Содержание

Введение

Эта статья обсуждает, как устранить неполадки trap-сообщений SNMP AAAAccSrvUnreachable и AAAAuthSrvUnreachable, которые инициированы из-за проблем достижимости с сервером Сервиса RADIUS, используемым для аутентификации абонентов (или операторы, входящие в узел, но это не то, что обсуждается здесь). Существует два подхода, которые могут использоваться для определения, когда любое из этих trap-сообщений инициирует. Эта статья объяснит, какие условия инициируют эти trap-сообщения и какие подходы к устранению проблем и сбор данных могут быть взяты, чтобы определить основную причину и решить их. Это также обсуждает некоторые потенциальные шаги исправления, которые можно рассмотреть.

Обратите внимание на то, что РЕЗУЛЬТАТОМ недостижимости будут ошибки вызова или бухгалтерские сбои, то же, как будто ответы радиуса являются отклонениями вместо акцептов. В то время как успех/сбой (аутентификация), скорость измерена независимо от таймаута/достижимости (существуют trap-сообщения и сигналы тревоги для этого), и может, конечно, быть проанализирован самостоятельно, фокус этой статьи будет на проблеме достижимости а не проблеме отклонения.

Пример выходных данных от LAB и фактических билетов используется повсюду, чтобы помочь вести домой дискуссии. Что, кажется, открытые IP - адреса в этой статье, **поддельные** адреса.

Триггеры trap-сообщения

Существует две других модели/алгоритма/подхода для выбора из определить статус сервера RADIUS и когда попробовать другой сервер, если происходят сбои:

Последовательные отказы в aaamgr обрабатывают подход

Исходный подход и тот, используемый чаще операторами, включают отслеживание количества сбоев, которые произошли подряд для определенного процесса aaamgr. Процесс aaamgr ответственен за всю обработку сообщения RADIUS и обмен с сервером RADIUS, и много процессов aaamgr будут существовать в шасси, каждый соединенный с процессами sessmgr (которые являются основными процессами, ответственными за управление вызовами). (Просмотрите все процессы aaamgr с, "показывают ресурсы для задачи" команда), определенный процесс aaamgr будет поэтому обрабатывать сообщения RADIUS для многих вызовов, не только одиночного вызова, и этот алгоритм включает отслеживание, сколько раз подряд определенный процесс aaamgr был не в состоянии получать ответ на тот же запрос, который это должно было повторно передать - "Таймаут Access-Request", как сообщается в "счетчиках show radius".

Текущие Последовательные отказы соответствующего встречного "Access-Request в менеджере", также от "счетчиков show radius" инкрементно увеличен, когда это происходит, и "show radius accounting (или аутентификация) подробная команда" серверов, указывают на метки времени изменения состояния радиуса от Активного до не Ответа (но никакое trap-сообщение SNMP, или журналы генерируются всего для одного сбоя). Вот пример для учета радиуса:

Если этот счетчик достигает настроенного значения (По умолчанию = 4) без того, чтобы когда-нибудь быть перезагруженным на конфигурируемый: (обратите внимание, что скобки [] используются для указания на дополнительный спецификатор, и в этих перехватах случаев учет устранения проблем (аутентификация является по умолчанию, если учет не задан),

радиус [бухгалтерские] последовательные отказы обнаруживать-неработающего-сервера 4

Затем этот сервер отмечен в течение периода настроенные (минуты):

радиус [бухгалтерский] deadtime 10

Trap-сообщение SNMP и журналы инициированы также, например, для аутентификации и/или считающий соответственно:

Trap-сообщения указывают на сервер, который недостижим. Примите во внимание любые образцы. Например, это происходит с одним сервером или другим или всеми серверами, и какова частота возврата - это происходит непрерывно или иногда?

Также обратите внимание, что все, что требуется для этого trap-сообщения, которое будет инициировано, для одного aaamgr для сбоя, и таким образом, хитрая часть об этом trap-сообщении - то, что это не указывает на степень проблемы. Это могло быть очень обширно или очень minoir - который является до оператора для определения и приближается к пониманию, которые обсуждены в этой статье.

статистика show snmp trap сообщит о числе раз, которое она инициировала начиная с загрузки, даже если были давно удалены более старые trap-сообщения. Данный пример показывает бухгалтерскую недостижимую проблему:

Обратите внимание на то, что aaamgr, о котором сообщают в вышеупомянутом примере, является #231. Это - управление aaamgr на ASR 5000, который находится на Карте управления системой (SMC). То, что обманывает в этих выходных данных, - то, что то, когда отдельный aaamgr или проблемы достижимости опыта aaamgrs, номер экземпляра сообщил в журналах, является управлением aaamgr экземпляр а не конкретный экземпляр (экземпляры), испытывающий проблему. Это - то, вследствие того, что, если бы много экземпляров испытывают проблемы достижимости, то регистрация заполнилась бы быстро, если бы о них все сообщили как таковые, и таким образом, дизайн должен был сообщить в общем относительно экземпляра управления, который, если бы вы не знали это, конечно обманул бы. В разделе устранения проблем более подробная информация будет предоставлена о том, как определить, какой aaamgr (s) отказывает. Запускаясь в некоторых версиях StarOS 17 и v18 +, это поведение было изменено так, чтобы о соответствующем aaamgr номере экземпляра, имеющем проблемы с подключением (как сообщается в trap-сообщениях SNMP), сообщили в журналах с определенным идентификатором (Cisco CDETS CSCum84773), хотя все еще только сообщают о первом возникновении (через множественный aaamgrs) этого случая.

Управление aaamgr является максимумом sessmgr номер экземпляра + 1, и так далее ASR 5500, который это 385 для Карты обработки данных (DPC) или 1153 (для DPC 2).

Как заметка на полях, управление aaamgr ответственно за обработку входов в систему оператора/администратора, а также обработка изменения запросов авторизации инициировала от самих серверов RADIUS.

При продолжении "show radius accounting (или аутентификация) подробная команда" серверов укажет на метки времени изменений состояния к Выключенному, который соответствует trap-сообщениям/журналам (напоминание: Не Ответ определил, ранее только одиночный aaamgr получение таймаута, тогда как Выключенный одиночный aaamgr то, чтобы заставлять достаточно последовательных таймаутов на конфигурацию инициировать Выключенный),

Если существует только один настроенный сервер, то он не отмечен, поскольку это было бы важно для настройки успешного вызова.

Стоящий упоминания то, что существует другой параметр, который может быть настроен на вызванной линии config обнаруживать-неработающего-сервера? тайм-аут ответа/b>?. Когда задано, сервер отмечен только, когда оба встречены последовательные отказы и условия response-timeout. Когда НИКАКИЕ ответы не получены к ALL запросы, отправленные к индивидуальному серверу, response-timeout задает период времени. (Обратите внимание на то, что этот таймер непрерывно перезагружался бы, поскольку получены ответы.) Это условие ожидалось бы, когда или сервер или сетевое подключение полностью не работают, по сравнению с частично компрометировал/ухудшал.

Вариант использования для этого был бы сценарием, где пакет в трафике заставляет последовательные отказы инициировать, но сразу в результате не желаемо отмечание сервера. Скорее сервер только быть отмеченным после того, как определенный период времени проходит, где никакие ответы не получены, эффективно представляя истинную недостижимость сервера.

Этот метод, просто обсужденный управления изменениями механизма состояний радиуса, зависит от рассмотрения всех процессов aaamgr и обнаружения того, которое инициирует условие отказавших повторных попыток. Этот метод подвергается до некоторой степени некоторой случайности сбоев, и так может не быть идеальным алгоритмом к обнаружению сбоев. Но это особенно хорошо в обнаружении aaamgr (s), которые сломаны, в то время как хорошо работают все другие.

Подход поддержки активности

Другой метод обнаружения достижимости сервера RADIUS использует фиктивные тестовые сообщения поддержки активности. Это включает постоянную передачу поддельных сообщений RADIUS вместо того, чтобы контролировать действующий трафик. Другое преимущество этого метода состоит в том, что это всегда активно, по сравнению с с последовательными отказами в подходе aaamgr, где могли быть периоды, куда никакой трафик сервера RADIUS не передается, и таким образом, нет никакого способа знать, существует ли проблема в течение тех времен, приводящих к задержанному обнаружению, когда попытки действительно начинают происходить. Также, когда сервер отмечен, эти пакеты Keepalive продолжают передаваться так, чтобы сервер мог быть повышен как можно скорее. Недостаток к этому подходу - то, что он пропускает проблемы, которые связаны к определенным aaamgr экземплярам, которые могут испытывать проблемы, потому что он использует управление aaaamgr экземпляр для тестовых сообщений.

Вот различные configurables соответствующие для этого подхода:

Команда? радиус (бухгалтерская) поддержка активности обнаруживать-неработающего-сервера? включает подход поддержки активности вместо последовательных отказов в подходе aaamgr. В приведенном выше примере система передает тестовое сообщение с Тестовым Именем пользователя Тестового имени пользователя и пароля имени пользователя каждые 30 секунд и повторяет каждые 3 секунды, если никакой ответ не получен и повторяет до 3 раз, после которого это отмечает сервер. Как только это получает свой первый ответ, это отмечает его, выполняют резервное копирование снова.

Вот является запрос аутентификации в качестве примера / ответом для вышеупомянутых параметров настройки:

Те же trap-сообщения SNMP используются для выражения недостижимых/вниз и достижимых / состояний радиуса как с последовательными отказами в подходе aaamgr:

? show radius противостоит всем? имеет раздел для того, чтобы отслеживать запросы поддержки активности об аутентификации и считать также? вот опознавательные счетчики:

Устранение проблем команд/подходов

Теперь, когда триггер для AAA, Недостижимые trap-сообщения были объяснены, следующий шаг, должен понять различные команды устранения проблем для использования для определения влияния и попытки выяснить основную причину. Недостижимость является очень широким условием. Это не объясняет, где недостижимость - в сети на сервере, или на ASR. Например, известно, были ли запросы даже отправлены

во-первых? Сервер получал запросы? Сделал это отвечает на запросы. Сделал ответы, возвращаются к ASR и если так, были они обработанный или отброшенный на внутреннем пути (т.е. потоки). Эта попытка раздела обратиться, как ответить на эти вопросы.

Основы конфигурации RADIUS

Там являются первыми некоторые основы, что нужно быть знакомым с относительно Конфигурации RADIUS. Большая часть конфигурации для RADIUS находится в в частности именованной группе, и все контексты имеют группу по умолчанию, которая может быть настроена следующим образом. Много раз конфигурации будут иметь всего одну группу, группу по умолчанию.

Если определенные именованные группы ааа используются, на них указывает следующий оператор, настроенный в профиле абонента или Названии точки приложения (APN) (в зависимости от технологии управления вызовами), например:

Примечание: Системные первые проверки, которые определенная группа ааа назначила на абонента, и затем проверяет по умолчанию группы ааа для дополнительного configurables, не определенного в определенной группе.

Вот полезные команды, которые суммируют все значения, назначенные на весь configurables в различных конфигурациях группы ааа. Это позволяет быстрый просмотр всего configurables включая значения по умолчанию, не имея необходимость исследовать конфигурацию вручную, и возможно помогать избегать делать ошибки при принятии определенных параметров настройки. Эти команды сообщают через все контексты:

Самым важным конфигурируемым является, конечно, доступ к серверу RADIUS и сами учетные серверы. Например:

Обратите внимание на функцию Max. скорости, которая ограничивает количество запросов, отправленных к серверу на aaamgr в секунду

Кроме того, IP-адрес NAS также требуется, чтобы быть определенным, который является IP-адресом на интерфейсе в контексте, от которого передаются запросы RADIUS, и ответы получены. Если не определенный, запросы не отправлены и контролируют, трассировки абонента могут не перенести очевидную ошибку (никакие передаваемые запросы RADIUS и никакая индикация почему).

Nas-ip-address атрибута RADIUS обращается 10.211.41.129

Обратите внимание на то, что, потому что и аутентификация и учет часто обрабатываются тем же сервером, другой номер порта используется для дифференциации аутентификации по сравнению с бухгалтерским трафиком на сервере RADIUS. Для стороны ASR5K номер исходного порта UDP НЕ задан и выбран шасси на aaamgr основе (больше на этом позже).

Обычно множественный доступ и учетные серверы заданы для обеспечений резервирования. Или циклический выбор или расположенный по приоритетам заказ могут быть настроены:

радиус [бухгалтерский] алгоритм {первый сервер | циклический алгоритм}

Первый параметр сервера приводит к запросам ALL, отправленным к серверу с пронумерованным самым низким образом приоритетом. Только то, когда сбои повторной попытки происходят, или хуже, сервер отмечен, является сервером со следующим приоритетом, который попробовали. Больше на этом ниже.

Когда радиус (учет или доступ) запрос будет отправлен, ответ ожидается. Когда ответ не получен в периоде ожидания (секунды):

радиус [бухгалтерский] таймаут 3

Запрос повторно передан до заданного числа раз:

радиус [бухгалтерские] максимальные числа попыток 5

Это означает, что запрос может быть отправлен в общей сложности максимальные числа попыток + 1 раз, пока он не разочаровывается в определенном сервере RADIUS, который попробовали. На этом этапе это пробует ту же последовательность к следующему серверу RADIUS в заказе. Если каждый из серверов был попробованными максимальными числами попыток + 1 раз без ответа, то требование отклонено, предположив, что нет никакой другой причины для сбоя до той точки.

Как заметка на полях, существуют configurables, которые обеспечивают пользователей для имения доступа, даже если бы аутентификация и считающий сбой из-за таймаутов ко всем серверам, хотя коммерческое развертывание вряд ли внедрило бы это:

радиус позволяет [бухгалтерскую] аутентификацию вниз

Кроме того, существуют configurables, которые могут ограничить абсолютное общее число передач определенного запроса через все настроенные серверы, и они отключены по умолчанию:

радиус [бухгалтерские] Max. передачи 256

Например, если это установлено = 1, то, даже если существует дополнительный сервер, он никогда не предпринимается, потому что когда-либо предпринимается только одна попытка для определенной абонентской настройки.

покажите средство ресурсов для задачи aaamgr все

Каждый процесс aaamgr соединен с, и "работает для" связанного процесса sessmgr (ответственный за полную обработку вызова) и расположен на другой Карте служб пакетной передачи (PSC) или Карте обработки данных (DPC), но использовании ID одинакового экземпляра. Также в выходных данных данного примера обращают внимание на специальный aaamgr экземпляр 231 работа Карты управления системой (SMC) для ASR 5000 (или Input Output Card менеджмента для (MIO) ASR 5500), который НЕ обрабатывает запросы абонента, но действительно привыкает для тестовых команд радиуса (см. последующий раздел для большего количества подробности о том), AND для обработки входа в систему CLI оператора.

В этом фрагменте aaamgr 107, расположенный на PSC 13, ответственен за обработку всей

обработки RADIUS для парного sessmgr 107, расположенного на PSC 1. Проблемы достижимости для aaamgr 107 влияют на запросы к sessmgr 107.

В следующем примере обратите внимание, что проблемы с aaamgr 92 влияют на парный sessmgr, как легко замечено когда по сравнению с другим sessmgrs относительно чисел сеансов:

счетчики show radius {{все | сервер <IP - сервер>} [экземпляр <aaamgr #>] | сводка}

Команда номера один, чтобы быть знакомой с является вариантами "счетчиков show radius"

Этот отчеты по командам назад много полезных счетчиков для того, чтобы решить проблемы радиуса. "Show radius противостоит всей" команде, очень ценно в отслеживании успеха и сбоев на основе сервера, и важно понять значение различных счетчиков, которые составляют эту команду, поскольку это может не быть очевидно. Команда контекстно-зависима и так должна быть выполнена в том же контексте, где определена группа (группы) ааа.

ВАЖНОЕ ПРИМЕЧАНИЕ: По неотслеживаемому периоду времени трудно сделать любые выводы из значений счетчика или отношений среди счетчиков. Когда решенная проблема происходит, для создания точных заключений лучший подход должен перезагрузить счетчики и контролировать их в течение времени.

В следующем результате обратите внимание "на Access-Request, Передаваемый" = 1, в то время как "Access-Request, Повторенный" = 3. Так, любой данный новый запрос к определенному серверу RADIUS только посчитан однажды, и все повторные попытки посчитаны отдельно. В этом случае это - в общей сложности 3 + 1 = 4 отправленные запроса доступа. Обратите внимание на встречные "Таймауты Access-Request" = 1. Одиночный таймаут происходит только, когда ALL сбой повторных попыток, так в этом случае, 3 повторных попытки без ответа приводят к 1 Таймауту (не 4). Это происходит через все настроенные серверы, пока нет успех, или все попытки отказали. Поэтому обратите внимание на счетчики, которые отслежены для каждого сервера отдельно. Вот пример этого, где:

Обратите внимание также, что таймауты НЕ посчитаны как сбои, результат, являющийся, что количество полученного Access-Accept и полученный Access-Reject не составит в целом Access-Request, Передаваемый, если будут какие-либо таймауты.

Анализ этих счетчиков может не быть абсолютно прямым. Например, для Мобильного IP (MIP) протоколируют, поскольку аутентификации отказывают, нет никакого Регистрационного Ответа MIP (RRP), передаваемый, и мобильный телефон может продолжить инициировать новые Запросы регистрации (RRQ) MIP, потому что это не получило RRP MIP. Каждый новый RRQ MIP заставляет PDSN передавать новый Запрос аутентификации, который сам может иметь его собственную серию повторных попыток. Это может быть замечено в поле Id наверху трассировки пакетов? это уникально для каждого набора повторных попыток. Результат состоит в том, что счетчики для Передаваемого, Повторенного, и Таймаут могут быть намного выше, чем ожидаемый для количества полученных вызовов. Существует опция, которой можно позволить минимизировать эти дополнительные повторные попытки, и она может быть установлена во Внешнем агенте (FA) (но не на Home Agent (HA)) сервис:? опознавательный ааа млн <6 выборов здесь>

оптимизировать-повторные-попытки?

Некоторые другие полезные счетчики:

"Ответ Access-Request, Отброшенный" - происходит, если вызов не в состоянии устанавливать при ожидании ответов на запросы аутентификации.

"Ответ Access-Request, Прошлый Раз" - указывает на любые задержки между оконечными точками, хотя это, очевидно, не указало бы, где задержка могла бы быть.

"Access-Request, Текущие Последовательные отказы в менеджере" касаются того, что было обсуждено в первом разделе по триггерам для AAA Недостижимые trap-сообщения. Это представляет aaamgr (s) с самым высоким количеством последовательных таймаутов.

"Текущий Access/Accounting-Request, С очередями", указывает на запросы, на которые не отвечают, и остающейся в очереди (учет обеспечивает наращивание очереди неопределенно, в то время как аутентификация не делает),

Наиболее распространенный сценарий, замеченный, когда о Недостижимом AAA сообщают, - то, что Таймауты Доступа и/или Отбрасывания Ответа также происходят, в то время как Ответы Доступа не не отстают от запросов.

Если доступ к priviledged режиму технической поддержки доступен, то дополнительное исследование может быть сделано на aaamgr уровне экземпляра, чтобы определить, ли один или несколько определенный aaamgrs причина увеличения полного "плохого" количества. Например, ищите aaamgrs, которые расположены на определенном PSC/DPC, имеющем высокие числа или возможно одиночный aaamgr или случайный aaamgrs, имеющие проблемы - ищут образцы. Если все или большая часть aaamgrs имеют проблемы, то существует увеличенная вероятность, что основная причина является любой внешней к шасси OR, проявляющий крупномасштабный на шасси. Проверки общей работоспособности должны быть сделаны в этом случае.

Вот пример выходных данных, показывая проблему с определенным aaamgr для учета. (Проблема, оказалось, была дефектом в межсетевом экране между ASR5K и сервером RADIUS, который блокировал трафик от определенного aaamgr экземпляра (114) порт). За трехнедельный период только 48 ответов были получены, уже более чем 100,000 таймаутов произошли (и это doesn? t включают, повторно передает).

В заключение определите, какие счетчики инкрементно увеличиваются, для который серверы, и в какой скорость.

покажите средство подсистемы сеанса {aaamgr | sessmgr} {все | экземпляр <экземпляр #>}

В то время как это выходит за рамки этой статьи для исследования всех лишних выходных данных от этой команды, пара примеров стоят посмотреть на. Как то любое другое, устранение проблем сравнивая выходные данные, между какой, как полагают, хорошо по сравнению с плохими aaamgr экземплярами, часто показывает, что сообщили очевидные различия в значениях. Это могло быть отражено в общем числе запросов, сбоя/доли успешных попыток, аутентификация отменила и т.д. Как напоминание, убедиться очистить подсистему сеанса (один экземпляр не может быть очищен, они все должны быть очищены), чтобы устранить любую историю, которая могла потенциально предоставить облачное изображение текущего состояния.

Продолжая ту же проблему, упомянутую ранее относительно одиночного aaamgr, отказывающего для учета, здесь выведен от другого узла с той же самой проблемой кроме другого sessmr экземпляра 36. Обратите внимание на все содержательные поля сбоем aaamgr и как те значения увеличиваются в течение долгого времени с двумя перехватами

команды. Выходные данные Meanwhile от экземпляра 37 показывают как пример работы aaamgr.

Нужно также работать, показывают ресурсы для задачи для проверки для любых неровных чисел сеансов (используемый столбец) среди всего sessmgrs. Если кто-либо найден, проверьте парный aaamgrs для тех sessmrs с этой командой, чтобы видеть, существуют ли какие-либо поля, которые являются вне линии - если проблема происходит из-за RADIUS тогда существует хороший шанс найти что-то.
В примере ресурсов для задачи показа в предыдущем разделе был signficantly более низкое число сеансов на sessmgr 92, который был соединен к aaamgr 92. Выходные данные от подсистемы сеанса показа показывают значительное возрастание в Max. выдающемся общем количестве, и аутентификация aaa удалила счетчики и подняла Текущие Max. выдающиеся счетчики. Можно использовать функцию grep, оперативную на шасси и/или Блокноте ++ или другой мощный поисковый редактор для быстрого анализа данных. Выполните команду многократно для наблюдения то, что значения увеличивают или остаются поднятыми:

ping

traceroute

ФУНКЦИЯ ПРОВЕРКИ СВЯЗНОСТИ ICMP PING тестирует основное подключение, чтобы видеть, может ли AAA-сервер быть достигнут или нет. Эхо-запрос, возможно, должен быть получен с ключевым словом src в зависимости от сети и должен быть сделан от контекста AAA для имения значения. Если эхо-запрос к сбоям сервера, то попытайтесь пропинговать посреднические элементы включая адрес следующего узла в контексте, подтвердив, что существует Запись ARP к адресу следующего маршрутизатора, если отказывает эхо-запрос. Traceroute может также помочь с проблемами маршрутизации.

тестовый экземпляр радиуса x аутентификация {<group> группы радиуса | все | <port> порта <ip> сервера} <password> <username>

тестовый экземпляр радиуса x считающий {группа радиуса <имя группы> | все | <port> порта <ip> сервера}

С доступом к командам Tech Support Test можно далее протестировать, в состоянии ли определенный aaamgr достигнуть какого-либо сервера RADIUS. Для теста подключения базовой конфигурации RADIUS, независимого от любого определенного aaamgr экземпляра, используют версию общего назначения этой команды, которая не задает определенного экземпляра #, но использует экземпляр управления по умолчанию. Если это отказывает, то это может указать к более широкой проблеме, независимой от определенных экземпляров.

Эта команда отправляет запрос базовой проверки подлинности или бухгалтерский **запуск**, и **остановите** запросы, и ждет ответа. Для аутентификации используйте любое имя пользователя и пароль, в этом случае ответ отклонения ожидался бы, подтверждая, что RADIUS работает, как разработано, или известное рабочее имя пользователя/пароль могло использоваться, в этом случае должен быть получен принять ответ

Вот пример выходных данных из протокола монитора и выполнения опознавательной версии команды на шасси лабораторной работы: Вот пример от оперативного шасси:

Вот пример выходных данных от выполнения бухгалтерской версии команды. Пароль не необходим.

Следующий результат для того же aaamgr экземпляра 36, просто упомянул, где сломано подключение к определенному учетному серверу RADIUS:

```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC 2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS Start to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Stop to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Start to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 10113.0 ms
```

информация show radius [группа радиуса <имя группы>] экземпляр {X | все}

Это отчеты по командам ID потока Модуля сетевого процессора (NPU) и порт UDP, используемый настроенным IP-адресом NAS для соединения с серверами RADIUS. Об этом сообщают в разделе группы ааа по умолчанию выходных данных. Конечно, номер порта может быть полезным, если нужно совпасть с Пакетами RADIUS в захвате пакета с определенным aaamgr экземпляром #. (Обратите внимание на то, что потоки NPU являются сложными и не что-то обсужденное в этой статье кроме объекта, который специалист службы поддержки был бы в состоянии исследовать далее.) Это также отслеживает ожидающие запросы к серверу. В той же проблеме в качестве примера, используемой всюду по этой статье, только определенный сервер RADIUS <==> IP NAS/, парный порт UDP отказал, как выделено.

```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC 2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS Start to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Stop to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Start to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 10113.0 ms
```

абонент монитора

Абонент монитора может использоваться, чтобы определить, предпринята ли

аутентификация, по крайней мере, и обрабатывается ли ответ для проверяемых вызовов. Включите опцию 'S', которая обозначает Информацию Отправителя Sessmgr - эффективно сообщающий относительно sessmgr или aaamgr экземпляра #, который обрабатывает рассматриваемый обмен сообщениями. Вот пример для MIP, обращаются к HA , подключающему к sessmgr / aaamgr экземпляры 132.

```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC 2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS Start to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Stop to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Start to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 10113.0 ms
```

Существует пример сбоя в конце этой статьи также.

Захват пакета

Иногда существует недостаточно информации о ASR для определения, почему проблемы достижимости происходят, в этом случае захват пакета будет необходим. Когда решение проблем отдельного подписчика, определение соответствующих пакетов в трассировке должны быть легкими. В противном случае, если проблема связана к определенным ports/aaamgr экземплярам, зная порт UDP, используемый с обоих концов определенного aaamgr экземпляра # **<==>**, пара сервера RADIUS могла быть полезной. Попытка перехвата во множественных местах в сети может быть необходимой для определения, где пакеты становятся отброшенными. В проблеме, проанализированной всюду по этой статье, это был захват пакета в просто правильном месте в пути передачи между ASR и сервером RADIUS, который был прорывом в решении проблемы.

Исправления

Этот последний раздел предлагает некоторые идеи для перепосреднических проблем с подключением RADIUS. Они не представлены ни в каком конкретном заказе, а скорее просто списке для рассмотрения в процессе устранения проблем.

Если сервер RADIUS становится перегруженным, загрузка могла бы быть уменьшена через значение (по умолчанию 256) настроенный для? радиус (считающий) Max. выдающийся?, который устанавливает предел для количества выдающихся (оставшихся без ответа) запросов о любом данном процесс aaamgr. Если предел достигнут, журналы могут указать на это:? подведенный для присвоения идентификатора сообщения для сервера проверки подлинности RADIUS x. x . x . x : 1812?.

Сообщения RADIUS ограничения скорости к определенным серверам могут также помочь уменьшать загрузку через ключевое слово rate-limit для строк настройки соответствующего сервера.

Иногда это не проблема подключения, но увеличенного бухгалтерского трафика, который не является проблемой с RADIUS persay, но указывающий на другую область, такую как увеличенные пересмотры ppp, которые вызывают больше учета, запускается и

останавливается. Таким образом, возможно, должен устранить неполадки за пределами RADIUS для обнаружения причины или триггера для признаков наблюдаемыми.

Если во время процесса устранения проблем было решено удалить проверку подлинности RADIUS или учетный сервер из списка оперативных серверов по любой причине, существует (не-config) команда, которая возьмет сервер вне обслуживания неопределенно, пока это не будет желаемо для откладывания его в обслуживании. Это - более чистый подход, чем необходимость удалить его из конфигурации вручную:

```
{отключают |, включают} радиус [бухгалтерский] сервер x. x . x . x
```

```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC
2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response
receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1,
port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS
Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-
trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port
1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS Start to
accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Stop
to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS
Start to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-
trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port
1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to
accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time
for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting
Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting
server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response
was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response
receivedRound-trip time for response was 10113.0 ms
```

PSC или миграция DPC или переключатель линейной карты могут часто очищать причину проблемы к факту, что миграция приводит к перезапуску процессов на карте, включая npumgr, который был причиной проблем время от времени относительно потоков NPU.

Когда миграция PSC была сделана, но в содержательном скручивании с вышеупомянутым примером aaamgr 92, AAA фактически ЗАПУСТИЛИСЬ Недостижимые сбои. Когда миграция PSC была сделана, делая резерв PSC 11, это было инициировано из-за исчезновения потока NPU. Когда это было сделано активным час спустя, фактическое влияние недостающего потока запустилось для aaamgr 92. Проблемы как это очень трудно решить без помощи со стороны Технической поддержки.


```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC
2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response
receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1,
port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS
Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-
trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port
1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS Start to
accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Stop
to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS
Start to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-
trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port
1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to
accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time
for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting
Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting
server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response
was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response
receivedRound-trip time for response was 10113.0 ms
```

Вопрос был временно решен с переключателем порта, который вызвал карту PSC, которая имела отсутствие поток NPU для aaamgr 92, который больше не будет связываться с картой активной линии.

```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC
2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response
receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1,
port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS
Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-
trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port
1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS Start to
accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Stop
to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS
Start to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-
trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port
1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to
accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time
for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting
Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting
server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response
was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response
receivedRound-trip time for response was 10113.0 ms
```

Последнее trap-сообщение сбоя:

```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC
2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response
receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1,
port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS
Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-
trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port
1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS Start to
accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Stop
to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS
Start to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-
trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port
1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to
accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time
for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting
Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting
server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response
was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response
receivedRound-trip time for response was 10113.0 ms
```

Точно так же перезапускающие определенные aaamgrs, которые вовлекают, могут также решить вопросы, хотя это - действие, которое должна сделать Техническая поддержка, так как она включает ограниченные команды Tech Support. В примере aaamgr 92, представленном в разделе ресурсов для задачи показа ранее, это было предпринято, но не помогло, потому что основная причина не была aaamgr 92, а скорее пропавшими без вести поток NPU, в котором aaamgr 92 нуждался (это была проблема NPU, не проблема aaamgr). Вот соответствующие выходные данные попытки. "покажите, что таблица задачи" выполнена для показа ассоциации идентификатора процесса и экземпляра # 92 задачи.

```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC
2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response
receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1,
port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS
Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-
trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port
1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS Start to
accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Stop
to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS
```

```
Start to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-
trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port
1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to
accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time
for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting
Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting
server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response
was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response
receivedRound-trip time for response was 10113.0 ms
```

Заключительный пример

Вот заключительный пример реального простоя в действующей сети, которая сплачивает многие команды устранения проблем и подходы, обсужденные в этой статье. Обратите внимание на то, что этот узел обрабатывает 3G MIP, и Долгосрочное развитие (LTE) 4G и типы вызова Развитых данных пакета высокой скорости (eHRPD).

