Internet Engineering Task Force (IETF)
Request for Comments: 6598
BCP: 153
Updates: 5735
Category: Best Current Practice
ISSN: 2070-1721

J. Weil
Time Warner Cable
V. Kuarsingh
Rogers Communications
C. Donley
CableLabs
C. Liljenstolpe
Telstra Corp.
M. Azinger
Frontier Communications

April 2012

Резерв IANA для совместно используемого префикса IPv4

IANA-Reserved IPv4 Prefix for Shared Address Space

Тезисы

Этот документ служит запросом на выделение блока адресов IPv4 /10 для совместного использования (Shared Address Space[1] - SAS) с целью удовлетворения потребностей устройств CGN[2]. Предполагается, что сервис-провайдеры будут использовать SAS для адресации интерфейсов, соединяющих устройства CGN с пользовательским оборудованием (CPE[3]).

Блок адресов SAS отличается от приватных адресов RFC 1918, поскольку он предназначен для использования в сетях сервис-провайдеров. Однако эти адреса можно использовать и подобно приватным адресам RFC 1918 на маршрутизирующем оборудовании, которое способно транслировать адреса между своими интерфейсами при идентичности адресов на двух разных интерфейсах. Более подробная информация приведена ниже.

Этот документ детализирует выделение дополнительного блока адресов IPv4 для специального применения и служит обновлением RFC 5735.

Статус документа

Этот документ относится к категории обмена опытом (Internet Best Current Practice - BCP).

Документ является результатом работы IETF[4]. Документ представляет согласованное мнение сообщества IETF. Документ был вынесен на публичное обсуждение и одобрен для публикации IESG[5]. Дополнительную информацию о серии документов BCP можно найти в разделе 2 RFC 5741.

Информацию о текущем статусе документа и способы передачи откликов на него можно найти по ссылке http://www.rfc-editor.org/info/rfc6598.

Примечание IESG

Многие операторы указывали на потребность в выделении блока адресов IPv4 специального назначения, описанного в этом документе. В процессе обсуждения сообществом IETF было достигнуто трудное соглашение о выделении такого блока.

Хотя временные меры (типа описанного здесь выделения блока адресов специального назначения) могут в краткосрочной перспективе решить некоторые эксплуатационные проблемы, IESG и IETF продолжают придерживаться мнения о необходимости развертывания IPv6.

[1]Разделяемое (совместно используемое) пространство адресов.
[2]Carrier-Grade NAT.
[3]Customer Premises Equipment.
[4]Internet Engineering Task Force.
[5]Internet Engineering Steering Group.

Оглавление

1. Введение

Адресное пространство IPv4 близко к полному исчерпанию. Однако ISP продолжают расширение использования IPv4, пока протокол IPv6 не развернут полностью. Для этого многие ISP разворачивают устройства трансляции адресов CGN, как описано в [RFC6264]. Поскольку устройства CGN используются в сетях, где предполагаются публичные адреса, а доступные в настоящее время приватные адреса вызывают проблемы при использовании в таком контексте, сервис-провайдерам требуется новый блок адресов IPv4 с маской /10. Этот блок будет называться «пространством для совместного использования» (Shared Address Space) и послужит для адресации интерфейсов, соединяющих устройства CGN с пользовательским оборудованием (CPE).

Блок адресов SAS подобен приватному адресному пространству [RFC1918] в том смысле, что для него не обеспечивается глобальной адресации и адреса из этого блока могут использоваться одновременно на множестве устройств. Однако для адресов SAS имеется ряд ограничений, не присущих приватным адресам [RFC1918]. В частности, эти адреса могут применяться только в сетях сервис-провайдеров или на маршрутизирующем оборудовании, которое способно транслировать адреса через интерфейсы маршрутизаторов, когда адреса двух разных интерфейсов оказываются идентичными.

В этом документе запрашивается выделение блока адресов IPv4 /10 для использования в качестве SAS. По мнению многих ISP размер /10 является минимумом, который позволит развернуть устройства CGN на региональной основе без необходимости организации вложенных CGN. Например, как описано в [ISP-SHARED-ADDR], маски /10 достаточно для обслуживания точек присутствия в регионе Токио.

В этом документе детализировано выделение блока адресов IPv4 специального назначения. Документ также является обновлением [RFC5735].

2. Описание уровня 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 RFC 2119 [RFC2119].

3. Альтернативы SAS

Интерфейсы, соединяющие устройства CGN с оборудованием CPE, предположительно могут адресоваться с использованием любого из перечисленных адресных пространств:

- легитимно выделенные адреса из глобально маршрутизируемого пространства (уникальные);
- узурпированные адреса из глобально маршрутизируемого пространства (т. е., захват адресов);
- адреса [RFC1918];
- разделяемое адресное пространство SAS.

Сервис-провайдеры могут использовать для адресации упомянутых интерфейсов легитимно выделенные им адреса с глобальной маршрутизацией. Хотя такое решение не создает каких-либо проблем, оно непрактично по причине дефицита адресов IPv4. Хотя региональные регистраторы (RIR[1]) имеют достаточные ресурсы для выделения блока /10, который будут совместно использовать сервис-провайдеры региона, эти регистраторы не могут выделить уникальный блок адресов такого размера для каждого сервис-провайдера.

Сервис-провайдерам **недопустимо** использовать для адресации рассматриваемых интерфейсов узурпированные адреса из глобально маршрутизируемого пространства (захват адресов). Если сервис-провайдер начнет анонсировать захваченные адреса в сеть Internet, это окажет деструктивное воздействие на легитимных владельцев анонсируемого блока и не позволит обмениваться данными с ними. Даже если сервис-провайдер не будет анонсировать захваченные адреса за пределы своей сети, сам провайдер и его клиенты могут потерять связность с легитимными владельцами захваченных адресов.

Сервис-провайдер может использовать для адресации рассматриваемых интерфейсов пространство [RFC1918], если выполняется хотя бы одно из перечисленных ниже условий:

- сервис-провайдер знает, что CPE/NAT работают корректно при использовании адресов из блока [RFC1918] на внешнем и внутреннем интерфейсах;
- сервис-провайдер знает, что блок адресов [RFC1918], используемый на интерфейсах между CGN и CPE, не применяется на пользовательской стороне CPE.

[1]Regional Internet Registry.

Пока у сервис-провайдера нет уверенности в выполнении хотя бы одного из приведенных условий, он не может без опаски использовать адреса [RFC1918] и вынужден прибегать к пространству SAS. Обычно это возникает в случаях неуправляемого сервиса, когда пользователи предоставляют свои устройства CPE и сами выбирают адресацию для внутренней сети.

4. Использование разделяемого пространства CGN

Блок адресов SAS в пространстве IPv4 предназначен для использования сервис-провайдерами с целью реализации CGN. Кроме того, SAS можно использовать в качестве дополнительного пространства адресов без глобальной маршрутизации на маршрутизирующем оборудовании, которое способно выполнять трансляцию адресов через интерфейсы маршрутизатора, когда адреса идентичны для двух разных интерфейсов.

Устройства **должны** быть способны выполнять трансляцию адресов при использовании двух идентичных диапазонов SAS на двух разных интерфейсах.

Пакеты с адресом отправителя или получателя из блока SAS **недопустимо** пересылать через границы сервис-провайдеров. Провайдеры **должны** отфильтровывать такие пакеты на входе в свою сеть. Единственным исключением из этого правила является случай деловых отношений (например, хостинг услуг CGN).

При использовании одной инфраструктуры DNS[1] сервис-провайдерам **недопустимо** включать адреса из блока SAS в файлы зон. При использовании расщепленной инфраструктуры DNS сервис-провайдерам **недопустимо** включать адреса SAS в файлы доступных извне зон.

Реверсивные запросы DNS для адресов SAS **недопустимо** пересылать в глобальную инфраструктуру DNS. Провайдерам DNS **следует** отфильтровывать запросы на реверсивное преобразование DNS для адресов SAS на серверах с поддержкой рекурсии. Это делается для предотвращения организации чего-либо типа AS112.net для приватного блока адресов [RFC1918], чей хост некорректно передает запросы реверсивного преобразования DNS в публичную сеть [RFC6304].

Поскольку сервис CGN требует использования непересекающихся адресных пространств с каждой стороны домашнего NAT и CGN, устройства, использующие адреса SAS для целей, отличающихся от CGN, как описано в этом документе, явно будут сталкиваться с проблемами развертывания или подключения услуг CGN в тот момент, когда у них закончится запас публичных адресов IPv4.

5. Риски

5.1. Анализ

Некоторые приложения, определив внешний адрес локального устройства CPE, проверяют, относится ли он к адресам специального назначения, и результат этой проверки оказывает влияние на дальнейшее поведение. При выделении нового блока адресов IPv4 в качестве адресов специального назначения и использовании адреса из этого блока на внешнем интерфейсе CPE некоторые из упомянутых выше приложений могут давать отказы в работе.

В качестве примера предположим, что приложению нужно, чтобы его партнер (или некое иное устройство) инициировал входящее соединение по адресу внешнего интерфейса CPE. Приложение определяет внешний адрес своего CPE и проверяет, относится ли этот адрес к блоку специального назначения. Если адрес относится к специальным, приложение делает корректный вывод о недоступности адреса из публичной сети Internet и ведет себя соответственно. Если адрес не относится к специальным, приложение предполагает доступность этого адреса из глобальной сети Internet и ведет себя по-другому.

Допущение о доступности адресов, не относящихся к блокам специального назначения из глобальной сети Internet в общем случае безопасно, но не всегда верно (например, на внешнем интерфейсе CPE может использоваться публичный адрес из блока, который не анонсируется в публичную сеть Internet, поскольку он находится за CGN). Следовательно, ряд приложений в таких ситуациях может вести себя некорректно.

5.2. Эмпирические данные

Основным мотивом выделения блока SAS является потребность в адресном пространстве для CGN. Применение и влияние CGN ранее было описано в документах [RFC6269] и [NAT444-IMPACTS]. Ниже перечислены некоторые службы, на которые CGN оказывают негативное влияние:

1. Консольные игры - некоторые игровые приложения сталкиваются с проблемами в случае попыток соединения между собой двух игроков с одинаковыми внешними публичными адресами IPv4.
2. Видео-потоки - оказывается влияние на производительность при использовании одной из нескольких популярных технологий потокового видео для доставки множества видео-потоков пользователям, находящимся за отдельными маршрутизаторами CPE.
3. Одноранговые (Peer-to-peer) приложения - некоторые одноранговые приложения не могут нормально работать по причине невозможности открыть входные порты через CGN. Кроме того, некоторые клиенты SIP не могут получать входящие вызовы, пока не будет инициирован исходящий трафик или открыт входной порт через CGN using с использованием протокола PCP[2] [PCP-BASE] или аналогичного механизма.
4. Геолокация - системы геолокации идентифицируют местоположение сервера CGN, а не конечного хоста.
5. Одновременный вход в систему (login) - некоторые web-сайты (особенно банковские системы и сайты социальных сетей) ограничивают число одновременных входов в систему с одного публичного адреса IPv4.
6. 6to4 - системы 6to4 требуют глобально доступных адресов и не будут работать в сетях, где используются адреса с ограниченной топологический доступностью (такие, как адреса за CGN).

[1]Общей для внешнего мира и клиентов сервис-провайдера. *Прим. перев.*
[2]Port Control Protocol.

На основе тестов, описанных в [NAT444-IMPACTS], можно сделать вывод, что влияние CGN на приведенные выше приложения 1-5 не зависит от использования публичных адресов, блока SAS или приватных адресов [RFC1918]. Однако для систем 6to4 эти три варианта дают разные результаты.

Как описано в документе [RFC6343], маршрутизаторы CPE не пытаются инициализировать туннели 6to4, когда на их WAN-интерфейсах заданы адреса [RFC1918] или [RFC5735]. При использовании уникальных в глобальном масштабе идресов или адресов SAS такие устройства могут пытаться инициализировать туннель 6to4, но не достигнут успеха в этом. Сервис-провайдеры могут снизить остроту проблемы за счет использования управляемых провайдером туннелей 6to4 [6to4-PMT] или блокирования маршрута к 192.88.99.1 и генерации сообщение IPv4 о недоступности адресата[1] [RFC6343]. Когда диапазон адресов является общеизвестным (как в случае SAS), производители маршрутизаторов CPE могут включить соответствующий блок адресов в свой список адресов специального назначения (например, [RFC5735]) и трактовать блок SAS аналогично адресам [RFC1918]. Когда адрес CGN-CPE не является общеизвестным, как при использовании уникальных публичных адресов, производителям маршрутизаторов CPE значительно сложнее решить эту проблему.

Таким образом, сравнение адресов [RFC1918] и SAS показывает, что SAS оказывает дополнительное влияние на связность 6to4, которое может быть ослаблено за счет действий сервис-провайдеров или производителей маршрутизаторов CPE. С другой стороны, использование адресного пространства [RFC1918] создает больше проблем по сравнению с SAS в тех случаях, когда абоненты и сервис-провайдер используют перекрывающееся пространство адресов [RFC1918], которое выходит из под контроля сервис-провайдера для случая предоставления неуправляемого обслуживания. Сервис-провайдеры указали, что решение проблем, связанных с перекрытием адресов [RFC1918] по разные стороны маршрутизатора CPE, сложнее, нежели снижение влияния использования SAS на системы 6to4.

6. Вопросы безопасности

Подобно другим адресам специального назначения IPv4 [RFC5735], адреса SAS не порождают напрямую дополнительных проблем безопасности. Тем не менее, в сети Internet нет средств защиты от злоупотреблений такими адресами. Могут быть организованы атаки на основе неожиданного использования похожих адресов специального назначения. Операторам следует рассмотреть этот документ и определить связанные с выделяемым адресным блоком проблемы безопасности, которые могут возникать в конкретных операционных средах. Им следует также рассмотреть вопрос о включении блока адресов SAS в свои списки фильтрации на входе (Ingress Filter) [RFC3704], если их Internet-услуги включают CGN.

Для снижения влияния возможного злоупотребления адресами SAS (использование, отличное от CGN или аналогичных услуг) следует соблюдать перечисленные ниже ограничения:

- маршрутную информацию о сетях SAS **недопустимо** анонсировать через границы сервис-провайдеров; провайдеры **должны** отфильтровывать входящие анонсы в части адресов SAS;
- пакеты с адресами отправителя или получателя из блока SAS **недопустимо** пересылать через границы сервис-провайдеров; провайдеры **должны** отфильтровывать такие пакеты на входных каналах;
- сервис-провайдерам **недопустимо** включать адреса SAS в доступные извне зоны DNS;
- реверсивные запросы DNS для адресов SAS **недопустимо** пересылать в глобальную инфраструктуру DNS;
- провайдерам DNS **следует** отфильтровывать реверсивные запросы DNS для адресов SAS на рекурсивных серверах имен.

7. Согласование с IANA

Агентство IANA зафиксировало выделение блока адресов IPv4 /10 для использования в качестве SAS.

Для адресов совместного использования (SAS) выделен блок 100.64.0.0/10.

8. Литература

8.1. Нормативные документы

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

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

[RFC5735] Cotton, M. and L. Vegoda, "Special Use IPv4 Addresses", BCP 153, RFC 5735, January 2010.

8.2. Дополнительная литература

[6to4-PMT] Kuarsingh, V., Ed., Lee, Y., and O. Vautrin, "6to4 Provider Managed Tunnels", Work in Progress[2], February 2012.

[ISP-SHARED-ADDR] Yamagata, I., Miyakawa, S., Nakagawa, A., Yamaguchi, J., and H. Ashida, "ISP Shared Address", Work in Progress, January 2012.

[NAT444-IMPACTS] Donley, C., Howard, L., Kuarsingh, V., Berg, J., and J. Doshi, "Assessing the Impact of Carrier-Grade NAT on Network Applications", Work in Progress[3], November 2011.

[PCP-BASE] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", Work in Progress[4], March 2012.

[1]ICMP destination unreachable.
[2]Работа опубликована в RFC 6732. *Прим. перев.*
[3]Работа опубликована в RFC 7021. *Прим. перев.*
[4]Работа опубликована в RFC 6887. *Прим. перев.*

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC6264] Jiang, S., Guo, D., and B. Carpenter, "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition", RFC 6264, June 2011.

[RFC6269] Ford, M., Ed., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", RFC 6269, June 2011.

[RFC6304] Abley, J. and W. Maton, "AS112 Nameserver Operations", RFC 6304, July 2011.

[RFC6343] Carpenter, B., "Advisory Guidelines for 6to4 Deployment", RFC 6343, August 2011.

Приложение A. Благодарности

Ниже приведен алфавитный список людей, внесших свой вклад в подготовку документа или приславших отклики на него. Спасибо им.

Stan Barber

John Brzozowski

Isaiah Connell

Greg Davies

Owen DeLong

Kirk Erichsen

Wes George

Chris Grundemann

Tony Hain

Philip Matthews

John Pomeroy

Barbara Stark

Jean-Francois Tremblay

Leo Vegoda

Steven Wright

Ikuhei Yamagata

Адреса авторов

Jason Weil

Time Warner Cable

13820 Sunrise Valley Drive

Herndon, VA 20171

USA

EMail: jason.weil@twcable.com

Victor Kuarsingh

Rogers Communications

8200 Dixie Road

Brampton, ON L6T 0C1

Canada

EMail: victor.kuarsingh@gmail.com

Chris Donley

CableLabs

858 Coal Creek Circle

Louisville, CO 80027

USA

EMail: c.donley@cablelabs.com

Christopher Liljenstolpe

Telstra Corp.

7/242 Exhibition Street

Melbourne, VIC 316

Australia

Phone: +61 3 8647 6389

EMail: cdl@asgaard.org

Marla Azinger

Frontier Communications

Vancouver, WA

USA

Phone: +1.360.513.2293

EMail: marla.azinger@frontiercorp.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com