Network Working Group
Request for Comments: 3927
Category: Standards Track

S. Cheshire
Apple Computer
B. Aboba
Microsoft Corporation
E. Guttman
Sun Microsystems

May 2005

**Динамическая настройка адреса IPv4 Link-Local**

**Dynamic Configuration of IPv4 Link-Local Addresses**

**Статус документа**

Этот документ задаёт проект стандартного протокола Internet для сообщества Internet и служит приглашение к дискуссии в целях развития и совершенствования протокола. Текущий статус стандартизации протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Распространение документа не ограничивается.

**Авторские права**



**Аннотация**

Для участия в работе распределенных сетей IP хосту нужны адреса IP на его интерфейсах, заданные вручную или автоматически с помощью механизмов типа сервера DHCP[1]. К сожалению данные для настройки адресов доступны не всегда. Поэтому для хостов будет преимуществом возможность использовать хотя бы часть сетевых функций IP при отсутствии настроенного адреса. Этот документ описывает для хостов способ автоматической настройка для интерфейсов адресов IPv4 из префикса 169.254/16, которые подходят для коммуникаций с другими устройствами, подключёнными к тому же физическому (или логическому) каналу.

Адреса IPv4 Link-Local не подходят для коммуникаций с устройствами, которые не подключены к тому же физическому (или логическому) каналу, и применяются лишь в тех случаях, когда стабильные, маршрутизируемые адреса не доступны (например, специализированные или изолированные сети. Данный документ не рекомендует использовать на одном интерфейсе адрес IPv4 Link-Local и маршрутизируемый адрес одновременно.

# Оглавление



[1]Dynamic Host Configuration Protocol - протокол динамической настройки конфигурации хоста.

# *1. Введение*

По мере роста популярности протокола Internet становится все более ценной возможность использования привычных инструментов IP типа протокола FTP не только для глобальных, но и для локальных коммуникаций. Например, два человека с переносными компьютерами, поддерживающими беспроводные соединения IEEE 802.11 [802.11], могут пожелать обмениваться файлами через такое соединение. Для таких людей желательно обеспечить возможность использования программ IP без неудобств, связанных с ручной настройкой статических адресов IP или их получением от сервера DHCP [RFC2131].

В этом документе описан метод, с помощью которого хост может автоматически настроить для своего интерфейса адрес IPv4 из префикса 169.254/16, который будет пригоден для локальных коммуникаций (Link-Local) через этот интерфейс. Это особенно полезно в средах, где нет других механизмов настройки конфигурации. Префикс IPv4 169.254/16 зарегистрирован агентством IANA специально для таких целей. Выделение адреса IPv6 Link-Local описано в документе IPv6 Stateless Address Autoconfiguration [RFC2462].

Локальные коммуникации с использованием адресов IPv4 Link-Local подходят только для связи между устройствами, подключёнными к одному физическому (или логическому) каналу. Адреса IPv4 Link-Local не пригодны для связи с устройствами, которые не подключены непосредственно к одному физическому (или логическому) каналу.

Microsoft Windows 98 (и более поздние версии) и Mac OS 8.5 (и более поздние версии) уже поддерживают такую возможность. Данный документ стандартизует использование локальных (Link-Local) адресов IPv4 и описывает правила трактовки таких адресов хостами и маршрутизаторами. В частности, описано поведение маршрутизаторов при получении ими пакетов с адресами IPv4 Link-Local в поле отправителя или получателя. Для хостов рассматривается заявление и защита локальных адресов, поддержка локального и маршрутизируемого адреса IPv4 на одном интерфейсе и вопросы связанные с множеством интерфейсов на хосте.

## 1.1. Уровни требований

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 [RFC2119].

## 1.2. Терминология

Этот документ описывает адресацию Link-Local для коммуникаций IPv4 между двумя хостами на одном канале. Множество хостов относятся к одному каналу при выполнении двух условий:

- если хост A передаёт хосту B из того же множества пакет с использованием индивидуальной, групповой или широковещательной адресации, данные (payload) канального уровня сохраняются неизменными;
- широковещательный пакет, переданный через канал любым хостом из данного множества, может быть принят каждым хостом из этого множества.

Заголовок канального уровня может быть изменён (например, в Token Ring Source Routing [802.5]), но данные (payload) канального уровня не меняются. В частности, если любое пересылающее пакет устройство меняет какую-либо часть заголовка IP или данных IP, пакет больше не считается относящимся к тому же каналу. Это означает, что пакет может проходить через повторители, мосты, концентраторы или коммутаторы, оставаясь на том же канале в понимании данного документа, но не может проходить в этом смысле через устройства типа маршрутизаторов IP, которые уменьшают значение TTL или как-то иначе меняют заголовок IP.

В этом документе термин «маршрутизируемый адрес» (routable address) означает все действующие индивидуальные адреса IPv4, не входящие в префикс 169.254/16, которые могут пересылаться маршрутизаторами. Сюда входят все публичные адреса IP и приватные адреса типа 10/8 [RFC1918], но не адреса петлевых интерфейсов типа 127.0.0.1.

Всякий раз, когда в этом документе используется термин «хост» при описании использования адресов IPv4 Link-Local, это относится также к маршрутизаторам, которые являются источниками или предполагаемыми получателями пакетов, содержащих адрес IPv4 Link-Local в поле отправителя или получателя.

В тех случаях, когда в документе используется термин «IP-адрес отправителя» или «IP-адрес получателя» в контексте пакета ARP, это относится к полям пакета ARP, указанным в спецификации ARP [RFC826] как ar$spa (протокольный адрес отправителя) и ar$tpa (протокольный адрес получателя), соответственно. Для описанных в этом документе применений ARP каждое из этих полей всегда содержит адрес IP.

В этом документе термин «проба ARP» относится к пакетам ARP Request, передаваемым по широковещательному адресу в локальный канал с нулевым значением IP-адреса отправителя. Поле аппаратного адреса отправителя **должно** содержать аппаратный адрес передавшего пакет интерфейса. Поле аппаратного адреса получателя игнорируется и его **следует** заполнять нулями. В поле IP-адреса получателя **должен** указываться проверяемый адрес.

Термин «анонсы ARP» в этом документе относится к пакетам ARP Request, передаваемым по широковещательному адресу в локальный канал, аналогично описанным выше пробам ARP, за исключением того, что в полях IP-адресов отправителя и получателя указывается анонсируемый адрес.

Константы указываются заглавными буквами, их значения приведены в разделе 9.

## 1.3. Применимость

Эта спецификация применима для всех ЛВС IEEE 802 [802], включая Ethernet [802.3], Token-Ring [802.5] и беспроводные ЛВС IEEE 802.11 [802.11], а также для других технологий канального уровня, которые работают со скоростями не менее 1 Мбит/с, имеют время кругового обхода не более 1 секунды и поддерживают ARP [RFC826]. Термин IEEE 802 в документе относится ко всем таким сетевым технологиям.

Технологии канального уровня с поддержкой ARP, работающие со скоростями ниже 1 Мбит/с или временем кругового обхода больше 1 секунды, могут потребовать подбора значений для перечисленных ниже параметров.

(a) Число проб ARP и интервалы между ними (см. PROBE_NUM, PROBE_MIN и PROBE_MAX в параграфе 2.2.1).

(b) Число анонсов ARP и интервалы между ними (ANNOUNCE_NUM и ANNOUNCE_INTERVAL в параграфе 2.4).

(c) Максимальная скорость, с которой могут выполняться попытки объявления адреса (см. RATE_LIMIT_INTERVAL и MAX_CONFLICTS в параграфе 2.2.1).

(d) Граница интервала при конфликте между ARP, ниже которой хост **должен** изменить конфигурацию вместо попытки защиты своего адреса (см. DEFEND_INTERVAL в параграфе 2.5).

Технологии канального уровня, не поддерживающие ARP, могут использовать другие методы определения занятости адресов IP. Однако применение механизмов объявления и защиты (claim-and-defend) адресов для таких сетей выходит за рамки этого документа.

Данная спецификация предназначена для использования в небольших специализированных (ad hoc) сетях, где один канал используется для соединения небольшого числа хостов. Хотя в принципе доступны 65024 адресов IPv4 Link-Local, попытки использовать все эти адреса на локальном канале обречены на высокую вероятность конфликтов и потребуют от хостов затраты значительного времени на поиск доступного адреса.