история show snmp trap

Одними только trap-сообщениями можно подтвердить, что отправная точка совпадает с тем, о чем клиент сообщил как 19:25 UTC. Как в стороне, обратите внимание, что trap-сообщения AAAAuthSvrUnreachable для основного сервера 209.165.201.3 не начинали происходить до несколько часов спустя (не ясный, почему, но хороший для замечания; но **учет недостижимого** к тому серверу запустился сразу же),

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun Dec 29 19:38:13 2013 Internal trap notification 42
(AAAAccSvrUnreachable) server 6 ip address 209.165.201.8
...
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
```

покажите ресурсы для задачи

Выходные данные показывают намного более низкое количество запросов к DPC 8/1. На основе этого одного, без дальнейшего анализа, один COULD предполагает, что существует проблема на DPC 8, и предложите опцию для миграции на резервный DPC. Но важно подтвердить то, что фактическое влияние абонента - в этих сценариях, как правило, абоненты соединятся успешно на последующей попытке, и поэтому влияние не является слишком значительным для абонента, и они, вероятно, ни о чем не сообщат поставщику, предполагая, что нет никакого простоя плоскости пользователей, также продолжающегося (который возможен в зависимости от того, что сломано).

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun Dec 29 19:38:13 2013 Internal trap notification 42
(AAAAccSvrUnreachable) server 6 ip address 209.165.201.8
...
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
```

абонент монитора

Настройка вызова была поймана, где не было никакого ответа на запрос аутентификации к основным 209.165.201.3 для sessmgr 242 на DPC 9/1, который, оказывается, имеет его парный aaamgr нахождение на DPC 8/1, подтверждая сбои вследствие 3G к AAA, недостижимому на 8/1. Это также подтверждает, что даже при том, что не было никаких trap-сообщений AAAAuthSrvUnreachable для 209.165.201.3 до того момента времени, это не означает, что нет проблемы для обработки ответов для того сервера (как показано выше, trap-сообщения действительно запускаются, но несколько часов спустя).


```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun Dec 29 19:38:13 2013 Internal trap notification 42
(AAAAccSvrUnreachable) server 6 ip address 209.165.201.8
...
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
```


покажите sub [сводка] smgr-экземпляр X

То, что является содержательным, - то, что число сеансов для sessmgr 242 подобно другой работе sessmgrs. Дополнительное исследование показало, что 4G, которую вызовы, также размещенные на этом шасси, смогли подключить и таким образом, они составили из-за отсутствия способности вызовов Мобильного IP 3G соединиться. Можно определить, что,

возвращаясь, насколько 8 часов, который был после простоя, запустились, никаких призывов MIP к этому sessmgr 242, при возвращении 9 часов к тому, прежде чем простой запустился, существуют подключенные вызовы:

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun Dec 29 19:38:13 2013 Internal trap notification 42
(AAAAccSvrUnreachable) server 6 ip address 209.165.201.8
...
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
```

LTE и вызовы eHRPD показывают более высокое соотношение вызовам MIP при сравнении sessmgrs, которые связаны с работой и сломаны aaamgrs:

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun Dec 29 19:38:13 2013 Internal trap notification 42
(AAAAccSvrUnreachable) server 6 ip address 209.165.201.8
...
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
```

тестовый экземпляр радиуса X серверов проверки подлинности

Все aaamgrs на 8/1 мертвы? никакие тестовые команды экземпляра радиуса не работают ни для одного из тех aaamgrs, но действительно работают для aaamgrs на 8/0 и других картах:

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
```

```
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun Dec 29 19:38:13 2013 Internal trap notification 42
(AAAAccSvrUnreachable) server 6 ip address 209.165.201.8
...
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
```

show radius противостоит всем

Ведущая команда для устранения проблем RADIUS показывает много таймаутов, которые увеличивают quckly:

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun Dec 29 19:38:13 2013 Internal trap notification 42
(AAAAccSvrUnreachable) server 6 ip address 209.165.201.8
...
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
```

Исправление

Во время периодов технического обслуживания миграция DPC 8 - 10 решила вопрос, trap-сообщения AAAAuthSrvUnreachable остановились, и DPC 8 был RMA'd, и основная причина была полна решимости быть отказом оборудования на DPC 8 (подробные данные того сбоя не важны для знания в целях этой статьи).

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun Dec 29 19:38:13 2013 Internal trap notification 42
(AAAAccSvrUnreachable) server 6 ip address 209.165.201.8
...
```

```
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
```