Internet Engineering Task Force (IETF)
Request for Comments: 5881
Category: Standards Track
ISSN: 2070-1721

D. Katz
D. Ward
Juniper Networks

June 2010

Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)

BFD для IPv4 и IPv6 через один интервал (hop)

Аннотация

Этот документ описывает применение протокола обнаружения двухсторонней пересылки (Bidirectional Forwarding Detection или BFD) для IPv4 и IPv6 при одном интервале пересылки IP (hop).

Статус документа

Этот документ является проектом стандарта Internet (Internet Standards Track).

Документ подготовлен IETF[1] и содержит согласованный взгляд сообщества IETF. Документ обсуждался публично и одобрен для публикации IESG[2]. Дополнительная информация о стандартах Internet приведена в разделе 2 RFC 5741.

Информацию о текущем состоянии данного документа, обнаруженных ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc5881.

1. Введение

Одним из важных применений протокола BFD [BFD] является отслеживание связности IPv4 и IPv6 между соединёнными напрямую (без маршрутизаторов) системами. Это может служить дополнением к механизмам обнаружения в протоколах маршрутизации или применяться для отслеживания связности хоста с маршрутизатором и решения других задач.

Этот документ содержит сведения, требуемые для использования BFD в такой среде. Взаимодействия между BFD и другими протоколами и системными функциями описаны в документе «BFD Generic Applications» [BFD-GENERIC].

1.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119 [KEYWORDS].

2. Применение и ограничения

Протокол (приложение) BFD может применяться любой парой систем, взаимодействующих по протоколу IPv4 и/или IPv6 через один интервал IP (hop), включая физические и виртуальные каналы, туннели и т. п.

Каждая сессия BFD между парой систем **должна** проходить по своему пути сетевого уровня в обоих направлениях. Это нужно для корректного демультиплексирования, а также потому, что в противном случае (по определению) будет возникать несколько сессий для защиты одного пути.

Если BFD применяется с IPv4 и IPv6 на определённом пути, для каждого протокола **должна** создаваться своя сессия BFD (с инкапсуляцией в соответствующий протокол) через данный канал.

При использовании функции BFD Echo переданные пакеты незамедлительно возвращаются отправителю на интерфейс, который их передал. Это может взаимодействовать с другими механизмами, используемыми на двух системах, реализующих BFD. В частности, входная фильтрация [BCP38] не совместима со способом передачи пакетов Echo. Реализации, поддерживающие функцию Echo, **должны** обеспечивать отсутствие входной фильтрации на интерфейсе, применяющем функцию Echo или задавать исключение для входящих пакетов Echo.

От реализаций функции Echo также требуются прикладные интерфейсы (Application Programming Interface или API), которых может не быть в каждой системе. Система с поддержкой функции Echo **должна** быть способна передавать пакеты по своему адресу, для чего обычно требуется обходить обычный поиск в таблице пересылки. Как правило для этого требуется доступ к API для обхода функциональности уровня IP.

[1] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

Отметим, что протокол BFD предназначен для роли механизма OAM[1], служащего для проверки связности и соединений. Он применим для сетевых служб (например, взаимодействие между маршрутизаторами, пользователем и шлюзом, конечными точками LSP/каналов и обнаружение отказов оборудования). В таких ситуациях от оператора требуется корректное обеспечение скоростей, с которыми передаются пакеты BFD, чтобы избежать перегрузок (например, каналов, устройств ввода-вывода, процессоров) и ложных обнаружений отказов. Это не применимо для обнаружения отказов между приложениями через Internet, поскольку в сети не обеспечиваются требуемое обнаружение и предотвращение перегрузок и поэтому нет возможности предотвратить коллапс. Системы «хост-хост» или «приложение-приложение», развёрнутые через Internet, будут требовать инкапсуляции BFD в транспортный протокол, «дружественный» к TCP (TCP-friendly) [TFRC].

3. Инициализация и демультиплексирование

В описываемом варианте применения между двумя системами через данный интерфейс (физический или логический) для конкретного протокола будет создаваться лишь 1 сессия BFD. Эта сессия BFD должна быть привязана к данному интерфейсу. Таким образом, обе системы **должны** быть в роли активных (Active), передавая начальные пакеты BFD Control с Your Discriminator =0 и любой пакет BFD от удалённой машины с Your Discriminator = 0 **должен** ассоциироваться с сессией, привязанной к удалённой системе, интерфейсу и протоколу.

4. Инкапсуляция

Пакеты BFD Control **должны** передаваться в дейтаграммах UDP с портом получателя 3784 внутри пакетов IPv4 или IPv6. Порт отправителя **должен** быть из диапазона от 49152 до 65535. Для всех пакетов BFD Control, связанных с определённой сессией **должен** использоваться один порт отправителя UDP (source port). Для всех сессий BFD в системе **следует** выбирать уникальные номера портов. При одновременном использовании более 16384 сессий BFD номер порта UDP **можно** использовать в нескольких сессиях, но число сессий с одним номером порта **следует** минимизировать. Реализация **может** использовать номер порта отправителя UDP для демультиплексирования входящих пакетов BFD Control, но в конечном итоге для демультиплексирования пакетов в нужную сессию **должны** применяться механизмы [BFD].

Пакеты BFD Echo **должны** передаваться в дейтаграммах UDP с портом получателя 3785 внутри пакетов IPv4 или IPv6. Номер порта отправителя UDP эта спецификация не задаёт. Адрес получателя **должен** выбираться так, чтобы вызвать на удалённой системе пересылку пакета обратно в локальную систему. Адрес отправителя **должен** выбираться так, чтобы предотвратить генерацию удалённой системой сообщений ICMP или Neighbor Discovery Redirect. В частности адресу отправителя **не следует** быть частью подсети интерфейса, через который передаётся пакет BFD Echo, а также **не следует** быть адресом IPv6 link-local, пока нет уверенности (информации из других источников) в том, что удалённая система не будет передавать сообщений Redirect.

Пакеты BFD Echo **должны** передаваться так, чтобы гарантировать их получение удалённой системой. Например, в средах с множественным доступом это требует указания в качестве получателя адреса удалённой системы на канальном уровне.

Для выполнения приведённых выше требований возможно придётся обходить некоторые функции уровня IP, особенно в реализациях на хостах.

5. Проблемы TTL/Hop Limit

Если в сессии не применяется аутентификация BFD, все пакеты BFD Control в этой сессии **должны** передаваться со значением 255 в поле TTL или Hop Limit. Все полученные пакеты BFD Control, демультиплексируемые в сессию, **должны** отбрасываться, если TTL или Hop Limit отличается от 255. Описание механизма приведено в [GTSM].

Если в сессии применяется аутентификация BFD, все пакеты BFD Control **должны** передаваться со значением 255 в поле TTL или Hop Limit. Полученные пакеты BFD Control, демультиплексируемые в сессию, **могут** отбрасываться, если TTL или Hop Limit отличается от 255. При проверке TTL/Hop Limit она **может** выполняться до криптографической аутентификации, что позволяет избежать на приёмной стороне расчётов для пакетов, которые будут отброшены.

В контексте этого параграфа «использование аутентификации» означает передачу пакетов BFD Control с установленным битом Authentication, включающих Authentication Section, и отбрасывание всех демультиплексируемых в сессию пакетов, которые не были аутентифицированы (в соответствии с базовой спецификацией BFD).

6. Вопросы адресации

Реализации **должны** гарантировать передачу всех пакетов BFD Control по пути без маршрутизаторов (one-hop), защищённому BFD.

В сетях с множественным доступом пакеты BFD Control **должны** передаваться с адресами отправителя и получателя, относящимися к подсети (адресованные на интерфейсы подсети или отправленные из подсети).

На каналах «точка-точка» адрес отправителя пакета BFD Control **недопустимо** использовать для идентификации сессии. Это означает, что исходный пакет BFD **должен** восприниматься с любого адреса отправителя, а последующие пакеты BFD **должны** демультиплексироваться лишь по полю Your Discriminator (как обычно). Это позволяет при необходимости менять адрес отправителя. Если адрес отправителя в полученном пакете изменился, локальной системе **недопустимо** указывать его в качестве адреса получателя исходящих пакетов BFD Control, **должен** сохраняться адрес, заданный при создании сессии. Реализация **может** уведомить приложение о смене адреса соседа, чтобы приложение могло поменять адрес получателя или предпринять иные действия. Отметим, что проверка TTL/Hop Limit, описанная в разделе 5 (или применение аутентификации) предотвращает получение пакетов BFD от всех отправителей, кроме непосредственного соседа.

[1] Operations, Administration, and Maintenance - эксплуатация, администрирование и поддержка (управление).

7. BFD в туннеле

Имеется много механизмов для туннелирования IPv4 и IPv6 через произвольную топологию. Если туннельный механизм не декрементирует TTL или Hop Limit для сетевого протокола, в котором передаются пакеты, описанный в этом документе механизм может служить для проверки живучести туннеля. **Следует** применять механизм аутентификации BFD и это настоятельно рекомендуется.

8. Взаимодействие с IANA

Порты 3784 и 3875 выделены IANA для использования в пакетах BFD Control и BFD Echo, соответственно.

9. Вопросы безопасности

В этом варианте применения значение TTL=255[1] при передаче и получении пакетов в сочетании с привязкой к входному интерфейсу представляется обеспечивающим характеристики защиты, эквивалентные другим протоколам, используемым в инфраструктуре, поскольку подделка становится нетривиальной задачей. Влияние этого механизма на защиту рассматривается в [GTSM].

Влияние аутентификации BFD на защиту рассматривается в [BFD].

Использование проверки TTL=255 вместе с аутентификацией BFD обеспечивает снижение вычислительных издержек за счёт отбрасывания неаутентифицированных пакетов и может быть полезно в реализациях, где криптографическая контрольная сумма может быть подвержена атакам с отказом в обслуживании (denial-of-service). Использование этих механизмов (или отказ от них) не влияет на совместимость.

10. Литература

10.1. Нормативные документы

[BFD] Katz, D. and D. Ward, "Bidirectional Forwarding Detection", RFC 5880, June 2010.

[BFD-GENERIC] Katz, D. and D. Ward, "Generic Application of Bidirectional Forwarding Detection (BFD)", RFC 5882, June 2010.

[GTSM] Gill, V., Heasley, J., Meyer, D., Savola, P., Ed., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, October 2007.

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

10.2. Дополнительная литература

[BCP38] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[TFRC] Floyd, S., Handley, M., Padhye, J., and J. Widmer, "TCP Friendly Rate Control (TFRC): Protocol Specification", RFC 5348, September 2008.

Адреса авторов

Dave Katz
Juniper Networks
1194 N. Mathilda Ave.
Sunnyvale, CA 94089-1206
USA
Phone: +1-408-745-2000
EMail: dkatz@juniper.net

Dave Ward
Juniper Networks
1194 N. Mathilda Ave.
Sunnyvale, CA 94089-1206
USA
Phone: +1-408-745-2000
EMail: dward@juniper.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1] Очевидно, что в этом разделе авторы подразумевали TTL и Hop Limit. *Прим. перев.*