Сетевые операторы, имеющие более 1300 хостов на одном канале, могут рассматривать вопрос о разбиении этого канала на две или более подсети. Хост, подключающийся к каналу, где уже имеется 1300 хостов, при выборе адреса IPv4 Link-Local имеет вероятность с первой попытки найти свободный локальный адрес около 98%, при двух попытках вероятность возрастает до 99,96%. Вероятность того, что потребуется более 10 попыток, составляет около $10^{-17}$.

## 1.4. Протокол прикладного уровня

Локальные адреса IPv4 и их динамическая настройка оказывают существенное влияние на использующие эти адреса приложения (см. раздел 6). Многие приложения предполагают, что адреса взаимодействующих с ними партнёров являются маршрутизируемыми, сравнительно редко меняющимися и уникальными. Эти допущения неверны для адресов IPv4 Link-Local или смешанного использования локальных и маршрутизируемых адресов IPv4. Поэтому некоторые приложения могут работать корректно в среде IPv4 Link-Local или смешанной среде с локальными и маршрутизируемыми адресами, а для других могут потребоваться изменения или будет теряться часть функций. В некоторых случаях приложения невозможно изменить для работы в таких условиях.

Поэтому локальные адреса IPv4 следует применять лишь в тех случаях, когда стабильные маршрутизируемые адреса не доступны (например, в специализированных или изолированных сетях) или в контролируемых ситуациях, когда отмеченные ограничения и их воздействие на приложения понятны и приемлемы. Этот документ рекомендует не использовать локальные и маршрутизируемые адреса IPv4 на одном интерфейсе.

Использование адресов IPv4 Link-Local для коммуникаций, выходящих за пределы локального канала, с высокой вероятностью приведёт к возникновению проблем. Это может произойти в любом приложении, использующем вложенные адреса IPv4 Link-Local при коммуникациях с хостами, не подключёнными к тому же каналу. Примеры приложений с вложенными адресами включают IPsec, Kerberos 4/5, FTP, RSVP, SMTP, SIP, X-Windows/Xterm/Telnet, Real Audio, H.323 и SNMP [RFC3027].

Для предотвращения использования локальных адресов IPv4 в коммуникациях, выходящих за пределы локального канала, рекомендуются перечисленные ниже меры.

a. Адреса IPv4 Link-Local **недопустимо** указывать в DNS[1]. Отображение адресов IPv4 на имена хостов происходит в форме запросов DNS вида x.x.x.x.in-addr.arpa. При использовании локальных адресов, которые имеют смысл только на данном канале, недопустима передача таких запросов DNS за пределы локального соединения. Клиентам DNS **недопустимо** передавать запросы DNS для имён, относящихся к домену «254.169.in-addr.arpa.». Рекурсивные серверы DNS, получая запросы от некорректно работающих клиентов для имён из домена «254.169.in-addr.arpa.», **должны** по умолчанию возвращать RCODE 3, правомочно заявляя об отсутствии таких имён в DNS.

b. В приложениях следует использовать имена, преобразуемые в глобальном масштабе в маршрутизируемые адреса, когда такие имена доступны. Имена, отображающиеся только на локальные адреса (используемые протоколами типа Link Local Multicast Name Resolution [LLMNR]), **недопустимо** использовать во внешних коммуникациях. Адреса IPv4 и имена, которые могут отображаться только на локальный канал, **не следует** пересылать за пределы этого канала. Адреса IPv4 Link-Local **следует** передавать лишь при использовании локального адреса для получателя или отправителя. Это должно предотвратить выход локальных адресов за пределы контекста их применимости.

c. Если имена, преобразуемые в глобально маршрутизируемые адреса, не доступны, но имеются адреса с глобальной маршрутизацией, их следует применять вместо адресов IPv4 Link-Local .

[1]Domain Name System - система доменных имён.

## 1.5. Вопросы автоматической настройки

Реализации автоматической настройки адресов IPv4 Link-Local **должны** предполагать конфликты адресов и **должны** быть готовы к аккуратному выбору другого адреса в таких случаях, как описано в разделе 2. Требование детектирования и обработки конфликтов применяется в течение всего срока использования хостом локального адреса 169.254/16, а не только при начальной настройке интерфейса. Например, конфликт адресов может возникнуть после завершения загрузки хоста, если к этой сети подключится другой хост, как описано в разделе 4.

## 1.6. Запрет других применений

Отметим, что адреса из префикса 169.254/16 **не следует** задавать вручную или с помощью сервера DHCP, поскольку это может приводить к использованию хостом такого адреса без выполнения правил, связанных с обнаружением дубликатов и автоматической настройки, применяемых для этого префикса. Хотя спецификация DHCP [RFC2131] указывает, что клиенту DHCP **следует** проверять полученный вновь адрес с помощью ARP, это не является обязательным. В спецификации указано, что серверу DHCP перед выделением адреса **следует** проверять его с помощью запроса ICMP Echo, но это тоже не обязательно и даже в том случае, когда сервер выполняет такую проверку её результат не будет иметь смысла, если сервер DHCP не подключён напрямую к локальному каналу, поскольку адреса IPv4 Link-Local не маршрутизируются.

Администраторам, желающим настроить свои локальные адреса (вручную, с помощью сервера DHCP или иного механизма, не описанного здесь), следует использовать один из приватных префиксов [RFC1918], а не 169.254/16.

## 1.7. Множество интерфейсов

Дополнительные вопросы возникают для хостов с несколькими активными интерфейсами, из которых часть или все используют адреса IPv4 Link-Local. Эти вопросы рассматриваются в разделе 3.

## 1.8. Взаимодействие с маршрутизируемыми адресами

Бывают случаи, когда устройствам с адресами Link-Local нужно взаимодействовать с устройством, имеющим маршрутизируемый адрес, на том же физическом канале. Правила таких коммуникаций рассмотрены в параграфе 2.6.

Это позволяет, например, переносному компьютеру, имеющему только маршрутизируемый адрес для взаимодействия с web-серверами по всему миру, в то же время печатать документы на локальном принтере с адресом IPv4 Link-Local.

## 1.9. Когда настраивают адрес IPv4 Link-Local

Наличие на интерфейсе адресов с разными областями действия без адекватного способа определить условия использования каждого из адресов усложняют работу приложений и путают пользователя. Хост а адресом, подключенный к каналу, может взаимодействовать со всеми хостами этого канала независимо от использования маршрутизируемых или локальных адресов. По этой причине хосту **не следует** использовать на одном интерфейсе маршрутизируемые и локальные адреса. Термин «пригодный для работы адрес» (operable address) используется для обозначения адреса, обеспечивающего коммуникации в текущем сетевом контексте (см. ниже). Когда доступен пригодный для работы маршрутизируемый адрес, хосту **не следует** назначать для того же интерфейса ещё и адрес IPv4 Link-Local. Однако в процессе перехода от маршрутизируемого адреса к локальному (и наоборот) оба адреса могут использоваться одновременно при соблюдении приведённых ниже правил.

1. Назначение адреса IPv4 Link-Local интерфейсу определяется лишь состоянием интерфейса и не зависит от каких-либо других протоколов типа DHCP. Хосту **недопустимо** менять своё поведение и использовать другие протоколы (например, DHCP), поскольку он имеет адрес IPv4 Link-Local на своём интерфейсе.
2. Если хост обнаружил, что интерфейс, которому был ранее назначен адрес IPv4 Link-Local, имеет доступный маршрутизируемый адрес, хост **должен** использовать маршрутизируемый адрес при инициировании новых коммуникаций и **должен** прекратить анонсирование доступности адреса IPv4 Link-Local с помощью любых механизмов. Хосту **следует** продолжать использование адреса IPv4 Link-Local для организованных ранее коммуникаций и он **может** продолжать восприятие новых коммуникаций по адресу IPv4 Link-Local. Способы получения на интерфейсе маршрутизируемого адреса включают:
   - ручную настройку;
   - назначение сервером DHCP;
   - перемещение (роуминг) хоста в сеть, где назначенный ранее адрес пригоден для работы.
3. Если хост обнаруживает, что на интерфейсе больше нет доступного маршрутизируемого адреса, он **может** определить подходящий адрес IPv4 Link-Local (см. раздел 2) и назначить его интерфейсу. Причины утраты интерфейсом маршрутизируемого адреса включают:
   - удаление адреса вручную;
   - завершение срока аренды адреса в DHCP;
   - перемещение (роуминг) хоста в сеть, где маршрутизируемый адрес больше не пригоден для работы.

Определение системой пригодности адреса для работы не является чётким и изменения сетевого контекста (например, смена маршрутизатора) могут влиять на пригодность адреса. В частности, перемещение хоста в другую сеть с большой вероятностью (но не обязательно) меняет состояние пригодности настроенного адреса, но определить такое перемещение не всегда просто.

В работе Detection of Network Attachment (DNA) in IPv4 [DNAv4] приведено дополнительное рассмотрение вопросов назначения адресов и определения их пригодности для использования.

# 2. Выбор адреса, защита и доставка

В следующих параграфах описан алгоритм выбора адресов IPv4 Link-Local, их защиты и доставки пакетов IPv4 с локальными адресами.

Хосты Windows и Mac OS уже поддерживают автоматическую настройку адресов Link-Local IPv4 в соответствии с описанными в этом разделе правилами. Однако при обнаружении каких-либо проблем взаимодействия стандартное решение определяет этот документ, а не та или иная реализация.

## 2.1. Выбор локального адреса

Хост, желающий настроить адрес IPv4 Link-Local, выбирает его из диапазона 169.254.1.0 - 169.254.254.255 (включительно) с использованием генератора псевдослучайных чисел с однородным распределением. Префикс IPv4 169.254/16 зарегистрирован агентством IANA специально для таких целей. Первые и последние 256 адресов префикса 169.254/16 зарезервированы для использования в будущем и их **недопустимо** выбирать для использования хостом с помощью этого механизма динамической настройки.

Алгоритм генерации псевдослучайных значений **должен** выбираться так, чтобы разные хосты не генерировали одинаковые последовательности чисел. Если хост имеет доступ к стабильной информации, которая различается для каждого хоста (например, адрес IEEE 802 MAC), генератору псевдослучайных чисел **следует** использовать такую информацию в качестве основы для создания «затравки» (seed). Это означает, что даже при использовании лишь этого источника «затравочной» информации хост обычно будет выбирать один и тот же адрес IPv4 Link-Local при каждой загрузке, что может быть удобно для отлаживания и решения других операционных задач. Инициализация генератора псевдослучайных чисел с использованием часов или иного источника информации, который даёт (или может давать) одинаковые значения на каждом хосте, **не** подходит для этой цели, поскольку группа хостов при одновременном включении будет генерировать одинаковые последовательности, что приведёт к бесконечной последовательности конфликтов адресов.

Хосты, оборудованные стабильным хранилищем, **могут** записывать выбранный адрес IPv4 для каждого интерфейса. При загрузке хосту с записанным прежним адресом **следует** использовать этот адрес в качестве первого кандидата для пробы. Это повышает стабильность адресации. Например, если группа хостов выключается на ночь и включается на следующее утро, они будут использовать прежние адреса вместо выбора новых и разрешения возникающих при этом конфликтов.

## 2.2. Объявление локального адреса

После выбора адреса IPv4 Link-Local хост **должен** убедиться, что этот адрес не занят, прежде чем использовать его. При переходе сетевого интерфейса из неактивного состояния в активное хост не знает об уже используемых на канале локальных адресах IPv4, поскольку точка подключения могла измениться или интерфейс мог быть не активен в момент объявления конфликтующего адреса.

Когда хост сразу же начинает использовать адрес IPv4 Link-Local, который уже занят другим хостом, это будет нарушать работу того хоста. Поскольку точка подключения хоста могла измениться и в новой сети может быть доступен маршрутизируемый адрес, поэтому хост не может предполагать, что адрес IPv4 Link-Local является предпочтительным.

Перед использованием адреса IPv4 Link-Local (например, в поле отправителя пакета IPv4 или в поле Sender IPv4 пакета ARP) хост **должен** выполнить описанную ниже проверку для обеспечения уверенности в том, что использование адреса IPv4 Link-Local не вызовет проблем.

Примерами событий, приводящих к переходу интерфейса в активное состояние, могут служить:

перезагрузка (включение) или выход из состояния «сна» (если сетевой интерфейс не был активен во время «сна») с активизацией сетевого интерфейса;

изменение аппаратного состояния IEEE 802 (подходящее для типа среды и механизма защиты), показывающее, что интерфейс активизируется;

организация связи с беспроводной базовой станцией или сетью ad hoc.

Хосту недопустимо выполнять эту проверку периодически, как само собой разумеющуюся. Это приведёт к напрасному расходу пропускной способности сети и не требуется, поскольку хосты могут пассивно определять конфликты адресов, как описано в параграфе 2.5.

### *2.2.1. Детали проверки*

На канальном уровне типа IEEE 802, который поддерживает ARP, обнаружение конфликтов выполняется с помощью проб ARP. Для канальных технологий без поддержки ARP могут использоваться другие механизмы проверки занятости конкретного адреса IPv4. Однако применение в таких сетях механизма объявления и защиты адреса выходит за рамки этого документа.

Хост пытается проверить занятость адреса путём отправки широковещательного запроса ARP для данного адреса. Клиент **должен** заполнить поле sender hardware address в запросе ARP, указав в нем аппаратный адрес интерфейса, через который передаётся пакет. Поле sender IP address **должно** быть заполнено нулями, чтобы избежать загрязнения кэшей ARP на других хостах того же канала в тех случаях, когда адрес уже занят другим хостом. Поле target hardware address игнорируется и его **следует** заполнять нулями. В поле target IP address **должен** быть указан проверяемый адрес. Созданный таким образом запрос ARP с нулём в поле sender IP address называется пробой ARP (ARP Probe).

При готовности хоста к началу проверки ему следует сначала выждать случайный интервал времени из диапазона 0 - PROBE_WAIT секунд с равномерным распределением, затем передать PROBE_NUM пробных пакетов со случайными интервалами из диапазона PROBE_MIN - PROBE_MAX. Если с момента начала проверки до истечения ANNOUNCE_WAIT секунд после финальной пробы хост получает какой-либо пакет ARP (Request или Reply) на интерфейсе, использованном для отправки проб, где sender IP address указывает проверяемый адрес, хост **должен** считать, что этот адрес уже используется другим хостом, **должен** выбрать новый псевдослучайный адрес и повторить

процедуру проверки. В дополнение к этому при получении хостом любого пакета ARP, в котором target IP address указывает проверяемый адрес, а sender hardware address не является аппаратным адресом настраиваемого интерфейса хоста, этот хост **должен** считать, что возник конфликт адресов и выбирать новый адрес, как описано выше. Такое может происходить при одновременной попытке двух (и более) хостов выбрать один адрес IPv4 Link-Local.

Хосту следует поддерживать счётчик адресных конфликтов, с которыми он столкнулся в процессе настройки адреса, и в случае превышения порога MAX_CONFLICTS хост **должен** ограничить скорость проб для новых адресов значением не больше одного адреса в течение RATE_LIMIT_INTERVAL. Это позволяет избежать катастрофических «штормов» ARP в случаях патологических отказов, когда злонамеренный хост отвечает на все пробы ARP, вынуждая легитимные хосты входить в бесконечный цикл проверки занятости адресов.

Если по истечении ANNOUNCE_WAIT секунд после отправки последнего пакета ARP Probe хост не получил пакета ARP Reply или ARP Probe, он может заявлять выбранный адрес IPv4 Link-Local.

## 2.3. Сокращённые тайм-ауты

Могут появляться сетевые технологии, для которых подойдут более короткие задержки, нежели задано в этом документе. Для таких технологий могут быть подготовлены соответствующие публикации IETF в другими рекомендуемыми значениями PROBE_WAIT, PROBE_NUM, PROBE_MIN и PROBE_MAX.

## 2.4. Анонсирование адреса

Проверив уникальность выбранного адреса, хост **должен** анонсировать этот адрес в ANNOUNCE_NUM широковещательных пакетов ARP с интервалом ANNOUNCE_INTERVAL секунд. Анонс ARP идентичен описанному выше пакету ARP Probe за исключением того, что в полях адресов IP устанавливается выбранный хостом адрес IPv4. Эти анонсы ARP позволяют убедиться в том, что у других хостов на канале не осталось устаревших записей в кэшах ARP от другого хоста, который ранее использовал этот адрес.

## 2.5. Обнаружение конфликтов и защита

Детектирование адресных конфликтов не ограничивается описанной выше фазой выбора адреса, когда хост передаёт пробы ARP. Обнаружение конфликтов непрерывный процесс, который работает в течение всего срока использования адреса IPv4 Link-Local. В любой момент получение на интерфейсе хоста пакета ARP (запрос или отклик), в котором sender IP address указывает IP-адрес хоста, установленный на этом интерфейсе, а sender hardware address не совпадает с аппаратным адресом этого интерфейса, говорит о конфликте адресов.

Хост **должен** отвечать на конфликтующие пакеты ARP в соответствии с пунктом (a) или (b).

(a) При получении конфликтующего пакета ARP хост **может** незамедлительно настроить новый адрес IPv4 Link-Local, как описано выше, или перейти к п. (b).

(b) Если у хоста имеются активные соединения TCP или иные причины сохранять прежний адрес IPv4, а в течение последних DEFEND_INTERVAL секунд не было других конфликтующих пакетов ARP, хост **может** попытаться защитить свой адрес, записав время приёма конфликтующего пакета ARP и передав после этого один анонс ARP, указывающий его адрес IP и аппаратный адрес в качестве адресов отправителя ARP. После этого хост может продолжать использование адреса без каких-либо дополнительных действий. Однако, если это не первый конфликтующий пакет ARP, который получил хост, и записанное время предыдущего конфликтующего пакета ARP попадает в интервал DEFEND_INTERVAL секунд, хост **должен** немедленно прекратить использование адреса и выбрать себе новый адрес IPv4 Link-Local, как описано выше. Это требуется для того, чтобы два хоста не попали в бесконечный цикл попыток защиты одного адреса.

Хост **должен** ответить на конфликтующие пакеты ARP в соответствии с п. (a) или (b). Игнорирование конфликтующих пакетов ARP **недопустимо**.

Вынужденная смена адресов может нарушать работу, приводя к разрыву соединений TCP. Однако предполагается, что такие ситуации будут возникать редко, а непреднамеренное дублирование адресов в любом случае приведёт к нарушению коммуникаций. Невозможно использование двумя хостами сети одного адреса IP без нарушения работы.

Перед отказом от адреса в результате конфликта хостам **следует** предпринять попытку активного сброса соединений, использующих этот адрес. Это смягчит некоторые угрозы безопасности, вызываемые перенастройкой адресов, как описано в разделе 5.

Настройка нового адреса сразу при обнаружении конфликта является лучшим способом быстро восстановить нужные коммуникации. Описанный выше механизм использует широковещательную передачу единственного анонса ARP для защиты адреса, что значительно смягчает проблему, помогая увеличить шансы сохранения адреса одним из конфликтующих хостов.

Все пакеты ARP (отклики и запросы), содержащие адрес Link-Local в качестве IP-адреса отправителя, **должны** передаваться с использованием широковещания канального уровня, а не индивидуальной адресации. Это помогает своевременно обнаруживать дубликаты адресов. Пример, показывающий, как это помогает, приведён в разделе 4.

## 2.6. Использование адресов и правила пересылки

Для хостов, соответствующих этой спецификации, имеются дополнительные правила, которые следует выполнять независимо от использования на хосте адресов IPv4 Link-Local.

### *2.6.1. Использование адреса отправителя*

Поскольку хост может иметь адрес IPv4 Link-Local в дополнение к адресам, заданным другими способами (например, вручную или от сервера DHCP), такой хост может выбирать адрес отправителя при отправке пакета или организации соединения TCP.

При одновременной доступности IPv4 Link-Local и маршрутизируемого адреса на одном интерфейсе в качестве адреса отправителя следует предпочитать маршрутизируемый адрес для новых коммуникаций, но пакеты, отправленные с адреса IPv4 Link-Local также будут доставляться. Адрес IPv4 Link-Local можно продолжать использовать в качестве адреса отправителя, если переход на предпочтительный адрес будет нарушать коммуникации в результате требований протокола вышележащего уровня (например, для имеющихся соединений TCP). Дополнительная информация приведена в параграфе 1.7.

Многодомным хостам приходится выбирать выходной интерфейс независимо от того, используется ли для получателя адрес IPv4 Link-Local. Детали этого выбора выходят за рамки документа. После выбора интерфейса многодомному хосту следует отправлять пакеты с адресами Link-Local в соответствии с данной спецификацией, как будто выбранный интерфейс является единственным. Дополнительное рассмотрение многодомных хостов приведено в разделе 3.

### *2.6.2. Правила пересылки*

Независимо от используемого интерфейса при отправке пакетов адресату из префикса 169.254/16 (кроме широковещательного адреса 169.254.255.255 для Link-Local) отправитель **должен** передать запрос ARP для адреса получателя и после этого отправлять пакеты напрямую адресату в том же физическом канале. Это **должно** выполняться при использовании на интерфейса как адреса Link-Local, так и маршрутизируемого адреса IPv4.

Во многих реализациях сетевого стека обеспечение такой функциональности столь же просто, как добавление маршрута, указывающего, что сеть 169.254/16 подключена напрямую. Однако такой подход не будет работать на маршрутизаторах и многодомных хостах (см. раздел 3).

Хосту **недопустимо** передавать пакеты с адресом получателя IPv4 Link-Local какому-либо маршрутизатору для пересылки.

Если адресом получателя является индивидуальный адрес не из префикса 169.254/16, хосту **следует** указать в качестве адреса отправителя подходящий маршрутизируемый адрес IPv4 (при наличии). Если по какой-либо причине хост решит отправлять пакет с адреса IPv4 Link-Local (например, на интерфейсе нет маршрутизируемых адресов), он **должен** передать запрос ARP для адреса получателя и затем отправлять пакет с адреса IPv4 Link-Local по маршрутизируемому адресу IPv4 напрямую получателю, подключённому к тому же физическому каналу. Хосту **недопустимо** отправлять пакет маршрутизатору для пересылки.

В случаях, когда устройство имеет единственный интерфейс и только адрес Link-Local IPv4, это требование можно перефразировать как «ARP для всех». Во многих сетевых стеках поведение «ARP for everything» может быть реализовано столь же просто, как отсутствие в конфигурации основного маршрутизатора, указание в качестве адреса основного маршрутизатора 0.0.0.0 или своего адреса Link-Local IPv4. Поведение многодомных хостов рассмотрено в разделе 3.

## 2.7. Локальные адреса не пересылаются

Для приложений, передающих пакеты с адреса IPv4 Link-Local разумно по умолчанию устанавливать IPv4 TTL = 1. Это подходит не для всех случаев, поскольку некоторые приложения могут требовать установки других значений IPv4 TTL.

Пакеты IPv4, в которых адрес отправителя и/или получателя относится к префиксу 169.254/16, **недопустимо** передавать какому-либо маршрутизатору для пересылки, а получившему такой пакет сетевому устройству **недопустимо** пересылать пакет независимо от значения TTL в заголовке IPv4. Аналогично, маршрутизатору или другому хосту **недопустимо** без разбора отвечать на все запросы ARP для адресов из префикса 169.254/16. Естественно, маршрутизатор может отвечать на запросы ARP для одного или нескольких адресов IPv4 Link-Local, объявленных им для собственного использования в соответствии с описанным в этом документе протоколом «объявить и защитить».

Эти ограничения применимы и к групповым пакетам. Пакеты IPv4 с адресом отправителя Link-Local **недопустимо** пересылать за пределы локального канала, даже если в них указан групповой адрес получателя.

## 2.8. Пакеты Link-Local являются локальными

Правило «без пересылки» означает, что хосты считают все адреса 169.254/16 напрямую подключены к тому же каналу. Адресный префикс 169.254/16 **недопустимо** делить на подсети. Данная спецификация использует основанное на ARP обнаружение конфликтов, при котором используется широковещательная рассылка в локальную подсеть. Поскольку такие широковещательные пакеты не пересылаются, разделение префикса на подсети приведёт к тому, что конфликты адресов останутся не обнаруженными.

Это не означает запрет для устройств Link-Local коммуникаций, выходящих за пределы локального канала. Хосты IP с адресами Link-Local и обычными маршрутизируемыми адресами IPv4 могут использовать эти маршрутизируемые адреса без дополнительных ограничений.

## 2.9. Протоколы вышележащих уровней

Аналогичные рассуждения применимы к уровням, лежащим выше IP.

Например, дизайнерам Web-страниц (включая автоматически генерируемые страницы) **не следует** включать ссылки с адресами IPv4 Link-Local, если предполагается доступность страниц за пределами локального соединения.

Адреса IPv4 Link-Local могут меняться с течением времени и имеют ограниченную область действия, **недопустимо** включение адресов IPv4 Link-Local в DNS.

## 2.10. Вопросы приватности

Другой причиной ограничения выхода адресов IPv4 Link-Local за пределы локального соединения являются вопросы приватности. Если адрес IPv4 Link-Local выводить из хэшированного MAC-адреса, некоторые считают, что это даёт опосредованную связь с конкретным человеком и может использоваться для слежки за ним. В рамках локального соединения аппаратные адреса в пакетах доступны для просмотра, но пока адреса IPv4 Link-Local не выходят за

пределы локального соединения, это не позволяет злоумышленнику получить какую-либо информацию в дополнение к возможности прямого наблюдения аппаратных адресов.

## 2.11. Взаимодействие клиента DHCPv4 с машинами состояний IPv4 Link-Local

Как указано в Приложении A, ранние реализации IPv4 Link-Local используют модифицированную машину состояний DHCP. Опыт показывает, что эти изменения снижают надёжность сервиса DHCP.

Устройствам, поддерживающим IPv4 Link-Local и клиента DHCPv4, не следует менять поведения клиента DHCPv4 для поддержки конфигурации IPv4 Link-Local. В частности, настройка адреса IPv4 Link-Local, независимо от того, отвечает ли в данное время сервер DHCP, не является достаточным основанием для отказа от действующей аренды DHCP, остановки попыток клиента DHCP получить новый адрес IP, изменения тайм-аутов DHCP или смены поведения машины состояний DHCP иным способом.

Этот вопрос подробно рассмотрен в работе «Detection of Network Attachment (DNA) in IPv4» [DNAv4].

# *3. Множество интерфейсов*

Приведённые здесь рассуждения применимы к хостам с множеством адресов IP, независимо от наличия у них множества физических интерфейсов. Системы с множеством интерфейсов включают логические конечные точки (туннели, виртуальны частные сети и т. п.), а также множество логический сетей в одной физической среде. Такие системы часто называют многодомными (multi-homing).

Хосты, имеющие более одного активного интерфейса и выбирающие динамическую настройку адресов IPv4 Link-Local на одном или нескольких интерфейсах, будут сталкиваться с разными проблемами. В этом разделе рассматриваются проблемы, но не указаны возможные способы их решения. На момент подготовки документа общего решения этих проблем не было известно. Разработчикам нужно принимать эти проблемы во внимание до реализации описанного здесь протокола в системах, которые могут иметь более одного активного интерфейса для стека TCP/IP, поддерживающего многодомные системы.

## 3.1. Область действия адресов

Хост может быть подключён одновременно к множеству сетей. Было бы хорошо использовать во всех сетях одно адресное пространство, но это не так. Адреса, используемые в одной сети (например, находящейся за NAT или использующей адреса IPv4 Link-Local), не могут также использоваться в другой сети.

Было бы неплохо, если бы приложения не видели адресов, однако они видят. Большинство приложения использует TCP/IP, ожидая сообщений с любого интерфейса через определённый порт для конкретного транспортного протокола. Приложения обычно знают (и заботятся) о том, что им пришло сообщение. Приложения знают адрес отправителя сообщения, по которому они будут отвечать.

Первой проблемой для адресов с ограниченной областью действия является выбор интерфейса. Многодомный хост имеет множество адресов. Какой из них следует использовать в качестве адреса отправителя при передаче пакетов конкретному получателю? На этот вопрос обычно отвечают ссылкой на таблицу маршрутизации, которая указывает на какой интерфейс (с каким адресом) следует передавать пакеты и как это делать (напрямую или путём пересылки маршрутизатору). Выбор осложняется адресами с ограниченной областью действия, поскольку диапазон адресов получателя может быть неоднозначным. Таблица может не дать верного ответа. Эта проблема связана с выбором следующего маршрутизатора (next-hop), рассмотренным в параграфе 3.2.

Вторая проблема связана с распространением параметров с ограниченной областью действия за пределы этой области. Этот вопрос рассматривается в разделе 7.

Эти проблемы можно решить. Одним из способов является раскрытие информации об области действия приложениям, чтобы они знали, в какой области находятся их партнёры. Таким образом можно выбрать корректный интерфейс и обеспечить безопасную процедуру в отношении адресов пересылки и других параметров с ограниченной областью действия. Возможны и другие решения, но ни один из методов не стандартизован для IPv4 и не задан этим документом. Хорошая реализация API может смягчить проблемы, показывая область действия приложениям, для которых такая информация важна, или инкапсулируя информацию с ограниченной областью действия и логику так, чтобы приложения могли работать корректно, не зная области действия адресов.

Разработчикам следует принимать меры по решению этих проблем, а не отмахиваться от них. При наличии достаточного опыта можно надеяться на разработку спецификаций, задающих решение проблем адресов с ограниченной областью действия на многодомных хостах.

## 3.2. Неоднозначность адресов

Это основная проблема для случая доступности получателей IPv4 Link-Local через несколько интерфейсов. Что делать хосту, если ему нужно передать пакет получателю L с адресом Link-Local и ARP связывает L с несколькими каналами?

Даже в случае привязки адреса Link-Local в данный момент к единственному каналу нет гарантии сохранения такой однозначности в будущем. Другие хосты на других интерфейсах также могут объявить адрес L.

Одним из возможных вариантов является поддержка лишь для случаев, когда приложение явно указывает интерфейс для передачи.

Для этой проблемы нет стандартного или очевидного решения. Существующие программы для стека протоколов IPv4 большей частью не способны работать при неоднозначности адресов. Это не мешает разработчикам искать решения и создавать программы, способные эти решения использовать, для поддержки хостов, которые смогут динамически настраивать адреса IPv4 Link-Local одновременно на нескольких интерфейсах. Однако такое решение почти наверняка не будет применимо для имеющихся приложений и прозрачно для протоколов вышележащих уровней.

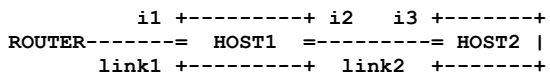
С учётом того, что стек IP должен иметь исходящий интерфейс, связанный с пакетом, который нужно передать по адресу Link-Local, выбор интерфейса является обязательным. Выходной интерфейс невозможно определить из полей

заголовка пакета типа адресов получателя и отправителя (например, с помощью таблицы пересылки). Поэтому привязка выходного интерфейса должна выполняться явно и иными способами. Спецификация не задаёт этих способов.

## 3.3. Взаимодействие с хостами, имеющими маршрутизируемый адрес

В этом документе уделяется внимание переходу от применения адресов IPv4 Link-Local к маршрутизируемым адресам (см. параграф 1.5). Цель заключается в том, чтобы позволить хосту с одним интерфейсом сначала поддерживать конфигурацию Link-Local, а затем аккуратно перейти к использованию маршрутизируемого адреса. Поскольку в процессе перехода у хоста временно может быть более одного активного адреса, к нему будут применимы описанные в параграфе 3.1 проблемы ограничения области действия адресов. Когда хост получает маршрутизируемый адрес, ему не нужно сохранять свой адрес Link-Local для взаимодействия с другими устройствами на том же канале, использующими адреса Link-Local, - любой хост, соответствующий данной спецификации знает, что независимо от адреса отправителя получатель IPv4 Link-Local должен быть доступен путём прямой пересылки (без использования маршрутизаторов). Для хоста, взаимодействующего с хостом, имеющим адрес Link-Local, не требуется наличие адреса Link-Local.

Хост с адресом IPv4 Link-Local может передавать пакеты получателям, не имеющим адресов IPv4 Link-Local. Если хост не является многодомным, эта процедура проста и однозначна - используется ARP и прямая пересылка в канал. Однако для многодомных хостов правила маршрутизации более сложны особенно в случаях, когда один из его интерфейсов имеет маршрутизируемый адрес и принятый по умолчанию маршрут идёт к маршрутизатору через этот интерфейс. Ниже представлен пример, иллюстрирующий эту проблему и общее решение для неё.




HOST1 подключён к каналам link1 и link2. Интерфейс i1 имеет маршрутизируемый адрес, а i2 - адрес IPv4 Link-Local. HOST1 имеет принятый по умолчанию маршрут к маршрутизатору ROUTER через интерфейс i1. HOST1 будет направлять пакеты для получателей из 169.254/16 на интерфейс i2 для отправки напрямую.

HOST2 имеет адрес IPv4 (не Link-Local) на интерфейсе i3.

Используя протокол преобразования имён или поиска служб, HOST1 может узнать адрес HOST2. Поскольку адрес HOST2 не относится к префиксу 169.254/16, правила маршрутизации HOST1 будут направлять дейтаграммы для HOST2 через интерфейс i1 маршрутизатору ROUTER. Если у маршрутизатора ROUTER нет маршрута к HOST2, дейтаграммы от HOST1 не попадут на HOST2.

Решением проблемы будет попытка хоста локально связаться (используя ARP) с каждым хостом, для которого он получает сообщение ICMP об ошибке (код ICMP 0, 1, 6 или 7 [RFC792]). В этом случае хост будет перебирать все подключённые каналы поочерёдно. Такой подход был успешно реализован на некоторых хостах IPv6. В нашем примере HOST1 при невозможности доступа к HOST2 через ROUTER будет пытаться передать пакеты HOST2 через интерфейс i2 и это приведёт к успеху.

Можно решить эту проблему с помощью методов, описанных в параграфе 3.2, или иными способами, которые здесь не рассмотрены. Спецификация не предлагает стандартного решения и не препятствует разработчикам поддерживать многодомные конфигурации при условии решения описанных здесь проблем для применяемых на хосте приложений.

## 3.4. Непреднамеренный автоиммунный отклик

Следует соблюдать осторожность в случаях, когда многодомный хост имеет более одного интерфейса в один и тот же канал и все эти интерфейсы поддерживают автонастройку IPv4 Link-Local. Если эти интерфейсы попытаются получить один адрес, хост будет защищаться от самого себя, что приведёт к отказу алгоритма объявления адресов. Простейшим способом решения этой проблемы является независимое использование алгоритма для каждого интерфейса с адресом IPv4 Link-Local.

В частности, пакеты ARP, которые используются для объявления адреса, связанного с конкретным интерфейсом, указывают конфликт лишь при их получении с указанным аппаратным адресом другого интерфейса.

Если хост имеет два интерфейса в один канал, объявление или защита адресов для этих интерфейсов должны гарантированно заканчиваться с разными адресами интерфейсов, как будто они находятся на разных хостах. Отметим, что некоторые способы, с помощью которых хост может обнаружить у себя два интерфейса в один канал, могут быть неожиданными и не очевидными, например, при наличии на хосте интерфейсов Ethernet и 802.11, соединённых мостом (иногда даже без ведома пользователя).

# *4. «Сращивание» разделённой сети*

Хосты на разных каналах могут пользоваться совпадающими адресами IPv4 Link-Local. Если такие разъединённые сети позднее объединяются или связываются мостом, могут возникнуть адресные конфликты. Когда какой-либо хост попытается связаться с другим хостом сети, он в какой-то момент передаст широковещательный пакет ARP, который позволит всем участвующим хостам обнаружить конфликт адресов.

При обнаружении такого конфликта последующее изменение конфигурации может нарушить работу, вызывая разрыв соединений TCP. Однако предполагается, что такие ситуации будут редки. Для использования доступны 65024 адреса IPv4 Link-Local, поэтому при объединении небольших сетей вероятность возникновения конфликта адресов достаточно мала.

При объединении двух больших сетей (сети с большим числом хостов в сегменте) вероятность конфликта растёт. В таких случаях объединение ранее разделённых сетей будет вынуждать один или множество хостов сменить свой адрес IPv4 Link-Local с последующим разрывом соединений TCP. Там, где такие объединения происходят часто (например, в удалённых сетях, связанных мостом) это может быть существенной помехой. Однако при не слишком большом числе хостов в объединяемых сегментах возникающий в результате объединения и возникающего при этом конфликта адресов, будет невелик.

Передача откликов ARP с адресом отправителя IPv4 Link-по широковещательному адресу вместо индивидуального гарантирует обнаружение конфликтов в тот момент, когда они создают потенциальную проблему, но не раньше. Например, если были соединены две ранее изолированные сети, где хосты A и B имеют одинаковый адрес Link-Local (X), ситуация может сохраняться, пока A, B или какой-то иной хост не попытаются начать взаимодействие. Если некий хост C передаст запрос ARP для адреса X, на который хосты A и B ответят обычными откликами ARP по индивидуальному адресу, хост C увидит конфликт, но A и B не будут знать об этом конфликте, поскольку они не видят пакетов друг друга. Широковещательная передача откликов позволит хостам A и B увидеть конфликтующие пакеты ARP и принять соответствующие меры.

Отметим, что периодическая отправка беспричинных ARP в попытках более раннего обнаружения конфликтов не требуется, ведёт к ненужному расходу пропускной способности и в реальности может нанести вред. Например, если разрозненные каналы соединяются на короткое время и снова будут разделены до того, как начнутся взаимодействия с участием A или B, кратковременный конфликт адресом не сыграет никакой роли и смена адресов не потребуется. В этом случае инициирование ненужной реконфигурации не принесёт никакой пользы. Хостам **не следует** периодически передавать беспричинных пакетов ARP.

# *5. Вопросы безопасности*

Использование адресов IPv4 Link-Local может открывать хост для новых атак. В частности, на хосте без адресов IP стек IP не используется и он не восприимчив к атакам, основанным на IP. Настроив рабочий адрес хост может стать уязвимым для таких атак.

Протокол ARP [RFC826] является незащищённым. Вредоносные хосты могут отправлять в сеть подставные пакеты ARP, нарушая работу других хостов. Например, такой хост может отвечать на все запросы ARP откликами со своим аппаратным адресом, заявляя свои права на каждый адрес в сети.

Примечание. Существуют типы локальных соединений (типа беспроводных ЛВС), которые не обеспечивают физической защиты. По причине наличия таких каналов разработчикам было бы совершенно неразумно предполагать, что устройство, подключённое только к локальному каналу, может обойтись без обычных мер защиты. Отказ от реализации таких мер будет подвергать пользователей существенным рискам.

Для хостов, использующих IPv4 Link-Local возникает другая угроза, связанная с принудительной сменой конфигурации и нарушением работы. Подключенный к каналу злоумышленник может передавать пакеты ARP, которые будут вызывать разрыв всех соединений и переход на новый адрес. Атакующий может вынуждать хост с адресом IPv4 Link-Local выбрать определённые адреса или препятствовать выбору некоторых адресов. Это другая угроза, создаваемая подставными пакетами ARP, описанными выше.

Разработчикам и пользователям следует принимать во внимание, что получение и замена адреса в соответствии с параграфом 2.5 открывает возможность простого захвата соединений TCP другим узлом.

Разработчикам рекомендуется обеспечивать адекватную защиту ресурсов каждого устройства и хоста от известных и предполагаемых угроз. Хотя использование адресов IPv4 Link-Local может снижать число угроз для устройств с таким адресом, разработчикам устройств, поддерживающих протокол IP, не следует надеяться на отсутствие таких угроз в локальной сети устройства.

Хотя могут встречаться отдельные типы устройств и среды, где сеть обеспечивает адекватную защиту доступных устройству ресурсов, было бы ошибкой считать в общем случае, что при использовании на устройстве лишь адресов IPv4 Link-Local требования к защите снижаются.

Во всех случаях, независимо от использования адресов IPv4 Link-Local, на устройствах, поддерживающих протокол IP, необходимо реализовать средства анализа известных и предполагаемых угроз, которым может подвергаться конкретное устройство или хост, и обеспечивать механизмы защиты, предотвращающие или снижающие уровень риска, связанного с такими угрозами.

# *6. Вопросы программирования приложений*

Использование автоматически настраиваемых адресов IPv4 Link-Local предъявляет дополнительные требования к разработчикам приложений и может приводить к отказам в имеющихся программах.

## 6.1. Смена адресов, отказы и восстановление

Используемые приложением адреса IPv4 Link-Local могут меняться со временем и в некоторых программах в таких случаях могут возникать отказы. Например, имеющиеся соединения TCP будут разрываться, потребуется заново находить серверы, адреса которых изменились, операции чтения и записи будут возвращать ошибки и т. п.

Производителям приложений, которые будут использовать реализации IP с поддержкой адресов IPv4 Link-Local, **следует** детектировать и купировать события, связанные со сменой адресов. Разработчикам реализаций IPv4 с поддержкой настройки адресов IPv4 Link-Local **следует** выдавать приложениям информацию о смене адреса.

## 6.2. Ограниченная пересылка идентификаторов местоположения

Адреса IPv4 Link-Local **недопустимо** пересылать через протоколы прикладного уровня (например, в URL) адресатам, находящимся за пределами локального соединения (см. параграф 2.9 и раздел 3).

Существующие распределенные программы, которые пересылают адресную информацию, могут сталкиваться с отказами. Например, FTP [RFC959] (при работе не в пассивном режиме) передаёт IP-адрес клиента. Предположим, что клиент начал работу, имея лишь адрес Link-Local, а затем получи маршрутизируемый адрес IP и взаимодействует с сервером FTP за пределами локального соединения. Если клиент FTP передаст свой старый адрес Link-Local вместо нового маршрутизируемого адреса IP в команде FTP port, сервер FTP не сможет организовать соединение с клиентом для передачи данных и операция FTP завершится отказом.

## 6.3. Неоднозначность адресов

Прикладные программы на многодомных хостах с поддержкой автоматической настройки адресов IPv4 Link-Local на нескольких интерфейсах могут сталкиваться с отказами.

Это обусловлено тем, что приложение полагается на однозначность адресов IPv4, но для адресов IPv4 Link-Local такая однозначность обеспечивается лишь в рамках одного соединения. На хосте, подключённом к нескольким каналам один и тот же адрес может появляться сразу на нескольких интерфейсах или сначала на одном, затем на другом. Большинство имеющихся программ не готовы к таким ситуациям. В будущем предполагается разработка программных интерфейсов, предотвращающих такие проблемы. Этот вопрос рассмотрен в разделе 3.

# *7. Маршрутизаторы*

Маршрутизатору **недопустимо** пересылать пакеты с адресом IPv4 Link-Local в поле отправителя или получателя, независимо от настройки принятого по умолчанию маршрута и маршрутов, полученных от протоколов динамической маршрутизации.

Маршрутизатору, получившему пакет с адресом отправителя или получателя IPv4 Link-Local, **недопустимо** пересылать такой пакет. Это предотвращает пересылку пакетов обратно в сегмент сети, из которого они получены или в другой сегмент.

# *8. Взаимодействие с IANA*

Агентство IANA выделило префикс 169.254/16 для использования, описанного в этом документе. Первые и последние 256 адресов диапазона (169.254.0.x и 169.254.255.x) выделены для Standards Action в соответствии с Guidelines for Writing an IANA (BCP 26) [RFC2434]. Других услуг IANA этот документ не запрашивает.

# *9. Константы*

Ниже перечислены ограничительные константы, используемые протоколом. Их настройка пользователем не предполагается.

| | | |
|---|---|---|
| `PROBE_WAIT` | 1 секунда | Начальная случайная задержка. |
| `PROBE_NUM` | 3 | Число пробных пакетов. |
| `PROBE_MIN` | 1 секунда | Минимальная задержка между повторными пробами. |
| `PROBE_MAX` | 2 секунды | Максимальная задержка между повторными пробами. |
| `ANNOUNCE_WAIT` | 2 секунды | Задержка перед анонсированием. |
| `ANNOUNCE_NUM` | 2 | Число пакетов с анонсами. |
| `ANNOUNCE_INTERVAL` | 2 секунды | Интервал между пакетами анонсирования. |
| `MAX_CONFLICTS` | 10 | Максимальное число конфликтов перед снижением скорости. |
| `RATE_LIMIT_INTERVAL` | 60 секунд | Задержка между последовательными попытками. |
| `DEFEND_INTERVAL` | 10 секунд | Минимальный интервал между защитными пакетами ARP. |

# *10. Литература*

## 10.1. Нормативные документы

[RFC792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[RFC826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

[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.

## 10.2. Дополнительная литература

[802] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.

[802.3] ISO/IEC 8802-3 Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, (also ANSI/IEEE Std 802.3- 1996), 1996.

[802.5] ISO/IEC 8802-5 Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 5: Token ring access method and physical layer specifications, (also ANSI/IEEE Std 802.5-1998), 1998.

[802.11] 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. 802.11-1999, 1999.

[RFC959] Postel, J. and J. Reynolds, "File Transfer Protocol", STD 9, RFC 959, October 1985.

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

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC3027] Holdrege, M. and P. Srisuresh, "Protocol Complications with the IP Network Address Translator", RFC 3027, January 2001.

[DNAv4] Aboba, B., "Detection of Network Attachment (DNA) in IPv4", Work in Progress[1], July 2004.

[LLMNR] Esibov, L., Aboba, B. and D. Thaler, "Linklocal Multicast Name Resolution (LLMNR)", Work in Progress[2], June 2004.

## *Благодарности*

Авторы благодарят (в алфавитном порядке) Jim Busse, Pavani Diwanji, Donald Eastlake 3rd, Robert Elz, Peter Ford, Spencer Giacalone, Josh Graessley, Brad Hards, Myron Hattig, Hugh Holbrook, Christian Huitema, Richard Johnson, Kim Yong-Woon, Mika Liljeberg, Rod Lopez, Keith Moore, Satish Mundra, Thomas Narten, Erik Nordmark, Philip Nye, Howard Ridenour, Daniel Senie, Dieter Siegmund, Valery Smyslov и Ryan Troll за их вклад в работу.

## *Приложение A. Ранние реализации*

### A.1. Apple Mac OS 8.x и 9.x.

Mac OS выбирает адрес IP с использованием псевдослучайных значений. Выбранный адрес записывается в постоянное хранилище для использования после перезагрузки, когда это возможно.

Mac OS передаёт 9 пакетов DHCPDISCOVER с интервалами 2 секунды между ними. Если не было получено отклика на эти сообщения (18 секунд), выполняется автоматическая настройка адреса.

При обнаружении занятости выбранного адреса Mac OS будет выбирать новый случайный адрес, предпринимая для этого не более одной попытки в течение каждых 2 секунд.

Автоматически настроенные системы Mac OS проверяют наличие сервера DHCP каждые 5 минут. Если сервер DHCP найден, Mac OS не удалось получить аренду, сохраняется прежний (настроенный автоматически) адрес IP. если Mac OS получает новую аренду, все существующие соединения сбрасываются без уведомления. Это может приводить к разрыву организованных пользователем сессий. После получения новой аренды Mac OS не будет создавать новых соединений с заданным автоматически адресом IP.

Системы Mac OS не передают пакетов, адресованных получателю Link-Local, принятому по умолчанию шлюзу (если он имеется), такие адреса всегда считаются локальными.

Системы Mac OS по умолчанию передают все индивидуальные пакеты с TTL = 255. Групповые и широковещательные пакеты тоже передаются с TTL = 255, если они отправлены с адреса 169.254/16.

Mac OS реализует автоматическое обнаружение среды (sense where), если оборудование (и драйверы) поддерживают его. При обнаружении подключения на интерфейс будут передаваться сообщения DHCPDISCOVER. Это означает, что система будет выходить из автоматически сконфигурированного режима сразу же при восстановлении соединения.

### A.2. Apple Mac OS X версии 10.2

Mac OS X выбирает адрес IP с использованием псевдослучайных значений. Выбранный адрес записывается в в память и может использоваться при последующих попытках автоматической настройке адреса при однократной загрузке системы.

Автоматическая настройка адреса Link-Local зависит от результатов процесса DHCP. DHCP передаёт два пакета с тайм-аутами в 1 и две секунды. Если отклик не получен (3 секунды), начинается автонастройка. DHCP продолжает передавать пакеты в течение 60 секунд.

В начале процесса автонастройки генерируется 10 случайных уникальных адресов IP, которые проверяются по одному каждые 2 секунды. Процесс проверки завершается при обнаружении первого свободного адреса или после проверки всех.

Если DHCP не даёт результата, процесс останавливается на 5 минут, затем запускается снова. После получения адреса от DHCP настроенный автоматически адрес Link-Local удаляется, однако подсеть Link-Local остаётся.

Автоматическая настройка выполняется в каждый момент только для одного интерфейса.

Mac OS X гарантирует связывание с подсетью Link-Local подключённого интерфейса с высшим приоритетом. Пакеты, направленные по адресу Link-Local, никогда не передаются заданному по умолчанию шлюзу (если он есть). Адреса Link-local всегда привязываются к локальному сегменту.

Mac OS реализует автоматическое обнаружение среды, если оборудование и драйверы поддерживают его. Когда индикатор сетевой среды показывает соединение, процесс автоматической настройки запускается вновь и пытается использовать назначенный ранее адрес Link-Local. При индикации отключения о сети система ждёт 4 секунды до отмены настроенного адреса Link-Local и подсети. Если соединение не восстанавливается, система выбирает другой интерфейс для автоматической настройки.

Mac OS X по умолчанию передаёт все индивидуальные пакеты с TTL = 255. Групповые и широковещательные пакеты тоже передаются с TTL = 255, если они отправлены с адреса 169.254/16.

### A.3. Microsoft Windows 98/98SE

Системы Windows 98/98SE выбирают адрес IPv4 Link-Local с использованием псевдослучайных значений. Алгоритм выбора адреса основан на расчёте хэш-значения MAC-адреса, поэтому при большом наборе хостов должно быть равномерное распределение выбранных адресов из блока 169.254/16. Определение начального адреса IPv4 Link-Local на основе адреса MAC также предполагает попытку получения системой того же адреса при перезагрузке, если не возникает конфликта.

[1]Работа завершена и опубликована в RFC 4436. *Прим. перев.*
[2]Работа завершена и опубликована в RFC 4795. *Прим. перев.*

В состоянии INIT клиент DHCP Windows 98/98SE передаёт 4 сообщения DHCPDISCOVER с интервалом 6 секунд. При отсутствии отклика (24 секунды) хост начинает автоматическую настройку адреса.

Число попыток автоматической настройки для систем 98/98SE составляет 10. После 10 неудачных попыток автоматической настройки адреса IPv4 хост будет загружаться без адреса IPv4.

Автоматически настроенные системы Windows 98/98SE проверяют наличие серверов DHCP каждые 5 минут. Если сервер DHCP найден, но Windows 98 не удалось получить аренду, система сохраняет автоматически настроенный адрес IPv4 Link-Local. Если Windows 98/98SE удалось получить аренду, имеющиеся соединения отбрасываются без уведомления. После получения адреса в аренду Windows 98/98SE больше не будет применять автоматически настроенный адрес IPv4 Link-Local.

Системы Windows 98/98SE с адресом IPv4 Link-Local не передают пакеты, направленные по адресам IPv4 Link-Local в заданный по умолчанию шлюз, если он имеется. Такие адреса всегда считаются локальными.

Системы Windows 98/98SE по умолчанию передают исходящие индивидуальные пакеты с TTL = 128. Настройка TTL выполняется путём установки в реестре Windows подходящего значения ключа HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters\DefaultTTL типа REG_DWORD. Однако это значение будет использоваться для всех пакетов. Это позволяет установить по умолчанию TTL = 255, но не даёт возможности задать по умолчанию TTL = 1 для пакетов IPv4 Link-Local.

Системы Windows 98/98SE не поддерживают автоматического обнаружения подключений. Это значит, что проблемы с соединениями (типа отключения кабеля) могут помешать системе связаться с сервером DHCP и приведут к автоматической настройке адреса. После устранения проблемы (например, при подключении кабеля) ситуация не будет корректироваться незамедлительно. Поскольку система не способна обнаружить подключение, она продолжит использовать автоматически настроенный адрес, не пытаясь получить аренду от сервера DHCP.

Сервер DHCP из состава Windows 98SE ICS[1] (реализация NAT) по умолчанию выделяет адреса из блока 192.168/16.

Однако этот префикс можно изменить путём редактирования реестра и не выполняется никаких проверок, позволяющих предотвратить выделение адресов из префикса IPv4 Link-Local. При такой настройке Windows 98SE ICS будет переписывать заголовки пакетов из префикса IPv4 Link-Local и пересылать их за пределы локального соединения. Windows 98SE ICS не маршрутизирует автоматически префикс IPv4 Link-Local и хосты, получившие адреса от DHCP не смогут взаимодействовать с устройствами, имеющими только локальный адрес.

Существуют и другие домашние шлюзы, которые по умолчанию выделяют адреса из префикса IPv4 Link-Local. Системы Windows 98/98SE могут использовать адрес 169.254/16 IPv4 Link-Local в качестве адреса отправителя при взаимодействии с хостами из других префиксов. Windows 98/98SE не поддерживает запросов и анонсов маршрутизаторов. Системы Windows 98/98SE не будут автоматически находить заданный по умолчанию маршрутизатор в режиме автоматической настройки адреса.

## A.4. Windows XP, 2000 и ME

Поведение автоматической настройки адресов в системах Windows XP, Windows 2000 и Windows ME отличается от поведения Windows 98/98SE лишь поддержкой перечисленных ниже свойств.

Детектирование подключения к среде передачи.

Обнаружение маршрутизаторов.

Прослушивание RIP.

В Windows XP, 2000 и ME реализовано детектирование подключения к среде. При обнаружении такого подключения через интерфейс передаётся сообщение DHCPREQUEST или DHCPDISCOVER. Это означает незамедлительный выход системы из режима автонастройки при восстановлении доступа к среде.

Windows XP, 2000 и ME также поддерживают обнаружение маршрутизаторов, хотя по умолчанию оно отключено. В Windows XP и 2000 поддерживается также прослушивание протокола RIP. Это может приводить к неожиданному обнаружению маршрутизатора в режиме автоматической настройки адресов.

ICS в системах Windows XP/2000/ME ведёт себя как в Windows 98SE применительно к выделению адресов и трансляции (NAT) для префикса Link-Local.

### Адреса авторов

**Stuart Cheshire**

Apple Computer, Inc.

1 Infinite Loop

Cupertino

California 95014, USA

Phone: +1 408 974 3207

EMail: rfc@stuartcheshire.org

**Bernard Aboba**

Microsoft Corporation

[1]Internet Connection Sharing - совместное использование соединения Internet.

One Microsoft Way

Redmond, WA 98052

Phone: +1 425 818 4011

EMail: bernarda@microsoft.com

**Erik Guttman**

Sun Microsystems

Eichhoelzelstr. 7

74915 Waibstadt Germany

Phone: +49 7263 911 701

EMail: erik@spybeam.org

**Перевод на русский язык**

Николай Малых

nmalykh@protokols.ru

**Полное заявление авторских прав**



**Интеллектуальная собственность**

IETF не принимает какой-либо позиции в отношении действительности или объема каких-либо прав интеллектуальной собственности (Intellectual Property Rights или IPR) или иных прав, которые, как может быть заявлено, относятся к реализации или использованию описанной в этом документе технологии, или степени, в которой любая лицензия, по которой права могут или не могут быть доступны, не заявляется также применение каких-либо усилий для определения таких прав. Сведения о процедурах IETF в отношении прав в документах RFC можно найти в BCP 78 и BCP 79.

Копии раскрытия IPR, предоставленные секретариату IETF, и любые гарантии доступности лицензий, а также результаты попыток получить общую лицензию или право на использование таких прав собственности разработчиками или пользователями этой спецификации, можно получить из сетевого репозитория IETF IPR по ссылке http://www.ietf.org/ipr.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.

**Подтверждение**

Финансирование функций RFC Editor обеспечено Internet Society.