Internet Engineering Task Force (IETF)
Request for Comments: 7558
Category: Informational
ISSN: 2070-1721

K. Lynn
Verizon Labs
S. Cheshire
Apple, Inc.
M. Blanchet
Viagenie
D. Migault
Ericsson

July 2015

Requirements for Scalable DNS-Based Service Discovery (DNS-SD) / Multicast DNS (mDNS) Extensions

Требования к расширяемому обнаружению служб на основе DNS с использованием mDNS

Аннотация

Обнаружение служб на основе DNS (DNS-SD) через Multicast DNS (mDNS) широко применяется сегодня для обнаружения и распознавания служб и имён на локальном соединении, но здесь рассматривается расширение DNS-SD/mDNS для обнаружения служб за пределами локального канала. Документ содержит постановку задачи и список требований к расширяемому DNS-SD.

Статус документа

Документ не содержит спецификации стандартов Internet и публикуется с информационными целями.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 5741.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc7558.

Оглавление

[1] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Обнаружение служб на основе DNS [DNS-SD] в сочетании с технологией Multicast DNS [mDNS] широко применяется для обнаружения и распознавания служб и имён на локальном канале. Однако при переходе к многоканальным домашним и кампусным сетям становится явным, что mDNS (по устройству) не работает через маршрутизаторы. DNS-SD может также применяться с обычным (unicast) DNS для обнаружения служб в более широкой (глобальной) области, но такая возможность ещё не получила широкого распространения. Это несоответствие потребностей пользователей и современной практики привело к разработке таких улучшений, как петиция Educause [EP].

В ответ на это и другие признаки спроса было предложено несколько решений, позволяющих обнаружить службы за пределами локального канала на основе различных специализированных методов. На данный момент нет единого мнения относительно лучшего подхода для долгосрочного развития протокола обнаружения служб на основе DNS.

Решение Multicast DNS в современной форме оптимизировано даже для сетевых технологий, где передача группового трафика обходится сравнительно дорого. Беспроводные сети, такие как Wi-Fi [IEEE.802.11], могут столкнуться проблемами при высоком уровне трафика mDNS по причине значительных издержек на передачу группового трафика. Беспроводные mesh-сети, такие как 6LoWPAN[1] [RFC4944], фактически являются многоканальными подсетями [RFC4903], где групповые пакеты должны пересылаться промежуточными узлами. В интересах конечных пользователей, администраторов и производителей следует развивать сотрудничество в контексте IETF для создания эффективного, расширяемого решения с обеспечением совместимости на основе стандартов.

В этом документе содержится постановка задачи и собраны требования для расширяемых решений DNS-SD/mDNS.

1.1. Термины и сокращения

Service - служба, сервис
: Конечная точка (хост или порт), прослушивающая данный прикладной протокол. Службы идентифицируются именами экземпляров (Service Instance Name).

DNS-SD
: Обнаружение служб на основе DNS [DNS-SD] - это обычное приложение с записями DNS о ресурсах и сообщениями для более простого именования, обнаружения и определения местоположения служб. При автономном использовании этот термин относится к unicast-протоколу для распределенных сетей.

mDNS
: Multicast DNS [mDNS] - это механизм, упрощающий распределенную реализацию функций в стиле DNS (включая DNS-SD) на локальном канале без необходимости применения традиционной инфраструктуры DNS.

SSD
: Расширяемое обнаружение служб (Scalable Service Discovery или Scalable DNS-SD) - это будущее расширение DNS-SD (и возможно mDNS) в соответствии с требованиями этого документа.

Scope of Discovery - область обнаружения
: Подмножество локального или глобального пространства имён (например, субдомен DNS), являющееся целью данного запроса SSD.

Zero Configuration
: Развёртывание SSD, не требующее администрирования (могут быть необязательные функции администрирования).

Incremental Deployment - постепенное развёртывание
: Упорядоченный переход по мере развития сети с переходом от DNS-SD/mDNS к SSD.

2. Постановка задачи

Обнаружение служб за пределами локального канала возможно является одной из наиболее важных функций, отсутствующих в модели DNS-SD на основе mDNS (DNS-SD over mDNS или DNS-SD/mDNS). Другие вопросы и требования кратко изложены ниже.

2.1. Именование и обнаружение на нескольких каналах

Список желаемых улучшений DNS-SD/mDNS от сетевых администраторов исследовательского и образовательного сообщества был опубликован в петиции Educause [EP]. Ниже кратко изложены технические аспекты петиции.

