Network Working Group
Request for Comments: 2486
Category: Standards Track

B. Aboba
Microsoft
M. Beadles
WorldCom Advanced Networks

January 1999

Идентификатор доступа в сеть

The Network Access Identifier

Статус документа

Данный документ содержит спецификацию стандартного протокола Internet, предложенного сообществу Internet, и является приглашением к дискуссии в целях развития этого протокола. Сведения о текущем состоянии стандартизации протокола вы найдете в документе "Internet Official Protocol Standards" (STD 1). Документ можно распространять без ограничений.

Авторские права

1. Тезисы

Для повышения уровня интероперабельности служб роуминга и туннелирования желательно иметь стандартизованный метод идентификации пользователей. В этом документе предлагается синтаксис идентификатора доступа в сеть (NAI[1]) - идентификатора пользователя (userID), представляемого клиентом в процессе аутентификации PPP. Предполагается, что такие идентификаторы представляют интерес для поддержки роуминга и туннелирования. «Возможность роуминга[2]» можно определить, как возможность использования любого из множества доступных поставщиков услуг доступа в Internet (ISP[3]) при наличии соглашения на обслуживание лишь с одним из провайдеров. Примерами ситуаций, когда может потребоваться роуминг, являются «конфедерации ISP» и обеспечиваемый через ISP доступ в корпоративную сеть.

2. Введение

Интерес к роумингу возник сравнительно недавно у пользователей, подключающихся к сети Internet по коммутируемым телефонным линиям. Наиболее интересны следующие ситуации:

- Региональные ISP, работающие на определенных территориях, могут объединяться для обслуживания пользователей на большей территории.
- Национальные ISP могут объединяться с другими национальными ISP-компаниями для предоставления доступа по коммутируемым линиям в нескольких странах.
- Предприятия, которые хотят предложить своим сотрудникам полнофункциональный пакет услуг доступа по коммутируемым линиям в глобальном масштабе. Такой пакет услуг может включать доступ в Internet, а также защищенный доступ в корпоративные сети с использованием технологии виртуальных частных сетей (VPN[4]), с помощью протоколов туннелирования PPTP, L2F, L2TP, IPSEC.

Для расширения интероперабельности служб роуминга и туннелирования желательно иметь стандартизованный метод идентификации пользователей. В данном документе предлагается синтаксис идентификаторов доступа в сеть (NAI). Примеры реализации систем с использованием NAI и описание семантики идентификаторов можно найти в документе [1].

2.1. Терминология

Ниже приводятся определения некоторых терминов, которые достаточно часто используются в документе.

Network Access Identifier

Идентификатором доступа в сеть (NAI) называют идентификатор пользователя (userID), представленный клиентом в процессе аутентификации PPP. При роуминге назначение NAI состоит в идентификации пользователя и соответствующей маршрутизации запроса на аутентификацию. Отметим, что идентификатору NAI совсем не обязательно совпадать с пользовательским адресом электронной почты или значением userID, переданным в прикладную программу.

[1] Network Access Identifier.
[2] Roaming capability.
[3] Internet service provider.
[4] Virtual Private Network.

Network Access Server

Сервер доступа в сеть (NAS) представляет собой устройство, к которому клиенты обращаются по коммутируемым телефонным линиям для получения доступа в сеть. В контексте PPTP серверы доступа обычно называют концентраторами доступа PPTP (PAC[1]), а в контексте L2TP – концентраторами доступа L2TP (LAC[2]).

Roaming Capability

Возможность роуминга можно определить, как возможность использования любого из множества провайдеров Internet при наличии формального соглашения лишь с одним из ISP. Примерами ситуаций, когда требуется использование роуминга, могут служить «конфедерации ISP» и обеспечиваемый через ISP доступ в корпоративную сеть.

Tunneling Service

Туннельный сервис – это любой тип сетевых услуг, обеспечиваемых с использованием протоколов туннелирования типа PPTP, L2F, L2TP, IPSEC. Примером туннельного сервиса является защищенный доступ в корпоративные сети с использованием технологии виртуальных частных сетей (VPN).

2.2. Спецификация требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с [9].

2.3. Цель

Как отмечено в [1], существует множество служб, поддерживающих роуминг для доступа по коммутируемым линиям, и число ISP, вовлеченных в роуминговые соглашения, быстро растет.

Для того, чтобы предлагать пользователям возможности роуминга, требуется идентификация «домашнего» сервера аутентификации для пользователей. Для роуминга такая задача может быть решена с помощью идентификаторов доступа в сеть (NAI), представляемых пользователями серверам NAS на начальном этапе аутентификации PPP. Предполагается также, что серверы доступа будут использовать NAI как часть процесса создания нового туннеля для определения конечной точки этого туннеля.

2.4. Замечания для разработчиков

В этом документе предлагаются идентификаторы NAI в форме user@realm[3]. Отметим, что пользовательская часть NAI полностью соответствует требованиям BNF, указанным в [5], а BNF для области (realm) допускает использование цифр, что противоречит требованиям BNF, описанным в [4]. Это изменение отражает реальную ситуацию, поскольку доменные имена, начинающиеся с цифр, которые не допускаются требованиями BNF документа [4], реально используются в FQDN (например, 3com.com) и корректно обрабатываются современными программами.

Отметим, что от разработчиков серверов NAS может потребоваться изменение выпускаемых устройств для поддержки NAI в соответствии с данным документом. Устройства, обслуживающие NAI, **должны** поддерживать идентификаторы NAI размером до 72 октетов.

3. Определение формата NAI

Описанный ниже синтаксис NAI приводится в формате ABNF, соответствующем требованиям [7]. Синтаксис имен пользователей соответствует требованиям [5], а синтаксис идентификаторов областей – обновленной версии [4].

```
nai          = username / ( username "@" realm )
username     = dot-string
realm        = realm "." label
label        = let-dig * (ldh-str)
ldh-str      = *( Alpha / Digit / "-" ) let-dig
dot-string   = string / ( dot-string "." string )
string       = char / ( string char )
char         = c / ( "\" x )
let-dig      = Alpha / Digit
Alpha        = %x41-5A / %x61-7A   ; A-Z / a-z
Digit        = %x30-39  ;0-9
c            = < любые из 128 символов ASCII, кроме символов special и SP >
x            = %x00-7F  ; все 128 символов ASCII без исключений
SP           = %x20 ; символ пробела
special      = "<" / ">" / "(" / ")" / "[" / "]" / "\" / "."
                / "," / ";" / ":" / "@" / %x22  / Ctl
Ctl          = %x00-1F / %x7F
               ; управляющие символы (с кодом ASCII от 0 до 31 включительно и 127)
```

Примеры корректных идентификаторов доступа в сеть включают:

```
fred@3com.com
fred@foo-9.com
fred_smith@big-co.com
fred=?#$&*+-/^smith@bigco.com
```

[1] PPTP Access Concentrator
[2] L2TP Access Concentrator
[3] Пользователь@область (сеть)

```
fred@bigco.com
nancy@eng.bigu.edu
eng!nancy@bigu.edu
eng%nancy@bigu.edu
```

Ниже показаны примеры некорректных NAI:

```
fred@foo
fred@foo_9.com
@howard.edu
fred@bigco.com@smallco.com
eng:nancy@bigu.edu
eng;nancy@bigu.edu
<nancy>@bigu.edu
```

4. Литература

[1] Aboba, B., Lu J., Alsop J., Ding J. and W. Wang, "Review of Roaming Implementations", RFC 2194, September 1997.

[2] Rigney C., Rubens A., Simpson W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138[1], April 1997.

[3] Rigney C., "RADIUS Accounting", RFC 2139[1], April 1997.

[4] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035[1], November 1987.

[5] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821[2], August 1982.

[6] Gulbrandsen A. and P. Vixie, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2052, October 1996.

[7] Crocker, D. and P. Overrell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234[1], November 1997.

[8] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401[3], November 1998.

[9] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119[1], March 1997.

5. Вопросы безопасности

Поскольку идентификаторы NAI показывают принадлежность пользователя к сети, они могут помочь атакующим в исследовании пространства пользовательских имен. Обычно такая проблема возникает при использовании протоколов, в которых пользовательские имена передаются открытым текстом через сеть Internet (таких, как протокол RADIUS, описанный в документах [2] и [3]). Для предотвращения утечки сведений об именах пользователей, можно применять конфиденциальные службы, обеспечиваемые IPSEC [8].

6. Согласование с IANA

В этом документе определено новое пространство имен, которое требует администрирования, - пространство используемых в NAI имен realm. Чтобы избавиться от создания новых административных структур, управление именами областей NAI разумно совместить с администрированием доменных имен DNS.

Имена областей NAI должны быть уникальными и права на использование данного значения NAI realm для роуминга приобретаются вместе с правом использования соответствующего доменного имени (FQDN). Всякий, кто пожелает использовать имя NAI realm, должен сначала приобрести право использования соответствующего FQDN. Использование NAI realm без прав на использование соответствующего FQDN приведет к возникновению конфликтов и, следовательно, должно быть запрещено.

Отметим, что использование FQDN в качестве имени области не подразумевает использования DNS для поиска сервера аутентификации или маршрутизации используемых при аутентификации данных. Поскольку роуминг данных обеспечивается в сравнительно небольших областях, существующие реализации обычно поддерживают сведения о серверах аутентификации в домене и маршрутизируют данные аутентификации на основе локальных сведений из конфигурационных параметров proxy. Реализации, описанные в документе [1] не требуют использования DNS для поиска сервера аутентификации в домене, хотя такой поиск можно осуществить с использованием записей DNS SRV, описанных в [6]. Существующим реализациям не требуются и динамические протоколы маршрутизации или иные средства глобального распространения маршрутных данных. Отметим также, что идентификатор NAI совсем не обязан представлять собой корректный адрес электронной почты.

7. Благодарности

Спасибо Глену Зорну (Glen Zorn) из Microsoft за полезные дискуссии.

8. Адреса авторов

Bernard Aboba

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052

[1]Перевод этого документа имеется на сайте www.protocols.ru. *Прим. перев.*
[2]Этот документ признан устаревшим и заменен RFC 2821, который, в свою очередь, был заменен RFC 5321. Переводы документов доступны на сайте www.protocols.ru. *Прим. перев.*
[3]Этот документ в настоящее время заменен RFC 4301, перевод которого доступен на сайте www.protocols.ru. *Прим. перев.*

Phone: 425-936-6605

EMail: bernarda@microsoft.com

Mark A. Beadles

WorldCom Advanced Networks

5000 Britton Rd.

Hilliard, OH 43026

Phone: 614-723-1941

EMail: mbeadles@wcom.net

Перевод на русский язык

Николай Малых

EMail: nmalykh@gmail.com

9. Полное заявление авторских прав