Internet Engineering Task Force (IETF)
Request for Comments: 8201
STD: 87
Obsoletes: 1981
Category: Standards Track
ISSN: 2070-1721

J. McCann
Digital Equipment Corporation
S. Deering
Retired
J. Mogul
Digital Equipment Corporation
R. Hinden, Ed.
Check Point Software

July 2017

Path MTU Discovery for IP version 6

Обнаружение MTU на пути для IPv6.

Аннотация

Этот документ описывает определение MTU[1] для пути (Path MTU Discovery или PMTUD) для протокола IP версии 6. Механизм по большей части создан на основе RFC 1191, определяющего Path MTU Discovery для IP версии 4. Документ отменяет RFC 1981.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[2] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[3]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc8201.

Оглавление

[1] Maximum Transmission Unit - максимальный передаваемый блок.
[2] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[3] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Когда узел IPv6 имеет большой объем данных для передачи другому узлу, эти данные передаются в серии пакетов IPv6, размер которых не превышает Path MTU (PMTU). Другим вариантом является фрагментация большого пакета в серию фрагментов, размер которых не превышает PMTU.

Обычно предпочтительно использовать для пакетов наибольший размер, поддерживаемый на пути между источником и получателем без необходимости фрагментации IPv6. Такой размер называется Path MTU и он равен минимальному значению MTU среди всех каналов, образующих путь. Этот документ задаёт стандартный механизм для определения PMTU на произвольном пути.

Узлам IPv6 следует реализовать Path MTU Discovery чтобы обнаруживать и использовать пути с PMTU больше минимального размера IPv6 MTU [RFC8200]. Минимальная реализация IPv6 (например, ПЗУ загрузки) может отказаться от реализации Path MTU Discovery. Узлы, не реализующие Path MTU Discovery должны использовать минимальное значение IPv6 MTU, заданное в [RFC8200], как максимальный размер пакета. В многих случаях это ведёт к использованию пакетов размером меньше возможного, поскольку на многих путях PMTU превышает минимальное значение IPv6 MTU. Узел, передающий пакеты размером существенно меньше Path MTU, потребляет избыточные ресурсы сети и может иметь неоптимальную пропускную способность.

Реализующие Path MTU Discovery узлы, передающие пакеты размером больше минимального IPv6 MTU, могут сталкиваться с проблемами связности, если сообщения ICMPv6 [ICMPv6] не передаются или блокируются. Например, это может приводить к тому, что соединение TCP после корректного трехэтапного согласования «зависает» при передаче данных. Такое состояние называют «чёрной дырой» (black-hole connection) [RFC2923]. Механизм Path MTU Discovery полагается при определении MTU для пути на сообщения ICMPv6 PTB.

Определённое в этом документе расширение для Path MTU Discovery описано в [RFC4821]. RFC 4821 определяет механизм для уровня пакетирования (Packetization Layer Path MTU Discovery или PLPMTUD), предназначенный для использования на путях, где доставка хосту сообщений ICMPv6 не гарантируется.

> Примечание. Этот документ обновляет [RFC1981], опубликованный до [RFC2119]. Хотя в RFC 1981 применяется стиль написания требований «следует/должно» с выделением шрифтом, в этом документе не применяются соглашения RFC 2119 по такому выделению.

2. Термины

node - узел
Устройство, реализующее IPv6.

router - маршрутизатор
Узел, пересылающий пакеты IPv6, не адресованные явно ему.

host - хост
Любой узел, не являющийся маршрутизатором.

upper layer - вышележащий уровень
Протокольный уровень, расположенный непосредственно над IPv6. Примерами являются транспортные протоколы TCP и UDP, протоколы управления типа ICMP, протоколы маршрутизации, такие как OSPF, а также протоколы, «туннелируемые» через IPv6 (т. е., инкапсулированные в пакеты IPv6), такие как IPX (Internetwork Packet Exchange - пакет межсетевого обмена), AppleTalk или IPv6.

