Internet Engineering Task Force (IETF)
Request for Comments: 7276
Category: Informational
ISSN: 2070-1721

T. Mizrahi
Marvell
N. Sprecher
Nokia Solutions and Networks
E. Bellagamba
Ericsson
Y. Weingarten
June 2014

An Overview of Operations, Administration, and Maintenance (OAM) Tools

Обзор инструментария OAM

Аннотация

Базовый термин OAM[1] относится к набору средств для обнаружения и изоляции отказов, а также измерения производительности. За многие годы инструменты OAM были созданы для разных уровней стека протоколов.

Этот документ описывает некоторые инструменты OAM, определенные в IETF в контексте индивидуальной адресации IP, MPLS, MPLS-TP[2], псевдопроводов и TRILL[3]. Документ посвящен инструментам для обнаружения и изоляции отказов в сетях, а также для мониторинга производительности. Аспекты управления и поддержки OAM выходят за рамки этого документа. Функции восстановления, такие как FRR[4] и защитное переключение также не рассматриваются здесь, хотя они зачастую вызываются протоколами OAM.

Целевая аудитория документа включает производителей сетевого оборудования, сетевых операторов и разработчиков стандартов. Документ может служить справочником по основным инструментам OAM, определенным в IETF. В конце документа представлен список инструментария OAM и функций OAM.

Статус документа

Документ не является проектом стандарта Internet и публикуется с информационными целями.

Документ является результатом работы IETF[5] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[6]. Не все одобренные IESG документы претендуют на статус Internet Standard (см. раздел 2 в RFC 5741).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc7276.

Авторские права

Авторские права (Copyright (c) 2014) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (http://trustee.ietf.org/license-info), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

Оглавление

[1] Operations, Administration, and Maintenance - эксплуатация, администрирование, обслуживание.
[2] MPLS Transport Profile - транспортный профиль MPLS.
[3] Transparent Interconnection of Lots of Links - прозрачное соединение между множеством каналов.
[4] Fast Reroute - быстрая перемаршрутизация.
[5] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[6] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

OAM служит общим термином для обнаружения, изоляции, информирования об отказах и мониторинга работы сетей.

Имеется несколько интерпретаций аббревиатуры OAM. В этом документе используется Operations, Administration, and Maintenance (эксплуатация, администрирование, обслуживание), как рекомендовано в разделе 3 [OAM-Def].

Здесь рассмотрены несколько инструментов OAM, определенных IETF в контексте индивидуальной адресации IP, MPLS, MPLS-TP, псевдопроводов и TRILL.

Документ посвящён инструментам для обнаружения и изоляции отказов в сетях, а также для мониторинга производительности. Поэтому документ рассматривает инструменты для мониторинга и измерения на уровне данных, а вопросы управления и поддержки OAM выходят за рамки этого документа. Функции восстановления, такие как FRR и защитное переключение также не рассматриваются здесь, хотя они зачастую вызываются протоколами OAM.

1.1. Обоснование

Методы OAM, исходно применявшиеся в традиционных технологиях связи, таких как E1 и T1, перешли в PDH[1], а затем в SONET/SDH[2]. ATM была возможно первой технологией со встроенной изначально поддержкой OAM, тогда как в других технологиях функции OAM обычно добавлялись специальным образом уже после определения и развёртывания технологии. Сети на основе пакетов традиционно считались ненадёжными и доставляющими данные по мере возможности (best effort). По мере развития пакетных сетей они становились базовым транспортом для передачи данных и телефонии, заменив традиционные транспортные протоколы. Поэтому предполагается, что в пакетных сетях будет обеспечиваться «операторский уровень» и, в частности, поддержка более развитых функций OAM в дополнение к ICMP и router hello, которые традиционно служили для обнаружения отказов.

[1]Plesiochronous Digital Hierarchy - плезиохронная цифровая иерархия.
[2]Synchronous Optical Network/Synchronous Digital Hierarchy - синхронная оптическая сеть, синхронная цифровая иерархия.

Поскольку типичная сеть имеет многоуровневую архитектуру, набор протоколов OAM также включает множество уровней, каждый из которых имеет свои протоколы OAM. Кроме того, OAM может применяться на разных уровнях сетевой иерархии, формируя многоуровневое решение OAM, как показано в примере на рисунке 1.

Рисунок 1 показывает сеть, в которой трафик IP между двумя абонентскими границами передается через операторскую сеть MPLS. На уровне провайдера применяется MPLS OAM для мониторинга соединений между двумя граничными точками, а на уровне абонента применяется IP OAM для сквозного мониторинга соединений между двумя абонентскими сетями.

```
             |<------------ Абонентский уровень OAM ------------>|
                   IP OAM (Ping, Traceroute, OWAMP, TWAMP)

                          |<-Провайдерский уровень->|
                              MPLS OAM (LSP Ping)

      +-----+       +-----+                         +-----+      +-----+
      |     |       |     |=========================|     |      |     |
      |     |-------|     |          MPLS           |     |------|     |
      |     |  IP   |     |                         |     |  IP  |     |
      +-----+       +-----+                         +-----+      +-----+
      Граница       Граница                        Граница       Граница
      абонента      провайдера                     провайдера   абонента
```

Рисунок 1. Пример многоуровневой организации OAM.

1.2. Целевая аудитория

Этот документ предназначен прежде всего указанным ниже категориям читателей.

- Организации, разрабатывающие стандарты, включая рабочие группы IETF и другие организации, могут воспользоваться этим документом при разработке новых протоколов OAM или поиске возможности применения имеющихся инструментов OAM для новых технологий.
- Производители оборудования и сетевые операторы могут пользоваться этим документом в качестве краткого справочника по инструментам IETF OAM.

Следует отметить, что для понимания и использования этого документа нужны некоторые базовые знания в части OAM. Предполагается, что читателю понятен термин OAM [OAM-Def], мотивы использования OAM и различия между OAM и управлением сетью [OAM-Mng].

1.3. Связанные с OAM работы в IETF

Этот документ содержит обзор разных наборов инструментов OAM, определённых IETF. Описанные здесь инструменты OAM применимы к индивидуальному трафику IP, MPLS, псевдопроводам, MPLS-TP и TRILL. Инструменты OAM имеются и для других технологий, но они выходят за рамки документа.

Этот документ сосредоточен на документах IETF, опубликованных как RFC, а другие работы, связанные с OAM, не рассматриваются. В IETF определены протоколы и инструменты OAM в разном контексте. Эти работы разделены на несколько крупных категорий связанных с OAM документов RFC, которые перечислены в таблице 1. Каждая категория определяет набор логически связанных RFC, хотя некоторые группы пересекаются.

Дальнейшее обсуждение в этом документе упорядоченно по этим группам (сокращения описаны в параграфе 2.1).

Таблица 1. Инструментальные средства OAM в документах IETF.

Инструмент	***Транспортная технология***
IP Ping	IPv4/IPv6
IP Traceroute	IPv4/IPv6
BFD	Базовая
MPLS OAM	MPLS
MPLS-TP OAM	MPLS-TP
Pseudowire OAM	Псевдопровода
OWAMP и TWAMP	IPv4/IPv6
TRILL OAM	TRILL

Этот документ сосредоточен на инструментах OAM, разработанных в IETF. Краткий обзор наиболее значимых стандартов OAM, разработанных другими организациями, приведен в приложении A.2.

1.4. Сосредоточенность на уровне данных

Инструменты OAM могут и достаточно часто работают совместно с уровнем управления и/или уровнем поддержки. OAM обеспечивает инструменты для измерений и мониторинга на уровне данных. Инструменты OAM часто используют функции уровня управления, например, для инициализации сессий OAM с целью обмена параметрами. Инструменты OAM взаимодействуют с уровнем поддержки для подачи сигналов и зачастую инструменты OAM могут активироваться уровнем поддержки (и уровнем управления), например, для обнаружения неполадок.

Рассмотрение средств поддержки уровня управления и функциональности уровня поддержки выходит за рамки этого документа, который сосредоточен на представлении инструментов уровня данных, применяемых в OAM. Функции восстановления, такие как быстрая перемаршрутизация (FRR) и защитные переключения, которые также часто вызываются протоколами OAM, не рассматриваются в этом документе.

Поскольку протоколу OAM используются для мониторинга уровня данных, они должны иметь возможность тестировать этот уровень с максимально возможной точностью. Поэтому важно обеспечить совместную передачу трафика инструментов OAM и трафика уровня данных, для которого выполняется мониторинг.

2. Терминология

2.1. Сокращения

ACH
Associated Channel Header - заголовок связанного канала.

AIS
Alarm Indication Signal - сигнал индикации тревоги.

ATM
Asynchronous Transfer Mode - асинхронный режим передачи.

BFD
Bidirectional Forwarding Detection - детектирование двухсторонней пересылки.

CC
Continuity Check - проверка непрерывности (работы).

CC-V
Continuity Check and Connectivity Verification - проверка связности и непрерывности.

CV
Connectivity Verification - проверка связности.

DM
Delay Measurement - измерение задержки.

ECMP
Equal-Cost Multipath - множество равноценных путей.

FEC
Forwarding Equivalence Class - класс эквивалентной пересылки.

FRR
Fast Reroute - быстрая перемаршрутизация.

G-ACh
Generic Associated Channel - базовый связанный канал.

GAL
Generic Associated Channel Label - метка базового связанного канала.

ICMP
Internet Control Message Protocol - протокол управляющих соединений Internet.

L2TP
Layer 2 Tunneling Protocol - протокол туннелирования на канальном уровне.

L2VPN
Layer 2 Virtual Private Network - виртуальная частная сеть на канальном уровне.

L3VPN
Layer 3 Virtual Private Network - виртуальная частная сеть на сетевом уровне.

LCCE
L2TP Control Connection Endpoint - конечная точка управляющего соединения L2TP.

LDP
Label Distribution Protocol - протокол распространения меток.

LER
Label Edge Router - краевой маршрутизатор по меткам.

LM
Loss Measurement - измерение потерь.

LSP
Label Switched Path - путь с коммутацией по меткам.

LSR
Label Switching Router - маршрутизатор с коммутацией по меткам.

ME
Maintenance Entity - элемент (сущность) обслуживания.

MEG
Maintenance Entity Group - группа элементов (сущностей) обслуживания.

MEP
MEG End Point - конечная точка MEG.

MIP
MEG Intermediate Point - промежуточная точка MEG.

MP
Maintenance Point - точка обслуживания.

MPLS
Multiprotocol Label Switching - многопротокольная коммутация по меткам.

MPLS-TP
MPLS Transport Profile - транспортый профиль MPLS.

MTU
Maximum Transmission Unit - максимальный передаваемый блок.

OAM
Operations, Administration, and Maintenance - эксплуатация, администрирование, обслуживание.

OWAMP
One-Way Active Measurement Protocol - протокол одностороннего активного измерения.

PDH
Plesiochronous Digital Hierarchy - плезиохронная цифровая иерархия

PE
Provider Edge - провайдерский край (периметр)

PSN
Public Switched Network - коммутируемая сеть общего пользования.

PW
Pseudowire - псевдопровод.

PWE3
Pseudowire Emulation Edge-to-Edge - сквозной псевдопровод.

RBridge
Routing Bridge - маршрутизирующий мост.

RDI
Remote Defect Indication - индикация удаленного дефекта.

SDH
Synchronous Digital Hierarchy - синхронная цифровая иерархия.

SONET
Synchronous Optical Network - синхронная оптическая сеть.

TRILL
Transparent Interconnection of Lots of Links - прозрачное соединение множества каналов.

TTL
Time To Live - время жизни.

TWAMP
Two-Way Active Measurement Protocol - протокол двухстороннего активного измерения.

VCCV
Virtual Circuit Connectivity Verification - проверка связности виртуального устройства (канала).

VPN
Virtual Private Network - виртуальная частная сеть.

2.2. Терминология в стандартах OAM

2.2.1. Базовые термины

В разных стандартах OAM используется множество терминов. В этом разделе сравниваются термины разных стандартов OAM без цитирования соответствующих определений.

Интересный обзор термина OAM и его производных представлен в [OAM-Def]. Справочник терминов MPLS-TP представлен в [TP-Term], где приведен хороший обзор некоторых терминов, связанных с OAM.

2.2.2. OAM

Приведенное ниже определение OAM заимствовано из [OAM-Def].

Компоненты аббревиатуры OAM (и предоставление) определяются, как показано ниже.

- Операции (operations) выполняются для поддержания работоспособности сети (и обеспечиваемых сетью услуг). Они включают мониторинг и поиск неполадок. В идеале проблемы следует находить до того, как они начнут влиять на пользователей.
- Администрирование (administration) включает контроль ресурсов сети и их использования, а также учет, который нужен для отслеживания ресурсов и контролируемой сети.
- Поддержка (maintenance) включает действия по техническому обслуживанию, направленные на содействие обновлению и ремонту, например, замену оборудования, установку программных обновления, добавления в сеть новых устройств. Поддержка также включает корректировку и предупреждающие меры для обеспечения более эффективного управления сетью, например, настройку конфигурации и параметров устройств.

2.2.3. Функции, инструменты и протоколы

OAM Function - функция OAM
Функцией OAM является тип инструментального измерения или диагностики.
Функции OAM являются неделимыми (atomic) блоками OAM и каждая функция определяет некую возможность OAM.
Типовые примеры функций OAM представлены в разделе 3.

OAM Protocol - протокол OAM
Протокол OAM служит для реализации одной или множества функций OAM.
Примером такого протокола является OWAMP-Test [OWAMP].

OAM Tool - инструмент OAM
Инструментом OAM называют конкретный способ выполнения одной или множества функций OAM.
В некоторых случаях протокол OAM является инструментом, например, OWAMP-Test. В иных случаях инструмент OAM применяет множество протоколов, которые могут быть не связаны строго с OAM, например, Traceroute (параграф 4.2) можно реализовать с использованием UDP и сообщений ICMP без протоколов OAM.

2.2.4. Уровни данных, управления и поддержки

Data Plane - уровень данных
Уровень данных представляет собой набор функций, применяемых для передаче данных в рассматриваемом «слое» или уровне [ITU-Terms].
Уровень данных называют также уровнем пересылки и пользовательским уровнем.

Control Plane - уровень управления
Уровень управления представляет собой набор протоколов и механизмов, позволяющих маршрутизаторам эффективно узнавать, как пересылать пакеты в направлении их конечного получателя (см. [Comp]).

Management Plane – уровень поддержки
Термин уровень поддержки (Management Plane), как описано в [Mng], применяется для описания обмена сообщениями по протоколам управления (часто доставляются с помощью IP и транспортных протоколов IP) между программами управления и управляемыми объектами, такими как узлы сети.

Сравнение уровней данных, управления и поддержки
Различие между уровнями не всегда достаточно четко. Например, приведенное выше определение Control Plane может подразумевать, что инструменты OAM (ping, BFD и др.) фактически относятся к уровню управления.

Этот документ посвящен инструментам для мониторинга уровня данных. Хотя эти инструменты можно отнести к уровню управления, на деле они контролируют уровень данных и поэтому трафик OAM для мониторинга уровня данных должен передаваться вместе с трафиком, для которого выполняется мониторинг.

Другая неопределенность относится к различию между уровнями поддержки и управления. Уровень поддержки можно считать отдельным, но он может перекрываться с уровнем управления (см. [Mng]).

2.2.5. Участники процесса

Инструменты OAM используются между двумя (или более) партнерами. В документах IETF применяются различные термины для обозначения участников OAM. В таблице 2 указаны термины, применяемые для каждого набора инструментов, описанных здесь.

Таблица 2. Точки поддержки.

Инструмент	Термины
Ping/Traceroute ([ICMPv4], [ICMPv6], [TCPIP-Tools])	Host - хост Node - узел Interface - инетрфейс Gateway - шлюз
BFD [BFD]	System - система
MPLS OAM [MPLS-OAM-FW]	LSR
MPLS-TP OAM [TP-OAM-FW]	End Point - MEP - конечная точка MEP Intermediate Point - MIP - промежуточная точка MEP
Pseudowire OAM [VCCV]	PE LCCE
OWAMP и TWAMP ([OWAMP], [TWAMP])	Host - хост End system - конечная система
TRILL OAM [TRILL-OAM]	RBridge - маршрутизирующий мост

2.2.6. Режим активации

Разные инструменты OAM можно использовать в одном из двух, описанных ниже, режимах активации.

Proactive - проактивный

Инструмент запускается заранее и работает в непрерывном режиме. Сообщения передаются периодически и отсутствие заданного числа сообщений считается ошибкой.

On-demand - по запросу

Инструмент запускается специально (воможно, вручную) для обнаружения конкретной аномалии.

2.2.7. Проверка связности и непрерывности

В протоколах OAM применяются два разных класса функций контроля отказов - проверка связности (Connectivity Verification) и проверка непрерывности работы (Continuity Check). Различия между этими функциями определены в [MPLS-TP-OAM] и данный документ следует этому определению.

Проверка непрерывности

Continuity Check используется для проверки доступности адресата обычно в проактивном режиме, хотя может вызываться и по запросу.

Проверка связности

Функция Connectivity Verification (CV) позволяет одному из партнеров (Alice) проверить наличие соединения с другим (Bob). Отмечено, что при выполнении функции CV на уровне данных «ожидаемый путь» предопределен уровнем управления или уровнем поддержки. Протокол CV обычно использует сообщение CV, на которое передается отклик CV. Функция CV может вызываться проактивно или по запросу.

Инструменты CV часто служат также для проверки путей, позволяя Алисе проверить, что сообщения от Боба приходят по корректному пути, т. е. проверяется не только связность двух MP, но и соответствие пути между ними ожидаемому, что позволяет обнаруживать изменения топологии.

Функции CV можно применять и для проверки MTU на пути между парой точек.

Проверки связности и непрерывности считаются взаимно дополняющими механизмами и зачастую применяются совместно.

2.2.8. Режимы коммуникаций

Connection-Oriented

В ориентированных на соединения технологиях организуется сквозное соединение (протоколом управления или системой поддержки) до начала передачи данных.

Для указания соединений обычно применяются их идентификаторы. В ориентированных на соединения технологиях зачастую (но не всегда) для всех пакетов одного соединения используется общий путь через сеть.

Connectionless

В технологиях без организации соединений данные обычно передаются между конечными точками без предварительных операций. Пакеты маршрутизируются независимо и поэтому пути пакетов через сеть могут различаться.

Обсуждение

Описанные здесь инструменты OAM поддерживают как технологии на основе соединений, так и без таковых.

В ориентированных на соединения технологиях OAM служит для мониторинга **конкретного** соединения, пакеты OAM передаются по одному маршруту с пакетами данных и обрабатываются аналогично. В технологиях без организации соединений OAM применяется между источником и получателем без указания конкретного соединения. Например, IP Ping (параграф 4.1) проверяет доступность заданного адресата для конкретного источника, а ориентированный на соединения тест LSP Ping (параграф 4.4.1) служит для мониторинга заданного LSP (соединение) и позволяет отслеживать все пути, используемые LSP.

Следует отметить, что в некоторых случаях для мониторинга протоколов без организации соединений применяются ориентированные на соединения протоколы OAM. Например, протокол IP не использует явных соединений, но для его мониторинга может применяться BFD (параграф 4.3), ориентированный на соединения.

2.2.9. Парные и многоточечные службы

Point-to-point (P2P)

Служба P2P (точка-точка) доставляет данные от одного источника к одному получателю.

Point-to-multipoint (P2MP)

Многоточечная служба P2MP доставляет данные от источника одному или множеству получателей (см. [Signal]).

MP2MP представляет собой службу доставки данных из одного или множества источников одному или многим получателям (см. [Signal]).

