Internet Engineering Task Force (IETF)
Request for Comments: 7606
Updates: 1997, 4271, 4360, 4456, 4760,
5543, 5701, 6368
Category: Standards Track
ISSN: 2070-1721

E. Chen, Ed.
Cisco Systems, Inc.
J. Scudder, Ed.
Juniper Networks
P. Mohapatra
Sproute Networks
K. Patel
Cisco Systems, Inc.

August 2015

Пересмотр обработки ошибок в сообщениях BGP UPDATE

Revised Error Handling for BGP UPDATE Messages

Аннотация

В соответствии с базовой спецификацией BGP, узел BGP, получивший сообщение UPDATE с искажённым атрибутом, должен разорвать сессию, через которую был получен такой атрибут. Такое поведение нежелательно, поскольку сброс сессии будет оказывать влияние не только на маршруты, связанные с некорректным атрибутом, но и на другие приемлемые маршруты, обмен которыми произошёл в этой сессии. Этот документ частично пересматривает обработку ошибок для сообщений UPDATE и содержит рекомендации для авторов документов, определяющих новые атрибуты. Кроме того, обновляются процедуры обработки ошибок для многих имеющихся атрибутов.

Этот документ служит обновлением для RFC 1997, 4271, 4360, 4456, 4760, 5543, 5701 и 6368.

Статус документа

Этот документ является проектом стандарта (Internet Standards Track).

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительная информация о документах BCP представлена в разделе 2 документа RFC 5741.

Информация о текущем статусе этого документа, обнаруженных ошибках и способах обратной связи может быть найдена по ссылке http://www.rfc-editor.org/info/rfc7606.

Оглавление

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

1. Введение

В соответствии с базовой спецификацией BGP [RFC4271], узел BGP, получивший сообщение UPDATE с некорректно сформированным атрибутом, должен разорвать сессию, через которую был получен такой атрибут. Такое поведение нежелательно, поскольку сброс сессии будет оказывать влияние не только на маршруты, связанные с некорректным атрибутом, но и на другие приемлемые маршруты, обмен которыми произошёл в этой сессии. В случае необязательных переходных атрибутов поведение особенно проблематично и может приводить к уязвимостям защиты. Это связано с тем, что атрибуты могут распространяться без проверки на промежуточных маршрутизаторах, если те не распознают атрибут. В результате могут возникать «туннели атрибутов» и когда атрибут поступит на понимающий его маршрутизатор сброшенная сессия может быть не связана с маршрутизатором, послужившим причиной отказа и сброса. Хуже того, проблемные атрибуты, которые могут быть связаны с одним обновлением от единственного маршрутизатора, на момент обнаружения проблемы могут уже оказаться многократно размноженными и это может приводить к сбросу множества партнерских сессий BGP. В результате ущерб может многократно возрастать.

Цель пересмотра обработки ошибок в сообщениях UPDATE заключается в минимизации влияния на маршрутизацию искажённых сообщений UPDATE с сохранением, по возможности, корректной работы протокола. Это может быть в значительной степени обеспечено за счёт поддержки имеющихся сессий и сохранения корректных маршрутов с одновременным удалением маршрутов, содержащихся в некорректно сформированном сообщении UPDATE.

Этот документ частично пересматривает обработку ошибок в сообщениях UPDATE и содержит рекомендации для авторов документов, определяющих новые атрибуты. Кроме того, пересмотрена обработка ошибок для множества имеющихся атрибутов. В частности, пересмотрены процедуры обработки ошибок [RFC1997], [RFC4271], [RFC4360], [RFC4456], [RFC4760], [RFC5543], [RFC5701] и [RFC6368].

1.1. Уровни требований

Ключевые слова необходимо (MUST), недопустимо (MUST NOT), требуется (REQUIRED), нужно (SHALL), не нужно (SHALL NOT), следует (SHOULD), не следует (SHOULD NOT), рекомендуется (RECOMMENDED), возможно (MAY), необязательно (OPTIONAL) в данном документе должны интерпретироваться в соответствии с [RFC2119].

2. Модели обработки ошибок

В этом документе отмечены 4 разных подхода к обработке ошибок в сообщениях BGP UPDATE. Эти методы перечислены ниже в порядке снижения жёсткости.

