Internet Engineering Task Force (IETF)
Request for Comments: 8013
Category: Standards Track
ISSN: 2070-1721

D. Joachimpillai
Verizon
J. Hadi Salim
Mojatatu Networks

February 2017

Протокол ForCES - логические функциональные блоки между FE

Forwarding and Control Element Separation (ForCES) Inter-FE Logical Functional Block (LFB)

Аннотация

В этом документе описано, как расширить топологию логического функционального блока (Logical Functional Block или LFB) ForCES[1] за пределы элемента пересылки (Forwarding Element или FE) путём определения класса inter-FE LFB. Этот класс обеспечивает возможность передачи данных и метаданных через FE без изменения спецификации ForCES. Документ фокусируется на сетях Ethernet.

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/rfc8013.

Оглавление

[1]Forwarding and Control Element Separation - разделение элементов пересылки и управления.
[2]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[3]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

В архитектуре ForCES обслуживание пакетов можно смоделировать путём построения графа одного или множества экземпляров LFB. Подробности этого можно найти в спецификации модели ForCES [RFC5812].

Модель ForCES описывает обработку внутри одного элемента пересылки (FE) в терминах логических функциональных блоков (LFB), включая обеспечение элемента управления (CE[1]) для организации и изменения последовательности обработки и параметров отдельных LFB.

В некоторых случаях будет давать преимущества расширение этого представления для обработки, выполняемое множеством элементов FE. Это может служить для масштабирования путём распределения обработки между элементами или использования специального оборудования, имеющегося в определённых FE.

С учётом того, что архитектура ForCES inter-LFB требует возможности передавать метаданные между LFB, необходимо определить механизмы расширения имеющихся возможностей и обеспечения передачи метаданных между LFB в разных элементах FE.

В этом документе описано как расширить топологию LFB за пределы элемента FE, т. е. организовать связность между FE без изменения определений ForCES. В качестве среды для соединения элементов FE рассматривается Ethernet.

2. Термины и соглашения

2.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с [RFC2119].

2.2. Определения

Этот документ использует перечисленные ниже термины, которые определены в нескольких документах ForCES - [RFC3746], [RFC5810], [RFC5811], [RFC5812], [RFC7391], [RFC7408].

Control Element (CE) - элемент управления;
Forwarding Element (FE) - элемент пересылки;
FE Model - модель FE; LFB (Logical Functional Block) Class - класс (или тип) LFB; LFB Instance - экземпляр LFB; LFB Model - модель LFB; LFB Metadata - метаданные LFB; ForCES Component - компонента ForCES;
LFB Component - компонента LFB;
ForCES Protocol Layer (ForCES PL) - уровень протокола ForCES;
ForCES Protocol Transport Mapping Layer (ForCES TML) - уровень транспортного отображения ForCES.

3. Проблема и примеры её проявления

Назначением этого документа является решение вопроса передачи определённых протоколом ForCES метаданных вместе с данными пакета между физическими или виртуальными элементами FE для распределенной обработки LFB.

3.1. Допущения

- Элементы FE, вовлечённые в inter-FE LFB, относятся к одному элементу сети (NE[2]) и находятся в одной административно частной сети, что означает их близость.
- Элементы FE уже соединены между собой через сеть Ethernet. Этот выбор обусловлен широким распространением технологии Ethernet для организации соединений между FE. Для передачи данных и метаданных может быть определён другой транспорт вышележащего (типа UDP over IP) или нижележащего уровня, но эти случаи не рассматриваются в данном документе.

3.2. Простые случаи применения

Для иллюстрации проблемы здесь представлены два примера, которые начинаются с одного FE с полной функциональностью LFB, а затем расщепляются на множество FE для достижения той же цели.

3.2.1. Базовый маршрутизатор IPv4

Образец топологии LFB, представленный на рисунке 1, показывает граф обслуживания для базового сервиса пересылки IPv4 в рамках одного FE. На рисунке в качестве узлов графа показаны классы LFB, а не множество экземпляров класса LFB.

Поскольку целью рисунка 1 является демонстрация передачи данных и метаданных в нисходящем и восходящем направлении на графе экземпляров LFB, на нем не показаны какие-либо порты и упоминаются лишь базовые входные и выходные LFB, а также не указаны исключительные случаи и передача ошибок. Оставлены без внимания и детали Reverse Path Filtering, ECMP, обработки группового трафика и т. п. Иными словами, это не является полной иллюстрацией приложения для пересылки IPv4, более полное описание можно найти в документе, посвящённом LFBLibrary [RFC6956].

Вывод входных LFB, попадающий в IPv4 Validator LFB, будет включать пакеты IPv4 и (в зависимости от реализации) те или иные метаданные, типа смещений в разных заголовках, метаданных классификации, сведений о физических и виртуальных портах, данных о туннелировании и т. п. Эти данные совместно будем называть входными метаданными.

[1]Control Element.
[2]Network Element.

Как только проверка пакетов (например, пригодность значений TTL) валидатором IPv4 закончится, он передаёт пакеты в IPv4 unicast LPM[1] LFB.

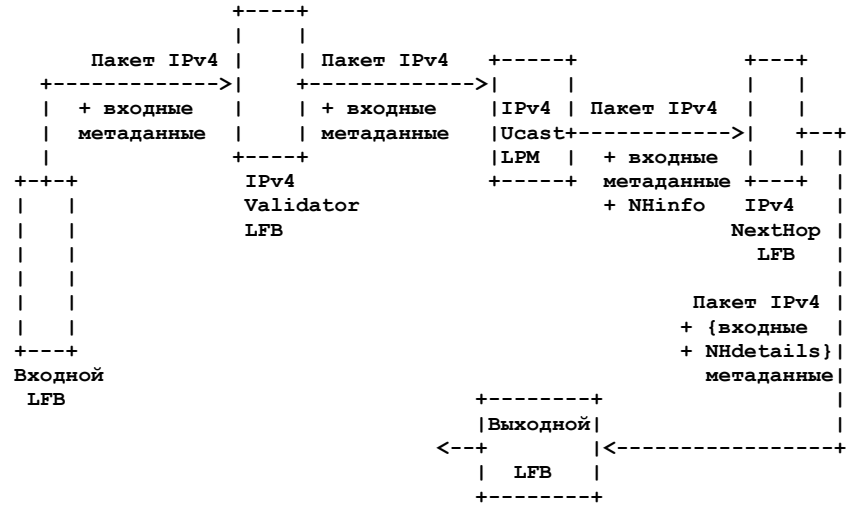

Рисунок 1. Топология LFB базового обслуживания пакетов IPv4.

Блок IPv4 unicast LPM LFB выполняет поиск LPM в таблице IPv4 FIB, используя IP-адрес получателя в качестве ключа поиска. Результатом обычно является селектор следующего интервала пересылки (next-hop) который передаётся в нисходящем направлении как метаданные.

Блок NextHop LFB получает пакет IPv4 со связанными с ним метаданными данными о следующем интервале NH[2]. Блок NextHop LFB принимает метаданные NH и выводит из них индекс для поиска в таблице next-hop с целью нахождения нужной информации о выходе. Результат поиска используется для определения деталей next-hop, которые будут применяться в нисходящем направлении на выходе. Эти данные могут включать любую информацию об отправителе и получателе (в нашем случае адреса MAC[3]), а также выходной порт[4].

Рассмотрение деталей выходного LFB выходит за рамки нашего обсуждения. Достаточно отметить, что в этом блоке или около него пакет IPv4 будет передан в выходной порт (например, физический или виртуальный порт Ethernet).

3.2.1.1. Распределенный базовый маршрутизатор IPv4

На рисунке 2 показано, что топологию LFB маршрутизатора с рисунка 1 можно разделить между двумя элементами FE (например, два контроллера ASIC[5]). На рисунке 2 изображена топология LFB разделённая между двумя FE после IPv4 unicast LPM LFB.

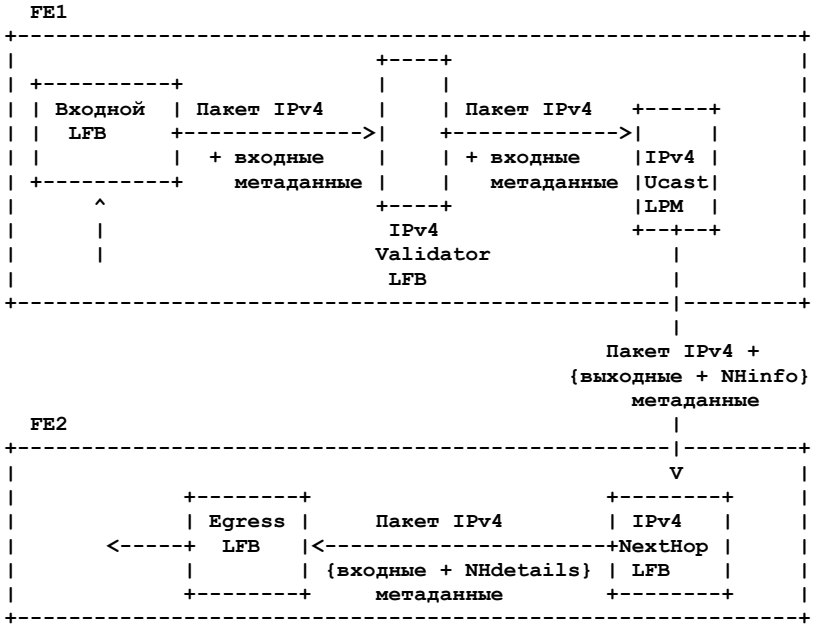

Рисунок 2. Расщепление топологии LFB для обслуживания пакетов IPv4.

Некоторые фирменные технологии организации соединений (например, Broadcom HiGig over XAUI [brcm-higig]) позволяют передавать пакет IPv4 и связанные с ним метаданные между IPv4 Unicast LFB и IPv4NextHop LFB через два FE.

Этот документ определяет inter-FE LFB - стандартный механизм для инкапсуляции, генерации, приёма и декапсуляции пакетов и связанных с ними метаданных FE через соединения Ethernet.

[1]Longest-Prefix-Matching - максимальный размер соответствия префикса.
[2]Next-hop.
[3]Media Access Control - управление доступом к среде передачи.
[4]В этом LFB обычно выполняется также декрементирование TTL и пересчет контрольной суммы IP.
[5]Application-Specific Integrated Circuit - специализированная микросхема.

3.2.2. Произвольная сетевая функция

В этом параграфе будет показан пример произвольной сетевой функции NF[1] без какой-либо детализации. Каждая такая функция может включать более одного блока LFB.

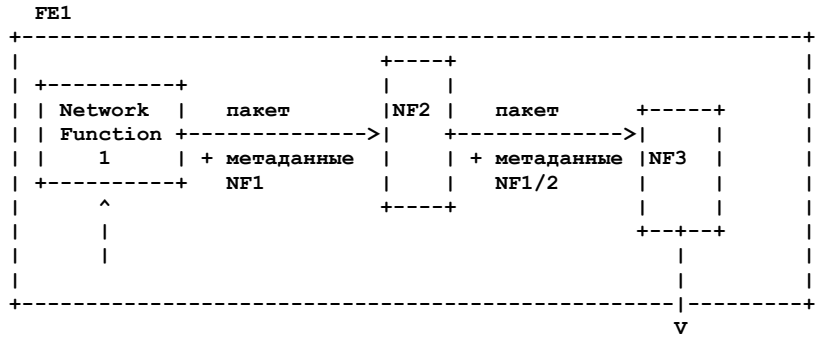

Рисунок 3. Цепочка сетевых функций внутри одного FE.

Пример на рисунке 3 типичен для большинства устройств обработки пакетов, где имеются функции типа глубокой инспекции пакетов (DPI[2]), NAT, маршрутизации и т. п., соединённых в цепочку для обработки пакетов в потоках.

3.2.2.1. Распределенная произвольная сетевая функция

Цепочку функций на рисунке 3 можно разделить между тремя FE как показано на рисунке 4. Мотивом такого разделения может быть масштабирование или реализация функций в устройствах разных производителей. Конечным результатом будет однотипное обслуживание пакетов разных потоков, проходящих через цепочку.

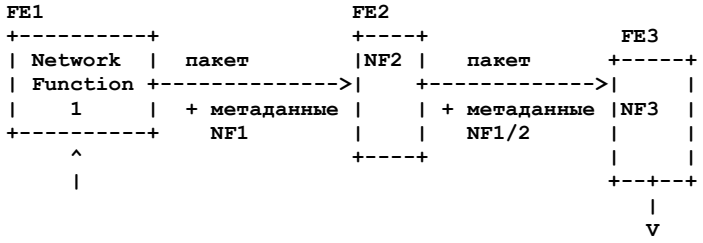

Рисунок 4. Цепочка сетевых функций в нескольких FE.

4. Обзор Inter-FE LFB

Требования связности между FE выполняются с помощью определения класса inter-FE LFB. Использование определения стандартного класса LFB предполагает отсутствие изменений, вносимых в архитектуру ForCES в части базовых LFB (FE Protocol или Object LFB). Это решение было принято после рассмотрения альтернативного варианта, который требовал изменения возможностей FE Object (SupportedLFBs) и компоненты LFBTopology для описания возможностей связности между FE, а также рабочей топологии экземпляров LFB.

4.1. Вставка Inter-FE LFB ne 15

Топология распределенного блока LFB, показанная на рисунке 2, заново представлена на рисунке 5 для демонстрации inter-FE LFB.

Как можно видеть на рисунке 5, та же информация передаётся между IPv4 unicast LPM LFB и IPv4 NH LFB на выходную сторону inter-FE LFB. Эта информация представлена как множество вводов в выходной экземпляр inter-FE LFB. Каждый ввод представляет уникальный набор информации о выборе.

На выходе inter-FE LFB принятый пакет и метаданные используются для выбора деталей инкапсуляции при передаче сообщений в направлении выбранного соседнего FE. Эти детали включают включают в себя указание передающего и принимающего FE (абстрагируются как адреса MAC в соответствии с параграфом 5.2), могут передаваться также метаданные, пришедшие вместе с исходным пакетом IPv4.

На входной стороне inter-FE LFB полученный пакет и связанные с ним метаданные служат для того, чтобы определить продолжение графа. Это включает выбор исходных метаданных и следующего экземпляра класса LFB для продолжения обработки. На рисунке 5 выбран экземпляр IPv4NextHop LFB и метаданные для передачи этому блоку.

Входная сторона inter-FE LFB использует часть переданной информации и передаёт пакет IPv4 вместе с входными метаданными и NHinfo блоку IPv4NextHop LFB как это делалось раньше на рисунках 1 и 2.

[1]Network Function.
[2]Deep packet inspection.

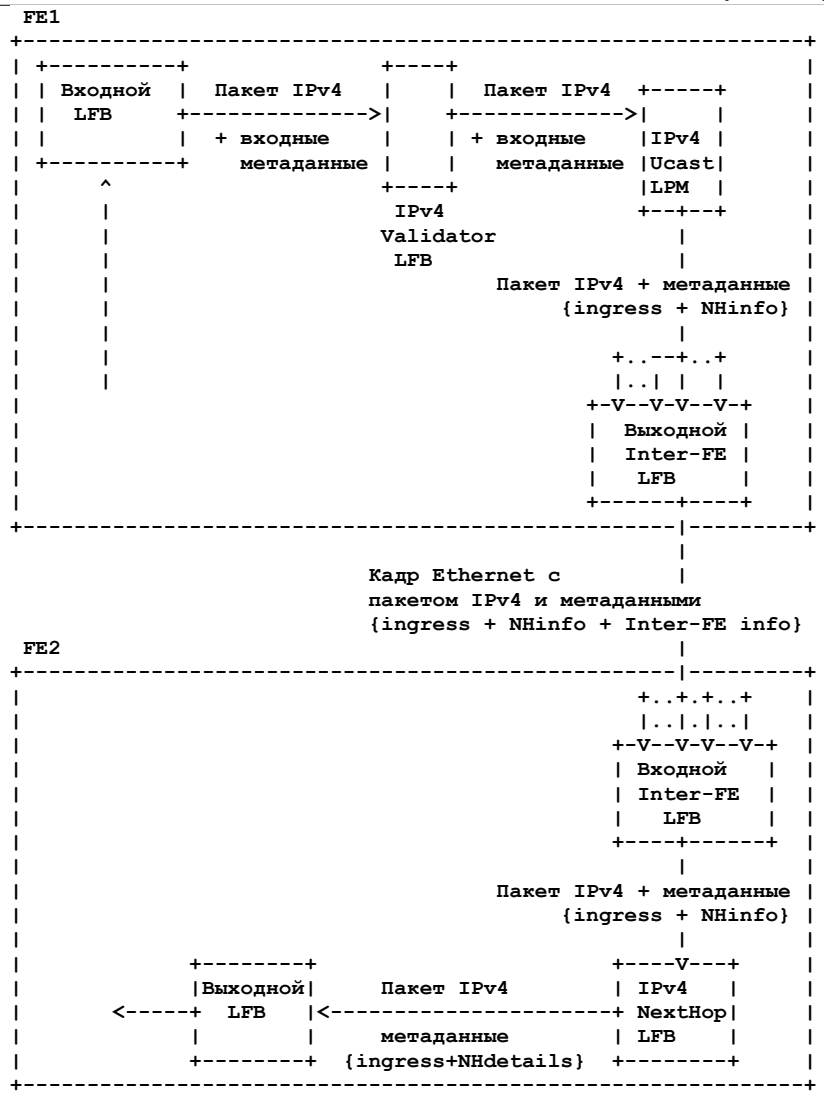

Рисунок 5. Расщепление сервиса пересылки IPv4 с помощью Inter-FE LFB.

5. Связность Inter-FE Ethernet

В параграфе 5.1 рассмотрены некоторые вопросы, связанные с использованием Ethernet в качестве транспорта, и способы смягчения проблем.

В параграфе 5.2 определён формат данных для передачи через Ethernet. Имеющиеся реализации данной спецификации, работающие на основе Linux Traffic Control [linux-tc], описаны в [tc-ife].

5.1. Проблемы связности Inter-FE Ethernet

Нужно рассмотреть несколько проблем, которые могут возникать при непосредственной инкапсуляции Ethernet.

5.1.1. Проблема MTU

В результате добавления данных к существующим кадрам Ethernet может возникать проблема MTU. Меры предотвращения приведены ниже.

- Использование больших MTU когда это возможно (например, кадров jumbo).
- Ограничения объёма метаданных, которые могут быть переданы. Наше определение позволяет фильтровать выбранные метаданные для инкапсуляции в кадр, как описано в разделе 6. Рекомендуется определять размер MTU выходного порта так, чтобы обеспечить включение метаданных максимального размера для передачи между FE. В такой конфигурации порт настраивается на «обман» вышележащих уровней путём заявления им значения MTU, которое меньше реального. Установка MTU может быть выполнена с помощью управления ForCES для LFB порта (или иным способом). Фактически при явном определении уровнем управления значения MTU для выходного порта неявно задаётся объем метаданных, которые можно будет передать. При выборе значения MTU следует быть осторожным - для пакетов IPv4 минимальный размер составляет 64 октета [RFC791], а для IPv6 - 1280 октетов [RFC2460].

5.1.2. Вопросы качества обслуживания

Необработанный (raw) пакет, прибывающий на интерфейс inter-FE LFB (от экземпляра восходящего LFB) может иметь метаданные класса обслуживания (CoS[1]) показывающие, как следует трактовать пакет с точки зрения качества обслуживания (QoS[2]).

[1]Class-of-Service.
[2]Quality-of-Service.

Результирующий кадр Ethernet будет в конечном итоге (предпочтительно) трактоваться нисходящим LFB (обычно экземпляр LFB для порта) и его маркировка CoS будет выполняться с точки зрения приоритета. Иными словами, наличие inter-FE LFB не меняет семантики CoS.

5.1.3. Проблемы перегрузок

Предполагается, что большая часть проходящего через FE трафика, который использует inter-FE LFB, будет относиться к протоколу IP и в общем случае для него будет поддерживаться контроль насыщения [UDP-GUIDE]. Например, если перегрузка вызовет отбрасывание пакета TCP с дополнительными метаданными ForCES между элементами FE, можно надеяться, что передающий узел TCP отреагирует на это так же, как при отбрасывании пакета в другой точке, где не используется протокол ForCES. Поэтому дополнительные механизмы контроля насыщения между элементами FE не задаются.

Однако рост размера пакетов в результате добавления метаданных ForCES явно потребует дополнительной пропускной способности в каналах между FE по сравнению с передачей того же трафика без метаданных ForCES. Поэтому при использовании инкапсуляции inter-FE **следует** реализовать организацию трафика.

Кроме того, блоки inter-FE LFB **должны** разворачиваться только в рамках одной сети (с одним оператором) или в сетях смежных взаимодействующих операторов, где обеспечивается совместное предотвращение перегрузок. Это считается управляемой средой (Controlled Environment) в соответствии с определением параграфа 3.6 [UDP-GUIDE]. **Следует** принимать дополнительные меры по ограничению влияния трафика с инкапсуляцией inter-FE на иной трафик типа перечисленных ниже:

- ограничение скорости всего трафика inter-FE LFB на восходящем LFB;
- управление прерыванием цепей [circuit-b];
- изоляция трафика inter-FE с помощью выделенных интерфейсов или VLAN.

5.2. Инкапсуляция Inter-FE Ethernet

Инкапсуляция в линии Ethernet показана на рисунке 6, а приводящий к ней процесс описан в разделе 6. Кадр выравнивается по 32-битовой границе.

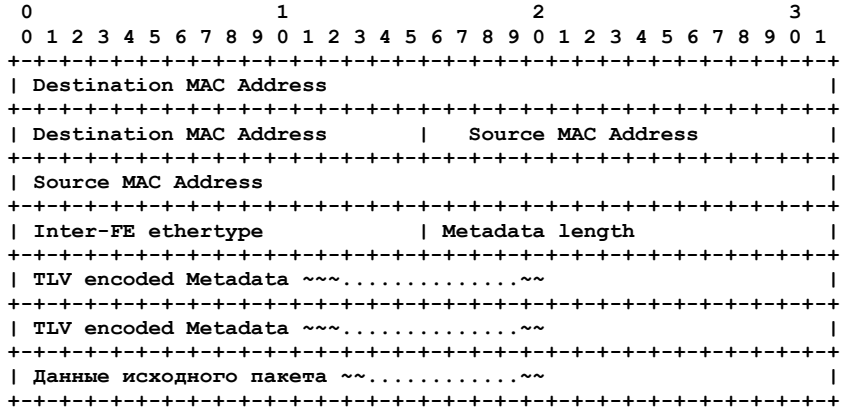

Рисунок 6. Формат пакета.

Назначение полей заголовка Ethernet (рисунок 6) кратко описано ниже.

- Destination MAC Address используется для указания Destination FEID по политике CE (см. раздел 6).
- The Source MAC Address используется для указания Source FEID по политике CE (см. раздел 6).
- Поле ethertype служит для идентификации кадра как inter-FE LFB (шестнадцатеричное значение ED3E).
- 16-битовое поле Metadata length указывает общий размер метаданных (включая само поле размера).
- Один или множество 16-битовых блоков TLV с метаданными следуют за полем Metadata length. Тип TLV указывает идентификатор метаданных. Будут использоваться идентификаторы метаданных ForCES, зарегистрированные в IANA. Все TLV выравниваются по 32-битовой границе. Понятно, что применение 16-битовых TLV ограничивает размер идентификаторов метаданных 16 битами вместо определённых в ForCES 32 битовых идентификаторов компонент при использовании ILV[1]. Однако на момент публикации этого документа 16-битовое пространство кажется достаточным, а модель TLV выбрана благодаря обеспечиваемой ею экономии 4 байтов на единицу метаданных по сравнению с использованием ILV.
- Данные исходного пакета размещаются после метаданных, как показано на рисунке 6.

6. Подробное описание Ethernet Inter-FE LFB

Ethernet inter-FE LFB имеет два блока LFB для групп входных портов и три LFB выходных портов (см. рисунок 7).

Блок inter-FE LFB определяет две компоненты, поддерживающие обработку, описанную в параграфе 6.1.

6.1. Обработка данных

Экземпляр inter-FE LFB может быть размешен на выходе FE-источника. На рисунке 5 показан пример FE-источника FE1. В таком случае экземпляр inter-FE LFB получает через группу портов EgressInGroup необработанный пакет и связанные с ним метаданные от предшествующих экземпляров LFB. Входная информация служит для выбора способа генерации и инкапсуляции нового кадра. Набор всех вариантов хранится в LFB-компоненте IFETable, описанной ниже.

[1]Index-Length-Value.

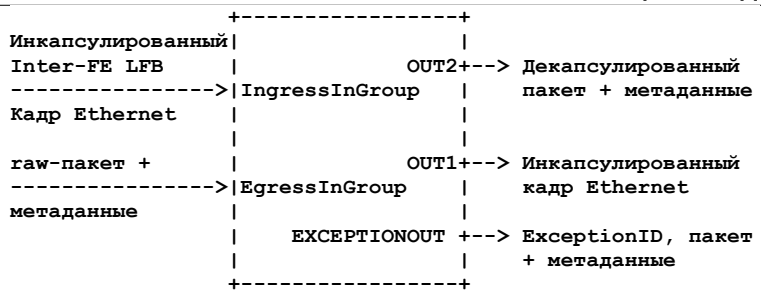

Рисунок 7. Inter-FE LFB.

Обработанный инкапсулированный кадр Ethernet передаётся через OUT1 нисходящему экземпляру LFB при завершении обработки или в порт EXCEPTIONOUT при возникновении отказа.

Экземпляр inter-FE LFB может быть размешен на входе принимающего FE. На рисунке 5 показан пример FE-получателя FE2[1]. В таком случае inter-FE LFB получает через порт LFB в группе IngressInGroup инкапсулированный кадр Ethernet. Успешная обработка пакета будет приводить к отправке raw-пакета и связанных с ним метаданных блоку LFB, подключённому к порту OUT2. При отказе данные передаются в EXCEPTIONOUT.

6.1.1. Выходная обработка

Выходной блок inter-FE LFB получает пакет и связанные с ним метаданные на порту LFB группы входных портов экземпляра LFB, помеченной EgressInGroup.

Реализация LFB может использовать входной порт LFB (в группе EgressInGroup) для отображения на индекс таблицы, используемый для поиска в IFETable.

Если поиск завершился успехом, соответствующая строка таблицы с данными IFEInfo извлекается в форме кортежа (необязательные IFETYPE и StatId, DSTFE[2], SRCFE [3] и необязательные метафильтры). Списки метафильтров определяют «белый» список метаданных для передачи соседнему FE. Блок inter-FE LFB будет выполнять с помощью полученного кортежа перечисленные ниже действия.

- Увеличение значений счётчиков пакетов и байтов в соответствующей записи IFEStats.
- При наличии MetaFilterList применяются фильтры ко всем полученным метаданным. Если подходящих данных для передачи в нисходящем направлении не найдено, обработка завершается и пакет вместе с метаданными передаётся в порт EXCEPTIONOUT с exceptionID = EncapTableLookupFailed [RFC6956].
- Проверка размера дополнительных данных в заголовке кадре Ethernet и инкапсулированных данных на предмет соответствия MTU. Если размер превышен, увеличивается значение счётчика пакетов с ошибками, а пакет и метаданные передаются в порт EXCEPTIONOUT с exceptionID = EncapTableLookupFailed [RFC6956].
- Создание заголовка Ethernet.
- Установка адреса Destination MAC в заголовке Ethernet в соответствии со значением поля DSTFE.
- Установка адреса Source MAC в заголовке Ethernet в соответствии со значением поля SRCFE.
- При наличии поля IFETYPE установка для поля ethertype значения из IFETYPE. При отсутствии IFETYPE используется стандартное для inter-FE LFB шестнадцатеричное значение ethertype ED3E.
- Инкапсуляция всех разрешённых метаданных в TLV с использованием metaID в качестве поля типа в заголовке TLV. Блоки TLV следует выравнивать по 32-битовым границам путём добавления нулей в конце.
- Обновление размера метаданных с учётом суммарного размера TLV + 2 байта (размер поля Metadata length).

