Internet Engineering Task Force (IETF)
Request for Comments: 9119
Category: Informational
ISSN: 2070-1721

C. Perkins
Lupin Lodge
M. McBride
Futurewei
D. Stanley
HPE
W. Kumari
Google
JC. Zúñiga
SIGFOX

October 2021

Multicast Considerations over IEEE 802 Wireless Media

Групповая передача в беспроводных средах IEEE 802

Аннотация

Хорошо известные проблемы с групповой адресацией (multicast) помешали развёртыванию группового взаимодействия в сетях 802.11 (Wi-Fi) и других беспроводных средах локального действия. В этом документе описаны известные ограничения группового обмена на канальном уровне (L2) в беспроводных сетях (в основном 802.11). Описаны также некоторые возможности улучшения, найденные IETF и IEEE 802 для беспроводных сред, а также некоторые варианты использования, способные повысить производительность сетей. Кроме того, приведены некоторые рекомендации по использованию и комбинированию этих улучшений, а также рассмотрены вопросы эксплуатации.

Статус документа

Документ относится к категории информационных и не задаёт стандартов Internet.

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 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9119.

Оглавление

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

1. Введение

Хорошо известные проблемы с групповой адресацией помешали развёртыванию группового взаимодействия в сетях 802.11 [dot11] и других локальных беспроводных средах, как описано в [mc-props] и [mc-prob-stmt]. Проблемы наблюдались при групповой адресации в протоколах IETF, использующих беспроводные среды IEEE 802. Хотя улучшения для групповой передачи были разработаны в IETF и IEEE 802, между спецификациями и реализациями, а также настройками сохраняется несовместимость.

Многие протоколы IETF зависят от широковещательной или групповой доставки управляющих сообщений множеству получателей. Групповая адресация позволяет передать данные множеству заинтересованных получателей без необходимости отправки копии каждому. При широковещательной передаче данные отправляются каждому устройству, независимо от его заинтересованности в них. Групповая передача применяется для таких целей, как обнаружение соседей (Neighbor Discovery или ND), лавинная рассылка по сети и распознавание адресов, а также для снижения нагрузки на сеть при передаче данных, предназначенных множеству адресатов. Помимо использования широковещательной и групповой передачи для пакетов управления, её применяют многие приложения, такие как Push To Talk[1] в больницах, видеослужбы на предприятиях, университетах и в жилых домах, отправляя групповые пакеты IP устройствам конечных пользователей, которые все чаще применяют Wi-Fi.

Протоколы IETF обычно полагаются на многоуровневую структуру протоколов для снижения или исключения зависимости протоколов более высокого уровня от конкретной природы уровня MAC или физической среды. В случае групповой передачи протоколы верхних уровней обычно разрабатывались в предположении, что передача пакета по адресу IP равноценна в плане помех и доступа к сетевой среде, независимо от использования индивидуального, группового или широковещательного IP-адреса получателя. Эта модель подходит для сетей с передачей по кабелю, таким как Ethernet. К сожалению во многих беспроводных средах «стоимость» доступа к среде может существенно меняться. Групповая передача через сеть Wi-Fi часто имеет столь низкую производительность, что её просто не разрешают. Были разработаны некоторые усовершенствования для протоколов IETF, которые предполагалось использовать в основном в беспроводных средах. Однако эти улучшения обычно не получали широкого распространения в большинстве беспроводных сетей.

Беспроводные протоколы IEEE 802 были разработаны с некоторыми функциями для поддержки группового трафика. Например, для передачи групповых кадров применяется более низкая частота модуляции и они могут быть получены всеми станциями в ячейке, независимо от расстояния и затухания на пути от базовой станции или точки доступа (Access Point или AP). Однако такие передачи с более низкочастотной модуляцией дольше занимают среду, препятствуя эффективной передаче трафика с более высокочастотной модуляцией для расположенных близко станций. По этой и другим причинам рабочие группы IEEE 802, такие как 802.11, разработали средства повышения эффективности групповой передачи на уровне L2 [ietf_802-11]. Дополнительное улучшение работы при использовании групповой передачи может быть достигнуто с помощью некоторых эксплуатационных и конфигурационных решений (см. раздел 5).

Похоже, все уже согласились с тем, что эти проблемы не будут решены в ближайшее время в первую очередь из-за того, что это дорого и групповая передача не обеспечивает надёжности. По сравнению с индивидуальным трафиком Wi-Fi, групповой рассматривается как нечто второсортное, несмотря на наличие множества протоколов, использующих multicast-передачу. Нужны какие-то средства повышения надёжности групповой передачи. Протокол IPv6 ND, насыщающий каналы Wi-Fi является лишь частью проблемы. В решении могут помочь классы трафика Wi-Fi. Этот документ нацелен на прояснение вопроса о том, какие проблемы следует решать в IETF, а какие - в IEEE (раздел 8).

В этом документе подробно описаны проблемы, вызываемые групповой передачей в беспроводных сетях, включая высокую частоту потерь пакетов, отсутствие подтверждений и низкую скорость данных. Рассмотрены также некоторые усовершенствования, разработанные в IETF и IEEE 802.11 для улучшения влияния среды передачи на групповой трафик. Приведены рекомендации для разработчиков в части применения и комбинирования этих улучшений, а также некоторые советы по выбору режимов работы. Вполне возможно, что документ будет полезен также разработчикам будущих беспроводных спецификаций IEEE.

2. Терминология

ACK
Подтверждение канального уровня 802.11 L2.

AES-CCMP
Протокол AES-Counter Mode CBC-MAC.

AP
Точка доступа IEEE 802.11.

Basic rate - базовая скорость
Наименьшая среди подключённых устройств скорость, обычно применяемая для широковещательного и группового трафика.

[1] Нажмите для разговора.

DVB-H
Digital Video Broadcasting - Handheld - переносное устройство для цифрового приёма видео.

DVB-IPDC
Digital Video Broadcasting - Internet Protocol Datacasting - передача данных IP через цифровое вещание видео.

DTIM
Delivery Traffic Indication Map (карта индикации доставки трафика) - информационный элемент, сообщающий о наличии или отсутствии у ассоциированных станций буферизованных групповых или широковещательных кадров.

MCS
Modulation and Coding Scheme - схема модуляции и кодирования.

NOC
Network Operations Center - сетевой операционный центр.

PER
Packet Error Rate - частота ошибок в пакетах.

STA
Станция 802.11 (например, переносное устройство).

TIM
Traffic Indication Map (карта индикации трафика) - информационный элемент, сообщающий о наличии или отсутствии у ассоциированных станций буферизованных индивидуальных кадров.

TKIP
Temporal Key Integrity Protocol - протокол защиты целостности временных ключей.

WiMAX
Worldwide Interoperability for Microwave Access

WPA
Wi-Fi Protected Access - защищённый доступ к Wi-Fi.

3. Известные проблемы групповой передачи

3.1. Проблемы на уровне L2 и ниже

В этом параграфе описаны некоторые проблемы, связанные с использованием групповой передачи в беспроводных сетях IEEE 802.

3.1.1. Ненадёжность групповой передачи

Надёжность группового трафика обычно значительно ниже, чем индивидуального. Поскольку для групповой передачи применяется режим «один со многими», для подтверждения доставки требуется передача множества пакетов. Однако для групповой передачи подтверждения (ACK) не применяются и точка доступа (AP) не знает, требуется ли повторная отправка. Даже в кабельной части Internet с этим зачастую связан нежелательно высокий уровень ошибок. В результате групповые приложения внедряются сравнительно медленно, хотя протоколы для них давно доступны. В беспроводных сетях ситуация значительно хуже и очень чувствительна к наличию фонового трафика. В результате может наблюдаться очень высокая частота пакетных ошибок (packet error rate или PER) из-за отсутствия повторов передачи и снижения скорости отправки. PER представляет собой долю (в процентах) пакетов, которые не были получены устройством. Нередко этот уровень превышает 5%, что особенно неприятно для видео и других данных, где нужна высокая скорость и надёжность.

3.1.2. Низкая и переменная скорость передачи данных

Групповая передача по кабелям отличается от беспроводной, поскольку кабельные каналы обычно работают на фиксированной скорости. Скорость передачи в Wi-Fi зависит от близости STA к AP. Полоса видеопотоков и пропускная способность в большой сети Wi-Fi будет меняться при перемещении устройства. Это влияет на возможности решений QoS эффективно резервировать пропускную способность и обеспечивать контроль подачи данных в сеть.

Для аутентифицированных и подключённых к AP беспроводных станций мощность, требуемая для хорошего приёма может существенно меняться от станции к станции. Для индивидуальной передачи целью является минимальное энергопотребление при максимальной скорости доставки данных получателю. Для групповой передачи цель заключается в достижении максимального числа получателей, которые могут корректно принять групповые пакеты. Обычно AP должна использовать существенно меньшую скорость передачи при высоком потреблении энергии, чтобы даже самая удалённая станция получила пакет, например, как кратко описано в разделе 4 [RFC5757]. Поэтому скорость передачи, например, видеопотока может быть ограничена окружением менее надёжного получателя, подключённого к AP.

Поскольку более отказоустойчивые схемы модуляции и кодирования (modulation and coding scheme или MCS) обеспечивают большую дальность, но меньшую скорость, широковещательный и групповой трафик обычно передаётся с наименьшей среди всех подключённых устройств скоростью. Эту скорость называют базовой. Уровень дополнительных помех зависит от конкретной беспроводной технологии. Фактически, совместимость с более старыми устройствами и многопоточные реализации позволяют передавать индивидуальный трафик со скоростью несколько Гбит/с, а разница скорости передачи группового или широковещательного трафика и оптимальной скорости индивидуального трафика может превышать 3 порядка. Некоторые методы повышения спектральной эффективности, такие как пространственное мультиплексирование в системах с несколькими входами и выходами (Multiple Input Multiple Output или MIMO) недоступны для нескольких получателей. Совместимость со старыми версиями не является единственным фактором ограничения скорости групповой передачи.

Проводная групповая передача также влияет на беспроводные LAN, когда AP служит расширением кабельного сегмента. В этом случае групповые и широковещательные кадры на проводной стороне ЛВС копируются в беспроводную сеть (Wireless Local Area Network или WLAN). Поскольку широковещательные сообщения передаются с более отказоустойчивыми схемами MCS, многие большие кадры отправляются с малой скоростью через беспроводный канал.

3.1.3. Пропускная способность и влияние на помехи

Передача с более низкой скоростью дольше занимает беспроводную среду и отнимает эфирное время других коммуникаций, снижая общую пропускную способность. Кроме того, передача с более высоким уровнем сигнала, требуемая для доставки всем STA, связанным с AP, пропорционально повышает помехи другим пользователям радиоканалов.

3.1.4. Влияние энергосбережения на групповой трафик

Одной из характеристик групповой передачи в Wi-Fi является настройка каждой станции на пробуждение по приёму группового кадра, даже если тот будет в итоге отброшен. Это оказывает сильное влияние на потребляемую станцией энергию. По этой причине были найдены некоторые обходные пути, такие как направленная групповая передача (Directed Multicast Service или DMS), описанная в разделе 4, чтобы избежать пробуждения станций.

Групповая и индивидуальная передача может плохо работать с механизмами энергосбережения IEEE 802.11e в силу перечисленных ниже причин.

- Клиенты могут быть не способны оставаться в спящем режиме из-за частого пробуждения групповыми пакетами управления.
- Индивидуальный пакет задерживается, пока STA не проснётся и не запросит его. Задержка индивидуального трафика может также служить для экономии энергии, а также повышения эффективности и вероятности агрегирования.
- Групповой трафик задерживается в беспроводной сети, если любая из STA в сети применяет энергосбережение. Все STA, связанные с AP, должны быть активны для получения группового трафика.
- Пакеты могут отбрасываться из-за ограничений буферов в AP и STA без AP.

3.2. Проблемы на уровне L3 и выше

В этом параграфе рассматриваются некоторые протоколы IETF и возможное снижение их производительности при использовании групповых управляющих сообщений. Типичными примерами использования групповых пакетов служат:

- сигнализация плоскости управления;
- обнаружение соседей;
- распознавание адресов;
- обнаружение служб;
- приложения (доставка видео, данных складов и т. п.);
- маршрутизация по запросу;
- создание магистрали;
- другие протоколы L3 (не IP).

Протокол пользовательских дейтаграмм (User Datagram Protocol или UDP наиболее распространён для доставки группового трафика. Сам по себе, протокол UDP не обеспечивает гарантий и сообщения могут теряться или менять порядок доставки.

3.2.1. Проблемы IPv4

Ниже представлены некоторые типовые протоколы обнаружения, использующие групповую или широковещательную передачу по протоколу IPv4.

- ARP [RFC0826].
- DHCP [RFC2131].
- Multicast DNS (mDNS) [RFC6762].
- Universal Plug and Play (uPnP) [RFC6970].

После начальной настройки ARP (см. ниже), DHCP и uPnP применяются достаточно редко, но обнаружение служб может происходить в любой момент. Некоторые широко распространённые протоколы обнаружения служб (например, для поиска принтеров) используют механизм mDNS (групповой), который операторы часто блокируют. Даже при отслеживании групповой передачи [RFC4541] (которое обеспечивает сохранение пропускной способности сегментов сети, где ни один узел не заявил интереса в получении пакетов по этому групповому адресу) одновременно может регистрироваться много устройств, существенно снижая производительность сети.

3.2.2. Проблемы IPv6

В IPv6 групповая передача применяется более широко, включая протоколы:

- DHCPv6 [RFC8415];
- Protocol Independent Multicast (PIM) [RFC7761];
- IPv6 Neighbor Discovery Protocol (NDP) [RFC4861];
- Multicast DNS (mDNS) [RFC6762];
- Router Discovery [RFC4286].

Сообщения IPv6 NDP Neighbor Solicitation (NS) при обнаружении дубликатов адресов (Duplicate Address Detection или DAD) и поиске адресов могут использовать групповую адресацию с областью действия на локальном канале (link-

scope). В отличие от IPv4, узел IPv6 обычно использует несколько адресов и может часто менять их по соображениям приватности. Влияние групповых сообщений возрастает при мобильности устройств. Анонсы маршрутизаторов (Router advertisement или RA) также периодически передаются по групповым адресам.

Сосед может считаться потерянным при отказе нескольких пакетов Neighbor Discovery подряд.

3.2.3. Проблемы MLD

Обнаружение слушателей группового трафика (Multicast Listener Discovery или MLD) [RFC4541] применяется для обнаружения членов multicast-группы, подключённых к портам коммутатора. Пересылка групповых кадров в область с поддержкой Wi-Fi может использовать поддержку коммутатором сведений о пересылке на аппаратном уровне. По причине интенсивного применения групповой передачи в IPv6 для каждой станции STA с адресом IPv6 потребуется хранить в коммутаторе состояние для нескольких (возможно многих) групповых адресов solicited-node. Это групповые адреса IPv6Ю используемые протоколом NDP для проверки занятости адресов IPv6 на локальном канале. Групповые адреса, для которых не установлено состояние пересылки (возможно по причине недостатка памяти в коммутаторе), будут вызывать лавинную рассылку во все порты коммутатора. Некоторые производители коммутаторов не поддерживают MLD для групповой передачи link-scope, по причине требований к поддержке состояний.

3.2.4. Ложное обнаружение соседей

В Internet существует фоновое сканирование трафика (люди, занимающиеся поиском уязвимых машин) и «обратное рассеяние» (отклики на обманный трафик и т. п.). Это означает, что маршрутизаторы очень часто передают пакеты по адресам IPv4, которые могут не использоваться. При назначении IP-адреса хосту маршрутизатор передаёт широковещательный запрос ARP, получает отклик ARP и кэширует его, а затем трафик может быть доставлен хосту. Когда IP-адрес не используется, маршрутизатор передаёт 1 или несколько широковещательных запросов ARP и не получает на них отклика. Это означает, что запись в кэш ARP не вносится и следующий пакет по этому адресу IP приведёт к новой широковещательной передаче запросов ARP.

Частота этих запросов ARP пропорциональна размеру подсетей, темпам сканирования и обратного рассеяния, а также времени хранения маршрутизатором состояний для отсутствия ответов ARP. Оказывается, что эта частота обратно пропорциональная заполненности подсети (действительные ARP сохраняются в кэше без широковещательных повторов, а неиспользуемые адреса IP не отвечают на запросы, что увеличивает широковещательный трафик). В зависимости от используемого пространства адресов, времени суток, заполненности сети и других (неизвестных) факторов могут наблюдаться тысячи широковещательных пакетов в секунду. Наблюдалось около 2000 широковещательных пакетов в секунду в сети IETF NOC во время конференций.

С помощью протокола Neighbor Discovery для IPv6 [RFC4861] узлы распознают адреса путём групповой передачи сообщений Neighbor Solicitation, запрашивающих у узлов адрес канального уровня. Сообщения Neighbor Solicitation передаются по групповому адресу solicited-node. Целевой узел возвращает адрес канального уровня в индивидуальном сообщении Neighbor Advertisement. Одной пары пакетов с запросом и откликом достаточно для инициатора и цели, чтобы узнать адреса канального уровня друг друга (инициатор включает его в Neighbor Solicitation).

В кабельных сетях нет большой разницы между индивидуальным, групповым и широковещательным трафиком. В результате аппаратной фильтрации (см., например, [Deri-2010]) непреднамеренный лавинный трафик (или избыточные групповые кадры Ethernet) в кабельной сети может быть значительно «дешевле» по сравнению с беспроводными сетями, где спящие устройства пробуждаются для обработки пакетов. Кабельные сети Ethernet как правило являются коммутируемыми, что дополнительно снижает помехи от группового трафика. Фактически не возникает проблем с коллизиями и планированием за исключением случаев чрезвычайно высокой загрузки порта. В беспроводных сетях это не так и оборудование зачастую неспособно передавать большие объёмы широковещательного и группового трафика, что ведёт к отбрасыванию значительной части таких пакетов. Поэтому при подключении хоста он зачастую не может завершить процедуру DHCP и пакеты IPv6 RA отбрасываются, что препятствует доступу пользователя в сеть.

4. Оптимизация группового протокола

В этом разделе описаны некоторые пути оптимизации, предложенные в IEEE 802 и IETF для смягчения или исключения проблем, отмеченных в разделе 3.

4.1. Proxy ARP в 802.11-2012

AP знает адреса L2 (Medium Access Control или MAC) и IP всех связанных с ней STA. Таким образом, AP выступает центральным «менеджером» для всех 802.11 STA в наборе базовых служб (Basic Service Set или BSS). Proxy ARP легко реализовать на AP, обеспечив указанные ниже преимущества.

- Снижение широковещательного трафика (передаётся с низкими MCS) в беспроводной среде.
- STA может более эффективно использовать спящий режим, поскольку запросы ARP для её адреса IP обрабатывает AP.
- Кадры ARP не попадают в беспроводную среду.
- Не требуется менять реализации STA.

Ниже приведён фрагмент спецификации из параграфа 10.23.13 [dot11-proxyarp].

> Когда AP поддерживает Proxy ARP «[...] AP нужно поддерживать сопоставление аппаратных адресов с адресами Internet для каждой связанной станции и обновлять сопоставление при смене станцией адреса Internet. При преобразовании адреса IPv4 с помощью запроса ARP от станции STA без AP, связанной с BSS, службе Proxy ARP нужно отвечать от имени STA на запрос ARP или пакет ARP Probe.

4.2. Регистрация адресов IPv6 и Proxy ND

В этом параграфе персональной беспроводной со слабым питанием (Low-Power Wireless Personal Area Network или 6LoWPAN) считается сеть со слабым питанием и потерями (Low-Power and Lossy Network или LLN), поддерживающая

сжатие заголовков 6LoWPAN (Header Compression или HC) [RFC6282]. Примером 6LoWPAN является сеть 6TiSCH [RFC9030]. Для контроля использования групповой передачи IPv6 через сети 6LoWPAN разработан стандарт 6LoWPAN Neighbor Discovery (6LoWPAN ND) [RFC6775], определяющий механизм регистрации адресов на основе центрального реестра, контролирующего уникальность адресов вместо неэффективного механизма DAD применяемого протоколом обнаружения соседей IPv6 (Neighbor Discovery Protocol или NDP) [RFC4861] [RFC4862].

Рабочая группа 6lo подготовила обновление [RFC6775]. Беспроводное устройство может регистрировать свой адрес на магистральном маршрутизаторе (Backbone Router) [RFC8929], который служит посредником к IPv6 NDP, работающему высокоскоростной магистрали агрегирования. Обновление также включает механизм прокси-регистрации от имени зарегистрированного узла, например, через маршрутизатор 6LoWPAN, к которому подключён мобильный узел.

Общая идея концепции магистрального маршрутизатора заключается в том, что широковещательные и групповые сообщения следует строго контролировать в разных WLAN и персональных беспроводных сетях (Wireless Personal Area Network или WPAN). Связность с конкретным каналом, обеспечивающим подсеть, следует сохранить на уровне L3. Модель работы Backbone Router показана на рисунке 1.

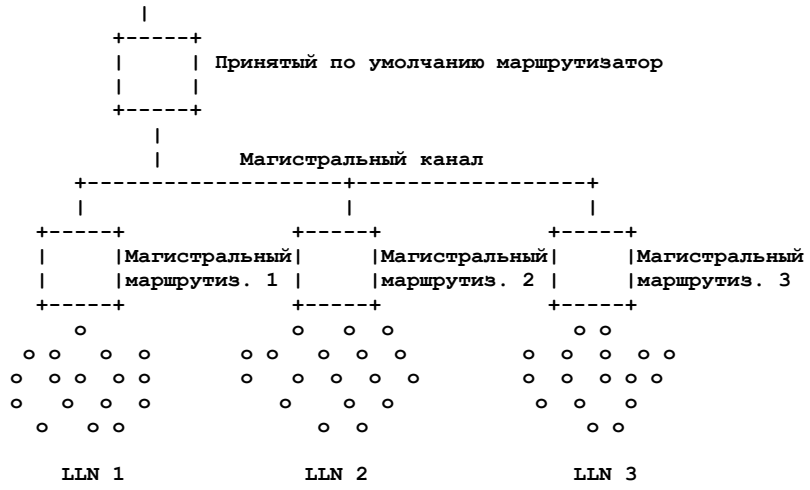

Рисунок 1. Магистральный канал и магистральные маршрутизаторы.

Узлы LLN могут свободно перемещаться из сети LLN, привязанной к одному магистральному маршрутизатору IPv6 BR, в сеть, привязанную к другому BR на той же магистрали, сохраняя все настроенные адреса IPv6. Маршрутизаторы BR поддерживают таблицу привязки (Binding Table) своих зарегистрированных адресов, которая служит распределенной базой данных обо всех узлах LLN. Расширение протокола NDP введено для обмена данными таблиц привязки через магистральный канал (Backbone Link) для обеспечения работы IPv6 Neighbor Discovery.

В [RFC6775] и последующем документе [RFC8505] рассматриваются потребности LLN и похожих методов, которые вероятно будут полезны для каналов любого типа, где подключены спящие устройства или следует ограничить широковещательный и групповой трафик.

4.3. Буферизация для увеличения срока службы батареи

Разработаны методы, позволяющие продлить срок службы батареи. Например, устройство может не просыпаться при получении точкой доступа (AP) группового пакета. AP действует от имени STA разными способами. Для включения функций экономии энергии в STA в своём наборе BSS точка доступа AP буферизует предназначенные STA кадры до времени, когда STA планирует приём. Если AP, например, выражает сообщение индикации доставки трафика (Delivery Traffic Indication Message или DTIM) 3, AP будет передавать групповой пакет через каждые 3 пакета. Фактически, когда любая отдельная беспроводная станция STA, связанная с AP, имеет включенный режим энергосбережения 802.11, AP буферизует все групповые кадры и передаёт их лишь после следующего сигнала DTIM.

На практике большинство AP будет передавать групповые пакеты каждые 30 секунд. Для индивидуальных пакетов AP может передавать сообщение индикации трафика (Traffic Indication Message или TIM), но для группового трафика AP передаёт широковещательное сообщение всем. DTIM управляет питанием, но STA могут сами решить, нужно ли просыпаться и когда отбрасывать пакет. К сожалению без должной административной настройки такие STA могут быть не способны определить, почему их групповые операции не работают.

4.4. Ограничение глубины аппаратной очереди группового буфера

Очередь CAB (Content after Beacon) служит для передачи буферизованных групповых кадров по сигналу. Если буферизовано много групповых кадров и очередь заполнена, она «заглушает» весь обычный трафик. Для ограничения ущерба, который может нанести буферизованный трафик, некоторые драйверы ограничивают объем групповых данных в очереди до доли beacon_interval. Пример этого приведён в [CAB].

4.5. Поддержка IPv6 в 802.11-2012

IPv6 использует NDP вместо ARP. Каждый узел IPv6 подписан для этого на специальный групповой адрес. Ниже приведён фрагмент текста из параграфа 10.23.13 в [dot11-proxyarp].

> При распознавании адреса IPv6 службе Proxy Neighbor Discovery нужно отвечать сообщением Neighbor Advertisement [...] от имени связанной станции STA на сообщение [ICMPv6] Neighbor Solicitation [...]. При смене сопоставления с MAC-адресом AP может передавать незапрошенные сообщения Neighbor Advertisement от имени STA.

Протокол NDP можно использовать для запроса дополнительных данных с использованием разных методов, включая:

- Maximum Transmission Unit;

- Router Solicitation;
- Router Advertisement.

Сообщения NDP передаются как групповые (широковещательные) кадры 802.11. Использование прокси помогает сохранять сообщения NDP вне беспроводной среды.

4.6. Использование индивидуальной передачи вместо групповой

Зачастую можно передать групповые сообщения управления и данных индивидуально каждой станции.

4.6.1. Обзор

Во многих случаях через канал Wi-Fi лучше передавать индивидуальные пакеты вместо групповых. Это избавляет от большинства проблем, связанных с групповой передачей через Wi-Fi, поскольку индивидуальные кадры подтверждаются и буферизуются для клиентов с энергосбережением. При таком подходе иногда приходится один и тот же пакет передавать несколько раз через канал Wi-Fi. Однако во многих случаях, таких как передача видео в домашней сети, это обеспечивает хороший компромисс, поскольку канал Wi-Fi имеет достаточную ёмкость для индивидуального трафика для каждой подписавшейся STA, даже если на восходящем канале в сеть доступа применяется multicast.

Имеется несколько технологий, которые можно применять для индивидуальной передачи через Wi-Fi.

4.6.2. Преобразование на уровне L2

Зачастую можно передать групповые сообщения управления и данных индивидуально каждой станции.

Хотя пока нет стандартизованного метода преобразования, имеется по меньшей мере одна широко распространённая реализация в коде моста Linux [bridge-mc-2-uc]. Разные производители также имеют свои фирменные решения. В общем случае эти реализации выполняют прямое сопоставление для групп и каналов, обнаруженный при отслеживании IGMP и MLD, в соответствующие индивидуальные адреса MAC.

4.6.3. Направленная групповая передача DMS

DMS (Directed Multicast Service) позволяет STA запросить у AP передачу адресованных в группу кадров, предназначенных для запрашивающих STA в виде кадров с индивидуальным адресом (преобразовать в unicast). Ниже указаны некоторые характеристики DMS.

- Требуются блоки агрегирования данных сервиса 802.11n MAC (Aggregate MAC Service Data Unit или A-MSDU).
- Кадры с индивидуальными адресами подтверждаются и буферизуются для энергосберегающих STA.
- Запрашивающая STA может указать характеристики для трафика DMS.
- Служба DMS определена в IEEE Std 802.11v-2011 [v2011].
- DMS требует изменений в реализациях AP и STA.

Служба DMS в настоящее время ещё не реализована в продукции. Дополнительная информация доступна в [Tramarin2017] и [Oliva2013].

4.6.4. Автоматическое туннелирование AMT

AMT (Automatic Multicast Tunneling) [RFC7450] обеспечивает возможность туннелирования групповых пакетов IP в индивидуальных пакетах через сеть, поддерживающую лишь unicast-передачу. Когда операционная система или приложение на станции STA имеет встроенный шлюз AMT, она может использовать индивидуальную адресацию для передачи по каналу Wi-Fi, развернув ретранслятор AMT в не относящейся к Wi-Fi части сети, соединённой с AP.

Рекомендуется в сетях с поддержкой групповой передачи, где развёрнуты ретрансляторы AMT, обеспечивать локальное обнаружение этих ретрансляторов с использованием описанных в [RFC8777] методов:

- обнаружение служб на основе DNS (DNS-SD) [RFC6763];
- общеизвестные адреса IP из раздела 7 в [RFC7450].

Шлюз AMT, реализующий несколько стандартных методов обнаружения, с большей вероятностью найдёт локальную сеть с поддержкой групповой адресации нежели организует соединение с нелокальным ретранслятором AMT восходящего направления.

4.7. GroupCast с повторами (GCR)

Механизм GCR (GroupCast with Retries, [dot11aa]) повышает надёжность за счёт использования незапрошенных повторов или механизма подтверждения блока. GCR повышает вероятность получения групповых кадров, но все же не обеспечивает гарантии.

Для механизма подтверждения блоков AP использует для каждого адресованного в группу кадра обычную групповую передачу. Повторные передачи адресуются в группу, но скрыты от STA, не поддерживающих 802.11aa. Применяется схема направленного подтверждения блоков для сбора статуса приёма от получателей и на основе этого выполняется повтор передачи.

GCR подходит для групп любого размера. По мере роста числа устройств в группе GCR может передавать запросы подтверждения блоков небольшим частям группы. GCR не требует менять реализации AP и STA.

GCR может вносить неприемлемую задержку. После отправки группы кадров данных AP выполняет ряд действий:

- индивидуальная передача запроса подтверждения блока (Block Ack Request или BAR) части группы;
- ожидание соответствующего подтверждения блока (Block Ack или BA);

- повтор пропущенных кадров;
- восстановление других операций, которые могли быть задержаны.

Такая задержка может быть неприемлема для некоторых типов трафика.

В 802.11 разрабатываются расширения для повышения производительности GCR:

- запросы BAR передаются с использованием нисходящего многопользовательского MIMO (MU-MIMO);
- отклики BA передаются с использованием восходящего MU-MIMO (свойство IEEE 801.11ax-2021);
- задержка может быть дополнительно снижена одновременным получением данных BA от нескольких STA.

5. Эксплуатационная оптимизация

В этом разделе описаны некоторые варианты эксплуатационной оптимизации, которые могут быть реализованы при развёртывании беспроводных сетей IEEE 802 для смягчения проблем, описанных в разделе 3.

5.1. Устранение проблем ложного обнаружения соседей

ARP Sponge

ARP Sponge размещаются в сети и узнают реально применяемые адреса IP. Они также прослушивают запросы ARP и, видя ARP для адреса IP, который по их мнению не используется, будут передавать в ответ свой MAC-адрес. Это значит, что маршрутизатор будет иметь сопоставление IP-MAC, которое он кэширует. Если позднее этот адрес IP будет выделен машине (например, через DHCP), ARP Sponge увидит это и прекратит отвечать для него. Беспричинные (Gratuitous) ARP (или ARP от машин к их шлюзам) будут заменять подменный адрес (sponged) в ARP-таблице маршрутизатора. Этот метод достаточно эффективен, но к сожалению демоны ARP Sponge не были предназначены для такого применения - один из наиболее распространённых ARP Sponge [arpsponge] был разработан для борьбы с исчезновением участников обмена в IXP (Internet Exchange Point) и тоже не оптимизирован для такой задачи. Для каждой подсети нужен один демон, настройка сложна (скорость сканирования, плотность заполнения, число повторов и т. п.), а иногда демон просто останавливается, что требует перезапуска, вызывающего нарушения работы.

Маршрутизаторы

Некоторые маршрутизаторы (часто на основе Linux) реализуют демон негативного кэширования ARP. Если маршрутизатор не видит откликов на ARP, можно задать сохранение этой информации в течение некоторого времени. К сожалению, часто используемые в ядре маршрутизаторы не поддерживают этого. Вместо этого при получении адреса IP подключившимся к сети хостом он передаёт запрос ARP для принятого по умолчанию шлюза (маршрутизатора). Маршрутизатор обновляет свой кэш, включая в него сопоставление IP с MAC-адресом хоста из запроса (пассивное обучение ARP).

Фильтрация неиспользуемых адресов

Распределение пользователей в беспроводных (под)сетях может меняться в различных вариантах применения, таких как конференции (например, переименовываются SSID (Service Set Identifier), некоторые SSID становятся непопулярными и т. п.). Это осложняет прогнозирование использования конкретных SSID, но его можно отслеживать по мере использования сетей. Настройка нескольких пулов DHCP в подсети и их последующее включение позволяет создавать большую подсеть, в которой используются лишь младшие части адресов. Это позволяет применять входные списки доступа по IP, блокирующие старшие адреса, которые не используются. Маршрутизатор не пытается пересылать пакеты в старшие части пространств адресов и не использует для них ARP. Этот метод показал свою эффективность, но он достаточно трудоёмкий и требует координации.

Запрет и фильтрация запросов ARP

В общем случае маршрутизатору не нужны запросы ARP для хостов, он может получить сопоставление IP-MAC из переданного хостом при подключении запроса ARP. Поэтому следует обеспечивать возможность запрета и/или фильтрации запросов ARP от маршрутизатора. К сожалению ARP является фундаментальной и низкоуровневой частью стека IP и зачастую выгружается из обычной плоскости управления. Хотя многие маршрутизаторы могут фильтровать трафик на уровне L2, обычно это реализовано в форме входного фильтра, а возможности выходной фильтрации широковещательного трафика ограничены. Это означает, что кажущееся очевидным решение просто отключить или фильтровать ARP на выходе на практике сложно выполнить или оно ограничено реализацией или архитектурой.

Трансляция NAT

Широковещательная передача часто может вызываться сканированием или обратным рассеянием извне Wi-Fi. Для снижения влияния широковещания можно применять трансляцию NAT для всей (или большей части) сети. Для неиспользуемых адресов в NAT не будет записей и маршрутизатор не будет применять ARP для них. Однако имеется много причин отказываться от применения NAT в таком режиме.

Межсетевые экраны с учётом состояния

Другим очевидным решением является установка межсетевого экрана с поддержкой состояний между беспроводной сетью и Internet. Этот экран будет блокировать входящий трафик, не связанный с исходящими запросами. Однако такой подход не согласуется с необходимостью и желанием некоторых организаций делать сеть максимально открытой и соблюдать сквозные (end-to-end) принципы. Участникам сети конференции следует оставаться хостами Internet и иметь возможность получения незапрошенных сообщений. Однако поддержка работоспособности и стабильности сети важнее и для этого может потребоваться межсетевой экран с поддержкой состояний.

5.2. Устранение ложных сообщений обнаружения служб

В сетях, где нужно поддерживать сотни STA, операторы сталкиваются со снижением производительности в результате одновременной регистрации множества устройств с применением mDNS. В сети с большим числом клиентов рекомендуется ограничивать пакеты mDNS, адресованные службам обнаружения небольших домашних сетей, чтобы избежать помех остальному трафику.

6. Групповая передача в других беспроводных средах

Многие из описанных выше случаев потери производительности наблюдались и в беспроводных сетях, отличных от 802.11. Например, проблемы с энергосбережением, избыточной загрузкой среды и малой надёжностью проявляются также в сетях 802.15.3 и 802.15.4. К сожалению спецификация среды 802.15 пока не включает механизмов, подобных разработанным для 802.11. Фактически проектирование 802.15 нацелено на минимизацию и многие функции реализуются в протоколах вышележащих уровней. Это ведёт к мешанине несовместимых и фирменных решений. В [uli] подробно рассматриваются проблемы и представлены предложения для группы задач, решающие проблемы, где объем групповых передач можно снизить.

Похожие соображения применимы и к другим беспроводным средам. В работе [RFC5757] приведено краткое рассмотрение для сред 802.16 WiMAX, 3GPP/3GPP2, DVB-H/DVB-IPDC, а также широковещательного и спутникового телевидения.

7. Рекомендации

В этом разделе представлены рекомендации по использованию и комбинированию некоторых улучшений, описанных в разделах 4 и 5. В будущих документах для протоколов, применяющих групповую сигнализацию, следует тщательно учитывать вопросы использования протокола в беспроводных сетях.

Следует применять прокси-методы для экономии пропускной способности сети и снижения расхода батарей в устройствах с энергосбережением. Устройства могут передавать индивидуальные сообщения своим прокси, а те будут заботиться о всех требуемых групповых операциях.

Групповую сигнализацию для беспроводных устройств следует выполнять с учётом снижения занятости процессоров.

8. Вопросы для обсуждения

В этом разделе предложены два вопроса для обсуждения в целях дальнейшего развития.

Во-первых, органам стандартизации (включая частные) следует создавать рекомендации, помогающие прояснить, когда лучше передавать групповые пакеты через кабельную, а не беспроводную сеть. Например, 802.1ak [IEEE802.1ak] работает с Ethernet и Wi-Fi, поэтому организации могут помочь в принятии решений о развёртывании, разработав рекомендации для групповой передачи через Wi-Fi, включая варианты передачи трафика по кабелям.

Во-вторых, надёжная регистрация в multicast-группах L2 и надёжные групповые операции L2 могут обеспечить хорошее решение для Wi-Fi. Не следует требовать поддержки 2^{24} для групповой работы, достаточно просто выбрать число битов, имеющих смысл для данного размера сети, чтобы ограничить число нежелательных передач разумным уровнем. Рабочие группы IEEE 802.1, 802.11, 802.15 следует поощрять к пересмотру групповой передачи L2 и разработке работоспособных решений.

9. Вопросы безопасности

Этот документ не добавляет и не меняет механизмов защиты. Групповую передачу в кабельных и беспроводных сетях, рассматриваемую здесь, можно защитить разными способами. Например, в [RFC4601], описано применение IPsec для проверки подлинности сообщений на локальном канале (link-local) при независимой от протокола групповой маршрутизации (Protocol Independent Multicast - Sparse Mode или PIM-SM). В [RFC5796] заданы механизмы проверки подлинности локальных сообщений PIM-SM link-local с использованием IPsec ESP (Encapsulating Security Payload) или AH (Authentication Header).

При использовании механизмов преобразования группового трафика в индивидуальный для передачи по радиоканалам точка доступа AP (или иной объект) вынуждена явно отслеживать абонентов, заинтересованных в определённом групповом трафике. Обычно такой компромисс разумен, но но это ведёт к тому, что другой объект отслеживает подписчиков группового трафика. Хотя такая информация при необходимости где-то уже отслеживается, это расширяет фронт атак, при которых возможна утечка возможно конфиденциальных сведений.

Как отмечено в [group_key], ненадёжная по природе групповая передача через беспроводную среду может вызывать небольшие проблемы для управления и обновления групповых ключей. В [group_key] сказано, что при использовании шифрования TKIP (WPA сейчас не рекомендуется) или AES-CCMP (WPA2/WPA3) групповые пакеты от AP к клиентам (FromDS) должны шифроваться с использованием отдельного ключа, известного всем клиентам (Group Key). Далее там же сказано «... большинство клиентов могут подключаться и просматривать web0страницы, проверять почту и т. п., даже когда групповая передача FromDS не работает. Поэтому многие не осознают наличие проблем с групповой передачей в их сети …».

Этот документ рекомендует применять прокси-методы для экономии пропускной способности сети и снижения расхода батарей в устройствах с энергосбережением. С такими методами обычно связаны вопросы безопасности, требующие иметь доверенные прокси во избежание недопустимого поведения. Одним из таких методов является ARP Sponge, где прослушиваются запросы ARP и при наблюдении ARP для адреса IP, который считается неиспользуемым, прокси возвращает свой MAC-адрес. Отравление ARP (poisoning) и фальшивые анонсы могут нарушить (например, DoS) работу этого и других прокси-методов.

10. Взаимодействие с IANA

Этот документ не требует действий IANA.

11. Литература

[arpsponge] Wessel, M. and N. Sijm, "Effects of IPv4 and IPv6 address resolution on AMS-IX and the ARP Sponge", July 2009, <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.182.4692>.

[bridge-mc-2-uc] "bridge: multicast to unicast", commit 6db6f0e, January 2017, <https://github.com/torvalds/linux/commit/6db6f0e>.

[CAB] "limit multicast buffer hardware queue depth", commit 2687951, June 2013, <https://patchwork.kernel.org/patch/2687951/>.

[Deri-2010] Deri, L. and J. Gasparakis, "10 Gbit Hardware Packet Filtering Using Commodity Network Adapters", RIPE 61, November 2010, <http://ripe61.ripe.net/presentations/138-Deri_RIPE_61.pdf>.

[dot11] IEEE, "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 (includes 802.11v amendment)", DOI 10.1109/IEEESTD.2021.9363693, IEEE Std 802.11-2020, December 2020, <https://standards.ieee.org/standard/802_11-2020.html>.

[dot11-proxyarp] Hiertz, G., Mestanov, F., and B. Hart, "Proxy ARP in 802.11ax", September 2015, <https://mentor.ieee.org/802.11/dcn/15/11-15-1015-01-00ax-proxy-arp-in-802-11ax.pptx>.

[dot11aa] IEEE, "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 Amendment 2: MAC Enhancements for Robust Audio Video Streaming", DOI 10.1109/IEEESTD.2012.6204193, IEEE Std 802.11aa-2012, March 2012, <https://standards.ieee.org/standard/802_11aa-2012.html>.

[group_key] "Subject: Why do some WiFi routers block multicast packets going from wired to wireless?", message to the Super User Q & A community, January 2017, <https://superuser.com/questions/730288/why-do-some-wifi-routers-block-multicast-packets-going-from-wired-to-wireless>.

[IEEE802.1ak] IEEE, "Local and Metropolitan Area Networks Virtual Bridged Local Area Networks - Amendment 07: Multiple Registration Protocol", DOI 10.1109/IEEESTD.2007.380667, IEEE Std 802.1ak-2007, June 2007, <https://www.ieee802.org/1/pages/802.1ak.html>.

[ietf_802-11] Stanley, D., "IEEE 802.11 multicast capabilities", November 2015, <https://mentor.ieee.org/802.11/dcn/15/11-15-1261-03-0arc-multicast-performance-optimization-features-overview-for-ietf-nov-2015.ppt>.

[mc-prob-stmt] Abrahamsson, M. and A. Stephens, "Multicast on 802.11", 2013, <https://www.iab.org/wp-content/IAB-uploads/2013/01/multicast-problem-statement.pptx>.

[mc-props] Stephens, A., "IEEE 802.11 multicast properties", September 2015, <https://mentor.ieee.org/802.11/dcn/15/11-15-1161-02-0arc-802-11-multicast-properties.ppt>.

[Oliva2013] de la Oliva, A., Serrano, P., Salvador, P., and A. Banchs, "Performance evaluation of the IEEE 802.11aa multicast mechanisms for video streaming", 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), pp. 1-9, DOI 10.1109/WoWMoM.2013.6583394, June 2013, <https://doi.org/10.1109/WoWMoM.2013.6583394>.

[RFC0826] Plummer, D., "An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, DOI 10.17487/RFC0826, November 1982, <https://www.rfc-editor.org/info/rfc826>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.

[RFC4286] Haberman, B. and J. Martin, "Multicast Router Discovery", RFC 4286, DOI 10.17487/RFC4286, December 2005, <https://www.rfc-editor.org/info/rfc4286>.

[RFC4541] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, DOI 10.17487/RFC4541, May 2006, <https://www.rfc-editor.org/info/rfc4541>.

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, DOI 10.17487/RFC4601, August 2006, <https://www.rfc-editor.org/info/rfc4601>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

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

[RFC5757] Schmidt, T., Waehlisch, M., and G. Fairhurst, "Multicast Mobility in Mobile IP Version 6 (MIPv6): Problem Statement and Brief Survey", RFC 5757, DOI 10.17487/RFC5757, February 2010, <https://www.rfc-editor.org/info/rfc5757>.

[RFC5796] Atwood, W., Islam, S., and M. Siami, "Authentication and Confidentiality in Protocol Independent Multicast Sparse Mode (PIM-SM) Link-Local Messages", RFC 5796, DOI 10.17487/RFC5796, March 2010, <https://www.rfc-editor.org/info/rfc5796>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/info/rfc6282>.

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

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

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>.

[RFC6970] Boucadair, M., Penno, R., and D. Wing, "Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Function (IGD-PCP IWF)", RFC 6970, DOI 10.17487/RFC6970, July 2013, <https://www.rfc-editor.org/info/rfc6970>.

[RFC7450] Bumgardner, G., "Automatic Multicast Tunneling", RFC 7450, DOI 10.17487/RFC7450, February 2015, <https://www.rfc-editor.org/info/rfc7450>.

[RFC7761] Fenner, B., Handley, M., Holbrook, H., Kouvelas, I., Parekh, R., Zhang, Z., and L. Zheng, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", STD 83, RFC 7761, DOI 10.17487/RFC7761, March 2016, <https://www.rfc-editor.org/info/rfc7761>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <https://www.rfc-editor.org/info/rfc8505>.

[RFC8777] Holland, J., "DNS Reverse IP Automatic Multicast Tunneling (AMT) Discovery", RFC 8777, DOI 10.17487/RFC8777, April 2020, <https://www.rfc-editor.org/info/rfc8777>.

[RFC8929] Thubert, P., Ed., Perkins, C.E., and E. Levy-Abegnoli, "IPv6 Backbone Router", RFC 8929, DOI 10.17487/RFC8929, November 2020, <https://www.rfc-editor.org/info/rfc8929>.

[RFC9030] Thubert, P., Ed., "An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH)", RFC 9030, DOI 10.17487/RFC9030, May 2021, <https://www.rfc-editor.org/info/rfc9030>.

[Tramarin2017] Tramarin, F., Vitturi, S., and M. Luvisotto, "IEEE 802.11n for Distributed Measurement Systems", 2017 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), pp. 1-6, May 2017.

[uli] Kinney, P., "LLC Proposal for 802.15.4", September 2015, <https://mentor.ieee.org/802.15/dcn/15/15-15-0521-01-wng0-llc-proposal-for-802-15-4.pptx>.

[v2011] IEEE, "Information technology -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: IEEE 802.11 Wireless Network Management", DOI 10.1109/IEEESTD.2011.5716530, IEEE Std 802.11v-2011, February 2011, <https://ieeexplore.ieee.org/document/5716530>.

Благодарности

Этот документ выиграл в результате обсуждения с перечисленными в алфавитном порядке людьми: Mikael Abrahamsson, Bill Atwood, Stuart Cheshire, Donald Eastlake 3rd, Toerless Eckert, Jake Holland, Joel Jaeggli, Jan Komissar, David Lamparter, Morten Pedersen, Pascal Thubert, Jeffrey (Zhaohui) Zhang.

Адреса авторов

Charles E. Perkins
Lupin Lodge
Phone: +1 408 255 9223
Email: charliep@lupinlodge.com

Mike McBride
Futurewei Technologies Inc.
2330 Central Expressway
Santa Clara, CA 95055
United States of America
Email: michael.mcbride@futurewei.com

Dorothy Stanley
Hewlett Packard Enterprise
6280 America Center Dr.
San Jose, CA 95002
United States of America
Phone: +1 630 363 1389
Email: dorothy.stanley@hpe.com

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
United States of America
Email: warren@kumari.net

Juan Carlos Zúñiga
SIGFOX
Montreal
Canada
Email: j.c.zuniga@ieee.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru