Network Working Group
Request for Comments: 5227
Updates: 826
Category: Standards Track

S. Cheshire
Apple Inc.
July 2008

IPv4 Address Conflict Detection

Обнаружение конфликтов адресов IPv4

Статус документа

В этом документе описан проект стандартного протокола Internet, предложенного сообществу Internet, документ служит приглашением к дискуссии в целях развития предложенного протокола. Текущее состояние стандартизации протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться свободно.

Аннотация

При попытке двух хостов на одном канале одновременно установить один адрес IPv4 (за исключением редких особых случаев, когда это заранее согласовано) возникают проблемы на одном или обоих хостах. В этом документе описаны (i) простые меры предосторожности для предотвращения таких проблем и (ii) простой механизм пассивного обнаружения проблемы, позволяющий администратору хоста узнать о её возникновении.

Оглавление

1. Введение

Исторически сложилось так, что настройка одного адреса IP на двух хостах Internet часто создавала раздражающую и трудно диагностируемую проблему.

Это печально, поскольку имеющийся протокол распознавания адресов (Address Resolution Protocol или ARP) обеспечивает хостам простой способ обнаружения этого типа конфигурационных ошибок и информирование о них пользователя. В спецификации DHCP [RFC2131] кратко отмечена роль ARP в обнаружении ошибок конфигурации, как показано в трёх приведённых ниже цитатах из RFC 2131:

- клиенту **следует** проверить недавно полученный адрес (например, с помощью ARP);
- клиенту **следует** окончательно проверить параметры (например, ARP для выделенного сетевого адреса);
- если обнаружено, что адрес уже занят (например, с помощью ARP), клиент **должен** передать серверу сообщение DHCPDECLINE.

К сожалению в спецификации DHCP нет рекомендаций для разработчиков в части количества передаваемых пакетов ARP, интервалов между ними и общего времени ожидания перед принятием решения о возможности бесконфликтного использования адреса и даже не указано, какие типы пакетов нужно прослушивать для принятия решения. Это оставляет неопределённость выбора действия, которое следует предпринимать, если после решения о возможности использования адреса обнаруживается его ошибочность. Не указаны также меры предосторожности, которые клиенту DHCP следует принимать для защиты от «патологических» отказов, например, при многократном предложении сервером DHCP того же адреса, который уже был много раз отвергнут.

Авторы спецификации DHCP возможно были вправе думать тогда, что ответы на эти вопросы представляются слишком простыми, прямыми и очевидными, но к сожалению это перенесло значительную часть сложностей реализации протокола на отдельных разработчиков. Этот документ пытается исправить упущение, чётко указал действия, требуемые в перечисленных ниже случаях.

1. Проверка возможности конфликта при использовании адреса, включая (a) активное использование этого адреса другим хостом на том же канале и (b) непреднамеренное совпадение начала использования двумя хостами одного адреса во время проверки возможности его применение (2.1. Зондирование адреса).

2. Последующее пассивное обнаружение использования того же адреса другим хостом в сети. Даже при использовании на всех хостах мер предосторожности такие конфликты все равно могут возникать, если хосты не обмениваются сведениями в процессе настройки интерфейсов. Это может происходить в беспроводных сетях, когда хост временно выходит за пределы доступности сети или на проводных интерфейсах Ethernet, если канал между двумя концентраторами (hub) не работал в момент настройки адреса. Хорошо организованный хост будет обрабатывать не только конфликты в процессе настройки интерфейса, но и возникшие позже конфликты в течение всего срока (2.4. Обнаружение конфликтов и защита адреса).

3. Ограничение числа попыток получения адреса при большом числе повторяющихся конфликтов (2.1. Зондирование адреса).

Детектирование конфликтов адресов IPv4 (Address Conflict Detection или ACD) не ограничивается клиентами DHCP. Обнаружение конфликтов полезно при настройке адресов вручную и при получении от сервера DHCP или иного источника. При обнаружении конфликта агенту настройки следует сообщать об ошибке. Если таким агентом является человек, уведомлением может быть текст на экране, сообщение протокола SNMP[1] или текстовое сообщение, отправленное на телефон. Для DHCP уведомлениями могут служить сообщения DHCP DECLINE для сервера. При настройке другими программами уведомления могут принимать форму соответствующих программных ошибок, информирующих о конфликте выбранного программой адреса с адресом другого хоста в сети. Программа может отказаться от работы с сетью или автоматически выбрать другой адрес для хоста, чтобы обеспечить максимально быстрое восстановление связности IP.

Выделение адресов IPv4 Link-Local [RFC3927] можно считать частным случаем этого механизма, где агентом настройки служит генератор псевдослучайных чисел а действием при обнаружении конфликта служит выбор другого случайного значения и повторение попытки. Фактически именно такая реализация IPv4 Link-Local была предложена в Mac OS 9 ещё в 1998 г. Если клиент DHCP не получил отклика от сервера DHCP, он может просто создать фиктивный отклик со случайным адресом 169.254.x.x. Если модуль ARP при этом укажет конфликт адресов, клиент DHCP повторяет попытку, создавая новый случайный адрес 169.254.x.x, пока конфликт не будет исчерпан. Реализация ACD как стандартной функции сетевого стека имеет побочный эффект, означающий, что половина работы для адресации IPv4 Link-Local уже сделана.

1.1. Используемые соглашения и термины

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

В этом документе слова «IP-адрес отправителя» и «целевой IP-адрес» в контексте пакетов ARP указывают поля пакета ARP, называемые в спецификации ARP [RFC826] ar$spa (протокольный адрес отправителя) and 'ar$tpa' (протокольный адрес цели), соответственно. Описанное в этом документе использование ARP предполагает, что эти поля содержат адреса IPv4.

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 передающего интерфейса. Поле IP-адреса отправителя **должно** быть заполнено нулями для предотвращения загрязнения кэша ARP на других хостах того же канала, если адрес уже занят другим хостом. Поле аппаратного адреса цели игнорируется и его **следует** заполнять нулями. Поле целевого адреса IP **должно** содержать проверяемый адрес. Пакет ARP Probe содержит вопрос: «Кто-нибудь использует этот адрес?» и предполагаемое утверждение: «Я надеюсь использовать этот адрес».

Термин «анонс ARP» в этом документе обозначает пакет ARP Request передаваемый в локальный канал по широковещательному адресу, похожий на описанный выше пакет ARP Probe, но с полями IP-адресов отправителя и получателя, содержащими анонсируемый адрес IP. Пакет содержит более сильное утверждение: «Я использую этот адрес».

Ниже перечислены временные ограничения, используемые в этом протоколе и упоминаемые в разделе 2, который подробно описывает протокол. Указанные значения являются фиксированными константами и не предполагается их переопределение разработчиками, операторами или пользователями. Константы указаны символьными именами для упрощения будущего стандарта, где может упоминаться этот документ, но в данный момент такого стандарта нет.

```
PROBE_WAIT            1 секунда   (исходная случайная задержка)
PROBE_NUM             3           (число пробных пакетов)
PROBE_MIN             1 секунда   (минимальная задержка при повторе проб)
PROBE_MAX             2 секунды   (максимальная задержка при повторе проб)
ANNOUNCE_WAIT         2 секунды   (задержка перед анонсированием)
ANNOUNCE_NUM          2           (число пакетов Announcement)
ANNOUNCE_INTERVAL     2 секунды   (интервал между пакетами Announcement)
MAX_CONFLICTS        10           (максимальное число конфликтов перед ограничением скорости)
RATE_LIMIT_INTERVAL  60 секунд    (задержка между последовательными попытками)
DEFEND_INTERVAL      10 секунд    (минимальный интервал между защитными ARP)
```

1.2. Связь с RFC 826

Документ не меняет правил для протокола RFC 826. Он не меняет формат пакетов или назначение полей. Имеющиеся правила генерации пакетов и откликов на них применяются в полном соответствии с RFC 826.

Документ расширяет RFC 826, задавая два правила, указанных ниже.

[1] Simple Network Management Protocol - простой протокол управления сетью.

(1) При настройке интерфейса следует генерировать ARP Request, чтобы обнаружить занятость адреса.

(2) Для каждого полученного пакета ARP должен выполняться тривиальный тест, позволяющий пассивно обнаруживать наличие конфликта. Для таких тестов не треьуется передача через сеть дополнительных пакетов, а нагрузка на CPU хоста практически не увеличивается, поскольку каждый хост, поддерживающий ARP, все равно должен обрабатывать каждый полученный пакет ARP в соответствии с правилами приема RFC 826. Эти правила уже включают проверку присутствия IP-адреса отправителя в кэше ARP, а дополнительная проверка заключается в сравнении IP-адреса отправителя с адресами данного хоста, что позволяет обойтись одной командой во многих архитектурах.

Как уже отмечено в RFC 826, пакета ARP Request выполняют две функции - утверждение и запрос.

Утверждение

Поля ar$sha (аппаратный адрес отправителя) и ar$spa (протокольный адрес отправителя) совместно утверждают, что данный протокольный адрес отображён (сопоставлен) с данным аппаратным адресом.

Запрос

Поля ar$tha (аппаратный адрес цели, 0) и ar$tpa (протокольный адрес цели) служат вопросом о возможности отображения данного протокольного адреса на данный аппаратный адрес.

В том документе разъясняется, что значит одно без другого.

Некоторые читатели могут отметить, что, вероятно, невозможно задать «чистый вопрос» и любой вопрос вызывает предположения о том, что спрашивающий хочет получить в ответ. Это похоже на указание свободного места с вопросом: «Здесь кто-нибудь сидит?», подразумевающим невысказанное: «Если нет, то сяду я». Пакет ARP Probe с нулём в поле IP-адреса отправителя может быть простым вопросом: «Кто-нибудь использует этот адрес?», но интеллектуальная реализация, понимающая как обнаружить конфликт адресов IPv4, должна быть способна распознать такой вопрос как предвосхищение заявления об использовании этого адреса.

Поэтому, если реализация в это же время задаёт очень похожий вопрос, ей следует понимать, что двое не могут сидеть на одном месте и следует попросить другое.

1.2.1. Широковещательные отклики ARP

В некоторых случаях обнаружения конфликта адресов IPv4 (Address Conflict Detection или ACD) может быть выгодно доставлять пакеты ARP Reply с использованием широковещательной адресации (вместо индивидуальной) поскольку это позволит раньше обнаруживать конфликты. Например, при динамической настройке адресов IPv4 Link-Local [RFC3927] механизм ACD используется так, как указано здесь, но дополнительно задана широковещательная передача ARP Reply, поскольку в данном контексте повышение надёжности и отказоустойчивости за счёт роста уровня широковещательного сочтено разумным компромиссом. В будущем могут появиться и другие спецификации с уместностью такого компромисса. Дополнительно этот вопрос рассматривается в параграфе 2.6. Широковещательные отклики ARP.

В RFC 826 подразумевается, что отклики на ARP Request обычно передаются по индивидуальным адресам, но допускается и широковещательная отправка ARP Reply. Правила восприятия пакетов в RFC 826 указывают, что содержимое поля ar$spa следует обрабатывать **до** проверки поля ar$op, поэтому любой хост с корректной реализацией восприятия пакетов по правилам RFC 826 будет правильно обрабатывать пакеты ARP Reply полученные через широковещательную рассылку на канале.

1.3. Применимость

Эта спецификация применима ко всем ЛВС IEEE 802 [802], включая Ethernet [802.3], Token-Ring [802.5] и беспроводные ЛВС IEEE 802.11 [802.11], а также к другим технологиям канального уровня, которые работают со скоростью по меньшей мере 1 Мбит/с, имеют задержку кругового обхода не более 1 секунды и используют протокол ARP [RFC826] для сопоставления адресов IP с адресами канального уровня. В этом документе для обозначения таких технологий применяется термин IEEE 802.

Технологии, поддерживающие ARP, но имеющие скорость меньше 1 Мбит/с или период кругового обхода больше 1 секунды, будут корректно работать с этим протоколом, но им чаще придется обрабатывать запоздалое обнаружения конфликтов уже после завершения фазы зондирования (Probing). Для таких каналов может указаться желательной настройка других значений перечисленных ниже параметров.

(a) PROBE_NUM, PROBE_MIN, PROBE_MAX - число пакетов ARP Probe и интервал между ними, описанные в параграфе 2.1.

(b) ANNOUNCE_NUM и ANNOUNCE_INTERVAL - число пакетов ARP Announcement и интервал между ними, описанные в параграфе 2.3.

(c) RATE_LIMIT_INTERVAL и MAX_CONFLICTS, задающие максимальную частоту попыток заявить адрес, как описано в параграфе 2.1.

(d) DEFEND_INTERVAL - пороговое значение интервала между конфликтующими ARP, делающее **недопустимыми** попытки защитить адрес при более частых конфликтах, как описано в параграфе 2.4.

Канальные технологии без поддержки ARP могут включать другие методы определения занятости адресов IP. Рассмотрение ACD для таких сетей выходит за рамки этого документа.

Для эффективной работы описанного здесь протокола не требуется его поддержка всеми хостами на канале. Для защиты поддерживающего эту спецификацию хоста от непреднамеренных адресных конфликтов достаточно корректной реализации партнёрами по каналу протокола ARP в соответствии с RFC 826. Когда партнер получает ARP Request, где целевой протокольный адрес совпадает с одним из адресов IP на данном интерфейсе, и корректно отвечает на него пакетом ARP Reply, запрашивающий хост может определить занятость этого адреса.

Эта спецификация позволяет хостам обнаруживать конфликты адресов на одном физическом канале. Метод ACD не может (и не должен) определять совпадение адресов, используемых хостами на разных физических каналах. Например адрес 10.0.0.1 [RFC1918] использует огромное число устройств во множестве разных сетей и это не

вызывает конфликтов, поскольку адреса связаны с разными каналами. Конфликт будет возникать лишь при использовании адреса двумя устройствами на одном канале[1] (это случается) и в этом случае механизм ACD будет чрезвычайно полезен для обнаружения конфликта и оповещения (или автоматического исправления).

В этом документ группа хостов считается относящейся к одному каналу при выполнении двух условий:

- при отправке хостом A пакета любому хосту B из той же группы по индивидуальному, групповому или широковещательному адресу данные пакета канального уровня доставляются в неизменном виде;
- широковещательный пакет, переданный в канал любым членом группы, будет получен каждым хостом этой группы.

Заголовок канального уровня может быть изменён (например, в Token Ring Source Routing [802.5]), но данные остаются неизменными. В частности, при изменении пересылающим устройством какой-либо части заголовка или данных IP пакет уже не будет относиться к тому же каналу. Это означает, что пакеты, доставляемые через повторители, мосты, концентраторы, коммутаторы, могут относиться к одному каналы, а пакеты, доставляемые через маршрутизатор IP, декрементирующий поле TTL или вносящий иные изменения в заголовок IP, - не могут.

Термин хост в этом документе в равной степени относится к интерфейсам маршрутизаторов и других многодомных устройств, независимо от пересылки (маршрутизации) пакетов таким устройством. Во многих случаях маршрутизатор является важной частью сетевой инфраструктуры с хорошо известным в локальном масштабе адресом IP, который считается достаточно стабильным. Например, адрес принятого по умолчанию маршрутизатора является одним из параметров, которые сервер DHCP обычно сообщает своим клиентам, но у сервера DHCP (по крайней мере до момента широкой реализации механизма DHCP Reconfigure [RFC3203]) нет способа уведомить своих клиентов о смене этого адреса. Поэтому для таких устройств обработка конфликтов путём выбора нового адреса IP не является лучшим вариантом. В таких случаях применяется вариант (c) из параграфа 2.4. Обнаружение конфликтов и защита адреса.

Однако даже при настройке адреса вручную заявление того же адреса IP другим устройством в сети будет загрязнять кэш ARP и препятствовать надёжной работе, поэтому оператору полезна информация о таких конфликтах. Если конфликт обнаруживается при настройке адреса вручную, оператора следует уведомлять сразу же, а при более позднем обнаружении конфликта полезно уведомить оператора по какому-либо асинхронному каналу связи. Несмотря на невозможность надёжной связи через вызвавший конфликт адрес, остаётся возможность проинформировать оператора по сохраняющемуся каналу связи, например, через другой интерфейс маршрутизатора, динамический адрес IPv4 link-local, рабочий адрес IPv6 или даже без использования технологии IP (локальный экран или последовательный терминал).

2. Проба адреса, анонсирование, обнаружение конфликтов и защита

В этом разделе описано начальное зондирование для безопасного детектирования уже занятых адресов, анонсирования выбранного адреса, проверки конфликтов и необязательного использования широковещания ARP Reply для обнаружения конфликтов.

2.1. Зондирование адреса

Перед началом использования адреса IPv4 (настроенного вручную, полученного от DHCP и пр.) реализующий эту спецификацию хост **должен** проверить занятость адреса путём широковещательной передачи пакетов ARP Probe. Это также применяется при переходе сетевого интерфейса в активное состояние в процессе пробуждения компьютера, при изменении состояния канала в результате подключения кабеля Ethernet, привязке беспроводного интерфейса 802.11 к новой базовой станции или ином изменении связности, когда хост получает активное соединение с логическим каналом.

Хосту **недопустимо** выполнять такую проверку периодически, поскольку это ведёт к ненужному расходу пропускной способности сети и не требуется благодаря возможности хостов обнаруживать конфликты в пассивном режиме, как описано в параграфе 2.4.

2.1.1. Детали зондирования

Хост проверяет занятость адреса, отправляя для него широковещательный пакет ARP Request. Клиент **должен** указать в поле *sender hardware address* пакета ARP Request аппаратный адрес интерфейса, из которого передаётся пакет. Поле *sender IP address* **должно** быть заполнено нулями, чтобы избежать загрязнения кэша ARP на других хостах канала, в случаях занятости адреса другим хостом. Поле *target hardware address* игнорируется и его **следует** заполнять нулями, а в поле *target IP address* **должен** быть указан проверяемый адрес. Пакет ARP Request, созданный описанным способом, с нулевым IP-адресом отправителя называют зондом ARP (ARP Probe).

Когда хост готов к передаче пробных пакетов, ему следует выждать случайное время из интервала с однородным распределением от 0 до PROBE_WAIT секунд, а затем передать PROBE_NUM проб со случайными интервалами от PROBE_MIN до PROBE_MAX (в секундах). Начальная задержка предотвращает одновременную отправку пробных пакетов при включении сразу множества устройств.

Если в интервале от начала зондирования до ANNOUNCE_WAIT после отправки последнего зонда хост получает на интерфейсе, откуда выполняется зондирование, любой пакет ARP (Request или Reply), где в поле *sender IP address* содержится адрес, для которого выполнялась проверка, хост **должен** считать это индикацией занятости адреса другим хостом и сообщить об этом агенту настройки (оператор, сервер DHCP и т. п.).

Кроме того, если в этом интервале хост получает пакет ARP Probe, где поле *target IP address* содержит проверяемый адрес, а *sender hardware address* отличается от аппаратных адресов данного хоста, хосту **следует** считать это конфликтом и сообщать о нем агенту настройки. Это может происходить при случайной настройке одного адреса на двух (и более) хостах, которые одновременно проверяют возможность использования этого адреса.

[1] Следует отметить, что конфликт может возникать и при использовании одного адреса на разных каналах, если между ними имеется маршрутизация. Но это уже иной контекст. *Прим. перев.*

Примечание. Проверка того, что *sender hardware address* не является аппаратным адресом какого-либо из интерфейсов хоста важна. Некоторые типы концентраторов Ethernet (их часто называют буферизованными повторителями) и многие беспроводные точки доступа могут в широковещательном режиме ретранслировать широковещательные пакеты всем получателям, включая исходного отправителя. По этой причине описанные выше предосторожности нужны для предотвращения путаницы в случаях, когда хост получит свои пакеты ARP.

Реализующий эту спецификацию хост **должен** принять меры по ограничению частоты проверки новых потенциальных адресов. Если хост обнаруживает не менее MAX_CONFLICTS конфликтов на данном интерфейсе, он **должен** ограничить частоту проверки адресов на этом интерфейсе - не более 1 попытки в течение RATE_LIMIT_INTERVAL. Это предотвращает катастрофические «штормы» ARP в случаях серьёзных проблем, таких как сервер DHCP, повторно выделяющий хосту один и тот же адрес. Это правило ограничения частоты проверки применяется не только к конфликтам на этапе начального зондирования, но и к более поздним конфликтам, рассматриваемым в параграфе 2.4.

Если в течение ANNOUNCE_WAIT секунд после отправки последнего пакета ARP Probe не было получено конфликтующего ARP Reply или ARP Probe, хост может считать проверяемый адрес свободным и использовать его.

2.2. Сокращение тайм-аута для других технологий

Могут появиться сетевые технологии, для которых уместны более короткие задержки, нежели требует этот документ. В последующих публикациях IETF для таких технологий могут быть представлены иные значения PROBE_WAIT, PROBE_NUM, PROBE_MIN и PROBE_MAX.

В ситуации, когда хосты на канале используют разные временные параметры, не возникает никаких проблем. Протокол не требует от всех хостов на канале реализации одной версии и даже не зависит от реализации на всех хостах канала. От хостов требуется лишь поддержка ARP в соответствии с RFC 826 и корректные ответы на полученные пакеты ARP Request. При использовании хостами разных временных параметров меняется лишь скорость настройки интерфейсов на хостах. В маловероятной ситуации, когда конфликт не обнаруживается на этапе зондирования, он будет замечен функцией обнаружения конфликтов, описанной в параграфе 2.4.

2.3. Анонсирование адреса

Проверив возможность использовать желаемый адрес, реализующий эту спецификацию хост **должен** объявить о начале использования этого адреса путём широковещательной передачи ANNOUNCE_NUM пакетов ARP Announcement с интервалом ANNOUNCE_INTERVAL секунд. Пакеты ARP Announcement похожи на ARP Probe, но в полях IP-адреса отправителя и получателя указывается выбранный хостом адрес IPv4. Пакеты ARP Announcement нужны для того, чтобы исключить из кэшей ARP записи, которые могли остаться от прежнего владельца адреса. Хост может начать использование адреса IP сразу после отправки двух первых пакетов ARP Announcement, при этом отправка второго ARP Announcement может выполняться одновременно с другими сетевыми операциями хоста.

2.4. Обнаружение конфликтов и защита адреса

Обнаружение адресных конфликтов не ограничено моментом начальной настройки конфигурации интерфейса, когда передаются пакеты ARP Probe. Обнаружение конфликтов - это непрерывный процесс, выполняющийся в течение всего срока использования адреса хостом. В любой момент получение хостом пакета ARP (Request или Reply), где в поле *sender IP address* указан один из адресов IP, настроенных на данном интерфейсе, а *sender hardware address* не соответствует адресу на интерфейсе хоста говорит о конфликте адресов, т. е. попытке другого хоста воспользоваться тем же адресом. Для разрешения конфликта хост **должен** отвечать на конфликтующий пакет ARP, как указано ниже.

(a) При получении конфликтующего пакета ARP хост **может** немедленно прекратить использование адреса, сообщив агенту настройки, как описано выше.

(b) Если у хоста есть активные соединения TCP или иные причины сохранить адрес IPv4 и он не видел конфликтующих пакетов ARP в последние DEFEND_INTERVAL секунд, он **может** попытаться защитить свой адрес, записывая время приёма конфликтного пакета ARP а затем передавая широковещательный пакет ARP Announcement со своим аппаратным и IP-адресом, своим адресом IP в поле *target IP address* и нулевым значением в поле *target hardware address*. После этого хост может продолжать обычное использование адреса без дополнительных действий. Однако если конфликтный пакет ARP не был первым в интервале DEFEND_INTERVAL, хост **должен** немедленно прекратить использовать адрес и уведомить агент настройки об ошибке, как описано выше. Это нужно для предотвращения зацикливания попыток защиты одного адреса двумя хостами.

(c) Если для хоста задано сохранение адреса при любых обстоятельствах (возможно потому, что хост должен иметь стабильный известный адрес IP, применяемый, например, для маршрута по умолчанию или сервера DNS), он **может** выбрать защиту адреса на неопределённый срок. При получении таким хостом конфликтного пакета ARP ему следует предпринять шаги по записи в журнал таких сведений, как адрес отправителя Ethernet из пакета ARP, и сообщить администратору о проблеме. Число таких уведомлений следует контролировать для предотвращения избыточных сообщений об ошибках. Если хост не получал других конфликтных пакетов ARP в последние DEFEND_INTERVAL секунд, он **должен** записать время получения конфликтного пакета ARP, а затем передать 1 широковещательный пакет ARP Announcement со своим аппаратным и IP-адресом. После этого хост может продолжать обычное использование адреса без дополнительных действий. Однако если конфликтный пакет ARP не был первым в интервале DEFEND_INTERVAL и время, записанное для предыдущего конфликтного пакета ARP, попадает в интервал DEFEND_INTERVAL, хосту **недопустимо** передавать другие защитные пакеты ARP Announcement. Это нужно для предотвращения зацикливания защиты одного адреса двумя некорректно настроенными хостами с использованием широковещания.

Хост, желающий обеспечить надёжную работу в сети, **должен** отвечать на конфликтные пакеты ARP в соответствии с пп. (a), (b), (c). Игнорирование конфликтных пакетов ARP ведёт к кажущимся случайными сетевым отказам, которые сложны в диагностике и очень расстраивают пользователей.

Принудительная замена адреса может приводить к обрыву соединений TCP (и других транспортных протоколов). Однако такие отказы должны быть редкими, а при дублировании адресов отказы неизбежны.

Перед отказом от адреса в результате конфликта хосту **следует** предпринять попытку активного сброса соединений, использующих этот адрес. Это снижает некоторые угрозы, которые могут быть связаны с перенастройкой адресов, как описано в разделе 5.

Для большинства клиентских машин, которым не требуется постоянный адрес IP, немедленный запрос у агента настройки (пользователь, клиент DHCP и т. п.) нового адреса при обнаружении конфликта является наилучшим способом быстрого восстановления коммуникаций. Описанный выше механизм широковещательной передачи одного сообщения ARP для защиты адреса несколько смягчает проблему, повышая вероятность сохранения адреса одним из двух конфликтующих хостов.

2.5. Продолжение работы

С момента отправки хостом первого пакета ARP Announcement до отказа от использования адреса IP хост **должен** отвечать на пакеты ARP Request в соответствии со спецификацией ARP [RFC826]. Это означает, в частности, что при получении пакета ARP Request, не вызывающего конфликта, где поле *target IP address* указывает один из адресов IP, настроенных на данном интерфейсе, хост **должен** отвечать пакетом ARP Reply, как описано в RFC 826. Это применимо как к обычным пакетам ARP Request с отличным от 0 IP-адресом отправителя, так и к пакетам Probe Request с нулевым IP-адресом отправителя.

2.6. Широковещательные отклики ARP

В корректно работающей сети с адресами, настроенными вручную или полученными надёжными клиентами от надёжных серверов DHCP, конфликту адресов возникают очень редко и пассивного мониторинга, описанного в параграфе 2.4, вполне достаточно. Если для двух хостов будет задан один адрес IP, рано или поздно один из них передаст широковещательный пакет ARP Request, который получит другой хост, что позволит обнаружить и устранить конфликт.

Однако кратковременное существование условий конфликта до его обнаружения возможно. Предположим, что хостам A и B непреднамеренно был назначен один адрес IP (X), а в момент проверки возможности использования этого адреса канал между хостами по какой-то причине не работал и конфликт не был обнаружен при настройке интерфейсов. Если после восстановления канала другой хост C передаст широковещательный пакет ARP Request для адреса X, не знающие о конфликте хосты A и B передадут индивидуальные (unicast) пакеты ARP Reply хосту C. Получивший эти отклики хост C будет сбит с толку, а хосты A и B не увидят отклик другого хоста и не будут знать о конфликте, продолжая работать, пока один из них не передаст широковещательный пакет ARP Request.

Быстрое обнаружение конфликтов можно обеспечить, передавая пакеты ARP Reply по широковещательному адресу для канала вместо широковещательной передачи ARP Request с индивидуальными откликами. Это **не рекомендуется** в общем случае, но другие спецификации на основе IPv4 ACD могут задавать при необходимости широковещательные отклики ARP Reply. Например, документ Dynamic Configuration of IPv4 Link-Local Addresses [RFC3927] задаёт широковещание для ARP Reply, поскольку в этом контексте обнаружение адресных конфликтов с использованием IPv4 ACD является не резурвной мерой, а единственным механизмом настройки конфигурации.

Широковещательная передача ARP Reply увеличивает объем широковещательного трафика (не более чем вдвое для худшего случая). При традиционном использовании ARP индивидуальные пакеты ARP Reply передаются лишь в ответ на широковещательные пакеты ARP Request, поэтому широковещательный режим ведёт к одному широковещательному пакету Reply в ответ на каждый широковещательный пакет Request. Во многих сетях трафик ARP составляет столь малую часть общего трафика, что его удвоение практически не будет заметно. Однако в некоторых сетях ситуация может отличаться, поэтому широковещание ARP Reply **не следует** применять во всех случаях. Использование широковещательных пакетов ARP Reply следует выбирать там, где это поможет быстрее обнаруживать конфликты, с учётом роста широковещательного трафика и нагрузки, связанной с его обработкой хостами.

3. ARP Announcement в ARP Request вместо ARP Reply

При обсуждении в IETF обнаружения адресных конфликтов IPv4 в период с 2000 г. по 2008 г. неоднократно возникал вопрос о передаче анонсов ARP с использованием незапрошенных пакетов ARP Reply. На первый взгляд такое решение представляется разумным и обычный пакет ARP Reply обеспечивает ответ на вопрос, а поскольку вопрос не был задан, ответ можно считать незапрошенным. Термин «незапрошенный отклик» (gratuitous reply) представляется корректным для анонсов ARP Announcement - ответ на вопрос, который не был задан.

Однако на практике имеется два аргумента в пользу пакетов ARP Request, один из которых связан с историческими причинами, другой является прагматическим. Исторический аргумент связан с тем, что (см. раздел 4) сообщения Gratuitous ARP описаны в документе [Ste94] как использующие пакеты ARP Request и это реализовано в BSD Unix, Microsoft Windows, Mac OS 9, Mac OS X и т. п. Попытки вынудить всех разработчиков перейти на использование пакетов ARP Reply представляются бесполезными.

Прагматический аргумент заключается в том, что пакеты ARP Request с большей вероятностью будут корректно работать с большинством имеющихся реализаций ARP, часть которых может не полностью соответствовать RFC 826. Правила приёма пакетов в RFC 826 указывают, что код операции проверяется последним в процессе обработки пакета и на практике может не оказывать влияния. Однако могут быть «творческие» реализации, в которых обработка пакета зависит от поля ar$op и есть несколько причин, по которым такие реализации будут скорее воспринимать незапрошенные пакеты ARP Request, нежели незапрошенные ARP Reply.

- Некорректная реализация ARP может ожидать передачу ARP Reply лишь по индивидуальным адресам. В RFC 826 это не сказано, но некорректная реализация может предполагать, что «принцип наименьших сюрпризов» диктует при наличии нескольких способов решения проблемы использование того, в котором меньше необычных свойств, поскольку он будет меньше влиять на возможность взаимодействия. Сообщения ARP Announcement должны передавать информацию всем хостам на канале. Поскольку пакеты ARP Request всегда являются широковещательными, в отличие от ARP Reply, приём широковещательного пакета ARP Request вызывает меньше удивления, нежели приём широковещательного пакета ARP Reply.

- Некорректная реализация ARP может предполагать, что пакеты ARP Reply могут быть получены лишь в качестве откликов на ARP Request, недавно переданных этой реализацией. Незапрошенные пакеты Reply могут просто игнорироваться.
- Некорректная реализация ARP может игнорировать пакеты ARP Reply, где ar$tha не совпадает с её аппаратным адресом.
- Некорректная реализация ARP может игнорировать пакеты ARP Reply, где ar$tpa отличается от её адреса IP.

Таким образом, имеется больше шансов отклонения некорректной реализацией ARP пакетов ARP Reply (которые обычно являются результатом запроса клиента), нежели пакетов ARP Request (обычно незапрошенных).

4. Историческое замечание

Некоторые читатели книги Stevens [Ste94] отмечали, что описанный в ней механизм Gratuitous ARP обеспечивает детектирования дубликатов адресов, делая ACD ненужным. Это ошибочное представления, То, что в книге Stevens названо Gratuitous ARP, является просто более описательным представлением ARP Announcement из данного документа. Эта традиционная реализация Gratuitous ARP передаёт лишь одно сообщение ARP Announcement при первоначальной настройке интерфейса. В результате «жертва» (владелец адреса) записывает ошибку, а нарушитель зачастую продолжает работу, даже не замечая проблему. Обе машины продолжают использовать один адрес IP и отказы возникают постоянно, поскольку каждый из хостов сбрасывает TCP-соединения другого. Предполагается, что администратор машины-жертвы увидит журнальное сообщение и исправит ошибку. Обычно для этого нужен физический доступ к такой машине, поскольку нет возможности поддерживать соединение TCP достаточно долго для выполнения нужной настройки.

Gratuitous ARP фактически не обеспечивают эффективного обнаружения дубликатов адресов и (на январь 2008 г.) большинство результатов поиска Google по фразе Gratuitous ARP дают рекомендации по отключению механизма.

Однако разработчикам IPv4 ACD следует помнить, что на момент написания этого документа использование Gratuitous ARP было еще достаточно широким. Шаги, описанные в параграфах 2.1 и 2.4 этого документа помогут обеспечить устойчивость хоста к некорректной настройке и конфликтам адресов даже в случаях, когда другой хост не следует этим правилам.

5. Вопросы безопасности

Механизм обнаружения адресных конфликтов IPv4 ACD основан на ARP [RFC826] и наследует проблемы безопасности этого протокола. Вредоносный хост может передавать в сеть обманные пакеты ARP, нарушающие работу других хостов. Например, он может отвечать на все пакеты ARP Request пакетами ARP Reply со своим аппаратным адресом, заявляя тем самым владение всеми адресами в сети.

Данная спецификация не усугубляет эту уязвимость ARP и даже несколько смягчает ее, поскольку реализующие спецификацию хосты пытаются автоматически сменить адрес и по меньшей мере информировать пользователя о конфликте.

Если хост при обнаружении конфликта ARP сам меняет адрес, как описано в п. (a) параграфа 2.4, это может упростить подключённому к каналу злоумышленнику захват соединений TCP. Активный сброс хостом всех имеющихся соединений перед отказом от адреса снижает этот риск.

6. Благодарности

Документ является результатом обсуждения в рабочей группе Zeroconf адресации IPv4 Link-Local [RFC3927], когда многим участниками было неясно, какие элементы управления локальными адресами относятся к данной проблеме (например, случайный выбор адреса) и какие элементы управления являются базовыми и применимыми ко всем механизмам настройки адресов IPv4 (например, обнаружение конфликтов). В обсуждение проблемы и редактирование документа внесли свой вклад Bernard Aboba, Randy Bush, Jim Busse, James Carlson, Alan Cox, Spencer Dawkins, Pavani Diwanji, Ralph Droms, Donald Eastlake III, Alex Elder, Stephen Farrell, Peter Ford, Spencer Giacalone, Josh Graessley, Erik Guttman, Myron Hattig, Mike Heard, Hugh Holbrook, Richard Johnson, Kim Yong-Woon, Marc Krochmal, Rod Lopez, Rory McGuire, Satish Mundra, Thomas Narten, Erik Nordmark, Randy Presuhn, Howard Ridenour, Pekka Savola, Daniel Senie, Dieter Siegmund, Valery Smyslov, Mark Townsley, Oleg Tychev, Ryan Troll.

7. Литература

7.1. Нормативные документы

[RFC826] 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, November 1982.

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

7.2. 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.

[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.

[RFC3203] T'Joens, Y., Hublet, C., and P. De Schrijver, "DHCP reconfigure extension", RFC 3203, December 2001.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, May 2005.

[Ste94] W. Stevens, "TCP/IP Illustrated, Volume 1: The Protocols", Addison-Wesley, 1994.

Адрес автора

Stuart Cheshire

Apple Inc.

1 Infinite Loop

Cupertino

California 95014

USA

Phone: +1 408 974 3207

EMail: rfc@stuartcheshire.org

Полное заявление авторских прав

Интеллектуальная собственность

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru