Network Working Group
Request for Comments: 2866
Category: Informational
Obsoletes: 2139

C. Rigney
Livingston

June 2000

RADIUS - средства учета

RADIUS Accounting

Статус документа

Этот документ содержит информацию, адресованную сообществу Internet. В документе не содержится каких-либо стандартов Internet. Допускается распространение документа без каких-либо ограничений.

Авторские права

Аннотация

Этот документ описывает протокол обмена учетными сведениями (accounting) между серверами доступа NAS и серверами учета (Accounting Server).

Примечание для разработчиков

В этом документе описывается протокол RADIUS Accounting. Первые версии RADIUS Accounting использовали протокол UDP через порт 1646, что приводило к возникновению конфликтов со службами sa-msg-port. Официально для RADIUS Accounting выделен порт 1813.

Оглавление

1. Введение....1
1.1. Спецификация уровня требований....2
1.2. Терминология....2
2. Работа протокола....2
2.1. Proxy....2
3. Формат пакетов....3
4. Типы пакетов....4
4.1. Accounting-Request....4
4.2. Accounting-Response....4
5. Атрибуты....5
5.1. Acct-Status-Type....5
5.2. Acct-Delay-Time....6
5.3. Acct-Input-Octets....6
5.4. Acct-Output-Octets....6
5.5. Acct-Session-Id....7
5.6. Acct-Authentic....7
5.7. Acct-Session-Time....7
5.8. Acct-Input-Packets....7
5.9. Acct-Output-Packets....8
5.10. Acct-Terminate-Cause....8
5.11. Acct-Multi-Session-Id....9
5.12. Acct-Link-Count....9
5.13. Таблица атрибутов....9
6. Согласование с IANA....10
7. Вопросы безопасности....10
8. Журнал изменений....10
9. Литература....10
10. Подтверждение....10
11. Адрес председателя....11
12. Адрес автора....11
13. Полное заявление авторских прав....11

1. Введение

Управление распределенными последовательными каналами и модемными пулами для большого числа пользователей может потребовать значительных усилий администраторов сети. Поскольку модемные пулы по определению являются каналами во внешний мир, они требуют пристального внимания с точки зрения безопасности, идентификации пользователей и учета их работы. Наиболее эффективным решением такой задачи является создание единой “базы данных” о пользователях, которая содержит идентификационные сведения (имена и пароли), а также конфигурационные параметры, определяющий предоставляемый пользователю сервис (например, SLIP, PPP, telnet, rlogin).

В документе [2] описан протокол RADIUS[1], используемый для идентификации пользователей и проверки их полномочий. В данном документе описывается расширение протокола RADIUS, обеспечивающее доставку учетных сведений о работе пользователей от серверов доступа (NAS) к серверам учета RADIUS accounting.

Данный документ заменяет RFC 2139 [1]. Список отличий приведенной здесь спецификации от RFC 2139 дан в приложении “Журнал изменений".

Основные свойства RADIUS Accounting:

Архитектура “клиент-сервер”

Сервер доступа (NAS[2]) выступает в качестве клиента служб RADIUS accounting. Клиент отвечает за передачу учетных сведений серверам RADIUS accounting.

Серверы RADIUS accounting отвечают за прием учетных запросов и возврат клиенту информации, подтверждающей получение запроса.

Сервер RADIUS accounting может выступать в качестве клиента-посредника (proxy client) других серверов RADIUS accounting.

Безопасность

Аутентификация транзакций между клиентом и сервером RADIUS accounting осуществляется с использованием разделяемого ключа (shared secret), который никогда не передается через сеть.

Возможность расширения

Все протокольные транзакции представляются в форме триплетов “атрибут-размер-значение”[3]. Новые атрибуты могут добавляться без нарушения работы существующих реализаций протокола.

1.1. Спецификация уровня 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 RFC 2119 [3]. Значение этих слов не зависит от шрифтового выделения.

1.2. Терминология

Ниже приведены определения некоторых терминов, часто встречающихся в документе.

Service - сервис, служба, обслуживание

Сервер NAS обеспечивает сервис (например, PPP или Telnet) для подключающихся по коммутируемым линиям пользователей.

Session - сессия, сеанс

Каждый тип сервиса, обеспечиваемого NAS пользователям, предоставляется в форме сеанса, начало которого определяется моментом предоставления первой услуги, а завершение - моментом выполнения последней услуги. Пользователь может организовать множество параллельных (одновременных) сеансов, если NAS поддерживает такой режим. Для каждого из таких сеансов поддерживается отдельное значение Acct-Session-Id.

Silently discard - отбрасывание без уведомления

Отбрасывание пакетов без дальнейшей обработки. Реализациям протокола **следует** обеспечивать возможность ведения журнала ошибок, включающего содержимое отбрасываемых без уведомления пакетов. Также **следует** поддерживать статистику (счетчики) таких событий.

2. Работа протокола

Когда клиент настроен на использование RADIUS Accounting на начальном этапе предоставления услуг этот клиент будет генерировать пакет Accounting Start, описывающий тип предоставляемого пользователю сервиса, который передается серверу RADIUS Accounting, возвращающему подтверждение приема такого пакета. При завершении пользовательского сеанса клиент будет генерировать пакет Accounting Stop, описывающий тип предоставленного пользователю сервиса. Этот пакет может также включать статистические сведения о работе пользователя - продолжительность сеанса, число пакетов и байтов, принятых и переданных пользователем. Пакет передается серверу RADIUS Accounting, который будет возвращать подтверждение приема.

Пакет Accounting-Request (Start или Stop) передается серверу RADIUS через сеть. Клиенту рекомендуется повторять передачу пакета Accounting-Request до тех пор, пока от сервера не будет получено подтверждение приема. Если в течение заданного времени подтверждение не будет получено, передача пакета повторяется заданное число раз. Клиент может также переслать запрос дополнительным серверам в тех случаях, когда основной сервер не работает или недоступен. Обращаться к альтернативному серверу после заданного числа неудачных попыток связи с основным сервером или в режиме перебора по кругу. Алгоритмы повтора и выбора альтернативного сервера являются предметом исследования и не рассматриваются детально в данной спецификации.

Сервер RADIUS accounting **может** делать запросы к другим серверам для выполнения полученного от клиента запроса. В таких случаях сервер сам выступает в роли клиента.

Если сервер RADIUS не может записать пакет учета, **недопустимо** передавать клиенту подтверждение Accounting-Response.

2.1. Proxy

Информация о серверах-посредниках RADIUS приведена в спецификации [2]. Серверы-посредники RADIUS Accounting работают идентично RADIUS Proxy, как показано в приведенном ниже примере.

1. NAS передает пакеты Accounting-Request пересылающему серверу.

---

[1]Remote Authentication Dial In User Service.

[2]Network Access Server - сервер доступа в сеть.

[3] Attribute-Length-Value. В последнее время для таких триплетов чаще используют обозначение TLV (Type-Length-Value - тип-размер-значение). *Прим. перев.*

2. Пересылающий сервер протоколирует пакет Accounting-Request (если это нужно), добавляет атрибут Proxy-State (если нужно) после имеющихся в пакете атрибутов Proxy-State, обновляет атрибут Request Authenticator и пересылает запрос удаленному серверу.

3. Удаленный сервер протоколирует пакет Accounting-Request (если это нужно), копирует все атрибуты Proxy-State, не меняя их порядка в пакет отклика и передает отклик Accounting-Response серверу-посреднику.

4. Пересылающий сервер удаляет из пакета последний атрибут Proxy-State (если он был добавлен на этапе 2), обновляет значение атрибута Response Authenticator и передает пакет Accounting-Response серверу NAS.

Для сервера-посредника **недопустимо** изменение присутствующих в пакете атрибутов Proxy-State или Class.

Сервер-посредник может прозрачно пересылать пакеты, передавая повторные пакеты по мере их получения, или принять на себя ответственность за передачу повторных пакетов (это удобно в тех случаях, когда сетевое соединение между посредником и удаленным сервером по своим характеристикам существенно отличается от соединения между посредником и NAS).

Когда пересылающий сервер принимает на себя ответственность за передачу повторов, политика такой передачи должна обеспечивать устойчивость и масштабируемость.

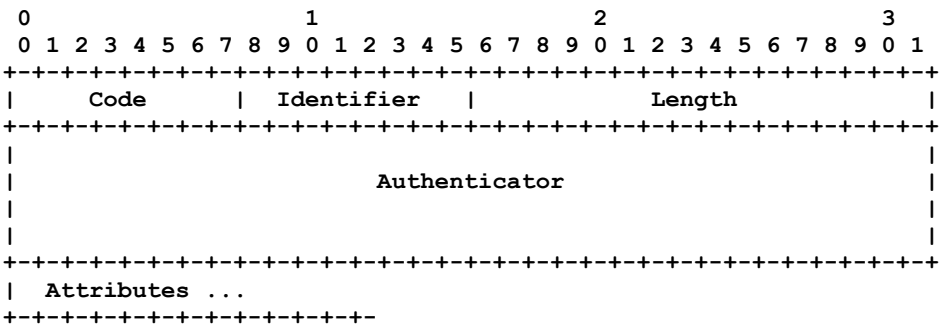
3. Формат пакетов

В поле данных пакетов UDP [4] инкапсулируется по одному пакету RADIUS Accounting и поле UDP Destination Port для протокола RADIUS должно содержать десятичное значение 1813.

При генерации откликов номера портов отправителя и получателя меняются местами.

В этом документе содержится спецификация протокола RADIUS. Ранние версии RADIUS Accounting использовали порт UDP 1646, что приводило к конфликтам со службами sa-msg-port. Официально выделенный для протокола RADIUS Accounting порт имеет номер 1813.

Ниже показан формат типового пакета RADIUS. Поля передаются слева направо и сверху вниз.



Code

Поле Code имеет размер 1 октет и содержит идентификатор типа пакета RADIUS. При получении пакета с некорректным значением поля Code такой пакет отбрасывается без уведомления.

Десятичные значения кодов для пакетов RADIUS Accounting показаны ниже.

4 Accounting-Request
5 Accounting-Response

Identifier

Поле Identifier размером 1 октет используется для сопоставления запросов с откликами. Сервер RADIUS может детектировать дубликаты запросов по совпадению IP-адреса отправителя, номеру порта отправителя и значению поля Identifier, если такие пакеты получены в течение короткого промежутка времени.

Length

Поле Length имеет размер 2 октета и показывает размер пакета с учетом полей Code, Identifier, Length, Authenticator и Attribute. Октеты за пределами указанного в поле размера значения **должны** трактоваться как заполнение и оставляться без внимания. Если размер пакета меньше значения поля Length, пакет **должен** отбрасываться без уведомления. Минимальный размер пакета составляет 20, а максимальный - 4095.

