RFC7844 comments Documentation

Release 0.1

juga

Jul 17, 2017
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Relevant RFCs</td>
<td>3</td>
</tr>
<tr>
<td>1.1</td>
<td>IETF DHC Working Group mailing list</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>RFC7844 DHCPv4 summary and comments</td>
<td>5</td>
</tr>
<tr>
<td>2.1</td>
<td>Message types</td>
<td>5</td>
</tr>
<tr>
<td>2.2</td>
<td>Message Options</td>
<td>7</td>
</tr>
<tr>
<td>2.3</td>
<td>Operational considerations</td>
<td>9</td>
</tr>
<tr>
<td>2.4</td>
<td>Not specified in RFC7844, but in RFC2131</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>Windows 10 RFC7844 implementation</td>
<td>13</td>
</tr>
<tr>
<td>4</td>
<td>Indices and tables</td>
<td>15</td>
</tr>
</tbody>
</table>
Relevant RFCs

- IETF DHC Working Group (forked) privacy repository
- DHCP Anonymity Profiles RFC7844
- DHCP Dynamic Host Configuration Protocol
- Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)

IETF DHC Working Group mailing list

messages discussing RFC7844:
- Searchable dhcwg mailing list
- dhcwg mailing list anonymity profiles filtered
- dhcwg mailing list anonymity profiles filtered mbox
RFC7844 DHCPv4 summary and comments

In order to reveal less identifying information, the options in DHCP should be reduced in number and be more “homogenous” for all implementations, as stated in [RFC 7844#section-2.4]:

The design of the Anonymity Profiles attempts to minimize the number of options and the choice of values, in order to reduce the possibilities of operating system fingerprinting.

To reveal still less identifying information most of the MAY, SHOULD keywords should be replaced by MUST or MUST NOT.

Most of the comments here are regarding the verbs (key words [RFC 2119]) used.

See RFC7844 DHCPv4 restricted version summary for what would be a more restrictive version of [RFC 7844], where the keywords are actually replaced. Use diff to see specific differences between these two documents.

Note: Extracts from the [RFC 7844] marked as literal blocks.

Message types

DHCP*

[RFC 7844#section-3.1]:

SHOULD randomize the ordering of options

This could be s/SHOULD/MUST

If this can not be implemented
MAY order the options by option code number (lowest to highest).

This could be s/MAY/MUST
DHCPDISCOVER

[RFC 7844#section-3.]:

MUST contain the Message Type option,

MAY contain the Client Identifier option,
MAY contain the Parameter Request List option.

This could be s/MAY/MUST NOT, though:

- Some servers will not answer to clients that does not contain the Client Identifier
- what RFC for DHCP server says about it?:

  SHOULD NOT contain any other option.

This could be s/SHOULD NOT/MUST NOT

DHCPREQUEST

[RFC 7844#section-3.]:

MUST contain the Message Type option,

MAY contain the Client Identifier option,
MAY contain the Parameter Request List option.

MAY, SHOULD NOT as in DHCPDISCOVER:

If in response to a DHCPOFFER,
MUST contain the corresponding Server Identifier option
MUST contain the Requested IP address option.

If the message is not in response to a DHCPOFFER (BOUND, RENEW),
MAY contain a Requested IP address option

This could be s/MAY/MUST?

DHCPDECLINE

[RFC 7844#section-3.]:

MUST contain the Message Type option,
MUST contain the Server Identifier option,
MUST contain the Requested IP address option;

MAY contain the Client Identifier option.

MAY as in DHCPDISCOVER

Why here there is not SHOULD NOT as in DHCPDISCOVER
DHCPRELEASE

[RFC 7844#section-3.]:

MUST contain the Message Type option and
MUST contain the Server Identifier option,

MAY contain the Client Identifier option.

MAY as in DHCPDISCOVER

To do not leak when the client leaves the network, this message type should not be implemented.

In this case, servers might run out of leases, but that is something that servers should fix decreasing the lease time.

DHCPINFORM

[RFC 7844#section-3.]:

MUST contain the Message Type option,

MAY contain the Client Identifier option,
MAY contain the Parameter Request List option.

It SHOULD NOT contain any other option.

MAY, SHOULD NOT as in DHCPDISCOVER

Message Options

Client IP address (ciaddr)

[RFC 7844#section-3.2]:

MUST NOT include in the message a Client IP address that has been obtained with a different link-layer address.

Requested IP Address Option (code 50)

[RFC 7844#section-3.3]:

SHOULD NOT use the Requested IP address option in DHCPDISCOVER messages.
MUST use the option when mandated (DHCPREQUEST)

If in INIT-REBOOT:
SHOULD perform a complete four-way handshake, starting with a DHCPDISCOVER

If the client can ascertain that this is exactly the same network to which it was previously connected, and if the link-layer address did not change, MAY issue a DHCPREQUEST to try to reclaim the current address.

2.2. Message Options
Client Hardware Address Field

[RFC 7844#section-3.4]:

The presence of this address is necessary for the proper operation of the DHCP service.

What should be interpreted as MUST:

If the hardware address is reset to a new randomized value, the DHCP client SHOULD use the new randomized value in the DHCP messages.

The client should be restarted when the hardware address changes and use the current address instead of the permanent one.

Client Identifier Option (code 61)

[RFC 7844#section-3.5]:

DHCP clients MUST use client identifiers based solely on the link-layer address that will be used in the underlying connection.

As in DHCPDISCOVER, it SHOULD NOT have this option.

Parameter Request List Option (PRL) (code 55)

[RFC 7844#section-3.6]:

SHOULD only request a minimal number of options in the PRL and SHOULD also randomly shuffle the ordering of option codes in the PRL. If this random ordering cannot be implemented, MAY order the option codes in the PRL by option code number (lowest to highest).

As in DHCPDISCOVER

Host Name option (code 12)

[RFC 7844#section-3.7]:

SHOULD NOT send the Host Name option. If they choose to send the option [..]

As in DHCPDISCOVER

Client FQDN Option (code 81)

[RFC 7844#section-3.8]:

SHOULD NOT include the Client FQDN option

As in DHCPDISCOVER
MAY include a special-purpose FQDN using the same host name as in the Host Name option, with a suffix matching the connection-specific DNS suffix being advertised by that DHCP server.

reason why it MAY:

Having a name in the DNS allows working with legacy systems that require one to be there.

**UUID/GUID-Based Client Machine Identifier Option (code 97)**

[RFC 7844#section-3.9]:

This option is part of a set of options for the Intel Preboot eXecution Environment (PXE).

Common sense seems to dictate that getting a new operating system from an unauthenticated server at an untrusted location is a really bad idea and that even if the option was available users would not activate it.

Nodes visiting untrusted networks MUST NOT send or use the PXE options.

**User and Vendor Class DHCP Options**

[RFC 7844#section-3.10]:

SHOULD NOT use the Vendor-Specific Information option (code 43), the Vendor Class Identifier option (code 60), the V-I Vendor Class option (code 124), or the V-I Vendor-Specific Information option (code 125),

This could be s/SHOULD NOT/MUST NOT?

**Operational considerations**

[RFC 7844#section-5.]:

Implementers SHOULD provide a way for clients to control when the anonymity profiles are used and when standard behavior is preferred.

**Not specified in RFC7844, but in RFC2131**

**Probe the offered IP**

[RFC 2131#section-2.2]:

2.3. Operational considerations
The allocating server SHOULD probe the reused address before allocating the address, e.g., with an ICMP echo request, and the client SHOULD probe the newly received address, e.g., with ARP.

The client SHOULD perform a check on the suggested address to ensure that the address is not already in use. For example, if the client is on a network that supports ARP, the client may issue an ARP request for the suggested address. When broadcasting an ARP request for the suggested address, the client must fill in its own hardware address as the sender’s hardware address, and 0 as the sender’s IP address, to avoid confusing ARP caches in other hosts on the same subnet.>>

The client SHOULD broadcast an ARP reply to announce the client's new IP address and clear any outdated ARP cache entries in hosts on the client's subnet.

This could be s/SHOULD/MUST.

Retransmission delays

Sending DHCPDISCOVER [RFC 2131#section-4.4.1]:

The client SHOULD wait a random time between one and ten seconds to desynchronize the use of DHCP at startup.

[RFC 2131#section-3.1]:

a client retransmitting as described in section 4.1 might retransmit the DHCPREQUEST message four times, for a total delay of 60 seconds

[RFC 2131#section-4.4.5]:

In both RENEWING and REBINDING states, if the client receives no response to its DHCPREQUEST message, the client SHOULD wait one-half of the remaining time until T2 (in RENEWING state) and one-half of the remaining lease time (in REBINDING state), down to a minimum of 60 seconds, before retransmitting the DHCPREQUEST message.

[RFC 2131#section-4.1]:

For example, in a 10Mb/sec Ethernet internetwork, the delay before the first retransmission SHOULD be 4 seconds randomized by the value of a uniform random number chosen from the range -1 to +1

Clients with clocks that provide resolution granularity of less than one second may choose a non-integer randomization value.

The delay before the next retransmission SHOULD be 8 seconds randomized by the value of a uniform number chosen from the range -1 to +1.
The retransmission delay SHOULD be doubled with subsequent retransmissions up to a maximum of 64 seconds.

Selecting offer algorithm

[RFC 2131#section-4.2]:

DHCP clients are free to use any strategy in selecting a DHCP server among those from which the client receives a DHCPOFFER message.

Client may choose to collect several DHCPOFFER messages and select the "best" offer.

If the client receives no acceptable offers, the client may choose to try another DHCPDISCOVER message.

[RFC 2131#section-4.4.1]:

The client collects DHCPOFFER messages over a period of time, selects one DHCPOFFER message from the (possibly many) incoming DHCPOFFER messages.

The time over which the client collects messages and the mechanism used to select one DHCPOFFER are implementation dependent.

Timers

[RFC 2131#section-4.4.5]:

Times T1 and T2 are configurable by the server through options. T1 defaults to \((0.5 \ast \text{duration
d_of
t_lease})\). T2 defaults to \((0.875 \ast \text{duration_of_lease})\). Times T1 and T2 SHOULD be chosen with some random "fuzz" around a fixed value, to avoid synchronization of client reacquisition.

Leases

[RFC 7844#section-3.3]:

There are scenarios in which a client connecting to a network remembers a previously allocated address, i.e., when it is in the INIT-REBOOT state. In that state, any client that is concerned with privacy SHOULD perform a complete four-way handshake, starting with a DHCPDISCOVER, to obtain a new address lease. If the client can ascertain that this is exactly the same network to which it was previously connected, and if the link-layer address did not change, the client MAY issue a DHCPREQUEST to try to reclaim the current address.
Windows 10 implements DHCP Anonymity Profiles\(^1\) on wireless devices when enabling hardware address randomization\(^2\).

---

\(^1\) DHCP Anonymity Profiles Update: https://www.ietf.org/proceedings/93/slides/slides-93-dhc-1.pdf


\(^3\) How and why to use random hardware addresses: https://support.microsoft.com/en-us/instantanswers/dd1d98f6-7253-9b21-2b7e-06aa6063de9b/how-and-why-to-use-random-hardware-addresses
CHAPTER 4

Indices and tables

• genindex
• modindex
• search
## Index

<table>
<thead>
<tr>
<th>RFC</th>
<th>Sections</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2119</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>RFC 2131</td>
<td>section-2.2</td>
<td>9</td>
</tr>
<tr>
<td>RFC 2131</td>
<td>section-3.1</td>
<td>10</td>
</tr>
<tr>
<td>RFC 2131</td>
<td>section-4.1</td>
<td>10</td>
</tr>
<tr>
<td>RFC 2131</td>
<td>section-4.2</td>
<td>11</td>
</tr>
<tr>
<td>RFC 2131</td>
<td>section-4.4.1</td>
<td>10, 11</td>
</tr>
<tr>
<td>RFC 2131</td>
<td>section-4.4.5</td>
<td>10, 11</td>
</tr>
<tr>
<td>RFC 7844</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-2.4</td>
<td>5</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3..</td>
<td>6, 7</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3.1</td>
<td>5</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3.10</td>
<td>9</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3.2</td>
<td>7</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3.3</td>
<td>7, 11</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3.4</td>
<td>8</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3.5</td>
<td>8</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3.6</td>
<td>8</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3.7</td>
<td>8</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3.8</td>
<td>8</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-3.9</td>
<td>9</td>
</tr>
<tr>
<td>RFC 7844</td>
<td>section-5..</td>
<td>9</td>
</tr>
</tbody>
</table>