- Сброс сессии - указан в базовой спецификации BGP [RFC4271], при этом передаётся сообщение NOTIFICATION и сессия разрывается.
- Запрет AFI/SAFI - раздел 7 в [RFC4760] позволяет узлу BGP, обнаружившему в сообщении ошибку для данного AFI/SAFI, «игнорировать все последующие маршруты с данным AFI/SAFI, принятые в этой сессии». Мы называем это «запретом отдельного AFI/SAFI» или «запретом AFI/SAFI».
- Трактовать как отзыв - в этом варианте сообщение UPDATE содержащее связанный с ошибкой атрибут пути, **должно** трактоваться, как будто все указанные в нем маршруты были отозваны в поле WITHDRAWN ROUTES (или в атрибуте MP_UNREACH_NLRI, если это подходит) сообщения UPDATE, что ведёт к удалению этих маршрутов из базы Adj-RIB-In в соответствии с процедурами [RFC4271].
- Отбрасывание атрибута - в этом варианте некорректно сформированный атрибут **должен** отбрасываться с нормальной обработкой оставшейся части сообщения UPDATE. Такой подход **недопустимо** применять за исключением тех случаев, когда соответствующий атрибут не влияет на выбор и установку маршрута.

3. Пересмотр обработки ошибок BGP UPDATE

Этот раздел вносит множество изменений в параграф 6.3 спецификации [RFC4271]. Трактовка конкретных атрибутов пути рассматривается в разделе 7.

a. Изменяется первый абзац параграфа.

   Старый текст

Все ошибки, детектируемые при обработке сообщений UPDATE, **должны** приводить к генерации сообщения NOTIFICATION с Error Code = UPDATE Message Error. Субкод ошибки уточняет её природу.

Новый текст

Ошибки, детектируемые при обработке сообщений UPDATE и требующие сброса сессии, **должны** приводить к генерации сообщения NOTIFICATION с Error Code = UPDATE Message Error. Субкод ошибки уточняет её природу.

b. Обработка для приведённого ниже случая сохраняется без изменений.

Если значение поля Withdrawn Routes Length или Total Attribute Length слишком велико (т. е., Withdrawn Routes Length + Total Attribute Length + 23 превосходит значение поля Length в заголовке сообщения), в поле Error Subcode **должно** устанавливаться значение Malformed Attribute List.

c. Обработка ошибок Attribute Flag изменяется в соответствии с приведённым ниже текстом.

Старый текст

Если в любом распознанном атрибуте возникает конфликт флагов (Attribute Flags) и типа атрибута (Attribute Type Code), **должно** устанавливаться значение Error Subcode = Attribute Flags Error. В поле Data **должен** включаться связанный с ошибкой атрибут (тип, размер и значение).

Новый текст

Если значение бита Optional или Transitive в поле Attribute Flags конфликтует с его заданным значением, атрибут **должен** считаться сформированным некорректно с использованием модели «трактовать как отзыв» (treat-as-withdraw), если спецификация атрибута на требует иной обработки некорректных значения Attribute Flags.

d. При отсутствии любого обязательного общеизвестного атрибута[1] в сообщении UPDATE должна использоваться модель «трактовать как отзыв» (treat-as-withdraw).

e. Модель «трактовать как отзыв» **должна** применяться для всех случаев, которые задают сброс сессии и включают любой из атрибутов ORIGIN, AS_PATH, NEXT_HOP, MULTI_EXIT_DISC или LOCAL_PREF.

f. **Должно** применяться «отбрасывание атрибута» для всех случаев, которые задают сброс сессии и включают атрибут ATOMIC_AGGREGATE или AGGREGATOR.

g. Если атрибут MP_REACH_NLRI или MP_UNREACH_NLRI [RFC4760] в сообщении UPDATE встречается более одного раза, **должно** быть передано сообщение NOTIFICATION с субкодом ошибки Malformed Attribute List. Если какой-то иной (известный или не распознанный) атрибут встречается в сообщении UPDATE несколько раз, все вхождения, отличающиеся от первого, **нужно** отбрасывать, продолжая обработку UPDATE.

