Network Working Group
Request for Comments: 4274
Category: Informational

D. Meyer
K. Patel
Cisco Systems

January 2006

Анализ протокола BGP-4

BGP-4 Protocol Analysis

Статус документа

В этом документе содержится информация для сообщества Internet. Документ не задаёт каких-либо стандартов Internet. Допускается свободное распространение документа.

Аннотация

Целью этого отчёта является документирование того, как требования для публикации протоколов маршрутизации в качестве Internet Draft Standard были удовлетворены для протокола BGP-4[1].

Этот документ удовлетворяет требованиям ко «второму отчёту», описанным в параграфе 6.0 документа RFC 1264. Для удовлетворения требований данный документ дополняет RFC 1774 и резюмирует основные свойства BGP-4, а также анализирует протокол с точки зрения масштабирования и производительности.

Оглавление

1. Введение....1
2. Основные свойства и алгоритмы BGP....2
2.1. Основные свойства....2
2.2. Алгоритмы BGP....2
2.3. Машина конечных состояний BGP (FSM)....2
3. Возможности BGP....3
4. Постоянные осцилляции партнёров. BGP....3
5. Рекомендации разработчикам....3
6. Производительность и масштабируемость BGP....3
6.1. Использование полосы канала и ресурсов процессора....3
6.1.1. Загрузка процессора (CPU)....4
6.1.2. Требования к памяти....4
7. Средства задания политики BGP и их подводные камни....4
7.1. Существование уникальной стабильной маршрутизации....5
7.2. Существование стабильной маршрутизации....5
8. Применимость....5
9. Благодарности....6
10. Вопросы безопасности....6
11. Литература....6
11.1. Нормативные документы....6
11.2. Дополнительная литература....7

1. Введение

BGP-4 представляет собой протокол маршрутизации между автономными системами, созданный для сетей TCP/IP. Версия 1 протокола BGP была опубликована в [RFC1105]. После этого были разработаны версии BGP с номерами 2, 3 и 4. Версия 2 была документирована в [RFC1163], версия 3 - в [RFC1267], а версия 4 - в [BGP4] (четвёртая версия протокола BGP далее будет обозначаться просто BGP). Отличия между версиями протокола рассмотрены в Приложении A документа [BGP4]. Возможные применения BGP в сети Internet описаны в документе [RFC1772].

BGP поддерживает бесклассовую междоменную маршрутизацию (Classless Inter-Domain Routing или CIDR) [RFC1519]. Поскольку ранние версии BGP не поддерживали CIDR, они признаны устаревшими и непригодными для использования в современной сети Internet.

Целью этого отчёта является документирование того, как требования для публикации протоколов маршрутизации в качестве Internet Draft Standard были удовлетворены для протокола BGP-4.

Этот документ удовлетворяет требованиям ко «второму отчёту», описанным в параграфе 6.0 документа RFC 1264. Для удовлетворения требований данный документ дополняет RFC 1774 и резюмирует основные свойства BGP-4, а также анализирует протокол с точки зрения масштабирования и производительности.

[1]Border Gateway Protocol version 4.

2. Основные свойства и алгоритмы BGP

В этой главе кратко рассматриваются ключевые функции и алгоритмы протокола BGP. BGP представляет собой протокол маршрутизации между автономными системами; он разработан для использования в среде, включающей множество автономных систем (АС). BGP предполагает, что маршрутизация внутри автономных систем осуществляется с помощью протоколов внутридоменной маршрутизации. BGP также предполагает, что пакеты данных маршрутизируются от отправителя в направлении получателя независимо от отправителя. BGP не делает предположений о протоколах внутридоменной маршрутизации, используемых в различных АС. В частности, BGP не требует от всех автономных систем использования одного протокола внутридоменной маршрутизации (т. е., протокола внутренней маршрутизации или IGP[1]).

В заключение отметим, что BGP является реальным протоколом междоменной маршрутизации и, в качестве такового, не вносит ограничений на топологию соединений между автономными системами. Информации, передаваемой посредством BGP, достаточно для построения графа связности автономных систем, из которого могут быть удалены маршрутные петли и к которому могут быть применены многочисленные правила политики маршрутизации на уровне автономной системы.

