Network Working Group
Request for Comments: 4675
Category: Standards Track

P. Congdon
M. Sanchez
Hewlett-Packard Company
B. Aboba
Microsoft Corporation

September 2006

Атрибуты RADIUS для поддержки VLAN и приоритета

RADIUS Attributes for Virtual LAN and Priority Support

Статус документа

В этом документе описан проект стандарта протокола для сообщества Internet; документ служит приглашением к дискуссии в целях развития протокола. Информацию о текущем состоянии стандартизации протокола можно найти в документе Internet Official Protocol Standards (STD 1). Данный документ может распространяться свободно.

Авторские права

Copyright (C) The Internet Society (2005).

Аннотация

В этом документе предложены дополнительные атрибуты RADIUS[1] для выделения VLAN[2] и приоритизации, используемые в целях контроля доступа к локальным сетям IEEE 802. Эти атрибуты могут использоваться с протоколами RADIUS и Diameter.

Оглавление

1. Введение

Этот документ описывает атрибуты VLAN и изменения приоритизации, которые могут быть полезны для управления доступом в локальные сети IEEE 802 [IEEE-802] с использованием протокола RADIUS или Diameter.

Хотя [RFC3580] разрешает присваивание VLAN на основе атрибутов туннеля, определённых в [RFC2868], в этом случае не обеспечивается поддержка более полного набора функций VLAN, определённого в стандарте [IEEE-802.1Q]. Атрибуты, определённые в данном документе, обеспечивают для протоколов RADIUS и Diameter аналоги переменных управления, поддерживаемых в [IEEE-802.1Q] и объектах MIB, которые определены в [RFC4363]. Кроме того, этот документ разрешает поддержку более широкого диапазона конфигураций [IEEE-802.1X].

1.1. Терминология

В этом документе используются следующие термины:

Network Access Server (NAS) - сервер доступа в сеть
Устройство, которое обеспечивает для пользователей услуги по предоставлению доступа в сеть. Для таких устройств также используется обозначение RADIUS client.

RADIUS server - сервер RADIUS
Сервер аутентификации RADIUS представляет собой объект, обеспечивающий сервис аутентификации для NAS.

RADIUS proxy
RADIUS-прокси действует как сервер аутентификации для NAS и клиент RADIUS для RADIUS-сервера.

[1]Remote Authentication Dial-In User Service - служба аутентификации удалённых пользователей при коммутируемом доступе.
[2]Virtual LAN - виртуальная ЛВС

1.2. 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].

1.3. Интерпретация атрибутов

Описанные в этом документе атрибуты применяются к одному экземпляру порта NAS (точнее говоря, к одному порту моста IEEE 802.1Q). Стандарты [IEEE-802.1Q], [IEEE-802.1D] и [IEEE-802.1X] не распознают более тонкое разделение, нежели уровень порта. В некоторых случаях (например, в беспроводных ЛВС IEEE 802.11) вместо физических портов используется понятие виртуального порта. Такие виртуальные порты обычно связаны с защищёнными соединениями[1] и представляются как станция или MAC[2]-адрес.

Атрибуты, определённые в этом документе, применяются на уровне отдельного пользователя и предполагается, что на каждый порт приходится один пользователь; однако в некоторых случаях порт может быть виртуальным. Если реализация NAS, соответствующая этому документу, поддерживает виртуальные порты, может оказаться возможным предоставление таким портам уникальных значений описанных здесь атрибутов. Такой подход позволяет множеству пользователей на одном физическом порту использовать уникальные для каждого пользователя наборы параметров аутентификации.

Если соответствующий данной спецификации сервер NAS получает пакет Access-Accept, содержащий определённый в этом документе атрибут, который сервер не может применить, сервер **должен** действовать как при получении пакета Access-Reject. [RFC3576] требует, чтобы сервер NAS, получивший запрос CoA-Request[3], отвечал на него пакетом CoA-NAK, если запрос включает неподдерживаемый атрибут. Рекомендуется включать в такой пакет CoA-NAK атрибут Error-Cause со значением Unsupported Attribute (401). Как указано в [RFC3576], смена авторизации является атомарной операцией, поэтому в такой ситуации не происходит разрыва сеанса и существующая конфигурация остаётся неизменной. В результате генерировать пакет учёта (accounting) не следует.

2. Атрибуты

2.1. Egress-VLANID

Атрибут Egress-VLANID представляет разрешённое значение IEEE 802 Egress VLANID для этого порта, показывающее какие значения VLANID разрешены для кадров с тегами и без тегов.

Как определено в [RFC3580], VLAN, выделенные с помощью туннельных атрибутов, применимы как к входящим VLANID для пакетов без тегов (PVID), так и к исходящим VLANID для пакетов без тегов. В противоположность этому атрибут Egress-VLANID задаёт лишь значение исходящего идентификатора VLANID для пакетов с тегами и без тегов. Атрибут Egress-VLANID **можно** включать в пакет RADIUS с туннельными атрибутами [RFC3580]; однако атрибут Egress-VLANID не является обязательным, если он используется для пакетов без тегов с тем же значением VLANID, которое включено в атрибуты туннеля. Для настройки VLAN без тегов в обоих направлениях **должны** использоваться атрибуты [RFC3580].

В пакеты Access-Request, Access-Accept, CoA-Request или Accounting-Request **можно** включать множество атрибутов Egress-VLANID; этот атрибут **недопустимо** передавать в пакетах Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK и CoA-NAK. Каждый атрибут добавляет указанную сеть VLAN к списку виртуальных ЛВС, разрешённых на выходе из данного порта.

Формат атрибута Egress-VLANID показан на рисунке. Поля передаются в порядке слева направо.

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

Type 56

Length 6

Value

Поле Value состоит из 4 октетов. Формат поля показан на рисунке.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Tag Indic.   |        Pad            |       VLANID          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

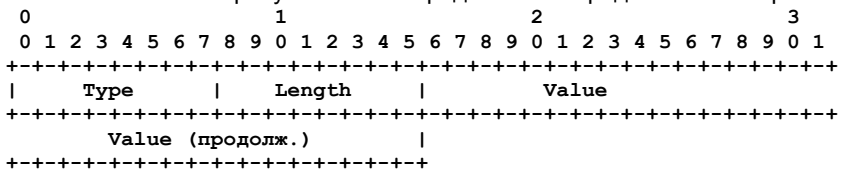
Поле Tag Indication имеет размер 1 октет и показывает, содержат (0x31) или не содержат (0x32) теги кадры VLAN. Поле заполнения (Pad) имеет размер 12 битов и **должно** иметь значение 0. 12-битовое поле VLANID содержит идентификатор VLAN VID [IEEE-802.1Q].

2.2. Ingress-Filters

Атрибут Ingress-Filters соответствует переменной Ingress Filter определённой для порта в стандарте [IEEE-802.1Q] (п. 8.4.5). Когда этот атрибут имеет значение Enabled, набор VLAN, разрешённых на входе в порт, должен соответствовать набору VLAN, разрешённых на выходе из порта. **Можно** включать лишь один атрибут Ingress-Filters в пакеты Access-Request, Access-Accept, CoA-Request, Accounting-Request и **недопустимо** включение этого атрибута в пакеты Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK или CoA-NAK.

[1] В оригинале - security association - защищённая связь. *Прим. перев.*
[2] Media Access Control - контроль доступа к среде.
[3] Change of Authorization Request - смена авторизации.

Формат атрибута Ingress-Filters показан на рисунке. Поля передаются в порядке слева направо.



Type 57

Length 6

Value

Поле Value имеет размер 4 октета и может включать значения:

1 - Enabled (разрешено);

2 - Disabled (запрещено).

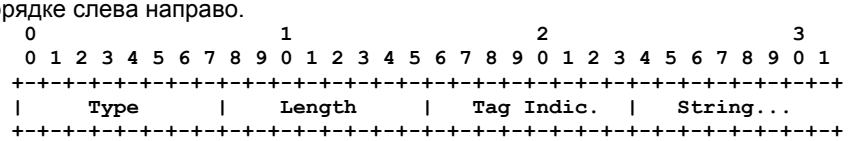
2.3. Egress-VLAN-Name

Пункт 12.10.2.1.3 (a) стандарта [IEEE-802.1Q] описывает административно присваиваемые имена VLAN, связанные VLAN-ID, определёнными для моста IEEE 802.1Q. Атрибут Egress-VLAN-Name представляет разрешённую VLAN для данного порта. Этот атрибут похож на Egress-VLANID, но отличается тем, что само значение VLAN-ID не задаётся и его не нужно знать; вместо идентификатора используется имя VLAN, позволяющее идентифицировать VLAN внутри данной системы.

Туннельные атрибуты, описанные в [RFC3580] могут вместе с Egress-VLAN-Name использоваться для настройки выходных VLAN в случае пакетов без тегов. Эти атрибуты могут использоваться одновременно и их **можно** включать в один пакет RADIUS. Когда атрибуты используются одновременно, список разрешённых VLAN представляет собой конкатенацию атрибутов Egress-VLAN-Name и Tunnel-Private-Group-ID (81). Атрибут Egress-VLAN-Name не меняет входную VLAN (называется также PVID) для пакетов без тегов на данном порту. Следует использовать туннельные атрибуты [RFC3580] вместо установки PVID.

Атрибут Egress-VLAN-Name содержит две части - первая показывает формат кадров VLAN (с тегами или без них), а вторая содержит имя VLAN.

Можно включать множество атрибутов Egress-VLAN-Name в пакеты Access-Request, Access-Accept, CoA-Request и Accounting-Request, но **не допускается** включение этого атрибута в пакеты Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK или CoA-NAK. Каждый атрибут добавляет именованную сеть VLAN в список разрешённых на выходе из порта VLAN. Формат атрибута Egress-VLAN-Name показан на рисунке. Поля передаются в порядке слева направо.



Type 58

Length >=4

Tag Indication

Поле Tag Indication имеет размер 1 октет и показывает наличие (0x31, ASCII '1') или отсутствие (0x32, ASCII '2') тегов в кадрах VLAN. Значения были выбраны для упрощения пользователям ввода нужного варианта.

String

Поле String имеет размер не менее 1 октета и содержит значение VLAN Name, как определено в стандарте [IEEE-802.1Q] п. 12.10.2.1.3 (a). [RFC3629] р**екомендует** использовать символы ISO[1] 10646 в кодировке UTF-8, но реализациям **следует** поддерживать трактовку этого поля без связи с кодировкой символов.

2.4. User-Priority-Table

В стандарте [IEEE-802.1D] п. 7.5.1 обсуждается вопрос регенерации (или повторного отображения) установленного для пользователя приоритета в кадрах, получаемых портом. Независимая для каждого порта конфигурация позволяет мосту устанавливать для полученных через порт кадров определённый уровень приоритета. В п. 6.3.9 [IEEE-802.1D] описано использование такой приоритизации:

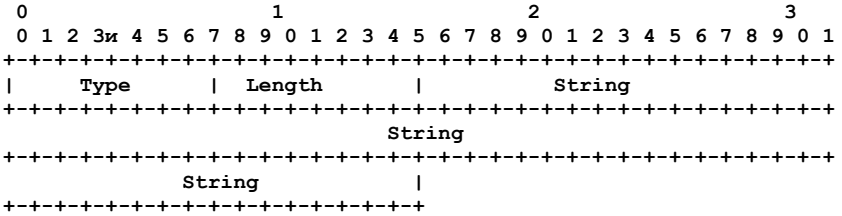
> Возможность указать приоритет пользователя в ЛВС IEEE 802 позволяет организовать сквозную значимость уровня приоритета в масштабе ЛВС на базе мостов (Bridged Local Area Network). В комбинации с отображением приоритета на классы трафика и приоритет доступа это позволяет обеспечить согласованное использование данных о приоритете в соответствии с возможностями мостов и MAC на пути передачи...
>
> При нормальных условиях приоритет не изменяется в процессе передачи через функцию трансляции моста; однако система управления сетью может контролировать распространение уровня приоритета пользователя. Таблица 7-1 обеспечивает возможность отобразить входящие значения приоритета независимо для каждого порта. По умолчанию регенерированное значение приоритета совпадает с полученным значением.

Этот атрибут представляет приоритизацию IEEE 802, которая будет использоваться для всех кадров, приходящих в порт. Стандарт [IEEE-802] определяет 8 значений приоритета. Пункт 14.6.2.3.3 стандарта [IEEE-802.1D] задаёт таблицу регенерации как 8 целочисленных значений в диапазоне 0-7. Переменные управления определены в п. 14.6.2.2.

[1] В оригинале слово ISO при указании набора символов по ошибке было пропущено. *Прим. перев.*

Один атрибут User-Priority-Table **можно** включать в пакеты Access-Accept и CoA-Request; **не допускается** включение этого атрибута в пакеты Access-Request, Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK, CoA-NAK и Accounting-Request. Поскольку таблица регенерации поддерживается только мостами, соответствующими стандарту [IEEE-802.1D], этот атрибут следует передавать только тем клиентам RADIUS, которые поддерживают этот стандарт.

Формат атрибута User-Priority-Table показан на рисунке. Поля передаются в порядке справа налево.



Type 59

Length 10

String

Поле String имеет размер 8 октетов и включает таблицу, которая отображает входящий уровень приоритета (если он установлен; по умолчанию 0) на один из 8 регенерируемых уровней. Первый октет отображает уровень 0 для входящего приоритета, второй - уровень 1 и т. д. Значение каждого октета представляет регенерируемый уровень приоритета для кадра.

Таким образом возможно преобразовать входящие уровни приоритета в более подходящие значения, принимая входящие уровни или изменяя их значения (например, отображая все входящие уровни на одно значение).

В спецификации [IEEE-802.1D] (Annex G) содержится полезное описание отображений типа трафика в классы трафика.

3. Таблица атрибутов

Приведённая ниже таблица показывает какие атрибуты и в каком количестве могут встречаться в пакетах различных типов.

Access-Request	*Access-Accept*	*Access-Reject*	*Access-Challenge*	*CoA-Req*	*Acct-Req*	*№*	*Аттрибут*
0+	0+	0	0	0+	0+	56	Egress-VLANID
0-1	0-1	0	0	0-1	0-1	57	Ingress-Filters
0+	0+	0	0	0+	0+	58	Egress-VLAN-Name
0	0-1	0	0	0-1	0	59	User-Priority-Table

Значения ячеек таблицы имеют следующий смысл:

0 этот атрибут **недопустимо** включать в пакеты данного типа;

0+ в пакете **может** присутствовать 0 и более экземпляров данного атрибута;

0-1 в пакете **может** присутствовать не более 1 экземпляра данного атрибута.

4. Протокол Diameter

При использовании с протоколом Diameter атрибуты, определённые в этой спецификации, могут применяться как пары атрибут-значение (AVP[1]) из пространства кодов 1-255 (пространство совместимости с атрибутами RADIUS). Следовательно, дополнительных значений Diameter Code не выделяется. Типы данных и правила флагов для атрибутов приведены в таблице.

Имя	*Тип*	*Правила AVP Flag*				
		MUST	*MAY*	*SHOULD NOT*	*MUST NOT*	*Encr*
Egress-VLANID	OctetString	M	P		V	Y
Ingress-Filters	Enumerated	M	P		V	Y
Egress-VLAN-Name	UTF8String	M	P		V	Y
User-Priority-Table	OctetString	M	P		V	Y

Для атрибутов из данной спецификации не устанавливается специальных требований преобразования из Diameter в RADIUS и обратно; атрибуты копируются в исходном виде за исключением изменений, относящихся к заголовкам, выравниванию и заполнению. Дополнительную информацию можно найти в [RFC3588] (параграф 4.1) и [RFC4005] (глава 9).

Все, что в данной спецификации сказано о применимости атрибутов к пакетам RADIUS Access-Request, относится и к Diameter AA-Request [RFC4005] или Diameter-EAP-Request [RFC4072]. Все, что применимо к пакетам Access-Challenge, относится также к Diameter AA-Answer [RFC4005] и Diameter-EAP-Answer [RFC4072] с Result-Code AVP = DIAMETER_MULTI_ROUND_AUTH.

Все, что сказано о Access-Accept, применимо и к сообщениям Diameter AA-Answer или Diameter-EAP-Answer, показывающим успешное завершение. Аналогично, все, что сказано о пакетах RADIUS Access-Reject, относится также к сообщениям Diameter AA-Answer и Diameter-EAP-Answer, показывающим отказ.

Все сказанное о пакетах COA-Request применимо к Diameter Re-Auth-Request [RFC4005].

Все сказанное о пакетах Accounting-Request применимо также к Diameter Accounting-Request [RFC4005].

[1]Attribute-value pair - пара «атрибут-значение».

5. Взаимодействие с IANA

Эта спецификация не создаёт каких-либо новых реестров.

Данный документ использует пространство имён RADIUS [RFC2865]; см. http://www.iana.org/assignments/radius-types. Добавление 4 значений в раздел "RADIUS Attribute Types" выполнено IANA. Добавленными атрибутами RADIUS являются:

56 - Egress-VLANID

57 - Ingress-Filters

58 - Egress-VLAN-Name

59 - User-Priority-Table

6. Вопросы безопасности

Эта спецификация описывает использование протоколов RADIUS и Diameter для идентификации, проверки полномочий и учёта в локальных сетях IEEE 802. Вопросы безопасности, связанные с протоколом RADIUS для таких приложений, описаны в [RFC3579] и [RFC3580]; проблемы безопасности, связанные с роумингом, рассмотрены в [RFC2607]. Для протокола Diameter вопросы безопасности, связанные с такими приложениями, рассмотрены в [RFC4005] и [RFC4072].

