результате этого они не смогут своевременно объявить об отказе в эмулируемом устройстве приложениям вышележащих уровней. Следовательно, при отказе PW устройствам PE1 и PE2 необходимо

инициировать передачу служебных сообщений, уведомляющих клиентский уровень CE1 и CE2, использующих данный PW как серверный уровень (в этом случае клиентским уровнем является эмулируемый сервис). Если происходит повреждение физического канала между PE1 и CE1, устройство PE1 должно инициировать передачу некоего служебного сообщения (или сообщений), которые будут уведомлять клиентский уровень CE2. Устройство PE2 также может быть вовлечено в процесс генерации служебных сообщений.

В редких случаях, когда в физическом соединении между CE возникает множество битовых ошибок, для физического соединения может декларироваться состояние Down с уведомлением клиентского уровня устройств CE. В псевдо-соединениях PW может происходить потеря пакетов, их повреждение или нарушение порядка доставки. Такие события могут рассматриваться как «обобщенные битовые ошибки¹» с декларированием для PW состояния Down и детектированием для PE необходимости генерации служебного сообщения, уведомляющего клиентский уровень CE.

В общем случае для каждого эмулируемого сервиса **должна** быть указана спецификация:

- условий, при которых требуется генерация служебных сообщений по инициативе PE;
- формата служебных сообщений;
- способов обработки служебных сообщений на удаленном PE.

Для детектирования состояний, в которых требуется генерация служебных сообщений (например, отказ PW), нужны механизмы мониторинга. Такие механизмы могут быть определены рабочей группой PWE3 или иными организациями.

Статус группы эмулируемых устройств может быть изменен в результате одного сетевого инцидента. Например, при отказе физического канала между CE и PE все эмулируемые устройства, работающие через этот канал тоже откажут. Желательно, чтобы одно сообщение использовалось для уведомления всей группы эмулируемых устройств, соединенных с одним удаленным PE. Метод PWE3 **может** обеспечивать тот или иной механизм уведомления об изменении состояния группы эмулируемых устройств. Одним из возможных вариантов является связывание каждого эмулируемого устройства с идентификатором группы (group ID) при организации PW для этого эмулируемого устройства. В служебном сообщении этот идентификатор группы может служить для указания на все эмулируемые устройства данной группы.

Если PE нужно генерировать и передавать служебное сообщение CE, устройство PE **должно** использовать служебное сообщение естественного сервиса. Это важно для сохранения прозрачности эмулируемых устройств с точки зрения CE.

Приведенные в этой главе требования согласованы с философией управления ITU-T для телекоммуникационных сетей [G805] (т. е., с концепцией уровень клиента/уровень сервера).

6. Управление эмулируемыми службами

Каждому методу PWE3 **следует** обеспечивать сетевым операторам те или иные механизмы для управления эмулируемым сервисом. Эти механизмы могут быть описаны ниже.

6.1. Базы MIB

Должны обеспечиваться базы SNMP MIB [SMIV2] для управления каждым эмулируемым устройством, а также псевдопроводом в целом. Эти базы MIB **следует** создавать с учетом приведенных ниже требований.

6.2. Общие требования к MIB

Новые базы MIB должны добавлять или расширять, когда это применимо, существующие таблицы, как определено в других, связанных с сервисом MIB для существующих типов сервиса таких, как MPLS или L2TP. Например, ifTable, как определено в Interface MIB [IFMIB] **должна** быть дополнена для поддержки учета пакетов, доставленных с нарушением порядка. Другим примером может служить расширение MPLS-TE-MIB [TEMIB] для эмуляции устройств через MPLS. Например, вместо того, чтобы переопределять tunnelTable для обеспечения устройствам PWE возможности использовать туннели MPLS, записи этой таблицы **должны** быть расширены для добавления связанных с PWE объектов. Еще одним примером может служить расширение IP Tunnel MIB [IPTUNMIB] таким способом, чтобы обеспечить связанную с PWE3 семантику при использовании отличного от MPLS транспорта для PSN. Такой подход упрощает естественное расширение объектов, определенных в существующих MIB с точки зрения управления, а также взаимодействие с существующими реализациями агентов управления.

Устройства подключения (AC) **должны** появляться как интерфейсы в таблице ifTable.

6.3. Настройка и обслуживание

Таблицы MIB **должны** быть разработаны с целью облегчения настройки конфигурации и обслуживания AC.

Базы MIB **должны** облегчать настройку и мониторинг AC внутри PSN.

6.4. Мониторинг производительности

Базы MIB **должны** собирать статистику производительности и данных об отказах.

Базы MIB **должны** содержать описание использования существующих счетчиков для эмуляции PW. Имеющиеся счетчики **не следует** заменять.

6.5. Контроль отказов и уведомления о них

В тех случаях, когда это применимо, **следует** определять уведомления для информирования сетевых операторов о любых интересующих их ситуациях, включая обнаруженные отказы при работе AC.

¹Generalized bit error.

Объекты, определенные для расширения связанных с протоколами уведомлений с целью добавления функциональности PWE, **должны** объяснять, каким образом эти уведомления генерируются.

6.6. Проверка и трассировка псевдопроводных соединений

Для целей сетевого управления в PW **следует** поддерживать механизм проверки соединений. Такая проверка, наряду с другими механизмами сигнализации, может сообщать оператору о потере PW удаленного соединения. Иногда желательно знать в точности функциональный путь PW при поиске неисправностей, поэтому **следует** обеспечивать функции трассировки пути, по которому передаются пакеты данных через PW.

7. Недостатки эмулируемых служб

Эмулируемым службам **следует** быть похожими на естественные типы сервиса, насколько это возможно, но полная идентичность **не требуется**. Декларация применимости сервиса PWE3 **должна** сообщать об ограничениях, присущих эмулируемым устройствам.

Некоторые базовые требования к сходству для эмулируемых устройств описаны ниже.

7.1. Характеристики эмулируемого сервиса

С точки зрения CE эмулируемое устройство характеризуется как выделенный (unshared) канал или устройство выбранного сервиса, хотя качество обслуживания для эмулируемого устройства может отличаться от аналогичных характеристик естественного сервиса. В частности, **должны** выполняться следующие требования:

- 1) **Должна** обеспечиваться возможность задать тип (например, Ethernet), наследуемый от естественного сервиса, скорость (например, 100 Мбит/с) и размер MTU для эмулируемого устройства, если это возможно для естественного устройства.
- 2) Если две конечных точки (CE1 и CE2) эмулируемого устройства #1 соединены с PE1 и PE2, соответственно, а точки CE3 и CE4 эмулируемого устройства #2 также соединены с PE1 и PE2, тогда PW этих двух эмулируемых устройств могут использовать один и тот же физический путь между PE1 и PE2. Но с точки зрения каждого из CE эмулируемое устройство **должно** представляться выделенным (unshared). Например, пара CE1/CE2 **не должна** знать о существовании эмулируемого устройства #2 или CE3/CE4.
- 3) При отказе в эмулируемом устройстве (на одной из ACs или в средней части PW) оба CE **должны** быть уведомлены своевременно, если такие уведомления поддерживаются для естественного сервиса (см. параграф 5.3). Трактовка понятия "своевременность" зависит от типа сервиса.
- 4) Если естественное устройство позволяет организовать отношения смежности для протокола маршрутизации (например, IGP), **должна** обеспечиваться возможность организации таких же отношений через эмулируемое устройство.

7.2. Качество обслуживания для эмулируемого сервиса

От эмулируемых устройств **не требуется** обеспечение такого же качества сервиса, который присущ естественным устройствам. Рабочая группа PWE3 лишь определяет механизмы эмуляции PW, но не сами эмулируемые типы сервиса. Уровень сервиса, достаточный для поддержки тех или иных эмулируемых служб между сервис-провайдером (SP) и его пользователями определяется этими сторонами и не входит в число задач рабочей группы PWE3.

8. Что не относится к числу требований

В различных частях этого документа обозначены некоторые характеристики (аспекты), которые не являются требованиями к эмулируемому сервису. Эти аспекты не входят в число задач рабочей группы PWE3. Краткий перечень таких вопросов приведен ниже:

- межсетевое взаимодействие¹;

В межсетевом взаимодействии IWF (Interworking Function) между двумя непохожими протоколами (например, ATM и MPLS, Frame Relay и ATM, ATM и IP, ATM и L2TP и т. п.) прерывает действие используемого в одной сети протокола и транслирует (т. е., отображает) управляющие данные PCI² в данные PCI того протокола, который используется в другой сети, для функций пользовательского, управляющего и контролирующего плана.

