InternetGatewayDevice:2 Device Template Version 1.01

For UPnP Versions *1.0* and *1.1*
Status: Standardized DCP (SDCP), Version 1.00
Date: *December 10, 2010*

This Standardized DCP has been adopted as a Standardized DCP by the Steering Committee of the UPnP Forum, pursuant to Section 2.1(c)(ii) of the UPnP Forum Membership Agreement. UPnP Forum Members have rights and licenses defined by Section 3 of the UPnP Forum Membership Agreement to use and reproduce the Standardized DCP in UPnP Compliant Devices. All such use is subject to all of the provisions of the UPnP Forum Membership Agreement.

THE UPNP FORUM TAKES NO POSITION AS TO WHETHER ANY INTELLECTUAL PROPERTY RIGHTS EXIST IN THE STANDARDIZED DCPS. THE STANDARDIZED DCPS 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, 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
Prakash Iyer, Ulhas Warrier	Intel Corporation
Mika Saaranen, Chair	Nokia
Fabrice Fontaine	Orange Labs

* Note: 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.

Contents

List of Tables

1.   Overview and Scope

This device template is compliant with the Universal Plug and Play Architecture, Version *1.0* and *1.1*.

This document defines the REQUIRED **ROOT** device:

urn:**schemas-upnp-org:device:***InternetGatewayDevice*.

The *InternetGatewayDevice* encapsulates all sub-devices and services for the Internet Gateway Device Control Protocol (DCP).

The Internet Gateway is an "edge" interconnect device between a residential Local Area Network (LAN) and the Wide Area Network (WAN), providing connectivity to the Internet. The gateway MAY be physically implemented as a dedicated, standalone device or modeled as a set of UPnP devices and services on a PC. This version of the DCP does not cover small business networks. Discovery and access to these services from outside the home network is not RECOMMENDED, unless adequate authentication, authorization and access control mechanisms are built into the device, beyond what is currently specified within the UPnP architecture framework.

Figure 1 below is a conceptual illustration of a generic Internet Gateway device consisting of one or more physical WAN and LAN interfaces.
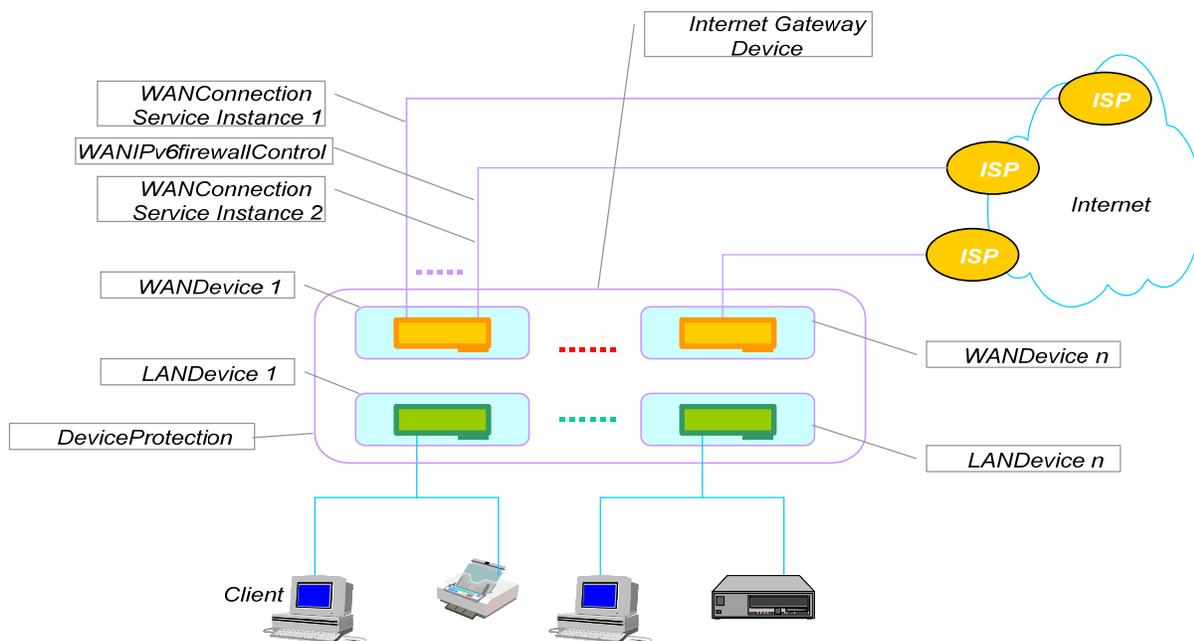
Figure 1: *InternetGatewayDevice* with LAN and WAN Interfaces

1.1.   Requirements for an Internet Gateway Device

The following list of requirements has been identified on the capabilities of an Internet Gateway in coming up with the devices and services hierarchy for the gateway DCP.

- The *InternetGatewayDevice* MUST support 1 WAN interface, but MAY support more than one physical WAN interface to connect to the Internet.
- The *InternetGatewayDevice* MUST support 1 LAN interface, but MAY support more than one physical LAN interface to connect to the residential network.

- The *InternetGatewayDevice* SHOULD support *DeviceProtection* defined in [DeviceProtection].
- The *InternetGatewayDevice* MUST support IGD Specific security as defined in section 2.3, but MAY implement stricter security policy.

An implementation MAY host the WAN interface and LAN interface (mentioned above) on the same physical network interface card (NIC).

- Each WAN interface MUST support one Internet connection, but MAY simultaneously support more than one Internet connection. Each of these connections will be modeled as instances of a service in the DCP.
- The *InternetGatewayDevice* MUST be IP addressable from the residential LAN at all times to be UPnP compliant. More specifically, in the case of gateways with broadband modems on the WAN side, the *InternetGatewayDevice* MUST be addressable.
  - When the device is not configured for WAN access or does not have any WAN connectivity.
  - Before, during and after modem and link configuration with a head-end device in the Internet service provider's central office.
- Connectivity on the WAN side MUST enable nodes on the residential LAN to access resources on the Internet. A gateway MAY support modems and/or connections on a modem to a service provider, not resulting in Internet connectivity – for example, POTS dial-up access to a modem bank of a home security monitoring service provider. Such connections are outside the scope and requirements of the gateway DCP.

In this document, an Internet connection implies IP connectivity to an Internet Service Provider. Figure 2 illustrates the hierarchy of devices and services in an *InternetGatewayDevice*. A physical modem on the WAN side and a connection interface/port on the LAN side of the *InternetGatewayDevice* are modeled by a *WANDevice* and a *LANDevice* instance respectively. Depending on the hardware capabilities of an Internet Gateway, more than 1 instance of *WANDevice* and/or *LANDevice* are possible in an actual implementation of the gateway DCP description document. Virtual connection interfaces – such as Virtual Circuits (VC) on a DSL modem, are modeled by one or more instances of *WANConnectionDevice*. Sub-devices and services mentioned in this document are defined in companion documents that together specify the DCP for an Internet Gateway. It is RECOMMENDED that *DeviceProtection* service will be connected to *InternetGatewayDevice* in the device and service hierarchy.
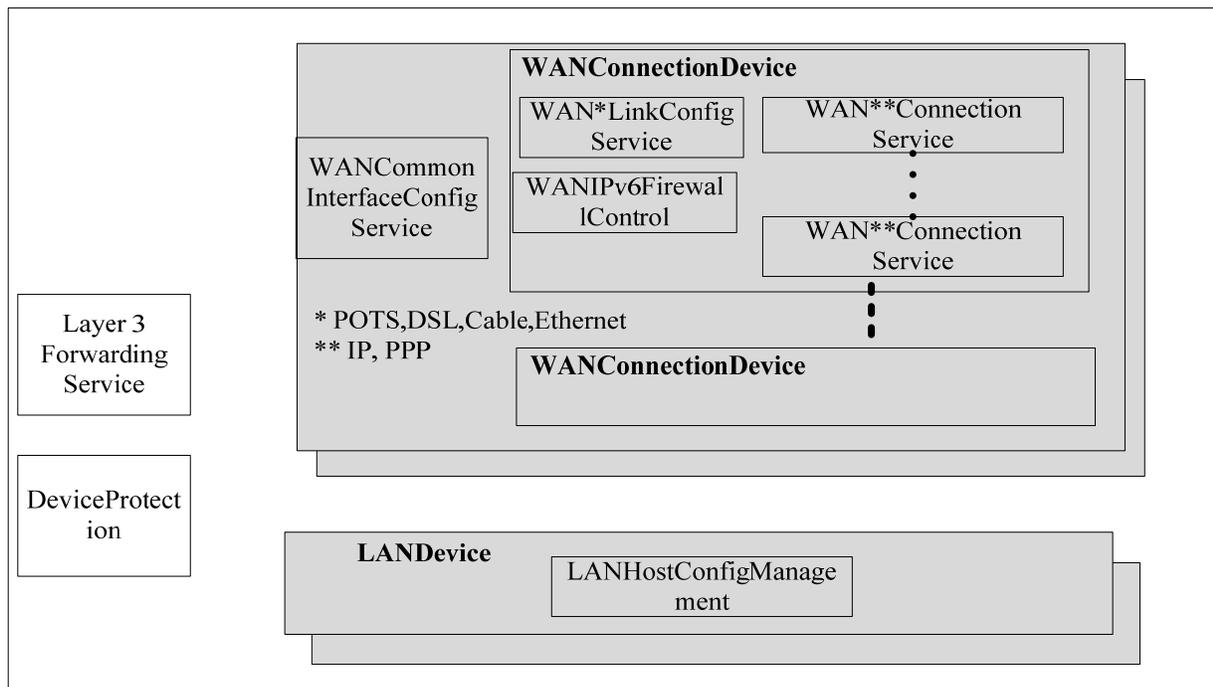

Figure 2: *InternetGatewayDevice* Devices and Services Hierarchy

1.2. Focus and Goals for DCP version 2.0

The Gateway Working Committee (IGD WC) agreed to focus on the following set of requirements in coming up with the hierarchy of devices and services for DCP v2.0.

- Update *WANIPConnection* service based on developer feedback and maintenance need
  - NAT terminology update
  - New actions better suited for application development
  - Limited port mapping lease time
  - Enhanced security for the actions and parameters
- Security and access control support
  - Allow basic IGD:1 compliant functionality without requiring new protocols to be supported
  - Protect and require authentication on functionality potentially creating security threats. These features will not be available for legacy control points and backward compatibility is limited in these cases where other role than *Public* is RECOMMENDED.
- Add support for IPv6 Firewall control (*WANIPv6FirewallControl*). This service allows creating and maintaining pinholes for inbound traffic from the Internet

Note: Due to lack of interest, *WANPPPConnection* service was NOT updated to reflect the changes made to *WANIPConnection*.

1.3. References

1.3.1. Normative References

This section lists the normative references used in this specification and includes the tag inside square brackets that is used for each such reference:

[DeviceProtection] – UPnP *DeviceProtection:1*, version 1.0, UPnP Forum, February 24, 2011.
Available at: http://upnp.org/specs/gw/UPnP-gw-DeviceProtection-v1-Service.pdf.

[WANDevice] – UPnP *WANDevice:2*, version 1.0, UPnP Forum, September 10, 2010.
Available at: http://upnp.org/specs/gw/UPnP-gw-WANDevice-v2-Device.pdf.

[WANConnectionDevice] – UPnP *WANConnectionDevice:2,* version 1.00, UPnP Forum, September 10, 2010.
Available at: http://upnp.org/specs/gw/UPnP-gw-WANConnectionDevice-v2-Device.pdf.

[WANIPConnection] – UPnP *WANIPConnection:2,* version 1.00, UPnP Forum, September 10, 2010.
Available at: http://upnp.org/specs/gw/UPnP-gw-WANIPConnection-v2-Service.pdf.

[WANIPv6FirewallControl] – UPnP *WANIPv6FirewallControl:1,* version 1.0, UPnP Forum, December 10, 2010.
Available at: http://upnp.org/specs/gw/UPnP-gw-WANIPv6FirewallControl-v1-Service.pdf.

[LANDevice] – UPnP *LANDevice:1,* version 1.0, UPnP Forum, November 19, 2001.
Available at: http://upnp.org/specs/gw/UPnP-gw-LANDevice-v1-Device.pdf.

[LANHostConfigManagement] – UPnP *LANHostConfigManagement:1,* version 1.0, UPnP Forum, November 19, 2001.
Available at: http://upnp.org/specs/gw/UPnP-gw-LANHostConfigManagement-v1-Service.pdf.

[L3Forwarding] – UPnP *Layer3Forwarding:1,* version 1.0, UPnP Forum, November 19, 2001.
Available at: http://upnp.org/specs/gw/UPnP-gw-Layer3Forwarding-v1-Service.pdf.

[WANCableLinkConfig] – UPnP *WANCableLinkConfig:1,* version 1.0, UPnP Forum, November 19, 2001.
Available at: http://upnp.org/specs/gw/UPnP-gw-WANCableLinkConfig-v1-Service.pdf.

[WANCommonInterfaceConfig] – UPnP *WANCommonInterfaceConfig:1,* version 1.0, UPnP Forum, November 19, 2001.
Available at: http://upnp.org/specs/gw/UPnP-gw-WANCommonInterfaceConfig-v1-Service.pdf.

[WANDSLLinkConfig] – UPnP *WANDSLLinkConfig:1,* version 1.0, UPnP Forum, November 19, 2001.
Available at: http://upnp.org/specs/gw/UPnP-gw-WANDSLLinkConfig-v1-Service.pdf

[WANEthernetLinkConfig] – UPnP *WANEthernetLinkConfig:1,* version 1.0, UPnP Forum, November 19, 2001.
Available at: http://upnp.org/specs/gw/UPnP-gw-WANEthernetLinkConfig-v1-Service.pdf.

[WANPOTSLinkConfig] – UPnP *WANPOTSLinkConfig:1,* version 1.0, UPnP Forum, November 19, 2001.
Available at: http://upnp.org/specs/gw/UPnP-gw-WANPOTSLinkConfig-v1-Service.pdf.

[WANPPPConnection] – UPnP *WANPPPConnection:1,* version 1.0, UPnP Forum, November 19, 2001.
Available at: http://upnp.org/specs/gw/UPnP-gw-WANPPPConnection-v1-Service.pdf.

[DEVICE] – UPnP Device Architecture, version 1.0, UPnP Forum, June 8, 2000.
Available at: http://upnp.org/specs/arch/UPnPDA10_20000613.pdf.
Latest version available at: http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0.pdf.

[ISO 8601] – Data elements and interchange formats – Information interchange -- Representation of dates and times, International Standards Organization, December 21, 2000.
Available at: ISO 8601:2000.

[RFC 2119] – IETF RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, S. Bradner, March 1997.
Available at: http://tools.ietf.org/html/rfc2119.

[RFC 3986] – IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax, T. Berners-Lee, R. Fielding, L.Masinter, January 2005.
Available at: http://tools.ietf.org/html/rfc3986.

[RFC 3339] – IETF RFC 3339, Date and Time on the Internet: Timestamps, G. Klyne, Clearswift Corporation, C. Newman, Sun Microsystems, July 2002.
Available at: http://tools.ietf.org/html/rfc3339.

[XML] – Extensible Markup Language (XML) 1.0 (Third Edition), François Yergeau, Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler, eds., W3C Recommendation, February 4, 2004.
Available at: http://www.w3.org/TR/2004/REC-xml-20040204.

[XML SCHEMA-2] – XML Schema Part 2: Data Types, Second Edition, Paul V. Biron, Ashok Malhotra, W3C Recommendation, 28 October 2004.
Available at: http://www.w3.org/TR/2004/REC-xmlschema-2-20041028.

2.   Device Definitions

2.1.   Device Type

The following device type identifies a device that is compliant with this template:

urn:**schemas-upnp-org:device**:*InternetGatewayDevice:2*

2.2.   Device Model

Products that expose devices of the type **urn:schemas-upnp-org:device:***InternetGatewayDevice:2* MUST implement minimum version numbers of all required embedded devices and services specified in the table below.

Table 1: Device Requirements

DeviceType	Root	Req. or Opt.[1]	ServiceType	Req. or Opt.[1]	Service ID[2]
			Layer3Forwarding:1	*O*	*L3Forwarding1*
			DeviceProtection:1	*O*	*DeviceProtection1*
			Other standard UPnP devices and Services go here	*X*	*TBD*
			Non-standard services embedded by an UPnP vendor go here.	*X*	*TBD*
WANDevice:2		*R*	*WANCommonInterfaceConfig:1*	*R*	*WANCommonIFC1*
			Non-standard services embedded by an UPnP vendor go here.	*X*	*TBD*
WANConnectionDevice:2 (an instance of WANDevice may include one or more WANConnectionDevice instances)		*R*	*WANPOTSLinkConfig:1*	*O for POTS modems*	*WANPOTSLinkC1*
			WANDSLLinkConfig:1	*O for DSL modems*	*WANDSLLinkC1*
			WANCableLinkConfig:1	*O for Cable modems*	*WANCableLinkC1*
			WANEthernetLinkConfig:1	*O for Ethernet attached modems*	*WANEthLinkC1*
			WANPPPConnection:1	*R for modems that support PPP based connections*	*Multiple instances possible within a WANConnectionDevice. ServiceIDs for multiple instances will be*

					WANPPPConn1, WANPPPConn2, WANPPPConn3 and so on.
			WANIPConnection:2	*R for modems that support IPv4 based connections*	*Only 1 instance per WANConnectionDevice is envisioned at this time, although the design could support multiple instances in future. ServiceIDs for multiple instances will be WANIPConn1, WANIPConn2, WANIPConn3 and so on.*
			WANIPv6FirewallControl:1	*O for IPv6 enabled IGDs*	*Only 1 instance per WANIPv6FirewallControl is envisioned at this time, although the design could support multiple instances in future. ServiceIDs for multiple instances will be WANIPv6Firewall1, WANIPv6Firewall2, WANIPv6Firewall3 and so on.*
			Non-standard services embedded by an UPnP vendor go here.	*X*	*TBD*
LANDevice:1		*O*	*LANHostConfigManagement:1*	*O*	*LANHostCfg1*
Non-standard devices embedded by an UPnP vendor go here.	*TBD*	*X*	*TBD*	*TBD*	*TBD*

[1] R = Required, O = Optional, X = Non-standard.

[2] Prefixed by urn:**upnp-org**:**serviceId**: .

2.2.1. Description of Device Requirements

As shown in the table above, the DCP defines 3 Connection services (*WANIPConnection*, *WANPPPConnection* and *WANIPv6FirewallControl*) and 4 *LinkConfig* services to accommodate various types of WAN interfaces and connection types. In addition, it includes *DeviceProtection* service for managing access control. The following table briefly describes the purpose of each of the services. An actual implementation of the DCP will instance only those *Connection* and *LinkConfig* services that are appropriate for the gateway device being modeled.

Table 2: Service Descriptions

Service Name	Service Description
WANPPPConnection	PPP connections originating at the gateway or relayed or bridged through the gateway
WANIPConnection	IPv4 connections originating or relayed or bridged through the gateway
WANPOTSLinkConfig	Configuration parameters associated with a WAN link on a Plain Old Telephone Service (POTS) modem
WANDSLLinkConfig	Configuration parameters associated with a WAN link on a Digital Subscriber Link (DSL) modem
WANCableLinkConfig	Configuration parameters associated with a WAN link on a cable modem
WANEthernetLinkConfig	Configuration parameters associated with an Ethernet- attached external modem (cable or DSL). If proprietary mechanisms are available to discover and configure an external modem, it is RECOMMENDED that modem-specific *LinkConfig* services be modeled instead of this service.
WANIPv6FirewallControl	Allows controlling IPv6 firewall to open Pinholes
DeviceProtection	This service facilitates authentication and access control in the gateway device

2.2.2. Relationships Between Services

Layer3Forwarding identifies a default service, which is a specific instance of *WAN{PPP/IP}Connection* for IPv4 connections (or *WANIPv6FirewallControl* for IPv6 connections) in a *WANConnectionDevice*. *WANCommonInterfaceConfig* defines variables and actions common across all instances of *WAN{PPP/IP}Connection*s and *WANIPv6FirewallControl*s in a *WANDevice*. There may also be dependencies between a specific instance of *WAN*LinkConfig* (where * can be POTS, DSL, Cable or Ethernet) and *WAN**Connection* (where ** can be PPP or IP) or *WANIPv6FirewallControl* service in a *WANConnectionDevice*.

DeviceProtection is used to create trusted relationship between *InternetGatewayDevice* and a control point. If an action requires authentication and authorization, then this service is used to create the relationship and to verify that the relationship exists. Section 2.3 defines what actions can be used without authentication, and also what level of authorization is RECOMMENDED for the rest of the actions that require higher level of security.

2.3.   Security policies (Normative)

This section RECOMMENDS a set of default security policies for roles and for assigning roles to services and actions.

2.3.1. Access control and user roles

InternetGatewayDevice:2 that implements the *DeviceProtection* service implements following user roles as defined in [DeviceProtection]:

- *Public* REQUIRES neither authentication nor authorization. This user role is intended for applications making e.g. port mappings for themselves and do not require any other sort of configuration.

- *Basic* level REQUIRES authentication and authorization as specified in this document. Authentication is based on [DeviceProtection]. *Basic* role is intended for standard operation like creating port mappings for other devices or controlling on-demand connectivity. Usually, *Basic* role is assigned to actions making impact on single device's service. It is expected that when a new device is introduced, it is in IGD case automatically granted *Basic* access level.

- *Admin* access is intended for management of settings and risky actions that are not required in normal usage. It is RECOMMENDED that administration interface SHOULD REQUIRE additional security measures. This access level is RECOMMENDED, if the changes made impact to whole network's service or has impact to the several services. For instance, configuring DNS or DHCP settings would be a good example.

- *Vendor-defined* roles can be created, but it is REQUIRED that all other roles are implemented and supported. It is also REQUIRED that control points supporting three predefined roles are able to operate with the gateway. Role names MUST be maximum 64 characters long and MUST NOT contain spaces. Role names not defined by the Forum MUST be prefixed with a Vendor Domain Name followed by a colon (such as "example.com:"). Forum-defined Role names MUST be defined in service specifications and/or DCP-specific security considerations documents published by Working Committees.

This document RECOMMENDS the default access level to be applied for each action of the legacy services (version 1 and version 2). In other words, this document does NOT REQUIRE that a vendor MUST implement the access level defined in this document for each action of his *InternetGatewayDevice:2* implementation. As a result, vendors are allowed to implement different access control policies than defined in this document. For example, a vendor can decide to set a *Public* access level for opening port mappings with ports lower than or equal to 1023 instead of a *Basic* access level.

When new users / control points are introduced and authorized with IGD, they SHOULD be automatically granted *Basic* access role. *Admin* level SHOULD be granted as defined in [DeviceProtection].

2.3.2. General policies

It is REQUIRED that *InternetGatewayDevice:2* contains the newest version of each service. Therefore, earlier versions must not be used if newer version exists.

It is RECOMMENDED that *DeviceProtection* service is implemented and applied. If *DeviceProtection* service is not implemented and applied it is RECOMMENDED that control points are able to access only actions and parameters defined as *Public* role in this document (see Tables below).

UPnP IGD MUST expose UPnP services only over the LAN interface. IGD MUST reject UPnP requests from the WAN interfaces.

2.3.3. *WANIPConnection:2*

The following table lists the RECOMMENDED access levels for the actions in the *WANIPConnection:2* service.

Table 3: *WANIPConnection:2* Actions

Name	Access level	Description
SetConnectionType()	*Admin*	Impacts connectivity for all applications
GetConnectionTypeInfo()	*Public*	Allows retrieving information
RequestConnection()	*Basic*	Starting a connection is normal operation and should not require strict security, but *Basic* authentication is RECOMMENDED
RequestTermination()	*Admin*	Ending connection impacts connectivity for all applications
ForceTermination()	*Admin*	See previous
SetAutoDisconnectTime()	*Admin*	IGD configuration – not part of normal usage
SetIdleDisconnectTime()	*Admin*	IGD configuration – not part of normal usage
SetWarnDisconnectDelay()	*Admin*	IGD configuration – not part of normal usage
GetStatusInfo()	*Public*	Allows retrieving information – does not change operation
GetAutoDisconnectTime()	*Public*	Allows retrieving information – does not change operation
GetWarnDisconnectDelay()	*Public*	Allows retrieving information – does not change operation
GetNATRSIPStatus()	*Public*	Allows retrieving information – does not change operation
GetGenericPortMappingEntry()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows retrieving information on device's own port mappings when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows retrieving information on device's own port mappings when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box scenario *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box scenario *with* well-known ports

GetSpecificPortMappingEntry()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows retrieving information on device's own port mappings when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows retrieving information on device's own port mappings when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box scenario *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box scenario *with* well-known ports
AddPortMapping()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows setting port mappings for device itself when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows setting port mappings for device itself when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box case *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box case *with* well-known ports

DeletePortMapping()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows removing port mappings for device itself when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows removing port mappings for device itself when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box case *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box case *with* well-known ports
DeletePortMappingRange()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows removing device's port mappings for device itself when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows removing device's port mappings for device itself when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box case *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box case *with* well-known ports
GetExternalIPAddress()	*Public*	Allows retrieving WAN interface's IP address

GetListOfPortMappings()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows retrieving information on device's own port mappings when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows retrieving information on device's own port mappings when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box scenario *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box case *with* well-known ports
AddAnyPortmapping()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows setting port mappings for device itself when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows setting port mappings for device itself when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box case *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box case *with* well-known ports

2.3.4. *WANPPPConnection:1*

The following table lists the RECOMMENDED access levels for the actions in the *WANPPPConnection:1* service.

Table 4: *WANPPPConnection:1* Actions

Name	Access level	Description
GetConnectionTypeInfo()	*Public*	Allows retrieving information

SetConnectionType()	*Admin*	Impacts connectivity for all applications
GetConnectionTypeInfo()	*Public*	Allows retrieving information
RequestConnection()	*Basic*	Starting a connection is normal operation and should not require strict security, but *Basic* authentication is RECOMMENDED
RequestTermination()	*Admin*	Ending connection impacts connectivity for all applications
ForceTermination()	*Admin*	Ending connection impacts connectivity for all applications
SetAutoDisconnectTime()	*Admin*	IGD configuration – not part of normal usage
SetIdleDisconnectTime()	*Admin*	IGD configuration – not part of normal usage
SetWarnDisconnectDelay()	*Admin*	IGD configuration – not part of normal usage
GetStatusInfo()	*Public*	Allows retrieving information – does not change operation
GetAutoDisconnectTime()	*Public*	Allows retrieving information – does not change operation
GetWarnDisconnectDelay()	*Public*	Allows retrieving information – does not change operation
GetNATRSIPStatus()	*Public*	Allows retrieving information – does not change operation
GetGenericPortMappingEntry()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows retrieving information on device's own port mappings when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows retrieving information on device's own port mappings when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box scenario *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box scenario *with* well-known ports

GetSpecificPortMappingEntry()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows retrieving information on device's own port mappings when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows retrieving information on device's own port mappings when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box scenario *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box scenario *with* well-known ports
AddPortMapping()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows setting port mappings for device itself when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows setting port mappings for device itself when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box case *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box case *with* well-known ports

DeletePortMapping()	*Public* for CP's IP address and ports greater than or equal to 1024	Allows removing device's port mappings when ports *are not* well-known ports
	Basic for CP's IP address and ports lower than or equal to 1023	Allows removing device's port mappings when ports *are* well-known ports
	Basic for other IP addresses and ports greater than or equal to 1024	*Basic* level access is RECOMMENDED for 3-box case *without* well-known ports
	Admin for other IP addresses and ports lower than or equal to 1023	*Admin* level access is RECOMMENDED for 3-box case *with* well-known ports
GetExternalIPAddress()	*Public*	Allows retrieving WAN interface's IP address
RequestConnection()	*Basic*	Starting a connection is normal operation and should not require strict security, but *Basic* authentication is RECOMMENDED
ConfigureConnection()	*Admin*	Allows configuring password and user name for PPP – hence *Admin* level access is RECOMMENDED
GetLinkLayerMaxBitRates()	*Public*	Informational action, no security threat
GetPPPEncryptionProtocol()	*Public*	Informational action, limited security threat
GetPPPCompressionProtocol()	*Public*	Informational action
GetPPPAuthenticationProtocol()	*Public*	Informational action, limited security threat
GetUserName()	*Admin*	User names should not be accessed via UPnP, serious security threat
GetPassword()	*Admin*	User names should not be accessed via UPnP, serious security threat

Vendors, ISP, or users MAY disable *GetPassword()* and *GetUsername()* actions, if so desired. This would be recommendable for added security.

2.3.5. *WANIPv6FirewallControl:1*

The following table lists the RECOMMENDED access levels for the actions in the *WANIPv6FirewallControl:1* service.

Table 5: *WANIPv6FirewallControl:1* Actions

Name	Access level	Description
GetFirewallStatus()	*Public*	This allows knowing if the firewall is active and if pinholes can be made through UPnP
AddPinhole()	*Basic* for a non-wildcarded *InternalPort*	*Basic* level access is RECOMMENDED to create any firewall pinholes as firewall control impacts the security of the local network
	Admin for a wildcarded *InternalPort*	*Admin* level access is RECOMMENDED to open a firewall pinhole with a wildcarded *InternalPort* as the pinhole created by this action could enable port scans for the specified destination address
UpdatePinhole()	*Basic* for a non-wildcarded *InternalPort*	*Basic* level access is RECOMMENDED to update any firewall pinholes as firewall control impacts the security of the local network
	Admin for a wildcarded *InternalPort*	*Admin* level access is RECOMMENDED to update a firewall pinhole with a wildcarded *InternalPort* as the pinhole updated by this action could enable port scans for the specified destination address
DeletePinhole()	*Basic* for a non-wildcarded *InternalPort*	*Basic* level access is RECOMMENDED to delete any firewall pinholes as firewall control impacts the security of the local network
	Admin for a wildcarded *InternalPort*	*Admin* level access is RECOMMENDED to delete a firewall pinhole with a wildcarded *InternalPort* as this level access is RECOMMENDED to create this type of pinhole
CheckPinholeWorking()	*Basic* for a non-wildcarded *InternalPort*	*Basic* level access is RECOMMENDED to check that a firewall pinhole is working as firewall control impacts the security of the local network
	Admin for a wildcarded *InternalPort*	*Admin* level access is RECOMMENDED to check that a firewall pinhole with a wildcarded *InternalPort* is working as this level access is RECOMMENDED to create this type of pinhole
GetOutboundPinholeTimeout()	*Public*	Information retrieval to allow CP's to know automatic pinhole expiration time

2.3.6. *LANHostConfigManagement:1*

LANHostConfigManagement:1 is risky service that should be implemented with minimal features and potentially also be disabled in normal operation, as it is not needed for typical IP configuration. Also it is RECOMMENDED that maximum level of security would be applied.

The following table lists the RECOMMENDED access levels for the actions in the *LANHostConfigManagement:1* service.

Table 6: *LANHostConfigManagement:1* Actions

Name	Access level	Description
SetDHCPServerConfigurable()	*Admin*	Allows enabling, disabling DHCP configuration – impacts to basic settings of the network -> *Admin*
GetDHCPServerConfigurable()	*Public*	Allows knowing if DHCP server can be configured over UPnP -> *Public*
SetDHCPRelay()	*Admin*	Allows enabling DHCP relay service, Impacts basic settings of the network-> *Admin*
GetDHCPRelay()	*Public*	Allows knowing if DHCP relay service is active or not. Informational action -> *Public*
SetSubnetMask()	*Admin*	Sets used subnet mask - > impacts basic setting of a network -> *Admin*
GetSubnetMask()	*Public*	Informational action -> *Public*
SetIPRouter()	*Admin*	Allows setting routers information in DHCP – impacts the network -> *Admin*
DeleteIPRouter()	*Admin*	Allows deleting a router's information in DHCP – impacts the network -> *Admin*
GetIPRoutersList()	*Public*	Allows getting information of current routers. Informational action, no serious threats as the information is provided by DHCP -> *Public*
SetDomainName()	*Admin*	Impacts basic network settings -> *Admin*
GetDomainName()	*Public*	Information provided also by DHCP and this is informational action -> *Public*
SetAddressRange()	*Admin*	This does impact basic settings of the network -> *Admin*
GetAddressRange()	*Public*	Informational action->*Public*
SetReservedAddress()	*Admin*	Allows setting addresses that are not distributed by DHCP. Impacts basic network settings -> *Admin*
DeleteReservedAddress()	*Admin*	Allows removing addresses the list of reserved addresses that are not distributed by DHCP. Impacts basic network settings -> *Admin*
GetReservedAddresses()	*Admin*	DHCP specific configuration -> *Admin*
SetDNSServer()	*Admin*	Impacts basic settings of the network->*Admin*
DeleteDNSServer()	*Admin*	Impacts basic settings of the network->*Admin*
GetDNSServers()	*Public*	Information distributed by DHCP -> *Public*

2.3.7. *Layer3Forwarding:1*

The following table lists the RECOMMENDED access levels for the actions in the *Layer3Forwarding:1* service.

Table 7: *Layer3Forwarding:1* Actions

Name	Access level	Description
SetDefaultConnectionService()	*Admin*	Impacts basic settings of the network->*Admin*
GetDefaultConnectionService()	*Public*	Informational action ->*Public*

2.3.8. *WANEthernetLinkConfig:1*

The following table lists the RECOMMENDED access levels for the actions in the *WANEthernetLinkConfig:1* service.

© 2010 UPnP Forum. All rights reserved.

Table 8: *WANEthernetLinkConfig:1* Actions

Name	Access level	Description
GetEthernetLinkStatus()	*Public*	Informational action ->*Public*

2.3.9. *WANCableLinkConfig:1*

The following table lists the RECOMMENDED access levels for the actions in the *WANCableLinkConfig:1* service.

Table 9: *WANCableLinkConfig:1* Actions

Name	Access level	Description
GetCableLinkConfigInfo()	*Public*	Informational action ->*Public*
GetDownstreamFrequency()	*Public*	Informational action ->*Public*
GetDownstreamModulation()	*Public*	Informational action ->*Public*
GetUpstreamFrequency()	*Public*	Informational action ->*Public*
GetUpstreamModulation()	*Public*	Informational action ->*Public*
GetUpstreamChannelID()	*Public*	Informational action ->*Public*
GetUpstreamPowerLevel()	*Public*	Informational action ->*Public*
GetBPIEncryptionEnabled()	*Public*	Informational action ->*Public*
GetConfigFile()	*Public*	Informational action ->*Public*
GetTFTPServer()	*Public*	Informational action ->*Public*

2.3.10. *WANDSLLinkConfig:1*

The following table lists the RECOMMENDED access levels for the actions in the *WANDSLLinkConfig:1* service.

Table 10: *WANDSLLinkConfig:1* Actions

Name	Access level	Description
SetDSLLinkType()	*Admin*	Impact network connectivity -> *Admin*
GetDSLLinkInfo()	*Public*	Informational action ->*Public*
GetAutoConfig()	*Public*	Informational action ->*Public*
GetModulationType()	*Public*	Informational action ->*Public*
SetDestinationAddress()	*Admin*	Impacts network connectivity -> *Admin*
GetDestinationAddress()	*Public*	Informational action ->*Public*
SetATMEncapsulation()	*Admin*	Impacts network connectivity -> *Admin*
GetATMEncapsulation()	*Public*	Informational action ->*Public*
SetFCSPreserved()	*Admin*	Impacts network connectivity -> *Admin*
GetFCSPreserved()	*Public*	Informational action ->*Public*

2.3.11. *WANCommonInterfaceConfig:1*

The following table lists the RECOMMENDED access levels for the actions in the *WANCommonInterfaceConfig:1* service.

Table 11: *WANCommonInterfaceConfig:1* Actions

Name	Access level	Description
SetEnabledForInternet()	*Admin*	Enables / disables network connectivity to Internet -> *Admin*
GetEnabledForInternet()	*Public*	Informational action ->*Public*
GetCommonLinkProperties()	*Public*	Informational action ->*Public*
GetWANAccessProvider()	*Public*	Informational action ->*Public*
GetMaximumActiveConnections()	*Public*	Informational action ->*Public*
GetTotalBytesSent()	*Public*	Informational action ->*Public*
GetTotalBytesReceived()	*Public*	Informational action ->*Public*
GetTotalPacketsSent()	*Public*	Informational action ->*Public*
GetTotalPacketsReceived()	*Public*	Informational action ->*Public*
GetActiveConnection()	*Public*	Informational action ->*Public*

2.3.12. *WANPOTSLinkConfig:1*

The following table lists the RECOMMENDED access levels for the actions in the *WANPOTSLinkConfig:1* service.

Table 12: *WANPOTSLinkConfig:1* Actions

Name	Access level	Description
SetISPInfo()	*Admin*	Impacts network connectivity -> *Admin*
SetCallRetryInfo()	*Admin*	Impacts network connectivity -> *Admin*
GetISPInfo()	*Public*	Informational action ->*Public*
GetCallRetryInfo()	*Public*	Informational action ->*Public*
GetFclass()	*Public*	Informational action ->*Public*
GetDataModulationSupported()	*Public*	Informational action ->*Public*
GetDataProtocol()	*Public*	Informational action ->*Public*
GetDataCompression()	*Public*	Informational action ->*Public*
GetPlusVTRCommandSupported()	*Public*	Informational action ->*Public*

2.4.   Theory of Operation

Each *WANDevice* in Figure 1 can be viewed as an instantiation of a physical WAN interface. If an *InternetGatewayDevice* provides multiple WAN physical interfaces to UPnP clients, each of these will typically be included in the device description document as distinct *WANDevice* instances. However, an implementation may choose to encapsulate more than one physical WAN interface in a single *WANDevice*. This may be done, for example, in applications that use asymmetric connections like a satellite downlink and POTS uplink. Another example would be where multiple physical WAN interfaces are pooled and presented as one device. Aspects such as load balancing between the pooled resources would be transparent to UPnP clients in this case.

All Internet connections are set up from or through a WAN interface of the *InternetGatewayDevice* to Internet Service Providers (ISPs). *WANDevice* is a container for all UPnP services associated with a physical WAN device. It is assumed that clients are connected to *InternetGatewayDevice* via a LAN (IP-based network). Each link on a WAN interface is modeled by an instance of *WANConnectionDevice* in *WANDevice*. A *WANConnectionDevice* in turn contains one link-specific *WAN*LinkConfig*[1] service (where * can be POTS, DSL, Cable or Ethernet) and one

---

[1] The WC has not defined link configuration services for interfaces types other than those listed above. If needed, these can be implemented as vendor-proprietary extensions.

or more instances of *WAN**Connection* service (where ** can be PPP or IP) for IPv4 connections (or *WANIPv6FirewallControl* service for IPv6 connections).

A *WANDevice* provides a *WANCommonInterfaceConfig* service that encapsulates Layer 1 and Layer 2 properties relevant to Internet access common to the specific WAN access type and across multiple *WAN**Connection* (and *WANIPv6FirewallControl*) service instances.

The gateway device may also support multiple physical LAN interfaces. It may support distinct subnets of client nodes on the residential network. Each *LANDevice* – identified in the device description document with a UDN – typically corresponds to a physical LAN interface (or port) on the *InternetGatewayDevice*. However, an implementation may choose to encapsulate more than one physical LAN interface in a single *LANDevice*. This would be the case if two LAN subnets that are bridged are to be presented as a single logical LAN interface. Devices on a LAN may configure, initiate and/or share Internet connections.

The *InternetGatewayDevice* may also support Layer-3 packet transformation and forwarding functions managed and applicable across all connection instances. These functions are currently modeled in *Layer3Forwarding* service. Layer-3 packet forwarding functions that are specific to a connection will be modeled in each *WAN**Connection* (or *WANIPv6FirewallControl*) service instance.

3.   XML Device Description

```xml
<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
  <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  <URLBase>base URL for all relative URLs</URLBase>
  <device>
    <deviceType>urn:schemas-upnp-
org:device:InternetGatewayDevice:2</deviceType>
    <friendlyName>short user-friendly title</friendlyName>
    <manufacturer>manufacturer name</manufacturer>
    <manufacturerURL>URL to manufacturer site</manufacturerURL>
    <modelDescription>long user-friendly title</modelDescription>
    <modelName>model name</modelName>
    <modelNumber>model number</modelNumber>
    <modelURL>URL to model site</modelURL>
    <serialNumber>manufacturer's serial number</serialNumber>
    <UDN>uuid:UUID</UDN>
    <UPC>Universal Product Code</UPC>
    <iconList>
      <icon>
        <mimetype>image/format</mimetype>
        <width>horizontal pixels</width>
        <height>vertical pixels</height>
        <depth>color depth</depth>
        <url>URL to icon</url>
      </icon>
      <!-- XML to declare other icons, if any, go here -->
    </iconList>
    <serviceList>
      <service>
        <serviceType>urn:schemas-upnp-
org:service:Layer3Forwarding:1</serviceType>
        <serviceId>urn:upnp-org:serviceId:L3Forwarding1</serviceId>
        <SCPDURL>URL to service description</SCPDURL>
        <controlURL>URL for control</controlURL>
        <eventSubURL>URL for eventing</eventSubURL>
      </service>
      <service>
        <serviceType>urn:schemas-upnp-
org:service:DeviceProtection:1</serviceType>
        <serviceId>urn:upnp-org:serviceId:DeviceProtection1</serviceId>
        <SCPDURL>URL to service description</SCPDURL>
        <controlURL>URL for control</controlURL>
        <eventSubURL>URL for eventing</eventSubURL>
      </service>
      <!-- Declarations for other services added by UPnP vendor (if any) go
here -->
    </serviceList>
    <deviceList>
      <device>
        <deviceType>urn:schemas-upnp-org:device:WANDevice:2</deviceType>
```

```xml
        <friendlyName>short user-friendly title</friendlyName>
        <manufacturer>manufacturer name</manufacturer>
        <manufacturerURL>URL to manufacturer site</manufacturerURL>
        <modelDescription>long user-friendly title</modelDescription>
        <modelName>model name</modelName>
        <modelNumber>model number</modelNumber>
        <modelURL>URL to model site</modelURL>
        <serialNumber>manufacturer's serial number</serialNumber>
        <UDN>uuid:UUID</UDN>
        <UPC>Universal Product Code</UPC>
        <iconList>
          <icon>
            <mimetype>image/format</mimetype>
            <width>horizontal pixels</width>
            <height>vertical pixels</height>
            <depth>color depth</depth>
            <url>URL to icon</url>
          </icon>
          <!-- XML to declare other icons, if any, go here -->
        </iconList>
        <serviceList>
          <service>
            <serviceType>urn:schemas-upnp-
org:service:WANCommonInterfaceConfig:1</serviceType>
            <serviceId>urn:upnp-org:serviceId:WANCommonIFC1</serviceId>
            <SCPDURL>URL to service description</SCPDURL>
            <controlURL>URL for control</controlURL>
            <eventSubURL>URL for eventing</eventSubURL>
          </service>
          <!-- Declarations for other services added by UPnP vendor (if any)
go here -->
        </serviceList>
        <deviceList>
          <device>
            <deviceType>urn:schemas-upnp-
org:device:WANConnectionDevice:2</deviceType>
            <friendlyName>short user-friendly title</friendlyName>
            <manufacturer>manufacturer name</manufacturer>
            <manufacturerURL>URL to manufacturer site</manufacturerURL>
            <modelDescription>long user-friendly title</modelDescription>
            <modelName>model name</modelName>
            <modelNumber>model number</modelNumber>
            <modelURL>URL to model site</modelURL>
            <serialNumber>manufacturer's serial number</serialNumber>
            <UDN>uuid:UUID</UDN>
            <UPC>Universal Product Code</UPC>
            <iconList>
              <icon>
                <mimetype>image/format</mimetype>
                <width>horizontal pixels</width>
                <height>vertical pixels</height>
                <depth>color depth</depth>
                <url>URL to icon</url>
              </icon>
              <!-- XML to declare other icons, if any, go here -->
            </iconList>
```

```xml
        <serviceList>
          <service>
            <serviceType>urn:schemas-upnp-
org:service:WANDSLLinkConfig²:1</serviceType>
            <serviceId>urn:upnp-org:serviceId:WANDSLLinkC1</serviceId>
            <SCPDURL>URL to service description</SCPDURL>
            <controlURL>URL for control</controlURL>
            <eventSubURL>URL for eventing</eventSubURL>
          </service>
          <service>
            <serviceType>urn:schemas-upnp-
org:service:WANIPConnection³:2</serviceType>
            <serviceId>urn:upnp-org:serviceId:WANIPConn1</serviceId>
            <SCPDURL>URL to service description</SCPDURL>
            <controlURL>URL for control</controlURL>
            <eventSubURL>URL for eventing</eventSubURL>
          </service>
          <!-- Declarations for other services added by UPnP vendor (if
any) go here -->
        </serviceList>
        <deviceList>
          <!-- Description of embedded devices added by UPnP vendor (if
any) go here -->
        </deviceList>
        <presentationURL>URL for presentation</presentationURL>
      </device>
    </deviceList>
    <presentationURL>URL for presentation</presentationURL>
  </device>
  <device>
    <deviceType>urn:schemas-upnp-org:device:LANDevice:1</deviceType>
    <friendlyName>short user-friendly title</friendlyName>
    <manufacturer>manufacturer name</manufacturer>
    <manufacturerURL>URL to manufacturer site</manufacturerURL>
    <modelDescription>long user-friendly title</modelDescription>
    <modelName>model name</modelName>
    <modelNumber>model number</modelNumber>
    <modelURL>URL to model site</modelURL>
    <serialNumber>manufacturer's serial number</serialNumber>
    <UDN>uuid:UUID</UDN>
    <UPC>Universal Product Code</UPC>
    <iconList>
      <icon>
        <mimetype>image/format</mimetype>
        <width>horizontal pixels</width>
        <height>vertical pixels</height>
        <depth>color depth</depth>
        <url>URL to icon</url>
      </icon>
```

---

[2] NOTE to implementers: This template is representative of one device type – a DSL modem in this case. Depending on the type of modem, substitute or add device specific service names.

[3] NOTE to implementers: This template is representative of one connection type –IP in this case. Depending on the type of connection, substitute or add device specific service names.

```xml
            <!-- XML to declare other icons, if any, go here -->
          </iconList>
          <serviceList>
            <service>
              <serviceType>urn:schemas-upnp-
org:service:LANHostConfigManagement:1</serviceType>
              <serviceId>urn:upnp-org:serviceId:LANHostCfg1</serviceId>
              <SCPDURL>URL to service description</SCPDURL>
              <controlURL>URL for control</controlURL>
              <eventSubURL>URL for eventing</eventSubURL>
            </service>
            <!-- Declarations for other services added by UPnP vendor (if any)
go here -->
          </serviceList>
          <deviceList>
            <!-- Description of embedded devices added by UPnP vendor (if any)
go here -->
          </deviceList>
          <presentationURL>URL for presentation</presentationURL>
        </device>
        <!-- Description of embedded devices added by UPnP vendor (if any) go
here -->
      </deviceList>
      <presentationURL>URL for presentation</presentationURL>
    </device>
</root>
```

4.   Test

No semantic tests are defined for this device.