

Network Working Group
Request for Comments: 3442
Updates: 2132
Category: Standards Track

T. Lemon
Nominum, Inc.
S. Cheshire
Apple Computer, Inc.
B. Volz
Ericsson
December 2002

The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4

Опция бесклассового статического маршрута для протокола DHCP версии 4

Статус документа

Этот документ содержит проект стандартного протокола Internet для сообщества Internet и служит запросом к обсуждению в целях развития и совершенствования. Текущее состояние стандартизации и статус протокола можно узнать из документа «Internet Official Protocol Standards» (STD 1). Документ можно распространять без ограничений.

Авторские права

Copyright (C) The Internet Society (2002). All Rights Reserved.

Тезисы

Этот документ определяет новую опцию протокола DHCP¹, которая передается от сервера DHCP клиенту DHCP для настройки у того списка статических маршрутов. Сети получателей в этих маршрутах являются бесклассовыми и каждый маршрут включает маску подсети.

Введение

Эта опция отменяет опцию Static Route (33), определенную в RFC 2132 [4].

Протокол IP [1] использует маршрутизаторы для передачи пакетов от хостов одной подсети IP хостам, подключенным к другой подсети IP. Когда хост IP (отправитель) хочет передать пакет другому хосту IP (получатель), он просматривает таблицу маршрутов для определения IP-адреса маршрутизатора, который следует использовать для пересылки пакета в направлении целевого хоста.

Таблица маршрутизации на хосте IP может поддерживаться множеством способов - с использованием протоколов маршрутизации, таких как RIP [8], обнаружения маршрутизаторов ICMP [6,9] или использования опции DHCP, определенной в RFC 2132 [4].

В сети, где уже применяется DHCP, использование протокола DHCP для обновления таблицы маршрутизации клиента DHCP дает несколько преимуществ. Это эффективно, поскольку использует сообщения, которые в любом случае будут передаваться. Это удобно - конфигурация сервера уже поддерживается, поэтому поддержка маршрутной информации (по крайней мере в относительно стабильной сети) не добавит много работы. Если услуги DHCP уже используются, другой инфраструктуры не нужно.

Протокол DHCP в соответствии с RFC 2131 [3] и опции, определенные в RFC 2132 [4], обеспечивают лишь механизм организации используемого по умолчанию маршрута или установки таблицы с маршрутами по классам адресов. Классовыми называют маршруты, в которых маска подсети неявно задается номером подсети (см. параграф 3.2 в STD 5, RFC 791 [1]).

Маршрутизация по классам вышла из употребления, поэтому опция DHCP Static Route стала бесполезной. В настоящее время бесклассовая маршрутизация [7, 10] стала общепринятой формой маршрутизации в Internet. В бесклассовой маршрутизации адреса IP состоят из номера сети (комбинация номера сети и номера подсети, описанная в RFC 950 [7]) и номера хоста.

В IP с классами номер сети и номер хоста выводились из адреса IP с использованием битовой маски, значение которой определялось несколькими первыми битами адреса IP. В IP без классов номер сети и номер хоста выводятся из адреса IP с использованием отдельного значения - маски подсети. Для определения сети, к которой относится данный маршрут, хост IP должен знать номер сети и маску подсети.

Опция Static Route (33) не указывала маску подсети для маршрутов, предполагая, что эта маска неявно определяется номером сети в каждой записи. Опция Classless Static Routes указывает маску подсети для каждой записи, поскольку маска может отличаться от определенной с помощью алгоритма из STD 5, RFC 791 [1] и STD 5, RFC 950 [7].

Определения

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14, RFC 2119 [2].

Ниже приведены определения используемых в документе терминов.

¹Dynamic Host Configuration Protocol - протокол динамической настройки конфигурации хоста.

DHCP client – клиент DHCP

Клиентом DHCP (клиентом) является хост Internet, использующий протокол DHCP для получения параметров конфигурации, таких как сетевой адрес.

DHCP server – сервер DHCP

Сервером DHCP (сервером) является хост Internet, который возвращает параметры конфигурации клиентам DHCP.

Link - канал

Любой набор точек подключения к сети, который будет принимать все широкоэвещательные кадры канального уровня, переданные любой из точек подключения. Этот термин применяется в DHCP, поскольку в некоторых случаях на канале может быть организована не одна подсеть IP. DHCP использует широкоэвещательный адрес local-network (все единицы), который не связан с подсетью и поэтому пакеты будут видны всем подключенным к каналу узлам, независимо от подсети или подсетей IP, которые на узле настроены.

Канал иногда называют доменом широкоэвещания или физическим сегментом сети.

Формат опции Classless Routes

Эта опция имеет код 121 и минимальный размер 5 байтов. Опция может содержать один или множество статических маршрутов, каждый из которых включает дескриптор адресатов и IP-адрес маршрутизатора, который следует использовать для этих адресатов.

```
Code Len Destination 1 Router 1
+-----+-----+-----+-----+-----+-----+
| 121 | n | d1 | ... | dN | r1 | r2 | r3 | r4 |
+-----+-----+-----+-----+-----+-----+
```

```
Destination 2 Router 2
+-----+-----+-----+-----+-----+
| d1 | ... | dN | r1 | r2 | r3 | r4 |
+-----+-----+-----+-----+-----+
```

В приведенном выше примере заданы 2 статических маршрута.

Дескриптор получателя описывает номер подсети IP и маску для конкретного получателя с использованием компактного формата. Запись состоит из октета, указывающего размер маски, за которым следуют все значимые октеты номера подсети.

Размер маски указывает число битов. Например, подсеть с номером 10.0.127.0 и маской 255.255.255.0 будет иметь размер маски 24.

Значимая часть номера подсети включает все октеты номера подсети, для которой соответствующий октет маски имеет отличное от нуля значение. Число значимых октетов равно размеру маски, поделенному на 8 с округлением в большую сторону, как показано в таблице.

Размер маски	Число значимых октетов
0	0
1-8	1
9-16	2
17-24	3
24-32	4

В следующей таблице приведены некоторые примеры представления разных номеров сети и масок.

Номер подсети	Маска подсети	Дескриптор адресата
0	0	0
10.0.0.0	255.0.0.0	8.10
10.0.0.0	255.255.255.0	24.10.0.0
10.17.0.0	255.255.0.0	16.10.17
10.27.129.0	255.255.255.0	24.10.27.129
10.229.0.128	255.255.255.128	25.10.229.0.128
10.198.122.47	255.255.255.255	32.10.198.122.47

Маршруты в локальные подсети

В некоторых случаях на канале может быть более одной подсети IP. При этом хост с IP-адресом из одной подсети может напрямую взаимодействовать с хостом, имеющим адрес IP из другой подсети на том же канале. Когда клиенту назначается IP-адрес из подсети на таком канале, для каждой другой подсети IP на этом канале сервер DHCP **можно** настроить на установку для маршрутизатора IP-адреса 0.0.0.0.

Например, рассмотрим случай наличия на канале трех подсетей IP - 10.0.0/24, 192.168.0/24, 10.0.21/24. Если клиенту назначен адрес IP 10.0.21.17, сервер может включить маршрут с адресатами 10.0.0/24 и маршрутизатором 0.0.0.0, а также маршрут с адресатами 192.168.0/24 и маршрутизатором 0.0.0.0.

Клиент DHCP, чей стек TCP/IP не обеспечивает такой возможности, **должен** игнорировать опцию Classless Static Routes, где указан IP-адрес маршрутизатора 0.0.0.0. Следует отметить, что описанное здесь поведение применимо лишь к опции Classless Static Routes, но не к опциям Static Routes и Router.

Поведение клиента DHCP

Не поддерживающие эту опцию клиенты DHCP **должны** игнорировать ее при получении от сервера DHCP. Поддерживающие опцию клиенты DHCP **должны** установить заданные в опции маршруты, за исключением указанных в параграфе «Маршруты в локальные подсети». Поддерживающим опцию клиентам DHCP **недопустимо** устанавливать маршруты, указанные в опции Static Routes (33), если присутствуют обе опции Static Routes и Classless Static Routes.

Клиенты DHCP, поддерживающие эту опцию и передающие опцию DHCP Parameter Request List, **должны** запрашивать эту опцию и опцию Router [4] в DHCP Parameter Request List.

Клиенты DHCP, поддерживающие эту опцию и передающие запрос списка параметров, **могут** также запросить опцию Static Routes для совместимости со старыми серверами, не поддерживающими Classless Static Routes. Код опции Classless Static Routes **должен** включаться в список запроса параметров до кодов опций Router и Static Routes, если они указываются.

Если сервер DHCP возвращает обе опции Classless Static Routes и Router, клиент DHCP **должен** игнорировать опцию Router.

Точно так же при возврате сервером обеих опций Classless Static Routes и Static Routes клиент DHCP **должен** игнорировать опцию Static Routes.