- выбор отдельных типов PW;
- точное соответствие эмулируемых устройств их естественным аналогам;
- определение механизмов сигнализации для туннелей PSN;
- определение механизмов управления трафиком для пакетов, содержащих PW PDU;
- обеспечение той или иной групповой адресации, которая не является естественной для эмулируемой среды.

Например, передача кадров Ethernet по групповым адресам IEEE-48 входит в число рассматриваемых вопросов, тогда как групповая адресация типа [MARS] не входит в их число.

9. Качество обслуживания (QoS)

Некоторые службы в естественной форме (например, ATM) могут предлагать более высокое качество обслуживания, нежели доступный в сети Internet уровень best effort³. Параметры QoS, следовательно, важны для того, чтобы эмулируемые услуги были совместимы (но не обязательно идентичны) с естественной их формой. Сетевые операторы

¹В оригинале - Service Interworking. *Прим. перев.*

²Protocol Control Information - управляющая информация протокола.

³По-русски, наверное, лучше всего сказать "сделаем, как сможем". *Прим. перев.*

сами определяют, как им обеспечивать QoS - они могут выбрать их с учетом имеющихся ресурсов и/или развернутых механизмов QoS.

Чтобы воспользоваться механизмами QoS, определенными другими рабочими группами (например, схемы управления трафиком, определенные группой DiffServ), желательно иметь некоторые механизмы, приводящие к дифференциации пакетов на основе инкапсуляции PDU. Эти механизмы не определены непосредственно в PWE3. Например, если получаемые в результате пакеты относятся к MPLS или IP, поля EXP или DSCP этих пакетов могут применяться для маркировки и дифференциации. PWE3 **может** включать рекомендации по маркировке и дифференциации.

Применимость PWE3 для того или иного типа сервиса зависит от чувствительности этого сервиса (или реализации CE) к задержкам и их вариациям, а также от способности прикладного уровня компенсировать задержки и их изменения. PWE3 может не подойти для служб, имеющих жесткие ограничения в части требований к задержкам.

10. Вопросы междоменного взаимодействия

Эмуляция PWE имеет значение для конечных точек PW и прозрачна для сетевых устройств между этими точками. Следовательно, междоменные PWE подобны внутридоменным PWE. Если конечные точки PW используют одну модель PWE, они могут эффективно взаимодействовать между собой, независимо от того, относятся эти точки к одному домену или к разным. Для междоменного взаимодействия могут стать более важными вопросы безопасности (например, **может** использоваться аутентификация конечных точек). При междоменном взаимодействии усложняется поддержка QoS, поскольку сервис-провайдеры не имеют сквозного контроля за трафиком и не могут изменять политику контроля трафика других провайдеров. Для решения задачи обеспечения QoS при междоменном взаимодействии требуется кооперация провайдеров. После того, как на уровне контракта будет достигнуто соглашение об обеспечении высокого качества обслуживания того или иного трафика (например, PWE), можно будет использовать механизмы, созданные другими рабочими группами (например, Diffserv).

Междоменные туннели PSN в общем случае сложнее с точки зрения организации, разрыва и поддержки, нежели туннели внутри домена. Но эта проблема относится к протоколам туннелирования PSN (таким, как MPLS и L2TPv3) и выходит за пределы PWE3.

11. Вопросы безопасности

Конечные устройства PW, механизмы демультимплексирования PW и данные естественного сервиса могут быть уязвимы для атак. PWE3 следует усиливать механизмы, обеспечиваемые демультимплексорами PW и уровнем PSN. Этим механизмам **следует** обеспечивать защиту конечных точек PW и механизмов демультимплексирования PW от атак на службы (DoS) и подмены модулей данных естественного сервиса. Предотвращение несанкционированного доступа к конечным точкам PW и другим сетевым устройствам в общем случае обеспечивает эффективную защиту от DoS-атак и подмены (spoofing), обеспечивая важный механизм защиты. **Следует** обеспечить также механизмы защиты от подмены туннелируемых данных PW. Проверка корректности трафика, адресованного конечной точкой мультиплексору PW является важной компонентой обеспечения целостности инкапсуляции PW. Могут использоваться протоколы защиты, типа [RFC2401].

12. Благодарности

Авторы выражают свою признательность М. Aissaoui, М. Bocci, S. Bryant, R. Cohen, N. Harrison, G. Heron, T. Johnson, A. Malis, L. Martini, E. Rosen, J. Rutemiller, T. So, Y. Stein, S. Vainshtein.

13. Литература

13.1. Нормативные документы

[IFMIB] McCloghrie, K. and F. Kastenholtz, "The Interfaces Group MIB", RFC 2863, June 2000.

[SMIV2] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Structure of Management Information Version 2 (SMIV2)", STD 58, RFC 2578, April 1999.

13.2. Ссылки

[G805] "Generic Functional Architecture of Transport Networks", ITU-T Recommendation G.805, 2000.

[IPTUNMIB] Thaler, D., "IP Tunnel MIB", RFC 2667, August 1999.

[L2TPv3] Lau, J., Townsley, M., and I. Goyret, et al., "Layer Two Tunneling Protocol (Version 3)", Work in Progress¹, June 2004.

[MARS] Armitage, G., "Support for Multicast over UNI 3.0/3.1 based ATM Networks", RFC 2022, November 1996.

[MPLS] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", [RFC 3031](#), January 2001.

[PWE3_ARCH] S. Bryant and P. Pate, et. al., "PWE3 Architecture", Work in Progress², March 2004.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", [RFC 2401](#)³, November 1998.

[TEMIB] Srinivasan, C., Viswanathan, A., and T. Nadeau, "Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)", RFC 3812, June 2004.

[UNI3.0] ATM Forum, "ATM User-Network Interface Specification Version 3.0", Sept. 1993.

¹Эта работа завершена и опубликована в RFC 3931, который частично обновлен RFC 5641. *Прим. перев.*

²Работа завершена и опубликована в [RFC 3985](#). *Прим. перев.*

³Этот документ признан устаревшим и заменен [RFC 4301](#). *Прим. перев.*

14. Адреса авторов

XiPeng Xiao (редактор)
Riverstone Networks
5200 Great America Parkway
Santa Clara, CA 95054
E-Mail: xxiao@riverstonenet.com

Danny McPherson (редактор)
Arbor Networks
E-Mail: danny@arbor.net

Prayson Pate (редактор)
Overture Networks
507 Airport Boulevard, Suite 111
Morrisville, NC, USA 27560
E-Mail: prayson.pate@overturenetworks.com

Vijay Gill
AOL Time Warner
E-Mail: vijaygill9@aol.com

Kireeti Kompella
Juniper Networks, Inc.
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
E-Mail: kireeti@juniper.net

Thomas D. Nadeau
Cisco Systems, Inc.
300 Beaver Brook Drive
Boxborough, MA 01719
E-Mail: tnadeau@cisco.com

Craig White
Level 3 Communications, LLC.
1025 Eldorado Blvd.
Broomfield, CO, 80021
E-Mail: Craig.White@Level3.com

Перевод на русский язык

Николай Малых
nmalykh@protokols.ru

15. Полное заявление авторских прав

Copyright (C) The Internet Society (2004).

К этому документу применимы права, лицензии и ограничения, указанные в BCP 78, и, за исключением указанного там, авторы сохраняют свои права.

Этот документ и содержащаяся в нем информация представлены "как есть" и автор, организация, которую он/она представляет или которая выступает спонсором (если таковой имеется), Internet Society и IETF отказываются от каких-либо гарантий (явных или подразумеваемых), включая (но не ограничиваясь) любые гарантии того, что использование представленной здесь информации не будет нарушать чьих-либо прав, и любые предполагаемые гарантии коммерческого использования или применимости для тех или иных задач.

Интеллектуальная собственность

IETF не принимает какой-либо позиции в отношении действительности или объема каких-либо прав интеллектуальной собственности (Intellectual Property Rights или IPR) или иных прав, которые, как может быть заявлено, относятся к реализации или использованию описанной в этом документе технологии, 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 RFC можно найти в BCP 78 и BCP 79.

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 из сетевого репозитория IETF IPR по ссылке <http://www.ietf.org/ipr>.

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. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.