Network Working Group
Request for Comments: 1918
Obsoletes: 1627, 1597
BCP: 5
Category: Best Current Practice

Y. Rekhter
Cisco Systems
B. Moskowitz
Chrysler Corp.
D. Karrenberg
RIPE NCC
G. J. de Groot
RIPE NCC
E. Lear
Silicon Graphics, Inc.
February 1996

Распределение адресов в частных IP-сетях

Address Allocation for Private Internets

Статус документа

Этот документ относится к числу обобщений реального опыта (Best Current Practices) сообщества Internet и приглашает к дополнительному обсуждению вопроса с целью дальнейшего развития. Документ может распространяться свободно.

1. Введение

В контексте данного документа предприятие рассматривается как автономная сеть на базе стека протоколов TCP/IP. В таком случае распределение адресов является внутренним делом предприятия.

Документ рассматривает вопросы распределения адресов в частных IP-сетях. Корректное распределение адресов обеспечивает полную связность на сетевом уровне между всеми хостами предприятия, а также между публичными (общедоступными) хостами разных предприятий. Использование в сети предприятия частных (private) адресов может привести к необходимости смены адресов хостов и сетей, если сеть станет публичной[1].

2. Мотивация

По мере распространения технологий TCP/IP (включая и сети, не входящие в Internet), все большее число предприятий начинает использовать эту технологию и связанную с ней адресацию в корпоративных сетях, которые зачастую даже не связаны с другими сетями или Internet.

Скорость роста сети Internet превосходит все ожидания. Экспоненциальное увеличение числа хостов в сети порождает новые потребности и связанные с ними проблемы. Одной из таких проблем является нехватка адресов для обеспечения уникальности адреса каждому хосту, подключенному к Internet. Другой, связанной с этим проблемой, является усложнение маршрутизации. Ведутся работы по поиску решения этих проблем на длительный срок. Одним из способов решения этой проблемы является пересмотр процедуры распределения адресов и ее влияния на сложность маршрутизации в Internet.

Для упрощения маршрутизации провайдерам Internet выделяются блоки адресов, из которых они потом выделяют адреса своим заказчикам. В результате такого распределения адресов маршруты к множеству заказчиков можно агрегировать (объединять) и для других (внешних) провайдеров такие маршруты будут выглядеть как единый маршрут [RFC1518], [RFC1519]. Для того, чтобы объединение маршрутов было достаточно эффективным, провайдеры Internet стимулируют своих заказчиков к переходу на адреса из выделенных провайдеру блоков (с таким переходом связана смена адресов в компьютерах заказчиков). Смена адресов может потребоваться множеству пользователей Internet.

Текущие размеры сети Internet и темпы ее роста не позволяют надеяться, что организациям, использующим в частных (изолированных) сетях адреса, не полученные официально от уполномоченного регистратора, могут быть сохранены при подключении корпоративной сети к Internet. Напротив, можно с уверенностью говорит, что при подключении такой организации к сети Internet в этой сети придется менять адреса IP для всех хостов, связанных с Internet.

Обычно уникальный адрес присваивается каждому хосту, который использует TCP/IP. Для того чтобы продлить срок существования IPv4, процедуры выделения адресов существенно ужесточены и сейчас не каждая организация может получить в свое распоряжение дополнительные адреса [RFC1466].

Хосты в сетях, использующих IP можно разделить на три категории:

1. Хосты, которым не требуется доступ в Internet или связь с другими сетями; хосты этой категории могут использовать IP-адреса, которые являются уникальными в масштабах данной сети, но могут совпадать с адресами хостов в других сетях.
2. Хосты, которым требуется доступ к ограниченному числу внешних служб (например, электронная почта, FTP, новости, удаленный доступ), который может быть организован с использованием промежуточных шлюзов

[1] Доступной пользователям из внешних по отношению к предприятию сетей. *Прим. перев.*

(например, шлюзов прикладного уровня). Для многих хостов этой категории неограниченный внешний доступ (на базе IP) может оказаться ненужным и даже нежелательным по соображениям безопасности. Подобно хостам первой категории такие хосты могут использовать IP-адреса, которые уникальны в масштабе предприятия, но могут совпадать с адресами хостов в других сетях.

3. Хосты, которым требуется на сетевом уровне доступ за пределы сети предприятия (обеспечивается по протоколу IP); адреса таких хостов должны быть уникальными в глобальном масштабе.

Будем говорить об адресах хостов первых двух категорий как о частных (private), а адреса третьей категории будем называть публичными (public).

Многим приложениям не требуется доступ во внешние сети (за пределы сети предприятия) для большинства хостов. В крупных предприятиях можно выделить часть хостов, использующих TCP/IP, но не требующих доступа за пределы предприятия на сетевом уровне.

Примерами ситуаций, когда внешний доступ не требуется, могут служить:

- Крупный аэропорт, использующий в залах прибытия и отправления терминалы, подключенные по TCP/IP. Таким терминалам крайне редко требуется доступ во внешние сети.
- Крупные организации (например, банки или торговые фирмы) часто используют TCP/IP в своих сетях. Большому числу локальных станций (кассовые машины, банкоматы и т. п.) крайне редко используют доступ во внешние сети.
- Для обеспечения безопасности многие предприятия используют шлюзы прикладного уровня для соединения своих сетей с Internet. Внутренняя сеть обычно не имеет прямого доступа в Internet, и связана с одним или несколькими шлюзами, доступными из сети Internet. В таких случаях внутренняя сеть может использовать IP-адреса, которые не являются уникальными.
- Для интерфейсов маршрутизаторов, обращенных внутрь корпоративной сети не требуется обеспечивать прямой доступ из внешних сетей.

3. Частные адреса

Служба распределения номеров IANA (Internet Assigned Numbers Authority) зарезервировала для частных сетей три блока адресов:

```
10.0.0.0        -   10.255.255.255  (префикс 10/8)
172.16.0.0      -   172.31.255.255  (префикс 172.16/12)
192.168.0.0     -   192.168.255.255 (префикс 192.168/16)
```

Будем называть первый блок 24-битовым, второй - 20-битовым, а третий - 16-битовым. Отметим, что первый блок представляет собой ни что иное, как одну сеть класса A, второй блок - 16 последовательных сетей класса B, а третий блок - 256 последовательных сетей класса C.

Любое предприятие может использовать IP-адреса из этих блоков без согласования с IANA или Internet-регистраторами. В результате, эти адреса используются на множестве предприятий. Таким образом, уникальность адресов сохраняется только в масштабе или нескольких предприятий, согласованно использующих общий блок адресов. В такой сети каждый хост может обмениваться информацией с любым другим хостом частной сети.

Если предприятию требуются уникальные адреса для связи с внешними сетями, такие адреса следует получать обычным путем через регистраторов Internet. Такие адреса никогда не будут входить ни в один из указанных выше блоков частных адресов.

Перед распределением адресов из частного и публичного блоков следует определить, какие из хостов сети должны иметь связь с внешними системами на сетевом уровне в настоящее время и в будущем – для таких хостов следует использовать публичные адреса. Остальным хостам можно присваивать адреса из частных блоков – это не помешает им взаимодействовать со всеми хостами корпоративной сети, независимо от того, какие адреса имеют эти хосты (частные или публичные). Однако прямой доступ во внешние сети для хостов с адресами из частного блока невозможен. Для организации доступа таких хостов во внешние шлюзы придется использовать специальные шлюзы[2] (например, шлюзы прикладного уровня).

Хосты с публичными адресами могут иметь прямую связь с внешними сетями и Internet. Хосты с публичными адресами могут обмениваться данными со всеми хостами корпоративной сети (независимо от типа адресов этих хостов), а также с публичными хостами других сетей. Публичные хосты, однако, не могут иметь прямого доступа к хостам других сетей, использующим частные адреса.

Перемещение хоста из частной сети в публичную (и обратное) связано со сменой IP-адреса, соответствующих записей DNS и изменением конфигурационных файлов на других хостах, которые идентифицируют хосты по их IP-адресам.

Поскольку частные адреса не имеют глобального значения, маршрутная информация о частных сетях не должна выходить за пределы этих сетей, а пакеты с частными адресами отправителей или получателей не должны передаваться через межсетевые каналы. Предполагается, что маршрутизаторы в публичных сетях (особенно маршрутизаторы провайдеров Internet) будут отбрасывать маршрутную информацию из частных сетей. Если маршрутизатор публичной сети получает такую информацию, ее отбрасывание не должно трактоваться как ошибка протокола маршрутизации.

Непрямые ссылки на адреса из частных блоков должны сохраняться внутри предприятия. Примерами таких записей могут служить RR-записи DNS, и другая информация со ссылками на внутренние частные адреса. Провайдеры Internet должны принимать меры против публичного распространения такой информации.

4. Преимущества и недостатки при использовании частных адресов

Очевидным преимуществом использования частных адресов является экономия адресного пространства Internet за счет использования частных адресов во множестве сетей, не связанных напрямую с Internet.

Предприятия также имеют преимущества в результате использования частных адресов. Блоки частных адресов достаточно велики и обеспечивают гибкость и свободу при распределении адресов для хостов частной сети. Это позволяет обойтись без смены адресов при внесении в сеть изменений или ее расширении.

[2] Для обозначения таких шлюзов часто используется термин прокси – proxy. *Прим. перев.*

По разным причинам в сети Internet уже возникали ситуации, когда предприятия, не подключенные к Internet, использовали для своих хостов IP-адреса из публичных блоков без согласования с IANA. В некоторых случаях эти адреса уже были выделены другим предприятиям. Если сеть с такими адресами потом будет подключаться к Internet, могут возникнуть серьезные проблемы, поскольку маршрутизация IP не может быть корректной при наличии в сети хостов с совпадающими адресами. Хотя провайдеры Internet должны предотвращать подобные ситуации путем использования маршрутных фильтров, на практике такая фильтрация осуществляется не всегда. Использование частных адресов в корпоративных сетях позволяет избежать проблем с маршрутизацией при подключении частной сети к Internet. Основным неудобством при использовании частных адресов является возможность возникновения существенных проблем при подключении корпоративной сети к Internet.

Если в сети используются частные адреса, то при ее подключении к Internet потребуется смена адресов IP для каждого хоста, которому предоставляется прямой доступ в Internet. Обычно расходы на такую замену адресов пропорциональны числу хостов, которые переносятся из частной сети в публичную. Однако, как было отмечено выше, смена адресов может потребоваться и при использовании в частной сети уникальных адресов[3].

Другой проблемой, которая может возникнуть при использовании частных адресов, является необходимость смены адресов при объединении двух или более сетей, если они использовали частные адреса из перекрывающихся блоков. Если вернуться к списку компаний, для которых рекомендовалось использовать частные адреса (параграф 2), можно заметить, что такие компании (сети) достаточно часто объединяются. Если в каждой из объединяемых сетей использовались частные адреса, в объединенной сети требование уникальности адресов каждого хоста может нарушаться. В результате возникает необходимость смены адресов для всех или части хостов.

Расходы на замену адресов могут быть снижены за счет использования средств автоматического распределения адресов (например, протокола DHCP). При выборе зоны использования частных адресов мы рекомендуем для таких зон сразу применять системы автоматического распределения адресов[4]. Вопросами замены адресов (процедура, рекомендации) занимается специальная рабочая группа IETF (PIER Working Group).

5. Практические рекомендации

Одним из возможных вариантов является разработка на начальном этапе плана распределения адресов для внутренней части сети, не связанной напрямую с другими сетями. После этого определяются публичные подсети и для них выделяются соответствующие блоки адресов.

Такой подход не порождает фиксированной навсегда схемы. Если статус одного или нескольких хостов впоследствии изменяется (от частного к публичному или наоборот), потребуется сменить адреса только для таких хостов[5]. Для того, чтобы избежать остановки сети при таких изменениях, целесообразно группировать хосты в подсети с учетом перспектив дальнейшего использования этих хостов.

Если подходящая схема организации подсетей может быть разработана и будет поддерживаться используемым в сети оборудованием, разумно воспользоваться для частной сети 24-битовым блоком адресов (сеть класса A) – это позволит создать достаточно большую сеть. Если разделение на подсети нереально, можно воспользоваться 16-битовым (сеть класса C) или 20-битовым (сеть класса B) блоком частных адресов.

Может показаться заманчивой перспектива использования частных и публичных адресов в одной физической сети. Хотя такое решение допустимо, оно содержит подводные камни, связанные с существованием нескольких подсетей IP в одной сети канального уровня. Рекомендуем с осторожностью использовать такой подход[6].

Настоятельно рекомендуется для маршрутизаторов, соединяющих предприятие с внешними сетями, использовать соответствующие фильтры для пакетов и маршрутов, предотвращающие передачу пакетов с частными адресами и информации о внутренних маршрутах во внешние по отношению к предприятию сети. Такие фильтры нужно устанавливать на маршрутизаторах по обе стороны канала между сетями. На входе в сеть предприятия должна также отфильтровываться вся входящая маршрутная информация для того, чтобы предотвратить ненужные проблемы с маршрутизацией во внутренней сети.

Две частных сети могут обмениваться информацией через публичную сеть, если использование частных адресов в обеих сетях согласовано. Для решения таких задач на границах частных сетей следует использовать инкапсуляцию.

Если несколько организаций, использующих частные адреса из указанных в данном документе блоков, захотят впоследствии связать свои сети по протоколу IP, существует риск нарушения требования уникальности адреса для каждого хоста в масштабе объединенной сети. Для снижения такого риска рекомендуется выбирать для использования группу адресов из допустимого блока случайным образом.

Если предприятие использует частные адреса или комбинацию частных и публичных адресов, клиенты DNS за пределами предприятия не должны видеть адресов из частного блока, поскольку такие адреса будут вводить в заблуждение другие системы. Одним из способов решения этой проблемы является использование уполномоченных серверов (authority server) для каждой зоны DNS, содержащей частные и публичные адреса. Один сервер будет доступен из публичной сети и должен содержать только те адреса частной сети, которые доступны извне (публичные адреса). Другой сервер будет доступен только из частной сети и должен содержать полный набор данных, включая частные адреса и публичные адреса, доступные из частной сети. Для того, чтобы обеспечить согласованность работы серверов, они должны использовать общий набор данных, но доступная из публичной сети информация должна соответствующим образом фильтроваться. Реализация такого решения влечет за собой некоторое усложнение сервера имен.

6. Вопросы безопасности

В данной работе вопросы безопасности не рассматриваются.

---

[3] Такая проблема зачастую возникает при смене провайдера Internet. *Прим. перев.*

[4] В этом случае для смены адресов не потребуется заново настраивать каждый хост – достаточно будет лишь заменить блок распределяемых адресов на сервере DHCP. *Прим. перев.*

[5] В таких случаях может также возникать необходимость в изменении сетевых соединений на физическом уровне.

[6] Современные средства поддержки VLAN позволяют достаточно легко решить эту проблему. *Прим. перев.*

7. Заключение

При использовании описанной в документе схемы даже крупным предприятиям требуются сравнительно небольшие блоки публичных адресов IP. В результате существенно снижается острота проблемы нехватки адресов в Internet и обеспечивается более эффективное использование уникальных в масштабах Сети адресов IP. Предприятие получает возможность гибкого распределения адресов из любого частного блока. Однако использование частных адресов в сети предприятия может потребовать замены адресов для части хостов при подключении корпоративной сети к Internet или другим IP-сетям.

8. Благодарности

Авторы выражают свою признательность Tony Bates (MCI), Jordan Becker (ANS), Hans-Werner Braun (SDSC), Ross Callon (Bay Networks), John Curran (BBN Planet), Vince Fuller (BBN Planet), Tony Li (Cisco Systems), Anne Lord (RIPE NCC), Milo Medin (NSI), Marten Terpstra (Bay Networks), Geza Turchanyi (RIPE NCC), Christophe Wolfhugel (Pasteur Institute), Andy Linton (connect.com.au), Brian Carpenter (CERN), Randy Bush (PSG), Erik Fair (Apple Computer), Dave Crocker (Brandenburg Consulting), Tom Kessler (SGI), Dave Piscitello (Core Competence), Matt Crawford (FNAL), Michael Patton (BBN) и Paul Vixie (Internet Software Consortium) за их вклад в работу и конструктивные замечания.

9. Литература

[RFC1466] Gerich, E., "Guidelines for Management of IP Address Space", RFC 1466, Merit Network, Inc., May 1993.
[RFC1518] Rekhter, Y., T. Li, "An Architecture for IP Address Allocation with CIDR", RFC 1518, September 1993.
[RFC1519] Fuller, V., Li, T., Yu, J., K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", RFC 1519, September 1993.

10. Адреса авторов

Yakov Rekhter
Cisco systems
170 West Tasman Drive
San Jose, CA, USA
Phone: +1 914 528 0090
Fax: +1 408 526-4952
EMail: yakov@cisco.com

Robert G Moskowitz
Chrysler Corporation
CIMS: 424-73-00
25999 Lawrence Ave
Center Line, MI 48015
Phone: +1 810 758 8212
Fax: +1 810 758 8173
EMail: rgm3@is.chrysler.com

Daniel Karrenberg
RIPE Network Coordination Centre
Kruislaan 409
1098 SJ Amsterdam, the Netherlands
Phone: +31 20 592 5065
Fax: +31 20 592 5090
EMail: Daniel.Karrenberg@ripe.net

Geert Jan de Groot
RIPE Network Coordination Centre
Kruislaan 409
1098 SJ Amsterdam, the Netherlands
Phone: +31 20 592 5065
Fax: +31 20 592 5090
EMail: GeertJan.deGroot@ripe.net

Eliot Lear
Mail Stop 15-730
Silicon Graphics, Inc.
2011 N. Shoreline Blvd.
Mountain View, CA 94043-1389
Phone: +1 415 960 1980
Fax: +1 415 961 9584
EMail: lear@sgi.com

Перевод на русский язык
Николай Малых
nmalykh@bilim.com