

Модели маршрутизации на основе правил

Models of Policy Based Routing

1. Статус документа

Целью данного документа является рассмотрение различных моделей маршрутизации на основе правил (политики) и показать их относительные преимущества. Обсуждение и комментарии приводятся с целью определения лучшей модели маршрутизации на базе правил, обеспечивающей также достаточный уровень масштабирования в больших системах связанных между собой сетей.

Документ может распространяться свободно.

2. Благодарности

Автор выражает свою признательность Yakov Rekhter (IBM Research), Milo Medin (NASA), Susan Hares (Merit/NSFNET), Jessica Yu (Merit/NSFNET) и Dave Katz (Merit/NSFNET) за их важный вклад в подготовку этого документа.

3. Обзор

Для оценки методов и моделей маршрутизации на основе правил необходимо исследовать контекст, в котором эта модель будет использоваться, и наличие различных методов, введения правил. Чаще всего используются модели:

- **Policy based distribution of routing information** (распространение маршрутных данных на основе правил).
- **Policy based packet filtering/forwarding** (фильтрация/пересылка пакетов на основе правил).
- **Policy based dynamic allocation of network resources** (распределение сетевых ресурсов на основе правил).

Для выбора конкретного метода, используемого в том или ином приложении, нужно принимать во внимание сравнение отдельных свойств этих методов. В некоторых случаях приходится использовать несколько методов.

При сравнении различных моделей маршрутизации на основе правил важно понимать, что каждая модель разработана с учетом выполнения некоторого набора требований. Требования, предъявляемые к разным моделям, могут перекрываться, но это совсем не обязательно. Даже при перекрытии требований в разных моделях могут различаться уровни гранулярности. Для первой модели требования могут быть сформулированы на уровне административного домена (Administrative Domain) или сети. Требования ко второй модели могут быть сформулированы на уровне конечной системы, а возможно и на уровне отдельного пользователя. Для третьей модели требования могут быть сформулированы как на уровне конечной системы, так и на уровне локального маршрутизатора, а также на уровнях маршрутного (Routing Domain) или административного (Administrative Domain) домена.

Каждая из этих моделей имеет свои преимущества в том или ином направлении. Эти методы могут использоваться независимо или совместно в различных комбинациях. Модель для описания распределения сетевых ресурсов на основе правил ортогональна модели распространения маршрутной информации на базе правил. Однако в конкретных реализациях эти модели могут взаимодействовать между собой.

При выборе методов для реализации к конкретной сети важно понимать требования отдельных сетевых приложений и осознавать последствия, которые могут возникнуть в результате взаимодействия нескольких методов.

Хотя неконтролируемая динамическая маршрутизация и распределение ресурсов могут обеспечивать лучшее поведение в реальном времени, использование маршрутизации на основе правил будет обеспечивать стабильное и предсказуемое поведение системы в соответствии с желаниями администратора.

4. Распределение маршрутных данных на основе правил

Цели

Задачей этой модели является организация потоков данных на базе политики распространения маршрутной информации. Реализация такой модели позволяет контролировать доступ к заданным сетевым ресурсам.

Модель реализуется на уровне сети или административного домена (политика на макроуровне).

Описание

Хорошим примером политики маршрутизации на базе правил распределения маршрутных данных является сеть с ее интерфейсами в сети среднего уровня [1, 2]. На интерфейсе в сеть NSFNET, осуществляется аутентификация и контроль маршрутной информации:

1. Аутентификация узла (peer) по адресу отправителя.
2. Проверка идентификации административного домена (в настоящий момент номера автономных систем EGP).
3. Проверка номера сети IP, которая анонсируется узлом-партнером по маршрутизации (routing peer).

4. Контроль метрики с помощью базы данных маршрутной политики (Routing Policy Data Base) чтобы разрешить для анонсированных номеров сетей IP прямой путь в NSFNET, а также менее предпочтительные пути.

На интерфейсе, пропускающем маршрутный трафик за пределы NSFNET, код маршрутизации NSS выполняет проверку полномочий (аутентификацию) маршрутизатора, действующего как партнер EGP, по его адресу и идентификации AD (номер AS).

Исходящие анонсы номеров сетей по протоколу EGP контролируются по AD или номерам отдельных сетей с помощью базы правил маршрутизации NSFNET Routing Policy Data Base.

Реализация маршрутной политики в NSFNET работает с июля 1988 и сообщество NSFNET приобрело большой опыт ее использования.

Другим примером политики управления распределением маршрутных данных может служить метод, предложенный для сети ESNET в работе [3].

Преимущества

Основное преимущество контроля за потоками маршрутной информации состоит в том, что этот метод позволяет создавать большие распределенные сети (WAN) с многосвязной топологией. Распределение ресурсов в дружественной среде возможно за счет фильтрации указанных номеров сетей и AD на уровне отдельного хоста. Другим важным преимуществом этой схемы является то, что она практически не снижает производительность сети, поскольку политика применяется только к пакетам протоколов маршрутизации. Маршрутные таблицы генерируются в результате реализации заданной политики. Это означает, что такая схема практически не оказывает влияние на скорость коммутации пакетов.

Недостатки

Распространение маршрутной информации на основе правил не использует фильтрации пакетов. Например, такое решение не может предотвратить злонамеренные атаки с помощью пакетов source routed. Хотя выделение ресурсов возможно, оно относится к фильтрации по номерам сетей или административным доменам, но не распространяется на конечные системы или отдельных пользователей.

Стоимость

Маршрутизация на основе правил в сети NSFNET реализована с использованием набора конфигурационных файлов, генерируемых на основе базы маршрутной информации. Для создания такой базы данных требуется представление о сети Internet в целом. Поскольку сеть Internet постоянно изменяется, требуется постоянно обновлять базу данных. Однако работа по сбору и поддержке информации о текущем состоянии Internet может выполняться как распределенная задача.

Поскольку управляемое на основе политики распространение маршрутной информации позволяет организовать фильтрацию по номерам сетей и AD, в базе маршрутной информации должны храниться сведения более чем о 1300 сетях, входящих в Internet сегодня¹.

5. Фильтрация/пересылка пакетов на основе правил

Цели

Задачей политики фильтрации и рассылки пакетов является управление потоками сетевого трафика на уровне отдельных пакетов. Такое управление предоставляет сетевому администратору возможность контроля за использованием сетевых ресурсов.

Реализация политики возможна на уровне конечной системы и даже на уровне отдельного пользователя (политика на микроуровне).

Описание

Пример политики маршрутизации на основе пакетов/потоков рассмотрен в работе [4]. В общем смысле рассылка и фильтрация пакетов на основе политики обеспечивает возможность весьма тонкого контроля за распределением пакетного трафика. Примером реализации рассылки и фильтрации на основе правил может служить механизм защиты, встроенный в структуру NSFNET NSS, посредством которого узлы сети могут защищаться от ненужных пакетов, адресованных в сеть NSFNET, на основе их фильтрации по IP-адресу получателя. Хотя этот механизм до сих пор не получил окончательного признания, он может быть реализован в считанные секунды.

Преимущества

Основным преимуществом этой схемы является то, что она позволяет управлять политикой для пакетов и выделения сетевых ресурсов на уровне отдельной конечной системы и даже отдельного пользователя. Эта схема не связана напрямую с распространением маршрутной информации. Если правила содержатся в самих пакетах, это позволяет идентифицировать пользователей и, в результате, обеспечить пользователям мобильность при сохранении рабочей среды.

Недостатки

Основным недостатком этой модели является ее потенциальное влияние на производительность маршрутизаторов, поскольку (по крайней мере, в случаях тонкой настройки) каждый пересылаемый пакет должен проверяться на соответствие политике. Это ограничение делает сомнительной возможность использования такой схемы в сегодняшней сети Internet², но модель может найти очень широкое применение в средах с коммутацией каналов (среда с поддержкой source-routed весьма похожа на системы с коммутацией каналов). Другая сложность может быть связана с многочисленностью правил в такой модели (это требует существенных усилий со стороны

¹1989 год. Прим. перев.

²Так казалось в 1989 году, а сегодня фильтрацию пакетов на основе правил обеспечивают даже простейшие маршрутизаторы, а зачастую фильтрация используется и на конечных станциях. Прим. перев.

администратора). Число правил особенно возрастает при реализации политики на уровне отдельных пользователей. Более того, передача правил потенциально в каждом пакете будет существенно повышать нагрузку на сеть и требовать дополнительных ресурсов. Это еще раз подчеркивает, что такая схема более подходит для ориентированных на соединения сетей (например, сети передачи данных общего пользования), где правила можно применять только в момент организации соединения. Вопрос масштабирования систем фильтрации и рассылки на основе правил в большой и неоднородной сети Internet, где правила могут создаваться любым участником, является открытым. Создание правил возможно даже в реальном масштабе времени. Масштабирование может потребовать иерархической структуры, а иерархия может вступить в противоречие с произвольной маршрутизацией по типу обслуживания (TOS), которая является одним из преимуществ данной модели.

Стоимость реализации

В больших системах с реализацией политики на уровне пакетов требуется создание маршрутной базы данных, содержащей значительный объем информации о правилах для отдельных станций и даже пользователей. Если предположить, что каждая из 1300 сетей имеет в среднем по 200 станций, это даст 260000 конечных станций в масштабе Internet. Каждая такая система будет вносить в базу данных информацию о желаемом трафике (включая тип обслуживания), возможно на уровне отдельных пользователей. В результате база правил достигнет гигантских размеров, особенно в случае использования различных правил для магистралей, сетей среднего уровня, кампусных сетей, подсетей, хостов и пользователей. Управление такой базой данных о маршрутизации пакетов может быть распределенным. Однако полностью распределенная база данных такого размера потребует встроенной системы проверки согласованности данных.

6. Динамическое распределение сетевых ресурсов на базе правил.

Цели

Гибкое и экономичное распределение сетевых ресурсов на основе текущих потребностей и заданных правил. Правила могут формулироваться на уровне административного домена (AD). Возможно также задать правила, которые будут регулировать выделение ресурсов для различных типов трафика (например, Telnet, FTP, предпочтительные приложения, управляющий трафик).

Реализация правил выделения сетевых ресурсов может происходить в перечисленных узлах сети:

- маршрутизаторы для уровня сетей и AD;
- коммутаторы устройств (каналов) для сетей;
- конечные системы, организующие соединения с сетью.

Описание

Распределение полосы на основе правил позволяет изменять параметры каналов (устройств) в соответствии с реальными потребностями. Если доступные сетевые ресурсы ограничены сверху, выделение полосы потребует управления на основе правил. Примером может служить конечная система, доступ к сетевым ресурсам которой для других станций и пользователей определяется набором правил (они могут выполняться автоматически или задаваться вручную). Примером динамического выделения полосы может служить коммутируемая компонента IDNX сети NSFNET или служба DRS (MCI Digital Reconfiguration Service), которую планируется реализовать в сети NSFNET.

Другой моделью выделения ресурсов (на уровне пакетов) может служить организация множества очередей. Такой подход позволяет управлять обработкой пакетов в зависимости от уровня важности (типа обслуживания) содержащегося в них трафика – важная информация (например, критичные к задержкам данные, пакеты мониторинга, управления, протоколов маршрутизации) может обрабатываться в первую очередь. Примером такого подхода может служить сеть NSFNET, где узлы отдают предпочтение трафику, связанному с магистралью NSFNET – это обеспечивает прогнозируемую передачу маршрутных данных, а также эффективный мониторинг и управление сетью. Можно использовать и полярный вариант этой модели – очереди для наименее предпочтительного трафика (например, фоновое копирование файлов).

Преимущества

Динамическое выделение полосы позволяет организовать гибкую среду, в которой полоса распределяется с учетом потребности узлов сети. Такой подход может обеспечить существенное снижение расходов в те периоды, когда реально требуется незначительная полоса. Этот метод потенциально может управлять выделением полосы для задач с переносом больших объемов информации в реальном масштабе времени за счет уменьшения полосы, предоставляемой другим узлам. Важно отметить, что распределение полосы не зависит от протокола и не оказывает влияния на протоколы маршрутизации и производительность пересылки пакетов

Распределение полосы на основе правил позволяет создавать динамические среды с прогнозируемым поведением. Правила выделения полосы на уровне пакетов или устройств (каналов) должны быть определены таким образом, чтобы они задавали согласованную и предсказуемую политику, позволяющую другим сетям или AD задать соответствующее распределение своих ресурсов.

Недостатки

Правила динамического распределения полосы в больших коммутируемых средах еще находятся в стадии разработки. В стадии разработки пока находятся и технические способы реконфигурации инфраструктуры в целях управления полосой.

Выделение полосы на основе правил может обеспечить тонкую настройку параметров производительности сети, но может также привести к неэффективной обработке (транзиту) трафика в других AD. Важно рассматривать правила управления ресурсами для сети в контексте AD этой сети. Административные домены должны согласовать свою политику выделения сетевых ресурсов с другими AD.

Техническая проблема совместного использования правил управления ресурсами может быть решена путем предоставления доступа к базе правил администраторам всех сетей и AD. Однако такой подход связан с решением целого ряда политических проблем и требует дополнительной проработки.

7. Обсуждение

Первая и вторая модели маршрутизации на основе правил похожи в том, что они ставят целью управление некоторыми потоками.

Такое управление позволяет контролировать доступ к дефицитным сетевым ресурсам (если дефицита не возникает, нет причин контролировать использование ресурса). Основное различие между этими моделями состоит в уровне контроля реализации – макроскопический или микроскопический.

Необходимость управления доступом к некоторым ресурсам связана с расходами на поддержку этих ресурсов. Если расходы на управление ресурсами превышают стоимость самих ресурсов, нет смысла «городить огород».

Если в какой-либо части Internet будет принято решение о необходимости использования на микроуровне политики на базе правил, реализация такой политики должна выполняться без значительного снижения производительности сетевой среды в целом. Локальные правила, заданные для некоторых областей маршрутизации (Routing Domain) или AD, не должны оказывать глобального влияния на трафик или маршрутизацию Internet. Правила для AD, обеспечивающих передачу транзитного трафика (например, NSFNET), не должны влиять на транзит ради получения локальных преимуществ.

В некоторых случаях модели маршрутизации на основе правил пытаются использовать взамен комплексного набора правил. Один из описанных в работе [4] сценариев рассматривает ситуацию, когда некое агентство имеет некоторые сетевые ресурсы (каналы, в приведённом примере), которые не всегда используются. Задача состоит в продаже этих ресурсов другим агентствам на то время, когда ресурс не требуется (в целях снижения расходов). Эта ситуация эквивалентна задаче поиска оптимального маршрута для заданного TOS при наличии сетевых ресурсов (например, каналов), параметры которых изменяются. Любые решения такой задачи должны принимать во внимание стабильность сети и маршрутов. Ситуация, в которой каналы, используемые для глобальных коммуникаций, являются субъектом произвольных локальных правил, требует дополнительного изучения. Другим вариантом решения задачи является временный отказ от незагруженных каналов с их возвратом в пользование телефонной компании. Такое решение похоже на планируемую в сети NSFNET систему MCI Digital Reconfiguration Service (DRS). Модель DRS представляется более понятной и простой в использовании, нежели сложная модель [4].

Модели маршрутизации на основе правил подчеркивают необходимость аккуратного решения задачи управления трафиком Internet при нормальной работе, во время неполадок и в моменты пиковой нагрузки. Эта задача не является новой. Однако за счет использования маршрутизации на основе правил могут быть достигнуты существенные преимущества.

