Network Working Group
Request for Comments: 3424
Category: Informational

L. Daigle, Ed.
Internet Architecture Board
IAB

November 2002

Соображения IAB по использованию UNSAF через NAT

IAB Considerations for UNilateral Self-Address Fixing (UNSAF) Across Network Address Translation

Статус документа

Этот документ содержит информацию для сообщества Internet и не задает каких-либо стандартов Internet. Документ может распространяться свободно.

Авторские права

Тезисы

По самой природе трансляции сетевых адресов (NAT[1]) взаимодействующие конечные точки, разделенные одним или множеством устройств NAT, не знают, как обозначить себя с использованием адресных областей своих (текущих или будущих) партнеров. Были внесены разные предложения для процессов UNSAF[2]. С помощью такого процесса конечная точка-инициатор пытается определить или зафиксировать адрес (и номер порта), с которым она будет известна другой конечной точке (например, чтобы иметь возможность использования данных адреса в протокольном обмене или анонсировать общедоступный адрес, по которому она будет принимать соединения).

В этом документе очерчены причины, по которым такие предложения могут рассматриваться лишь в качестве временных мер, а также конкретные вопросы, которые должны быть внимательно изучены до создания окончательного решения UNSAF.

1. Введение

По самой природе трансляции сетевых адресов (NAT) взаимодействующие конечные точки, разделенные одним или множеством устройств NAT не знают, как обозначить себя с использованием адресов, приемлемых в адресных диапазонах своих (текущих или будущих) партнеров — устройства NAT транслируют адреса. Для некоторых целей конечным точкам нужно знать адреса (и/или порты), под которыми они известны своим партнерам. Здесь можно выделить два случая - 1) клиент инициирует соединение, которое организует привязку адреса в устройстве NAT и выделение адреса, который является внешним по отношению к транслятору NAT, и 2) сервер принимает соединения извне, но не инициирует соединений сам и привязки адреса в NAT не создается. В таких случаях нужна фиксация адресных привязок до того, как начнется обмен данными.

Односторонняя фиксация своего адреса (UNSAF) — это процесс, с помощью которого конечная точка-инициатор пытается определить или зафиксировать адрес (и номер порта), с которым она будет известна другой конечной точке (например, чтобы иметь возможность использования данных адреса в протокольном обмене или анонсировать общедоступный адрес, по которому она будет принимать соединения).

Имеются лишь эвристические и обходные попытки добиться нужного эффекта, но 100% решения не найдено. Поскольку устройства NAT могут динамически отзывать или менять преобразования, нужны периодические опросы или средства поддержки жизнеспособности (keep-alive). Использование этих обходных решений в протоколах IETF **должно** рассматриваться, как временная мера, и нужен поиск лучшего, архитектурного решения. Явное намерение заключается в отказе от всех обходных решений при появлении эффективной технической модели.

2. Архитектурные аспекты, воздействующие на системы UNSAF

Вообще говоря, предложенные обходные решения подходят для случаев, когда происходят стандартные протокольные коммуникации между парами конечных точек, но для обеспечения возможности таких коммуникаций нужно сначала определить или зафиксировать воспринимаемый адрес конечной точки в другой адресной области. Предложения требуют, чтобы конечная точка искала «фиксацию» своего адреса, контактируя с участвующей службой (в другой адресной области) для определения своего адреса. Таким образом, появляется клиент UNSAF, взаимодействующий с некой формой сервиса UNSAF, который может быть (не обязательно) связан с целевой конечной точкой, с которой нужно организовать реальный обмен данными. В этом документе термины «сервер UNSAF» и «служба (сервис) UNSAF» будут указывать процесс, принимающий участие в определении адреса для процесса-инициатора (клиент UNSAF).

Все пользователям этих обходных решений следует принимать во внимание наличие конкретных технических проблем, препятствующих созданию общего решения, включая перечисленные ниже аспекты.

- Отсутствие уникальности нахождения «вне» (outside) NAT - возможны ситуации, когда нельзя сказать, где находится целевая конечная точка относительно инициатора — как клиенту UNSAF найти подходящий сервер UNSAF для отражения адреса? (см. Приложение C).

[1]Network Address Translation.
[2]UNilateral Self-Address Fixing - односторонняя фиксация своего адреса.

- В частности, по причине невозможности точно указать границу адресной области (внутри или снаружи, частная или публичная, несколько частных областей маршрутизации трафика) местоположение адреса можно определить лишь относительно конкретной точки сети. Если сервис UNSAF, отражающий адрес клиента UNSAF, размещается в другой подсети с маскированием NAT по отношению к некому другому сервису X, которым клиент желает воспользоваться, **не будет гарантии** совпадения «воспринимаемого» клиентом адреса от партнера UNSAF с адресом, видимым сервису X (см. Приложение C).

- В отсутствие связи с промежуточным устройством (midcom[1]) нет способа направить входящие коммуникации через промежуточное устройство (транслятор NAT, межсетевой экран) с надлежащим контролем. Обходя NAT, механизмы UNSAF могут также (непреднамеренно) обходить механизмы защиты. Особая опасность заключается в том, что внутренние машины невольно раскрываются для вредоносных коммуникаций с внешней стороны, который межсетевой экран должен блокировать. Это совершенно неприемлемо в тех случаях, когда процесс UNSAF работает на машине, имеющей возможность действовать от имени нескольких других.

- Предложенные обходные решения включают использование похожих на ping запросов для определения адреса, передаваемых от клиента UNSAF (инициатор) серверу UNSAF (ответчик), на которые тот отвечает по транспортному адресу инициатора, находясь в своей адресной области. Однако при использовании транспорта без организации явных соединений (например, UDP, IPsec ESP и т. п.) процесс UNSAF должен внимательно реагировать на смену отображения NAT для данного прикладного потока, поскольку это отображение может меняться непредсказуемо.

- Если клиент UNSAF периодически пытается обновить или переоценить состояние трансляции, на клиенте и сервере UNSAF требуется поддержка информации о предполагаемом состоянии соединения, для того, чтобы управлять адресами.

- Поскольку сервер UNSAF не интегрируется с устройством middlebox, он может лишь полагаться на прошлое поведение для предсказания будущего. Сервер не имеет специальной информации об эвристике трансляции адресов или воздействующих факторах.

- Обмен данными становится более «хрупким» за счет введения других серверов (серверы UNSAF), которые нужны для успешных коммуникаций между участниками — растет число устройств «с общей судьбой», участвующих в коммуникациях.

Обходные решения могут смягчить некоторые из отмеченных проблем, за счет жесткой фиксации сферы применения и внесения конкретных правок. Например:

- вместо поиска адреса от внешнего устройства NAT, применимость решения может быть ограничена получением «самозаданного» адреса (self-address) от некого конкретного сервиса для использования исключительно с этим сервисом;

- ограничение области действия внешних запросов для обслуживания (или инициирования обслуживания) с целью предотвращения неприемлемых нарушений защиты.

3. Практические вопросы

Из наблюдений за развернутыми сетями становится ясно, что разные реализации трансляторов NAT существенно отличаются по методам обработки разных случаев трафика и адресации.

Ниже перечислены некоторые из отмеченных особенностей поведения реализаций.

- Трансляторы NAT могут отбрасывать фрагменты пакеты в обоих направлениях — без полных заголовков TCP/UDP устройство NAT может оказаться неспособным выполнить отображение и просто отбросит пакет.

- Выпускаемые трансляторы NAT часто включают шлюзы приложений (ALG[2]), которые пытаются работать в зависимости от контекста по номерам портов отправителей и получателей. Поведение ALG может оказаться трудно предсказуемым и не всегда документировано.

- Большинство реализаций NAT с поддержкой ALG, которые пытаются транслировать прикладные протоколы TCP, выполняют свои функции не совсем корректно в тех случаях, когда транслируемая строка оказывается разделенной между несколькими сегментами TCP. В некоторых из таких трансляторов возникают отказы при наличии необязательных заголовков TCP (например, временных меток).

- Реализации NAT заметно различаются по способам обработки пакетов. Некоторые способны надежно работать лишь с пакетами TCP, но не UDP. Некоторые из пытающихся работать с UDP недостаточно аккуратно устанавливают таймеры старения потоков, значения которых могут меняться в широких пределах, делая поведение трансляторов непредсказуемым.

- Смена выделенных адресов и портов может происходить достаточно часто — в трансляторах NAT номера портов меняются всякий раз или это не предсказуемо, несколько трансляторов NAT могут быть включены параллельно для распределения нагрузки и это может приводить к частой смене адресов IP.

4. Архитектурные аспекты

Отмечая упомянутые выше подходы, как краткосрочные решения, IAB надеется, что в предложениях будут явно решены перечисленные ниже вопросы.

1. Точное определение конкретной проблемы, которая будет решаться с предложением UNSAF. Краткосрочные решения не следует обобщать для решения других проблем. Такие обобщения ведут к продолжению зависимости и применения краткосрочного решения, которое, в результате, уже не может называться краткосрочным.

[1]Middlebox communication.
[2]Application Layer Gateway — шлюз прикладного уровня.

2. Описание стратегии и плана перехода. Лучшими краткосрочными решениями будут те, которые будет постепенно исчезать по мере развертывания подходящей технологии.
3. Обсуждение конкретных проблем, которые могут сделать систему более «хрупкой». Например, подходы, включающие использование данных от множества сетевых уровней создают избыточные зависимости, усложняют отладку и делают переход более трудным.
4. Определение долгосрочных требований, обоснованные технические решения, поиск правильного долгосрочного решения.
5. Обсуждение влияния отмеченных технических проблем на развернутые системы NAT и отчеты о результатах.

5. Вопросы безопасности

Как общий класс обходных решений, предложения UNSAF могут создавать проблемы безопасности (дыры), поскольку в отсутствие связи с промежуточными устройствами нет способа направить входящие коммуникации через межсетевой экран с надлежащим контролем (с соблюдением политики безопасности, а не обходом ее).

Приложение A. Члены IAB на момент создания документа

Harald Alvestrand

Ran Atkinson

Rob Austein

Fred Baker

Leslie Daigle

Steve Deering

Sally Floyd

Ted Hardie

Geoff Huston

Charlie Kaufman

James Kempf

Eric Rescorla

Mike St. Johns

Приложение B. Благодарности

В подготовке этого документа важную роль сыграли подробные комментарии и предложения от Thomas Narten, Bernard Aboba, Keith Moore и James Woodyatt.

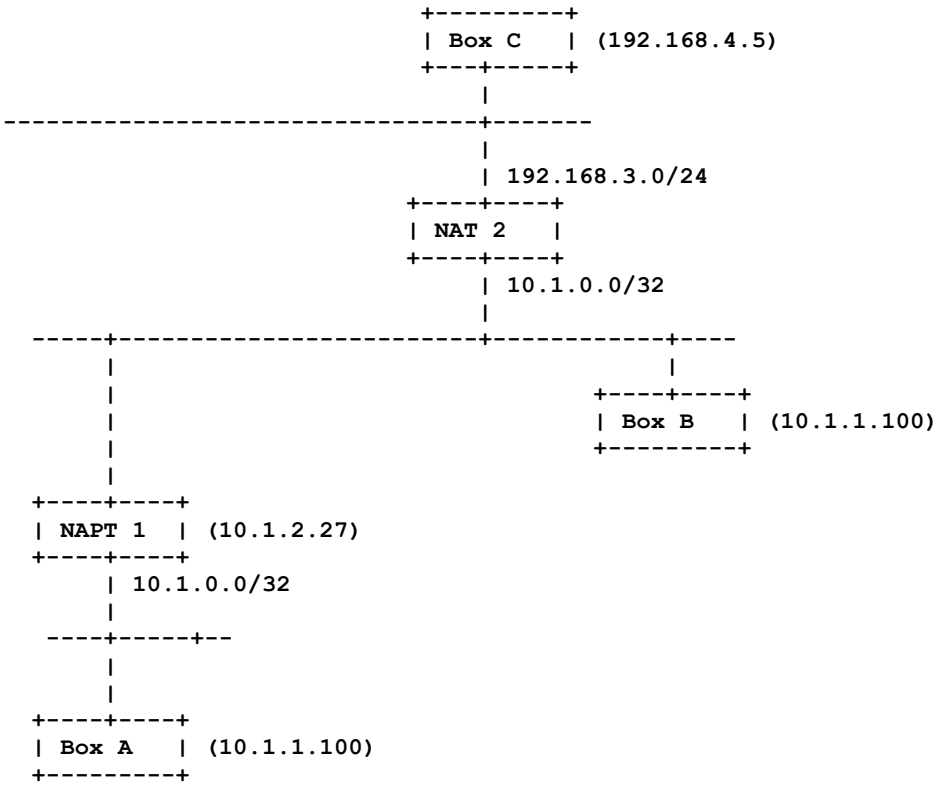
Исходный вариант документа был подготовлен, когда в состав IAB входили Steve Bellovin, Brian Carpenter, Jon Crowcroft, John Klensin и Henning Schulzrinne, которые внесли существенный вклад в создание документа.

Приложение C. Примеры NAT

C.1 Корпоративная сеть с NAT

На рисунке приведен пример ситуации, когда сложно описать, кто находится «снаружи» данной области адресации (связанной мостами NAPT). Такой вариант конфигурации может возникать в корпоративной среде, где разные подразделения используют свои подсети (каждая со своим пространством приватных адресов). Подразделения соединены между собой так, что они могут обмениваться данными через свои сети, но для доступа в Internet каждое использует свой транслятор NAPT с функциями МСЭ.

С точки зрения Box B адресом Box A будет 10.1.2.27 (внешний адрес транслятора). Однако с точки зрения Box C адрес Box A будет относиться к сети 192.168.3.0/24.



C.2 Пример реальной домашней сети

James Woodyatt представил приведенный ниже сценарий, основанный на реальных примерах продукции для домашних сетей:

- пользователь подключается к Internet через оператора широкополосного доступа, используя, например, линию DSL, подключенную к устройству, совмещающему в себе функции модема DSL и маршрутизатора/МСЭ с поддержкой NAT;
- такие устройства иногда поставляются со встроенными в ПО функциями автоматической настройки конфигурации и пользователь может воспринимать это, как часть услуг ISP;
- пользователь хочет также работать с хостом, имеющим только беспроводный интерфейс и покупает для этого точку беспроводного доступа, в которой по умолчанию включена трансляция NAT и сервер DHCP;
- в результате у пользователя возникают две области с приватными адресами — одна в проводной ЛВС, другая в беспроводной сети.

Более того, для основной масса пользователей слова «область адресов» (address realm) не значат ровным счетом ничего. Они просто хотят знать, почему сервер печати не доступен с беспроводного ноутбука. Протокол обнаружения устройств использует пакеты UDP с TTL=1, но это не имеет значения, поскольку все отклики будут отбрасываться транслятором NAT, не имеющим в своем составе ALG.

Адрес автора

Leslie Daigle

Редактор

Internet Architecture Board

IAB

EMail: iab@iab.org

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.