Network Working Group
Request for Comments: 3879
Category: Standards Track

C. Huitema
Microsoft
B. Carpenter
IBM

September 2004

Отмена адресов Site Local

Deprecating Site Local Addresses

Статус документа

В этом документе содержится спецификация протокола, предложенного сообществу Internet. Документ служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации протокола вы можете узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Авторские права

Аннотация

Этот документ рассматривает вопросы использования индивидуальных адресов IPv6 site-local в их исходной форме и формально отменяет их применение. Данная отмена не запрещает продолжение их использования до момента стандартизации и реализации замены.

1. Введение

В течение некоторого времени рабочая группа IPv6 занималась обсуждением множества вопросов, связанных с использованием локальных для сайта (site local) адресов. На заседании в марте 2003 года группа достигла определённого соглашения по этим вопросам в части замены таких адресов в их предложенной изначально форме. Хотя единодушия по этому вопросу не было достигнуто, на заседании в июле 2003 года рабочая группа подтвердила необходимость документирования этих проблем и последующего принятия решения об отказе от использования индивидуальных адресов IPv6 site-local.

Локальные для сайта адреса были определены в архитектуре адресации IPv6 [RFC3513] (параграф 2.5.6).

В оставшейся части этого документа описаны негативные аспекты применения локальных для сайта адресов и приведён формальный отказ от их использования.

Цели такой отмены и решения по замене адресов будут описаны в дополнительных документах. Однако формальный отказ не отменяет применение ранее развёрнутых адресов site-local до момента стандартизации и реализации замены.

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с BCP 14, RFC 2119 [RFC2119].

2. Негативные эффекты адресов Site Local

Обсуждения в рабочей группе IPv6 привели к обнаружению некоторых недостатков текущей модели локальной для сайта адресации. Эти недостатки можно разделить не две категории - неоднозначность адресации и нечёткость определения сайта.

Как было отмечено, адресация site local не обеспечивает однозначности - адреса типа FEC0::1 могут присутствовать на множестве сайтов, а сам адрес не содержит какой-либо индикации сайта, к которому он относится. Это создаёт проблемы для разработчиков приложений и маршрутизаторов, а также сетевых администраторов. Проблема связана с нечёткостью определения сайта. Более подробное рассмотрение этого вопроса будет приведено ниже.

2.1. Проблема разработчиков - область действия идентификаторов

Отклики разработчиков показывают, что локальная адресация трудна для корректного использования в приложениях. В частности, это отмечено для многодомных хостов, которые могут быть подключены к нескольким сайтам одновременно, а также для мобильных хостов, которые могут подключаться к множеству сайтов.

Приложение может узнать или вспомнить, что некий корреспондент использует адрес FEC0::1234:5678:9ABC, а потом попытаться поместить такой адрес в структуру адреса сокета и организовать соединение. Такая попытка завершится отказом, поскольку не будет задана переменная site identifier, как в FEC0::1234:5678:9ABC%1 (использование символа % в качестве разделителя для идентификатора зоны задано в [SCOPING]). Проблема усугубляется тем, что идентификатор сайта меняется в зависимости от конкретизации хоста (например, может быть %1 или %2), что не позволяет сохранить идентификатор хоста в памяти или узнать у сервера имён.

Проблема для разработчиков вызвана неоднозначностью локальных для сайта адресов. Поскольку такие адреса не однозначны, разработчики приложений поддерживают идентификаторы сайтов для уточнения адресов хостов. Поддержка таких идентификаторов достаточно сложна для понимания и реализации.

2.2. Проблема разработчиков - локальная адресация

Простые приложения клиент-сервер с разделяемым адресом IP на прикладном уровне усложняются при использовании адресации IPv6 site-local. Эти приложения должны будут принимать интеллектуальные решения в части прохождения адресов через границу сайта. На практике для решения таких вопросов приложениям потребуется информация о топологии сети. Локальные для сайта адреса могут быть применены для случаев, когда клиент и сервер размещаются на одном сайте, но попытки использовать их для разнесённых между сайтами клиентов и серверов будут заканчиваться неожиданными ошибками (например, сбросом соединения партнёром) или организаций соединений не с тем узлом. Отказоустойчивость и безопасность при отправке пакетов неизвестному хосту может существенно меняться от приложения к приложению.

Приложения с множеством участников (Multi-party), которые передают адреса IP на прикладном уровне, сталкиваются с особой проблемой. Даже если узел может корректно определить место нахождения удалённого узла (на этом же или другом сайте), он не сможет узнать по какому адресу нужно отправлять пакеты для него. Наилучшим выходом для таких приложений может оказаться переход на использование только глобальных адресов. Однако это будет препятствовать использованию таких приложений в изолированных и периодически подключаемых сетях, для которых доступны только адреса site-local, и может приводить к несовместимости с использованием в некоторых случаях адресов site-local для контроля доступа.

Таким образом, неоднозначность локальных для сайта адресов ведёт к неожиданному поведению приложений в тех случаях, когда данные в пакетах приложения используют локальные адреса, относящиеся к другим сайтам.

2.3. Проблема администраторов - утечки

Поддержка локальных для сайта адресов IPv6 во многих случаях проще работы с приватными блоками адресов RFC 1918 [RFC1918] в некоторых сетях IPv4. Теоретически, адреса, определённые в RFC 1918 должны использоваться только локально и не появляться в сети Internet. На практике такие адреса «утекают» в публичные сети. Комбинация утечек и неоднозначностей будет вызывать проблемы управления сетями.

Имена и адреса хостов приватных сетей могут «утекать» в почтовых сообщениях, web-страницах или файлах. Использование приватных адресов в полях отправителя или получателя запросов TCP или сообщений UDP (например, DNS или traceroute) будут приводить к отказам или доставке откликов на совершенно другие хосты.

Опыт использования адресов RFC 1918 показал также некоторые нетривиальные утечки в дополнение к приватным адресам в заголовках. Приватные адреса могут указываться также реверсных запросах DNS, которые будут создавать бесполезную загрузку инфраструктуры DNS. В общем случае многие приложения, использующие адреса IP напрямую, будут в конечном итоге приводить к путаницам и отказам.

Утечки вряд ли можно предотвратить. В то время, как некоторые приложения по своей природе имеют ограниченную область действия (например, Router Advertisement, Neighbor Discovery), большинство приложений не имеет таких концептуальных ограничений. В результате происходят утечки через границы (stuff leaks across the borders). Неоднозначность локальной для сайта адресации будет препятствовать поиску причин утечек. В результате утечки становятся трудно уловимыми, что вызывает разочарование администраторов.

2.4. Проблема маршрутизаторов - рост сложности

Неоднозначность локальных для сайта адресов создаёт сложности и для маршрутизаторов. Теоретически локальны адреса применяются только в рамках одного неразрывного сайта и все маршрутизаторы могут трактовать их, как однозначные. На практике же требуются специальные механизмы для случаев, когда сайт «разорван» на несколько частей или маршрутизатор обслуживает несколько сайтов.

В теории сайты никогда не должны «разрываться». На практике при использовании локальной для сайта адресации в большой сети некоторые компоненты сайта могут оказаться не подключёнными к нему непосредственно в результате того или иного разделения сети. Это потребует маршрутизировать пакеты с адресами site-local через те или иные промежуточные сети (например, опорную сеть оператора), не относящиеся к данному сайту. На практике это ведёт к использованию технологий туннелирования, многосайтовых маршрутизаторов или комбинации этих методов.

Неоднозначность адресации имеет очевидные проявления на многосайтовых маршрутизаторах. В классической архитектуре маршрутизации выходной интерфейс непосредственно определяется адресом получателя в соответствии с единой таблицей маршрутизации. Однако для маршрутизатора, соединённого с несколькими сайтами, маршрутизация пакетов с локальными для сайта адресами зависит также от интерфейса, через который пакет был принят. Интерфейсы связываются с сайтами и маршрутные записи для адресов site-local становятся зависимыми от сайта. Поддержка такой возможности требует реализации специальных функций в протоколах маршрутизации с методов виртуализации таблиц маршрутизации и пересылки, которые обычно применяются для VPN. Это создаёт дополнительные сложности при реализации и обслуживании маршрутизаторов.

Сложность управления сетями дополнительно возрастает за счёт того, что хотя на сайтах может поддерживаться привычная маршрутизация с доменами и областями, факторы, определяющие границы сайтов, отличаются от факторов, ограничивающих области и домены.

На многодомных маршрутизаторах (например, граничных маршрутизаторах сайтов) процесс пересылки усложняется за счёт применения фильтрации, позволяющей изолировать от проникновения наружу пакетов с локальными для сайта адресами. Этот процесс фильтрации может, в свою очередь, воздействовать на пересылку пакетов (например, ошибки в реализации могут приводить к отбрасыванию пакетов, направленных по глобальным адресам даже если такой адрес относится к целевому сайту).

Таким образом, неоднозначность адресации затрудняет управление многосайтовыми маршрутизаторами, которые требуются для поддержки «разорванных» сайтов и работы имеющихся протоколов маршрутизации.

2.5. Определение сайта

Существующее определение областей действия (scope) следует идеализированной концентрической модели. Предполагается, что хосты подключены к каналу, относящемуся к сайту, который, в свою очередь, относится к сети

Internet. Пакеты могут передаваться в свой (тот же) канал, на свой сайт или за пределы сайта. Однако споры вокруг определения сайта длятся уже много лет и согласия не достигнуто. Это говорит о том, что такое согласие маловероятно.

За пределами локального канала (link-local) границы области действия определены достаточно плохо. Что такое сайт? Является ли сайтом корпоративная сеть в целом или сайты должны быть территориально локализованы? Многие современные сети разделены на внутреннюю часть и внешнюю ДМЗ[1], отделённую межсетевым экраном. Серверы в ДМЗ доступны как из внутренней сети, так и для хостов Internet. Относятся ли хосты ДМЗ и внутренней сети к одному сайту?

Разные люди будут давать различные определения сайта. Такое определение может базироваться на границах безопасности, доступности, маршрутизации, QOS, административных или иных границах, а также на разных комбинациях этих границ. Весьма маловероятно определение области, удовлетворяющее всем этим требованиям.

Имеются хорошо известные и важные случаи, когда основанный на областях действия подход не будет работать, - сети, не соединённые напрямую, мобильные узлы, мобильные сети, междоменные VPN, сети с использованием хостинга, случаи слияния или разделения сетей и т. п. В частности, это означает, что «область действия» (scope) невозможно отобразить концентрическими кругами, как в примитивной модели канал/локальный/глобальный (link/local/global). Области могут перекрываться или проникать одна в другую. Принадлежность пары хостов к одной области может даже отличаться для разных протоколов.

Отметим в заключение, что современная концепция сайта наивна и не отражает эксплуатационных требований.

3. Разработка более эффективного решения

В предыдущем разделе приведены аргументы против локальных для сайта (site-local) адресов. Тем не менее, очевидны и некоторые преимущества такой адресации, без которых такие адреса были бы уже давно удалены из спецификации. Преимуществом таких адресов является простота, стабильность и частных характер распределения. Однако такие преимущества могут быть достигнуты и при использовании иной архитектуры. Примером может служить [Hinden/Haberman], где адреса не содержат неоднозначностей и не имеют явной области действия.

Наличие однозначной адресации в значительной мере снимает головную боль разработчиков за счёт избавления от необходимости работы с идентификаторами сайтов. Приложения могут использовать адреса, как будто они являются уникальными в глобальном масштабе, и стек протоколов может пользоваться стандартными методами определения интерфейсов, которые следует использовать. Однако часть головной боли остаётся по причине того, что эти адреса не всегда доступны, но приложения могут решать проблему недоступности адресов, пытаясь организовать соединение в другое время или с иным адресом. Теоретически, позднее может быть введён более изощрённый механизм с областями действия.

Наличие однозначных адресов не устраняет проблемы утечек, однако, благодаря однозначности, поиск и устранение утечек становятся много проще.

Наличие однозначных адресов будет решать большую часть проблем маршрутизаторов, которые в этом случае могут применять стандартные механизмы маршрутизации и не будут вынуждены поддерживать отдельные таблицы маршрутов на каждом интерфейсе. Некоторые проблемы сохраняются на граничных маршрутизаторах, которым требуется отфильтровать пакеты от некого множества отправителей, но эта задача легко разрешима.

Избавление от необходимости явного заявления области действия будет устранять проблемы, связанные с неоднозначностью понятия сайта. Недоступность некоторых адресов при возникновении такой необходимости может быть обеспечена средствами межсетевого экранирования. Правила экранирования можно легко приспособить к разным конфигурациям сетей, отвергая трафик из диапазонов новых однозначных адресов.

Остаётся вопрос anycast-адресации. Такие адреса являются неоднозначными по своему устройству, поскольку они относятся, по определению, ко всем хостам, которым был присвоен данный адрес anycast. Локальные для канала или глобальные адреса могут оказаться «впечатанными» в программный код. Нужны дополнительные исследования необходимости использования адресов anycast с областью действия между локальной для канала и глобальной.

4. Отказ от применения

Этот документ формально отменяет использование префикса локальных для сайта (site-local) индивидуальных адресов IPv6, определённого в [RFC3513], как 1111111011 или FEC0::/10. Специальная обработка для этого префикса **должна** быть исключена из новых реализаций. Префикс **недопустимо** выделять для иного применения до того, как он будет заново стандартизован IETF. Новые версии архитектуры адресации [RFC3513] будут включать эту информацию.

Реализации маршрутизаторов **следует** настраивать для отказа от маршрутизации этого префикса по умолчанию.

Упоминания локальных для сайта адресов следует удалить из новых версий документов Default Address Selection for Internet Protocol version 6 [RFC3484], Basic Socket Interface Extensions for IPv6 [RFC3493] и Internet Protocol Version 6 (IPv6) Addressing Architecture [RFC3513]. Имеющиеся упоминания локальных адресов следует удалить из новых версий других документов IETF при их обновлении. Такие документы включают [RFC2772, RFC2894, RFC3082, RFC3111, RFC3142, RFC3177, RFC3316].

Существующие реализации и развёрнутые системы **могут** продолжать использование этого префикса.

5. Вопросы безопасности

Использование адресов site-local может оказывать негативное влияние на безопасность сетей по причине утечек, неоднозначности и возможности некорректной маршрутизации, как указано в разделе 2. Отказ от применения неоднозначных адресов решит большую часть этих проблем.

Префикс индивидуальных адресов site-local обеспечивает возможность некоторых блокировок в правилах межсетевых экранов и правилах отбора адресов, что обычно рассматривают, как средство защиты, позволяющее предотвратить

[1] «Демилитаризованная» зона.

прохождение пакетов через административную границу. Такие правила блокировки можно создать для любого префикса, включая будущую замену префикса локальных для сайта адресов. Если такие правила блокировки выполняются, отказ от применения префикса site-local не снижает уровня безопасности.

6. Взаимодействие с IANA

Агентству IANA направлен запрос на маркировку префикса FEC0::/10, как отменённого (deprecated) со ссылкой на данный документ. Последующее использование этого префикса для тех или иных целей потребует прохождения процедуры стандартизации (IETF Standards Action) [RFC2434].

7. Благодарности

Авторы благодарны Fred Templin, Peter Bieringer, Chirayu Patel, Pekka Savola и Alain Baudot за обзор начальной версии документа. Текст параграфа 2.2 включает два абзаца из версии Margaret Wasserman, описывающие влияние локальной для сайта адресации. Alain Durand указал на необходимость пересмотра существующего RFC со ссылками на локальные для сайта адреса.

8. Литература

8.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

8.2. Информационные ссылки

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2772] ockell, R. and R. Fink, "6Bone Backbone Routing Guidelines", RFC 2772, February 2000.

[RFC2894] Crawford, M., "Router Renumbering for IPv6", RFC 2894, August 2000.

[RFC3082] Kempf, J. and J. Goldschmidt, "Notification and Subscription for SLP", RFC 3082, March 2001.

[RFC3111] Guttman, E., "Service Location Protocol Modifications for IPv6", RFC 3111, May 2001.

[RFC3142] Hagino, J. and K. Yamamoto, "An Ipv6-to-IPv4 Transport Relay Translator", RFC 3142, June 2001.

[RFC3177] IAB and IESG, "IAB/IESG Recommendations on Ipv6 Address", RFC 3177, September 2001.

[RFC3316] Arkko, J., Kuijpers, G., Soliman, H., Loughney, J., and J. Wiljakka, "Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts", RFC 3316, April 2003.

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, February 2003.

[Hinden/Haberman] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", Work in Progress, June 2004.

[SCOPING] Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", Work in Progress, August 2004.

9. Адреса авторов

Christian Huitema
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
USA
EMail: huitema@microsoft.com

Brian Carpenter
IBM Corporation
Sauemerstrasse 4
8803 Rueschlikon
Switzerland
EMail: brc@zurich.ibm.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

10. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.