h. Если в сообщении UPDATE имеется множество связанных с атрибутами ошибок и для их обработки задана одна и та же модель (как описано в разделе 2), **должна** применяться указанная модель. В остальных случаях **должно** выбираться наиболее сильное действие.

i. Для поля Withdrawn Routes **должна** проверяться синтаксическая корректность таким же способом, как для поля NLRI[2]. Этот вопрос дополнительно рассмотрен ниже в параграфе 5.3.

j. В заключение отметим, что для использования модели «трактовать как отзыв» требуется успешно провести анализ всего поля NLRI и/или атрибутов MP_REACH_NLRI и MP_UNREACH_NLRI, который более подробно рассматривается в разделе 5. Если это невозможно, продолжается использование процедур [RFC4271] и/или [RFC4760], а это означает, что **должна** применяться модель «сброс сессии» (или «запрет AFI/SAFI).

4. Поля размера атрибутов

Существует две ситуации с ошибками, когда значение Total Attribute Length может противоречить размеру включённых атрибутов пути, которые сами содержат поля размера.

- В первом случае добавление размера последнего атрибута пути будет вызывать превышение Total Attribute Length при анализе вложенных атрибутов.
- Во втором случае остаётся меньше трёх (или четырёх при установленном в поле Attribute Flags флаге Extended Length) на момент начала анализа атрибута. Т. е., этот случай возникает, когда ещё не все данные включены в атрибуты пути, но уже не остаётся места для представления одного атрибута пути с минимальным размером.

В любом из этих случаев возникает ошибка и **должна** использоваться модель «трактовать как отзыв» (если нет другой, более серьёзной ошибки, требующей более жёсткой реакции) а значение Total Attribute Length **должно** основываться на обеспечении возможности определить начало поля NLRI.

Для всех атрибутов пути, для которых не указано наличие поля размера, способного иметь значение 0, нулевой размер атрибута **нужно** считать синтаксической ошибкой. Из числа атрибутов пути, рассматриваемых в данной спецификации, только AS_PATH и ATOMIC_AGGREGATE могут корректно иметь нулевой размер.

5. Разбор полей NLRI

5.1. Представление NLRI

Для того, чтобы облегчить выделение поля NLRI в сообщении UPDATE с искажёнными атрибутами:

[1]Отметим, что в соответствии с [RFC4760] атрибут классифицирован, как эффективно дискреционный (необязательный).
[2]Network Layer Reachability Information - информация о доступности на сетевом уровне.

- атрибут MP_REACH_NLRI или MP_UNREACH_NLRI (при его наличии) **нужно** кодировать как самый первый атрибут пути в сообщении UPDATE;
- в сообщение UPDATE **недопустимо** включать более одного из перечисленных элементов - непустое поле Withdrawn Routes, непустое поле NLRI, атрибут MP_REACH_NLRI, атрибут MP_UNREACH_NLRI.

Поскольку в старых узлах BGP эти ограничения могут отсутствовать, реализации **должны** быть готовы принимать эти поля в любых позициях и комбинациях.

Если используется кодирование [RFC4271], поле NLRI для семейства индивидуальных (unicast) адресов IPv4 передаётся сразу же вслед за всеми атрибутами в сообщении UPDATE. При получении такого сообщения UPDATE поле NLRI можно определить, используя значения Message Length, Withdrawn Route Length и Total Attribute Length (когда они согласованы), содержащиеся в сообщении, вместо того, чтобы опираться на размеры отдельных атрибутов в сообщении.

5.2. Отсутствие NLRI

[RFC4724] определяет сообщение End-of-RIB (EoR), которое может быть представлено сообщением UPDATE, содержащим лишь атрибут MP_UNREACH_NLRI, которые представляет отсутствие NLRI (это может быть также совсем пустое сообщение UPDATE при использовании «унаследованного» кодирования). Во всех остальных документированных случаях сообщение UPDATE содержит лишь отзываемые маршруты (в поле Withdrawn Routes или атрибуте MP_UNREACH_NLRI) или анонсирует доступные маршруты (в поле NLRI или атрибуте MP_REACH_NLRI).