Полученный пакет передаётся следующему экземпляру LFB, подключённому к LFB-порту OUT1.

Если поиск не дал результата, исходный пакет и связанные с ним метаданные передаются в порт EXCEPTIONOUT с exceptionID = EncapTableLookupFailed [RFC6956]. Отметим, что порт EXCEPTIONOUT LFB является абстракцией и реализация может просто отбрасывать соответствующие пакеты.

6.1.2. Входная обработка

Входящий пакет inter-FE LFB распознаётся по полю ethertype и опционально по MAC-адресам отправителя и получателя. Соответствующие пакеты отображаются на порт экземпляра LFB в группе IngressInGroup. Запись таблицы IFETable, соответствующая порту экземпляра LFB, может иметь фильтры метаданных. В таком случае входная обработка должна применять эти фильтры в качестве «белого» списка для выделения разрешённых метаданных.

- Увеличение значений счётчиков пакетов и байтов.
- В соответствии со значением поля Metadata length извлекаются значения метаданных из TLV. Для каждого блока при наличии фильтров значение metaID сравнивается со списком соответствующей строки IFETable. Если фильтр разрешает метаданные, устанавливается соответствующее поле метаданных. Если встречается неизвестный идентификатор метаданных или фильтр не разрешает metaID, предполагается, что реализация игнорирует их, увеличивает значение счётчика пакетов с ошибками и обрабатывает другие метаданные.
- По завершении обработки всех метаданных экземпляр inter-FE LFB переходит к данным исходного пакета (пропускает заголовок IFE). В этот момент восстанавливается исходный пакет, переданный выходному inter-FE

[1]В оригинале ошибочно сказано FE1, см. http://www.rfc-editor.org/errata/eid5358. *Прим. перев.*
[2]Destination MAC address.
[3]Source MAC address.

LFB в FE-источнике. Этот пакет вместе с восстановленными метаданными передаётся в нисходящем направлении следующему экземпляру LFB на графе.

При отказе в процессе обработки на входном или выходном LFB пакет и метаданные передаются в порт EXCEPTIONOUT с соответствующим кодом ошибки. Отметим, что порт EXCEPTIONOUT LFB является абстракцией и реализация может просто отбрасывать соответствующие пакеты, как отмечено выше.

6.2. Компоненты

Имеется две компоненты LFB, к которым обращается CE (см. определения в разделе 8).

Первой компонентой, которая заполняется элементом CE, является массив, называемый таблицей IFETable. Строки массива являются структурами IFEInfo. Каждая структура IFEInfo включает необязательные поля IFETYPE и StatId, MAC-адрес получателя (DSTFE), MAC-адрес отправителя (SRCFE) и необязательный массив разрешённых metaID (MetaFilterList).

Вторая компонента (ID 2) заполняется элементом FE и считывается CE - это индексированный массив, называемый таблицей IFEStats. Каждая строка IFEStats содержит статистические данные в структуре bstats.

Отметим, что StatId указывает связи между IFETable и IFEStats - реализация может создать отображение между строками IFETable и IFEStats, используя поле StatId в соответствующей строке IFETable. В этом случае в строке IFETable должно присутствовать поле StatId. Другие реализации могут отображать строки IFETable на строки IFEStats во время подготовки. Ещё одним вариантом реализации является отказ от указания StatId в IFETable и использование строки IFETable в качестве индекса IFEStats. Поэтому поле StatId является необязательным.