После вывода номера и маски подсети из дескриптора адресата клиент DHCP **должен** сбросить в 0 все биты номера подсети, для которых соответствующий бит маски имеет значение 0. Иными словами, номер подсети в таблице маршрутизации определяется результатом логической операции AND (И) для номера подсети и маски подсети из опции Classless Static Routes. Например, если сервер передал маршрут с получателем 129.210.177.132 (шестнадцатеричное значение 81D4B184) и маской подсети 255.255.255.128 (шестнадцатеричное значение FFFFFFF80), клиент будет устанавливать маршрут с получателем 129.210.177.128 (шестнадцатеричное значение 81D4B180).

Предотвращение ограничения размеров

Поскольку полная таблица маршрутов может быть достаточно большой, стандартного максимального размера сообщений DHCP в 576 октетов может оказаться недостаточно для некоторых опций Classless Static Route. По этой причине клиентам, реализующим опцию Classless Static Route, **следует** передать опцию Maximum DHCP Message Size [4], если стек TCP/IP у клиента DHCP способен принимать более крупные дейтаграммы IP. В этом случае клиенту **следует** указывать в качестве значения этой опции как минимум значение MTU на интерфейсе, который настраивается. Клиент **может** указать для этой опции любое значение вплоть до максимального размера пакета UDP, который он готов принять (отметим, что значение опции Maximum DHCP Message Size ограничивает общий размер пакета с учетом заголовков IP и UDP).

Клиенты DHCP, запрашивающие эту опцию, и передающие ее серверы DHCP **должны** поддерживать конкатенацию опций DHCP [5]. В терминологии RFC 3396 [5] опция Classless Static Route Option является требующей конкатенации.

Администрирование серверов DHCP

Многие клиенты могут не поддерживать опцию Classless Static Routes. Поэтому администраторы серверов DHCP настраивают свои серверы на отправку опций Router и Classless Static Routes, при этом следует указывать используемые по умолчанию маршрутизаторы в обеих опциях Router и Classless Static Routes.

Когда клиент DHCP запрашивает опцию Classless Static Routes, а также одну или обе опции Router и Static Routes, а сервер DHCP передает этому клиенту опцию Classless Static Routes, серверу **не следует** включать опции Router и Static Routes.

Вопросы безопасности

Возможные атаки на протокол DHCP рассмотрены в разделе 7 спецификации DHCP [3] и в документе по аутентификации сообщений DHCP [11].

Опцию Classless Static Routes можно использовать для перенаправления сетевого трафика путем указания некорректных IP-адресов для маршрутизаторов. Это может быть DoS¹-атака, где указывается недействительный IP-адрес маршрутизатора или MITM²-атака, где указывается специальный адрес IP для сбора и анализа пакетов. Это не создает новой проблемы, поскольку опции Router и Static Routes, определенные в RFC 2132 [4] имели такие же уязвимости.

Взаимодействие с IANA

Для этой опции DHCP выделен код 121 в списке опций DHCP, поддерживаемом IANA.

Нормативные документы

[1] Postel, J., "Internet Protocol", STD 5, [RFC 791](#), September 1981.

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

[3] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.

[4] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), March 1997.

[5] Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, November 2002.

¹Denial of Service - отказ в обслуживании.

²Man-in-the-middle - перехват и изменение пакетов с участием человека.

Дополнительная литература

- [6] Postel, J., "Internet Control Message Protocol", STD 5, [RFC 792](#), September 1981.
- [7] Mogul, J. and J. Postel, "Internet Standard Subnetting Procedure", STD 5, [RFC 950](#), August 1985.
- [8] Hedrick, C., "Routing Information Protocol", RFC 1058, June 1988.
- [9] Deering, S., "ICMP Router Discovery Messages", RFC 1256, September 1991.
- [10] Pummill, T. and B. Manning, "Variable Length Subnet Table For IPv4", RFC 1878, December 1995.
- [11] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", [RFC 3118](#), June 2001.

Права интеллектуальной собственности

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Адреса авторов

Ted Lemon

Nominum, Inc.
2385 Bay Road
Redwood City, CA 94063
EMail: Ted.Lemon@nominum.com

Stuart Cheshire

Apple Computer, Inc.
1 Infinite Loop
Cupertino
California 95014
USA
Phone: +1 408 974 3207
EMail: rfc@stuartcheshire.org

Bernie Volz

Ericsson
959 Concord Street
Framingham, MA, 01701
Phone: +1 508 875 3162
EMail: bernie.volz@ericsson.com

Перевод на русский язык

Николай Малых
nmalykh@gmail.com

Полное заявление авторских прав

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.