Internet Engineering Task Force (IETF)
Request for Comments: 8992
Category: Informational
ISSN: 2070-1721

S. Jiang, Ed.
Huawei Technologies Co., Ltd
Z. Du
China Mobile
B. Carpenter
Univ. of Auckland
Q. Sun
China Telecom

May 2021

Autonomic IPv6 Edge Prefix Management in Large-Scale Networks

Управление граничными префиксами IPv6 в больших сетях

Аннотация

Этот документ задаёт две автономных технических задачи для управления префиксами IPv6 на границе больших сетей ISP с расширением для поддержки префиксов IPv4. Важным назначением документа является его использование для проверки устройства различных компонентов автономной (самоуправляемой) сетевой инфраструктуры.

Статус документа

Документ не содержит какой-либо спецификации (Internet Standards Track) и публикуется с информационными целями.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Не все документы, одобренные IESG, претендуют на статус стандартов Internet, дополнительную информацию о стандартах можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8992.

Оглавление

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

1. Введение

Исходным назначением этого документа была проверка устройства инфраструктуры автономных сетей (Autonomic Networking Infrastructure или ANI) для реалистических вариантов использования. Показаны возможные применения ANI для выделения префиксов IP и описаны подходы к построению систем для этого. Полностью стандартизованное решение потребует более детальной проработки, поэтому документ имеет статус информационного.

Документ определяет две автономных технических задачи для управления префиксами IPv6 в больших сетях с расширением для поддержки префиксов IPv4. Основы автономных сетей описаны в [RFC7575] и [RFC7576]. Базовый протокол автономной сигнализации (GeneRic Autonomic Signaling Protocol или GRASP) описан в [RFC8990] и может использовать технические задачи для разработки решения по автономному управлению префиксами. Важной целью этого документа является его использование для проверки устройства GRASP и других компонентов ANI, как описано в [RFC8993].

Документ не является полной функциональной спецификацией системы автономного управления префиксами и не описывает детали параметров задач GRASP и процедур автономных агентов служб (Autonomic Service Agent или ASA), требуемых для построения полной системы. Вместо этого описана архитектурная модель, использующая компоненты ANI, варианты и аспекты развёртывания, а также определены задачи GRASP, применяемые для построения системы. Приведены также примеры основных параметров.

Документ не рассматривает все варианты управления префиксами IPv6. Фактически предполагается, что основные элементы инфраструктуры уже имеют адреса и префиксы. Документ посвящён вопросам максимально автономного управления префиксами на границах большой сети. Это специально рассчитано на сети поставщиков услуг Internet (Internet Service Provider или ISP). Хотя между ISP и крупными корпоративными сетями имеется сходство, требования для этих случаев различаются. В любом варианте область действия решения предполагается ограниченной одним доменом управления, как в любой автономной сети.

Решение является достаточно общим, но вопросы его применения за пределами управления граничными префиксами, включая некоторые или все инфраструктурные префиксы, оставлены для будущего обсуждения. Полное решение включает множество аспектов, не рассматриваемых здесь. После назначения префиксов маршрутизаторам нужно сообщать о них системе маршрутизации по мере их ввода в эксплуатацию, а при освобождении префиксов нужно исключать их из маршрутизации. У разных операторов могут применяться разные правила в части срока действия префиксов, а также централизованные или распределенные пулы свободных префиксов. В автономных сетях эти свойства определяются устройством соответствующих агентов ASA.

Задачи GRASP являются просто блоками построения системы.

Отдельный риск распределенного назначения префиксов в больших сетях заключается в том, что со временем это может приводить к фрагментации адресного пространства и ненужному росту внутренних таблиц маршрутизации. Степень этого риска зависит от алгоритмов и правил, применяемых в ASA. Снижение риска может даже само стать автономной функцией.

2. Терминология

Ключевые слова **должно** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

В этом документе применяется терминология, заданная в [RFC7575].

3. Постановка задачи

Рассматриваемым здесь примером использования автономных сетей является автономное управление префиксами IPv6 на границе больших сетей ISP.

Хотя делегирование префиксов (DHCPv6 Prefix Delegation или DHCPv6-PD) [RFC8415] поддерживает автоматическое делегирование префиксов IPv6 одним маршрутизатором для другого, управление префиксами во многом зависит от планирования людьми. Иными словами, не существует базовой информации или правил для автономного принятия решений о размере префиксов, которые каждый маршрутизатор должен запрашивать или получать в зависимости от его роли в сети. Роли могут задаваться для отдельных устройств или быть базовыми (граничный маршрутизатор, внутренний маршрутизатор и т. п.). Кроме того, управление префиксами IPv6, выполняемое людьми, после исходного планирования часто бывает жёстким и статичным.

Задача, которую нужно решать автономным сетям, заключается в динамическом управлении адресным пространством IPv6 больших сетей с обеспечением эффективного использования адресов IPv6. Здесь задача сужена до назначения префиксов на границе сети вблизи маршрутизаторов доступа, поддерживающих отдельных абонентов с фиксированным подключением, мобильных клиентов и корпоративных абонентов. Предполагается, что в инфраструктуре ядра сети уже имеются должным образом назначенные префиксы. Рассматриваемый здесь подход автономных сетей основан на допущении о наличии базового протокола обнаружения и согласования, позволяющего прямое согласование между интеллектуальными маршрутизаторами IP. Протокол GRASP [RFC8990] предназначен для решения подобных задач.

3.1. Предполагаемый опыт пользователей и администраторов

Для администраторов больших сетей предполагается, что управление адресным пространством на границе сети можно осуществляться с минимальными усилиями, поскольку устройства на границе сети добавляются и удаляются, а клиенты всех типов присоединяются к сети и покидают её. В идеальном варианте администратору достаточно задать 1 префикс IPv6 для всей сети и начальный размер префикса для каждой роли устройств. Что касается пользователей,

назначение префиксов происходит как в любой другой сети. Фактическое использование префиксов нужно регистрировать для возможных операций автономного управления, включая аудит и отслеживание инцидентов.

3.2. Анализ параметров и информации

Для конкретных целей управления адресами каждое граничное устройство реализует несколько параметров, часть которых может настраиваться до подключения.

- Идентификация, проверка подлинности и полномочий данного устройства. Предполагается, что для этого будет применяться процесс защищённой начальной загрузки в автономной сети [RFC8995], после чего устройство сможет безопасно участвовать в автономных операциях.
- Роль устройства (см. примеры в параграфе 6.1).
- Размер префикса IPv6 для этого устройства.
- Префикс IPv6, назначенный этому устройству и устройствам нисходящего направления.

Сеть в целом будет реализовать указанные ниже параметры.

- Отождествление привязки доверия, являющейся удостоверяющим центром (certification authority или CA), поддерживаемым администраторами сети, который используется в процессе защищённой начальной загрузки.
- Общее пространство адресов IPv6, доступных для граничных устройств (1 или несколько префиксов IPv6).
- Исходный размер префикса для каждой роли устройств.

3.2.1. Параметры, которые устройство может задавать для себя

В этом параграфе выделены те из перечисленных выше параметров, которым не нужны внешние сведения для установки соответствующими устройствами подходящих значений, принятых по умолчанию, после начальной загрузки или сбоя в сети.

- Принятая по умолчанию роль устройства.
- Принятый по умолчанию размер префикса IPv6 для устройства.
- Криптографическое отождествление устройства, требуемое для защищённой начальной загрузки [RFC8995].

Производитель может поставлять устройства с настроенной ролью и принятым по умолчанию размером префикса, которые можно изменить с помощью автономного механизма. Криптографическое отождествление задаёт производитель.

3.2.2. Сведения, требуемые для сетевых операций

В этом параграфе указаны параметры, которые могут потребовать оперативного вмешательства для установки значений, отличных от заданных по умолчанию.

- Размер префикса IPv6 для устройства. Значение должно задаваться в соответствии с ролью устройства.
- Исходный размер префикса для каждой роли устройств.
- Возможность устройства запрашивать дополнительные адреса.
- Правила, связанные с запросом дополнительных адресов, например, запрос при использовании определённого числа или доли выделенных ранее адресов.

3.2.3. Сравнение с имеющимися решениями

В этом параграфе приведено краткое сравнение приведённого выше варианта с имеющимися решениями. В настоящее время управление адресами по-прежнему полагается в основном на планирование людьми, а после начального планирования является жёстким и статичным. Запросы адресов будут отвергаться, если пространство адресов исчерпано.

Некоторые функции автономного и динамического управления адресами можно реализовать путём расширения имеющихся протоколов, например, DHCPv6-PD [RFC8415] для запроса префиксов IPv6 в соответствии с ролью устройства. Однако задание унифицированных ролей устройств может оказаться не совсем практичным, поскольку некоторые функции невозможно настроить по ролям с помощью имеющихся протоколов делегирования префиксов.

Преимущество применения базового протокола обнаружения и согласования вместо конкретных решений заключается в возможности включения дополнительных параметров в автономное решение без создания новых механизмов. Это является основным аргументом в пользу базового (общего) подхода.

3.3. Взаимодействие с другими устройствами

3.3.1. Сведения, требуемые от других устройств

В этом параграфе указаны те из вышеупомянутых параметров, которым нужны внешние сведения от соседних устройств (включая устройства восходящего направления). Во многих случаях для установки или оптимизации значений нужен диалог с соседним устройством.

- Сведения об отождествлении привязки доверия.
- Необходимость обнаружения устройства, от которого можно получить адреса IPv6.
- Сведения о начальном размере префикса для каждой роли устройств, особенно для устройств нисходящего направления относительно данного устройства.

- Принятое по умолчанию значение размера префикса IPv6 может быть переопределено.
- Устройству требуется запросить и получить 1 или несколько префиксов IPv6 для себя и своих устройств нисходящего направления.
- Устройство может отвечать на запросы делегирования префиксов от устройств нисходящего направления.
- Устройству может потребоваться выделение дополнительного пространства адресов IPv6, если прежние уже исчерпаны.

3.3.2. Мониторинг, диагностика и отчёты

В этом параграфе рассмотрены роли устройств в процессах мониторинга, диагностики отказов и отчётности.

- Фактическое назначение адресов нужно регистрировать для возможных автономных операций управления.
- В общем случае сведения об использовании адресного пространства следует сообщать сетевым администраторам в абстрактной форме, например, в виде статистики или визуализации.
- Следует сообщать о предсказуемом исчерпании адресного пространства.

4. Решение для автономного управления граничными префиксами

В этом разделе описаны компоненты решения для автономного управления префиксами на границе сети. Как отмечено в разделе 1, это не является полным описанием решений, которое будет зависеть от деталей реализации соответствующих агентов ASA. Используется базовый протокол обнаружения и согласования, заданный в [RFC8990]. Соответствующие задачи GRASP определены в разделе 5.

Описанные ниже процедуры выполняются агентом ASA в каждом устройстве, вовлечённом в решение. Далее они называются PrefixManager ASA.

4.1. Поведение устройства, запрашивающего префикс

Если устройство с PrefixManager ASA исчерпало свой пул адресов, оно может запросить дополнительные адреса для распределения. Устройству следует определить размер запрашиваемого префикса и запросить его с помощью механизма, описанного в разделе 6. Хотя устройство может задавать принятый по умолчанию размер выделения, значение этого размера может меняться динамически и устройство может запрашивать больше или меньше адресов, руководствуясь локальной эвристикой.

Агенту PrefixManager ASA, нуждающемуся в дополнительном пространстве адресов, следует сначала найти партнёров, которые могут предоставить такие адреса. ASA следует передать сообщение GRASP Discovery с опцией PrefixManager Objective (см. раздел 2 в [RFC8650] и параграф 5.1) для нахождения партнёров, поддерживающих эту опцию. Затем следует выбрать одного из таких партнёров (скорей всего, ответившего первым).

Если сообщение GRASP Discovery Response содержит опцию Divert, указывающую PrefixManager ASA вне канала, запрашивающий агент ASA может инициировать согласование с указанным ASA для определения возможности получить префикс запрошенного размера.

В любом случае запрашивающий агент ASA выступает инициатором согласования GRASP путём отправки сообщения GRASP Request с опцией PrefixManager Objective, указывая в ней размер запрашиваемого префикса. Это запускает процесс согласования GRASP.

В процессе согласования агент ASA будет на каждом шаге решать, следует ли принимать предложенный префикс. Это решение зависит от реализации как и решение о завершении согласования.

Как вариант, ASA может инициировать обнаружение GRASP в ускоренном (rapid) режиме с вложенным запросом согласования, если это реализовано.

4.2. Поведение устройства, предоставляющего префикс

Хотя бы одно устройство в сети должно быть настроено с исходным пулом доступных префиксов, отмеченным в параграфе 3.2. Кроме того, поставщиком префиксов может служить любое устройство.

Устройству, получившему сообщение Discovery с опцией PrefixManager Objective, следует передавать в ответ сообщение GRASP Response, если это устройство включает PrefixManager ASA. Дополнительные сведения о процессе обнаружения приведены в [RFC8990]. Когда этот агент ASA получает последующее сообщение Request, ему следует выполнить последовательность согласования GRASP, используя сообщения Negotiate, Confirm Waiting, Negotiation End. Сообщения Negotiate содержат опцию PrefixManager Objective, которая указывает префикс, предлагаемый запрашивающему ASA, и размер этого префикса. Как указано в [RFC8990], согласование продолжается, пока любая из сторон не передаст сообщение Negotiation End. Если согласование успешно, агент ASA, предоставивший префикс, удаляет согласованный префикс из своего пула, а запрашивающий ASA добавляет его себе. При отказе согласования сторона, передающая сообщение Negotiation End, может включить в него строку кода ошибки.

В процессе согласования ASA на каждом этапе решает, какого размера префикс следует предлагать. Это решение, равно как и решение о завершении согласования, зависит от реализации.

Как вариант, ASA может выполнять согласование в ответ на обнаружение GRASP в ускоренном (rapid) режиме, если он это реализует.

Эта спецификация не зависит от встраивания всех PrefixManager ASA в маршрутизаторы, но это вполне естественный сценарий. В иерархической топологии сети данный маршрутизатор обычно предоставляет префиксы маршрутизаторам нижележащего уровня иерархии и, скорей всего, содержит первый агент PrefixManager ASA, обнаруживаемый этими маршрутизаторами. Однако модель обнаружения GRASP включает функцию перенаправления, делающую этот вариант неисключительным и нисходящий PrefixManager ASA может согласовать новый префикс с устройством, отличным от вышестоящего маршрутизатора.

Нехватка ресурсов может приводить шлюзовой маршрутизатор к запросу дополнительных ресурсов у своего вышестоящего устройства, что ведёт к созданию независимого процесса обнаружения и согласования GRASP. Во время этого процесса шлюзовому маршрутизатору следует передавать сообщение Confirm Waiting маршрутизатору, создавшему исходный запрос, для расширения времени ожидания. Когда ресурс станет доступным, шлюзовой маршрутизатор отвечает сообщением GRASP Negotiate с размером префикса, соответствующим запросу.

Алгоритм выбора префикса на предоставляющих префиксы устройствах зависит от реализации.

4.3. Поведение после успешного согласования

После получения сообщения GRASP Negotiation End, указывающего наличие префикса приемлемого размера, запрашивающее устройство может использовать согласованный префикс без дополнительных сообщений.

В некоторых случаях управление префиксами на основе ANI/GRASP может работать вместе с DHCPv6-PD [RFC8415] как дополнение. Например, метод на основе ANI/GRASP можно использовать внутри домена, а DHCPv6-PD - вне (т. е. через административную границу). Можно также применять ANI/GRASP внутри домена, а DHCP/DHCPv6-PD - на границе домена для клиентов (не ANI). Другим примером является применение внутри домена ANI/GRASP, а RADIUS [RFC2865] - для предоставления префиксов устройствам клиентов.

4.4. Регистрация префиксов

В автономной системе управления префиксами все назначения префиксов выполняются устройствами без участия человека. Может потребоваться регистрация всей истории назначения префиксов, например, для обнаружения и отслеживания потерянных префиксов после отказов или для исполнений юридических требований. Однако процессы регистрации и отчётности выходят за рамки этого документа.

5. Задачи автономного управления префиксами

В этом разделе определяются опции технических задач GRASP для поддержки автономного управления префиксами.

5.1. Опция Edge Prefix Objective

Опция PrefixManager Objective является опцией GRASP Objective, соответствующей спецификации GRASP [RFC8990]. Она имеет имя PrefixManager (см. радел 8) и передаёт в своём значении размер и фактические биты префикса. Поскольку протокол GRASP основан на кратком представлении двоичных объектов (Concise Binary Object Representation или CBOR) [RFC8949], формат опции PrefixManager Objective на языке краткого определения данных (Concise Data Definition Language или CDDL) [RFC8610] имеет вид

```
objective = ["PrefixManager", objective-flags, loop-count,
             [length, ?prefix]]

loop-count = 0..255          ; как в спецификации GRASP
objective-flags /=           ; как в спецификации GRASP
length = 0..128              ; размер запрошенного или предложенного префикса
prefix = bytes .size 16      ; предложенный префикс в двоичном формате
```

Использование режима пробного прогона (dry run) в GRASP **не рекомендуется** для этой цели, поскольку он потребует от обоих агентов ASA сохранять сведения о состоянии для соответствующего согласования, что не даёт реальной пользы - запрашивающий ASA не может основывать какие-либо решения на основе успеха пробного согласования.

5.2. Расширение для IPv4

Ниже представлена расширенная версия задачи PrefixManager, поддерживающая IPv4 за счёт добавления флага.

```
objective = ["PrefixManager", objective-flags, loop-count, prefval]

loop-count = 0..255          ; как в спецификации GRASP
objective-flags /=           ; как в спецификации GRASP

prefval /= pref6val
pref6val = [version6, length, ?prefix]
version6 = 6
length = 0..128              ; размер запрошенного или предложенного префикса
prefix = bytes .size 16      ; предложенный префикс в двоичном формате

prefval /= pref4val
pref4val = [version4, length4, ?prefix4]
version4 = 4
length4 = 0..32              ; размер запрошенного или предложенного префикса
prefix4 = bytes .size 4      ; предложенный префикс в двоичном формате
```

Управление префиксами и адресами IPv4 существенно сложнее, чем для IPv6, в связи с распространённостью NAT, неоднозначностью адресов [RFC1918] и совместным использованием адресов [RFC6346]. Эти сложности могут потребовать дальнейшего расширения задачи с добавлением полей, не описанных в этом документе.

6. Параметры управления префиксами

Реализация менеджера префиксов **должна** включать принятые по умолчанию значения всех требуемых параметров. Однако внутри одного административного домена оператор сети **может** менять принятые по умолчанию параметры для всех устройств в той или иной роли. Таким образом, можно применять нужную политику для каждого устройства простым способом без традиционных файлов конфигурации. Как отмечено в параграфе 4.1, отдельные автономные устройства также могут динамически менять своё поведение. Например, оператор **может** изменить принятый по умолчанию размер префикса для каждого типа ролей. Задачу управления размерами префиксов, которая включает сведения о сопоставлении роли устройства с принятым по умолчанию размером префикса, можно лавинно разослать через сеть с использованием автономной плоскости управления (Autonomic Control Plane или ACP) [RFC8994].

```
    objective = ["PrefixManager.Params", objective-flags, any]

    loop-count = 0..255          ; как в спецификации GRASP
    objective-flags /=           ; как в спецификации GRASP
```

Объект any представляет определения соответствующих параметров (как в примере ниже), передаваемых как объект CBOR в подходящем формате. Это можно лавинно разослать всем узлам и любой агент PrefixManager ASA, не получивший сообщение по какой-либо причине, сможет получить копию через индивидуальную синхронизацию GRASP. При получении параметров управления префиксами каждое устройство может выбрать принятый по умолчанию размер префикса в соответствии со своей ролью.

6.1. Пример параметров управления префиксами

Параметры содержат сведения о ролях устройств и принятых на них по умолчанию размерах префиксов в автономном домене. Предположим, например, что оператор сети радио-доступа (IP Radio Access Network или IPRAN) хочет задать для контроллера радиосети (Radio Network Controller Site Gateway или RSG) размер префикса 34, для шлюза агрегирования (Aggregation Site Gateway или ASG) - 44, а для шлюза сотового узла (Cell Site Gateway или CSG) - 56. Это можно описать значение цели PrefixManager.Params в виде

```
[
   [["role", "RSG"],["prefix_length", 34]],
   [["role", "ASG"],["prefix_length", 44]],
   [["role", "CSG"],["prefix_length", 56]]
]
```

Пример представлен в формате JSON [RFC8259], который легко перевести в CBOR. Можно представить параметры в форме YANG [RFC7950], используя отображение YANG в CBOR [CORE-YANG-CBOR].

Для наглядности ниже представлен вариант топологии, который может служить примером использования описанного в документе механизма.

Сеть IPRAN служит для транзитной мобильной связи, включая базовые станции, контроллеры радиосети (Radio Network Controller или RNC) для 3G или пакетное ядро для LTE и сеть IP между ними, как показано на рисунке 1. Объекты eNB (Evolved Node B), RNC, SGW (Serving Gateway) и MME (Mobility Management Entity) являются элементами сети, определёнными в 3GPP. Элементы CSG, ASG и RSG определены в решении IPRAN. Топология IPRAN на рисунке 1 включает кольца Ring1 (ASG1->RSG1->RSG2->ASG2->ASG1), Ring2 (CSG1->ASG1->ASG2->CSG2->CSG1) и Ring3 (CSG3->ASG1->ASG2->CSG3). В реальном развёртывании IPRAN может быть больше станций, колец и маршрутизаторов, а сеть обычно зависит от проектирования и настройки с участием людей, что не обеспечивает ни гибкости, ни экономической эффективности.

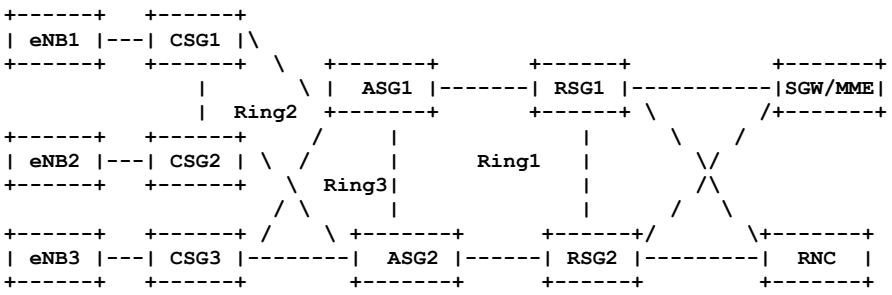

Рисунок 1. Топология сети IPRAN.

Если IPRAN поддерживает ANI/GRASP, узлам сети сети следует выполнять согласование между собой и принимать автономные решения в соответствии со своим статусом и собранными из сети сведениями. Параметры управления префиксами следует включать в обмен информацией. Маршрутизаторам следует знать роли своих соседей, принятый по умолчанию размер префикса для каждой роли и т. п. Шлюзам ASG следует поддерживать запросы префиксов у RSG, а шлюзам CSG - у ASG. В каждом запросе шлюзам ASG и CSG следует указывать размер префикса или свою роль для запроса префикса принятого по умолчанию размера.

7. Вопросы безопасности

Соответствующие вопросы безопасности рассмотрены в [RFC8990]. Предпочтительной моделью защиты является доверие к устройствам в соответствии с процедурой защищённой загрузки [RFC8995] и наличие защищённой плоскости ACP [RFC8994].

При использовании DHCPv6-PD **рекомендуется** применять аутентификацию DHCPv6 или Secure DHCPv6.

8. Взаимодействие с IANA

Этот документ определяет 2 новые опции GRASP Objective: PrefixManager и PrefixManager.Params. Агентство IANA добавило их в реестр GRASP Objective Names, заданный в [RFC8990].

9. Литература

9.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

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

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

[RFC8990] Bormann, C., Carpenter, B., Ed., and B. Liu, Ed., "GeneRic Autonomic Signaling Protocol (GRASP)", RFC 8990, DOI 10.17487/RFC8990, May 2021, <https://www.rfc-editor.org/info/rfc8990>.

[RFC8994] Eckert, T., Ed., Behringer, M., Ed., and S. Bjarnason, "ACK Autonomic Control Plane (ACP)", RFC 8994, DOI 10.17487/RFC8994, May 2021, <https://www.rfc-editor.org/info/rfc8994>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

9.2. Дополнительная литература

[CORE-YANG-CBOR] Veillette, M., Ed., Petrov, I., Ed., and A. Pelov, "CBOR Encoding of Data Modeled with YANG", Work in Progress[1], Internet-Draft, draft-ietf-core-yang-cbor-15, 24 January 2021, <https://tools.ietf.org/html/draft-ietf-core-yang-cbor-15>.

[DHCP-YANG-MODEL] Liu, B., Ed., Lou, K., and C. Chen, "Yang Data Model for DHCP Protocol", Work in Progress, Internet-Draft, draft-liu-dhc-dhcp-yang-model-07, 12 October 2018, <https://tools.ietf.org/html/draft-liu-dhc-dhcp-yang-model-07>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, DOI 10.17487/RFC3046, January 2001, <https://www.rfc-editor.org/info/rfc3046>.

[RFC6221] Miles, D., Ed., Ooghe, S., Dec, W., Krishnan, S., and A. Kavanagh, "Lightweight DHCPv6 Relay Agent", RFC 6221, DOI 10.17487/RFC6221, May 2011, <https://www.rfc-editor.org/info/rfc6221>.

[RFC6346] Bush, R., Ed., "The Address plus Port (A+P) Approach to the IPv4 Address Shortage", RFC 6346, DOI 10.17487/RFC6346, August 2011, <https://www.rfc-editor.org/info/rfc6346>.

[RFC7575] Behringer, M., Pritikin, M., Bjarnason, S., Clemm, A., Carpenter, B., Jiang, S., and L. Ciavaglia, "Autonomic Networking: Definitions and Design Goals", RFC 7575, DOI 10.17487/RFC7575, June 2015, <https://www.rfc-editor.org/info/rfc7575>.

[RFC7576] Jiang, S., Carpenter, B., and M. Behringer, "General Gap Analysis for Autonomic Networking", RFC 7576, DOI 10.17487/RFC7576, June 2015, <https://www.rfc-editor.org/info/rfc7576>.

[RFC8650] Voit, E., Rahman, R., Nilsen-Nygaard, E., Clemm, A., and A. Bierman, "Dynamic Subscription to YANG Events and Datastores over RESTCONF", RFC 8650, DOI 10.17487/RFC8650, November 2019, <https://www.rfc-editor.org/info/rfc8650>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

[RFC8993] Behringer, M., Ed., Carpenter, B., Eckert, T., Ciavaglia, L., and J. Nobre, "A Reference Model for Autonomic Networking", RFC 8993, DOI 10.17487/RFC8993, May 2021, <https://www.rfc-editor.org/info/rfc8993>.

Приложения A. Обзор внедрения

В этом приложении приведены логические модели развёртывания и пояснения к целевым моделям для облегчения понимания описанных в документе механизмов.

Параграф A.1 посвящён двум наиболее распространенным моделям развёртывания DHCP, параграф A.2 - модели PD, описанной в этом документе. Следует отметить, что на практике применяется большее число моделей.

A.1. Управление адресами и префиксами через DHCP

Развёртывание граничного сервера DHCP требует, чтобы каждый маршрутизатор, соединённый с устройствами на стороне клиента (Customer Premises Equipment или CPE), был сервером DHCP выделяющий адреса IPv4/IPv6 устройствам CPE и, возможно, префиксы IPv6 через DHCPv6-PD для поддерживающих IPv6 устройств CPE, являющихся маршрутизаторами, за которыми размещены ЛВС.

Это требует выполнения различных конфигурационных функций через некую внутреннюю (backend) систему (сервер конфигурации на рисунке 2). Число адресных префиксов на граничных интерфейсах следует поддерживать с некоторым запасом - больше числа подключённых CPE, чтобы адресное пространство использовалось эффективно.

[1]Опубликовано в RFC 9254. *Прим. перев.*

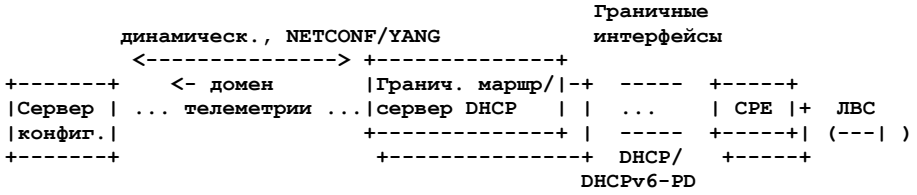

Рисунок 2. Модель развёртывания DHCP без центрального сервера.

Сервер конфигурации должен предоставить адресные префиксы краевых интерфейсов и параметры DHCP для каждого граничного маршрутизатора. Использование слишком мелких префиксов ведёт к росту таблиц маршрутизации в домене, показанном на рисунке, а использование больших префиксов ведёт к избыточному расходу адресов. Это не очень актуально для IPv6, но при включении в модель IPv4 проблема становится серьёзной. Нет стандарта, описывающего алгоритмы, с помощью которых серверы конфигурации могли бы наилучшим способом выполнять такую динамическую настройку для оптимизации размера таблиц маршрутизации и эффективного использования адресного пространства. В настоящее время нет полной модели данных YANG, которую сервер конфигурации мог бы использовать для выполнения этих действий (включая телеметрию адресов, назначенных распределенными серверами DHCP). Например, модель данных YANG для управления операциями сервера DHCP находится в стадии разработки [DHCP-YANG-MODEL].

В связи с упомянутыми и другими проблемами применяется описанная ниже модель развёртывания DHCP.

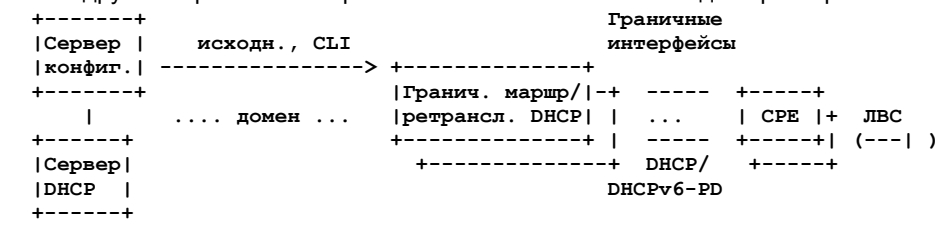

Рисунок 3. Модель развёртывания DHCP с центральным сервером.

Распространение динамических изменений граничным маршрутизаторам исключается за счёт использования центрального сервера DHCP и смены роли граничного маршрутизатора с сервера на ретранслятор DHCP. Конфигурация граничных маршрутизаторов остаётся статичной. Функция ретранслятора DHCP включает граничный интерфейс и/или опции идентификации абонента в запросы DHCP от устройств CPE (например, [RFC3046] [RFC6221]), а у сервера DHCP имеются полные правила назначения адресов и префиксов для каждого граничного маршрутизатора, интерфейса, группы абонентов. Когда ретранслятор DHCP видит отклик DHCP, он вставляет статические маршруты для назначенных адресов и префиксов в таблицу граничного маршрутизатора и эти маршруты распространяются протоколом IGP (или BGP) внутри домена, чтобы все CPE и ЛВС были доступны через домен, показанный на рисунке.

Полной стандартизации таких решений не существует. Например, в параграфе 19.1.3 [RFC8415] просто говорится о «(неопределённом) протоколе или ином обмене по отдельному каналу (out-of-band) для настройки маршрутной информации для делегированных префиксов на любом маршрутизаторе, через который клиент может пересылать трафик».

A.2. Управление префиксами через ANI/GRASP

Для вариант использования ANI и агентов ASA, управляющих префиксами (PM-ASA) с помощью GRASP, модель развёртывания показана на рисунке 4.

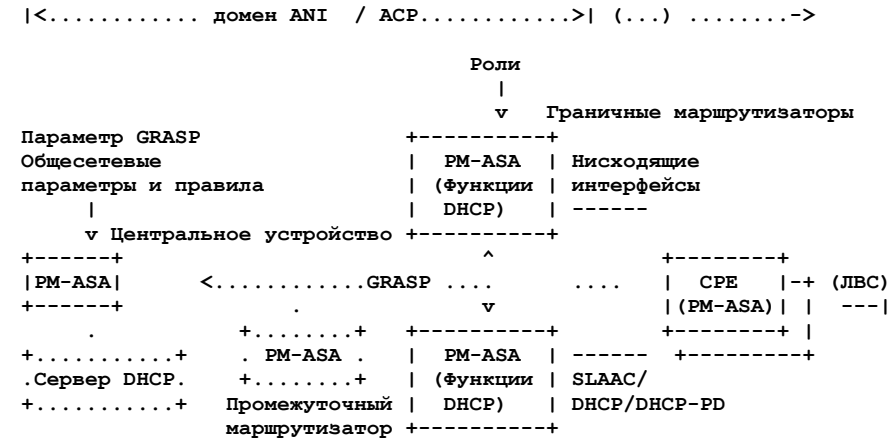

Рисунок 4. Модель развёртывания с использованием ANI/GRASP.

В сети применяется домен ANI с ACP [RFC8994] между центральным устройством (например, маршрутизатором или устройством управления с поддержкой ANI) и граничными маршрутизаторами. ANI/ACP предоставляет создаваемый автоматически (zero-touch) канал связи между устройствами и разрешает использовать протокол GRASP [RFC8990] не только для взаимодействия партнёров, но и для распространения и лавинной рассылки информации.

На центральном устройстве и граничных маршрутизаторах используются программные агенты ASA для поддержки описанных в этом документе функций автономного управления префиксами IPv6 на границе. Агенты PM-ASA совместно обеспечивают функцию автономного управления префиксами, как описано ниже.

Граничные маршрутизаторы могут исполнять разные роли в зависимости от типа и числа присоединённых устройств CPE. Каждый граничный маршрутизатор может быть RSG, ASG или CSG в сетях агрегирования мобильных устройств (см. параграф 6.1). Механизмы осознания маршрутизаторами своей роли выходят за рамки этого документа.

Ниже приведены некоторые соображения, связанные с моделью развёртывания.

1. В решении с минимальным управлением префиксами центральное устройство использует описанную в этом документе задачу GRASP PrefixManager.Params для распространения параметров граничным маршрутизаторам сети в соответствии с их ролями. Агент PM-ASA использует параметры, относящиеся к его роли для локальной настройки функций имеющейся адресации. Поскольку PM-ASA не управляет динамическим назначением фактических префиксов IPv6, можно рассмотреть указанные ниже варианты:

   1.a Граничный маршрутизатор соединяется через интерфейсы нисходящего направления с каждым (хостом) CPE, которому нужен адрес. PM-ASA устанавливает для каждого такого интерфейса маршрутизатор, запрашивающий DHCP (в соответствии с [RFC8415]) для запроса префикса IPv6 для интерфейса. Адрес маршрутизатора на нисходящем интерфейсе может быть параметром из задачи GRASP. CPE назначает адреса из префикса через анонсы маршрутизаторов (Router Advertisement или RA) или PM-ASA управляет локальным сервером DHCPv6 для назначения адресов устройствам CPE. Нужен центральный сервер DHCP, выполняющий функции делегирующего маршрутизатора DHCP (в соответствии с [RFC8415]). Его адрес может быть параметром из задачи GRASP.

   1.b Граничный маршрутизатор подключается через нисходящие интерфейсы к (управляемым клиентом) устройствам CPE, которые являются маршрутизаторами и запрашивают DHCPv6. Необходимость этого может выводиться из роли или параметров GRASP, а PM-ASA устанавливает функцию ретрансляции DHCP для пересылки запросов центральному серверу DHCP как в п. 1.a.

2. В решении без центрального сервера DHCP агенты PM-ASA на граничных маршрутизаторах не только изучают параметры из PrefixManager.Params, но и применяют GRASP для запроса и согласования фактического выделения префиксов IPv6 через задачу GRASP PrefixManager, как описано ниже. В простейшем случае префиксы делегируются через эту задачу GRASP от PM-ASA в центральном устройстве, которое должно изначально иметь большой пул адресов. Затем делегированные префиксы используются PM-ASA на граничных маршрутизаторах для настройки префиксов нисходящих интерфейсов с целью их назначения через RA/SLAAC хостам CPE. Агенты PM-ASA могут также запускать локальные серверы DHCP (как в п. 1.a) для назначения через DHCP адресов из выделенных префиксов устройствам CPE. Это включает хосты CPE, запрашивающие адреса IPv6 и маршрутизаторы CPE, которым нужны префиксы IPv6. Агентам PM-ASA нужно управлять пулами адресов, запрошенными через GRASP, и выделять части этих пулов интерфейсам и запущенным серверам DHCP. Они должны отслеживать использование адресов и в соответствии с этим запрашивать дополнительные префиксы при нехватке или возвращать ненужные адреса.

   Это решение весьма похоже на предыдущую модель развёртывания IPv6 DHCP без центрального сервера DHCP, а ANI/ACP/GRASP и PM-ASA обеспечивают автоматизацию позволяющую упростить этот подход.

3. Пулы адресов для выделения префиксов не обязательно брать из одного центрального узла. Агент PM-ASA на граничном маршрутизаторе, получивший большой (короткий) префикс от центрального PM-ASA, может предлагать более мелкие префиксы агентам PM-ASA в соседних маршрутизаторах. Протокол GRASP можно использовать так, чтобы агенты PM-ASA могли находить и выбирать задачи у ближайших соседних PM-ASA, что позволит максимизировать агрегирование. PM-ASA будет впоследствии запрашивать более мелкие префиксы, когда исчерпает свой пул (от центрального узла) и не сможет больше получить от того большой префикс. Поскольку дополнительные префиксы получаются от топологически ближайшего PM-ASA, число более длинных префиксов, включаемых в таблицы маршрутизации, будет ограничено и топологическая близость повышает шансы того, что агрегирование префиксов в IGP скорей всего ограничит область, в которой требуется маршрутизировать более длинные префиксы.

4. Вместо оптимизации делегирования префиксов между партнёрами (peer-to-peer) можно организовать иерархию PM-ASA (на рисунке 4 показан точками промежуточного маршрутизатора). Это потребует дополнительных параметров в задаче PrefixManager для построения иерархии PM-ASA, через которую можно делегировать префиксы.

5. В случаях, когда CPE являются частью домена ANI (например, управляемые CPE), GRASP будет распространяться на сайты фактических клиентов и сможет управлять PM-ASA. Все варианты, описанные в пп. 1 - 4, подойдут для CPE, выступающего граничным маршрутизатором, с некоторыми изменениями - (a) маршрутизатору CPE, скорей всего, не потребуется самому запускать DHCPv6-PD и достаточно назначать адреса DHCP и (b) граничные маршрутизаторы, к которым подключён CPE, скорей всего, будут идеальным местом для запуска иерархических экземпляров PD-ASA, как описано в п. 1.

Благодарности

Значимые комментарии были получены от William Atwood, Fred Baker, Michael Behringer, Ben Campbell, Laurent Ciavaglia, Toerless Eckert, Joel Halpern, Russ Housley, Geoff Huston, Warren Kumari, Dan Romascanu, Chongfeng Xie.

Адреса авторов

Sheng Jiang (editor)
Huawei Technologies Co., Ltd
Q14, Huawei Campus
No. 156 Beiqing Road
Hai-Dian District, Beijing
100095
China
Email: jiangsheng@huawei.com

Zongpeng Du
China Mobile
32 Xuanwumen West St
Xicheng District, Beijing

100053
China
Email: duzongpeng@chinamobile.com

Brian Carpenter
University of Auckland
School of Computer Science
PB 92019
Auckland 1142
New Zealand
Email: brian.e.carpenter@gmail.com

Qiong Sun
China Telecom
118 Xizhimennei St
Beijing
100035
China
Email: sunqiong@chinatelecom.cn

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru