Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 23 April 2026

J. Woodworth
D. Ballew
Lumen Technologies, Inc.
T. Wicinski
Cox Communications, Inc.

20 October 2025

Defend the World from IoT Remote-threats & Malware
draft-woodworth-dhcp-dwirm-00

Abstract

Internet of Things (IoT) devices are commonly added to home networks without fully understanding which services (hosts, ports, protocols) are being provided or consumed for those devices to operate. As a result, they are essentially unmanaged threats with full access to that network and the internet. The Defend the World from IoT Remote-threats & Malware (DWIRM) extension to DHCP provides a framework for IoT devices to negotiate services that the local router in turn enforces as policy.

Ed note

Text inside square brackets ([]) is additional background information, answers to frequently asked questions, general musings, etc. They will be removed before publication. This document is being collaborated on in google drive at <https://drive.google.com/drive/folders/18FPj9DCoRJolb77SKsS1q61shCgBfxYb?usp=sharing>. The most recent version of the document, open issues, etc should all be available here. The authors gratefully accept pull requests.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 23 April 2026.

Table of Contents

1. Introduction

The DWIRM extension to DHCP defines an "IoT Profile" JSON object defining which services are provided and consumed by that device broken into categories, and specific requirements. Based on local router policies and potential interaction with the network administrator, an optionally amended service confirmation is provided and enforced.

For example, consider the following DHCPDWIRMCLIENT message:

```
{
    "IoT Profile" : {
        "Description" : "Example Brand Security Camera"
       ,"Provide"     : {
            "Video Stream"  : {
                "Ports"     : "88-99"
               ,"PortFwd"   : "88-99:8088-8099"
               ,"Rate"      : "2Mbps"
               ,"Schedule"  : "00:00-23:59"
               ,"Hints"     : "RTSP"
            }
           ,"Management"    : {
                "Ports"     : "80,443,22"
               ,"Rate"      : "15Kbps"
               ,"Schedule"  : "00:00-23:59"
               ,"Hints"     : "HTTP,HTTPS,SSH"
            }
        }
       ,"Consume"     : {
            "Firmware Update"     : {
                "Endpoints" : [
                    "https://update.example.com/prod/9876543v2/upgrade"
                   ,"https://mirror.example-com.example.net:8888/...de"
                   ,"sftp://update.example.com:/prod/9876543v2/upgrade"
                ]
               ,"Rate"      : "5Mbps"
               ,"Schedule"  : "02:00-04:59"
            }
        }
    }
}
```

The IoT device (DWIRMCLIENT) identifies itself as "Example Brand Security Camera," providing "Video Stream" and "Management" services, and consuming a "Firmware Update" service. In addition to specific port ranges, the expected transfer rates and operational time windows are offered.

If DWIRM is supported by the local router, this message would be followed by a corresponding DHCPDWIRMSERVER message notifying the DWIRM client device of any changes in enforcement based on the local router policy. If, for any reason, this the local router is unable to respond within 100 milliseconds, it will continue with a DHCPOFFER. In this scenario, the DWIRM client will accept an unsolicited DHCPDWIRMSERVER message from the local router.

In this example, the the DWIRM server, responds with the following message:

```
{
    "IoT Profile" : {
        "Description" : "Example Brand Security Camera"
       ,"Provide"     : {
            "Video Stream"  : {
                "Ports"     : "88-99"
               ,"PortFwd"   : ""
               ,"Rate"      : "2Mbps"
               ,"Schedule"  : "00:00-23:59"
               ,"Hints"     : "RTSP"
            }
           ,"Management"    : {
                "Ports"     : "80,443,22"
               ,"Rate"      : "15Kbps"
               ,"Schedule"  : "00:00-23:59"
               ,"Hints"     : "HTTP,HTTPS,SSH"
            }
        }
       ,"Consume"     : {
            "Firmware Update"     : {
                "Endpoints" : [
                    "https://update.example.com/prod/9876543v2/upgrade"
                   ,"https://mirror.example-com.example.net:8888/...de"
                   ,"sftp://update.example.com:/prod/9876543v2/upgrade"
                ]
               ,"Rate"      : "5Mbps"
               ,"Schedule"  : "02:00-04:59"
            }
        }
    }
}
```

This DHCPDWIRMSERVER message is identical to the request, with the exception of the "PortFwd" option, which has been left blank, indicating port-forwarding will not be enabled.

The DWIRM server may also a special JSON object to fully allow or deny the DWIRM client request, by using the "Status" sub-object, as shown below.

```
{
    "IoT Profile" : {
        "Description" : "Example Brand Security Camera"
       ,"Status" : "Deny"
    }
}
```

1.1. Problem Statement

A myriad of IoT devices currently exist on the internet, with more each day. This poses great risks to the local network, as well as to the internet as a whole. By requiring devices to provide specifics around how it is seen on the local network, safeguards can be put in place to restrict those devices to those services (least privilege).

It is the hopes of the authors, that by understanding how a device expects to be used, will lead to the elimination of large scale malware bots targeting IoT devices.

1.2. Background and Terminology

The reader is assumed to be familiar with the basic DHCP terminology defined in [RFC2132] and subsequent RFCs that update them in [RFC3442], [RFC3942], [RFC4361], [RFC4833] and [RFC5494].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when, and only when, they appear in all capitals, as shown here.

2. The "IoT Profile" Object

Fundamental to DWIRM negotiation is the structure of the "IoT Profile" object. It defines how services are to be advertised and managed and is broken into the following strings and sub-objects:

2.1. Description:

The description is a string used to provide a user friendly device description to the user.

2.2. Provide:

The provide object contains one or more category objects, described below, that the device offers to the network.

2.3. Consume:

The consume object contains one or more category objects, described below, that the device connects to, over the network.

2.4. Status:

The status object is used exclusively by the DWIRM server and MUST contain a value of "Accept" or "Deny." This is used to accept or deny the DWIRM client’s request, in full.

2.5. Category:

The category object provides specific requirements for that specific service category. The category key name will be used to inform the local router policy or local network administrator the type of service consumed or provided. This key name will come from a managed DWIRM category registry. Default option values from each category are also provided as part of this registry.

2.5.1. Defined Categories:

This document defines the following baseline categories:

2.5.1.1. Full Access:

This is a special access request for home computing devices, such as smartphones, desktops, laptops and tablets. It is strongly recommended this category be accompanied by a form of DHCP based authentication so it cannot be abused by IoT devices.

2.5.1.2. HTTP:

This defines an HTTP service around the clock on ports 80 and 443.

2.5.2. Category Options:

The options listed in this section must exist or be defaulted to the local network administrator’s settings. It is strongly recommended these defaults are of least-privileged.

2.5.2.1. Endpoints:

The endpoints option provides an array of hostnames, IP-Addresses, and URL’s the device expects to connect to. Based on local router capabilities, it can enforce restrictions based on this option.

2.5.2.2. Hints:

The hints option provides protocol specific details that can be used to identify and restrict activity being conducted over provided ports.

2.5.2.3. PortFwd:

The portfwd option provides a request to the local router that MAY be used to automatically provide a port-forwarding service from the external WAN connection to the internal IP-address assigned to the requesting IoT device.

The format for this field is a list of ranges [a-b] separated by commas [,] for this internal ports of the device; a colon [:]; and a list of ranges [a-b] separated by commas [,] for the external ports on the WAN. Ranges can be a hyphenated range of low port to high port, or a single port, without a hyphen.

The number of ranges and number of usable ports within those ranges on the internal side MUST match the number of ranges and number of usable within those ranges on the external side.

2.5.2.4. Ports:

The ports option provides a list of ranges [a-b] separated by commas [,]. Ranges can be a hyphenated range of low port to high port, or a single port, without a hyphen.

2.5.2.5. Rate:

This option specifies the maximum throughput to be expected by the device for the specified service. Common abbreviations for (k)ilo, (m)ega, and (g)igi, can be used in this option, and are case-insensitive. The value of "Line" may also be used to specify the line-rate of the local router’s network interface.

2.5.2.6. Schedule:

This option specifies when this service is authorized to be active. It consists of two time-fields separated by a hyphen [-]. Each time-field consists of a two digit hour field, in 24-hour format, followed by a colon [:], followed by a two digit minute field. The time-zone for this option defaults to Greenwich Mean Time (GMT), but may be overridden by appending "L" for the local time zone, or a standard three character time-zone abbreviation to the end of this field. The string of "All Day" is also accepted as an alias for "00:00-23:59".

3. DHCP Message Type-53 Types

3.1. DHCPDWIRMCLIENT:

This provides the mechanism for the client to provide the JSON encapsulated "IoT Profile" object.

3.2. DHCPDWIRMSERVER:

This provides the mechanism for the server to respond with the JSON encapsulated "IoT Profile" object.

4. Interactions with other IoT Management Offerings

This does not take into account other IoT management offerings such as Matter or Threads at this time. There are possibilities for collaboration.

5. Known Limitations

There are no known limitations.

6. Security Considerations

There are no known security considerations.

7. Privacy Considerations

There are no known privacy considerations.

8. IANA Considerations

IANA is requested to assign DHCP Message Types for DHCPDWIRMCLIENT and DHCPDWIRMSERVER, as well as a registry for managing categories and default service capabilities.

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <https://www.rfc-editor.org/rfc/rfc2132>.

[RFC3442] Lemon, T., Cheshire, S., and B. Volz, "The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4", RFC 3442, DOI 10.17487/RFC3442, December 2002, <https://www.rfc-editor.org/rfc/rfc3442>.

[RFC3942] Volz, B., "Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options", RFC 3942, DOI 10.17487/RFC3942, November 2004, <https://www.rfc-editor.org/rfc/rfc3942>.

[RFC4361] Lemon, T. and B. Sommerfeld, "Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)", RFC 4361, DOI 10.17487/RFC4361, February 2006, <https://www.rfc-editor.org/rfc/rfc4361>.

[RFC4833] Lear, E. and P. Eggert, "Timezone Options for DHCP", RFC 4833, DOI 10.17487/RFC4833, April 2007, <https://www.rfc-editor.org/rfc/rfc4833>.

[RFC5494] Arkko, J. and C. Pignataro, "IANA Allocation Guidelines for the Address Resolution Protocol (ARP)", RFC 5494, DOI 10.17487/RFC5494, April 2009, <https://www.rfc-editor.org/rfc/rfc5494>.

Authors' Addresses

John Woodworth
Lumen Technologies, Inc.
2355 Dulles Corner Blvd, Ste 200 300
Arlington, VA 22203
United States of America
Email: John.Woodworth@Lumen.com

Dean Ballew
Lumen Technologies, Inc.
2355 Dulles Corner Blvd, Ste 200 300
Herndon, VA 20171
United States of America
Email: Dean.Ballew@Lumen.com

Tim Wicinski
Cox Communications, Inc.
Email: tjw.ietf@gmail.com