Authenticator

Поле Authenticator имеет размер 16 октетов. Старший октет поля передается первым. Значение поля применяется для аутентификации при обмене сообщениями между клиентом и сервером RADIUS accounting.

Request Authenticator

В пакетах Accounting-Request значение атрибута Authenticator, называемое Request Authenticator, представляет собой 16-октетное хэш-значение MD5 [5].

NAS и сервер RADIUS используют разделяемый ключ. Поле Request Authenticator в пакетах Accounting-Request содержит необратимое хэш-значение MD5, рассчитанное для потока октетов Code + Identifier + Length + 16 нулевых октетов + атрибуты запроса + разделяемый ключ (+ означает конкатенацию значений). 16-октетное хэш-значение MD5 помещается в поле Authenticator пакета Accounting-Request.

Отметим, что атрибут Request Authenticator в пакетах Accounting-Request вычисляется несколько иначе, нежели для атрибут Request Authenticator в пакетах RADIUS Access-Request, поскольку пакеты Accounting-Request не содержат атрибута User-Password.

Response Authenticator

Поле Authenticator в пакетах Accounting-Response называется Response Authenticator и содержит необратимое хэш-значение MD5, рассчитанное для потока октетов полей Code, Identifier, Length, значения Request Authenticator из пакета Accounting-Request, на который передается отклик, атрибутов отклика и разделяемого ключа. Полученное в результате 16-октетное хэш-значение MD5 помещается в поле Authenticator пакета Accounting-Response.

Attributes

Пакет может включать более одного экземпляра атрибутов некоторых типов. В таких случаях порядок атрибутов **следует** сохранять. Порядок разнотипных атрибутов значения не имеет.

4. Типы пакетов

Тип пакета RADIUS определяется значением поля Code в первом октете.

4.1. Accounting-Request

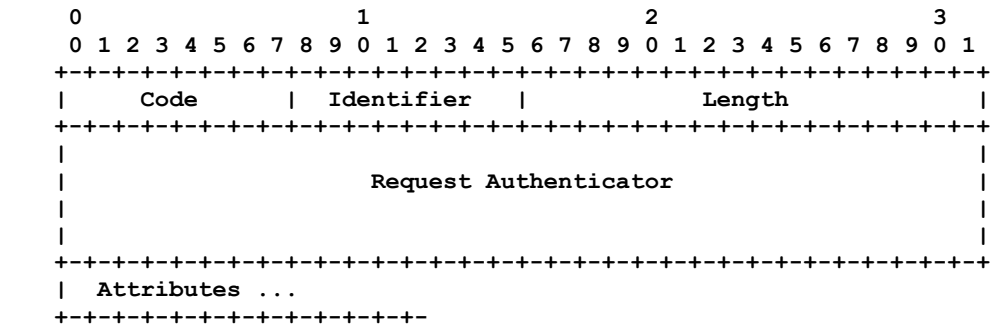
Пакеты Accounting-Request передаются от клиентов (обычно сервер доступа NAS или proxy) серверам RADIUS accounting и содержат информацию, используемую для учета предоставленных пользователю услуг. Клиент передает пакет RADIUS с Code = 4 (Accounting-Request).

При получении пакета Accounting-Request сервер **должен** передать отклик Accounting-Response, если учетный пакет был записан без ошибок. При возникновении той или иной ошибки передача отклика **недопустима**.

Атрибуты, допустимые для пакетов Access-Request и Access-Accept, могут использоваться в пакетах Accounting-Request. Однако в пакеты Accounting-Request **недопустимо** включение атрибутов User-Password, CHAP-Password, Reply-Message, State. В каждом пакете Accounting-Request **должен** присутствовать по крайней мере один из атрибутов NAS-IP-Address или NAS-Identifier. В пакеты также **следует** включать по крайней мере один из атрибутов NAS-Port или NAS-Port-Type, если сервер NAS способен различать свои порты.

Если пакет Accounting-Request включает атрибут Framed-IP-Address, последний **должен** содержать IP-адрес пользователя. Если в пакете Access-Accept используется специальное значение Framed-IP-Address, говорящее серверу NAS о выделении или согласовании IP-адреса для пользователя, атрибут Framed-IP-Address (если он есть) в пакете Accounting-Request **должен** содержать действительный адрес IP, выделенный или согласованный для пользователя.

Формат пакетов Accounting-Request показан ниже. Поля пакета передаются слева направо.



Code* = *4

Identifier

Значение поля Identifier **должно** меняться при всяком изменении содержимого поля Attributes и при получении корректного отклика на предыдущий запрос. При повторной передаче пакетов без их изменения значение поля Identifier **должно** сохраняться.

Отметим, что при включении атрибутов Acct-Delay-Time в пакет Accounting-Request значение Acct-Delay-Time будет обновляться при повторной передаче пакета, следовательно изменение содержимого поля Attributes требует заново вычислять значения полей Identifier и Request Authenticator.

Request Authenticator

Поле Request Authenticator в пакетах Accounting-Request содержит 16-октетное хэш-значение MD5, рассчитанное в соответствии с описанной выше процедурой (см. Request Authenticator).

Attributes

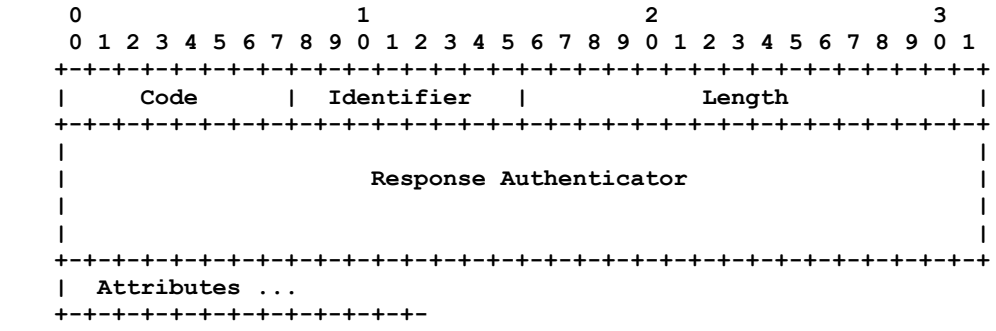
Поле Attributes имеет переменную длину и содержит список атрибутов.

4.2. Accounting-Response

Пакеты Accounting-Response передаются сервером RADIUS accounting клиенту в качестве подтверждения приема и успешной записи пакетов Accounting-Request. Если принятый пакет Accounting-Request был записан без ошибок, сервер RADIUS accounting должен передать пакет с Code = 5 (Accounting-Response). При получении пакета Accounting-Response клиент проверяет значение поля Identifier для определения соответствия отправленному запросу Accounting-Request. Поле Response Authenticator должно содержать корректный отклик для ожидающего пакета Accounting-Request. Некорректные пакеты отбрасываются без уведомления.

Пакеты Accounting-Response могут не содержать никаких атрибутов.

Формат пакетов Accounting-Response показан ниже. Поля пакета передаются слева направо.



Code = 5

Identifier

Поле Identifier содержит копию одноименного поля из пакета Accounting-Request, послужившего причиной передачи пакета Accounting-Response.

Response Authenticator

Поле Response Authenticator в пакетах Accounting-Response содержит 16-октетное значение MD5, рассчитанное в соответствии с описанной выше процедурой (см. Response Authenticator).

Attributes

Поле Attributes имеет переменную длину и содержит список атрибутов.

5. Атрибуты

Атрибуты RADIUS используются для передачи информации, связанной с аутентификацией и проверкой полномочий пользователей, а также учетом их работы.

Некоторые атрибуты **могут** присутствовать в пакете в нескольких экземплярах (это указывается ниже при описании атрибутов).

Завершение списка атрибутов определяется значением поля Length в пакетах RADIUS.

Формат атрибутов показан ниже. Поля атрибута передаются слева направо.

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |  Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

Однооктетное поле, определяющее тип атрибута. Актуальные значения поля типа для атрибутов RADIUS вы можете узнать из последнего варианта документа Assigned Numbers [6]. Значения 192-223 предназначены для экспериментальных целей, значения 224-240 зарезервированы для разработчиков (специфические для реализации типы), а значения 241-255 являются резервными и не должны использоваться. Рассматриваемые в данной спецификации значения приведены в таблице.

Значение	***Тип***	***Значение***	***Тип***
1-39	См. спецификацию RADIUS [2]	46	Acct-Session-Time
40	Acct-Status-Type	47	Acct-Input-Packets
41	Acct-Delay-Time	48	Acct-Output-Packets
42	Acct-Input-Octets	49	Acct-Terminate-Cause
43	Acct-Output-Octets	50	Acct-Multi-Session-Id
44	Acct-Session-Id	51	Acct-Link-Count
45	Acct-Authentic	60+	См. спецификацию RADIUS [2]

Length

Однооктетное поле Length указывает размер данного атрибута с учетом полей Type, Length и Value. При получении атрибута с некорректно указанным размером в пакетах Accounting-Request, такие пакеты **должны** отбрасываться без уведомления.

Value

Необязательное поле Value содержит значение атрибута. Формат и размер значения атрибута определяются значениями полей Type и Length.

Отметим, что ни один из типов RADIUS не использует в качестве завершения NUL-символ (hex 00). В частности, значения типа text и string в протоколе RADIUS не завершаются NUL-символом. Для каждого атрибута имеется поле размера, поэтому символы завершения не требуются. Значения типа text представляет собой последовательность символов в кодировке UTF-8 10646 [7], а значения типа string содержат 8-битовые бинарные данные. Серверы и клиенты RADIUS **должны** быть способны работать со строками, содержащими NUL-символы. При реализации RADIUS на основе языка C не следует использовать для обработки строк функцию strcpy().

Значение атрибута может относиться к одному из пяти поддерживаемых типов данных. Отметим, что тип text является частным случаем (подмножеством) типа string.

text от 1 до 253 октетов, содержащих символы в кодировке UTF-8 10646 [7]. **Недопустима** передача текстовых атрибутов нулевой длины. В таких случаях следует просто исключить атрибут.

string от 1 до 253 октетов, содержащих бинарные данные (значения от 0 до 255, включительно). **Недопустима** передача string-атрибутов нулевой длины. В таких случаях следует просто исключить атрибут.

address 32-битовое значение, первый октет является старшим.

integer 32-битовое беззнаковое целое, первый октет является старшим.

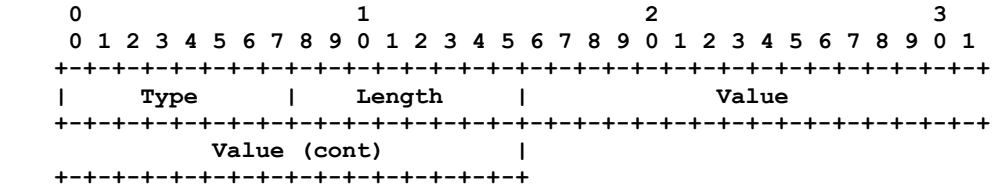
time 32-битовое беззнаковое целое (первый октет является старшим), показывающее число секунд, прошедших с 1 января 1970 г. (00:00:00 по Гринвичу - UTC). Стандартные атрибуты RADIUS не используют этот тип, но он добавлен для будущих расширений.

5.1. Acct-Status-Type

Этот атрибут определяет на что указывает данный пакет Accounting-Request - начало (Start) или завершение (Stop) обслуживания пользователя.

Атрибут **может** использоваться клиентом для маркировки начала учета (например, при загрузке) путем указания Accounting-On или для маркировки завершения учета (например, перед перезагрузкой) с помощью Accounting-Off.

Формат атрибута Acct-Status-Type показан ниже. Поля передаются слева направо.



Type = 40
Length = 6
Value

Четырехоктетное поле.

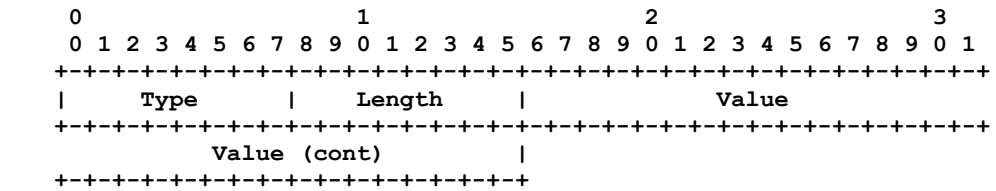
1 Start
2 Stop
3 Interim-Update
7 Accounting-On
8 Accounting-Off
9-14 Зарезервированы для Tunnel Accounting
15 Зарезервировано для отказов (Failed)

5.2. Acct-Delay-Time

Этот атрибут показывает число секунд, в течение которых клиент пытается передать данную запись, и значение атрибута может вычитаться из времени доставки пакета на сервер для приблизительного определения момента генерации пакета Accounting-Request (время передачи через сеть не принимается во внимание).

Отметим, что изменение Acct-Delay-Time требует менять значение поля Identifier (см. выше).

Формат атрибута Acct-Delay-Time показан ниже. Поля передаются слева направо.



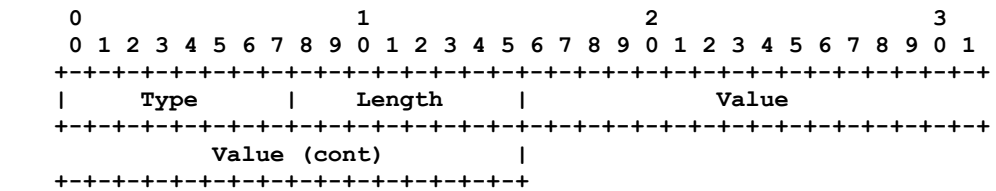
Type = 41
Length = 6
Value

Четырехоктетное поле.

5.3. Acct-Input-Octets

Этот атрибут показывает количество октетов, полученных из порта за время, в течение которого предоставляется данный сервис. Атрибут может включаться только в пакеты Accounting-Request, где Acct-Status-Type = Stop.

Формат атрибута Acct-Input-Octets показан ниже. Поля передаются слева направо.



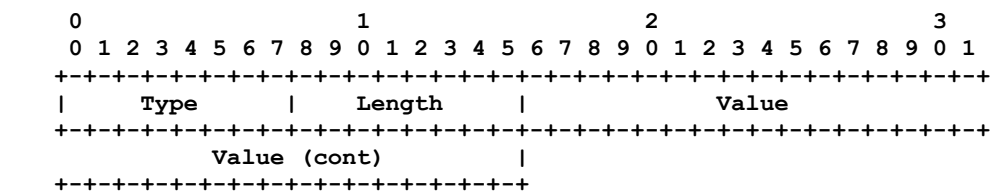
Type = 42
Length = 6
Value

Четырехоктетное поле.

5.4. Acct-Output-Octets

Этот атрибут показывает количество октетов, переданных в порт в течение всего срока предоставления данного сервиса. Атрибут может использоваться только в пакетах Accounting-Request с Acct-Status-Type = Stop.

Формат атрибута Acct-Output-Octets показан ниже. Поля передаются слева направо.



Type = 43
Length = 6
Value

Четырехоктетное поле.

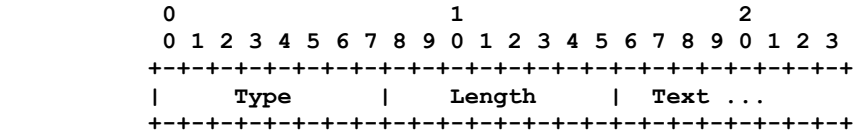
5.5. Acct-Session-Id

Этот атрибут содержит уникальное значение Accounting ID, упрощающее поиск соответствия между стартовыми и конечными записями в журнальном файле. Стартовая и конечная запись для данной сессии **должны** иметь одинаковые значения Acct-Session-Id. Пакеты Accounting-Request **должны** включать атрибут Acct-Session-Id. **Возможно** включение атрибута Acct-Session-Id в пакеты Access-Request; в таких случаях сервер NAS **должен** использовать такое же значение Acct-Session-Id в пакетах Accounting- Request для данной сессии.

Значение атрибута Acct-Session-Id **следует** задавать в кодировке UTF-8 10646 [7].

Например, можно использовать 8-значные шестнадцатеричные идентификаторы в буквами верхнего регистра и увеличивать значение двух старших цифр при каждой перезагрузке (полное использование всех значений после 256 перезагрузок). Остальные 6 цифр позволяют задать значения от 0 (для первого пользователя после перезагрузки) до 2^{24}-1 (около 16 миллионов), что позволяет организовать соответствующее число сеансов за время между перезагрузками.. Возможны и другие схемы построения уникальных значений атрибута

Формат атрибута Acct-Session-Id показан ниже. Поля передаются слева направо.



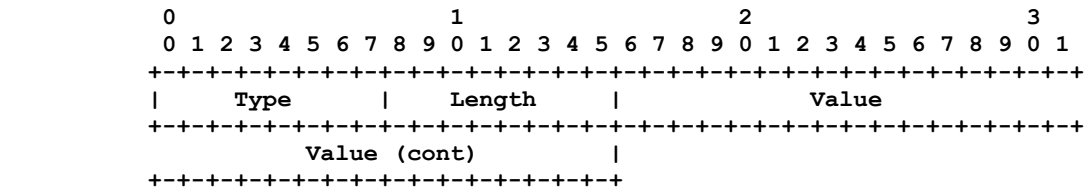
Type = 44
Length ≥ ***3***
String

Значение поля String **следует** задавать в кодировке UTF-8 10646 [7].

5.6. Acct-Authentic

Этот атрибут **может** включаться в пакеты Accounting-Request для индикации того, что пользователь уже прошел аутентификацию с помощью протокола RADIUS, собственно NAS или иным способом. Если предоставление сервиса пользователям обеспечивается без аутентификации, учетные записи генерировать **не следует**.

Формат атрибута Acct-Authentic показан ниже. Поля передаются слева направо.



Type = 45
Length = 6
Value

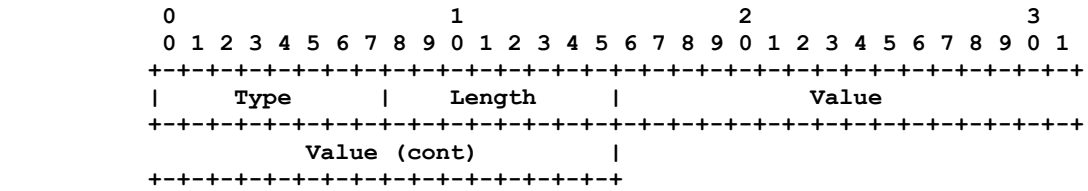
Четырехоктетное поле.

1 RADIUS
2 Local (локальная аутентификация)
3 Remote (удаленная аутентификация)

5.7. Acct-Session-Time

Этот атрибут показывает время обслуживания пользователя (в секундах). Атрибут может присутствовать только в пакетах Accounting-Request, где Acct-Status-Type = Stop.

Формат атрибута Acct-Session-Time показан ниже. Поля передаются слева направо.



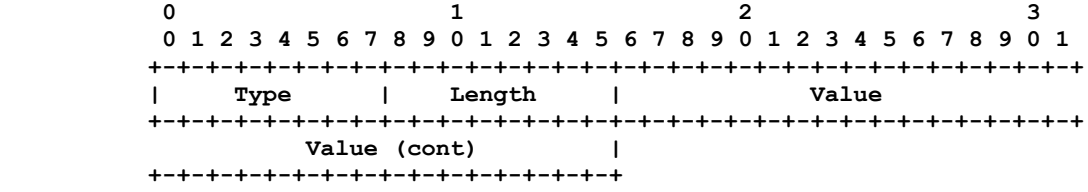
Type = 46
Length = 6
Value

Четырехоктетное поле.

5.8. Acct-Input-Packets

Этот атрибут показывает общее число пакетов, полученных из порта за все время обслуживания пользователя Framed User, и может включаться только в пакеты Accounting-Request с Acct-Status-Type = Stop.

Формат атрибута Acct-Input-packets показан ниже. Поля передаются слева направо.



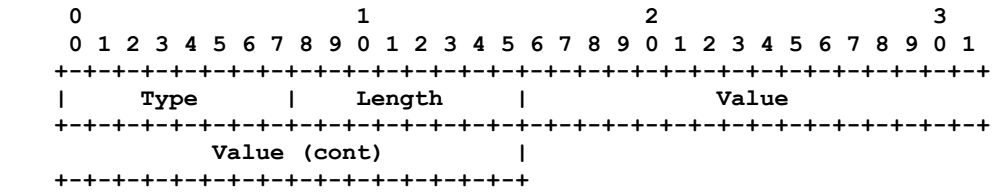
Type = 47
Length = 6
Value

Четырехоктетное поле.

5.9. Acct-Output-Packets

Этот атрибут показывает общее число пакетов, переданных в порт за все время обслуживания пользователя Framed User, и может включаться только в пакеты Accounting-Request с Acct-Status-Type = Stop.

Формат атрибута Acct-Output-Packets показан ниже. Поля передаются слева направо.



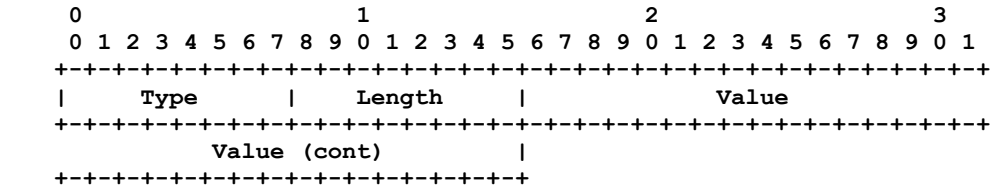
Type = 48
Length = 6
Value

Четырехоктетное поле.

5.10. Acct-Terminate-Cause

Этот атрибут показывает причину завершения сеанса и может включаться только в пакеты Accounting-Request, где Acct-Status-Type = Stop.

Формат атрибута Acct-Terminate-Cause показан ниже. Поля передаются слева направо.



Type = 49
Length = 6
Value

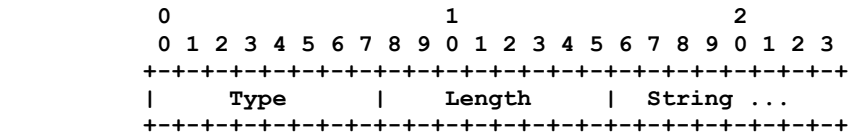
Четырехоктетное поле Value содержит код причины завершения сеанса:

Значение	***Тип***	***Описание***
1	User Request	Прекращение сеанса по инициативе пользователя (например с помощью LCP Terminate или выхода из сети - log out).
2	Lost Carrier	На порту был сброшен сигнал DCD (детектирование несущей).
3	Lost Service	Сервис больше не предоставляется (например, разорвано соединение пользователя с хостом).
4	Idle Timeout	Истекло время допустимого бездействия (Idle timer).
5	Session Timeout	Достигнута максимальная продолжительность сеанса.
6	Admin Reset	Сессия или порт сброшены администратором.
7	Admin Reboot	Администратор прекратил обслуживание пользователей NAS (например, для перезагрузки NAS).
8	Port Error	Сервер NAS обнаружил для порта ошибку, потребовавшую разрыва сессии.
9	NAS Error	Сервер NAS обнаружил (не связанную с портом), потребовавшую разрыва сессии.
10	NAS Request	Сервер NAS завершил сессию по неизвестной причине.
11	NAS Reboot	Сервер NAS завершил сессию для аварийной перезагрузки.
12	Port Unneeded	Сервер NAS завершил сессию потому, что уровень использования ресурсов слишком мал (например, в случаях выделения полосы по запросу реально достижимая скорость позволяет отключить один из портов).
13	Port Preempted	Сервер NAS завершил сеанс для предоставления порта пользователю с более высоким приоритетом.
14	Port Suspended	Сервер NAS завершил сеанс для прерывания виртуальной сессии.
15	Service Unavailable	Сервер NAS не может предоставить запрошенный сервис.
16	Callback	Сервер NAS прерывает текущую сессию для организации обратного соединения (callback).
17	User Error	Ошибка в полученных от пользователя данных, вызвавшая прекращение сеанса.
18	Host Request	Нормальное завершение сеанса хостом.

5.11. Acct-Multi-Session-Id

Этот атрибут содержит уникальный идентификатор Accounting ID, позволяющий связать воедино множество сеансовых записей в журнальном файле. Каждая сессия имеет свое значение Acct-Session-Id, а значения идентификатора “мультисессии” Acct-Multi-Session-Id будут совпадать для связанных сессий. Настоятельно рекомендуется указывать значения атрибутов Acct-Multi-Session-Id в кодировке UTF-8 10646 [7].

Формат атрибута Acct-Session-Id показан ниже. Поля передаются слева направо.



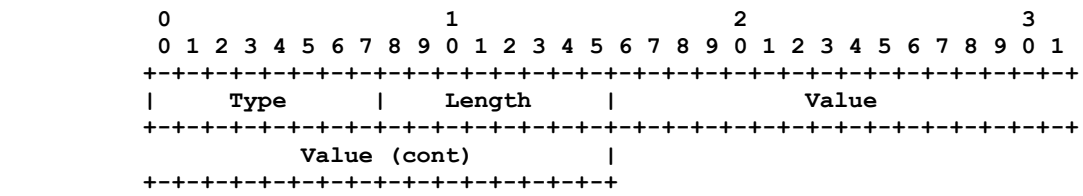
Type = 50
Length ≥ 3
String

Значение поля String **следует** задавать в кодировке UTF-8 10646 [7].

5.12. Acct-Link-Count

Этот атрибут указывает число соединений, относящихся к данной “мультисессии”, на момент генерации записи. Сервер NAS **может** включать атрибут Acct-Link-Count в любые пакеты Accounting-Request, которые могут быть связаны с многоканальными соединениями.

Формат атрибута Acct-Link-Count показан ниже. Поля передаются слева направо.



Type = 51
Length = 6
Value

Четырехоктетное поле Value содержит число соединений для данной “мультисессии” (Multilink Session). Этот атрибут упрощает серверу учета связывание воедино информации для множества сессий одной “мультисессии”. Когда число пакетов Accounting-Request, полученных с Acct-Status-Type = Stop, одинаковыми значениями Acct-Multi-Session-Id и уникальными значениями Acct-Session-Id равно наибольшему значению Acct-Link-Count, появляющемуся в таких пакетах Accounting-Requests, это говорит о получении всех финишных (Stop) запросов Accounting-Requests для данной многоканальной сессии.

В таблице показан пример 8 пакетов Accounting-Requests. Для простоты не имеющие к делу отношения атрибуты опущены.

Multi-Session-Id	*Session-Id*	*Status-Type*	*Link-Count*
"10"	"10"	Start	1
"10"	"11"	Start	2
"10"	"11"	Stop	2
"10"	"12"	Start	3
"10"	"13"	Start	4
"10"	"12"	Stop	4
"10"	"13"	Stop	4
"10"	"10"	Stop	4

5.13. Таблица атрибутов

В таблице приведен список всех атрибутов, которые могут встречаться в пакетах Accounting-Request. В пакеты Accounting-Response следует включать лишь атрибуты Proxy-State и Vendor-Specific.

Число	*Атрибут*	*Число*	*Атрибут*	*Число*	*Атрибут*
0-1	User-Name	0-1	Callback-Id	0-1	Framed-AppleTalk-Zone
0	User-Password	0+	Framed-Route	1	Acct-Status-Type
0	CHAP-Password	0-1	Framed-IPX-Network	0-1	Acct-Delay-Time
0-1	NAS-IP-Address[1]	0	State	0-1	Acct-Input-Octets
0-1	NAS-Port	0+	Class	0-1	Acct-Output-Octets
0-1	Service-Type	0+	Vendor-Specific	1	Acct-Session-Id
0-1	Framed-Protocol	0-1	Session-Timeout	0-1	Acct-Authentic
0-1	Framed-IP-Address	0-1	Idle-Timeout	0-1	Acct-Session-Time

[1] Пакеты Access-Request должны включать по крайней мере один из атрибутов NAS-IP-Address и NAS-Identifier.

Число	Атрибут	Число	Атрибут	Число	Атрибут
0-1	Framed-IP-Netmask	0-1	Termination-Action	0-1	Acct-Input-Packets
0-1	Framed-Routing	0-1	Called-Station-Id	0-1	Acct-Output-Packets
0+	Filter-Id	0-1	Calling-Station-Id	0-1	Acct-Terminate-Cause
0-1	Framed-MTU	0-1	NAS-Identifier[1]	0+	Acct-Multi-Session-Id
0+	Framed-Compression	0+	Proxy-State	0+	Acct-Link-Count
0+	Login-IP-Host	0-1	Login-LAT-Service	0	CHAP-Challenge
0-1	Login-Service	0-1	Login-LAT-Node	0-1	NAS-Port-Type
0-1	Login-TCP-Port	0-1	Login-LAT-Group	0-1	Port-Limit
0	Reply-Message	0-1	Framed-AppleTalk-Link	0-1	Login-LAT-Port
0-1	Callback-Number	0-1	Framed-AppleTalk-Network		

Ниже разъяснены использованные в таблице обозначения.

0 **недопустимо** включение данного атрибута в пакеты этого типа;

0+ атрибут является необязательным и **может** присутствовать в нескольких экземплярах;

0-1 необязательный атрибут, который **может** присутствовать в единственном экземпляре;

1 обязательный атрибут, который **должен** присутствовать в единственном экземпляре.

6. Согласование с IANA

Коды типа пакетов (Packet Type Code), типы атрибутов (Attribute Type) и их значения (Attribute Value), определенные в данной спецификации, зарегистрированы в IANA (Internet Assigned Numbers Authority) и относятся к пространству имен RADIUS как описано в разделе "Согласование с IANA" документа RFC 2865 [2] в соответствии с требованиями BCP 26 [8].

7. Вопросы безопасности

Вопросы безопасности обсуждаются в параграфах, относящихся к значениям Authenticator, которые передаются в запросах и откликах и при создании которых применяются разделяемые ключи (эти ключи никогда не передаются через сеть).

8. Журнал изменений

- Кодировка US-ASCII заменена UTF-8.
- Добавлены замечания по Proxy-серверам.
- Атрибут Framed-IP-Address должен содержать реальный IP-адрес пользователя.
- При передаче атрибута Acct-Session-ID в пакете Access-Request это же значение должно использоваться в пакетах Accounting-Request для данной сессии.
- Добавлены новые значения атрибута Acct-Status-Type.
- Добавлен параграф “Согласование с IANA”.
- Обновлены ссылки.
- Текстовые строки являются подмножеством типа string.

9. Литература

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

[2] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

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

[4] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[5] Rivest, R. and S. Dusse, "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[6] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994.

[7] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

[8] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

10. Подтверждение

Исходный вариант протокола RADIUS был разработан Стивом Вилленсом (Steve Willens) из Livingston Enterprises для линейки серверов доступа PortMaster.

11. Адрес председателя

Взаимодействием участников рабочей группы руководил:

Carl Rigney

Livingston Enterprises

4464 Willow Road

Pleasanton, California 94588

Phone: +1 925 737 2100

EMail: cdr@telemancy.com

12. Адрес автора

Связанные с этим документом вопросы можно адресовать автору:

Carl Rigney

Livingston Enterprises

4464 Willow Road

Pleasanton, California 94588

EMail: cdr@telemancy.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

13. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечивалось Internet Society.