Таким образом, если встречается сообщение UPDATE, которое включает отличные от MP_UNREACH_NLRI атрибуты пути и не содержит ни одного доступного NLRI, мы не можем быть уверены в успешном разборе NLRI, как того требует раздел 3 в п. (j). По этой причине при наличии в таком сообщении любой ошибки в атрибутах пути и любой ошибки, задающей отличный от attribute discard вариант обработки, **должна** применяться модель «сброс сессии».

5.3. Синтаксическая корректность полей NLRI

Поле NLRI или Withdrawn Routes **нужно** считать «синтаксически некорректным», если выполняется любое из приведённых ниже условий.

- Размер любого из включённых NLRI превышает 32.
- При разборе NLRI, содержащихся в поле, размер последнего NLRI превышает размер оставшихся в поле данных.

Аналогично, атрибут MP_REACH_NLRI или MP_UNREACH_NLRI **нужно** считать некорректным, если выполняется любое из приведённых ниже условий.

- Размер любого из включённых NLRI не согласуется с данным AFI/SAFI (например, IPv4 NLRI имеет размер больше 32 или IPv6 NLRI больше 128).
- При разборе NLRI в атрибуте размер последнего NLRI превышает размер оставшихся в атрибуте данных.
- Флаг атрибута не соответствуют указанным в [RFC4760].
- Размер атрибута MP_UNREACH_NLRI меньше 3 или размер атрибута MP_REACH_NLRI меньше 5.

5.4. Typed NLRI

Некоторые семейства адресов (например, MCAST-VPN [RFC6514], MCAST-VPLS [RFC7117] EVPN [RFC7432]) имеют типизованные NLRI. Поскольку поддерживаемые семейством типы значений могут быть не выражаемыми в расширении MP-BGP[1] [RFC4760], возможны ситуации, когда узел BGP анонсирует поддержку данного семейства и подсемейства адресов, хотя он не поддерживает конкретный тип NLRI в AFI/SAFI.

Узел BGP, анонсирующий поддержку такого типизованного семейства адресов, **должен** обрабатывать маршруты с нераспознанными типами NLRI путём отбрасывания таких маршрутов, если соответствующая спецификация для данного семейства адресов не задаёт иного поведения.

6. Эксплуатационные вопросы

Хотя вариант обработки ошибок «трактовать как отзыв», определённый в разделе 2, делает все возможное для сохранения корректности BGP, было замечено, что сообщение UPDATE, полученные в сессиях IBGP[2] и обработанные по этому варианту, могут приводить к несогласованности маршрутизации внутри автономной системы (AS). Последствия этого могут включать долгоживущие маршрутные петли и чёрные дыры. Это неприятно, однако предполагается, что проблема будет редко возникать на практике и, что более важно, негативное влияние будет существенно меньше чем при использовании вариант «сброс сессии».

При реальном обнаружении искажённого атрибута в сессии IBGP рекомендуется идентифицировать маршруты с искажённым атрибутом и отследить до входного маршрутизатора сети, через который эти маршруты был получены или где они были созданы для предотвращения генерации или приёма таких маршрутов. Это поможет сохранить в сети согласованную маршрутизацию.

Даже при отсутствии рассогласования маршрутов вариант «трактовать как отзыв» может приводить к полной недоступности или неоптимальной маршрутизации для адресов, чьи маршруты содержались в затронутом сообщении UPDATE.

Отметим, что «трактовка как отзыва» отличается от полного отбрасывания сообщения UPDATE. Отбрасывание нарушает базовый принцип BGP в части постепенных обновлений (incremental update) и может приводить к сохранению неприемлемых маршрутов.

[1]Multiprotocol BGP - мультипротокольное расширение BGP.
[2]Internal BGP - внутренний BGP.

С учётом упомянутых возможных проблем узел BGP должен обеспечивать возможности отладки для обнаружения и устранения проблем, связанных искажением атрибутов. В число таких возможностей должна входить, по крайней мере, запись в системный журнал вовлечённых в проблему NLRI, а также самих сообщений UPDATE. Эти сообщения UPDATE следует анализировать для обнаружения источника проблем.

В разделе 8 отмечено, что вариант «отбрасывание атрибута» не следует применять, когда этот атрибут влияет или может влиять на выбор маршрута. Хотя все указанные в этом документе случаи применения варианта «отбрасывания атрибута» не воздействуют по умолчанию на выбор маршрута, правила маршрутизации в принципе могут быть заданы таким образом, что отбрасывание искажённого атрибута будет влиять на этот выбор. Операторам следует быть осторожными при создании правил, принимая во внимание возможные последствия отбрасывания атрибутов. В общем случае пока такие правила применяются только для внешних сессий BGP, проблема корректности не возникает.

7. Процедуры обработки ошибок для существующих атрибутов

В следующих параграфах будут подробно рассмотрены условия обработки ошибок для разных атрибутов пути и указаны варианты, которые следует применять для обработки искажений в атрибутах. Реализации могут применять иные методы контроля ошибок, не рассмотренные здесь. Однако и в таких случаях указанные здесь варианты обработки обычно могут быть применены.

В этом разделе рассматриваются все атрибуты пути, определённые на момент создания документа, для которых не была определена обработка ошибок в соответствии с разделом 8 и которые не помечены как отменённые (deprecated) в реестре BGP Path Attributes [IANA-BGP-ATTRS]. Для атрибутов 17 (AS4_PATH), 18 (AS4_AGGREGATOR), 22 (PMSI_TUNNEL), 23 (Tunnel Encapsulation Attribute), 26 (AIGP), 27 (PE Distinguisher Labels) и 29 (BGP-LS Attribute) применяется обработка ошибок, описанная в разделе 8, поэтому здесь они не рассматриваются. Атрибуты 11 (DPA), 12 (ADVERTISER), 13 (RCID_PATH / CLUSTER_ID), 19 (SAFI Specific Attribute), 20 (Connector Attribute), 21 (AS_PATHLIMIT) и 28 (BGP Entropy Label Capability Attribute) были отменены и также не рассматриваются здесь.

7.1. ORIGIN

Атрибут ORIGIN считается искажённым, если размер атрибута отличается от 1 или значение атрибута не определено [RFC4271].

Сообщения UPDATE с искажённым атрибутом ORIGIN **нужно** обрабатывать по варианту «трактовать как отзыв».

7.2. AS_PATH

Атрибут AS_PATH считается искажённым, если в нем встречается сегмент нераспознанного типа или искажённый сегмент. Сегмент считается искажённым при выполнении любого из приведённых ниже условий.

- Возникает «переполнение», когда поле Path Segment Length последнего сегмента будет давать значение, выходящее за пределы Attribute Length.
- Имеется «нехватка», когда после финального разобранного сегмента остаётся лишь один октет (т. е. оставшихся данных не хватает даже для пустого заголовка сегмента).
- Поле Path Segment Length имеет значение 0.

Сообщение UPDATE с искажённым атрибутом AS_PATH **нужно** обрабатывать по варианту «трактовать как отзыв».

В [RFC4271] также сказано, что реализация «**может** проверить, что самая левая ... AS в атрибуте AS_PATH совпадает с автономной системой передавшего сообщение партнёра». Реализациям BGP **следует** также обрабатывать маршруты, для которых не проходит такая проверка, по варианту «трактовать как отзыв», но они **могут** применять вариант «сброс сессии», если это задано в конфигурации.

7.3. NEXT_HOP

Атрибут считается искажённым, если его размер отличается от 4 [RFC4271].

Сообщение UPDATE с искажённым атрибутом NEXT_HOP **нужно** обрабатывать по варианту «трактовать как отзыв».

7.4. MULTI_EXIT_DISC

Атрибут считается искажённым, если его размер отличается от 4 [RFC4271].

Сообщение UPDATE с искажённым атрибутом MULTI_EXIT_DISC **нужно** обрабатывать по варианту «трактовать как отзыв».

7.5. LOCAL_PREF

Обработка ошибок [RFC4271] изменяется как показано ниже:

- если атрибут LOCAL_PREF получен от внешнего соседа, его **нужно** обрабатывать по варианту «отбросить атрибут»;
- когда атрибут LOCAL_PREF получен от внутреннего соседа, его **нужно** считать искажённым, если размер отличается от 4. При наличии искажения сообщение UPDATE **нужно** обрабатывать по варианту «трактовать как отзыв».

7.6. ATOMIC_AGGREGATE

Атрибут **нужно** считать искажённым, если его размер отличается от 0 [RFC4271].

Сообщение UPDATE с искажённым атрибутом ATOMIC_AGGREGATE **нужно** обрабатывать по варианту «отбросить атрибут».

7.7. AGGREGATOR

Ошибки этого атрибута, указанные в [RFC4271], пересмотрены как указано ниже.

Атрибут AGGREGATOR **нужно** считать искажённым, если выполняется любое из приведённых ниже условий:

- размер атрибута не равен 6 (когда поддержка 4-октетных номеров AS не анонсирована партнёром и таких номеров не было принято от него [RFC6793]).
- размер атрибута не равен 8 (когда партнёр анонсирует и передаёт 4-октетные номера AS).

Сообщение UPDATE с искажённым атрибутом AGGREGATOR **нужно** обрабатывать по варианту «отбросить атрибут».

7.8. Community

Обработка ошибок, указанная в [RFC1997], пересмотрена как показано ниже.

- Атрибут Community **нужно** считать искажённым, если он не кратен 4.
- Сообщение UPDATE с искажённым атрибутом Community **нужно** обрабатывать по варианту «трактовать как отзыв».

7.9. ORIGINATOR_ID

Обработка ошибок, указанная в [RFC4456], пересмотрена как показано ниже.

- Если атрибут ORIGINATOR_ID получен от внешнего соседа, его **нужно** обрабатывать по варианту «отбросить атрибут».
- Когда атрибут получен от внутреннего соседа, его **нужно** считать искажённым, если размер отличается от 4. При наличии искажения сообщение UPDATE **нужно** обрабатывать по варианту «трактовать как отзыв».

7.10. CLUSTER_LIST

Обработка ошибок, указанная в [RFC4456], пересмотрена как показано ниже.

- Когда атрибут CLUSTER_LIST получен от внешнего соседа, его **нужно** обрабатывать по варианту «отбросить атрибут».
- Когда атрибут получен от внутреннего соседа, его **нужно** считать искажённым, если размер не кратен 4. При наличии искажения сообщение UPDATE **нужно** обрабатывать по варианту «трактовать как отзыв».

7.11. MP_REACH_NLRI

Если Length в поле Next Hop Network Address атрибута MP_REACH не соответствует ожидаемому значению, атрибут считается искажённым. Поскольку следующий интервал предшествует в атрибуте полю NLRI, такая ситуация не позволяет надёжно определить NLRI, поэтому **должен** использоваться вариант «сброс сессии» или «запрет AFI/SAFI».

Термин «ожидаемое» не является достаточно точным и относится к размеру адреса следующего интервала для Address Family Identifier или Subsequent Address Family Identifier, который может меняться в зависимости от используемого расширения. Например, при использовании [RFC5549] адрес следующего интервала будет иметь размер 4 или 16.

Дополнительное рассмотрение обработки этого атрибута приведено в разделах 3 и 5.

7.12. MP_UNREACH_NLRI

Обработка этого атрибута рассмотрена в разделах 3 и 5.

7.13. Traffic Engineering

Отметим, что в [RFC5543] не указано конкретно, что считается «искажением» атрибута пути Traffic Engineering. В будущих версиях этой спецификации такая информация может быть включена. А пока реализация, определившая (по той или иной причине) наличие в сообщении UPDATE искажённого атрибута пути Traffic Engineering **должна** использовать вариант «трактовать как отзыв».

7.14. Extended Community

Описанная в [RFC4360] обработка ошибок пересмотрена как показано ниже.

- Атрибут Extended Community **нужно** считать искажённым, если его размер не кратен 8.
- Сообщение UPDATE с искажённым атрибутом Extended Community **нужно** обрабатывать по варианту «трактовать как отзыв».

Отметим, что для узлов BGP **недопустимо** считать ошибкой нераспознанный тип или субтип Extended Community.

7.15. IPv6 Address Specific Extended Community

Описанная в [RFC5701] обработка ошибок пересмотрена как показано ниже.

- Атрибут IPv6 Address Specific Extended Community **нужно** считать искажённым, если его размер не кратен 20.
- Сообщение UPDATE с искажённым атрибутом IPv6 Address Specific Extended Community **нужно** обрабатывать по варианту «трактовать как отзыв».

Отметим, что для узлов BGP **недопустимо** считать ошибкой нераспознанный тип или субтип IPv6 Address Specific Extended Community.

7.16. ATTR_SET

Заключительный параграф раздела 5 в [RFC6368] меняется как показано ниже.

Старый текст

> Сообщение UPDATE с искажённым атрибутом ATTR_SET **нужно** обрабатывать следующим образом. Если флаг Partial установлен, а флаг Neighbor-Complete сброшен, сообщение UPDATE считается отзывом маршрута, как описано в [OPT-TRANS-BGP]. В противном случае (т. е. флаг Partial сброшен или флаг Neighbor-Complete установлен) **должна** использоваться процедура из базовой спецификации BGP-4 [RFC4271] для случая Optional Attribute Error.

Новый текст

> Сообщение UPDATE с искажённым атрибутом ATTR_SET **нужно** обрабатывать по варианту «трактовать как отзыв».

Кроме того, нормативная ссылка на [OPT-TRANS-BGP] удаляется из [RFC6368].

8. Рекомендации для авторов спецификаций BGP

Документы, задающие новые атрибуты BGP, **должны** указать, когда атрибут считается ошибочным (искажённым) и как обрабатывать такие ошибки. Допустимые варианты обработки ошибок описаны в разделе 2. Модель «трактовать как отзыв» (treat-as-withdraw) обычно является предпочтительной, а модель «сброс сессии» (session reset) применять не рекомендуется. Авторам документов BGP также рекомендуется прочесть обзор, посвящённый необязательным переходным атрибутом в первом абзаце «Введения» настоящего документа. В документы **следует** также включать рассмотрение отладочных средств, которые могут потребоваться для диагностики в случаях искажения атрибута.

Для любого атрибута, искажение которого обрабатывается по варианту «отбрасывание атрибута» (attribute discard) вместо treat-as-withdraw, важно рассмотреть возможное влияние такого выбора. В частности, если рассматриваемый атрибут влияет или может влиять на выбор или установку маршрута обычно отбрасывание атрибута создаёт больше опасности, если тщательный анализ не подтверждает обратное. При анализе следует принимать во внимание достижение компромисса между сохранением связности и возникновением побочных эффектов.

Авторы могут ссылаться на примеры в разделе 7.

9. Вопросы безопасности

В этой спецификации решается вопрос уязвимости узлов BGP к возможным атакам, где злоумышленник может создавать искажённые необязательные переходные атрибуты, которые не распознаются участвующими в процессе маршрутизаторами. Промежуточные маршрутизаторы, не распознав атрибут, передают его дальше без проверки. Когда искажённый атрибут приходит на распознающий данный тип атрибутов маршрутизатор, тот сбрасывает сессию, в которой получен атрибут. Поскольку между атакующим и распознающим этот тип атрибута может быть достаточно большая «дистанция», этот тип атак создаёт потенциальную опасность.

Улучшенная обработка ошибок в соответствии с этой спецификацией может оказывать негативное влияние при использовании в будущем для защиты BGP механизмов с неизвестными криптографическими слабостями. Например, при использовании (гипотетического) механизма, который не обеспечивает защиты целостности атакующий может изменять шифротекст, влияя тем самым на поведение получателя и наблюдая за его реакцией. До создания этой спецификации использовался просто разрыв сессии BGP, но использование этой спецификации даёт атакующему возможность предпринять множество попыток. Хотя таких механизмов, защищающих лишь конфиденциальность, в настоящее время не применяется, в прошлом были определены механизмы с подобными (не обязательно доступными для использования) уязвимостями [RFC7366]. Рекомендуемый сегодня для предотвращения таких проблем подход заключается в использовании шифров AEAD[1] [RFC5116] и отбрасывание сообщений, не прошедших проверку.

А других аспектах данная спецификация не меняет параметров безопасности BGP.

10. Литература

10.1. Нормативные документы

[IANA-BGP-ATTRS] IANA, "BGP Path Attributes", <http://www.iana.org/assignments/bgp-parameters>.

[RFC1997] Chandra, R., Traina, P., and T. Li, "BGP Communities Attribute", RFC 1997, DOI 10.17487/RFC1997, August 1996, <http://www.rfc-editor.org/info/rfc1997>.

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

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <http://www.rfc-editor.org/info/rfc4271>.

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <http://www.rfc-editor.org/info/rfc4360>.

[RFC4456] Bates, T., Chen, E., and R. Chandra, "BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)", RFC 4456, DOI 10.17487/RFC4456, April 2006, <http://www.rfc-editor.org/info/rfc4456>.

[RFC4724] Sangli, S., Chen, E., Fernando, R., Scudder, J., and Y. Rekhter, "Graceful Restart Mechanism for BGP", RFC 4724, DOI 10.17487/RFC4724, January 2007, <http://www.rfc-editor.org/info/rfc4724>.

[1] Authenticated Encryption with Additional Data - аутентифицированное шифрование с дополнительными данными.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <http://www.rfc-editor.org/info/rfc4760>.

[RFC5543] Ould-Brahim, H., Fedyk, D., and Y. Rekhter, "BGP Traffic Engineering Attribute", RFC 5543, DOI 10.17487/RFC5543, May 2009, <http://www.rfc-editor.org/info/rfc5543>.

[RFC5701] Rekhter, Y., "IPv6 Address Specific BGP Extended Community Attribute", RFC 5701, DOI 10.17487/RFC5701, November 2009, <http://www.rfc-editor.org/info/rfc5701>.

[RFC6368] Marques, P., Raszuk, R., Patel, K., Kumaki, K., and T. Yamagata, "Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 6368, DOI 10.17487/RFC6368, September 2011, <http://www.rfc-editor.org/info/rfc6368>.

[RFC6793] Vohra, Q. and E. Chen, "BGP Support for Four-Octet Autonomous System (AS) Number Space", RFC 6793, DOI 10.17487/RFC6793, December 2012, <http://www.rfc-editor.org/info/rfc6793>.

10.2. Дополнительная литература

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <http://www.rfc-editor.org/info/rfc5116>.

[RFC5549] Le Faucheur, F. and E. Rosen, "Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop", RFC 5549, DOI 10.17487/RFC5549, May 2009, <http://www.rfc-editor.org/info/rfc5549>.

[RFC6514] Aggarwal, R., Rosen, E., Morin, T., and Y. Rekhter, "BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs", RFC 6514, DOI 10.17487/RFC6514, February 2012, <http://www.rfc-editor.org/info/rfc6514>.

[RFC7117] Aggarwal, R., Ed., Kamite, Y., Fang, L., Rekhter, Y., and C. Kodeboniya, "Multicast in Virtual Private LAN Service (VPLS)", RFC 7117, DOI 10.17487/RFC7117, February 2014, <http://www.rfc-editor.org/info/rfc7117>.

[RFC7366] Gutmann, P., "Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7366, DOI 10.17487/RFC7366, September 2014, <http://www.rfc-editor.org/info/rfc7366>.

[RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", RFC 7432, DOI 10.17487/RFC7432, February 2015, <http://www.rfc-editor.org/info/rfc7432>.

Благодарности

Авторы благодарят Juan Alcaide, Deniz Bahadir, Ron Bonica, Mach Chen, Andy Davidson, Bruno Decraene, Stephen Farrell, Rex Fernando, Jeff Haas, Chris Hall, Joel Halpern, Dong Jie, Akira Kato, Miya Kohno, Warren Kumari, Tony Li, Alton Lo, Shin Miyakawa, Tamas Mondal, Jonathan Oddy, Tony Przygienda, Robert Raszuk, Yakov Rekhter, Eric Rosen, Shyam Sethuram, Rob Shakir, Naiming Shen, Adam Simpson, Ananth Suryanarayana, Kaliraj Vairavakkalai, Lili Wang и Ondrej Zajicek за их замечания и обсуждение, а также рецензирование этого документа.

Адреса авторов

Enke Chen (редактор)

Cisco Systems, Inc.

Email: enkechen@cisco.com

John G. Scudder (редактор)

Juniper Networks

Email: jgs@juniper.net

Pradosh Mohapatra

Sproute Networks

Email: mpradosh@yahoo.com

Keyur Patel

Cisco Systems, Inc.

Email: keyupate@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru