ВЫБОР АДРЕСОВ IPV6

Н. Н. Диваков
Кафедра автоматизированных систем обработки информации, Гомельский государственный университет имени Франциска Скорины,физический факультет
Гомель, Республика Беларусь
E-mail: {divakov}divakovn@gmail.com

В системах, работающих одновременно с IPv4 и IPv6, процедура выбора адресов еще сложнее, и нужны правила, какие адреса предпочтительнее. Выбор адресов может быть между IPv4 и IPv6, адресами с различными зонами действия (scopes), публичными и частными адресами и т.д.. Некоторые правила представляются очевидными, например, выбор адреса, использование которого не запрещено, но программа должна делать правильный выбор в любом варианте. Вообще, пары адресов отправителя и получателя должны иметь согласованные области действия и типы (scopes) (напр., местный IPv6, 6to4, или IPv4-mapped), следует предпочитать меньшие зоны действия, местные адреса и т.д.

Введение

Окончание IPv4-адресов — истощение запаса адресов, которые были не распеделены, в системе адресации IPv4. Мировое адресное пространство глобально находится под управлением американской некоммерческой организацией IANA, а также пятью региональными интернет-регистраторами, которые отвечают за назначение IP-адресов конечным пользователям на определённых территориях, и локальными интернет-регистраторами, такими как интернет-провайдеры. IPv6 (англ. Internet Protocol version 6) — новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при её использовании в Интернете, за счёт использования длины адреса 128бит вместо 32. Протокол был разработан IETF.

Содержание документа

Система адресации IPv4, как правило, имеет один уникастный адрес, который может быть либо может и не быть глобально маршрутизируемым,а также адрес обратной связи (127.0.0.1).Отличием интерфейса IPv6 является наличие локального адреса обратной связи, локального адреса канала, уникального локального адреса и глобально маршрутизируемого адреса. Для большой сети необходимо использовать более одного адреса определенного типа. Не существует огранчений при присвоении дополнительных адресов.Для любого пакета существует выбор при использовании адреса отправителя, также существует возможность выбора и для адреса назначения. В системах, работающих одновременно с IPv4 и IPv6 необходимы еще более сложные действия для выбора предпочтительных адресов[2]. Одним из нововведений является таблица адресации, которая позволяет администраторам вводить новые и редактировать уже существующие правила выбора адресов. IPv4 адреса приведенные в таблице адресации, как IPv4-mapped IPv6-адреса, и они являются областью соотвествия адресам IPv6 локально-канальным или глобальным. В процессе присвоении адреса таблица анализируется и осуществляется поиск записи с наиболее длинным префиксом, соответствующему адресу. Далее приходит ответ с соответствующими значениями приоритета и меткой. Что в свою очередь позволяет обеспечить согласование меток отправителя и получателя и предпочтение родного IPv6 по отношению к IPv4 или различным туннельным адресам (6to4 или v4-совместимых)[3]. Первым действием в процессе выбора адреса отправителя является формирование списка кандидатов. Выбор необходимо согласовывать с интерфейсом и рабочей областью (scope). Следующим шагом является упорядочивание кандидатов, следуя списку правил, начиная с правила 1:

1. Предпочтителен адрес отправителя, который равен адресу места назначения.
2. Предпочтительная минимальная область действия, которая столь же велика, как и область места назначения. (Это правило является обязательным.)
3. Предпочтителен адрес, который не является нежелательным.
4. Предпочтителен домашний адрес, если только приложение не требует обратного.
5. Предпочтителен адрес исходящего интерфейса для данного места назначения.
6. Предпочтителен адрес, который соответствует метке места назначе-ния в таблице политики.
7. Предпочтителен публичный адрес по сравнению с временным адре-сом, если только приложение не требует обратного.
8. Использовать адрес с наиболее длинным префиксом, общим с адре-сом места назначения.

Когда осуществляется выбор адреса места назначения необходимо пользоваться таким же набором правил. Основым отличием является то, что выбор места назначения включает в себя запрос, какой отправитель будет использоваться в каждом из вариантов. Когда канал содер-

жит более одного маршрутизатора, или пограничный маршрутизатор соединен с более чем одним сервис-провайдером, может использоваться несколько префиксов. Еще одной причиной усложнения администрирования сети в IPv6 является перенумерация сайтов, то есть изменение префиксов. Таким образом префиксы в IPv6 не являются статичными. Наиболее частой причиной перенумерации сетевых префиксов является смена сервис-провайдера. Перенумерация может оказаться необходимой, когда компании с большими корпоративными сетями производят реорганизацию, или когда провайдер сам вынужден произвести перенумерацию. Перенумерация влияет на большое число компонент: маршрутизаторы, firewall, фильтры, DNS, DHCPv6, конфигурационные таблицы системы, приложения, программы управления сетью[1]. Так как интерфейсы могут получить адреса с новыми префиксами и они не осуществляют перенумерацию, RFC-4192 содержит описание шагов, которые необходимо осуществить для обеспечения нормальной работы сети. Процесс включает в себя выделение для каналов субпрефиксов новых префиксов и обновление адресов со старыми префиксами. Эта процедура включает в себя:

- ручное присвоение адресов интерфейсам маршрутизаторов;
- маршрутную информацию и префиксы каналов, анонсируемые маршрутизаторами;
- адреса маршрутизаторов, firewall и пакетных фильтров управления доступом;
- адреса, присвоенные интерфейсам посредством адресной автоконфигурации;
- адреса и другую информацию, предоставляемую DHCPv6;
- DNS-записи (AAAA и PTR-рекорды, а также DNSSEC);
- все другие случаи использования адресов, командных последовательностей, конфигурационных файлов.

Многие организации предпочитают получить блоки адресов /48. Это позволяет организации поддерживать до 65,000 субсетей. Существует три типа адресов:

- unicast: Идентификатор одиночного интерфейса. Пакет, посланный по уникастному адресу, доставляется интерфейсу, указанному в адресе;
- anycast: Идентификатор набора интерфейсов (принадлежащих разным узлам). Пакет, посланный по эникастному адресу, доставляется одному из интерфейсов, указанному в адресе (ближайший, в соответствии с мерой, определенной протоколом маршрутизации);
- multicast: Идентификатор набора интерфейсов (обычно принадлежащих разным узлам). Пакет, посланный по мультикастинг-адресу, доставляется всем интерфейсам, заданным этим адресом.

В IPv6 не существует широковещательных адресов, их функции переданы мультикастинг-адресам. В IPv6, все нули и все единицы являются допустимыми кодами для любых полей, если не оговорено исключение.

Заключение

Альтернативным протоколом автоматизации является SLAAC (Stateless Address AutoConfiguration. Он представляет собой нормальным путем получения динамических адресов IPv6, но он не предоставляет такой информации как адреса DNS и NTP серверов и не осуществляет динамических обнавлений DNS. SCAAC не предлагает также централизованного контроля присвоения адресов, который бывает необходим для некоторых сетевых операторов. DHCPv6 отслеживает присвоение адресов. DHCPv6 не описан в рамках IPv6-стандартов, но по мере расширения использования IPv6, нужда в DHCPv6 возрастает. Чтобы минимизировать угрозы при внедрении IPv6 рекомендуется предпринять следующее:

- чтобы ограничить доступ к адресной ситуации, следует использовать различные типы IPv6-адресации (частная адресация, уникальные локальные адреса, разбросанное выделение адресов и т.д.);
- чтобы усложнить сканирование сети, присваивать идентификаторы субсети и интерфейсов случайным образом;
- разработать для предприятия политику выборочной фильтрации ICMPv6. Важные для работы сети ICMPv6-сообщения должны быть доступны, остальные следует блокировать;
- использовать IPsec для аутентификации и конфиденциальности;
- идентифицировать возможные слабости в защите доступа к сети в среде IPv6;
- ввести проверки, которые могли быть не нужны при работе с IPv4 из-за низкого уровня угроз (в политике безопасности использовать запреты по умолчанию, а также активировать систему безопасности маршрутизации.
- уделить повышенное внимание аспектам безопасности для таких механизмов передачи, как протоколы туннелирования;
- для сетей, использующих исключительно IPv4, блокировать весь трафик IPv6.

1. Тихий ,Я. IPv6 для знатоков IPv4 / Я.Тихий // – М.:Axioma, 2008. – 256 с.
2. Нэйл, Р. М. IPv6. Администрирование сетей / Р. М. Нэйл, Д. Мэлоун – М.:КУДИЦ-Пресс, 2007. – 320 с.
3. Bieringer, P. Linux IPv6 HOWTO / Р. Медведев, // Вест. аритмол. – 2009. – 500 с.