Данный документ определяет новые атрибуты, которые могут включаться в существующие пакеты RADIUS, и защищаются, как описано в [RFC3579] и [RFC3576]. Для протокола Diameter атрибуты защищаются в соответствии с документом [RFC3588], содержащим детальное описание этой задачи.

Механизмы защиты, поддерживаемые в RADIUS и Diameter, фокусируются на предотвращении подмены пакетов атакующим или изменения пакетов в процессе доставки. Эти механизмы не защищают уполномоченные серверы или посредников (proxy) RADIUS/Diameter от вставки атрибутов с деструктивными целями.

Атрибуты VLAN, передаваемые сервером или посредником RADIUS/Diameter, могут разрешить доступ к сетям VLAN, для которых отсутствуют полномочия. Значение этой уязвимости может быть ограничено путём проверки на уровне NAS. Например, сервер NAS можно настроить на восприятие только некоторого подмножества значений VLANID от данного сервера или посредника RADIUS/Diameter.

Атакующий, получивший контроль над сервером или посредником RADIUS/Diameter, может изменить таблицу приоритетов, что позволит ему снизить качество обслуживания (путём снижения уровня приоритета поступающих в порт кадров) или организовать DoS-атаку (путём повышения уровня приоритета для трафика на множестве портов устройства, приводящего к перегрузке коммутатора или дефициту полосы канала).

7. Литература

7.1. Нормативные документы

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

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865[1], June 2000.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[RFC4363] Levi, D. and D. Harrington, "Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions", RFC 4363, January 2006.

[IEEE-802] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990[2].

[IEEE-802.1D] IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, IEEE Std 802.1D-2004[3], June 2004.

[IEEE-802.1Q] IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks, P802.1Q-2003, January 2003[4].

7.2. Дополнительная литература

[IEEE-802.1X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2004[5], December 2004.

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

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

[RFC3576] 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.

[1] Документ был частично обновлён в RFC 2868, RFC 3575, RFC 5080. *Прим. перев.*
[2] Современная версия этого стандарта доступна по ссылке http://standards.ieee.org/getieee802/download/802-2001.pdf. *Прим. перев.*
[3] Этот стандарт доступен по ссылке http://standards.ieee.org/getieee802/download/802.1D-2004.pdf. *Прим. перев.*
[4] Современная версия этого стандарта доступна по ссылке http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf. *Прим. перев.*
[5] Этот стандарт доступен по ссылке http://standards.ieee.org/getieee802/download/802.1X-2004.pdf. *Прим. перев.*

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

8. Благодарности

Авторы рады отметить Joseph Salowey из Cisco, David Nelson из Enterasys, Chuck Black из Hewlett-Packard и Ashwin Palekar из Microsoft.

Адреса авторов

Paul Congdon
Hewlett-Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5662
Roseville, CA 95747
Phone: +1 916 785 5753
Fax: +1 916 785 8478
EMail: paul.congdon@hp.com

Mauricio Sanchez
Hewlett-Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5559
Roseville, CA 95747
Phone: +1 916 785 1910
Fax: +1 916 785 1815
EMail: mauricio.sanchez@hp.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
Phone: +1 425 706 6605
Fax: +1 425 936 7329
EMail: bernarda@microsoft.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Copyright (C) The Internet Society (2006).

К этому документу применимы права, лицензии и ограничения, указанные в BCP 78, и, за исключением указанного там, авторы сохраняют свои права.

Этот документ и содержащаяся в нем информация представлены "как есть" и автор, организация, которую он/она представляет или которая выступает спонсором (если таковой имеется), Internet Society и IETF отказываются от каких-либо гарантий (явных или подразумеваемых), включая (но не ограничиваясь) любые гарантии того, что использование представленной здесь информации не будет нарушать чьих-либо прав, и любые предполагаемые гарантии коммерческого использования или применимости для тех или иных задач.

Интеллектуальная собственность

IETF не принимает какой-либо позиции в отношении действительности или объема каких-либо прав интеллектуальной собственности (Intellectual Property Rights или IPR) или иных прав, которые, как может быть заявлено, относятся к реализации или использованию описанной в этом документе технологии, 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 RFC можно найти в BCP 78 и BCP 79.

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 из сетевого репозитория IETF IPR по ссылке http://www.ietf.org/ipr.

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. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.

Подтверждение

Финансирование функций RFC Editor обеспечено IETF Administrative Support Activity (IASA).