Internet Engineering Task Force (IETF)
Request for Comments: 8655
Category: Standards Track
ISSN: 2070-1721

N. Finn
Huawei
P. Thubert
Cisco
B. Varga
J. Farkas
Ericsson

October 2019

Deterministic Networking Architecture

Архитектура детерминированых сетей

Аннотация

В этом документе описана базовая архитектура детерминированных сетей (DetNet[1]), обеспечивающая возможность передачи конкретного группового и индивидуального трафика приложений, работающих в реальном масштабе времени, с минимальными потерями и ограниченной задержкой внутри сетевого домена. Используемые методы включают 1) резервирование ресурсов плоскости данных для индивидуальных (или агрегированных) потоков DetNet на некоторых или всех промежуточных узлах пути, 2) обеспечение явных маршрутов для потоков, которые не меняются сразу при изменении топологии сети, и 3) распределение данных из пакетов потока DetNet во времени и/или пространстве для обеспечения доставки каждого пакета, несмотря на потери в пути. DetNet работает на уровне IP и предоставляет услуги на основе технологий нижележащих уровней, таких как MPLS и TSN[2] (IEEE 802.1).

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[3] и представляет согласованный взгляд сообщества IETF. Документ прошел открытое обсуждение и был одобрен для публикации IESG[4]. 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 https://www.rfc-editor.org/info/rfc8655.

Оглавление

[1]Deterministic Networking.
[2]Time-Sensitive Networking - чувствительные ко времени сети.
[3]Internet Engineering Task Force.
[4]Internet Engineering Steering Group.

1. Введение

В документе представлена архитектура детерминированных сетей DetNet, которая обеспечивает возможность доставки потоков данных с очень низкими потерями пакетов и ограниченной сквозной задержкой. Архитектура DetNet предназначена для сетей с единым администрированием или управляемых тесно связанными администраторами, включая кампусные сети и частные сети WAN. DetNet не рассчитана на большие группы доменов, такие как Internet.

DetNet работает на уровне IP и обеспечивает услуги на основе технологий нижележащих уровней, таких как MPLS и IEEE 802.1 TSN. DetNet обеспечивает надежные и доступные услуги путем выделения сетевых ресурсов (таких как пропускная способность каналов и буферное пространство) для потоков DetNet и/или классов потоков, а также репликации пакетов в несколько путей. Не занятые резервы ресурсов доступны для прочего (не DetNet) трафика, если гарантии соблюдены.

Документ Deterministic Networking Problem Statement [RFC8557] является введением в DetNet, а в Deterministic Networking Use Cases [RFC8578] обоснована потребность в архитектуре. Конкретные методы идентификации потоков DetNet и назначения им определенных путей через сеть рассмотрены в [DETNET-FRAMEWORK].

Целью DetNet является создание конвергентных сетей, включая объединение критичных сетей без протокола IP в общую сетевую инфраструктуру. Присутствие потоков DetNet не мешает другим потокам, а преимущества потоков DetNet в большинстве случаев не должны препятствовать нормальной работе имеющихся механизмов QoS[1] если для потоков DetNet достаточно пропускной способности. Для данной пары отправитель-получатель могут поддерживаться одновременно DetNet и иные потоки. Конечным системам и приложениям не требуются специальные интерфейсы для потоков DetNet. Сети не привязаны к определенной топологии и типы подключений не ограничиваются. Любое приложение, создающее поток данных, который можно охарактеризовать как занимающий ограниченную пропускную способность, должно иметь возможность использовать преимущества DetNet при условии резервирования требуемых ресурсов. Резервирование может организовать само приложение через управление сетью или централизованный контроллер приложений, а также иные средства, например, это можно сделать путем резервирования по запросу через распределенную плоскость управления по протоколу RSVP[2] [RFC2205]. Требования QoS для потоков DetNet могут быть выполнены, если все узлы сети в домене DetNet поддерживают возможности DetNet. Узлы DetNet могут соединяться с использованием разных технологий (4.1.2. Обзор плоскости данных DetNet), при этом узлы подсетей могут не знать о DetNet (4.1.3. Модель эталонной сети).

Многим приложениям, рассчитанным на услуги DetNet, нужна возможность синхронизировать часы оконечных систем с микросекундной точностью. Некоторые методы управления очередями, определенные в разделе 4.5. Очереди, формирование, планирование и вытеснение трафика, также требуют синхронизации между узлами сети. Средства обеспечения такой синхронизации в этом документе не рассматриваются. DetNet может использовать разные методы синхронизации часов, определенные в других документах, для решения своих задач, диктуемых рынком.

2. Терминология

2.1. Используемые в документе термины

Ниже приведены определения терминов, используемых в этом документе.

[1]Quality-of-Service - качество обслуживания.
[2]Resource Reservation Protocol - протокол резервирования ресурсов.

allocation - выделение

Выделение ресурсов для поддержки потока DetNet. В зависимости от реализации ресурс может отдаваться за пределы DetNet, когда он не нужен потоку DetNet.

App-flow - поток приложения

Данные (payload), передаваемые через службы DetNet.

DetNet compound flow и DetNet member flow - составной поток DetNet и поток участника DetNet

Составным потоком DetNet называется поток DetNet, разделенный на несколько дубликатов потоков членов DetNet для защиты на подуровне сервиса DetNet. Потоки членов объединяются в один составной поток DetNet без дублирования пакетов. Понятия «составной поток» и «поток участника» не являются абсолютными. Составной поток DetNet, содержащий множество потоков членов DetNet, может быть включен в составной поток более высокого уровня.

DetNet destination - получатель DetNet

Конечная система, способная завершать поток DetNet.

DetNet domain - домен DetNet

Часть сети, поддерживающая DetNet. Включает конечные системы и узлы DetNet.

DetNet edge node - краевой узел DetNet

Экземпляр ретранслятора DetNet, выступающий в качестве источника и получателя на подуровне службы DetNet. Например, он может включать функцию посредника подуровня DetNet для защиты сервиса DetNet (добавление и удаление данных упорядочения пакетов) одной или множества конечных систем, начинать или завершать выделение ресурсов на подуровне пересылки DetNet в новых потоках DetNet. Такой узел аналогичен маршрутизатору LER[1] или PE[2].

DetNet flow - поток DetNet

Последовательность пакетов, соответствующих уникальному идентификатору потока, для которых обеспечивается сервис DetNet. Поток включает заголовки DetNet для подуровней сервиса и пересылки DetNet.

DetNet forwarding sub-layer - подуровень пересылки DetNet

Функциональность DetNet разделена на два подуровня. Одним из них является подуровень пересылки DetNet, который может также обеспечивать выделение ресурсов для потоков DetNet на путях через базовую сеть.

DetNet intermediate node - промежуточный узел DetNet

Ретранслятор или промежуточный узел DetNet.

DetNet node - узел DetNet

Краевой узел, ретранслятор или промежуточный узел DetNet.

DetNet relay node - ретранслятор DetNet

Узел DetNet, включающий функцию подуровня сервиса, которая соединяет разные пути пересылки DetNet для обеспечения защиты сервиса. Ретранслятор DetNet участвует в работе сервисного подуровня DetNet. Обычно он также включает функции подуровня пересылки DetNet и в этом случае совмещается с транзитным узлом.

DetNet service sub-layer - сервисный подуровень DetNet

Функциональность DetNet разделена на два подуровня. Одним из них является сервисный подуровень DetNet, обеспечивающий услуги DetNet (например, защиту сервиса).

DetNet service proxy - прокси службы DetNet

Посредник, обеспечивающий отображение между потоками приложений и потоками DetNet.

DetNet source - источник DetNet

Конечная система, способная создавать поток DetNet.

DetNet system - система DetNet (система)

Поддерживающая DetNet конечная система, промежуточный узел или ретранслятор.

DetNet transit node - транзитный узел DetNet

Узел DetNet, работающий на подуровне пересылки DetNet и использующий коммутацию канального и/или сетевого уровня между несколькими каналами и/или подсетями для обеспечения путей сервисного подуровня DetNet. Обычно такой узел обеспечивает выделение ресурсов для этих путей. Примером транзитного узла является LSR[3].

DetNet-UNI

Интерфейс пользователь-сеть (User-to-Network Interface - UNI) с функциональностью DetNet. Это опорная точка на уровне пакетов, способная выполнять функции инкапсуляции, синхронизации, поддержки состояния и т. п.

end system - конечная система

Обычно называется хостом в документах RFC и конечной станцией в стандартах IEEE 802. В этом документе рассматриваются конечные системы, являющиеся отправителями или получателями потоков DetNet, которые могут (но не обязаны) поддерживать подуровни сервиса и пересылки DetNet.

link

Соединение между двумя узлами DetNet. Это может быть физический канал или сетевая технология, обеспечивающие приемлемую доставку трафика для потоков DetNet.

Packet Elimination Function (PEF) - функция исключения дубликатов

Функция, исключающая дублирование копий пакетов, для предотвращения лавинной пересылки пакетов в сеть или дублирования пакетов, выходящих из домена DetNet. PEF может быть реализована на граничном узле, ретрансляторе или конечной системе DetNet.

Packet Replication Function (PRF) - функция репликации пакетов

Функция, реплицирующая пакеты потоков DetNet и пересылающая их на один или несколько следующих интервалов домена DetNet. Число пакетов, передаваемых на следующий интервал, является параметром потока DetNet в точке репликации. PRF можно реализовать на граничном узле, ретрансляторе или конечной системе.

PREOF

Общее название функций репликации, исключения дубликатов и упорядочения.

Packet Ordering Function (POF) - функция упорядочения пакетов

Функция восстановления порядка пакетов в потоке DetNet, которая может быть реализована на граничном узле, ретрансляторе или конечной системе DetNet.

reservation - резервирование

Набор ресурсов, выделяемых отправителю и одному или множеству получателей на узлах и подсетях, связанных с потоком DetNet, для обеспечения сервиса DetNet.

[1]Label Edge Router - краевой маршрутизатор по меткам.
[2]Provider Edge - краевой маршрутизатор провайдера.
[3]MPLS Label Switch Router - маршрутизатор с коммутацией по меткам.

2.2. Термины, используемые TSN и DetNet

Этот параграф служит словарем для перевода терминов, применяемых группой TSN [IEEE802.1TSNTG] в составе IEEE 802.1 WG, в термины рабочей группы WG в рамках IETF.

Listener - слушатель
Термин, используемый в IEEE 802.1, для получателей потоков DetNet.

Relay system - ретранслятор
Термин, используемый в IEEE 802.1, для промежуточных узлов DetNet.

Stream - поток
Термин, используемый в IEEE 802.1, для потоков DetNet.

Talker - "оратор"
Термин, используемый в IEEE 802.1, для источников потоков DetNet.

3. Обеспечение качества обслуживания в DetNet

3.1. Основные цели определения DetNet QoS

DetNet QoS можно выразить несколькими способами, указанными ниже.

- Минимальная и максимальная сквозная задержка между отправителем и получателем, своевременная доставка и ограниченные вариации задержки.
- Доля теряемых пакетов в разных условиях, связанных с рабочими состояниями узлов и каналов.
- Верхняя граница нарушения порядка доставки пакетов. Здесь следует отметить, что некоторые приложения DetNet совсем не позволяют нарушать порядок доставки.

Отличительной чертой DetNet является работа исключительно с худшими вариантами сквозной задержки, ее вариаций и нарушения порядка доставки. Нормальные, усредненные и типовые значения малоинтересны, поскольку они не влияют на способность систем выполнять свои задачи в реальном масштабе времени. В общем случае тривиальная система управления очередями по приоритетам будет давать для потока данных лучшую среднюю задержку, нежели DetNet, однако она не подходит для DetNet при учете наибольшей задержки.

В DetNet используются три метода обеспечения качества обслуживания:

- 3.2.1. Выделение ресурсов;
- 3.2.2. Защита сервиса;
- 3.2.3. Явные маршруты.

Выделение ресурсов происходит путем назначения ресурса (например, буферной емкости или пропускной способности канала) потоку или группе потоков DetNet по пути их следования. Выделение ресурсов существенно снижает или даже исключает потерю пакетов в результате конфликтов при передаче пакетов в сети, но применимо лишь к потоку DetNet, ограниченному у отправителя по размеру пакетов и скорости их передачи. Поскольку предполагается ограничение скорости потоков DetNet и предоставление в DetNet достаточных ресурсов (включая пропускную способность), применять контроль перегрузок на транспортном уровне [RFC2914] для потоков приложений (App-flow) не требуется, однако при подобающем выделении ресурсов контроль перегрузок не будет оказывать негативного влияния.

Выделение ресурсов выполняет требования DetNet QoS по задержке и потере пакетов. С учетом ограниченности буферов на узлах DetNet выделение ресурсов обязательно влияет на максимальную сквозную задержку. Выделение ресурсов также решает проблему потери пакетов, связанной с конкуренцией.

Другим важным вкладом в потерю пакетов являются случайные ошибки в среде и сбои в оборудовании. Защитой сервиса называются механизмы, используемые в DetNet для устранения таких потерь. Применяемые механизмы ограничены необходимостью выполнять требования пользователей к задержкам. В параграфах 3.2.2.2. Репликация и устранение копий и 3.2.2.3. Кодирование пакетов для защиты сервиса описаны два метода защиты сервиса, но могут применяться и другие механизмы. Например, может использоваться кодирование пакетов для защиты сервиса от случайных ошибок в среде, а репликация и устранение копий - для защиты от сбоев оборудования. Этот механизм распределяют потоки DetNet по нескольким путям в пространстве и/или времени, поэтому потеря некоторых путей не обязательно приведет к потере каких-либо пакетов.

Пути обычно (но не обязательно) являются явными маршрутами, поэтому они как правило не страдают от временных прерываний, вызванных схождением протоколов маршрутизации или мостов.

Эти три метода могут применяться по отдельности или совместно. Возможно использование любой комбинации, включая полное отсутствие (без DetNet). Однако некоторые сочетания используются чаще. Такое разделение обеспечивает согласованность стека протоколов и максимальную совместимость с имеющимися и разрабатываемыми стандартами (в IETF и других организациях). Ниже приведено несколько примеров типовых сочетаний.

- Комбинация явных маршрутов и защиты сервиса является методом организации бесшовной избыточности в кольцевой топологии, как описано в [IEC-62439-3]. В этом случае явные маршруты обеспечиваются за счет ограничения физической топологии сети кольцом. Упорядочение, репликация и устранение дубликатов обеспечиваются добавлением тегов в начале или в конце кадров Ethernet. В [RFC8227] представлен другой пример в контексте MPLS.
- Выделение ресурсов в качестве единственного метода было предложено в IEEE 802.1 Audio Video Bridging [IEEE802.1BA]. Пока в сети не возникает отказов, потеря пакетов в результате конкуренции на выходе может быть устранена с помощью протокола резервирования (например, Multiple Stream Registration Protocol [IEEE802.1Q]), формирователей в каждом мосту и соблюдения нужных размеров.
- Использование всех трех методов обеспечивает максимальную защиту.

Имеются и другие доступные (и развернутые) методы обеспечения приемлемой задержки и потери пакетов для многих приложений. К таким методам относится приоритизация и предоставление избыточных ресурсов (over-provisioning).

Однако такие методы лучше всего работают при отсутствии в сети значимого объема некритичного трафика (если такой трафик поддерживается). Они могут работать лишь в тех случаях, когда критичный к задержкам и потерям трафик составляет малую часть от теоретической пропускной способности сети, все системы работают корректно и нет конечных систем, действия которых нарушают работу сети.

Определено, применяется или разрабатывается много механизмов реализации каждого из отмеченных выше методов. Предполагается, что определенная здесь архитектура DetNet поможет производителям, пользователям и «вертикальным» органам стандартизации (отраслевым) сделать выбор между доступными реализациями сетей DetNet.

3.2. Механизмы обеспечения DetNet QoS

3.2.1. Выделение ресурсов

3.2.1.1. Устранение потерь в результате конкуренции

Основным способом достижения гарантий QoS в DetNet является снижение или даже полное устранение потери пакетов в результате конкуренции в выходных очередях на узлах DetNet. Это можно реализовать лишь обеспечением достаточного объема буферов, чтобы пакеты не терялись в результате нехватки буферной емкости. Отметим, что в общем случае не предполагается реакция потоков приложений на неявные [RFC2914] или явные [RFC3168] уведомления о перегрузке.

Обеспечение адекватной буферизации требует от отправителя и каждого узла в пути DetNet к получателю (почти каждый узел, см. параграф 4.3.3) аккуратного регулирования своего вывода, чтобы не превышалась скорость для каждого потока DetNet за исключением кратких периодов сочетания с мешающим трафиком. Любой пакет, отправленный раньше времени, может добавлять объем буферов, требуемых на следующем узле DetNet, что может приводить к выходу за пределы выделенных отдельному потоку DetNet ресурсов. Кроме того, на входе в домен DetNet должны применяться функции ограничения скорости (например, правила для трафика) и механизмы формовки (например, [RFC2475]). Это нужно для соблюдения требований DetNet, а также для защиты остального (не DetNet) трафика от некорректно работающих источников трафика DetNet. Отметим, что большие буферы создают некоторые проблемы (см. например, [BUFFERBLOAT]).

Описанные в параграфе 4.5 механизмы нижних уровней обеспечивают требуемое регулирование передачи в конечных системах или узлах DetNet с учетом выделения ресурсов. Выделенную для потока DetNet пропускную способность или буферы требуется обеспечить. Узел DetNet может иметь другие ресурсы, требующие выделения и/или планирования, которые могут быть без этого перегружены и вызывать отказ при резервировании.

3.2.1.2. Снижение вариаций задержки

Основной целью DetNet является обеспечение возможности сведения отличных от IP сетей с критичными (sensitive) приложениями в единую сетевую инфраструктуру. Это требует аккуратной эмуляции развернутых в настоящее время под конкретные задачи сетей, которые основаны, например, на аналоговых (к примеру, с модуляцией 4 - 20 мА) и цифровых последовательных линиях (или шинах) для обеспечения надежных, синхронизированных коммуникаций без вариации задержек. Хотя задержка аналоговой передачи определяется в основном скоростью света, традиционные последовательные каналы обычно медленны (кбит/с) по сравнению с Gigabit Ethernet, а некоторая задержка, как правило, допустима. А вот чрезмерные вариации задержки могут влиять на стабильность систем управления.

Приложения, разработанные для последовательных каналов, обычно не обеспечивают компенсации вариаций задержки по причине их отсутствия в таких линиях. Для потоков DetNet обычно предполагается упорядоченная доставка и точное время приема влияет на процессы. Для объединения таких приложений желательно эмулировать все свойства последовательной линии, такие как доставку сигналов синхронизации, полную изоляцию потоков и фиксированную задержку. Хотя минимальные вариации задержки (заданные минимальной и максимальной сквозной задержкой) допустимы в DetNet, пакетные сети вносят свои ограничения. В общем случае рекомендуется применять комбинацию указанных ниже мер.

- Синхронизация с точностью в доли микросекунды между всеми конечными системами.
- Поле времени выполнения в пакетах приложений.

Снижение вариаций задержки обеспечивается механизмами, описанными в параграфе 4.5, которые также обеспечивают выделение ресурсов.

3.2.2. Защита сервиса

Защита сервиса нацелена на снижение или предотвращение потери пакетов в результате отказов оборудования, включая случайные ошибки в среде передачи или памяти. Такие потери можно существенно сократить за счет распределения данных по множеству не связанных между собой путей пересылки. В [RFC6372] описаны различные методы защиты сервиса, например, линейная защита 1+1. Функциональные детали дополнительного метода описаны в параграфе 3.2.2.2 и могут быть реализованы в соответствии с параграфом 3.2.2.3 или [DETNET-MPLS] для обеспечения защиты 1+n. Выбор механизмов защиты сервиса зависит от сценария и требований.

3.2.2.1. Упорядоченная доставка

Побочным эффектом защиты сервиса может быть нарушение порядка доставки, что повышает требования к буферизации пакетов на приемной стороне для корректной обработки данных. Пакеты с нарушенным порядком доставки также влияют на вариации задержки в потоке. Гарантии сервиса DetNet включают максимальное сохранение порядка доставки в качестве ограничения. Сохранение порядка было бы действительным ограничением, отражающим неприемлемость нарушения для конечных систем. Для сохранения порядка доставки в DetNet может применяться функция POF (3.2.2.2. Репликация и устранение копий).

3.2.2.2. Репликация и устранение копий

В этом параграфе описан метод защиты сервиса за счет передачи копий пакета по нескольким путям.

Подуровень сервиса DetNet включает функции PRF, PEF и POF для использования в ретрансляторах, краевых и оконечных устройствах DetNet при обработке пакетов. Эти функции могут быть включены на ретрансляторах, краевых и оконечных устройствах DetNet. Все три функции обозначают общим термином PREOF. Метод защиты сервиса за счет репликации и устранения копий пакетов включает четыре возможности, указанные ниже.

- Для пакетов составного потока DetNet обеспечивается информация о порядке. Это может быть выполнено путем включения порядковых номеров или временных меток как части DetNet, наследования из пакетов (например, в протоколах вышележащих уровней) или использования иных физических свойств (например, точного времени приема пакетов по радиоканалу). Обычно это выполняется однократно вблизи источника.
- PRF реплицирует пакеты в несколько потоков участников DetNet и обычно передает их по разным путям к получателю, например, с помощью явных маршрутов, описанных в параграфе 3.2.3. Место и механизм использования PRF внутри узла DetNet определяется реализацией.
- PEF устраняет дубликаты пакетов потока DetNet на основе данных о порядке и истории приема пакетов. На выходе PEF всегда остается один пакет. Операция может выполняться любым узлом DetNet в пути для экономии сетевых ресурсов в нисходящем направлении, особенно при наличии нескольких точек репликации. Обычно это происходит на самом краю сети DetNet, предпочтительно вблизи получателя. Место и механизм использования PEF внутри узла DetNet определяется реализацией.
- POF использует информацию о порядке для восстановления нарушенного порядка пакетов в потоке DetNet.

Порядок применения узлом DetNet функций PEF, POF и PRF к потоку DetNet определяется реализацией.

Некоторые механизмы защиты сервиса опираются на переключение с одного потока на другой при обнаружении отказа потока. В противоположность этому репликация и устранение копий комбинирует потоки участников DetNet из разных путей и выполняет на уровне пакетов выбор отбрасываемых (например, по информации о порядке).

В простейшем случае это эквивалентно 1) репликации каждого пакета у отправителя с двумя интерфейсами и 2) передаче их через сеть по разным путям (разделение SRLG[1]) к похожим двудомным получателям, которые 3) восстанавливают порядок пакетов и 4) отбрасывают дубликаты. Это обеспечивает сохранение одного пути даже при отказе некоторых промежуточных узлов DetNet. Информация о порядке служит также для обнаружения потерь.

Ретрансляторы DetNet в сети могут поддерживать репликацию и устранение копий в разных точках сетевого пути, что обеспечивает устойчивость к множественным отказам. Это показано на рисунке 1, где два ретранслятора реплицируют (R) потоки DetNet на входе, передают потоки членов DetNet другому ретранслятору и конечной системе, а также устраняют дубликаты (E) на выходном интерфейсе в сторону конечной системы справа. При отказе любого канала в сети составной поток DetNet сохраняется. Кроме того, обеспечивается работа при отказе двух каналов, если они размещены в разных сегментах сети.

