Network Working Group
Request for Comments: 3575
Updates: 2865
Category: Standard Track

B. Aboba
Microsoft

July 2003

Взаимодействие с IANA для протокола RADIUS

IANA Considerations for RADIUS

(Remote Authentication Dial In User Service)

Статус документа

Этот документ содержит спецификацию проекта стандартного протокола Internet и служит приглашением к дискуссии в целях развития протокола. Текущее состояние стандартизации и статус протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться свободно.

Авторские права

Аннотация

Этот документ описывает вопросы, требующие согласования с агентством IANA[1], в части протокола RADIUS[2].

Документ служит обновлением RFC 2865.

1. Введение

В этом документе приведены рекомендации для агентства IANA, относящиеся к регистрации значений, связанных с протоколом RADIUS, который определен в [RFC2865], в соответствии с документом BCP 26, [RFC2434]. Документ также резервирует коды типа пакетов, которые используются или будут использоваться в Internet.

1.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с [RFC2119].

1.2. Терминология

Термины «пространство имен» (name space), «выделенное значение» (assigned value), «регистрация» (registration) трактуются в соответствии с определениями BCP 26.

Процедуры распределения «для приватного использования» (Private Use), «в порядке очередности» (First Come First Served), «экспертная оценка» (Expert Review), «требуется спецификация» (Specification Required), «одобрение IESG» (IESG Approval), «согласие IETF» (IETF Consensus), «стандартизация» (Standards Action) трактуются здесь в соответствии с определениями BCP 26.

2. Взаимодействие с IANA

В протоколе RADIUS имеется три пространства имен, требующих регистрации: коды типа пакетов (Packet Type Code), типы атрибутов (Attribute Type) и значения атрибутов (Attribute Value) (для некоторых атрибутов). Этот документ не создает новых реестров IANA, поскольку реестры для протокола RADIUS были созданы в [RFC2865].

RADIUS не относится к протоколам общего назначения и выделение значений **не следует** выполнять с целями, отличными от AAA[3].

2.1. Рекомендуемые правила регистрации

Для регистрационных запросов, где следует консультироваться с назначенным экспертом (Designated Expert), такого эксперта следует назначать ответственному директору направления IESG. Это сделано для того, чтобы любая регистрация сопровождалась публикацией RFC. Тем не менее, эксперт может одобрить регистрацию до публикации документа в том случае, когда он понимает, что RFC будет опубликован. Эксперт будет направлять запрос в список рассылки AAA WG (или другой список, указанный руководителем направления) для получения комментариев и рецензирования, включая документ Internet-Draft. Не позже 30 после этого эксперт должен будет принять или отвергнуть запрос на регистрацию, опубликовав свое решение в списке рассылок AAA WG (или заменяющей его конференции), а также сообщить свое решение агентству IANA. Отказ должен сопровождаться разъяснением причин и, по возможности, рекомендациями по корректировке запроса для возможности его удовлетворения.

---

[1] Internet Assigned Numbers Authority.
[2] Remote Authentication Dial In User Service - аутентификация удаленных пользователей при доступе по коммутируемым телефонным линиям.
[3] Authentication, Authorization or Accounting - аутентификация, проверка полномочий или учет.

Значения Packet Type Code занимают диапазон от 1 до 253. Коды RADIUS Type в диапазонах 1-5 и 11-13 были выделены в [RFC2865], а коды 40-45 и 250-253 — в настоящем документе. Коды 250-253 предназначены для экспериментов (Experimental Uses), а коды 254-255 зарезервированы. Значения Packet Type Code 6-10, 12-13, 21-34 и 50-51 не выделены в каких-либо документах IETF RFC и остаются резервными до появления соответствующих спецификаций. Это позволит избежать проблем при взаимодействии с нестандартными расширениями RADIUS, которые используются или будут использоваться в сети Internet. Поскольку новые значения кодов Packet Type будут оказывать существенное влияние на интероперабельность, для выделения новых значений Packet Type Code требуется одобрение IESG (IESG Approval). Это сделано для того, чтобы выделение значений сопровождалось публикацией RFC. В первую очередь следует распределять коды 52-249, а затем 14-20, 35-39 и 46-49. Список кодов типа приведен в Приложении A.

Типы атрибутов имеют значения в диапазоне от 1 до 255 и относятся к числу дефицитных ресурсов RADIUS, поэтому распределять значения нужно с осторожностью. Атрибуты типов 1-53, 55, 60-88, 90-91, 94-100 уже выделены, при этом значения 17 и 21 могут быть выделены для нового применения. Атрибуты типов 17, 21, 54, 56-59, 89, 101-191 могут выделяться с согласия IETF (IETF Consensus). Выделять значения типов 17 и 21 рекомендуется только по исчерпании других значений.

Отметим, что в протоколе RADIUS определен механизм фирменных (Vendor-Specific) расширений (Attribute 26) для функций, применяемых только в реализациях RADIUS одного производителя, когда не возникает требований по совместимости. Для функций, присущих только реализациям одного производителя, рекомендуется использовать этот тип вместо выделения глобального типа атрибута.

В [RFC2865] сказано:

> 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.

Следовательно, значения Attribute Type из диапазона 192-240 рассматриваются в качестве предназначенных для приватных систем (Private Use), а для значений 241-255 требуется стандартизация (Standards Action).

Некоторые атрибуты (например, NAS-Port-Type) протокола RADIUS определяют набор значений в соответствии с разными смыслами. Для каждого атрибута может существовать до 2^{32} значений. Дополнительные значения могут быть выделены в соответствии с процедурой Designated Expert. Исключением из этого правила является атрибут Service-Type (6), значения которого определяют новые режимы работы RADIUS. Значения 1-16 для этого атрибута уже выделены. Для выделения новых значений Service-Type используется согласование с IETF (IETF Consensus). Это сделано для того, чтобы выделение каждого значения сопровождалось публикацией RFC.

3. Литература

3.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC2865] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

3.2. Дополнительная литература

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC2867] Zorn, G., Aboba, B. and D. Mitton, "RADIUS Accounting Modifications for Tunnel Protocol Support", RFC 2867, June 2000.

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[RFC2869] Rigney, C., Willats, W. and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[RFC2869bis] Aboba, B. and P. Calhoun, "RADIUS Support for Extensible Authentication Protocol (EAP)", Work in Progress[1].

[RFC2882] Mitton, D., "Network Access Servers Requirements: Extended RADIUS Practices", RFC 2882, July 2000.

[RFC3162] Aboba, B., Zorn, G. and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[DynAuth] Chiba, M., Dommety, G., Eklund, M., Mitton, D. and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

4. Вопросы безопасности

Вопросы безопасности, рассмотренные в [RFC2434], в общем случае применимы и к настоящему документу. Вопросы безопасности, связанные с протоколом RADIUS, рассмотрены в документах [RFC2607], [RFC2865], [RFC3162], [DynAuth] и [RFC2869bis].

Приложение A - Типы пакетов RADIUS

Ниже приведен список кодов RADIUS Packet Type. Этот список является инструкцией агентству IANA по публикации значений в реестре Packet Type Codes. Отметим, что коды 40-45, определенные в [DynAuth], формально выделены

[1] Работа завершена и опубликована в RFC 3579. *Прим. перев.*

настоящим документом. Коды 40-45 были указаны в [RFC2882] и применяются в реализациях. С учетом широкого распространения этих кодов их следует считать практически не возвратными.

Номер	*Имя сообщения*	*Документ*
1	Access-Request	[RFC2865]
2	Access-Accept	[RFC2865]
3	Access-Reject	[RFC2865]
4	Accounting-Request	[RFC2865]
5	Accounting-Response	[RFC2865]
6	Accounting-Status[1]	[RFC2882]
7	Password-Request	[RFC2882]
8	Password-Ack	[RFC2882]
9	Password-Reject	[RFC2882]
10	Accounting-Message	[RFC2882]
11	Access-Challenge	[RFC2865]
12	Status-Server[2]	[RFC2865]
13	Status-Client[2]	[RFC2865]
21	Resource-Free-Request	[RFC2882]
22	Resource-Free-Response	[RFC2882]
23	Resource-Query-Request	[RFC2882]
24	Resource-Query-Response	[RFC2882]
25	Alternate-Resource-Reclaim-Request	[RFC2882]
26	NAS-Reboot-Request	[RFC2882]
27	NAS-Reboot-Response	[RFC2882]
28	Reserved	
29	Next-Passcode	[RFC2882]
30	New-Pin	[RFC2882]
31	Terminate-Session	[RFC2882]
32	Password-Expired	[RFC2882]
33	Event-Request	[RFC2882]
34	Event-Response	[RFC2882]
40	Disconnect-Request	[DynAuth]
41	Disconnect-ACK	[DynAuth]
42	Disconnect-NAK	[DynAuth]
43	CoA-Request	[DynAuth]
44	CoA-ACK	[DynAuth]
45	CoA-NAK	[DynAuth]
50	IP-Address-Allocate	[RFC2882]
51	IP-Address-Release	[RFC2882]
250-253	Experimental Use	
254	Reserved	
255	Reserved	[RFC2865]

Заявление об интеллектуальной собственности

IETF не занимает какой-либо позиции в отношении действительности или объёма каких-либо прав интеллектуальной собственности или иных прав, которые могут быть заявлены как относящиеся к реализации или применению технологии, описанной в этом документе, или степени, в которой любая лицензия, по которой права могут или не могут быть доступны, не заявляется также применение каких-либо усилий для определения таких прав. Сведения о процедурах IETF в отношении прав в документах, связанных со стандартами, можно найти в BCP-11. Копии раскрытия IPR, предоставленные секретариату IETF, и любые гарантии доступности лицензий, а также результаты попыток получить общую лицензию или право на использование таких прав собственности разработчиками или пользователями этой спецификации, можно получить в IETF Secretariat.

[1] В настоящее время Interim Accounting.
[2] Экспериментальный.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Эту информацию следует направлять исполнительному директоу IETF (Executive Director).

Благодарности

Спасибо Ignacio Goyret из Lucent, Allison Mankin из Lucent Bell Labs, Thomas Narten из IBM, Glen Zorn и Harald Alvestrand из Cisco за дискусии, относящиеся к этому документу.

Адреса авторов

Bernard Aboba

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052

EMail: bernarda@microsoft.com

Phone: +1 425 706 6605

Fax: +1 425 936 7329

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено IETF IASA[1].

[1]Administrative Support Activity.