link - канал
Коммуникационный объект или среда, посредством которых узлы могут взаимодействовать на канальном уровне (уровне, расположенном непосредственно под IPv6). Примерами могут служить сети Ethernet (с мостами или без них), каналы PPP, сети X.25, Frame Relay или ATM, а также туннели сетевого или вышележащих уровней (например, IPv4 или IPv6).

interface - интерфейс
Подключение узла к каналу.

address - адрес
Идентификатор уровня IPv6 для интерфейса или группы интерфейсов.

packet - пакет
Заголовок IPv6 и данные (payload). Пакет может иметь размер не больше PMTU, а при большем размер он фрагментируется на серию пакетов (фрагментов), размером не более PMTU.

link MTU - MTU для канала
Максимальный передаваемый блок (максимальное число октетов в пакете, который можно передать по каналу).

path - путь
Множество каналов, по которым пакет проходит от узла-источника к получателю.

path MTU - MTU для пути
Минимальное значение среди MTU каналов на пути между узлом-источником и получателем.

PMTU
MTU для пути.

Path MTU Discovery - определение MTU для пути
Процесс определения PMTU для пути.

EMTU_S
Эффективное значение MTU для передачи. Используется протоколами вышележащего уровня для ограничения размера пакетов IP, помещаемых в очередь на передачу [RFC6691] [RFC1122].

EMTU_R
Эффективное значение MTU для приёма, т. е. наибольший размер пакета, который может собрать получатель [RFC1122].

flow - поток
Последовательность пакетов из одного источника к одному получателю (индивидуальному или групповому), для которых отправитель хочет получить специальную обработку на промежуточных маршрутизаторах.

flow id - идентификатор потока
Комбинация адреса источника и отличной от 0 метки потока.

3. Обзор протокола

Этот документ описывает метод динамического определения PMTU для пути. Основная идея состоит в том, что узел-источник изначально считает значением PMTU величину (известную) MTU первого этапа пути (first hop). Если какой-либо из переданных пакетов оказывается слишком велик для пересылки тем или иным узлом на пути, этот узел отбросит пакет и передаст источнику сообщение ICMPv6 Packet Too Big (PTB). При получении такого сообщения источник снижает предполагаемое значение PMTU для пути в соответствии с MTU столкнувшегося с проблемой пересылки узла, указанному в сообщении PTB. Снижение PMTU заставляет источник передавать пакеты меньшего размера или менять значение EMTU_S, чтобы заставить вышележащий уровень снизить размер передаваемых пакетов IP.

Процесс Path MTU Discovery завершается, когда оценка узлом-источником значения PMTU не превышает фактическое значение PMTU. Отметим, что до завершения этого процесса может произойти несколько итераций «передан пакет - получено сообщение PTB», поскольку на дальнейшем пути может оказаться несколько узлов с меньшими MTU. Узел может прервать процесс определения, перейдя к передаче пакетов с минимальным значением IPv6 MTU.

PMTU для пути может меняться с течением времени в результате изменения топологии маршрутов. Снижение PMTU обнаруживается получением сообщений PTB. Для обнаружения роста PMTU на пути узел периодически повышает предполагаемое значение PMTU. Это почти всегда ведёт к отбрасыванию пакетов и получению сообщений PTB, поскольку в большинстве случаев PMTU на пути не меняется. Поэтому попытки обнаружить рост PMTU на пути следует предпринимать нечасто.

Path MTU Discovery может работать как для индивидуальных, так и для групповых адресатов. В случае группового получателя пакеты к разным узлам группы могут идти по разным путям. Каждый из путей может иметь своё значение PMTU и один групповой пакет может вызывать множество сообщений, каждое из которых указывает своё значение next-hop MTU. Минимальное значение PMTU из числа полученных определяет размер последующих пакетов для этого группового адресата.

Отметим, что механизм Path MTU Discovery должен применяться даже в тех случаях, когда узел считает, что адресат подключён к тому же каналу, поскольку адресат может иметь значение PMTU меньше чем MTU для канала. В ситуации когда соседний маршрутизатор служит прокси-ND [ND] для того или иного получателя, адресат может казаться подключённым напрямую, а фактически быть отделен несколькими маршрутизаторами.

4. Требования к протоколу

Как отмечено в разделе 1, от узлов IPv6 не требуется реализация Path MTU Discovery и требования этого раздела относятся лишь к реализациям, поддерживающим Path MTU Discovery.

Узлам следует должным образом проверять содержимое (payload) сообщения ICMPv6 PTB для уверенности в том, что оно служат ответом на переданный ранее трафик (т. е. сообщает об ошибке, связанной с пакетом IPv6, действительно переданным приложением) в соответствии с [ICMPv6].

При получении узлом сообщения PTB, указывающего next-hop MTU меньше минимального IPv6 MTU, узел должен отбросить сообщение. Узлам недопустимо снижать оценку Path MTU до значения меньше минимального IPv6 MTU в ответ на получение сообщения PTB.

Когда узел получил сообщение PTB, он должен снизить оценку PMTU для соответствующего пути на основе значения поля MTU в сообщении. Точное поведение узла в такой ситуации не задаётся, поскольку требования приложений могут различаться, а разные варианты реализаций могут использовать свои стратегии.

После приёма сообщения PTB узел должен попытаться избежать получения таких сообщений в ближайшем будущем, уменьшая размер пакетов, передаваемых по этому пути. Использование PMTU, превышающих минимальное значение IPv6 MTU, может вызвать сообщения PTB. Поскольку на такие сообщения (и отбрасывание вызвавших их пакетов) тратятся ресурсы сети, использующие Path MTU Discovery узлы должны снижать PMTU как можно быстрее.

Узлы могут обнаруживать рост PMTU, но для этого нужно передавать пакеты размером больше текущей оценки PMTU, а вероятность роста PMTU невелика, поэтому такие попытки должны быть нечастыми. Попытки обнаружить рост PMTU (путём передачи пакета размером больше текущего значения) недопустимо предпринимать раньше чем через 5 минут после приёма сообщения PTB для данного пути. Рекомендуется устанавливать для таймера удвоенное минимальное значение (10 минут).

Узлу недопустимо увеличивать оценку Path MTU в ответ на сообщение PTB, поскольку сообщение со значением Path MTU выше текущей оценки может оказаться устаревшим пакетом, «застрявшим» в сети, ложным пакетом, связанным с DoS[1]-атакой), или следствием наличия нескольких путей к адресату (с разными PMTU).

5. Вопросы реализации

В этом разделе рассмотрены вопросы, связанные с реализацией Path MTU Discovery. Это не спецификация, а просто замечания в помощь разработчикам. Рассматривается несколько вопросов:

- на каких уровнях реализуется Path MTU Discovery;
- как кэшируются данные PMTU;
- как удаляются устаревшие сведения PMTU;
- что делает транспортный уровень и уровни над ним?

5.1. Уровни

В архитектуре IP выбор размера передаваемого пакета выполняет протокол на уровне выше IP. В этом документе такие протоколы называются «протоколами пакетирования». Обычно эту роль играет транспортный протокол

[1]Denial-of-service - отказ в обслуживании.

(например, TCP), но это могут быть и вышележащие протоколы (например, протокол, работающий на основе транспорта UDP).

Реализация Path MTU Discovery на уровне пакетирования упрощает некоторые проблемы взаимодействия уровней, но имеет ряд недостатков - может потребоваться переработка реализации для каждого протокола пакетирования, сложно обмениваться данными PMTU между разными уровнями пакетирования, а ориентированным на соединения состояниям в некоторых уровнях пакетирования может быть сложно поддерживать сведения PMTU достаточно долго. Поэтому предлагается хранить сведения PMTU на уровне IP, а уровню ICMPv6 - обрабатывать сообщения PTB. Уровни пакетирования могут реагировать на изменение PMTU сменой размера передаваемых сообщений. Для поддержки этих уровней для уровня пакетирования может потребоваться способ узнавать у смене значения MMS_S (максимальный размер передаваемого транспортного сообщения [RFC1122]).

MMS_S - это размер транспортного сообщения, рассчитываемый вычитанием размера заголовка IPv6 (включая заголовки расширения IPv6) из максимального размера пакета IP, который можно передать (EMTU_S). Значение MMS_S ограничено рядом факторов, включая PMTU, поддержку фрагментации и сборки пакетов, ограничения сборки пакетов (см. параграф 4.5 в [RFC8200]). Когда источник может обеспечивать фрагментацию, для EMTU_S устанавливается значение EMTU_R, указанное получателем с использованием протокола вышележащего уровня или на основе требований протокола (1500 октетов для IPv6). При передаче сообщения размером больше PMTU отправитель создаёт фрагменты, размер которых ограничен значением PMTU. Если фрагментация у отправителя нежелательна, для EMTU_S устанавливается значение PMTU и предполагается, что вышележащий протокол сам выполнит фрагментацию (и сборку) или иным способом ограничит размер сообщения.

Тем не менее, рекомендуется применять уровень пакетирования, чтобы избежать отправки сообщений, требующих фрагментации у отправителя (меры предотвращения фрагментации описаны в [FRAG]).

5.2. Сохранение сведений PMTU

В идеальном случае значение PMTU следует связывать с конкретным путём, по которому пакеты проходят между отправителем и получателем. Однако в большинстве случаев узел не имеет сведений для полного и точного определения такого пути. Скорее узел должен связывать PMTU с неким локальным представлениям пути, выбор которого остаётся за реализацией. На узлах с несколькими интерфейсами данные Path MTU следует поддерживать для каждого канала IPv6. В случае группового получателя пакеты могут идти по разным путям т локальное представления должно отражать как можно более широкий набор путей.

Реализация может поддерживать по меньшей мере 1 значение PMTU для всех передаваемых узлом пакетов, используя для этого минимальное среди известных узлу значений PMTU. Такой подход вероятно приведёт к передаче по многим путям пакетов с размером меньше возможного. В случае маршрутизации по нескольким путям (например, Equal-Cost Multipath Routing - ECMP) между источником и получателем может существовать множество путей.

Реализация может применять в качестве локального представления пути адрес получателя. Значение PMTU, связанное с получателем, будет минимальным из PMTU для всех известных путей к этому адресату. Этот подход обеспечивает оптимальный размер пакетов для каждого адресата[1] и хорошо интегрируется с концептуальной моделью хоста, описанной в [ND] - значение PMTU может храниться в соответствующей записи кэша адресатов.

Если применяются потоки [RFC8200], реализация может использовать flow id в качестве локального представления пути. Пакеты для одного адресата, относящиеся к разным потокам, могут использовать разные пути, как в случае ECMP с выбором пути на основе flow id. Такой подход может обеспечить оптимальный размер пакетов для каждого потока, обеспечивая более тонкую детализацию, чем поддержка PMTU по адресатам. Для пакетов с заданной источником маршрутизацией (пакеты с заголовком IPv6 Routing [RFC8200]) локальное представления пути может задавать source-route.

Исходно PMTU для пути предполагается равным (известному) значению MTU для первого канала на пути (first-hop).

Получив сообщение PTB, узел определяет путь, к которому оно относится на основе содержимого принятого сообщения. Например, если для локального представления пути применяется адрес получателя, принадлежность к пути указывает адрес получателя в вызвавшем сообщение пакете.

> Примечание. Если исходный пакет включал заголовок Routing, этот заголовок следует использовать для определения местоположения адреса получателя в исходном пакете. Если Segments Left = 0, адресом получателя будет поле Destination Address в заголовке IPv6, в ином случае - последний адрес (Address[n]) в заголовке Routing.

Затем узел использует в качестве предварительного значения PMTU большее из значений поля MTU в сообщении PTB и минимального IPv6 MTU и сравнивает предварительное значение PMTU с имеющимся. Если предварительное значение PMTU меньше, оно заменяет собой имеющееся значение PMTU для пути.

Уровни пакетирования должны уведомляться о снижении PMTU. Любой экземпляр уровня пакетирования (например, соединение TCP), активно использующий путь, информируется о снижении оценки PMTU.

> Примечание. Даже если сообщение PTB содержит заголовок исходного пакета, указывающий UDP, уровень TCP должен уведомляться о снижении, если его соединения используют данный путь.

Кроме того, экземпляр, который отправил пакет, вызвавший сообщение PTB, следует уведомлять об отбрасывании его пакета, даже при неизменности PMTU, чтобы отброшенные данные были переданы снова.

> Примечание. Реализация может избежать применения асинхронных уведомлений о снижении PMTU, откладывая уведомление до попытки передачи следующего пакета, размером больше PMTU. При таком подходе попытка передачи пакета размером больше PMTU должна вызывать отказ функции SEND с возвратом подходящего сообщения об ошибке. Этот подход может оказаться более подходящим для уровней пакетирования без организации соединений (таких как основанные на UDP), которые (в некоторых реализациях) может быть трудно «уведомить» с уровня ICMPv6. В этом случае можно использовать обычный механизм повтора по тайм-ауту для повтора передачи отброшенных пакетов.

[1] Заявление представляется весьма сомнительным, поскольку при передаче по пути с PMTU больше минимального для имеющегося набора путей размер пакета явно будет меньше возможного. *Прим. перев.*

Важно понимать, что уведомление использующих путь экземпляров уровня пакетирования об изменении PMTU отличается от информирования конкретного экземпляра об отбрасывании пакета, которое должно происходить как можно скорее (асинхронно с точки зрения уровня пакетирования), тогда как уведомление о смене PMTU можно задержать до момента создания пакета уровнем пакетирования.

5.3. Отбрасывание устаревших сведений PMTU

Топология межсетевого взаимодействия динамична и маршруты меняются со временем. Хотя локальное представление пути может сохраняться, фактический путь может стать иным и кэшированная хостом информация PMTU устаревает.

Если устаревшее значение PMTU слишком велико, это будет обнаружено почти сразу после отправки достаточно большого пакета по этому пути. Для обнаружения слишком малых устаревших значений PMTU какого-либо механизма нет, поэтому реализации следует поддерживать «старение» кэшированных записей. Когда значение PMTU не снижается слишком долго (порядка 10 минут), следует проверить возможность применения большего значения PMTU.

> Примечание. Реализации следует предоставлять возможность изменения времени ожидания, включая установку «бесконечного» значения. Например, узлы подключённые по каналу с большим MTU к устройству, соединённому с Internet каналом с меньшим MTU, никогда не увидят новых нелокальных значений PMTU, поэтому им не следует предпринимать попыток такого обнаружения.

5.4. Действия уровня пакетирования

Уровень пакетирования (например, TCP) должен использовать PMTU для путей, применяемых в соединении и ему недопустимо передавать сегменты, которые будут приводить к пакетам размером больше PMTU, за исключением пробных пакетов PMTU Discovery (эти пакеты не фрагментируются до PMTU). Простая реализация может запрашивать это значение у уровня IP при создании каждого сегмента, но это может быть неэффективно. Реализация обычно кэширует другие значения, выведенные из PMTU, и может оказаться проще использовать асинхронные уведомления при смене PMTU, при котором эти переменные также обновляются.

Реализация TCP должна сохранять также максимальный размер сегмента (Maximum Segment Size или MSS), полученный от партнёра, который представляет EMTU_R (наибольший пакет, который может быть собран получателем), и ей недопустимо передавать сегменты больше этого MSS, независимо от PMTU. Значение, передаваемое в опции TCP MSS, не зависит от PMTU и определяется ограничением сборки у получателя (EMTU_R). Значение опции MSS используется другой стороной соединения, которая может иметь своё значение PMTU. Информация о выборе опции TCP MSS приведена в разделе 5 и параграфе 8.3 [RFC8200].

Приём сообщения PTB говорит об отбрасывании пакета узлом, передавшим это сообщение ICMPv6. Протокол вышележащего уровня с гарантией доставки будет обнаруживать такие потеря и восстанавливать данные с помощью механизмов повтора передачи. Повтор может приводить к задержкам в зависимости от используемого вышележащим протоколом метода обнаружения потерь. Если процесс Path MTU Discovery требует нескольких шагов для определения PMTU на всем пути, это может в конечном итоге задержать повтор передачи на много интервалов кругового обхода. Как вариант, повтор передачи может происходить сразу при уведомлении о снижении Path MTU, но лишь для конкретного соединения, указанного в сообщении PTB. При повторе следует использовать размер пакета не больше нового значения PMTU.

> Примечание. Уровень пакетирования, обнаруживший потерю пробного пакета, должен изменить размер сегмента при повторе передачи. Однако применения значения из последнего сообщения PTB может привести к дополнительным потерям, обусловленных меньшими PMTU на последующих маршрутизаторах пути. Это приведёт к потере всех повторных сегментов и вызовет ненужную перегрузку а также передачу дополнительных пакетов, когда какой-либо маршрутизатор объявит меньшее значение MTU. Поэтому уровень пакетирования, использующий повтор передачи, отвечает также за контроль перегрузок при повторах [RFC8085].

Потерю, вызванную зондом PMTU и указанную сообщением PTB, недопустимо считать индикацией перегрузки, поэтому окно перегрузки можно не менять.

5.5. Проблемы других транспортных протоколов

В некоторых транспортных протоколах не разрешается изменение пакетирования при повторной передаче., т. е. после попытки передать сегмент определённого размера транспорт не может разделить этот сегмент на меньшие для повтора передачи. В таких случаях исходный сегмент может быть фрагментирован уровнем IP при повторной передаче. Для последующих сегментов, передаваемых в первый раз, следует выбирать размер не больше Path MTU.

Path MTU Discovery для IPv4 [RFC1191] использует NFS в качестве примера приложения на основе UDP, получающего преимущества от обнаружения PMTU. Позднее в [RFC7530] было указано, что поддерживаемый между NFS и IP транспортный уровень должен применять стандартизованный IETF транспортный протокол, в котором указано предотвращение перегрузки в сети. В качестве такого транспорта применяются TCP, Stream Control Transmission Protocol (SCTP) [RFC4960] и Datagram Congestion Control Protocol (DCCP) [RFC4340], которые отвечают за соответствие передаваемых сегментов (кроме зондов) значению Path MTU и поддержку зондов PMTU Discovery при необходимости.

5.6. Интерфейс управления

Предполагается, что реализация позволяет системным утилитам:

- отключать Path MTU Discovery для указанного пути;
- менять значение PMTU, связанное с заданным путём.

Первый вариант можно реализовать с помощью флага, связанного с путём, при установке которого уровень IP не передаёт в соответствующий канал пакеты размером больше минимального IPv6 MTU. Эти возможности можно применить для обработки аномалий или при неспособности протокола маршрутизации получить значения Path MTU.

Реализации следует также обеспечивать способ изменения таймаута старения сведений PMTU.

6. Вопросы безопасности

Этот механизм Path MTU Discovery открывает возможность для двух DoS-атак на основе ложных сообщений PTB.

В первом варианте ложные сообщения указывают слишком малые значения PMTU. Узлу-жертве никогда не следует устанавливать PMTU меньше минимального IPv6 MTU. Снижение PMTU в результате атаки ведёт к неоптимальной производительности.

Второй тип атак указывает значение PMTU выше реального, использование которого жертвой может привести к её временной блокировке в результате отбрасывания пакетов каким-либо из маршрутизаторов. В течение одного кругового обхода узел может увидеть свою ошибку (из сообщения PTB от маршрутизатора), но частый повтор такой атаки приведёт к отбрасыванию многих пакетов. Однако узлам недопустимо увеличивать PMTU на основе сообщений PTB, поэтому они не уязвимы для таких атак.

Обе эти атаки могут создавать «чёрные дыры» в соединениях, когда трехэтапное согласование TCP проходит нормально, а последующая передача данных «зависает».

Злоумышленник также может вызвать проблемы, заблокировав получение жертвой сообщений PTB, но для этого есть более простые DoS-атаки.

Если фильтрация ICMPv6 препятствует получению сообщений ICMPv6 PTB, источник не сможет узнать фактическое значение MTU для пути. В документе "Packetization Layer Path MTU Discovery" [RFC4821] предложен механизм, не использующий сообщения ICMPv6 и обеспечивающий более высокую отказоустойчивость по сравнению со стандартным PMTUD. Он не подвержен возникновению «чёрных дыр» из-за фильтрации сообщений ICMPv6 (см. рекомендации по такой фильтрации в [RFC4890].

7. Взаимодействие с IANA

Этот документ не требует действий IANA.

8. Литература

8.1. Нормативные документы

[ICMPv6] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <http://www.rfc-editor.org/info/rfc4443>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <http://www.rfc-editor.org/info/rfc8200>.

8.2. Дополнительная литература

[FRAG] Kent, C. and J. Mogul, "Fragmentation Considered Harmful", In Proc. SIGCOMM '87 Workshop on Frontiers in Computer Communications Technology, DOI 10.1145/55483.55524, August 1987.

[ND] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <http://www.rfc-editor.org/info/rfc4861>.

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <http://www.rfc-editor.org/info/rfc1122>.

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, DOI 10.17487/RFC1191, November 1990, <http://www.rfc-editor.org/info/rfc1191>.

[RFC1981] McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, DOI 10.17487/RFC1981, August 1996, <http://www.rfc-editor.org/info/rfc1981>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2923] Lahey, K., "TCP Problems with Path MTU Discovery", RFC 2923, DOI 10.17487/RFC2923, September 2000, <http://www.rfc-editor.org/info/rfc2923>.

[RFC4340] Kohler, E., Handley, M., and S. Floyd, "Datagram Congestion Control Protocol (DCCP)", RFC 4340, DOI 10.17487/RFC4340, March 2006, <http://www.rfc-editor.org/info/rfc4340>.

[RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, DOI 10.17487/RFC4821, March 2007, <http://www.rfc-editor.org/info/rfc4821>.

[RFC4890] Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC 4890, DOI 10.17487/RFC4890, May 2007, <http://www.rfc-editor.org/info/rfc4890>.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <http://www.rfc-editor.org/info/rfc4960>.

[RFC6691] Borman, D., "TCP Options and Maximum Segment Size (MSS)", RFC 6691, DOI 10.17487/RFC6691, July 2012, <http://www.rfc-editor.org/info/rfc6691>.

[RFC7530] Haynes, T., Ed. and D. Noveck, Ed., "Network File System (NFS) Version 4 Protocol", RFC 7530, DOI 10.17487/RFC7530, March 2015, <http://www.rfc-editor.org/info/rfc7530>.

[RFC8085] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage Guidelines", BCP 145, RFC 8085, DOI 10.17487/RFC8085, March 2017, <http://www.rfc-editor.org/info/rfc8085>.

Приложение A. Сравнение с RFC 1191

RFC 1981 (отменен этим документом) был основан по большей части на RFC 1191, описывавшем Path MTU Discovery для IPv4. Некоторые части RFC 1191 не были использованы в RFC 1981:

router specification - спецификация маршрутизатора
Сообщения PTB и соответствующее поведение маршрутизаторов описаны в [ICMPv6].