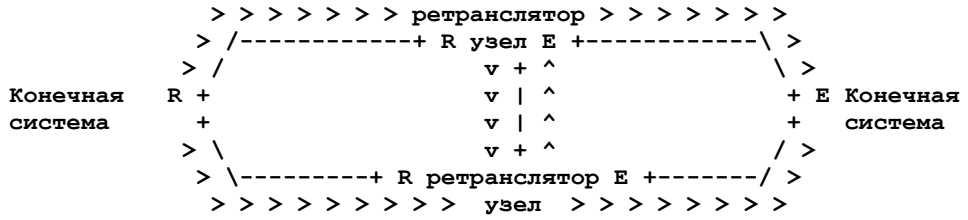

Рисунок 1. Репликация и исключение потоков.

Репликация и устранение копий не реагируют и не исправляют отказы, они полностью пассивны. Поэтому повторяющиеся сбои, ошибочные фильтры пакетов или неверная маршрутизация обрабатываются так же, как отказы оборудования - с помощью типовых протоколов маршрутизации и мостов.

При объединении потоков участника, проходящих по путям разной длины, может потребоваться дополнительная буферизация для выравнивания задержки на разных путях. Это выравнивание обеспечивает результирующему составному потоку соответствие ограничениям пропускной способности даже после восстановления при отказе одного из путей. Дополнительная буферизация может также служить для соблюдения порядка пакетов.

3.2.2.3. Кодирование пакетов для защиты сервиса

Существуют методы защиты сервиса с использованием нескольких путей, включающие кодирование информации в пакетах, относящихся к потоку DetNet, в виде множества блоков передачи с объединением данных из нескольких пакетов в один блок. Такие методы, называемые сетевым кодированием, могут служить для защиты сервиса DetNet.

3.2.3. Явные маршруты

В сетях, управляемых типичными протоколами динамической маршрутизации, такими как IS-IS или OSPF, события в сетевой топологии той или иной части сети могут, по меньшей мере в течение короткого времени, влиять на доставку данных в участках сети, удаленных от точки отказа или восстановления. Даже использование резервных путей через сеть (например, как определено в [RFC6372]) не устраняет вероятность потери пакетов. Кроме того, побочным эффектом изменения маршрутов может быть нарушение порядка доставки.

Многие сети, работающие в реальном масштабе времени, основаны на кольце из двухпортовых устройств с относительно простым протоколом управления кольцом. Это обеспечивает резервирование пути для защиты сервиса с минимальным числом проводов. Дополнительным преимуществом кольцевой топологии часто является возможность использования протоколов управления, отличающихся от применяемых в многосвязных (mesh) сетях, и соответствующее сокращение времени отклика на изменение топологии. Недостатком кольцевой топологии является большее число этапов пересылки (hop) и соответствующий рост задержки на типичном пути.

Для получения преимуществ малого числа этапов пересылки вместе с защитой даже от очень коротких перебоев в связи DetNet использует явные маршруты, где путь данного потока DetNet не меняется сразу и может не измениться

[1]Shared Risk Link Group - группа каналов с общим риском.

совсем в результате событий смены топологии. Защита сервиса (параграфы 3.2.2 и 3.2.2.3) при явных маршрутах обеспечивает высокую вероятность сохранения непрерывной связности. Явные маршруты можно создавать разными способами, например, с помощью RSVP-TE [RFC3209], SR[1] [RFC8402], SDN [RFC8453], IS-IS [RFC7813] и т. п. Явные маршруты обычно применяются в MPLS TE[2] LSP[3].

Побочным эффектом распределения потока по нескольким путям может быть нарушение порядка доставки, особенно при смене одного пути на другой для комбинирования потока. Это не зависит от применяемого метода распространения и также используется для защиты сервиса по явным маршрутам. Как описано в параграфе 3.2.2.1, нарушение порядка доставки влияет на вариации задержки потока и размер буферов, требуемых для обработки данных. Поэтому гарантии сервиса DetNet включают максимальное нарушение порядка в качестве ограничения. Использование явных маршрутов помогает обеспечить упорядоченную доставку, поскольку маршрут не меняется незамедлительно при изменении топологии и смену пути можно планировать, т. к. это просто переключение маршрута.

3.3. Дополнительные цели DetNet

Многие приложения требуют от DetNet предоставления дополнительных услуг, включая использование других механизмов QoS (3.3.1. Сосуществование с обычным трафиком) и защиту от некорректно работающих передатчиков (3.3.2. Устранение отказов).

3.3.1. Сосуществование с обычным трафиком

Сеть DetNet поддерживает выделение значительной части пропускной способности потокам DetNet. Однако, независимо от объема выделенных для потоков DetNet ресурсов, целью DetNet является сосуществование с имеющимися схемами классов обслуживания (CoS[4]), например, DiffServ. Важно, чтобы не относящийся к DetNet трафик не нарушал потоки DetNet (см. параграф 3.3.2 и раздел 5). Поэтому возникает ряд требований.

- Пропускная способность (возможность передачи), не занятая потоками DetNet, доступна для прочих пакетов.
- Потоки DetNet могут формоваться или планироваться для обеспечения параметров задержки высокоприоритетных пакетов, не относящихся к DetNet.
- При детальном планировании возможностей передачи для потоков DetNet алгоритм планирования должен оставлять достаточно возможностей передачи прочих пакетов с учетом потребностей пользователей сети. Подробное планирование также позволяет разделять буферные ресурсы по времени между потоками DetNet.

Следует избегать подавления трафика, не относящегося к DetNet, например, с помощью правил или формовки трафика (например, [RFC2475]). Таким образом, финальным эффектом наличия в сети потоков DetNet будет в основном уменьшение пропускной способности, доступной для другого трафика.

3.3.2. Устранение отказов

Отказоустойчивым системам, работающим в реальном масштабе времени, требуется снижение числа возможных отказов. В сети DetNet следует применять фильтры и правила для обнаружения приема пакетов DetNet не на том интерфейсе, не в то время или в избыточном количестве. Кроме того, фильтры и ограничители могут отбрасывать ошибочные пакеты или потоки, а также инициировать отключение сбойного потока или интерфейса.

Важно также применять на границе сети фильтры и перемаркировку услуг для предотвращения ошибочного отнесения чужих пакетов к DetNet, воздействующего на ресурсы, выделенные для DetNet. В частности, передачу трафика DetNet в сети, которые не были заранее подготовлены для обслуживания трафика DetNet, следует считать сбоем. Для предотвращения этого настоятельно рекомендуется применение выходных фильтров или эквивалентных механизмов на границе сети DetNet и поддерживающих DetNet сетей. В этом контексте подготовка имеет широкий смысл, включая административные решения в части передачи трафика в нисходящую сеть.

Отметим, что передача потоков приложений, не применяющих контроль перегрузок на транспортном уровне в соответствии с [RFC2914], в сеть, не подготовленную для обработки такого трафика, должна считаться сбоем и пресекаться. Созданные функцией PRF потоки участников DetNet должны считаться не использующими контроль перегрузок на транспортном уровне даже при наличии такого контроля в исходных потоках приложений, поскольку PREOF может удалять индикацию перегрузки в функции PEF (например, отбрасывание, маркеры ECN, рост задержки).

Механизмы поддержки этих требований зависят от плоскости данных и реализации. Решения для плоскости данных будут описаны в соответствующих документах. Имеются также стандартизованные или стандартизуемые методы для поддержки задач по устранению отказов, которые обеспечивают высокую вероятность предотвращения влияний некорректно работающих систем на хорошо организованные потоки DetNet, за исключением отказов приемных интерфейсов, находящихся непосредственно под некорректно работающим устройством. Примерами таких методов являются функции контроля и формовки трафика (например, описанные в [RFC2475]), разделение потоков по очередям с ограничением скорости на уровне потока, а также применение активного управления очередями [RFC7567].

4. Архитектура DetNet

4.1. Модель стека DetNet

Функции DetNet (раздел 3. Обеспечение качества обслуживания в DetNet) реализованы на двух смежных подуровнях стека протоколов - сервис DetNet и пересылка DetNet. Подуровень сервиса предоставляет услуги DetNet (например, защиту сервиса) вышележащему уровню стека и приложениям. Подуровень пересылки поддерживает услуги DetNet в базовой сети, например, путем предоставления явных маршрутов и резервирования ресурсов для потоков DetNet.

[1]Segment Routing - сегментная маршрутизация.
[2]Traffic Engineering - организация трафика.
[3]Label Switched Path - путь с коммутацией по меткам.
[4]Class-of-Service.

4.1.1. Представление модели стека протоколов

На рисунке 2 представлена концептуальная модель уровней плоскости данных DetNet. Можно сравнить ее с моделью из [IEEE802.1CB], Annex C.

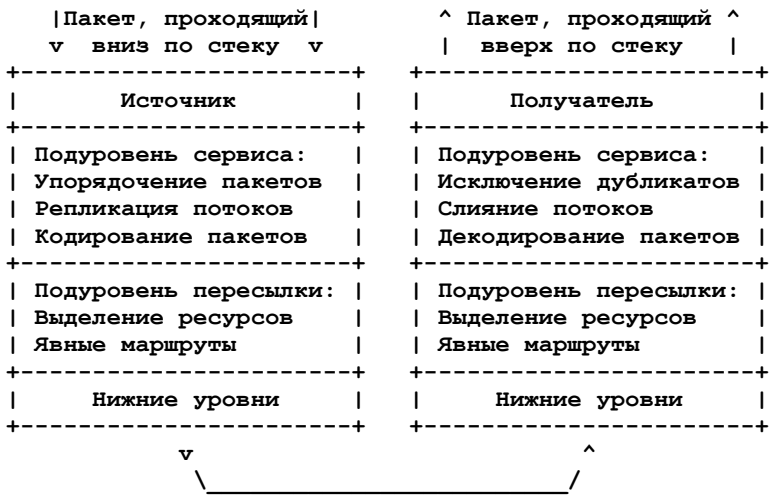

Рисунок 2. Стек протоколов плоскости данных DetNet.

Для данного приложения и даже сети могут требоваться не все подуровни из числа перечисленных ниже.

Application - приложение

На рисунке приложения показаны как отправитель и получатель.

Packet sequencing - упорядочение пакетов

Как часть сервисного подуровня DetNet, функция упорядочения пакетов представляет порядковые номера для репликации и устранения дубликатов в защите сервиса DetNet (3.2.2.2. Репликация и устранение копий) и партнером этого подуровня является исключение дубликатов. Этот подуровень не требуется, если предполагается упорядочение пакетов и устранение дубликатов для потоков DetNet вышележащим протоколом.

Duplicate elimination - исключение дубликатов

Как часть сервисного подуровня DetNet, отбрасывает все дубликаты пакетов на основе порядковых номеров, представленных партнером (упорядочение пакетов) для репликации потоков DetNet. Подуровень может работать с потоками членов и составными потоками. Репликация может также работать на основе точного времени приема в сети с планированием. Подуровень устранения дубликатов может также восстанавливать порядок пакетов в потоке, нарушенный потерей пакетов в одном из множества путей потока.

Flow replication - репликация потоков

Как часть защиты сервиса DetNet, пакеты, относящиеся к составному потоку DetNet, реплицируются в два или более потоков участника DetNet. Эта функция отделена от упорядочения пакетов. Репликация потока может быть явной репликацией и перемаркировкой или выполняться, например, на основе методов, похожих на обычную групповую репликацию с последующим выделением ресурсов. Партнером является подуровень слияния потоков.

Flow merging - слияние потоков

Как часть сервисного подуровня DetNet, функция слияния потоков объединяет потоки членов DetNet для поднимающихся по стеку пакетов, относящихся к конкретному составному потоку DetNet. Слияние потоков DetNet вместе с подуровнями упорядочения, устранения дубликатов и репликации для потоков DetNet обеспечивает репликацию и устранение дубликатов (3.2.2. Защита сервиса). Партнером служит подуровень репликации.

Packet encoding - кодирование пакетов

Как часть защиты сервиса DetNet, кодирование пакетов дополняет их упорядочение и репликацию потоков, комбинируя информацию нескольких пакетов DetNet (возможно из разных составных потоков DetNet) и передавая ее в пакетах других потоков членов DetNet. Партнером является подуровень декодирования.

Packet decoding - декодирование пакетов

Как часть защиты сервиса DetNet, декодирование пакетов дополняет слияние потоков и устранение дубликатов, беря пакеты из разных потоков членов DetNet и извлекая из них исходные пакеты составных потоков, использованных функцией кодирования. Партнером является подуровень кодирования.

Resource allocation - выделение ресурсов

Подуровень пересылки DetNet обеспечивает выделение ресурсов (4.5. Очереди, формирование, планирование и вытеснение трафика). Используемые механизмы очередей и формовки трафика обычно предоставляются базовой сетью. Они могут быть тесно связаны со способами предоставления путей для потоков DetNet. На рисунке выделение путей и ресурсов объединено.

Explicit routes - явные маршруты

Явные маршруты являются фиксированными путями, работающими на подуровне пересылки DetNet и определяемыми заранее для предотвращения воздействий схождения сетей (маршрутов) на потоки DetNet.

Функции OAM[1] используют сигнализацию в основной полосе или по отдельному каналу для проверки эффективности обеспечения параметров QoS. Эти функции не показаны на рисунке 2 и могут размещаться на разных уровнях. OAM может включать специальные теги, добавляемые в пакеты для трассировки ошибок реализации или настройки сети, что позволяет определить пакеты, являющиеся репликами, найти ретрансляторы DetNet, выполняющие репликацию, и определить сегмент, предназначенный для реплики. Активные и гибридные методы OAM требуют дополнительного расхода полосы для контроля отказов и мониторинга производительности в домене DetNet. Например, OAM может генерировать специальные тестовые зонды или добавлять свою информацию в пакеты данных.

Функции репликации и устранения дубликатов могут выполняться у отправителя и получателя составного потока DetNet, а также в ретрансляторах DetNet.

[1]Operations, Administration, and Maintenance - эксплуатация, администрирование, поддержка.

4.1.2. Обзор плоскости данных DetNet

«Детерминированные сети» организуются из поддерживающих DetNet конечных систем, краевых узлов и ретрансляторов DetNet, которые совместно предоставляют услуги DetNet. Ретрансляторы и краевые узлы DetNet соединены между собой транзитными узлами DetNet (например, LSR), которые поддерживают DetNet, но не обеспечивают услуг DetNet. Все узлы DetNet подключаются к подсетям, при этом канал «точка-точка» считается вырожденной подсетью. Эти подсети обеспечивают совместимые с DetNet услуги для поддержки трафика DetNet. Примерами технологий подсетей являются MPLS TE, IEEE 802.1 TSN и OTN[1]. Возможны многоуровневые системы DetNet, где одна подсеть DetNet предоставляет услуги системе DetNet более высокого уровня. Простая концептуальная сеть DetNet показана на рисунке 3. Отметим, что на этом и последующих рисунках «Пересылка» и Fwd относятся к подуровню пересылки DetNet, а «сервис» и Svc - к подуровню сервиса DetNet (4.1.1. Представление модели стека протоколов).

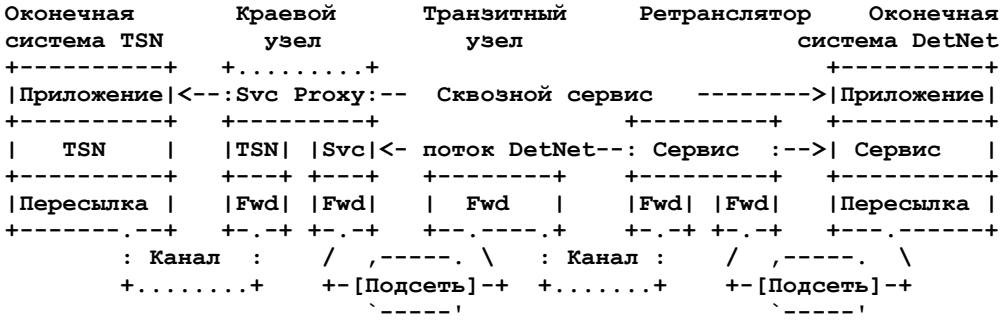

Рисунок 3. Простая сеть с поддержкой DetNet.

Плоскость данных DetNet разделена на два подуровня - сервис DetNet и пересылка DetNet. Это помогает изучать и оценивать разные комбинации доступных решений на уровне данных, некоторые из них показаны на рисунке 4. Это разделение на подуровни DetNet полезно, но не является формальным требованием. Некоторые технологии могут предоставлять услуги DetNet без выделения этих уровней.

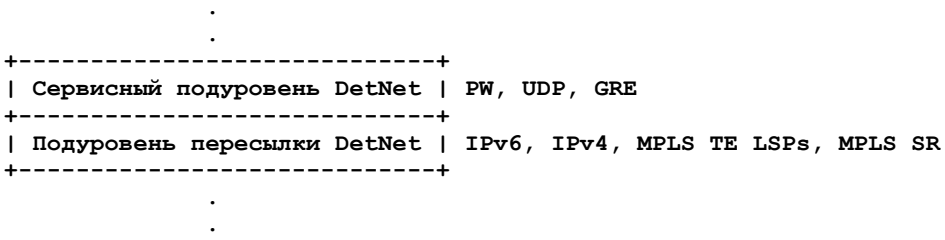

Рисунок 4. Адаптация DetNet к уровню данных.

В некоторых сетях конечные системы исходно обеспечивают инкапсуляцию потоков DetNet со всей информацией, нужной узлам DetNet (например, потоки DetNet на основе протокола RTP[2] [RFC3550], передаваемые через сети UDP/IP или псевдопровода PW[3]). В иных случаях формат инкапсуляции может существенно отличаться.

Имеется много вариантов организации плоскости данных для трафика DetNet за счет выбора технологического решения для подуровней сервиса пересылки DetNet.

Одним из основных различий между плоскостями данных являются базовые заголовки, используемые узлами DetNet. Например, базовый сервис может предоставляться на основе меток MPLS или заголовков IP. Этот выбор влияет на базовую логику пересылки для подуровня сервиса DetNet. Отметим, что в обоих случаях для адресации узлов DetNet служат адреса IP. Выбранная для подуровня пересылки DetNet технология тоже должна отображаться не технологию подсети, соединяющей узлы DetNet. Например, потоки DetNet могут отображаться на потоки TSN.

4.1.3. Модель эталонной сети

На рисунке 5 дано другое представление связанных с сервисом DetNet опорных точек и основных компонентов.

Интерфейсы DetNet-UNI (U на рисунке 5) в этом документе считаются опорными точками для пакетов и обеспечивают соединение с пакетной сетью. Интерфейс DetNet-UNI вожет обеспечивать множество функций, включая:

- инкапсуляцию потоков DetNet в соответствии с сетевой технологией;
- предоставление статуса доступности ресурсов для их резервирования;
- предоставление услуг синхронизации для конечных систем;
- поддержка сигнализации для организации резервирования в сети без контроллера или с использованием контроллера, работающего лишь с сетью, а не с конечными системами.

Внутренние опорные конечных систем (между приложением App и NIC[4]) более сложны с точки зрения управления и могут предъявлять дополнительные требования (например, предполагать упорядоченную доставку во внутренние опорные точки, где не обязательно такая доставка выполняется через DetNet-UNI).

[1]Optical Transport Network - оптическая транспортная сеть.
[2]Real-time Transport Protocol - протокол доставки в реальном масштабе времени.
[3]Pseudowire.
[4]Network Interface Card - плата сетевого интерфейса.

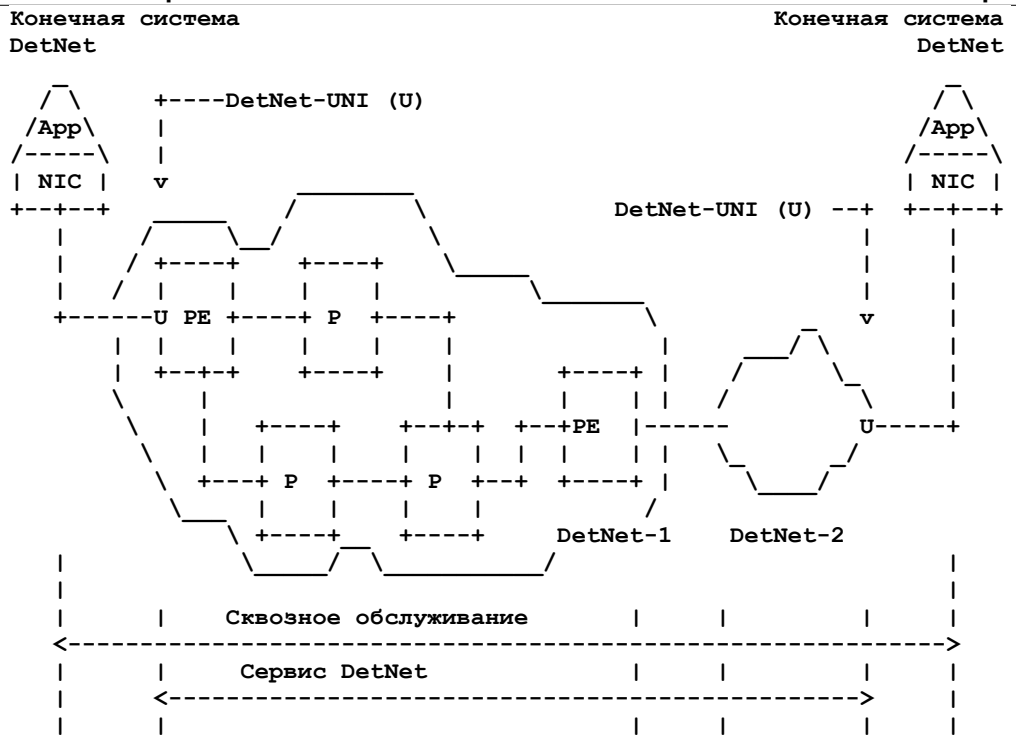

Рисунок 5. Эталонная модель сервиса DetNet (многодоменная).

4.2. Системы DetNet

4.2.1. Конечные системы

Трафик потока приложения может иметь тип CBR (постоянная скорость) или VBR (переменная скорость) и инкапсуляцию L1, L2 или L3 (например, TDM[1], Ethernet, IP). Эти характеристики являются входными данными для резервирования ресурсов и могут быть упрощены для обеспечения детерминизма при пересылке пакетов (например, резервирование для пиковой скорости трафика VBR и т. п.).

Конечная система может не знать о подуровне пересылки или сервиса DetNet, т. е. не включать относящихся к DetNet функций. Системы с функциональностью DetNet в домене DetNet могут применять один или разные подуровни пересылки. Категории конечных систем показаны на рисунке 6.

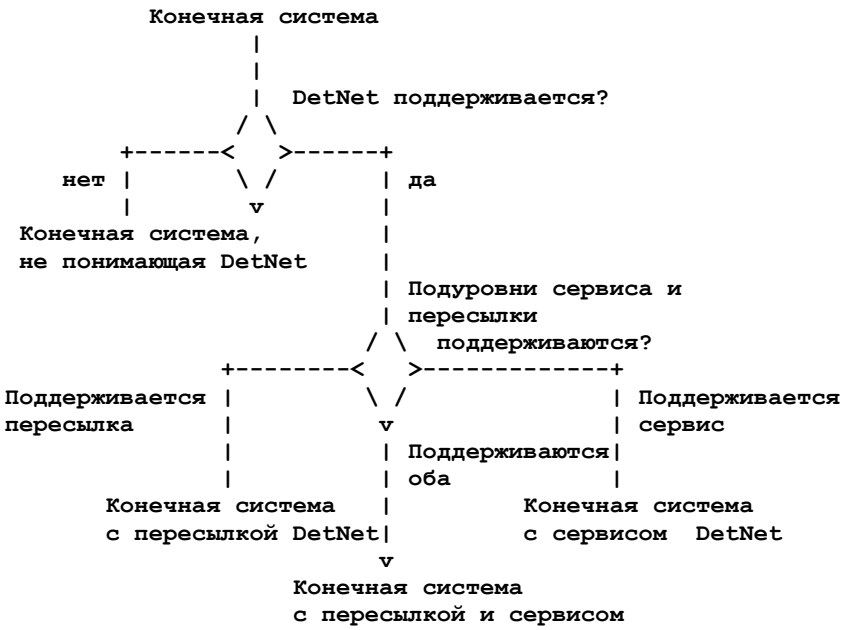

Рисунок 6. Категории конечных систем.

Ниже перечислены примеры известных конечных систем.

DetNet unaware - без поддержки DetNet
Классический вариант, требующий промежуточное устройство (прокси).

DetNet f-aware - с поддержкой пересылки DetNet
Система, которая знает о подуровне пересылки DetNet. Ей известны некоторые функции TSN (например, резервирование), но неизвестно о защите сервиса.

DetNet s-aware - с поддержкой сервиса DetNet
Система, которая знает о подуровне сервиса DetNet. Она предоставляет порядковые номера, но не знает о выделении ресурсов.

[1]Time-division multiplexing - мультиплексирование с разделением по времени.

DetNet sf-aware - с поддержкой пересылки и сервиса DetNet

Полнофункциональная конечная система DetNet. Она поддерживает функции DetNet и обычно использует ту же парадигму пересылки, которая применяется в подключенном домене DetNet. Может считаться встроенной частью домена DetNet.

4.2.2. Ретрансляторы, краевые и транзитные узлы DetNet

Как показано на рисунке 3, краевые узлы DetNet служат посредниками (proxy), ретрансляторы DetNet, обеспечивающие подуровень сервиса DetNet, знают о DetNet, а транзитным узлам DetNet нужно знать лишь о подуровне пересылки.

В общем случае поток DetNet проходит через один или множество узлов, не знающих о DetNet, между двумя узлами DetNet, обеспечивающими подуровень пересылки DetNet для этого потока. Здесь могут возникать нарушения или отказы DetNet QoS. Администраторы сетей должны 1) обеспечить настройку не знающих о DetNet узлов для минимизации потерь и задержки пакетов, а также 2) предоставить достаточное буферное пространство на транзитных узлах DetNet, которые следуют за узлами, не поддерживающими DetNet, для компенсации вариаций задержки.

4.3. Потоки DetNet

4.3.1. Типы потоков DetNet

Поток DetNet может иметь разные форматы при пересылке его пакетов между партнерскими конечными системами в зависимости от типа этих систем. В соответствии с типами конечных систем в этом документе выделяется несколько типов потоков DetNet, требования которых к узлам DetNet различаются.

App-flow - поток приложения

Данные, передаваемые в потоке DetNet между двумя не знающими о DetNet конечными системами. App-flow не включает связанных с DetNet атрибутов и не задает конкретных требований к узлам DetNet.

DetNet-f-flow - поток, знающий о пересылке

Конкретный формат потока DetNet, требующий выделения ресурсов от подуровня пересылки DetNet.

DetNet-s-flow - поток, знающий о сервисе

Конкретный формат потока DetNet, требующий защиты сервиса от подуровня сервиса DetNet.

DetNet-sf-flow - поток, знающий о пересылке и сервисе

Конкретный формат потока DetNet, требующий функции подуровней пересылки и сервиса DetNet при доставке.

4.3.2. Поведение источника передачи

В плане выделения ресурсов поток DetNet может быть синхронным или асинхронным. В синхронных потоках DetNet по меньшей мере узлы DetNet (возможно и конечные системы) синхронизированы (обычно с точностью не хуже 1 мксек). За счет передачи разных потоков или классов потоков DetNet в разное время с использованием повторяющихся расписаний на синхронизированных узлах DetNet, ресурсы (такие как буферы и пропускную способность) можно совместно использовать для разных потоков DetNet. Для синхронных потоков DetNet нужен компромисс между точным планированием и уменьшением потребных ресурсов (особенно буферов).

Асинхронные потоки DetNet не скоординированы с точным расписанием, поэтому ретрансляторы и конечные системы должны предполагать худший вариант взаимодействия разных потоков DetNet при использовании буферных ресурсов. Асинхронные потоки DetNet характеризуются:

- максимальным размером пакетов;
- интервалом наблюдения;
- максимальным числом передач в течение интервала наблюдения.

Эти параметры вместе с информацией о применяемом стеке протоколов (и размере добавляемых в пакет заголовков) позволяют определить пропускную способность, требуемую для потока DetNet.

При использовании сервиса DetNet источник должен соблюдать заданные пределы. При передаче меньшего объема данных неиспользуемые ресурсы (такие, как пропускная способность) могут быть отданы системой DetNet для другого трафика, пока все гарантии соблюдаются. Предоставление свободных ресурсов другим потокам DetNet не имеет смысла. Эти потоки DetNet имеют выделенные им ресурсы в предположении, что все потоки DetNet могут использовать ресурсы в течение длительного времени.

В DetNet не предполагается, что потоки приложений будут реагировать на уведомления о перегрузке [RFC2914] или [RFC3168]. Предполагается, что для осмысленности потока DetNet он должен доставляться целиком. Т. е. приложения для работы в реальном масштабе времени, представляющие интерес для DetNet, требуют, чтобы потеря данных в сети была минимальной.

Хотя DetNet стремится минимизировать изменения, которые нужно внести в приложения для перехода от цифровых сетей специального назначения к сетям IP, не удается избавиться от необходимости выделения ресурсов до запуска приложения. Во-первых, сеть не может обеспечить конечную задержку и практически нулевую потерю пакетов при произвольно высоком уровне загрузки. Во-вторых, для достижения практически нулевой потери пакетов в потоках DetNet узлам DetNet требуются выделенные буферы для конкретных потоков или классов потоков DetNet. Требования каждого резервирования должны преобразовываться в параметры, управляющие в каждой системе DetNet очередями, формовкой и планированием трафика, которые должны быть распространены между узлами и конечными системами.

Предполагается, что все узлы в домене DetNet будут обеспечивать поведение, требуемое для предоставления конкретного сервиса DetNet. Если сам узел не знает о сервисе DetNet, смежные с ним узлы DetNet должны обеспечить ему подобающую поддержку сервиса DetNet. Например, узел IEEE 802.1 TSN можно использовать для соединения узлов DetNet и эти узлы могут отображать потоки DetNet на потоки 802.1 TSN. Другим примером является домен MPLS-TE или MPLS-TP[1], используемый для соединения узлов DetNet, которые могут отображать потоки DetNet на TE LSP, обеспечивающие требования QoS для сервиса DetNet.

[1]Transport Profile - транспортный профиль.

4.3.3. Неполные сети

Наличие в сети промежуточных узлов или подсетей, не способных предложить полные услуги DetNet, осложняет промежуточным устройствам и контроллерам выделение ресурсов, поскольку требуется выделение для потоков DetNet дополнительных буферов в точках, нисходящих по отношению к не поддерживающим DetNet промежуточным узлам. Эти дополнительные буферы могут увеличивать задержку и ее вариации.

4.4. Организация трафика для DetNet

TEAS[1] [TEAS] определяет архитектуру организации трафика, применимую для пакетных и иных сетей. С точки зрения TEAS организацией трафика (TE[2]) считаются методы, позволяющие операторам управлять обработкой определенных потоков трафика в своих сетях.

Благодаря созданию явных оптимизированных путей, DetNet можно считать новой, специализированной ветвью TE, наследующей архитектуру с разделением по плоскостям (уровням). Архитектура DetNet включает три плоскости - (пользовательские) приложения, контроллер и сеть. Это похоже на уровни, приведенные на рисунке 1 в Software-Defined Networking (SDN): Layers and Architecture Terminology [RFC7426], и контроллеры из [RFC8453] и [RFC7149].

4.4.1. Плоскость приложений

В соответствии [RFC7426] плоскость приложений включает приложения и службы. В частности, здесь присутствует пользовательский агент - специализированное приложение, взаимодействующее с конечным пользователем и оператором для запроса услуг DetNet с помощью элемента управления потоком (FME[3]), который может размещаться в одной из конечных систем.

В плоскости приложений интерфейс управления позволяет согласовать потоки между конечными системами. Представление обеспечивается абстракцией потока TSpec[4], используемой для размещения резервирования на (северном) интерфейсе сервиса и в плоскости приложения. Это связано с абстракцией местоположения, такой как адрес IP или имя (DNS), для идентификации конечных систем и, возможно, задания узлов DetNet.

4.4.2. Плоскость контроллера

Плоскость контроллера соответствует плоскостям Control и Management в [RFC7426], хотя CCAMP[5] (в соответствии с определением рабочей группы CCAMP [CCAMP]) задает дополнительное различие между управлением и измерениями. Когда различие между элементами управления, измерений и другими объектами управления (Management) не существенно, для упрощения применяется термин «плоскость контроллера» (представляет все), а CPF[6] указывает любое устройство, работающее в этой плоскости, будь то PCE[7] [RFC4655], NME[8] или протокол распределенного управления. CPF является основным элементом контроллера, отвечающим за расчет детерминированных путей, применяемых в сетевой плоскости.

(Северный) интерфейс сервиса позволяет приложениям из прикладной плоскости взаимодействовать с объектами плоскости контроллера, как показано на рисунке 7.

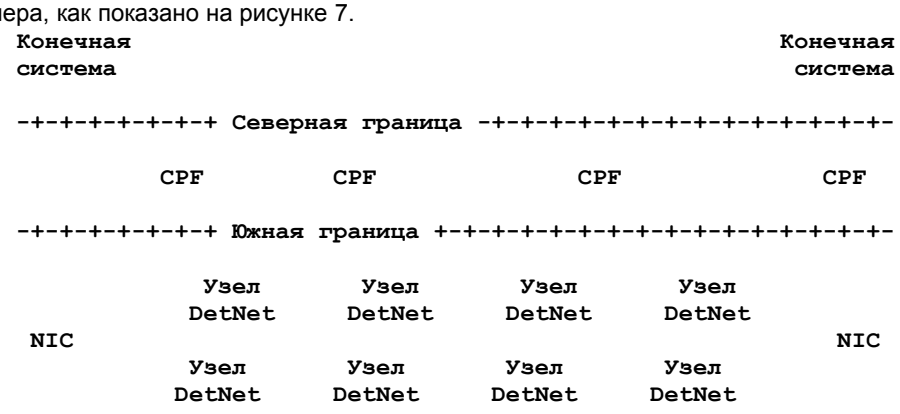

Рисунок 7. Интерфейсы северной и южной границы.

Несколько CPF могут действовать совместно для реализации запросов от FME как поведения на уровне потока или интервала (hop), задаваемого на узлах DetNet для каждого отдельного потока. CPF размещают каждый поток через детерминированный набор узлов DetNet, чтобы выполнить ограничения на уровне потоков (такие как защита и задержки) и оптимизировать общий результат по таким показателям, как абстрактная агрегированная стоимость. Детерминированная структура обычно сложней прямого назначения и включает резервные пути с одной или несколькими точками репликации и устранения дубликатов. Большие сети рассматриваются в разделе 4.9.

4.4.3. Плоскость сети

Плоскость сети представляет сетевые устройства и протоколы в целом, независимо от уровня, на котором работают устройства. Плоскость включает уровни (плоскости) данных и операций (например, OAM).

Плоскость сети включает сетевые адаптеры (NIC) в конечных системах, которые обычно являются хостами IP, и узлах DetNet, которыми обычно служат маршрутизаторы IP и коммутаторы MPLS.

[1]Traffic Engineering Architecture and Signaling - архитектура и сигнализация для организации трафика.
[2]Traffic Engineering - организация трафика.
[3]Flow Management Entity - элемент управления потоком.
[4]Traffic Specification - спецификация трафика.
[5]Common Control and Measurement Plane - общая плоскость управления и измерений.
[6]Controller Plane Function - функция плоскости контроллера.
[7]Path Computation Element - элемент расчета пути.
[8]Network Management Entity - элемент управления сетью.

Южный (сетевой) интерфейс позволяет объектам плоскости контроллера взаимодействовать с устройствами в плоскости сети, как показано на рисунке 7. Этот интерфейс использует и расширяет TEAS для описания физической топологии и ресурсов в плоскости сети.

Узлы DetNet (и, возможно, сетевые адаптеры конечных систем) раскрывают свои возможности и физические ресурсы контроллеру (CPF) и обновляют CPF своим динамическим восприятием топологии через южный интерфейс. В ответ CPF организуют пути на уровне потоков, обеспечивая характеристики потока, которые более тесно связаны с работой узла DetNet, нежели TSpec.

В сетевой плоскости узлы DetNet могут обмениваться информацией о состоянии путей между смежными узлами DetNet и, возможно, к конечным системам и пересылать пакеты в рамках ограничений, связанных с каждым потоком, или (при невозможности пересылки) выполнять такие операции, как отбрасывание или деклассификация.

В этом документе основное внимание уделено южному интерфейсу и сетевой плоскости.

4.5. Очереди, формирование, планирование и вытеснение трафика

DetNet обеспечивает ограничение задержки за счет резервирования пропускной способности и буферов на каждом узле DetNet в пути потока DetNet. Однако резервирование не решает всех задач. Разработчики и пользователи многих фирменных и стандартных сетевых решений для работы в реальном масштабе времени отмечают необходимость стандартов для методов плоскости данных, позволяющих обеспечивать эти гарантии в сетях с оборудованием разных производителей. Основная причина заключается в том, что изменение задержки в одной системе DetNet ведет к необходимости увеличения размера буферов в следующей системе или системах DetNet, что ведет к дополнительному росту задержки на этапах пересылки.

Стандартные алгоритмы организации очередей и выбора передачи позволяют TE (4.4. Организация трафика для DetNet) рассчитать вклад задержки на каждом узле в общую задержку DetNet, размер буферов на каждом узле DetNet для каждого инкрементного потока DetNet, а также, что более важно, преобразовать спецификацию потока в набор значений для объектов управления на каждом ретрансляторе и конечной системе. Например, рабочая группа IEEE 802.1 задала набор алгоритмов очередей, формовки и планирования, позволяющий каждому узлу DetNet или центральному контроллеру рассчитать эти значения. Эти алгоритмы включают:

- формовщик на основе кредитов [IEEE802.1Qav] (включено в [IEEE802.1Q]);
- очереди с ограничением по времени и чередующимся расписанием на основе синхронизированных часов [IEEE802.1Qbv] (включен во [IEEE802.1Q]);
- синхронизированные двойные (или тройные) буферы, управляемые синхронизированными часами [IEEE802.1Qch] (включено в [IEEE802.1Q]);
- вытеснение передачи пакетов Ethernet пакетами с более строгими требованиями к задержке [IEEE802.1Qbu] (включен в [IEEE802.1Q]) [IEEE802.3br] (включено в [IEEE802.3]).

Хотя эти методы в настоящее время включены лишь в стандарты Ethernet [IEEE802.3] и мостов, следует отметить, что они (за исключением, возможно, вытеснения пакетов) применимы к средам иных типов, а также к маршрутизаторам. В других средах могут применяться свои методы (например, [TSCH-ARCH] и [RFC7554]). В IETF также разработаны свои методы (например, [RFC8289] и [RFC8033]). DetNet может включить эти определения в будущем и описать их применение на узлах DetNet.

4.6. Экземпляр сервиса

Экземпляр сервиса представляет все функции, нужные на узле DetNet для организации сквозного сервиса между UNI.

Эталонная модель сети DetNet показана на рисунке 8 для сервиса DetNet (т. е. между парой DetNet-UNI). На рисунке конечные системы (A и B) подключены напрямую к граничным узлам сети IP/MPLS (PE1 и PE2). Для конечных систем, участвующих в коммуникациях DetNet, подключение может потребоваться до организации потока приложения, которому нужны услуги DetNet. Такой экземпляр сервиса, относящийся к подключению, и экземпляр, выделенный для сервиса DetNet, используют общий доступ. Пакеты, относящиеся к потоку DetNet, выбираются фильтром, настроенным для доступа (F1 и F2). В результате связанный с потоком доступ (Доступ-A + F1 и Доступ-B + F2) завершается в связанном с потоком экземпляре сервиса (SI-1 и SI-2). Туннель обеспечивает связность экземпляров.

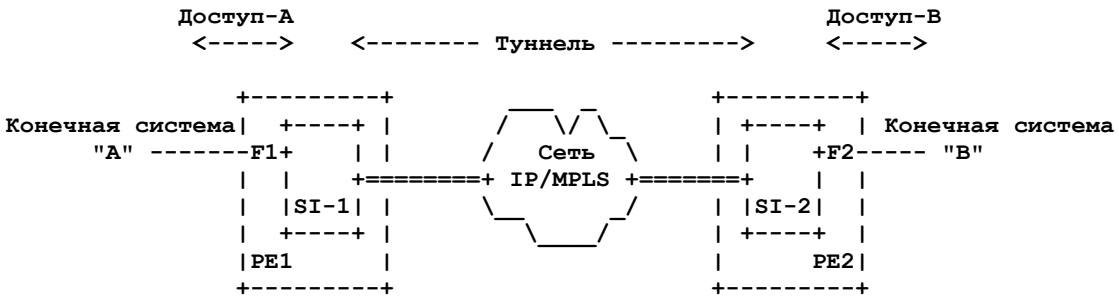

Рисунок 8. Эталонная модель сети DetNet.

Туннель используется исключительно для пакетов потока DetNet между SI-1 и SI-2. Экземпляры сервиса настроены на реализацию функций DetNet и связанной с потоком пересылки DetNet. Экземпляры и туннель могут поддерживать несколько потоков DetNet. Для совместного использования экземпляров сервиса несколькими потоками нужно соответственно заполнить таблицы пересылки этих экземпляров.

Туннель может иметь особые свойства. Например, в DetNet L3 имеются отличия использования PW для трафика DetNet от модели, описанной в [RFC6658]. В варианте DetNet псевдопровод PW служит лишь для потока DetNet, тогда как в [RFC6658] сказано:

Пакетный PW выглядит для клиентского уровня как один канал «точка-точка». Организация и поддержка смежности на сетевом уровне между клиентскими устройствами будет следовать обычной практике поддержки нужных отношений на уровне клиентов.

и

Этот пакетный псевдопровод используется для транспортировки всех протоколов L2 и L3 между LSR1 и LSR2.

Дополнительные детали зависят от сетевой технологии и описаны в [DETNET-FRAMEWORK].

4.7. Идентификация потоков на границах технологии

В этом разделе описаны действия, которые нужно выполнять на границах технологий, включая Ethernet, как одну из них. Идентификация потоков для плоскостей данных MPLS и IP описана в [DETNET-MPLS] и [DETNET-IP].

4.7.1. Экспорт идентификации потоков

Узлу DetNet может потребоваться отобразить конкретные потоки на потоки нижележащих уровней (Stream) для обеспечения требуемых услуг по управлению очередями и формовке трафика.

- Конечная система-источник L2 (не IP) X может передавать множество потоков другой конечной системе L2 Y. Эти потоки могут включать потоки DetNet с разными требованиями QoS, а также потоки иного трафика.
- Маршрутизатор может передавать любое число потоков другому маршрутизатору. Здесь также могут быть потоки DetNet с разными требованиями QoS и потоки, не относящиеся к DetNet.
- Два маршрутизатора могут быть разделены мостами. Чтобы мосты могли организовать очереди и формовку на уровне потоков, им нужно идентифицировать отдельные потоки.
- Маршрутизатор LER может иметь LSP для обслуживания трафика, направленного по конкретному адресу IP и содержащего лишь не относящиеся к DetNet потоки. При запросе потока DetNet в тот же адрес может потребоваться отдельный LSP, чтобы все маршрутизаторы LSR в пути к получателю обеспечили нужные очереди и формовку трафика.

Необходимость информирования нижележащих уровней о потоках не уникальна для DetNet. Но с учетом сложности уровней и ретрансляции через туннели, которые доступны разработчикам, в DetNet требуется модель идентификации потоков, которая лучше просмотра пакетов. Это не означает, что не будет применяться просмотр пакетов на уровне L4/L5 или возможность стандартизована, однако возможны варианты.

Ретранслятор DetNet может направлять потоки DetNet по разным путям, используя разные методы идентификации.

- Одиночному потоку DetNet от маршрутизатора A, проходящему через сеть мостов в маршрутизатор B, можно назначить идентификатор TSN Stream, уникальный для сети мостов. После этого мосты смогут узнавать поток без просмотра заголовков вышележащих уровней. Принимающий маршрутизатор также должен понимать и воспринимать TSN Stream.
- Потоку DetNet от LSR A к LSR B можно назначить метку, отличающуюся от метки другого трафика в тот же IP.

В обоих случаях имеющийся поток DetNet может содержать в себе множество других потоков DetNet (не путайте составные потоки и потоки участников DetNet). Для этого требуется корректная подготовка потока DetNet для передачи агрегированных потоков.

Таким образом, вместо просмотра пакетов можно экспортировать информацию вышележащего уровня на нижележащий. Требование поддержки того или иного (или обоих) метода идентификации потоков является сложностью, относящейся к моделям управления DetNet.

4.7.2. Отображение атрибутов потока между уровнями

Пересылка пакетов потока DetNet через домены с разной технологией может потребовать от нижних уровней осведомленности о конкретных потоках вышележащих уровней. Такой «экспорт идентификации потоков» требуется всякий раз, когда в пути меняется парадигма пересылки (например, пара LSR соединена через домен мостов L2). В DetNet рассматриваются три типичных метода пересылки:

- маршрутизация IP;
- коммутация по меткам MPLS;
- мосты Ethernet.

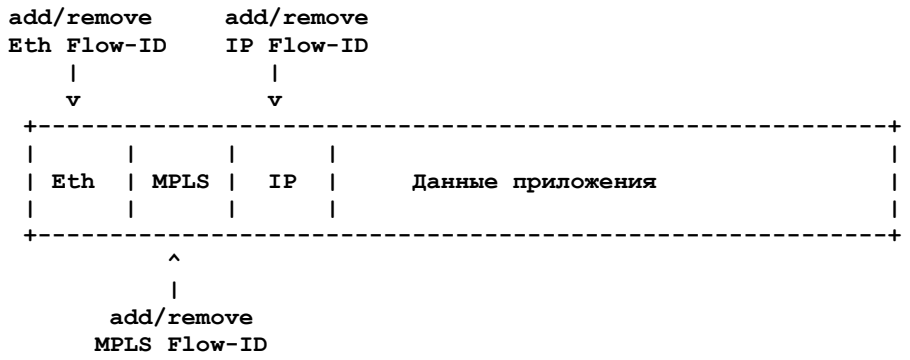

Рисунок 9. Пакет с множеством Flow-ID.

На рисунке 9 показан пакет с несколькими Flow-ID и указаны точки добавления и удаления каждого Flow-ID.

Дополнительными (в зависимости от домена) Flow-ID могут быть:

- идентификаторы, созданные специальной функцией домена;
- идентификаторы, полученные добавлением Flow-ID к App-flow.

Значение Flow-ID должно быть уникальным в рамках домена. Отметим, что Flow-ID, добавляемые к App-flow, продолжают оставаться в пакетах, но некоторые узлы могут не иметь функций для их распознавания, поэтому используется дополнительный Flow-ID.

4.7.3. Примеры отображений Flow-ID

Узлы IP и MPLS предполагаются настроенными на вталкивание дополнительных (зависящих от домена) Flow-ID при передаче трафика коммутатору Ethernet, как показано в примерах ниже.

На рисунке 10 показана конечная система IP (IP-A), подключенная через два коммутатора Ethernet (ETH-n) к маршрутизатору IP (IP-1).

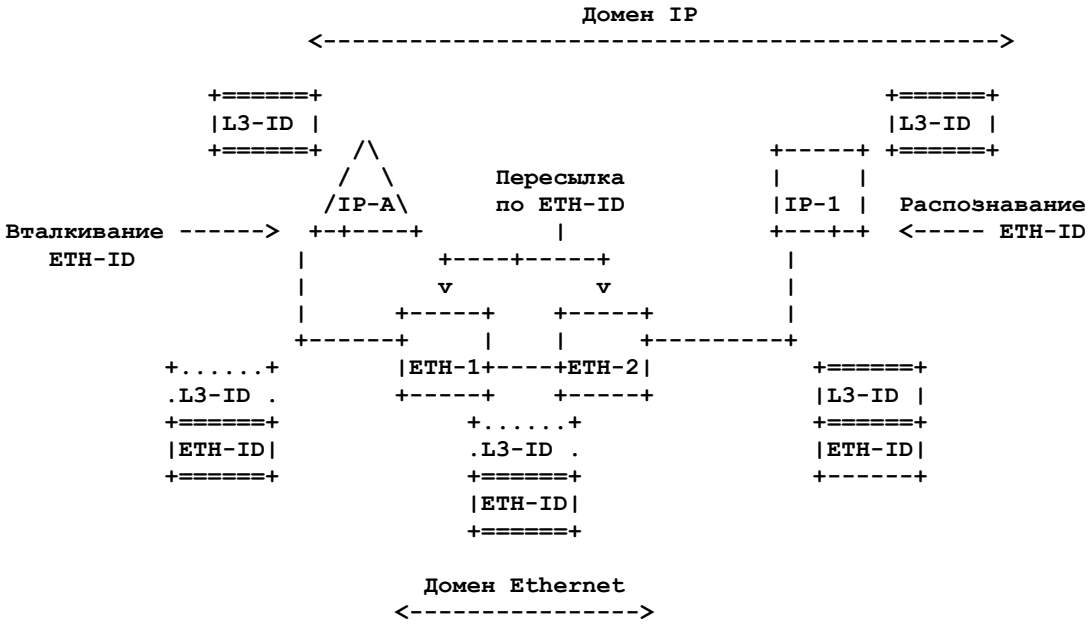

Рисунок 10. Соединение узлов IP через домен Ethernet.

Система IP-A использует исходный идентификатор потока приложения L3-ID, но она подключена к домену Ethernet, поэтому помещает в пакет, связанный с этим доменом, Flow-ID (ETH-ID) перед отправкой пакета ETH-1. Коммутатор ETH-1 может распознать поток по ETH-ID и пересылает его ETH-2, который коммутирует пакет маршрутизатору IP. Маршрутизатор IP-1 должен быть настроен на прием группового потока, указанного Ethernet Flow-ID. Он является устройством L3 и декодирует идентификатор потока данных по полям L3-ID в полученных пакетах.

На рисунке 11 показаны узлы домена MPLS (PE-n и P-m) соединенные через два коммутатора Ethernet (ETH-n).

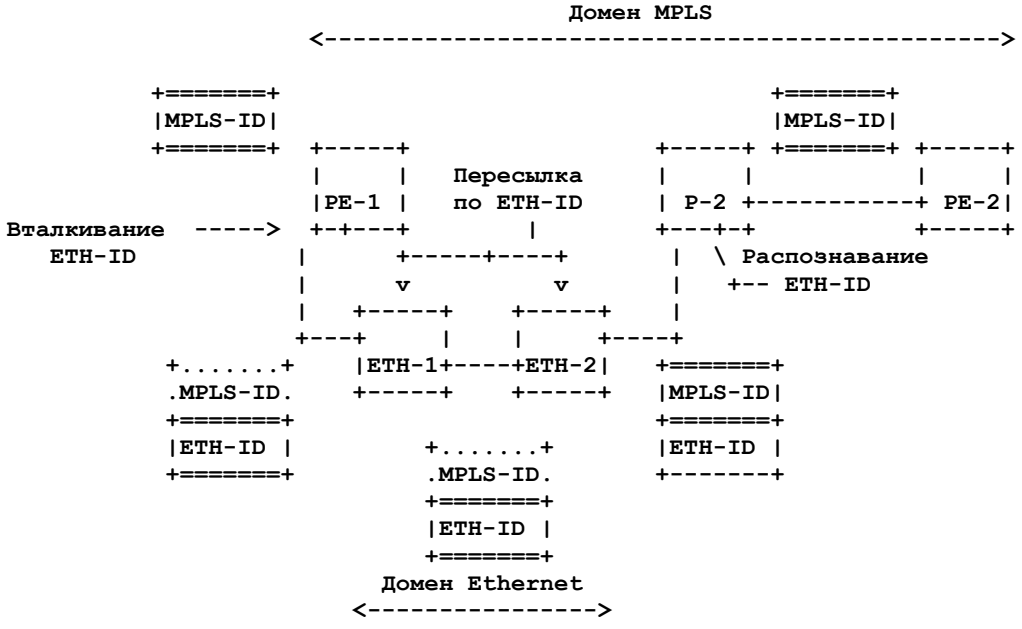

Рисунок 11. Соединение узлов MPLS через домен Ethernet.

PE-1 использует идентификатор MPLS-ID, но этот узел подключен к домену Ethernet и вталкивает идентификатор для этого домена (ETH-ID) перед отправкой пакета ETH-1. Коммутатор ETH-1 может распознать поток данных по ETH-ID и пересылает его ETH-2, который коммутирует пакеты узлу MPLS (P-2). Узел P-2 должен быть настроен на получение группового потока по Ethernet Flow-ID. Он является узлом MPLS и декодирует идентификатор потока данных по полям MPLS-ID в принятых пакетах.

Из приведенных примеров можно понять, что при изменении или экспорте способов идентификации потока DetNet нужно соответствующим образом менять или экспортировать средства информирования о порядковых номерах.

4.8. Анонсирование ресурсов, возможностей и соседства

Для подготовки сервиса DetNet нужно иметь указанные ниже сведения.

- Данные о возможностях системы DetNet, которые нужны для точного выделения ресурсов этой и другим системам DetNet. Это включает, например, реализуемые алгоритмы очередей и формирования трафика (4.5. Очереди, формирование, планирование и вытеснение трафика), объем буферов для выделения DetNet, наихудшие допустимые задержка и нарушение порядка доставки.
- Фактическое состояние ресурсов DetNet на узле DetNet.
- Идентификационные данные соседей системы DetNet и характеристики каналов между системами DetNet, включая задержку в наносекундах.

4.9. Большие сети

Резервирование для отдельных потоков DetNet требует обширной информации о состоянии в каждом узле DetNet, особенно если требуется адекватное устранение отказов (3.3.2. Устранение отказов). Плоскость данных DetNet для поддержки большого числа потоков DetNet должна обеспечивать агрегирование потоков DetNet. Такие агрегированные потоки могут рассматриваться плоскостями данных узлов DetNet как отдельные потоки DetNet. Без такого агрегирования система на уровне ретранслятора может ограничивать размеры сетей DetNet. Примеры используемых методов включают иерархию MPLS и коды IP DiffServ (DSCP).

4.10. Совместимость с уровнями L2

Стандарты, обеспечивающие похожие возможности в сетях на основе (лишь) мостов, были созданы в IEEE 802 LAN/MAN Standards Committee. Представленная архитектура описывает абстрактную модель, которая может применяться к L2 и L3, а также к каналам, не определенным IEEE 802.

Конечные системы с поддержкой DetNet и узлы DetNet могут соединяться через подсети, т. е. технологией L2. Эти подсети будут предоставлять совместимые с DetNet услуги для поддержки трафика DetNet. Примеры технологий таких подсетей включают MPLS TE, IEEE 802.1 TSN и каналы точка-точка в OTN. Возможны и многоуровневые системы DetNet, где сеть DetNet выступает в качестве подсети для системы DetNet более высокого уровня.

5. Вопросы безопасности

Вопросы безопасности DetNet подробно рассмотрены в [DETNET-SECURITY]. Здесь обсуждаются лишь вопросы безопасности, связанные в архитектурой DetNet.

Уникальными для DetNet аспектами безопасности являются вопросы QoS в DetNet, которые связаны с максимально низкой потерей пакетов и ограниченной сквозной задержкой. DetNet может работать на основе MPLS или IP (v4 и v6), наследуя их защитные свойства в плоскостях данных и управления.

Вопросы безопасности для DetNet ограничены (например, по сравнению с открытой сетью Internet), DetNet работает только внутри одного административного домена (1. Введение). В первую очередь нужно обеспечить безопасность запроса и управления ресурсами DetNet, конфиденциальность данных DetNet и доступность DetNet QoS.

Для защиты запросов и управления ресурсами DetNet может применяться аутентификация и контроль полномочий для каждого устройства, подключенного к домену DetNet, что наиболее важно для устройств управления сетью. Управление сетью DetNet может быть централизованным или распределенным (внутри административного домена). Для централизованного управления вопросы безопасности в сетях ACTN[1] рассмотрены в разделе 9 [RFC8453]. При использовании протоколов распределенного управления предполагается, что безопасность DetNet обеспечивается свойствами применяемых протоколов. В любом случае возможности манипулировать административно задаваемыми параметрами предоставляются лишь уполномоченным элементам (лицам).

Для обеспечения конфиденциальности данных в DetNet потоки приложений можно защищать с использованием возможностей базовой технологии. Например, может применяться шифрование, обеспечиваемое IPsec [RFC4301] для потоков IP и MACSec [IEEE802.1AE] для потоков Ethernet (L2).

Идентификация DetNet на уровне потоков может предоставить атакующим дополнительную информацию о потоках данных (в сети обычно нет идентификации на уровне потока). Это свойство, присущее DetNet, оказывает влияние на безопасность и должно учитываться при решении вопроса о выборе DetNet в качестве технологии передачи данных.

Для обеспечения бесперебойной доступности DetNet QoS могут применяться меры защиты от DoS-атак и добавления задержек. Для защиты от атак на службы (DoS) избыточный трафик злонамеренных или неисправных устройств можно предотвращать или ослаблять, например, с помощью контроля допуска трафика на входе в домен DetNet, как описано в параграфе 3.2.1, или с помощью методов устранения отказов, описанных в параграфе 3.3.2. Для предотвращения задержки пакетов устройствами за пределами домена DetNet выбор технологии DetNet может смягчить MITM[2]-атаки, например, за счет аутентификации и контроля полномочий устройств внутри домена DetNet.

Поскольку механизмы DetNet и приложения, опирающиеся на DetNet, могут широко применять методы, требующие синхронизации часов, точность, доступность и целостность синхронизации очень важны. Этот вопрос рассмотрен в [RFC7384].

Известны случаи применения к DetNet самых разных требований безопасности. Целью этого раздела является предоставление основы для решения общих проблем безопасности всех вариантов и реализаций DetNet без учета специфики инфраструктуры защиты, которая может не подойти для конкретного случая. Предполагается, что при разработке и реализации систем DetNet будут учитываться особенности конкретного устройства и реализаций.

[1]Abstraction and Control of Traffic Engineered Network.
[2]Man-in-the-middle - перехват и изменение трафика с участием человека.

6. Вопросы конфиденциальности

DetNet обеспечивает QoS и для этих механизмов применяются базовые соображения. В частности, маркировка позволяет атакующим сопоставить потоки или выбрать определенный тип потока для более предметного анализа.

Требование к каждому (или почти каждому) узлу пути потока DetNet идентифицировать потоки DetNet может открывать новую возможность атак на конфиденциальность, если парадигма DetNet будет использоваться более широко.

7. Взаимодействие с IANA

Документ не требует действий со стороны IANA.

8. Литература

[BUFFERBLOAT] Gettys, J. and K. Nichols, "Bufferbloat: Dark Buffers in the Internet", DOI 10.1145/2063176.2063196, Communications of the ACM, Volume 55, Issue 1, January 2012, <https://doi.org/10.1145/2063176.2063196>.

[CCAMP] IETF, "Common Control and Measurement Plane (ccamp)", October 2019, <https://datatracker.ietf.org/wg/ccamp/charter/>.

[DETNET-FRAMEWORK] Varga, B., Farkas, J., Berger, L., Fedyk, D., Malis, A., Bryant, S., and J. Korhonen, "DetNet Data Plane Framework", Work in Progress[1], Internet-Draft, draft-ietf-detnet-data-plane-framework-02, 13 September 2019, <https://tools.ietf.org/html/draft-ietf-detnet-data-plane-framework-02>.

[DETNET-IP] Varga, B., Farkas, J., Berger, L., Fedyk, D., Malis, A., Bryant, S., and J. Korhonen, "DetNet Data Plane: IP", Work in Progress[2], Internet-Draft, draft-ietf-detnet-ip-01, 1 July 2019, <https://tools.ietf.org/html/draft-ietf-detnet-ip-01>.

[DETNET-MPLS] Varga, B., Farkas, J., Berger, L., Fedyk, D., Malis, A., Bryant, S., and J. Korhonen, "DetNet Data Plane: MPLS", Work in Progress, Internet-Draft, draft-ietf-detnet-mpls-01, 1 July 2019, <https://tools.ietf.org/html/draft-ietf-detnet-mpls-01[3]>.

[DETNET-SECURITY] Mizrahi, T., Grossman, E., Hacker, A., Das, S., Dowdell, J., Austad, H., Stanton, K., and N. Finn, "Deterministic Networking (DetNet) Security Considerations", Work in Progress, Internet-Draft, draft-ietf-detnet-security-05, 29 August 2019, <https://tools.ietf.org/html/draft-ietf-detnet-security-05[4]>.

[IEC-62439-3] IEC, "Industrial communication networks — High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)", TC 65 / SC 65C, IEC 62439-3:2016, March 2016, <https://webstore.iec.ch/publication/24447>.

[IEEE802.1AE] IEEE, "IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security", IEEE 802.1AE-2018, <https://ieeexplore.ieee.org/document/8585421>.

[IEEE802.1BA] IEEE, "IEEE Standard for Local and metropolitan area networks--Audio Video Bridging (AVB) Systems", IEEE 802.1BA-2011, <https://ieeexplore.ieee.org/document/6032690>.

[IEEE802.1CB] IEEE, "IEEE Standard for Local and metropolitan area networks--Frame Replication and Elimination for Reliability", DOI 10.1109/IEEESTD.2017.8091139, IEEE 802.1CB-2017, October 2019, <https://ieeexplore.ieee.org/document/8091139>.

[IEEE802.1Q] IEEE, "IEEE Standard for Local and Metropolitan Area Network--Bridges and Bridged Networks", IEEE 802.1Q-2018, <https://ieeexplore.ieee.org/document/8403927>.

[IEEE802.1Qav] IEEE, "IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks Amendment 12: Forwarding and Queuing Enhancements for Time-Sensitive Streams", IEEE 802.1Qav-2009, <https://ieeexplore.ieee.org/document/5375704>.

[IEEE802.1Qbu] IEEE, "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks -- Amendment 26: Frame Preemption", IEEE 802.1Qbu-2016, <https://ieeexplore.ieee.org/document/7553415>.

[IEEE802.1Qbv] IEEE, "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks - Amendment 25: Enhancements for Scheduled Traffic", IEEE 802.1Qbv-2015, <https://ieeexplore.ieee.org/document/7440741>.

[IEEE802.1Qch] IEEE, "IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks--Amendment 29: Cyclic Queuing and Forwarding", IEEE 802.1Qch-2017, <https://ieeexplore.ieee.org/document/7961303>.

[IEEE802.1TSNTG] IEEE, "Time-Sensitive Networking (TSN) Task Group", <https://1.ieee802.org/tsn/>.

[IEEE802.3] IEEE, "IEEE Standard for Ethernet", IEEE 802.3-2018, <https://ieeexplore.ieee.org/document/8457469>.

[IEEE802.3br] IEEE, "IEEE Standard for Ethernet Amendment 5: Specification and Management Parameters for Interspersing Express Traffic", IEEE 802.3br, <https://ieeexplore.ieee.org/document/7900321>.

[1]Работа опубликована в RFC 8938. *Прим. перев.*
[2]Работа опубликована в RFC 8939. *Прим. перев.*
[3]Доступен более свежий вариант https://tools.ietf.org/html/draft-ietf-detnet-mpls-13. *Прим. перев.*
[4]Доступен более свежий вариант https://tools.ietf.org/html/draft-ietf-detnet-security-12. *Прим. перев.*

[RFC2205] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, DOI 10.17487/RFC2205, September 1997, <https://www.rfc-editor.org/info/rfc2205>.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, DOI 10.17487/RFC2475, December 1998, <https://www.rfc-editor.org/info/rfc2475>.

[RFC2914] Floyd, S., "Congestion Control Principles", BCP 41, RFC 2914, DOI 10.17487/RFC2914, September 2000, <https://www.rfc-editor.org/info/rfc2914>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, DOI 10.17487/RFC3168, September 2001, <https://www.rfc-editor.org/info/rfc3168>.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <https://www.rfc-editor.org/info/rfc3209>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <https://www.rfc-editor.org/info/rfc3550>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4655] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <https://www.rfc-editor.org/info/rfc4655>.

[RFC6372] Sprecher, N., Ed. and A. Farrel, Ed., "MPLS Transport Profile (MPLS-TP) Survivability Framework", RFC 6372, DOI 10.17487/RFC6372, September 2011, <https://www.rfc-editor.org/info/rfc6372>.

[RFC6658] Bryant, S., Ed., Martini, L., Swallow, G., and A. Malis, "Packet Pseudowire Encapsulation over an MPLS PSN", RFC 6658, DOI 10.17487/RFC6658, July 2012, <https://www.rfc-editor.org/info/rfc6658>.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014, <https://www.rfc-editor.org/info/rfc7149>.

[RFC7384] Mizrahi, T., "Security Requirements of Time Protocols in Packet Switched Networks", RFC 7384, DOI 10.17487/RFC7384, October 2014, <https://www.rfc-editor.org/info/rfc7384>.

[RFC7426] Haleplidis, E., Ed., Pentikousis, K., Ed., Denazis, S., Hadi Salim, J., Meyer, D., and O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology", RFC 7426, DOI 10.17487/RFC7426, January 2015, <https://www.rfc-editor.org/info/rfc7426>.

[RFC7554] Watteyne, T., Ed., Palattella, M., and L. Grieco, "Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement", RFC 7554, DOI 10.17487/RFC7554, May 2015, <https://www.rfc-editor.org/info/rfc7554>.

[RFC7567] Baker, F., Ed. and G. Fairhurst, Ed., "IETF Recommendations Regarding Active Queue Management", BCP 197, RFC 7567, DOI 10.17487/RFC7567, July 2015, <https://www.rfc-editor.org/info/rfc7567>.

[RFC7813] Farkas, J., Ed., Bragg, N., Unbehagen, P., Parsons, G., Ashwood-Smith, P., and C. Bowers, "IS-IS Path Control and Reservation", RFC 7813, DOI 10.17487/RFC7813, June 2016, <https://www.rfc-editor.org/info/rfc7813>.

[RFC8033] Pan, R., Natarajan, P., Baker, F., and G. White, "Proportional Integral Controller Enhanced (PIE): A Lightweight Control Scheme to Address the Bufferbloat Problem", RFC 8033, DOI 10.17487/RFC8033, February 2017, <https://www.rfc-editor.org/info/rfc8033>.

[RFC8227] Cheng, W., Wang, L., Li, H., van Helvoort, H., and J. Dong, "MPLS-TP Shared-Ring Protection (MSRP) Mechanism for Ring Topology", RFC 8227, DOI 10.17487/RFC8227, August 2017, <https://www.rfc-editor.org/info/rfc8227>.

[RFC8289] Nichols, K., Jacobson, V., McGregor, A., Ed., and J. Iyengar, Ed., "Controlled Delay Active Queue Management", RFC 8289, DOI 10.17487/RFC8289, January 2018, <https://www.rfc-editor.org/info/rfc8289>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[RFC8453] Ceccarelli, D., Ed. and Y. Lee, Ed., "Framework for Abstraction and Control of TE Networks (ACTN)", RFC 8453, DOI 10.17487/RFC8453, August 2018, <https://www.rfc-editor.org/info/rfc8453>.

[RFC8557] Finn, N. and P. Thubert, "Deterministic Networking Problem Statement", RFC 8557, DOI 10.17487/RFC8557, May 2019, <https://www.rfc-editor.org/info/rfc8557>.

[RFC8578] Grossman, E., Ed., "Deterministic Networking Use Cases", RFC 8578, DOI 10.17487/RFC8578, May 2019, <https://www.rfc-editor.org/info/rfc8578>.

[TEAS] IETF, "Traffic Engineering Architecture and Signaling (teas)", October 2019, <https://datatracker.ietf.org/doc/charter-ietf-teas/>.

[TSCH-ARCH] Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", Work in Progress, Internet-Draft, draft-ietf-6tisch-architecture-26, 27 August 2019, <https://tools.ietf.org/html/draft-ietf-6tisch-architecture-26[1]>.

Благодарности

Авторы благодарны Lou Berger, David Black, Stewart Bryant, Rodney Cummings, Ethan Grossman, Craig Gunther, Marcel Kiessling, Rudy Klecka, Jouni Korhonen, Erik Nordmark, Shitanshu Shah, Wilfried Steiner, George Swallow, Michael Johas Teener, Pat Thaler, Thomas Watteyne, Patrick Wetterwald, Karl Weber и Anca Zamfir за их вклад в эту работу.

Адреса авторов

Norman Finn

Huawei

3101 Rio Way

Spring Valley, California 91977

United States of America

Phone: +1 925 980 6430

Email: nfinn@nfinnconsulting.com

Pascal Thubert

Cisco Systems

Batiment T3

Village d'Entreprises Green Side, 400, Avenue de Roumanille

06410 Biot - Sophia Antipolis

France

Phone: +33 4 97 23 26 34

Email: pthubert@cisco.com

Balázs Varga

Ericsson

Budapest

Magyar tudosok korutja 11

1117

Hungary

Email: balazs.a.varga@ericsson.com

János Farkas

Ericsson

Budapest

Magyar tudosok korutja 11

1117

Hungary

Email: janos.farkas@ericsson.com

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru

[1]Доступен более свежий вариант https://tools.ietf.org/html/draft-ietf-6tisch-architecture-30. *Прим. перев.*