6.3. Модель XML для Inter-FE LFB

```
<LFBLibrary xmlns="urn:ietf:params:xml:ns:forces:lfbmodel:1.1"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       provides="IFE">
  <frameDefs>
     <frameDef>
         <name>PacketAny</name>
          <synopsis>Произвольный пакет</synopsis>
     </frameDef>
     <frameDef>
         <name>InterFEFrame</name>
         <synopsis>Кадр Ethernet с инкапсулированными данными IFE</synopsis>
     </frameDef>
  </frameDefs>

  <dataTypeDefs>
    <dataTypeDef>
       <name>bstats</name>
       <synopsis>Базовая статистика</synopsis>
    <struct>
        <component componentID="1">
         <name>bytes</name>
         <synopsis>Общее число просмотренных байтов</synopsis>
         <typeRef>uint64</typeRef>
        </component>

        <component componentID="2">
         <name>packets</name>
         <synopsis>Общее число просмотренных пакетов</synopsis>
         <typeRef>uint32</typeRef>
        </component>

        <component componentID="3">
         <name>errors</name>
         <synopsis>Общее число пакетов с ошибками</synopsis>
         <typeRef>uint32</typeRef>
        </component>
    </struct>
   </dataTypeDef>

     <dataTypeDef>
        <name>IFEInfo</name>
        <synopsis>Описание информации строки таблицы IFE</synopsis>
        <struct>
           <component componentID="1">
             <name>IFETYPE</name>
             <synopsis>ethertype для исходящего кадра IFE</synopsis>
             <optional/>
             <typeRef>uint16</typeRef>
           </component>
           <component componentID="2">
             <name>StatId</name>
             <synopsis>Индекс таблицы статистики</synopsis>
             <optional/>
             <typeRef>uint32</typeRef>
           </component>
           <component componentID="3">
             <name>DSTFE</name>
             <synopsis>MAC-адрес получателя целевого FE</synopsis>
```

```
            <typeRef>byte[6]</typeRef>
          </component>
          <component componentID="4">
            <name>SRCFE</name>
            <synopsis>MAC-адрес отправителя FE-источника</synopsis>
            <typeRef>byte[6]</typeRef>
          </component>
          <component componentID="5">
            <name>MetaFilterList</name>
            <synopsis>Таблица фильтров разрешённых метаданных</synopsis>
            <optional/>
            <array type="variable-size">
              <typeRef>uint32</typeRef>
            </array>
           </component>
        </struct>
    </dataTypeDef>
  </dataTypeDefs>

  <LFBClassDefs>
    <LFBClassDef LFBClassID="18">
      <name>IFE</name>
      <synopsis>Этот LFB описывает параметры связности IFE</synopsis>
      <version>1.0</version>

        <inputPorts>
          <inputPort group="true">
           <name>EgressInGroup</name>
           <synopsis>
                   Группа входных портов на выходной стороне.
                   Она ожидает кадры Ethernet любого типа.
           </synopsis>
           <expectation>
                <frameExpected>
                <ref>PacketAny</ref>
                </frameExpected>
           </expectation>
          </inputPort>

          <inputPort  group="true">
           <name>IngressInGroup</name>
           <synopsis>
                   Группа входных портов на входной стороне.
                   Она ожидает кадры Ethernet с инкапсуляцией interFE.
            </synopsis>
           <expectation>
                <frameExpected>
                <ref>InterFEFrame</ref>
                </frameExpected>
           </expectation>
         </inputPort>
        </inputPorts>

        <outputPorts>
          <outputPort>
            <name>OUT1</name>
            <synopsis>Выходной порт на выходной стороне</synopsis>

            <product>
               <frameProduced>
                 <ref>InterFEFrame</ref>
               </frameProduced>
            </product>
         </outputPort>

         <outputPort>
           <name>OUT2</name>
            <synopsis>Выходной порт на входной стороне</synopsis>
           <product>
              <frameProduced>
                <ref>PacketAny</ref>
              </frameProduced>
           </product>
        </outputPort>

        <outputPort>
          <name>EXCEPTIONOUT</name>
          <synopsis>Путь обработки исключений</synopsis>
          <product>
             <frameProduced>
               <ref>PacketAny</ref>
             </frameProduced>
             <metadataProduced>
               <ref>ExceptionID</ref>
             </metadataProduced>
          </product>
```

```
        </outputPort>
     </outputPorts>

     <components>
        <component componentID="1" access="read-write">
           <name>IFETable</name>
           <synopsis>Таблица всех связей inter-FE</synopsis>
           <array type="variable-size">
              <typeRef>IFEInfo</typeRef>
           </array>
        </component>

       <component componentID="2" access="read-only">
         <name>IFEStats</name>
         <synopsis>Статистика, соответствующая таблице IFETable</synopsis>
         <typeRef>bstats</typeRef>
       </component>
     </components>
   </LFBClassDef>
  </LFBClassDefs>

  </LFBLibrary>
```

Рисунок 8. Inter-FE LFB XML.

7. Взаимодействие с IANA

Агентство IANA зарегистрировало приведённое в таблице имя класса LFB в субреестре Logical Functional Block (LFB) Class Names and Class Identifiers реестра Forwarding and Control Element Separation (ForCES) <https://www.iana.org/assignments/forces>.

Имя и идентификатор класса LFB.

Идентификатор класса	Имя класса LFB	Версия LFB	Описание	Документ
18	IFE	1.0	Блок IFE LFB служит для стандартизации inter-FE LFB в сетевых элементах ForCES	RFC 8013

8. Взаимодействие с IEEE

Этот документ включает запрос на выделение нового значения протокола Ethernet, как указано в параграфе 5.2.

9. Вопросы безопасности

Элементы FE, вовлечённые в inter-FE LFB, относятся к одному NE и находятся в частной ЛВС Ethernet с единым администрированием. Несмотря на наличие доверия к политике управления и её трактовке в пути данных, реализациям inter-FE LFB **следует** поддерживать услуги защиты, обеспечиваемые MACsec[1] [ieee8021ae]. Методы MACsec пока недостаточно распространены в традиционном оборудовании для обработки пакетов, хотя они имеются в новых версиях ядра Linux kernel (распространённого достаточно широко) [linux-macsec]. Ожидается, что со временем большинство FE будут поддерживать MACsec.

MACsec обеспечивает услуги защиты типа аутентификации сообщений и необязательной защиты конфиденциальности. Эти услуги можно настраивать вручную или автоматически с помощью MKA[2] на основе модели IEEE 802.1x [ieee8021x] EAP[3]. Ожидается, что реализации FE начнут с использования на уровне управления общих ключей, а затем перейдут к автоматическому управления ключами.

Ниже перечислены механизмы MACsec, которые нужны для inter-FE LFB.

- Механизмы защиты в масштабе NE для всех элементов FE. После включения защиты в зависимости от выбранного уровня (например, аутентификация и конфиденциальность) эти услуги будут действовать для inter-FE LFB в течение всей сессии.
- Операторам **следует** задавать одинаковые правила безопасности для всех участвующих элементов FE в кластере NE. Это обеспечит единообразие действий и позволит избавиться от ненужных сложностей при настройке политики. Иными словами, ключи SAK[4] следует распространять заранее. При использовании MKA элементы FE должны идентифицировать себя с помощью ключей CAK[5] и их имён CKN[6]. В качестве метода EAP **следует** использовать EAP-TLS.
- Операторам **следует** задавать строгий режим проверки, при котором все незащищённые или непроверяемые кадры **должны** отбрасываться.

Следует отметить, что с учётом приведённых выше вариантов компрометация FE позволит объекту, работающему в этом FE, создавать обманные inter-FE или менять их содержимое, что приведёт к нежелательным результатам.

10. Литература

10.1. Нормативные документы

[ieee8021ae] IEEE, "IEEE Standard for Local and metropolitan area networks Media Access Control (MAC) Security", IEEE 802.1AE-2006, DOI 10.1109/IEEESTD.2006.245590, <http://ieeexplore.ieee.org/document/1678345/>.

[1]Media Access Control Security.
[2]MACsec Key Agreement - согласование ключей MACsec.
[3]Extensible Authentication Protocol - расширяемый протокол аутентификации.
[4]Security Association Key - ключ защищённой связи.
[5]Connectivity Association Key - ключ ассоциации связности.
[6]Connectivity Association Key Name - имя ключа ассоциации связности.

[ieee8021x] IEEE, "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control.", IEEE 802.1X-2010, DOI 10.1109/IEEESTD.2010.5409813, <http://ieeexplore.ieee.org/document/5409813/>.

[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>.

[RFC5810] Doria, A., Ed., Hadi Salim, J., Ed., Haas, R., Ed., Khosravi, H., Ed., Wang, W., Ed., Dong, L., Gopal, R., and J. Halpern, "Forwarding and Control Element Separation (ForCES) Protocol Specification", RFC 5810, DOI 10.17487/RFC5810, March 2010, <http://www.rfc-editor.org/info/rfc5810>.

[RFC5811] Hadi Salim, J. and K. Ogawa, "SCTP-Based Transport Mapping Layer (TML) for the Forwarding and Control Element Separation (ForCES) Protocol", RFC 5811, DOI 10.17487/RFC5811, March 2010, <http://www.rfc-editor.org/info/rfc5811>.

[RFC5812] Halpern, J. and J. Hadi Salim, "Forwarding and Control Element Separation (ForCES) Forwarding Element Model", RFC 5812, DOI 10.17487/RFC5812, March 2010, <http://www.rfc-editor.org/info/rfc5812>.

[RFC7391] Hadi Salim, J., "Forwarding and Control Element Separation (ForCES) Protocol Extensions", RFC 7391, DOI 10.17487/RFC7391, October 2014, <http://www.rfc-editor.org/info/rfc7391>.

[RFC7408] Haleplidis, E., "Forwarding and Control Element Separation (ForCES) Model Extension", RFC 7408, DOI 10.17487/RFC7408, November 2014, <http://www.rfc-editor.org/info/rfc7408>.

10.2. Дополнительная литература

[brcm-higig] Broadcom, "HiGig", <http://www.broadcom.com/products/ethernet-communication-and-switching/switching/bcm56720>.

[circuit-b] Fairhurst, G., "Network Transport Circuit Breakers", Work in Progress, draft-ietf-tsvwg-circuit-breaker-15[1], April 2016.

[linux-macsec] Dubroca, S., "MACsec: Encryption for the wired LAN"[2], Netdev 11, Feb 2016.

[linux-tc] Hadi Salim, J., "Linux Traffic Control Classifier-Action Subsystem Architecture"[3], Netdev 01, Feb 2015.

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <http://www.rfc-editor.org/info/rfc791>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC3746] Yang, L., Dantu, R., Anderson, T., and R. Gopal, "Forwarding and Control Element Separation (ForCES) Framework", RFC 3746, DOI 10.17487/RFC3746, April 2004, <http://www.rfc-editor.org/info/rfc3746>.

[RFC6956] Wang, W., Haleplidis, E., Ogawa, K., Li, C., and J. Halpern, "Forwarding and Control Element Separation (ForCES) Logical Function Block (LFB) Library", RFC 6956, DOI 10.17487/RFC6956, June 2013, <http://www.rfc-editor.org/info/rfc6956>.

[tc-ife] Hadi Salim, J. and D. Joachimpillai, "Distributing Linux Traffic Control Classifier-Action Subsystem"[4], Netdev 01, Feb 2015.

[UDP-GUIDE] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage Guidelines", Work in Progress[5], draft-ietf-tsvwg-rfc5405bis-19, October 2016.

Благодарности

Авторы благодарны Joel Halpern и Dave Hood за плодотворные дискуссии. Evangelos Haleplidis много сделал для улучшения этого документа. Alia Atlas был AD-спонсором этого документа и внес множество критических замечаний. Авторы признательны Joel Halpern и Sue Hares, которые в роли рецензентов от Routing Area помогли сформировать содержимое этого документа. David Black приложил значительные усилия по проверке разумности решения в части контроля перегрузок. Russ Housley подготовил обзор Gen-ART, Joe Touch - обзор TSV, а Shucheng LIU (Will) - обзор OPS. Suresh Krishnan помог при рецензировании IESG. Авторы благодарны Stephen Farrell за его усилия по подготовке раздела, посвящённого безопасности.

Адреса авторов

Damascane M. Joachimpillai

Verizon

60 Sylvan Rd

Waltham, MA 02451

United States of America

Email: damascene.joachimpillai@verizon.com

Jamal Hadi Salim

[1]Работа опубликована в RFC 8084. *Прим. перев.*
[2]Статья доступна по ссылке. *Прим. перев.*
[3]Статья доступна по ссылке. *Прим. перев.*
[4]Статья доступна по ссылке. *Прим. перев.*
[5]Работа опубликована в RFC 8085. *Прим. перев.*

Mojatatu Networks

Suite 200, 15 Fitzgerald Rd.

Ottawa, Ontario K2H 9G1

Canada

Email: hadi@mojatatu.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru