Network Working Group
Request for Comments: 1812
Obsoletes: 1716, 1009
Category: Standards Track

F. Baker, Editor
Cisco Systems

June 1995

Требования к маршрутизаторам IPv4

Requirements for IP Version 4 Routers

Статус документа

Этот документ содержит спецификацию стандарта, предложенного сообществу Internet, и служит приглашением к дискуссии в целях дальнейшего развития. Текущее состояние стандартизации вы можете узнать из документа «Internet Official Protocol Standards» (STD 1). Документ можно распространять свободно.

Предисловие

Этот документ представляет собой обновленный вариант RFC 1716 - исторического документа, описывающего требования к маршрутизаторам. RFC 1716 является результатом большой работы целой группы специалистов, но на сегодняшний день уже не отражает современных технологий и не может рассматриваться в качестве стандарта.

Перед редактором данного документа была поставлена задача описать требования к маршрутизаторам с учетом современного состояния, чтобы данный стандарт мог использоваться как спецификация требований и руководство для разработчиков. Редактора просили обновить документ, чтобы сделать его полезным при спецификации поставок маршрутизаторов и их разработке. При подготовке документа использовался опыт предшественников и подготовленные ими тексты. Все хорошее в документе от предшественников, за ошибки отвечает редактор.

Содержание и форма этого документа в значительной степени являются результатами работы руководителя группы, а также автора и первого редактора документа – Филиппа Алмквиста (Philip Almquist). Большая работа проделана также редактором предыдущей версии – Фрэнком Кастенхольцем (Frank Kastenholz). Без его работы этот документ просто не увидел бы света.

Оглавление

1. Введение

Этот документ заменяет RFC 1716 «Requirements for Internet Gateways» ([INTRO:1]).

В документе определяются и обсуждаются требования к устройствам, выполняющим функции пересылки пакетов на сетевом уровне стека протоколов IP. Сообщество Internet обычно называет такие устройства маршрутизаторами IP или просто маршрутизаторами, в модели OSI подобные устройства называются промежуточными системами (intermediate system). Во многих старых документах Internet эти устройства называют шлюзами (gateway), однако в последнее время толкование термина gateway несколько изменилось и этим словом обозначают, прежде всего, шлюзы прикладного уровня.

Маршрутизатор IP отличается от других устройств коммутации пакетов тем, что он проверяет заголовки пакетов IP в процессе коммутации. Обычно маршрутизатор удаляет заголовок канального уровня из полученных пакетов, меняет заголовок IP и включает в пакет новый заголовок канального уровня в соответствии с дальнейшей передачей пакета.

Авторы этого документа признают, как и читатели, что многие маршрутизаторы поддерживают более одного протокола. Поддержка множества стеков протоколов будет требоваться для все большей части Internet в ближайшем будущем. В этом документе, однако, не делается попыток описать требования Internet для каких-либо протокольных стеков за исключением TCP/IP.

В документе рассматриваются стандартные протоколы, которые должен использовать подключенный к Internet маршрутизатор, и даны ссылки на RFC и другие документы, описывающие современные спецификации таких протоколов. В документе также исправлены ошибки, допущенные в упомянутых источниках, обсуждаются дополнительные вопросы и даются рекомендации для разработчиков.

Для каждого протокола в этом документе приводится также явный набор требований, рекомендаций и опций. Читатель должен понимать, что список приведенных в документе требований не может быть полным. Такие списки всех требований определяются, прежде всего, в спецификациях стандартных протоколов, а в этом документе приведены лишь поправки, уточнения и дополнения к требованиям стандартов.

Этот документ следует читать вместе с RFC, описывающими требования к хостам Internet ([INTRO:2] и [INTRO:3]). Хосты и маршрутизаторы Internet должны обеспечивать возможность передачи и приема дейтаграмм IP. Основным различием между хостами и маршрутизаторами Internet является реализация в маршрутизаторах алгоритмов пересылки пакетов, которая не требуется от хостов. Каждый хост Internet, работающий как маршрутизатор, должен соответствовать всем требованиям, приведенным в настоящем документе.

Модель взаимодействия открытых систем предполагает, что маршрутизаторы при необходимости должны корректно работать, как хосты Internet. В документе приведены рекомендации по решению этой задачи. Для упрощения структуры документа и его последующих обновлений из документа исключено обсуждение требований к хостам, рассмотренных в [INTRO:2] и [INTRO:3], а в соответствующих местах просто даны ссылки на эти документы. В отдельных случаях требования, приведенные в [INTRO:2] и [INTRO:3], несколько изменены в данном документе.

Качественные реализации протоколов, выполненные с соблюдением соответствующих RFC, не будут сколь-нибудь значительно отклоняться от требований данного документа. Подготовка таких реализаций зачастую требует взаимодействия с технической частью сообщества Internet и должна следовать принятой практике разработки коммуникационных приложений. Во многих случаях приведенные в этом документе требования уже указаны в спецификациях протоколов и включение их в данный документ является отчасти избыточным. Такое дублирование требований обусловлено, в частности, тем фактом, что некоторые реализации маршрутизаторов были выполнены некорректно, что вызывает проблемы с точки зрения взаимодействия, производительности и устойчивости систем.

В документе обсуждается и разъясняется множество требований и рекомендаций. Простое указание списка требований было бы опасно в силу перечисленных ниже причин:

- некоторые из приведенных в документе требований более важны, чем другие, а отдельные функции являются необязательными;
- некоторые функции критичны для определенных применений маршрутизаторов, но могут не играть никакой роли в других случаях;
- существует множество причин, по которым продукция той или иной компании, предназначенная для применения в специфических условиях, может использовать другой набор требований к реализации.

Однако спецификациям, приведенным в документе, нужно следовать для обеспечения взаимодействия в сложной и разнородной среде Internet. Хотя большинство современных реализаций не соответствует приведенным требованиям в той или иной степени, соответствие данной спецификации является идеалом, к которому следует стремиться разработчикам.

Приведенные требования основаны на современной архитектуре Internet. Документ будет обновляться по мере развития сети в целях обеспечения большей ясности и включения дополнительной информации в тех областях, которые будут меняться.

1.1 Работа с документом

1.1.1 Организация документа

В этом документе используется многоуровневая структура, как в [INTRO:2] и [INTRO:3]. Раздел 2 описывает уровни архитектуры Internet. В разделе 3 рассматривается канальный уровень (Link Layer), разделы 4 и 5 посвящены протоколам сетевого уровня (Internet Layer) и механизмам пересылки, в разделе 6 обсуждается транспортный уровень (Transport Layer). Протоколам вышележащих уровней посвящены разделы 7 - 9. В разделе 7 обсуждаются протоколы обмена маршрутной информацией, в разделе 8 рассматриваются вопросы управления сетями, а в разделе 9 обсуждаются прочие протоколы вышележащих уровней. В заключительном разделе рассматриваются функции эксплуатации и обслуживания. Такая организация документа выбрана в целях простоты, ясности и соответствия

структуре RFC, описывающих требования к хостам. Приложения к данному документу включают библиографию, глоссарий и некоторые прогнозы в части будущих направлений стандартизации маршрутизаторов.

При описании требований предполагается, что реализация отражает используемые здесь уровни структурирования протоколов. Однако жесткое следование описанной структуре уровней может оказаться неудобным для реализации протокольных стеков и подготовки рекомендаций для разработчиков. Протоколы различных уровней взаимодействуют между собой с использованием достаточно сложных механизмов и в некоторых случаях одна функция может включать в себя несколько разных уровней. Существует множество вариантов реализации, для которых жесткое деление на уровни не подходит. Разработчикам следует внимательно прочесть документы [INTRO:4] и [INTRO:5].

Все основные части данного документа включают в себя несколько параграфов, перечисленных ниже.

(1) Введение

(2) **Общие вопросы** - рассматриваются спецификации протокола по разделам исходного стандарта, указываются и исправляются ошибки, обсуждаются требования, которые могли быть неточно или некорректно определены, а также приводятся дополнительные разъяснения и уточнения.

(3) **Частные вопросы** - обсуждается устройство протокола и вопросы реализации, которые не были включены в общий раздел.

Во многих темах данного документа содержатся также параграфы, помеченные как **Обсуждение** или **Реализация**. Эта информация приведена для дополнительного уточнения и разъяснения текста предшествующих требований. В параграфах **Реализация** описываются варианты, которые разработчики могут использовать в качестве модели. Параграфы **Обсуждение** и **Реализация** не являются частью стандарта.

1.1.2 Уровни требований

В этом документе слова, обозначающие уровень требований, выделены жирным шрифтом. В число таких слов входят:

- **Обязательно** (MUST)

  Этот уровень означает, что соответствующее требование спецификации является необходимым. Отказ от выполнения таких требований приведет к возникновению критических ошибок. Не существует никаких причин, которые могли бы обосновать отказ от выполнения требования.

- **Обязательно для реализации** (MUST IMPLEMENT)

  Эта фраза означает, что соответствующий элемент является обязательным для каждой реализации, но может быть выключен по умолчанию.

- **Недопустимо** (MUST NOT)

  Этот уровень используется для обозначения полного запрета.

- **Следует** (SHOULD)

  Этот уровень означает, что могут существовать причины, по которым та или иная реализация может не соответствовать данному требованию. Разработчикам следует принимать во внимание, что отказ от реализации таких требований может приводить к возникновению проблем.

- **Следует реализовать** (SHOULD IMPLEMENT)

  Эта фраза обозначает уровень, когда тот или иной элемент следует реализовать, но он может быть отключен по умолчанию.

- **Не следует** (SHOULD NOT)

  Эта фраза относится к тем случаям, когда существуют причины, в силу которых описываемое поведение допустимо и даже полезно. Однако разработчикам следует понимать, что к решению вопроса о реализации любого поведения с такой меткой, нужно подходить осторожно.

- **Возможно** (MAY)

  Этот уровень используется для обозначения необязательных элементов. Одни производители могут поддерживать такие требования, а другие - отказаться от их выполнения.

1.1.3 Соответствие спецификации

Некоторые требования применимы ко всем маршрутизаторам, а иные связаны только с теми маршрутизаторами, в которых реализованы определенные функции или протоколы. В следующих параграфах описываются **общие** требования, применимые к каждому маршрутизатору, и набор требований, возникающих в результате реализации определенных функций или протоколов.

Отметим, что не все **общие** требования провозглашены непосредственно в данном документе. Спецификация включает фрагменты требований к хостам из документов [INTRO:2] и [INTRO:3]. С точки зрения соответствия спецификации не имеет значения, где провозглашены **общие** требования - в данном документе или спецификациях требований к хостам.

Реализация считается условно совместимой с данной спецификацией, если она соответствует всем **общим** требованиям уровней MUST, MUST IMPLEMENT и MUST NOT. При выполнении всех **общих** требований уровней SHOULD, SHOULD IMPLEMENT, и SHOULD NOT реализация считается безусловно совместимой. Реализация не соответствует требованиям, если она не является условно (или безусловно) совместимой (т. е., в ней не выполняется хотя бы одно из **общих** требований уровня MUST, MUST IMPLEMENT или MUST NOT).

В данной спецификации встречаются упоминания о том, что в реализации **следует** поддерживать переменные управления и этим переменным **следует** по умолчанию присваивать некие значения. Безусловно совместимые

реализации поддерживают принятое по умолчанию поведение и соответствующие переменные. Для условно совместимых реализацией должно быть явно документировано наличие принятых по умолчанию значений переменных или возможность задания значений при отсутствии принятых по умолчанию. Если реализация не соответствует ни одному из этих вариантов, она считается несовместимой с данной спецификацией.

Для всех требований уровня SHOULD и SHOULD NOT маршрутизатор может поддерживать конфигурационные опции, которые позволят задать поведение маршрутизатора, отклоняющееся от требований данной спецификации. Наличие таких опций не нарушает условной совместимости со спецификацией, если принятые по умолчанию значения опций обеспечивают работу маршрутизатора в соответствии с требованиями спецификации.

Более того, в тех случаях, когда данный документ не содержит явных запретов, значения некоторых опций могут приводить к нарушению требований уровня MUST или MUST NOT. Маршрутизаторы, поддерживающие такие опции, остаются совместимыми со спецификацией (условно или безусловно), если каждая из таких опций по умолчанию использует значение, которое обеспечивает соответствие маршрутизатора требованиям спецификации. Авторы данной спецификации настоятельно рекомендуют разработчикам отказаться от таких опций даже в тех случаях, когда они обусловлены требованиями рынка. Те или иные требования отнесены к уровню MUST или MUST NOT по той причине, что специалисты в данной сфере сочли эти требования важными с точки зрения взаимодействия и корректной работы Internet. Производителям следует взвешенно оценивать потребности пользователей, удовлетворение которых может приводить к нарушению спецификации.

Естественно, данный документ не является полной спецификацией маршрутизатора IP, а скорее служит профилем OSI. Например, документ требует реализации множества протоколов. Хотя большая часть спецификаций таких протоколов не дублируется в документе, разработчикам следует выполнять требования соответствующих спецификаций.

1.2 Отношения с другими стандартами

Существует несколько документов, тесно связанных с данной спецификацией:

- *INTERNET OFFICIAL PROTOCOL STANDARDS*

  Этот документ описывает процесс принятия стандартов Internet и содержит списки стандартов для протоколов с указанием состояния каждого стандарта. На момент подготовки документа текущая версия STD 1 была представлена в RFC 1780[1], [ARCH:7]. Этот документ периодически обновляется и следует пользоваться его последней версией.

- *Assigned Numbers*

  В этом документе содержится список значений, выделенных для параметров, которые используются различными протоколами. Например, коды протоколов IP, номера портов TCP, коды опций Telnet, типы оборудования ARP, имена типов терминалов. На момент подготовки спецификации текущая версия STD 2 содержалась в RFC 1700, [INTRO:7][2]. Данный документ периодически обновляется и следует пользоваться последней версией.

- *Host Requirements*

  Эта пара документов содержит спецификации требований к хостам и разъяснения неоднозначностей в спецификациях стандартов. Отметим, что указанные в этих документах требования применимы и к маршрутизаторам, если в настоящем документе явно не сказано иное. На момент подготовки этого документа текущая версия требований к хостам опубликована в RFC 1122 и RFC 1123 (STD 3), [INTRO:2] и [INTRO:3].

- *Router Requirements* (ранее Gateway Requirements)

  Настоящий документ.

Отметим, что эти документы создавались и обновлялись в разное время. При обнаружении противоречий следует отдавать предпочтение информации, содержащейся в более новом документе.

Эти и другие протоколы Internet можно получить по адресу:

The InterNIC

DS.INTERNIC.NET

InterNIC Directory and Database Service

info@internic.net

+1-908-668-6587

URL: http://ds.internic.net/[3]

1.3 Общие вопросы

В этом параграфе рассматривается несколько вопросов, с которыми следует разобраться каждому разработчику программ Internet.

1.3.1 Постоянное изменение Internet

Непредсказуемо быстрый рост Internet порождает проблемы управления и масштабирования в гигантских системах передачи дейтаграмм. В результате решения таких проблем изменяются и спецификации, описываемые в данном документе. Постоянно разрабатываются новые протоколы маршрутизации и обновляются существующие протоколы. Кроме того, появляются новые и изменяются существующие протоколы уровня Internet. Маршрутизаторы играют

[1] На момент публикации этого перевода текущая версия STD 1 была представлена в RFC 5000. *Прим. перев.*
[2] В соответствии с RFC 3232 документ Assigned Numbers утратил силу и список выделенных значений доступен в базе данных на сайте www.iana.org. *Прим. перев.*
[3] Сайт ds.internic.net в настоящее время не поддерживается, а копии документов RFC можно найти на сайте www.rfc-editor.org. *Прим. перев.*

важнейшую роль в работе сети Internet, а число установленных в сети маршрутизаторов во много раз меньше числа хостов Internet. Разработчики должны быть готовы к тому, что стандарты для маршрутизаторов будут появляться значительно чаще, чем стандарты для хостов. Изменения планируются и осуществляются под контролем и с участием производителей сетевой продукции и организаций, ответственных за работу сетей.

Обновление и постоянное совершенствование являются неотъемлемыми чертами современных сетевых протоколов и такая ситуация будет сохраняться еще достаточно долго. Разработчики коммуникационных программ для стека протоколов Internet (или иных протоколов) должны поддерживать и обновлять свои программы с учетом изменяющихся спецификаций для того, чтобы не оставить в беде несчастных пользователей. Internet представляет собой большую коммуникационную сеть и пользователи постоянно контактируют между собой через эту сеть. Опыт и знания разработчиков, реализованные в их программах, за короткое время становятся достоянием технического сообщества Internet.

1.3.2 Принцип устойчивости

Для протоколов всех уровней существует общее правило, которому приложения должны следовать во избежание проблем с устойчивостью и взаимодействием [TRANS:2]:

Предъявлять жесткие требования по отношению к себе,
быть более мягким по отношению к другим[1].

Программы должны уметь обрабатывать все мыслимые ошибки, не имеет значения вероятность возникновения той или иной ошибки - раньше или позже пакет с любой возможной комбинацией ошибок и/или атрибутов будет получен и программа должна быть готова к обработке такого пакета. Если программа не может эффективно обрабатывать ошибки, она приведет прямой дорогой к хаосу. В общем случае лучше предположить, что сеть наводнена зловредными объектами, которые постоянно передают пакеты, предназначенные для нанесения максимального вреда. Такое предположение обеспечит высокий уровень защиты. Наиболее серьезные проблемы в Internet связаны с неисследованными механизмами, включающимися с малой вероятностью, намерения обычных злоумышленников никогда не могут принести такого вреда!

На всех уровнях программ маршрутизаторов должны быть реализованы средства адаптации. В качестве простого примера рассмотрим спецификацию протокола, использующего численные значения для какого-либо поля в заголовке (например, тип, номер порта или код ошибки), - при разработке следует предполагать, что используемая нумерация неполна. Если спецификация протокола предполагает четыре возможных кода ошибки, приложение должно уметь обрабатывать по крайней мере пять типов ошибок (4 заданных и все остальные). Появление не определенных в спецификации кодов должно протоколироваться (см. ниже), но не должно нарушать работу системы.

Почти так же важен и другой аспект - программы на других маршрутизаторах могут содержать определения, которые могут толкнуть маршрутизатор на неразумные, но допустимые с точки зрения протокола действия. Естественным решением будет «поиск неразумных хостов» - программы маршрутизатора должны быть готовы не просто переносить появление неразумных хостов, но и участвовать в процессе ограничения вредных воздействий, которые подобные хосты могут нанести сетевым объектам общего пользования.

1.3.3 Протоколирование ошибок

Сеть Internet включает огромное количество разнотипных систем, в каждой из которых реализовано множество протоколов и уровней, некоторые из таких систем наверняка содержат ошибки в программах стека протоколов Internet. В результате сложности, разнотипности и использования распределенных функций диагностика Internet является весьма непростой задачей.

Упростить поиск проблем помогает использование хостами специальных средств протоколирования ошибок и странностей в поведении протоколов. При записи таких событий важно включать максимум диагностической информации. Часто бывает весьма полезно записывать заголовки пакетов, вызывающих ошибки. Однако следует знать меру - средства протоколирования ошибок не должны отнимать слишком много ресурсов маршрутизатора и снижать эффективность его работы.

При записи информации об ошибках существует вероятность получения журнальных файлов огромного размера - таких ситуаций можно избежать, используя «циклический» журнал или включая запись только для диагностики определенных сбоев. Полезно также фильтровать и считать повторяющиеся последовательные сообщения. Представляется привлекательной приведенная ниже стратегия:

(1) всегда считать аномальные события и делать содержимое счетчиков доступным с помощью протоколов управления сетью (см. главу 8.);

(2) поддерживать возможность выбора протоколируемых событий (например, записывать все ошибки, связанные с хостом X).

Дополнительную информацию по вопросам протоколирования работы вы найдете в [MGT:5].

1.3.4 Настройка конфигурации

Идеальной реализацией маршрутизатора будет та, на которой настройка стека протоколов Internet будет полностью автоматизирована (self-configuring). Однако этот идеал недостижим и на практике к нему не удается даже серьезно приблизиться. Многочисленные попытки разработчиков упростить настройку конфигурации на деле приносят больше вреда, нежели пользы. Маршрутизатор, способный начать работу без каких-либо настроек, почти наверняка выберет некорректное значение хотя бы для одного параметра, что может привести к возникновению серьезных проблем в любой из сетей, к которым подключен такой маршрутизатор.

В этом документе вы будете часто встречать требования, где параметры являются опциями настройки. Существует несколько причин появления таких требований. В некоторых случаях это обусловлено отсутствием согласия по вопросу выбора наилучшего значения и в будущем может потребоваться установка иного значения параметра. В других случаях значение параметра может зависеть от внешних факторов (например, распределение нагрузки, скорость, топология

[1] В оригинале «Be conservative in what you do, be liberal in what you accept from others.» *Прим. перев.*

соседних сетей) и алгоритмы автоматической настройки могут отсутствовать или не обеспечивать полной настройки параметров. Причиной использования таких параметров могут послужить и административные требования.

Наконец, часть конфигурационных опций может потребоваться для обеспечения взаимодействия с устаревшими или содержащими ошибки реализациями протоколов, распространяемыми без исходных кодов (к несчастью, такое встречается в Internet достаточно часто). Для обеспечения корректного сосуществования с такими «сбойными» системами администраторам зачастую приходится «расстраивать» (mis-configure) корректно работающие системы. Такие проблемы будут решаться сами собой по мере удаления сбойных систем, но разработчики не должны оставлять этот вопрос без внимания.

Когда мы говорим, что параметр требует настройки, это не означает требования читать значение параметра из конфигурационного файла при каждой загрузке. Мы рекомендуем разработчикам устанавливать для таких параметров используемые по умолчанию значения - тогда в конфигурационных файлах могут содержаться лишь те значения, которые не совпадают с принятыми по умолчанию.

В этом документе для ряда случаев указаны значения, которые следует использовать по умолчанию. Выбор принятых по умолчанию значений является достаточно важным вопросом для случаев использования вместе с существующими сбойными системами. По мере продвижения Internet к полной интероперабельности, принятые по умолчанию значения будут реализовать официальный протокол, а не «расстраивать» систему для обеспечения совместимости с плохо работающими реализациями. Хотя рынок заставляет некоторых производителей устанавливать по умолчанию значения для «расстройки», мы рекомендуем использовать по умолчанию значения, соответствующие стандарту.

В заключении отметим, что производители продукции должны предоставлять полную документацию по всем конфигурационным параметрам, указывая допустимые значения и описывая влияние параметров на работу системы.

1.4 Алгоритмы

В данном документе рассматривается несколько алгоритмов, которые могут использоваться в маршрутизаторах. Эти алгоритмы не являются обязательными сами по себе и маршрутизатор не обязан реализовать каждый алгоритм, описанный в этом документе. Реализация просто должна обеспечивать характеристики, которые извне представляются в точности такими же, как при использовании данного алгоритма.

Описание алгоритмов отличается от способов, которые хорошие разработчики могут использовать для реализации этих алгоритмов. Грамотный разработчик будет выбирать такие алгоритмы и методы реализации, которые будут обеспечивать соответствие требованиям, но могут быть проще или работать более эффективно.

Отметим, что искусство разработки эффективных реализаций маршрутизаторов выходит за пределы данного документа.

2. Архитектура INTERNET

В этом разделе не содержится каких-либо требований, однако здесь даны полезные сведения об основах архитектуры Internet и маршрутизаторов.

Рассмотрению основ архитектуры Internet и поддерживаемых протоколов посвящена книга DDN Protocol Handbook [ARCH:1], основы архитектуры рассмотрены также в работах [ARCH:2], [ARCH:3], [ARCH:4]. Архитектура и протоколы Internet рассматриваются также во многих книгах, включая [ARCH:5] и [ARCH:6].

2.1 Введение

Сеть Internet состоит из множества соединенных между собой пакетных сетей, которые поддерживают обмен информацией между хостами на основе стека протоколов Internet. Этот стек включает IP[1], ICMP[2], IGMP[3] и различные протоколы транспортного и прикладного уровня. Как указано в параграфе 1.2, IESG[4] периодически выпускает документ Official Protocols, содержащий список всех протоколов Internet.

Все протоколы Internet используют IP в качестве базового механизма передачи. IP представляет собой межсетевой сервис, основанный на обмене дейтаграммами (без организации прямых соединений), и обеспечивает адресацию, задание типа обслуживания, фрагментацию-сборку и защиту. Протоколы ICMP и IGMP рассматриваются как часть IP, хотя они работают на основе протокола IP. Протокол ICMP обеспечивает передачу сообщений об ошибках, управление потоком данных и другие средства управления. Протокол IGMP обеспечивает для хостов и маршрутизаторов механизмы включения в группы IP multicast и выхода из таких групп.

Гарантированная доставка данных в стеке протоколов Internet обеспечивается с помощью протоколов транспортного уровня типа TCP[5], которые поддерживают сквозное управление соединениями, повтором передачи и порядком доставки пакетов. На транспортном уровне также обеспечивается сервис без организации прямых соединений (connectionless) на основе протокола UDP[6].

2.2 Элементы архитектуры

2.2.1 Протокольные уровни

Для связи через Internet на хостах должен использоваться многоуровневый набор протоколов, соответствующий стеку протоколов Internet. Обычно на хостах реализован по крайней мере один протокол для каждого из уровней.

Уровни протоколов, используемые в архитектуре Internet, описаны в работе [ARCH:7].

- **Прикладной уровень** (Application Layer)

[1]Internet Protocol - протокол Internet.
[2]Internet Control Message Protocol - протокол обмена управляющими сообщениями.
[3]Internet Group Management Protocol - протокол управления группами.
[4]Internet Engineering Steering Group.
[5]Transmission Control Protocol - протокол управления передачей.
[6]User Datagram Protocol - протокол пользовательских дейтаграмм.

Прикладной уровень располагается в верхней части стека протоколов Internet. В стеке Internet прикладной уровень не разделен на подуровни, хотя некоторые из протоколов прикладного уровня Internet содержат внутренние подуровни. Прикладной уровень стека Internet объединяет в себе функции двух уровней (Presentation - уровень представления и Application - прикладной) эталонной модели OSI [ARCH:8].

Мы будем различать две категории протоколов прикладного уровня - пользовательские протоколы, которые предоставляют услуги непосредственно пользователю, и протоколы поддержки (служебные), обеспечивающие системные функции общего назначения. Наиболее распространенными пользовательскими протоколами Internet являются:

- Telnet (удаленный вход в систему);
- FTP (передача файлов);
- SMTP (доставка электронной почты).

Существует множество стандартизованных и частных пользовательских протоколов.

Служебные протоколы используются для преобразования имен, загрузки ОС и управления - к числу таких протоколов относятся SNMP, BOOTP, RARP, DNS (Domain Name System) и многочисленные протоколы маршрутизации.

Относящиеся к маршрутизаторам протоколы прикладного уровня рассмотрены в разделах 7 - 9.

- **Транспортный уровень** (Transport Layer)

Транспортный уровень обеспечивает сквозную связь (end-to-end) между приложениями через сеть. Этот уровень является эквивалентом транспортного уровня эталонной модели OSI, но включает в себя также функции сеансового уровня OSI, связанные с организацией и завершением сеансов.

На транспортном уровне используются два основных протокола:

- Transmission Control Protocol (TCP) - протокол управления передачей;
- User Datagram Protocol (UDP) - протокол пользовательских дейтаграмм.

TCP представляет собой основанный на соединениях (connection-oriented) транспортный сервис с гарантированной доставкой пакетов, обеспечивающий надежную доставку с сохранением порядка пакетов и управлением потоком данных. Протокол UDP не использует явных соединений (connectionless) и передает данные в виде дейтаграмм без гарантии доставки. Исследовательскими организациями были разработаны и другие протоколы транспортного уровня, которые могут получить статус стандартных протоколов.

Более подробное описание протоколов транспортного уровня приведено в разделе 6.

- **Уровень Internet** (Internet Layer)

Все транспортные протоколы используют протокол IP для передачи данных от отправителя к получателю. IP представляет собой службу доставки дейтаграмм без организации соединений, не обеспечивающую сквозной гарантии доставки. При доставке на хост получателя дейтаграммы IP могут оказаться поврежденными, кроме того, не гарантируется сохранение порядка их доставки, отдельные дейтаграммы могут быть потеряны, а некоторые - продублированы. Если требуются гарантии доставки, ответственность за такие гарантии должны брать на себя вышележащие уровни. Протокол IP отвечает за адресацию, обозначение типа сервиса, фрагментацию и сборку, а также защиту.

Передача данных без организации соединений лежит в основе протокола IP и является одной из основных характеристик архитектуры Internet.

Управляющий протокол ICMP является важной составной частью IP, хотя с точки зрения архитектуры он работает поверх IP (т. е., использует IP для передачи данных, подобно транспортным протоколам TCP и UDP). ICMP обеспечивает доставку сообщений об ошибках, перегрузке сети и перенаправлении пакетов для первого маршрутизатора (first-hop).

IGMP представляет собой протокол уровня Internet, используемый для организации динамических групп хостов с целью группового обмена информацией (IP multicasting).

Протоколы уровня Internet (IP, ICMP и IGMP) более подробно рассмотрены в разделе 4.

- **Канальный уровень** (Link Layer)

Для связи с непосредственно подключенными к нему сетями хост должен поддерживать коммуникационный протокол, используемый для обмена данными с сетью. Мы будем называть его протоколом канального уровня (Link Layer).

В некоторых старых документах этот уровень называется сетевым (Network Layer), но это совсем не то, что сетевой уровень модели OSI.

Этот уровень включает все функции, расположенные ниже уровня Internet и выше физического уровня (Physical Layer - соединения, кодирование сигналов). Канальный уровень отвечает за корректную доставку сообщений, между которыми он не делает различий.

Протоколы канального уровня в общем случае не попадают в сферу стандартов Internet - в сети Internet просто используются существующие стандарты, когда это возможно. Таким образом, стандарты Internet для канального уровня отвечают только за преобразование адресов и передачу пакетов IP с использованием того или иного протокола канального уровня. Стандарты Internet для канального уровня рассмотрены в разделе 3.

2.2.2 Сети

От входящих в состав Internet сетей требуется лишь передача пакетов без организации прямых соединений. Согласно спецификации IP дейтаграммы могут доставляться с ошибками, нарушением порядка, дублированием или потерей отдельных пакетов.

Для эффективной работы протоколов, использующих IP (например, TCP), требуется чтобы количество теряемых пакетов было достаточно малым. В сетях, работающих на основе прямых соединений, обеспечивается высокая надежность доставки через виртуальные устройства (каналы), существенно повышающая сквозной уровень устойчивости системы, но такой устойчивости не требуется для работы Internet.

Входящие в Internet сети можно разделить на два основных класса:

- Локальные сети (ЛВС, LAN)

  ЛВС могут быть устроены по-разному. В общем случае ЛВС обычно имеет небольшие размеры в пространстве (например, одно или несколько зданий) и обеспечивает широкополосные каналы с малыми задержками. Локальные сети могут быть пассивными (например, Ethernet) или активными (например, ATM).

- Распределенные сети (WAN)

  Разнесенные на значительные расстояния хосты и ЛВС объединяются в так называемые распределенные или территориальные сети[1]. Такие сети могут иметь сложную внутреннюю структуру каналов и пакетных коммутаторов, а могут строиться на базе простых соединений «точка-точка».

2.2.3 Маршрутизаторы

Входящие в Internet сети соединяются между собой с помощью устройств пересылки дейтаграмм IP, называемых маршрутизаторами IP. В это документе зачастую будет использоваться просто термин «маршрутизатор» взамен полного названия «маршрутизатор IP». Во многих старых документах для обозначения маршрутизаторов используется термин «шлюз» (gateway).

Изначально маршрутизаторы были реализованы в виде программ коммутации пакетов, выполняемых на процессорах общего назначения. Однако разработка специализированных процессоров позволила снизить цены на маршрутизаторы и повысить их пропускную способность, поэтому в современных маршрутизаторах используют в основном специализированные процессоры. Данная спецификация применима ко всем маршрутизаторам, независимо от их устройства.

Маршрутизатор соединяет два или более логических интерфейса, представленные подсетями IP или безадресными соединениями «точка-точка» (см. параграф 2.2.7). Таким образом, каждый маршрутизатор имеет по крайней мере один физический интерфейс. Пересылка дейтаграмм IP в общем случае требует от маршрутизатора выбрать адрес и подходящий интерфейс для передачи пакета следующему маршрутизатору (next-hop) или конечному получателю. Этот выбор, называемый трансляцией (relaying) или пересылкой (forwarding), зависит от базы маршрутных данных в маршрутизаторе. Эту базу называют также таблицей пересылки или таблицей маршрутизации. Термин «маршрутизатор» происходит от процесса построения маршрутной базы данных, протоколы маршрутизации и параметры конфигурации взаимодействуют между собой в процессе, называемом маршрутизацией.

Базу данных о маршрутах следует поддерживать динамически, в соответствии с текущей топологией Internet. Маршрутизаторы обычно обмениваются между собой маршрутными данными и сведениями о доступности путей.

Маршрутизаторы обеспечивают только доставку дейтаграмм и стараются минимизировать информацию о состоянии, требуемую для решения этой задачи, в целях повышения уровня гибкости и устойчивости.

Устройства коммутации пакетов могут работать также на канальном уровне. Такие устройства называют мостами (bridge). Связанные мостами сегменты сетей используют общий префикс IP и представляют собой одну подсеть IP. Эти устройства не рассматриваются в данном документе.

2.2.4 Автономные системы

Автономная система (AS) представляет собой сегмент сетевой топологии, который включает набор подсетей (с подключенными к ним хостами), соединенных между собой набором маршрутизаторов. Предполагается, что маршрутизаторы и подсети автономной системы управляются и обслуживаются одной организацией. Внутри AS маршрутизаторы могут использовать один или несколько протоколов внутренней маршрутизации, а иногда несколько наборов метрик. Предполагается, что автономная система представляется для других AS единой системой с согласованной внутренней маршрутизацией и картиной адресатов, доступных через данную AS. Автономные системы указываются номерами AS.

Концепция автономных систем играет важную роль в маршрутизации Internet (см. параграф 7.1).

2.2.5 Архитектура адресации

Дейтаграммы IP содержат 32-битовые адреса отправителя и получателя, каждый из этих адресов делится на 2 части, называемые префиксом сети и номером хоста в данной сети.

```
IP-address ::= { <Network-prefix>, <Host-number> }
```

Для доставки дейтаграммы конечному адресату последний маршрутизатор на пути должен отобразить номер хоста (Host-number) или полный адрес IP на адрес канального уровня для этого хоста.

2.2.5.1 Классическая архитектура адресации IP

Классическая адресация, описанная в [INTERNET:2], полезна для описания исторического использования префиксов сетей. Этот язык разработан для описания адресов и используется в данном документе.

[1] Иногда их еще называют глобальными. *Прим. перев.*

Простейшими вариантами префиксов в классической схеме являются префиксы сетей класса A, B, C, D и E. Эти префиксы можно идентифицировать по значениям старших битов адреса, что позволяет легко разделить адрес на префикс сети и номер хоста. Префиксы классической адресации подробно рассматриваются в [INTERNET:18], а краткое их описание приведено ниже.

0xxx - класс A - индивидуальные адреса общего назначения со стандартным 8-битовым префиксом.

10xx - класс B - индивидуальные адреса общего назначения со стандартным 16-битовым префиксом.

110x - класс C - индивидуальные адреса общего назначения со стандартным 24-битовым префиксом.

1110 - класс D - групповые адреса (IP Multicast) с 28-битовым префиксом без возможности агрегирования.

1111 - класс E - зарезервирован для экспериментов.

Эта простая нотация была расширена путем введения концепции подсетей. Подсети потребовались для того, чтобы можно было создавать сколь угодно сложные структуры ЛВС в организациях без взрывного роста числа сетевых префиксов и усложнения маршрутизации. Подсети обеспечивают многоуровневую иерархию структуры маршрутизации для Internet. Связанное с подсетями расширение, описанное в [INTERNET:2], является обязательной частью архитектуры Internet. Основная идея заключается в разделении поля <Host-number> на две части - номер подсети и номер хоста в этой подсети:

```
IP-address ::={ <Network-number>, <Subnet-number>, <Host-number> }
```

Соединенные между собой физические сети организации используют общий префикс, но различаются номерами подсетей. Эти различия между подсетями обычно невидимы за пределами сети. Таким образом при маршрутизации в остальной части Internet используется только префикс сети (поле <Network-prefix>) из IP-адреса получателя. Маршрутизаторы за пределами сети трактуют поля <Submet-number>[1] и <Host-number> как неделимую часть 32-битового адреса IP. В сети, разделенной па подсети, маршрутизаторы используют расширенный префикс сети:

```
{ <Network-number>, <Subnet-number> }
```

Биты, включенные в расширенный префикс, исторически указываются 32-битовыми масками, которые называют масками подсетей. Биты <Subnet-number> **следует** задавать в виде непрерывной последовательности между полями <Network-number> и <Host-number>. В более современных протоколах взамен понятия маски подсети используется размер префикса - значение, которое указывает число битов в расширенном префиксе. Это число совпадает с количеством старших битов адреса, выделяемых с помощью маски подсети. В данном документе предполагается, что все маски подсетей могут быть выражены с помощью длины префиксов.

Создатели концепции подсетей предполагали, что каждая часть сети организации будет иметь единственный номер подсети. На практике часто возникает потребность создать несколько подсетей в одном физическом сегменте сети. Поэтому маршрутизаторы должны быть способны поддерживать несколько подсетей на одном физическом интерфейсе и трактовать (с точки зрения маршрутизации) такой интерфейс как набор [логических] интерфейсов в каждую из подсетей.

2.2.5.2 Бесклассовая междоменная маршрутизация

Взрывной рост сети Internet вынудил к пересмотру политики распределения адресов. Традиционные сети общего назначения (классы A, B и C) были изменены для более эффективного использования 32-битового адресного пространства IP. Бесклассовая междоменная маршрутизация (CIDR[2]) [INTERNET:15] является методом, широко распространенным в современных магистральных сетях Internet для более эффективного использования адресов. CIDR позволяет обеспечить маршрутизацию между сетями произвольных размеров. В этой модели хосты и маршрутизаторы не делают каких-либо предположений об использовании адресных блоков. Адреса классов D (IP Multicast) и E (экспериментальные) были сохранены главным образом из-за принятой политики их выделения.

По определению, CIDR включает три элемента:

- топологически осмысленное распределение адресов;
- протоколы маршрутизации, способные агрегировать информацию о доступности на сетевом уровне;
- согласованный алгоритм пересылки (longest match – максимальная длина совпадения).

Использование концепции сетей и подсетей отошло в прошлое, хотя принятая терминология сохранилась и по-прежнему используется. На смену пришла более эффективная концепция сетевых префиксов. Префикс сети, по определению, является непрерывной последовательностью старших битов адреса, которая указывает некое множество сетей, остальные биты адреса определяют номер хоста. Не требуется использовать однородные префиксы в сети Internet. Для снижения объемов маршрутной информации полезно разделить Internet на домены адресов. Внутри таких доменов доступна детальная информация о входящих в домен сетях, а за пределы домена анонсируется только префикс сети.

Классическая архитектура адресации IP использует адреса и маски подсетей для разделения номера хоста и префикса сети. При использовании концепции префиксов достаточно просто указывать размер префикса. Оба варианта работы с адресами продолжают использоваться. Корректные с точки зрения архитектуры маски подсетей можно представить с помощью размера префикса. Для того, чтобы такое преобразование было возможно, должны выполняться несколько условий:

- маска должна представлять собой непрерывную последовательность единиц в старших битах;
- остальная часть маски должна содержать непрерывную последовательность нулей;
- эти части не должны пересекаться.

Маршрутизаторам **следует** всегда трактовать маршруты, как префиксы, а также **следует** отвергать конфигурационные параметры и маршрутные данные, не совместимые с этой моделью.

```
IP-address ::= { <Network-prefix>, <Host-number> }
```

[1] В оригинале ошибочно указано <Network-prefix>. *Прим. перев.*
[2] Classless Inter Domain Routing.

При использовании CIDR набор адресатов, связанных с адресным префиксом в таблице маршрутизации, может включать свою внутреннюю иерархию. Маршрут, описывающий меньший набор адресатов (более длинный префикс), является более конкретным, нежели маршрут к большему набору адресатов (более короткий префикс), который, следовательно, является менее конкретным. Маршрутизаторы должны использовать при пересылке пакетов более конкретный маршрут (с более длинным префиксом).

2.2.6 IP Multicasting

IP multicasting представляет собой расширение групповой адресации канального уровня для сетей IP. С помощью групповой адресации одну дейтаграмму можно передать множеству хостов без ее передачи всем хостам. В расширенном случае такие хосты могут принадлежать к различным адресным доменам. Такой набор хостов называют multicast-группой. Каждая группа представляется IP-адресом класса D. Дейтаграмма, переданная по адресу группы, будет доставляться каждому члену этой группы с использованием таких же механизмов как для индивидуального (unicast) трафика IP. Отправитель групповой дейтаграммы не обязан быть членом группы.

Семантика принадлежности к группам IP multicast рассматривается в работе [INTERNET:4]. В документе описаны механизмы включения хостов и маршрутизаторов в группы и выхода из групп. В том же документе содержится спецификация протокола IGMP, используемого для мониторинга принадлежности к группам IP.

Пересылка групповых дейтаграмм IP осуществляется с использованием статической маршрутной информации или с помощью протоколов групповой маршрутизации. Устройства, пересылающие групповые дейтаграммы IP, называют также multicast-маршрутизаторами. Такой маршрутизатор может (но не обязан) быть также обычным маршрутизатором IP. Групповые дейтаграммы пересылаются на основе анализ адресов отправителя и получателя. Более подробное описание пересылки пакетов IP multicast приводится в параграфе 5.2.1. В приложении D обсуждаются протоколы групповой маршрутизации.

2.2.7 Безадресные линии и префиксы сетей

Обычно каждый сетевой интерфейс хоста или маршрутизатора IP имеет свой IP-адрес. Это может приводить к неразумному расходу адресов IP, поскольку будет требовать выделения сетевого префикса для каждого соединения «точка-точка».

Для решения этой проблемы была предложена и реализована концепция безадресных (unnumbered) соединений между парой точек. Такие линии не имеют своего сетевого префикса и, следовательно, интерфейсы такого соединения не имеют адресов IP.

Поскольку архитектура IP традиционно предполагает наличие IP-адреса у каждого интерфейса, использование безадресных соединений может приводить к интересным дилеммам. Например, некая опция IP (скажем, Record Route) указывает, что маршрутизатор должен поместить в опцию адрес своего интерфейса, но этот интерфейс не имеет адреса IP. Кроме того, возможны ситуации (см. главу 5), когда маршруты содержат IP-адрес следующего маршрутизатора (next hop). Маршрутизатор ожидает, что такой адрес будет относиться к одной из (под)сетей, с которыми маршрутизатор соединен. Это предположение будет некорректным если маршрутизатор подключен к безадресной линии «точка-точка».

Для решения подобных проблем были предложены две схемы. В первом варианте пара маршрутизаторов, соединенных безадресной линией рассматриваются не как два маршрутизатора, а как две половинки одного виртуального маршрутизатора. Безадресная линия «точка-точка» в этом случае рассматривается, как внутренняя шина такого виртуального маршрутизатора. Две половины виртуального маршрутизатора координируют свои действия таким образом, чтобы они функционировали в точности как один маршрутизатор.

Эта схема согласуется с архитектурой IP, но имеет два существенных недостатка. Во-первых, хотя такая схема и работает хорошо при использовании одной линии «точка-точка», она не подходит для многосвязной системы маршрутизаторов, соединенных множеством безадресных линий. Второй недостаток заключается в том, что взаимодействие между половинками виртуального маршрутизатора является достаточно сложным и не стандартизовано, что ведет к несовместимости маршрутизаторов от разных производителей при соединении их безадресными линиями «точка-точка».

В виду наличия этих недостатков данная спецификация предлагает альтернативную схему, которая была «разработана» неоднократно, но исходная ее разработка принадлежит, по-видимому, Филу Кэрну (Phil Karn). В этой схеме маршрутизатор, имеющий безадресные соединения, имеет также специальный адрес IP, который в данном документе обозначается термином router-id. Значение router-id является одним из IP-адресов маршрутизатора (каждый маршрутизатор имеет по крайней мере один адрес IP). Значение router-id используется в качестве адреса IP для всех безадресных интерфейсов.

2.2.8 Специфические варианты маршрутизаторов

2.2.8.1 Хосты со встроенной маршрутизацией

Маршрутизатор может быть автономной компьютерной системой, предназначенной для выполнения функций пересылки пакетов IP. Однако возможна реализация функций маршрутизатора и на обычном хосте, операционная система которого поддерживает возможность подключения к двум или более сетям. Популярным вариантом такой ОС со встроенными функциями маршрутизации является Berkeley BSD. Поддержка функций маршрутизации в ОС общего назначения упрощает построение сетей, но использование таких ОС таит подводные камни.

(1) Если хост имеет только один действующий сетевой интерфейс, такой хост не следует использовать в качестве маршрутизатора.

Например, хосты со встроенными функциями маршрутизации, которые пересылают широковещательные пакеты и дейтаграммы в ту же сеть, могут вызывать пакетные лавины.

(2) Если (многодомный) хост используется как маршрутизатор, к нему предъявляются все требования, перечисленные в этом документе.

Например, поддержка протоколов маршрутизации и мониторинг системы так же непросты в реализации и важны для хоста со встроенной маршрутизацией, как и для специализированного маршрутизатора.

Требования к маршрутизаторам Internet могут меняться независимо от изменения ОС. Администраторы, обслуживающие хосты со встроенной маршрутизацией в Internet, должны поддерживать и обновлять код маршрутизации. Такое обновление может потребовать наличия исходных кодов встроенного маршрутизатора.

(3) Хост, на котором используется встроенный код маршрутизации, становится частью инфраструктуры Internet. Таким образом, ошибки в программах или настройке могут осложнять взаимодействие с другими хостами. Вследствие этого такой хост утратит часть автономности.

Во многих случаях администраторам хостов со встроенными функциями маршрутизации требуется отключить эти функции. При использовании хоста в качестве маршрутизатора такой запрет будет вызывать проблемы.

(4) Хост со встроенными функциями маршрутизации одновременно используется для решения других задач и их требования по работе и обслуживанию могут вступать в противоречие с аналогичными требованиями для маршрутизаторов.

Например, операции по настройке и обслуживанию маршрутизаторов зачастую выполняются удаленно из центра управления сетью, такое управление может потребовать привилегированного доступа, который администраторы хостов обычно не хотят предоставлять удаленным пользователям.

2.2.8.2 Прозрачные маршрутизаторы

Существуют две модели соединения локальных и распределенных сетей в Internet. В первой модели ЛВС присваивается префикс сети и все маршрутизаторы в Internet должны знать путь к этой сети. Во второй модели ЛВС используют префикс (и адресное пространство) распределенной сети, через которую они подключены. Маршрутизаторы, которые поддерживают вторую модель, называют маршрутизаторами с совместным использованием адресов[1] или прозрачными маршрутизаторами[2]. Данная спецификация посвящена маршрутизаторам, использующим первую модель, но не исключает использования прозрачных маршрутизаторов.

Основная идея прозрачных маршрутизаторов заключается в том, что хосты, расположенные в ЛВС за этим маршрутизатором, используют адреса из префикса распределенной сети перед маршрутизатором. В некоторых случаях такая модель может оказаться весьма полезной, а сколь-нибудь серьезных недостатков у нее нет.

Слова «за» и «перед» маршрутизатором показывают одно из ограничений этой модели - она подходит лишь для географически (или топологически) ограниченной тупиковой[3] сети. Такое ограничение требует использования специфической организации адресов. IP-адреса хостов ЛВС отображаются не небольшое количество (обычно один) адресов распределенной сети. Такое отображение выполняется с обеспечением совместимости с отображением { IP address <-> network address }, используемым в распределенной сети.

В распределенной сети могут использоваться многодомные хосты, но это может приводить к проблемам в маршрутизации, если интерфейсы географически или топологически разделены. Многодомные хосты в двух (и более) распределенных сетях вызывают проблемы в результате возможности спутать адреса.

Поведение таких хостов с точки зрения другого хоста, который кажется находящимся в той же сети, может отличаться, если прозрачный маршрутизатор не может полностью эмулировать сервис распределенной сети. Например, в сети ARPANET используется протокол канального уровня, обеспечивающий индикацию Destination Dead[4] в ответ на попытку передачи пакета хосту, который был выключен. Однако при наличии прозрачного маршрутизатора между ARPANET и ЛВС Ethernet хост в ARPANET не будет получать индикацию Destination Dead для хостов Ethernet.

2.3 Характеристики маршрутизаторов

Маршрутизаторы Internet выполняют перечисленные ниже функции.

(1) Поддержка протоколов Internet, указанных в этом документе, включая протоколы IP, ICMP и другие.

(2) Поддержка интерфейсов в две или большее число пакетных сетей. Для каждой подключенной сети маршрутизатор должен выполнять функции, требуемые в этой сети. Такие функции обычно включают:

- инкапсуляцию и декапсуляцию дейтаграмм IP в кадры подключенной сети и из них (например, поддержка заголовков и контрольных сумм Ethernet);
- прием и передача дейтаграмм IP с размером вплоть до верхнего предела, поддерживаемого сетью; этот размер называют MTU[5];
- трансляция IP-адреса получателя в соответствующий адрес подключенной сети (например, в аппаратный адрес Ethernet), если такая трансляция нужна;
- реакция на сообщения системы управления трафиком и контроля ошибок.

См. раздел 3 (Канальный уровень).

(3) Прием и пересылка дейтаграмм Internet. Важной частью этого процесса является управление буферами, контроль насыщения и беспристрастность при пересылке.

- детектирование ошибок и генерация при необходимости сообщений ICMP;
- отбрасывание дейтаграмм с нулевым значением времени жизни;

[1] Address sharing router.
[2] Transparent router.
[3] Не используемой для транзитного трафика. *Прим. перев.*
[4] Адресат «умер».
[5] Maximum Transmission Unit - максимальный размер передаваемого блока.

– фрагментация дейтаграмм при необходимости в соответствии со значением MTU в следующей по маршруту сети.

Более подробные сведения приведены в разделах 4. Протоколы уровня INTERNET и 5. Уровень INTERNET - пересылка.

(4) Выбор следующего маршрутизатора (next-hop) для каждой дейтаграммы IP на основе информации из базы данных о маршрутах. Более подробная информация содержится в разделе 5. Уровень INTERNET - пересылка.

(5) Поддержка (в большинстве случаев) протокола внутренней маршрутизации (IGP[1]) для передачи маршрутной информации и алгоритмов определения доступности другим маршрутизаторам в своей автономной системе. В дополнение к этому от некоторых маршрутизаторов требуется поддержка протокола внешней маршрутизации (EGP[2]) для обмена топологической информацией с другими автономными системами. Дополнительная информация приведена в разделе 7. Прикладной уровень - протоколы маршрутизации.

(6) Поддержка функций сетевого управления, включая загрузку, отладку, отчеты о состоянии, отчеты об исключительных ситуациях и управление. Дополнительная информация приведена в разделах 8. Прикладной уровень – протоколы управления сетью и 10. Эксплуатация и обслуживание.

Производители маршрутизаторов имеют множество вариантов выбора в части производительности, сложности и функциональности для каждого маршрутизатора. При выборе может оказаться полезным рассматривать Internet, как гетерогенную неполносвязную систему. В силу технологических и географических причин эта система представляет собой глобальную опорную сеть со множеством подключенных к ней по краям ЛВС. Все больше таких краевых сетей оказывается связанными между собой, что делает их менее изолированными и более требовательными к маршрутизации.

- Глобальная система соединений (опорная сеть) состоит из множества WAN-сетей, к которым подключены маршрутизаторы нескольких AS; незначительное количество хостов подключено напрямую к таким сетям.

- Большинство хостов подключено к ЛВС. Многие организации имеют кластеры локальных сетей, связанные между собой локальными маршрутизаторами. Каждый кластер соединен через один или несколько маршрутизаторов с глобальной опорной сетью. Если кластер подключен только в одной точке, такая сеть называется тупиковой или краевой[3].

К маршрутизаторам опорной сети обычно предъявляются перечисленные ниже требования.

- Поддержка расширенных алгоритмов маршрутизации и пересылки.

  Для таких маршрутизаторов требуются алгоритмы, которые являются достаточно динамичными, отличаются незначительными издержками на обработку и поддерживают маршрутизацию по типам обслуживания. Вопросы предотвращения перегрузок пока решены не полностью (см. параграф 5.3.6). Ожидается улучшение ситуации в этой сфере по мере проведения исследований.

- Высокий уровень доступности.

  Такие маршрутизаторы должны быть весьма надежными и работать безостановочно. Отказы программ и оборудования могут оказывать широкое (иногда глобальное) воздействие. В случае отказа должна обеспечиваться возможность быстрого восстановления. В любой среде маршрутизатор должен обеспечивать устойчивую работу и возможность функционирования (хотя бы с ограниченными функциями) в условиях экстремального насыщения или сбоев в сетевых ресурсах.

- Расширенные эксплуатационные возможности и функции обслуживания.

  Маршрутизаторы Internet обычно работают без постоянного присмотра человека, а управление осуществляется удаленно из сетевых центров. Для решения этих задач могут потребоваться изощренные средства мониторинга и контроля трафика и других событий, а также для диагностики при отказах.

- Высокая производительность.

  Для организации протяженных соединений Internet в основном используются полнодуплексные каналы 56 кбит/с, DS1 (1,544 Мбит/с) или DS3 (45 Мбит/с). В локальных сетях обычно используется полудуплексная среда Ethernet (10 Мбит/с) или (существенно реже) FDDI (100 Мбит/с). Однако технологии сетевых сред постоянно совершенствуются и в будущем станет возможным существенное расширение пропускной способности.

Требования к маршрутизаторам, используемым в краевых ЛВС (например, в кампусных сетях), определяются в основном потребностями локальной сети. Это могут быть устройства с высоким или средним уровнем производительности, возможно выпущенные разными производителями, используемые одной организацией (например, вычислительным центром). Такие маршрутизаторы должны характеризоваться невысоким уровнем задержки, устойчивостью к взрывному росту трафика, а также возможностью управления ресурсами в зависимости от задержки и типа обслуживания. В таких средах условия эксплуатации и обслуживания менее формализованы, но важность их от этого не снижается. Важность обеспечения динамических механизмов маршрутизации возрастает по мере усложнения сетей и расширения их связности.

Сети имеют свойство расширяться, происходит замена устаревшего оборудования, поэтому вопросы взаимодействия маршрутизаторов разных производителей становятся все более актуальными.

Несмотря на отсутствие полной связности в системе Internet, многие части ее требуют резервирования соединений. Расширение связности позволяет обеспечить надежный сервис даже при отказах отдельных каналов и маршрутизаторов и может также повышать эффективность работы Internet за счет сокращения путей и обеспечения дополнительной пропускной способности соединительных каналов. К сожалению, расширение связности влечет за собой усложнение алгоритмов выбора наилучшего пути к тому или иному адресату.

[1]Internal Gateway Protocol - протокол внутреннего шлюза.
[2]External Gateway Protocol - протокол внешнего шлюза.
[3]Stub network.

2.4 Архитектурные допущения

Современная архитектура Internet базируется на понятии коммуникационных систем. Применительно к маршрутизаторам это означает приведенные ниже требования.

- Internet - это **сеть сетей**.

  Каждый хост напрямую подключен к одной или нескольким сетям, соединение хоста с Internet является только концептуальным. Два хоста одной сети взаимодействуют между собой с использованием того же набора протоколов, который будет применяться при взаимодействии с хостами удаленных сетей.

- Маршрутизаторы не сохраняют информации о состоянии соединений.

  В целях повышения устойчивости коммуникационной системы маршрутизаторы разрабатываются для не связанной с состоянием пересылки каждого пакета IP, независимо от других пакетов. В результате для повышения устойчивости могут организовываться избыточные пути, используемые при возникновении сбоев в сетях или маршрутизаторах.

  Вся информация о состоянии, требуемая для обеспечения сквозного управления потоком данных и гарантий доставки, поддерживается на хостах в программах транспортного и прикладного уровня. Эта информация сосредоточена на паре конечных точек, участвующих в сеансе обмена информацией, и будет теряться только при отказе одной из этих точек. Маршрутизаторы управляют потоком сообщений лишь опосредованно, путем отбрасывания пакетов или увеличения задержки.

  Отметим, что разработчики новых протоколов могут реализовать в маршрутизаторах хранение некоторых сведений о состоянии[1]. Это наиболее вероятно для групповой маршрутизации, резервирования ресурсов и пересылки на основе состояния потоков данных.

- Вопросы сложной маршрутизации должны решаться в маршрутизаторах.

  Маршрутизация является сложной задачей и выполняется она маршрутизаторами, а не хостами. Это является важной предпосылкой для изоляции используемых на хостах программ от изменений, которые могут быть вызваны неизбежной эволюцией архитектуры маршрутизации Internet.

- Система должна быть устойчива к изменениям сети.

  Одной из важных характеристик Internet является устойчивость к изменению различных параметров сетей — пропускная способность каналов, задержки, потеря пакетов, изменение порядка доставки, максимальный размер пакетов. Важную роль играет также устойчивость к отказам в отдельных сетях, маршрутизаторах и хостах за счет использования остающихся соединений. Конечной целью является создание полностью открытой системы межсетевых соединений - маршрутизаторы Internet должны обеспечивать надежное и эффективное взаимодействие с любым маршрутизатором или хостом Internet при соединениях через различные пути Internet.

  Иногда разработчики преследуют менее амбициозные цели. Например, в ЛВС условия обычно значительно более мягкие, нежели в Internet в целом - задержки и число теряемых пакетов существенно ниже, а порядок доставки не нарушается. Некоторые производители выпускают маршрутизаторы, которые достаточно хороши в простых средах ЛВС, но плохо работают при взаимодействии с другими сетями. Производители позиционируют такую продукцию для ограниченного использования в средах ЛВС. Однако изолированные ЛВС рано или поздно утрачивают свою изоляцию, соединяются с другими сетями и могут оказаться связанными с глобальной системой Internet. В результате такие «усеченные» маршрутизаторы начинают создавать проблемы.

  Требования данного документа относятся к полнофункциональным маршрутизаторам и только соответствующие этим требованиям маршрутизаторы могут использоваться практически в любой части Internet.

3. Канальный уровень

В работе [INTRO:1] подробно рассматриваются стандарты канального уровня (передача IP с использованием различных протоколов канального уровня, преобразование ARP и т. п.), однако в данном документе предполагается, что материалы по канальному уровню будут вынесены в отдельный документ. Этот документ будет применим как к хостам, так и к маршрутизаторам и не будет отменять рассмотренные в [INTRO:1] вопросы, связанные с канальным уровнем.

3.1 Введение

К маршрутизаторам предъявляются на канальном уровне точно такие же требования, как к другим типам систем Internet. Эти требования рассмотрены в главе 3 документа Requirements for Internet Gateways [INTRO:1]. Маршрутизатор **должен** соответствовать всем требованиям, **следует** также соблюдать приведенные в документе рекомендации. Поскольку указанный документ выпущен достаточно давно, ниже приводятся некоторые дополнительные требования и разъяснения.

Обсуждение

Предполагается, что сообщество Internet подготовит стандарт требований к канальному уровню Internet, который заменит собой данную главу и главу «INTERNET LAYER PROTOCOLS» в документе [INTRO:1].

3.2 Интерфейс между канальным уровнем и IP

Здесь не предпринимается попыток спецификации интерфейса между канальным уровнем и вышележащими уровнями. Однако отметим, что в других частях данного документа (в частности, в разделе 5) используется информация, связанная с передачей через такой интерфейс.

В этом разделе используются следующие определения:

- физический адрес отправителя (Source physical address);

[1] Сейчас это уже стало реальностью. *Прим. перев.*

адрес канального уровня для хоста или маршрутизатора, от которого получен пакет;

- физический адрес получателя (Destination physical address);

  адрес канального уровня для хоста или маршрутизатора, которому передается пакет.

Информация, передаваемая от канального уровня на сетевой (Internetwork Layer), для каждого принятого пакета включает:

(1) пакет IP [5.2.2];

(2) размер данных в кадре канального уровня (без учета заголовков канального уровня) [5.2.2];

(3) идентификацию физического интерфейса, от которого был получен пакет IP [5.2.3];

(4) классификацию физического адреса получателя пакета, как индивидуального, группового или широковещательного адреса канального уровня [4.3.2], [5.3.4].

В дополнение к этому канальный уровень также должен предоставить:

(5) физический адрес отправителя.

Информация, которая должна приходить от сетевого уровня на канальный для каждого передаваемого пакета, включает:

(1) пакет IP [5.2.1];

(2) размер пакета IP [5.2.1];

(3) физический интерфейс получателя [5.2.1];

(4) IP-адрес следующего интервала [5.2.1];

В дополнение к этому сетевому уровню также следует предоставить:

(5) значение приоритета для канального уровня [5.3.3.2]

Канальный уровень должен также уведомлять уровень Internetwork, если при передаче пакета на канальном уровне возникает ошибка, связанная с предпочтениями канального уровня [5.3.3.3].

3.3 Частные вопросы

3.3.1 Трейлерная инкапсуляция

Маршрутизаторы, подключённые к сетям Ethernet 10 Мбит/с, **могут** принимать и пересылать пакеты, инкапсулированные с использованием трейлеров, описанных в [LINK:1]. Однако маршрутизаторам **не следует** самим порождать пакетов с трейлерной инкапсуляцией. Для маршрутизаторов **недопустима** генерация пакетов с трейлерной инкапсуляцией без предварительной проверки с использованием механизма, описанного в [INTRO:2], возможности восприятия пакетов с трейлерной инкапсуляцией их получателем. Маршрутизаторам **не следует** соглашаться (используя указанный выше механизм) на восприятие пакетов с трейлерной инкапсуляцией.

3.3.2 Протокол преобразования адресов - ARP

Маршрутизаторы, поддерживающие ARP, **должны** быть совместимы с требованиями [INTRO:2], **следует** также добиваться безусловной совместимости.

Для канального уровня **недопустима** передача сообщений Destination Unreachable[1] для адресов IP по причине отсутствия для адреса записи в кэше ARP, **следует** собирать в очередь небольшое число дейтаграмм в течение запроса/отклика ARP и передавать сообщение Destination Unreachable для находящегося в очереди адреса лишь после неудачной попытки трансляции адреса.

Маршрутизатор не **должен** доверять любым откликам ARP, содержащим информацию о том, что адрес канального уровня другого хоста или маршрутизатора является широковещательным или групповым адресом.

3.3.3 Совместное использование Ethernet и 802.3

Маршрутизаторы, подключенные к сетям Ethernet 10 Мбит/с, **должны** соответствовать требованиям Ethernet, указанным в [INTRO:2]. **Следует** также добиваться безусловной совместимости с этими требованиями.

3.3.4 Максимальный размер блока - MTU

Величина MTU для каждого логического интерфейса **должно** быть настраиваемой с возможностью выбора любого значения, допустимого для такого интерфейса.

Многие протоколы канального уровня определяют максимальный размер передаваемого кадра. В таких случаях для маршрутизатора **недопустимо** устанавливать значения MTU, которые позволят передавать кадры больше, чем разрешает протокол канального уровня. Однако маршрутизаторам **следует** пытаться принимать пакеты даже в тех случаях, когда их размер превышает MTU.

Обсуждение

Отметим, что существует более жесткое требование для хостов, указанное в [INTRO:2], в соответствии с которым значение MTU для каждого физического интерфейса должно быть настраиваемым.

Если в сети используется значение MTU меньше, чем максимальный размер кадра на канальном уровне, маршрутизатор может получать пакеты, размер которых превышает MTU, от некорректно настроенных или не полностью инициализированных хостов. В соответствии с провозглашенными выше принципами устойчивости маршрутизатору следует по возможности принимать такие пакеты.

[1] Адресат недоступен.

3.3.5 Протокол PPP

Вопреки [INTRO:1], Internet имеет стандартный протокол для соединений «точка-точка» - протокол PPP[1], описанный в [LINK:2], [LINK:3], [LINK:4], [LINK:5].

Интерфейсом канала «точка-точка» может быть любой интерфейс, предназначенный для передачи данных через такие каналы (коммутируемая или выделенная телефонная линия, виртуальное соединение типа ISDN и т. п.). Обычно для таких линий используются стандартные модемы или битовые последовательные интерфейсы (например, RS-232, RS-449 или V.35), работающие в синхронном или асинхронном режиме. Мультиплексируемые виртуальные каналы зачастую используют специализированные физические интерфейсы.

Последовательный интерфейс общего назначения использует такую же физическую среду, как линия «точка-точка», но поддерживает использование сетей канального уровня, наряду с соединениями «точка-точка». Сети канального уровня (такие, как X.25 или Frame Relay) используют свою спецификацию канального уровня для IP. Маршрутизаторы, использующие линии «точка-точка» или последовательные интерфейсы общего назначения, **должны** поддерживать протокол PPP.

Протокол PPP **должен** поддерживаться для всех имеющихся в маршрутизаторе последовательных интерфейсов общего назначения. Маршрутизатор **может** также поддерживать для линий «точка-точка» протоколы, отличные от PPP. Для интерфейсов «точка-точка» **следует** включать поддержку протокола PPP по умолчанию или требовать настройки канального протокола до активизации интерфейса. Для последовательных интерфейсов общего назначения **следует** требовать настройку конфигурации протокола канального уровня до активизации интерфейса.

3.3.5.1 Введение

В этом параграфе рассматриваются рекомендации для разработчиков маршрутизаторов по обеспечению взаимодействия с другими маршрутизаторами при использовании протокола PPP на синхронных и асинхронных каналах.

Очень важно понимание разработчиками семантики механизма согласования опций. Опции дают локальному устройству способ показать удаленному устройству, что локальное устройство будет воспринимать от удаленного, а не то, что локальное устройство желает передавать удаленному. Удаленное устройство само примет решение о том, что ему удобнее передавать с учетом набора опций, который локальное устройство провозгласило приемлемым. Следовательно, совершенно естественно для удаленного партнера подтвердить (ACK) все указанные опции в конфигурационном запросе LCP Configuration Request (CR), даже если удаленное устройство не поддерживает ту или иную из этих опций. Отметим еще раз, что опции являются лишь механизмом индикации партнеру того, что может быть принято от него, а не того, что ему будет передаваться.

3.3.5.2 Опции LCP

Протокол управления каналом PPP (LCP[2]) поддерживает множество опций, которые могут согласовываться между партнерами. Эти опции включают (наряду с другими) сжатие полей адреса и управления, сжатие поля протокола, схему отображения асинхронных символов[3], максимальный размер принимаемого блока (MRU[4]), мониторинг качества канала (LQM[5]), «магическое число» для детектирования «петель» (loopback detection), протокол парольной аутентификации PAP[6], протокол согласования запросов проверки подлинности CHAP[7] и 32-битовую контрольную сумму кадра (FCS[8]).

Маршрутизатор **может** использовать компрессию полей адреса и управления на синхронных и асинхронных каналах. Сжатие поля протокола также **может** использоваться на синхронных и асинхронных каналах. Маршрутизатор, показывающий, что он может воспринимать такую компрессию, **должен** поддерживать также несжатые заголовки PPP.

Обсуждение

Перечисленные опции управляют представлением заголовков PPP. Обычно заголовок PPP содержит поля адреса, управления и протокола. Для каналов «точка-точка» в качестве адреса используется значение 0xFF, указывающее «широковещательный» адрес. Поле управления содержит значение 0x03 (Unnumbered Information - безадресная информация). Идентификатор протокола представляет собой 2-байтовое значение, которое определяет тип содержимого поля данных в кадре. Если система согласует сжатие полей адреса и управления, она показывает своему партнеру, что будет принимать кадры PPP, не содержащие этих полей, равно как и кадры с такими полями в начале заголовка. Такая индикация не говорит о том, что система будет передавать кадры с удаленными из заголовка полями адреса и управления.

Будучи согласованной, компрессия поля протокола, показывает, что система готова принимать сжатые до одного байта идентификаторы протокола в тех случаях, когда такое сжатие возможно. Такое согласование не требует от партнера передачи сжатых полей протокола.

Использование компрессии полей адреса и управления несовместимо с адресуемым режимом[9] PPP.

Реализация

Некоторые устройства не способны работать с заголовками переменной длины. В таких случаях для удаленного партнера становится важной передача полных заголовков PPP. Разработчики могут обеспечить такое решение путем запрета передачи опции сжатия полей адреса и управления удаленному партнеру. Даже если удаленная сторона показывает возможность приема сжатых заголовков, это не обязывает локальный маршрутизатор передавать такие заголовки.

---

[1] Point-to-Point Protocol.
[2] Link Control Protocol.
[3] Asynchronous character map.
[4] Maximum Receive Unit.
[5] Link Quality Monitoring.
[6] Password Authentication Protocol.
[7] Challenge Handshake Authentication Protocol.
[8] Frame Check Sequence.
[9] Numbered mode.

Маршрутизатор **должен** согласовать используемую схему ACCM[1] для асинхронных каналов PPP, но ему **не следует** согласовывать ACCM для синхронных каналов. Если маршрутизатор принимает попытку согласования ACCM для синхронного канала, он **должен** подтвердить (ACK) эту опцию и игнорировать ее.

Обсуждение

Реализации, поддерживающие синхронный и асинхронный режим работы, могут использовать общий код согласования опций. В таких ситуациях становятся возможными попытки согласования ACCM для синхронных каналов.

Маршрутизатору **следует** согласовать значение максимального размера принимаемых кадров (MRU). Даже если система запросила при согласовании значение MRU < 1500 байтов, она **должна** быть способна принимать кадры размером до 1500 байтов.

Маршрутизатору **следует** согласовывать и поддерживать опцию мониторинга качества канала (LQM).

Обсуждение

В данном документе не обсуждаются правила оценки качества канала. Однако весьма важно (см. параграф 3.3.6), чтобы маршрутизатор мог отключать сбойные каналы.

Маршрутизатору **следует** реализовать и согласовывать опцию magic number для детектирования петель (loopback).

Маршрутизатор **может** поддерживать опции аутентификации PAP и/или CHAP.

Маршрутизатор **должен** поддерживать 16-битовые контрольные суммы FCS и **может** поддерживать 32-битовые контрольные суммы.

3.3.5.3 Опции протокола IPCP[2]

Маршрутизатор **может** предлагать согласование адреса IP и **должен** воспринимать отказ (REJect) от такого согласования.

Маршрутизаторам, работающим при скорости канала 19200 бит/с и ниже, **следует** реализовать и предлагать партнеру использование сжатие заголовков по алгоритму Van Jacobson (VJ). Маршрутизаторам, реализующим компрессию VJ, **следует** поддерживать возможности административного отключения сжатия.

3.3.6 Тестирование интерфейса

Маршрутизатор **должен** поддерживать механизм, который позволяет программам маршрутизации определять доступность физического интерфейса. Для мультиплексируемых интерфейсов, где виртуальные каналы открыты для ограниченного набора соседей, **должен** поддерживаться механизм определения доступности виртуального канала. Маршрутизаторам **следует** поддерживать механизм, позволяющий программам маршрутизации проверить качество работы физического интерфейса. Маршрутизатор **должен** поддерживать механизм уведомления программ маршрутизации об активации и деактивации физического интерфейса в результате действий администратора. Маршрутизатор **должен** поддерживать механизм уведомления программ маршрутизации о доступности и недоступности интерфейса канального уровня, вызванной любыми причинами.

Обсуждение

Для маршрутизаторов критически важно наличие механизма определения корректности работы сетей. Невозможность определения неработающего канала или принятия соответствующих мер при обнаружении такого канала может вести к появлению «черных дыр».

Механизмы обнаружения проблем зависят от протоколов канального уровня и используемого оборудования. Задача состоит в обеспечении максимальной эффективности детектирования отказов на канальном уровне.

4. Протоколы уровня INTERNET

4.1 Введение

В данном разделе и разделе 5 обсуждаются протоколы, используемые на уровне Internet[3] - IP, ICMP и IGMP. Поскольку пересылка пакетов является важнейшей темой для документа, посвященного маршрутизаторам, раздел 5 посвящен исключительно протоколам, непосредственно связанным с пересылкой пакетов. В данном разделе обсуждаются остальные вопросы, связанные с протоколами уровня Internet.

4.2 Протокол INTERNET - IP

4.2.1 Введение

Маршрутизаторы **должны** поддерживать протокол IP, описанный в [INTERNET:1]. Они также **должны** поддерживать обязательные расширения этого протокола - подсети (определены в [INTERNET:2]), широковещание IP (определено в [INTERNET:3]) и бесклассовую маршрутизацию CIDR (определена в [INTERNET:15]).

Разработчикам маршрутизаторов нет необходимости добиваться совместимости с параграфом «Internet Protocol - IP» документа [INTRO:2], поскольку информация из этого параграфа полностью продублирована или заменена в настоящем документе. Маршрутизаторы **должны** быть совместимыми и **следует** делать их безусловно совместимыми с относящимися к IP требованиями параграфа «SPECIFIC ISSUES» в документе [INTRO:2].

Далее в этом документе для некоторых ситуаций в качестве действия указывается отбрасывание полученной дейтаграммы без уведомления[4]. Это означает отбрасывание дейтаграммы без дальнейшей обработки и без передачи ее отправителю какого-либо сообщения об ошибке с помощью ICMP (см. параграф 4.3). Однако в процессе диагностики проблем маршрутизатору **следует** обеспечивать возможность записи информации о событиях в системный журнал (см.

[1] Asynchronous Control Character Map – отображение асинхронных кодов (символов) управления.
[2] IP Control Protocol — протокол управления IP.
[3] Сетевой уровень модели OSI.
[4] Silently discard.

параграф 1.3.3), включая и отбрасывание дейтаграмм без уведомления. Маршрутизатору **следует** также вести подсчет отброшенных дейтаграмм.

4.2.2 Общие вопросы

RFC 791 [INTERNET:1] содержит спецификацию протокола IP.

4.2.2.1 Опции - RFC 791, параграф 3.2

В дейтаграммах, получаемых самим маршрутизатором, уровень IP **должен** интерпретировать понятные ему опции IP и сохранять остальные опции неизменными для их использования протоколами вышележащих уровней.

Протоколам вышележащих уровней может потребоваться возможность установки опций IP в передаваемых ими дейтаграммах или проверки опций в принятых дейтаграммах. В последующих параграфах документа рассматриваются вопросы поддержки конкретных опций IP, требуемых протоколам вышележащих уровней.

Обсуждение

Ни данный документ, ни [INTRO:2] не определяют порядок обработки опций в одном заголовке IP. Хосты и маршрутизаторы, устанавливающие в заголовке множество опций, должны принимать во внимание возможность неоднозначной трактовки некоторых опций, установленных вместе с опцией source-route.

Ниже приведены требования для отдельных опций IP:

(a) Опция защиты (Security)

Некоторые среды требуют наличия опции Security в каждом передаваемом или принимаемом пакете. Маршрутизаторам **следует** реализовать поддержку опции защиты в соответствии с обновленным описанием [INTERNET:5].

Обсуждение

Отметим, что опции защиты, описанные в [INTERNET:1] и RFC 1038 ([INTERNET:16]) утратили свою силу.

(b) Опция идентификатора потока (Stream Identifier)

Эта опция утратила силу и маршрутизаторам **не следует** устанавливать ее в генерируемых дейтаграммах. Маршрутизатор **должен** игнорировать эту опцию в принимаемых дейтаграммах.

(c) Опции задания маршрута отправителем (Source Route)

Маршрутизатор **должен** быть способен действовать, как конечный адресат заданного отправителем маршрута. Если маршрутизатор получает пакет, который содержит завершенный маршрут, заданный отправителем, это говорит о том, что пакет доставлен по назначению. В таких случаях указатель ссылается за пределы последнего поля и адрес получателя в заголовке IP указывает на данный маршрутизатор. Опция **должна** передаваться в неизменном виде транспортному уровню (или для обработки сообщений ICMP).

В общем случае корректный отклик на дейтаграмму с заданным отправителем маршрутом возвращается по тому же пути, который использовался для доставки дейтаграммы. Маршрутизатор **должен** обеспечить способ, который позволит транспортным протоколам и приложениям обратить маршрут source route из принятой дейтаграммы. Этот инвертированный маршрут source route **должен** быть помещен в дейтаграммы, которые генерируются (см. [INTRO:2]) в тех случаях, когда маршрутизатор не смог выполнить требования политики. Однако при соблюдении политики **может** быть выбран иной путь.

Некоторые приложения в маршрутизаторах **могут** требовать обеспечения возможности указания маршрута source route пользователем.

Для маршрутизаторов **недопустима** генерация пакетов, содержащих множество опций source route. Описание поведения маршрутизатора в тех случаях, когда ему нужно переслать пакет, содержащий множество опций source route, приведено в параграфе 5.2.4.1.

При создании опции source route (маршрутизатор генерирует дейтаграмму с заданной им маршрутизацией или опция помещается в пакет в результате действия специального фильтра) эта опция **должна** быть корректно сформирована даже в тех случаях, когда она создается путем обращения записанного маршрута, который ошибочно включает адрес источника (см. случай (B) в приведенном ниже обсуждении).

Обсуждение

Предположим, что дейтаграмма source route маршрутизируется из источника S получателю D через маршрутизаторы G1, G2, Gn. Отправитель S создает дейтаграмму с IP-адресом G1 в качестве получателя, а опция source route содержит остальной путь к конечному адресату. Однако в спецификации имеется неоднозначность, которая позволяет в опции source route передаваемых S дейтаграмм установить вариант (A) или (B):

(A): {>>G2, G3, ... Gn, D} <---- корректно

(B): {S, >>G2, G3, ... Gn, D} <---- ошибка

(знак >> представляет указатель). Если передается вариант (A), дейтаграмма, принятая D, будет содержать опцию {G1, G2, ... Gn >>} с IP-адресами отправителя и получателя. При использовании варианта (B) полученная в D дейтаграмма также будет содержать в опции IP-адреса отправителя и получателя, но опция будет иметь форму {S, G1, ...Gn >>} (хост-отправитель будет указан как первый интервал маршрута).

(d) Опция записи маршрута (Record Route)

Маршрутизаторы **могут** поддерживать опцию Record Route в дейтаграммах, созданных ими.

(e) Опция Timestamp

Маршрутизаторы **могут** поддерживать опцию Timestamp в дейтаграммах, созданных ими. При этом должны выполняться перечисленные ниже правила.

- Когда созданная маршрутизатором дейтаграмма содержит опцию Timestamp, маршрутизатор **должен** записать в опцию значение временной метки, при соблюдении любого из указанных ниже условий:
  - поле адреса IP не задано заранее;
  - первый заданный адрес IP является адресом логического интерфейса[1], через который дейтаграмма будет передаваться.
- Если маршрутизатор получает адресованную непосредственно ему дейтаграмму с опцией Timestamp, он **должен** поместить в опцию значение текущего времени (если в поле опции имеется для этого пространство) до передачи опции на транспортный уровень или передачи сообщения ICMP на обработку. При отсутствии пространства в поле опции маршрутизатор **должен** увеличить значение Overflow Count[2] в опции.
- Значение временной метки должно соответствовать правилам, приведенным в [INTRO:2].

Реализация

Для обеспечения максимальной пользы от временных меток в опции timestamp, помещаемое в опцию значение должно быть как можно ближе к моменту реального приема пакета маршрутизатором. Для генерируемых маршрутизатором дейтаграмм включаемое в опцию значение должно как можно точнее совпадать со временем доставки дейтаграммы на канальный уровень для ее передачи.

Опция timestamp позволяет использовать нестандартное время, но при отсутствии синхронизации часов практическая польза от этой опции исчезает. Следовательно, в маршрутизаторах полезно реализовать поддержку протокола NTP[3] для синхронизации часов.

4.2.2.2 Адреса в опциях - RFC 791, параграф 3.1

Маршрутизаторы включают свой адрес в опции Record Route, Strict Source и Record Route, Loose Source и Record Route или Timestamp. Когда маршрутизатор помещает свой адрес в такую опцию, он **должен** использовать IP-адрес того логического интерфейса, через который будет передан пакет. Если это правило невозможно выполнить по причине отсутствия IP-адреса у выходного интерфейса (безадресный интерфейс), маршрутизатор **должен** указать взамен значение router-id (это значение совпадает с одним из IP-адресов маршрутизатора). Значения Router ID могут задаваться для устройства в целом или для отдельных каналов. Адрес, используемый в качестве значения router-id, **недопустимо** менять без участия администратора (даже при перезагрузке устройства). Примером ситуации со сменой идентификатора является такое изменение конфигурации, при котором адрес, заданный в качестве router-id, перестает использоваться в данном маршрутизаторе. Маршрутизаторы с множеством безадресных интерфейсов **могут** использовать множество значений router-id. Каждый безадресный интерфейс **должен** быть связан с отдельным значением router-id. Эта связь не должна изменяться (даже при перезагрузке) без смены конфигурационных параметров маршрутизатора.

Обсуждение

Данная спецификация не допускает существования маршрутизаторов, которые не имеют хотя бы одного адреса IP. Это ограничение не представляется серьезным, поскольку маршрутизатору нужен адрес IP в соответствии с требованиями к управлению, рассмотренными в главе 8, даже если маршрутизатор подключен только к каналам «точка-точка».

Реализация

Одним из способов выбора router-id, обеспечивающим соответствие требованиям спецификации, является использование наименьшего (или наибольшего) значения из присвоенных маршрутизатору адресов IP (при сравнении адреса трактуются как 32-битовые целые числа).

4.2.2.3 Неиспользуемые биты заголовка IP - RFC 791, параграф 3.1

Заголовок IP содержит два резервных бита - один бит в поле Type of Service[4], а второй в поле Flags[5]. Для маршрутизаторов **недопустимо** устанавливать в этих битах значение 1 для генерируемых самим маршрутизатором пакетов. **Недопустимо** также отбрасывание (отказ от приема или пересылки) пакетов на том лишь основании, что один или оба резервных бита имеют отличное от нуля значение, т. е. для маршрутизатора **недопустима** проверка значений этих битов.

Обсуждение

В будущих версиях протокола эти резервные биты могут использоваться. Приведенные здесь правила предназначены для того, чтобы новые варианты протокола могли быть применены без необходимости обновления всех маршрутизаторов в Internet.

4.2.2.4 Тип обслуживания (ToS) - RFC 791, параграф 3.1

Байт типа обслуживания в заголовке IP делится на три части: поле предпочтений (Precedence, 3 старших бита), поле типа обслуживания (Type of Service или TOS, следующие 4 бита) и резервное поле (младший бит).

Правила для резервного бита рассмотрены в параграфе 4.2.2.3.

Более глубокое рассмотрение поля TOS вы можете найти в документе [ROUTE:11].

Описание поля Precedence приведено в параграфе 5.3.3. Спецификация RFC 795 (Service Mapping) устарела и ее **не следует** использовать в реализации.

4.2.2.5 Контрольная сумма заголовка - RFC 791, параграф 3.1

Как сказано в параграфе 5.2.2, маршрутизатор **должен** проверять значения контрольной суммы в заголовках IP каждого принятого пакета и **должен** отбрасывать пакеты с некорректным значением контрольной суммы. Для реализаций **недопустимо** поддерживать возможность отключить проверку контрольных сумм.

---

[1] Или значением router-id, если дейтаграмма будет передаваться через безадресный интерфейс.
[2] Счетчик переполнений.
[3] Network Time Protocol – протокол сетевого времени.
[4] Тип обслуживания.
[5] Флаги.

Маршрутизатор **может** использовать инкрементальное обновление контрольной суммы заголовка IP в тех случаях, когда единственным изменением в пакете является уменьшение поля времени жизни в заголовке. Такой подход снижает вероятность незамеченного повреждения заголовка пакета маршрутизатором. Инкрементальное обновление контрольной суммы рассматривается в документе [INTERNET:6].

Реализация

Более детальное описание контрольных сумм заголовка IP, включая советы по реализации, содержится в документах [INTERNET:6] и [INTERNET:7].

4.2.2.6 Неопознанные опции заголовка - RFC 791, параграф 3.1

Маршрутизатор **должен пропу4скать** нераспознанные опции IP. Вследствие этого маршрутизатор **должен** поддерживать опции End of Option List и No Operation, поскольку эти опции не включают значения размера.

Обсуждение

Все новые опции IP будут явно включать размер.

4.2.2.7 Фрагментация - RFC 791, параграф 3.2

Маршрутизатор **должен** поддерживать фрагментацию пакетов в соответствии с документом [INTERNET:1].

При фрагментации дейтаграммы IP маршрутизатору **следует** минимизировать число создаваемых фрагментов, передавать фрагменты **следует** в соответствии с их порядком. Методы фрагментации, в которых один фрагмент может быть существенно меньше другого, **могут** приводить к тому, что первый фрагмент будет иметь наименьший размер.

Обсуждение

Существует несколько методов фрагментации, получивших распространение в Internet. Один из методов состоит в расщеплении дейтаграммы таким образом, чтобы размер первого фрагмента совпадал со значением MTU, а последующие фрагменты имели близкий к этому размер меньше MTU. Такой выбор размеров обусловлен двумя причинами. Для первого фрагмента выбирается эффективное значение MTU для текущего пути между хостами, а размер последующих фрагментов выбирается из соображений минимизации числа фрагментов дейтаграммы IP. Другой метод использует разбиение дейтаграммы IP на фрагменты размера MTU, а последний фрагмент содержит оставшуюся часть дейтаграммы [INTERNET:1].

В некоторых реализациях стека TCP/IP при прохождении через маршрутизатор дейтаграммы IP фрагментируются в пакеты, размер которых не превышает 576 байтов. Это делается для того, чтобы на оставшейся части пути полученные фрагменты не пришлось фрагментировать еще раз. Такой подход, однако, создает достаточно высокую нагрузку на принимающий хост, поскольку число фрагментов одной дейтаграммы может быть достаточно большим. Передача мелких пакетов снижает также эффективность работы сетей, где значение MTU изменяется только один раз и существенно превышает 576 байтов. Примерами могут служить сети IEEE 802.5 (MTU = 2048) или Ethernet (MTU = 1500).

В другом из обсуждаемых методов фрагментации дейтаграммы IP разбиваются на пакты приблизительно одного размера, который не превышает значение MTU для сети на следующем интервале пути. Такой подход используется для минимизации числа фрагментов при дополнительной фрагментации и обеспечения одинаковой задержки для каждого фрагмента.

Маршрутизаторам **следует** создавать как можно меньшее число фрагментов дейтаграмм IP.

Опыт работы с медленными машинами вселяет надежду, что при возникновении необходимости фрагментации передача сначала мелкого фрагмента увеличивает шансы того, что хост с медленным интерфейсом получит все фрагменты.

4.2.2.8 Сборка фрагментов - RFC 791, параграф 3.2

Как сказано в соответствующем параграфе документа [INTRO:2], маршрутизатор **должен** поддерживать сборку фрагментов дейтаграмм, адресованных самому маршрутизатору.

4.2.2.9 Время жизни - RFC 791, параграф 3.2

Обработка значений времени жизни (TTL) для созданных или принятых маршрутизатором пакетов определяется [INTRO:2], а в данном документе не задается никаких изменений. Однако, поскольку остальная часть раздела «Протокол IP» документа [INTRO:2] дублируется в данном документе, продублируем и этот параграф.

Отметим, в частности, что для маршрутизатора **недопустимо** проверять значение TTL в пакете за исключением тех случаев, когда маршрутизатор пересылает пакет.

Для маршрутизаторов **недопустима** генерация и пересылка пакетов с TTL = 0.

Для маршрутизаторов **недопустимо** отбрасывать дейтаграммы лишь потому, что они имеют значение TTL, равное 0 или 1, если пакет адресован данному маршрутизатору и все прочие параметры пакета корректны, маршрутизатор **должен** пытаться принять такой пакет.

Для генерируемых маршрутизатором сообщений уровень IP **должен** принимать во внимание, что транспортный уровень устанавливает значение TTL для каждой передаваемой дейтаграммы. При использовании фиксированного значения TTL, **должна** обеспечиваться возможность выбора этого значения. Время жизни **следует** делать больше типичного диаметра Internet и в настоящее время рекомендуется выбирать значение вдвое больше диаметра с учетом будущего расширения сети. Рекомендуемые значения времени жизни обычно помещаются в документ Assigned Numbers[1]. Поле TTL выполняет две функции - ограничивает время жизни сегментов TCP (см. RFC 793 [TCP:1], стр. 28) и предотвращает возникновение в Internet маршрутных петель. Хотя поле TTL определено, как время в секундах, этот параметр используется также в качестве счетчика интервалов, поскольку каждый маршрутизатор должен уменьшать значение этого поля по крайней мере на единицу.

Когда время жизни дейтаграммы истекло (TTL=0), маршрутизаторам (но не конечному получателю) следует отбрасывать дейтаграмму. Хосты, функционирующие как маршрутизаторы (пересылка пакетов между интерфейсами), должны следовать правилам обработки TTL, принятым для маршрутизаторов.

[1] В настоящее время значения Assigned Numbers доступны в базе данных на сайте www.iana.org. *Прим. перев.*

Протоколы вышележащих уровней могут пожелать установить свое значение TTL, чтобы расширить «зону доступности» для некоторых ресурсов Internet. Такой подход используется некоторыми средствами диагностики и предполагается, что он будет полезен для поиска «ближайшего» сервера данного класса с использованием групповой адресации IP. Тот или иной транспортный протокол может также пожелать установить свое граничное значение TTL для времени жизни дейтаграмм.

Используемое по умолчанию фиксированное значение TTL должно быть не меньше «диаметра» Internet (т. е., максимально длинного из возможных путей). Разумно выбирать значение, равное удвоенному диаметру, с учетом постоянного расширения Internet. На момент создания документа сообщения, пересекающие США, зачастую проходят через 15 - 20 маршрутизаторов, следовательно, значение TTL должно быть не менее 40; общепринятым является значение TTL = 64.

4.2.2.10 Широковещательная рассылка во множество подсетей (Multi-subnet Broadcast) - RFC 922

Использование рассылки широковещательных пакетов во все подсети (All-subnets broadcast или multi-subnet broadcast в [INTERNET:3]) запрещено. См. параграф 5.3.5.3.

4.2.2.11 Адресация - RFC 791, параграф 3.2

Как было отмечено в параграфе 2.2.5.1, существует 5 классов адресов IP - от A до E. Класс D служит для групповой адресации IP [INTERNET:4], а класс E зарезервирован для экспериментов. Различия между адресами классов A, B и C не столь важны - эти классы в настоящий момент представляют лишь исторический интерес.

Групповой адрес IP представляет собой 28-битовый логический адрес, который относится к группе хостов и может быть временным или постоянным. Постоянные групповые адреса распределяются агентством IANA[1] [INTRO:7], а временные адреса могут динамически выделяться для временных групп. Принадлежность к группам определяется динамически на основе протокола IGMP [INTERNET:4].

Рассмотрим некоторые важные частные случаи индивидуальных адресов IP общего назначения с использованием нотации:

`{ <Префикс сети>, <Номер хоста> }`

значение -1 будет использоваться для полей, содержащих только единицы, а 0 – для полей, содержащих только нули.

(a) { 0, 0 }

Данный хост в данной сети. Этот адрес **недопустимо** указывать в качестве адреса отправителя для маршрутизаторов за исключением случаев передачи адреса отправителя в процессе инициализации, посредством которого хост узнает свой IP-адрес (например, при использовании протокола BOOTP).

Входящие дейтаграммы со значением { 0, 0 } в поле отправителя, полученные для локальной доставки (см. параграф 5.2.3), **должны** приниматься маршрутизатором, если он поддерживает соответствующий протокол и способен явно определить действие, которое нужно выполнить. В остальных случаях маршрутизатор **должен** без уведомления отбрасывать дейтаграммы, содержащие в качестве адреса отправителя значение { 0, 0 }.

Обсуждение

В некоторых протоколах определяются конкретные действия в ответ на получение дейтаграмм с адресом отправителя { 0, 0 }. Примерами таких протоколов могут служить BOOTP и ICMP (Mask Request). Корректная работа таких протоколов зачастую зависит от возможности получения дейтаграмм с адресом отправителя { 0, 0 }. Однако для большинства других протоколов лучше будет игнорировать дейтаграммы с адресом отправителя { 0, 0 }, поскольку их источником может являться некорректно настроенный хост или маршрутизатор. Таким образом, если маршрутизатор знает, что делать с дейтаграммами, содержащими адрес отправителя { 0, 0 }, он **должен** принимать их, в противном случае маршрутизатор **должен** отбрасывать такие дейтаграммы.

См. также информацию о нестандартном использовании адреса { 0, 0 } в параграфе 4.2.3.1.

(b) { 0, <Номер хоста> }

Указывает хост данной сети. Для маршрутизаторов **недопустима** передача пакетов с таким адресом в поле отправителя, но такой адрес **может** использоваться маршрутизатором в процессе инициализации для определения маршрутизатором своего адреса IP.

(c) { -1, -1 }

Широковещательный адрес с ограниченной областью распространения[2]. **Недопустимо** использовать это значение в качестве адреса отправителя.

Дейтаграммы, содержащие этот адрес в поле получателя, будут получены каждым хостом и маршрутизатором, подключенным к физической сети, но не будут пересылаться за пределы этой сети.

(d) { <Префикс сети>, -1 }

Направленное широковещание[3] - широковещательные пакеты для указанного сетевого префикса. Такой адрес **недопустимо** использовать в качестве адреса получателя за исключением тех случаев, когда отправитель является одной из двух конечных точек соединения «точка-точка» с маской размером 31 бит. Маршрутизатор **может** генерировать пакеты Network Directed Broadcast. Маршрутизатор **может** иметь конфигурационную опцию, позволяющую ему принимать пакеты направленного широковещания, однако по умолчанию эта опция **должна** быть

---

[1] Internet Assigned Number Authority.

[2] Limited broadcast.

[3] Текст этого пункта изменен в соответствии с RFC 2644 и RFC 3021. Перевод исходного текста имел вид: «Направленный широковещательный адрес - пакеты с таким адресом в поле получателя предназначены для всех хостов сети с указанным префиксом. **Недопустимо** использовать такой адрес в поле отправителя. Маршрутизатор может генерировать пакеты Network Directed Broadcast. Маршрутизатор **должен** принимать пакеты Network Directed Broadcast, однако маршрутизатор **может** иметь конфигурационную опцию, предотвращающую восприятие таких пакетов. Данная опция по умолчанию **должна** разрешать прием пакетов Network Directed Broadcast.». *Прим. перев.*

отключена и, таким образом, маршрутизатору **недопустимо** принимать пакеты Network Directed Broadcast, пока это явно не задано в конфигурации.

(e) { 127, <любое значение> }

Внутренний loopback-адрес хоста. Адреса этого типа **недопустимо** использовать за пределами данного хоста.

(f)[1] **{ <Номер сети>, <Номер подсети>, 0 }**

Номер подсети. Такой адрес **не следует** использовать в качестве адреса отправителя за исключением тех случаев, когда отправитель является одной из двух конечных точек соединения «точка-точка» с маской размером 31 бит. Для других типов каналов пакеты с таким адресом в поле получателя **следует** отбрасывать без уведомления. Если такие пакеты не отбрасываются, они **должны** трактоваться, как широковещательные пакеты IP.

Значение <Префикс сети> задается административным путем так, чтобы этот префикс был уникальным в пределах домена маршрутизации, к которому подключено устройство.

Не допускается использование адресов IP со значениями 0 или -1 в полях <Номер хоста> и <Префикс сети> за исключением перечисленных выше специальных случаев. Это требование неявно указывает, что каждое из полей должно иметь размер не менее 2 битов.

Обсуждение

В предыдущей версии данного документа было указано, что номера подсетей не должны иметь значение 0 или -1 и размер этого поля должен быть не менее 2 битов. В среде CIDR номер подсети является расширением префикса сети и не может интерпретироваться без остальной части префикса. Следовательно, приведенное выше ограничение не имеет смысла при использовании CIDR и может игнорироваться без всякого риска.

Дополнительное обсуждение широковещательных адресов приведено в параграфе 4.2.3.1.

Когда маршрутизатор порождает любую дейтаграмму, она **должна** содержать в поле отправителя один из IP-адресов маршрутизатора (не групповой и не широковещательный). Единственным исключением являются дейтаграммы, которые могут использоваться в процессе инициализации.

В большинстве случаев дейтаграммы, направленные по групповым или широковещательным адресам, должны обрабатываться так, будто они направлены по одному из IP-адресов маршрутизатора:

- маршрутизатор **должен** нормально принимать и обрабатывать любые пакеты с широковещательным адресом получателя;
- маршрутизатор **должен** нормально принимать и обрабатывать любые пакеты, переданные по групповому адресу, для которого у маршрутизатора запрошен прием.

Термин «адрес конкретного получателя[2]» означает локальный IP-адрес хоста. В заголовке IP в качестве адреса получателя должен указываться адрес конкретного хоста, если пакет не является широковещательным или групповым (в таких случаях адресом конкретного получателя является IP-адрес физического интерфейса, через который принимается дейтаграмма).

Маршрутизатор **должен** без уведомления отбрасывать все дейтаграммы, содержащие в поле отправителя адрес IP, не соответствующий приведенным в этом разделе правилам. Проверка корректности адреса отправителя осуществляется на уровне IP или (когда это возможно) каждым протоколом транспортного уровня. Маршрутизатору **следует** учитывать отбрасываемые дейтаграммы.

Обсуждение

Некорректный адрес отправителя в дейтаграммах может быть связан с широковещательной передачей на канальном уровне дейтаграмм, адресованных конкретному хосту или некорректными настройками других хостов или маршрутизаторов.

4.2.3 Специальные вопросы

4.2.3.1 Широковещательные адреса IP

В силу исторических причин существует ряд адресов IP (как стандартных, так и нестандартных), которые используются для индикации широковещательных пакетов IP.

(1) [3]**Должны** трактоваться, как широковещательные пакеты IP, все пакеты, направленные по адресу 255.255.255.255 или { <Префикс сети>, -1 }.

На каналах «точка-точка» с маской размером 31 бит, пакеты, направленные по адресу { <Префикс сети>, -1 }, соответствующему одной из конечных точек этого канала, **должны** трактоваться, как направленные маршрутизатору, на котором установлен этот адрес.

(2) [4]**Следует** отбрасывать без уведомления (т. е., без доставки даже работающим на маршрутизаторе приложениям) все пакеты, направленные по адресу 0.0.0.0 или { <Префикс сети>, 0 }. Если такие пакеты не отбрасываются, они **должны** трактоваться, как широковещательные пакеты IP (см. параграф 5.3.5). **Может** использоваться конфигурационная опция, позволяющая принимать такие пакеты. По умолчанию **следует** устанавливать для этой опции отбрасывание пакетов.

---

[1]Этот пункт добавлен в соответствии с изменениями, внесенными RFC 3021. *Прим. перев.*

[2]Specific-destination address.

[3]Текст этого пункта изменен в соответствии с RFC 3021. Перевод исходного текста имел вид: «Маршрутизатор **должен** трактовать, как широковещательные, пакеты IP, направленные по адресу 255.255.255.255 или { <Префикс сети>, -1 }.». *Прим. перев.*

[4]Текст этого пункта изменен в соответствии с RFC 3021. Перевод исходного текста имел вид: «Маршрутизатору **следует** отбрасывать без уведомления непосредственно при получении (т. е., без попыток доставки тому или иному приложению на маршрутизаторе) все пакеты, направленные по адресу 0.0.0.0 или {<Префикс сети>, 0 }. Если такие пакеты не отбрасываются маршрутизатором без уведомления, он **должен** трактовать их, как широковещательные пакеты (см. параграф 5.3.5). В маршрутизаторах **может** использоваться конфигурационный параметр, разрешающий принимать такие пакеты. По умолчанию этот параметр **следует** устанавливать на отбрасывание пакетов без уведомления.». *Прим. перев.*

На каналах «точка-точка» с маской размером 31 бит, пакеты, направленные по адресу { <Префикс сети>, 0 }, соответствующему одной из конечных точек этого канала, **должны** трактоваться, как направленные маршрутизатору, на котором установлен этот адрес.

(3) Маршрутизатору **следует** (по умолчанию) использовать адрес ограниченного широковещания 255.255.255.255 для широковещательных дейтаграмм IP, адресованных в подключенные (под)сети, за исключением случаев передачи откликов ICMP Address Mask Reply, как показано в параграфе 4.3.3.9. Маршрутизатор **должен** принимать широковещательные пакеты с ограниченной областью распространения.

(4) [1]**Не следует** генерировать дейтаграммы, направленные по адресу 0.0.0.0 или {<Префикс сети>, 0 }. **Может** использоваться конфигурационная опция, позволяющая генерировать такие пакеты (вместо использования подходящего формата широковещания). По умолчанию для опции **следует** использовать значение, не позволяющее генерировать такие пакеты.

На каналах «точка-точка» с маской размером 31 бит в конфигурации **следует** разрешать генерацию дейтаграмм, направленных по адресу { <Префикс сети>, 0 }.

Обсуждение

Для случая (2) маршрутизатор обычно не может распознавать адреса в формате { <Префикс сети>, 0 }, если у него нет интерфейса с таким сетевым префиксом. В таких случаях правила п. (2) теряют силу, поскольку с точки зрения маршрутизатора дейтаграмма не является широковещательным пакетом IP.

4.2.3.2 Групповая адресация IP

Маршрутизаторам **следует** выполнять требования документа Host Requirements [INTRO:2] по части групповой адресации IP. Маршрутизаторам IP **следует** поддерживать локальную групповую адресацию IP для всех подключенных сетей. При наличии спецификации отображения групповых адресов IP на адреса канального уровня (см. спецификации передачи IP-over-xxx) **следует** использовать эту спецификацию, но **можно** также с помощью конфигурационного параметра задавать использование взамен такого отображения широковещательной рассылки на канальном уровне. На каналах «точка-точка» и всех прочих интерфейсах пакеты с групповой адресацией инкапсулируются в широковещательные кадры канального уровня. Поддержка групповой адресации IP включает генерацию групповых дейтаграмм, присоединение к группам, получение multicast-дейтаграмм и выход из групп. Это подразумевает выполнение всех требований [INTERNET:4], включая поддержку IGMP (см. параграф 4.4).

Обсуждение

Хотя документ [INTERNET:4] называется Host Extensions for IP Multicasting (расширение программ хостов для поддержки групповой адресации IP), он применим ко всем системам IP (как хостам, так и маршрутизаторам). В частности, поскольку маршрутизаторы могут входить в multicast-группы, будет корректно выполнение связанной с хостами части IGMP и информирование о своей принадлежности к группе всех multicast-маршрутизаторов, которые могут присутствовать в подключенных сетях (независимо от того, поддерживает ли сам входящий в группу маршрутизатор multicast-маршрутизацию).

Некоторые протоколы маршрутизации могут явно требовать поддержки групповой адресации IP (например, OSPF [ROUTE:1]) или такая поддержка рекомендуется (например, ICMP Router Discovery [INTERNET:13]).

4.2.3.3 Определение MTU для пути

Для предотвращения фрагментации или минимизации ее влияния желательно знать значения MTU на пути от отправителя к получателю. Значением MTU для пути (path MTU) считается минимальное среди значений MTU на всех интервалах этого пути. В документе [INTERNET:14] описан метод динамического определения максимального размера передаваемых блоков (MTU) для произвольного пути в Internet. Для путей, проходящих через маршрутизаторы, которые не поддерживают [INTERNET:14], этот метод не позволяет корректно определить значение Path MTU, но он всегда выбирает Path MTU с максимально возможной точностью и во многих случаях точность определения Path MTU превышает точность при использовании старых методов или принятой сегодня практики.

Когда маршрутизатор создает дейтаграмму IP, ему **следует** использовать описанную в [INTERNET:14] схему для ограничения размера дейтаграммы. Если маршрут к получателю дейтаграммы был получен от протокола маршрутизации, обеспечивающего информацию о значении Path MTU, можно продолжать использование схемы [INTERNET:14], но **следует** использовать значение Path MTU, полученное от протокола маршрутизации, как стартовое приближение для Path MTU и верхнюю границу значения Path MTU.

4.2.3.4 Подсети

В некоторых ситуациях может оказаться желательным соединение подсетей той или иной сети с использованием путей, которые не являются частью разделенной на подсети сети. Такой случай называют «поддержкой подсетей, не являющихся непрерывными».

Маршрутизаторы **должны** поддерживать подсети, которые не являются непрерывными.

Реализация

В классических сетях IP описанная ситуация является экзотической, а при использовании CIDR встречается сплошь и рядом. Следовательно, для маршрутизатора **недопустимо** делать какие-либо предположения об архитектуре подсетей и **следует** трактовать каждый маршрут как обобщенный префикс сети.

Обсуждение

Internet расширяется с возрастающей скоростью и это приводит к некоторым сложностям в адресации IP. Основным фактором являются жесткие границы классов адресов IP. Это снижает эффективность распределения адресов и осложняет агрегирование нескольких префиксов сетей в один маршрутный анонс. Отказ от классов адресов IP и связанных с ними жестких границ позволяет трактовать каждый маршрут как обобщенный префикс сети.

[1]Текст этого пункта изменен в соответствии с RFC 3021. Перевод исходного текста имел вид: «Для маршрутизатора **недопустимо** порождать пакеты, адресованные в 0.0.0.0 или { <Префикс сети>, 0 }. Маршрутизатор **может** поддерживать конфигурационный параметр, позволяющий генерировать такие пакеты взамен широковещательных пакетов соответствующего формата, но по умолчанию **следует** устанавливать значение этого параметра для запрета такой генерации.». *Прим. перев.*

Технология, используемая для решения проблемы с жесткими границами классов адресов, получила название «бесклассовая междоменная маршрутизация» (CIDR) [INTERNET:15].

Адресный блок, связанный с тем или иным сетевым префиксом, может быть поделен на субблоки различных размеров и префиксы, связанные с этими субблоками, будут иметь разную длину. Например, внутри блока с 8-битовым сетевым префиксом один субблок может иметь префикс размером 16 битов, другой - 18, третий - 14 и т. д.

Маршрутизаторы **должны** поддерживать префиксы переменной длины как для своих интерфейсов, так и для таблиц маршрутизации.

4.3 Протокол ICMP

4.3.1 Введение

ICMP представляет собой вспомогательный протокол, обеспечивающий возможности диагностики и передачу сообщений об ошибках в сетях IP. Протокол описан в документе [INTERNET:8]. Маршрутизаторы **должны** поддерживать протокол ICMP.

Сообщения ICMP делятся на 2 класса.

Сообщения ICMP об ошибках.

Destination Unreachable - адресат недоступен (см. параграф 4.3.3.1).

Redirect - перенаправление (см. параграф 4.3.3.2).

Source Quench - «заткнуть рот» отправителю (см. параграф 4.3.3.3).

Time Exceeded - время жизни истекло (см. параграф 4.3.3.4).

Parameter Problem - проблема с параметрами (см. параграф 4.3.3.5).

Запросы ICMP.

Echo - эхо (см. параграф 4.3.3.6).

Information - информация (см. параграф 4.3.3.7).

Timestamp - временная метка (см. параграф 4.3.3.8).

Address Mask - маска адреса (см. параграф 4.3.3.9).

Router Discovery - обнаружение маршрутизаторов (см. параграф 4.3.3.10).

Общие требования к ICMP рассматриваются в следующем параграфе.

4.3.2 Общие вопросы

4.3.2.1 Неизвестные типы сообщений

При получении сообщения ICMP неизвестного типа, оно **должно** передаваться пользовательскому интерфейсу ICMP (если маршрутизатор поддерживает его) или отбрасываться без уведомления (если маршрутизатор не поддерживает пользовательский интерфейс ICMP).

4.3.2.2 TTL для сообщений ICMP

При генерации сообщения ICMP маршрутизатор **должен** инициализировать значение TTL. Значения TTL для откликов ICMP недопустимо брать из породивших эти отклики пакетов.

4.3.2.3 Заголовок исходного сообщения

Исторически каждое сообщение ICMP об ошибке включает заголовок IP и первые 8 байтов данных из дейтаграммы, вызвавшей ошибку. В настоящее время такой подход утратил актуальность по причине использования туннелей IP-in-IP и других технологий. Следовательно, в дейтаграммы ICMP **следует** включать как можно больше данных из исходного пакета без превышения дейтаграммой ICMP размера 576 байтов. Возвращаемый заголовок IP (и данные из пакета) **должен** быть идентичен полученной информации за исключением того, что маршрутизатор не обязан восстанавливать данные из заголовка IP, которые были изменены в процессе пересылки дейтаграммы до возникновения ошибки (например, уменьшение TTL или смена опций). Отметим, что требования параграфа 4.3.3.5 в некоторых могут отменять приведенные здесь правила (например, для сообщений Parameter Problem маршрутизатор должен восстановить значение поля, с которым связана проблема).

4.3.2.4 Адрес отправителя сообщения ICMP

Если в данном документе явно не указано иное, IP-адрес отправителя в сообщениях ICMP, создаваемых маршрутизатором, **должен** быть одним из адресов IP, связанных с физическим интерфейсом, через который будет передаваться сообщение ICMP. Если интерфейс не имеет адреса IP, следует использовать взамен значение router-id (см. параграф 5.2.5).

4.3.2.5 Поля TOS и Precedence

В сообщениях ICMP об ошибках **следует** устанавливать такое же значение поля TOS, какое было в вызвавшем передачу этого сообщения пакете, если установка такого значения не приведет к незамедлительному отбрасыванию сообщения ICMP по причине отсутствия маршрута к получателю. В случае невозможности копирования TOS из исходного пакета сообщение ICMP **должно** передаваться с нормальным (нулевым) полем TOS. В откликах ICMP **следует** устанавливать в поле TOS значение одноименного поля из соответствующего запроса ICMP.

Сообщения ICMP Source Quench, если они передаются, **должны** иметь в поле IP Precedence такое же значение, как в одноименном поле вызвавшего передачу Source Quench пакета. Прочие сообщения ICMP об ошибках (Destination Unreachable, Redirect, Time Exceeded, Parameter Problem) **следует** передавать со значением 6 (INTERNETWORK CONTROL) или 7 (NETWORK CONTROL) в поле Precedence. Значение IP Precedence для таких сообщений **можно** делать настраиваемым (опция).

В откликах ICMP **должно** использоваться значение поля IP Precedence из заголовка соответствующего запроса ICMP.

4.3.2.6 Source Route

Если пакет, вызвавший передачу сообщения ICMP об ошибке, содержал опцию source route, в сообщение ICMP также **следует** включать опцию source route такого же типа (strict - строгий или loose - мягкий), создаваемую путем обращения части записанного в опции маршрута до указателя. Исключением являются случаи передачи сообщений ICMP Parameter Problem, связанных с опцией source route в исходном пакете, или ситуации, когда маршрутизатор знает, что выбранная политика не позволит доставить такое сообщение ICMP.

Обсуждение

В средах, использующих опцию безопасности U.S. Department of Defense[1] (см. [INTERNET:5]), может потребоваться включение этой опции в сообщения ICMP. Информацию об использовании этой опции можно получить в Defense Communications Agency.

4.3.2.7 Когда не следует передавать сообщения ICMP об ошибках

Передача сообщений ICMP об ошибках **недопустима** в ответ на:

- сообщение ICMP об ошибке;
- пакеты с ошибками в заголовке IP (см. описание проверок в параграфе 5.2.2), за исключением явно указанных в параграфе 5.2.2 случаев необходимости генерации сообщения ICMP;
- пакеты, направленные по широковещательным и групповым адресам;
- пакеты, переданные в групповых или широковещательных кадрах канального уровня;
- пакеты, в которых поле отправителя содержит нулевой префикс сети или некорректный адрес (см. параграф 5.3.7);
- любые фрагменты дейтаграмм роме первого (т. е., пакеты с отличным от нуля значением смещения в заголовке IP).

Кроме того, сообщения ICMP об ошибках **недопустимо** передавать во всех случаях, для которых в данном документе указана необходимость отбрасывания таких пакетов без уведомления.

Примечание. Эти ограничения имеют превосходство над любыми требованиями, указанными в других документах для передачи сообщений ICMP об ошибках.

Обсуждение

Эти правила предназначены для предотвращения широковещательных штормов, когда маршрутизаторы или хосты начинают передавать сообщения ICMP об ошибках в ответ на широковещательные пакеты. Например, широковещательный пакет, адресованный в несуществующий порт UDP, может вызвать лавину дейтаграмм ICMP Destination Unreachable от всех устройств, которые не поддерживают указанный в пакете порт. В больших сетях Ethernet такие события могут выводить сеть из строя на секунды или более продолжительное время.

Каждый пакет, который является широковещательным в подключенной сети, должен иметь корректный широковещательный адрес IP в поле получателя (см. параграф 5.3.4 и документ [INTRO:2]). Однако некоторые устройства нарушают это правило. Следовательно, для обнаружения широковещательных пакетов маршрутизаторы должны проверять наличие широковещательного адреса канального уровня и адрес IP.

Реализация+

Для реализации этих правил требуется, чтобы канальный уровень информировал уровень IP при получении широковещательного пакета канального уровня (см. параграф 3.1).

4.3.2.8 Ограничение скорости

Маршрутизатор, который передает сообщения ICMP Source Quench, **должен** быть способен ограничивать скорость генерации сообщений. Маршрутизатору также **следует** обеспечивать возможность ограничения скорости генерации других типов сообщений ICMP об ошибках (Destination Unreachable, Redirect, Time Exceeded, Parameter Problem). Параметры ограничения скорости **следует** делать настраиваемыми в конфигурации маршрутизатора. Применение ограничений скорости генерации сообщений ICMP (например, для маршрутизатора в целом или независимо для каждого интерфейса) определяется разработчиками.

Обсуждение

Для маршрутизаторов, передающих сообщения ICMP об ошибках, возникают две проблемы: (1) расход полосы в исходящем направлении и (2) загрузка ресурсов маршрутизатора (например, память, время процессора).

Для снижения остроты этих проблем маршрутизаторам следует ограничивать скорость генерации сообщений ICMP об ошибках. По тем же причинам маршрутизаторам следует ограничивать частоту генерации и для некоторых других сообщений ICMP (например, Echo Reply).

Реализация

Для ограничения скорости генерации сообщений ICMP об ошибках существует несколько методов.

(1) Ограничение на основе счетчиков - например, передача сообщения ICMP об ошибке на каждые N отброшенных пакетов (в целом или для отдельного хоста-отправителя). Этот механизм удобен для сообщений ICMP Source Quench, но не подходит для других сообщений ICMP.

(2) Ограничение по таймеру - например, передача сообщения ICMP об ошибке в данный адрес или по всем адресам не более 1 раза в течение T миллисекунд.

(3) Ограничение по полосе - например, скорость, с которой сообщения ICMP передаются через тот или иной интерфейс, не должна составлять более заданной части пропускной способности канала.

4.3.3 Специфические вопросы

4.3.3.1 Destination Unreachable

[1] Министерства обороны США.

Если маршрутизатор не может переслать пакет адресату потому, что не знает маршрута (в том числе, принятого по умолчанию), он **должен** направить отправителю пакета сообщение ICMP Destination Unreachable с кодом 0 (Network Unreachable - сеть недоступна). Если маршрутизатор знает путь к адресату пакета, но значение TOS для этого маршрута отличается от принятого по умолчанию TOS (0000) и значения TOS в заголовке пакета, маршрутизатор **должен** направить отправителю пакета сообщение ICMP Destination Unreachable с кодом 11 (Network Unreachable for TOS - сеть недоступна для заданного TOS).

Если пакет должен пересылаться хосту непосредственно подключенной к маршрутизатору сети (т. е. данный маршрутизатор является последним на пути) и маршрутизатор знает об отсутствии других путей к этому хосту, он **должен** генерировать сообщение Destination Unreachable с кодом 1 (Host Unreachable - хост недоступен). Если пакет пересылается хосту подключенной к маршрутизатору сети и маршрутизатор не может переслать этот пакет по той причине, что значение TOS для подключенной сети отличается от принятого по умолчанию (0000) и заданного в заголовке пакета, маршрутизатор **должен** передать отправителю пакета сообщение Destination Unreachable с кодом 12 (Host Unreachable for TOS - хост недоступен для заданного TOS).

Обсуждение

Смысл состоит в том, что маршрутизатор генерирует сообщение о недоступности хоста или сети, если он совсем не знает пути к нему (включая принятый по умолчанию маршрут). Если маршрутизатор знает один или несколько путей к адресату, но они не могут использоваться в соответствии с требованиями TOS, маршрутизатор генерирует сообщение о недоступности для заданного значения TOS.

4.3.3.2 Redirect

Сообщения ICMP Redirect генерируются для информирования локального хоста о том, что ему следует использовать другой маршрутизатор на следующем этапе пересылки для того или иного трафика.

В противоположность требованиям документа [INTRO:2], маршрутизатор **может** игнорировать сообщения ICMP Redirect при выборе пути для созданных им пакетов, если данный маршрутизатор использует протокол маршрутизации или пересылка пакетов разрешена для маршрутизатора и интерфейса в ту сеть, куда передается пакет.

4.3.3.3 Source Quench

Маршрутизаторам **не следует** генерировать сообщения ICMP Source Quench. Как сказано в параграфе 4.3.2, маршрутизатор, который генерирует сообщения Source Quench, **должен** быть способен ограничивать скорость их генерации.

Обсуждение

Исследования показывают, что сообщения Source Quench увеличивают расход полосы, но не обеспечивают эффективного и корректного способа решения проблемы перегрузок (см., например, [INTERNET:9] и [INTERNET:10]). В параграфе 5.3.6 рассмотрены современные методы решения проблем перегрузки и насыщения каналов.

Маршрутизатор **может** игнорировать получаемые сообщения ICMP Source Quench.

Обсуждение

Маршрутизатор может получать адресованные ему сообщения Source Quench от других маршрутизаторов или хостов при передаче им пакетов от данного маршрутизатора. К таким пакетам могут относиться, например, обновления EGP или адресованные хостам пакеты telnet. В документах [INTERNET:11] и [INTERNET:12] предлагается механизм реагирования уровня IP на сообщения Source Quench путем управления скоростью передачи пакетов, однако этот механизм пока является экспериментальным и не может быть рекомендован.

4.3.3.4 Time Exceeded

Когда при пересылке пакетов маршрутизатором значение TTL становится равным 0, применимы рекомендации параграфа 5.2.3.8.

При сборке адресованных ему пакетов маршрутизатор действует как обычный хост Internet. Следовательно, он должен соответствовать требованиям [INTRO:2] в части сборки фрагментов.

Когда маршрутизатор получает адресованные ему сообщения Time Exceeded, он **должен** выполнять требования [INTRO:2].

4.3.3.5 Parameter Problem

Маршрутизатор **должен** генерировать сообщение Parameter Problem для любых ошибок, с которыми не связаны специальные сообщения ICMP об ошибках. Заголовок IP или поле опции IP, включая байт, на который ссылается указатель, **должны** быть скопированы в заголовок IP, возвращаемый в сообщении ICMP. Исключения из этого правила приведены в параграфе 4.3.2.

В документе [INTRO:2] определен новый вариант сообщений Parameter Problem

Code 1 = required option is missing (требуемая опция отсутствует).

Обсуждение

Этот вариант в настоящее время используется в военных системах при отсутствии в пакетах опции безопасности.

4.3.3.6 Echo Request/Reply

Маршрутизатор **должен** поддерживать сервер ICMP Echo, который принимает адресованные маршрутизатору запросы Echo и передает в ответ соответствующие отклики. Маршрутизатор **должен** быть готов к приему и сборке, а также передаче откликов на дейтаграммы ICMP Echo Request размером не менее 576 байтов и значений MTU подключенных сетей.

Сервер Echo **может** игнорировать запросы ICMP Echo, переданные по групповым и широковещательным адресам IP.

Маршрутизаторам **следует** поддерживать конфигурационную опцию, которая, будучи включенной, обеспечит игнорирование всех запросов ICMP Echo, при наличии этой опции по умолчанию **должны** быть включены отклики на эхо-запросы.

Обсуждение

Нейтральное отношение к групповым и широковещательным пакетам Echo Request соответствует [INTRO:2] (параграф Echo Request/Reply).

Как сказано в параграфе 10.3.3, маршрутизатор **должен** также поддерживать интерфейс с прикладным уровнем для передачи пакетов Echo Request и приема Echo Reply в целях диагностики. Все сообщения ICMP Echo Reply **должны** передаваться этому интерфейсу.

IP-адрес отправителя в сообщениях ICMP Echo Reply **должен** совпадать с конкретным адресом получателя в соответствующем сообщении ICMP Echo Request.

Данные, полученные в сообщении ICMP Echo Request, **должны** полностью включаться в отклик Echo Reply.

Если в полученном сообщении ICMP Echo Request имеется опция Record Route и/или Timestamp, эту опцию (опции) **следует** обновить с включением текущего маршрутизатора в заголовок IP сообщения Echo Reply, не отсекая опцию по размеру. Таким образом записанный маршрут будет включать весь путь кругового обхода.

Если в полученном сообщении ICMP Echo Request присутствует опция Source Route, маршрут возврата для сообщения Echo Reply **должен** быть обращением пути, указанного опцией Source Route, если у маршрутизатора нет уверенности, что принятая политика не позволит доставить сообщение по этому маршруту.

4.3.3.7 Information Request/Reply

Для маршрутизатора **недопустима** генерация сообщений такого типа и отклики на них.

Обсуждение

Пара сообщений Information Request/Reply предназначена для поддержки самонастраиваемых систем (типа бездисковых станций) и позволяет определить префикс IP в процессе загрузки. Однако, в настоящее время такой подход устарел. Более эффективные механизмы получения параметров и определения своего адреса IP обеспечивают протоколы RARP и BOOTP.

4.3.3.8 Timestamp и Timestamp Reply

Маршрутизатор **может** поддерживать сообщения Timestamp и Timestamp Reply. Если такая поддержка реализована в маршрутизаторе выполняются перечисленные ниже действия.

- Сервер ICMP Timestamp **должен** возвращать сообщение Timestamp Reply в ответ на каждое полученное сообщение Timestamp. Серверу **следует** обеспечивать минимальные вариации задержки передачи откликов на запросы.
- Запросы ICMP Timestamp, направленные по широковещательным и групповым адресам IP, могут отбрасываться без уведомления.
- IP-адрес отправителя в сообщении ICMP Timestamp Reply **должен** совпадать с адресом получателя, указанным в соответствующем сообщении Timestamp.
- При получении опции Source Route в сообщении ICMP Timestamp Request, маршрут возврата для сообщения Timestamp Reply **должен** быть инверсией пути, записанного в Source Route, если у маршрутизатора нет уверенности, что принятая политика не позволит доставить сообщение по такому маршруту.
- Если в сообщении Timestamp Request присутствует опция Record Route и/или Timestamp, эта опция (опции) должна быть обновлена с включением текущего маршрутизатора и помещена в заголовок сообщения Timestamp Reply.
- Если маршрутизатор обеспечивает для прикладного уровня интерфейс передачи сообщений Timestamp Request, входящие сообщения Timestamp Reply **должны** передавать пользовательскому интерфейсу ICMP.

Предпочтительный вариант значений timestamp (стандартное время) - выраженное в миллисекундах универсальное время (Universal Time). Однако при указании времени с разрешением 1 мсек могут возникать сложности. Например, многие системы используют внутренние часы, синхронизируемые от электросети (50 или 60 Герц). Следовательно, значения стандартного времени допускают некоторый произвол.

(a) стандартное время **должно** обновляться не менее 16 раз в секунду (т. е., не менее шести младших битов могут содержать неопределенные значения);

(b) точность стандартного времени **должна** приблизительно соответствовать тактовой частоте процессора.

Реализация

Для выполнения второго условия маршрутизатору может потребоваться корректировка часов с использованием сервера точного времени при загрузке или перезапуске маршрутизатора. Для корректировки часов рекомендуется использовать протокол Time Server на основе UDP. Более эффективным решением является синхронизация часов по протоколу NTP (Network Time Protocol), который обеспечивает точность порядка 1 мсек, однако такая синхронизация не является обязательной.

4.3.3.9 Address Mask Request/Reply

Маршрутизаторы **должны** поддерживать прием запросов ICMP Address Mask Request и генерацию соответствующих откликов ICMP Address Mask Reply. Эти сообщения определены в [INTERNET:2].

Маршрутизаторам **следует** поддерживать для каждого логического интерфейса конфигурационную опцию, определяющую допустимость генерации откликов Address Mask Request для этого интерфейса, по умолчанию такая опция **должна** разрешать генерацию откликов. Для маршрутизаторов **недопустима** передача откликов на сообщения Address Mask Request, если не известна корректная маска.

Для маршрутизаторов **недопустимо** отвечать на запросы Address Mask Request, переданные с адреса 0.0.0.0 и поступившие на физический интерфейс, с которым связано множество логических интерфейсов, если маски для логических интерфейсов различаются.

Маршрутизаторам **следует** проверять полученные сообщения ICMP Address Mask Reply на предмет соответствия указанной в них маски имеющимся у маршрутизатора сведениям о маске. Если сообщение ICMP Address Mask Reply представляется ошибочным, маршрутизатору **следует** записать в системный журнал полученное в сообщении значение маски и IP-адрес отправителя. Для маршрутизаторов **недопустимо** использование сообщений ICMP Address Mask Reply для определения корректной маски.

Поскольку хосты могут оказаться не способными определить маску, если в момент загрузки хоста маршрутизатор был недоступен, маршрутизатор **может** по своей инициативе передать широковещательное сообщение ICMP Address Mask Reply для каждого из своих логических интерфейсов после настройки соответствующей маски. Однако такое поведение может представлять опасность в средах с масками переменной длины. Следовательно, при реализации этой функции широковещательная передача незапрошенных сообщений Address Mask Reply недопустима для логических интерфейсов, которые:

- не настроены на передачу незапрошенных сообщений Address Mask Reply (каждый логический интерфейс **должен** иметь конфигурационный параметр, определяющий возможность передачи таких сообщений и по умолчанию этот параметр **должен** запрещать широковещательную передачу сообщений Address Mask Reply без запроса);

- разделяют однотипные (но не идентичные) сетевые префиксы и физический интерфейс.

Для широковещательной передачи сообщений Address Mask Reply **должна** использоваться адресация в формате { <Префикс сети>, -1 } .

Широковещательный адрес 255.255.255.255 **должен** использоваться для широковещательных откликов Address Mask Reply на каналах «точка-точка» с маской подсети размером 31 бит[1].

Обсуждение

Возможность запрета передачи откликов Address Mask Reply маршрутизаторами требуется на некоторых сайтах, которые умышленно передают своим хостам некорректные маски адресов. Предполагается, что эта необходимость отпадет по мере того, как хосты станут соответствовать требованиям стандарта Host Requirements.

Второе требование (см. выше) и необходимость использования указанного формата адресации служат для предотвращении проблем, возникающих при использовании множества префиксов IP в одной физической сети.

4.3.3.10 Анонсирование маршрутизаторов

IP-маршрутизатор **должен** поддерживать связанную с маршрутизаторами часть протокола ICMP Router Discovery [INTERNET:13] на всех подключенных сетях, для которых маршрутизатор поддерживает групповую или широковещательную адресацию IP. Реализация **должна** включать все конфигурационные переменные, указанные для маршрутизаторов, с заданными значениями по умолчанию.

Обсуждение

Маршрутизаторы не обязаны поддерживать связанную с хостами часть протокола ICMP Router Discovery Protocol, но такая поддержка может оказаться полезной при работе в режиме отключенной пересылки пакетов (маршрутизации).

Обсуждение

Отметим, что для хостов характерно использование RIP версии 1 в качестве протокола обнаружения маршрутизаторов. Такие хосты прослушивают трафик RIP и используют извлеченную из него информацию для выбора маршрутизатора первого интервала для того или иного адресата. Хотя такое поведение хостов не является нормальным, разработчики по-прежнему достаточно часто используют его.

4.4 Протокол управления группами INTERNET - IGMP

IGMP [INTERNET:4] представляет собой протокол, используемый для обмена информацией между хостами и multicast-маршрутизаторами одной физической сети для управления принадлежностью к multicast-группам. Multicast-маршрутизаторы используют протокол групповой маршрутизации для поддержки групповой пересылки IP через Internet.

Маршрутизаторам **следует** реализовать связанную с хостами часть протокола IGMP.

5. Уровень INTERNET - пересылка

5.1 Введение

В этом разделе рассматривается процесс пересылки пакетов в маршрутизаторах.

5.2 Функция пересылки пакетов

Для функции пересылки пакетов IP не существует отдельной спецификации. Процесс пересылки описан в спецификациях протокола IP ([INTERNET:1], [INTERNET:2], [INTERNET:3], [INTERNET:8], [ROUTE:11]).

5.2.1 Алгоритм пересылки

Поскольку ни в одной из первичных спецификаций протокола нет детального описания алгоритма пересылки пакетов, такое описание представлено здесь. В этом параграфе дается общее описание алгоритма, а отдельные детали (такие, как способы предотвращения перегрузок) рассматриваются ниже.

От реализаций не требуется точного следования алгоритмам, описанным в параграфах 5.2.1.1, 5.2.1.2 и 5.2.1.3. Многие разработчики программ в целях повышения производительности пересылки пакетов используют иные решения, которые в конечном итоге дают такой же результат, как описанный здесь алгоритм. Детали реализации алгоритма пересылки не рассматриваются в этом документе (в частности по той причине, что они могут сильно зависеть от архитектуры маршрутизатора). Вместо этого ниже приводятся общие требования к выполняемым при пересылке операциям с учетом их порядка.

[1] Это предложение добавлено в соответствии с RFC 3021. *Прим. перев.*

(1) Маршрутизатор **должен** проверять заголовок IP, как описано в параграфе 5.2.2, до выполнения любых операций, основанных на содержащейся в заголовке информации. Это позволяет маршрутизатору обнаружить и отбросить ошибочные пакеты до того, как будут затрачены ресурсы на их обработку.

(2) Обработка некоторых опций IP требует от маршрутизатора включения своего адреса IP в эту опцию. Как указано в параграфе 5.2.4, в опцию **должен** включаться адрес логического интерфейса, через который пакет передается, или значение router-id, если пакет передается через интерфейс, не имеющий адреса. Таким образом, обработка подобных опций не может быть завершена до принятия решения о выборе интерфейса для передачи пакета.

(3) Маршрутизатор не может проверять и уменьшать значение TTL до того, как он убедится, что пакет не адресован самому маршрутизатору (причины этого указаны в параграфе 4.2.2.9).

(4) Когда пакет адресован данному маршрутизатору, заголовок IP **недопустимо** менять (за исключением вставки временной метки в опции Timestamp). Таким образом, до того как маршрутизатор определит, не адресован ли пакет ему, он не может изменять заголовок IP так, чтобы от внесенных изменений потом было невозможно отказаться.

5.2.1.1 Общие вопросы

В этом параграфе рассматриваются принципы пересылки пакетов. Данный алгоритм применим ко всем типам пересылаемых пакетов - unicast (конкретный адресат), multicast (группа), broadcast (широковещательный пакет).

(1) Маршрутизатор получает пакет IP (вместе с дополнительной информацией о пакете, рассмотренной в параграфе 3.1), от канального уровня (Link Layer).

(2) Маршрутизатор проверяет корректность заголовка IP, как описано в параграфе 5.2.2. Отметим, что сборка фрагментов IP не выполняется за исключением тех случаев, когда пакет адресован самому маршрутизатору (см. п. (4) в предыдущем параграфе).

(3) Маршрутизатор выполняет большую часть операций по обработке опций IP. Как описано в параграфе 5.2.4, некоторые опции IP требуют дополнительной обработки после принятия решения о маршрутизации (выбора выходного интерфейса).

(4) Маршрутизатор проверяет IP-адрес получателя дейтаграммы, как описано в параграфе 5.2.3, чтобы определить, как должна происходить дальнейшая обработка дейтаграммы. Здесь возможны три варианта:

- дейтаграмма адресована маршрутизатору и ее следует поместить в локальную очередь, выполнив при необходимости сборку фрагментов;
- дейтаграмма не адресована маршрутизатору и ее следует поместить в очередь для пересылки;
- дейтаграмму следует поместить в очередь для пересылки, но ее копия также должна быть помещена в очередь для локальной доставки.

5.2.1.2 Конкретный адресат (Unicast)

Поскольку локальная доставка хорошо описана в [INTRO:2], ниже предполагается, что дейтаграмма IP предназначена для пересылки. Если пакет направлен по индивидуальному адресу IP, выполняются перечисленные ниже этапы.

(5) Модуль пересылки определяет IP-адрес следующего маршрутизатора (обычно путем просмотра таблицы маршрутизации). Эта процедура более детально описана в параграфе 5.2.4. Процедура также определяет сетевой интерфейс, который должен использоваться для передачи пакета.

(6) Модуль пересылки проверяет допустимость пересылки пакета. Адреса отправителя и получателя должны быть корректны в соответствии с требованиями параграфов 5.3.7 и 5.3.4. Если маршрутизатор поддерживает административные ограничения на пересылку (типа описанных в параграфе 5.3.9), эти ограничения должны быть приняты во внимание.

(7) Модуль пересылки уменьшает (по крайней мере на 1) значение TTL в заголовке пакета и проверяет его, как описано в параграфе 5.3.1.

(8) Модуль пересылки выполняет все операции по обработке опций IP, которые не могли быть выполнены на этапе (3).

(9) Модуль пересылки при необходимости фрагментирует пакет, как описано в параграфе 4.2.2.7. Поскольку этот этап выполняется после выбора выходного интерфейса (этап 5), все фрагменты дейтаграммы будут передаваться через один интерфейс.

(10) Модуль пересылки определяет адрес канального уровня для следующего интервала. Механизм определения адреса зависит от используемого протокола канального уровня (см. раздел 3).

(11) Модуль пересылки инкапсулирует дейтаграмму IP (и каждый из ее фрагментов) в соответствующий кадр канального уровня и помещает в очередь выходного интерфейса, выбранного на этапе 5.

(12) Модуль пересылки при необходимости передает сообщение ICMP redirect, как описано в параграфе 4.3.3.2.

5.2.1.3 Группа (Multicast)

Если адрес получателя является групповым адресом IP, выполняются перечисленные ниже этапы пересылки.

Основные различие между пересылкой индивидуальных и групповых дейтаграмм IP заключаются в следующем:

- групповые дейтаграммы IP обычно пересылаются на основе адресов отправителя и получателя в заголовке IP;
- для групповых дейтаграмм IP используется поиск по расширяющимся кругам;
- групповые дейтаграммы IP пересылаются с использованием групповой адресации канального уровня;
- сообщения ICMP об ошибках никогда не передаются в ответ на групповые дейтаграммы IP.

Отметим, что пересылка групповых дейтаграмм IP является в некоторой степени экспериментальной. Поэтому описанный ниже алгоритм не является обязательным и приведен лишь в качестве примера.

(5a) На основе IP-адресов отправителя и получателей из заголовка дейтаграммы маршрутизатор определяет, следует ли принимать дейтаграмму через данный интерфейс для дальнейшей пересылки. При отрицательном ответе дейтаграмма отбрасывается без уведомления. Метод определения пригодного входного интерфейса зависит от используемого алгоритма групповой маршрутизации. В одном из простейших алгоритмов RPF[1] пригоден будет тот интерфейс, который бы использовался для отправки индивидуальных пакетов по адресу отправителя дейтаграммы.

(6a) На основе IP-адресов отправителя и получателей из заголовка дейтаграммы маршрутизатор определяет выходные интерфейсы для пересылки дейтаграммы. Для реализации поиска по расширяющимся кругам (см. [INTERNET:4]) каждому выходному интерфейсу ставится в соответствие минимальное значение TTL. Копия multicast-дейтаграммы пересылается через каждый из выходных интерфейсов, для которого минимальное значение TTL не превышает значение TTL в заголовке дейтаграммы. Этот этап выполняется раздельно для каждого интерфейса.

(7a) Маршрутизатор уменьшает на 1 значение TTL в заголовке пакета.

(8a) Модуль пересылки выполняет все операции по обработке опций IP, которые не могли быть выполнены на этапе (3).

(9a) Модуль пересылки при необходимости выполняет фрагментацию дейтаграммы, как описано в параграфе 4.2.2.7.

(10a) Модуль пересылки определяет адрес канального уровня для использования при инкапсуляции дейтаграммы в кадр канального уровня. Механизм определения адреса зависит от протокола канального уровня. В локальных сетях используется групповой или широковещательный адрес канального уровня для передачи групповых дейтаграмм IP. Более детальную информацию вы найдете в соответствующих спецификациях IP-over-xxx.

(11a) Модуль пересылки инкапсулирует дейтаграмму IP (и каждый из ее фрагментов) в соответствующий кадр канального уровня и помещает в очереди соответствующих сетевых интерфейсов.

5.2.2 Проверка корректности заголовка IP

До того, как маршрутизатор начнет обработку пакета IP, он **должен** выполнить перечисленные ниже операции проверки корректности заголовка IP, позволяющие убедиться в осмысленности этого заголовка. При отрицательном результате любого из перечисленных ниже тестов пакет **должен** быть отброшен без уведомления. Информацию об ошибке **следует** записать в системный журнал маршрутизатора.

(1) Размер пакета, полученный от канального уровня, должен быть достаточным для размещения дейтаграммы IP минимального размера (20 байтов).

(2) Контрольная сумма в заголовке IP должны быть корректной.

(3) Поле IP version должно содержать значение 4. Если значение поля отличается от 4, пакет относится к другой версии протокола IP (например, IPng[2] или ST-II).

(4) Поле IP header length должно иметь значение, достаточное для дейтаграммы IP минимального размера (20 байтов = 5 слов).

(5) Значение поля IP total length должно быть достаточно большим для включения заголовка дейтаграммы IP, размер которого указан в поле IP header length.

Для маршрутизаторов **недопустимо** наличие конфигурационных опций, позволяющих отключить любую из перечисленных выше проверок. Если пакет прошел тесты 2 и 3, значение поля IP header length не менее 4, а значения поля IP total length и размера пакета, сообщенного канальным уровнем, не менее 16, маршрутизатор **может** передать сообщение ICMP Parameter Problem с указателем на поле IP header length (если не прошел тест 4) или IP total length (если не прошел тест 5). Однако он по-прежнему **должен** отбросить такой пакет, а информацию об ошибке **следует** записать в системный журнал.

Приведенные здесь правила (и документ в целом) относятся только в протоколу IP версии 4. Эти правила не следует рассматривать, как запрет поддержки в маршрутизаторах других версий протокола IP. Более того, если маршрутизатор может корректно определить принадлежность пакета к другой версии IP, он не должен трактовать такой пакет, как ошибочный в контексте настоящего документа.

Реализация

В целях протоколирования ошибок желательно (хотя и не всегда возможно) определять, в чем заключается некорректность заголовка. Ошибочные заголовки могут быть обусловлены рядом причин, включая:

- отсечение части заголовка IP на канальном уровне;
- использование в дейтаграмме версии протокола IP, отличающейся от стандартной (4);
- повреждение заголовка IP в процессе передачи пакета;
- некорректное создание заголовка IP отправителем.

Проверку заголовка желательно выполнять с соблюдением указанного выше порядка, поскольку этот порядок представляется наиболее удобным для определения причины ошибки. Для протоколирования ошибок может также оказаться полезной проверка принадлежности пакета к иным версиям протокола IP (в частности, IPng или ST-II); такие проверки нужно выполнять на основе соответствующих спецификаций.

В дополнение к перечисленным тестам **следует** проверять, что размер пакета, сообщенный канальным уровнем, достаточен для размещения дейтаграммы, размер которой указан в поле IP total length заголовка IP. Если окажется, что пакет был усечен по длине, такой пакет **должен** быть отброшен, информацию об ошибке **следует** записать в

[1] Reverse path forwarding - пересылка по обратному пути. *Прим. перев.*
[2] IPv6 в современной терминологии. *Прим. перев.*

системный журнал, а маршрутизатору **следует** передать сообщение ICMP Parameter Problem с указателем на поле IP total length.

Обсуждение

Поскольку любой протокол вышележащего уровня, озабоченный сохранностью данных, будет детектировать отсечение части пакета при доставке конечному получателю, предложенная выше проверка не является абсолютно необходимой для маршрутизаторов. Однако выполнение такой проверки в маршрутизаторах может существенно упростить задачу определения точки, в которой происходит отсечение части пакета. Кроме того, такая проверка сократит загрузку нисходящих потоков маршрутизатора за счет того, что поврежденные пакеты не будут передаваться.

Наконец, если адрес получателя в заголовке пакета не совпадает ни с одним из IP-адресов маршрутизатора, последнему **следует** убедиться в отсутствии в заголовке пакета опций Strict Source Route и Record Route. Если такая опция присутствует, маршрутизатору **следует** записать в системный журнал сообщение об ошибке и передать отправителю сообщение ICMP Parameter Problem с указателем на IP-адрес получателя.

Обсуждение

Некоторые люди считают, что маршрутизатору следует в таких случаях передавать сообщение Bad Source Route вместо Parameter Problem. Однако, если пакет не проходит указанную проверку, это обычно говорит о протокольной ошибке на предыдущем маршрутизаторе, тогда как сообщение Bad Source Route будет означать, что исходный отправитель задал несуществующий или недоступный путь через сеть.

5.2.3 Решение о локальной доставке

При получении пакета маршрутизатор должен решить, адресован этот пакет самому маршрутизатору (пакет следует доставлять локально) или другой системе (пакет следует переслать). Существует также комбинированный вариант, когда некоторые широковещательные или групповые пакеты могут одновременно пересылаться и доставляться локально. Маршрутизатор **должен** определить, какой из трех перечисленных случаев имеет место с помощью приведенных ниже правил.

1) Незавершенными считаются те опции source route, указатель которых не ссылается за последнюю запись в маршруте source route. Когда пакет содержит незавершенную опцию source route, указатель в этой опции ссылается вперед, если он не указывает на последний адрес в опции или следующий адрес не является одним из адресов самого маршрутизатора. В последнем (нормальном) случае пакет пересылается (и не доставляется локально) независимо от соответствия приведенным ниже правилам.

2) Пакет доставляется локально и не пересылается в следующих случаях:

   - адрес получателя точно соответствует одному из IP-адресов маршрутизатора;
   - в поле получателя указан широковещательный адрес ограниченного действия ({-1, -1});
   - пакет направлен по групповому адресу IP, для которого пересылка никогда не выполняется (например, 224.0.0.1 или 224.0.0.2) и хотя бы один из логических интерфейсов, связанных с физическим интерфейсом, приняшим пакет, является членом данной multicast-группы.

3) Пакет передается модулю пересылки и доставляется локально в следующих случаях:

   - в качестве адреса получателя указан широковещательный адрес IP, который соответствует хотя бы одному из логических интерфейсов маршрутизатора, но не соответствует адресам логических интерфейсов, связанных с физическим интерфейсом, через который был принят пакет;
   - пакет направлен по групповому адресу IP, который может использоваться для пересылки (в отличие от адресов 224.0.0.1 и 224.0.0.2), и по крайней мере один из логических интерфейсов, связанных с принявшим пакет физическим интерфейсом, является членом группы, которой пакет адресован.

4) Пакет доставляется локально, если он направлен по широковещательному адресу IP, отличному от широковещательного адреса ограниченного действия, которому соответствует хотя бы один адрес логического интерфейса, связанного с принявшим пакет физическим интерфейсом. Пакет также передается модулю пересылки, если канал, через который был принят пакет, не использует инкапсуляцию, не поддерживающую различий между широковещательной и индивидуальной адресацией (например, путем использования в таких случаях разных адресов канального уровня).

5) В остальных случаях пакет передается модулю пересылки.

Обсуждение

Требования последнего предложения п. 4 - обеспечение корректной обработки пакетов в случаях получения пакетов directed broadcast для другого префикса в той же физической сети. Обычно все работает в соответствии с ожиданиями - отправитель передает широковещательный пакет маршрутизатору с использованием unicast-адреса канального уровня. Маршрутизатор отмечает, что пакет получен, как unicast и, следовательно, должен быть направлен в другую сеть, нежели та, из которой он прибыл. Следовательно, маршрутизатор может без риска передать этот пакет с использованием широковещательного адреса канального уровня в ту же физическую сеть через тот же (физический) интерфейс, который принял пакет. Однако, если маршрутизатор не может определить, что пакет был получен, как unicast-кадр канального уровня, упомянутое требование позволяет маршрутизатору считать, что он выполняет безопасную, но некорректную пересылку (а не рискованную, но корректную).

Реализация

Как указано в параграфе 5.3.4, пакеты, полученные в широковещательных кадрах канального уровня, в общем случае не пересылаются маршрутизатором. Имеет смысл просто не передавать пакеты модулю пересылки, поскольку они все равно будут отбрасываться в соответствии с приведенными здесь правилами.

В некоторых случаях канальный уровень (в силу аппаратных особенностей или программного кода драйверов) может передавать маршрутизатору копии всех передаваемых в среде широковещательных и групповых кадров канального уровня. Описанный здесь подход позволяет упростить реализацию для тех случаев, когда пакет доставляется локально и передается модулю пересылки, поскольку пересылка пакета будет автоматически

приводить к получению маршрутизатором копии пакета, которую он может использовать для локальной доставки. Однако в таких случаях нужно быть внимательным, чтобы предотвратить трактовку полученных «возвратных» (loop-back) пакетов, как обычных принятых пакетов (и применения к ним правил пересылки и т. п.).

Даже при отсутствии таких особенностей канального уровня необходимо сделать копию целого пакета для помещения в очереди пересылки и локальной доставки с учетом того, что дейтаграмма может быть фрагментирована и требуется собрать фрагменты для локальной доставки, не выполняя такой сборки для пересылаемых пакетов. Одним из простых способов решения этой задачи является установка для каждого пакета в выходной очереди маршрутизатора специального флага, который показывает, нужно ли поместить пакет в очередь для локальной доставки после пересылки этого пакета.

5.2.4 Определение адреса следующего интервала

Когда маршрутизатор пересылает пакет, он должен определить, передается этот пакет конечному адресату или следующему маршрутизатору. В последнем случае требуется также определить маршрутизатор, которому нужно передать пакет. В этом разделе рассматриваются способы определения этого маршрутизатора.

Ниже перечислены используемые в этом разделе термины и сокращения:

- LSRR - опция IP Loose Source and Record Route;
- SSRR - опция IP Strict Source and Record Route;
- опция Source Route - LSRR или SSRR;
- адрес окончательной доставки[1] - точка, куда пакет в конце концов должен быть передан - последний адрес в заданном отправителем маршруте доставки пакета или IP-адрес получателя в заголовке пакета без опции source-route;
- смежный - доступный без прохождения через маршрутизаторы IP;
- адрес следующего интервала - IP-адрес смежного хоста или маршрутизатора, которому пакет будет передан на следующем интервале;
- IP-адрес получателя - адрес окончательной доставки для случаев, когда не используется заданная отправителем маршрутизация (в этом случае адресом получателя служит следующий адрес, указанный в source route);
- непосредственный получатель[2] - узел, система, маршрутизатор или конечная система, указанная IP-адресом получателя.

5.2.4.1 IP-адрес получателя

Если выполняются перечисленные ниже условия:

- адрес получателя в заголовке IP совпадает с одним из адресов маршрутизатора;
- пакет содержит опцию Source Route;
- указатель в опции Source Route не ссылается за пределы этой опции,

IP-адресом получателя является адрес, на который ссылается указатель опции Source Route. Если выполняются следующие условия:

- адрес получателя в заголовке IP совпадает с одним из адресов маршрутизатора;
- пакет содержит опцию Source Route;
- указатель в опции Source Route ссылается за пределы этой опции,

сообщение адресовано системе, анализирующей его[3].

Маршрутизатор **должен** использовать IP-адрес получателя, а не адрес окончательной доставки (последний адрес в опции source route) при определении режима обработки пакета.

Наличие в пакете нескольких опций source route является ошибкой. При получении такой дейтаграммы маршрутизатору **следует** отбрасывать пакет, передавая его отправителю сообщение ICMP Parameter Problem с указателем на начало второй опции source route.

5.2.4.2 Выбор между локальной доставкой и пересылкой

После того, как была определена необходимость пересылки пакета IP в соответствии с правилами, указанными в параграфе 5.2.3, **должен** использоваться описанный ниже алгоритм определения прямой доступности[4] непосредственного получателя (см. [INTERNET:2]).

(1) Для каждого сетевого интерфейса, не имеющего адреса IP (безадресные линии обсуждаются в параграфе 2.2.7), сравнивается значение router-id на другой стороне соединения с IP-адресом получателя. При совпадении адресов пакет можно передавать через данный интерфейс.

Обсуждение

Иными словами, маршрутизатор или хост на другой стороне соединения является адресатом пакета или следующим интервалом заданного отправителем маршрута для пакета с опцией source route.

(2) Если на первом этапе сетевой интерфейс не был выбран, для каждого из IP-адресов маршрутизатора выполняются следующие операции:

[1] Ultimate Destination Address.
[2] Immediate Destination.
[3] Данному маршрутизатору. *Прим. перев.*
[4] Расположения непосредственного получателя в одной из подключенных к маршрутизатору сетей. *Прим. перев.*

(a) Выделяется сетевой префикс, используемый интерфейсом.

Реализация

Результат этой операции обычно вычисляется в процессе инициализации маршрутизатора и сохраняется для последующего использования.

(b) Выделяется соответствующий набор битов из IP-адреса получателя для пакета.

(c) Сравниваются полученные сетевые префиксы и при совпадении пакет может передаваться через соответствующий интерфейс.

(3) Если получателем не является ни router-id соседнего маршрутизатора на безадресном соединении, ни узел непосредственно подключенной к маршрутизатору сети, это говорит, что на пути к адресату присутствуют другие маршрутизаторы (данный маршрутизатор не является последним). Выбор маршрутизатора и адреса IP для следующего интервала описан в параграфе 5.2.4.3. В случае хоста, не являющегося маршрутизатором, может использоваться принятый по умолчанию маршрут.

В работе [ARCH:9, NRHP] рассматриваются некоторые специальные случаи (например, наличие множества (под)сетей IP в одной сети канального уровня). За исключением заданных политикой ограничений, хосты и маршрутизаторы, находящиеся в одной сети канального уровня, могут взаимодействовать между собой напрямую, даже если они находятся в разных (под)сетях IP, при наличии адекватной информации. Протокол NHRP[1] позволяет узлам IP определять «оптимальный» адрес канального уровня для передачи пакетов через такую сеть канального уровня в направлении удаленного адресата.

(4) Если выбранный следующий интервал доступен через интерфейс, настроенный на использование NHRP, применимы перечисленные ниже дополнительные операции.

(a) Сравнивается IP-адрес получателя с адресами получателей в кэше NHRP. При обнаружении искомого адреса в кэше, дейтаграмма передается по соответствующему кэшированному адресу канального уровня.

(b) Если адрес не найден в кэше, создается пакет запроса NHRP, содержащий IP-адрес получателя. Это сообщение передается серверу NHRP, заданному для интерфейса. В качестве такого сервера может использоваться логически выделенный процесс или объект в самом маршрутизаторе.

(c) Сервер NHRP в ответ на запрос сообщит подходящий адрес канального уровня для передачи этой (и последующих) дейтаграммы адресату. Во время ожидания отклика от сервера NHRP система **может** передать дейтаграмму (дейтаграммы) «традиционному» маршрутизатору следующего интервала.

5.2.4.3 Адрес следующего интервала

Комментарии

Маршрутизаторы используют описанный в предыдущем параграфе алгоритм для определения присутствия IP-адреса получателя в смежной сети. При положительном ответе адрес следующего интервала совпадает с IP-адресом получателя. В противном случае пакет должен пересылаться через другой маршрутизатор для доставки непосредственному получателю. Выбор этого маршрутизатора рассматривается в данном параграфе.

Если пакет содержит SSRR, маршрутизатор **должен** отбросить пакет и передать его отправителю сообщение об ошибке ICMP Bad Source Route. В противном случае маршрутизатор ищет IP-адрес получателя в своей таблице маршрутизации для выбора следующего интервала пересылки.

Обсуждение

В соответствии со спецификацией протокола IP опция Strict Source Route должна содержать последовательность узлов, через которые должен проходить пакет (пакет передается от узла source route к следующему, проходя только через промежуточные сети). Таким образом, если маршрутизатор не является смежным со следующим узлом source route, заданный отправителем маршрут не может быть завершен. Следовательно, маршрутизатор будет отвергать такие пакеты, возвращая отправителю сообщение ICMP Bad Source Route.

Целью процесса выбора следующего интервала является проверка записей в базе пересылки маршрутизатора (FIB) и выбор лучшего маршрута (если такой имеется) для пакета из числа путей, представленных в FIB.

Концептуально любой алгоритм поиска маршрутов начинается с набора кандидатов, в качестве которого используется вся таблица FIB. Алгоритм включает последовательность этапов, на которых отбрасываются некоторые маршруты из числа кандидатов. Такие этапы называют правилами сокращения. Обычно при завершении работы алгоритмов из набора кандидатов остается единственный маршрут. Если после сокращения остается пустой набор (нет маршрута), пакет отбрасывается по причине недоступности адресата. Возможно также завершение работы алгоритма с несколькими оставшимися кандидатами. В этом случае маршрутизатор может произвольно выбрать один из оставшихся маршрутов или воспользоваться режимом распределения нагрузки между этими маршрутами, выбирая из них тот, который дольше не использовался.

При выборе для пакета следующего интервала маршрутизатор **должен** использовать приведенные ниже правила сокращения, за исключением правила 3 (Weak TOS). Если маршрутизатор использует значение TOS при выборе следующего интервала, правило 3 должно применяться с соблюдением приведенного здесь порядка. Эти правила **должны** быть (концептуально) применены к FIB в том порядке, как они представлены ниже (в силу исторических причин дополнительные правила сокращения и другой алгоритм выбора следующего интервала рассматриваются в приложении E.)

Обсуждение

Правило 3 является необязательным и в параграфе 5.3.2 сказано, что маршрутизатору лишь **следует** принимать во внимание значение TOS при выборе решения о пересылке.

(1) Базовое соответствие (Basic Match)

Это правило отбрасывает все маршруты к адресату, отличающиеся от IP-адреса получателя для пакета. Например, если в пакете указан IP-адрес получателя 10.144.2.5, на этом этапе будет отброшен маршрут в сеть

[1] Next Hop Routing Protocol.

128.12.0.0/16, но останутся любые маршруты в сети 10.0.0.0/8 и 10.144.0.0/16, а также принятые по умолчанию маршруты.

Говоря более точно, мы предполагаем, что каждый маршрут имеет атрибут назначения (route.dest) и соответствующий ему размер префикса (route.length) для задания количества значимых битов в route.dest. IP-адрес получателя пересылаемого пакета - это ip.dest. Данное правило отбрасывает из набора кандидатов все маршруты, кроме тех, для которых route.length старших битов route.dest и ip.dest совпадают.

Например, если IP-адрес получателя пакета 10.144.2.5 и имеются префиксы 10.144.1.0/24, 10.144.2.0/24 и 10.144.3.0/24, данное правило оставит только 10.144.2.0/24 (единственный маршрут, в котором 24 старших бита совпадают с 24 старшими битами IP-адреса получателя в пакете).

(2) Соответствие максимальной длины (Longest Match)

Правило Longest Match является усовершенствованным вариантом правила Basic Match, описанного выше. После сокращения по правилу Basic Match, алгоритм проверяет оставшиеся маршруты для выбора пути с максимальным значением route.length. Все остальные маршруты отбрасываются.

Например, если в пакете задан IP-адрес получателя 10.144.2.5 и остались префиксы 10.144.2.0/24, 10.144.0.0/16 и 10.0.0.0/8, среди них будет выбран префикс 10.144.2.0/24, поскольку для него длина соответствия является наибольшей.

(3) Наименьшие требования к TOS (Weak TOS)

Каждый маршрут имеет атрибут типа обслуживания (route.tos), возможные значения которого совпадают со значениями, используемыми для поля TOS в заголовках IP. Протоколы маршрутизации, распространяющие информацию TOS, заполняют значения route.tos применительно к маршрутам, добавляемым в FIB. Маршруты от других протоколов маршрутизации трактуются как маршруты с принятым по умолчанию значением TOS (0000). Поле TOS в заголовке маршрутизируемого пакета будем обозначать ip.tos.

Для набора кандидатов проверяется наличие среди них маршрутов, для которых route.tos = ip.tos. При наличии таких маршрутов все остальные маршруты отбрасываются. Если среди кандидатов такого маршрута нет, отбрасываются все маршруты, для которых значение route.tos отлично от нуля.

Дополнительное обсуждение маршрутизации на базе правила Weak TOS можно найти в [ROUTE:11].

Обсуждение

Это правило позволяет выбрать из числа кандидатов те маршруты, для которых значение TOS совпадает со значением поля TOS в заголовке пакета. Если такие маршруты отсутствуют, рассматриваются маршруты с принятым по умолчанию значением TOS. Маршруты с отличным от нуля значением TOS, которое не совпадает с полем TOS в заголовке пакета, никогда не используются, даже если такой маршрут является единственным путем к адресату.

(4) Наилучшая метрика (Best Metric)

Каждый маршрут имеет атрибут метрики (route.metric) и идентификатор домена маршрутизации (route.domain). Каждый маршрут из множества кандидатов сравнивается с остальными маршрутами этого множества. Если для двух маршрутов значения route.domain совпадают, а значение route.metric для одного из маршрутов существенно «хуже», такой маршрут отбрасывается из числа кандидатов. Сравнение параметров метрики обычно сводится к простому арифметическому сравнению, хотя некоторые протоколы могут использовать структурированную метрику, требующую для сравнения более сложных операций.

(5) Политика производителя (Vendor Policy)

Vendor Policy представляет собой «последний шанс» выбора маршрута, когда приведенные выше правила не позволили сделать такой выбор. Алгоритм сокращения Vendor Policy определяется производителем (см. параграф 5.2.4.4).

Описанный алгоритм имеет два существенных недостатка. Разработчики маршрутизаторов, по-видимому, смогут преодолеть эти недостатки и использовать свое решение как часть правила Vendor Policy.

(1) Классы маршрутов IS-IS и OSPF не обслуживаются напрямую.

(2) Отличные от типа обслуживания свойства пути (например, MTU) игнорируются.

Следует также отметить малую эффективность использования TOS - протоколам маршрутизации, поддерживающим TOS, неявно отдается предпочтение при пересылке пакетов с отличным от нуля полем TOS.

Правила сокращения Basic Match и Longest Match выбирают маршруты с учетом их типа в том порядке, как показано ниже.

(1) Host Route (маршрут к хосту) - маршрут к указанной конечной системе.

(2) Hierarchical Network Prefix Routes (маршруты к иерархическим сетевым префиксам) - маршрут к отдельному сетевому префиксу. Отметим, что FIB может содержать несколько маршрутов к сетевым префиксам, которые являются частью других префиксов (один префикс представляет собой другой префикс, к которому добавлены биты). Эти префиксы выбираются в порядке уменьшения размера.

(3) Default Route (маршрут по умолчанию) - это путь во все сети, для которых не определено явных маршрутов. Такой маршрут можно определить как маршрут с префиксом нулевой длины.

Если после применения правил сокращения остается пустой набор маршрутов (ничего не найдено), пакет **должен** быть отброшен с передачей отправителю сообщения ICMP об ошибке (ICMP Bad Source Route, если IP-адрес получателя взят из опции source route, ICMP Destination Host Unreachable или Destination Network Unreachable в остальных случаях, в соответствии в правилами параграфа 4.3.3.1).

5.2.4.4 Административные предпочтения

Одним из предложенных механизмов реализации правила сокращения Vendor Policy является использование административных предпочтений, которые представляют собой простой алгоритм приоритизации. Идея этого метода состоит в задании административным путем уровней приоритета для маршрутов, что позволяет выбирать наиболее предпочтительный путь из числа возможных.

Каждый маршрут получает уровень приоритета на основе различных атрибутов этого маршрута. Один из вариантов механизма установки уровней приоритета предложен ниже. Уровни приоритета выражаются целыми числами в диапазоне [0..255]. Значение 0 соответствует высшему приоритету, а 254 - низшему. Значение 255 устанавливается для маршрутов, которые никогда не следует использовать. На первом этапе правила сокращения Vendor Policy отбрасываются все маршруты, кроме тех, которые имеют высший приоритет. Маршруты с приоритетом 255 отбрасываются во всех случаях.

Использование этого правила сопряжено с риском возникновения маршрутных петель. Поскольку не существует протокола, обеспечивающего согласованность выбранных для маршрутизатора предпочтений с предпочтениями, заданными для маршрутизаторов соседних сетей, администраторы должны с осторожностью относиться к заданию своих предпочтений.

- **Address Match** (соответствие адреса)

  Полезно иметь возможность присвоить одинаковый уровень предпочтения для всех маршрутов (полученных из одного домена маршрутизации) к любому из указанного набора адресатов, включающего всех получателей, которые соответствуют заданному префиксу сети.

- **Route Class** (класс маршрута)

  Для протоколов маршрутизации, поддерживающих различия, полезно иметь возможность присвоить один уровень предпочтения для всех маршрутов (полученных из одного домена маршрутизации), имеющих одинаковый класс (внутри области, между областями, внешний с внутренней метрикой, внутренний с внешней метрикой).

- **Interface** (интерфейс)

  Полезно иметь возможность установить одинаковый уровень предпочтения для всех маршрутов (полученных из одного домена маршрутизации), которые будут передавать пакеты через один логический интерфейс маршрутизатора (логические интерфейсы в общем случае взаимно-однозначно отображаются на сетевые интерфейсы маршрутизатора, за исключением того, что любой сетевой интерфейс, имеющий множество адресов IP, будет иметь множество связанных с ним логических интерфейсов).

- **Source router** (маршрутизатор-источник)

  Полезно иметь возможность установить одинаковый уровень предпочтения для всех маршрутов (полученных из одного домена маршрутизации), которые были получены от любого набора маршрутизаторов, чьи обновления имеют адрес отправителя, соответствующий заданному сетевому префиксу.

- **Originating AS** (исходная АС)

  Для протоколов маршрутизации, обеспечивающих информацию об автономной системе, полезно иметь возможность установить одинаковый уровень предпочтения для всех маршрутов (полученных из одного домена маршрутизации), начинающихся из одного домена маршрутизации. Для маршрутов BGP исходная АС является первой автономной системой, указанной в атрибуте AS_PATH. Для внешних маршрутов OSPF в качестве исходной АС могут рассматриваться младшие 16 битов тега внешнего маршрута, если для тега установлен бит Automatic и значение Path Length отличается от 3.

- **External route tag** (тег внешнего маршрута)

  Полезно иметь возможность установить одинаковый уровень предпочтения для всех внешних маршрутов OSPF (полученных из одного домена маршрутизации), для которых теги внешнего маршрута соответствуют любому из списка заданных значений. Поскольку тег внешнего маршрута может содержать структурированное значение, может оказаться полезным обеспечение возможности проверки соответствия отдельных полей тега.

- **AS path** (путь в АС)

  Полезно иметь возможность установить одинаковый уровень предпочтения для всех внешних маршрутов BGP (полученных из одного домена маршрутизации), для которых AS path «соответствует» любому набору заданных значений. Пока не ясно до конца, какой тип соответствия будет наиболее полезным. Простая опция позволяет выбирать все маршруты, где указанная АС присутствует (или, наоборот, отсутствует) в атрибуте AS_PATH. Более общий, но в некоторых случаях более сложный вариант, позволит выбирать все маршруты, для которых AS path соответствует заданному регулярному выражению.

5.2.4.5 Распределение нагрузки

При завершении процесса выбора следующего интервала в списке кандидатов может остаться несколько маршрутов. В таких случаях маршрутизатор может использовать различные варианты выбора. Можно произвольно выбрать один маршрут, отбросив все остальные. Можно сократить число кандидатов путем сравнения параметров метрики. Возможно также оставить в списке кандидатов более одного маршрута и использовать механизм распределения трафика между ними. Следует отметить, что распределение трафика может быть полезно в определенных случаях, но не всегда. Поэтому разработчикам механизмов распределения нагрузки следует давать администраторам возможность отключить эту функцию.

5.2.5 Неиспользуемые биты заголовка IP - RFC 791, параграф 3.1

Заголовок IP включает несколько резервных битов в полях Type of Service и Flags. Для маршрутизаторов **недопустимо** отбрасывание пакетов на том лишь основании, что один или несколько резервных битов имеют ненулевое значение.

Маршрутизаторы **должны** игнорировать резервные биты и пересылать пакеты без изменения этих битов. Если маршрутизатор фрагментирует пакет, он **должен** скопировать эти биты в каждый фрагмент.

Обсуждение

В будущих реализациях протокола IP резервные биты заголовка могут использоваться. Приведенные выше правила обеспечивают совместимость с новыми версиями протокола без необходимости одновременного обновления всех маршрутизаторов в Internet.

5.2.6 Фрагментация и сборка - RFC 791, параграф 3.2

Как было сказано в параграфе 4.2.2.7, маршрутизатор **должен** поддерживать фрагментацию IP.

Для маршрутизаторов **недопустима** сборка фрагментов перед пересылкой пакетов.

Обсуждение

Существует мнение, что в некоторых средах сборка маршрутизаторами фрагментов транзитных дейтаграмм может повысить производительность. Однако фрагменты могут перемещаться к конечному адресату по разным путям, поэтому на транзитном маршрутизаторе могут появиться не все фрагменты дейтаграммы и попытка собрать их будет обречена на неудачу.

Приведенные в этом параграфе правила не имеют отношения к фрагментации или сборке, которую маршрутизатор может выполнять на канальном уровне.

Если дейтаграмма IP инкапсулирована в другую дейтаграмму IP (например, для организации туннеля), которая была фрагментирована, требуется собрать фрагменты для того, чтобы переслать исходную дейтаграмму. Приведенное выше правило не препятствует такой сборке.

5.2.7 Протокол ICMP

Общие требования для протокола ICMP были рассмотрены в главе 4.3. В последующих параграфах обсуждаются сообщения ICMP, которые передаются только маршрутизаторами.

5.2.7.1 Destination Unreachable

Сообщения ICMP Destination Unreachable передаются маршрутизатором в ответ на пакеты, которые невозможно переслать по причине недоступности адресата (или следующего интервала на пути к нему) или сервиса. Примером могут служить пакеты, адресованные отсутствующему хосту (нет отклика на запросы ARP) или направленные в сети, к которым маршрутизатор не знает действительного пути.

Маршрутизатор **должен** обеспечивать возможность генерации сообщений ICMP Destination Unreachable, **следует** также обеспечивать возможность выбора кода отклика для более точного указания причины ошибки.

В документах [INTERNET:8] и [INTRO:2] определены перечисленные ниже коды ошибок.

0 = **Network Unreachable** (сеть недоступна) - генерируется маршрутизатором в тех случаях, когда путь в сеть адресата недоступен.

1 = **Host Unreachable** (хост недоступен) - генерируется маршрутизатором при недоступности маршрута к хосту сети, непосредственно подключенной к маршрутизатору (хост не отвечает на запросы ARP).

2 = **Protocol Unreachable** (протокол недоступен) - генерируется маршрутизатором в тех случаях, когда указанный в пакете транспортный протокол не поддерживается транспортным уровнем конечного получателя.

3 = **Port Unreachable** (порт недоступен) - генерируется маршрутизатором в тех случаях, когда указанный в заголовке пакета транспортный протокол (например, UDP) не способен демультиплексировать дейтаграмму на транспортный уровень конечного получателя и отсутствует протокольный механизм для информирования об этой ошибке отправителя.

4 = **Fragmentation Needed and DF Set** (требуется фрагментация, но установлен флаг DF) - генерируется маршрутизатором в тех случаях, когда ему требуется фрагментировать дейтаграмму, содержащую в заголовке флаг DF.

5 = **Source Route Failed** (невозможна указанная отправителем маршрутизация) - генерируется маршрутизатором в тех случаях, когда невозможно переслать пакет на следующий интервал, заданный опцией source route.

6 = **Destination Network Unknown** (неизвестна сеть адресата) - этот код **не следует** использовать в сообщениях, поскольку некоторые маршрутизаторы трактуют его как отсутствие сети адресата (взамен **следует** использовать код 0).

7 = **Destination Host Unknown** (получатель неизвестен) - генерируется только в тех случаях, когда маршрутизатор может определить (на канальном уровне), что хоста-адресата не существует.

11 = **Network Unreachable For Type Of Service** (сеть недоступна для заданного типа обслуживания) - генерируется маршрутизатором в тех случаях, когда путь в сеть адресата с запрошенным в заголовке или принятым по умолчанию значением TOS недоступен.

12 = **Host Unreachable For Type Of Service** (хост недоступен для заданного типа обслуживания) - генерируется маршрутизатором в тех случаях, когда отсутствует возможность пересылки пакета в результате того, что ни один из путей к адресату не соответствует указанному в пакете или принятому по умолчанию (0) значению TOS.

Здесь определяются несколько дополнительных кодов.

13 = **Communication Administratively Prohibited** (связь запрещена администратором) - генерируется в тех случаях, когда маршрутизатор не может переслать пакет по причине заданной администратором фильтрации.

14 = **Host Precedence Violation** (недопустимый уровень предпочтений) - передается первым маршрутизатором на пути доставки хосту-отправителю, чтобы показать недопустимость запрошенных предпочтений для данной комбинации «отправитель – получатель» (хосты или сети), протокола вышележащего уровня и порта отправителя/получателя.

15 = **Precedence cutoff in effect** (уровень предпочтений слишком низок) - сетевой оператор задал минимальный уровень предпочтений, а дейтаграмма была передана с более низким уровнем.

Примечание. В документе [INTRO:2] определен код 8 для изолированного хоста-отправителя. Маршрутизаторам **не следует** генерировать сообщения с кодом 8, взамен **следует** использовать код 0 (Network Unreachable) или 1 (Host Unreachable). В [INTRO:2] также определен код 9 (связь с сетью адресата запрещена административно) и 10 (связь с хостом-адресатом запрещена административно). Эти коды были предназначены для устройств сквозного шифрования, используемых в вооруженных силах США. Маршрутизаторам **следует** использовать определенный здесь код 13 (Communication Administratively Prohibited), если они фильтруют пакеты в соответствии с заданной администратором политикой.

Маршрутизаторы **могут** поддерживать конфигурационную опцию, которая позволяет отключить генерацию сообщений с кодом 13. При включенной опции в ответ на пакеты, отброшенные в силу административного запрета на пересылку, не будет передаваться никаких сообщений ICMP об ошибке.

Аналогично маршрутизаторы **могут** поддерживать конфигурационную опцию для запрета генерации сообщений с кодами 14 (Host Precedence Violation) и 15 (Precedence Cutoff in Effect). При включенной опции в ответ на пакеты с нарушением уровня предпочтений не будет передаваться никакого сообщения ICMP об ошибке.

Маршрутизаторы **должны** использовать код Host Unreachable или Destination Host Unknown, если другие хосты сети адресата продолжают быть доступными, поскольку в противном случае хост-отправитель может принять ошибочное решение о недоступности всей сети.

В документе [INTERNET:14] описана несколько отличающаяся модификация сообщений Destination Unreachable с кодом 4 (Fragmentation needed and DF set). При генерации сообщений Destination Unreachable с кодом 4 маршрутизатор **должен** использовать эту форму.

5.2.7.2 Redirect

Сообщения ICMP Redirect используются для того, чтобы сообщить локальному хосту о том, что ему следует использовать другой маршрутизатор next hop для определенного типа трафика.

Для маршрутизаторов **недопустима** генерация сообщений Redirect for Network или Redirect for Network and Type of Service (коды 0 и 2), описанных в [INTERNET:8]. Маршрутизаторы **должны** быть способны генерировать сообщения Redirect for Host (код 1) и **следует** также поддерживать генерацию сообщений Redirect for Type of Service and Host (код 3), описанных в [INTERNET:8].

Обсуждение

Если подключенная напрямую к маршрутизатору сеть не разделена на подсети (в классическом смысле), маршрутизатор может генерировать сообщения Network Redirect, применимые ко всем хостам заданной сети. Использование Network Redirect, а не Host Redirect может привести к некоторому снижению уровня трафика и занимаемого таблицей маршрутизации размера. Однако эта экономия невелика, а наличие подсетей порождает неоднозначность определения маски, используемой для интерпретации сообщений Network Redirect. В среде CIDR сложно точно указать случаи допустимости использования сообщений Network Redirect. Следовательно, маршрутизаторы должны передавать только сообщения Host (или Host and Type of Service) Redirect.

Сообщения с кодом 3 (Redirect for Host and Type of Service) генерируются в тех случаях, когда пакет, вызвавший перенаправление, имеет адресата, для которого путь, выбранный маршрутизатором, зависит (в частности) от запрошенного значения TOS.

Маршрутизаторы, генерирующие сообщения Redirect с кодом 3 (Host and Type of Service), **должны** иметь конфигурационную опцию (включенную по умолчанию), которая позволит генерировать сообщения с кодом 1 (Host) взамен сообщений с кодом 3. Маршрутизатор **должен** передавать сообщения Redirect с кодом 1 вместо сообщений Redirect с кодом 3, если конфигурация настроена соответствующим образом.

Если маршрутизатор не способен генерировать сообщения Redirect с кодом 3, он **должен** взамен генерировать сообщения Redirect с кодом 1.

Для маршрутизаторов **недопустима** генерация сообщений Redirect, если не выполняются все перечисленные ниже условия:

- пакет будет пересылаться в тот же физический интерфейс, через который он был принят;
- IP-адрес отправителя в пакете относится к той же логической (под)сети, что и IP-адрес следующего интервала;
- пакет не содержит опции IP source route.

Адрес отправителя в сообщениях ICMP Redirect **должен** относиться к той же логической (под)сети, что и адрес получателя.

Для маршрутизаторов, использующих протоколы маршрутизации (отличные от статических маршрутов), **недопустимо** принимать во внимание пути, полученные в сообщениях ICMP Redirect, при пересылке пакетов. Если маршрутизатор не использует протоколы маршрутизации, он **может** иметь конфигурацию, которая позволяет использовать маршруты из сообщений ICMP Redirect для пересылки пакетов.

Обсуждение

ICMP Redirect обеспечивает маршрутизаторам механизм механизм доставки маршрутных данных хостам. Маршрутизаторы используют для получения маршрутной информации иные механизмы и поэтому им нет резона руководствоваться сообщениями Redirect. Использование сообщений Redirect, противоречащих другой маршрутной информации, с очевидностью приводит к возникновению маршрутных петель.

С другой стороны, если маршрутизатор не функционирует в качестве такового, он **должен** соответствовать требованиям, предъявляемым к хостам.

5.2.7.3 Time Exceeded

Маршрутизатор **должен** генерировать сообщения Time Exceeded с кодом 0 (In Transit), когда он отбрасывает дейтаграммы с истекшим временем жизни (поле TTL). Маршрутизатор **может** поддерживать для своих интерфейсов опции, отключающие генерацию таких сообщений на уровне интерфейса, но по умолчанию опции **должны** обеспечивать генерацию сообщений.

5.2.8 Протокол IGMP

Протокол IGMP [INTERNET:4] используется хостами и multicast-маршрутизаторами одной физической сети для включения хостов в группы и выхода из них. Multicast-маршрутизаторы используют сведения о принадлежности хостов к группам вместе с протоколами групповой маршрутизации для поддержки пересылки пакетов IP с групповой адресацией через Internet.

Маршрутизаторам **следует** реализовать связанную с multicast-маршрутизаторами часть протокола IGMP.

5.3 Конкретные вопросы

5.3.1 Время жизни

Поле TTL (время жизни) в заголовке IP определяет таймер, ограничивающий срок существования дейтаграммы в сети. Это 8-битовое поле показывает время жизни в секундах. Каждый маршрутизатор (или иной модуль), обрабатывающий пакет, **должен** уменьшить значение поля TTL по крайней мере на 1, даже если обработка пакета заняла меньше секунды. Поскольку такая ситуация является весьма частой, значение поля TTL определяет скорее счетчик интервалов на пути дейтаграммы через Internet.

Когда маршрутизатор пересылает пакет, он **должен** уменьшить значение TTL по крайней мере на 1. Если обработка пакета занимает более 1 секунды, маршрутизатор **может** уменьшать значение TTL каждую секунду в процессе обработки.

Если значение TTL уменьшается до 0 (или меньше), пакет **должен** отбрасываться и, если пакет направлен не по групповому адресу, маршрутизатор **должен** генерировать сообщение ICMP Time Exceeded с кодом 0 (TTL Exceeded in Transit) для отправителя пакета. Отметим, что для маршрутизаторов **недопустимо** отбрасывание индивидуальных (unicast) или широковещательных (broadcast) пакетов IP с отличным от нуля значением TTL лишь на том основании, что данный маршрутизатор может предсказать завершение срока жизни пакета на другом маршрутизаторе по пути к конечному адресату. Однако маршрутизатор **может** отбрасывать пакеты, направленные по групповым адресам IP, с отличным от нуля временем жизни для более эффективной реализации алгоритма поиска по расширяющимся кольцам (см. [INTERNET:4]).

Обсуждение

Значение IP TTL используется (иной раз, шизофренически) в качестве ограничителя числа интервалов доставки и времени жизни пакета. Использование поля в качестве счетчика интервалов имеет важное значение для решения проблем маршрутизации, которые могут привести к утрате работоспособности сети при возникновении петли в маршрутизации. Функция ограничения времени жизни используется протоколами транспортного уровня (такими, как TCP), чтобы обеспечить гарантированную доставку данных. Многие современные реализации трактуют поле TTL исключительно как счетчик интервалов и часть сообщества Internet считает, что функции ограничения времени жизни пакетов должны быть реализованы в транспортных протоколах, которым такое ограничение требуется.

В данной спецификации мы с неохотой решили последовать вере многих производителей маршрутизаторов в то, что функцию ограничения времени можно сделать необязательной. Производители аргументируют это тем, что реализация функции ограничения времени достаточно сложна, а используют ее далеко не все. Производители указывают также на то, что известно мало достоверных случаев, когда отказ от ограничения времени приводил к нарушению работы протокола TCP (естественно, мы понимаем, что эта проблема встречается достаточно редко и ее сложно воспроизвести, поэтому малое число документированных случаев вовсе не говорит о том, что не было большого числа случаев, не отраженных документально).

Категории групповой адресации IP (такие, как поиск по расширяющимся кругам) могут не работать в соответствии с ожиданиями, если значение TTL не будет трактоваться как счетчик интервалов. То же самое можно сказать о traceroute.

Сообщения ICMP Time Exceeded необходимы, поскольку диагностическая утилита traceroute не будет работать без них.

Таким образом, проблема заключается в выборе между сохранением двух очень полезных инструментов и предотвращением достаточно редких и кратковременных проблем, которые могут оказаться несуществующими совсем. В результате было выбрано сохранение инструментов.

5.3.2 Тип обслуживания

Байт типа обслуживания (Type-of-Service или TOS) в заголовке IP делится на три части: поле предпочтений (Precedence - три старших бита), поле собственно TOS (следующие 4 бита) и резервное поле (младший бит). Правила обращения с резервным битом были описаны в параграфе 4.2.2.3. Поле предпочтений будет рассмотрено в параграфе 5.3.3. Более подробное обсуждение поля TOS и его использования можно найти в документе [ROUTE:11].

Маршрутизатору **следует** принимать во внимание значение поля TOS в заголовке пакета IP при выборе решения о пересылке пакета. В оставшейся части этого параграфа рассматриваются правила, применимые к маршрутизаторам, которые соответствуют этому требованию.

Маршрутизатор **должен** поддерживать значение TOS для каждого маршрута в своей таблице маршрутизации. Маршрутам, полученным от протоколов маршрутизации, которые не поддерживают TOS, **должно** присваиваться значение TOS=0 (принятое по умолчанию значение TOS).

Для выбора пути к адресату маршрутизатор **должен** использовать алгоритм, эквивалентный описанному ниже.

(1) Найти в своей таблице маршрутизации все доступные пути к адресату (см. параграф 5.2.4).

(2) При отсутствии хотя бы одного пути отбросить пакет по причине недоступности адресата (см. параграф 5.2.4).

(3) Если один или несколько маршрутов к адресату имеют значение TOS, совпадающее со полем TOS в заголовке пакета, выбирать путь с наиболее предпочтительной метрикой.

(4) При отсутствии таких маршрутов повторить п. 3 для поиска маршрутов с TOS = 0.

(5) Если на этапах 3 и 4 не было выбрано ни одного маршрута, пакет отбрасывается, поскольку адресат недоступен. Маршрутизатор возвращает отправителю сообщение об ошибке ICMP Destination Unreachable с соответствующим кодом - Network Unreachable with Type of Service (11) или Host Unreachable with Type of Service (12).

Обсуждение

Хотя поле TOS редко применялось в прошлом, сейчас его использование является обязательным в соответствии с требованиями к хостам документов [INTRO:2] и [INTRO:3]. Поддержка TOS в маршрутизаторах может стать **обязательной** в будущем, но ее **следует** реализовать уже сейчас.

Множество людей предполагает, что значение TOS следует использовать для воздействия на другие аспекты функции пересылки. Например,

(1) маршрутизатор может помещать пакеты с установленным битом Low Delay (малая задержка) впереди других пакетов в выходных очередях;

(2) маршрутизатор форсирует отбрасывание пакетов, что может предотвратить отбрасывание пакетов с установленным битом High Reliability.

Эти идеи более подробно рассматриваются в документе [INTERNET:17], но мы не имеем достаточного опыта для того, чтобы давать рекомендации по таким вопросам.

5.3.3 IP Precedence

В этом параграфе приведены требования и рекомендации по обработке поля IP Precedence в маршрутизаторах. Уровень предпочтения определяет схему выделения сетевых ресурсов на основе относительной важности различных потоков трафика. Спецификация протокола IP определяет значения, используемые в поле Precedence для различных типов трафика.

Основным механизмом обработки уровня предпочтения в маршрутизаторах является преимущественное выделение ресурсов (включая управление очередями и контроль насыщения на основе уровня предпочтения) и выбор средств управления приоритизацией на канальном уровне. Маршрутизатор также выбирает уровень предпочтений для трафика протоколов маршрутизации, а также управления и контроля, порождаемого самим маршрутизатором. Более подробное рассмотрение параметров IP Precedence и реализации механизмов приводится в документе [FORWARD:6].

Управление очередями на основе уровня предпочтения, рассматриваемое в этом параграфе, включает (но не ограничивается) очереди на пересылку и выходные очереди. Предполагается, что маршрутизаторам, поддерживающим уровни предпочтения, следует также использовать индикацию уровня предпочтения во всех точках процесса обработки, связанных с выделением ограниченных ресурсов (таких, как буферы или соединения канального уровня). Набор таких точек зависит от реализации.

Обсуждение

Хотя изначально поле Precedence предназначалось для использования в системах DOD[1], где пики трафика или серьезные повреждения сети рассматривались как присущие сети угрозы, использование этого поля оказалось полезным и для множества гражданских сетей IP. Несмотря на то, что емкость сетевых каналов за последние годы значительно возросла, выросли и потоки трафика, порождаемого пользователями, поэтому перегрузки в сети время от времени возникают. Поскольку протоколы маршрутизации и управления на базе IP приобрели важное значение для обеспечения работы Internet, перегрузка каналов вызывает два неприятных явления в сети.

(1) Значительные задержки могут приводить к потере пакетов протоколов маршрутизации. В результате эти протоколы могут принимать ошибочные решения об изменении топологии сети и распространять эту информацию другим маршрутизаторам. Это приведет к нестабильности картины маршрутизации и увеличению нагрузки на маршрутизаторы, которые будут вынуждены обрабатывать дополнительную информацию о фиктивных изменениях топологии.

(2) Значительные задержки могут оказывать влияние на работу систем сетевого управления, которые в результате получения устаревших данных о состоянии сети могут оказывать дополнительное отрицательное воздействие.

Реализация и аккуратное использование механизма предпочтений позволяет решить обе эти проблемы.

5.3.3.1 Управление очередями на основе предпочтений

Маршрутизаторам **следует** реализовать механизм управления очередями на основе предпочтений. Такое управление очередью означает, что при выборе пакетов для передачи в (логический) канал пакеты с более высоким уровнем предпочтения помещаются в очередь первыми. Маршрутизаторы, реализующие механизм управления очередями на основе предпочтений, **должны** также поддерживать конфигурационный параметр, позволяющий отключить такое управление очередями на уровне IP.

Маршрутизатор **может** реализовать другие механизмы управления пропускной способностью на основе правил, которые работают более эффективно, нежели управление очередями на основе предпочтений, но эти механизмы **должны** быть отключаемыми (т. е., вместо них будет использоваться строгое упорядочивание очередей на основе предпочтений).

Как описано в параграфе 5.3.6, маршрутизаторы, реализующие механизм управления очередями на основе предпочтений, в случаях насыщения отбрасывают сначала пакеты с более низким уровнем предпочтения.

Прерывание обработки или передачи пакета не рассматривается как функция уровня IP. Некоторые протоколы других уровней могут поддерживать такие функции.

5.3.3.2 Отображение предпочтений нижележащего уровня

Маршрутизаторы, реализующие управление очередями на основе предпочтений, **должны**, а прочим маршрутизаторам **следует** реализовать отображение предпочтений нижележащего уровня.

Маршрутизаторы, реализующие такое отображение:

- **должны** быть способны отображать значение IP Precedence на приоритет канального уровня в тех случаях, когда последний поддерживает приоритизацию;
- **должны** иметь конфигурационный параметр для выбора используемой по умолчанию трактовки приоритета канального уровня для всего трафика IP;

[1] Министерство обороны США.

- **следует** обеспечивать возможность настройки нестандартного отображения предпочтений IP на значения приоритета канального уровня для каждого интерфейса.

Обсуждение

Некоторые исследования позволяют усомниться в работоспособности функций приоритизации отдельных протоколов канального уровня, а в отдельных сетях могут использоваться содержащие ошибки механизмы приоритизации на канальном уровне. Представляется разумным обеспечить механизм обхода приоритизации на канальном уровне при возникновении проблем в сети.

С другой стороны, имеются предложения по использованию новых стратегий управления очередями (например, резервирование полосы в различных средах или службы с малой задержкой). Специальные службы и стратегии организации очередей для поддержки новых механизмов сейчас исследуются и стандартизуются.

Разработчики могут принимать во внимание, что корректное отображение предпочтений IP на приоритеты канального уровня требуется политикой DOD для систем TCP/IP, используемых в сетях Министерства обороны США. Поскольку эти требования были предназначены для поощрения (а не форсирования) использования механизма предпочтений в надежде на повышение качества сервиса Internet для всех пользователей, маршрутизаторам, поддерживающим управление очередями на основе предпочтений, следует по умолчанию обеспечивать строгое упорядочивание очередей на основе предпочтений, независимо от запрошенного типа обслуживания.

5.3.3.3 Обработка предпочтений для всех маршрутизаторов

Ниже приведены требования к маршрутизаторам (независимо от поддержки управления очередями на основе предпочтений), относящиеся к обработке предпочтений.

(1) **Должны** принимать и обрабатывать входящий трафик для всех уровней предпочтения, пока заданная администратором политика не требует иного.

(2) **Могут** реализовать фильтр для административного ограничения уровней предпочтения, используемых некоторыми источниками трафика. При наличии такого фильтра для него **недопустима** фильтрация сообщений ICMP об ошибках Destination Unreachable, Redirect, Time Exceeded и Parameter Problem. Для поддержки такого фильтра требуются также процедуры фильтрации пакетов по адресам.

Обсуждение

Фильтрацию по уровню предпочтения следует применять к заданным парам IP-адресов (отправитель-получатель), протоколам, портам и т. п.

Когда пакет отбрасывается фильтром, **следует** передавать отправителю сообщение ICMP Destination Unreachable с кодом 14, если генерация таких сообщений не отключена с помощью конфигурационных параметров.

(3) **Могут** реализовать функцию ограничения, которая позволяет установить на маршрутизаторе политику, отвергающую или отбрасывающую трафик с уровнем предпочтения ниже заданного. Эта функция может активизироваться административным путем или с помощью эвристических методов, но всегда **должна** поддерживаться опция для запрета всех эвристических механизмов, которые работают без участия человека. При отбрасывании пакетов функцией ограничения **следует** генерировать сообщения ICMP Destination Unreachable с кодом 15, если такая генерация не отключена с помощью конфигурационных параметров.

Для маршрутизатора **недопустимо** отвергать пересылку дейтаграмм с полем предпочтения 6 (Internetwork Control) или 7 (Network Control) на основании лишь ограничения по уровню предпочтения. Однако в комбинации с другими критериями уровень предпочтения может использоваться для ограничения трафика даже с высокими уровнями предпочтения.

Обсуждение

Неограниченная фильтрация по уровню предпочтения может привести к отсечению трафика протоколов маршрутизации и сетевого управления. В общем случае для хостов следует ограничивать трафик по уровню предпочтения 5 (CRITIC/ECP) или ниже, но в некоторых системах такое требование может оказаться неприменимым.

(4) **Недопустимо** изменение уровня предпочтения для пакетов, источником которых данный маршрутизатор не является.

(5) **Следует** обеспечивать возможность настройки различных уровней предпочтения для каждого поддерживаемого протокола маршрутизации и управления (за исключением протоколов типа OSPF, которые самостоятельно устанавливают уровень предпочтения).

(6) **Допускается** настройка предпочтений для протоколов маршрутизации или управления независимо на каждом интерфейсе.

(7) Маршрутизаторы д**олжны** подобающим образом реагировать на индикацию ошибок, связанных с предпочтениями на канальном уровне, если такая индикация обеспечивается. При отбрасывании пакета по причине невозможности его передачи в канал в результате связанных с предпочтениями условий, **следует** генерировать сообщение ICMP Destination Unreachable с кодом 15, если такая генерация не отключена с помощью параметров конфигурации.

Обсуждение

Описанный в (3) механизм ограничения на основе уровня предпочтений является в некоторой степени спорным. В зависимости от топологического места расположения точки реализации ограничения транзитный трафик может быть направлен протоколами маршрутизации в область ограничения, где этот трафик будет отброшен. В такой ситуации могут возникать проблемы, если между парой обменивающихся данными точек существует также путь без ограничений по уровню предпочтения. Предложенный способ решения этой проблемы включает обеспечение некой минимальной пропускной способности для всех уровней предпочтения даже в условиях перегрузки или распространение сведений об ограничении трафика по уровню предпочтения с помощью протоколов маршрутизации. В силу отсутствия общепринятого (и реализованного) решения этой проблемы рекомендуется с осторожностью относиться к использованию ограничений по уровню предпочтения в транзитных сетях.

На транспортном уровне может легитимно выполняться функция, запрещенная правилом 4 (см. выше). Изменение уровней предпочтения может оказывать влияние на работу TCP и (возможно) других протоколов. Корректная реализация является нетривиальной задачей.

Значение правил (5) и (6) (а также обсуждения IP Precedence в сообщениях ICMP в параграфе 4.3.2) состоит в том, что биты IP precedence следует устанавливать независимо от того, обрабатывает ли их данный маршрутизатор. Предполагается, что в будущих спецификациях протоколов маршрутизации и сетевого управления будут указаны требования по установке битов IP Precedence для сообщений, передаваемых с помощью этих протоколов.

Использование правила (7) зависит от протокола канального уровня. Обычно маршрутизатору следует прервать попытки передачи неприемлемого трафика для данного адресата на некоторый период и возвратить отправителю сообщение ICMP Destination Unreachable с кодом 15 (сервис недоступен для запрошенного уровня предпочтений). В течение некоторого времени также не следует пытаться восстановить прерванное соединение канального уровня.

5.3.4 Пересылка широковещательных пакетов канального уровня

Инкапсуляция пакетов IP для большинства протоколов канального уровня (за исключением PPP) позволяет получателю отличать групповые и широковещательные пакеты от индивидуальных путем простой проверки заголовков канального уровня (обычно адреса канального уровня для получателя). Правила этого параграфа, относящиеся к широковещательным кадрам канального уровня, применимы только к тем протоколам канального уровня, которые позволяют отличать широковещательную адресацию, аналогично и правила для групповых кадров канального уровня относятся лишь к тем протоколам канального уровня, которые позволяют отличать групповую адресацию.

Для маршрутизатора **недопустимо** пересылать любые пакеты, полученные маршрутизатором в широковещательных кадрах канального уровня, если эти пакеты не направлены по групповым адресам IP. В последнем случае предполагается, что использование широковещательной адресации на канальном уровне обусловлено отсутствием эффективного multicast-сервиса.

Для маршрутизатора **недопустимо** пересылать любые пакеты, полученные в групповых кадрах канального уровня, если эти пакеты не направлены по групповым адресам IP.

Маршрутизатору **следует** отбрасывать без уведомления пакеты, полученные в широковещательных кадрах канального уровня и не направленные по широковещательному или групповому адресу IP.

Когда маршрутизатор передает пакет в широковещательном кадре канального уровня, IP-адрес получателя **должен** быть действительным групповым или широковещательным адресом IP.

5.3.5 Пересылка широковещательных пакетов уровня Internet (IP)

Существует два основных типа широковещательных адресов IP - limited broadcast (широковещание ограниченного действия) и directed broadcast (направленное широковещание). Кроме того, существуют три подтипа направленного широковещания - пакеты, направленные в сеть с указанным префиксом, пакеты, направленные в указанную подсеть, и пакеты во все подсети указанной сети. Отнесение маршрутизатором широковещательных пакетов к одной из перечисленных категорий зависит от самого широковещательного адреса и понимания маршрутизатором структуры (если таковая имеется) подсетей сети адресата. Один и тот же широковещательный пакет может по-разному классифицироваться различными маршрутизаторами.

IP-адрес ограниченного широковещания определяется как значение, состоящее только из единиц: { -1, -1 } или 255.255.255.255.

Адрес для широковещания в сеть с указанным префиксом состоит из префикса IP-сети, сопровождаемого локальной частью, содержащей только единицы, или { <Network-prefix>, -1 }. Например, широковещательный адрес для класса A будет иметь вид net.255.255.255, для класса B - net.net.255.255, а для класса C – net.net.net.255, где net задает байты префикса сети.

Направленное широковещание во все подсети (all-subnets-directed-broadcast) не определено в среде CIDR и использование таких адресов запрещено первой версией данного документа.

Как было сказано в параграфе 4.2.3.1, маршрутизатор может сталкиваться с нестандартной широковещательной адресацией IP:

- 0.0.0.0 - устаревшая форма широковещательного адреса ограниченного действия;
- { <Network-prefix>, 0 } - устаревшая форма широковещания, направленного в сеть с указанным префиксом (network-prefix-directed broadcast).

Как было указанно в этом параграфе, пакеты, направленные по любому из этих адресов, **следует** отбрасывать без уведомления, но если отбрасывания не происходит, эти пакеты **должны** трактоваться согласно тем же правилам, которые применяются к пакетам, адресованным с использованием описанных выше современных форм широковещательной адресации. Эти правила рассматриваются в следующих параграфах.

5.3.5.1 Широковещательная адресация ограниченного действия

Пакеты Limited broadcast **недопустимо** пересылать или отбрасывать. Пакеты Limited broadcast **можно** и **следует** передавать взамен directed broadcast, если ограниченного широковещания будет достаточно.

Обсуждение

Некоторые маршрутизаторы включают серверы UDP, которые заново передают (resend) запросы к другим серверам (с использованием индивидуальной или широковещательной адресации). Приведенное выше требование не следует интерпретировать, как запрет на использование таких серверов. Отметим однако, что такие серверы при некорректной настройке могут приводить к возникновению маршрутных петель. Поэтому провайдерам таких серверов нужно подробно и аккуратно описать процедуры настройки, а также рассмотреть вопрос об уменьшении значения TTL в передаваемых такими серверами пакетах.

5.3.5.2 Направленное широковещание

Маршрутизатор **должен** классифицировать, как направленные в указанную префиксом сеть широковещательные пакеты (Network-Prefix-Directed broadcast), все корректные пакеты directed broadcast, адресованные в удаленную сеть или непосредственно подключенную сеть, не разделенную на подсети. Отметим, что в CIDR такой адрес представляется адресом хоста в сети, заданной префиксом; мы устраняем проверку связанной с хостом части сетевого префикса. Поскольку задан маршрут и нет правил его отмены, маршрутизатор **должен** пересылать пакеты Network-Prefix-Directed broadcast. Маршрутизатор **может** передавать пакеты Network-Prefix-Directed broadcast.

Маршрутизатор **может** поддерживать опцию для запрета приема пакетов network-prefix-directed broadcast для интерфейса и **должен** иметь опцию для запрета пересылки пакетов network-prefix-directed broadcast. По умолчанию эти опции **должны** разрешать прием и пересылку широковещательных пакетов, адресованных в сеть с указанным префиксом[1].

Обсуждение

Вопрос о пересылке или отказе от пересылки пакетов directed broadcast является в некоторой степени спорным. В данном документе решение о пересылке зависит от наличия у маршрутизатора информации о префиксе сети адресата. Маршрутизатор не может классифицировать сообщение как unicast или directed broadcast, если префикс сети не известен. Возникновение вопроса «пересылать - не пересылать» по определению возможно только на маршрутизаторе последнего интервала пересылки.

5.3.5.3 Широковещательные пакеты во все подсети (All-subnets-directed)

В первой версии этого документа описан алгоритм распределения пакетов directed broadcast во все подсети для классического[2] номера сети. Сейчас такая рассылка считается «нарушением» и известны некоторые случаи отказов алгоритма.

В домене маршрутизации CIDR, где классические номера сетей IP не имеют смысла, концепция all-subnets-directed-broadcast (широковещательная передача во все подсети) также лишена смысла. По имеющейся у рабочей группы информации такой алгоритм рассылки ни разу не был реализован на практике и сейчас его можно рассматривать как достояние истории.

5.3.5.4 Широковещание, направленное в подсеть

В первой версии документа рассматривались процедуры обработки широковещательных пакетов, направленных в подсеть (subnet-directed-broadcast). В домене маршрутизации CIDR такие пакеты невозможно отличить от широковещательной передачи в сеть (net-drected-broadcast). Следовательно, такие пакеты должны трактоваться в соответствии с параграфом 5.3.5.2, как network-prefix directed broadcast.

5.3.6 Контроль насыщения

Перегрузка в сети определяется как условия, когда запросы на выделение ресурсов (обычно полосы каналов или процессорного времени) превосходят реальные возможности. Механизмы предотвращения насыщения пытаются исключить возникновение таких ситуаций, а механизмы восстановления после перегрузки пытаются возобновить нормальную работу сети. Маршрутизаторы могут вносить свой вклад в работу обоих механизмов. На изучение проблем нехватки ресурсов было потрачено много сил. Рекомендуем читателям ознакомиться с документом [FORWARD:2], в котором приводится обзор работ в этом направлении. Важную информацию по вопросам насыщения содержат [FORWARD:3], [FORWARD:4], [FORWARD:5], [FORWARD:10], [FORWARD:11], [FORWARD:12], [FORWARD:13], [FORWARD:14], [INTERNET:10], а также ряд других работ.

Объем памяти, которая должна быть доступна на маршрутизаторе для обслуживания запросов при пиковой нагрузке, когда хосты используют подходящую политику контроля насыщения (например, описанную в [FORWARD:5]), является функцией от произведения полосы канала на величину задержки для использующего канал пути. Следовательно, объем памяти должен увеличиваться с ростом произведения Bandwidth*Delay. Точная функция, связывающая объем памяти с вероятностью отбрасывания пакетов при насыщении, неизвестна.

Когда маршрутизатор получает пакет, который требует выделения отсутствующей уже памяти, он должен (по определению, а не по декрету) отбросить этот или какой-то другой (другие) пакет. Выбор отбрасываемого пакета требует дополнительных исследований. Наиболее разумным на сегодняшний день решением является отбрасывание пакета из потока данных, который наиболее сильно загружает канал. Однако здесь могут играть роль и другие факторы, включая уровни предпочтения, активное резервирование полосы и сложности, связанные с выбором пакета.

Маршрутизатор **может** отбросить только что полученный пакет - такое решение является простейшим, но отнюдь не лучшим. Идеальным решением будет выбор для отбрасывания пакета одной из наиболее загружающих канал сессий с учетом правил QoS[3]. Рекомендуемой политикой в среде дейтаграмм, использующей очереди FIFO, является отбрасывание пакетов, случайно выбранных из очереди (см. [FORWARD:5]). Эквивалентным алгоритмом для маршрутизаторов, использующих взвешенные очереди, будет выбор пакета из самой длинной очереди или той очереди, которая использует наибольшее виртуальное время (см. [FORWARD:13]). Маршрутизатор **может** использовать эти алгоритмы для выбора отбрасываемого пакета.

Если маршрутизатор использует политику отбрасывания (например, Random Drop[4]), в соответствии с которой он выбирает отбрасываемый пакет из некоторого пула подходящих пакетов:

- при упорядочивании очереди по уровню предпочтений (см. параграф 5.3.3.1) для маршрутизатора **недопустимо** отбрасывание пакета, для которого уровень предпочтения в заголовке IP выше, чем у какого-либо из остающихся пакетов;

---

[1] В RFC 2644 этот абзац выражен в иной формулировке: «Маршрутизатор **может** иметь опцию, разрешающую прием широковещательных пакетов для заданной префиксом сети (network-prefix-directed broadcast) на уровне интерфейсов и **может** иметь опцию для разрешения пересылки таких пакетов. Эти опции по умолчанию **должны** быть отключены, чтобы блокировать прием и передачу пакетов network-prefix-directed broadcast.» *Прим. перев.*

[2] Не CIDR. *Прим. перев.*

[3] Quality of Service - качество обслуживания.

[4] Случайный выбор пакета для отбрасывания.

- маршрутизатор **может** может защитить от отбрасывания пакеты, в которых заголовок IP запрашивает TOS для максимальной надежности, за исключением тех случаев, когда такая защита будет нарушать предыдущее правило;

- маршрутизатор **может** защитить от отбрасывания фрагментированные пакеты IP, основываясь на теории о том, что отбрасывание фрагмента дейтаграммы может повысить уровень перегрузки за счет того, что отправитель будет повторно передавать все фрагменты;

- чтобы предотвратить возмущения маршрутизации и нарушение работы функций управления, маршрутизатор **может** обеспечить защиту от отбрасывания для пакетов, используемых для контроля маршрутизации, управления каналами и сетью; для выделенных маршрутизаторов (т. е., маршрутизаторов, которые не используются одновременно в качестве хостов, терминальных серверов и т. п.) можно реализовать это правило путем запрета отбрасывания пакетов, в которых адрес отправителя или получателя относится к самому маршрутизатору.

Прогрессивные методы контроля насыщения включают «понятие беспристрастности», в соответствии с которым «пользователь», наказываемый отбрасыванием пакетов, является одним из тех, кто вносит наибольший вклад в создание насыщения. Независимо от механизма, используемого для контроля за насыщением полосы, важно обеспечить достаточно низкий уровень загрузки процессора в маршрутизаторе, чтобы не возникало насыщения производительности процессора.

Как описано в параграфе 4.3.3.3, этот документ **не рекомендует** маршрутизаторам передавать сообщений Source Quench отправителям отброшенных пакетов. Механизм ICMP Source Quench весьма малоэффективен и нет нужды использовать его в маршрутизаторах, а хостам не следует активно применять этот механизм для индикации насыщения.

5.3.7 Фильтрация непригодных адресов

IP-адрес отправителя является непригодгым, если он относится к числу специальных адресов IP, указанных в параграфах 4.2.2.11 и 5.3.7, или не является индивидуальным адресом.

IP-адрес получателя является непригодгым, если он относится к тем адресам, которые указаны, как недопустимые для получателя в параграфе 4.2.3.1, или адресам класса E (за исключением 255.255.255.255).

Маршрутизатору **не следует** пересылать никаких пакетов, которые содержат непригодгым адрес отправителя или отправитель относится к сети 0. Маршрутизатору **не следует** пересылать любые пакеты, исходящие из сети 127 (за исключением пакетов, передаваемых через интерфейс loopback). Маршрутизатор **может** поддерживать параметр, который позволяет администратору отключать такие проверки, но по умолчанию эти проверки **должны** выполняться.

Маршрутизатору **не следует** пересылать какие-либо пакеты, в которых указан непригодгым адрес получателя, или пакеты, направленные в сеть 0. Маршрутизатору **не следует** пересылать какие-либо пакеты, адресованные в сеть 127, за исключением пакетов, пересылаемых через интерфейс loopback. Маршрутизатор **может** иметь параметр, который позволяет администратору отключить такие проверки, но по умолчанию эти проверки **должны** выполняться.

Если маршрутизатор отбрасывает пакет в соответствии с приведенными здесь правилами, ему **следует** записать в системный журнал по крайней мере IP-адреса отправителя и получателя и если проблема связана с адресом отправителя, физический интерфейс, через который поступил пакет, и адрес канального уровня для хоста или маршрутизатора, от которого был принят пакет.

5.3.8 Проверка адреса отправителя

Маршрутизаторам **следует** поддерживать возможность фильтрации трафика на основе сравнения адреса отправителя в пакете и таблицы пересылки для логического интерфейса, через который пакет был получен. Если такая фильтрация разрешена, маршрутизатор **должен** отбрасывать пакет без уведомления, если он был принят через интерфейс, отличающийся от того, через который будет пересылаться пакет, направленный по адресу отправителя. Иными словами, если маршрутизатор не будет пересылать пакет, содержащий данный адрес, через определенный интерфейс, ему не следует доверять этому адресу, указанному в поле отправителя, для пакета, поступившего через тот же интерфейс.

Если такая фильтрация реализована в маршрутизаторе, она **должна** быть отключена по умолчанию.

Обсуждение

Такая фильтрация может повышать уровень безопасности в некоторых случаях, но она приведет к ненужному отбрасыванию пакетов в случае использования асимметричных путей, когда прием и передача могут происходить через разные интерфейсы маршрутизатора.

5.3.9 Фильтрация пакетов и списки доступа

Для обеспечения безопасности и ограничения трафика через определенные части сети маршрутизаторам **следует** поддерживать возможность селективной пересылки (фильтрации) пакетов. Если такие фильтры реализованы в маршрутизаторе, **следует** также обеспечить возможность настройки их конфигурации на пересылку всех пакетов или селективную пересылку на основе сетевых префиксов отправителей и получателей. **Возможна** также фильтрация пакетов на основе других атрибутов. Для каждого адреса отправителя или получателя **следует** обеспечивать возможность указания любого размера префикса.

Обсуждение

Функции фильтрации пакетов позволяют запретить доступ внешних хостов к внутренней сети с использованием определенных протоколов или ограничить обмен данными между некоторыми хостами. Фильтры также позволяют предотвратить некоторые типы нарушений защиты, когда внешние хосты пытаются замаскировать себя под внутренние.

Если маршрутизатор поддерживает фильтрацию, ему **следует** обеспечивать возможность создания хотя бы одного списка доступа из перечисленных ниже:

- включенные (Include) - список определений, в соответствии с которым сообщения будут пересылаться;

- исключенные (Exclude) - список определений, в соответствии с которым сообщения **не** будут пересылаться.

«Определение» в данном контексте включает префиксы адресов отправителей/получателей и может также включать другие параметры (например, тип протокола IP или номер порта TCP).

Маршрутизатор **может** поддерживать конфигурационные параметры для выбора между списком включенных/исключенных или эквивалентные средства управления фильтрацией.

Для адресов отправителей/получателей **должно** поддерживаться значение (например, any - любой, адрес с маской, содержащей только нули, или префикс нулевой длины), которому будут соответствовать любые адреса.

В дополнение к адресным парам маршрутизатор **может** поддерживать фильтрацию на основе произвольных комбинаций протоколов транспортного и/или прикладного уровня, а также номеров портов отправителей и получателей.

Маршрутизатор **должен** разрешать отбрасывание пакетов без уведомления (т. е., без передачи сообщений ICMP).

Маршрутизаторам **следует** обеспечивать возможность передачи соответствующих сообщений ICMP о недоступности при отбрасывании пакетов. В сообщениях ICMP **следует** указывать Communication Administratively Prohibited (код 13) в качестве причины недоступности адресата.

Маршрутизаторам **следует** обеспечивать возможность настройки передачи сообщений ICMP о недоступности адресата (код 13) для каждой комбинации адресных пар, типа протокола и номера порта.

Маршрутизатору **следует** вести учет отбрасываемых пакетов, а также **следует** обеспечивать возможность записи в журнальные файлы информации об отдельных пакетах, которые не были пересланы.

5.3.10 Групповая маршрутизация

Маршрутизаторам IP **следует** поддерживать пересылку групповых пакетов IP на основе статических таблиц групповой маршрутизации или динамических маршрутов, полученных от протоколов групповой маршрутизации (например, DVMRP [ROUTE:9]). Маршрутизаторы, поддерживающие пересылку групповых пакетов IP, называют multicast-маршрутизаторами.

5.3.11 Управление пересылкой

Для каждого физического интерфейса маршрутизатору **следует** поддерживать конфигурационный параметр, позволяющий отключать пересылку пакетов через данный интерфейс. При отключенной для интерфейса пересылке:

- маршрутизатор **должен** отбрасывать без уведомления все пакеты, полученные через данный интерфейс, но не адресованные самому маршрутизатору;
- **недопустимо** передавать пакеты через этот интерфейс за исключением пакетов, созданных самим маршрутизатором;
- **недопустимо** анонсировать с помощью любых протоколов маршрутизации доступность путей через этот интерфейс.

Обсуждение

Эта функция позволяет администратору отключить сетевой интерфейс маршрутизатора, сохранив при этом возможность его использования для управления сетью.

В идеальном случае эта функция применяется к логическим, а не физическим интерфейсам. Однако реализация такого подхода невозможна, поскольку не существует способа определить, через какой логический интерфейс был принят пакет, за исключением случаев взаимно-однозначного соответствия между логическими и физическими интерфейсами.

5.3.12 Смена состояний

В процессе работы маршрутизатора интерфейсы могут утрачивать и восстанавливать работоспособность, их может отключать и снова включать администратор. Кроме того, пересылка пакетов может быть запрещена или разрешена после запрета для отдельного интерфейса или маршрутизатора в целом. Хотя такие смены состояния происходят достаточно редко, они играют важную роль в обеспечении корректной работы маршрутизатора.

5.3.12.1 Прекращение пересылки

Когда маршрутизатор прекращает пересылку пакетов, он должен прекратить анонсирование всех маршрутов, за исключением путей, полученных от других маршрутизаторов. Маршрутизатор **может** продолжать прием и использование маршрутов от других маршрутизаторов в своем домене маршрутизации. Если маршрутная база данных сохраняется, для маршрутизатора **недопустимо** прекращать учет времени для хранящихся в базе маршрутных записей. Если маршрутизатор запоминает маршруты, полученные от других маршрутизаторов, для этих маршрутов **недопустимо** прекращение учета времени. Маршрутизатор **должен** отбрасывать любые маршруты, для которых истекло время, как это делается при включенной пересылке.

Обсуждение

Когда маршрутизатор прекращает пересылку, он перестает быть маршрутизатором. Продолжая оставаться хостом, он должен соответствовать требованиям документа Host Requirements [INTRO:2]. Однако маршрутизатор может оставаться пассивным участником одного или нескольких доменов маршрутизации. Поэтому маршрутизатор может продолжать поддержку базы данных о маршрутах, прослушивая другие маршрутизаторы в своем домене маршрутизации. Однако в таких случаях маршрутизатор не имеет права анонсировать какие-либо маршруты из своей таблицы, поскольку он не поддерживает пересылку пакетов. Единственным исключением из этого правила является анонсирование маршрута, который использует только другой маршрутизатор, по запросу последнего.

Маршрутизатор **может** передавать сообщения ICMP о недоступности адресатов отправителям пакетов, которые данный маршрутизатор не может переслать. Маршрутизатору **не следует** передавать сообщений ICMP redirect.

Обсуждение

Отметим, что передача сообщений ICMP о недоступности адресата является прерогативой маршрутизаторов (эти сообщения не передаются хостами). Приведенное выше правило является исключением из правил для хостов и

предназначено для обеспечения возможности изменения картины маршрутизации пакетов в кратчайшие сроки во избежание возникновения «черной дыры».

5.3.12.2 Начало пересылки

Когда маршрутизатор начинает пересылку пакетов, ему **следует** ускорить передачу новой маршрутной информации всем маршрутизаторам, с которыми он обычно обменивается маршрутными данными.

5.3.12.3 Интерфейс отключен или произошел отказ

При отказе или отключении интерфейса маршрутизатор **должен** удалить все связанные с этим интерфейсом маршруты из своей таблицы и прекратить анонсирование этих маршрутов. Маршрутизатор **должен** также отключить все статические маршруты, которые могут использовать данный интерфейс. Если маршрутизатору известны другие маршруты для того же адресата и TOS, он **должен** выбрать из них лучший путь и добавить его в свою таблицу маршрутизации. Маршрутизатору **следует** передавать сообщения ICMP destination unreachable или ICMP redirect в ответ на все пакеты, которые он не может переслать по причине недоступности интерфейса.

5.3.12.4 Интерфейс включен

При включении недоступного ранее интерфейса маршрутизатор **должен** заново включить все связанные с этим интерфейсом статические маршруты. Если маршруты, которые будут использовать этот интерфейс, становятся известны маршрутизатору, эти маршруты **должны** быть оценены в сравнении со всеми другими известными маршрутизатору путями и маршрутизатор **должен** принять решение о выборе пути для включения в свою таблицу маршрутизации. Разработчикам следует использовать рекомендации раздела «7. Прикладной уровень - протоколы маршрутизации» для реализации механизма выбора маршрута.

Маршрутизатору следует ускорить передачу новых маршрутных данных всем маршрутизаторам, с которыми он обычно обменивается такой информацией.

5.3.13 Опции IP

Некоторые опции (такие, как Record Route и Timestamp), включают «гнезда», куда маршрутизатор записывает свой адрес при пересылке пакета. Однако каждая такая опция имеет ограниченное пространство «гнезд» и маршрутизатор может столкнуться с проблемой отсутствия свободного места в опции для записи своего адреса. Ни одно из перечисленных ниже требований не следует трактовать как необходимость записи адреса в опцию при отсутствии в ней свободного места. В параграфе 5.2.5 обсуждается вопрос выбора маршрутизатором адреса для записи в опцию.

5.3.13.1 Неизвестные опции

Нераспознанные маршрутизатором опции IP в пересылаемых пакетах **должны** передаваться без изменений.

5.3.13.2 Опция безопасности (Security)

Некоторые среды требуют наличия опции Security в каждом пакете, такие требования выходят за пределы данного документа и спецификации стандарта IP. Отметим однако, что опции безопасности, описанные в документах [INTERNET:1] и [INTERNET:16], устарели. В маршрутизаторах **следует** реализовать поддержку обновленной опции безопасности, которая описана в [INTERNET:5].

Обсуждение

Маршрутизаторы, предназначенные для использования в сетях со множеством уровней защиты, должны поддерживать фильтрацию пакетов на основе меток IPSO (RFC 1108). Для реализации этого маршрутизатор должен позволять администратору задавать нижний (например, Unclassified – не классифицируется) и верхний (например, Secret - секретно) предел для каждого интерфейса. Достаточно часто (но не всегда) значения пределов могут совпадать (например, интерфейс с одним уровнем). Пакеты, которые фильтр IPSO классифицировал, как выходящие за пределы заданного диапазона, следует отбрасывать без уведомления, следует также поддерживать счетчик таких отброшенных пакетов.

5.3.13.3 Опция идентификатора потока (Stream Identifier)

Эта опция устарела. При наличии опции Stream Identifier в пересылаемом пакете маршрутизатор **должен** игнорировать ее и передавать без изменений.

5.3.13.4 Опции Source Route

Маршрутизаторы **должны** реализовать поддержку опции source route в пересылаемых пакетах. Маршрутизатор **может** иметь конфигурационный параметр, включающий отбрасывание всех пакетов с опцией source route, однако **недопустимо** такое отбрасывание по умолчанию.

Обсуждение

Возможность задания отправителем маршрута передачи дейтаграмм через Internet имеет важное значение для некоторых средств диагностики сетей. Однако заданная отправителем маршрутизация может использоваться для обхода установленных администратором правил и политики безопасности. В частности, системы, где для административного разделения используются манипуляции с таблицами маршрутов вместо других методов (таких, как фильтрация пакетов), могут быть уязвимы при использовании пакетов с опцией source route.

Комментарии редактора

Системы фильтрации пакетов могут быть обмануты с помощью заданной отправителем маршрутизации на всех маршрутизаторах за исключением последнего на пути source route. Ни маршруты, ни фильтры сами по себе не обеспечивают полной защиты.

5.3.13.5 Опция записи маршрута (Record Route)

Маршрутизаторы **должны** поддерживать опцию записи маршрута (Record Route) для пересылаемых пакетов.

Маршрутизатор **может** поддерживать конфигурационный параметр, который будет заставлять маршрутизатор игнорировать опции Record Route в пересылаемых пакетах. При наличии такого параметра по умолчанию опция записи маршрута **должна** обрабатываться маршрутизатором. Этот параметр не должен оказывать влияния на обработку

опций Record Route в пакетах, полученных самим маршрутизатором (в частности, опция Record Route в запросах ICMP echo должна по-прежнему обрабатываться в соответствии с параграфом 4.3.3.6).

Обсуждение

Некоторые люди полагают, что опция Record Route ведет к снижению уровня безопасности, поскольку она раскрывает информацию о топологии сети. Данный документ позволяет отключить на маршрутизаторе обработку опции.

5.3.13.6 Опция Timestamp

Маршрутизаторы **должны** поддерживать в пересылаемых пакетах опцию timestamp (временная метка). Значение метки **должно** соответствовать правилам, указанным в документе [INTRO:2].

Если поле флагов имеет значение 3 (timestamp и указанный заранее адрес), маршрутизатор **должен** добавить свою временную метку, если указанный следующим адрес соответствует какому-либо из IP-адресов маршрутизатора. Не обязательно совпадение указанного адреса с адресом получившего пакет интерфейса или интерфейса, через который пакет будет передаваться.

Реализация

В целях более эффективного использования временных меток в поле timestamp предлагается включать в эту опцию время, максимально близкое к моменту получения дейтаграммы маршрутизатором. Для дейтаграмм, созданных маршрутизатором, значение временной метки должно быть максимально близким к моменту передачи дейтаграммы сетевому уровню для ее отправки.

Маршрутизатор **может** поддерживать конфигурационный параметр, который будет приводить к игнорированию опции Timestamp в пересылаемых дейтаграммах, когда слово флагов имеет значение 0 (только временная метка) или 1 (временная метка и зарегистрированный адрес IP). При поддержке маршрутизатором такого параметр последний **должен** быть отключен по умолчанию (т. е., маршрутизатор не должен игнорировать опцию timestamp). Этот параметр не должен влиять на обработку опций Timestamp в дейтаграммах, полученных самим маршрутизатором (в частности, опции Timestamp в адресованных маршрутизатору дейтаграммах и запросах ICMP будут по-прежнему обрабатываться в соответствии с параграфом 4.3.3.6).

Обсуждение

Подобно опции Record Route опция Timestamp может раскрывать информацию о топологии сети. Некоторые люди считают это небезопасным.

6. Транспортный уровень

От маршрутизаторов не требуется реализации протоколов транспортного уровня за исключением тех протоколов, которые нужны для работы поддерживаемых маршрутизатором протоколов прикладного уровня. На практике это означает, что большинство маршрутизаторов поддерживает протоколы TCP и UDP.

6.1 Протокол UDP

Спецификация протокола UDP сдержится в документе [TRANS:1].

Маршрутизатор, поддерживающий протокол UDP, **должен** быть совместимым со спецификацией и **следует** делать маршрутизаторы безусловно совместимыми с требованиями [INTRO:2], за исключением перечисленных ниже случаев.

- Эта спецификация не задает интерфейса между протоколами различных уровней. Таким образом, от интерфейсов маршрутизаторов не требуется соответствия требованиям [INTRO:2] за исключением тех, выполнение которых связано с корректностью работы поддерживаемых маршрутизатором протоколов прикладного уровня.

- В отличие от требований документа [INTRO:2] приложениям **не следует** отключать генерацию контрольных сумм UDP.

Обсуждение

Хотя отдельные протоколы прикладного уровня могут требовать наличия контрольной суммы UDP в принимаемых дейтаграммах UDP, общего требования наличия контрольной суммы UDP в дейтаграммах UDP не выдвигается. Естественно, что при наличии в дейтаграмме контрольной суммы UDP последняя должна проверяться и при несоответствии дейтаграмма должна отбрасываться.

6.2 Протокол TCP

Спецификация протокола TCP содержится в документе [TRANS:2].

Маршрутизатор, поддерживающий протокол TCP, **должен** быть совместимым со спецификацией и **следует** делать маршрутизаторы безусловно совместимыми с требованиями [INTRO:2], за исключением перечисленных ниже случаев.

- Эта спецификация не задает интерфейса между протоколами различных уровней. Таким образом, от маршрутизаторов не требуется соответствия требованиям [INTRO:2] за исключением тех, выполнение которых связано с корректностью работы поддерживаемых маршрутизатором протоколов прикладного уровня.

  Использование флага Push - *RFC 793, параграф 2.8*

  Передача полученного флага PSH на прикладной уровень является **необязательной**.

  Urgent Pointer - *RFC 793, параграф 3.1*

  Уровень TCP **должен** уведомлять (асинхронно) прикладной уровень при получении указателя важности (Urgent) в отсутствие данных, помеченных ранее, как важные, или в тех случаях, когда указатель важности относится к более ранним данным в потоке. **Должен** обеспечиваться способ, с помощью которого приложения могут получить информацию о количестве важных данных, которые нужно прочесть из соединения, или, по крайней мере, определить наличие непрочитанных важных данных.

TCP Connection Failures (отказы в соединениях)

Приложение **должно** обеспечивать возможность установки значения для R2 в отдельном соединении. Например, интерактивное приложение может установить для R2 бесконечное значение, дающее пользователю возможность разрыва соединения.

TCP Multihoming (многодомные хосты)

Если приложение на многодомном хосте не задает локальный адрес IP при активном открытии соединения TCP, уровень TCP **должен** запросить у уровня IP выбор локального адреса IP до передачи (первого) пакета SYN. См. описание функции GET_SRCADDR() в параграфе 3.4 документа [INTRO:2].

Опции IP

Приложение **должно** обеспечивать возможность задания опции source route, когда оно активно открывает соединение TCP, и **должно** принять значение уровня предпочтения из опции source route, полученной в дейтаграмме.

- По аналогичным причинам от маршрутизаторов не требуется соответствия любому из требований [INTRO:2].

- Требования, касающиеся опции Maximum Segment Size в [INTRO:2], следует трактовать следующим образом: маршрутизатор, поддерживающий связанную с хостами часть MTU (см. параграф 4.2.3.3 настоящего документа), использует по умолчанию SendMSS=536 только в тех случаях, когда неизвестно значение path MTU, при известном path MTU значение SendMSS = path MTU - 40.

- Требования, касающиеся опции Maximum Segment Size в [INTRO:2], следует трактовать следующим образом: сообщения ICMP Destination Unreachable с кодами 11 и 12 указывают на дополнительные программные ошибки. Поэтому такие сообщения **недопустимо** использовать в качестве причины для разрыва соединений TCP.

Обсуждение

Следует отметить, что реализация TCP в маршрутизаторах должна соответствовать следующим требованиям [INTRO:2]:

- обеспечивать настраиваемое значение TTL [Time to Live: RFC 793, параграф 3.9];
- обеспечивать интерфейс для настройки поведения keep-alive (если пакеты keep-alive применяются [TCP Keep-Alive];
- обеспечивать механизм передачи сообщений об ошибках и возможность управления этим механизмом [Asynchronous Reports];
- обеспечивать возможность выбора типа обслуживания [Type-of-Service].

Общая парадигма заключается в том, что тот или иной интерфейс должен соответствовать всем предъявляемым к интерфейсам требованиям, если он виден за пределами маршрутизатора. Например, если маршрутизатор поддерживает протокол telnet, он будет генерировать трафик, передаваемый через внешние сети. Следовательно, маршрутизатор должен обеспечивать возможность задания типа обслуживания, обеспечивающего корректную работу протокола telnet.

7. Прикладной уровень - протоколы маршрутизации

7.1 Введение

В силу технических, административных и политических причин система маршрутизации Internet состоит из двух компонент - внутренняя и внешняя маршрутизация. Концепция автономной системы (AS), как определено в параграфе 2.2.4, играет ключевую роль в разделении внутренней и внешней маршрутизации. Эта концепция позволяет обозначить набор маршрутизаторов, где происходит переход от внутренней маршрутизации к внешней. Дейтаграмма IP может проходить через маршрутизаторы двух и более AS на пути к адресату и автономные системы должны обеспечивать друг друга топологической информацией, позволяющей организовать пересылку дейтаграмм. Протоколы внутренней маршрутизации (Interior gateway protocol или IGP) служат для распространения маршрутной информации внутри AS (для маршрутизации внутри AS), а протоколы внешней маршрутизации (Exterior gateway protocol или или EGP) служат для обмена маршрутной информацией между AS (маршрутизации между автономными системами).

7.1.1 Вопросы безопасности маршрутизации

Маршрутизация является одним из немногих мест, где либеральное отношение (Robustness Principle) к принимаемой информации неприменимо. Маршрутизаторам следует быть достаточно строгими по отношению к маршрутной информации, принимаемой от других систем маршрутизации.

Маршрутизатору **следует** обеспечивать возможность ранжирования источников маршрутной информации по уровню доверия к ним. Такое ранжирование неявно присутствует в модели маршрутизации с транзитными и тупиковыми AC, использующей EGP и различные протоколы внутренней маршрутизации. Важность такого ранжирования возрастает при переходе к централизованному ядру с высоким уровнем доверия.

Маршрутизатору **следует** обеспечивать механизм фильтрации маршрутов, которые явно не являются пригодными (например, маршрутов в сеть 127).

По умолчанию для маршрутизаторов **недопустимо** распространение маршрутных данных, которые этот маршрутизатор не использует сам, не доверяет или считает непригодными. В редких случаях может потребоваться распространение информации, вызывающей подозрения, и такое распространение следует использовать только при прямом участии человека.

Маршрутизаторам следует быть хоть немного параноиками при решении вопросов о восприятии маршрутных данных из любого источника, особая осторожность требуется при распространении полученной из других источников информации. Более конкретные рекомендации приводятся ниже.

7.1.2 Предпочтения

За исключением тех случаев, когда спецификации конкретных протоколов маршрутизации явно указывают иное, маршрутизаторам **следует** устанавливать в поле IP Precedence генерируемых маршрутизатором дейтаграмм IP с маршрутной информацией значение 6 (INTERNETWORK CONTROL).

Обсуждение

Трафик протоколов маршрутизации (**за очень редкими исключениями**) следует передавать через сети с максимальным уровнем предпочтения. Если маршрутная информация не может пройти через систему, картина маршрутизации становится искаженной.

7.1.3 Проверка корректности сообщений

Аутентификация обмена между партнерами включает несколько проверок. Применение паролей и явных списков соседей, от которых могут приниматься данные, обеспечивает повышение устойчивости базы данных о маршрутах. Маршрутизаторам **следует** поддерживать средства управления, обеспечивающие возможность явного создания списка доверенных соседей. Маршрутизаторам **следует** поддерживать аутентификацию обмена с соседями для тех протоколов маршрутизации, которые используются системой.

Маршрутизаторам **следует** проверять своих соседей по адресам отправителей и интерфейсам, через которые поступают сообщения от соседей - для соседей, находящихся в непосредственно подключенной к маршрутизатору подсети, следует ограничивать обмен данными через интерфейсы, ведущие в другие сети. Полученные через другие интерфейсы сообщения **следует** отбрасывать без уведомления.

Обсуждение

Указанные здесь проверки позволяют предотвратить угрозы безопасности и возникновение различных проблем с маршрутизацией.

7.2 Протоколы внутренней маршрутизации

7.2.1 Введение

Протоколы внутренней маршрутизации IGP используются для распространения маршрутной информации между маршрутизаторами одной автономной системы (AS). Независимо от используемого для реализации конкретного IGP алгоритма, он должен обеспечивать выполнение следующих функций:

(1) быстрая реакция на изменения внутренней топологии AS;

(2) наличие механизма, позволяющего предотвратить постоянное изменение маршрутизации в результате смены состояния отдельных устройств;

(3) обеспечивать быстрое схождение (конвергенцию) для свободной от петель маршрутизации;

(4) минимальный расход полосы;

(5) поддержка равноценных маршрутов для распределения нагрузки;

(6) поддержка механизмов аутентификации для передачи маршрутных обновлений.

Используемые сегодня протоколы IGP можно разделить на протоколы, основанные на алгоритмах distance-vector (вектор удаленности) и link-state (состояние канала).

Ниже подробно рассматривается несколько IGP, включая наиболее распространенные и перспективные протоколы. В сети Internet используется также множество других протоколов внутридоменной маршрутизации.

Маршрутизатор, поддерживающий любой протокол маршрутизации (отличный от статических маршрутов), **должен** поддерживать протокол OSPF (см. параграф 7.2.2). Маршрутизатор **может** также поддерживать дополнительные протоколы IGP.

7.2.2 Протокол OSPF

Протоколы маршрутизации на основе выбора кратчайшего пути (Shortest Path First или SPF) представляют собой класс алгоритмов выбора пути с учетом состояния каналов, основанных на алгоритме Dijkstra. Хотя протоколы на основе SPF использовались еще в сети ARPANET, они лишь сравнительно недавно приобрели популярность в средах IP и OSI. В системах на основе SPF каждый маршрутизатор получает полную информацию о топологии в процессе лавинной рассылки, обеспечивающей гарантированную доставку данных. После получения информации каждый маршрутизатор использует алгоритм SPF для построения таблицы маршрутизации IP. Протокол маршрутизации OSPF является одной из реализаций алгоритма SPF. Современная версия протокола OSPF v2 описана в документе [ROUTE:1]. Отметим, что документ RFC 1131, в котором содержится спецификация первой версии протокола OSPF, утратил силу.

Отметим, что для выполнения требований параграфа 8.3 маршрутизаторы, поддерживающие протокол OSPF, **должны** поддерживать также OSPF MIB [MGT:14].

7.2.3 Протокол обмена между промежуточными системами - DUAL IS-IS

Комитет ANSI[1] X3S3.3 разработал протокол внутридоменной маршрутизации, получивший название Intermediate System to Intermediate System Routeing Exchange Protocol[2].

Применение этого протокола в сетях IP описано в документе [ROUTE:2], где протокол назван Dual IS-IS (иногда его называют Integrated IS-IS). Протокол IS-IS основан на алгоритме SPF и обладает всеми преимуществами этого класса протоколов.

[1] American National Standards Institute - Национальный институт стандартов США.
[2] Протокол обмена маршрутной информацией между промежуточными системами.

7.3 Протоколы внешней маршрутизации

7.3.1 Введение

Протоколы внешней маршрутизации используются для передачи другим AS информации о доступности некого набора сетей, являющегося внутренним по отношению к отдельной автономной системе.

Сфера применения таких протоколов является предметом изучения IETF. Протокол EGP (Exterior Gateway Protocol), описанный в Приложении F.1 традиционно использовался для обмена маршрутной информацией между AS, но сейчас он стал достоянием истории. Протокол BGP[1] лишен множества ограничений и недостатков EGP и быстро приобретает популярность. От маршрутизаторов не требуется реализации протоколов маршрутизации между AS. Однако, если маршрутизатор поддерживает EGP, он также **должен** поддерживать протокол BGP. Хотя протокол RIP (см. параграф Приложение F.2[2]) и не предназначен для внешней маршрутизации, он иногда используется в качестве протокола маршрутизации между AS.

7.3.2 Протокол граничного шлюза BGP

7.3.2.1 Введение

BGP-4 представляет собой протокол маршрутизации между AS, используемый для обмена данными о доступности сетей с другими узлами BGP. Информация для сети включает полный список AS, через которые будет проходить трафик на пути в сеть. Эта информация может использоваться для предотвращения маршрутных петель на пути доставки. Информации достаточно для построения графа связности AS, из которого могут быть исключены маршрутные петли и приняты некоторые решения в части политики на уровне AS.

Протокол BGP определен в документе [ROUTE:4]. Документ [ROUTE:5] описывает использование BGP в Internet и содержит рекомендации для разработчиков. В документах [ROUTE:12] и [ROUTE:13] можно найти дополнительную информацию о протоколе.

В соответствии с требованиями параграфа 8.3 маршрутизатор, поддерживающий протокол BGP, **должен** также поддерживать BGP MIB [MGT:15].

Чтобы охарактеризовать набор решений в части политики, которые могут быть приняты с использованием BGP, следует сфокусироваться на правиле, по которому AS анонсирует в соседние AS только те маршруты, которые данная AS использует сама. Это правило отражает парадигму поэтапной маршрутизации, используемую в сети Internet. Отметим, что некоторые правила могут не поддерживаться этой парадигмой и будут требовать использования иных механизмов (например, задаваемой отправителем маршрутизации - source routing). В частности, BGP не позволяет AS передавать в соседнюю AS трафик в предположении, что та будет пересылать этот трафик по маршруту, отличающемуся от пути для трафика, происходящего из данной AS. С другой стороны, BGP может поддерживать любые правила, согласующиеся с парадигмой поэтапной маршрутизации.

Разработчикам BGP настоятельно рекомендуется строго следовать рекомендациям, приведенным в главе 6 документа [ROUTE:5].

7.3.2.2 Протокол Walk-through

Хотя протокол BGP позволяет реализовать достаточно сложные варианты политики маршрутизации (см., например, параграф 4.2 в [ROUTE:5]), поддержка сложной политики не требуется от всех реализаций BGP. Однако любая реализация BGP должна удовлетворять приведенным ниже требованиям.

(1) **Следует** позволять AS контроль над анонсами полученных по протоколу BGP маршрутов в смежные AS. Разработчикам **следует** поддерживать такие средства контроля по крайней мере на уровне отдельной сети. Реализациям протокола **следует** также поддерживать такие средства контроля на уровне автономной системы, где в качестве AS может рассматриваться автономная система, из которой исходит маршрут, или автономная система, анонсирующая маршрут в локальную систему (смежная AS).

(2) **Следует** позволять AS отдавать предпочтение определенному пути к адресату (при наличии множества маршрутов). **Следует** реализовать функцию, позволяющую администратору присваивать вес автономным системам и выбирать маршрут с минимальным весом (вес маршрута определяется как сумма весовых параметров всех AS в атрибуте AS_PATH, связанном с маршрутом).

(3) **Следует** позволять AS игнорировать маршруты с некоторыми AS в атрибуте AS_PATH. Такая функция может быть реализована с использованием метода, указанного в п. (2), когда нежелательным AS присваивается бесконечный вес. Процесс выбора маршрута должен игнорировать пути с бесконечным весом.

7.3.3 Маршрутизация между AS без использования протоколов EGP

Возможен обмен маршрутными данными между парой AS или доменов маршрутизации с различными стандартными протоколами внутренней маршрутизации без использования стандартных протоколов внешней маршрутизации. Наиболее распространенным способом такого обмена является независимое использование обоих протоколов внутренней маршрутизации на одном из граничных шлюзов с передачей маршрутной информации между этими процессами.

Как и передача маршрутных данных от EGP к IGP без использования подходящих механизмов управления, обмен маршрутной информацией между двумя IGP на одном маршрутизаторе может приводить к возникновению маршрутных петель.

[1] Border Gateway Protocol - протокол граничного шлюза.
[2] В оригинале ошибочно указан параграф 7.2.4. *Прим. перев.*

7.4 Статическая маршрутизация

Статическая маршрутизация обеспечивает явное указание следующего интервала на пути к определенному адресату. Маршрутизаторам **следует** обеспечивать способ задания статического маршрута к адресату, указанному сетевым префиксом. **Следует** также поддерживать возможность задания метрики для каждого статического маршрута.

Маршрутизатор, поддерживающий протокол динамической маршрутизации, **должен** позволять задание статических маршрутов с любыми значениями метрики, которые используются протоколом маршрутизации. Маршрутизатор **должен** обеспечивать пользователю возможность задания списка статических маршрутов, которые могут (или не могут) анонсироваться с использованием протокола маршрутизации. В дополнение к этому маршрутизаторам **следует** поддерживать для статических маршрутов перечисленную ниже дополнительную информацию, если они поддерживают протокол маршрутизации, способный эту информацию использовать:

- TOS;
- маски подсетей;
- размеры префиксов;
- метрику протокола маршрутизации, который может импортировать маршрут.

Обсуждение

Мы считаем, что требуется поддержка только тех параметров, которые могут быть полезны данному протоколу маршрутизации. Необходимость поддержки TOS не означает для разработчика необходимость поддержки других параметров, если они не используются.

Предпочтение статического маршрута перед динамическим (или наоборот), а также значения метрики, используемые для выбора пути при конфликте между статическим и динамическим маршрутом, **следует** делать настраиваемым для каждого статического маршрута.

Маршрутизатор **должен** позволять связывание метрики со статическими маршрутами для каждого поддерживаемого домена маршрутизации. Каждое такое значение метрики **должно** быть явно связано с соответствующим доменом маршрутизации. Например:

```
route 10.0.0.0/8 via 192.0.2.3 rip metric 3
route 10.21.0.0/16 via 192.0.2.4 ospf inter-area metric 27
route 10.22.0.0/16 via 192.0.2.5 egp 123 metric 99
```

Обсуждение

Предлагается (в идеальном случае) для статических маршрутов использовать вместо метрики уровень предпочтения (поскольку значения метрики можно сравнивать только с метрикой других маршрутов в том же домене маршрутизации, метрика статического маршрута может сравниваться лишь с метрикой других статических маршрутов). Такое предложение вступает в конфликт с некоторыми реализациями, где для статических маршрутов реально используется метрика, и та же метрика служит для выбора между статическим и динамическим маршрутом к одному адресату. Поэтому в данном документе используется термин «метрика» вместо термина «уровень предпочтения».

Такой механизм позволяет включать статические маршруты в RIP или OSPF (и иные протоколы в зависимости от метрики домена). Таким образом может применяться алгоритм поиска маршрутов, принятый в домене. Однако здесь не возникает «утечки» маршрутов, поскольку включение статического маршрута в домен динамической маршрутизации еще не дает маршрутизатору полномочий на распространение этого маршрута в домен маршрутизации.

Для статических маршрутов, не включенных в конкретный домен маршрутизации, поиск маршрута выполняется в следующем порядке:

(1) базовое соответствие (Basic match);

(2) соответствие максимальной длины (Longest match);

(3) минимальное значение TOS (если TOS поддерживается);

(4) лучшая метрика (метрика зависит от реализации).

Последний пункт может показаться ненужным, но он весьма полезен в тех случаях, когда нужно задать основной статический маршрут через один интерфейс и дополнительный маршрут через другой с автоматической сменой маршрута при отказе основного интерфейса.

7.5 Фильтрация маршрутной информации

Каждый маршрутизатор в сети принимает решения о пересылке на основе информации, хранящейся в его базе данных для пересылки. В простых сетях содержимое маршрутной базы данных может быть задано статически. По мере роста и усложнения сети возникает потребность в динамическом обновлении базы данных.

Для максимальной эффективности передачи трафика в сети необходимо обеспечить механизм контроля за распространением информации, используемой маршрутизатором при построении базы данных о пересылке. Механизм контроля включает способ выбора достоверных источников маршрутной информации и тех частей полученных данных, которым можно доверять. В результате таблица маршрутизации представляет собой отфильтрованную часть доступных сведений о маршрутах.

Кроме повышения эффективности маршрутизации механизм контроля позволяет повысить уровень стабильности системы за счет отбрасывания непригодных маршрутов.

В некоторых случаях локальная политика может запрещать широкое распространение полной маршрутной информации.

Приведенные здесь требования к фильтрации относятся только к протоколам, не использующим SPF, и никак не связаны с маршрутизаторами, которые не используют протоколы типа distance vector.

7.5.1 Проверка маршрута

Маршрутизатору **следует** протоколировать, как ошибки, любые анонсы маршрутов, нарушающих приведенные в этом документе требования, если только протокол маршрутизации, от которого получено обновление, не использует такие значения для представления специальных маршрутов (например, маршрута, используемого по умолчанию).

7.5.2 Базовая фильтрация маршрутов

Фильтрация маршрутных данных позволяет контролировать пути, используемые маршрутизатором для пересылки принимаемых пакетов. Маршрутизатору следует определить какие источники маршрутных данных он будет прослушивать и каким маршрутам будет доверять. Следовательно, маршрутизатор **должен** обеспечивать возможность указания:

- логических интерфейсов, через которые будет приниматься маршрутная информация, и маршрутов, которые будут приниматься от каждого логического интерфейса;
- маршрутов (все или только принятый по умолчанию), которые будут анонсироваться через логический интерфейс.

Некоторые протоколы маршрутизации не признают логические интерфейсы в качестве источников маршрутных данных. В таких случаях маршрутизатор **должен** обеспечивать возможность задать:

- другие маршрутизаторы, от которых будет приниматься маршрутная информация.

Предположим для примера, что маршрутизатор, подключен к одной или нескольким ветвям и магистрали более крупной сети. Поскольку каждая из таких ветвей имеет только один путь наружу, маршрутизатор может просто передавать в нее принятый по умолчанию маршрут. В магистральную сеть маршрутизатор будет анонсировать пути в подключенные к нему ветви.

7.5.3 Расширенная фильтрация маршрутов

По мере роста сетей и усложнения их топологии требуется более изощренная фильтрация маршрутов. Поэтому маршрутизаторам **следует** обеспечивать возможность независимого задания для каждого протокола маршрутизации:

- логических интерфейсов или маршрутизаторов, от которых будут приниматься маршрутные данные (маршруты), и маршрутов, которым следует доверять, для каждого логического интерфейса или маршрутизатора;
- маршрутов, которые будут передаваться через логический интерфейс;
- маршрутной информации, которая будет передаваться (если такой выбор поддерживается протоколом маршрутизации).

Во многих случаях имеет смысл упорядочить маршрутные данные от других маршрутизаторов по уровню надежности вместо того, чтобы просто доверять выбору, сделанному в первом пункте (см. выше). Маршрутизатор **может** обеспечивать возможность задания:

- уровня надежности или предпочтения для каждого полученного маршрута, маршрут с более высоким уровнем будет иметь преимущество независимо от связанной с ним маршрутной метрики.

Если маршрутизатор поддерживает установку уровней предпочтения для маршрутов, **недопустимо** распространять какие-либо маршруты, которые не были приняты этим маршрутизатором по уровню предпочтения, как информацию «из первых рук». Если используемый протокол маршрутизации не позволяет различать информацию из первых и третьих рук, для маршрутизатора **недопустимо** анонсировать какие-либо маршруты, которые он сам не выбрал по уровню предпочтения.

Обсуждение

Предположим для примера, что маршрутизатор получил путь в сеть C от маршрутизатора R и путь в ту же сеть от маршрутизатора S. Если маршрутизатор R рассматривается, как более надежный источник маршрутных данных по сравнению с S, трафик в сеть C будет пересылаться маршрутизатору R независимо от маршрута, полученного от S.

Данные для маршрутов, которые маршрутизатор не использует (информация от маршрутизатора S в предыдущем примере) **недопустимо** передавать другим маршрутизаторам.

7.6 Обмен информацией протоколов внешней маршрутизации

Маршрутизаторы **должны** обеспечивать возможность обмена маршрутной информацией между различными протоколами внутренней маршрутизации, если на одном маршрутизаторе могут работать независимые процессы маршрутизации IP. Маршрутизаторы **должны** обеспечивать механизм предотвращения маршрутных петель в тех случаях, когда они настроены на двухсторонний обмен маршрутными данными между двумя различными процессами внутренней маршрутизации. Маршрутизаторы **должны** обеспечивать механизм приоритизации для выбора маршрутов от независимых процессов маршрутизации. Маршрутизаторам **следует** обеспечивать административный контроль обмена IGP-IGP, когда последний осуществляется через административные границы.

Маршрутизаторам следует обеспечивать механизм для трансляции или преобразования метрики на уровне сетей. Маршрутизаторы (или протоколы маршрутизации) **могут** разрешать глобальное предпочтение для внешних маршрутов, импортируемых в IGP.

Обсуждение

Разные протоколы IGP используют различную метрику, что требует наличия того или иного механизма трансляции при передаче протоколу маршрутизации данных от другого протокола, который работает с иной метрикой. Некоторые протоколы IGP могут поддерживать несколько экземпляров[1] на одном маршрутизаторе или группе маршрутизаторов. В таких случаях метрика может передаваться без изменения или транслироваться.

Существует по крайней мере два метода трансляции метрики между различными процессами маршрутизации. Статический вариант (или пересчет метрики) использует существование анонса маршрута в одном IGP для генерации анонса маршрута в другой IGP с данной метрикой. Трансляция или табличный метод использует метрику

[1] Независимых процессов. *Прим. перев.*

одного IGP для создания метрики другого IGP с помощью специальной функции (например, добавление константы) или просмотра таблицы соответствия.

Двухсторонний обмен маршрутной информацией может представлять опасность при отсутствии механизма контроля за обратной связью. Это та же проблема, которая возникает в протоколах на основе «вектора удаленности» и решается с помощью «расщепления горизонта» (split horizon), а в протоколах EGP - с помощью правила «третьих рук». Маршрутные петли можно предотвратить явно за счет использования таблиц или списков разрешенных/запрещенных маршрутов или неявно с помощью использования split horizon, отказа от информации из «третьих рук» или установки меток для маршрутов. Разработчикам рекомендуется применять неявные механизмы, позволяющие упростить администрирование для сетевых операторов.

8. Прикладной уровень – протоколы управления сетью

Этот раздел содержит требования, которые являются более важными по сравнению с требованиями раздела REMOTE MANAGEMENT[1] в документе [INTRO:3].

8.1 Протокол SNMP

8.1.1 Элементы протокола SNMP

Маршрутизаторы **должны** поддерживать управление по протоколу SNMP [MGT:3]. Протокол SNMP **должен** работать с использованием UDP/IP в качестве протоколов транспортного и сетевого уровня. **Возможна** поддержка других протоколов управления (см., например, [MGT:25, MGT:26, MGT:27, and MGT:28]). Управление по протоколу SNMP **должно** работать так, будто протокол SNMP реализован в самом маршрутизаторе. В частности, **должно** обеспечиваться воздействие на работу системы управления путем передачи запросов SNMP по любому из адресов IP, присвоенных интерфейсам маршрутизатора. Реальное управление может выполняться маршрутизатором или прокси-агентом для маршрутизатора.

Обсуждение

Последнее правило предназначено для обеспечения возможности управления через прокси (устройство-посредник отвечает на пакеты SNMP, содержащие в заголовке один из IP-адресов маршрутизатора) или реализацию SNMP в самом маршрутизаторе, отвечающую на пакеты SNMP соответствующим образом.

Важно, чтобы команды управления можно было передавать по одному из IP-адресов маршрутизатора. При диагностике сетевых неполадок один из IP-адресов маршрутизатора может оказаться единственным идентификатором маршрутизатора, определение адресов маршрутизатора возможно путем просмотра таблиц других маршрутизаторов.

Должны быть реализованы все операции SNMP (get, get-next, get-response, set и trap).

Маршрутизаторы **должны** обеспечивать механизм ограничения скорости генерации сообщений SNMP trap. Маршрутизаторы **могут** обеспечивать такой механизм с помощью алгоритма асинхронной передачи сигналов управления, описанного в [MGT:5].

Обсуждение

Несмотря на общее согласие с необходимостью ограничения скорости генерации trap-сообщений, пока отсутствует единое мнение по поводу способа реализации такого ограничения. Упомянутый алгоритм является экспериментальным.

8.2 Таблица групп

Для упрощения в данной спецификации предполагается наличие в маршрутизаторе абстрактной таблицы community. Эта таблица содержит несколько записей, каждая из которых относится к одной группе (community) и включает параметры, требуемые для полного определения атрибутов этой группы. Реализация метода абстрактной таблицы групп управления зависит от разработчика.

Таблица групп маршрутизатора **должна** поддерживать по крайней мере одну запись и **следует** поддерживать не менее двух записей.

Обсуждение

Таблица групп, не содержащая записей, будет совершенно бесполезной. Это означает, что маршрутизатор не будет распознавать ни одной группы и операции SNMP будут отвергаться.

Следовательно, одна запись является минимальным размером таблицы групп. Поддержка двух записей позволяет создать одну группу с правами только на чтение информации и другую группу с возможностью записи.

Маршрутизаторы **должны** позволять пользователю вручную (т. е., без использования SNMP) проверять, добавлять, удалять и изменять записи в таблице групп SNMP. Пользователю **должна** обеспечиваться возможность установки имени группы или создания представления MIB. Пользователю **должна** предоставляться возможность настройки группы как read-only (не допускаются операции SET) или read-write (допускаются операции SET).

Пользователю **должна** обеспечиваться возможность определить хотя бы один адрес IP, по которому будут передаваться уведомления для каждой группы или представления MIB, если используется механизм trap. Эти адреса **следует** задавать независимо для групп SNMP или представлений MIB. **Следует** обеспечить возможность включения и выключения передачи уведомлений для группы или представления MIB.

Маршрутизатору **следует** обеспечивать возможность задания списка разрешенных узлов управления для любой группы. При наличии такого списка маршрутизатор **должен** проверять адрес отправителя дейтаграмм SNMP и отбрасывать дейтаграммы, если адрес отправителя отсутствует в списке разрешенных узлов. При отбрасывании дейтаграммы маршрутизатор **должен** выполнить все операции, применимые для случаев несоответствия при аутентификации SNMP.

[1] В переводе RFC 1123 эта глава носит название “Удаленное управление”. *Прим. перев.*

Обсуждение

Эта система аутентификации имеет весьма ограниченные возможности, но в комбинации в различными фильтрами пакетов может несколько повысить уровень безопасности.

Таблица групп **должна** сохраняться в энергонезависимой памяти.

В исходную таблицу групп **следует** включать одну запись с именем public и правами read-only (только чтение). По умолчанию для этой группы **недопустима** передача сообщений trap. Если группа public реализована, она **должна** сохраняться в таблице групп до тех пор, пока администратор не переименует или не удалит ее.

Обсуждение

По умолчанию генерация сообщений trap для группы public отключена. Trap PDU передаются по индивидуальным адресам IP. Эти адреса должны настраиваться в маршрутизаторе. До того, как адрес будет задан администратором, сообщения trap посылать просто некуда. Следовательно, передача сообщений trap для группы public по умолчанию должна быть отключена. Естественно, что администратор может включить генерацию таких сообщений при настройке маршрутизатора.

8.3 Стандартные MIB

В маршрутизаторах реализуются все MIB, относящиеся к маршрутизаторам:

- **должны** быть реализованы группы MIB-II [MGT:2] System, Interface, IP, ICMP и UDP;
- **требуется** реализация Interface Extensions MIB [MGT:18];
- **требуется** реализация IP Forwarding Table MIB [MGT:20];
- если маршрутизатор реализует TCP (например, для Telnet), **требуется** реализация группы MIB-II [MGT:2] TCP.;
- если маршрутизатор реализует EGP, **требуется** реализация группы MIB-II [MGT:2] EGP;
- если маршрутизатор поддерживает OSPF, **требуется** реализация OSPF MIB [MGT:14];
- если маршрутизатор поддерживает BGP, **требуется** реализация BGP MIB [MGT:15];
- если маршрутизатор имеет интерфейс Ethernet, 802.3 или StarLan, **требуется** реализация Ethernet-Like MIB [MGT:6];
- если маршрутизатор имеет интерфейс 802.4, **требуется** реализация 802.4 MIB [MGT:7];
- если маршрутизатор имеет интерфейс 802.5, **требуется** реализация 802.5 MIB [MGT:8];
- если маршрутизатор имеет интерфейс FDDI, который реализует ANSI SMT 7.3, **требуется** реализация FDDI MIB [MGT:9];
- если маршрутизатор имеет интерфейс FDDI, который реализует ANSI SMT 6.2, **требуется** реализация FDDI MIB [MGT:29];
- если маршрутизатор имеет интерфейс, который использует сигнализацию V.24 (например, RS-232, V.10, V.11, V.35, V.36 или RS-422/423/449), **требуется** реализация RS-232 MIB [MGT:10];
- если маршрутизатор имеет интерфейс T1/DS1, **требуется** реализация T1/DS1 MIB [MGT:16];
- если маршрутизатор имеет интерфейс T3/DS3, **требуется** реализация T3/DS3 MIB [MGT:17];
- если маршрутизатор имеет интерфейс SMDS, **требуется** реализация SMDS Interface Protocol MIB [MGT:19];
- если маршрутизатор поддерживает протокол PPP на любом из своих интерфейсов, **требуется** реализация PPP MIB [MGT:11], [MGT:12] и [MGT:13];
- если маршрутизатор поддерживает протокол RIP версии 2, **требуется** реализация RIP Version 2 MIB [MGT:21];
- если маршрутизатор поддерживает протокол X.25 на любом из своих интерфейсов, **требуется** реализация X.25 MIB [MGT:22, MGT:23 и MGT:24].

8.4 MIB от производителей

Стандартные и экспериментальные MIB не перекрывают всего диапазона данных о статистике, состоянии, конфигурации и управлении, которые могут быть доступны для элементов сети. Однако такая информация может оказаться весьма полезной. Производители маршрутизаторов (и других сетевых устройств) обычно разрабатывают фирменные расширения MIB для использования такой информации. Такие базы называются MIB от производителя (Vendor Specific MIB).

MIB от производителя для маршрутизаторов **должны** обеспечивать доступ ко всей информации о статистике, состоянии, конфигурации и управлении, которая не доступна с помощью реализованных стандартных и экспериментальных MIB. Эта информация **должна** быть доступна для операций мониторинга и контроля.

Обсуждение

Это требование предназначено для обеспечения возможности выполнять на маршрутизаторе с помощью протокола SNMP операции, доступные с консоли, и наоборот. Для использования SNMP требуется выполнить некий минимальный набор операций настройки (например, установить для маршрутизатора адрес IP). Эта начальная настройка не может быть выполнена с помощью SNMP. Однако после проведения начальной настройки система сетевого управления обеспечивает поддержку всех возможностей управления.

Производителям **следует** обеспечивать спецификации для всех переменных Vendor Specific MIB. Эти спецификации **должны** соответствовать SMI [MGT:1], а описания должны быть выполнены в формате, указанном в документе [MGT:4].

Обсуждение

Доступность Vendor Specific MIB для пользователей является насущной необходимостью. Без такой информации пользователи не смогут настроить свои системы сетевого управления для использования параметров фирменных расширений MIB и параметры останутся бесполезными.

Формат спецификаций MIB также задан. Имеются специальные программы, которые читают спецификации MIB и генерируют требуемые для работы систем сетевого управления таблицы. Эти программы обычно понимают только стандартный формат спецификации MIB.

8.5 Сохранение изменений

Параметры, измененные с помощью SNMP, **могут** сохраняться в энергонезависимой памяти.

Обсуждение

Причины того, что это требование имеет уровень «**могут»**, следующие:

- Физическая природа энергонезависимой памяти не задается данным документом. Следовательно, параметры могут сохраняться в микросхемах NVRAM/EEPROM, на локальных дисках (съемных или фиксированных), в файлах на серверах TFTP, BOOTP и т. п. Предположим, что информация хранится в файле, доступном по протоколу TFTP. В этом случае изменение конфигурационных параметров на маршрутизаторе будет требовать копирования этих параметров на сервер. Возможно также редактирование конфигурационного файла на сервере с последующим копированием его на маршрутизатор. Решение этой проблемы не представляется очевидным.

  К хосту, используемому для хранения конфигурационной информации, предъявляются дополнительные требования кроме поддержки на нем сервера TFTP и разработчикам неразумно полагаться на то, что у каждого потенциального заказчика имеется подходящий хост.

- Синхронизация внесенных изменений с содержимым энергонезависимой памяти продолжает оставаться предметом дискуссий. Некоторые считают, что все изменения следует записывать незамедлительно, а другие предпочитают изменять содержимое энергонезависимой памяти с помощью явно задаваемых команд.

9. Прикладной уровень – прочие протоколы

Для всех дополнительных протоколов прикладного уровня, поддерживаемых маршрутизатором, **должна** обеспечиваться совместимость с соответствующими требованиями [INTRO:3], **следует** также стараться обеспечить безусловную совместимость.

9.1 BOOTP

9.1.1 Введение

Протокол BOOTP[1] работает на основе UDP/IP и позволяет при загрузке хостов получать конфигурационные параметры с сервера без участия оператора. BOOTP обеспечивает для хоста уведомление о выделенном ему адресе IP, адресе сервера загрузки и имени файла для загрузки в память хоста и последующего исполнения ([APPL:1]). С помощью протокола BOOTP возможна также установка для хоста других конфигурационных параметров, включая локальный размер сетевого префикса или маску подсети, локальное время, адреса используемых по умолчанию маршрутизаторов и адреса различных серверов Internet ([APPL:2]).

9.1.2 Агенты BOOTP Relay

Зачастую клиенты BOOTP и серверы BOOTP, с которыми работают такие клиенты, могут находиться в разных (под)сетях IP. В таких случаях требуется дополнительный агент, передающий сообщения BOOTP между клиентами и серверами. Такие агенты изначально назывались агентами пересылки. Однако во избежание путаницы с функциями пересылки IP в маршрутизаторах для агентов стали использовать термин BOOTP relay (транслятор).

Обсуждение

Агент BOOTP relay выполняет функции, отличающиеся от обычной пересылки пакетов IP в маршрутизаторах. Маршрутизатор «переключает» дейтаграммы между сетями более или менее прозрачно, а транслятор BOOTP принимает сообщения протокола BOOTP, как конечный адресат и в результате генерирует новые сообщения BOOTP. Не следует рассматривать трансляторы BOOTP, как простые системы пересылки пакетов.

Функции трансляции BOOTP обычно реализуются в маршрутизаторах, соединяющих между собой клиентов и серверы, хотя транслятор может быть реализован и на отдельном хосте в подсети клиента.

Маршрутизатор **может** выполнять функции транслятора BOOTP. Если такие функции реализованы, маршрутизатор **должен** соответствовать требованиям спецификации [APPL:3].

В параграфе 5.2.3 рассматривалась ситуация, когда пакет доставляется локально (маршрутизатору). Все локально доставляемые пакеты UDP, адресованные в порт BOOTPS (67), передаются для специальной обработки логическому транслятору BOOTP в маршрутизаторе.

В параграфах 4.2.2.11 и 5.3.7 обсуждались непригодные IP-адреса отправителей. Согласно приведенным правилам, для маршрутизатора недопустима пересылка дейтаграмм IP с адресом отправителя 0.0.0.0. Однако маршрутизаторы, поддерживающие функции транслятора BOOTP, **должны** принимать для локальной доставки сообщения BOOTREQUEST с IP-адресом отправителя 0.0.0.0.

10. Эксплуатация и обслуживание

Приведенные в этом разделе требования имеют более высокий приоритет для маршрутизаторов, нежели требования, документа [INTRO:3], относящиеся к расширению модуля IP.

Средства поддержки эксплуатации и обслуживания (O&M) составляют существенную часть реализации любого маршрутизатора. Хотя эти функции не представляются непосредственно связанными с интероперабельностью, они важны для администратора, который должен обслуживать маршрутизатор и находить источники проблем при

[1]Bootstrap Protocol - протокол загрузки.

возникновении последних. В этот раздел включено также обсуждение вопросов инициализации маршрутизаторов и функций, помогающих администратору обеспечивать безопасность маршрутизатора и учет трафика для своих сетей.

10.1 Введение

Операции O&M для маршрутизаторов включают:

- диагностику аппаратных проблем в процессорном модуле маршрутизатора, сетевых интерфейсах, подключенных сетях, модемах и коммуникационных каналах;
- установку нового оборудования;
- инсталляцию новых программ;
- перезагрузку маршрутизатора после аварий;
- настройку маршрутизатора и изменение его конфигурации;
- обнаружение и диагностику проблем в Internet (например, перегрузки), маршрутных петель, некорректных адресов IP, черных дыр, пакетных лавин и некорректно ведущих себя хостов;
- изменение топологии сети - временное (например, на период решения проблем) или постоянное;
- мониторинг состояния и производительности маршрутизаторов и подключенных к ним сетей;
- сбор статистики трафика для ее использования при планировании сети;
- координацию перечисленных выше действий с производителями и консультантами.

Маршрутизаторы и соединенные с ними коммуникационные каналы часто работают под централизованной системой O&M. Обслуживающая организация может поддерживать сетевой центр (NOC) для выполнения функций O&M. Важно обеспечить для маршрутизаторов возможность удаленного управления и мониторинга из таких центров через Internet, поскольку маршрутизаторы могут не быть подключены непосредственно к сети NOC. Поскольку отказы в сети могут временно нарушать доступ через сеть, многие NOC обеспечивают доступ к маршрутизаторам по дополнительным каналам, которые зачастую организуются с использованием коммутируемых телефонных линий и модемов, подключенных к консольным портам маршрутизаторов.

Поскольку передаваемые через сеть пакеты IP зачастую используют маршрутизаторы, находящиеся под управлением нескольких центров NOC, диагностика проблемы в Internet часто требует координации действий множества NOC. В некоторых случаях один маршрутизатор может контролироваться из нескольких NOC, но этого не следует делать без необходимости, поскольку избыточный мониторинг будет снижать производительность маршрутизатора.

Средства мониторинга, используемые в NOC, могут существенно различаться по своей изощренности. Современные реализации систем мониторинга включают многооконные динамические системы отображения маршрутизатора в целом. В будущем предполагается использование методов AI для автоматической диагностики проблем.

Обсуждаемые здесь функции O&M являются лишь частью большой и сложной задачи управления Internet. В управление вовлечено не только множество организаций, но и протоколы различных уровней. Например, на современном этапе развития архитектуры Internet существует сильная зависимость между реализациями TCP на хостах и возможным насыщением на уровне IP в системах маршрутизации [OPER:1]. Следовательно, диагностика проблем насыщения будет в некоторых случаях требовать мониторинга статистики TCP на хостах. В настоящее время ведутся интенсивные исследования по вопросам управления Internet и, в частности, функций O&M в маршрутизаторах. Эти исследования уже привели к разработке стандартов для O&M в маршрутизаторах. В этой сфере может оказаться весьма значительным также вклад разработчиков.

10.2 Инициализация маршрутизатора

10.2.1 Начальная настройка маршрутизатора

Существует минимальный набор условий, которые должны быть выполнены до того, как маршрутизатор сможет начать пересылку пакетов. Для маршрутизатора **недопустимо** разрешать пересылку пакетов на любом из физических интерфейсов, пока не будет выполнено хотя бы одно из приведенных ниже условий:

(1) маршрутизатор знает адрес и маску или размер префикса по крайней мере одного логического интерфейса, связанного с данным физическим интерфейсом;

(2) маршрутизатор знает, что данный интерфейс является безадресным (unnumbered) и известен адрес router-id.

Для этих параметров **должны** явно выполняться следующие требования:

- для маршрутизатора **недопустимо** использование заводских (принятых по умолчанию в исходной конфигурации) установок для адресов IP, размера префиксов или router-id;
- для маршрутизатора **недопустимо** предполагать что не настроенный интерфейс является безадресным.

Обсуждение

Существуют маршрутизаторы, которые выпускаются с предустановленными адресами интерфейсов. Это приводит к тому, что маршрутизатор начинает анонсировать установленные по умолчанию адреса в активные сети.

10.2.2 Инициализация адреса и префикса

Маршрутизатор **должен** обеспечивать возможность установки статических значений адресов IP и масок или длины префиксов и сохранения этих параметров в энергонезависимой памяти.

Маршрутизатор **может** получать свои IP-адреса и соответствующие им маски динамически в процессе инициализации системы (см. параграф 10.2.3).

При поддержке динамической настройки **должна** обеспечиваться возможность выбора используемого метода получения динамических параметров.

Как было сказано в параграфе 4.2.2.11, адреса IP не должны иметь значение 0 или -1 в полях <Номер хоста> и <Префикс сети>. Поэтому маршрутизаторам **не следует** позволять установку таких адресов или масок, которые нарушали бы данное правило.

Обсуждение

При использовании произвольных масок возможно возникновение ситуаций, в которых маршрутизация становится невозможной или бессмысленной (т. е., возникает два или более маршрута с различными масками одинакового размера к одному адресату). Это является одним из наиболее сильных аргументов в пользу применения сетевых префиксов и причиной запрета на использование масок, не являющихся непрерывными.

Маршрутизатору **следует** выполнять перечисленные здесь проверки для всех задаваемых масок:

- маска не должна состоять только из единиц или только из нулей (префикс сети не может иметь размер 0 или 32);
- все биты, соответствующие сетевому префиксу в маске должны иметь значение 1;
- биты, соответствующие сетевому префиксу, должны образовывать непрерывную последовательность.

Обсуждение

Маски, связанные с маршрутами, иногда так же называют масками подсетей. Приведенные выше требования не относятся к таким маскам.

10.2.3 Загрузка через сеть с использованием протоколов BOOTP и TFTP

Было много дискуссий о том, как можно и следует загружать маршрутизаторы через сеть. Эти дискуссии велись в основном о протоколах BOOTP и TFTP. Сегодня существуют маршрутизаторы, использующие протокол TFTP для загрузки через сеть. Нет причин, которые не позволяли бы использовать протокол BOOTP для поиска сервера, с которого следует взять загрузочный образ.

BOOTP применяется конечными системами и требует некоторых усилий для использования при загрузке маршрутизаторов. Если маршрутизатор использует BOOTP для нахождения сервера загрузки, ему следует передать сообщение BOOTP Request со своим аппаратным адресом для первого интерфейса или (если маршрутизатор имеет какую-то предварительную настройку) аппаратного адреса любого другого интерфейса, либо другое число для включения в поле аппаратного адреса пакета BOOTP. Последняя возможность позволяет маршрутизаторам без аппаратных адресов (например, только с синхронными интерфейсами) использовать протокол BOOTP для обнаружения сервера загрузки. После этого можно использовать протокол TFTP для загрузки образа, указанного в сообщении BOOTP Reply. Если на маршрутизаторе нет настроенных устройств или номеров, он **может** циклически перебирать аппаратные адреса интерфейсов, пока сервером BOOTP не будет найдено соответствие.

Маршрутизаторам **следует** реализовать возможность сохранения параметров, полученных с помощью BOOTP, в локальной энергонезависимой памяти. Маршрутизатор **может** поддерживать возможность хранения полученного через сеть загрузочного образа на стабильном локальном устройстве хранения[1].

Маршрутизатор **может** поддерживать для удаленного пользователя возможность запросов на загрузку маршрутизатором нового образа. Следует различать получение нового образа из трех разных мест - указанного в запросе, последнего использованного для загрузки или найденного с помощью протокола BOOTP.

10.3 Эксплуатация и обслуживание

10.3.1 Введение

Существует множество моделей реализации функций O&M в маршрутизаторах. Один из полярных вариантов обеспечивает лишь возможность локального выполнения функций O&M (например, с помощью терминала, подключенного к маршрутизатору). Другим крайним случаем является модель, поддерживающая лишь удаленный режим с минимальном набором функций, которые должны быть выполнены локально (например, инициирование загрузки), и полным набором функций O&M, выполняемых из NOC. Существуют также промежуточные модели, в которых персонал NOC может подключиться к маршрутизатору, как к хосту, используя протокол Telnet, для выполнения функций, которые доступны также локально. Модель, обеспечивающая только локальный доступ, может подходить для сетей с небольшим числом маршрутизаторов, но обычно маршрутизаторы обслуживаются удаленно из NOC и поэтому для большинства маршрутизаторов требуется обеспечение удаленного доступа к функциям O&M.

Удаленный доступ к функциям O&M может осуществляться с помощью программных агентов управления. В прямом варианте маршрутизатор будет поддерживать функции O&M удаленно напрямую из NOC с использованием стандартных протоколов Internet (например, SNMP, UDP или TCP), в опосредованном варианте эти протоколы будут поддерживаться агентом управления, который обеспечивает контроль за маршрутизатором с помощью фирменных протоколов. Прямой вариант является более предпочтительным, хотя возможны и другие варианты. Использование специального оборудования и/или программ, существенно повышающих стоимость маршрутизаторов, не рекомендуется, однако некоторые производители могут предлагать агент управления как встроенную компоненту сети, частью которой являются маршрутизаторы. В таких случаях требуется возможность доступа к агентам управления с удаленных сайтов на основе стандартных протоколов Internet, а также обеспечение функциональности, эквивалентной локальному доступу к агентам.

Желательно, чтобы агент управления и все программные инструменты для NOC, которые обеспечивает производитель, работали как пользовательские программы в стандартных операционных системах. Использование стандартных протоколов Internet (UDP и TCP) для связи с маршрутизаторами упрощает эту задачу.

Средства удаленного мониторинга и (особенно) управления маршрутизаторами порождают серьезную проблему контроля доступа, которую следует принимать во внимание. Нужно с осторожностью относиться к контролю за использованием ресурсов маршрутизатора, выделяемых для выполнения таких функций. Нежелательно, чтобы

[1] Носитель, содержимое которого не теряется при перезагрузке (например, диск или flash-память). *Прим. перев.*

система мониторинга отнимала заметную часть процессорного времени маршрутизатора. С другой стороны, функции O&M должны иметь достаточно высокий приоритет для того, чтобы их можно было использовать даже в периоды перегрузки маршрутизатора, поскольку именно в таких случаях актуальность O&M существенно возрастает.

10.3.2 Доступ по отдельному каналу (Out Of Band)

Маршрутизаторы **должны** поддерживать доступ по отдельному каналу (Out-Of-Band или OOB). Для OOB-доступа **следует** поддерживать такую же функциональность, как для доступа по основному каналу (in-band). Для этого варианта доступа **следует** реализовать систему контроля доступа с целью предотвращения несанкционированного подключения к маршрутизатору.

Обсуждение

Доступ по отдельному каналу будет предоставлять NOC возможность подключения к маршрутизатору в период его недоступности через сеть.

OOB-доступ является важным инструментом сетевого администратора. Он позволяет подключаться к оборудованию, независимо от состояния сетевых соединений. Существует множество способов организации доступа по отдельному каналу. Выбор конкретного способа не так важен, как независимость подключения от состояния сетевых соединений. Примером OOB-доступа может служить подключение к маршрутизатору через последовательный порт с использованием модема.

Важно, чтобы OOB-доступ обеспечивал такую же функциональность, как и подключение по основному каналу. Доступ по основному каналу имеет свои ограничения, связанные с невозможностью подключения к оборудованию при его недоступности через сеть. Этот тип доступа сохраняет свою важность при настройке конфигурации и диагностике проблем, не связанных с прерыванием доступности маршрутизатора через сеть.

10.3.2 Функции O&M в маршрутизаторах

10.3.2.1 Обслуживание - диагностика оборудования

Каждому маршрутизатору **следует** поддерживать возможность работы в качестве автономного[1] устройства для локальной настройки и обслуживания. Это значит, что **следует** поддерживать возможности диагностики маршрутизатора с использованием только работающих на этом маршрутизаторе программ. Маршрутизаторам **следует** обеспечивать возможность работы средств диагностики в случаях отказов. Предложения по аппаратным и программным средствам диагностики даны в параграфе 10.3.3.

10.3.2.2 Контроль - запись содержимого памяти и перезагрузка

Маршрутизатор **должен** поддерживать для режимов in-band и out-of-band механизмы, позволяющие администратору перезагружать маршрутизатор, останавливать и возобновлять его работу. Маршрутизаторам **следует** также поддерживать механизм (например, watchdog-таймер), который будет автоматически перезагружать маршрутизатор при его «зависании» в результате аппаратных или программных отказов.

Маршрутизатору **следует** поддерживать механизм записи содержимого памяти (dump) и другой полезной информации при возникновении критических ошибок в работе. Эти данные следует записывать на стабильный локальный носитель или передавать на другой хост с использованием таких механизмов, как TFTP (см. [OPER:2], [INTRO:3]).

10.3.2.3 Контроль - настройка конфигурации

Каждый маршрутизатор имеет конфигурационные параметры, которые должны быть установлены. **Следует** обеспечивать возможность изменения параметров без перезагрузки маршрутизатора, в крайних случаях **можно** предлагать администратору перезагрузку. Существуют ситуации, когда изменение параметров невозможно без перезагрузки (например, смена IP-адреса интерфейса[2]). В таких случаях следует принимать меры по минимизации времени нарушения работы маршрутизатора и окружающих сетей.

Следует обеспечивать возможность настройки конфигурации маршрутизатора через сеть в ручном или автоматическом режиме. Маршрутизатору **следует** поддерживать возможность загрузки параметров с другого хоста или маршрутизатора. Это означает, что **следует** обеспечить прикладную программу или функцию маршрутизатора для преобразования формата конфигурационного файла, понятного человеку, в формат, используемый программой управления конфигурацией маршрутизатора. Маршрутизатору **следует** поддерживать стабильную среду хранения информации для записи конфигурационных параметров. **Не следует** полагаться при хранении конфигурации на такие механизмы, как RARP, ICMP Address Mask Reply, **можно** не полагаться и на BOOTP.

Обсуждение

Необходимо отметить, что в будущем RARP, ICMP Address Mask Reply, BOOTP и другие механизмы могут потребоваться для поддержки автоматической настройки конфигурации маршрутизаторов. Хотя в будущем маршрутизаторы смогут поддерживать автоматическую настройку конфигурации, не следует применять ее в рабочих сетях до тех пор, пока системы автоматической настройки не будут подобающим образом протестированы. Это **не** означает полного отказа от использования автоматических средств настройки конфигурации. В тех случаях, когда предполагается автоматическая настройка, может оказаться разумным позволить маршрутизатору выполнить операции по автоматической настройке конфигурации, а потом проигнорировать заданные автоматически параметры.

10.3.2.4 Загрузка системных программ через сеть

Маршрутизатору **следует** сохранять свой загрузочный образ в локальной энергонезависимой памяти (PROM, NVRAM, или диск). **Возможна** также поддержка загрузки программного кода через сеть с другого хоста или маршрутизатора.

Маршрутизатор, хранящий загрузочный образ в локальной энергонезависимой памяти, **можно** настроить и на загрузку через сеть. Маршрутизаторам, предлагающим такую возможность, **следует** поддерживать возможность задания конфигурации, при которой будет автоматически включаться загрузка с локального образа, если загрузка через сеть окажется невозможной.

---

[1] Не подключенного к сетям. *Прим. перев.*

[2] В современных маршрутизаторах изменение адреса IP на сетевом интерфейсе обычно не требует перезагрузки. *Прим. перев.*

Обсуждение

Важно обеспечить возможность автоматической загрузки и начала работы маршрутизатора. Память NVRAM может быть одним из решений для маршрутизаторов, используемых в больших сетях, поскольку изменение кода в ПЗУ (PROM) потребует больших затрат времени от администраторов, обслуживающих множество сетей или сети, расположенные на большой территории. Важно обеспечить возможность загрузки системных программ через сеть, поскольку это дает существенно более быстрый способ исправления программных ошибок или добавления новых возможностей по сравнению с заменой кода в PROM. Для маршрутизаторов, использующих NVRAM вместо PROM, также будет полезна загрузка через сеть с последующей записью загрузочного образа в NVRAM.

Маршрутизаторам **следует** выполнять базовые проверки загружаемого кода, независимо от способа загрузки, для обнаружения и (возможно) исправления имеющихся в образе ошибок.

Маршрутизаторы **могут** также поддерживать различные варианты конфигурации в зависимости от работающих программ. Если конфигурационные команды меняют одну версию программ на другую, будет полезно пользоваться той конфигурацией, которая совместима с загружаемыми программами.

10.3.2.5 Обнаружение и обработка конфигурационных ошибок

Должны обеспечиваться механизмы детектирования и обработки ошибок в конфигурационных параметрах. Если команда выполняется некорректно, маршрутизатору **следует** выдавать сообщение об ошибке. Для маршрутизатора **недопустимо** воспринимать некорректно сформированные команды, как правильные.

Обсуждение

Возможны ситуации, в которых не удается обнаружить ошибки (например, команда не содержит синтаксических ошибок, но недопустима по сути выполняемого набора операций). Такие ситуации могут детектироваться маршрутизатором, но могут также оставаться незамеченными.

Другим случаем ошибочной конфигурации является некорректная настройка сети, к которой подключен маршрутизатор. Маршрутизатор **может** детектировать ошибки в конфигурации сети. Маршрутизатор **может** протоколировать такие ошибки, чтобы администратор смог обнаружить возможные проблемы в сети.

Обсуждение

Примером описанной ситуации может служить случай, когда в сети имеется другой маршрутизатор с таким же адресом или маршрутизатор с некорректной маской. При обнаружении такой проблемы маршрутизатор скорей всего не сможет сам исправить ошибку, поэтому от такого детектирования может быть больше вреда, чем пользы.

10.3.2.6 Минимизация «разрушений»

Следует обеспечивать минимальное воздействие смены конфигурации маршрутизатора на работу сети. **Недопустимо** сбрасывать таблицы маршрутизации без необходимости при внесении простых изменений в конфигурацию маршрутизатора. Если маршрутизатор использует несколько протоколов маршрутизации, **недопустимо** чтобы прерывание работы одного протокола нарушало работу других протоколов маршрутизации за исключением тех случаев, когда маршрутная информация была получена от прекратившего работу протокола.

Обсуждение

Задача сетевых администраторов состоит в обеспечении эффективного доступа пользователей к сети. Перезагрузка конфигурации маршрутизатора с целью простого изменения параметров может привести к нарушению картины маршрутизации и последующему нарушению работы сети и ее пользователей. Например, при сбросе таблицы маршрутизации будет теряться принятый по умолчанию маршрут и маршруты к сайтам внутри сети. Такое нарушение будет приводить к достаточно продолжительному простою в работе пользователей сети. Целью данного параграфа является подчеркивание важности сохранения работоспособности сети в тех случаях, когда это возможно.

10.3.2.7 Контроль – поиск неисправностей

(1) Маршрутизатор **должен** обеспечивать доступ через сеть (in-band) для управления, но (за исключением случаев, указанных в параграфе 8.2) из соображений безопасности по умолчанию такой доступ **следует** отключать. Производители **должны** указывать в документации установленное по умолчанию состояние для любого доступа в режиме in-band. Для такого доступа **следует** обеспечивать средства контроля, позволяющие предотвратить несанкционированный доступ.

Обсуждение

Доступ через сеть предназначен, прежде всего, для использования стандартных сетевых протоколов, которые могут оказывать или не оказывать влияния на состояние работы маршрутизатора. Это требование включает (но не ограничивается) консольный доступ Telnet/RLOGIN, а также операции SNMP.

Возникает противоречие между требованиями безопасности и доступности маршрутизатора для настройки. Любой автоматический доступ к маршрутизатору может снижать уровень безопасности, но такой доступ может играть важную роль для заказчиков, чтобы сделать маршрутизатор доступным через сеть, как только он будет подключен. По крайней мере один производитель выпускает маршрутизаторы, не имеющие консольного порта и полностью зависящие от возможности доступа через сеть для настройки конфигурационных параметров.

Производители вправе разрешить доступ к маршрутизатору через сеть по умолчанию, но они также несут ответственность за обеспечение безопасности своих маршрутизаторов.

(2) Маршрутизатор **должен** обеспечивать возможность инициирования передачи запросов ICMP. **Следует** реализовать перечисленные ниже опции:

- выбор шаблона (pattern) для поля данных;
- выбор размера пакетов;
- запись маршрута (Record route).

Дополнительно **могут** быть реализованы следующие опции:

- Loose source route;

- Strict source route;
- Timestamp.

(3) Маршрутизаторам **следует** обеспечивать возможность инициирования трассировки с помощью traceroute. Если поддерживается такая трассировка, **следует** использовать программу traceroute сторонних разработчиков.

Для каждого из трех перечисленных выше пунктов (если они реализованы) **следует** обеспечивать контроль доступа с целью предотвращения использования этих функций не имеющим соответствующих полномочий персоналом.

10.4 Вопросы безопасности

10.4.1 Аудит и журналы аудита

Аудит и учет работы являются проклятием для операторов, но эти функции важны для тех, кто отвечает за безопасность сетей и вопросы оплаты счетов пользователями. В контексте безопасности аудит является желательным, поскольку он помогает сохранить работоспособность сети и защитить ее ресурсы от недопустимого использования, не требуя расходов, превышающих стоимость самих ресурсов.

(1) Изменения конфигурации

Маршрутизаторам **следует** обеспечивать метод аудита изменений конфигурации хотя бы в такой простой форме, как сохранение инициалов оператора и времени внесения изменений.

Обсуждение

Протоколирование конфигурационных изменений (кто, когда и что поменял) весьма полезно, особенно в тех случаях, когда локальный трафик вдруг начал передаваться через Аляску. Важна также возможность возврата к предыдущей конфигурации.

(2) Учет пакетов

Производителям следует с должным вниманием отнестись к поддержке системы учета трафика между парами хостов или сетей. Настоятельно рекомендуется обеспечить также механизм ограничения сбора такой информации заданными парами хостов или сетей.

Обсуждение

Матрица трафика, как сказано выше, может давать оператору представление о тенденциях в работе сети, которые могут быть незаметными в другой статистике. Это также позволяет идентифицировать хосты и сети, которые пытаются исследовать структуру подключенных сетей (например, один внешний хост пытается передать пакеты по всем адресам IP подключенной к маршрутизатору сети).

(3) Аудит безопасности

Маршрутизаторы **должны** обеспечивать метод аудита безопасности в части отказов и нарушений, включая:

- отказы при проверке полномочий: некорректные пароли, недопустимые группы SNMP, непригодные маркеры;
- нарушения правил доступа: запрещенные маршруты Source Route, фильтруемые адресаты;
- успешная проверка полномочий: правильные пароли для Telnet-доступа через сети и терминального доступа.

Маршрутизаторы **должны** поддерживать метод ограничения или отключения функций аудита, но по умолчанию поддержку аудита **следует** включать. Возможные методы аудита включают списки нарушений при попытках доступа с консоли, если такой доступ имеется, протоколирование и учет нарушений внутренними средствами или передача этих сведений на удаленный сервер безопасности с использованием механизма SNMP trap или механизма ведения журнальных файлов Unix (syslog). Маршрутизатор **должен** поддерживать по крайней мере один из таких механизмов и **может** реализовать множество механизмов.

10.4.2 Контроль конфигурации

Производитель несет ответственность за обеспечение контроля конфигурации при загрузке программного кода в выпускаемые им маршрутизаторы. В частности, если производитель обеспечивает обновление программ через Internet, ему следует также обеспечивать для заказчиков возможность подтверждения загрузки и возможно проверку контрольных сумм в процессе загрузки.

Обсуждение

Многие производители обеспечивают уведомление об изменениях программ через Internet. Эту тенденцию следует приветствовать, но такое обновление программ может порождать уязвимости в системе контроля за конфигурацией маршрутизаторов.

Если производитель обеспечивает своим заказчикам возможность удаленного изменения конфигурации маршрутизатора (например, через сессии Telnet), такую возможность **следует** делать настраиваемой и по умолчанию ее **следует** отключать. Маршрутизатору **следует** выполнять аутентификацию пользователя перед тем, как разрешить удаленное изменение конфигурации. При проверке подлинности пользователей **не следует** передавать секретные сведения (параметры аутентификации) через сеть. Например, при поддержке сессий telnet производителю **следует** реализовать процедуры аутентификации типа Kerberos, S-Key и т. п..

Обсуждение

Предоставление своему оператору полного доступа к вашим маршрутизаторам может оказаться необходимым, предоставление такого доступа кому-то другому является безрассудством.

Для маршрутизаторов **недопустимо** наличие недокументированных потайных способов доступа и паролей. Производитель **должен** гарантировать, что все варианты доступа и пароли, которые могли использоваться в процессе разработки и отладки продукции будут удалены до того, как продукция будет поставлена заказчикам.

Обсуждение

Производители несут перед своими заказчиками ответственность за обеспечение информации об умышленно сохраненных в системе уязвимостях (например, доступ через сеть). Потайные лазейки и master-пароли,

оставленные умышленно или неумышленно, могут сделать такой маршрутизатор серьезной проблемой в работающей сети. Возможные преимущества при обслуживании маршрутизатора никак не компенсируют потенциальных проблем.

11. Литература

Разработчикам следует принимать во внимание, что стандарты для протоколов Internet время от времени изменяются. Приведенные здесь ссылки были актуальны на момент создания этого документа, но внимательные разработчики всегда будут проверять наличие более новых версий RFC или их отмены другими, более новыми RFC[1]. В документе [INTRO:6] указаны различные способы получения текущего списка RFC.

APPL:1. Croft, B., and J. Gilmore, "Bootstrap Protocol (BOOTP)", RFC 951[2], Stanford University, Sun Microsystems, September 1985.

APPL:2. Alexander, S., and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 1533[3], Lachman Technology, Inc., Bucknell University, October 1993.

APPL:3. Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, Carnegie Mellon University, October 1993.

ARCH:1. DDN Protocol Handbook, NIC-50004, NIC-50005, NIC-50006 (three volumes[4]), DDN Network Information Center, SRI International, Menlo Park, California, USA, December 1985.

ARCH:2. V. Cerf and R. Kahn, "A Protocol for Packet Network Intercommunication"[5], IEEE Transactions on Communication, May 1974. Включена в [ARCH:1].

ARCH:3. J. Postel, C. Sunshine, and D. Cohen, "The ARPA Internet Protocol", Computer Networks, volume 5, number 4, July 1981. Включена в [ARCH:1].

ARCH:4. B. Leiner, J. Postel, R. Cole, and D. Mills, :The DARPA Internet Protocol Suite", Proceedings of INFOCOM '85, IEEE, Washington, DC, March 1985. Also in: IEEE Communications Magazine, March 1985. Also available from the Information Sciences Institute, University of Southern California as Technical Report ISI-RS-85-153.

ARCH:5. D. Comer, "Internetworking With TCP/IP Volume 1: Principles, Protocols, and Architecture"[6], Prentice Hall, Englewood Cliffs, NJ, 1991.

ARCH:6. W. Stallings, "Handbook of Computer-Communications Standards Volume 3: The TCP/IP Protocol Suite", Macmillan, New York, NY, 1990.

ARCH:7. Postel, J., "Internet Official Protocol Standards", STD 1, RFC 1780[7], Internet Architecture Board, March 1995.

ARCH:8. Information processing systems - Open Systems Interconnection - Basic Reference Model[8], ISO 7498[9], International Standards Organization, 1984.

ARCH:9 R. Braden, J. Postel, Y. Rekhter, "Internet Architecture Extensions for Shared Media", RFC 1620[10], 05/20/1994

FORWARD:1. IETF CIP Working Group (C. Topolcic, Editor), "Experimental Internet Stream Protocol", Version 2 (ST-II), RFC 1190[11], October 1990.

FORWARD:2. Mankin, A., and K. Ramakrishnan, Editors, "Gateway Congestion Control Survey", RFC 1254, MITRE, Digital Equipment Corporation, August 1991.

FORWARD:3. J. Nagle, "On Packet Switches with Infinite Storage", IEEE Transactions on Communications, volume COM-35, number 4, April 1987[12].

FORWARD:4. R. Jain, K. Ramakrishnan, and D. Chiu, "Congestion Avoidance in Computer Networks With a Connectionless Network Layer", Technical Report DEC-TR-506[13], Digital Equipment Corporation.

FORWARD:5. V. Jacobson, "Congestion Avoidance and Control", Proceedings of SIGCOMM '88, Association for Computing Machinery[14], August 1988.

FORWARD:6. W. Barns, "Precedence and Priority Access Implementation for Department of Defense Data Networks", Technical Report MTR-91W00029, The Mitre Corporation, McLean, Virginia, USA, July 1991.

FORWARD:7 Fang, Chen, Hutchins, "Simulation Results of TCP Performance over ATM with and without Flow Control", presentation to the ATM Forum, November 15, 1993.

FORWARD:8 V. Paxson, S. Floyd "Wide Area Traffic: the Failure of Poisson Modeling"[15], сокращенная версия опубликована в SIGCOMM '94.

[1]Поскольку между подготовкой оригинала и перевода прошло значительное время, мы постарались отметить изменения в RFC, произошедшие за это время. *Прим. перев.*
[2]В RFC 1395, RFC 1497, RFC 1532, RFC 1542 и RFC 5494 содержатся изменения и дополнения. *Прим. перев.*
[3]Этот документ заменен RFC 2132. *Прим. перев.*
[4]Этот документ доступен в сети — том1, том 2, том 3. *Прим. перев.*
[5]Копия статьи доступна по ссылке http://www.cse.ucsc.edu/research/ccrg/CMPE252/Papers/1974.pdf. *Прим. перев.*
[6]Книга доступна по ссылке. *Прим. перев.*
[7]В настоящее время список стандартов Internet доступен по ссылке http://www.rfc-editor.org/rfcxx00.html. *Прим. перев.*
[8]В настоящее время этот стандарт адаптирован в Российской федерации, как ГОСТ Р ИСО 7498-2-99. *Прим. перев.*
[9]В исходном документе ошибочно указано ISO 7489. *Прим. перев.*
[10]В исходном документе по ошибке номер RFC не указан. *Прим. перев.*
[11]Этот документ заменен RFC 1819. *Прим. перев.*
[12]Эта работа опубликована также в RFC 970. *Прим. перев.*
[13]Документ доступен по ссылке http://arxiv.org/ftp/cs/papers/9809/9809095.pdf. *Прим. перев.*
[14]Документ доступен по ссылке. *Прим. перев.*
[15]Документ доступен по ссылке http://www.cs.ucsb.edu/~ravenben/classes/276/papers/pf95.pdf. *Прим. перев.*

FORWARD:9 Leland, Taqqu, Willinger and Wilson, "On the Self-Similar Nature of Ethernet Traffic", Proceedings of SIGCOMM '93[1], September, 1993.

FORWARD:10 S. Keshav "A Control Theoretic Approach to Flow Control", SIGCOMM 91[2], pages 3-16

FORWARD:11 K.K. Ramakrishnan and R. Jain, "A Binary Feedback Scheme for Congestion Avoidance in Computer Networks", ACM Transactions of Computer Systems, volume 8, number 2[3], 1980.

FORWARD:12 H. Kanakia, P. Mishara, and A. Reibman]. "An adaptive congestion control scheme for real-time packet video transport", In Proceedings of ACM SIGCOMM 1994, pages 20-31, San Francisco, California, September 1993.

FORWARD:13 A. Demers, S. Keshav, S. Shenker, "Analysis and Simulation of a Fair Queuing Algorithm", 93 pages 1-12[4]

FORWARD:14 Clark, D., Shenker, S., and L. Zhang, "Supporting Real-Time Applications in an Integrated Services Packet Network: Architecture and Mechanism", 92 pages 14-26[5]

INTERNET:1. Postel, J., "Internet Protocol", STD 5, RFC 791, USC/Information Sciences Institute, September 1981.

INTERNET:2. Mogul, J., and J. Postel, "Internet Standard Subnetting Procedure", STD 5, RFC 950, Stanford, USC/Information Sciences Institute, August 1985.

INTERNET:3. Mogul, J., "Broadcasting Internet Datagrams in the Presence of Subnets", STD 5, RFC 922, Stanford University, October 1984.

INTERNET:4. Deering, S., "Host Extensions for IP Multicasting", STD 5, RFC 1112[6], Stanford University, August 1989.

INTERNET:5. Kent, S., "U.S. Department of Defense Security Options for the Internet Protocol", RFC 1108, BBN Communications, November 1991.

INTERNET:6. Braden, R., Borman, D., and C. Partridge, "Computing the Internet Checksum", RFC 1071, USC/Information Sciences Institute, Cray Research, BBN Communications, September 1988.

INTERNET:7. Mallory T., and A. Kullberg, "Incremental Updating of the Internet Checksum", RFC 1141[7], BBN Communications, January 1990.

INTERNET:8. Postel, J., "Internet Control Message Protocol", STD 5, RFC 792[8], USC/Information Sciences Institute, September 1981.

INTERNET:9. A. Mankin, G. Hollingsworth, G. Reichlen, K. Thompson, R. Wilder, and R. Zahavi, "Evaluation of Internet Performance - FY89", Technical Report MTR-89W00216, MITRE Corporation, February, 1990.

INTERNET:10. G. Finn, A "Connectionless Congestion Control Algorithm", Computer Communications Review, volume 19, number 5, Association for Computing Machinery, October 1989.

INTERNET:11. Prue, W., and J. Postel, "The Source Quench Introduced Delay (SQuID)", RFC 1016, USC/Information Sciences Institute, August 1987.

INTERNET:12. McKenzie, A., "Some comments on SQuID", RFC 1018, BBN Labs, August 1987.

INTERNET:13. Deering, S., "ICMP Router Discovery Messages", RFC 1256, Xerox PARC, September 1991.

INTERNET:14. Mogul J., and S. Deering, "Path MTU Discovery", RFC 1191, DECWRL, Stanford University, November 1990.

INTERNET:15 Fuller, V., Li, T., Yu, J., and K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy" RFC 1519[9], BARRNet, cisco, Merit, OARnet, September 1993.

INTERNET:16 St. Johns, M., "Draft Revised IP Security Option", RFC 1038[10], IETF, January 1988.

INTERNET:17 Prue, W., and J. Postel, "Queuing Algorithm to Provide Type- of-service For IP Links", RFC 1046, USC/Information Sciences Institute, February 1988.

INTERNET:18 Postel, J., "Address Mappings", RFC 796, USC/Information Sciences Institute, September 1981.

INTRO:1. Braden, R., and J. Postel, "Requirements for Internet Gateways", STD 4, RFC 1009[11], USC/Information Sciences Institute, June 1987.

INTRO:2. Internet Engineering Task Force (R. Braden, Editor), "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, USC/Information Sciences Institute, October 1989.

INTRO:3. Internet Engineering Task Force (R. Braden, Editor), "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, USC/Information Sciences Institute, October 1989.

INTRO:4. Clark, D., "Modularity and Efficiency in Protocol Implementations", RFC 817, MIT Laboratory for Computer Science, July 1982.

INTRO:5. Clark, D., "The Structuring of Systems Using Upcalls", Proceedings of 10th ACM SOSP, December 1985.

[1]Документ доступен по ссылке http://www-net.cs.umass.edu/cs691s/leland.pdf. *Прим. перев.*
[2]Документ доступен по ссылке http://blizzard.cs.uwaterloo.ca/keshav/home/Papers/data/91/pp_sigcomm.pdf. *Прим. перев.*
[3]Документ доступен по ссылке http://cseweb.ucsd.edu/classes/fa01/cse222/papers/jain-decbit-tocs90.pdf. *Прим. перев.*
[4]Документ доступен по ссылке. *Прим. перев.*
[5]Документ доступен по ссылке http://pages.cs.wisc.edu/~suman/courses/640/papers/clark92sigcomm.pdf. *Прим. перев.*
[6]В RFC 2236, который был заменен RFC 3376, содержатся изменения и дополнения к этому документу. *Прим. перев.*
[7]В RFC 1624 содержатся изменения и дополнения к этому документу. *Прим. перев.*
[8]В RFC 950 и RFC 4884 содержатся изменения и дополнения к этому документу. *Прим. перев.*
[9]Этот документ обновлен RFC 4632. *Прим. перев.*
[10]Этот документ заменен RFC 1108. *Прим. перев.*
[11]Этот документ утратил силу и заменен настоящим RFC 1812. *Прим. перев.*

INTRO:6. Jacobsen, O., and J. Postel, "Protocol Document Order Information", RFC 980, SRI, USC/Information Sciences Institute, March 1986.

INTRO:7. Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700[1], USC/Information Sciences Institute, October 1994.

INTRO:8. DoD Trusted Computer System Evaluation Criteria[2], DoD publication 5200.28-STD, U.S. Department of Defense, December 1985.

INTRO:9 Malkin, G., and T. LaQuey Parker, Editors, "Internet Users' Glossary", FYI 18, RFC 1392[3], Xylogics, Inc., UTexas, January 1993.

LINK:1. Leffler, S., and M. Karels, "Trailer Encapsulations", RFC 893, University of California at Berkeley, April 1984.

LINK:2 Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661[4], Daydreamer July 1994.

LINK:3 McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", RFC 1332[5], Merit May 1992.

LINK:4 Lloyd, B., and W. Simpson, "PPP Authentication Protocols", RFC 1334[6], L&A, Daydreamer, May 1992.

LINK:5 Simpson, W., "PPP Link Quality Monitoring", RFC 1333[7], Daydreamer, May 1992.

MGT:1. Rose, M., and K. McCloghrie, "Structure and Identification of Management Information of TCP/IP-based Internets", STD 16, RFC 1155, Performance Systems International, Hughes LAN Systems, May 1990.

MGT:2. McCloghrie, K., and M. Rose (Editors), "Management Information Base of TCP/IP-Based Internets: MIB-II", STD 16, RFC 1213[8], Hughes LAN Systems, Inc., Performance Systems International, March 1991.

MGT:3. Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", STD 15, RFC 1157, SNMP Research, Performance Systems International, MIT Laboratory for Computer Science, May 1990.

MGT:4. Rose, M., and K. McCloghrie (Editors), "Towards Concise MIB Definitions", STD 16, RFC 1212, Performance Systems International, Hughes LAN Systems, March 1991.

MGT:5. Steinberg, L., "Techniques for Managing Asynchronously Generated Alerts", RFC 1224, IBM Corporation, May 1991.

MGT:6. Kastenholz, F., "Definitions of Managed Objects for the Ethernet-like Interface Types", RFC 1398[9], FTP Software, Inc., January 1993.

MGT:7. McCloghrie, K., and R. Fox "IEEE 802.4 Token Bus MIB", RFC 1230[10], Hughes LAN Systems, Inc., Synoptics, Inc., May 1991.

MGT:8. McCloghrie, K., Fox R., and E. Decker, "IEEE 802.5 Token Ring MIB", RFC 1231[11], Hughes LAN Systems, Inc., Synoptics, Inc., Cisco Systems, Inc., February 1993.

MGT:9. Case, J., and A. Rijsinghani, "FDDI Management Information Base", RFC 1512, The University of Tennesse and SNMP Research, Digital Equipment Corporation, September 1993.

MGT:10. Stewart, B., Editor "Definitions of Managed Objects for RS-232-like Hardware Devices", RFC 1317[12], Xyplex, Inc., April 1992.

MGT:11. Kastenholz, F., "Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol", RFC 1471, FTP Software, Inc., June 1992.

MGT:12. Kastenholz, F., "The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol", RFC 1472, FTP Software, Inc., June 1992.

MGT:13. Kastenholz, F., "The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol", RFC 1473, FTP Software, Inc., June 1992.

MGT:14. Baker, F., and R. Coltun, "OSPF Version 2 Management Information Base", RFC 1253[13], ACC, Computer Science Center, August 1991.

MGT:15. Willis, S., and J. Burruss, "Definitions of Managed Objects for the Border Gateway Protocol (Version 3)", RFC 1269[14], Wellfleet Communications Inc., October 1991.

MGT:16. Baker, F., and J. Watt, "Definitions of Managed Objects for the DS1 and E1 Interface Types", RFC 1406[15], Advanced Computer Communications, Newbridge Networks Corporation, January 1993.

[1] В RFC 3232 документ Assigned Numbers отменен, данные доступны на сайте www.iana.org. *Прим. перев.*
[2] Копия этого документа доступна на сайте http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html. *Прим. перев.*
[3] Этот документ заменен RFC 1983. *Прим. перев.*
[4] В RFC 2153 содержатся изменения и дополнения к этому документу. *Прим. перев.*
[5] Этот документ обновлен RFC 3241. *Прим. перев.*
[6] Этот документ заменен RFC 1994, который был обновлен RFC 2484. *Прим. перев.*
[7] Этот документ заменен RFC 1989. *Прим. перев.*
[8] В RFC 2011, RFC 2012, RFC 2013 содержатся изменения и дополнения к этому документу. *Прим. перев.*
[9] Этот документ заменен RFC 1623, который был заменен RFC 1643, а тот был отменен RFC 3638. *Прим. перев.*
[10] В RFC 1239 содержатся изменения и дополнения к этому документу. *Прим. перев.*
[11] Этот документ заменен RFC 1743, а тот, в свою очередь, - RFC 1748. *Прим. перев.*
[12] Этот документ заменен RFC 1659. *Прим. перев.*
[13] Этот документ заменен RFC 1850, а тот, в свою очередь, - RFC 4750. *Прим. перев.*
[14] Этот документ заменен RFC 4273. *Прим. перев.*
[15] Этот документ заменен RFC 2495, тот - RFC 3895, а последний - RFC 4805. *Прим. перев.*

MGT:17. Cox, T., and K. Tesink, Editors "Definitions of Managed Objects for the DS3/E3 Interface Types", RFC 1407[1], Bell Communications Research, January 1993.

MGT:18. McCloghrie, K., "Extensions to the Generic-Interface MIB", RFC 1229[2], Hughes LAN Systems, August 1992.

MGT:19. Cox, T., and K. Tesink, "Definitions of Managed Objects for the SIP Interface Type", RFC 1304[3], Bell Communications Research, February 1992.

MGT:20 Baker, F., "IP Forwarding Table MIB", RFC 1354[4], ACC, July 1992.

MGT:21. Malkin, G., and F. Baker, "RIP Version 2 MIB Extension", RFC 1724, Xylogics, Inc., Cisco Systems, November 1994

MGT:22. Throop, D., "SNMP MIB Extension for the X.25 Packet Layer", RFC 1382, Data General Corporation, November 1992.

MGT:23. Throop, D., and F. Baker, "SNMP MIB Extension for X.25 LAPB", RFC 1381, Data General Corporation, ACC, November 1992.

MGT:24. Throop, D., and F. Baker, "SNMP MIB Extension for MultiProtocol Interconnect over X.25", RFC 1461, Data General Corporation, May 1993.

MGT:25. Rose, M., "SNMP over OSI", RFC 1418, Dover Beach Consulting, Inc., March 1993.

MGT:26. Minshall, G., and M. Ritter, "SNMP over AppleTalk", RFC 1419, Novell, Inc., Apple Computer, Inc., March 1993.

MGT:27. Bostock, S., "SNMP over IPX", RFC 1420, Novell, Inc., March 1993.

MGT:28. Schoffstall, M., Davin, C., Fedor, M., and J. Case, "SNMP over Ethernet", RFC 1089[5], Rensselaer Polytechnic Institute, MIT Laboratory for Computer Science, NYSERNet, Inc., University of Tennessee at Knoxville, February 1989.

MGT:29. Case, J., "FDDI Management Information Base", RFC 1285[6], SNMP Research, Incorporated, January 1992.

OPER:1. Nagle, J., "Congestion Control in IP/TCP Internetworks", RFC 896, FACC, January 1984.

OPER:2. Sollins, K., "TFTP Protocol (revision 2)", RFC 1350[7], MIT, July 1992.

ROUTE:1. Moy, J., "OSPF Version 2", RFC 1583[8], Proteon, March 1994.

ROUTE:2. Callon, R., "Use of OSI IS-IS for Routing in TCP/IP and Dual Environments", RFC 1195[9], DEC, December 1990.

ROUTE:3. Hedrick, C., "Routing Information Protocol", RFC 1058[10], Rutgers University, June 1988.

ROUTE:4. Lougheed, K., and Y. Rekhter, "A Border Gateway Protocol 3 (BGP-3)", RFC 1267[11], cisco, T.J. Watson Research Center, IBM Corp., October 1991.

ROUTE:5. Gross, P, and Y. Rekhter, "Application of the Border Gateway Protocol in the Internet", RFC 1772, T.J. Watson Research Center, IBM Corp., MCI, March 1995.

ROUTE:6. Mills, D., "Exterior Gateway Protocol Formal Specification", RFC 904, UDEL, April 1984.

ROUTE:7. Rosen, E., "Exterior Gateway Protocol (EGP)", RFC 827[12], BBN, October 1982.

ROUTE:8. Seamonson, L, and E. Rosen, "STUB" "Exterior Gateway Protocol", RFC 888[12], BBN, January 1984.

ROUTE:9. Waitzman, D., Partridge, C., and S. Deering, "Distance Vector Multicast Routing Protocol", RFC 1075, BBN, Stanford, November 1988.

ROUTE:10. Deering, S., Multicast Routing in Internetworks and Extended LANs, Proceedings of '88, Association for 1122Computing Machinery[13], August 1988.

ROUTE:11. Almquist, P., "Type of Service in the Internet Protocol Suite", RFC 1349[14], Consultant, July 1992.

ROUTE:12. Rekhter, Y., "Experience with the BGP Protocol", RFC 1266, T.J. Watson Research Center, IBM Corp., October 1991.

ROUTE:13. Rekhter, Y., "BGP Protocol Analysis", RFC 1265, T.J. Watson Research Center, IBM Corp., October 1991.

TRANS:1. Postel, J., "User Datagram Protocol", STD 6, RFC 768, USC/Information Sciences Institute, August 1980.

TRANS:2. Postel, J., "Transmission Control Protocol", STD 7, RFC 793, USC/Information Sciences Institute, September 1981.

[1]Этот документ заменен RFC 2496, а тот - RFC 3896. *Прим. перев.*
[2]Этот документ заменен RFC 1573, тот - RFC 2233, а последний - RFC 2863. *Прим. перев.*
[3]Этот документ заменен RFC 1694. *Прим. перев.*
[4]Этот документ заменен RFC 2096, а тот - RFC 4292. *Прим. перев.*
[5]Этот документ заменен 4789. *Прим. перев.*
[6]В RFC 1512 содержатся изменения и дополнения к этому документу. *Прим. перев.*
[7]В RFC 1782 - RFC 1785, RFC 2347 - RFC 2349 содержатся изменения и дополнения к этому документу. *Прим. перев.*
[8]Этот документ заменен RFC 2178, а тот - RFC 2328, обновленным в RFC 5709. *Прим. перев.*
[9]В RFC 1349 (отменен RFC 2474) содержатся изменения и дополнения к этому документу. *Прим. перев.*
[10]В RFC 1388 (отменен RFC 1723, который, в свою очередь, был отменен RFC 2453, обновленным RFC 4822) содержатся изменения и дополнения к этому документу. *Прим. перев.*
[11]Спецификация современной версии протокола BGP4 содержится в RFC 4271. *Прим. перев.*
[12]В RFC 904 содержатся изменения и дополнения к этому документу. *Прим. перев.*
[13]Копия этой статьи доступна по ссылке http://pages.cs.wisc.edu/~akella/CS740/S08/740-Papers/DC88.pdf. *Прим. перев.*
[14]Этот документ заменен RFC 2474, который был обновлен в RFC 3168 и RFC 3260. *Прим. перев.*

Приложение A. Требования к хостам SOURCE-ROUTING

С учетом приведенных ниже ограничений хост **может** использоваться в качестве промежуточного интервала (intermediate hop) заданного отправителем маршрута, пересылая дейтаграммы с опцией source route на следующий заданный интервал.

Однако при выполнении таких функций хост **должен** подчиняться всем имеющим отношение к таким случаям правилам для маршрутизатора, пересылающего дейтаграммы с заданной отправителем маршрутизацией [INTRO:2]. Эти требования перечислены ниже.

(A) TTL

Значение поля TTL **должно** уменьшаться и дейтаграммы могут отбрасываться, как указано для маршрутизаторов в документе [INTRO:2].

(B) ICMP Destination Unreachable

Хост **должен** быть способен генерировать сообщения Destination Unreachable с кодами:

4 Fragmentation Required but DF Set, когда дейтаграмма с заданным отправителем маршрутом не может быть фрагментирована в соответствии с требованиями сети, куда ее нужно переслать;

5 Source Route Failed, когда дейтаграмма с заданным отправителем маршрутом не может быть переслана (например, в результате проблем с маршрутизацией или по причине того, что следующий интервал , заданный в опции strict source route, не относится к подключенной сети).

(C) IP-адрес отправителя

Пересылаемые дейтаграммы с заданным отправителем маршрутом **могут** иметь (и обычно имеют) адрес отправителя, который не совпадает ни с одним из адресов пересылающего хоста.

(D) Опция Record Route

Хост, пересылающий дейтаграмму с заданной отправителем маршрутизацией и опцией Record Route, **должен** сделать свою запись в эту опцию, если в последней имеется свободное место.

(E) Опция Timestamp

Хост, пересылающий дейтаграмму с заданным отправителем маршрутом и опцией Timestamp, **должен** добавить в опцию текущую временную метку согласно правилам работы с опцией.

Для определения правил, ограничивающих пересылку хостами дейтаграмм с заданным отправителем маршрутом используется термин local source-routing (локальная пересылка), если следующий интервал доставки доступен через тот же физический интерфейс, через который была принята эта дейтаграмма, в противном случае используется термин non-local source-routing (нелокальная пересылка).

Хостам разрешено выполнять локальную пересылку дейтаграмм с заданным отправителем маршрутом без каких-либо ограничений.

Хост, поддерживающий нелокальную пересылку дейтаграмм с заданным отправителем маршрутом, **должен** иметь конфигурационный параметр для запрета пересылки и по умолчанию такая пересылка **должна** быть запрещена.

Хост **должен** соответствовать всем требованиям, предъявляемым к маршрутизаторам, в части настраиваемых фильтров, ограничивающих нелокальную пересылку дейтаграмм с заданным отправителем маршрутом [INTRO:2].

Если хост получает дейтаграмму с незавершенным маршрутом source route и не пересылает ее по какой-либо причине, ему **следует** вернуть отправителю сообщение ICMP Destination Unreachable с кодом 5 (Source Route Failed), если сама дейтаграмма не была сообщением ICMP об ошибке.

Приложение B. Глоссарий

В этом приложении даны определения терминов, использованных в документе, а также некоторых терминов общего назначения, которые могут представлять интерес. Более полный список терминологических определений общего назначения представлен в документе [INTRO:9].

Autonomous System (AS) - *автономная система*

Автономная система представляет собой сегмент сетевой топологии, который состоит из набора подсетей (с подключенными к ним хостами), соединенных между собой маршрутизаторами. Предполагается, что маршрутизаторы и подсети находятся под управлением (O&M) одной организации. Внутри AS маршрутизаторы могут использовать один или множество протоколов внутренней маршрутизации и иногда несколько наборов метрик. Предполагается, что с точки зрения других AS данная автономная система представляет согласованный план внутренней маршрутизации и картину адресатов, доступных через данную AS. Автономные системы идентифицируются своими номерами.

Connected Network - *подключенная сеть*

Сеть (сетевой префикс), в которую маршрутизатор имеет интерфейс и которую часто называют локальной сетью или подсетью данного маршрутизатора. Однако два последних термина могут приводить к путанице и, следовательно, использование термина «подключенная сеть» является более корректным.

Connected (Sub)Network - *подключенная (под)сеть*

Подключенная (под)сеть представляет собой подсеть IP, в которую маршрутизатор имеет интерфейс. См. также Connected Network.

Datagram - *дейтаграмма*

Единица информации, передаваемая между парой модулей IP. Протокол IP не обеспечивает гарантированной доставки дейтаграмм и не использует механизмов сквозного или поэтапного подтверждения доставки. Не используется в IP и контроля за потоками данных. См. также IP.

Default Route - *маршрут по умолчанию*

Запись таблицы маршрутизации, используемая для передачи любых данных, адресованных во все сети, для которых в таблице маршрутизации отсутствуют явные записи.

Dense Mode *- режим Dense*

При групповой пересылке могут использоваться две парадигмы. В режиме Dense групповые пакеты сетевого уровня пересылаются, как групповые кадры канального уровня во все интерфейсы, за исключением принявшего исходный пакет, если маршрутизатору не запрещена групповая пересылка. См. также Sparse Mode.

EGP

Протокол внешнего шлюза (Exterior Gateway Protocol). Протокол, используемый для распространения маршрутной информации между шлюзами (маршрутизаторами), соединяющими автономные системы. См. также IGP.

EGP-2

Протокол EGP версии 2. Это протокол внешней маршрутизации, разработанный для обмена маршрутными данными между автономными системами в сети Internet.

Forwarder *- модуль пересылки*

Логический объект в маршрутизаторе, отвечающий за «коммутацию» пакетов между интерфейсами маршрутизатора. Модуль пересылки также принимает решения о помещении пакета в очередь локальной доставки, очередь пересылки или одновременно в обе очереди.

Forwarding - *пересылка*

Пересылка представляет собой процесс, выполняемый маршрутизатором по отношению к каждому полученному пакету. Пакет может быть воспринят самим маршрутизатором, передан через один или несколько интерфейсов маршрутизатора или одновременно воспринят локально и переслан в другой интерфейс (интерфейсы).

Forwarding Information Base (FIB) *- база данных о пересылке*

Таблица, содержащая информацию, необходимую для пересылки дейтаграмм IP. Каждая запись таблицы содержит, как минимум, идентификатор интерфейса и адрес следующего интервала на пути пересылки к заданному адресату (префиксу сети).

Fragment - *фрагмент*

Дейтаграмма IP, содержащая часть пакета вышележащего уровня, который невозможно передать через сеть целиком.

General Purpose Serial Interface *- последовательный интерфейс общего назначения*

Физическая среда, обеспечивающая возможность организации соединения между парой систем и настраиваемая на работу в режиме «точка-точка», но поддерживающая также канальный уровень на базе протоколов типа X.25 или Frame Relay. Канальный уровень позволяет подключать другие системы к коммутаторам и вышележащие уровни мультиплексируют виртуальные устройства для соединений. См. также Point to Point Line.

IGP

Протокол внутреннего шлюза (Interior Gateway Protocol). Протокол, распространяющий маршрутные данные внутри автономной системы. См. также EGP.

Interface IP Address - *IP-адрес интерфейса*

Адрес IP и размер сетевого префикса, присвоенные определенному интерфейсу маршрутизатора.

Internet Address *- адрес Internet*

Специальное значение, позволяющее идентифицировать хост в internet. Адрес состоит из 2 частей - IP-адреса и длины префикса. Длина префикса показывает, какая часть старших битов адреса относится к префиксу сети.

IP

Internet Protocol. Протокол сетевого уровня в Internet, описанный в RFC 791. Протокол IP не гарантирует доставку пакетов (т. е., не поддерживает сквозного или поэтапного подтверждения доставки).

IP Datagram - *дейтаграмма IP*

Дейтаграмма IP представляет собой единицу информационного обмена для протокола IP. Дейтаграмма IP состоит из заголовка IP, за которым следуют данные - сообщение протокола вышележащего уровня (TCP, UDP, ICMP и пр.).

Дейтаграмма IP представляет собой законченный объект сквозного обмена данными на уровне IP. Дейтаграмма IP может состоять из одного или множества фрагментов IP.

В данном документе термин «дейтаграмма», приведенный без дополнительных уточнений, относится к дейтаграмме IP.

IP Fragment - *фрагмент IP*

Фрагмент IP представляет собой часть дейтаграммы IP. Фрагмент IP состоит из заголовка IP, за которым следует часть данных вышележащего уровня исходной дейтаграммы IP или дейтаграмма целиком.

Один или несколько фрагментов IP образуют дейтаграмму IP.

В этом документе термин «фрагмент», приведенный без дополнительных уточнений, относится к фрагменту IP.

IP Packet - *пакет IP*

Дейтаграмма IP или фрагмент IP.

В данном документе термин «пакет», приведенный без дополнительных уточнений, означает пакет IP.

Logical [network] interface - *логический [сетевой] интерфейс*

Логический [сетевой] интерфейс представляет собой путь соединения с сетью, указанный уникальным адресом IP[1].

Martian Filtering *- фильтрация пакетов с недопустимыми адресами[2]*

Отбрасывание пакетов, содержащих в заголовке недопустимые адреса отправителей или получателей.

MTU (Maximum Transmission Unit) - *максимальный размер передаваемого блока*

Размер наибольшего пакета, который можно передать или принять через логический интерфейс. Размер учитывает заголовок IP, но не учитывает заголовки или кадрирование канального уровня.

---

[1] Не совсем точное определение. Интерфейс может быть безадресным. У интерфейса должен быть уникальный в масштабе системы (хоста, маршрутизатора) идентификатор, но это не обязательно адрес IP. *Прим. перев.*

[2] В буквальном переводе - «фильтрация марсианских пакетов». *Прим. перев.*

***Multicast** - групповой пакет*

Пакет, адресованный множеству хостов. См. также broadcast.

***Multicast Address** - групповой адрес*

Специальный тип адреса, который позволяет передать пакет множеству хостов.

Для таких адресов используются также термины Functional Address и Group Address.

***Network Prefix** - префикс сети*

Часть адреса IP, обозначающая множество систем. Префикс выделяется из адреса IP путем применения операции AND (логическое И) к значениям адреса и маски подсети или путем выбора числа старших битов адреса, заданного размером префикса, и установки для оставшихся битов значения 0.

***Originate** - происхождение*

Пакеты, передаваемые маршрутизатором, можно разделить на 2 категории: 1) полученные и пересылаемые в другие интерфейсы и 2) созданные самим маршрутизатором (например, анонсы маршрутов). О пакетах, созданных самим маршрутизатором, говорят как о пакетах, происходящих от маршрутизатора.

***Packet** - пакет*

Пакет представляет собой единицу данных, передаваемую через интерфейс между уровнем Internet и канальным уровнем. Пакет включает заголовок IP и данные. Пакет может быть полной дейтаграммой IP или фрагментом IP.

***Path** - путь*

Последовательность маршрутизаторов и (под)сетей, через которые пакет проходит от определенного маршрутизатора к конечному адресату. Отметим, что путь имеет два направления и нет ничего странного в том, что пакеты между данной парой хостов идут разными путями в каждом из направлений.

***Physical Network** - физическая сеть*

Физическая сеть представляет собой сеть (или часть internet), которая непрерывна на канальном уровне. Внутренняя структура такой сети (если она имеется) прозрачна для уровня Internet.

В этом документе несколько сетевых сред, соединенных между собой мостами или повторителями, рассматриваются, как физическая сеть, поскольку они прозрачны для IP.

***Physical Network Interface** - физический сетевой интерфейс*

Физический интерфейс в подключенную сеть, имеющий (возможно уникальный) адрес канального уровня. Множество физических интерфейсов одного маршрутизатора могут использовать общий адрес канального уровня, но адреса канального уровня для всех маршрутизаторов одной физической сети должны быть уникальными.

***Point to Point Line** - линия «точка-точка»*

Физическая среда, способная соединять между собой пару систем. В данном документе этот термин используется только для обозначения линий, соединяющих между собой объекты IP. См. также General Purpose Serial Interface.

***Router** - маршрутизатор*

Выделенный компьютер специального назначения, соединенный с несколькими сетями. Маршрутизатор «коммутирует» пакеты между сетями и этот процесс называется пересылкой (forwarding). Процесс пересылки может повторяться для одного пакета множество раз на разных маршрутизаторах, пока пакет не будет доставлен конечному адресату.

***RPF (Reverse Path Forwarding)** - пересылка по обратному пути*

Метод, который может быть полезен для определения следующего интервала при пересылке групповых или широковещательных пакетов.

***Silently Discard** - отбрасывание без уведомления*

В этом документе описано несколько ситуаций, когда маршрутизатор отбрасывает пакеты (или дейтаграммы), не уведомляя об этом их отправителя. Это означает, что маршрутизатор просто отбрасывает пакет без дальнейшей обработки и не передает в результате никаких сообщений ICMP об ошибках (см. параграф 4.3.2). Однако для диагностики проблем маршрутизаторам следует поддерживать возможность записи информации о фактах отбрасывания в журнальные файлы системы (см. параграф 1.3.3), сохраняя в файле содержимое отбрасываемых пакетов, и вести учет числа таких пакетов.

***Silently Ignore** - игнорирование без уведомления*

Говорят, что маршрутизатор игнорирует ошибки или какие-либо условия без уведомления в тех случаях, когда маршрутизатор не выполняет в ответ на событие таких операций, как генерация сообщения об ошибке, запись в системный журнал или генерация сообщения для протокола сетевого управления, игнорируя (или отбрасывая) источник таких ошибок. В частности, маршрутизатор не генерирует в таких случаях сообщений ICMP об ошибках.

Sparse Mode

При групповой пересылке возможны два варианта - в режиме Sparse групповые дейтаграммы сетевого уровня пересылаются, как групповые кадры канального уровня маршрутизаторам и хостам, которые запросили такую пересылку. В исходном состоянии пересылка находится в инверсном режиме Dense, т. е. предполагается, что никто не хочет получать групповые пакеты. См. также Dense Mode.

***Specific-destination address** - адрес конкретного получателя*

Адрес получателя в заголовке IP, если последний не содержит группового или широковещательного IP-адреса. В последнем случае адресом конкретного получателя считается IP-адрес физического интерфейса, через который был получен пакет.

***Subnet** - подсеть*

Часть сети, которая может быть физически независимой сетью, разделяющая сетевой адрес с другими частями сети и отличающаяся от них номером подсети. Подсеть по отношению к сети - то же самое, что сеть по отношению к internet.

***Subnet number** - номер подсети*

Часть IP-адреса, идентифицирующая данную подсеть. Номер подсети игнорируется в процессах internet-маршрутизации, но принимается во внимание при маршрутизации внутри intranet.

***TOS (Type Of Service)** - тип обслуживания*

Поле заголовка IP, которое представляет уровень гарантий, ожидаемых от сетевого уровня транспортным уровнем или приложениями.

TTL (Time To Live) - *время жизни*

Поле в заголовке IP определяющее срок существования пакета в сети. Значение поля представляет собой комбинацию таймера и счетчика интервалов в сети.

Приложение C. Перспективы развития документа

В этом приложении приведен список направлений, которые могут быть разработаны в будущих версиях документа.

При подготовке документа Router Requirements рабочая группа столкнулась с некоторыми архитектурными вопросами. Каждый из этих вопросов в той или иной степени затронут в этом документе, но остается открытым в архитектуре IP.

Большинство представленных здесь тем относится к областям, где применяются сравнительно новые технологии и пока не разработаны соответствующие требования по причине отсутствия нужного для этого опыта.

Другие темы представляют собой области, в которых еще ведутся исследования и на которые предусмотрительным разработчикам следует обратить пристальное внимание.

(1) SNMP версии 2.

(2) Дополнительные SNMP MIB.

(7) Более детальные требования для передачи маршрутов между разными протоколами маршрутизации.

(8) Безопасность маршрутизаторов.

(9) Безопасность протоколов маршрутизации.

(10) Безопасность протоколов межсетевого взаимодействия (Internetwork Protocol layer). Следует включить в документ результаты многочисленных работ по безопасности IP.

(12) Расщепление нагрузки (Load Splitting).

(13) Передача фрагментов по разным путям.

(15) Множество логических (под)сетей в одной кабельной сети. Требования к маршрутизаторам не требуют поддержки такой возможности. Мы пытаемся идентифицировать компоненты архитектуры (например, пересылка directed broadcast или генерация сообщений Redirect), где нужна аккуратная формулировка правил для обеспечения корректной работы и пытаемся отделить логические интерфейсы от физических. Однако мы не изучали этот вопрос достаточно детально и не готовы утверждать, что все сформулированные в этом документе правила будут корректно работать при наличии множества логических (под)сетей в одной кабельной среде.

(15) Контроль насыщения и управление ресурсами. По совету экспертов IETF (Mankin и Ramakrishnan) внесено возражение против использования (**не следует**) Source Quench и приведены некоторые конкретные соображения на эту тему (параграф 5.3.6).

(16) Разработка документа с требованиями для канального уровня, которые будут общими для маршрутизаторов и хостов.

(17) Разработка алгоритма общего назначения PPP LQM.

(18) Исследование другой информации (см. предыдущие пункты и главу 3.2), передаваемой между уровнями - значение MTU для физической сети, отображение предпочтений IP на приоритеты канального уровня и т. п.

(19) Решение вопроса о том, следует ли канальному уровню уведомлять IP при неудаче преобразования адреса (как это делается при уведомлении уровня IP канальным уровнем в случае возникновения проблем со значениями приоритета).

(20) Следует ли требовать от всех маршрутизаторов реализации DNS resolver?

(21) Следует ли позволять пользователям применять имя хоста вместо адреса IP при настройке конфигурации маршрутизатора или в командах ping и traceroute?

(22) Работы Алмквиста (Almquist) по поводу следующего интервала (next hop) и утечки маршрутов (route leaking) нужно заново рассмотреть, привести в соответствии с текущей ситуацией и опубликовать.

(23) Требуется проведение исследований по поводу целесообразности использования перенаправления в соответствии с запрошенным уровнем предпочтения. Если это будет признано нецелесообразным, следует ли воспринимать перенаправления по типу обслуживания?

(24) RIPv2, RIP+CIDR и сетевые префиксы переменной длины.

(25) BGP-4 CIDR становится важным и все делают ставку на BGP-4. Мы не можем оставить этот вопрос без внимания. Возможно следует описать различия между BGP-3 и BGP-4, а также рассмотреть вопросы обновления ...

(26) Поддержка Loose Source Route Mobile IP и некоторых типов групповой передачи может стать более важной. Возможно для этих требований нужно поднять уровень до «**следует**» (как предлагает Fred Baker).

Приложение D. Протоколы групповой маршрутизации

Групповая передача (Multicasting) является сравнительно новой технологией в семействе протоколов IP. Она пока распространена недостаточно широко и не является общепринятой. Однако можно предположить рост интереса к этой технологии в будущем.

В этом приложении кратко описаны некоторые технологии, которые исследуются для передачи группового трафика через Internet.

Предусмотрительным разработчикам следует контролировать это направление исследований для своевременной подготовки функций групповой маршрутизации в своей продукции.

В этом приложении не содержится никаких стандартов и не задаются какие-либо требования.

D.1 Введение

Протоколы групповой маршрутизации обеспечивают возможность пересылки групповых дейтаграмм IP через сети TCP/IP. В общем случае эти алгоритмы пересылают дейтаграммы на основе указанных в заголовках адресов отправителей и получателей. В дополнение к этому может потребоваться пересылка дейтаграммы нескольким членам группы, иной раз требующая репликации дейтаграммы и ее передачи через множество интерфейсов.

Протоколы групповой маршрутизации разработаны существенно слабее протоколов маршрутизации индивидуального трафика IP. Для стека TCP/IP документированы три экспериментальных протокола групповой маршрутизации. Все они используют протокол IGMP (см. параграф 4.4) для мониторинга принадлежности к группам.

D.2 Протокол DVMRP

Протокол DVMRP[1], описанный в [ROUTE:9], основан на технологии Distance Vector или Bellman-Ford. Протокол предназначен для маршрутизации только групповых дейтаграмм и делает это в пределах одной автономной системы. DVMRP является реализацией алгоритма Truncated Reverse Path Broadcasting, описанного в [ROUTE:10]. Кроме того, протокол поддерживает туннелирование групповых дейтаграмм IP через домены, не поддерживающие групповую адресацию.

D.3 Групповое расширение для OSPF - MOSPF

Протокол MOSPF, разработка которого еще продолжается[2], обеспечивает совместимость с протоколом OSPF и позволяет пересылать как групповые, так и индивидуальные дейтаграммы IP в пределах автономной системы. Маршрутизаторы MOSPF можно смешивать с маршрутизаторами OSPF в одном домене маршрутизации и они будут интероперабельны в части пересылки индивидуальных дейтаграмм. OSPF представляет собой протокол маршрутизации с учетом состояния каналов, основанный на алгоритме SPF.

Кроме анонсирования состояния канала, которое показывает принадлежность к группам, маршрутизаторы MOSPF могут рассчитывать путь multicast-дейтаграммы, как дерево с корнем в точке отправки. Ветви, не содержащие членов групп, могут отбрасываться, что позволяет избавиться от ненужных пересылок.

D.4 Независимая от протокола групповая передача - PIM

Протокол PIM[3], разработка которого еще продолжается[4], представляет собой протокол групповой маршрутизации, который работает поверх существующей unicast-инфраструктуры. PIM обеспечивает поддержку режимов dense и sparse для пересылки группового трафика. Этот протокол отличается от других тем, что он использует модель явного присоединения для sparse-групп. Подключение к группе происходит на общем дереве и может изменяться на уровне дерева отправителя. Там, где полоса достаточно широка и используется dense-режим подключения к группам, издержки могут быть снижены за счет лавинной рассылки данных во все каналы (за исключением тех, где отсутствуют члены группы) с последующим отсечением ненужных.

Приложение E. Другие алгоритмы определения Next-Hop

В параграфе 5.2.4.3 рассмотрен алгоритм, который маршрутизаторы должны использовать при выборе следующего интервала для пересылки пакета.

В этом приложении приводится ретроспективный взгляд на проблему выбора следующего интервала и представлены несколько дополнительных правил сокращения и алгоритмов выбора next-hop, которые можно встретить в Internet.

В приложении представлены черновые материалы из неопубликованной работы Филиппа Алмквиста (Philip Almquist) Ruminations on the Next Hop[5].

В этом приложении не содержится никаких стандартов и не задаются какие-либо требования.

E.1. Немного истории

Будет полезен краткий экскурс в историю вопроса, начиная с периода, который иногда называют «классической моделью» принятия маршрутизаторами решения о пересылке. Эта модель старше протокола IP. В данной модели маршрутизаторы обмениваются информацией с помощью одного протокола маршрутизации (например, RIP). Данный протокол полностью определяет для маршрутизаторов содержимое базы данных о пересылке (FIB). Алгоритм поиска маршрута тривиален - маршрутизатор просто просматривает FIB в поисках пути, атрибуты которого в точности совпадают с сетевым префиксом адреса получателя в пакете. Если такой маршрут найден, он будет использован для пересылки пакета, при отсутствии нужного маршрута адресат считается недоступным. Поскольку протокол маршрутизации сохраняет только один маршрут к каждому адресату, проблемы выбора маршрута из нескольких просто не возникает.

Спустя годы эта классическая модель была несколько расширена. С использованием маршрутов по умолчанию, подсетей и путей к хостам стало возможным присутствие в таблице маршрутов нескольких записей, которые в разной степени соответствуют адресату пакета. Проблема выбора одного маршрута из нескольких легко решалась с помощью соглашения об иерархии маршрутов - маршруты к хостам были предпочтительней маршрутов в подсети, последние были более предпочтительны, нежели маршруты в сети и самых низший уровень занимали маршруты, используемые по умолчанию.

Разработка технологий поддержки масок подсетей переменной длины (переменной длины префиксов) не изменила суть алгоритма, хотя его описание стало несколько сложнее. Для упрощения и упорядочения архитектуры было

[1]Distance Vector Multicast Routing Protocol.
[2]Разработка протокола завершена и его спецификация опубликована в RFC 1584. *Прим. перев.*
[3]Protocol Independent Multicast — независимая от протокола групповая адресация.
[4]Спецификация протокола PIM-SM (Sparse Mode) опубликована в RFC 2362. *Прим. перев.*
[5]Размышления о следующем интервале.

введено понятие сетевых префиксов. Сейчас мы говорим, что каждый маршрут в сеть с определенным префиксом имеет связанное с этим маршрутом значение длины префикса, задаваемое числом битов. Такое же представление возможно и с использованием классических масок подсетей. Маршрут не может использоваться для передачи по нему пакетов, пока все старшие биты сетевого префикса для этого маршрута не будут совпадать с соответствующими битами в адресе получателя. Маршруты с большим числом битов в маске являются более предпочтительными. Это простое обобщение иерархии маршрутов, рассмотренной выше, и в остальной части документа мы будем считать наиболее предпочтительным маршрут с максимальной длиной соответствия.

Другим изменением классической модели стал отказ от допущения, что протокол маршрутизации полностью контролирует содержимое таблицы маршрутизации. Сначала появились статические маршруты. В результате возникла возможность наличия в таблице двух маршрутов к одному адресату - статического и динамического. Когда это произошло, маршрутизаторы начали поддерживать правила (настраиваемые с помощью параметров конфигурации или заданные разработчиками программ маршрутизации) для выбора между статическими и динамическими маршрутами. Однако эти правила использовались, по сути, лишь для выбора в случае совпадения размера префиксов у статического и динамического маршрутов. С помощью правил подобного типа невозможно, например, сделать более предпочтительным маршрут, принятый по умолчанию, поскольку для него длина совпадения всегда равна нулю.

Дополнительные изменения классической модели связаны с разработкой протоколов междоменной маршрутизации. Традиционные протоколы маршрутизации стали обозначать аббревиатурой IGP (interior gateway protocol - протокол внутреннего шлюза) и на каждом сайте Internet появились странные создания, названные внешними шлюзами, которые с помощью протокола EGP обменивались информацией с несколькими центральными маршрутизаторами BBN[1] и одновременно использовали протокол IGP для обмена с другими маршрутизаторами своего сайта. Оба протокола хотели иметь контроль над содержимым таблицы маршрутизации. Теоретически это могло приводить к наличию в маршрутизаторе трех путей (EGP, IGP, статический маршрут) к одному адресату. С учетом топологии Internet того времени после некоторых дебатов было принято правило, в соответствии с которым маршруты IGP считались более предпочтительными по сравнению с маршрутами EGP. Однако проблемы, связанные с длиной соответствия, остались нерешенными. Полученный от IGP маршрут по умолчанию никогда не будет более предпочтительным по сравнению с маршрутом в сеть, полученным от EGP.

Хотя топология и картина маршрутизации в Internet с тех пор существенно изменились, слегка модифицированная версия классической модели продолжает использоваться в Internet (с протоколом BGP взамен EGP). Концептуально (а часто и в реализациях) каждый маршрутизатор имеет таблицу маршрутизации и один или несколько процессов для протоколов маршрутизации. Каждый из таких процессов может по своему усмотрению добавлять записи в таблицу, а также изменять или удалять свои записи в таблице. При маршрутизации пакета маршрутизатор выбирает лучший маршрут по максимальной длине соответствия с учетом правил выбора при одинаковой длине. Хотя эта обновленная классическая модель используется до сих пор, ей присущ ряд недостатков.

- Игнорируются (хотя это не обязательно) характеристики путей (такие, как тип обслуживания и MTU).
- Не поддерживаются протоколы маршрутизации (такие, как OSPF и Integrated IS-IS), которым нужен алгоритм выбора маршрута, отличающийся от сравнения длины соответствия.
- Нет согласия между производителями по поводу механизма tie-breaking[2]. Этот механизм зачастую сложно (а иногда невозможно) настроить таким образом, чтобы маршрутизатор выбирал при прочих равных маршрут в соответствии с заданными администратором предпочтениями.

E.2. Дополнительные правила сокращения

В параграфе 5.2.4.3 определено несколько правил сокращения при выборе маршрутов из FIB. Ниже приведены дополнительные правила, которые можно использовать для сокращения.

- **Класс маршрута OSPF**

  Протоколы маршрутизации, которые могут поддерживать области, или различают внутренние и внешние маршруты, деля их на классы по типу используемой при расчете маршрута информации. Маршрут всегда выбирается из наиболее предпочтительного класса, затем из следующего по уровню предпочтения (если ничего не найдено в первом) и т. д. В OSPF используются классы (в порядке убывания уровня предпочтений) intra-area (внутри области), inter-area (между областями), type 1 external (внешние маршруты с внутренней метрикой), type 2 external. Дополнительно можно задать для маршрутизатора набор адресов, которые будут доступны внутри области и для которых не будут использоваться маршруты между областями или внешние пути даже при недоступности маршрута внутри области.

  Говоря точнее, предполагается, что каждый маршрут имеет атрибут, называемый классом маршрута (route.class), который присваивается протоколом маршрутизации. Набор маршрутов-кандидатов проверяется на предмет наличия в нем маршрутов с route.class = intra-area. При наличии таких маршрутов все остальные кандидаты исключаются из списка. Если маршрута внутри области не найдено, маршрутизатор проверяет, не относится ли получатель пакета к диапазонам адресов, указанных для локальной области. При положительном ответе весь набор оставшихся кандидатов удаляется, а при отрицательном кандидаты проверяются на предмет наличия среди них маршрутов с route.class = inter-area. Если такие маршруты найдены, все остальные кандидаты отбрасываются. При отсутствии межобластных маршрутов проверяется наличие маршрутов с route.class = type 1 external. Если такие маршруты найдены, все прочие кандидаты исключаются из списка.

- **Класс маршрута IS-IS**

  Классы маршрутов IS-IS работают аналогично классам OSPF. Однако набор классов, используемых в Integrated IS-IS, отличается, поэтому нет возможности установить взаимно-однозначное соответствие между классами маршрутов IS-IS и OSPF. К числу используемых в Integrated IS-IS классов относятся (в порядке снижения уровня предпочтений) intra-area (внутриобластные), inter-area (межобластные), external (внешние).

[1] BBN Core Gateway - маршрутизаторы, которые составляли опорную сеть Internet тех времен.
[2] Выбор маршрута при одинаковой длине соответствия. *Прим. перев.*

Внутренние классы Integrated IS-IS эквивалентны внутренним классам OSPF. Кроме того, класс external в Integrated IS-IS эквивалентен классу type 2 external в OSPF. Однако протокол Integrated IS-IS не различает межобластные маршруты и внешние маршруты с внутренней метрикой (оба типа маршрутов относятся к классу inter-area). В результате OSPF предпочитает межобластные маршруты внешним путям с внутренней метрикой, а в Integrated IS-IS эти два типа имеют одинаковый уровень предпочтения.

- **Политика IDPR**

  Рабочая группа IETF по правилам междоменной маршрутизации (Inter-domain Policy Routing) разработала протокол маршрутизации, получивший название IDPR[1], для поддержки в Internet основанной на правилах маршрутизации. Пакеты с некоторой комбинацией атрибутов заголовка (конкретные комбинации адресов отправителя и получателя, специальные опции IDPR source route) должны использовать маршруты, обеспечиваемые протоколом IDPR. Таким образом, в отличие от других правил сокращения, IDPR Policy будет применяться до всех прочих правил сокращения, кроме базового соответствия (Basic Match).

  В частности, IDPR Policy проверяет пересылаемые пакеты на предмет наличия в них атрибутов, требуемых для пересылки с использованием основанных на правилах маршрутов. При позитивном ответе IDPR Policy удаляет из списка кандидатов все маршруты, не обеспечиваемые протоколом IDPR.

E.3 Некоторые алгоритмы поиска маршрутов

В этом параграфе проверяются некоторые алгоритмы поиска маршрутов в таблице, которые уже используются или предложены для использования. Каждое описание алгоритма содержит список правил сокращения в порядке их применения. Отмечены сильные и слабые стороны алгоритмов.

E.3.1 Пересмотренный классический алгоритм

Пересмотренный классический алгоритм представляет собой вариант традиционного алгоритма, рассмотренного в параграфе E.1. Этапы сокращения перечислены ниже.

1. Basic match (базовое соответствие).
2. Longest match (максимальная длина соответствия).
3. Best metric (лучшая метрика).
4. Policy (политика).

В некоторых реализациях этап Policy не используется, поскольку он нужен лишь в тех случаях, когда маршруты используют несравнимую метрику (получены из разных доменов маршрутизации).

Преимущества алгоритма

(1) Наличие множества реализаций и широкое распространение.

(2) Простота для понимания и реализации (за исключением этапа Policy, который может быть достаточно сложным).

Недостатки

(1) Не обрабатываются классы маршрутов IS-IS и OSPF, поэтому не могут применяться протоколы Integrated IS-IS и OSPF.

(2) Не обрабатывается поле TOS и другие атрибуты пути.

(3) Механизм использования политики совершенно не стандартизован и зачастую зависит от реализации. Это требует дополнительных усилий от разработчиков (которым требуется создать подходящий механизм для политики) и пользователей, которые должны понять, как пользоваться этим механизмом. Отсутствие стандартов также осложняет создание согласованных конфигураций для маршрутизаторов различных производителей, что ведет к существенному снижению уровня интероперабельности маршрутизаторов.

(4) Фирменные механизмы политики, предлагаемые производителями, зачастую не подходят для использования в сложных участках Internet.

(5) Алгоритм не описан в каком-либо доступном документе или стандарте. По сути он является частью фольклора Internet.

E.3.2 Вариант алгоритма из спецификации Router Requirements

Часть членов рабочей группы Router Requirements предложила использовать несколько отличающийся вариант алгоритма, описанного в параграфе 5.2.4.3. В этом варианте соответствие запрошенного типа обслуживания рассматривается, как более важный аргумент, нежели наибольшая длина соответствия адреса. Например, этот алгоритм позволяет отдавать предпочтение заданному по умолчанию маршруту, если тот имеет пригодный тип обслуживания, а маршрут с максимальной длиной соответствия обеспечивает принятое по умолчанию значение TOS (0). Алгоритм, описанный в параграфе 5.2.4.3, будет давать обратный результат.

Этапы сокращения перечислены ниже.

1. Basic match (базовое соответствие).
2. Weak TOS (наименьшие требования к TOS).
3. Longest match (максимальная длина соответствия).
4. Best metric (лучшая метрика).
5. Policy (политика).

[1] Inter-Domain Policy Routing – междоменная маршрутизация на основе правил

Дебаты между сторонниками описанного здесь варианта и сторонниками алгоритма, рассмотренного в параграфе 5.2.4.3, показали, что обе стороны могут показать случаи, когда предлагаемый ими алгоритм делает маршрутизацию более простой и понятной, нежели другой алгоритм. Данный вариант имеет те же преимущества и недостатки, что и алгоритм, описанный в параграфе 5.2.4.3, с той лишь разницей, что он использует правило Weak TOS до правила Longest Match и это делает его вариант менее совместимым с протоколами OSPF и Integrated IS-IS, нежели стандартный алгоритм, предложенный в Router Requirements.

E.3.3 Алгоритм OSPF

OSPF использует алгоритм, который почти идентичен алгоритму из Router Requirements, но в отличие от последнего различает классы маршрутов OSPF.

Этапы сокращения перечислены ниже.

1. Basic match (базовое соответствие).
2. Route Classes OSPF (класс маршрута OSPF).
3. Longest match (максимальная длина соответствия).
4. Weak TOS (наименьшие требования к TOS).
5. Best metric (лучшая метрика).
6. Policy (политика).

Поддержка этапа сокращения по типу обслуживания присутствует не всегда. При ее отсутствии этап 4 просто не выполняется.

Данный алгоритм имеет некоторые преимущества по сравнению с пересмотренным классическим алгоритмом.

(1) Поддержка маршрутизации по типу обслуживания.

(2) Правила документированы, а не являются частью фольклора Internet.

(3) Алгоритм (очевидно) работает с протоколом OSPF.

Однако этот алгоритм сохраняет некоторые недостатки пересмотренного классического алгоритма.

(1) Игнорируются свойства пути, отличные от типа обслуживания (например, MTU).

(2) Как и пересмотренный классический алгоритм, этот алгоритм не описывает детали (и не требует наличия) этапа Policy, что делает этот шаг существенно зависимым от разработчика.

Алгоритм OSPF имеет дополнительный недостаток (отсутствующий в пересмотренном классическом алгоритме) - внутренние (intra-area или inter-area) маршруты OSPF всегда рассматриваются, как более приоритетные по сравнению с маршрутами, полученными от других протоколов маршрутизации, даже если маршрут OSPF имеет меньшую длину совпадения с адресом получателя. Такое решение на уровне политики может оказаться недопустимым в некоторых сетях.

Наконец, следует отметить, что поддержка TOS в алгоритме OSPF приводит к тому, что при пересылке пакетов с отличным от нуля значением TOS неявно предпочитаются те протоколы маршрутизации, которые поддерживают TOS. Такое решение может оказаться неприемлемым в некоторых случаях.

E.3.4 Алгоритм Integrated IS-IS

Протокол Integrated IS-IS использует алгоритм, который почти совпадает с алгоритмом OSPF. Отличие состоит в том, что Integrated IS-IS использует другой набор классов и несколько иначе обрабатывает поле TOS. Этапы сокращения перечислены ниже.

1. Basic match (базовое соответствие).
2. IS-IS Route Classes (классы маршрутов IS-IS).
3. Longest match (максимальная длина соответствия).
4. Weak TOS (наименьшие требования к TOS).
5. Best metric (лучшая метрика).
6. Policy (политика).

Хотя Integrated IS-IS использует TOS, этот протокол способен лишь поддерживать маршруты для небольшого заданного подмножества положительных значений TOS в заголовке IP. Пакеты, содержащие другие значения TOS, будут маршрутизироваться с использованием принятого по умолчанию TOS (0).

Поддержка сокращения по типу обслуживания не является обязательной. Если такое сокращение не используется, этап 4 просто пропускается. Как и для OSPF, спецификация не включает описания этапа Policy.

Данный алгоритм имеет некоторые преимущества по сравнению с пересмотренным классическим алгоритмом.

(1) Поддержка маршрутизации по типу обслуживания.

(2) Правила документированы, а не являются частью фольклора Internet.

(3) Алгоритм (очевидно) работает с протоколом Integrated IS-IS.

Однако этот алгоритм сохраняет некоторые недостатки пересмотренного классического алгоритма.

(1) Игнорируются свойства пути, отличные от типа обслуживания (например, MTU).

(2) Как и пересмотренный классический алгоритм, этот алгоритм не описывает детали (и не требует наличия) этапа Policy, что делает этот шаг существенно зависимым от разработчика.

(3) Алгоритм не поддерживает OSPF по причине различий между классами маршрутов в IS-IS и OSPF. Кроме того, в силу ограниченной поддержки протоколом IS-IS значений поля TOS, некоторые реализации алгоритма Integrated IS-IS не поддерживают принятую в OSPF интерпретацию TOS.

Алгоритм Integrated IS-IS имеет дополнительный недостаток (отсутствующий в пересмотренном классическом алгоритме) - внутренние (intra-area или inter-area) маршруты IS-IS всегда рассматриваются как более приоритетные по сравнению с маршрутами, полученными от других протоколов маршрутизации, даже если маршрут IS-IS имеет меньшую длину совпадения с адресом получателя. Такое решение на уровне политики может оказаться недопустимым в некоторых сетях.

Наконец, следует отметить, что поддержка TOS в алгоритме Integrated IS-IS отличается теми же недостатками, которые были указаны для алгоритма OSPF.

Вопросы безопасности

Хотя этот документ посвящен скорей взаимодействию маршрутизаторов, нежели безопасности, многие параграфы документа так или иначе связаны с вопросами сетевой безопасности.

Разные люди по разному относятся к безопасности. Применительно к маршрутизаторам в сферу безопасности попадает все, что помогает сохранить работоспособность сети и обеспечить нормальное функционирование Internet в целом. Применительно к этому документу вопросы безопасности включают защиту от атак на службы, целостность и аутентификацию (применительно к двум первым пунктам). Сохранение конфиденциальности имеет достаточно большое значение, но этот вопрос слабо связан с маршрутизаторами (по крайней мере, в контексте этого документа).

В нескольких местах этого документа имеются подпараграфы с названием «Вопросы безопасности». В таких параграфах обсуждаются конкретные проблемы безопасности, связанные с темой основного параграфа.

В этом документе редко встречаются выражения типа: «сделайте так и ваш маршрутизатор будет защищен». Скорее вы прочтете что-либо вроде: «это хорошая идея и ее реализация **может** повысить уровень безопасности Internet и вашей локальной системы».

К сожалению, это характеризует современное состояние вопроса. Лишь немногие сетевые протоколы, используемые в маршрутизаторах, имеют хорошо проработанные встроенные средства обеспечения безопасности. Производители и разработчики протоколов по-прежнему уделяют достаточно мало внимания вопросам защиты. Прогресс наблюдается и в этом направлении, но идет он очень мелкими «детскими» шагами (такими, как добавление проверки подлинности партнеров для протоколов маршрутизации BGP и OSPF).

В частности, в данном документе отмечены современные исследования в направлении разработки и совершенствования средств обеспечения сетевой безопасности. Направления исследования и разработки на момент создания документа (декабрь 1993) включали IP Security, SNMP Security и технологии проверки подлинности общего назначения.

Несмотря на сказанное выше, существуют доступные как производителям, так и пользователям меры повышения уровня безопасности для маршрутизаторов. Производителям следует обзавестись копией документа Trusted Computer System Evaluation Criteria [INTRO:8]. Даже если производитель не пожелает выполнить формальности по проверке соответствия продукции требованиям указанного документа, последний обеспечит превосходное руководство по вопросам безопасности для вычислительной техники.

Приложение F: История протоколов маршрутизации

Некоторые протоколы маршрутизации достаточно широко используются в Internet, но авторы этого документа не считают возможным рекомендовать их применение. Это обусловлено не тем, что протоколы работают некорректно, а при их разработке использовались представления о характеристиках Internet (простая маршрутизация, отсутствие правил, сеть с «централизованной маршрутизацией» и администрированием, ограниченная сложность, ограниченный диаметр сети), которые не соответствуют сегодняшнему состоянию Internet. Фрагменты Internet, где продолжается использование таких протоколов, обычно отделены доменами с ограниченной функциональностью.

В качестве жеста доброй воли в этом приложении дается информация, касающаяся таких реализаций протоколов маршрутизации.

F.1 Протокол внешнего шлюза EGP

F.1.1 Введение

EGP представляет собой протокол внешнего шлюза, используемый для обмена данными о доступности адресатов между маршрутизаторами одной или разных автономных систем. EGP не рассматривается как протокол маршрутизации, поскольку в нем нет стандартной интерпретации полей дальности (т. е., метрики) в обновлениях EGP и дальность можно сравнивать только между маршрутизаторами одной AS. EGP создан для предоставления информации о доступности как соседних маршрутизаторов, так и путей к маршрутизаторам, не являющимся непосредственными соседями.

EGP определен в документе [ROUTE:6]. Разработчики скорей всего захотят прочесть также документы [ROUTE:7] и [ROUTE:8], содержащие полезные объяснения и фундаментальные материалы.

Обсуждение

Спецификация EGP имеет серьезные ограничения, наиболее важное из которых связано с тем, что маршрутизаторы могут анонсировать только те сети, что доступны в автономной системе данного маршрутизатора. Это ограничивает распространение информации EGP от других маршрутизаторов для предотвращения долгоживущих маршрутных петель. Такое ограничение EGP не позволяет поддерживать более 2 уровней иерархии.

RFC 975 не является частью спецификации EGP и этот документ следует игнорировать.

F.1.2 «Сквозной контроль» протокола

Непрямые соседи - RFC 888, стр. 26

Реализация EGP **должна** включать поддержку непрямых соседей (indirect neighbor).

Интервалы опроса - RFC 904, стр. 10

Интервалы между повторами для команд Hello и Poll **следует** делать настраиваемыми, но **должно** быть задано минимальное время, используемое по умолчанию.

Интервалы, по истечении которых маршрутизатор будет отвечать на команды Hello и Poll, **следует** делать настраиваемыми, но **должно** быть установлено минимальное значение, используемое по умолчанию.

Доступность соседей - RFC 904, стр. 15

По умолчанию для реализации **недопустимо** предоставление внешнего списка маршрутизаторов в другие автономные системы - в пакеты Update Response/Indication следует включать только внутренний список маршрутизаторов вместе с сетями, доступными через них. Однако реализация **может** поддерживать конфигурационный параметр, разрешающий предоставление списка внешних маршрутизаторов. Для реализации протокола **недопустимо** включение во внешний список маршрутизаторов, полученных из внешних списков маршрутизаторов других автономных систем, т. е. **должна** выполняться операция «расщепления горизонта» (split-horizon) на уровне автономной системы.

Если в сообщение Network Reachability требуется включить более 255 внутренних или более 255 внешних маршрутизаторов, сети, доступные через маршрутизаторы, которые не могут быть включены в список, **должны** добавляться к списку одного из включенных в обновление маршрутизаторов. Пользователю **следует** предоставить возможность выбора маршрутизатора, к списку которого производится добавление, но по умолчанию **следует** добавлять их к списку маршрутизатора, адрес которого совпадает с адресом отправителя в пакетах обновлений EGP.

Обновления EGP содержат последовательность блоков номеров сетей, а каждый блок такой последовательности включает список номеров сетей, доступных через определенный маршрутизатор и находящихся на определенном расстоянии. Если через какой-то маршрутизатор доступно более 255 сетей, находящихся от него на одинаковых расстояниях, список таких сетей расщепляется на множество блоков. Если же список содержит более 255 блоков для сетей, доступных через определенный маршрутизатор, адрес этого маршрутизатора указывается столько раз, сколько требуется для включения в обновление всех блоков.

Незапрошенные обновления - RFC 904, стр. 16

Если сеть является общей с партнером, реализация протокола **должна** передавать незапрошенные обновления при переходе записи в состояние Up, когда сеть-источник является общей.

Доступность соседей - RFC 904, стр. 6, 13-15

Таблица на стр. 6, которая описывает значения j и k (пороги up и down для соседа), содержит некорректную информацию. Корректная таблица приведена ниже.

```
Name    Active  Passive Description
-----------------------------------------------
 j        3       1     neighbor-up threshold
 k        1       0     neighbor-down threshold
```

Значение для k в пассивном режиме также указано некорректно на стр. 14 документа RFC 904. Значения в скобках следует читать как:

```
(j = 1, k = 0, and T3/T1 = 4)
```

В целях оптимизации протокол может задерживать передачу Hello в тех случаях, когда близок к завершению интервал Poll. Если реализация поддерживает оптимизацию, **следует** поддерживать задаваемый пользователем параметр для запрета этой оптимизации.

Таймер прерывания - RFC 904, стр. 6, 12, 13

Реализация EGP **должна** включать поддержку таймера прерывания, описанного в параграфе 4.1.4 RFC 904. Реализации **следует** использовать таймер прерывания в состоянии Idle для автоматической генерации события Start с целью перезапуска машины протокола. Рекомендуются значение P4 для критических ошибок (Administratively prohibited, Protocol Violation и Parameter Problem) и P5 – для прочих ошибок. **Не следует** запускать таймер прерывания при ручной генерации событий Stop (например, с использованием протокола управления сетью).

Получение команды Cease в состоянии Idle - RFC 904, стр. 13

Когда машина состояний EGP находится в состоянии Idle, она **должна** отвечать на команды Cease откликами Cease-ack.

Режим Hello Polling - RFC 904, стр. 11

Реализация EGP **должна** включать поддержку активного и пассивного режимов опроса.

Сообщения Neighbor Acquisition - RFC 904, стр. 18

Как отмечено, интервалы Hello и Poll следует включать только в сообщения Request и Confirm. Поэтому размер сообщений EGP Neighbor Acquisition составляет 14 байтов для Request или Confirm и 10 байтов для Refuse, Cease или Cease-ack. Для реализации протокола **недопустимо** передавать 14-байтовые сообщения Refuse, Cease или Cease-ack, но такие сообщения **должны** приниматься от других.

Порядковые номера - RFC 904, стр. 10

Пакеты откликов или индикации с порядковым номером, отличным от S, **должны** отбрасываться. Порядковый номер S при передаче **должен** увеличиваться непосредственно перед передачей команды Poll, а не в другое время.

F.2 Протокол RIP

F.2.1 Введение

Спецификация протокола RIP содержится в документе [ROUTE:3]. Хотя протокол RIP играет достаточно важную роль в Internet, он будет заменяться более современными протоколами IGP (такими, как описано выше). Маршрутизаторам, реализующим протокол RIP, **следует** поддерживать RIP версии 2 [ROUTE:?][1], если они поддерживают маршруты CIDR.

[1]Современный вариант спецификации протокола RIPv2 содержится в RFC 1721. *Прим. перев.*

Если в сети используется коммутируемый доступ (occasional access), маршрутизаторам, реализующим RIP, **следует** поддерживать расширение Demand RIP [ROUTE:?][1].

Одним из распространенных применений RIP является протокол обнаружения маршрутизаторов, упомянутый в параграфе 4.3.3.10.

F.2.2 Общие вопросы

Реакция на изменения топологии - [ROUTE:3], стр. 11

Реализация RIP **должна** обеспечивать механизм тайм-аута для маршрутов. Поскольку сообщения время от времени могут теряться, **недопустимо** объявлять маршрут непригодным на основании отсутствия одного обновления.

По умолчанию реализация **должна** ждать в течение 6 интервалов обновления прежде, чем объявить маршрут непригодным. Маршрутизатор **может** поддерживать конфигурационный параметр для выбора периода ожидания.

Обсуждение

Для обеспечения стабильной маршрутизации важно, чтобы все маршрутизаторы в автономной системе RIP использовали одинаковый интервал (тайм-аут) для объявления маршрута непригодным. Следовательно, важна поддержка по умолчанию тайм-аута, заданного в спецификации RIP.

Однако заданное спецификацией требование слишком консервативно для сред, где потеря пакетов происходит достаточно редко. В таких средах администраторы могут пожелать уменьшить время ожидания для более быстрого восстановления маршрутизации после отказов.

Реализация

Существует очень простой механизм, который маршрутизатор может использовать для выполнения требований по объявлению маршрутов непригодными по истечении заданного времени. Всякий раз, при сканировании таблицы маршрутов на предмет поиска устаревших записей (тайм-аут) маршрутизатор смотрит также возраст для наиболее давно обновленного маршрута, для которого еще не наступил тайм-аут. Вычитание этого возраста из значения тайм-аута позволяет определить время, по истечении которого маршрутизатору следует снова просканировать таблицу для удаления устаревших маршрутов.

Split Horizon - [ROUTE:3], стр. 14-15

Реализация RIP **должна** поддерживать схему «расщепления горизонта», используемую для предотвращения проблем, связанных с передачей обновлений маршрутизатору, от которого они были получены.

Реализации RIP **следует** поддерживать схему Split horizon with poisoned reverse[2] - вариант «расщепления горизонта», который включает передачу маршрутов, полученных от какого-либо маршрутизатора, ему же с установкой бесконечного значения метрики. Поскольку эта схема увеличивает объем служебного трафика, реализация протокола **может** включать опцию, определяющую, когда следует возвращать «испорченный» маршрут. Реализации **следует** ограничивать время, когда она передает обратно маршруты с бесконечной метрикой.

Реализация

Оба описанных ниже алгоритма можно использовать для ограничения времени, когда «порча» применима к возвращаемому маршруту. Первый алгоритм наиболее сложен, но он выполняет работу по передаче «испорченных» маршрутов только в тех случаях, когда это необходимо.

Задачей обоих алгоритмов является обеспечение «порчи» возвращаемого маршрута для всех путей, которые были изменены в течение последнего интервала Route Lifetime (обычно 180 сек.), если нет уверенности в том, что предыдущий маршрут использует тот же выходной интерфейс. Значение Route Lifetime используется по той причине, что оно задает время, в течение которого RIP будет сохранять старый маршрут до объявления его состояния.

В этих алгоритмах используются перечисленные ниже временные интервалы.

Tu (The Update Timer - таймер обновления) - число секунд между обновлениями RIP, по умолчанию обычно составляет 30 секунд.

Rl (The Route Lifetime - время жизни маршрута) - число секунд, в течение которых маршрут предполагается пригодным без необходимости обновления, по умолчанию обычно 180 сек.

Ul (The Update Loss - число потерянных обновлений) - число последовательных обновлений, которые могут быть потеряны или не получены по причине отказа до того, как RIP удалит маршрут. Значение Ul рассчитывается, как (Rl/Tu)+1. Единица добавляется для того, чтобы учесть, что до первого уменьшения значения счетчика ifcounter проходит менее Tu секунд с момента инициализации. Обычно параметр Ul имеет значение 7 = (180/30)+1.

In - значение счетчика ifcounter в момент получения (обновления) информации о маршруте. Это значение составляет Ul-4 (4 - значение таймера сборки мусора RIP, разделенное на 30).

Первый алгоритм

- С каждым маршрутом (destination) ассоциируется счетчик ifcounter. «Испорченный» маршрут возвращается для всех маршрутов, которые имеют положительное значение ifcounter.
- После передачи обычного (не инициированного - triggered или вызванного запросом) обновления все отличные от 0 значения ifcounter уменьшаются на 1.
- При создании маршрута счетчик ifcounter устанавливается с учетом следующих условий:
  - если новый маршрут заменяет собой пригодный маршрут и старый маршрут использует иной (логический) выходной интерфейс, устанавливается ifcounter = Ul;
  - если новый маршрут устанавливается взамен статического и прежний маршрут использует иной (логический) выходной интерфейс, устанавливается ifcounter = MAX(0, Ul – INT(число секунд, в течение которых маршрут был в состоянии stale, деленное на Ut);

[1] Это расширение описано в RFC 1582. *Прим. перев.*

[2] «Расщепление горизонта» с возвратом «испорченного» маршрута.

- если такого маршрута не было совсем, устанавливается ifcounter = In;
- во всех прочих случаях устанавливается ifcounter = 0.

- Протокол RIP также поддерживает таймер сброса (resettimer). «испорченный» маршрут возвращается всем маршрутизаторам, для которых не истекло время resettimer (независимо от значения ifcounter).
- При старте, перезапуске, сбросе и в других случаях очистки таблицы маршрутов RIP протокол устанавливает для таймера сброса значение RI.

Второй алгоритм отличается от первого тем, что:

- в тех случаях, когда для счетчика ifcounter устанавливается ненулевое значение, оно всегда равно RI/Tu;
- таймер сброса не используется.

Инициированные (Triggered) обновления - [ROUTE:3], стр. 15-16; стр. 29

Инициированные (их называет еще triggered или flash) обновления представляют собой механизм для незамедлительного уведомления соседних маршрутизаторов о добавлении, изменении или удалении маршрутов. Маршрутизатор **должен** передавать инициированные обновления при удалении маршрутов или увеличении значения метрики. Маршрутизатор **может** передавать инициированные обновления при добавлении маршрутов или уменьшении значения метрики.

Поскольку инициированные обновления могут вызывать избыточный рост служебного трафика, реализация протокола **должна** использовать перечисленные ниже механизмы для ограничения частоты инициированных обновлений.

(1) Когда маршрутизатор передает инициированное обновление, он устанавливает для таймера случайное значение в диапазоне от 1 до 5 секунд. Недопустима генерация маршрутизатором других инициированных обновлений до завершения отсчета этого таймера.

(2) Если маршрутизатор будет генерировать инициированное обновление во время действия таймера, он устанавливает флаг, показывающий, желательность инициированного обновления. Маршрутизатору следует также записывать информацию об этом в системный журнал.

(3) По истечении заданного для таймера времени, маршрутизатор проверяет флаг и при его наличии передает одно обновление, содержащее все зафиксированные изменения. После этого флаг сбрасывается и снова запускается описанный выше таймер.

(4) Флаг сбрасывается также при передаче обычного обновления.

В инициированные обновления **следует** включать все маршруты, которые были изменены с момента передачи последнего (не инициированного) обновления. **Недопустимо** включение в инициированные обновления маршрутов, которые не были изменены с момента передачи последнего обычного обновления.

Обсуждение

Передача всех маршрутов (независимо от их обновления) совершенно не нужна в инициированных обновлениях, поскольку размеры таблиц во многих маршрутизаторах Internet могут привести с слишком большому расходу полосы на передачу таких инициированных обновлений.

Использование UDP - [ROUTE:3], стр. 18-19.

В пакетах RIP, передаваемых по широковещательным адресам IP, следует устанавливать начальное значение TTL = 1.

Отметим, что в соответствии с параграфом 6.1 этого документа маршрутизатору **следует** использовать контрольные суммы UDP в генерируемых пакетах RIP. Пакеты RIP с некорректным значением контрольной суммы UDP **должны** отбрасываться, но **недопустимо** отбрасывание полученных пакетов RIP лишь по той причине, что они не содержат контрольной суммы UDP.

Вопросы адресации - [ROUTE:3], стр. 22

Реализации RIP **следует** поддерживать маршруты к хостам (host route). При отсутствии такой поддержки маршруты к хостам, полученные в обновлениях, **должны** игнорироваться, как указано на стр. 27 документа [ROUTE:3]. Маршрутизатор **может** протоколировать отбрасывание маршрутов к хостам.

Для описания принятого по умолчанию маршрута используется специальный адрес 0.0.0.0. Принятый по умолчанию маршрут используется в качестве последнего шанса (т. е., при отсутствии в таблице маршрута к нужному адресату). Маршрутизатор **должен** обеспечивать возможность создания записи RIP для адреса 0.0.0.0.

Обработка принимаемой информации - отклики: [ROUTE:3], стр. 26

При обработке обновлений **должны** выполняться следующие проверки:

- отклики **должны** приходить из порта UDP с номером 520;
- адрес отправителя **должен** относиться к непосредственно подключенной подсети (или сети без подсетей);
- **недопустимо** принимать пакеты, в которых адрес совпадает с одним из адресов маршрутизатора.

Обсуждение

Некоторые сети, среды и интерфейсы позволяют передающему узлу принимать пакеты, передаваемые им в широковещательном режиме. Для маршрутизаторов недопустим прием собственных пакетов, содержащих обновления таблицы маршрутизации, и обработка таких пакетов (в предположении, что эти пакеты передавались каким-то другим маршрутизатором сети).

Для реализации **недопустимо** заменять существующий маршрут, если метрика полученного маршрута совпадает с метрикой существующего, за исключением использования описанных ниже эвристических методов.

Реализация протокола **может** поддерживать эвристические методы при замене существующих в таблице маршрутов обновленными маршрутами с совпадающим значением метрики. Обычно бесполезна замена пути через один маршрутизатор сети на путь через другой маршрутизатор, если оба маршрута имеют одинаковую метрику. Однако для маршрута, анонсированного одним из маршрутизаторов, может заканчиваться отсчет тайм-аута. Вместо ожидания завершения этого отсчета можно по истечении заданного времени использовать взамен новый маршрут. При реализации такого метода **требуется** выждать по крайней мере половину оставшегося до тайм-аута времени прежде, чем устанавливать новый маршрут.

F.2.3 Частные вопросы

RIP Shutdown

Реализации протокола RIP **следует** поддерживать процедуру изящного завершения работы (graceful shutdown) с использованием перечисленных ниже этапов.

(1) Завершение обработки входящей информации.

(2) Генерация 4 обновлений со случайными интервалами от 2 до 4 секунд. Эти обновления содержат все маршруты, которые были анонсированы ранее, но с некоторыми изменениями в их метрике. Маршруты с бесконечной метрикой не изменяются, а маршруты с конечной метрикой должны быть анонсированы с метрикой 15 (бесконечность - 1).

Обсуждение

На самом деле в п. (2) должна устанавливаться метрика 16 (бесконечность). Установка значения 15 обусловлена желанием предотвратить проблемы на некоторых старых хостах, которые перехватывают протокол RIP. Такие хосты будут (ошибочно) разрывать соединения TCP при попытке передачи дейтаграммы через соединение в то время, когда нет пути к адресату (даже если период отсутствия пути составляет лишь несколько секунд, пока RIP выбирает другой путь к адресату).

RIP Split Horizon и статические маршруты

Схему Split horizon **следует** по умолчанию применять к статическим маршрутам. Реализации протокола **следует** обеспечивать для каждого статического маршрута возможность указать, следует ли для него использовать «расщепление горизонта».

F.3 Протокол обмена между шлюзами - GGP

Протокол GGP[1] признан устаревшим и реализовать его **не следует**.

Благодарности

Если б нам
Хотя бы десять тысяч англичан
Из тех, что праздными теперь сидят
На родине!

Кто этого желает?
Кузен мой Уэстморленд? Ну нет, кузен:
Коль суждено погибнуть нам, - довольно
Потерь для родины; а будем живы, -
Чем меньше нас, тем больше будет славы.
Да будет воля божья! Не желай
И одного еще бойца нам в помощь.
Клянусь Юпитером, не алчен я!
Мне все равно: пусть на мой счет живут;
Не жаль мне: пусть мои одежды носят,
Вполне я равнодушен к внешним благам.
Но, если грех великий - жаждать славы,
Я самый грешный из людей на свете.
Нет, не желай, кузен, еще людей нам.
Клянусь создателем, я б не хотел
Делиться славой с лишним человеком.
Нет, не желай подмоги, Уэстморленд,
А лучше объяви войскам, что всякий,
Кому охоты нет сражаться, может
Уйти домой; получит он и пропуск
И на дорогу кроны в кошелек.
Я не хотел бы смерти рядом с тем,
Кто умереть боится вместе с нами.
Сегодня день святого Криспиана;
Кто невредим домой вернется, тот
Воспрянет духом, станет выше ростом
При имени святого Криспиана.
Кто, битву пережив, увидит старость,
Тот каждый год и канун, собрав друзей.
Им скажет; "Завтра праздник Криспиана",
Рукав засучит и покажет шрамы:
"Я получил их в Криспианов день".
Хоть старики забывчивы, но этот
Не позабудет подвиги свои
В тот день; и будут наши имена
На языке его средь слов привычных:
Король наш Гарри, Бедфорд, Эксетер,
Граф Уорик, Толбот, Солсбери и Глостер
Под звон стаканов будут поминаться.
Старик о них расскажет повесть сыну,
И Криспианов день забыт не будет
Отныне до скончания веков;
С ним сохранится память и о нас -
О нас, о горсточке счастливцев, братьев.
Тот, кто сегодня кровь со мной прольет,
Мне станет братом: как бы ни был низок,
Его облагородит этот день;
И проклянут свою судьбу дворяне,
Что в этот день не с нами, а в кровати:
Язык прикусят, лишь заговорит
Соратник наш в бою в Криспинов день.

Уильям Шекспир (перевод Е. Бируковой)

Этот документ является результатом работы группы IETF Router Requirements. Подобные документы включают в себя результаты работы многих людей, которые могут быть указаны в тексте документа. Множество производителей оборудования и программ, сетевых администраторов и других специалистов из сообщества Internet потратили свое время и силы на повышение качества этого документа. Редактор хочет выразить им всем свою искреннюю благодарность.

Нынешний редактор документа также хочет выразить свою искреннюю признательность и и высокую оценку работы первого редактора документа - Филиппа Алмквиста (Philip Almquist). Без его работы в качестве редактора и руководителя группы этот документ просто не был бы написан. Хочется также выразить глубокую и искреннюю признательность редактору предыдущей версии документа - Фрэнку Кастенхольцу (Frank Kastenholz). Фрэнк из набора разрозненной информации создал законченный документ, содержащий полезные описания технологии IP в ее состоянии на 1991 год. Остается лишь надеяться, что современное (1994 год) отражение этой технологии также окажется полезным и понятным.

Philip Almquist, Jeffrey Burgan, Frank Kastenholz и Cathy Wittbrodt написали основные части этого документа. К числу людей, которые также внесли свой вклад в написание основной части, относятся Bill Barns, Steve Deering, Kent England, Jim Forster, Martin Gross, Jeff Honig, Steve Knowles, Yoni Malachi, Michael Reilly, Walt Wimer.

В документ также включены материалы, которые подготовили Andy Malis, Paul Traina, Art Berggreen, John Cavanaugh, Ross Callon, John Lekashman, Brian Lloyd, Gary Malkin, Milo Medin, John Moy, Craig Partridge, Stephanie Price, Yakov Rekhter, Steve Senum, Richard Smith, Frank Solensky, Rich Woundy и другие, кто незаслуженно опущен в этом списке.

[1] GATEWAY TO GATEWAY PROTOCOL - протокол взаимодействия шлюзов.

Некоторые фрагменты этого документа были заимствованы из более ранних документов (в основном из RFC 1122, который подготовил Bob Braden и группа Host Requirements, а также RFC 1009, который написали Bob Braden и Jon Postel). Благодарим авторов этих документов за их работу.

Jim Forster был сопредседателем рабочей группы Router Requirements на раннем этапе деятельности и внес важный вклад в успешный старт работы. Jon Postel, Bob Braden и Walt Prue также внесли свой вклад в успех, обеспечив подготовку обширной информации перед началом работы группы. На следующих этапах работы Phill Gross, Vint Cerf и Noel Chiappa обеспечивали участников группы ценной информацией и поддержкой.

Mike St. Johns координировал взаимодействие группы со специалистами по безопасности, а Frank Kastenholz - со специалистами по сетевому управлению. Allison Mankin и K. K. Ramakrishnan обеспечили экспертизу по вопросам контроля насыщения и распределения ресурсов.

В этот список можно было включить еще многих людей, которые внесли свой вклад в работу группы Router Requirements, взаимодействуя с ее членами по электронной почте или участвуя в конференциях. Особо следует отметить усилия Ross Callon и Vince Fuller в работе над сложными вопросами выбора маршрутов и передачи маршрутных данных.

Редактор благодарит своего работодателя - Cisco Systems - за возможность тратить время на эту работу.

Адрес редактора

Fred Baker

Cisco Systems

519 Lado Drive

Santa Barbara, California 93111

USA

Phone:+1 805-681-0115

EMail: fred@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru