Simple Host Discovery and Configuration Protocol
<draft-d1f-shdcp-00.txt>

Status of this Memo

This document is an Internet-Draft.

Internet-Drafts are working documents of the Internet Engineering
Task Force (IETF), its areas, and its working groups.
Note that other groups may also distribute working documents
as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months
and may be updated, replaced, or obsoleted by other documents at
any time. It is inappropriate to use Internet-Drafts as
reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html

This Internet-Draft is submitted in full conformance with the
provisions of BCP 78 and BCP 79.

Distribution of this memo is unlimited.

Copyright and License Notice

Copyright (c) 2013 IETF Trust and the persons identified
as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date
of publication of this document.
Please review these documents carefully, as they describe
your rights and restrictions with respect to this document.

Abstract

The Simple Host Discovery and Configuration Protocol (SHDCP)
provides a mechanism used when an Internet host with almost no
configuration has to be discovered and, at the same time,
configured to some IPv4 network.
This task can not be accomplished by DHCP.
Other known protocols are too complicated or proprietary.
The key feature of the proposed protocol is simplicity.
1. Introduction

1.1. Scope

This document applies only to IPv4 over Ethernet. The IPv6 has its own discovery and configuration mechanisms that are not covered by this document.

1.2. Problem Statement

A number of embedded device types exists which are Internet hosts with an IPv4 network stack and without an IPv4 address assigned. These devices are intended to be used in an Ethernet Local Area Network (LAN) with IPv4 addresses. The devices must be adapted to user’s LAN environment. The devices have no mechanism to adapt to user’s LAN environment besides communication via the built-in Ethernet port.

The following solutions are neither possible nor acceptable:

* Pre-assigning static IPv4 addresses at factory can conflict with existing user’s LAN environment.

* Assigning IPv4 addresses with DHCP:
  * requires that a DHCP server exists in user’s LAN environment;
  * if a DHCP server exists, it is difficult to determine what is new unknown host that sent the DHCP discovery request.

* Assigning Link-local addresses automatically will not conflict with user’s LAN environment, but it would be difficult to communicate with such device from user’s control point host which can have other network subnet address.

Other discovery protocols are either too complicated or solve only discovery task but not initial device
configuration with assigning IPv4 address.

1.3. Proposed Solution

The SHDCP is intended to do a minimal task of discovery of new hosts and assigning them a minimal address configuration that conforms to user’s LAN environment and that would be enough to communicate and configure the device by higher level protocols.

2. Terminology

"Control Point"
A Control Point is an Internet host with a SHDCP client program used for discovery and configuration of other Internet hosts (devices) by SHDCP. Control Point may have a human operator.

"Device"
A Device is an Internet host that provides some type of service. Device allows to be discovered and configured by the SHDCP Control Point with configuration parameters such as a network address. Device must have its own unique Ethernet address.

"SHDCP client"
A SHDCP client is a program that implements function of a Control Point.

"SHDCP server"
A SHDCP server is a program that implements function of a SHDCP Device - responds to discovery requests, announces Device, configures Device on a configure request.

3. Protocol Description

3.1. Device States

Device has following states:

* UNCONFIGURED

This state is factory default.

Device may have any IPv4 address assigned which is not used to communicate by SHDCP.

Device must have its own unique Ethernet address which is the key for SHDCP communications.

* CONFIGURED

This state is achieved either by SHDCP configuration or any other configuration method by higher level protocols.

Device can be configured by SHDCP CONFIGURE request only once. Configured device must reject any other SHDCP configure
requests.

* DHCP

Device have its current IPv4 address assigned by DHCP.

3.2. Model of Operation

The SHDCP Control Point discovers SHDCP Devices using broadcast UDP packets with an assigned UDP port (not yet allocated by IANA).

Discovery packets have the command field filled with value of DISCOVERY_REQUEST.

The Device responds with a packet with the command field filled by value of DISCOVERY_RESPONSE. The Flag bits must be filled with current Device states. Other part of the response packet is filled with current network configuration and optional strings which describe other device features.

The Device can optionally send ANNOUNCE packets which almost the same as DISCOVERY_RESPONSE. The only difference is the command value. ANNOUNCE packets can be sent on each device startup and on each change of device’s network configuration.

The Control Point sends a CONFIGURE packet destined to the Device by the Ethernet address. Only unconfigured device accepts this type of packet and performs requested configuration.

The only difference in Devices is their own Ethernet addresses.

<table>
<thead>
<tr>
<th>Host</th>
<th>Control point</th>
</tr>
</thead>
<tbody>
<tr>
<td>* -&gt; ANNOUNCE</td>
<td>*</td>
</tr>
<tr>
<td>* &lt;- DISCOVERY_REQUEST</td>
<td>*</td>
</tr>
<tr>
<td>* -&gt; DISCOVERY_RESPONSE</td>
<td>*</td>
</tr>
<tr>
<td>* &lt;- CONFIGURE</td>
<td>*</td>
</tr>
</tbody>
</table>

3.3. IP Header Values

Time to Live
A TTL value of 1 is used.

Type of Service
A TOS value of 0 is used.

Protocol
A UDP (User Datagram Protocol) value of 17 is used.

Source Address
The device IP address on the interface if one has been
configured (or learned through an address assignment mechanism). Otherwise 0.0.0.0 should be used.

Destination Address

Broadcast address 255.255.255.255.

3.4. UDP Header Values

Destination Port

FIXME <SHDCP port> is not assigned by IANA

3.5. Packet Structure

<table>
<thead>
<tr>
<th>Offset</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5</td>
<td>Signature, sequence of 5 ASCII symbols ‘SHDCP’</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>Protocol version, 0</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>Command</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>Flags</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>Reserved, 0</td>
</tr>
<tr>
<td>10</td>
<td>6</td>
<td>Ethernet address, in network byte order</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>IPv4 address, in network byte order</td>
</tr>
<tr>
<td>20</td>
<td>4</td>
<td>IPv4 netmask, in network byte order</td>
</tr>
<tr>
<td>24</td>
<td>4</td>
<td>IPv4 broadcast address, in network byte order</td>
</tr>
<tr>
<td>28</td>
<td>4</td>
<td>IPv4 gateway address, in network byte order</td>
</tr>
<tr>
<td>32</td>
<td>Variable</td>
<td>Optional, sequence of zero terminated ASCII strings</td>
</tr>
</tbody>
</table>

Command | Value Message direction
---------|------------------------|
ANNOUNCE | 0   host -> control point (like RESPONSE) |
DISCOVERY_REQUEST | 1   control point -> host |
DISCOVERY_RESPONSE | 2   host -> control point |
CONFIGURE | 3   control point -> host |

Flags | Value Description
--------|------------------------|
CONFIGURED | 1   Host is configured |
DHCP       | 2   Host uses DHCP |

Optional strings field is a sequence of zero terminated ASCII strings.

String1\0String2\0String3\0[...]

where \0 is string terminating zero octet.

Strings are limited by common packet length.

It is recommended to use strings by pairs as key and value.
Example:

"type"    "camera" | "router" | whatever
"vendor"  "Sigrand"
"model"   "SG-1C-121"
"sw_ver"  "1.0.3703"
"hw_ver"  "1"
It is recommended that a packet with strings fits in a single Ethernet packet.

The default maximum transmission unit for UDP messages is 1400 bytes excluding UDP and other headers. This length is more than enough for any reasonable payload.

### 3.6. Packet Repeats

Since the protocol has no acknowledgement mechanisms, it is common practice to compensate possible packet loss by repeating messages several times.

* DISCOVERY_REQUEST and ANNOUNCE should be repeated 4 times with 0.5 seconds interval.

* DISCOVERY_RESPONSE should be sent only once on each of DISCOVERY_REQUEST packets.

* CONFIGURE should be sent only once to each device. The Control point can verify that CONFIGURE succeeds either by receiving ANNOUNCE from the reconfigured device or by sending DISCOVERY_REQUEST to the device selectively.

### 3.7. Security Considerations

The protocol has no security mechanisms. Unconfigured devices may be caught up by any unauthorized person. This is compensated by one time configuration — once configured, devices must ignore any other CONFIGURE requests. Other security should be provided by higher level protocols.

### 3.8. IANA Considerations

UDP port number for the protocol should be assigned by IANA. A single number of the User Ports range from 1024-49151 would be acceptable.

### A. Authors’ Addresses

Dmitry Fedorov  
Sigrand LLC  
Lavrentieva prospect 6/6  
ofﬁce 16  
Novosibirsk 630090  
Russia

Phone: +7 913 915 8477  
E-mail: dmitry@sigrand.com

### B. Full Copyright Statement
This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

C. Disclaimer

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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."