UPnP Device Architecture V1.1
Annex A – IP Version 6 Support

THE UPNP FORUM TAKES NO POSITION AS TO WHETHER ANY INTELLECTUAL PROPERTY RIGHTS EXIST IN THE STANDARDIZED DCPS AND DCP FRAMEWORKS. THE STANDARDIZED DCPS AND DCP FRAMEWORKS ARE PROVIDED "AS IS" AND "WITH ALL FAULTS". THE UPNP FORUM MAKES NO WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE STANDARDIZED DCPS AND ANNEXES, INCLUDING BUT NOT LIMITED TO ALL IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OF REASONABLE CARE OR WORKMANLIKE EFFORT, OR RESULTS OR OF LACK OF NEGLIGENCE.

Authors *	Company
Mark Baugher	Cisco
Cathy Chan	Nokia
Barbara Stark	AT&T
Mika Saaranen	Nokia
Tony Hain	Cisco

* The UPnP Forum in no way guarantees the accuracy or completeness of this author list and in no way implies any rights for or support from those members listed. This list is not the specifications' contributor list that is kept on the UPnP Forum's website.

IPv6 Update to UDA v1.1

This revision to the UPnP Device Architecture Annex A is motivated by changes made to the IPv6 standard in the address types used by an IPv6 node for its various addresses. The IETF deprecated site-local Unicast [RFC3879] and replaced it with Unique Local Addressing [RFC4193]. The current UDA 1.1 Annex A was published between the deprecation of Site-Local Unicast and the publication of its ULA replacement. As a result, UDA 1.1 Annex A uses the term “global address”, which is now ambiguous since both ULA and GUA are defined to be globally scoped. This revision updates Annex A for ULA.

This revision also restricts the use of a Global Unicast Address in site-local multicast by assigning it a lower preference than ULA for use in an SSDP LOCATION URL. A GUA is prefered only when a ULA is not available, i.e. when ULA prefix is not provided in an IPv6 gateway Router Advertisement [RFC4861] or from DHCPv6 [RFC3315]. Furthermore, this revision deprecates the use of global multicast, which UDA 1.1 Annex A permits for SSDP NOTIFY and M-SEARCH messages. Only link-scope and site-scope multicast are permitted by this revision.

These changes ensure that UPnP unicast messages can be routed on all networks that a site-local multicast SSDP message can reach. Site-routing is achieved with or without a ULA prefix; a ULA is only preferred over a GUA. A GUA may be used when no ULA is available. This approach avoids dependency on global routing for site routing and is consistent with UPnP architecture and practice, which does not assume a global address or operation across the Internet or even that a router is present. For example, UPnP Remote Access defines global operation through a “remote access server” that filters and manages UPnP messaging over a wide-area network connection. Use of this globally-routable service is a specially-defined extension to UPnP.

Preference of a ULA prefix is an architectural choice. No doubt, the vast majority of dual-stack UPnP deployments will have a global prefix available on the home network, even during times that the home network loses its Internet connection. Nonetheless, this update to Annex A chooses to also support routed UPnP networks that are never connected to the Internet such as a home security system that does not use globally-routable addresses or that is not even connected to the IPv6 Internet.

Thus, this revision enables UPnP for routed home networks when there are interfaces that cannot be bridged[1] in a single router or when there are multiple routers on the home network. These are two advantages of IPv6 over IPv4 : IPv6 better accomodates future applications that require plug-and-play setup, and it solves current problems that IPv4 systems have with multiple routers hosting multiple RFC 1918 [BCP0005] networks (a double NAT). With this revision to UDA Annex A, UPnP dual-stack devices can reap these and other benefits by running IPv6 and IPv4 in a “dual stack” configuration.

[1] IEEE 802.14.5 supports home automation protocols that run over low-powered networks, such as a security or energy-monitoring sensor network. The fact that 802.14.5 uses a 64-bit address means that it cannot be bridged to Wi-Fi, Ethernet, MoCA, or other LANs. The solution for interconnecting the networks is to enable routing across the router. In cases where there are multiple routers in the home or private network, routing is also needed. This revision to Annex A accommodates routed private networks with site-routing without resorting to globally-routable addresses.

Annex A. IP Version 6 Support

[Normative]

A.1 Introduction

Most of today's Internet uses IPv4, which was first standardized in 1981. IPv4 has been remarkably resilient in spite of its age, but it is beginning to have problems. Most importantly, there is a growing shortage of IPv4 addresses, which are needed by all new machines added to the Internet. Deployment of large numbers of UPnP devices will only exacerbate the shortage.

IPv6 fixes a number of problems in IPv4, such as the limited number of available IPv4 addresses. It also adds many improvements to IPv4 in areas such as routing and network auto configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years during a transition period.

This Annex describes mechanisms by which devices and control points based on the UPnP Device Architecture MAY be used on IPv6 networks.

A.2 General Principles

Devices and control points MUST implement IPv4 and support IPv4-only operation, and SHOULD implement IPv6 and support dual stack (IPv4 and IPv6) operation. Vendors MAY choose to allow IPv6-only operation as a policy alternative, but a device and a control point MUST run IPv4 in order to be certified. All IPv6 devices and control points that implement both stacks are therefore inherently multi-homed.

An IPv6 device or control point MAY also have multiple IPv6 addresses based on the scoping definitions for the IPv6 address space. The basic principle is that the unicast addresses advertised by a device MUST be consistent with scope used for that multicast advertisement message. The scoping rules are arranged based on the degree of ”routeability” provided by a particular scope. The three scopes currently operational are:

- Link Scope (the stations reachable without routing) which uses addresses called Link Local Addresses.
- Site scope (a private network consisting of one or more links bounded by a site’s edge) which uses addresses called Unique Local Addresses (ULA). Strictly speaking, unicast ULA messages are “site-routable” but globally scoped. Inclusive of all local links contained at the site. This document assumes that site-local multicast routing and ULA routing will be identical on a site.
- Global scope (the Internet) which uses addresses called Globally Unique Addresses (GUA). Inclusive of Site Scope.

See RFC 4291 Section 2.7 for multicast scope definitions.

Since a UPnP device uses multicast for advertisements and multicast eventing, and there is a corresponding scope defined for multicast, the rules set forth below define the selection of unicast addresses in the context of the multicast scope used for multicast messages. In addition, a UPnP device MUST adhere to all multi-homed behaviors described in this document.

The following requirements apply to devices and control points using the UPnP Device Architecture over IPv6. This is an overview of the process. Implementers MUST refer to the cited references for details.

- Devices and control points MUST include only the link local unicast address in all multicast messages that are multicast to the link scope FF02::C for SSDP and FF02::130 for multicast eventing. These addresses are assigned to UPnP by the Internet Assigned Numbers Authority [IANA]. Ports are assigned by UPnP; see “Advertisements” and “Eventing” sections below. Devices and control points MUST listen on link scope. See RFC 4862 for details of link local addressing.

- Devices and control points MUST implement SLAAC (RFC 4862) for address assignment on each IPv6-enabled interface. They MAY implement DHCPv6 with the IA-NA option (RFC 3315) for address assignment. Once the address assignment process is complete, the device or control point will have exactly one link local address available (unless Duplicate Address Detection failed) and zero, one, or more ULA and/or GUA addresses available for use, on an IPv6-enabled interface.

- If a ULA is available, devices and control points MUST use an acquired ULA in all multicast messages that are multicast to the site scope FF05::C or FF05::130. If there is no ULA, but there is at least one GUA, then the device or control point MUST use one of its GUA addresses in all multicast messages that are multicast to the site scope FF05::C or FF05::130.

- Devices and control points MUST NOT send multicast messages on Global Scope.

- A device MUST listen for unicast SSDP traffic on all scopes on which it has advertised, for each UPnP-enabled interface. Control points MUST listen for unicast SSDP traffic in order to identify and control devices.

- The hop limit of each IP packet for a site-scope multicast message MUST be configurable and MUST default to 5.

- Devices and control points MAY select the IPv6 interface or interfaces (see Section I above on the defintion of a UPnP interface) over which UPnP is enabled. If a device or control point runs UPnP on an IPv6 interface, it MUST follow the rules stated above on each interface.

- Devices MUST use the selection rules described in RFC 3484 for the LOCATION URL value in an SSDP message or for the source address in a multicast message that is multicast on the site scope.

Summary of Address Usage

	Link	Site	Global	Link	Site	global
Device Address	Multicast On			Unicast address used as source address[2]		
Link (link local)	Y		Never	Y		
Site (ULA)		Y	Never		Y	
Global (GUA)		Y	Never			Y

A.2.1 Device operation

A device supporting both IPv4 and IPv6 simultaneously MUST be advertised using the same Unique Service Name (USN) on both IPv4 and IPv6 and MUST have identical device description documents and service description documents when accessed from both protocols. The device must also conform to other multi-homed descriptions in the respective sections of the document.

A.2.2 Control point operation

Control points can use the matching USNs of IPv4 and IPv6 announcements of dual stack IPv4/IPv6 devices to treat dual-stack devices as a single device. For example, a control point MAY subscribe to events on IPv6 and invoke actions on IPv4 based on the state information received on the IPv6 interface. In addition, the control point must also conform to other multi-homed descriptions in the respective sections of this document.

A.3 Addressing

RFC 4862, RFC 4193 and RFC 3315 describe how a physical device obtains an IPv6 address.

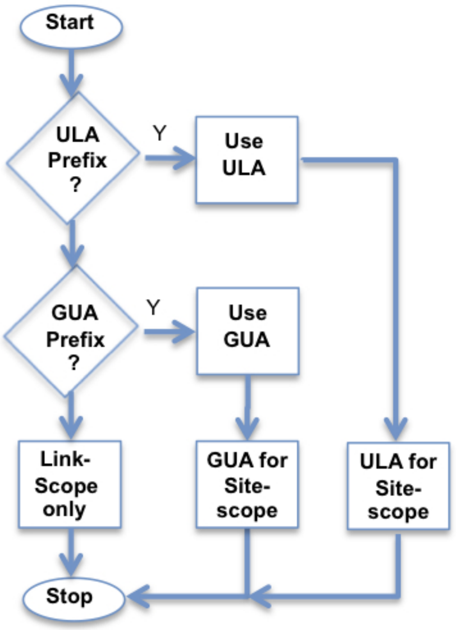
IPv6 multicast addresses include a component (scope) which determines the propagation of a message. The multicast scope for UPnP MUST be link local or site scope. Further, since the multicast addresses used are permanently assigned, the scope is encompassing. That is, link local scope is contained in site scope.

In IPv6 networks, a link local IP address is assigned per interface by the physical device, and therefore UPnP devices or control points on IPv6-enabled devices will always have a link local address. In addition, a device or control point MAY or MAY NOT have a Unique Local Address (ULA) or a Global Unicast Address available to it. IPv6 devices or control points are "multi-homed" when they run UPnP on one or more IPv6 addresses for an interface: a link local address for local link traffic is always available, a globally routable address is usually available, and a site-routable address, using a ULA, is available when the router advertises a ULA prefix. In some scenarios, devices or control points MAY only have a link-local address available to them; reasons for this include underlying device capability, administrative policy, and availability of ULA and global prefixes. Link-local addresses are generated by the physical device itself, without referring to an outside router or server such as a DHCPv6 server.

[2] This is the unicast address used by the device or control point in its multicast messages, i.e. the source IP address in the multicast messages, as well as the LOCATION URL for advertisement messages sent by devices.

Thus, there are two considerations for UPnP IPv6 addressing. The first is availability: If the gateway/router does not advertise a GUA or ULA prefix, then UPnP IPv6 addressing is strictly link-local addressing. The second is policy: This Annex recommends that ULA be preferred over GUA in address selection, as illustrated in the following flowchart.

- Address Selection of the unicast IPv6 address in SSDP
  - Link-scope SSDP multicast selects a link-local unicast address
  - Site-scope SSDP multicast selects a ULA or GUA
- Device prefers a ULA *if its IPv6 node has a ULA prefix*
  - *If not, it prefers to use a globally-routable unicast address, a GUA*
  - *If Device has no global address then it sends only to link scope*
- The Device always sends link-scope SSDP
- The Device optionally sends to site scope
  - If policy allows site-scope SSDP
  - If IPv6 node has a ULA or GUA
- CPs must listen on link and site scope



In addition to the address(es) assigned by the address selection process shown above, each device or control point, acting as a normal IPv6 node, listens for traffic on several multicast addresses: link-local scope all-nodes multicast address `FF02::1`; the site scope all-nodes multicast address `FF05::1` and multicast addresses of joined groups on each interface.

A.3.1 UPnP Messaging on IPv6 Interfaces

At a minimum, a UPnP Device and a Control Point MUST both listen and send on IPv6 link-local scope multicast and unicast addresses. A UPnP device MUST send announcements and multicast eventing messages to, and listen for search requests on the assigned-to-UPnP link-local scope multicast addresses and receive connections on a link-local unicast address that it has advertised. A UPnP Control Point MUST listen for announcements and multicast eventing messages on the assigned-to-UPnP link-local scope multicast addresses and be capable of requesting service definition using a link-local unicast address.

Additionally, a UPnP Device and Control Point MUST be capable of both listening and sending on site-scope multicast and site-routable (ULA or GUA) addresses. Whether or not a particular Device or Control Point uses site-scope is a policy decision. In order to accommodate routed home networks, this specification REQUIRES site-scope capability in UPnP Devices and Controls Points, but its use is OPTIONAL.

Not all private-network gateway devices that support dual-stack will necessarily support ULA prefix delegation. When there is no ULA available, but there is a GUA available from the underlying device, the UPnP Device MUST use a GUA in its site-scope multicast messages, and a UPnP Control Point SHOULD use that GUA in communicating with a Device that is off-link but on a routed home network. This assumes conformance to RFC 3484 and a policy in which a ULA is preferred by a UPnP Device over a GUA for source-address selection, e.g. the address used in a LOCATION URL sent in a NOTIFY message.

A.3.2 Summary of boot/startup process

- For IPv4, Auto-IP addressing is performed as specified in section 0 “Addressing” in the main document (UDA 1.1). of this document.

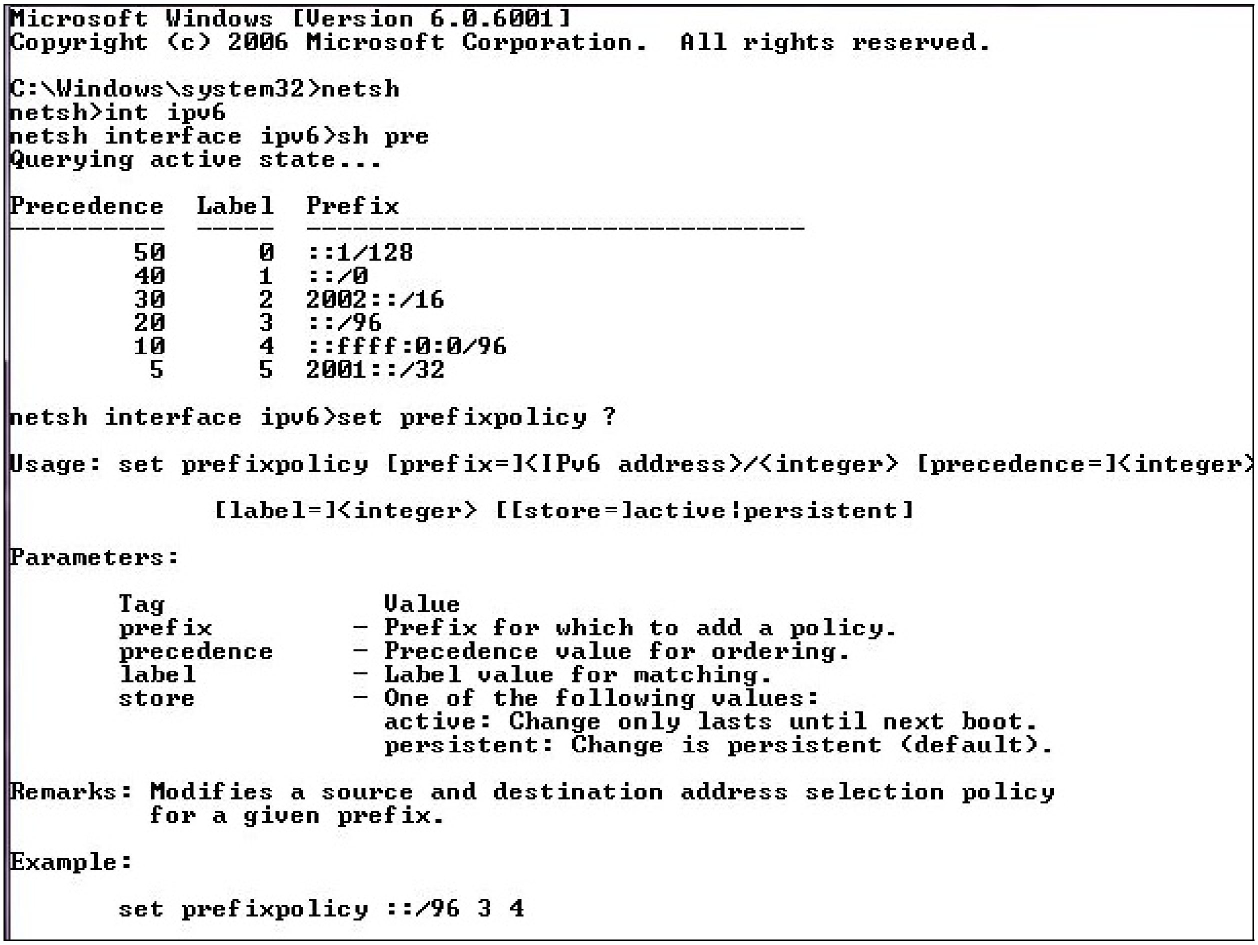
- Optionally, for IPv6, address assignment is performed as specified in RFC 4862, RFC 4193 and RFC 3315. This address assignment is handled by the underlying IPv6 stack. That stack is expected to make all IPv6 addresses available to UPnP applications.

A.3.3 IPv6 Address Selection and RFC 3484

As described in the normative sections above, UPnP dual-stack Devices operate both at IPv6 multicast link-local-scope and site-scope by default, and advertise their services in SSDP messages sent in site-scope multicast packets *in addition to* link-scope multicast. As explained above, the default is for UPnP dual-stack devices to prefer a ULA over a GUA. This policy preference is only a small part of the general problem of address selection in IPv6 nodes as explained in RFC 3484, which was published prior to when the ULA Proposed Standard was published by the IETF in RFC 4193.

A.3.4 Setting UPnP Policy on Windows Vista™ [Informative]

Vendors of IPv6 end systems use RFC 3484 and at least one vendor, Microsoft, exposes an interface to an IPv6 address selection process. By default, the IPv6 address selection does not specify the preferences between ULA and GUA addresses. The table below shows a default table followed by the set prefixpolicy command syntax.



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>netsh
netsh>int ipv6
netsh interface ipv6>sh pre
Querying active state...

Precedence  Label  Prefix
----------  -----  --------------------------------
        50      0  ::1/128
        40      1  ::/0
        30      2  2002::/16
        20      3  ::/96
        10      4  ::ffff:0:0/96
         5      5  2001::/32

netsh interface ipv6>set prefixpolicy ?

Usage: set prefixpolicy [prefix=]<IPv6 address>/<integer> [precedence=]<integer>

             [label=]<integer> [[store=]active|persistent]

Parameters:

       Tag              Value
       prefix         - Prefix for which to add a policy.
       precedence     - Precedence value for ordering.
       label          - Label value for matching.
       store          - One of the following values:
                        active: Change only lasts until next boot.
                        persistent: Change is persistent (default).

Remarks: Modifies a source and destination address selection policy
         for a given prefix.

Example:

       set prefixpolicy ::/96 3 4
```

To implement the UPnP-default of preferring ULA over GUA for site-scope multicast sources, a non-default Vista preferences table is created using the netsh set command applied to prefixpolicy.

```
There is a command line interface for managing some of the stack parameters on Windows: netsh.
>netsh  ?
netsh>int ipv6
netsh interface ipv6>sh pre
Querying active state...

Precedence  Label  Prefix
----------  -----  ----------
    90      0      ::1/128
    65      1      fc00::/7
    60      1      fd00::/7
    50      2      2000::/3
    40      3      2002::/16
    30      3      2001::/32
    20      4      ::/0
    10      5      ::ffff:0:0/96
     5      6      ::/96
     4      6      fec0::/10
```

The prefix fc00::/7 and fd00::7 are Unique Local Address prefixes. Which one is used depends on whether the prefix is locally or globally assigned, i.e. it depends on the value of the L-Bit [RFC4193]. The following table explains the prefixes that appear in the netsh command shown.

PREFIX	*USE*
::1/128	Self
fc00::/7	Managed Local
fd00::/7	Unmanged Local
2000::/3	RIR Managed Global
2002::/16	Tunnel – 6to4
2001::/32	Tunnel - Teredo
::/0	Default
::ffff:0:0/96	IPv4
::/96	Deprecated – AutoTunnel
fec0::/10	Deprecated – Site Local

Note that when the prefix policy is changed, the default table is deleted, and It is necessary to re-initialize the entire table according to the guidelines given above. The first change to the default table is to increase the Precedence of the loopback address ::1/128 to 90 as shown below.

```
netsh interface ipv6>set prefixpolicy ::1/128 90 0
Ok.
```

```
netsh interface ipv6>sh pre
Querying active state...

Precedence  Label  Prefix
----------  -----  --------------------------------
      90      0    ::1/128
```

The remaining preferences can be in a similar manner to create the complete preference table shown above.

```
netsh interface ipv6>add prefixpolicy fc00::/7 65 1
Ok.

netsh interface ipv6>sh pre
Querying active state...

Precedence  Label  Prefix
----------  -----  --------------------------------
      90      0    ::1/128
      65      1    fc00::/7
```

A.4 Discovery

The UPnP discovery phase does not substantially change when used over IPv6. All definitions of section 1 “Discovery” in the main document (UDA 1.1). Section 1 of this document MUST be followed, except when a change is mentioned in this section.

IGMP is the protocol used by IPv4 to ensure that incoming multicast traffic is forwarded by a router to the network segment to which the router is attached. IGMP requires that the devices and control points attached to the network segment contact the router to notify it of their interest in certain multicast addresses. The protocol that provides this service in IPv6 is Multicast Listener Discovery protocol (MLD). UPnP Control points and devices MUST participate in the MLD protocol (either directly, or indirectly via APIs to an IPv6 stack) for any link-local and site scope UPnP IPv6 multicast message.

IP addresses embedded in UPnP messages and descriptions sent in response to requests received on IPv6 addresses will generally be literal addresses formatted according to RFC 3986 and RFC 5952 (including those in discovery messages, the URLBase element of the device description (if specified), and HTTP HOST header fields). Together with the UUID, the BOOTID.UPNP.ORG header field allows control points to recognize when a message received on a different protocol or address is referring to the same device that is multi-homed (in this case, the BOOTID.UPNP.ORG field value will be the same in all announcements), as opposed to being a new advertisement from a device which has changed from one protocol or address to another (in this case, the BOOTID.UPNP.ORG field value will differ between the old and the new announcement).

For backward compatibility with control points implementing UPnP over IPv6 according to the provisions of Annex A to UPnP Device Architecture version 1.0, devices SHOULD include an OPT header field and NLS header field in addition to the BOOTID.UPNP.ORG header field. The OPT header field is defined by the HTTP Extension Framework (RFC 2774); the OPT header field is used (rather than MAN) because it is possible for a control point to function without recognizing the NLS header field, although the user experience will be suboptimal (and IPv4-only control points may not recognize NLS). The NLS field value, as defined in Annex A to UPnP Device Architecture version 1.0, contains a string value which must change whenever the network configuration of the device changes. It was recommended in that Annex that a GUID be used as the NLS field value, but other mechanisms for producing a unique value were permitted. Since under UPnP Device Architecture version 1.1 the BOOTID.UPNP.ORG field value is required to be unique on each device reboot or configuration change, the field value of the NLS header field can be set the same as the field value of the BOOTID.UPNP.ORG header field to simplify implementation.

A.4.1 Advertisement

For IPv6, a device advertises over IPv6 according to the following guidelines:

- SSDP announcements are sent to `[FF0X::C]:1900` (with "X" being either 1, 2 or 5 and set appropriately depending on the multicast scope upon which the announcement is being sent). Control points listen to these addresses and ports to detect when new devices are available on the network.

- As described in section 1.2.2 "Device available – NOTIFY with ssdp:alive" in the main document (UDA 1.1), announcements sent over IPv6 MAY have a different CACHE-CONTROL field value and MAY be sent with a different frequency than announcements sent over IPv4. When all advertisements, both over IPv4 and IPv6, have expired, the control point MUST assume that the device (or service) is no longer available.

- The SSDP HOST field value contains an IPv6 address instead of an IPv4 address. The Internet Assigned Numbers Authority has registered a multicast address and port for SSDP: an address MUST be of the form `FF0X::C`. This is a variable scope multicast address where X is changed to represent the appropriate scope. A device advertising on the local link would use a scope of 2 and address [FF02::C]:1900. A site-scope advertisement on the home network would use scope 5 [see 2.7 of RFC 4291] and MUST specify address [FF05::C]:1900.

- The SSDP LOCATION field value contains the URL of the root device description document. Typically, a literal IPv6 address formatted according to RFC 3986 will be used. An IPv6 address MUST be contained within brackets if a port is specified. The host address in the URL MUST be valid within the current scope (the address or scope on which the announcement is being sent). Specifically, a device advertising over IPv6 MUST NOT use an IPv4 address in the SSDP LOCATION header field. The site-scope rules of RFC 3484 MUST be followed by UPnP IPv6 nodes.

- The OPT and NLS header fields SHOULD be included.

The example below incorporates this syntax.

```
NOTIFY * HTTP/1.1
HOST: [FF02::C]:1900
CACHE-CONTROL: max-age = seconds until advertisement expires
LOCATION: URL for UPnP description of this device
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: same value as BOOTID field value
```

```
NT: notification type
NTS: ssdp:alive
SERVER: OS/version UPnP/1.1 product/version
BOOTID.UPNP.ORG: number increased each time device sends an initial announce or update
message
CONFIGID.UPNP.ORG: number used for caching description information
USN: composite identifier for the advertisement
```

A.4.2 Advertisement: Device unavailable

All ssdp:byebye messages MUST be sent to the IPv6 multicast address as described in section A.4.1 "Advertisement", and SHOULD contain the OPT and NLS header fields. Otherwise, the behavior is the same as IPv4. An example of an ssdp:byebye message has the following syntax.

```
NOTIFY * HTTP/1.1
HOST: [FF02::C]:1900
NT: notification type
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: same value as BOOTID field value
NTS: ssdp:byebye
BOOTID.UPNP.ORG: number increased each time device sends an initial announce or update
message
CONFIGID.UPNP.ORG: number used for caching description information
USN: composite identifier for the advertisement
```

A.4.3 Advertisement: Device update

All ssdp:update messages MUST be sent to the IPv6 multicast address as described in section A.4.1 "Advertisement", and SHOULD contain the OPT and NLS header fields. Otherwise, the behavior is the same as IPv4. An example of an ssdp:update message has the following syntax.

```
NOTIFY * HTTP/1.1
HOST: [FF02::C]:1900
LOCATION: URL for UPnP description for root device
NT: notification type
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: same value as BOOTID field value
NTS: ssdp:update
USN: composite identifier for the advertisement
BOOTID.UPNP.ORG: BOOTID value that the device has used in its previous announcements
CONFIGID.UPNP.ORG: number used for caching description information
NEXTBOOTID.UPNP.ORG: new BOOTID value that the device will use in subsequent announcements
SEARCHPORT.UPNP.ORG: number identifies port on which device responds to unicast M-SEARCH
```

A.4.4 Search

When a control point is added to the network, it MAY send multicast M-SEARCH requests on IPv4 address(es), IPv6 address(es), or both. When searching over IPv6, a control point can freely choose the scope of the search (link local scope or site scope), allowing it to better direct its search. It should be noted that the source address of the M-SEARCH can influence [RFC3484] how and where the M-SEARCH is routed for link and site scopes. Aside from using an IPv6 multicast address and including an IPv6 address in the header fields, M-SEARCH messages are unchanged. An example of an M-SEARCH message has the following syntax. In addition, M-SEARCH messages MAY be unicast to IPv6 addresses of known devices, similar to IPv4 unicast M-SEARCH messages.

```
M-SEARCH * HTTP/1.1
HOST: [FF02::C]:1900
MAN: "ssdp:discover"
MX: seconds to delay response
ST: search target
```

A.4.5 Search response

To be found, a device MUST send a response to the source IP address and port that sent the request to the multicast address, and SHOULD include the OPT and NLS header fields in the message. An example of a search response message has the following syntax.

```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age = seconds until advertisement expires
DATE: when response was generated
EXT:
LOCATION: URL for UPnP description of this device
SERVER: OS/version UPnP/1.1 product/version
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: same value as BOOTID field value
ST: search target
BOOTID.UPNP.ORG: number increased each time device sends an initial announce or update
message
CONFIGID.UPNP.ORG: number used for caching description information
USN: composite identifier for the advertisement
```

A.5 Description

Description documents MUST be sent using the same address on which the HTTP GET was received. Otherwise, behavior is the same as IPv4.

A.6 Control

Responses to SOAP messages during the Control phase MUST be sent on the same address on which the request was received. Otherwise, behavior is the same as IPv4.

A.7 Eventing

When subscribing to events over IPv6, the <deliveryURL> (or URLs) specified in the CALLBACK header field of the SUBSCRIBE message MUST be reachable by the device. This means, for example, when sending a SUBSCRIBE request to a device using a link-local IPv6 address, the <deliveryURL> MUST specify an IPv6 address on the same link, which is a node's link-local address.

IPv4 addresses MUST NOT be included in the CALLBACK header field of a SUBSCRIBE message sent over IPv6. IPv6 addresses MUST NOT be included in the CALLBACK header field of a SUBSCRIBE message sent over IPv4.

IPv6 multicast event messages MUST be sent to `[FF0X::130]:7900` (with "X" being equal to the address scope used in advertisement). To receive IPv6 multicast event messages, control points MUST listen to these addresses and ports.

To send a multicast event message, a publisher MUST send a message with method NOTIFY in the following format. Values in *italics* below are placeholders for actual values. Refer to section 4.3.3 "Multicast Eventing: Event messages: NOTIFY" in the main document (UDA 1.1) for an explanation of the elements. All IP addresses contained in the event MUST be IPv6 format and scoped as above.

```
NOTIFY * HTTP/1.1
HOST: [FF0X::130]:7900 *** note the address and the port number are different from SSDP ***
CONTENT-TYPE: text/xml; charset="utf-8"
USN: Unique Service Name for the publisher
SVCID: ServiceID from SCPD
NT: upnp:event
NTS: upnp:propchange
SEQ: monotonically increasing sequence count
LVL: event importance
BOOTID.UPNP.ORG: number increased each time device sends an initial announce or an update
message

<?xml version="1.0"?>
<e:propertyset xmlns:e="urn:schemas-upnp-org:event-1-0">
    <e:property>
        <variableName>new value</variableName>
    </e:property>
    <!-- Other variable names and values (if any) go here. -->
</e:propertyset>
```

A.8 Presentation

Responses to HTTP GET requests for presentation pages MUST be sent using the same address on the same interface on which the HTTP GET was received.

Presentation pages retrieved over IPv6 MUST NOT contain IPv4 addresses. Presentation pages retrieved over IPv4 MUST NOT contain IPv6 addresses.

It is RECOMMENDED that fully qualified URLs to resources on the device are not embedded in HTML presentation pages, but that relative URLs are used instead, so that the host portion of the embedded URLs does not need to be modified to match the address on which the GET was received.

A.9 References

A.9.1 Normative

BCP 0005

Address Allocation for Private Internets. Available at: http://www.ietf.org/rfc/rfc1918.txt

IANA

Internet Protocol Version 6 Multicast Addresses. Available at: http://www.iana.org/assignments/ipv6-multicast-addresses/.

RFC 3986

Format for Literal IPv6 Addresses in URLs. Available at: http://www.ietf.org/rfc/rfc3986.txt.

RFC 2774

HTTP Extension Framework. Available at: http://www.ietf.org/rfc/rfc2774.txt.

RFC 4862
IPv6 Stateless Address Autoconfiguration. Available at: http://www.ietf.org/rfc/rfc4862.txt.

RFC 3315
Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Available at: http://www.ietf.org/rfc/rfc3315.txt.

RFC 3484
Default Address Selection for Internet Protocol version 6 (IPv6). Available at: http://www.ietf.org/rfc/rfc3484.txt.

RFC 3879
Deprecating Site-local Addresses. Available at: http://www.ietf.org/rfc/rfc3879.txt.

RFC 3986
Uniform Resource Identifiers (URI): Generic Syntax. Available at: http://www.ietf.org/rfc/rfc3986.txt.

RFC 4291
IP Version 6 Addressing Architecture. Available at: http://www.ietf.org/rfc/rfc4291.txt.

RFC 4861
Neighbor Discovery for IP Version 6 (IPv6). Available at: http://www.ietf.org/rfc/rfc4861.txt.

RFC 4193
Unique Local IPv6 Unicast Addresses. Available at: http://www.ietf.org/rfc/rfc4193.txt.

RFC 5952
A Recommendation for IPv6 Address Text Representation. Available at: http://www.ietf.org/rfc/rfc5952.txt.

A.9.2 Informative

RFC 3493
Basic Socket Interface Extensions for IPv6. Available at: http://www.ietf.org/rfc/rfc3493.txt.