             Discovering Provisioning Domain Names and Data
              draft-ietf-intarea-provisioning-domains-01

Abstract

   An increasing number of hosts access the Internet via multiple
   interfaces or, in IPv6 multi-homed networks, via multiple IPv6 prefix
   configurations.

   This document describes a way for hosts to identify such means,
   called Provisioning Domains (PvDs), with Fully Qualified Domain Names
   (FQDN). Those identifiers are advertised in a new Router
   Advertisement (RA) option and, when present, are associated with the
   set of information included within the RA.

   Based on this FQDN, hosts can retrieve additional information about
   their network access characteristics via an HTTP over TLS query.
   This allows applications to select which Provisioning Domains to use
   as well as to provide configuration parameters to the transport layer
   and above.

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 August 13, 2018.

Copyright Notice

Table of Contents

1. Introduction

     It has become very common in modern networks for hosts to access the
     internet through different network interfaces, tunnels, or next-hop
     routers. To describe the set of network configurations associated
     with each access method, the concept of Provisioning Domain (PvD) was
     defined in [RFC7556].

     This document specifies a way to identify PvDs with Fully Qualified
     Domain Names (FQDN), called PvD IDs. Those identifiers are
     advertised in a new Router Advertisement (RA) [RFC4861] option called
     the PvD ID Router Advertisement option which, when present,
     associates the PvD ID with all the information present in the Router
     Advertisement as well as any configuration object, such as addresses,
     deriving from it. The PVD ID Router Advertisement option may also
     contain a set of other RA options. Since such options are only
     considered by hosts implementing this specification, network
     operators may configure hosts that are 'PvD-aware' with PvDs that are
     ignored by other hosts.

     Since PvD IDs are used to identify different ways to access the
     internet, multiple PvDs (with different PvD IDs) could be provisioned
     on a single host interface. Similarly, the same PvD ID could be used
     on different interfaces of a host in order to inform that those PvDs
     ultimately provide identical services.

     This document also introduces a way for hosts to retrieve additional
     information related to a specific PvD by means of an HTTP over TLS
     query using an URI derived from the PvD ID. The retrieved JSON
     object contains additional information that would typically be
     considered unfit, or too large, to be directly included in the Router
     Advertisement, but might be considered useful to the applications, or
     even sometimes users, when choosing which PvD and transport should be
     used.

2. Terminology

     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].

     In addition, this document uses the following terminology:

   Provisioning Domain (PvD):   A set of network configuration
      information; for more information, see [RFC7556].

   PvD ID: A Fully Qualified Domain Name (FQDN) used to identify a
      PvD.

   Explicit PvD: A PvD uniquely identified with a PvD ID. For more
      information, see [RFC7556].

   Implicit PvD: A PvD that, in the absence of a PvD ID, is identified
      by the host interface to which it is attached and the address of
      the advertising router.

3. Provisioning Domain Identification using Router Advertisements

   Explicit PvDs are identified by a PvD ID. The PvD ID is a Fully
   Qualified Domain Name (FQDN) which MUST belong to the network
   operator in order to avoid naming collisions. The same PvD ID MAY be
   used in several access networks when they ultimately provide
   identical services (e.g., in all home networks subscribed to the same
   service).

3.1. PvD ID Option for Router Advertisements

   This document introduces a Router Advertisement (RA) option called
   PvD ID Router Advertisement option. It is used to convey the FQDN
   identifying a given PvD (see Figure 1), bind the PvD ID with
   configuration information received over DHCPv4 (see Section 3.3.2),
   enable the use of HTTP over TLS to retrieve the PvD Additional
   Information JSON object (see Section 4), as well as contain any other
   RA options which would otherwise be valid in the RA.

```
 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      |H|L|A|       Reserved      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Sequence Number            |                         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                          ...
...                            PvD ID FQDN                     ...
...              +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
...              |                 Padding                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                              ...
...            Router Advertisement message header            ...
...              (Only present when A-flag is set)             ...
...                                                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Options ...
+-+-+-+-+-+-+-+-+-+-
```
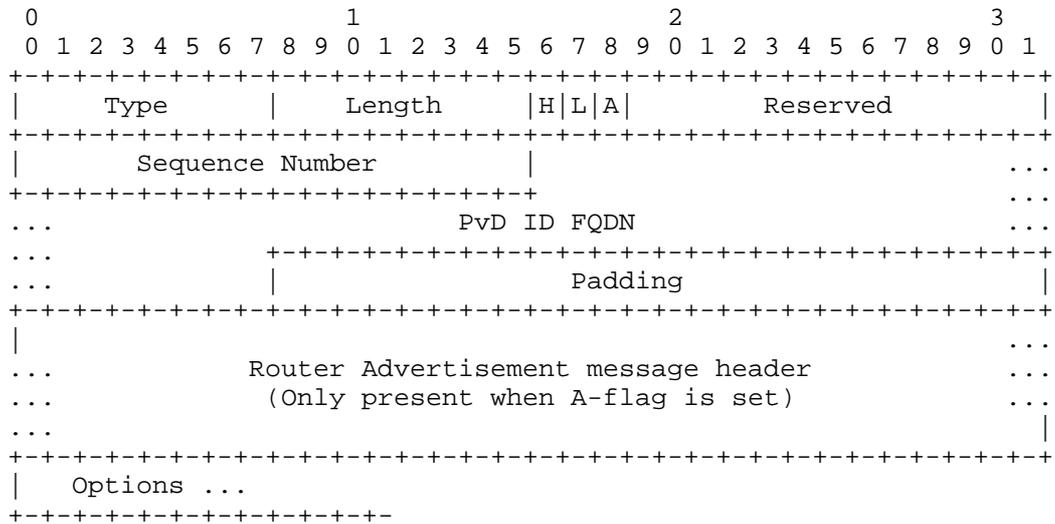
Figure 1: PvD ID Router Advertisements Option format

Type   :   (8 bits) To be defined by IANA. Current
   experimentation uses the value of 254.

Length   :   (8 bits) The length of the option in units of 8
   octets, including the Type and Length fields, the Router
   Advertisement message header, if any, as well as the RA options
   that are included within the PvD ID Option.

H-flag   :   (1 bit) 'HTTP' flag stating whether some PvD
   Additional Information is made available through HTTP over TLS, as
   described in Section 4.

L-flag   :   (1 bit) 'Legacy' flag stating whether the router is
   also providing IPv4 information using DHCPv4 (see Section 3.3.2).

A-flag   :   (1 bit) 'Advertisement' flag stating whether the PvD
   ID Option is followed (right after padding to the next 64 bits
   boundary) by a Router Advertisement message header (See section
   4.2 of target="RFC4861"/>).

Reserved   :   (13 bits) Reserved for later use. It MUST be set to
   zero by the sender and ignored by the receiver.

Sequence Number: (16 bits) Sequence number for the PvD Additional
   Information, as described in Section 4.

   PvD ID FQDN :   The FQDN used as PvD ID encoded in DNS format, as
      described in Section 3.1 of [RFC1035]. Domain names compression
      described in Section 4.1.4 of [RFC1035] MUST NOT be used.

   Padding   :   Zero or more padding octets to the next 8 octets
      boundary. It MUST be set to zero by the sender, and ignored by
      the receiver.

   RA message header :   (16 octets) When the A-flag is set, a full
      Router Advertisement message header as specified in [RFC4861].
      The 'Type', 'Code' and 'Checksum' fields (i.e. the first 32 bits),
      MUST be set to zero by the sender and ignored by the receiver.
      The other fields are to be set and parsed as specified in
      [RFC4861] or any updating documents.

   Options :   Zero or more RA options that would otherwise be valid as
      part of the Router Advertisement main body, but are instead
      included in the PvD ID Option such as to be ignored by hosts that
      are not 'PvD-aware'.

   Here is an example of a PvD ID option with example.org as the PvD ID
   FQDN and including a RDNSS and prefix information options:

```
    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: 254     | Length: 12    |0|0|0|         Reserved        |
   +---------------+-------------------------------+---------------+
   |      Sequence Number          |       7       |       e       |
   +---------------+-------------------------------+---------------+
   |      m        |       a       |       m       |       p       |
   +---------------+-------------------------------+---------------+
   |      l        |       e       |       3       |       o       |
   +---------------+-------------------------------+---------------+
   |      r        |       g       |       0       |   0 (padding) |
   +---------------+---------------+---------------+---------------+
   |  0 (padding)  |  0 (padding)  |  0 (padding)  |  0 (padding)  |
   +---------------+---------------+---------------+---------------+
   |   RDNSS option (RFC 6106) length: 5                        ...
   ...                                                          ...
   ...                                                            |
   +---------------------------------------------------------------+
   | Prefix Information Option (RFC 4861) length: 4             ...
   ...                                                            |
   ...                                                            |
   +---------------------------------------------------------------+
```
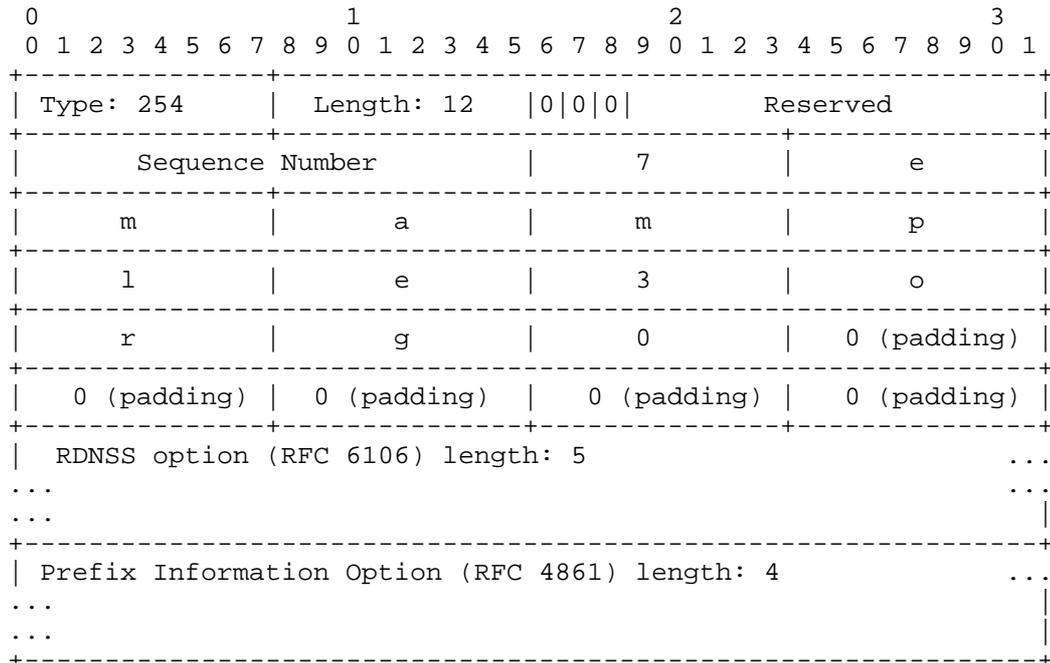
3.2. Router Behavior

   A router MAY send RAs containing at most one PvD ID RA option, but
   MUST NOT include more than one PvD ID RA option in each RA. In
   particular, the PvD ID RA option MUST NOT contain further PvD ID RA
   options.

   The PvD ID Option MAY contain zero, one, or more RA options which
   would otherwise be valid as part of the same RA. Such options are
   processed by PvD-aware hosts, while ignored by others.

   In order to provide multiple different PvDs, a router MUST send
   multiple RAs. Different explicit PvDs MAY be advertised with RAs
   using the same IPv6 source address; but different implicit PvDs,
   advertised with different RAs, MUST use different link local
   addresses.

   Whenever an RA, for a single PvD, would need to be sent via multiple
   packets, the PvD ID RA option header (i.e., all fields except the
   'Options' field) MUST be repeated in all the transmitted RAs. But
   the options within the 'Options' field, MAY be transmitted only once,
   included in one of the transmitted PvD ID RA options.

3.3. Host Behavior

   Hosts MUST associate received RAs and included configuration
   information (e.g., Router Valid Lifetime, Prefix Information
   [RFC4861], Recursive DNS Server [RFC8106], Routing Information
   [RFC4191] options) with the explicit PvD identified by the first PvD
   ID Option present in the received RA, if any, or with the implicit
   PvD identified by the host interface and the source address of the
   received RA otherwise.

   In case multiple PvD ID options are found in a given RA, hosts MUST
   ignore all but the first PvD ID option.

   Similarly, hosts MUST associate all network configuration objects
   (e.g., default routers, addresses, more specific routes, DNS
   Recursive Resolvers) with the PvD associated with the RA which last
   updated the object. For example, addresses that are generated using
   a received Prefix Information option (PIO) are associated with the
   PvD of the last received RA which included the given PIO.

   PvD IDs MUST be compared in a case-insensitive manner (i.e., A=a),
   assuming ASCII with zero parity while non-alphabetic codes must match
   exactly (see also Section 3.1 of [RFC1035]). For example,
   pvd.example.com or PvD.Example.coM would refer to the same PvD.

While resolving names, executing the default address selection
algorithm [RFC6724] or executing the default router selection
algorithm ([RFC2461], [RFC4191] and [RFC8028]), hosts MAY consider
only the configuration associated with an arbitrary set of PvDs.

For example, a host MAY associate a given process with a specific
PvD, or a specific set of PvDs, while associating another process
with another PvD. A PvD-aware application might also be able to
select, on a per-connection basis, which PvDs should be used. In
particular, constrained devices such as small battery operated
devices (e.g. IoT), or devices with limited CPU or memory resources
may purposefully use a single PvD while ignoring some received RAs
containing different PvD IDs.

The way an application expresses its desire to use a given PvD, or a
set of PvDs, or the way this selection is enforced, is out of the
scope of this document. Useful insights about these considerations
can be found in [I-D.kline-mif-mpvd-api-reqs].

3.3.1. DHCPv6 configuration association

When a host retrieves configuration elements using DHCPv6 (e.g.,
addresses or DNS recursive resolvers), they MUST be associated with
the explicit or implicit PvD of the RA received on the same
interface, sent from the same LLA, and with the O-flag or M-flag set
[RFC4861]. If no such PvD is found, or whenever multiple different
PvDs are found, the host behavior is unspecified.

This process requires hosts to keep track of received RAs, associated
PvD IDs, and routers LLA; it also assumes that the router either acts
as a DHCPv6 server or relay and uses the same LLA for DHCPv6 and RA
traffic (which may not be the case when the router uses VRRP to send
its RA).

3.3.2. DHCPv4 configuration association

When a host retrieves configuration elements from DHCPv4, they MUST
be associated with the explicit PvD received on the same interface,
whose PVD ID Options L-flag is set and, in the case of a non point-
to-point link, using the same datalink address. If no such PvD is
found, or whenever multiple different PvDs are found, the
configuration elements coming from DHCPv4 MUST be associated with the
implicit PvD identified by the interface on which the DHCPv4
transaction happened. The case of multiple explicit PvD for an IPv4
interface is undefined.

3.3.3. Interconnection Sharing by the Host

The situation when a node receives an RA on one interface (e.g.
cellular) and shares this connectivity by also acting as a router by
transmitting RA on another interface (e.g. WiFi) is known as
'tethering'. It can be done as ND proxy. The exact behavior is TBD
but it is expected that the one or several PvD associated to the
shared interface (e.g. cellular) will also be advertised to the
clients on the other interface (e.g. WiFi).

4. Provisioning Domain Additional Information

Additional information about the network characteristics can be
retrieved based on the PvD ID. This set of information is called PvD
Additional Information, and is encoded as a JSON object [RFC7159].

The purpose of this additional set of information is to securely
provide additional information to applications about the connectivity
that is provided using a given interface and source address pair. It
typically includes data that would be considered too large, or not
critical enough, to be provided within an RA option. The information
contained in this object MAY be used by the operating system, network
libraries, applications, or users, in order to decide which set of
PvDs should be used for which connection, as described in
Section 3.3.

4.1. Retrieving the PvD Additional Information

When the H-flag of the PvD ID Option is set, hosts MAY attempt to
retrieve the PvD Additional Information associated with a given PvD
by performing an HTTP over TLS [RFC2818] GET query to https://<PvD-
ID>/.well-known/pvd [RFC5785]. Inversely, hosts MUST NOT do so
whenever the H-flag is not set.

Note that the DNS name resolution of the PvD ID, the PKI checks as
well as the actual query MUST be performed using the considered PvD.
In other words, the name resolution, PKI checks, source address
selection, as well as the next-hop router selection MUST be performed
while using exclusively the set of configuration information attached
with the PvD, as defined in Section 3.3. In some cases, it may
therefore be necessary to wait for an address to be available for use
(e.g., once the Duplicate Address Detection or DHCPv6 processes are
complete) before initiating the HTTP over TLS query. If the PvD
allows for temporary address per [RFC4941], then hosts SHOULD use a
temporary address to fetch the PvD Additional Information and SHOULD
deprecate the used temporary address and generate a new temporary
address afterward.

If the HTTP status of the answer is greater than or equal to 400 the
host MUST abandon and consider that there is no additional PvD
information. If the HTTP status of the answer is between 300 and
399, inclusive, it MUST follow the redirection(s). If the HTTP
status of the answer is between 200 and 299, inclusive, the host MAY
get a file containing a single JSON object. When a JSON object could
not be retrieved, an error message SHOULD be logged and/or displayed
in a rate-limited fashion.

After retrieval of the PvD Additional Information, hosts MUST keep
track of the Sequence Number value received in subsequent RAs
including the same PvD ID. In case the new value is greater than the
value that was observed when the PvD Additional Information object
was retrieved (using serial number arithmetic comparisons [RFC1982]),
or whenever the validity time included in the PVD Additional
Information JSON object is expired, hosts MUST either perform a new
query and retrieve a new version of the object, or, failing that,
deprecate the object and stop using the additional information
provided in the JSON object.

Hosts retrieving a new PvD Additional Information object MUST check
for the presence and validity of the mandatory fields specified in
Section 4.3. A retrieved object including an expiration time that is
already past or missing a mandatory element MUST be ignored. In
order to avoid synchronized queries toward the server hosting the PvD
Additional Information when an object expires, a host which last
retrieved an object at a time A, including a validity time B, SHOULD
renew the object at a uniformly random time in the interval
[(B-A)/2,A].

The PvD Additional Information object includes a set of IPv6 prefixes
(under the key "prefixes") which MUST be checked against all the
Prefix Information Options advertised in the RA. If any of the
prefixes included in the PIO is not covered by at least one of the
listed prefixes, the PvD associated with the tested prefix MUST be
considered unsafe and MUST NOT be used. While this does not prevent
a malicious network provider, it does complicate some attack
scenarios, and may help detecting misconfiguration.

4.2. Operational Consideration to Providing the PvD Additional
      Information

Whenever the H-flag is set in the PvD RA Option, a valid PvD
Additional Information object MUST be made available to all hosts
receiving the RA by the network operator. In particular, when a
captive portal is present, hosts MUST still be allowed to perform
DNS, PKI and HTTP over TLS operations related to the retrieval of the
object, even before logging into the captive portal.

Routers MAY increment the PVD ID Sequence number in order to inform host that a new PvD Additional Information object is available and should be retrieved.

The server providing the JSON files SHOULD also check whether the client address is part of the prefixes listed into the additional information and SHOULD return a 403 response code if there is no match.

4.3. PvD Additional Information Format

The PvD Additional Information is a JSON object.

The following table presents the mandatory keys which MUST be included in the object:

JSON key	Description	Type	Example
name	Human-readable service name	UTF-8 string [RFC3629]	"Awesome Wifi"
expires	Date after which this object is not valid	[RFC3339]	"2017-07-23T06:00:00Z"
prefixes	Array of IPv6 prefixes valid for this PVD	Array of strings	["2001:db8:1::/48", "2001:db8:4::/48"]

A retrieved object which does not include a valid string associated with the "name" key at the root of the object, or a valid date associated with the "expires" key, also at the root of the object, MUST be ignored. In such cases, an error message SHOULD be logged and/or displayed in a rate-limited fashion. If the PIO of the received RA is not covered by at least one of the "prefixes" key, the retrieved object SHOULD be ignored.

The following table presents some optional keys which MAY be included in the object.

```
+---------------+----------------+---------+---------------------+
| JSON key      | Description    | Type    | Example             |
+---------------+----------------+---------+---------------------+
| localizedName | Localized user-| UTF-8   | "Wifi Genial"       |
|               | visible service| string  |                     |
|               | name, language |         |                     |
|               | can be selected|         |                     |
|               | based on the   |         |                     |
|               | HTTP Accept-   |         |                     |
|               | Language header|         |                     |
|               | in the request.|         |                     |
| dnsZones      | DNS zones      | array   | ["example.com","sub.e|
|               | searchable and | of DNS  | xample.org"]        |
|               | accessible     | zones   |                     |
| noInternet    | No Internet,   | boolean | true                |
|               | set when the   |         |                     |
|               | PvD only       |         |                     |
|               | provides       |         |                     |
|               | restricted     |         |                     |
|               | access to a set|         |                     |
|               | of services    |         |                     |
+---------------+----------------+---------+---------------------+
```

It is worth noting that the JSON format allows for extensions.
Whenever an unknown key is encountered, it MUST be ignored along with
its associated elements.

4.3.1. Private Extensions

   JSON keys starting with "x-" are reserved for private use and can be
   utilized to provide information that is specific to vendor, user or
   enterprise. It is RECOMMENDED to use one of the patterns "x-FQDN-
   KEY" or "x-PEN-KEY" where FQDN is a fully qualified domain name or
   PEN is a private enterprise number [PEN] under control of the author
   of the extension to avoid collisions.

4.3.2. Example

   Here are two examples based on the keys defined in this section.

```
   {
     "name": "Foo Wireless",
     "localizedName": "Foo-France Wifi",
     "expires": "2017-07-23T06:00:00Z",
     "prefixes" : ["2001:db8:1::/48", "2001:db8:4::/48"],
   }
```

```
    {
      "name": "Bar 4G",
      "localizedName": "Bar US 4G",
      "expires": "2017-07-23T06:00:00Z",
      "prefixes": ["2001:db8:1::/48", "2001:db8:4::/48"],
    }
```

4.4. Detecting misconfiguration and misuse

   When a host retrieves the PvD Additional Information, it MUST verify
   that the TLS server certificate is valid for the performed request
   (e.g., that the Subject Name is equal to the PvD ID expressed as an
   FQDN). This authentication creates a secure binding between the
   information provided by the trusted Router Advertisement, and the
   HTTPS server. But this does not mean the Advertising Router and the
   PvD server belong to the same entity.

   Hosts MUST verify that all prefixes in the RA PIO are covered by a
   prefix from the PvD Additional Information. An adversarial router
   willing to fake the use of a given explicit PvD, without any access
   to the actual PvD Additional Information, would need to perform NAT66
   in order to circumvent this check.

   It is also RECOMMENDED that the HTTPS server checks the source
   addresses of incoming connections (see Section 4.1). This check give
   reasonable assurance that neither NPTv6 [RFC6296] nor NAT66 were used
   and restricts the information to the valid network users.

5. Operation Considerations

   This section describes some use cases of PvD. For sake of
   simplicity, the RA messages will not be described in the usual ASCII
   art but rather in an indented list. For example, a RA message
   containing some options and a PvD ID option that also contains other
   options will be described as:

   o RA Header: router lifetime = 6000

   o Prefix Information Option: length = 4, prefix = 2001:db8:cafe::/64

   o PvD ID header: length = 3+ 5 +4 , PvD ID FQDN = example.org,
      A-flag = 0 (actual length of the header with padding 24 bytes = 3
      * 8 bytes)

      * Recursive DNS Server: length = 5, addresses=
         [2001:db8:cafe::53, 2001:db8:f00d::53]

      * Prefix Information Option: length = 4, prefix =
         2001:db8:f00d::/64

   It is expected that for some years, networks will have a mix of PvD-
   aware hosts and PvD-ignorant hosts. If there is a need to give
   specific information to PvD-aware hosts only, then it is recommended
   to send TWO RA messages: one for each class of hosts. For example,
   here is the RA for PvD-ignorant hosts:

   o RA Header: router lifetime = 6000 (PvD-ignorant hosts will use
      this router as a default router)

   o Prefix Information Option: length = 4, prefix = 2001:db8:cafe::/64

   o Recursive DNS Server Option: length = 3, addresses=
      [2001:db8:cafe::53]

   o PvD ID header: length = 3+ 2, PvD ID FQDN = foo.example.org,
      A-flag = 1 (actual length of the header 24 bytes = 3 * 8 bytes)

      * RA Header: router lifetime = 0 (PvD-aware hosts will not use
         this router as a default router), implicit length = 2

   And here is a RA example for PvD-aware hosts:

   o RA Header: router lifetime = 0 (PvD-ignorant hosts will not use
      this router as a default router)

   o PvD ID header: length = 3+ 2 + 4 + 3, PvD ID FQDN = example.org,
      A-flag = 1 (actual length of the header 24 bytes = 3 * 8 bytes)

      * RA Header: router lifetime = 1600 (PvD-aware hosts will use
         this router as a default router), implicit length = 2

      * Prefix Information Option: length = 4, prefix =
         2001:db8:f00d::/64

      * Recursive DNS Server Option: length = 3, addresses=
         [2001:db8:f00d::53]

   In the above example, PvD-ignorant hosts will only use the first RA
   sent from their default router and using the 2001:db8:cafe::/64
   prefix. PvD-aware hosts will autonomously configure addresses from
   both PIOs, but will only use the source address in 2001:db8:f00d::/64
   to communicate past the first hop router since only the router
   sending the second RA will be used as default router; similarly, they
   will use the DNS server 2001:db8:f00d::53 when communicating with
   this adress.

6. Security Considerations

   Although some solutions such as IPsec or SeND [RFC3971] can be used
   in order to secure the IPv6 Neighbor Discovery Protocol, actual
   deployments largely rely on link layer or physical layer security
   mechanisms (e.g. 802.1x [IEEE8021X]) in conjunction with RA Guard
   [RFC6105].

   This specification does not improve the Neighbor Discovery Protocol
   security model, but extends the purely link-local trust relationship
   between the host and the default routers with HTTP over TLS
   communications which servers are authenticated as rightful owners of
   the FQDN received within the trusted PvD ID RA option.

   It must be noted that Section 4.4 of this document only provides
   reasonable assurance against misconfiguration but does not prevent an
   hostile network access provider to wrong information that could lead
   applications or hosts to select an hostile PvD. Users should always
   apply caution when connecting to an unknown network.

7. Privacy Considerations

   Retrieval of the PvD Additional Information over HTTPS requires early
   communications between the connecting host and a server which may be
   located further than the first hop router. Although this server is
   likely to be located within the same administrative domain as the
   default router, this property can't be ensured. Therefore, hosts
   willing to retrieve the PvD Additional Information before using it
   without leaking identity information, SHOULD make use of an IPv6
   Privacy Address and SHOULD NOT include any privacy sensitive data,
   such as User Agent header or HTTP cookie, while performing the HTTP
   over TLS query.

   From a privacy perspective, retrieving the PvD Additional Information
   is not different from establishing a first connexion to a remote
   server, or even performing a single DNS lookup. For example, most
   operating systems already perform early queries to well known web
   sites, such as http://captive.example.com/hotspot-detect.html, in
   order to detect the presence of a captive portal.

   There may be some cases where hosts, for privacy reasons, should
   refrain from accessing servers that are located outside a certain
   network boundary. In practice, this could be implemented as a
   whitelist of 'trusted' FQDNs and/or IP prefixes that the host is
   allowed to communicate with. In such scenarios, the host SHOULD
   check that the provided PvD ID, as well as the IP address that it
   resolves into, are part of the allowed whitelist.

8. IANA Considerations

   IANA is asked to assign the value TBD from the IPv6 Neighbor
   Discovery Option Formats registry for the PvD ID Router Advertisement
   option.

   IANA is asked to assign the value "pvd" from the Well-Known URIs
   registry.

   IANA is asked to create and maintain a new registry entitled
   "Additional Information PvD Keys" containing ASCII strings. The
   initial content of this registry are given in Section 4.3; future
   assignments are to be made through Expert Review [BCP36].

   Finally, IANA is asked to create and maintain a new registry entitled
   "PvD ID Router Advertisement option Flags" reserving bit positions
   from 0 to 15 to be used in the PvD ID Router Advertisement option
   bitmask. Bit position 0, 1 and 2 are reserved by this document (as
   specified in Figure 1). Future assignments require a Standard Track
   RFC document.

9. Acknowledgements

   Many thanks to M. Stenberg and S. Barth for their earlier work:
   [I-D.stenberg-mif-mpvd-dns], as well as to Basile Bruneau who was
   author of an early version of this document.

   Thanks also to Marcus Keane, Mikael Abrahamson, Ray Bellis, Lorenzo
   Colitti, Bob Hinden, Tatuya Jinmei, Erik Kline, Ted Lemon, Jen
   Lenkova, Mark Townsley and James Woodyatt for useful and interesting
   discussions.

   Finally, special thanks to Thierry Danis and Wenqin Shao for their
   valuable inputs and implementation efforts ([github]), Tom Jones for
   his integration effort into the NEAT project and Rigil Salim for his
   implementation work.

10. References

10.1. Normative references

   [RFC1035] Mockapetris, P., "Domain names - implementation and
              specification", STD 13, RFC 1035, DOI 10.17487/RFC1035,
              November 1987, <https://www.rfc-editor.org/info/rfc1035>.

   [RFC1982] Elz, R. and R. Bush, "Serial Number Arithmetic", RFC 1982,
              DOI 10.17487/RFC1982, August 1996,
              <https://www.rfc-editor.org/info/rfc1982>.

   [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/info/rfc2119>.

   [RFC2461]   Narten, T., Nordmark, E., and W. Simpson, "Neighbor
               Discovery for IP Version 6 (IPv6)", RFC 2461,
               DOI 10.17487/RFC2461, December 1998,
               <https://www.rfc-editor.org/info/rfc2461>.

   [RFC2818]   Rescorla, E., "HTTP Over TLS", RFC 2818,
               DOI 10.17487/RFC2818, May 2000,
               <https://www.rfc-editor.org/info/rfc2818>.

   [RFC3629]   Yergeau, F., "UTF-8, a transformation format of ISO
               10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November
               2003, <https://www.rfc-editor.org/info/rfc3629>.

   [RFC4861]   Narten, T., Nordmark, E., Simpson, W., and H. Soliman,
               "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,
               DOI 10.17487/RFC4861, September 2007,
               <https://www.rfc-editor.org/info/rfc4861>.

   [RFC7159]   Bray, T., Ed., "The JavaScript Object Notation (JSON) Data
               Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March
               2014, <https://www.rfc-editor.org/info/rfc7159>.

   [RFC8126]   Cotton, M., Leiba, B., and T. Narten, "Guidelines for
               Writing an IANA Considerations Section in RFCs", BCP 26,
               RFC 8126, DOI 10.17487/RFC8126, June 2017,
               <https://www.rfc-editor.org/info/rfc8126>.

10.2. Informative references

   [github]   Cisco, "IPv6-mPvD github repository",
               <https://github.com/IPv6-mPvD>.

   [I-D.kline-mif-mpvd-api-reqs]
               Kline, E., "Multiple Provisioning Domains API
               Requirements", draft-kline-mif-mpvd-api-reqs-00 (work in
               progress), November 2015.

   [I-D.stenberg-mif-mpvd-dns]
               Stenberg, M. and S. Barth, "Multiple Provisioning Domains
               using Domain Name System", draft-stenberg-mif-mpvd-dns-00
               (work in progress), October 2015.

   [IEEE8021X]
              IEEE, "IEEE Standards for Local and Metropolitan Area
              Networks: Port based Network Access Control, IEEE Std".

   [PEN]   IANA, "Private Enterprise Numbers",
              <https://www.iana.org/assignments/enterprise-numbers>.

   [RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet:
              Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002,
              <https://www.rfc-editor.org/info/rfc3339>.

   [RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander,
              "SEcure Neighbor Discovery (SEND)", RFC 3971,
              DOI 10.17487/RFC3971, March 2005,
              <https://www.rfc-editor.org/info/rfc3971>.

   [RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and
              More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191,
              November 2005, <https://www.rfc-editor.org/info/rfc4191>.

   [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy
              Extensions for Stateless Address Autoconfiguration in
              IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007,
              <https://www.rfc-editor.org/info/rfc4941>.

   [RFC5785] Nottingham, M. and E. Hammer-Lahav, "Defining Well-Known
              Uniform Resource Identifiers (URIs)", RFC 5785,
              DOI 10.17487/RFC5785, April 2010,
              <https://www.rfc-editor.org/info/rfc5785>.

   [RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J.
              Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105,
              DOI 10.17487/RFC6105, February 2011,
              <https://www.rfc-editor.org/info/rfc6105>.

   [RFC6296] Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix
              Translation", RFC 6296, DOI 10.17487/RFC6296, June 2011,
              <https://www.rfc-editor.org/info/rfc6296>.

   [RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown,
              "Default Address Selection for Internet Protocol Version 6
              (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012,
              <https://www.rfc-editor.org/info/rfc6724>.

   [RFC7556] Anipko, D., Ed., "Multiple Provisioning Domain
              Architecture", RFC 7556, DOI 10.17487/RFC7556, June 2015,
              <https://www.rfc-editor.org/info/rfc7556>.

   [RFC8028]   Baker, F. and B. Carpenter, "First-Hop Router Selection by
               Hosts in a Multi-Prefix Network", RFC 8028,
               DOI 10.17487/RFC8028, November 2016,
               <https://www.rfc-editor.org/info/rfc8028>.

   [RFC8106]   Jeong, J., Park, S., Beloeil, L., and S. Madanapalli,
               "IPv6 Router Advertisement Options for DNS Configuration",
               RFC 8106, DOI 10.17487/RFC8106, March 2017,
               <https://www.rfc-editor.org/info/rfc8106>.

Appendix A. Changelog

   Note to RFC Editors: Remove this section before publication.

A.1. Version 00

   Initial version of the draft. Edited by Basile Bruneau + Eric Vyncke
   and based on Basile's work.

A.2. Version 01

   Major rewrite intended to focus on the the retained solution based on
   corridors, online, and WG discussions. Edited by Pierre Pfister.
   The following list only includes major changes.

      PvD ID is an FQDN retrieved using a single RA option. This option
      contains a sequence number for push-based updates, a new H-flag,
      and a L-flag in order to link the PvD with the IPv4 DHCP server.

      A lifetime is included in the PvD ID option.

      Detailed Hosts and Routers specifications.

      Additional Information is retrieved using HTTP-over-TLS when the
      PvD ID Option H-flag is set. Retrieving the object is optional.

      The PvD Additional Information object includes a validity date.

      DNS-based approach is removed as well as the DNS-based encoding of
      the PvD Additional Information.

      Major cut in the list of proposed JSON keys. This document may be
      extended later if need be.

      Monetary discussion is moved to the appendix.

      Clarification about the 'prefixes' contained in the additional
      information.

Clarification about the processing of DHCPv6.

A.3. Version 02

The FQDN is now encoded with ASCII format (instead of DNS binary) in the RA option.

The PvD ID option lifetime is removed from the object.

Use well known URI "https://<PvD-ID>/.well-known/pvd"

Reference RFC3339 for JSON timestamp format.

The PvD ID Sequence field has been extended to 16 bits.

Modified host behavior for DHCPv4 and DHCPv6.

Removed IKEv2 section.

Removed mention of RFC7710 Captive Portal option. A new I.D. will be proposed to address the captive portal use case.

A.4. WG Document version 00

Document has been accepted as INTAREA working group document

IANA considerations follow RFC8126 [RFC8126]

PvD ID FQDN is encoded as per RFC 1035 [RFC1035]

PvD ID FQDN is prepended by a one-byte length field

Marcus Keane added as co-author

dnsZones key is added back

draft of a privacy consideration section and added that a temporary address should be used to retrieve the PvD additional information

per Bob Hinden's request: the document is now aiming at standard track and security considerations have been moved to the main section

A.5. WG Document version 01

     Removing references to 'metered' and 'characteristics' keys.
     Those may be in scope of the PvD work, but this document will
     focus on essential parts only.

     Removing appendix section regarding link quality and billing
     information.

     The PvD RA Option may now contain other RA options such that PvD-
     aware hosts may receive configuration information otherwise
     invisible to non-PvD-aware hosts.

     Clarify that the additional PvD Additional Information is not
     intended to modify host's networking stack behavior, but rather
     provide information to the Application, used to select which PvDs
     must be used and provide configuration parameters to the transport
     layer.

     The RA option padding is used to increase the option size to the
     next 64 (was 32) bits boundary.

     Better detail the Security model and Privacy considerations.

Authors' Addresses

   Pierre Pfister
   Cisco
   11 Rue Camille Desmoulins
   Issy-les-Moulineaux 92130
   France

   Email: ppfister@cisco.com

   Eric Vyncke (editor)
   Cisco
   De Kleetlaan, 6
   Diegem 1831
   Belgium

   Email: evyncke@cisco.com

   Tommy Pauly
   Apple

   Email: tpauly@apple.com

David Schinazi
Apple

Email: dschinazi@apple.com