УДК 004.4, 004.6, 004.7

**ОБЕСПЕЧЕНИЕ ПЕРЕДАЧИ ПОТОКОВЫХ ДАННЫХ ИЗ ЛОКАЛЬНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ NAT[1]**

Тейхриб Антон Павлович
*ООО "Смартьюб", Екатеринбург, Россия*

В статье приводится описание различных типов NAT, которые могут использоваться при передаче потоковых данных. Описаны механизмы, которые могут применяться для обеспечения передачи потоковых данных через NAT

Ключевые слова: NAT, STUN, TURN, ICE, TEREDO, ПЕРЕДАЧА ПОТОКОВЫХ ДАННЫХ

UDC 004.4, 004.6, 004.7

**DATA STREAMING FROM LAN WITH NAT**

Teykhrib Anton Pavlovich
*Smartube Company, Yekaterinburg, Russia*

In this article, different types of NAT, which can be used in case of data streaming, are described. Also, different NAT traversal solutions suitable for data streaming are presented

Keywords: NAT, STUN, TURN, ICE, TEREDO, DATA STREAMING

Использование трансляции сетевых адресов NAT (Network Address Translation) в локальных сетях является одной из важнейших особенностей, влияющих на разработку программного обеспечения, связанного с приемом и передачей потоковых данных. В рамках данной статьи рассматривается взаимодействие пользователя и некоторого сервиса, которое осуществляется с целью обмена потоковыми данными между ними. Данное взаимодействие строится на основе использования в качестве сигнального протокола — SIP, а также протокола RTP для непосредственной передачи потоковых данных.

## Преобразование сетевых адресов

Преобразование сетевых адресов является ключевым моментом с точки зрения доступности сервиса конечному пользователю при взаимодействии посредством открытых каналов доступа. Переход между локальными сетями, а также между локальной и глобальной сетью, как правило, связан с трансляцией адресов. Случай вложенности локальных сетей, при котором осуществляется трансляция адресов на границе между ними, не является принципиальным и не рассматривается в рамках данной статьи.

[1] Работа поддерживается Министерством образования и науки Российской Федерации, ГК 14.514.11.4012.

В Таблице 1 приведены возможные варианты сочетания расположения сервиса и конечного пользователя относительно сети и количество используемых трансляций адресов.

Таблица 1 - Варианты сочетания расположения сервиса и конечного пользователя

| | Сервис в локальной сети | Сервис имеет непосредственный доступ к глобальной сети Интернет с предоставлением «белого» ip адреса |
|---|---|---|
| Пользователь в локальной сети | Используется две трансляции адресов: на стороне сервиса и на стороне конечного пользователя | Используется одна трансляция адресов на стороне конечного пользователя |
| Пользователь имеет непосредственный доступ к глобальной сети Интернет с предоставлением «белого» ip адреса | Используется одна трансляция адресов на стороне сервиса | Используется одна трансляция адресов на стороне конечного пользователя |

Преобразование сетевых адресов оказывает значительное влияние на доступность сервиса: конечный пользователь в локальной сети может быть недоступен из глобальной сети или информация, отправляемая конечным пользователем в сервис, например контактные данные, может оказаться недействительной в глобальной сети. Для обеспечения хорошего уровня доступности сервиса необходимо минимизировать количество трансляций адресов, что может быть достигнуто за счет выставления сервиса в глобальной сети с присвоением ему сетевого адреса. Это доступное организационное решение позволит ликвидировать преобразование сетевых адресов на стороне сервиса и, таким образом, остается решить только задачу корректной обработки трансляций на стороне пользователя сервиса.

Далее рассматриваются доступные технологии для решения проблемы обеспечения доступности сервиса при наличии преобразования

сетевых адресов, а также технологии, которые могут использоваться для разрешения возникающих сопутствующих проблем.

## Особенности передачи потоковых данных при использовании NAT

Сигнальный протокол SIP предназначен для установления соединения, завершения соединения и определения параметров соединения, таких как, используемые форматы передачи данных, информация о конечных точках для соединения, типы потоковых данных и т.п. Для непосредственной передачи потоковых данных используется протокол RTP. Передача потоковых данных осуществляется между конечными точками и с параметрами соединения, которые были определены по сигнальному протоколу. Передача потоковых данных начинается после установления соединения по сигнальному протоколу и заканчивается после завершения соединения по сигнальному протоколу.

Преобразование сетевых адресов изменяет конечные точки, которые используются для передачи потоковых данных и дальнейших сигнальных сообщений. При этом выявляется следующая проблема: с одной стороны NAT подменяет адрес и порт на транспортном уровне, с другой стороны пакеты содержат в себе адреса и порты на уровне приложений. Это приводит к недостоверности приходящих сообщений и невозможности корректной их обработки и, как следствие, к следующим инцидентам: невозможность установить сеанс передачи данных; сеанс создан, однако потоковые данные не передаются; сеанс создан, однако потоковые данные передаются только в одну сторону. Прозрачность для приложения — одно из основных преимуществ NAT, но она не дает возможности получать необходимую информацию приложениям, использующим NAT, что затрудняет формирование сигнальных сообщений.

## Типы NAT

Стандарты определяют несколько типов NAT, использование которых имеет свои особенности. В первой версии стандарта STUN предлагается ввести следующие типы NAT [5]:

- Конический — все запросы от одного и того же локального ip адреса и порта привязываются к одному и тому же внешнему ip адресу и порту, все пакеты, приходящие на этот внешний ip адрес и порт направляются данному локальному узлу вне зависимости от ip адреса и порта источника этих пакетов.
- Ограниченный конический — аналогичен коническому, особенность данного типа состоит в том, что внешние пакеты перенаправляются локальному узлу только в случае, если до этого локальный узел уже отправлял пакеты этому внешнему отправителю (проверка осуществляется по ip адресу).
- Конический, ограниченный по порту — аналогичен ограниченному коническому, дополнительно выполняется проверка по порту внешнего отправителя.
- Симметричный — все запросы от одного и того же локального ip адреса и порта направленные одному адресату привязываются к одному и тому же внешнему ip адресу и порту, в случае смены адресата, данному локальному узлу будет привязана другая пара «ip адрес-порт».

Для выполнения приема и передачи потоковых данных необходимо определять тип NAT и внешние ip адрес и порт, которые будут использоваться для взаимодействия с сервисом. Описание влияния того или иного типа NAT на передачу сигнальных сообщений и потоковых данных представлено в Таблице 2.

Таблица 2 - Влияние типа NAT на передачу данных

| Тип NAT | Влияние |
|---|---|
| Конический | При формировании сигнальных сообщений достаточно получить свой внешний ip адрес и порт, и затем в теле сообщений подменять свой локальный на полученный внешний.<br>Дальнейших проблем в данном случае не будет, т.к. с помощью NAT пакеты будут успешно маршрутизироваться на локальный ip адрес и порт |
| Ограниченный конический | Ситуация аналогичная коническому, особенность в том, что необходимо выполнять отправку какого-либо пакета на ip адрес сервиса |
| Конический, ограниченный по порту | Ситуация аналогична ограниченному коническому, особенность в том, что пакет должен быть отправлен на ip адрес и порт сервиса |
| Симметричный | Данный случай является самым сложным, т.к. необходимо получать два внешних ip адреса и порта.<br>Первый будет привязан в случае сигнального взаимодействия с сервисом, а другой необходимо получить для передачи потоковых данных |

Представленная выше классификация типов NAT считается слишком общей и не позволяет определить все возможные варианты настройки NAT. Существует альтернативный вариант, представленный в более позднем стандарте [3], который учитывает следующие характеристики и делает классификацию NAT более точной:

- Привязка адресов и портов — данная характеристика определяет механизм, по которому назначаются внешний ip адрес и порт: независимый от адресата, зависящий от ip адреса адресата или зависящий от порта и ip адреса адресата. Для описания вариантов отображения используется схема сети, представленная на рисунке 1.

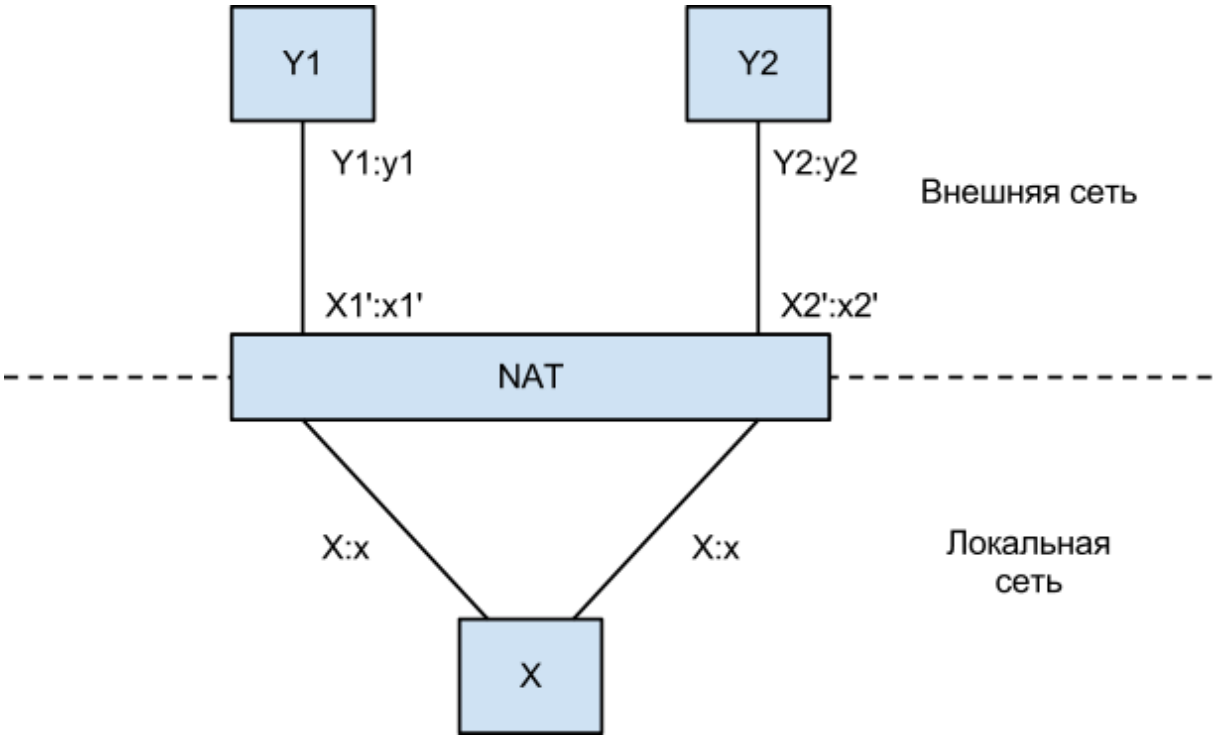


Рисунок 1 - Демонстрационная схема сети.

На рисунке 1 пара ip адрес: порт для узла Y1 обозначена «Y1:y1», а пара внешний ip адрес: порт — «X1':x1'». Соответственно, независимый от адресата — X1' = X2' и x1' = x2' вне зависимости от значений Y2 и y2. Зависящий от ip адреса адресата —X1' = X2' и x1' = x2' только в том случае, если Y1 = Y2. Зависящий от порта и ip адреса адресата — X1' = X2' и x1' = x2' только в том случае, если Y1 = Y2 и y1 = y2.

- Назначение порта — данная характеристика определяет, каким образом назначается внешний порт, в частности: способы разрешения инцидентов в случае наличия нескольких пользователей, обращающихся наружу с одного порта; «парность» портов — четным локальным портам назначаются четные внешние порты и, аналогично, нечетным, данное свойство связывается с протоколом RTP для передачи потоковых данных, а также протоколом RTCP, который используется для управления потоковой передачей данных, и последовательность назначаемых портов.

- Длительность сохранения привязки — характеристика определяет длительность сохранения назначенной пары «внешний ip адрес:порт» для некоторого локального узла.
- Фильтрация трафика — данная характеристика определяет правила, по которым фильтруются входящие пакеты. Возможны следующие варианты. Фильтрация, независимая от источника — для получения пакета на некоторый внешний ip адрес:порт достаточно отправить исходящий пакет на любой ip адрес:порт. Фильтрация, зависящая от ip адреса источника — пакет на некоторый внешний ip адрес:порт может быть получен только от источника, ip адрес которого совпадает с тем, на который до этого был отправлен пакет, сформировавший данную привязку. Фильтрация, зависящая от порта и ip адреса источника — пакет на некоторый внешний ip адрес:порт может быть получен только от источника, ip адрес и порт которого совпадает с тем, на который до этого был отправлен пакет, сформировавший данную привязку.
- Возможность передачи данных через внешний интерфейс в локальную сеть — данная характеристика определяет возможность взаимодействия двух узлов, расположенных в локальной сети передавать данные через внешний интерфейс.
- Использование шлюзов уровня приложений (ALG), т.к. некоторые устройства трансляции адресов работают на уровне приложения, например, заменяя локальный ip адрес:порт на привязанный внешний ip адрес:порт в теле пакета на уровне приложения.
- Предсказуемость — данная характеристика определяет, меняется ли способ привязки ip адреса и порта во время работы транслятора.

- Отправка сообщений ICMP о недоступности порта.
- Возможность фрагментации исходящих пакетов.
- Возможность получения фрагментированных входящих пакетов.

В рамках передачи потоковых данных наибольший интерес представляют следующие характеристики, влияющие на взаимодействие с сервисом: привязка адресов и портов, длительность сохранения привязки, фильтрация трафика и использование ALG. Для успешного выполнения приема и передачи потоковых данных необходимо расширить круг задач и, кроме определения типа NAT и внешних ip адрес и порт, которые будут использоваться для взаимодействия с сервисом, определять необходимость использования ALG и длительности сохранения привязки. Далее рассматриваются технологии, используемые для решения данных задач.

## Технологии решения проблем, связанных с использованием NAT

Для решения проблем взаимодействия посредством NAT используются различные технологии:

- STUN — набор средств для прохождения сессий через NAT, в том числе реализующих алгоритм определения типа [4].
- TURN — средства для обхода NAT на основе транслирующих серверов [6].
- ICE — техника интерактивной установки соединения STUN или TURN [2].
- Teredo — туннелирование ipv6 UDP трафика через NAT.

STUN — сетевой протокол для прохождения сессий через NAT, позволяющий клиенту определить свой внешний ip-адрес, способ трансляции адреса и порт во внешней сети, связанный с определённым внутренним номером порта а также реализующий алгоритм определения типа NAT [4].

На данный момент существует два варианта протокола: первый вариант стандарта (Classic STUN) и текущий вариант стандарта (STUN). Classic STUN предлагает алгоритм определения типа NAT и позволяет определять внешний ip адрес и порт, которые привязываются локальному узлу NAT транслятором. Использование STUN подразумевает, что есть некий сервер, реализующий данный протокол, который имеет два публично доступных ip адреса.

Следует учитывать, что в таком режиме могут быть пройдены только различные варианты конического NAT. Симметричный NAT обладает другими характеристиками фильтрации пакетов и способами привязки ip адреса и порта, что не позволяет использовать полученные внешний ip адрес и порт, так как либо при обращении к сервису он будет другой, либо пакеты от сервиса не будут переданы клиенту. Для решения описанной проблемы необходимо использовать технологии TURN для обхода NAT на основе транслирующего сервера, который будет непосредственного взаимодействовать с клиентом. При этом сам транслирующий сервер имеет внешний ip адрес и далее дополнительных трансляций адресов не выполняется. TURN позволяет узлу за NAT получать входящие данные через TCP или UDP соединения и предназначен для решения ситуаций, которые возникают в случае использования NAT, привязывающих ip адреса и порты в зависимости от ip адреса адресата, или от ip адреса и порта адресата. Схема сети, в которой осуществляется взаимодействие TURN, представлена на рисунке 2.

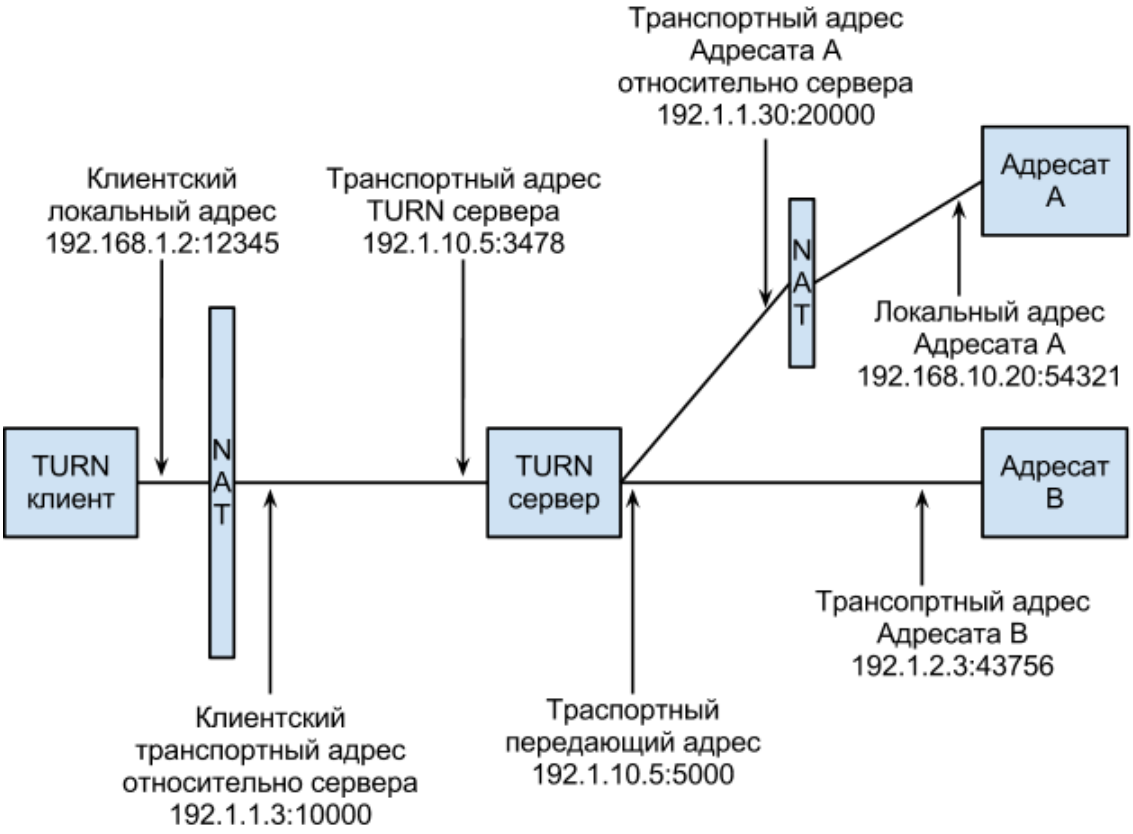


Рисунок 2 - Схема сети TURN

Взаимодействие в сети TURN осуществляется по определенному алгоритму. Клиент инициирует создание передающего адреса и в дальнейшем управляет этой привязкой. Если адресат хочет отправить некоторые данные клиенту, то он отправляет их на передающий адрес, а затем TURN сервер передает их в виде TURN пакета клиенту. Взаимодействие возможно с несколькими адресатами одновременно через один передающий адрес, индикация адресата задается в TURN пакете. За счет того, что ip адрес и порт TURN сервера, с которыми осуществляется взаимодействие, являются фиксированными, способ привязки ip адреса и порта, а также фильтрация трафика перестают оказывать негативное влияние на передачу данных.

Таким образом, использование TURN позволяет избежать проблем, возникающих при использовании NAT, привязывающих ip адреса и порты в зависимости от ip адреса адресата, либо от ip адреса и порта адресата. На данный момент TURN считается включенным в STUN, как один из

способов прохода NAT. Рекомендуется использовать TURN только, как крайнюю меру, в случае, когда использование STUN не позволяет осуществить передачу данных, использование TURN во всех случаях передачи данных приводит к тому, что весь трафик взаимодействия между узлами начинает проходить через TURN сервер. Определить наиболее подходящий метод для конкретных условий передачи потоковых данных позволяет ICE протокол [2], который регламентирует механизм выбора между STUN или TURN.

Teredo изначально предназначался для передачи ipv6 пакетов по ipv4, однако может использоваться и самостоятельно. Данная технология осуществляет взаимодействия с NAT аналогичным STUN, отличие заключается в том, что используется привязка не ipv4 адреса, а ipv6 и взаимодействие осуществляется путем обертывание ipv6 пакета в ipv4 [1] рисунок 3.

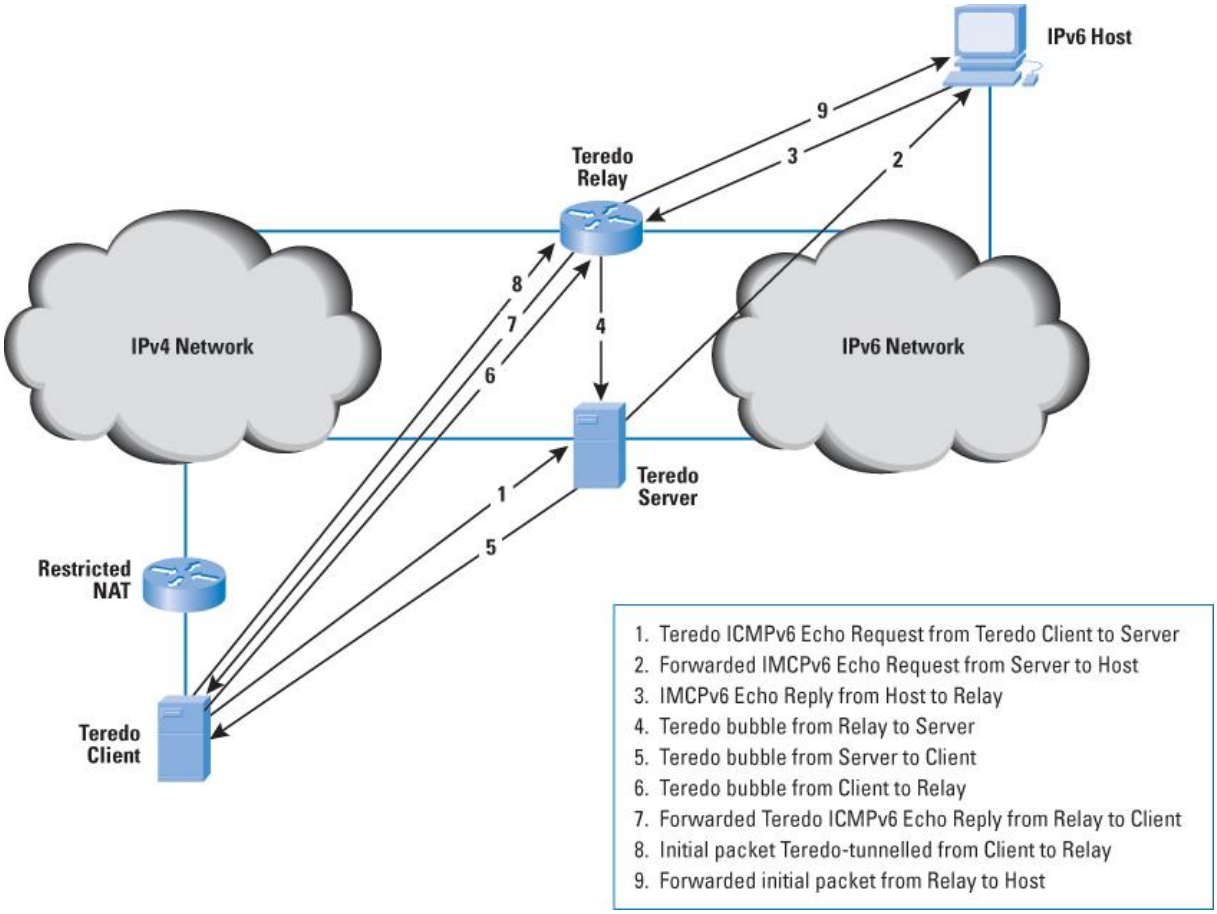


Рисунок 3. Схема сети Teredo

Недостатком метода Teredo является то, что он не позволяет работать с симметричным NAT. Узел, расположенный за симметричным NAT, будет иметь два разных адреса при взаимодействии с teredo реле и teredo сервером.

Альтернативным вариантом решения проблем, связанных с использованием NAT, является разработка самостоятельного решения, которое может быть интегрировано в сервис. Существенное отличие его от представленных выше вариантов заключается в том, что при обеспечении взаимодействия сервиса и конкретного ПО клиента можно добиться сокращения издержек, за счет мультиплексирования сигнальной информации и потоковых данных на одном ip адресе и порту, а также протокола для определения внешнего ip адреса и порта клиента. Благодаря такой парадигме может быть использована урезанная версия STUN, всего с одним ip адресом.

## Выводы

В статье были рассмотрены различные типы NAT для передачи потоковых данных из локальных сетей, на основе взаимодействия пользователя и некоторого сервиса, обеспечивающего обработку потоковых данных. На основе сравнения различных вариантов стандартизованных технологий использования NAT был получен вывод, что полностью решить проблему прохождения NAT позволяет использование протокола ICE. Отмечено, что данный протокол является достаточно сложным в реализации, поэтому альтернативным способом является использование собственного способа для прохождения NAT, который позволит применить стандартизованных технологий в сокращенном варианте, при условии сохранении работоспособности сервиса.

Работа поддерживается Министерством образования и науки Российской Федерации, ГК 14.514.11.4012.

**Список литературы:**

1. Geoff Huston, APNIC [Электронный ресурс]: The Internet Protocol Journal, Volume 14, No.1 Transitioning Protocols – Режим доступа: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-1/141_protocols.html
2. Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols [Электронный ресурс]: PROPOSED STANDARD – April 2010 – Режим доступа: http://tools.ietf.org/html/rfc5245
3. Network Address Translation (NAT) Behavioral Requirements for Unicast UDP [Электронный ресурс]: PROPOSED STANDARD – January 2007 – Режим доступа: http://tools.ietf.org/html/rfc4787
4. Session Traversal Utilities for NAT (STUN) [Электронный ресурс]: PROPOSED STANDARD – October 2008 – Режим доступа: http://tools.ietf.org/html/rfc5389
5. STUN — Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) [Электронный ресурс]: PROPOSED STANDARD – March 2003 – Режим доступа: http://tools.ietf.org/html/rfc3489
6. Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN) [Электронный ресурс]: PROPOSED STANDARD – April 2010 – Режим доступа: http://tools.ietf.org/html/rfc5766

**References:**

1. Geoff Huston, APNIC [Electronic resource]: The Internet Protocol Journal, Volume 14, No.1 Transitioning Protocols – Mode Access: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-1/141_protocols.html
2. Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols [Electronic resource]: PROPOSED STANDARD – April 2010 – Mode Access: http://tools.ietf.org/html/rfc5245
3. Network Address Translation (NAT) Behavioral Requirements for Unicast UDP [Electronic resource]: PROPOSED STANDARD – January 2007 – Mode Access: http://tools.ietf.org/html/rfc4787
4. Session Traversal Utilities for NAT (STUN) [Electronic resource]: PROPOSED STANDARD – October 2008 – Mode Access: http://tools.ietf.org/html/rfc5389
5. STUN — Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) [Electronic resource]: PROPOSED STANDARD – March 2003 – Mode Access: http://tools.ietf.org/html/rfc3489
6. Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN) [Electronic resource]: PROPOSED STANDARD – April 2010 – Mode Access: http://tools.ietf.org/html/rfc5766