2.1. Основные свойства

Ключевыми свойствами протокола являются способ записи (нотация) атрибутов пути и агрегирование NLRI[2].

Атрибуты пути обеспечивают BGP гибкость и расширяемость. Эти атрибуты могут быть общеизвестными (well-known), обязательными или необязательными. Использование дополнительных атрибутов обеспечивает возможность проведения экспериментов, которые могут затрагивать группу маршрутизаторов BGP, не влияя на остальную часть Internet. Новые дополнительные атрибуты могут добавляться практически так же, как добавляются опции для протоколов (например, Telnet [RFC854]).

Одним из наиболее важных атрибутов пути является AS_PATH[3]. По мере перемещения информации о доступности через Internet к этим данным (AS_PATH) добавляется список автономных систем, через которые информация проходит. В результате этого добавления формируется атрибут AS_PATH. Использование AS_PATH обеспечивает простой способ удаления петель в маршрутной информации. В дополнение к этому AS_PATH является мощным и универсальным механизмом маршрутизации на основе правил.

BGP расширяет возможности AS_PATH путём включения наборов автономных систем, а также списков АС с помощью атрибута AS_SET. Расширенный формат позволяет сгенерированным объединенным (aggregate) маршрутам передавать информацию о пути из более специфичных маршрутов, использованных для агрегирования. Следует отметить, однако, что на момент создания этого документа атрибут AS_SET достаточно редко использовался в Internet [ROUTEVIEWS].

2.2. Алгоритмы BGP

Алгоритм, используемый BGP, не является в чистом виде ни алгоритмом на базе «векторов удаления» (distance vector algorithm), ни алгоритмом на основе состояний каналов (link state algorithm). Вместо этого протокол использует модифицированный алгоритм distance vector, который называют алгоритмом Path Vector[4]. Этот алгоритм использует информацию о пути для того, чтобы избавиться от проблем, присущих алгоритму distance vector. Каждый маршрут BGP объединяет в себе информацию об адресате с информацией о пути к нему. Информация о пути (её называют ещё информацией AS_PATH) сохраняется в атрибутах AS_PATH. Эта информация помогает BGP детектировать петли AS, позволяя в результате узлам BGP выбирать маршруты без петель.

BGP использует стратегию нарастающих обновлений для снижения расхода полосы каналов и процессорного времени. Таким образом, после начального обмена полной маршрутной информацией пара маршрутизаторов BGP обменивается между собой только данными об изменении этой информации. Такая стратегия нарастающих обновлений требует использования надёжного транспорта между парами маршрутизаторов BGP для обеспечения корректной работы. BGP решает эту задачу за счёт использования надёжного транспорта TCP.

В дополнение к нарастающим обновлениям BGP добавил концепцию агрегирования (объединения) маршрутов так, что информация о группе адресатов, использующих иерархическое распределение адресов (например, CIDR), может быть агрегирована и передана как одно значение NLRI.

В заключение отметим, что BGP является самодостаточным протоколом, т. е., BGP задаёт обмен маршрутной информацией как между узлами BGP в разных автономных системах, так и между узлами BGP одной АС.

2.3. Машина конечных состояний BGP (FSM)

Машина конечных состояний BGP FSM[5] представляет собой набор правил, которые применяются к указанным в конфигурации партнёрам BGP для операций BGP. Реализация BGP требует, чтобы узел BGP присоединялся к порту TCP с номером 179 и прослушивал его для восприятия всех новых соединений BGP от своих партнёров. Машина конечных состояний BGP должна инициализироваться и поддерживаться для каждого нового входящего или исходящего соединения. Однако в стабильном (установившемся) состоянии поддерживается только один экземпляр BGP FSM для каждого соединения.

В течение коротких периодов времени возможны ситуации, когда узел BGP может иметь входящее и исходящее соединение с одним партнёром. Это приводит к созданию двух разных BGP FSM для одного партнёра (вместо одной). Для решения этой проблемы используются правила разрешения конфликтов в соединениях BGP, определённые в спецификации [BGP4].

Состояния BGP FSM перечислены ниже.

---

[1] Interior gateway protocol - протокол внутреннего шлюза.
[2] Network Layer Reachability Information - информация о доступности на сетевом уровне.
[3] Autonomous System Path - путь через АС.
[4] Вектор пути. Более подробную информацию об этом алгоритме можно найти в RFC 1322. *Прим. перев.*
[5] Finite State Machine.

IDLE: в этом состоянии узел BGP отвергает все входящие соединения.

CONNECT: в этом состоянии узел BGP ожидает завершения процедуры организации соединения TCP.

ACTIVE: в этом состоянии узел BGP пытается обрести партнёра путём прослушивания и восприятия соединений TCP.

OPENSENT: узел BGP ожидает сообщения OPEN от своего партнёра.

OPENCONFIRM: узел BGP ожидает от своего партнёра сообщения KEEPALIVE или NOTIFICATION.

ESTABLISHED: соединение BGP организовано и узел обменивается с партнёром. сообщениями UPDATE, NOTIFICATION и KEEPALIVE.

Существует множество событий BGP, происходящих в перечисленных выше состояниях BGP FSM для партнёров. BGP. Поддержка этих событий может быть обязательной или опциональной. События управляются логикой протокола, являющейся частью BGP, или действиями оператора через интерфейс управления протокола BGP.

События BGP делятся на несколько типов - дополнительные события (Optional event), связанные с необязательными атрибутами сессии (Optional Session attribute), административные события (Administrative Event), события, связанные с таймерами (Timer Event), события, связанные с соединениями TCP (TCP Connection-based Event), и события, связанные с сообщениями BGP (BGP Message-based Event). Детальное описание FSM и событий BGP приведено в документе [BGP4].

3. Возможности BGP

Механизм BGP capability [RFC3392] обеспечивает простой и гибкий способ расширения возможностей протокола. В частности, этот механизм позволяет узлу BGP анонсировать своим партнёрам в процессе организации соединения различные дополнительные возможности, поддерживаемые этим узлом, и получать аналогичную информацию от партнёров. Благодаря этому в базовый протокол BGP включены только необходимые функции и обеспечивается гибкий механизм согласования расширенных функций.

4. Постоянные осцилляции партнёров. BGP

При обнаружении ошибок в соединении с партнёром. узел BGP разрывает соответствующее соединение и переводит FSM в состояние IDLE. Для повторной организации соединения с партнёром. узлу BGP требуется событие Start. Если ошибка сохраняется, а узел BGP генерирует событие Start автоматически, это может привести повторяющимся сменам маршрутов (flapping). Хотя в большинстве реализации BGP поддерживаются механизмы подавления осцилляций, методы подавления устойчивых осцилляций выходят за пределы базовой спецификации BGP.

5. Рекомендации разработчикам

Устойчивая к ошибкам реализация BGP должна быть достаточно “консервативной в работе”. Это значит, что при ограниченном числе префиксов может обеспечиваться устойчивость к произвольно высокому уровню изменчивости маршрута. Высокий уровень изменчивости не должен оказывать значительного влияния на время схождения при спорадических изменениях стабильных в общем случае маршрутов.

Устойчивая к ошибкам реализация BGP должна обладать следующими характеристиками:

1. Способность работать при почти произвольно высоком уровне изменчивости маршрутов (route flap) без потери связи с партнёром. (отказа от передачи сообщений keepalive) или потери партнерских отношений (adjacency) для других протоколов в результате высокой загрузки BGP.
2. Нестабильность подмножества маршрутов не должна оказывать влияния на анонсирование маршрутов и пересылку пакетов, связанные с множеством стабильных маршрутов.
3. Нестабильность не должна возникать в результате наличия партнёров. с высоким уровнем нестабильности или иной скоростью процессора, а также в результате нагрузки, воздействующей на скорость обработки маршрутов. Такие нестабильные партнёры не должны оказывать существенного влияния на время схождения для стабильных в общем случае маршрутов.

Существует множество устойчивых к ошибкам реализаций BGP. Создание такой реализации является нетривиальной, но достижимой задачей.

6. Производительность и масштабируемость BGP

В этой главе рассматриваются вопросы загрузки полосы каналов, памяти маршрутизатора и ресурсов процессора для работы BGP в нормальных условиях. В частности рассматриваются вопросы масштабирования BGP и ограничения этого протокола.

6.1. Использование полосы канала и ресурсов процессора

Непосредственно после организации соединения BGP партнёры обмениваются полными наборами маршрутной информации. Если обозначить общее число маршрутов в Internet N, все атрибуты путей (для всех N маршрутов), полученных от партнёра, - A и предположить, что сети равномерно распределены между автономными системами, максимальная полоса, расходуемая на первоначальный обмен данными между парой партнёров. BGP (P) составит

```
BW = O((N + A) * P)
```

При разработке BGP-4 одной из задач было снижение размера множества записей NLRI, которые будут передаваться между граничными маршрутизаторами. Схема агрегирования, определённая в [RFC1519], описывает объединение маршрутов провайдерами, повсеместно используемое сегодня в сети Internet.

Преимущества, достигнутые в результате анонсирования небольшого числа крупных агрегированных блоков (взамен множества более мелких блоков по классам сетей), сложно оценить с точки зрения экономии полосы. Если мы просто

будем перечислять все компоненты агрегированных блоков, как сети того или иного класса, такое рассмотрение не будет учитывать неиспользуемое адресное пространство, зарезервированное для будущего расширения сети. Более эффективным показателем успеха схемы агрегирования BGP является сравнение числа записей NLRI в современной сети Internet (многосвязной в глобальном масштабе) со скоростью роста числа маршрутов до внедрения BGP.

На момент подготовки этого документа полный набор внешних маршрутов, передаваемых с использованием BGP, включал приблизительно 134000 записей [ROUTEVIEWS].

6.1.1. Загрузка процессора (CPU)

Важной особенностью протокола BGP является то, что расход процессорного времени определяется только стабильностью сети, поскольку при любом изменении происходит обмен сообщениями BGP UPDATE. Если сеть BGP стабильна, все маршрутизаторы BGP в этой сети будут находиться в устойчивом состоянии. В этом случае расход полосы каналов и ресурсов процессора, связанный с работой BGP, будет обусловлен только передачей сообщений BGP KEEPALIVE. Сообщения KEEPALIVE передаются только между партнёрами. Предлагаемый интервал обмена такими сообщениями составляет 30 секунд. Сообщения KEEPALIVE достаточно малы (19 октетов) и практически не требуют обработки. В результате расход полосы на передачу сообщений KEEPALIVE составляет около 5 бит/сек. Практика показывает, что связанная с этими сообщениями дополнительная нагрузка (в терминах расхода полосы и процессорного времени), пренебрежимо мала.

В периоды нестабильности BGP-маршрутизаторы в сети генерируют обновления маршрутной информации и обмениваются этими обновлениями с помощью сообщений BGP UPDATE. Максимальная дополнительная нагрузка возникает в тех случаях, когда каждое сообщение UPDATE содержит информацию только для одной сети. Следует отметить, что на практике изменения маршрутов локализованы относительно атрибутов пути (т. е., изменяемые маршруты имеют общие атрибуты пути). В таких случаях информацию для множества сетей можно передать в одном сообщении UPDATE, что приведёт к существенному снижению расхода полосы (см. Приложение F.1 к документу [BGP4]).

6.1.2. Требования к памяти

Для оценки максимального расхода памяти при работе BGP обозначим общее число сетей в Internet, как N, среднее значение AS distance (количество автономных систем) на пути через Internet, как M, а общее число уникальных путей (AS path), как A. Максимальный расход памяти (MR) может составить

```
MR = O(N + (M * A))
```

Поскольку значение M (AS distance) является медленно возрастающей функцией уровня связности Internet, для практических задач наибольший размер потребной памяти имеет порядок произведения общего числа сетей в Internet на число партнёров. локальной системы. Ожидается, что общее число сетей в Internet будет расти гораздо быстрее, нежели среднее число соседей маршрутизатора. В результате расход памяти для работы BGP будет линейно связан с общим числом сетей в Internet.

Приведённая ниже таблица показывает типовые требования к оперативной памяти для маршрутизатора, поддерживающего BGP. Среднее число маршрутов, анонсируемых каждым партнёром. обозначено как N, общее число уникальных AS path - A, среднее число AS на пути через Internet (AS distance) - M (дистанция на уровне автономных систем задаётся числом AS), число октетов, требуемых для сохранения одной сети, - R, а число байтов, требуемых для сохранения одной AS в AS path - P. Предполагается, что каждая сеть представлена 4 байтами, каждая AS - двумя и каждая сеть достижима через некоторую часть полного множества узлов (число узлов BGP на сеть). Для оценки объёма требуемой памяти используется формула

```
MR = (((N * R) + (M * A) * P) * S).
```

Число сетей (N)	*Среднее число AS на пути (M)*	*Число AS path (A)*	*Число узлов BGP на сеть (P)*	*Расход памяти (MR)*
100000	20	3000	20	10400000
100000	20	15000	20	20000000
120000	10	15000	100	78000000
140000	15	20000	100	116000000

При анализе требований BGP к памяти мы фокусировались на размере таблицы BGP RIB, игнорируя детали реализации. В частности, мы получили значения верхней границы размера таблицы BGP RIB. Например, в период создания этого документа таблица BGP RIB в типовом магистральном маршрутизаторе содержала порядка 120 000 записей. Основываясь на этом значении можно задаться вопросом о возможности создания маршрутизатора для работы с таблицей, содержащей 1 000 000 записей. Очевидно, что ответ на этот вопрос зависит от реализации BGP. Устойчивая к ошибкам реализация BGP с разумным расходованием памяти и ресурсов процессора должна обеспечивать масштабирование до такого уровня.

7. Средства задания политики BGP и их подводные камни

BGP отличается от других распространённых протоколов маршрутизации IP тем, что картина маршрутизации определяется с использованием развитой семантики правил маршрутизации (routing policy). Хотя правила маршрутизации BGP являются одним из основных вопросов, которые должны принимать во внимание сетевые операторы, важно отметить, что языки и методы задания правил маршрутизации BGP не являются частью спецификации протокола (пример языка описания политики вы найдёте в [RFC2622]). Спецификация BGP включает несколько явных и неявных ограничений для языков описания правил. Такие языки обычно создаются разработчиками и развиваются в процессе взаимодействия с сетевыми инженерами в среде с нехваткой независимых от разработчиков стандартов.

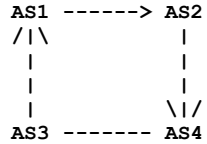
Сложность типовых конфигураций BGP (по крайней мере в сетях провайдеров) неуклонно возрастает. Производители маршрутизаторов зачастую предлагают сотни специальных команд для настройки BGP и эти наборы команд продолжают расширяться. Например группы BGP (BGP community) [RFC1997] позволяют создавать правила со специальными тегами маршрутов, которые могут использоваться другими маршрутизаторами BGP. Многие провайдеры позволяют своим заказчикам (а иногда и партнёрам) использовать группы (community) для задания области действия и предпочтений. В связи с этим написание конфигурации BGP включает все больше аспектов,

связанных с программированием. Это позволяет операторам кодировать сложные правила для того, чтобы учесть множество непредусмотренных ситуаций и обеспечивает возможность экспериментов с правилами маршрутизации. Такая гибкость правил является одной из основных причин того, что протокол BGP так хорошо подходит для использования в коммерческой среде сегодняшней сети Internet.

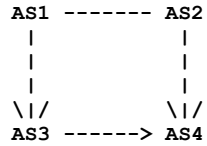
Однако широкие возможности создания правил имеют и теневую сторону, которую не всегда принимают во внимание. В частности, можно создавать локальные правила, которые будут приводить к расхождению (divergence) и другим глобальным аномалиям в маршрутизации (таким, как непреднамеренная неопределённость маршрутов). Если взаимодействующие правила, которые вызывают такие аномалии, определены в различных AS, это может приводить к возникновению весьма сложных в обнаружении и исправлении аномалий. В следующих параграфах будут описаны два таких случая, связанных с существованием (или нехваткой) стабильной картины маршрутизации.

7.1. Существование уникальной стабильной маршрутизации

Легко создать набор правил, для которого BGP не сможет гарантировать уникальность стабильной картины маршрутизации. Пример этого приводится ниже. Рассмотрим 4 автономных системы AS1, AS2, AS3 и AS4. AS1 и AS2 являются партнёрами. и обеспечивают транзит для AS3 и AS4, соответственно. Предположим, что AS3 обеспечивает транзит для AS4 (в этом случае AS3 является пользователем AS1, а AS4 - многодомным пользователем AS3 и AS2). AS4 может пожелать использовать канал в AS3 в качестве резервного и передать AS3 значение community, задающее для AS3 более низкий уровень предпочтения, нежели для маршрутов через AS1. Схема такой маршрутизации с резервированием показана на рисунке.



Канал AS3-AS4 должен в этой схеме использоваться лишь в тех случаях, когда соединение AS2-AS4 перестаёт работать (для исходящего трафика AS4 просто делает маршруты, полученные от AS2, более предпочтительными). Такое решение повсеместно используется в современной сети Internet. Отметим, однако, что в данной конфигурации имеется и другое стабильное решение, показанное на рисунке.



В этом случае AS3 не транслирует группу "depref my route[1]", полученную от AS4 в группу "depref my route" для AS1. Следовательно, если AS1 “слышит” маршрут в AS4 через AS3, она будет предпочитать этот маршрут (поскольку AS3 является заказчиком). Такое состояние может быть достигнуто, например, в результате инициирования “корректного” резервного маршрута с последующим обрывом и восстановлением сеанса BGP между AS2-AS4. В общем случае у BGP нет оснований для того, чтобы предпочесть “запланированный” вариант перед “аномальным”. В результате выбор картины маршрутизации будет зависеть от непредсказуемого порядка обмена сообщениями BGP.

Хотя этот пример достаточно прост, многие операторы могут не понимать, что источником проблем является неожиданный вариант взаимодействия правил BGP в автономных системах, который может приводить к существованию множества стабильных вариантов маршрутизации. В реальной сети Internet взаимодействие правил может оказаться значительно более сложным. Мы предполагаем, что описанные аномалии будут возникать более часто по мере того, как будут появляться новые способы задания правил маршрутизации BGP. Например, расширенные группы (extended community) обеспечивают дополнительную гибкость передачи сигнальной информации внутри AS и между автономными системами, нежели обычные группы [RFC1997]. В то же время использование групп сетевыми операторами постоянно расширяется для решения задач управления междоменным трафиком.

7.2. Существование стабильной маршрутизации

Можно создать набор правил, для которого BGP не сможет гарантировать наличие стабильной картины маршрутизации (или, хуже того, любая картина маршрутизации будет стабильной). Например, в [RFC3345] описано несколько сценариев, которые ведут к осцилляциям маршрутов, связанным с использованием атрибута MED (Multi-Exit Discriminator). Осцилляции маршрутов будут возникать в BGP, когда набор правил не даёт решения. Т. е., при отсутствии стабильной картины маршрутизации, удовлетворяющей заданному набору правил, BGP не имеет выбора, но пытается найти его. В дополнение к этому даже при наличии для данной конфигурации BGP стабильной картины маршрутизации, протокол может оказаться неспособным найти эту картину. В результате BGP может пойти по “узкой дорожке” не приводящей к решению.

Дивергенция[2] протокола, однако, не является проблемой, связанной только с использованием атрибута MED. Такая ситуация может возникать и в тех случаях, когда не используется атрибут MED. Следовательно, как при непреднамеренном индетерминизме, описанном выше, этот тип дивергенции является непредусмотренным следствием “мягкого” характера языков описания правил BGP.

8. Применимость

В этом параграфе мы рассмотрим среды, для которых протокол BGP хорошо подходит, и среды, для которых он не подходит. Ответ на этот вопрос частично даётся в главе 2 спецификации BGP [BGP4][3]:

> «Для того чтобы охарактеризовать набор решений, которые могут быть реализованы с использованием BGP, следует принять правило, по которому узел BGP может анонсировать узлам-партнерам (peer) в соседних AS только те маршруты, которые этот узел использует сам. Это правило отражает парадигму поэтапной (hop-by-hop)

[1] Снизить уровень предпочтения для моего маршрута.
[2] Невозможность схождения. *Прим. перев.*
[3] Эта ссылка является ошибочной. Приведённая в оригинале цитата перенесена из документа [RFC1774], который содержит ссылку на RFC 1771 (предыдущий вариант спецификации BGP-4). Здесь приведена цитата из перевода RFC 1771. *Прим. перев.*

маршрутизации, используемую в сети Internet для большинства случаев. Отметим, что некоторые правила не могут поддерживаться в рамках парадигмы "hop-by-hop" и, следовательно, требуется использовать другие методы маршрутизации (такие, как source routing). Например, BGP не позволяет AS передавать в соседнюю AS информацию, показывающую маршрут, отличающийся от того, который будет использоваться для трафика, происходящего из соседней AS. С другой стороны, BGP может поддерживать любые правила, соответствующие парадигме поэтапной маршрутизации. Поскольку в современной сети Internet используется только парадигма поэтапной маршрутизации и BGP может поддерживать любые правила, соответствующие этой парадигме, протокол BGP очень распространён для маршрутизации между AS в современной сети Internet.»

Одной из важнейших особенностей BGP является то, что протокол включает только базовый набор функций, обеспечивая в то же время гибкий механизм расширения функциональности. Например, механизм BGP capabilities обеспечивает простой и гибкий метод добавления новых возможностей для протокола. Наконец, в силу того, что протокол BGP был разработан с учётом обеспечения гибкости и расширяемости, новые и/или изменившиеся требования могут быть удовлетворены с использованием существующих механизмов.

Протокол BGP хорошо подходит для решения задач маршрутизации между автономными системами в любой сети, работающей на основе IP [RFC791] и использующей парадигму поэтапной (hop-by-hop) маршрутизации.

9. Благодарности

Благодарим Paul Traina за работу над предыдущими версиями этого документа. Elwyn Davies, Tim Griffin, Randy Presuhn, Curtis Villamizar и Atanu Ghosh также внесли много значимых поправок на этапах подготовки документа.

10. Вопросы безопасности

BGP обеспечивает для защиты гибкие механизмы с различными уровнями сложности. Для аутентификации сеансов BGP используются адреса сессий BGP и номера AS. Поскольку сессии BGP используют протокол TCP (и IP) для организации гарантированной доставки, для сеансов BGP могут использоваться дополнительные средства аутентификации и защиты, применяемые для протоколов TCP и IP.

BGP использует опцию TCP MD5 для проверки данных и защиты от подмены сегментов TCP. Использование опции TCP MD5 для протокола BGP подробно описано в документе [RFC2385]. Управление ключами TCP MD5 обсуждается в документе [RFC3562]. Шифрование данных BGP обеспечивается с помощью механизма IPsec, который шифрует данные протокола IP (включая данные TCP и BGP). Механизм IPsec может использоваться как в транспортном, так и в туннельном режиме. Этот механизм описан в документе [RFC2406]. Как опция TCP MD5, так и механизм IPsec на сегодняшний день недостаточно широко используются для защиты BGP в Internet. Следовательно, достаточно сложно оценить их реальное влияние на работу BGP. Однако оба эти механизма относятся к числу средств защиты на базе протоколов TCP и IP, расход полосы, загрузка процессора и расход памяти для BGP будут такими же, как и для других протоколов, работающих на основе TCP и IP.

BGP использует значение IP TTL для защиты сеансов EBGP[1]) от различных атак на уровне TCP или IP, ведущих в избыточному расходу процессорного времени. Это простой механизм фильтрации сегментов BGP (TCP) по значению поля TTL в заголовке IP сегментов BGP (TCP), передаваемых в сеансах EBGP. Механизм BGP TTL описан в документе [RFC3682]. Использование [RFC3682] оказывает на производительность такое же влияние, как использование любых правил на базе списков ACL[2] для протокола BGP.

Такие гибкие механизмы защиты на уровне TCP и IP позволяют протоколу BGP предотвратить вставку, удаление или изменение данных BGP, отслеживание данных, кражу сеансов и т. п. Однако протокол BGP уязвим для атак, которым подвержен протокол TCP. В документе [BGP-VULN] рассматриваются уязвимости протокола BGP. На момент создания настоящего документа велись работы по созданию и определению подходящей защитной инфраструктуры в рамках самого протокола BGP для обеспечения аутентификации и защиты маршрутной информации - к таким работам относятся [SBGP] и [SOBGP].

11. Литература

11.1. Нормативные документы

[BGP4] Rekhter, Y., Li., T., and S. Hares, Eds., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC1519] Fuller, V., Li, T., Yu, J., and K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", RFC 1519, September 1993.

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC1997] Chandra, R., Traina, P., and T. Li, "BGP Communities Attribute", RFC 1997, August 1996.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

[RFC3345] McPherson, D., Gill, V., Walton, D., and A. Retana, "Border Gateway Protocol (BGP) Persistent Route Oscillation Condition", RFC 3345, August 2002.

[RFC3562] Leech, M., "Key Management Considerations for the TCP MD5 Signature Option", RFC 3562, July 2003.

[RFC3682] Gill, V., Heasley, J., and D. Meyer, "The Generalized TTL Security Mechanism (GTSM)", RFC 3682, February 2004.

[RFC3392] Chandra, R. and J. Scudder, "Capabilities Advertisement with BGP-4", RFC 3392[3], November 2002.

[BGP-VULN] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, January 2006.

[1] External BGP
[2] access control list - список управления доступом.
[3] Этот документ заменён RFC 5492. *Прим. перев.*

[SBGP] Seo, K., S. Kent and C. Lynn, "Secure Border Gateway Protocol (Secure-BGP)", IEEE Journal on Selected Areas in Communications Vol. 18, No. 4, April 2000, pp. 582-592.

11.2. Дополнительная литература

[RFC854] Postel, J. and J. Reynolds, "Telnet Protocol Specification", STD 8, RFC 854, May 1983.

[RFC1105] Lougheed, K. and Y. Rekhter, "Border Gateway Protocol (BGP)", RFC 1105, June 1989.

[RFC1163] Lougheed, K. and Y. Rekhter, "Border Gateway Protocol (BGP)", RFC 1163, June 1990.

[RFC1264] Hinden, R., "Internet Routing Protocol Standardization Criteria", RFC 1264, October 1991.

[RFC1267] Lougheed, K. and Y. Rekhter, "Border Gateway Protocol 3 (BGP-3)", RFC 1267, October 1991.

[RFC1772] Rekhter, Y., and P. Gross, Editors, "Application of the Border Gateway Protocol in the Internet", RFC 1772, March 1995.

[RFC1774] Traina, P., "BGP-4 Protocol Analysis", RFC 1774, March 1995.

[RFC2622] Alaettinoglu, C., Villamizar, C., Gerich, E., Kessens, D., Meyer, D., Bates, T., Karrenberg, D., and M. Terpstra, "Routing Policy Specification Language (RPSL)", RFC 2622, June 1999.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[ROUTEVIEWS] Meyer, D., "The Route Views Project", http://www.routeviews.org.

[SOBGP] White, R., "Architecture and Deployment Considerations for Secure Origin BGP (soBGP)", Work in Progress, May 2005.

Адреса авторов

David Meyer

EMail: dmm@1-4-5.net

Keyur Patel

Cisco Systems

EMail: keyupate@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Интеллектуальная собственность

Подтверждение

Финансирование функций RFC Editor обеспечено IETF Administrative Support Activity (IASA).