8. Учет в сравнении с маршрутизацией на основе правил

Достаточно часто вопросы учёта (Accounting) и маршрутизации на основе правил (Policy Based Routing) рассматриваются совместно. Хотя оба подхода предназначены для решения задачи контроля за распределением дефицитных ресурсов, эти подходы, тем не менее, следует различать.

Основная разница между этими методами состоит в том, что при учете объединяется историческая информация и сведения о правилах для слежения за использованием сети. Учетные данные могут включать механизмы ограничения (например, для какой-то организации может быть выделен лишь определенный процент динамически разделяемой полосы). Следовательно, правила могут оказывать влияние на учет. Сетевой учет обычно включает сведения о маршрутах (на всех уровнях от AD до конечных систем) и данные об уровне трафика (счетчики пакетов или октетов).

Учет может использоваться с любой из описанных выше моделей маршрутизации на базе правил. Подобно организации политики на макро и микроуровне, учет также может вестись на различных уровнях. Можно собирать учетные данные на уровне AD, сети, хоста и даже отдельных пользователей. Однако, поскольку учет может использовать иерархическую структуру, микроучет может поддерживаться на уровне сетей и хостов, а макроучет – на уровне сетей или AD. Примером может служить уровень трафика, передаваемого чрез интерфейс между NSFNET и сетью среднего уровня (mid-level network) или между сетью среднего уровня и кампусной сетью. Более того, NSFNET имеет средства учета тенденций в трафике для отдельных сетей или приложений.

Полные схемы учета испытывают те же сложности, которые были описаны выше, а также должны обрабатывать потенциально очень большие объемы дополнительной информации. Как отмечено в работе [4], правила могут оказывать влияние на методы сбора учетной информации (например, возникает вопрос учета в целях оплаты пакетов, которые впоследствии были отброшены в результате применения правил). Учет на микроуровне может не обеспечить достаточного масштабирования.

Более того, с точки зрения финансового учета не очевидно, что сервис, обеспечиваемый на сетевом уровне, хорошо отображается на типы услуг, за которые пользователи сети готовы платить. В телефонной сети (или сети передачи данных общего пользования) пользователи платят за сквозной (end-to-end) сервис и ожидают высокого качества обслуживания с точки зрения вероятности ошибок и величины задержки (вполне возможно, что они не захотят платить за сервис, который представляется как неприемлемый unacceptable). В межсетевой среде с гетерогенным администрированием и недостатком сквозного контроля может сделать такое решение неприемлемым.

Для решения более узких (специальных) задач может использоваться упрощенный учет. Одним из решений такого типа является мониторинг картины сетевого трафика. При обнаружении недопустимого (недозволенного) трафика система учета может зафиксировать этот факт и позволяет предпринять определенные действия, меняющие политику или права доступа (блокировка хостов или сетей). Отметим, что такое решение существенно меньше влияет на пересылку пакетов маршрутизаторами, но требует наличия распределенной базы правил, которую может использовать система учета. Поскольку эта модель по своей природе является статистической, время реакции для нее существенно увеличивается.

9. Литература

- [1] Rekhter, Y., "EGP and Policy Based Routing in the New NSFNET Backbone", RFC 1092, IBM Research, February 1989.
- [2] Braun, H-W., "The NSFNET Routing Architecture", RFC 1093, Merit/NSFNET Project, February 1989.
- [3] Collins, M., and R. Nitzan, "ESNET Routing", DRAFT Version 1.0, LLNL, May 1989.
- [4] Clark, D., "Policy Routing in Internet Protocols", RFC 1102, M.I.T. Laboratory for Computer Science, May 1989.

Адрес автора

Hans-Werner Braun

Merit Computer Network

University of Michigan

1075 Beal Avenue

Ann Arbor, Michigan 48109

Telephone: 313 763-4897

Fax: 313 747-3745

E-Mail: hwb@merit.edu

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru