Network Working Group
Request for Comments: 1413
Obsoletes: 931

M. St. Johns
US Department of Defense

February 1993

Протокол идентификации

Identification Protocol

Статус документа

Этот документ содержит спецификацию стандарта, предложенного сообществу Internet, и является запросом к обсуждению в целях дальнейшего развития протокола.

Состояние стандартизации документа можно выяснить в "IAB Official Protocol Standards"[1]. Документ может распространяться свободно.

1. Введение

Протокол идентификации (Identification Protocol, ident, Ident Protocol) обеспечивает способ идентификации пользователя для конкретного соединения TCP. Используя на входе номера пары соединенных между собой портов TCP, протокол возвращает строку символов, идентифицирующую владельца данного соединения на стороне сервера.

Первоначально протокол идентификации называли Authentication Server Protocol (протокол аутентификации сервера). Новое имя лучше отражает суть протокола. Данный документ является результатом работы группы TCP Client Identity Protocol в составе IETF.

2. Обзор

Протокол представляет собой сервис на основе соединений TCP. Сервер слушает соединения TCP для порта 113 (десятичный номер). После организации соединения сервер читает строку данных, содержащую сведения о цели соединения. При существовании идентификатора пользователя для соединения сервер передает этот идентификатор в качестве отклика. После этого сервер может закрыть соединение или продолжить диалог «запрос-отклик».

Серверу следует закрывать соединение по истечении заданного конфигурационными параметрами тайм-аута (60-180) при отсутствии каких-либо запросов. Клиент может закрыть соединение в любой момент, однако для компенсации возможных задержек в сети клиенту следует выждать по крайней мере 30 секунд после запроса прежде, закрыть соединение.

3. Ограничения

Передача запросов допустима только для полностью организованных соединений. Запрос содержит номера пары портов (локальный - удаленный), используемых для идентификации соединения и получаемых с указанием локального и удаленного адресов. Это означает, что пользователь с адресом A может запрашивать у сервера B только информацию о соединении между A и B.

4. Формат запросов и откликов

Сервер воспринимает простые текстовые запросы в формате:

<port-on-server>, <port-on-client>

где <port-on-server> указывает порт TCP (десятичное значение) для адресата (хоста, где работает сервер ident), а <port-on-client> указывает порт TCP (десятичное значение) на клиентской системе.

Важно отметить, что если клиент на хосте A хочет сделать запрос серверу на хосте B о соединении, заданном локально (на хосте A) парой портов 23, 6191 (входящее соединение TELNET), клиент должен сделать запрос для пары 6191, 23 (идентификация соединения с точки зрения хоста B).

Например:

```
6191, 23
```

Отклик имеет формат:

<port-on-server>, <port-on-client> : <resp-type> : <add-info>

где <port-on-server> и <port-on-client> совпадают с номерами портов в запросе, <resp-type> идентифицирует тип отклика, а <add-info> содержит зависящие от контекста данные.

Возвращаемая информация связана с соединением TCP, заданным параметрами <server-address>, <client-address>, <port-on-server>, <port-on-client> (<server-address> и <client-address> - IP-адреса обеих сторон соединения, а <port-on-server> и <port-on-client> - параметры запроса)

Например:

```
6193, 23 : USERID : UNIX : stjohns
6195, 23 : ERROR : NO-USER
```

5. Типы откликов

Отклики могут быть двух типов:

USERID

[1] В настоящее время – Internet Official Protocol Standards (RFC 3000). *Прим. перев.*

В этом случае строка <add-info> содержит название операционной системы (возможно, с указанием поддерживаемого набора символов), за которым следует разделитель ":" и строка идентификации.

Если отклик содержит набор символов, последний отделяется от имени операционной системы запятой (,). Для обозначения набора символов используются стандартные идентификаторы. Если набор символов не указан, предполагается US-ASCII (см. ниже).

Идентификаторы операционной системы должны указываться в соответствии с документов RFC 1340[1], Assigned Numbers или его «наследниками».

В дополнение к идентификаторам ОС, указанным в Assigned Numbers можно использовать специальный идентификатор "OTHER" (прочие ОС).

Если в качестве операционной системы не возвращается значение "OTHER", предполагается, что сервер возвращает «нормальную» идентификацию пользователя, который владеет данным соединением (строка символов, позволяющая однозначно определить пользователя – например, имя пользователя в системе или пользовательская часть почтового адреса). Если указана операционная система (т.е., строка отклика не содержит "OTHER"), предполагается, что имя пользователя также имеет смысл (например, для использования в качестве аргумента команды finger или как части почтового адреса).

Значение "OTHER" говорит о том, что дальнейшие данные являются неформатированной строкой печатных символов используемого в системе набора. Отклик "OTHER" следует возвращать, если идентификатор пользователя не соответствует описанным выше требованиям. Например, такой отклик следует передавать, если вместо имени пользователя возвращается реальное имя или телефонный номер из пользовательской записи UNIX.

Предполагается, что идентификатор пользователя содержит только печатные символы используемого в системе набора.

Идентификатор представляет собой строку октетов, не включающую символов (восьмеричное представление) 000 (NUL), 012 (LF) и 015 (CR). Важно подчеркнуть, что символы пробела (040), следующие за двоеточием, **являются** частью строки идентификатора и не должны игнорироваться. Обычно строка отклика завершается последовательностью CR/LF. Подчеркнем, что строка может содержать печатные символы, но **не обязана** содержать только их.

ERROR

Если по каким-то причинам владелец соединения не может быть определен, строка <add-info> сообщает о причине. Возможны следующие значения <add-info>:

INVALID-PORT

Один из портов указан некорректно. Такой отклик возвращается, если номер какого-нибудь (или обоих) из портов выходит за допустимые пределы (порты TCP могут нумероваться от 1 до 65535) или не является целым числом.

NO-USER

Указанное парой портов соединение в настоящее время не используется или принадлежит неизвестному объекту.

HIDDEN-USER

Сервер может определить пользователя, но не сообщает о нем по требованию этого пользователя.

UNKNOWN-ERROR

Причину ошибки не удается определить (любая причина, не указанная выше). Такой отклик может возвращаться и в тех случаях, когда сервер может определить причину ошибки, но не желает ее сообщать. Если на сервере реализована такая возможность, она должна быть настраиваемой и по умолчанию сервер должен возвращать корректное сообщение об ошибке.

В дальнейшем могут быть добавлены другие коды отклики. При использовании нестандартных откликов они должны начинаться с символа "X".

В дополнение к возврату откликов сервер может разрывать соединения, не возвращая никакого отклика. Преждевременное завершение соединения (клиент не получил символа EOL) должно трактоваться клиентом как отклик "ERROR : UNKNOWN-ERROR".

Формальный синтаксис

```
<request> ::= <port-pair> <EOL>
<port-pair> ::= <integer> "," <integer>
<reply> ::= <reply-text> <EOL>
<EOL> ::= "015 012"  ; CR-LF – идентификатор завершения строки
<reply-text> ::= <error-reply> | <ident-reply>
<error-reply> ::= <port-pair> ":" "ERROR" ":" <error-type>
<ident-reply> ::= <port-pair> ":" "USERID" ":" <opsys-field> ":" <user-id>
<error-type> ::= "INVALID-PORT" | "NO-USER" | "UNKNOWN-ERROR" | "HIDDEN-USER" |  <error-token>
<opsys-field> ::= <opsys> [ "," <charset>]
<opsys> ::= "OTHER" | "UNIX" | <token> ... и т. п.;  (см. "Assigned Numbers")
<charset> ::= "US-ASCII" | ... и т. п.;  (см. "Assigned Numbers")
<user-id> ::= <octet-string>
<token> ::= 1*64<token-characters> ; 1-64 символа
<error-token> ::= "X"1*63<token-characters> ; 2-64 символов, начинающихся с X
```

[1] В настоящее время RFC 1700. *Прим. перев.*

```
<integer> ::= 1*5<digit> ; 1-5 цифр.
<digit> ::= "0" | "1" ... "8" | "9" ; 0-9
<token-characters> ::= <a-z, A-Z, -, .!@#$%^&*()_=+.,<>/?"'~`{}[]; >
                   ; строчные и прописные буквы латиницы и другие печатные символы, кроме ":".

<octet-string> ::= 1*512<octet-characters>
<octet-characters> ::= <любые октеты от 00 до 377 (восьм.), кроме NUL(000), CR(015), LF (012)>
```

Примечания:

1. Для обеспечения интероперабельности различных реализаций в части трактовки символов пробела следует придерживаться общего принципа: «будь консервативным при передаче и либеральным на приеме». Клиентам и серверам не следует генерировать избыточных пробелов, но они должны воспринимать строки с лишними пробелами от других. Избыточные пробелы могут встречаться везде, кроме собственно маркеров (token). В частности, дополнительные пробелы могут встречаться в начале и в конце строк запросов и откликов. Однако дополнительные пробелы недопустимы в отклике с идентификатором пользователя после двоеточия вслед за именем операционной системы, поскольку в этом случае они будут трактоваться как часть имени пользователя (именем пользователя считается вся последовательность символов от двоеточия до символов завершения строки CR/LF). Символы CR/LF **не должны** рассматриваться как часть идентификатора пользователя.

2. Вопреки сказанному выше, серверам следует ограничивать число пробелов между элементами (маркерами) до минимально возможного (полезного). Клиент может разорвать соединение, получив более 1000 символов без сигнала завершения строки <EOL>.

3. Размер идентификатора пользователя следует ограничивать 512 символами, а размер маркера - 64 символами, поскольку: a) новые маркеры (т. е., OPSYS или ERROR-TYPE) будут иметь размер не более 64 символов и b) серверу **не следует** передавать более 512 октетов идентификатора пользователя, а клиент **должен** принимать первые 512 октетов идентификатора пользователя. Вследствие этих ограничения сервер **должен** возвращать наиболее важную часть идентификатора пользователя в первых 512 октетах.

4. Следует использовать только те наборы символов и идентификаторы этих наборов, которые указаны в RFC 1340, "Assigned Numbers" и более новых вариантах этого документа[1]. Идентификаторы набора символов применимы только к полям идентификации пользователя, а все остальные поля должны использовать набор символов US-ASCII.

5. Хотя поле <user-id> было определено выше как <octet-string> (строка октетов), оно должно соответствовать по формату и набору символов значению поля <opsys-field>; описанного выше.

6. Идентификатор набора символов обеспечивает для клиента контекст, позволяющий печатать или сохранять строку идентификации пользователя. Если клиент не может распознать или использовать указанный набор символов, ему следует трактовать строку идентификации как строку октетов (OCTET), сохраняя вместе с ней идентификатор использованного набора символов. Строку октетов в таких случаях следует печатать, сохранять и обрабатывать с 16-ричном представлении (0-9a-f) в дополнение к используемому клиентской реализацией представлению (это обеспечивает возможность стандартного представления в различных реализациях).

6. Вопросы безопасности

Уровень достоверности информации, возвращаемой данным протоколом, зависит от настроек запрашиваемого хоста и политики поддерживающей хост организации. Например, ПК, используемый в открытой лаборатории, может возвращать о себе любые сведения, которые пожелает указать пользователь. Более того, хост может возвращать специально искаженную (ложную) информацию.

Протокол Identification не предназначен для авторизации (проверки полномочий) или управления доступом. В лучшем случае этот протокол обеспечивает некоторые дополнительные сведения о соединениях TCP, в худшем - возвращает ошибочную, некорректную или умышленно искаженную информацию.

Использование возвращаемых протоколом сведений для каких-либо целей, кроме аудита, настоятельно не рекомендуется. В частности, использование протокола Identification для принятия решений о предоставлении доступа в качестве основного (т. е., при отсутствии других проверок) или дополнительного средства может существенно снизить уровень безопасности хоста.

Сервер идентификации может собирать сведения о пользователях, объектах и процессах, которые зачастую могут содержать приватные данные. Сервер идентификации обеспечивает услуги по типу служб CallerID, поддерживаемых некоторыми телефонными компаниями, и требования к сообщаемым сервером сведениям формируются так же, как к данным CallerID. Если вы не желаете поддерживать службу finger из соображений ограничения доступа к сведениям о пользователях, вам нецелесообразно использовать и протокол идентификации.

7. Благодарности

Благодарим Дэна Бернштейна (Dan Bernstein), который оживил интерес к данному протоколу и указал на досадные ошибки в RFC 931.

Литература

[1] St. Johns, M., "Authentication Server", RFC 931, TPSC, January 1985.

[2] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1340[1], USC/Information Sciences Institute, July 1992.

[1] Последняя версия этого документа содержится в RFC 1700, но в соответствии с RFC 3232 документ STD 2 утратил силу. Значения Assigned Numbers следует искать в базе данных, доступной на сайте www.iana.org/numbers.html. *Прим. перев.*

Адрес автора

Michael C. St. Johns

DARPA/CSTO

3701 N. Fairfax Dr

Arlington, VA 22203

Phone: (703) 696-2271

EMail: stjohns@DARPA.MIL

Перевод на русский язык

Николай Малых

nmalykh@gmail.com