Don't Fragment bit - флаг запрета фрагментирования.
Флаг DF не применяется в пакетах IPv6.

TCP MSS discussion - обсуждение TCP MSS
Выбор значения для передачи в опции TCP MSS рассматривается в [RFC8200].

old-style messages - сообщения старого стиля
Все сообщения PTB указывают MTU связанного с ошибкой канала.

MTU plateau tables - таблицы плато MTU
Не нужны, поскольку сообщения старого стиля не применяются.

Приложение B. Отличия от RFC 1981

Этот документ основан на RFC 1981, но отличается от него, как указано ниже.

- В разделе 1. Введение поясняется, что целью PMTUD является снижение фрагментации IPv6.
- В раздел 1. Введение добавлен текст о влиянии на PMTUD блокировки сообщений ICMPv6.
- В раздел 1. Введение добавлено примечание о том, что данный документ не следует RFC 2119 и указывает уровни требований «должен/следует» строчными буквами.
- В раздел 1. Введение добавлена краткая информация о PLPMTUD и ссылка на RFC 4821.
- Исправлен текст раздела 2. Термины в соответствии с современной терминологией уровня пакетирования.
- В раздел 4. Требования к протоколу добавлено пояснение о том, что узлам следует проверять содержимое сообщения ICMP PTB в соответствии с RFC 4443, а также обрабатывать снижение PMTU как можно быстрее.
- Из раздела 4. Требования к протоколу исключён текст о сообщении PTB, указывающем next-hop MTU меньше минимального IPv6 MTU, поскольку это исключено из [RFC8200].
- В параграф 5.2. Сохранение сведений PMTU добавлен текст об отбрасывании сообщений ICMPv6 PTB, указывающих MTU меньше минимального IPv6 MTU.
- В параграф 5.2. Сохранение сведений PMTU добавлено разъяснение о сохранении хостом с несколькими интерфейсами сведений Path MTU для каждого канала.
- Из параграфа 5.2. Сохранение сведений PMTU удалён текст о Routing Header type 0 (RH0), поскольку этот заголовок отменен RFC 5095. Исключена также устаревшая классификация безопасности.
- Изменено название параграфа 5.4. Действия уровня пакетирования и текст первого абзаца в нем для обобщения содержимого параграфа на все уровни пакетирования (а не только TCP).
- Уточнён текст параграфа 5.4. Действия уровня пакетирования в части применения обычных методов повтора передачи уровня пакетирования.
- Из параграфа 5.4. Действия уровня пакетирования исключён текст, описывающий 4.2 BSD, поскольку он устарел, а также исключена ссылка на TP4.
- Обновлён текст параграфа 5.5. Проблемы других транспортных протоколов о NFS с включением современных ссылок и удалением устаревших сведений.
- В раздел 6. Вопросы безопасности добавлен абзац о «чёрных дырах» соединений при отсутствии сообщений PTB, а также сравнение с PLPMTUD.
- Обновлён параграф Благодарности.
- Внесены редакторские правки.

Благодарности

Спасибо авторам и участникам создания [RFC1191], послужившего основой для этого документа, а также членам рабочей группы IPng за их рецензии и конструктивную критику.

Спасибо также участникам работы над этим обновлением Path MTU Discovery for IP Version 6, включая членов рабочей группы 6MAN, рецензентов от руководства направлением, IESG и особенно Joe Touch и Gorry Fairhurst.

Адреса авторов

Jack McCann

Digital Equipment Corporation

Stephen E. Deering

Retired

Vancouver, British Columbia

Canada

Jeffrey Mogul

Digital Equipment Corporation

Robert M. Hinden (editor)

Check Point Software

959 Skyway Road

San Carlos, CA 94070

United States of America

Email: bob.hinden@gmail.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru