UPnP Device Architecture V1.0
Annex A – IP Version 6 Support

This Annex to the UPnP Device Architecture V1.0 has been submitted by Microsoft Corporation to the UPnP Forum pursuant to Section 2.4(e) of the UPnP Membership Agreement. UPnP Forum Members have rights and licenses defined by Section 3 of the UPnP Membership Agreement to use and reproduce this Annex in association with Standardized DCPs and Extended DCPs in UPnP Compliant Devices. All such use is subject to all of the provisions of the UPnP Membership Agreement.

A.1 INTRODUCTION

Most of today's internet uses IPv4, which is now nearly twenty years old. 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 autoconfiguration. 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 based on the UPnP Device Architecture V1.0 may be used on IPv6 networks.

A.2 GENERAL PRINCIPLES

Devices using the UPnP Device Architecture V1.0 over IPv6:

- MUST support link-local addresses and scopes as the default configuration. This means listening and broadcasting on **`FF02::C`**, the link-local scope multicast address for SSDP.

- MUST use scoping of IPv6 addresses to control the propagation of SSDP messages instead of relying on the Hop Limit (equivalent to the TTL limit in IPv4).

- MAY support subnet scope **`FF03::C`**, administrative scope **`FF04::C`** and site-local scope **`FF05::C`** as a configurable option. If one of these scopes is selected, the device will support it *in addition to* the link-local scope.

- MAY provide the ability to select which interface or interfaces over which the device will be visible to UPnP control points, in devices that support multiple interfaces.

- MAY use the Network Location Signature (NLS), described later in this document, to carry a unique signature for the networking state of the device. If implemented, the NLS MUST change each time the network addresses over which the device is visible to UPnP control points change in the device, so that control points can recognize when a received advertisement represents a duplicate of one received on a different stack or address rather than an indication that the device has received a new address and the old one should be disregarded. Every announcement on every scope, site, and interface includes the same NLS value.

A.2.1 Link-local scope

Link-local scope SHALL be the default scope for operation over IPv6. The device will choose the set of link-local addresses to be used. The default value is one link-local address per interface. In case more than one link-local address is available for any particular interface, one of the addresses is selected and used for that interface; devices SHOULD use the same address as previously used whenever possible.

A.2.2 Site-local scope

Site-local addresses and scopes MAY also be supported in UPnP devices. If supported and enabled, the

administrator SHALL specify the scope(s) in which the UPnP device is to be active. If the scope is not otherwise specified, the default value SHALL be to use link-local scope only.

If site-local scope support is enabled, during initialization the device SHALL attempt to obtain a site-local address by sending a Router Solicitation message and then executing a site-local address configuration sequence. Unless a particular subset of interfaces is specified by the administrator or device default,, UPnP operation SHALL be enabled on all interfaces. If more than one site-local address is available on any particular interface, or across a set of interfaces, and they are all valid in the same site for the specified scope, then one site-local address SHALL be selected and used as the IP source address and LOCATION for UPnP operations on the interface(s) on which the address is valid; devices SHOULD use the same address as previously used whenever possible. If site-local addresses belong to two or more different sites, then one site-local address SHALL be selected for each site. The NLS value, if provided, SHALL be the same across all networks, sites, addresses, and interfaces.

Up to three announcements are sent per interface, one using the IPv4 address, the second using the link-local IPv6 address, and the third using the site-local address, if enabled.

A.2.3 Device operation

A device supporting both IPv4 and IPv6 simultaneously SHALL be advertised using the same USN on both IPv4 and IPv6 *only* if the device description document and presentation resources are identical when accessed from both protocols. If there is any difference in the description of the device or its services when operating on IPv6 versus IPv4, the device SHALL NOT be advertised with the same USN on both networks; instead, it SHALL be advertised as two separate devices with distinct USN values. It is the responsibility of the device to determine the services to be advertised on each of the addresses. For example, advertising certain Internet Gateway features on IPv6 addresses may not be useful, in which case the device should not do it. (Throughout the remainder of this Annex, a single physical device which contains two or more “logical” devices that have different USNs is considered to be separate devices.)

A.2.4 Control point operation

A UPnP device which advertises on multiple networks, multiple addresses, or multiple interfaces SHOULD be displayed only once in the control point user interface in order to reduce user confusion. UPnPv1 control points typically use the LOCATION and USN headers to identify and discard duplicate advertisements, but this may not be sufficient when a control point supporting multiple networks, addresses, or interfaces receives announcements from a device which also supports multiple networks, address, or interfaces - the USNs will still match, but the location URL may be different (each may contain a different literal numeric IP address). In this case, if the device follows the guidelines above, the NLS header values will match across all networks, address, and interfaces, allowing the control point to properly determine that the device is accessible through multiple LOCATIONs rather than having changed LOCATION.

The control point MAY use any of the URLs received in LOCATION headers to access the device - the device description or presentation page - on the local network.

Regardless of which way, from what address, and how many announcements a control point receives, it will unambiguously know that they were sent by the same device, so long as the device properly implements the NLS header.

A device BYE-BYE message received on either IPv4 or IPv6 SHOULD cause all instances of the device to be removed from the control point cache of known devices.

A.3 ADDRESSING

UPnPv1 devices MAY support IPv4, IPv6, or both. The following sections describe how a device obtains an IPv6 address. The mechanisms described do not differ in any significant way from those described in the IPv6 standards. Note that in most implementations, the actions described are likely performed by the IPv6 stack and do not require any special coding by UPnP implementers.

Unlike when using IPv4, where each device must have a DHCP client to try to obtain an address initially, DHCP is unnecessary in an IPv6 network. Addresses are automatically configured in new ways.

In IPv6 networks, link-local addresses are determined per interface on the device, and therefore IPv6 devices will always have a link-local address. In addition, unicast addresses (site local or global addresses), and the loopback address **::1** are also determined for each interface although a device may or may not have a site-local or global address. Typical IPv6 devices are logically multi-homed because they always have at least two addresses with which they can receive packets – a link-local address for local link traffic and a routable site-local or global address. In some scenarios, devices may only have a link-local address; reasons for this include device sophistication (and thereby device capability) and administrative policy. Link-local addresses are assigned immediately at the device, without referring to an outside server such as a DHCP server. Site-local and global addresses are determined through the use of RA (Router Advertisement) messages in conversation with the local router. With site multihoming, source address selection rules are complicated.

The UPnP architecture exploits IPv6 link-local and site-local addresses. Link-local addresses are used between on-same-link neighbors (and in IPv6's own Neighbor Discovery process). Site-local addresses are used between nodes communicating with other nodes in the same site.

This section describes the IPv6 autoconfiguration of link-local and site-local addresses in more detail. In addition to the address assigned by this process, each device, acting as a normal IPv6 host, listens for traffic on several multicast addresses: node-local scope all-nodes multicast address **FF01::1**; link-local scope all-nodes multicast address **FF02::1**; and multicast addresses of joined groups on each interface.

A.3.1 IPv6 link-local address autoconfiguration

Link-local addresses use a **FE80::/64** prefix. The IPv6 link-local address autoconfiguration process is summarized as follows:

1. A tentative link-local address is derived at the device by local automatic assignment.

2. Duplicate address detection is performed on the link.

3. If not unique, manual configuration of the link-local address is required.

4. If unique, the tentative link-local address is reset to "valid".

5. Other autoconfiguration steps take place.

The details of this process are described below.

1. A tentative link-local address is derived at the device based on the link-local prefix of **FE80::/64** and concatenating that with the 64 bit interface identifier for each interface on the device. The interface identifier is generally based on a unique token derived from the MAC address, such as the IEEE EUI-64 number. This tentative address is assigned a formal state of "tentative".

2. Duplicate address detection is performed by the device to verify the uniqueness of the tentative

link-local address. This is done by sending a Neighbor Solicitation (NS) ICMPv6 message to the network (local link) with its Target Address field set to the tentative link-local address of the device. Multiple NS messages are sent, to ensure conflict detection.

3. If a Neighbor Advertisement ICMPv6 message sent in response to the Neighbor Solicitation message is received, this indicates that another device on the local link is already using the tentative link-local address, and autoconfiguration must stop. At this point, it is conventional to assume that manual configuration of the device's address must be performed. However, this is an infrequent case due to the algorithm used to create the tentative addresses. For example, this is often based on an augmented or processed version of the device's interface's MAC address, which is rarely duplicated. (Note there is no standard way to create the tentative address, but the MAC-based algorithm is common.) Further, devices may attempt to generate random interface IDs (limited to several retries to avoid never-ending attempts before declaring failure).

4. If no Neighbor Advertisement message (sent in response to the Neighbor Solicitation message) is received, the tentative link-local address is assumed to be unique and valid on that link. The link-local address is initialized for the interface and its state changed from "tentative" to "valid".

5. The solicited-node multicast link-layer address corresponding to this new valid address is also registered with the network adapter. Then autoconfiguration proceeds to perform stateless address autoconfiguration with Router Solicitation and Router Advertisements (see site-local autoconfiguration process in the next section).

The lifetime of link-local addresses is unlimited. If a site-local address is later configured, the link-local address may continue to be used when appropriate.

A.3.2 IPv6 site-local address autoconfiguration

Site-local addresses use a **`FEC0::/48`** prefix. The IPv6 site-local address autoconfiguration process is part of the general non-link-local address autoconfiguration process using Router Solicitation and Router Advertisement messages, and is summarized as follows:

1. A Router Solicitation ICMPv6 message is sent on the local link.

2. If no Router Advertisement ICMPv6 messages are received, alternative address configuration must be performed.

3. If a Router Advertisement message is received, configuration parameters are set.

4. For each Prefix information received, including the site-local prefix, flags are checked and the prefix is processed accordingly. If appropriate, a tentative address is established (including a tentative site-local address), checked for duplication, and if not already in use, assigned to be "valid".

5. The Managed Address Configuration flag is checked.

6. The Other Stateful Configuration flag is checked.

The following provides details of this process.

1. Following the link-local process described earlier, the device sends a Router Solicitation ICMPv6 message to discover any router on the local link.

2. If no Router Advertisement ICMPv6 messages are received in response, then the device must use an alternative address configuration protocol to obtain its other addresses and certain other

configuration parameters, or use only the link-local address previously configured.

3. If a Router Advertisement message is received, certain configuration parameters are set (Hop Limit, Reachable Time, Retrans Timer, MTU) using the information carried in the message.

4. For each Prefix information received from the router in the RA message, which may include the site-local prefix:

    a. If the On-link flag is set to 1, the prefix is added to the device's prefix list.

    b. If the Autonomous flag is set to 1, the prefix and the 64-bit interface identified are used to derive a tentative address.

    c. Duplicate address detection is used to verify the uniqueness of the tentative address similarly to the link-local process.

    d. If the tentative address is already in use, it is not used.

    e. If the tentative address is not in use, the address is initialized (which includes setting the valid and preferred lifetime values for this address, plus registering the corresponding solicited-node multicast link-layer address with the network adapter).

5. If the Managed Address Configuration flag is set to 1 in the RA message, a stateful address configuration protocol must be used to obtain additional addresses.

6. If the Other Stateful Configuration flag is set to 1, a stateful address configuration protocol must be used to obtain additional configuration parameters.

A.3.3 IPv6 addresses and ports

UPnP devices and control points SHALL support:

- One link-local unicast address per IPv6 interface
- A unicast loopback address **`::1`** for the loopback interface
- A node-local scope all-nodes multicast address **`FF01::1`**
- A link-local scope all-nodes multicast address **`FF02::1`**
- The link-local scope multicast address for SSDP **`[FF02::C]:1900`**

UPnP devices and control points MAY support:

- One site-local unicast addresses per site (if a router is present and so configured)
- Additional multicast addresses for joined groups.
- The multicast address for SSDP for other scopes in which the device is active **`[FF0X::C]:1900`** (with "X" being set appropriately depending on the address scope upon with the announcement is being sent)

A.3.4 Summary of boot/startup process

- For IPv4, Auto-IP addressing is done as specified in the UPnP Device Architecture V1.0
    - Since DNS is not required to be present on the network, implementations typically use literal addresses.
- For IPv6, the device enumerates all interfaces and checks its stored configuration for scope and interface settings.
- For each IPv6 interface, the device invokes the IPv6 auto-configuration process
    - Derive tentative link-local address (FE80::/64 + 64 bit Interface ID)
    - Send multicast neighbor solicitation to ensure link-local uniqueness
        - If a reply is received, the IPv6 auto-configuration sequence stops and manual configuration is normally required (although provision may be made for attempting randomly-generated addresses).
    - Initialize link-local address
    - If site-local scope specified, attempt to obtain a site-local address
        - Send a router solicitation message
        - Execute site-local address configuration sequence.

A.4 DISCOVERY

The UPnP discovery phase does not substantially change when used over IPv6. Addresses sent on IPv6 addresses will generally be literal addresses formatted according to RFC 2732 (including those in discovery messages, the <URLBase> element of the device description (if specified), and HTTP and GENA HOST headers). The NLS header is added to SSDP to allow control points to recognize when a message received on a different protocol or address is referring to the same device as opposed to being a new advertisement from a device whose address has changed.

A.4.1 Advertisement

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

- SSDP announcements are sent to **`[FF0X::C]:1900`** (with “X” being set appropriately depending on the address scope upon with the announcement is being sent) Control points listen to these addresses and ports to detect when new devices are available on the network.
- The SSDP LOCATION header contains the URL of the root device description document. Typically, a literal address will be used. When multiple IPv6 addresses are available, one will be chosen in link-local scope per interface and one in site-local scope per device for each site.
- One link-local address will be advertised for each interface.
- One site-local address for each unique site will be advertised per device.

- SSDP announcements SHALL NOT be sent to or received from IPv6 Global addresses.

For both IPv4 and IPv6 announcements, the new SSDP NLS extension header field SHOULD be provided. If it is provided, the NLS value specifies a string (which is recommended to be a GUID) that identifies the current state of IP addresses used by the device for UPnP operation. The same NLS value SHALL be sent in all advertisements and search responses sent by the device, on all addresses, scopes, networks, and interfaces.

In IPv6 announcements, the SSDP HOST header will typically contain a literal IPv6 address, formatted according to RFC 2732, followed by a port. The LOCATION field requires that an IPv6 address be contained within brackets if a port is specified. The examples below incorporate this syntax.

```
NOTIFY * HTTP/1.1
HOST: [FF02::C]:1900
CACHE-CONTROL: max-age = 1600
LOCATION: http://[deviceIPv6addr]:port/descriptiondocname
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: network location signature
NT: search target
NTS: ssdp:alive
SERVER: OS/version UPnP/1.0 product/version
USN: advertisement UUID
```

Listed below are details for the altered and added header fields appearing in the listing above. In the listing above and others throughout this section, HTTP header values are case sensitive.

HOST

Required. Multicast address and port are registered for SSDP by Internet Assigned Numbers Authority (IANA). For IPv6, 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. For example, a device advertising on the local link would use a scope of 2 and address **FF02::C**. Port 1900 MUST be specified.

LOCATION

Required. This is a single URL to the root device description, specified by the vendor of the UPnP device. For IPv6, the URL uses a host address valid within the current scope (the address or scope on which the announcement is being sent).

OPT and NLS

RECOMMENDED for both IPv4 and IPv6. The OPT header is defined by the HTTP Extension Framework (RFC 2774). The NLS header contains a string value which must change whenever the network configuration of the device changes (e.g., if any of the assigned or calculated IP addresses change). It is RECOMMENDED that a GUID (in the standard UUID text format, for example, “0000002F-0000-0000-C000-000000000046”) be used for this purpose, since all UPnP devices must already have the ability to generate GUIDs; however, other techniques are possible. The NLS value SHALL be at least 1 and no more than 64 characters in length. The OPT header is used (rather than MAN) because it is possible for a control point to function without recognizing the NLS header, although the user experience will be suboptimal (and IPv4-only control points may not recognize NLS).

A.4.2 Advertisement: Device unavailable

When a device and its services are going to be removed from the network, the device should multicast an **ssdp:byebye** message corresponding to each of the **ssdp:alive** messages it multicasted that have not already expired. Similarly, if an interface change notification is received after an announcement, the

device should cancel existing advertisements.

```
NOTIFY * HTTP/1.1
HOST: [FF02::C]:1900
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: network location signature
NT: search target
NTS: ssdp:byebye
USN: advertisement UUID
```

Furthermore, devices need to remember their prior IP addresses in the event that some or all of them have changed. If that is the case, new advertisements have to be sent, using the same sequence described above.

A.4.3 Search

When a control point is added to the network, it MAY send a multicast M-SEARCH request on its IPv4 address(es), IPv6 address(es), or both. By default, searches are sent only in link-local scope on IPv6 interfaces; searches may also be sent on one or more of the site-local scopes if site-local capability is enabled by an administrator. Aside from using an IPv6 multicast address, M-SEARCH messages are unchanged. An example of an M-SEARCH message has the following syntax.

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

Search messages do not contain the NLS field.

A.4.4 Search response

To be found, a device SHALL send a response to the source IP address and port that sent the request to the multicast channel.

Responses to M-SEARCH are intentionally parallel to advertisements, and as such, follow the same pattern as listed for NOTIFY with **`ssdp:alive`** (above), including the NLS header field. The only difference is the NT header, which is an ST header in a search response. The response MUST be sent in the following format.

```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age = 1600
DATE: Wed, 12 Jun 2002 07:01:56 GMT
EXT:
SERVER: OS/version UPnP/1.0 product/version
LOCATION: http://[deviceIPv6addr]:port/descriptiondocname
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: network location signature
ST: search target
 USN: advertisement UUID
```

A.5 DESCRIPTION

Description documents SHOULD be sent on the same interface and using the same address on which the HTTP GET was received.

It is RECOMMENDED that <URLBase> not be used on devices that support multiple protocols, interfaces, or addresses, but that the address from which the description document is retrieved serve as the URLBase, for simplicity of implementation. If URLBase is provided, it SHOULD reflect the IP address to which the HTTP GET request was sent to read the description, since that address is known to be reachable by the requesting control point. All URLs in the remainder of the description SHOULD be relative to URLBase, or to the URL from which the description was read, using the rules specified in section 5 of RFC 2396, except those specifically intended to be "off the device" (such as `<manufacturerURL>` and `<modelURL>`).

If any element of the device description other than URLBase is different for operation over IPv4 vs. IPv6, and the device is a dual-stack device, then the device SHALL be advertised as two separate devices, with a unique USN and UDN for each stack. If it were to be advertised as a single device with a common USN, UDN, and NLS on both IPv4 and IPv6, dual-stack control points might assume that the descriptions are the same and choose to download the description only once (on the preferred interface). For example, an Internet Gateway may make different actions and state variables visible to IPv6 devices than are available to IPv4 devices; the gateway should be advertised as two devices, one for IPv4 and one for IPv6.

A.6 CONTROL

Responses to SOAP messages during the Control phase SHOULD be sent on the same interface and using the same address on which the request was received.

Any fully-qualified URLs contained in action or response arguments that refer to a resource on the device itself SHALL have the HOST portion of the URL set appropriately so that the resource will be reachable by the control point that requested the action. This might be accomplished by using the value specified in the HTTP HOST header of the control request.

A.7 EVENTING

When subscribing to events over IPv6, the **`<deliveryURL>`** (or URLs) specified in the CALLBACK header of the SUBSCRIBE message SHOULD be nominally reachable by the device. This means, for example, when sending a SUBSCRIBE request to a device using a link-local IPv6 address, the **`<deliveryURL>`** SHALL specify a link-local IPv6 address; site-local IPv6 addresses and IPv4 addresses should not be included in the CALLBACK header of the same SUBSCRIBE message. Control Points SHALL NOT mix IP address types, scopes, sites, or interfaces in a single CALLBACK header.

A.8 PRESENTATION

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

It is recommended that fully-qualified URLs to resources on the device not be embedded in HTML presentation pages, but that relative URLs be 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.