Примечание. Определения P2MP и MP2MP заимствованы из [Signal]. Хотя [Signal] относится к службам P2MP и MP2MP в MPLS, эти определения подходят и в других случаях.

Обсуждение

Описанные в документе инструменты OAM включают средства для служб как P2P, так и P2MP.

Различие между службами P2P и P2MP влияет на соответствующие инструменты OAM. Мониторинг служб P2P обычно проще, поскольку включает лишь пару конечных точек. Услуги P2MP и MP2MP сложнее для мониторинга. Например, в P2MP механизм OAM не только проверяет доступность каждого получателя, но и проверяет целостность и отсутствие петель в дереве распространения P2MP.

2.2.10. Отказы

Термины «отказ» (Failure), «сбой» (Fault) и «дефект» (Defect) используются в стандартах взаимозаменяемо применительно к неполадкам, которые моут быть обнаружены путем проверки связности или непрерывности. В некоторых стандартах, таких как 802.1ag [IEEE802.1Q], эти термины не различаются, а в других могут обозначать разные типы неполадок.

Терминология IETF MPLS-TP OAM основана на терминологии ITU-T, где эти три понятия трактуются, к описано ниже [ITU-T-G.806].

Fault - сбой

Термин Fault указывает неспособность выполнить требуемое действие, например, неудача при доставке пакета.

Defect - дефект

Термин Defect означате прерывание нормальной работы, такое как продолжительный период, в течение которого пакеты не могут быть доставлены.

Failure - отказ

Термин Failure указывает прерывание требуемой функции. Термин Defect относится к ограниченным во времени неполадкам, а отказ может быть долговременным.

3. Функции OAM

В этом разделе приведен краткий обзор функций OAM общего назначения, используемых в связанных с OAM стандартах. Эти функции применяются в стандартах OAM, описанных в документе.

- Проверка связности (CV), проверка пути и проверка непрерывности (CC) описаны в параграфе 2.2.7.
- Обнаружение пути и локализация неисправностей.

  Эта функция может служить для трассировки пути к адресату, т. е. идентификации узлов этого пути. При доступности множества путей к конкретному адресату эта функция трассирует один из доступных путей. При возникновении отказа функция пытается определить место неполадок.

  Отметим, что термин «трассировка маршрута» (или Traceroute), используемый в контексте IP и MPLS, иногда относится к «трассировке пути» в контексте других протоколов, например, TRILL.
- Мониторинг производительности обычно включает:
  - учет потерь (LM) - мониторинг числа теряемых пакетов;
  - измерение задержки (DM) - мониторинг задержки и ее вариаций (jitter).

4. Подробное описание инструментов IETF OAM

В этом разделе представлено подробное описание связанных с OAM инструментов из наборов, указанных в таблице 1.

4.1. IP Ping

Ping является одним из основным диагностических приложений в сетях IP и работает на основе ICMP. В соответствии с [NetTerms], ping является сокращением Packet internet groper, хотя термин используется настолько широко, что стал самодостаточным. Как указано в [NetTerms], - это программа для тестирования доступности адресатов с помощью отправки им сообщений ICMP Echo и ожидания отклика.

Обмен запросами и откликами ICMP Echo в Ping служит функцией CC для протокола IP. Источник передает пакет с запросом ICMP Echo, а получатель возвращает отклик Echo. Программа ICMP Ping существует в двух вариантах - [ICMPv4] для IPv4 и [ICMPv6] для IPv6.

Ping можно применять для индивидуального или группового адресата. В последнем случае все члены multicast-группы будут возвращать отправителю отклик Echo.

Реализации Ping обычно применяют сообщения ICMP. UDP Ping является вариантом программы с использованием сообщений UDP вместо ICMP Echo.

Ping является односторонним инструментом CC, т. е. позволяет проверить доступность адресата **инициатору** запроса Echo. Если желательно проверить доступность в обоих направлениях, обе стороны вызывают Ping независимо.

Отметим, что в результате фильтрации ICMP на некоторых маршрутизаторах и межсетевых экранах программа Ping может иногда не работать в сети Internet. Это ограничение относится и к Traceroute.

4.2. IP Traceroute

Traceroute ([TCPIP-Tools], [NetTools]) позволяет пользователю проследить путь между источником и адресатом IP.

В наиболее распространенном варианте реализации Traceroute [TCPIP-Tools] программа передает серию пакетов в порт адресата UDP 33434. По умолчанию Traceroute начинает с передачи трех пакетов (это число настраивается в большинстве реализаций Traceroute), со значением IP TTL (Hop Limit для IPv6) 1 в адрес получателя. Срок жизни этих пакетов заканчивается на первом маршрутизаторе в пути, поэтому маршрутизатор возвращает три сообщения ICMP Time Exceeded приложению Traceroute. Затем Traceroute передает три других пакета UDP с TTL = 2. Срок действия этих пакетов завершается на втором маршрутизаторе и он возвращает сообщения ICMP. Этот процесс продолжается с ростом значения TTL, пока пакеты не достигнут адресата. Поскольку ни одно приложение не прослушивает порт 33434 у адресата, он возвращает сообщения ICMP Destination Unreachable, указывающие недоступность порта. Это указывает приложению Traceroute завершение проверки. Программа Traceroute выводит время кругового обхода для каждой итерации.

Хотя Traceroute является средством поиска пути из A в B, следует отметить, что трафик из A в B зачастую пересылается по множеству равноценных путей (ECMP). Paris Traceroute [PARIS] является расширением Traceroute, которое пытается найти все доступные пути из A в B путем сканирования различных полей заголовков (например, портов UDP) в пробных пакетах.

Отметим, что Traceroute - это приложение, а не протокол и поэтому имеет множество разных реализаций. Одна из наиболее распространенных реализаций применяет пробные пакеты UDP, как отмечено выше. Есть другие реализации, работающие с пакетами ICMP и TCP.

Отметим, что маршрутизация IP может быть асимметричной и Traceroute показывает путь лишь в одном направлении.

Несколько расширений ICMP ([ICMP-MP], [ICMP-Int]) были определены в контексте Traceroute, включая сообщение ICMP Destination Unreachable, которое может применяться приложениями Traceroute.

Traceroute позволяет определять путь для **индивидуальных** адресов. Для групповой адресации определен аналогичный инструмент [mtrace], который позволяет проследить маршрут группового пакета IP от источника к конкретному адресату.

4.3. BFD

4.3.1. Обзор

Хотя для разных протоколов в стеке было определено множество инструментов OAM, двухстороннее детектирование пересылки [BFD], определенное рабочей группой IETF BFD, является базовым средством OAM, которое может быть развернуто для разных типов инкапсуляции и сред передачи. В IETF были определены варианты для IP ([BFD-IP], [BFD-Multi]), MPLS LSP [BFD-LSP] и псевдопроводов [BFD-VCCV]. Применение BFD в MPLS-TP определено в [TP-CC-CV].

BFD включает двк основных функции OAM, использующие два типа пакетов, BFD Control и BFD Echo.

4.3.2. Терминология

BFD работает между **системами**. Протокол BFD применяется между двумя или множеством систем после организации **сессии**.

4.3.3. BFD Control

BFD поддерживает двухстороннюю проверку непрерывности (CC), используя пакеты BFD, передаваемые в рамках сессии BFD, которая может работать в одном из двух режимов, описанных ниже.

- Асинхронный (проактивный) режим использует периодическую отправку пакетов BFD Control. Если получатель не обнаруживает пакетов BFD Control в течение заданного интервала, он сообщает об ошибке.
- В режиме работы по запросу пакеты BFD Control передаются по запросу. При возникновении потребности система инициирует отправку серии пакетов BFD Control для проверки непрерывности сессии. Пакеты BFD Control передаются в каждом направлении независимо.

Каждая из конечных точек (их называют системами) отслеживаемого пути поддерживает свою идентификацию сессии с помощью дискриминатора (Discriminator) и оба дискриминатора включаются в пакеты BFD Control, передаваемые между системами. Системы обмениваются своими дискриминаторами в момент организации сессии. В дополнение к этому согласуется скорость передачи (и приема) на основе данных, включенных в пакеты управления. Во время сессии скорость передачи может быть согласована заново.

В процессе нормальной работы (т. е. при отсутствии отказов) сессия BFD находится в состоянии Up (активна). Если в течение интервала, заданного параметром Detection Time, не будет получено пакетов BFD Control, сессия переводится в состояние Down (отключено). Время детектирования является функцией заданной в конфигурации или согласованной скорости передачи и параметра Detect Mult, определяющего число пакетов BFD Control, после отсутствия которых объявляется состояние Down. Этот параметр включается в пакет BFD Control.

4.3.4. BFD Echo

Пакет BFD Echo создается одним из партнеров и возвращается отправителю. Эхо-фукция может вызываться в проактивном режиме или по запросу.

Функция BFD Echo определена в BFD для IPv4 и IPv6 ([BFD-IP]), но не применяется в BFD для MPLS LSP и PW, а также в BFD для MPLS-TP.

4.4. MPLS OAM

Рабочая группа IETF MPLS определила OAM для MPLS LSP. Требования и схема описаны в [MPLS-OAM-FW] и [MPLS-OAM], соответственно. Определенным в этом контексте инструментом OAM является is LSP Ping [LSP-Ping]. Определение OAM для служб P2MP дано в [MPLS-P2MP].

BFD для MPLS [BFD-LSP] обеспечивает дополнительные средства обнаружения отказов на уровне данных, как описано ниже.

4.4.1. LSP Ping

Инструмент LSP Ping разрабатывался на основе парадигмы Ping/Traceroute и может работать в одном из двух режимов:

- Ping - приложение LSP Ping служит для сквозной проверки CV между двумя LER;
- режим Traceroute применяется для поэтапного (hop-by-hop) поиска неисправностей.

LSP Ping работает на базе операции ICMP Ping (CV на уровне данных) с дополнительной проверкой согласованности уровней данных и управления для классов FEC, а также обнаружением проблем MTU.

Функциональность Traceroute можно использовать для изоляции и локализации отказов MPLS с помощью индикатора TTL для инкрементной идентификации части пути LSP, которую удается пройти до отказа на канале или узле.

В сетях MPLS проблема заключается в том, что трафик данного LSP может быть распределен по множеству равноценных путей (ECMP). LSP Ping отслеживает все доступные пути LSP путем мониторинга различных FEC. Отметим, что MPLS-TP не применяет ECMP и поэтому не требует тестов OAM по разным путям.

Другая проблема заключается в том, что MPLS LSP может не иметь обратного пути, поскольку трафик от выходного LSR к входному LSR не обязательно передавать через MPLS LSP и он может проходить по другому маршруту, например, IP. Поэтому отклик на сообщение LSP Ping не так прост, как для IP Ping, где отвечающий узел просто меняет местами IP-адреса отправителя и получателя. Отметим, что этой проблемы не возникает в MPLS-TP, где путь возврата всегда доступен.

Следует отметить, что LSP Ping поддерживает однозначное указание LSP в рамках домена адресации. Указание проверяется с использованием полной идентификации FEC. LSP Ping можно расширять, добавляя информацию, нужную для поддержки новой функциональности с помощью конструкций TLV[1]. Использование TLV обычно обрабатывается на уровне управления, поскольку его сложно реализовать на аппаратном уровне.

LSP Ping поддерживает асинхронную активацию и вызовы по запросу.

4.4.2. BFD для MPLS

BFD [BFD-LSP] можно использовать для обнаружения отказов на уровне данных MPLS LSP.

Сессия BFD организуется для каждого проверяемого MPLS LSP. Пакеты BFD Control должны передаваться по тому же пути, что и тестируемый LSP. Если LSP связан с множеством FEC, сессия BFD организуется для каждого FEC.

Хотя LSP Ping можно применять для обнаружения отказов на уровне данных MPLS и проверки уровня данных MPLS LSP относительно уровня управления, BFD можно применять лишь для первого случая. BFD можно использовать вместе с LSP Ping, как в случае MPLS-TP (параграф 4.5.4).

4.4.3. OAM для VPN в сетях MPLS

В IETF опеределены два класса VPN - L2VPN и L3VPN. В [L2VPN-OAM] представлены требования и схема OAM в контексте L2VPN, а также определены уровни OAM для L2VPN в сетях MPLS. В [L3VPN-OAM] представлен схема работы и управления для L3VPN.

4.5. MPLS-TP OAM

4.5.1. Обзор

Рабочая группа MPLS определила набор инструментов OAM, удовлетворяющий требованиям MPLS-TP OAM. Полный набор требований к MPLS-TP OAM представлен в [MPLS-TP-OAM] и включает общие требования к поведению инструментов OAM и набор поддерживаемых ими операций. Набор требуемых механизмов более подробно рассмотрен в [TP-OAM-FW], где описана общая архитектура системы OAM и приведен обзор функций инструментов.

Некоторое базовые требования к набору инструментов OAM для MPLS-TP приведены ниже.

- От MPLS-TP OAM требуется поддержка работа в средах как с поддержкой IP, так и без таковой. В среде IP, где доступна маршрутизация и пересылка IP, инструментам MPLS-TP OAM следует опираться на возможности маршрутизации и пересылки IP. В остальных средах инструменты OAM должны быть способны обходиться без маршрутизации и пересылки IP.
- Пакеты OAM должны передаваться вместе с пользовательским трафиком (в основной полосе) и не требуется различать эти типы пакетов на уровне данных. С этим требованием связан принцип независимости MPLS-TP OAM от имеющегося уровня управления, хотя это не должно исключать возможности применения функциональности уровня управления. Пакеты OAM указываются меткой GAL[2], для которой в MPLS зарезервировано значение 13.

[1]Type-Length-Value - типа, размер, значение.
[2]Generic Associated Channel Label - метка базового связанного канала.

4.5.2. Терминология

Элемент обслуживания (ME)

Инструменты MPLS-TP OAM разработаны для мониторинга и управления ME. В соответствии с [TP-OAM-FW] ME определят связи (отношения) между двумя точками транспортного пути, к которым применяются операции мониторинга и управления.

Термин Maintenance Entity (ME) используется в рекомендациях ITU-T (например, [ITU-T-Y1731]), а также в терминологии MPLS-TP ([TP-OAM-FW]).

Группа элементов обслуживания (MEG)

Один или множество ME на одном транспортном пути, для которых выполняется общий мониторинг и управление (см. [TP-OAM-FW]).

Точка обслуживания (MP)

Точкой обслуживания (MP) называют функциональный элемент, который определен на узле сети и может инициировать сообщения OAM и/или реагировать на них. Этот документ сосредоточен на функциональности уровня данных MP, хотя MP взаимодействуют также с уровнями управления и администрирования.

Термин MP используется в IEEE 802.1ag и был адаптирован в MPLS-TP ([TP-OAM-FW]).

MEG End Point (MEP)

Конечной точкой ME (MEP) называют каждую из точек ME, она может инициировать сообщения OAM и/или отвечать на них (см. [TP-OAM-FW]).

MEG Intermediate Point (MIP)

Между MEP может присутствовать одна или множество промежуточных точек ME (см. [TP-OAM-FW]).

Точки MIP обычно не создают кадров OAM (за исключением используемых для уведомлений AIS), но способны реагировать на приходящие кадры OAM. MIP в MPLS-TP идентифицируют пакеты OAM, адресованные им, по истечени срока жизни (поле TTL) пакета OAM. Термин «точка обслуживания» (MP) обычно включает MEP и MIP.

Восходящие (Up) и нисходящие (Down) MEP

В IEEE 802.1ag [IEEE802.1Q] определено различие между Up MEP и Down MEP. MEP выполняет мониторинг трафика в направлении сети или в направлении моста. Down MEP - это точка MEP, принимающая пакеты OAM из сети и передающая такие пакеты в направлении сети. Up MEP принимает пакеты от моста и передает в направлении моста. В MPLS-TP ([TP-OAM-FW]) используется похожее различие в местоположении MEP - входная, выходная или пересылающая функция узла (Down/Up MEP). Размещение важно при определении точки отказа.

Отметим, что термины Up MEP и Down MEP никак не связаны с обычно применяемыми терминами Up/Down, где Down говорит о нерабочем, а Up - о рабочем состоянии.

Это различие между Up и Down MEP определено в [TP-OAM-FW], но не применялось в других MPLS-TP RFC на момент написания этого документа.

4.5.3. Базовый связанный канал

Для выполнения требований передачи трафика MPLS-TP OAM в основной полосе MPLS-TP использует базовый связанный канал G-ACh, определенный в [G-ACh] для трафика OAM на базе LSP. Этот механизм основан на тех же концепциях, которые применяются механизмами PWE3 ACH [PW-ACH] и VCCV [VCCV]. Однако для удовлетворения потребностей LSP, отличающихся от PW, были определены две приведенные ниже концепции [G-ACh].

- Заголовок связанного канала (ACH), формат которого похож на PW Control Word [PW-ACH], является 4-байтовым заголовком в начале пакетов OAM.
- Метка базового связанного канала GAL с зарезервированным в MPLS значением 13 указывает, что пакет относится к ACH и данные следуют сразу за стеком меток.

Хотя G-ACh был определен как часть MPLS-TP, следует отметить, что G-ACh является базовым средством, которое можно применять в MPLS в целом, а не только в MPLS-TP.

4.5.4. Инструменты MPLS-TP OAM

Для реализации требуемой от набора инструментов OAM функциональности рабочая группа MPLS провела анализ имеющихся инструментов OAM от IETF и ITU-T. Результаты анализа опубликованы в [OAM-Analys]. MPLS-TP использует комбинацию инструментов OAM, основанную на предшествующих стандартах и адаптированную к требованиям [MPLS-TP-OAM]. Базовые блоки этого решения включают:

- двухстороннее детектирование пересылки ([BFD], [BFD-LSP]) для проактивных тестов CC и CV;
- LSP Ping [LSP-Ping] дле тестов CV по запросу;
- новые пакеты протокола, использующие G-ACH для расширения функцинальности;
- протоколы измерения производительности.

В следующих параграфах описаны инструменты OAM, определенные для MPLS-TP [TP-OAM-FW].

4.5.4.1. Проверка непрерывности и связности

Тесты CC и CV представлены в параграфе 2.2.7 этого документа. Как показано здесь, эти инструменты могут использоваться проактивно или по запросу. В проактивном режиме инструменты обычно применяются в тандеме.

Для MPLS-TP имеется два разных инструмента - проактивный определен в [TP-CC-CV], а используемый по запросу - в [OnDemand-CV]. При работе по запросам эта функция должна поддерживать мониторинг между MEP, а также между MEP и MIP. В [TP-OAM-FW] отмечено, что в тестах CV требуется включать в сообщения CC-V однозначное указание MEG для мониторинга и MEP - инициатора сообщения.

Проактивный инструмент [TP-CC-CV] основан на расширении BFD (параграф 4.3) с дополнительным ограничением скорости передачи и приема на основе конфигурации, заданной оператором. Инструмент для проверок по запросу [OnDemand-CV] является адаптацией LSP Ping (параграф 4.4.1) в соответствии с требованиями MPLS-TP.

4.5.4.2. Трассировка маршрута

[MPLS-TP-OAM] указывает потребность в функциональности, позволяющей конечной точке пути идентифицировать промежуточные и конечные точки пути. Эта функция будет применяться в тестах по запросу. Обычно такой путь применяется для двухсторонних PW, LSP и секций (Section), а односторонние пути могут поддерживаться лишь при наличии пути возврата. Инструмент для этого основан на функциональности LSP Ping (параграф 4.4.1) и описан в [OnDemand-CV].

4.5.4.3. Блокировка пути

Функция Lock Instruct [Lock-Loop] служит для уведомления конечной точки транспортного пути о необходимости административного запрета транспортного пути. Обычно это применяется вместе с той или иной интрузивной функцией OAM, например, измерением производительности или диагностическим тестированием, для минимизации побочного влияния на пользовательский трафик.

4.5.4.4. Сообщение о блокировке

Функция Lock Reporting применяется конечной точкой пути для информирования удаленной стороны о блокировке, влияющей на путь.

4.5.4.5. Сообщение о тревоге

Сообщения о тревоге [TP-Fault] позволяют подавить аварийные сигналы после обнаружения неполадок на серверном подуровне. Эти сообщения применяются промежуточными точками пути, которые узнают о сбое в пути и информируют об этом конечные точки. В [TP-OAM-FW] указано, что это может быть результатом дефекта, обнаруженного на серверном подуровне. Генерируется сигнал AIS, который сохраняется до устранения проблемы. Последующие действия этой функции описаны в [TP-OAM-FW].

4.5.4.6. Индикация удаленного дефекта (RDI)

RDI применяется проактивно конечной точкой пути для уведомления партнерской конечной точки о дефекте, обнаруженном в двухсторонних коммуникациях между ними. В [MPLS-TP-OAM] указано, что эта функция может быть применена к односторонним LSP лишь при наличии пути возврата. В [TP-OAM-FW] указано, что эта функция связана с проактивной функцией CC-V.

4.5.4.7. Индикация отказа клиента (CFI)

Функция CFI определена в [MPLS-TP-OAM] для того, что позволить распространение информации с одного края сети на другой. Эта информация относится к дефектам клиентов, при которых клиент не может поддерживать уведомлений о тревоге.

4.5.4.8. Мониторинг производительности

Определение мониторинга производительности MPLS было вызвано требованиями MPLS-TP [MPLS-TP-OAM], но дано в общем виде для MPLS в [MPLS-LM-DM]. Дополнительный документ [TP-LM-DM] определяет профиль мониторинга производительности для MPLS-TP.

4.5.4.8.1. Измерение потерь (LM)

Функция измерения потери пакетов служит для проверки качества обслуживания. Потеря пакетов в соответствии с [IPPM-1LM] и [MPLS-TP-OAM] показывает отношение числа потерянных пользовательских пакетов к общему числу пакетов, переданных в интервале времени.

Ниже указаны два возможных способа определения этого измерения.

- При использовании пакетов OAM можно рассчитать статистику на основе серии пакетов OAM. Однако этот показатель является искусственным и может не отражать реальность, поскольку часть потерь пакетов может зависеть от их размера и реализации MEP, участвующих в протоколе.
- Можно передавать граничные сообщения в начале и в конце периода замера в течение которого пакеты подсчитываются на передающей и приемной стороне. После завершающей измерение границы элемент пути OAM может посчитать частоту потерь.

4.5.4.8.2. Измерение задержки (DM)

Функция измерения задержки служит для определения задержки в одно или двух направлениях между парой конечных точек пути (PW, LSP, Section).

- Односторонняя задержка в соответствии с [IPPM-1DM] - это время от начала передачи первого бита пакета узлом-источником до получения последнего бита приемником. Отметим, что это измерение требует синхронизации часов в конечных точках.
- Двухсторонняя задержка в соответствии с [IPPM-2DM] - это время от начала передачи первого бита пакета узлом-источником до получения последнего бита этим же узлом после «заворота» пакета на удаленной стороне. Отметим, что в результате асимметрии пути односторонняя задержка между точками может отличаться от половины значения двухсторонней задержки. Синхронизация часов при измерении двухсторонней задержки не требуется.

Для каждой из этих функций DM возможно измерение как задержки, так и ее вариаций. Измерение задержки выполняется с помощью пакетов OAM с временными метками, передаваемых между участвующими MEP.

4.6. OAM для псевдопроводов

4.6.1. OAM для псевдопроводов с использованием VCCV

VCCV в соответствии с [VCCV] обеспечивает способ сквозного детектирования отказов и средства диагностики для PW (независимо от технологии туннелирования). Функция коммутации VCCV обеспечивает канал управления (CC), связанный с каждым PW. [VCCV] определяет три типа CC, т. е. 3 возможных метода передачи и идентификации сообщений OAM.

- Тип 1. VCCV по основному каналу, как описано в [VCCV], называется также PWE3 Control Word with 0001b as first nibble[1]. Используется заголовок связанного канала PW [PW-ACH].
- Тип 2. VCCV по отдельному каналу, как описано в [VCCV], называется также MPLS Router Alert Label. Канал управления создается с помощью метки MPLS router alert [MPLS-ENCAPS] непосредственно над меткой PW.
- Тип 3. VCCV с минимальным TTL, как описано в [VCCV], называется также MPLS PW Label with TTL == 1, где канал управления указывается значение TTL = 1 в метке PW.

VCCV в настоящее время поддерживает инструменты OAM ICMP Ping, LSP Ping и BFD. ICMP и LSP Ping инкапсулируются в IP перед отправкой через PW ACH. BFD для VCCV [BFD-VCCV] поддерживает два режима инкапсуляции - IP/UDP (с заголовокм IP/UDP) или PW-ACH (без заголовка IP/UDP) и обеспечивает поддержку сигнализации состояния AC. Использование канала управления VCCV обеспечивает контекст, основанный на метке MPLS-PW, который нужен для привязки и загрузки сессии BFD для конкретного псевдопровода (FEC), избавляя от необходимости обмена значениями Discriminator.

VCCV состоит из двух компонент: (1) сигнальная компонента для передачи возможностей VCCV как часть метки VC и (2) коммутационная компонента, заставляющая трактовать данные PW как пакет управления.

VCCV не зависит напрямую от наличия уровняуправления. Анонсирование возможностей VCCV может выполняться как часть сигнализации PW при использовании LDP. В случае ручной настройки PW согласованность опций на обеих сторонах должен обеспечить оператор. Вариант ручной настройки был создан специально для обработки случаев использования MPLS-TP, где не требуется уровень управления. Однако эта функция полезна и для других случаев, таких как мобильный транспорт.

Рабочая группа PWE3 провела исследование VCCV [VCCV-SURVEY] и анализ применяемых на практике механизмов.

4.6.2. OAM для псевдопроводов с использованием G-ACh

Как отмечено выше, VCCV поддерживает OAM для PW за счет применения канала управления (CC) для пакетов OAM. При использовании PW в сетях MPLS-TP вместо CC, определенных в VCCV, можно применять G-ACh, как определено в [PW-G-ACh].

4.6.3. Устройство присоединения - отображение псевдопровода

Рабочая группа PWE3 определила отображение и уведомление о дефектных состояниях между псевдопроводом (PW) и устройствами присоединения (AC[2]) при сквозной эмуляции сервиса. Это отображение очень важно для сквозной функциональности. Отображение обеспечивается, в частности, [PW-MAP], [L2TP-EC] для псевдопроводов L2TPv3 и параграфом 5.3 [ATM-L2] для ATM.

В [L2VPN-OAM] приведены требования и схема OAM в контексте L2VPN и определены уровни OAM для L2VPN на основе псевдопроводов.

Отображение, заданное в [Eth-Int], позволяет организовать сквозную эмуляцию Ethernet через псевдопровода.

4.7. OWAMP и TWAMP

4.7.1. Обзор

Рабочая группа IPPM в IETF определила общие критерии и метрику для мониторинга производительности IP ([IPPM-FW]). В RFC, опубликованных этой группой, определена метрика для проверки связности [IPPM-Con], измерения задержки ([IPPM-1DM], [IPPM-2DM]) и потери пакетов [IPPM-1LM]. Следует отметить, что работа IETF в контексте метрики производительности не ограничивается сетями IP. В [PM-CONS] представлены общие рекомендации для рассмотрения новых параметров производительности.

Рабочая группа IPPM определила не только метрику измерения производительности, но и протоколы для выполнения измерений. В [OWAMP] и [TWAMP] определены методы и протоколы измерения производительности в сетях IP.

OWAMP [OWAMP] позволяет измерять в одном направлении характеристики сетей IP, такие как задержка и потеря пакетов. Для корректной работы OWAMP требуется корректная установка времени суток на всех конечных точках.

Протокол TWAMP [TWAMP] обеспечивает похожую функциональность и позволяет проводить измерения в одном или двух (round-trip — круговой обход) направлениях.

OWAMP и TWAMP включают в себя по два протокола, указанных ниже.

- OWAMP-Control/TWAMP-Control служит для инициирования, запуска и остановки тестовых сессий, а также сбора результатов теста. Тесты CC и CV выполняются и подтверждаются с помощью организации соединения TCP для управляющего протокола OWAMP/TWAMP.
- OWAMP-Test/TWAMP-Test служит для обмена тестовыми пакетами между двумя узлами. Поддерживаются функции измерения задержки и потерь, а также обнаружение иных аномалий, таких как дублирование и изменение порядка пакетов.

Хотя [OWAMP] и [TWAMP] определяют инструменты для измерения производительности, следует отметить, что точность этих инструментов не задается и зависит от масштаба, реализации и конфигурации сети.

Для мониторинга производительности определены и другие протоколы, например, в MPLS-TP OAM ([MPLS-LM-DM], [TP-LM-DM]) и Ethernet OAM [ITU-T-Y1731].

[1] PWE3 Control Word with 0001b as first nibble — управляющее слово PWE3 с первым полубайтом 0001b.
[2] Attachment Circuit.

4.7.2. Протоколы управления и тестирования

Протоколы управления OWAMP и TWAMP работают на основе TCP, а протоколы тестирования применяют UDP. Задача протоколов управления заключается в инициировании, запуске и остановке тестовой сессии, а для OWAMP также в сборе результатов. Протоколы тестирования передают тестовые пакеты (с порядковыми номерами и временными метками) по тестируемому пути IP в соответствии с планированием, а затем записывают статистику прибывших пакетов. Можно одновременно организовать множество сессий, каждая из которых будет иметь свой идентификатор, и задать число передаваемых пакетов, размер заполнения (размер пакета), время начала и планирование передачи (постоянный или псевдослучайный интервал с экспоненциальным распределением). Статистика записывается в соответствии с подходящими IPPM RFC.

С точки зрения безопасности тестовые пакеты OWAMP и TWAMP сложно обнаружить, поскольку это обычные пакеты UDP с согласованными номерами портов, не имеющие статических параметров. OWAMP и TWAMP также включают опции аутентификации и шифрования как для управляющих, так и для тестовых пакетов.

4.7.3. OWAMP

OWAMP определяет логические роли Session-Sender, Session-Receiver, Server, Control-Client и Fetch-Client. Session-Sender создает тестовый трафик, который принимает Session-Receiver. Server настраивает и поддерживает сессию, а также возвращает результаты. Control-Client инициирует запросы тестовых сессий, запускает сессии и может инициировать их завершение. Fetch-Client запрашивает результаты завершенной сессии. Один хост может выступать одновременно в нескольких ролях, например, Control-Client, Fetch-Client и Session-Sender, а другой может выступать в качестве Server и Session-Receiver.

В типичной сессии OWAMP элемент Control-Client организует соединение TCP с портом 861 на элементе Server, который отвечает приветственным сообщением, указывающим поддерживаемые режимы защиты и целостности. Control-Client отвечает с использованием выбранного режима коммуникаций и Server воспринимает этот режим. Затем Control-Client запрашивает и полностью описывает тестовую сессию, а Server отвечает информацией о приемлемости и поддержке. Дополнительные сообщения позволяют запросить несколько сессий. Далее Control-Client запускает тестовую сессию, Server подтверждает ее и инструктирует элемент Session-Sender начать тест. Session-Sender передает тестовые пакеты с псевдослучайным заполнением элементу Session-Receiver, пока сессия не будет завершена или Control-Client не остановит ее.

По завершении Session-Sender передает элементу Server отчет с данными от Session-Receiver. Затем Fetch-Client может передать запрос элементу Server, который отвечает подтверждением и сразу же передает результаты.

4.7.4. TWAMP

TWAMP определяет несколько логических ролей - Session-Sender, Session-Reflector, Server и Control-Client. Они похожи на роли OWAMP, но Session-Reflector не собирает информации о пакетах и не требуется для Fetch-Client.

В типовой сессии TWAMP элемент Control-Client организует соединение TCP с портом 862 на сервере и режим согласуется как в OWAMP. Затем Control-Client запрашивает сессию и начинает ее. Session-Sender передает тестовые пакеты с псевдослучайным заполнением элементу Session-Reflector, который возвращает их с временной меткой.

4.8. TRILL

Требования к OAM для TRILL заданы в [TRILL-OAM]. Проблема TRILL OAM, похожая на случай MPLS, состоит в том, что трафик между RBridge RB1 и RB2 может пересылаться по множеству путей. Поэтому протокол OAM между RB1 и RB2 должен быть способен отслеживать все доступные пути между парой мостов RBridge.

На момент написания этого документа процесс определения инструментов TRILL OAM еще не был завершен. В этом параграфе приведены основные требования TRILL OAM [TRILL-OAM].

- Проверка непрерывности (CC) — протокол TRILL OAM должен поддерживать функцию CC между любой парой RBridge.
- Проверка связности (CV) — связность между парой RBridge может быть проверена на уровне потока.
- Трассировка пути позволяет RBridge отследить все доступные пути к партнерскому RBridge.
- Мониторинг производительности позволяет RBridge отслеживать потери и задержки пакетов, отправленных партнерскому RBridge.

5. Сводка

В этом разделе приведена сводка инструментов и функций OAM, представленных в этом документе. Сводка включает основные средства OAM, определенные в IETF. Этот компактный список будет полезен разным читателям - от сетевых операторов до разработчиков стандартов. Сводка включает короткий параграф с рекомендациями для производителей сетевого оборудования.

5.1. Сводка инструментов OAM

В этом параграфе приведена краткая сводка описанных в документе наборов инструментов OAM.

Подробный список RFC, относящихся к каждому набору, приведен в приложении A.1.

Таблица 3. Связанные с OAM инструменты IETF.

Инструмент	*Описание*	*Технология*
IP Ping	Ping ([IntHost], [NetTerms]) представляет собой простую программу для тестирования доступности с использованием сообщений ICMP Echo ([ICMPv4], [ICMPv6]).	IPv4/IPv6

IP Traceroute	Traceroute ([TCPIP-Tools], [NetTools]) является приложением, которое позволяет пользователям трассировать путь между источником и адресатом IP с идентификацией промежуточных узлов пути. При наличии нескольких путей Traceroute проверяет один из них. Наиболее распространенная реализация Traceroute использует сообщения UDP, хотя есть и реализации на основе протоколов ICMP и TCP. Paris Traceroute [PARIS] является расширением, которое пытается найти все доступные пути между точками A и B путем сканирования различных полей заголовков.	IPv4/IPv6
BFD	Двухстороннее детектирование пересылки (BFD) определено в [BFD] как модель облегченного базового инструмента OAM. Целью является определение базового средства для использования с разными типами инкапсуляции, сетевого окружения и сред передачи.	Все
MPLS OAM	MPLS LSP Ping в соответствии с определением [MPLS-OAM], [MPLS-OAM-FW] и [LSP-Ping] является инструментом OAM для парных и многоточечных MPLS LSP. Инструмент имеет две основных функции - Ping и Traceroute. BFD [BFD-LSP] является дополнительным средством поиска отказов на уровне данных MPLS LSP.	MPLS
MPLS-TP OAM	Средства MPLS-TP OAM определены в нескольких RFC. Требования OAM для транспортного профиля MPLS (MPLS-TP) заданы в [MPLS-TP-OAM]. Каждый из инструментов набора OAM определен в своем RFC, как указано в приложении A.1.	MPLS-TP
OWAMP и TWAMP	Протоколы активного измерения в одном [OWAMP] и двух [TWAMP] направлениях определены рабочей группой IP Performance Metrics (IPPM) в IETF. Эти протоколы позволяют измерять разные параметры, включая потерю пакетов, задержку и ее вариации, дублирование и изменение порядка доставки.	IPv4/IPv6
Pseudowire OAM	Архитектура PWE3 OAM определяет каналы управления, поддерживающие использование имеющихся инструментов IETF OAM для псевдопровода (PW). Каналы управления, определенные в [VCCV] и [PW-G-ACh], могут применяться вместе с ICMP Ping, LSP Ping и BFD для выполнения тестов CC и CV. Кроме того, каналы поддерживают использование любых инструментов OAM на базе MPLS-TP для распространения их функциональности на PW.	Pseudowire
TRILL OAM	Требования к OAM в TRILL определены в [TRILL-OAM] и включают, CC, CV, трассировку пути и мониторинг производительности. На момент написания этого документа работа по детальному определению инструментов TRILL OAM не была завершена.	TRILL

5.2. Сводка функций OAM

В таблице 4 указаны функции OAM, поддерживаемые каждым набором инструментов, который рассмотрен в этом разделе. В столбцах таблицы указаны типовые функции OAM, описанные в параграфе 1.3.

Таблица 4. Функциональность OAM в инструментах IETF OAM.

Инструменты	***Проверка связности***	***Верификация связности***	***Обнаружение пути***	***Мониторинг производит.***	***Другие функции***
IP Ping	Echo				
IPTraceroute			Traceroute		
BFD	BFD Control/Echo	BFD Control			RDI с применением BFD Control
MPLS OAM (LSP Ping)		Режим Ping	Режим Traceroute		
MPLS-TP OAM	CC	CV (проактивно или по запросу)	Трассировка маршрута	-LM -DM	-Diagnostic Test -Lock -Alarm Reporting -Client Failure Indication -RDI
Pseudowire OAM	BFD	-BFD -ICMP Ping -LSP Ping	LSP Ping	-DM -LM	
OWAMP и TWAMP	Протокол управления				
TRILL OAM	CC	CV	Трассировка пути	-DM -LM	

5.3. Рекомендации производителям сетевого оборудования

Как отмечено в параграфе 1.4, от инструментов OAM требуется способность тестировать реальный уровень данных с максимально возможной точностью. Хотя это может показаться очевидным, следует подчеркнуть важность одинаковой обработки трафика OAM и трафика уровня данных, для которого выполняется мониторинг.

6. Вопросы безопасности

OAM имеет тесную связь со стабильностью сети. Успешная атака на протокол OAM может создать иллюзию отказов или воспрепятствовать детектированию реальных отказов и это может приводить к отказам в обслуживании.

Некоторые из представленных в документе инструментов OAM включают механизмы безопасности, обеспечивающие защиту целостности, что позволяет предотвратить подмену и искажение атакующими пакетов OAM. Например, [BFD] включает необязательный механизм аутентификации для пакетов BFD Control с использованием SHA1, MD5 или простого пароля. В [OWAMP] и [TWAMP] имеется 3 режима защиты - без аутентификации (unauthenticated), с аутентификацией (authenticated) и шифрование (encrypted). Для аутентификации применяется SHA1 в качестве алгоритма HMAC, а для шифрования служит алгоритм AES.

Конфиденциальность обычно не требуется от протоколов OAM. Однако использование шифрования (например, в [OWAMP] и [TWAMP]) может усложнить атакующим идентификацию пакетов OAM и атаки на протоколы OAM.

OAM может применяться также в качестве средства зондирования сети - данные об адресах, номерах портов, топологии и производительности сети могут быть получены путем пассивного перехвата пакетов OAM или активной генерации пакетов OAM и сбора откликов на них. Полученная информация может применяться для организации атак. Отметим, что часть такой информации (например, адреса и номера портов) может быть получена даже при использовании шифрования ([OWAMP], [TWAMP]).

Дополнительную информацию по вопросам безопасности протоколов OAM можно найти в соответствующих разделах документов, упомянутых здесь.

7. Благодарности

Авторы признательны Sasha Vainshtein, Carlos Pignataro, David Harrington, Dan Romascanu, Ron Bonica, Benoit Claise, Stewart Bryant, Tom Nadeau, Elwyn Davies, Al Morton, Sam Aldrin, Thomas Narten и другим членам рабочей группы OPSA WG за полезные комментарии в почтовой конференции.

Этот документ был подготовлен с использованием шаблона 2-Word-v2.0.template.dot.

8. Литература

8.1. Нормативные документы

[OAM-Def] Andersson, L., van Helvoort, H., Bonica, R., Romascanu, D., and S. Mansfield, "Guidelines for the Use of the "OAM" Acronym in the IETF", BCP 161, RFC 6291, June 2011.

8.2. Дополнительная литература

[ATM-L2] Singh, S., Townsley, M., and C. Pignataro, "Asynchronous Transfer Mode (ATM) over Layer 2 Tunneling Protocol Version 3 (L2TPv3)", RFC 4454, May 2006.

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

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

[BFD-IP] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)", RFC 5881, June 2010.

[BFD-LSP] Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)", RFC 5884, June 2010.

[BFD-Multi] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD) for Multihop Paths", RFC 5883, June 2010.

[BFD-VCCV] Nadeau, T., Ed., and C. Pignataro, Ed., "Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)", RFC 5885, June 2010.

[Comp] Bonaventure, O., "Computer Networking: Principles, Protocols and Practice", 2008.

[Dup] Uijterwaal, H., "A One-Way Packet Duplication Metric", RFC 5560, May 2009.

[Eth-Int] Mohan, D., Ed., Bitar, N., Ed., Sajassi, A., Ed., DeLord, S., Niger, P., and R. Qiu, "MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking", RFC 7023, October 2013.

[G-ACh] Bocci, M., Ed., Vigoureux, M., Ed., and S. Bryant, Ed., "MPLS Generic Associated Channel", RFC 5586, June 2009.

[ICMP-Ext] Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "ICMP Extensions for Multiprotocol Label Switching", RFC 4950, August 2007.

[ICMP-Int] Atlas, A., Ed., Bonica, R., Ed., Pignataro, C., Ed., Shen, N., and JR. Rivers, "Extending ICMP for Interface and Next-Hop Identification", RFC 5837, April 2010.

[ICMP-MP] Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "Extended ICMP to Support Multi-Part Messages", RFC 4884, April 2007.

[ICMPv4] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[ICMPv6] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[IEEE802.1Q] IEEE, "IEEE Standard for Local and metropolitan area networks - Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks", IEEE 802.1Q, October 2012.

[IEEE802.3ah] IEEE, "IEEE Standard for Information technology - Local and metropolitan area networks - Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications", IEEE 802.3ah, clause 57, December 2008.

[IntHost] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[IPPM-1DM] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Delay Metric for IPPM", RFC 2679, September 1999.

[IPPM-1LM] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Packet Loss Metric for IPPM", RFC 2680, September 1999.

[IPPM-2DM] Almes, G., Kalidindi, S., and M. Zekauskas, "A Round-trip Delay Metric for IPPM", RFC 2681, September 1999.

[IPPM-Con] Mahdavi, J. and V. Paxson, "IPPM Metrics for Measuring Connectivity", RFC 2678, September 1999.

[IPPM-FW] Paxson, V., Almes, G., Mahdavi, J., and M. Mathis, "Framework for IP Performance Metrics", RFC 2330, May 1998.

[ITU-G8113.1] ITU-T, "Operations, Administration and Maintenance mechanism for MPLS-TP in Packet Transport Network (PTN)", ITU-T Recommendation G.8113.1/Y.1372.1, November 2012.

[ITU-G8113.2] ITU-T, "Operations, administration and maintenance mechanisms for MPLS-TP networks using the tools defined for MPLS", ITU-T Recommendation G.8113.2/Y.1372.2, November 2012.

[ITU-T-CT] Betts, M., "Allocation of a Generic Associated Channel Type for ITU-T MPLS Transport Profile Operation, Maintenance, and Administration (MPLS-TP OAM)", RFC 6671, November 2012.

[ITU-T-G.806] ITU-T, "Characteristics of transport equipment - Description methodology and generic functionality", ITU-T Recommendation G.806, January 2009.

[ITU-T-Y1711] ITU-T, "Operation & Maintenance mechanism for MPLS networks", ITU-T Recommendation Y.1711, February 2004.

[ITU-T-Y1731] ITU-T, "OAM Functions and Mechanisms for Ethernet-based Networks", ITU-T Recommendation G.8013/Y.1731, July 2011.

[ITU-Terms] ITU-R/ITU-T, "ITU-R/ITU-T Terms and Definitions", 2013, <http://www.itu.int/pub/R-TER-DB>.

[L2TP-EC] McGill, N. and C. Pignataro, "Layer 2 Tunneling Protocol Version 3 (L2TPv3) Extended Circuit Status Values", RFC 5641, August 2009.

[L2VPN-OAM] Sajassi, A., Ed., and D. Mohan, Ed., "Layer 2 Virtual Private Network (L2VPN) Operations, Administration, and Maintenance (OAM) Requirements and Framework", RFC 6136, March 2011.

[L3VPN-OAM] El Mghazli, Y., Ed., Nadeau, T., Boucadair, M., Chan, K., and A. Gonguet, "Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management", RFC 4176, October 2005.

[Lock-Loop] Boutros, S., Ed., Sivabalan, S., Ed., Aggarwal, R., Ed., Vigoureux, M., Ed., and X. Dai, Ed., "MPLS Transport Profile Lock Instruct and Loopback Functions", RFC 6435, November 2011.

[LSP-Ping] Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", RFC 4379, February 2006.

[Mng] Farrel, A., "Inclusion of Manageability Sections in Path Computation Element (PCE) Working Group Drafts", RFC 6123, February 2011.

[MPLS-ENCAPS] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and A. Conta, "MPLS Label Stack Encoding", RFC 3032, January 2001.

[MPLS-LM-DM] Frost, D. and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", RFC 6374, September 2011.

[MPLS-OAM] Nadeau, T., Morrow, M., Swallow, G., Allan, D., and S. Matsushima, "Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks", RFC 4377, February 2006.

[MPLS-OAM-FW] Allan, D., Ed., and T. Nadeau, Ed., "A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM)", RFC 4378, February 2006.

[MPLS-P2MP] Yasukawa, S., Farrel, A., King, D., and T. Nadeau, "Operations and Management (OAM) Requirements for Point-to-Multipoint MPLS Networks", RFC 4687, September 2006.

[MPLS-TP-OAM] Vigoureux, M., Ed., Ward, D., Ed., and M. Betts, Ed., "Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks", RFC 5860, May 2010.

[mtrace] Fenner, W. and S. Casner, "A "traceroute" facility for IP Multicast", Work in Progress, July 2000.

[NetTerms] Jacobsen, O. and D. Lynch, "A Glossary of Networking Terms", RFC 1208, March 1991.

[NetTools] Enger, R. and J. Reynolds, "FYI on a Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices", FYI 2, RFC 1470, June 1993.

[OAM-Analys] Sprecher, N. and L. Fang, "An Overview of the Operations, Administration, and Maintenance (OAM) Toolset for MPLS-Based Transport Networks", RFC 6669, July 2012.

[OAM-Label] Ohta, H., "Assignment of the 'OAM Alert Label' for Multiprotocol Label Switching Architecture (MPLS) Operation and Maintenance (OAM) Functions", RFC 3429, November 2002.

[OAM-Mng] Ersue, M., Ed., and B. Claise, "An Overview of the IETF Network Management Standards", RFC 6632, June 2012.

[OnDemand-CV] Gray, E., Bahadur, N., Boutros, S., and R. Aggarwal, "MPLS On-Demand Connectivity Verification and Route Tracing", RFC 6426, November 2011.

[OWAMP] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, September 2006.

[PARIS] Augustin, B., Friedman, T., and R. Teixeira, "Measuring Load-balanced Paths in the Internet", IMC '07 Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, 2007.

[PM-CONS] Clark, A. and B. Claise, "Guidelines for Considering New Performance Metric Development", BCP 170, RFC 6390, October 2011.

[PW-ACH] Bryant, S., Swallow, G., Martini, L., and D. McPherson, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", RFC 4385, February 2006.

[PW-G-ACh] Li, H., Martini, L., He, J., and F. Huang, "Using the Generic Associated Channel Label for Pseudowire in the MPLS Transport Profile (MPLS-TP)", RFC 6423, November 2011.

[PW-MAP] Aissaoui, M., Busschbach, P., Martini, L., Morrow, M., Nadeau, T., and Y(J). Stein, "Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping", RFC 6310, July 2011.

[Reorder] Morton, A., Ciavattone, L., Ramachandran, G., Shalunov, S., and J. Perser, "Packet Reordering Metrics", RFC 4737, November 2006.

[Signal] Yasukawa, S., Ed., "Signaling Requirements for Point-to-Multipoint Traffic-Engineered MPLS Label Switched Paths (LSPs)", RFC 4461, April 2006.

[TCPIP-Tools] Kessler, G. and S. Shepard, "A Primer On Internet and TCP/IP Tools and Utilities", FYI 30, RFC 2151, June 1997.

[TP-CC-CV] Allan, D., Ed., Swallow Ed., G., and J. Drake Ed., "Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile", RFC 6428, November 2011.

[TP-Fault] Swallow, G., Ed., Fulignoli, A., Ed., Vigoureux, M., Ed., Boutros, S., and D. Ward, "MPLS Fault Management Operations, Administration, and Maintenance (OAM)", RFC 6427, November 2011.

[TP-LM-DM] Frost, D., Ed., and S. Bryant, Ed., "A Packet Loss and Delay Measurement Profile for MPLS-Based Transport Networks", RFC 6375, September 2011.

[TP-OAM-FW] Busi, I., Ed., and D. Allan, Ed., "Operations, Administration, and Maintenance Framework for MPLS-Based Transport Networks", RFC 6371, September 2011.

[TP-Term] van Helvoort, H., Ed., Andersson, L., Ed., and N. Sprecher, Ed., "A Thesaurus for the Interpretation of Terminology Used in MPLS Transport Profile (MPLS-TP) Internet-Drafts and RFCs in the Context of the ITU-T's Transport Network Recommendations", RFC 7087, December 2013.

[TRILL-OAM] Senevirathne, T., Bond, D., Aldrin, S., Li, Y., and R. Watve, "Requirements for Operations, Administration, and Maintenance (OAM) in Transparent Interconnection of Lots of Links (TRILL)", RFC 6905, March 2013.

[TWAMP] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, October 2008.

[VCCV] Nadeau, T., Ed., and C. Pignataro, Ed., "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires", RFC 5085, December 2007.

[VCCV-SURVEY] Del Regno, N., Ed., and A. Malis, Ed., "The Pseudowire (PW) and Virtual Circuit Connectivity Verification (VCCV) Implementation Survey Results", RFC 7079, November 2013.

Приложение A. Список документов OAM

A.1. Список документов IETF OAM

В таблице 5 перечислены связанные с OAM документы RFC, выпущенные IETF.

Важно подчеркнуть, что в таблице указаны разные по природе RFC. Например, некоторые из этих документов определяют инструменты или протоколы OAM (или то и другое), а другие определяют протоколы, не связанные напрямую с OAM, но применяемые инструментами OAM. В таблицу также включены RFC, определяющие требования к схемам OAM в конкретном контексте (например, MPLS-TP).

RFC в таблице разбиты по категориям, определенным в параграфе 1.3.

Таблица 5. Список RFC, связанных с IETF OAM.

Инструмент	***Название документа***	***Документ***
IP Ping	Requirements for Internet Hosts -- Communication Layers [IntHost]	RFC 1122
	A Glossary of Networking Terms [NetTerms]	RFC 1208
	Internet Control Message Protocol [ICMPv4]	RFC 792
	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification [ICMPv6]	RFC 4443
IP Traceroute	A Primer On Internet and TCP/IP Tools and Utilities [TCPIP-Tools]	RFC 2151
	FYI on a Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices [NetTools]	RFC 1470
	Internet Control Message Protocol [ICMPv4]	RFC 792
	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification [ICMPv6]	RFC 4443
	Extended ICMP to Support Multi-Part Messages [ICMP-MP]	RFC 4884
	Extending ICMP for Interface and Next-Hop Identification [ICMP-Int]	RFC 5837
BFD	Bidirectional Forwarding Detection (BFD) [BFD]	RFC 5880
	Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop) [BFD-IP]	RFC 5881

	Generic Application of Bidirectional Forwarding Detection (BFD)[BFD-Gen]	RFC 5882
	Bidirectional Forwarding Detection (BFD) for Multihop Paths [BFD-Multi]	RFC 5883
	Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs) [BFD-LSP]	RFC 5884
	Bidirectional Forwarding Detection for the Pseudowire Virtual Circuit Connectivity Verification (VCCV) [BFD-VCCV]	RFC 5885
MPLS OAM	Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks [MPLS-OAM]	RFC 4377
	A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM) [MPLS-OAM-FW]	RFC 4378
	Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures [LSP-Ping]	RFC 4379
	Operations and Management (OAM) Requirements for Point-to-Multipoint MPLS Networks [MPLS-P2MP]	RFC 4687
	ICMP Extensions for Multiprotocol Label Switching [ICMP-Ext]	RFC 4950
	Bidirectional Forwarding Detection for MPLS Label Switched Paths (LSPs) [BFD-LSP]	RFC 5884
MPLS-TP OAM	Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks [MPLS-TP-OAM]	RFC 5860
	MPLS Generic Associated Channel [G-ACh]	RFC 5586
	Operations, Administration, and Maintenance Framework for MPLS-Based Transport Networks [TP-OAM-FW]	RFC 6371
	Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile [TP-CC-CV]	RFC 6428
	MPLS On-Demand Connectivity Verification and Route Tracing [OnDemand-CV]	RFC 6426
	MPLS Fault Management Operations, Administration, and Maintenance (OAM) [TP-Fault]	RFC 6427
	MPLS Transport Profile Lock Instruct and Loopback Functions [Lock-Loop]	RFC 6435
	Packet Loss and Delay Measurement for MPLS Networks [MPLS-LM-DM]	RFC 6374
	A Packet Loss and Delay Measurement Profile for MPLS-Based Transport [TP-LM-DM]	RFC 6375
Pseudowire OAM	Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires [VCCV]	RFC 5085
	Bidirectional Forwarding Detection for the Pseudowire Virtual Circuit Connectivity Verification (VCCV) [BFD-VCCV]	RFC 5885
	Using the Generic Associated Channel Label for Pseudowire in the MPLS Transport Profile (MPLS-TP) [PW-G-ACh]	RFC 6423
	Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping [PW-MAP]	RFC 6310
	MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking [Eth-Int]	RFC 7023
OWAMP и TWAMP	A One-way Active Measurement Protocol (OWAMP) [OWAMP]	RFC 4656
	A Two-Way Active Measurement Protocol (TWAMP) [TWAMP]	RFC 5357
	Framework for IP Performance Metrics [IPPM-FW]	RFC 2330
	IPPM Metrics for Measuring Connectivity [IPPM-Con]	RFC 2678
	A One-way Delay Metric for IPPM [IPPM-1DM]	RFC 2679
	A One-way Packet Loss Metric for IPPM [IPPM-1LM]	RFC 2680
	A Round-trip Delay Metric for IPPM [IPPM-2DM]	RFC 2681
	Packet Reordering Metrics [Reorder]	RFC 4737
	A One-Way Packet Duplication Metric [Dup]	RFC 5560
TRILL OAM	Requirements for Operations, Administration, and Maintenance (OAM) in Transparent Interconnection of Lots of Links (TRILL) [TRILL-OAM]	RFC 6905

A.2. Отдельные документы других организаций

В дополнение к инструментам OAM, определенным IETF, IEEE и ITU-T тоже определили средства OAM для Ethernet и различных транспортных сетевых сред. Эти разные инструменты, определенные 3 организациями, зачастую тесно связаны и влияют друг на друга. ITU-T и IETF определили инструменты OAM для MPLS LSP, [ITU-T-Y1711] и [LSP-Ping]. Перечисленные ниже стандарты OAM от IEEE и ITU-T являются некоторым расширением указанных ранее инструментов IETF OAM и приведены лишь для справки.

- Инструменты OAM для уровня L2 определены ITU-T в [ITU-T-Y1731] и IEEE в 802.1ag [IEEE802.1Q]. Стандарт IEEE 802.3 определяет OAM для одноинтервальных (one-hop) каналов Ethernet [IEEE802.3ah].
- Комитет ITU-T определил OAM для MPLS LSP в [ITU-T-Y1711], MPLS-TP OAM в [ITU-G8113.1] и [ITU-G8113.2].

Следует отметить, что эти документы других организаций в основном имеют дело с функциями OAM ниже уровня IP (уровни L2, L2.5) и в некоторых случаях операторы используют многоуровневый подход к layered OAM, зависящий от организации сети.

В таблице 6 указаны некоторые стандарты OAM, опубликованные другими организациями (не IETF). Этот документ посвящен стандартам IETF OAM, но перечисленные в таблице документы упоминаются в нем.

Таблица 6. Список связанных с этим документом стандартов других организаций.

	Название документа	**Документ**
ITU-T MPLS OAM	Operation & Maintenance mechanism for MPLS networks [ITU-T-Y1711]	ITU-T Y.1711
	Assignment of the 'OAM Alert Label' for Multiprotocol Label Switching Architecture (MPLS) Operation and Maintenance (OAM) Functions [OAM-Label]	RFC 3429[1]
ITU-T MPLS-TP OAM	Operations, administration and Maintenance mechanisms for MPLS-TP networks using the tools defined for MPLS [ITU-G8113.2][2]	ITU-T G.8113.2
	Operations, Administration and Maintenance mechanism for MPLS-TP in Packet Transport Network (PTN)	ITU-T G.8113.1
	Allocation of a Generic Associated Channel Type for ITU-T MPLS Transport Profile Operation, Maintenance, and Administration (MPLS-TP OAM) [ITU-T-CT]	RFC 6671[3]
ITU-T Ethernet OAM	OAM Functions and Mechanisms for Ethernet-based Networks [ITU-T-Y1731]	ITU-T Y.1731
IEEE CFM	Connectivity Fault Management [IEEE802.1Q][4]	IEEE 802.1ag
IEEE DDCFM	Management of Data Driven and Data Dependent Connectivity Faults [IEEE802.1Q][5]	IEEE 802.1ag
OAM канального уровня IEEE 802.3	Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks [IEEE802.3ah][6]	IEEE 802.3ah

Адреса авторов

Tal Mizrahi
Marvell
6 Hamada St.
Yokneam 20692
Israel
EMail: talmi@marvell.com

Nurit Sprecher
Nokia Solutions and Networks
3 Hanagar St. Neve Ne'eman B
Hod Hasharon 45241
Israel
EMail: nurit.sprecher@nsn.com

Elisa Bellagamba
Ericsson
6 Farogatan St.
Stockholm 164 40
Sweden
Phone: +46 761440785
EMail: elisa.bellagamba@ericsson.com

Yaacov Weingarten
34 Hagefen St.
Karnei Shomron 4485500
Israel
EMail: wyaacov@gmail.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Этот документ IETF указан в таблице стандартов других организаций, поскольку он определен в качестве дополнения к ITU-T Y.1711.
[2]Этот документ описывает инструменты OAM, определенные IETF для MPLS-TP, а ITU-T G.8113.1 - определенные ITU-T.
[3]Этот документ IETF указан в таблице стандартов других организаций, поскольку он определен как дополнение к ITU-T G.8113.1.
[4]Исходное определение CFM было дано в IEEE 802.1ag, а сейчас включено в стандарт 802.1Q.
[5]Исходное определение DDCFM было дано в IEEE 802.1Qaw, а сейчас включено в стандарт 802.1Q.
[6]Исходное определение OAM канального уровня было дано в IEEE 802.3ah, а сейчас включено в стандарт 802.3.