- На предприятиях и в учреждениях распространено использование беспроводных каналов для доступа клиентов и кабельной инфраструктуры для серверов, которые обычно относятся к разным подсетям. Анонсирование услуг печати и потоковой передачи multimedia через DNS-SD на основе mDNS в настоящее время не обнаруживается клиентскими устройствами на другом канале. DNS-SD с обычным (unicast) DNS работает при размещении клиентов и серверов на разных каналах, но записи о ресурсах, описывающие службы, должны каким-то способом попадать в пространство имён unicast DNS.

- Записи о ресурсах DNS-SD можно вручную вносить в файл зоны обычного DNS [STATIC], но эту задачу должен выполнять администратор DNS. При динамическом выделении адресов IP устройствам, как это часто бывает при использовании DHCP, эта работа становится слишком трудоёмкой.

- Автоматической добавление записей DNS-SD с использованием DNS Update работает, но требует настройки на сервере DNS возможности использовать DNS Update и установки на устройствах свидетельств DNS Update для выполнения таких обновлений, что оказалось обременительным.

Поэтому нужен механизм заполнения пространства имён DNS соответствующими записями DNS-SD с меньшим объёмом ручного администрирования, нежели обычно требуется для традиционного (unicast) сервера DNS.

Ниже представлена сводка технических требований:

- расширяемость от сотен до тысяч устройств с поддержкой DNS-SD/mDNS в данной среде;

- одновременная работа с разными технологиями канального уровня для проводных и беспроводных сетей;

[1] IPv6 over Low-Power Wireless Personal Area Network - IPv6 в персональной беспроводной сети со слабым питанием.

- отсутствие значительного роста сетевого трафика (кабельного и беспроводного);
- рентабельность поддержки в масштабе предприятия.

2.2. Беспроводные ЛВС IEEE 802.11

Технология Multicast DNS изначально разрабатывалась для сетей Ethernet, доминировавших тогда на канальном уровне. В сетях Ethernet с общей средой групповые кадры вносят немного дополнительных требований по сравнению с индивидуальными. Однако в сетях 802.11 групповые кадры передаются с низкой скоростью, поддерживаемой всеми приёмниками. На практике это отнимает большую часть «эфирного времени» на передачу группового трафика. Некоторые администраторы блокируют групповой трафик или используют точки доступа, передающие групповые кадры как серию индивидуальных.

Надёжность беспроводных каналов может быть на несколько порядков ниже надёжности кабельных соединений. Для повышения надёжности передачи IEEE 802.11 MAC[1] требует подтверждения доставки индивидуальных кадров, однако подтверждение доставки групповых кадров не поддерживается. В результате в беспроводных сетях часто наблюдаются более значительные потери групповых кадров, нежели в кабельных каналах.

Для обнаружения служб в беспроводных сетях IEEE 802.11 требуется ограничить число передаваемых групповых кадров приемлемым низким значением или заменить их индивидуальными кадрами для использования функций надёжности на уровне MAC.

2.3. Сети со слабым питанием и потерями (LLN)

Новые технологии беспроводных mesh-сетей, такие как RPL[2] [RFC6550] и 6LoWPAN, вызвали несколько проблем для имеющихся систем DNS-SD/mDNS. Во-первых, групповая адресация на канале [RFC4291] определена для ближайших соседей (single-hop). беспроводная mesh-сеть, представляющая одну логическую подсеть, зачастую может включать несколько узлов пересылки [RFC4903], поэтому нужна большая область действия групповой адресации [RFC7346]. Для Multicast DNS область действия намеренно ограничивалась локальным каналом, чтобы не создавать дополнительный групповой трафик вне канала (off-link).

Кроме того, узлы со слабым питанием могут отключаться на длительное время по причине «засыпания» или в результате проблем с соединениями. В таких случаях узлы LLN могут не отвечать на запросы или не защищать свои имена на основе имеющихся решений.

3. Базовые варианты применения

Ниже определены несколько вариантов применения с разными характеристиками для описания мотивов и классификации целевых требований. Они упорядочены по росту сложности развёртывания и администрирования.

(A) Персональная сеть (Personal Area Network или PAN), простейший пример которой включает 1 сервер и одного клиента, например, переносной компьютер и принтер, на одном канале. PAN без маршрутизаторов могут работать без настройки конфигурации (Zero Configuration Networking) [ZC] с самостоятельным назначением адресов link-local [RFC3927] [RFC4862] и Multicast DNS [mDNS] для обнаружения имён и служб, как это в настоящее время используется в Mac OS X, iOS, Windows [B4W], Android [NSD].

(B) Классическая домашняя сеть или hotspot (точка доступа) с приведёнными ниже свойствами.

- Один выходной маршрутизатор. Сеть может иметь одного или несколько «восходящих» провайдеров или сетей, но весь входящий и выходящий из них трафик проходит через 1 маршрутизатор.
- Один уровень «иерархии». Общий физический канал или несколько связанных мостами физических каналов для формирования одного логического канала, подключённого к принятому по умолчанию маршрутизатору. Один логический канал обеспечивает 1 домен широковещания, что упрощает использование Multicast DNS на локальном канале, а также ARP, что позволяет ограничиться в такой сети одной подсетью IPv4.
- Один административный домен. Все узлы контролирует один администратор (не обязательно сетевой).

(C) Расширенные домашние сети и сети небольших предприятий [RFC7368]. Похожи на (B), но содержат множество проводных и/или беспроводных каналов, обычно за одним выходным маршрутизатором. Однако узлы пересылки в основном используют самонастройку и не требуют администрирования для протокола маршрутизации. Такие сети обычно не должны требовать и администрирования DNS.

(D) Сети предприятий. Сеть произвольного диаметра с единым администрированием. Основная часть устройств пересылки и защиты настраивается и обычно имеется несколько выходных маршрутизаторов. Большие сети конференций, которые в основном используют беспроводный доступ, например, применяемые на конференциях IETF, также относятся к этой категории.

(E) Сети ВУЗов. Похожи на (D), но администрирование ядра сети и оконечных сетей может быть разным.

(F) Mesh-сети, такие как RPL и 6LoWPAN. Многоканальные подсети с префиксами, заданными одним или несколькими граничными маршрутизаторами. Могут включать как элементы сети C, D или E.

4. Требования

Любое успешное решение SSD должно обеспечить баланс между противоречивыми целями, такими как расширяемость, возможность развёртывания и удобство использования. С учётом этого приведённые ниже требования не следует рассматривать изолированно.

[1] Medium Access Control - управление доступом к среде.
[2] Routing Protocol for LLNs - протокол маршрутизации для сетей со слабым питанием и потерями.

REQ1

Для случаев A, B, C следует применять режим Zero Configuration. Это предполагает способность клиентов и серверов автоматически определять принятую по умолчанию область анонсирования и поиска служб.

REQ2

Для случаев C, D, E следует обеспечивать способ настройки области обнаружения, поддерживающий диапазон топологически независимых зон (например, от подразделения до кампуса). Эта возможность должна присутствовать в протоколе и отдельные операторы не обязаны использовать её во всех случаях, в частности, для случая C может быть желательным режим Zero Configuration. При доступности нескольких областей должен быть способ перечисления вариантов выбора. Например, для C следует предлагать режим Zero Configuration (1 плоский список ресурсов) или настраиваемый (например, ресурсы, отсортированные по помещениям).

REQ3

Как отмечено в REQ2, область обнаружения не требуется согласовывать с топологией сети. Например, её можно привязать к физической удалённости (здания) или структуре организации (подразделения).

REQ4

Для случаев C, D, E следует предоставлять возможность поэтапного развёртывания решения.

REQ5

SSD следует основывать на имеющихся протоколах и развёртываниях DNS-SD/mDNS, работающих на локальном канале.

REQ6

SSD недопустимо оказывать негативное влияние или препятствовать работе других имеющихся протоколов и развёртываний.

REQ7

Механизм SSD должен быть способен работать в сетях, не ограниченных одним каналом или одной технологией, включая клиентов и службы на несмежных каналах.

REQ8

Желательно обеспечивать пользователям и устройствам возможность обнаружения служб на сайтах или в сетях, к которым они подключены.

REQ9

SSD следует обеспечивать эффективную работу на основных типах канальных уровней и каналов.

REQ10

В SSD следует учитывать сети, где энергопотребление является важным фактором, например, устройства со слабым питанием или «спящие» устройства.

REQ11

Механизм SSD должен обеспечивать возможность расширения до тысяч узлов с минимальной настройкой конфигурации и без снижения производительности сети. Возможным показателем является незначительное изменение трафика SSD на канале по мере роста числа служб.

REQ12

SSD следует обеспечивать единообразное взаимодействие с пользователем для случаев обнаружения локальных и удалённых служб.

REQ13

Предоставляемой механизмом SSD информации следует точно отражать текущее состояние обнаруживаемых в сети служб. Новая информация должна быть доступна в течение нескольких секунд, а устаревшие сведения не должны сохраняться неограниченно долго. В сети вся информация неизбежно в той или иной степени устаревает по прибытии к получателю хотя бы на несколько микросекунд. Поэтому всегда нужен инженерный компромисс между своевременностью и эффективностью. Решениям для SSD следует обеспечивать такой компромисс.

REQ14

Механизмам SSD следует работать в имеющихся сетях (описанные случаи A - F) без изменений сети на физическом или межсетевом уровне.

REQ15

Администратору анонсируемой службы следует предоставлять возможность управления анонсами за пределы локального канала.

5. Пространства имён

Пространство имён традиционного (unicast) DNS по большей части содержит уникальные в глобальном масштабе имена. Multicast DNS предоставляет каждому каналу своё пространство имён с уникальностью в контексте этого канала. Отыскивающим службы клиентам может потребоваться различать локальные и глобальные имена и указывать контекст для поиска одной службы в разных пространствах имён.

Устройства на разных каналах могут иметь одно имя mDNS (например, заданное по умолчанию производителем), поскольку уникальность имён mDNS гарантируется лишь на уровне канала. Это может создавать проблему неоднозначности меток при агрегировании результатов (например, для представления).

В SSD следует поддерживать метки на национальных языках в именах экземпляров служб (Service Instance Name), как это делается сегодня в DNS-SD/mDNS. Недопустимо влияние SSD на глобальное пространство имён и инфраструктуру DNS.

Проблему публикации локальных служб в глобальном пространстве имён DNS можно рассматривать как экспорт локальных записей о ресурсах и связанных с ними меток в некую зону DNS. Вопросы определения меток, взаимодействующих в локальном и глобальном пространстве имён, рассматриваются в [INTEROP-LABELS].

6. Вопросы безопасности

Поскольку SSD может автоматически собирать записи о ресурсах DNS-SD и публиковать их для широкого доступа, вопросы безопасности будут вероятно включать проблемы, отмеченные в спецификациях Multicast DNS [mDNS] и [DNS-SD]. В последующих параграфах выделены возможные угрозы, возникающие при развёртывании DNS-SD на множестве каналов или автоматическом администрировании DNS-SD.

6.1. Область обнаружения

В некоторых случаях владелец анонсируемой службы может не иметь чёткого указания области действия своего анонса. Например, в результате современного ограничения области действия mDNS одним каналом область действия анонсов по определению ограничена общим каналом между клиентом и сервером. Если анонс распространяется за пределы предусмотренного множества каналов, это может привести к раскрытию службы неуполномоченным (с точки зрения владельца) клиентам с возможностью последующих попыток подключения к анонсируемой службе. Это также раскрывает сведения (о хосте и службе) большему числу потенциальных злоумышленников.

Следует отметить, что обнаружение службы не обязательно предполагает её доступность, возможность подключения или использования данным клиентом. Механизмы контроля доступа к службам выходят за рамки этого документа.

Если область обнаружения должным образом не настроена и не ограничена, это ведёт к утечке информации за пределы сети.

6.2. Разные пространства имён

Возможны конфликты между локальным пространством имён и глобальными именами DNS. Без адекватной обратной связи ищущих службы клиент может не знать, подходит ли ему найденная служба, что также открывает фронт возможных атак.

6.3. Предоставление полномочий

DNSSEC может подтверждать действительность, но не точность записей в файле зоны. Модель доверия в глобальном DNS основана на том, что администраторы (люди) (a) вводят записи о ресурсах в файл зоны вручную или (b) настраивают сервер DNS для аутентификации доверенного устройства (например, сервера DHCP), которое может автоматически поддерживать такие записи.

Самозванец может зарегистрироваться на локальном канале и представиться легитимной службой. Такие «мошеннические» службы могут автоматически регистрироваться в unicast DNS-SD.

6.4. Проверка подлинности

До сих пор принцип plug-and-play в mDNS основывался на физическом подключении. Если устройство видимо через mDNS, оно предполагается доверенным. Однако это вряд ли корректно для чужих сетей. Если имеется риск обмана клиентов путём развёртывания мошеннических служб, следует рассмотреть вопрос аутентификации на уровне приложений. Вопросы проверки подлинности приложений выходят за рамки этого документа.

6.5. Контроль доступа

Контроль доступа означает возможность ограничить пользователям доступ к службам, анонсируемым через DNS-SD. В этом случае возможность обнаружить службы не означает автоматически возможность доступа к ней.

Хотя управление доступом к анонсируемым службам выходит за рамки DNS-SD, следует отметить, что контроль доступа сегодня зачастую обеспечивается инфраструктурой сайта (например, списки управления доступом на маршрутизаторах, межсетевые экраны) и/или соответствующими механизмами служб (например, аутентификация пользователей). Для сетевых принтеров, например, доступ может контролироваться по идентификаторам пользователей с вводом пароля. Программы Apple поддерживают такой контроль доступа для принтеров USB, совместно используемых через Mac OS X Printer Sharing, а также для многих сетевых принтеров. Таким образом, использование имеющихся в службах механизмов защиты (выходят за рамки DNS-SD) не создаёт новых проблем безопасности.

6.6. Вопросы приватности

Мобильные устройства, такие как смартфоны или ноутбуки, могут раскрывать местоположение владельцев при регистрации в разных зонах, что может создавать риски приватности. Таким устройствам недопустимо регистрировать свои службы в произвольных зонах без одобрения (согласия - opt-in) их пользователя. Однако следует обеспечивать возможность настройки одной или нескольких «безопасных» зон, где мобильные устройства могут автоматически регистрировать свои службы.

7. Литература

7.1. Нормативные документы

[DNS-SD] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <http://www.rfc-editor.org/info/rfc6763>.

[mDNS] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <http://www.rfc-editor.org/info/rfc6762>.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, DOI 10.17487/RFC3927, May 2005, <http://www.rfc-editor.org/info/rfc3927>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <http://www.rfc-editor.org/info/rfc4291>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <http://www.rfc-editor.org/info/rfc4862>.

[RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903, DOI 10.17487/RFC4903, June 2007, <http://www.rfc-editor.org/info/rfc4903>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <http://www.rfc-editor.org/info/rfc4944>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <http://www.rfc-editor.org/info/rfc6550>.

[RFC7346] Droms, R., "IPv6 Multicast Address Scopes", RFC 7346, DOI 10.17487/RFC7346, August 2014, <http://www.rfc-editor.org/info/rfc7346>.

[RFC7368] Chown, T., Ed., Arkko, J., Brandt, A., Troan, O., and J. Weil, "IPv6 Home Networking Architecture Principles", RFC 7368, DOI 10.17487/RFC7368, October 2014, <http://www.rfc-editor.org/info/rfc7368>.

7.2. Дополнительная литература

[B4W] "Bonjour (software)", <http://en.wikipedia.org/wiki/Bonjour_(software)>.

[EP] Badman, L., "Petitioning Apple: From Educause Higher Ed Wireless Networking Admin Group", July 2012, <https://www.change.org/p/from-educause-higher-ed-wireless-networking-admin-group>.

[IEEE.802.11] IEEE Computer Society, "IEEE Standard for Information technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11, <http://standards.ieee.org/about/get/802/802.11.html>.

[INTEROP-LABELS] Sullivan, A., "On Interoperation of Labels Between mDNS and DNS", Work in Progress, draft-sullivan-dnssd-mdns-dns-interop-01[1], October 2014.

[NSD] Android, "NsdManager", <http://developer.android.com/reference/android/net/nsd/NsdManager.html>.

[STATIC] "Manually Adding DNS-SD Service Discovery Records to an Existing Name Server", July 2013, <http://www.dns-sd.org/ServerStaticSetup.html>.

[ZC] Cheshire, S. and D. Steinberg, "Zero Configuration Networking: The Definitive Guide", O'Reilly Media, Inc., ISBN 0-596-10100-7, December 2005.

Благодарности

Авторы с благодарностью признают вклад в работу и комментарии от RJ Atkinson, Tim Chown, Guangqing Deng, Ralph Droms, Educause, David Farmer, Matthew Gast, Thomas Narten, Doug Otis, David Thaler, Peter Van Der Stok.

Адреса авторов

Kerry Lynn

Verizon Labs

50 Sylvan Road

Waltham, MA 95014

United States

Phone: +1 781 296 9722

Email: kerry.lynn@verizon.com

Stuart Cheshire

Apple, Inc.

1 Infinite Loop

Cupertino, CA 95014

United States

Phone: +1 408 974 3207

Email: cheshire@apple.com

Marc Blanchet

Viagenie

246 Aberdeen

Quebec, QC G1R 2E1

Canada

Email: Marc.Blanchet@viagenie.ca

URI: http://viagenie.ca

Daniel Migault

[1] Работа опубликована в RFC 8222. *Прим. перев.*

Ericsson

8400 Boulevard Decarie

Montreal, QC H4P 2N2

Canada

Phone: +1 514 452 2160

Email: daniel.migault@ericsson.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru