TECHNICAL REPORT

TR-98

Internet Gateway Device Data Model for TR-069

Issue: 1.1
Issue Date: November 2006

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This document is not binding on the Broadband Forum, any of its members, or any developer or service provider. This document is subject to change, but only with approval of members of the Forum.

This document is provided "as is," with all faults. Any person holding a copyright in this document, or any portion thereof, disclaims to the fullest extent permitted by law any representation or warranty, express or implied, including, but not limited to,
(a) any warranty of merchantability, fitness for a particular purpose, non-infringement, or title;
(b) any warranty that the contents of the document are suitable for any purpose, even if that purpose is known to the copyright holder;
(c) any warranty that the implementation of the contents of the documentation will not infringe any third party patents, copyrights, trademarks or other rights.

This publication may incorporate intellectual property. The Broadband Forum encourages but does not require declaration of such intellectual property. For a list of declarations made by Broadband Forum member companies, please see www.broadband-forum.org.

Version History

Version Number	Version Date	Version Editor	Changes
Issue 1	September 2005	Jeff Bernstein, 2Wire Barbara Stark, BellSouth	Issue 1
Issue 1 Amendment 1	November 2006	Jeff Bernstein, 2Wire John Blackford, 2Wire Mike Digdon, SupportSoft Heather Kirksey, Motive William Lupton, 2Wire Anton Okmianski, Cisco	Clarification of original document

Technical comments or questions about this document should be directed to:

Editor:	Jeff Bernstein	2Wire
	Barbara Stark	BellSouth
	John Blackford	2Wire
	Mike Digdon	SupportSoft
	Heather Kirksey	Motive
	William Lupton	2Wire
	Anton Okmianski	Cisco
WG Chairs	Greg Bathrick	PMC Sierra
	Heather Kirksey	Motive

Abstract:

Defines the Internet Gateway Device data model for the CPE WAN Management Protocol (TR-069).

Contents

1 Introduction

This document describes the Internet Gateway Device data model for the CPE WAN Management Protocol (TR-069). TR-069 defines the generic requirements of the management protocol methods which can be applied to any TR-069 CPE. It is intended to support a variety of different functionalities to manage a collection of CPE, including the following primary capabilities:

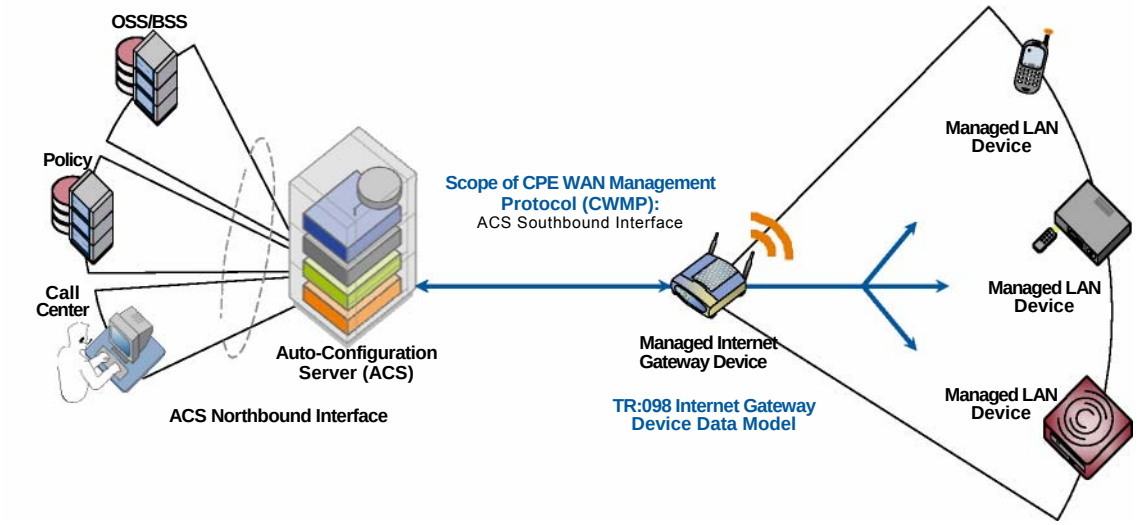
- Auto-configuration and dynamic service provisioning
- Software/firmware image management
- Status and performance monitoring
- Diagnostics

If TR-069 defines the generic methods for any device, other documents (such as this one) specify the managed objects, or data models, on which the generic methods act to configure, diagnose, and monitor the state of specific devices and services.

The following figure places TR-069 and this document in the end-to-end management architecture:

The ACS is a server that resides in the network and manages devices in the subscriber premises. It uses the methods, or RPCs, defined to TR-069 to get and set the state of the device, initiate diagnostic tests, download and upload files, and manage events. This document defines those objects applicable to management of an Internet Gateway Device delivering broadband service.

Figure 1 – Positioning in the End-to-End Architecture



The Internet Gateway Device data model follows the conventions defined in [3] for versioning of data models and the use of profiles.

1.1 Terminology

The following terminology is used throughout the series of documents defining the CPE WAN Management Protocol.

ACS	Auto-Configuration Server. This is a component in the broadband network responsible for auto-configuration of the CPE for advanced services.
B-NT	Broadband-Network Termination. A specific type of Broadband CPE used in DSL networks.
CPE	Customer Premises Equipment; refers to any TR-069-compliant device and therefore covers both Internet Gateway Devices and LAN-side end devices.
CWMP	CPE WAN Management Protocol. Defined in [2], CWMP is a communication protocol between an ACS and CPE that defines a mechanism for secure auto-configuration of a CPE and other CPe management functions in a common framework.
Data Model	A hierarchical set of Parameters that define the managed objects accessible via TR-069

for a particular device or service.

Device	Used interchangeably with CPE.
Event	An indication that something of interest has happened that requires the CPE to notify the ACS.
Internet Gateway Device	A CPE device, typically a broadband router, that acts as a gateway between the WAN and the LAN.
Parameter	A name-value pair representing a manageable CPE parameter made accessible to an ACS for reading and/or writing.
RPC	Remote Procedure Call.

1.2 Document Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

The key words “DEPRECATED” and “OBSOLETED” in this document are to be interpreted as defined in [3].

2 Data Model Definition

2.1 General Notation

Parameter names use a hierarchical form similar to a directory tree. The name of a particular Parameter is represented by the concatenation of each successive node in the hierarchy separated with a “.” (dot), starting at the trunk of the hierarchy and leading to the leaves. When specifying a partial path, indicating an intermediate node in the hierarchy, the trailing “.” (dot) is always used as the last character.

Parameter names MUST be treated as case sensitive.

In some cases, where multiple instances of an object can occur, the placeholder node name “{i}” is shown. In actual use, this placeholder is to be replaced by an instance number, which MUST be a positive integer (≥ 1). Because in some cases object instances can be deleted, instance numbers will in general not be contiguous.

2.2 Data Types

The parameters defined in this specification make use of a limited subset of the default SOAP data types [4]. The complete set of parameter data types along with the notation used to represent these types is listed in Table 1.

Table 1 – Data types

Type	Description
object	A container for parameters and/or other objects. The full path name of a parameter is given by the parameter name appended to the full path name of the object it is contained within.

Type	Description
string	For strings listed in this specification, a maximum allowed length can be listed using the form string(N), where N is the maximum string length in characters. For all strings a maximum length is either explicitly indicated or implied by the size of the elements composing the string. For strings in which the content is an enumeration, the longest enumerated value determines the maximum length. If a string does not have an explicitly indicated maximum length or is not an enumeration, the default maximum is 16 characters.
int	Integer in the range –2147483648 to +2147483647, inclusive. For some int types listed, a value range is given using the form int[Min:Max], where the Min and Max values are inclusive. If either Min or Max are missing, this indicates no limit.
unsignedInt	Unsigned integer in the range 0 to 4294967295, inclusive. For some unsignedInt types listed, a value range is given using the form unsignedInt[Min:Max], where the Min and Max values are inclusive. If either Min or Max are missing, this indicates no limit.
boolean	Boolean, where the allowed values are “0”, “1”, “true”, and “false”. The values “1” and “true” are considered interchangeable, where both equivalently represent the logical value *true.* Similarly, the values “0” and “false” are considered interchangeable, where both equivalently represent the logical value *false.*
dateTime	The subset of the ISO 8601 date-time format defined by the SOAP dateTime type. All times MUST be expressed in UTC (Universal Coordinated Time) unless explicitly stated otherwise in the definition of a parameter of this type. If absolute time is not available to the CPE, it SHOULD instead indicate the relative time since boot, where the boot time is assumed to be the beginning of the first day of January of year 1, or 0001-01 -01T00:00:00. For example, 2 days, 3 hours, 4 minutes and 5 seconds since boot would be expressed as 0001-01-03T03:04:05. Relative time since boot MUST be expressed using an untimezoned representation. Any untimezoned value with a year value less than 1000 MUST be interpreted as a relative time since boot. If the time is unknown or not applicable, the following value representing “Unknown Time” MUST be used: 0001-01 -01T00:00:00Z. Any dateTime value other than one expressing relative time since boot (as described above) MUST use timezoned representation (that is, it MUST include a timezone suffix).
base64	Base64 encoded binary. A maximum allowed length can be listed using the form base64(N), where N is the maximum length in characters after Base64 encoding.

All IP addresses and subnet masks are represented as strings in IPv4 dotted-decimal notation. Note that there is no IPv6 support at this time in the parameter list described in this specification. Unspecified or inapplicable IP addresses and subnet masks MUST be represented as empty strings unless otherwise specified by the parameter definition.

All MAC addresses are represented as strings of 12 hexadecimal digits (digits 0-9, letters A-F or a-f) displayed as six pairs of digits separated by colons. Unspecified or inapplicable MAC addresses MUST be represented as empty strings unless otherwise specified by the parameter definition.

For unsignedInt parameters that are used for statistics, e.g. for byte counters, the actual value of the statistic might be greater than the maximum value that can be represented as an unsignedInt. Such values SHOULD wrap around through zero.

For strings that are defined to contain comma-separated lists, the format is defined as follows. Between every pair of successive items in a comma-separated list there MUST be a separator. The separator MUST include exactly one comma character, and MAY also include one or more space characters before or after the comma. The entire separator, including any space characters, MUST NOT be considered part of the list items it separates. The last item in a comma-separated list MUST NOT be followed with a separator. Individual items in a comma-separated list MUST NOT include a space or comma character within them. If an item definition requires the use of spaces or commas, that definition MUST specify the use of an escape mechanism that prevents the use of these characters.

For string parameters whose value is defined to contain the full hierarchical name of an object, the representation of the object name MUST NOT include a trailing “dot.” An example of a parameter of this

kind in the InternetGatewayDevice data model is InternetGatewayDevice.Layer3Forwarding.Default-ConnectionService. For this parameter, the following is an example of a properly formed value:

InternetGatewayDevice.WANDevice. 1 .WANConnectionDevice.2.WANPPPConnection. 1

2.3 Vendor-Specific Parameters

A vendor MAY extend the standardized parameter list with vendor-specific parameters and objects. Vendor-specific parameters and objects MAY be defined either in a separate naming hierarchy or within the standardized naming hierarchy.

The name of a vendor-specific parameter or object not contained within another vendor-specific object MUST have the form:

X_<VENDOR>_VendorSpecificName

In this definition <VENDOR> is a unique vendor identifier, which MAY be either an OUI or a domain name. The OUI or domain name used for a given vendor-specific parameter MUST be one that is assigned to the organization that defined this parameter (which is not necessarily the same as the vendor of the CPE or ACS). An OUI is an organizationally unique identifier as defined in [5], which MUST formatted as a six-hexadecimal-digit string using all upper-case letters and including any leading zeros. A domain name MUST be upper case with each dot (".") replaced with a hyphen or underscore.

The VendorSpecificName MUST be a valid string as defined in 2.2, and MUST NOT contain a "." (period) or a space character.

Note – the use of the string "X_" to indicate a vendor-specific parameter implies that no standardized parameter can begin with "X_".

The name of a vendor-specific parameter or object that is contained within another vendor-specific object which itself begins with the prefix described above need not itself include the prefix.

The full path name of a vendor-specific parameter or object MUST NOT exceed 256 characters in length.

Below are some example vendor-specific parameter and object names:

InternetGatewayDevice.UserInterface.X_01 2345_AdBanner

InternetGatewayDevice.LANDevice. 1 .X_01 2345_LANInfraredInterfaceConfig.2.Status

X_GAMECO-COM_GameDevice.Info.Type

When appropriate, a vendor MAY also extend the set of values of an enumeration. If this is done, the vendor-specified values MUST be in the form "X_<VENDOR>_VendorSpecificValue". The total length of such a string MUST NOT exceed 31 characters.

2.4 InternetGatewayDevice Data Model

Table 2 defines version 1.2 of the InternetGatewayDevice data model. This definition is a superset of previously defined versions, 1.1 and 1.0. The table lists the objects defined for an Internet Gateway Device, and the corresponding parameters within those objects.

For a given implementation of this data model, the CPE MUST indicate support for the highest version number of any object or parameter that it supports. For example, even if the CPE supports only a single parameter that was introduced in version 1.2, then it would have to indicate support for version 1.2. The version number associated with each object and parameter is shown in the Version column of Table 2.

Table 2 – Definition of InternetGatewayDevice:1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.	object	-	The top-level object for an Internet Gateway Device.	-	1.0
DeviceSummary	string(1024)	-	As defined in [3].	-	1.1
LANDeviceNumberOfEntries	unsignedInt	-	Number of instances of LANDevice.	-	1.0
WANDeviceNumberOfEntries	unsignedInt	-	Number of instances of WANDevice.	-	1.0
InternetGatewayDevice.DeviceInfo.	object	-	This object contains general device information.	-	1.0
Manufacturer	string(64)	-	The manufacturer of the CPE (human readable string).	-	1.0
ManufacturerOUI	string(6)	-	Organizationally unique identifier of the device manufacturer. Represented as a six hexadecimal-digit value using all upper-case letters and including any leading zeros. The value MUST be a valid OUI as defined in [5].	-	1.0
ModelName	string(64)	-	Model name of the CPE (human readable string).	-	1.0
Description	string(256)	-	A full description of the CPE device (human readable string).	-	1.0
ProductClass	string(64)	-	Identifier of the class of product for which the serial number applies. That is, for a given manufacturer, this parameter is used to identify the product or class of product over which the SerialNumber parameter is unique.	-	1.0
SerialNumber	string(64)	-	Serial number of the CPE.	-	1.0
HardwareVersion	string(64)	-	A string identifying the particular CPE model and version.	-	1.0
SoftwareVersion	string(64)	-	A string identifying the software version currently installed in the CPE. To allow version comparisons, this element SHOULD be in the form of dot-delimited integers, where each successive integer represents a more minor category of variation. For example, 3.0.21where the components mean: Major.Minor.Build.	-	1.0

1 The full name of a Parameter is the concatenation of the object name shown in the yellow header with the individual Parameter name.

2 "W" indicates the parameter MAY be writable (if "W" is not present, the parameter is defined as read-only). For an object, "W" indicates object instances can be Added or Deleted.

3 The default value of the parameter on creation of an object instance via TR-069. If the default value is an empty string, this is represented by the symbol <Empty>. A hyphen indicates that no default value is specified. For a parameter in which no default value is specified, on creation of a parent object instance, the CPE MUST set the parameter to a value that is valid according to the definition of that parameter.

4 The Version column indicates the minimum data-model version required to support the associated Parameter or Object.

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
ModemFirmwareVersion	string(64)	-	A string identifying the version of the modem firmware currently installed in the CPE. This is applicable only when the modem firmware is separable from the overall CPE software.	-	1.0
EnabledOptions	string(1024)	-	Comma-separated list of the OptionName of each Option that is currently enabled in the CPE. The OptionName of each is identical to the Option Name element of the OptionStruct described in [2]. Only those options are listed whose State indicates the option is enabled.	-	1.0
AdditionalHardwareVersion	string(64)	-	A comma separated list of any additional versions. Represents any additional hardware version information the vendor might wish to supply.	-	1.0
AdditionalSoftwareVersion	string(64)	-	A comma separated list of any additional versions. Represents any additional software version information the vendor might wish to supply.	-	1.0
SpecVersion	string(16)	-	Represents the version of the specification implemented by the device. Currently 1.0 is the only available version. The value of this parameter MUST equal “1.0”. This parameter is DEPRECATED because its value is fixed and it therefore serves no purpose. However, it is a Forced Inform parameter and therefore cannot be OBSOLETED.	“1.0”	1.0
Provision ingCode	string(64)	W	Identifier of the primary service provider and other provisioning information, which MAY be used by the ACS to determine service provider-specific customization and provisioning parameters. If non-empty, this argument SHOULD be in the form of a hierarchical descriptor with one or more nodes specified. Each node in the hierarchy is represented as a 4-character sub-string, containing only numerals or upper-case letters. If there is more than one node indicated, each node is separated by a "." (dot). Examples: “TLCO” or “TLCO.GRP2”.	-	1.0
UpTime	unsignedInt	-	Time in seconds since the CPE was last restarted.	-	1.0
FirstUseDate	dateTime	-	Date and time in UTC that the CPE first both successfully established an IP-layer network connection and acquired an absolute time reference using NTP or equivalent over that network connection. The CPE MAY reset this date after a factory reset. If NTP or equivalent is not available, this parameter, if present, SHOULD be set to the Unknown Time value.	-	1.0
DeviceLog	string(32K)	-	Vendor-specific log(s).	-	1.0
VendorConfigFileNumberOfEntries	unsignedInt	-	Number of instances of VendorConfigFile.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.DeviceInfo.Vendor-ConfigFile.{i}.	object	-	Every instance of this object is a Vendor Configuration File, and contains parameters associated with the Vendor Configuration File. This table of Vendor Configuration Files is for information only and does not allow the ACS to operate on these files in any way. Whenever the CPE successfully downloads a configuration file as a result of the Download RPC with the FileType argument of "3 Vendor Configuration File", the CPE MUST update this table. If the name of the file (determined as described in the definition of the Name parameter) differs from that of any existing instance, then the CPE MUST create a new instance to represent this file. If instead, the name of the file is identical to that of an existing instance, then the CPE MUST update the content of the existing instance with the new version, date, and (optionally) description of the file.	-	1.0
Name	string(64)	-	Name of the vendor configuration file. If the CPE is able to obtain the name of the configuration file from the file itself, then the value of this parameter MUST be set to that name. Otherwise, if the CPE can extract the file name from the URL used to download the configuration file, then the value of this parameter MUST be set to that name. Otherwise, the value of this parameter MUST be set to the value of the TargetFileName argument of the Download RPC used to download this configuration file.	-	1.0
Version	string(16)	-	A string identifying the configuration file version currently used in the CPE. If the CPE is able to obtain the version of the configuration file from the file itself, then the value of this parameter MUST be set to the obtained value. Otherwise, the value of this parameter MUST be empty.	-	1.0
Date	dateTime	-	Date and time when the content of the current version of this vendor configuration file was first applied by the CPE.	-	1.0
Description	string(256)	-	A description of the vendor configuration file (human-readable string).	-	1.0
InternetGatewayDevice.DeviceConfig.	object	-	This object contains general configuration parameters.	-	1.0
PersistentData	string(256)	W	Arbitrary user data that MUST persist across CPE reboots.	-	1.0
ConfigFile	string(32K)	W	A dump of the currently running configuration on the CPE. This parameter enables the ability to backup and restore the last known good state of the CPE. It returns a vendor-specific document that defines the state of the CPE. The document MUST be capable of restoring the CPE's state when written back to the CPE using SetParameterValues.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.ManagementServer.	object	-	This object contains parameters relating to the CPE's association with an ACS.	-	1.0
URL	string(256)	W	URL, as defined in [8], for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL [6]. The "host" portion of this URL is used by the CPE for validating the ACS certificate when using SSL or TLS. Note that on a factory reset of the CPE, the value of this parameter might be reset to its factory value. If an ACS modifies the value of this parameter, it SHOULD be prepared to accommodate the situation that the original value is restored as the result of a factory reset.	-	1.0
Username	string(256)	W	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE. Note that on a factory reset of the CPE, the value of this parameter might be reset to its factory value. If an ACS modifies the value of this parameter, it SHOULD be prepared to accommodate the situation that the original value is restored as the result of a factory reset.	-	1.0
Password	string(256)	W	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE. When read, this parameter returns an empty string, regardless of the actual value. Note that on a factory reset of the CPE, the value of this parameter might be reset to its factory value. If an ACS modifies the value of this parameter, it SHOULD be prepared to accommodate the situation that the original value is restored as the result of a factory reset.	-	1.0
PeriodicInformEnable	boolean	W	Whether or not the CPE MUST periodically send CPE information to the ACS using the Inform method call.	-	1.0
PeriodicInformInterval	unsignedInt [1:]	W	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method if PeriodicInformEnable is true.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
PeriodicInformTime	dateTime	W	An absolute time reference in UTC to determine when the CPE will initiate the periodic Inform method calls. Each Inform call MUST occur at this reference time plus or minus an integer multiple of the PeriodicInformInterval. PeriodicInformTime is used only to set the "phase" of the periodic Informs. The actual value of PeriodicInformTime can be arbitrarily far into the past or future. For example, if PeriodicInform Interval is 86400 (a day) and if PeriodicInformTime is set to UTC midnight on some day (in the past, present, or future) then periodic Informs will occur every day at UTC midnight. These MUST begin on the very next midnight, even if PeriodicInformTime refers to a day in the future. The Unknown Time value defined in section 2.2 indicates that no particular time reference is specified. That is, the CPE MAY locally choose the time reference, and is required only to adhere to the specified PeriodicInformInterval. If absolute time is not available to the CPE, its periodic Inform behavior MUST be the same as if the PeriodicInformTime parameter was set to the Unknown Time value.	-	1.0
ParameterKey	string(32)	-	ParameterKey provides the ACS a reliable and extensible means to track changes made by the ACS. The value of ParameterKey MUST be equal to the value of the ParameterKey argument from the most recent successful SetParameterValues, AddObject, or DeleteObject method call from the ACS. The CPE MUST set ParameterKey to the value specified in the corresponding method arguments if and only if the method completes successfully and no fault response is generated. If a method call does not complete successfully (implying that the changes requested in the method did not take effect), the value of ParameterKey MUST NOT be modified. The CPE MUST only modify the value of ParameterKey as a result of SetParameterValues, AddObject, DeleteObject, or due to a factory reset. On factory reset, the value of ParameterKey MUST be set to empty.	-	1.0
ConnectionRequestURL	string(256)	-	HTTP URL, as defined in [8], for an ACS to make a Connection Request notification to the CPE. In the form: http://host:port/path The "host" portion of the URL MAY be the IP address for the management interface of the CPE in lieu of a host name.	-	1.0
ConnectionRequestUsername	string(256)	W	Username used to authenticate an ACS making a Connection Request to the CPE.	-	1.0
ConnectionRequestPassword	string(256)	W	Password used to authenticate an ACS making a Connection Request to the CPE. When read, this parameter returns an empty string, regardless of the actual value.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
UpgradesManaged	boolean	W	Indicates whether or not the ACS will manage upgrades for the CPE. If true (1), the CPE SHOULD NOT use other means other than the ACS to seek out available upgrades. If false (0), the CPE MAY use other means for this purpose.	-	1.0
KickURL	string(256)	-	Present only for a CPE that supports the Kicked RPC method. LAN-accessible URL, as defined in [8], from which the CPE can be "kicked" to initiate the Kicked RPC method call. MUST be an absolute URL including a host name or IP address as would be used on the LAN side of the CPE.	-	1.0
DownloadProgressURL	string(256)	-	Present only for a CPE that provides a LAN-side web page to show progress during a file download. LAN-accessible URL, as defined in [8], to which a web-server associated with the ACS MAY redirect a user's browser on initiation of a file download to observer the status of the download.	-	1.0
UDPConnectionRequestAddress	string(256)	-	Address and port to which an ACS MAY send a UDP Connection Request to the CPE (see Annex G of [2]). This parameter is represented in the form of an Authority element as defined in [8]. The value MUST be in one of the following two forms: host:port host When STUNEnable is true, the "host" and "port" portions of this parameter MUST represent the public address and port corresponding to the NAT binding through which the ACS can send UDP Connection Request messages (once this information is learned by the CPE through the use of STUN). When STUNEnable is false, the "host" and "port" portions of the URL MUST represent the local IP address and port on which the CPE is listening for UDP Connection Request messages. The second form of this parameter MAY be used only if the port value is equal to "80".	-	1.2
UDPConnectionRequestAddressNotification-Limit	unsignedInt	W	The minimum time, in seconds, between Active Notifications resulting from changes to the UDP-Connection RequestAddress (if Active Notification is enabled).	-	1.2
STUNEnable	boolean	W	Enables or disables the use of STUN by the CPE. This applies only to the use of STUN in association with the ACS to allow UDP Connection Requests.	-	1.2
STUNServerAddress	string(256)	W	Host name or IP address of the STUN server for the CPE to send Binding Requests if STUN is enabled via STUNEnable. If empty and STUNEnable is true, the CPE MUST use the address of the ACS extracted from the host portion of the ACS URL.	-	1.2
STUNServerPort	unsignedInt [0:65535]	W	Port number of the STUN server for the CPE to send Binding Requests if STUN is enabled via STUNEnable. By default, this SHOULD be the equal to the default STUN port, 3478.	-	1.2

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
STUNUsername	string(256)	W	If non-empty, the value of the STUN USERNAME attribute to be used in Binding Requests (only if message integrity has been requested by the STUN server). If empty, the CPE MUST NOT send STUN Binding Requests with message integrity.	-	1.2
STUNPassword	string(256)	W	The value of the STUN Password to be used in computing the MESSAGE-INTEGRITY attribute to be used in Binding Requests (only if message integrity has been requested by the STUN server). When read, this parameter returns an empty string, regardless of the actual value.	-	1.2
STUNMaximumKeepAlivePeriod	int[-1:]	W	If STUN Is enabled, the maximum period, in seconds, that STUN Binding Requests MUST be sent by the CPE for the purpose of maintaining the binding in the Gateway. This applies specifically to Binding Requests sent from the UDP Connection Request address and port. A value of -1 indicates that no maximum period is specified.	-	1.2
STUNMinimumKeepAlivePeriod	unsignedInt	W	If STUN Is enabled, the minimum period, in seconds, that STUN Binding Requests can be sent by the CPE for the purpose of maintaining the binding in the Gateway. This limit applies only to Binding Requests sent from the UDP Connection Request address and port, and only those that do not contain the BINDING-CHANGE attribute. This limit does not apply to retransmissions following the procedures defined in [9].	-	1.2
NATDetected	boolean	-	When STUN is enabled, this parameter indicates whether or not the CPE has detected address and/or port mapping in use. A true value indicates that the received MAPPED-ADDRESS in the most recent Binding Response differs from the CPE's source address and port. When STUNEnable is false, this value MUST be false.	-	1.2
ManageableDeviceNumberOfEntries	unsignedInt	-	Number of entries in the ManageableDevice table.	-	1.2
ManageableDeviceNotificationLimit	unsignedInt	W	The minimum time, in seconds, between Active Notifications resulting from changes to the ManageableDeviceNumberOfEntries (if Active Notification is enabled).	-	1.2
InternetGatewayDevice.ManagementServer.-ManageableDevice.{i}.	object	-	Each entry in this table corresponds to a distinct LAN Device that supports Device-Gateway Association according to Annex F of [2] as indicated by the presence of the DHCP option specified in that Annex.	-	1.2
ManufacturerOUI	string(6)	-	Organizationally unique identifier of the Device manufacturer as provided to the Gateway by the Device. Represented as a six hexadecimal-digit value using all upper-case letters and including any leading zeros. The value MUST be a valid OUI as defined in [5].	-	1.2
SerialNumber	string(64)	-	Serial number of the Device as provided to the Gateway by the Device.	-	1.2
ProductClass	string(64)	-	Identifier of the class of product for which the Device's serial number applies as provided to the Gateway by the Device. If the Device does not provide a Product Class, then this parameter MUST be left empty.	-	1.2

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.Time.	object	-	This object contains parameters relating an NTP or SNTP time client in the CPE.	-	1.0
NTPServer1	string(64)	W	First NTP timeserver. Either a host name or IP address.	-	1.0
NTPServer2	string(64)	W	Second NTP timeserver. Either a host name or IP address.	-	1.0
NTPServer3	string(64)	W	Third NTP timeserver. Either a host name or IP address.	-	1.0
NTPServer4	string(64)	W	Fourth NTP timeserver. Either a host name or IP address.	-	1.0
NTPServer5	string(64)	W	Fifth NTP timeserver. Either a host name or IP address.	-	1.0
CurrentLocalTime	dateTime	-	The current date and time in the CPE's local time zone.	-	1.0
LocalTimeZone	string(6)	W	The local time offset from UTC in the form: +hh:mm -hh:mm	-	1.0
LocalTimeZoneName	string(64)	W	Name of the local time zone (human readable string).	-	1.0
DaylightSavingsUsed	boolean	W	Whether or not daylight savings time is in use in the CPE's local time zone.	-	1.0
DaylightSavingsStart	dateTime	W	Date and time daylight savings time begins if used in local standard time. If daylight savings time is not used, this value is ignored.	-	1.0
DaylightSavingsEnd	dateTime	W	Date and time daylight savings time ends if used in local daylight time. If daylight savings time is not used, this value is ignored.	-	1.0
InternetGatewayDevice.UserInterface.	object	-	This object contains parameters relating to the user interface of the CPE.	-	1.0
PasswordRequired	boolean	W	Present only if the CPE provides a password-protected LAN-side user interface. Indicates whether or not the local user interface MUST require a password to be chosen by the user. If false, the choice of whether or not a password is used is left to the user.	-	1.0
PasswordUserSelectable	boolean	W	Present only if the CPE provides a password-protected LAN-side user interface and supports LAN-side Auto-Configuration. Indicates whether or not a password to protect the local user interface of the CPE MAY be selected by the user directly, or MUST be equal to the password used by the LAN-side Auto-Configuration protocol.	-	1.0
UpgradeAvailable	boolean	W	Indicates that a CPE upgrade is available, allowing the CPE to display this information to the user.	-	1.0
WarrantyDate	dateTime	W	Indicates the date and time in UTC that the warranty associated with the CPE is to expire.	-	1.0
ISPName	string(64)	W	The name of the customer's ISP.	-	1.0
ISPHelpDesk	string(32)	W	The help desk phone number of the ISP.	-	1.0
ISPHomePage	string(256)	W	The URL of the ISP's home page.	-	1.0
ISPHelpPage	string(256)	W	The URL of the ISP's on-line support page.	-	1.0
ISPLogo	base64 (5460)	W	Base64 encoded GIF or JPEG image. The binary image is constrained to 4095 bytes or less.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
ISPLogoSize	unsignedInt [0:4095]	W	Un-encoded binary image size in bytes. If ISPLogoSize input value is 0 then the ISPLogo is cleared. ISPLogoSize can also be used as a check to verify correct transfer and conversion of Base64 string to image size.	-	1.0
ISPMailServer	string(256)	W	The URL of the ISP's mail server.	-	1.0
ISPNewsServer	string(256)	W	The URL of the ISP's news server.	-	1.0
TextColor	string(6)	W	The color of text on the GUI screens in RGB hexidecimal notation (e.g., FF0088).	-	1.0
BackgroundColor	string(6)	W	The color of the GUI screen backgrounds in RGB hexidecimal notation (e.g., FF0088).	-	1.0
ButtonColor	string(6)	W	The color of buttons on the GUI screens in RGB hexidecimal notation (e.g., FF0088).	-	1.0
ButtonTextColor	string(6)	W	The color of text on buttons on the GUI screens in RGB hexidecimal notation (e.g., FF0088).	-	1.0
AutoUpdateServer	string(256)	W	The server the CPE can check to see if an update is available for direct download to it. This MUST NOT be used by the CPE if the InternetGateway-Device.ManagementServer.UpgradesManaged parameter is true (1).	-	1.0
UserUpdateServer	string(256)	W	The server where a user can check via a web browser if an update is available for download to a PC. This MUST NOT be used by the CPE if the I nternetGatewayDevice.ManagementServer.-UpgradesManaged parameter is true (1).	-	1.0
ExampleLogin	string(40)	W	An example of a correct login, according to ISP-specific rules.	-	1.0
ExamplePassword	string(30)	W	An example of a correct password, according to ISP-specific rules.	-	1.0
InternetGatewayDevice.Layer3Forwarding.	object	-	This object allows the handling of the routing and forwarding configuration of the device.	-	1.0
DefaultConnectionService	string(256)	W	Specifies the default WAN interface. The content is the full hierarchical parameter name of the default layer-3 connection object. Example: "InternetGatewayDevice.WANDevice.1.WAN-ConnectionDevice.2.WANPPPConnection.1".	-	1.0
ForwardNumberOfEntries	unsignedInt	-	Number of forwarding instances.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.Layer3Forwarding.-Forwarding.{i}.	object	W	Layer-3 forwarding table. In addition to statically configured routes, this table MUST include dynamic routes learned through layer-3 routing protocols, including RIP, OSPF, DHCP, and IPCP. The CPE MAY reject attempts to delete or modify a dynamic route entry. For each incoming packet, the layer-3 forwarding decision is conceptually made as follows: • Only table entries with a matching ForwardingPolicy are considered, i.e. those that either do not specify a ForwardingPolicy, or else specify a ForwardingPolicy that matches that of the incoming packet. • For the remaining table entries, those for which the source address/mask matches are sorted by longest prefix, i.e. with the most specific networks first (an unspecified source address is a wild-card and always matches, with a prefix length of zero). • For the remaining table entries, those for which the destination address/mask matches are sorted by longest prefix, i.e. with the most specific networks first (an unspecified destination address is a wild-card and always matches, with a prefix length of zero). • The first of the remaining table entries is applied to the packet.	-	1.0
Enable	boolean	W	Enables or disables the forwarding entry. On creation, an entry is disabled by default.	False	1.0
Status	string	-	Indicates the status of the forwarding entry. Enumeration of: “Disabled” “Enabled” “Error” (OPTIONAL) The “Error” value MAY be used by the CPE to indicate a locally defined error condition.	“Disabled”	1.0
Type	string	W	Indicates the type of route. Enumeration of: “Default” “Network” “Host” This parameter is DEPRECATED because its value could conflict with DestIPAddress and/or DestSubnetMask.	“Host”	1.0
DestIPAddress	string	W	Destination address. An empty string or a value of “0.0.0.0” indicates no destination address is specified. A Forwarding table entry for which DestIPAddress and DestSubnetMask are both empty or “0.0.0.0” is a default route.	<Empty>	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
DestSubnetMask	string	W	Destination subnet mask. An empty string or a value of "0.0.0.0" indicates no destination subnet mask is specified. If a destination subnet mask is specified, the DestSubnetMask is ANDed with the destination address before comparing with the DestIPAddress. Otherwise, the full destination address is used as is. A Forwarding table entry for which DestIPAddress and DestSubnetMask are both empty or "0.0.0.0" is a default route.	<Empty>	1.0
SourceIPAddress	string	W	Source address. An empty string or a value of "0.0.0.0" indicates no source address is specified.	<Empty>	1.0
SourceSubnetMask	string	W	Source subnet mask. An empty string or a value of "0.0.0.0" indicates no source subnet mask is specified. If a source subnet mask is specified, the SourceSubnetMask is ANDed with the source address before comparing with the SourceIPAddress. Otherwise, the full source address is used as is.	<Empty>	1.0
ForwardingPolicy	int[-1:]	W	Identifier of a set of classes or flows that have the corresponding ForwardingPolicy value as defined in the QueueManagement object. A value of -1 indicates no Forwarding Policy is specified. If specified, this forwarding entry is to apply only to traffic associated with the specified classes and flows.	-1	1.0
GatewayIPAddress	string	W	IP address of the gateway. Only one of GatewayIPAddress and Interface SHOULD be configured for a route. If both are configured, GatewayIPAddress and Interface MUST be self-consistent.	<Empty>	1.0
Interface	string(256)	W	Specifies the egress interface associated with this entry. The content is the full hierarchical parameter name of the layer-3 connection object. Example: "InternetGatewayDevice.WANDevice.1.WAN-ConnectionDevice.2.WANPPPConnection.1". Only one of GatewayIPAddress and Interface SHOULD be configured for a route. If both are configured, GatewayIPAddress and Interface MUST be self-consistent. For a route that was configured by setting GatewayIPAddress but not Interface, read access to Interface MUST return the full hierarchical parameter name for the route's egress interface.	-	1.0
ForwardingMetric	int[-1:]	W	Forwarding metric. A value of -1 indicates this metric is not used.	-1	1.0
MTU	unsignedInt [1:1540]	W	The maximum allowed size of an Ethernet frame for this route.	-	1.0
InternetGatewayDevice.Layer2Bridging.	object	-	Layer-2 bridging table. Specifies bridges between layer-2 LAN and/or WAN interfaces. Bridges can be defined to include layer-2 filter criteria to selectively bridge traffic between interfaces.	-	1.1
MaxBridgeEntries	unsignedInt	-	The maximum number of entries available in the Bridge table.	-	1.1
MaxFilterEntries	unsignedInt	-	The maximum number of entries available in the Filter table.	-	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
MaxMarkingEntries	unsignedInt	-	The maximum number of entries available in the Marking table.	-	1.1
BridgeNumberOfEntries	unsignedInt	-	Number of entries in the Bridge table.	-	1.1
FilterNumberOfEntries	unsignedInt	-	Number of entries in the Filter table.	-	1.1
MarkingNumberOfEntries	unsignedInt	-	Number of entries in the Marking table.	-	1.1
AvailableInterfaceNumberOfEntries	unsignedInt	-	Number of entries in the AvailableInterface table.	-	1.1
InternetGatewayDevice.Layer2Bridging.-Bridge.{i}.	object	W	Bridge table.	-	1.1
BridgeKey	unsignedInt	-	Unique key for each Bridge table entry.	-	1.1
BridgeEnable	boolean	W	Enables or disables this Bridge table entry.	False	1.1
BridgeStatus	string	-	The status of this Bridge table entry. Enumeration of: "Disabled" "Enabled" "Error" (OPTIONAL) The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	"Disabled"	1.1
BridgeName	string(64)	W	Human-readable name for this Bridge table entry.	<Empty>	1.1
VLANID	unsignedInt [0:4094]	W	The 802.1Q VLAN ID associated with this Bridge. A value of 0 indicates either Untagged or PriorityOnly tagging, which are treated identically.	0	1.1
InternetGatewayDevice.Layer2Bridging.Filter.-{i}.	object	W	Filter table containing filter entries each of which is associated with one Bridge as specified by a Bridge table entry.	-	1.1
FilterKey	unsignedInt	-	Unique key for each Filter table entry.	-	1.1
FilterEnable	boolean	W	Enables or disables this Filter table entry.	False	1.1
FilterStatus	string	-	The status of this Filter table entry. Enumeration of: "Disabled" "Enabled" "Error" (OPTIONAL) The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	"Disabled"	1.1
FilterBridgeReference	int[-1:]	W	The BridgeKey value of the Bridge table entry associated with this Filter. A value of -1 indicates the Filter table entry is not associated with a Bridge (and has no effect).	-1	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
ExclusivityOrder	unsignedInt	W	Whether or not the Filter definition is exclusive of all others. And if the entry is exclusive, order of precedence. A value of 1 or greater indicates an Exclusive Filter, where the value 1 indicates the first entry to be considered (highest precedence). A value of 0 indicates a Non-Exclusive Filter. For each packet, if the packet matches any Exclusive Filters, the packet is assigned to the Bridge associated with the highest precedence Exclusive Filter to which it matches (lowest ExclusivityOrder value). If and only if the packet does not match any Exclusive Filters, the packet is assigned to all Bridges associated with each Non-Exclusive Filter for which it matches the defining criteria. If a packet matches no Filter, it is discarded. When the ExclusivityOrder is set to match that of an existing Exclusive Filter (1 or greater), the value for the existing entry and all higher numbered entries is incremented (lowered in precedence) to ensure uniqueness of this value. A deletion or change in ExclusivityOrder of an Exclusive Filter causes ExclusivityOrder values of other Exclusive Filters (values 1 or greater) to be compacted. Note that the use of Exclusive Filters to associate a layer-3 router interface with LAN and/or WAN interfaces via a Bridge entry overrides the default association between layer-3 and layer-2 objects implied by the InternetGatewayDevice object hierarchy.	0	1.1
FilterInterface	string	W	The interface or interfaces associated with this Filter table entry. The bridge corresponding to this Filter table entry is defined to admit packets on ingress to the bridge from the specified interfaces that meet all of the criteria specified in the Filter table entry. The following values are defined. To associate this Filter with a single interface listed in the AvailableInterface table, the FilterInterface value is set to the value of corresponding AvailableInterfaceKey. “AllInterfaces” indicates that this Filter is associated with all LAN and WAN interfaces listed in the AvailableInterface table (all entries of InterfaceType LANInterface or WANInterface). “LANInterfaces” indicates that this Filter is associated with all LAN interfaces listed in the AvailableInterface table (all entries of InterfaceType LANInterface). “WANInterfaces” indicates that this Filter is associated with all WAN interfaces listed in the AvailableInterface table (all entries of InterfaceType WANInterface). An empty string indicates the Filter table entry is not associated with any interface (and has no effect)	<Empty>	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
VLANIDFilter	int[-1:4095]	W	The 802.1Q VLAN ID of packets to admit to the specified Bridge through the interfaces specified for this Filter. A value of -1 indicates that the default VLAN ID for the Bridge SHOULD be used instead (as specified by InternetGatewayDevice.Layer2Bridging.Bridge.-{i}.VLANID for the Bridge table entry associated with this Filter table entry). On creation of a Filter entry, the default value for this parameter MUST be -1.	-1	1.1
AdmitOnlyVLANTagged	boolean	W	If true, on ingress to the interfaces associated with this Filter, the Bridge admits only packets tagged with a VLAN ID that matches the VLANIDFilter parameter (or instead, the VLAN ID for the Bridge if VLANIDFilter is unspecified). If false, on ingress to the interfaces associated with this Filter, the Bridge admits both packets tagged with a VLAN ID that matches the VLANIDFilter parameter (or instead, the VLAN ID for the Bridge if VLANIDFilter is unspecified), and any Untagged or PriorityOnly packets. All Untagged or PriorityOnly packets are tagged on ingress with the value of the VLANID parameter. If the VLANIDFilter parameter (or instead, the VLAN ID for the Bridge if VLANIDFilter is unspecified) is equal to 0, then this parameter is ignored, and only packets that are Untagged or PriorityOnly packets are admitted.	False	1.1
EthertypeFilterList	string(256)	W	Comma-separated list of unsigned integers, each representing an Ethertype value.	<Empty>	1.1
EthertypeFilterExclude	boolean	W	If false, on ingress to the interfaces associated with this Filter, the Bridge is defined to admit only those packets that match one of the EthertypeFilterList entries (in either the Ethernet or SNAP Type header). If the EthertypeFilterList is empty, no packets are admitted. If true, on ingress to the interfaces associated with this Filter, the Bridge is defined to admit all packets except those packets that match one of the EthertypeFilterList entries (in either the Ethernet or SNAP Type header). If the EthertypeFilterList is empty, packets are admitted regardless of Ethertype.	True	1.1
SourceMACAddressFilterList	string(512)	W	Comma-separated list of MAC Addresses. Each list entry MAY optionally specify a bit-mask, where matching of a packet's MAC address is only to be done for bit positions set to one in the mask. If no mask is specified, all bits of the MAC Address are to be used for matching. For example, the list might be: "01:02:03:04:05:06, 1 :22:33:00:00:00/FF:FF:FF:00:00:00, 88:77:66:55:44:33"	<Empty>	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
SourceMACAddressFilterExclude	boolean	W	If false, on ingress to the interfaces associated with this Filter, the Bridge admits only those packets whose source MAC Address matches one of the SourceMACAddressFilterList entries. If the SourceMACAddressFilterList is empty, no packets are admitted. If true, on ingress to the interfaces associated with this Filter, the Bridge admits all packets except those packets whose source MAC Address matches one of the SourceMACAddressFilterList entries. If the SourceMACAddressFilterList is empty, packets are admitted regardless of MAC address.	True	1.1
DestMACAddressFilterList	string(512)	W	Comma-separated list of MAC Addresses. Each list entry MAY optionally specify a bit-mask, where matching of a packet's MAC address is only to be done for bit positions set to one in the mask. If no mask is specified, all bits of the MAC Address are to be used for matching. For example, the list might be: "01:02:03:04:05:06, 1 :22:33:00:00:00/FF:FF:FF:00:00:00, 88:77:66:55:44:33"	<Empty>	1.1
DestMACAddressFilterExclude	boolean	W	If false, on ingress to the interfaces associated with this Filter, the Bridge admits only those packets whose destination MAC Address matches one of the DestMACAddressFilterList entries. If the Dest-MACAddressFilterList is empty, no packets are admitted. If true, on ingress to the interfaces associated with this Filter, the Bridge admits all packets except those packets whose destination MAC Address matches one of the DestMACAddressFilterList entries. If the WANSourceMACAddressFilterList is empty, packets are admitted regardless of MAC address.	True	1.1
SourceMACFromVendorClassIDFilter	string(256)	W	A string used to identify one or more devices via DHCP for which MAC address filtering would subsequently apply. A device is considered matching if it its DHCP Vendor Class Identifier (Option 60 as defined in RFC 2132) in the most recent DHCP lease acquisition or renewal was equal to the specified value.	<Empty>	1.1
SourceMACFromVendorClassIDFilterExclude	boolean	W	If false, on ingress to the interfaces associated with this Filter, the Bridge admits only those packets whose source MAC Address matches that of a LAN device previously identified as described in Source-MACFromVendorClassIDFilter. If SourceMAC-FromVendorClassIDFilter is empty, no packets are admitted. If true, on ingress to the interfaces associated with this Filter, the Bridge admits all packets except those packets whose source MAC Address matches that of a LAN device previously identified as described in SourceMACFromVendorClassID-Filter. If the SourceMACFromVendorClassIDFilter is empty, packets are admitted regardless of MAC address.	True	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
DestMACFromVendorClassIDFilter	string(256)	W	A string used to identify one or more devices via DHCP for which MAC address filtering would subsequently apply. A device is considered matching if it its DHCP Vendor Class Identifier (Option 60 as defined in RFC 2132) in the most recent DHCP lease acquisition or renewal was equal to the specified value.	<Empty>	1.1
DestMACFromVendorClassIDFilterExclude	boolean	W	If false, on ingress to the interfaces associated with this Filter, the Bridge admits only those packets whose destination MAC Address matches that of a LAN device previously identified as described in DestMACFromVendorClassIDFilter. If DestMAC-FromVendorClassIDFilter is empty, no packets are admitted. If true, on ingress to the interfaces associated with this Filter, the Bridge admits all packets except those packets whose destination MAC Address matches that of a LAN device previously identified as described in DestMACFromVendorClassID-Filter. If the DestMACFromVendorClassIDFilter is empty, packets are admitted regardless of MAC address.	True	1.1
SourceMACFromClientIDFilter	string(256)	W	A string used to identify one or more devices via DHCP for which MAC address filtering would subsequently apply. A device is considered matching if it its DHCP Client Identifier (Option 61 as defined in RFC 2132) in the most recent DHCP lease acquisition or renewal was equal to the specified value.	<Empty>	1.1
SourceMACFromClientIDFilterExclude	boolean	W	If false, on ingress to the interfaces associated with this Filter, the Bridge admits only those packets whose source MAC Address matches that of a LAN device previously identified as described in Source-MACFromClientIDFilter. If SourceMACFrom-ClientIDFilter is empty, no packets are admitted. If true, on ingress to the interfaces associated with this Filter, the Bridge admits all packets except those packets whose source MAC Address matches that of a LAN device previously identified as described in SourceMACFromClientIDFilter. If the SourceMACFromClientIDFilter is empty, packets are admitted regardless of MAC address.	True	1.1
DestMACFromClientIDFilter	string(256)	W	A string used to identify one or more devices via DHCP for which MAC address filtering would subsequently apply. A device is considered matching if it its DHCP Client Identifier (Option 61 as defined in RFC 2132) in the most recent DHCP lease acquisition or renewal was equal to the specified value.	<Empty>	1.1
DestMACFromClientIDFilterExclude	boolean	W	If false, on ingress to the interfaces associated with this Filter, the Bridge admits only those packets whose destination MAC Address matches that of a LAN device previously identified as described in DestMACFromClientIDFilter. If DestMACFrom-ClientIDFilter is empty, no packets are admitted. If true, on ingress to the interfaces associated with this Filter, the Bridge admits all packets except those packets whose destination MAC Address matches that of a LAN device previously identified as described in DestMACFromClientIDFilter. If the DestMACFromClientIDFilter is empty, packets are admitted regardless of MAC address.	True	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
SourceMACFromUserClassIDFilter	string(256)	W	A string used to identify one or more devices via DHCP for which MAC address filtering would subsequently apply. A device is considered matching if it its DHCP User Class Identifier (Option 77 as defined in RFC 3004) in the most recent DHCP lease acquisition or renewal was equal to the specified value.	<Empty>	1.1
SourceMACFromUserClassIDFilterExclude	boolean	W	If false, on ingress to the interfaces associated with this Filter, the Bridge admits only those packets whose source MAC Address matches that of a LAN device previously identified as described in SourceMACFromUserClassIDFilter. If SourceMACFromUserClassIDFilter is empty, no packets are admitted. If true, on ingress to the interfaces associated with this Filter, the Bridge admits all packets except those packets whose source MAC Address matches that of a LAN device previously identified as described in SourceMACFromUserClassIDFilter. If the SourceMACFromUserClassIDFilter is empty, packets are admitted regardless of MAC address.	True	1.1
DestMACFromUserClassIDFilter	string(256)	W	A string used to identify one or more devices via DHCP for which MAC address filtering would subsequently apply. A device is considered matching if it its DHCP User Class Identifier (Option 77 as defined in RFC 3004) in the most recent DHCP lease acquisition or renewal was equal to the specified value.	<Empty>	1.1
DestMACFromUserClassIDFilterExclude	boolean	W	If false, on ingress to the interfaces associated with this Filter, the Bridge admits only those packets whose destination MAC Address matches that of a LAN device previously identified as described in DestMACFromUserClassIDFilter. If DestMACFromUserClassIDFilter is empty, no packets are admitted. If true, on ingress to the interfaces associated with this Filter, the Bridge admits all packets except those packets whose destination MAC Address matches that of a LAN device previously identified as described in DestMACFromUserClassIDFilter. If the DestMACFromUserClassIDFilter is empty, packets are admitted regardless of MAC address.	True	1.1
InternetGatewayDevice.Layer2Bridging.Marking.{i}.	object	W	Marking table identifying non-default layer-2 marking behavior for packets on egress from the specified interfaces.	-	1.1
MarkingKey	unsignedInt	-	Unique key for each Marking table entry.	-	1.1
MarkingEnable	boolean	W	Enables or disables this Marking table entry.	False	1.1
MarkingStatus	string	-	The status of this Marking table entry. Enumeration of: "Disabled" "Enabled" "Error" (OPTIONAL) The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	"Disabled"	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
MarkingBridgeReference	int[-1:]	W	The BridgeKey value of the Bridge table entry associated with this Marking table entry. A value of -1 indicates the Marking table entry is not associated with a Bridge (and has no effect). The effect of a Marking table entry applies only to packets that have been admitted to the specified bridge (regardless of the ingress interface).	-1	1.1
MarkingInterface	string	W	The interface or interfaces associated with this Marking table entry for which the specified marking behavior is to apply on egress from the associated bridge. The following values are defined. To associate this Marking table entry with a single interface listed in the AvailableInterface table, the MarkingInterface value is set to the value of corresponding AvailableInterfaceKey. "AllInterfaces" indicates that this Marking table entry is associated with all LAN and WAN interfaces listed in the AvailableInterface table (all entries of InterfaceType LANInterface or WANInterface). "LAN Interfaces" indicates that this Marking table entry is associated with all LAN interfaces listed in the AvailableInterface table (all entries of InterfaceType LANInterface). "WANInterfaces" indicates that this Marking table entry is associated with all WAN interfaces listed in the AvailableInterface table (all entries of InterfaceType WANInterface). An empty string indicates the Marking table entry table entry is not associated with any interface (and has no effect) If there is more than one enabled Marking table entry that specifies one or more of the same interfaces for the same bridge (identical values of MarkingBridgeReference), then for packets on egress from the specified bridge to those interfaces, the applied marking MUST be that specified in the Marking table entry among those in conflict with the lowest MarkingKey value. If an interface in a given bridge does not have a corresponding Marking table entry, the marking is left unchanged on egress.	<Empty>	1.1
VLANIDUntag	boolean	W	If true, on egress to the interfaces associated with this Marking table entry, all packets are Untagged. That is, the VLAN tag is stripped from the packet. If false, on egress to the interfaces associated with this Marking table entry, all VLAN tags are left intact (including those added on ingress).	False	1.1
VLANIDMark	int[-1 :4095]	W	The 802.1Q VLAN ID to be used on egress to the interfaces associated with this Marking table entry (if VLANIDUntag is false). A value of -1 indicates that the default VLAN ID for the Bridge SHOULD be used instead (as specified by InternetGatewayDevice.Layer2Bridging.Bridge.-{i}.VLANID for the Bridge table entry associated with this Marking table entry).	-1	1.1
EthernetPriorityMark	int[-1 :7]	W	Ethernet priority code (as defined in 802.1 D) to mark traffic with that falls into this Bridge on egress to the interfaces associated with this Marking table entry. A value of -1 indicates no change from the incoming packet or the mark assigned by the classifier.	-1	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
EthernetPriorityOverride	boolean	W	If false, on egress to the interfaces associated with this Marking table entry, the EthernetPriorityMark, if specified, is applied only to packets of priority 0. If true, on egress to the interfaces associated with this Marking table entry, the EthernetPriorityMark, if specified, is to be applied to all packets on this Bridge. If VLANIDUntag is true, then no priority marking is done since the tag containing the Ethernet priority is removed.	False	1.1
InternetGatewayDevice.Layer2-Bridging.AvailableInterface.{i}.	object	-	Table containing all LAN and WAN interfaces that are available to be referenced by the Bridge table. Only interfaces that can carry layer-2 bridged traffic are included.	-	1.1
AvailableInterfaceKey	unsignedInt	-	Unique key for each Interface entry.	-	1.1
InterfaceType	string	-	Whether the interface is a LAN-side or WAN-side interface, or a LAN-side or WAN-side connection to the Gateway's IP router. Enumeration of: "LAN Interface" "WAN Interface" "LAN RouterConnection" "WAN RouterConnection"	-	1.1
InterfaceReference	string(256)	-	This table SHOULD contain a single entry for each *available* LAN and WAN interface. For a WAN interface, this parameter is the full hierarchical parameter name of a particular WAN-ConnectionDevice. A WANConnectionDevice is considered available (included in this table) *only* if it supports layer-2 bridged traffic. That is, this table MUST include only WANConnectionDevices that contain either a WANEthernetLinkConfig object, or that contain a WANDSLLinkConfig object for which the LinkType is "EoA". For example: "InternetGatewayDevice.WANDevice. 1.WAN-ConnectionDevice.2" For a LAN interface, this parameter is the full hierarchical parameter name of a particular LAN**-InterfaceConfig object, or a WLANConfiguration object. This table SHOULD include one entry for each such object. For example: "InternetGatewayDevice.LANDevice. 1.LAN-LANEthernetInterfaceConfig.2" For a WAN-side connection to the Gateway's IP router, this parameter is the full hierarchical parameter name of a particular WAN**Connection service. This table SHOULD include an entry for each layer-3 WAN connection. For example: "InternetGatewayDevice.WANDevice. 1.WAN-ConnectionDevice.2.WANPPPConnection.1" For a LAN-side connection to the Gateway's IP router, this parameter is the full hierarchical parameter name of a particular LANDevice. This table SHOULD include an entry for each LAN Device, each of which is associated with a LAN-side layer-3 connection to the Gateway's IP router. For example: "InternetGatewayDevice.LANDevice.2"	-	1.1
InternetGatewayDevice.QueueManagement.	object	-	Queue management configuration object.	-	1.1
Enable	boolean	W	Enables or disables all queuing operation.	-	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
MaxQueues	unsignedInt	-	The maximum number of queues supported by the CPE. Calculated as the sum of the number of different queues pointed to by Classification table. For each entry in the Classification table, the count includes a queue for each egress interface to which the corresponding classified traffic could reach.	-	1.1
MaxClassificationEntries	unsignedInt	-	The maximum number of entries available in the Classification table.	-	1.1
ClassificationNumberOfEntries	unsignedInt	-	The number of entries in the Classification table.	-	1.1
MaxAppEntries	unsignedInt	-	The maximum number of entries available in the App table.	-	1.1
AppNumberOfEntries	unsignedInt	-	The number of entries in the App table.	-	1.1
MaxFlowEntries	unsignedInt	-	The maximum number of entries available in the Flow table.	-	1.1
FlowNumberOfEntries	unsignedInt	-	The number of entries in the Flow table.	-	1.1
MaxPolicerEntries	unsignedInt	-	The maximum number of entries available in the Policer table.	-	1.1
PolicerNumberOfEntries	unsignedInt	-	The number of entries in the Policer table.	-	1.1
MaxQueueEntries	unsignedInt	-	The maximum number of entries available in the Queue table.	-	1.1
QueueNumberOfEntries	unsignedInt	-	The number of entries in the Queue table.	-	1.1
DefaultForwardingPolicy	unsignedInt	W	Identifier of the forwarding policy associated with traffic not associated with any specified classifier.	-	1.1
DefaultPolicer	int[-1:]	W	Instance number of the Policer table entry for traffic not associated with any specified classifier. A value of -1 indicates a null policer.	-	1.1
DefaultQueue	unsignedInt	W	Instance number of the Queue table entry for traffic not associated with any specified classifier.	-	1.1
DefaultDSCPMark	int[-2:]	W	DSCP to mark traffic not associated with any specified classifier. A value of -1 indicates no change from the incoming packet. A value of -2 indicates automatic marking of DSCP based upon the EthernetPriority value of the incoming packet as defined in Annex A.	-	1.1
DefaultEthernetPriorityMark	int[-2:]	W	Ethernet priority code (as defined in 802.1D) to mark traffic not associated with any specified classifier. A value of -1 indicates no change from the incoming packet. A value of -2 indicates automatic marking of EthernetPriority based upon the DSCP value of the incoming packet as defined in Annex A.	-	1.1
AvailableAppList	string(1024)	-	Comma-separated list of URNs, each indicating a protocol supported for use as a ProtocolIdentifier in the App table. This list MAY include any of the URNs defined in Annex A as well as other URNs defined elsewhere.	-	1.1
InternetGatewayDevice.QueueManagement.-Classification.{i}.	object	W	Classification table.	-	1.1
ClassificationKey	unsignedInt	-	Unique key for each classification entry. This parameter is OBSOLETED because it serves no purpose (no other parameter references it).	-	1.1
ClassificationEnable	boolean	W	Enables or disables this classifier.	False	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
ClassificationStatus	string	-	The status of this classifier. Enumeration of: "Disabled" "Enabled" "Error" (OPTIONAL) The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	"Disabled"	1.1
ClassificationOrder	unsignedInt [1:]	W	Position of the classification entry in the order of precedence. A value of 1 indicates the first entry considered. For each packet, the highest ordered entry that matches the classification criteria is applied. All lower order entries are ignored. When this value is modified, if the value matches that of an existing entry, the Order value for the existing entry and all lower Order entries is incremented (lowered in precedence) to ensure uniqueness of this value. A deletion causes Order values to be compacted. When a value is changed, incrementing occurs before compaction.	-[5]	1.1
ClassInterface	string(256)	W	Classification criterion. Specifies the LAN or WAN ingress interface associated with this entry. The content is the full hierarchical parameter name of the particular WANDevice, WANConnectionDevice, WAN**-Connection, LANDevice, LAN**InterfaceConfig, or WLANConfiguration object. The following are WAN interface examples: "InternetGatewayDevice.WANDevice.2" "InternetGatewayDevice.WAN Device. 1.WAN-ConnectionDevice.2.WANPPPConnection.1" The following are LAN interface examples: "InternetGatewayDevice.LANDevice.3" "InternetGatewayDevice.LANDevice. 1.LAN-EthernetInterfaceConfig.2" "InternetGatewayDevice.LANDevice. 1 .WLAN-Configuration.3" The string "WAN" indicates this entry is to apply to traffic entering from any WAN interface. The string "LAN" indicates this entry is to apply to traffic entering from any LAN interface. The string "Local" indicates this entry is to apply to IP-layer traffic entering from a local source within the Internet Gateway Device. An empty value indicates this classification entry is to apply to all sources.	<Empty>	1.1
DestIP	string	W	Classification criterion. Destination IP address. An empty value indicates this criterion is not used for classification.	<Empty>	1.1
DestMask	string	W	Destination IP address mask. If non-empty, only the indicated network portion of the DestIP address is to be used for classification. An empty value indicates that the full DestIP address is to be used for classification.	<Empty>	1.1

5 The value on creation of a Classification table entry MUST be one greater than the largest current value.

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
DestIPExclude	boolean	W	If false, the class includes only those packets that match the (masked) DestIP entry, if specified. If true, the class includes all packets except those that match the (masked) DestIP entry, if specified.	False	1.1
SourceIP	string	W	Classification criterion. Source IP address. An empty value indicates this criterion is not used for classification.	<Empty>	1.1
SourceMask	string	W	Source IP address mask. If non-empty, only the indicated network portion of the SourceIP address is to be used for classification. An empty value indicates that the full SourceIP address is to be used for classification.	<Empty>	1.1
SourceIPExclude	boolean	W	If false, the class includes only those packets that match the (masked) SourceIP entry, if specified. If true, the class includes all packets except those that match the (masked) SourceIP entry, if specified.	False	1.1
Protocol	int[-1:]	W	Classification criterion. Protocol number. A value of -1 indicates this criterion is not used for classification.	-1	1.1
ProtocolExclude	boolean	W	If false, the class includes only those packets that match the Protocol entry, if specified. If true, the class includes all packets except those that match the Protocol entry, if specified.	False	1.1
DestPort	int[-1:]	W	Classification criterion. Destination port number. A value of -1 indicates this criterion is not used for classification.	-1	1.1
DestPortRangeMax	int[-1:]	W	Classification criterion. If specified, indicates the classification criterion is to include the port range from DestPort through DestPortRangeMax (inclusive). If specified, Dest-PortRangeMax MUST be greater than or equal to DestPort. A value of -1 indicates that no port range is specified.	-1	1.1
DestPortExclude	boolean	W	If false, the class includes only those packets that match the DestPort entry (or port range), if specified. If true, the class includes all packets except those that match the DestPort entry (or port range), if specified.	False	1.1
SourcePort	int[-1:]	W	Classification criterion. Source port number. A value of -1 indicates this criterion is not used for classification.	-1	1.1
SourcePortRangeMax	int[-1:]	W	Classification criterion. If specified, indicates the classification criterion is to include the port range from SourcePort through SourcePortRangeMax (inclusive). If specified, SourcePortRangeMax MUST be greater than or equal to SourcePort. A value of -1 indicates that no port range is specified.	-1	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
SourcePortExclude	boolean	W	If false, the class includes only those packets that match the SourcePort entry (or port range), if specified. If true, the class includes all packets except those that match the SourcePort entry (or port range), if specified.	False	1.1
SourceMACAddress	string	W	Classification criterion. Source MAC Address. An empty value indicates this criterion is not used for classification.	<Empty>	1.1
SourceMACMask	string	W	Bit-mask for the MAC address, where matching of a packet's MAC address with the SourceMAC-Address is only to be done for bit positions set to one in the mask. A mask of FF:FF:FF:FF:FF:FF or an empty string indicates all bits of the Source-MACAdress are to be used for classification.	<Empty>	1.1
SourceMACExclude	boolean	W	If false, the class includes only those packets that match the (masked) SourceMACAddress entry, if specified. If true, the class includes all packets except those that match the (masked) SourceMACAddress entry, if specified.	False	1.1
DestMACAddress	string	W	Classification criterion. Destination MAC Address. An empty value indicates this criterion is not used for classification. The use of destination MAC address as a classification criterion is primarily useful only for bridged traffic.	<Empty>	1.1
DestMACMask	string	W	Bit-mask for the MAC address, where matching of a packet's MAC address with the DestMACAddress is only to be done for bit positions set to one in the mask. A mask of FF:FF:FF:FF:FF:FF or an empty string indicates all bits of the DestMACAdress are to be used for classification.	<Empty>	1.1
DestMACExclude	boolean	W	If false, the class includes only those packets that match the (masked) DestMACAddress entry, if specified. If true, the class includes all packets except those that match the (masked) DestMACAddress entry, if specified.	False	1.1
Ethertype	int[-1:]	W	Classification criterion. Ethertype as indicated in either the Ethernet or SNAP Type header. A value of -1 indicates this criterion is not used for classification.	-1	1.1
EthertypeExclude	boolean	W	If false, the class includes only those packets that match the Ethertype entry, if specified. If true, the class includes all packets except those that match the Ethertype entry, if specified.	False	1.1
SSAP	int[-1:]	W	Classification criterion. SSAP element in the LLC header. A value of -1 indicates this criterion is not used for classification.	-1	1.1
SSAPExclude	boolean	W	If false, the class includes only those packets that match the SSAP entry, if specified. If true, the class includes all packets except those that match the SSAP entry, if specified.	False	1.1
DSAP	int[-1:]	W	Classification criterion. DSAP element in the LLC header. A value of -1 indicates this criterion is not used for classification.	-1	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
DSAPExclude	boolean	W	If false, the class includes only those packets that match the DSAP entry, if specified. If true, the class includes all packets except those that match the DSAP entry, if specified.	False	1.1
LLCControl	int[-1:]	W	Classification criterion. Control element in the LLC header. A value of -1 indicates this criterion is not used for classification.	-1	1.1
LLCControlExclude	boolean	W	If false, the class includes only those packets that match the LLCControl entry, if specified. If true, the class includes all packets except those that match the LLCControl entry, if specified.	False	1.1
SNAPOUI	int[-1:]	W	Classification criterion. OUI element in the SNAP header. A value of -1 indicates this criterion is not used for classification.	-1	1.1
SNAPOUIExclude	boolean	W	If false, the class includes only those packets that match the SNAPOUI entry, if specified. If true, the class includes all packets except those that match the SNAPOUI entry, if specified.	False	1.1
SourceVendorClassID	string(256)	W	Classification criterion. Used to identify one or more LAN devices, value of the DHCP Vendor Class Identifier (Option 60) as defined in RFC 2132. An empty value indicates this criterion is not used for classification.	<Empty>	1.1
SourceVendorClassIDExclude	boolean	W	If false, the class includes only those packets sourced from LAN devices that match the SourceVendorClassID entry, if specified. If true, the class includes all packets except those sourced from LAN devices that match the SourceVendorClassID entry, if specified.	False	1.1
DestVendorClassID	string(256)	W	Classification criterion. Used to identify one or more LAN devices, value of the DHCP Vendor Class Identifier (Option 60) as defined in RFC 2132. An empty value indicates this criterion is not used for classification.	<Empty>	1.1
DestVendorClassIDExclude	boolean	W	If false, the class includes only those packets destined for LAN devices that match the DestVendorClassID entry, if specified. If true, the class includes all packets except those destined for LAN devices that match the DestVendorClassID entry, if specified.	False	1.1
SourceClientID	string(256)	W	Classification criterion. Used to identify one or more LAN devices, value of the DHCP Client Identifier (Option 61) as defined in RFC 2132. An empty value indicates this criterion is not used for classification.	<Empty>	1.1
SourceClientIDExclude	boolean	W	If false, the class includes only those packets sourced from LAN devices that match the SourceClientID entry, if specified. If true, the class includes all packets except those sourced from LAN devices that match the SourceClientID entry, if specified.	False	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
DestClientID	string(256)	W	Classification criterion. Used to identify one or more LAN devices, value of the DHCP Client Identifier (Option 61) as defined in RFC 2132. An empty value indicates this criterion is not used for classification.	<Empty>	1.1
DestClientIDExclude	boolean	W	If false, the class includes only those packets destined for LAN devices that match the DestClientID entry, if specified. If true, the class includes all packets except those destined for LAN devices that match the DestClientID entry, if specified.	False	1.1
SourceUserClassID	string(256)	W	Classification criterion. Used to identify one or more LAN devices, value of the DHCP User Class Identifier (Option 77) as defined in RFC 3004. An empty value indicates this criterion is not used for classification.	<Empty>	1.1
SourceUserClassIDExclude	boolean	W	If false, the class includes only those packets sourced from LAN devices that match the SourceUserClassID entry, if specified. If true, the class includes all packets except those sourced from LAN devices that match the SourceUserClassID entry, if specified.	False	1.1
DestUserClassID	string(256)	W	Classification criterion. Used to identify one or more LAN devices, value of the DHCP User Class Identifier (Option 77) as defined in RFC 3004. An empty value indicates this criterion is not used for classification.	<Empty>	1.1
DestUserClassIDExclude	boolean	W	If false, the class includes only those packets destined for LAN devices that match the DestUserClassID entry, if specified. If true, the class includes all packets except those destined for LAN devices that match the DestUserClassID entry, if specified.	False	1.1
TCPACK	boolean	W	Classification criterion. If false, this criterion is not used for classification. If true, this criterion matches with all TCP segments that have the ACK control bit set.	False	1.1
TCPACKExclude	boolean	W	If false, the class includes only those packets that match the TCPACK entry, if specified. If true, the class includes all packets except those that match the TCPACK entry, if specified.	False	1.1
IPLengthMin	unsignedInt	W	Classification criterion. Minimum IP Packet Length (including header) in bytes.	0	1.1
IPLengthMax	unsignedInt	W	Classification criterion. Maximum IP Packet Length (including header) in bytes. A value of zero indicates that no maximum is specified (an umlimited maximum length).	0	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
IPLengthExclude	boolean	W	If false, the class includes only those packets whose length (including header) falls within the inclusive range IPLengthMin through IPLengthMax. A value of zero for both IPLengthMin and IPLengthMax allows any length packet. An equal non-zero value of IPLengthMin and IPLengthMax allows only a packets with the exact length specified. If true, the class includes all packets except those whose length (including header) falls within the inclusive range IPLengthMin through IPLengthMax.	False	1.1
DSCPCheck	int[-1:]	W	Classification criterion. DiffServ codepoint (defined in RFC 2474). If set to a Class Selector Codepoint (defined in RFC 2474), all DSCP values that match the first 3 bits will be considered a valid match. A value of -1 indicates this criterion is not used for classification.	-1	1.1
DSCPExclude	boolean	W	If false, the class includes only those packets that match the DSCPCheck entry, if specified. If true, the class includes all packets except those that match the DSCPCheck entry, if specified.	False	1.1
DSCPMark	int[-2:]	W	Classification result. DSCP to mark traffic with that falls into this classification entry. A value of -1 indicates no change from the incoming packet. A value of -2 indicates automatic marking of DSCP based upon the EthernetPriority value of the incoming packet as defined in Annex A.	-1	1.1
EthernetPriorityCheck	int[-1:]	W	Classification criterion. Current Ethernet priority as defined in 802.1 D. A value of -1 indicates this criterion is not used for classification.	-1	1.1
EthernetPriorityExclude	boolean	W	If false, the class includes only those packets that match the EthernetPriorityCheck entry, if specified. If true, the class includes all packets except those that match the EthernetPriorityC heck entry, if specified.	False	1.1
EthernetPriorityMark	int[-2:]	W	Classification result. Ethernet priority code (as defined in 802.1 D) to mark traffic with that falls into this classification entry. A value of -1 indicates no change from the incoming packet. A value of -2 indicates automatic marking of EthernetPriority based upon the DSCP value of the incoming packet as defined in Annex A.	-1	1.1
VLANIDCheck	int[-1:]	W	Classification criterion. Current Ethernet VLAN ID as defined in 802.1Q. A value of -1 indicates this criterion is not used for classification.	-1	1.1
VLANIDExclude	boolean	W	If false, the class includes only those packets that match the VLANIDCheck entry, if specified. If true, the class includes all packets except those that match the VLANIDCheck entry, if specified.	False	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
ForwardingPolicy	unsignedInt	W	Classification result. Identifier of the forwarding policy associated with traffic that falls in this classification.	0	1.1
ClassPolicer	int[-1:]	W	Classification result. Instance number of the Policer table entry for traffic that falls in this classification. A value of -1 indicates a null policer.	-1	1.1
ClassQueue	int[-1:]	W	Classification result. Instance number of the Queue table entry for traffic that falls in this classification. A value of -1 indicates a null queue. ClassQueue and ClassApp are mutually exclusive and one of the two MUST be specified. If ClassQueue is null, ClassApp MUST be specified, and vice versa.	-1	1.1
ClassApp	int[-1:]	W	Classification result. Instance number of the App table entry for traffic that falls in this classification. A value of -1 indicates a null App table entry. ClassQueue and ClassApp are mutually exclusive and one of the two MUST be specified. If ClassQueue is null, ClassApp MUST be specified, and vice versa.	-1	1.1
InternetGatewayDevice.QueueManagement.-App.{i}.	object	W	Application table.	-	1.1
AppKey	unsignedInt	-	Unique key for each App table entry. This parameter is OBSOLETED because it serves no purpose (no other parameter references it).	-	1.1
AppEnable	boolean	W	Enables or disables this App table entry.	False	1.1
AppStatus	string	-	The status of this App table entry. Enumeration of: "Disabled" "Enabled" "Error" (OPTIONAL) The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	"Disabled"	1.1
ProtocolIdentifier	string(256)	W	URN identifying the protocol associated with the given application. A set of defined URNs is given in Annex A.	<Empty>	1.1
AppName	string(64)	W	Human-readable name associated with this entry in the App table.	<Empty>	1.1
AppDefaultForwardingPolicy	unsignedInt	W	Identifier of the forwarding policy associated with traffic associated with this App table entry, but not associated with any specified flow.	0	1.1
AppDefaultPolicer	int[-1:]	W	Instance number of the Policer table entry for traffic associated with this App table entry, but not associated with any specified flow. A value of -1 indicates a null policer.	-1	1.1
AppDefaultQueue	int[-1:]	W	Instance number of the Queue table entry for traffic associated with this App table entry, but not associated with any specified flow. A value of -1 indicates a null queue.	-1	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
AppDefaultDSCPMark	int[-2:]	W	DSCP to mark traffic associated with this App table entry, but not associated with any specified flow. A value of -1 indicates no change from the incoming packet. A value of -2 indicates automatic marking of DSCP based upon the EthernetPriority value of the incoming packet as defined in Annex A.	-1	1.1
AppDefaultEthernetPriorityMark	int[-2:]	W	Ethernet priority code (as defined in 802.1 D) to mark traffic associated with this App table entry, but not associated with any specified flow. A value of -1 indicates no change from the incoming packet. A value of -2 indicates automatic marking of EthernetPriority based upon the DSCP value of the incoming packet as defined in Annex A.	-1	1.1
InternetGatewayDevice.QueueManagement.-Flow.{i}.	object	W	Flow table.	-	1.1
FlowKey	unsignedInt	-	Unique key for each Flow table entry. This parameter is OBSOLETED because it serves no purpose (no other parameter references it).	-	1.1
FlowEnable	boolean	W	Enables or disables this Flow table entry.	False	1.1
FlowStatus	string	-	The status of this Flow table entry. Enumeration of: "Disabled" "Enabled" "Error" (OPTIONAL) The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	"Disabled"	1.1
FlowType	string(256)	W	URN identifying the type of flow to be associated with the specified queue and policer. A set of defined URNs is given in Annex A.	<Empty>	1.1
FlowTypeParameters	string(256)	W	List of name-value pairs representing additional criteria to identify the flow type. The use and interpretation is specific to the particular FlowType URN.Encoded using the "x-www-form-urlencoded" content type defined in [7].	<Empty>	1.1
FlowName	string(64)	W	Human-readable name associated with this entry in the Flow table.	<Empty>	1.1
AppIdentifier	int[-1:]	W	Instance number of the App table entry associated with this flow. A value of -1 indicates the flow table is not associated with any App table entry.	-1	1.1
FlowForwardingPolicy	unsignedInt	W	Identifier of the forwarding policy associated with this flow.	0	1.1
FlowPolicer	int[-1:]	W	Instance number of the Policer table entry for traffic that falls in this flow. A value of -1 indicates a null policer.	-1	1.1
FlowQueue	int[-1:]	W	Instance number of the Queue table entry for traffic that falls in this flow. A value of -1 indicates a null queue.	-1	1.1
FlowDSCPMark	int[-2:]	W	DSCP to mark traffic with that falls into this flow. A value of -1 indicates no change from the incoming packet. A value of -2 indicates automatic marking of DSCP based upon the EthernetPriority value of the incoming packet as defined in Annex A.	-1	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
FlowEthernetPriorityMark	int[-2:]	W	Ethernet priority code (as defined in 802.1 D) to mark traffic with that falls into this flow. A value of -1 indicates no change from the incoming packet. A value of -2 indicates automatic marking of EthernetPriority based upon the DSCP value of the incoming packet as defined in Annex A.	-1	1.1
InternetGatewayDevice.QueueManagement.-Policer.{i}.	object	W	Policer table.	-	1.1
PolicerKey	unsignedInt	-	Unique key for each policer entry. This parameter is OBSOLETED because it serves no purpose (no other parameter references it).	-	1.1
PolicerEnable	boolean	W	Enables or disables this policer.	False	1.1
PolicerStatus	string	-	The status of this policer. Enumeration of: "Disabled" "Enabled" "Error" (OPTIONAL) The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	"Disabled"	1.1
CommittedRate	unsignedInt	W	Committed rate allowed for this policer in bits-per-second.	0	1.1
CommittedBurstSize	unsignedInt	W	Committed Burstsize in bytes.	0	1.1
ExcessBurstSize	unsignedInt	W	Excess Burstsize in bytes. Applied for a SingleRateThreeColor meter.	0	1.1
PeakRate	unsignedInt	W	Peak rate allowed for this Meter in bits-per-second. Applied for TwoRateThreeColor meters.	0	1.1
PeakBurstSize	unsignedInt	W	Peak Burstsize in bytes. Applied for TwoRateThreeColor meters.	0	1.1
MeterType	string	W	Identifies the method of traffic measurement to be used for this policer. Enumeration of: "SimpleTokenBucket" "SingleRateThreeColor" "TwoRateThreeColor" SimpleTokenBucket makes use of CommittedRate and CommittedBurstSize. SingleRateThreeColor makes use of CommittedRate, CommittedBurstSize, and ExcessBurstSize as defined in RFC 2697. TwoRateThreeColor makes use of CommittedRate, CommittedBurstSize, PeakRate, and PeakBurstSize as defined in RFC 2698.	"Simple-Token-Bucket"	1.1
PossibleMeterTypes	string	-	Comma-separated list of supported meter types. Each item is an enumeration of: "SimpleTokenBucket" "SingleRateThreeColor" "TwoRateThreeColor"	-	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
ConformingAction	string	W	Instructions for how to handle traffic that is conforming. Enumeration of: "Null" "Drop" "Count" <DSCP Value> Null corresponds with no action. A Count action increases the meter instance count statistics. <DSCP Value> is an unsigned integer that corresponds with a mark action overwriting the traffic's DSCP with the configured DSCP.	"Null"	1.1
PartialConformingAction	string	W	Instructions for how to handle traffic that is partially conforming (colored yellow). Enumeration of: "Null" "Drop" "Count" <DSCP Value> Null corresponds with no action. A Count action increases the meter instance count statistics. <DSCP Value> is an unsigned integer that corresponds with a mark action overwriting the traffic's DSCP with the configured DSCP.Only applies for three-color meters.	"Drop"	1.1
NonConformingAction	string	W	Instructions for how to handle traffic that is non-conforming. Enumeration of: "Null" "Drop" "Count" <DSCP Value> Null corresponds with no action. A Count action increases the meter instance count statistics. <DSCP Value> is an unsigned integer that corresponds with a mark action overwriting the traffic's DSCP with the configured DSCP.	"Drop"	1.1
CountedPackets	unsignedInt	-	Number of Packets counted as result of a count meter action.	0	1.1
CountedBytes	unsignedInt	-	Number of Bytes counted as result of a count meter action.	0	1.1
InternetGatewayDevice.QueueManagement.-Queue.{i}.	object	W	Queue table. This table can contain hardware queues. The CPE MAY refuse to allow hardware queues to be deleted.	-	1.1
QueueKey	unsignedInt	-	Unique key for each queue entry. This parameter is OBSOLETED because it serves no purpose (no other parameter references it).	-	1.1
QueueEnable	boolean	W	Enables or disables this queue.	False	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
QueueStatus	string	-	The status of this queue. Enumeration of: "Disabled" "Enabled" "Error" (OPTIONAL) The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	"Disabled"	1.1
QueueInterface	string(256)	W	Egress interfaces for which the specified queue MUST exist. This parameter MUST be in one of the following forms: The full hierarchical parameter name of the particular WAN Device, WANConnection-Device, WAN**Connection, LANDevice, LAN**InterfaceConfig, or WLANConfiguration object. The string "WAN", which indicates this entry applies to all WAN interfaces. The string "LAN", which indicates this entry applies to all LAN interfaces. An empty value, which indicates this classification entry is to apply to all interfaces. Packets classified into this queue that exit through any other interface MUST instead use the default queuing behavior specified in the Queue table entry referenced by InternetGatewayDevice.-QueueManagement.DefaultQueue. For the default queue itself (the Queue table entry referenced by I nternetGatewayDevice.Queue-Management.DefaultQueue), the value of the QueueInterface parameter MUST be ignored. That is, the default queue MUST exist on all egress interfaces.	<Empty>	1.1
QueueBufferLength	unsignedInt	-	Number of bytes in the buffer. Queue buffer size for all egress interfaces for which this queue exists. If the buffer size is not the same for all such egress interfaces, this parameter MUST b0	-	1.1
QueueWeight	unsignedInt	W	Weight of this queue in case of WFQ or WRR, but only used for queues of equal precedence.	0	1.1
QueuePrecedence	unsignedInt [1:]	W	Precedence of this queue relative to others. Lower numbers imply greater precedence.	1	1.1
REDThreshold	unsignedInt [0:100]	W	Random Early Detection threshold, used only when DropAlgorithm is RED. This is the minimum threshold (min_th) and is measured as a percentage of the queue size. If the value is set to zero, the CPE MUST choose a sensible value, e.g. 5 (but the value MUST still read back as zero). In this version of the data model, there is no way to set the maximum threshold (max_th). The CPE MUST choose a sensible value, e.g. three times the minimum threshold. In this version of the data model, there is no way to set the RED weight (w_q). The CPE MUST choose a sensible value, e.g. 0.002.	0	1.1

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
REDPercentage	unsignedInt [0:100]	W	Random Early Detection percentage, used only when DropAlgorithm is RED. This is the maximum value of the packet marking probability (max_p). If the value is set to zero, the CPE MUST choose a sensible value, e.g. 10 (but the value MUST still read back as zero). In this version of the data model, there is no way to set the RED weight (w_q). The CPE MUST choose a sensible value, e.g. 0.002.	0	1.1
DropAlgorithm	string	W	Dropping algorithm used for this queue if congested. Enumeration of: "RED" (Random Early Detection [10]) "DT" (Drop Tail) "WRED" (Weighted RED) "BLUE" ([11])	"DT"	1.1
SchedulerAlgorithm	string	W	Scheduling Algorithm used by scheduler. Enumeration of: "WFQ" (Weighted Fair Queueing) "WRR" (Weighted Round Robin) "SP" (Strict Priority)	"SP"	1.1
ShapingRate	int[-1:]	W	Rate to shape this queue's traffic to. For leaky bucket (constant rate shaping), this is the constant rate. For token bucket (variable rate shaping), this is the average rate. If <= 100, in percent of the rate of the highest rate-constrained layer over which the packet will travel on egress.[6] If > 100, in bits per second. A value of -1 indicates no shaping.	-1	1.1
ShapingBurstSize	unsignedInt	W	Burst size in bytes. For both leaky bucket (constant rate shaping) and token bucket (variable rate shaping) this is the bucket size and is therefore the maximum burst size.	-	1.1
InternetGatewayDevice.LANConfigSecurity.	object	-	This object contains generic device configuration information.	-	1.0
ConfigPassword	string(64)	W	A password to allow LAN access to protected auto-configuration services. If the CPE supports TR-064 (LAN-side DSL CPE Configuration Protocol), this parameter is to be used as the "dslf-config" password (as defined in TR-064). If the CPE has a user interface with password protection enabled, this parameter is also to be used as the user password for password-protected operations. However, this parameter MUST NOT be used to set the user password if the optional parameter I nternetGatewayDevice.UserInterface.-PasswordUserSelectable is true. When read, this parameter returns an empty string, regardless of the actual value.	-	1.0

6 For example, for packets destined for a WAN DSL interface, if the egress will be on a PPP or IP link with a specified ShapingRate, the percentage is calculated relative to this rate. Otherwise, if the ATM layer is rate-constrained, then the rate is calculated relative to this rate. Otherwise, the rate is calculated relative to the physical-layer DSL rate.

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.IPPingDiagnostics.	object	-	This object provides access to an IP-layer ping test.	-	1.0
DiagnosticsState	string	W	Indicates availability of diagnostic data. One of: "None" "Requested" "Complete" "Error_CannotResolveHostName" "Error_Internal" "Error_Other" If the ACS sets the value of this parameter to Requested, the CPE MUST initiate the corresponding diagnostic test. When writing, the only allowed value is Requested. To ensure the use of the proper test parameters (the writable parameters in this object), the test parameters MUST be set either prior to or at the same time as (in the same SetParameterValues) setting the DiagnosticsState to Requested. When requested, the CPE SHOULD wait until after completion of the communication session with the ACS before starting the diagnostic. When the test is completed, the value of this parameter MUST be either Complete (if the test completed successfully), or one of the Error values listed above. If the value of this parameter is anything other than Complete, the values of the results parameters for this test are indeterminate. When the diagnostic initiated by the ACS is completed (successfully or not), the CPE MUST establish a new connection to the ACS to allow the ACS to view the results, indicating the Event code "8 DIAGNOSTICS COMPLETE" in the Inform message. After the diagnostic is complete, the value of all result parameters (all read-only parameters in this object) MUST be retained by the CPE until either this diagnostic is run again, or the CPE reboots. After a reboot, if the CPE has not retained the result parameters from the most recent test, it MUST set the value of this parameter to "None". Modifying any of the writable parameters in this object except for this one MUST result in the value of this parameter being set to "None". While the test is in progress, modifying any of the writable parameters in this object except for this one MUST result in the test being terminated and the value of this parameter being set to "None". While the test is in progress, setting this parameter to Requested (and possibly modifying other writable parameters in this object) MUST result in the test being terminated and then restarted using the current values of the test parameters.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
Interface	string(256)	W	Specifies the WAN or LAN IP-layer interface over which the test is to be performed. The content is the full hierarchical parameter name of the interface. The following is a WAN interface example: "InternetGatewayDevice.WAN Device. 1.WAN-ConnectionDevice.2.WANPPPConnection.1" The following is a LAN interface example: "InternetGatewayDevice.LANDevice. 1.LAN-HostConfigManagement.IPInterface.1" The value of this parameter MUST be either a valid interface or an empty string. An attempt to set this parameter to a different value MUST be rejected as an invalid parameter value. If an empty string is specified, the CPE MUST use the interface as directed by its routing policy (Forwarding table entries) to determine the appropriate interface.	-	1.0
Host	string(256)	W	Host name or address of the host to ping.	-	1.0
NumberOfRepetitions	unsignedInt[1:]	W	Number of repetitions of the ping test to perform before reporting the results.	-	1.0
Timeout	unsignedInt[1:]	W	Timeout in milliseconds for the ping test.	-	1.0
DataBlockSize	unsignedInt[1:65535]	W	Size of the data block in bytes to be sent for each ping.	-	1.0
DSCP	unsignedInt [0:63]	W	DiffServ codepoint to be used for the test packets. By default the CPE SHOULD set this value to zero.	-	1.0
SuccessCount	unsignedInt	-	Result parameter indicating the number of successful pings (those in which a successful response was received prior to the timeout) in the most recent ping test.	-	1.0
FailureCount	unsignedInt	-	Result parameter indicating the number of failed pings in the most recent ping test.	-	1.0
AverageResponseTime	unsignedInt	-	Result parameter indicating the average response time in milliseconds over all repetitions with successful responses of the most recent ping test. If there were no successful responses, this value MUST be zero.	-	1.0
MinimumResponseTime	unsignedInt	-	Result parameter indicating the minimum response time in milliseconds over all repetitions with successful responses of the most recent ping test. If there were no successful responses, this value MUST be zero.	-	1.0
MaximumResponseTime	unsignedInt	-	Result parameter indicating the maximum response time in milliseconds over all repetitions with successful responses of the most recent ping test. If there were no successful responses, this value MUST be zero.	-	1.0
InternetGatewayDevice.LANDevice.{i}.	object	-	Each instance contains all LAN-related objects for a given bridged subnet.	-	1.0
LANEthernetInterfaceNumberOfEntries	unsignedInt	-	Number of instances of LANEthernetInterface-Config in this LANDevice.	-	1.0
LANUSBInterfaceNumberOfEntries	unsignedInt	-	Number of instances of LANUSBInterfaceConfig in this LANDevice.	-	1.0
LANWLANConfigurationNumberOfEntries	unsignedInt	-	Number of instances of WLANConfiguration in this LANDevice.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.LANDevice.{i}.LAN-HostConfigManagement.	object	-	This object enables reporting of LAN-related device information and setting and configuring LAN IP addressing.	-	1.0
DHCPServerConfigurable	boolean	W	Enables the configuration of the DHCP server on the LAN interface. If this variable is set to false, the CPE SHOULD restore its default DHCP server settings.	-	1.0
DHCPServerEnable	boolean	W	Enables or disables the DHCP server on the LAN interface.	-	1.0
DHCP Relay	boolean	-	Indicates if the DHCP server performs the role of a server (0) or a relay (1) on the LAN interface. This parameter is DEPRECATED because the functionality that it describes is not well-defined. The CPE MAY set it to the value that it thinks most appropriate, based on its configuration.	-	1.0
MinAddress	string	W	Specifies first address in the pool to be assigned by the DHCP server on the LAN interface.	-	1.0
MaxAddress	string	W	Specifies last address in the pool to be assigned by the DHCP server on the LAN interface.	-	1.0
ReservedAddresses	string(256)	W	Comma separated list of addresses marked reserved from the address allocation pool.	-	1.0
SubnetMask	string	W	Specifies the client's network subnet mask.	-	1.0
DNSServers	string(64)	W	Comma separated list of DNS servers offered to DHCP clients. Support for more than three DNS Servers is OPTIONAL.	-	1.0
DomainName	string(64)	W	Sets the domain name to provide to clients on the LAN interface.	-	1.0
IPRouters	string(64)	W	Comma separated list of IP addresses of routers on this subnet. Also known as default gateway. Support for more than one Router address is OPTIONAL.	-	1.0
DHCPLeaseTime	int[-1:]	W	Specifies the lease time in seconds of client assigned addresses. A value of -1 indicates an infinite lease.	-	1.0
UseAllocatedWAN	string	W	Enumeration of: "Normal" "UseAllocatedSubnet" "Passthrough" If Normal, then DHCP addresses are to be allocated out of a private address pool. If UseAllocatedSubnet, instructs the CPE to allocate DHCP addresses from the WAN subnet block for the WAN connection identified in AssociatedConnection. If Passth rough, then the specified LAN Host identified by the Passth rough MAC address is given the WAN IP address.	-	1.0
AssociatedConnection	string(256)	W	Specifies the connection instance for the connection to be used for address allocation if Use-AllocatedWAN is set to UseAllocatedSubnet or Passthrough. The content is the full hierarchical parameter name of the default layer-3 connection object. Example: "InternetGatewayDevice.WAN-Device.1 .WANConnectionDevice.2.WANPPP-Connection.1".	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
PassthroughLease	unsignedInt	W	DHCP lease time in seconds given to the specified LAN Host when the WAN IP address is passed-through. Note: A temporary private IP address with short lease (for example, 1 min) might be given to the passthrough LAN Host before the WAN IP address is acquired.	-	1.0
PassthroughMACAddress	string	W	Hardware address of the LAN Host that is used to passthrough the WAN IP address if UseAllocatedWAN is “Passth rough”.	-	1.0
AllowedMACAddresses	string(512)	W	Represents a comma-separated list of hardware addresses that are allowed to connect to this connection if MACAddressControlEnabled is 1 for a given interface.	-	1.0
IPInterfaceNumberOfEntries	unsignedInt	-	Number of IP interface at LAN side of the CPE. 1 is a typical value for CPE not supporting Multihomed interfaces. Support for more than one interface instance is OPTIONAL.	-	1.0
InternetGatewayDevice.LANDevice.{i}.LAN-HostConfigManagement. IPInterface.{i}.	object	W	IP interface table.	-	1.0
Enable	boolean	W	Enables or disables this entry. On creation, an entry is disabled by default.	False	1.0
IPInterfaceIPAddress	string	W	IP address of the LAN-side interface of the CPE.	<Empty>	1.0
IPInterfaceSubnetMask	string	W	Subnet mask of the LAN-side interface of the IGD.	<Empty>	1.0
IPInterfaceAddressingType	string	W	Represents the addressing method used to assign the LAN-side IP address of the CPE on this interface. Enumeration of: “DHCP” “Static” “AutoIP”	“DHCP”	1.0
InternetGatewayDevice.LANDevice.{i}.LAN-EthernetInterfaceConfig.{i}.	object	-	This object models an Ethernet LAN connection on a CPE device. This object MUST be implemented for CPE that contain an Ethernet interface on the LAN side.	-	1.0
Enable	boolean	W	Enables or disables this interface.	-	1.0
Status	string	-	Indicates the status of this interface. Enumeration of: “Up” “NoLink” “Error” (OPTIONAL) “Disabled” The “Error” value MAY be used by the CPE to indicate a locally defined error condition.	-	1.0
MACAddress	string	-	The physical address of the interface.	-	1.0
MACAddressControlEnabled	boolean	W	Indicates whether MAC Address Control is enabled or not on this interface. MAC Address Control limits the clients that connect to those that match a list of allowed MAC addresses specified in Internet-GatewayDevice.LANDevice.{i}.LANHostConfig-Management.AllowedMACAddresses.	-	1.0
MaxBitRate	string	W	The maximum upstream and downstream bit rate available to this connection. Enumeration of: “10” “100” “1000” “Auto”	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
DuplexMode	string	W	The duplex mode available to this connection. Enumeration of: "Half" "Full" "Auto"	-	1.0
InternetGatewayDevice.LANDevice.{i}.LAN-EthernetInterfaceConfig.{i}.Stats.	object	-	This object contains statistics for an Ethernet LAN interface on a CPE device.	-	1.0
BytesSent	unsignedInt	-	Total number of bytes sent over the interface since the CPE was last reset.	-	1.0
BytesReceived	unsignedInt	-	Total number of bytes received over the interface since the CPE was last reset.	-	1.0
PacketsSent	unsignedInt	-	Total number of packets sent over the interface since the CPE was last reset.	-	1.0
PacketsReceived	unsignedInt	-	Total number of packets received over the interface since the CPE was last reset.	-	1.0
InternetGatewayDevice.LANDevice.{i}.LAN-USBInterfaceConfig.{i}.	object	-	This object models a USB LAN connection on a CPE device. This object MUST be implemented for CPE that contain a USB interface on the LAN side	-	1.0
Enable	boolean	W	Enables or disables this interface.	-	1.0
Status	string	-	Indicates the status of this interface. Enumeration of: "Up" "NoLink" "Error" (OPTIONAL) "Disabled" The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	-	1.0
MACAddress	string	-	The physical address of the interface.	-	1.0
MACAddressControlEnabled	boolean	W	Indicates whether MAC Address Control is enabled or not on this interface. MAC Address Control limits the clients that connect to those that match a list of allowed MAC addresses specified in Internet-GatewayDevice.LANDevice.{i}.LANHostConfig-Management.AllowedMACAddresses.	-	1.0
Standard	string(6)	-	USB version supported by the device.	-	1.0
Type	string	-	Type of the USB interface. Enumeration of: "Host" "Hub" "Device"	-	1.0
Rate	string	-	Speed of the USB interface. Enumeration of: "Low" "Full" "High" (USB 2.0)	-	1.0
Power	string	-	Power configuration of the USB interface. Enumeration of: "Self" "Bus" "Unknown"	-	1.0
InternetGatewayDevice.LANDevice.{i}.LAN-USBInterfaceConfig.{i}.Stats.	object	-	This object contains statistics for a USB LAN interface on a CPE device.	-	1.0
BytesSent	unsignedInt	-	Total number of bytes sent over the interface since the CPE was last reset.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
BytesReceived	unsignedInt	-	Total number of bytes received over the interface since the CPE was last reset.	-	1.0
CellsSent	unsignedInt	-	Total number of cells sent over the interface since the CPE was last reset.	-	1.0
CellsReceived	unsignedInt	-	Total number of cells received over the interface since the CPE was last reset.	-	1.0
InternetGatewayDevice.LANDevice.{i}.WLAN-Configuration.{i}.	object	-	This object models an 802.11 LAN connection on a CPE device. This object MUST be implemented for CPE that contain an 802.11 interface on the LAN side.	-	1.0
Enable	boolean	W	Enables or disables this interface. When there are multiple WLANConfiguration instances, e.g. each instance supports a different 802.11 standard or has a different security configuration, this parameter can be used to control which of the instances are currently enabled.	-	1.0
Status	string	-	Indicates the status of this interface. Enumeration of: "Up" "Error" (OPTIONAL) "Disabled" The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	-	1.0
BSSID	string	-	The MAC address of the interface.	-	1.0
MaxBitRate	string(4)	W	The maximum upstream and downstream bit rate available to this connection in Mbps. Either "Auto", or the largest of the Operational DataTransm itRates values.	-	1.0
Channel	unsignedInt [0:255]	W	The current radio channel used by the connection. Note: There is currently no way of requesting automatic selection of a channel.	-	1.0
SSID	string(32)	W	The current service set identifier in use by the connection. The SSID is an identifier that is attached to packets sent over the wireless LAN that functions as a "password" for joining a particular radio network (BSS). Note: If an access point wishes to be known by more than one SS ID, it MUST provide a WLANConfiguration instance for each SSID.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
BeaconType	string	W	The capabilities that are currently enabled on the access point (and that are announced via beacons if BeaconAdvertisementEnabled is true). Write access to this parameter enables and disables such capabilities. An attempt to set this parameter to one of the required (mandatory) values MAY be rejected if (and only if) the requested capability is not available on this WLANConfiguration instance but is available on another WLANConfigu ration instance within this Internet Gateway Device. For example, only basic 802.11 might be supported by one virtual AP, and only WPA might be supported by another virtual AP. A value of “None” means that no capabilities are currently enabled on the access point and that no stations will be able to associate with it. Enumeration of: “None” “Basic” “WPA” “11i” (OPTIONAL) “BasicandWPA” (OPTIONAL, OBSOLETED) “Basicand1 1i’ (OPTIONAL, OBSOLETED) “WPAand1 1i” (OPTIONAL) “BasicandWPAand1 1i” (OPTIONAL, OBSOLETED) “11i” SHOULD be taken to refer to both the 802.11 i specification and to the WPA2 specification (any WPA2-certified device will implement all mandatory parts of the 802.11 i standard). The OBSOLETED values are those for Basic + WPA/WPA2 mixed modes, which are not permitted by the WPA specifications.	-	1.0
MACAddressControlEnabled	boolean	W	Indicates whether MAC Address Control is enabled or not on this interface. MAC Address Control limits the clients that connect to those that match a list of allowed MAC addresses specified in Internet-GatewayDevice.LANDevice.{i}.LANHostConfig-Management.AllowedMACAddresses.	-	1.0
Standard	string	-	Indicates which IEEE 802.11 standard this WLANConfiguration instance is configured for. Enumeration of: “ “ “g” Where each value indicates support for only the indicated standard. If the device is configured simultaneously for more than one standard, a separate WLANConfiguration instance MUST be used for each supported standard.	-	1.0
WEPKeyIndex	unsignedInt [1:4]	W	The index of the default WEP key.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
KeyPassphrase	string(63)	W	A passphrase from which the WEP keys are to be generated. This parameter is the same as the parameter InternetGatewayDevice.LANDevice.{i}.WLAN-Configuration.{i}.PreSharedKey.1 .KeyPassphrase for the same instance of WLANConfiguration. When either parameter is changed, the value of the other is changed as well. If KeyPassphrase is written, all four WEP keys are immediately generated. The ACS SHOULD NOT set the passphrase and also set the WEP keys directly (the result of doing this is undefined). This MUST either be a valid key length divided by 8, in which case each byte contributes 8 bits to the key, or else MUST consist of Hex digits and be a valid key length divided by 4, in which case each byte contributes 4 bits to the key. Note: If a passphrase is used, all four WEP keys will be the same. When read, this parameter returns an empty string, regardless of the actual value.	-	1.0
WEPEncryption Level	string(64)	-	Comma-separated list of the supported key lengths. Each entry in the list is an enumeration of: "Disabled" "40-bit" "104-bit" Any additional vendor-specific values MUST start with the key length in bits. This parameter does not enforce a given encryption level but only indicates capabilities. The WEP encryption level for a given key is inferred from the key length.	-	1.0
BasicEncryptionModes	string(31)	W	Encryption modes that are available when basic 802.11 is enabled. "WEPEncryption" implies that all wireless clients can use WEP for data encryption. Enumeration of: "None" "WEPEncryption" If this WLANConfiguration instance does not support basic 802.11 then this parameter MUST NOT be present in this instance of the WLANConfiguration object.	-	1.0
BasicAuthenticationMode	string(31)	W	Authentication modes that are available when basic 802.11 is enabled. Enumeration of: "None" (Open authentication) "EAPAuthentication" (OPTIONAL) "SharedAuthentication" (OPTIONAL) If this WLANConfiguration instance does not support basic 802.11 then this parameter MUST NOT be present in this instance of the WLANConfiguration object.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
WPAEncryptionModes	string(31)	W	Encryption modes that are available when WPA is enabled. Enumeration of: "WEPEncryption" (DEPRECATED) "TKIP Encryption" "WEPandTKIPEncryption" (DEPRECATED) "AESEncryption" (OPTIONAL) "WEPandAESEncryption" (OPTIONAL, DEPRECATED) "TKIPandAESEncryption" (OPTIONAL) "WEPandTKIPandAESEncryption" (OPTIONAL, DEPRECATED) If this WLANConfiguration instance does not support WPA then this parameter MUST NOT be present in this instance of the WLANConfiguration object. The DEPRECATED values are those that combine WEP with TKIP and/or AES, which is not permitted by the WPA specifications.	-	1.0
WPAAuthenticationMode	string(31)	W	Authentication modes that are available when WPA is enabled. Enumeration of: "PSKAuthentication" "EAPAuthentication" (OPTIONAL) If this WLANConfiguration instance does not support WPA then this parameter MUST NOT be present in this instance of the WLANConfiguration object.	-	1.0
IEEE1 1 iEncryptionModes	string(31)	W	Encryption modes that are available when 802.11 i is enabled. Enumeration of: "WEPEncryption" (DEPRECATED) "TKIPEncryption" (OPTIONAL) "WEPandTKIPEncryption" (DEPRECATED) "AESEncryption" "WEPandAESEncryption" (OPTIONAL, DEPRECATED) "TKIPandAESEncryption" (OPTIONAL) "WEPandTKIPandAESEncryption" (OPTIONAL, DEPRECATED) If this WLANConfiguration instance does not support 802.11 i then this parameter MUST NOT be present in this instance of the WLANConfiguration object. "IEEE11i" SHOULD be taken to refer to both the 802.11 i specification and to the WPA2 specification (any WPA2-certified device will implement all mandatory parts of the 802.11i standard). The DEPRECATED values are those that combine WEP with TKIP and/or AES, which is not permitted by the WPA2 specifications.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
IEEE1 1 iAuthenticationMode	string(31)	W	Authentication modes that are available when 802.11i is enabled. Enumeration of: "PSKAuthentication" "EAPAuthentication" (OPTIONAL) "EAPandPSKAuthentication" (OPTIONAL) If this WLANConfiguration instance does not support 802.11 i then this parameter MUST NOT be present in this instance of the WLANConfiguration object. "IEEE11i" SHOULD be taken to refer to both the 802.11i specification and to the WPA2 specification (any WPA2-certified device will implement all mandatory parts of the 802.11i standard).	-	1.0
PossibleChannels	string (1024)	-	The possible radio channels for the wireless standard (a, b or g) and the regulatory domain. Comma-separated list. Ranges in the form "n-m" are permitted. For example, for 802.1 1b and North America, would be "1-1 1".	-	1.0
BasicDataTransmitRates	string(256)	W	Comma-separated list of the maximum access point data transmit rates in Mbps for unicast, multicast and broadcast frames. For example, a value of "1,2", indicates that unicast, multicast and broadcast frames can be transmitted at 1 Mbps and 2 Mbps.	-	1.0
OperationalDataTransmitRates	string(256)	W	Comma-separated list of the maximum access point data transmit rates in Mbps for unicast frames (a superset of BasicDataTransmitRates). Given the value of BasicDataTransmitRates from the example above, OperationalDataTransmitRates might be "1,2,5.5,11", indicating that unicast frames can additionally be transmitted at 5.5 Mbps and 11 Mbps.	-	1.0
PossibleDataTransmitRates	string(256)	-	Comma-separated list of the data transmit rates for unicast frames at which the access point will permit a station to connect (a subset of OperationalData-TransmitRates). Given the values of BasicDataTransmitRates and OperationalDataTransmitRates from the examples above, PossibleDataTransmitRates might be "1,2,5.5", indicating that the AP will only permit connections at 1 Mbps, 2 Mbps and 5.5 Mbps, even though it could theoretically accept connections at 11 Mbps.	-	1.0
InsecureOOBAccessEnabled	boolean	W	Indicates whether insecure write access via mechanisms other than the CPE WAN Management Protocol is permitted to the parameters in this object.	-	1.0
BeaconAdvertisementEnabled	boolean	W	Indicates whether or not the access point is sending out beacons.	-	1.0
RadioEnabled	boolean	W	Indicates whether or not the access point radio is enabled.	-	1.0
AutoRateFallBackEnabled	boolean	W	Indicates whether the access point can automatically reduce the data rate in the event of undue noise or contention.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
LocationDescription	string (4096)	W	An XML description of information used to identify the access point by name and physical location. The CPE is not expected to parse this string, but simply to treat it as an opaque string. An empty string indicates no location has been set.	-	1.0
RegulatoryDomain	string(3)	W	802.1 1d Regulatory Domain String. First two octets are ISO/IEC 3166-1 two-character country code. The third octet is either " " (all environments), "O" (outside) or "I" (inside).	-	1.0
TotalPSKFailures	unsignedInt	-	The number of times pre-shared key (PSK) authentication has failed (relevant only to WPA and 802.11i).	-	1.0
TotalIntegrityFailures	unsignedInt	-	The number of times the MICHAEL integrity check has failed (relevant only to WPA and 802.11 i)	-	1.0
ChannelsInUse	string (1024)	-	The channels that the access point determines to be currently in use (including any that it is using itself). Comma-separated list. Ranges in the form "n-m" are permitted.	-	1.0
DeviceOperationMode	string(31)	W	The current access-point operating mode. The optional modes permit the AP to be configured as a wireless bridge (to bridge two wired networks), repeater (a bridge that also serves wireless clients), or wireless station. Ad hoc stations are not supported. Enumeration of: "I nfrastructureAccessPoint" "WirelessBridge" (OPTIONAL) "WirelessRepeater" (OPTIONAL) "WirelessStation" (OPTIONAL)	-	1.0
DistanceFromRoot	unsignedInt	W	The number of hops from the root access point to the wireless repeater or bridge.	-	1.0
PeerBSSID	string	W	The MAC address of the peer in wireless repeater or bridge mode.	-	1.0
AuthenticationServiceMode	string	W	Indicates whether another service is involved in client authentication (LinkAuthentication for a co-located authentication server; RadiusClient for an external RADIUS server). Enumeration of: "None" "LinkAuthentication" (OPTIONAL) "RadiusClient" (OPTIONAL)	-	1.0
TotalBytesSent	unsignedInt	-	Total number of bytes sent over the interface since the CPE was last reset.	-	1.0
TotalBytesReceived	unsignedInt	-	Total number of bytes received over the interface since the CPE was last reset.	-	1.0
TotalPacketsSent	unsignedInt	-	Total number of packets sent over the interface since the CPE was last reset.	-	1.0
TotalPacketsReceived	unsignedInt	-	Total number of packets received over the interface since the CPE was last reset.	-	1.0
TotalAssociations	unsignedInt	-	The number of devices currently associated with the access point. This corresponds to the number of entries in the Associated Deivce table.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.LANDevice.{i}.WLAN-Configuration.{i}.AssociatedDevice.{i}.	object	-	A table of the devices currently associated with the access point. The size of this table is given by InternetGatewayDevice.LANDevice.{i}.WLAN-Configuration.{i}.TotalAssociations. This object MUST be implemented for CPE that contain an 802.11 interface on the LAN side.	-	1.0
AssociatedDeviceMACAddress	string	-	The MAC address of an associated device.	-	1.0
AssociatedDeviceIPAddress	string(64)	-	The IP address or DNS name of an associated device.	-	1.0
AssociatedDeviceAuthenticationState	boolean	-	Whether an associated device has authenticated (true) or not (false).	-	1.0
LastRequestedUnicastCipher	string(256)	-	The unicast cipher that was most recently used for a station with a specified MAC address (802.11 i only).	-	1.0
LastRequestedMulticastCipher	string(256)	-	The multicast cipher that was most recently used for a station with a specified MAC address (802.11 i only).	-	1.0
LastPMKId	string(256)	-	The pairwise master key (PMK) that was most recently used for a station with a specified MAC address (802.11i only).	-	1.0
InternetGatewayDevice.LANDevice.{i}.WLAN-Configuration.{i}.WEPKey.{i}.	object	-	This is a table of WEP keys. The size of this table is fixed with exactly 4 entries (with instance numbers 1 through 4). This object MUST be implemented for CPE that contain an 802.11 interface on the LAN side.	-	1.0
WEPKey	string(128)	W	A WEP key expressed as a hexadecimal string. The WEP encryption level for a given key is inferred from the key length, e.g. 10 characters for 40-bit encryption, or 26 characters for 104-bit encryption (keys do not all have to be of the same length, although they will be if the CPE uses KeyPassphrase to generate them). If KeyPassphrase is written, all four WEP keys are immediately generated. The ACS SHOULD NOT set the passphrase and also set the WEP keys directly (the result of doing this is undefined). When read, this parameter returns an empty string, regardless of the actual value.	-	1.0
InternetGatewayDevice.LANDevice.{i}.WLAN-Configuration.{i}.PreSharedKey.{i}.	object	-	This is a table of preshared keys. The size of this table is fixed with exactly 10 entries (with instance numbers 1 through 10). This object MUST be implemented for CPE that contain an 802.11 interface on the LAN side.	-	1.0
PreSharedKey	string(64)	W	A literal WPA PSK expressed as a hexadecimal string. The first table entry contains the default PreSharedKey (InternetGatewayDevice.LAN-Device.{i}.WLANConfiguration.{i}.PreSharedKey.1.-PreSharedKey). If KeyPassphrase is written, the PSK is immediately generated. The ACS SHOULD NOT set the passphrase and also set the PSK directly (the result of doing this is undefined). When read, this parameter returns an empty string, regardless of the actual value.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
KeyPassphrase	string(63)	W	A passphrase from which the PSK is to be generated. The first table entry is the same as the parameter InternetGatewayDevice.LANDevice.{i}.WLAN-Configuration.{i}.KeyPassphrase for the same instance of WLANConfiguration. When either parameter is changed, the value of the other is changed as well. If KeyPassphrase is written, the PSK is immediately generated. The ACS SHOULD NOT set the passphrase and also set the PSK directly (the result of doing this is undefined). The key is generated as specified by WPA, which uses PBKDF2 from PKCS #5: Password-based Cryptography Specification Version 2.0 (RFC2898). When read, this parameter returns an empty string, regardless of the actual value.	-	1.0
AssociatedDeviceMACAddress	string	W	The MAC address associated with a preshared key, or an empty string if no MAC address is associated with the key.	-	1.0
InternetGatewayDevice.LANDevice.{i}.Hosts.	object	-	This object provides information about each of the hosts on the LAN, including those whose IP address was allocated by the CPE using DHCP as well as hosts with statically allocated IP addresses.	-	1.0
HostNumberOfEntries	unsignedInt	-	Number of entries in the Host table.	-	1.0
InternetGatewayDevice.LANDevice.{i}.Hosts.-Host.{i}.	object	-	Host table.	-	1.0
IPAddress	string	-	Current IP Address of the host.	-	1.0
AddressSource	string	-	Indicates whether the IP address of the host was allocated by the CPE using DHCP, was assigned to the host statically, or was assigned using automatic IP address allocation. Enumeration of: “DHCP” “Static” ”AutoIP”	-	1.0
LeaseTimeRemaining	int[-1:]	-	DHCP lease time remaining in seconds. A value of -1 indicates an infinite lease. The value MUST be 0 (zero) if the AddressSource is not DHCP.	-	1.0
MACAddress	string	-	MAC address of the host.	-	1.0
HostName	string(64)	-	The device’s host name or empty string if unknown.	-	1.0
InterfaceType	string	-	Type of physical interface through which this host is connected to the CPE. Enumeration of: “Ethernet” “USB” “802.11” “HomePNA” “HomePlug” “Other”	-	1.0
Active	boolean	-	Whether or not the host is currently present on the LAN. The method of presence detection is a local matter to the CPE. The ability to list inactive hosts is OPTIONAL. If the CPE includes inactive hosts in this table, this variable MUST be set to zero for each inactive host. The length of time an inactive host remains listed in this table is a local matter to the CPE.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.WANDevice.{i}.	object	-	Each instance contains all objects associated with a particular physical WAN interface.	-	1.0
WANConnectionNumberOfEntries	unsignedInt	-	Number of instances of WANConnectionDevice in this WAN Device.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-CommonInterfaceConfig.	object	-	This object models WAN interface properties common across all connection instances.	-	1.0
EnabledForInternet	boolean	W	Used to enable or disable access to and from the Internet across all connection instances.	-	1.0
WANAccessType	string	-	Specifies the WAN access (modem) type. Enumeration of: "DSL" "Ethernet" "POTS"	-	1.0
Layer1 UpstreamMaxBitRate	unsignedInt	-	Specifies the maximum upstream theoretical bit rate for the WAN device in bits per second. This describes the maximum possible rate given the type of interface assuming the best-case operating environment, regardless of the current operating rate. For example, if the physical interface is 1 00BaseT, this value would be 100000000, regardless of the current operating rate.	-	1.0
Layer1 DownstreamMaxBitRate	unsignedInt	-	Specifies the maximum downstream theoretical bit rate for the WAN device in bits per second. This describes the maximum possible rate given the type of interface assuming the best-case operating environment, regardless of the current operating rate. For example, if the physical interface is 1 00BaseT, this value would be 100000000, regardless of the current operating rate.	-	1.0
PhysicalLinkStatus	string	-	Indicates the state of the physical connection (link) from WANDevice to a connected entity. Enumeration of: "Up" "Down" "Initializing" "Unavailable"	-	1.0
WANAccessProvider	string(256)	-	Name of the Service Provider providing link connectivity on the WAN.	-	1.0
TotalBytesSent	unsignedInt	-	The cumulative counter for total number of bytes sent upstream across all connection service instances on the WAN device.	-	1.0
TotalBytesReceived	unsignedInt	-	The cumulative counter for total number of bytes received downstream across all connection service instances on the WAN device.	-	1.0
TotalPacketsSent	unsignedInt	-	The cumulative counter for total number of packets (IP or PPP) sent upstream across all connection service instances on the WAN device.	-	1.0
TotalPacketsReceived	unsignedInt	-	The cumulative counter for total number of packets (IP or PPP) received downstream across all connection service instances on the WAN device.	-	1.0
MaximumActiveConnections	unsignedInt	-	Indicates the maximum number of active connections the CPE can simultaneously support.	-	1.0
NumberOfActiveConnections	unsignedInt	-	Number of WAN connection service instances currently active on this WAN interface.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.WANDevice.{i}.WAN-CommonInterfaceConfig.Connection.{i}.	object	-	Active connection table.	-	1.0
ActiveConnectionDeviceContainer	string(256)	-	Specifies a WAN connection device object associated with this connection instance. The content is the full hierarchical parameter name of the WAN connection device. Example: “Internet-GatewayDevice.WANDevice.1 .WANConnection-Device.2”.	-	1.0
ActiveConnectionServiceID	string(256)	-	Specifies a WAN connection object associated with this connection instance. The content is the full hierarchical parameter name of the layer-3 connection object. Example: “InternetGateway-Device.WANDevice.1 .WANConnectionDevice.2.-WANPPPConnection. 1”.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-DSLInterfaceConfig.	object	-	This object models physical layer properties specific to a single physical connection of a DSL modem used for Internet access on a CPE. This object is intended for a CPE with a DSL modem WAN interface, and is exclusive of any other WAN*InterfaceConfig object within a given WAN-Device instance.	-	1.0
Enable	boolean	W	Enables or disables the link.	-	1.0
Status	string	-	Status of the DSL physical link. Enumeration of: “Up” “Initializing” “EstablishingLink” “NoSignal” “Error” (OPTIONAL) “Disabled” The “Error” value MAY be used by the CPE to indicate a locally defined error condition.	-	1.0
ModulationType	string	-	Indicates the type of modulation used on the connection. Enumeration of: “ADSL_G.dmt” “ADSL_G.lite” “ADSL_G.dmt.bis” “ADSL_re-adsl” “ADSL_2plus” “ADLS_four” “ADSL_ANSI_T1 .413” “G.shdsl” “IDSL” “HDSL” “SDSL” “VDSL”	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
LineEncoding	string	-	The line encoding method used in establishing the Layer 1 DSL connection between the CPE and the DSLAM. Note: Generally speaking, this variable does not change after provisioning. Enumeration of: "DMT" "CAP" "2B1Q" "43BT" "PAM" "QAM"	-	1.0
DataPath	string	-	Indicates whether the data path is fast (lower latency) or interleaved (lower error rate). Enumeration of: "Interleaved" "Fast"	-	1.0
InterleaveDepth	unsignedInt	-	ADSL Interleaved depth. This variable is only applicable if DataPath = Interleaved. Otherwise, the value of this parameter MUST be zero.	-	1.0
LineNumber	int[1:]	-	Signifies the line pair that the modem is using to connection. LineNumber = 1 is the innermost pair.	-	1.0
UpstreamCurrRate	unsignedInt	-	The current physical layer aggregate data rate (expressed in Kbps) of the upstream DSL connection.	-	1.0
DownstreamCurrRate	unsignedInt	-	The current physical layer aggregate data rate (expressed in Kbps) of the downstream DSL connection.	-	1.0
UpstreamMaxRate	unsignedInt	-	The current attainable rate (expressed in Kbps) of the upstream DSL channel.	-	1.0
DownstreamMaxRate	unsignedInt	-	The current attainable rate (expressed in Kbps) of the downstream DSL channel.	-	1.0
UpstreamNoiseMargin	int	-	The current signal-to-noise ratio (expressed in 0.1 db) of the upstream DSL connection.	-	1.0
DownstreamNoiseMargin	int	-	The current signal-to-noise ratio (expressed in 0.1 db) of the downstream DSL connection.	-	1.0
UpstreamAttenuation	int	-	The current upstream signal loss (expressed in 0.1 dB).	-	1.0
DownstreamAttenuation	int	-	The current downstream signal loss (expressed in 0.1 dB).	-	1.0
UpstreamPower	int	-	The current output power at the CPE's DSL interface (expressed in 0.1 dBmV),	-	1.0
DownstreamPower	int	-	The current received power at the CPE's DSL interface (expressed in 0.1 dBmV),	-	1.0
ATURVendor	string(8)	-	ATU-R vendor identifier as defined in G.994.1 and T1.413. In the case of G.994.1 this corresponds to the four-octet provider code, which MUST be represented as eight hexadecimal digits.	-	1.0
ATURCountry	string(4)	-	T.35 country code of the ATU-R vendor as defined in G.994.1, where the two-octet value defined in G.994.1 MUST be represented as four hexadecimal digits.	-	1.0
ATURANSIStd	unsignedInt	-	ATU-R T1 .413 Revision Number as defined in T1 .413 Issue 2.	-	1.0
ATURANSIRev	unsignedInt	-	ATU-R Vendor Revision Number as defined in T1 .413 Issue 2.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
ATUCVendor	string(8)	-	ATU-C vendor identifier as defined in G.994.1 and T1.413. In the case of G.994.1 this corresponds to the four-octet provider code, which MUST be represented as eight hexadecimal digits.	-	1.0
ATUCCountry	string(4)	-	T.35 country code of the ATU-C vendor as defined in G.994.1, where the two-octet value defined in G.994.1 MUST be represented as four hexadecimal digits.	-	1.0
ATUCANSIStd	unsignedInt	-	ATU-C T1 .413 Revision Number as defined in T1 .413 Issue 2.	-	1.0
ATUCANSIRev	unsignedInt	-	ATU-C Vendor Revision Number as defined in T1.413 Issue 2.	-	1.0
TotalStart	unsignedInt	-	Number of seconds since the beginning of the period used for collection of Total statistics. Statistics SHOULD continue to be accumulated across CPE reboots, though this might not always be possible.	-	1.0
ShowtimeStart	unsignedInt	-	Number of seconds since the most recent DSL Showtime—the beginning of the period used for collection of Showtime[7] statistics.	-	1.0
LastShowtimeStart	unsignedInt	-	Number of seconds since the second most recent DSL Showtime—the beginning of the period used for collection of LastShowtime statistics. If the CPE has not retained information about the second most recent Showtime (e.g., on reboot), the start of LastShowtime statistics MAY temporarily coincide with the start of Showtime statistics.	-	1.0
CurrentDayStart	unsignedInt	-	Number of seconds since the beginning of the period used for collection of CurrentDay statistics. The CPE MAY align the beginning of each CurrentDay interval with days in the UTC time zone, but is not required to do so. Statistics SHOULD continue to be accumulated across CPE reboots, though this might not always be possible.	-	1.0
QuarterHourStart	unsignedInt	-	Number of seconds since the beginning of the period used for collection of QuarterHour statistics. The CPE MAY align the beginning of each QuarterHour interval with real-time quarter-hour intervals, but is not required to do so. Statistics SHOULD continue to be accumulated across CPE reboots, though this might not always be possible.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-DSLInterfaceConfig.Stats.	object	-	This object contains statistics for a WAN DSL physical interface.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-DSLInterfaceConfig.Stats.Total.	object	-	This object contains DSL total statistics.	-	1.0
ReceiveBlocks	unsignedInt	-	Total number of successfully received blocks, where a block is as defined in RFC 2662.	-	1.0
TransmitBlocks	unsignedInt	-	Total number of successfully transmitted blocks, where a block is as defined in RFC 2662.	-	1.0
CellDelin	unsignedInt	-	Total number of cell-delineation errors (total seconds with NCD or LCD failures as defined in ITU-T Rec. G.997.1).	-	1.0

7 Showtime is defined as successful completion of the DSL link establishment process. The Showtime statistics are those collected since the most recent establishment of the DSL link.

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
LinkRetrain	unsignedInt	-	Total number of link-retrain errors (Full Initialization Count as defined in ITU-T Rec. G.997.1).	-	1.0
InitErrors	unsignedInt	-	Total number of initialization errors (LINIT failures as defined in ITU-T Rec. G.997.1).	-	1.0
InitTimeouts	unsignedInt	-	Total number of initialization timeout errors.	-	1.0
LossOfFraming	unsignedInt	-	Total number of loss-of-framing errors (LOF failures as defined in ITU-T Rec. G.997.1).	-	1.0
ErroredSecs	unsignedInt	-	Total number of errored seconds (ES-L as defined in ITU-T Rec. G.997.1).	-	1.0
SeverelyErroredSecs	unsignedInt	-	Total number of severely errored seconds (SES-L as defined in ITU-T Rec. G.997.1).	-	1.0
FECErrors	unsignedInt	-	Total number of FEC errors detected (FEC-C as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCFECErrors	unsignedInt	-	Total number of FEC errors detected by the ATU-C (FEC-CFE as defined in ITU-T Rec. G.997.1).	-	1.0
HECErrors	unsignedInt	-	Total number of HEC errors detected (HEC-P as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCHECErrors	unsignedInt	-	Total number of HEC errors detected by the ATU-C (HEC-PFE as defined in ITU-T Rec. G.997.1).	-	1.0
CRCErrors	unsignedInt	-	Total number of CRC errors detected (CV-C as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCCRCErrors	unsignedInt	-	Total number of CRC errors detected by the ATU-C (CV-CFE as defined in ITU-T Rec. G.997.1).	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-DSLInterfaceConfig.Stats.Showtime.	object	-	This object contains DSL statistics accumulated since the most recent DSL Showtime.	-	1.0
ReceiveBlocks	unsignedInt	-	Number of successfully received blocks since the most recent DSL Showtime, where a block is as defined in RFC 2662.	-	1.0
TransmitBlocks	unsignedInt	-	Number of successfully transmitted blocks since the most recent DSL Showtime, where a block is as defined in RFC 2662.	-	1.0
CellDelin	unsignedInt	-	Number of cell-delineation errors since the most recent DSL Showtime (total seconds with NCD or LCD failures as defined in ITU-T Rec. G.997.1).	-	1.0
LinkRetrain	unsignedInt	-	Number of link-retrain errors since the most recent DSL Showtime (Full Initialization Count as defined in ITU-T Rec. G.997.1).	-	1.0
InitErrors	unsignedInt	-	Number of initialization errors since the most recent DSL Showtime (LINIT failures as defined in ITU-T Rec. G.997.1).	-	1.0
InitTimeouts	unsignedInt	-	Number of initialization timeout errors since the most recent DSL Showtime.	-	1.0
LossOfFraming	unsignedInt	-	Number of loss-of-framing errors since the most recent DSL Showtime (LOF failures as defined in ITU-T Rec. G.997.1).	-	1.0
ErroredSecs	unsignedInt	-	Number of errored seconds since the most recent DSL Showtime (ES-L as defined in ITU-T Rec. G.997.1).	-	1.0
SeverelyErroredSecs	unsignedInt	-	Number of severely errored seconds since the most recent DSL Showtime (SES-L as defined in ITU-T Rec. G.997.1).	-	1.0
FECErrors	unsignedInt	-	Number of FEC errors detected since the most recent DSL Showtime (FEC-C as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCFECErrors	unsignedInt	-	Number of FEC errors detected by the ATU-C since the most recent DSL Showtime (FEC-CFE as defined in ITU-T Rec. G.997.1).	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
HECErrors	unsignedInt	-	Number of HEC errors detected since the most recent DSL Showtime (HEC-P as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCHECErrors	unsignedInt	-	Number of HEC errors detected by the ATU-C since the most recent DSL Showtime (HEC-PFE as defined in ITU-T Rec. G.997.1).	-	1.0
CRCErrors	unsignedInt	-	Number of CRC errors detected since the most recent DSL Showtime (CV-C as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCCRCErrors	unsignedInt	-	Number of CRC errors detected by the ATU-C since the most recent DSL Showtime (CV-CFE as defined in ITU-T Rec. G.997.1).	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-DSLInterfaceConfig.Stats.LastShowtime.	object	-	This object contains DSL statistics accumulated since the second most recent DSL Showtime.	-	1.0
ReceiveBlocks	unsignedInt	-	Number of successfully received blocks since the second most recent DSL Showtime, where a block is as defined in RFC 2662.	-	1.0
TransmitBlocks	unsignedInt	-	Number of successfully transmitted blocks since the second most recent DSL Showtime, where a block is as defined in RFC 2662.	-	1.0
CellDelin	unsignedInt	-	Number of cell-delineation errors since the second most recent DSL Showtime (total seconds with NCD or LCD failures as defined in ITU-T Rec. G.997.1).	-	1.0
LinkRetrain	unsignedInt	-	Number of link-retrain errors since the second most recent DSL Showtime (Full Initialization Count as defined in ITU-T Rec. G.997.1).	-	1.0
InitErrors	unsignedInt	-	Number of initialization errors since the second most recent DSL Showtime (LINIT failures as defined in ITU-T Rec. G.997.1).	-	1.0
InitTimeouts	unsignedInt	-	Number of initialization timeout errors since the second most recent DSL Showtime.	-	1.0
LossOfFraming	unsignedInt	-	Number of loss-of-framing errors since the second most recent DSL Showtime (LOF failures as defined in ITU-T Rec. G.997.1).	-	1.0
ErroredSecs	unsignedInt	-	Number of errored seconds since the second most recent DSL Showtime (ES-L as defined in ITU-T Rec. G.997.1).	-	1.0
SeverelyErroredSecs	unsignedInt	-	Number of severely errored seconds since the second most recent DSL Showtime (SES-L as defined in ITU-T Rec. G.997.1).	-	1.0
FECErrors	unsignedInt	-	Number of FEC errors detected since the second most recent DSL Showtime (FEC-C as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCFECErrors	unsignedInt	-	Number of FEC errors detected by the ATU-C since the second most recent DSL Showtime (FEC-CFE as defined in ITU-T Rec. G.997.1).	-	1.0
HECErrors	unsignedInt	-	Number of HEC errors detected since the second most recent DSL Showtime (HEC-P as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCHECErrors	unsignedInt	-	Number of HEC errors detected by the ATU-C since the second most recent DSL Showtime (HEC-PFE as defined in ITU-T Rec. G.997.1).	-	1.0
CRCErrors	unsignedInt	-	Number of CRC errors detected since the second most recent DSL Showtime (CV-C as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCCRCErrors	unsignedInt	-	Number of CRC errors detected by the ATU-C since the second most recent DSL Showtime (CV-CFE as defined in ITU-T Rec. G.997.1).	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.WANDevice.{i}.WAN-DSLInterfaceConfig.Stats.CurrentDay.	object	-	This object contains DSL statistics accumulated during the current day.	-	1.0
ReceiveBlocks	unsignedInt	-	Number of successfully received blocks during the current day, where a block is as defined in RFC 2662.	-	1.0
TransmitBlocks	unsignedInt	-	Number of successfully transmitted blocks during the current day, where a block is as defined in RFC 2662.	-	1.0
CellDelin	unsignedInt	-	Number of cell-delineation errors during the current day (total seconds with NCD or LCD failures as defined in ITU-T Rec. G.997.1).	-	1.0
LinkRetrain	unsignedInt	-	Number of link-retrain errors during the current day (Full Initialization Count as defined in ITU-T Rec. G.997.1).	-	1.0
InitErrors	unsignedInt	-	Number of initialization errors during the current day (LINIT failures as defined in ITU-T Rec. G.997.1).	-	1.0
InitTimeouts	unsignedInt	-	Number of initialization timeout errors during the current day.	-	1.0
LossOfFraming	unsignedInt	-	Number of loss-of-framing errors during the current day (LOF failures as defined in ITU-T Rec. G.997.1).	-	1.0
ErroredSecs	unsignedInt	-	Number of errored seconds during the current day (ES-L as defined in ITU-T Rec. G.997.1).	-	1.0
SeverelyErroredSecs	unsignedInt	-	Number of severely errored seconds during the current day (SES-L as defined in ITU-T Rec. G.997.1).	-	1.0
FECErrors	unsignedInt	-	Number of FEC errors detected during the current day (FEC-C as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCFECErrors	unsignedInt	-	Number of FEC errors detected by the ATU-C during the current day (FEC-CFE as defined in ITU-T Rec. G.997.1).	-	1.0
HECErrors	unsignedInt	-	Number of HEC errors detected during the current day (HEC-P as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCHECErrors	unsignedInt	-	Number of HEC errors detected by the ATU-C during the current day (HEC-PFE as defined in ITU-T Rec. G.997.1).	-	1.0
CRCErrors	unsignedInt	-	Number of CRC errors detected during the current day (CV-C as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCCRCErrors	unsignedInt	-	Number of CRC errors detected by the ATU-C during the current day (CV-CFE as defined in ITU-T Rec. G.997.1).	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-DSLInterfaceConfig.Stats.QuarterHour.	object	-	This object contains DSL statistics accumulated during the current quarter hour.	-	1.0
ReceiveBlocks	unsignedInt	-	Number of successfully received blocks during the current quarter hour, where a block is as defined in RFC 2662.	-	1.0
TransmitBlocks	unsignedInt	-	Number of successfully transmitted blocks during the current quarter hour, where a block is as defined in RFC 2662.	-	1.0
CellDelin	unsignedInt	-	Number of cell-delineation errors during the current quarter hour (total seconds with NCD or LCD failures as defined in ITU-T Rec. G.997.1).	-	1.0
LinkRetrain	unsignedInt	-	Number of link-retrain errors during the current quarter hour (Full Initialization Count as defined in ITU-T Rec. G.997.1).	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InitErrors	unsignedInt	-	Number of initialization errors during the current quarter hour (LINIT failures as defined in ITU-T Rec. G.997.1).	-	1.0
InitTimeouts	unsignedInt	-	Number of initialization timeout errors during the current quarter hour.	-	1.0
LossOfFraming	unsignedInt	-	Number of loss-of-framing errors during the current quarter hour (LOF failures as defined in ITU-T Rec. G.997.1).	-	1.0
ErroredSecs	unsignedInt	-	Number of errored seconds during the current quarter hour (ES-L as defined in ITU-T Rec. G.997.1).	-	1.0
SeverelyErroredSecs	unsignedInt	-	Number of severely errored seconds during the current quarter hour (SES-L as defined in ITU-T Rec. G.997.1).	-	1.0
FECErrors	unsignedInt	-	Number of FEC errors detected during the current quarter hour (FEC-C as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCFECErrors	unsignedInt	-	Number of FEC errors detected by the ATU-C during the current quarter hour (FEC-CFE as defined in ITU-T Rec. G.997.1).	-	1.0
HECErrors	unsignedInt	-	Number of HEC errors detected during the current quarter hour (HEC-P as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCHECErrors	unsignedInt	-	Number of HEC errors detected by the ATU-C during the current quarter hour (HEC-PFE as defined in ITU-T Rec. G.997.1).	-	1.0
CRCErrors	unsignedInt	-	Number of CRC errors detected during the current quarter hour (CV-C as defined in ITU-T Rec. G.997.1).	-	1.0
ATUCCRCErrors	unsignedInt	-	Number of CRC errors detected by the ATU-C during the current quarter hour (CV-CFE as defined in ITU-T Rec. G.997.1).	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-EthernetInterfaceConfig.	object	-	This object models physical layer properties specific to a single Ethernet physical connection used for Internet access on a CPE. This object is intended for a CPE with an Ethernet WAN interface, and is exclusive of any other WAN*InterfaceConfig object within a given WAN-Device instance. Note that this object is *not* related to the Ethernet protocol layer sometimes used in associated with a DSL connection.	-	1.0
Enable	boolean	W	Enables or disables this interface.	-	1.0
Status	string	-	Indicates the status of this interface. Enumeration of: "Up" "NoLink" "Error" (OPTIONAL) "Disabled" The "Error" value MAY be used by the CPE to indicate a locally defined error condition.	-	1.0
MACAddress	string	-	The physical address of the interface.	-	1.0
MaxBitRate	string	W	The maximum upstream and downstream bit rate available to this connection. Enumeration of: "10" "100" "Auto"	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
DuplexMode	string	W	The duplex mode available to this connection. Enumeration of: "Half" "Full" "Auto"	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-EthernetInterfaceConfig.Stats.	object	-	This object contains statistics for an Ethernet WAN interface on a CPE device.	-	1.0
BytesSent	unsignedInt	-	Total number of bytes sent over the interface since the CPE was last reset.	-	1.0
BytesReceived	unsignedInt	-	Total number of bytes received over the interface since the CPE was last reset.	-	1.0
PacketsSent	unsignedInt	-	Total number of packets sent over the interface since the CPE was last reset.	-	1.0
PacketsReceived	unsignedInt	-	Total number of packets received over the interface since the CPE was last reset.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-DSLConnectionManagement.	object	-	This object is intended for a CPE with a DSL modem WAN interface. *Note – This object was originally created to allow WANConnection devices and services to be added dynamically in the IGD object model in TR-064 because UPnP Device Architecture 1.0 did not contain this capability natively. Because in TR-069 objects can be created and removed using the AddObject and DeleteObject RPCs, WANConnection interfaces can be managed using these TR-069 mechanisms directly. Therefore, unlike the TR-064 equivalent, the ConnectionService table within this object is Read-Only in the TR-069 InternetGatewayDevice data model context.* This object is OBSOLETED because it serves no purpose.	-	1.0
ConnectionServiceNumberOfEntries	unsignedInt	-	Number of table entries in the ConnectionService table. This parameter is OBSOLETED because it is within an OBSOLETED object. The CPE MAY return a value of 0 for this parameter, regardless of the number of connection services, in which case no ConnectionService instances will exist.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-DSLConnectionManagement.Connection-Service.{i}.	object	-	This table contains an entry for each connection service. This object is OBSOLETED because it is within an OBSOLETED object.	-	1.0
WANConnectionDevice	string(256)	-	Specifies a WAN connection device object associated with this connection instance. The content is the full hierarchical parameter name of the WAN connection device. Example: "Internet-GatewayDevice.WANDevice.1 .WANConnection-Device.2". This parameter is OBSOLETED because it is within an OBSOLETED object.	-	1.0
WANConnectionService	string(256)	-	Specifies a WAN connection object associated with this connection instance. The content is the full hierarchical parameter name of the layer-3 connection object. Example: "InternetGateway-Device.WANDevice.1 .WANConnectionDevice.2.-WANPPPConnection. 1". This parameter is OBSOLETED because it is within an OBSOLETED object.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
DestinationAddress	string(256)	-	Destination address of the WANConnectionDevice entry. One of: PVC: VPI/VCI SVC: ATM connection name SVC: ATM address The "PVC:" or "SVC:" prefix is part of the parameter value and MUST be followed by 0 or 1 space characters. For example, possible values for this parameter are "PVC:8/23" or "PVC: 0/35". This parameter is OBSOLETED because it is within an OBSOLETED object.	-	1.0
LinkType	string	-	Link Type of the WANConnectionDevice entry. One of Link Types as described in WANDSLLinkConfig. This parameter is OBSOLETED because it is within an OBSOLETED object.	-	1.0
ConnectionType	string	-	Connection Type of the WANPPPConnection or WANIPConnection entry. One of PossibleConnectionTypes as described in WAN**Connection service. This parameter is OBSOLETED because it is within an OBSOLETED object.	-	1.0
Name	string(32)	-	User-readable name of the connection. This parameter is OBSOLETED because it is within an OBSOLETED object.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.WANDevice.{i}.WAN-DSLDiagnostics.	object	-	This object is to provide diagnostic information for a CPE with an ADSL2 or ADSL2+ modem WAN interface, but MAY also be used for ADSL.	-	1.0
LoopDiagnosticsState	string	W	Indicates availability of diagnostic data. One of: "None" "Requested" "Complete" "Error_Internal" "Error_Other" If the ACS sets the value of this parameter to Requested, the CPE MUST initiate the corresponding diagnostic test, which brings down the DSL connection while the test is operating. When writing, the only allowed value is Requested. When requested, the CPE SHOULD wait until after completion of the communication session with the ACS before starting the diagnostic. When the test is completed, the value of this parameter MUST be either Complete (if the test completed successfully), or one of the Error values listed above. If the value of this parameter is anything other than Complete, the values of the results parameters for this test are indeterminate. When the diagnostic initiated by the ACS is completed, the CPE MUST establish a new connection to the ACS to allow the ACS to view the results, indicating the corresponding reason in the Inform message. After the diagnostic is complete, the value of all result parameters (all read-only parameters in this object instance) MUST be retained by the CPE until either this diagnostic is run again, or the CPE reboots. After a reboot, if the CPE has not retained the result parameters from the most recent test, it MUST set the value of this parameter to "None".	-	1.0
ACTPSDds	int	-	Downstream actual power spectral density. Interpretation of the value is as defined in ITU-T Rec. G.997.1.	-	1.0
ACTPSDus	int	-	Upstream actual power spectral density. Interpretation of the value is as defined in ITU-T Rec. G.997.1.	-	1.0
ACTATPds	int	-	Downstream actual aggregate transmitter power. Interpretation of the value is as defined in ITU-T Rec. G.997.1.	-	1.0
ACTATPus	int	-	Upstream actual aggregate transmitter power. Interpretation of the value is as defined in ITU-T Rec. G.997.1.	-	1.0
HLINSCds	int	-	Downstream linear representation scale. Interpretation of the value is as defined in ITU-T Rec. G.997.1.	-	1.0
HLINpsds	string	-	Downstream linear channel characteristics per subcarrier. Comma-separated list of integers. Each successive pair of integers represents the real and imaginary parts of each complex value. Maximum number of complex pairs is 256 for ADSL and ADSL2, 512 for ADSL2+. Interpretation of the value is as defined in ITU-T Rec. G.997.1.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
QLNpsds	string	-	Downstream quiet line noise per subcarrier. Comma-separated list of integers. Maximum number of elements is 256 for ADSL and ADSL2, 512 for ADSL2+. Interpretation of the value is as defined in ITU-T Rec. G.997.1.	-	1.0
SNRpsds	string	-	Downstream SNR per subcarrier. Comma-separated list of integers. Maximum number of elements is 256 for ADSL and ADSL2, 512 for ADSL2+. Interpretation of the value is as defined in ITU-T Rec. G.997.1.	-	1.0
BITSpsds	string	-	Downstream bit allocation per subcarrier. Comma-separated list of integers. Maximum number of elements is 256 for ADSL and ADSL2, 512 for ADSL2+. Interpretation of the value is as defined in ITU-T Rec. G.997.1.	-	1.0
GAINSpsds	string	-	Downstream gain allocation per subcarrier. Comma-separated list of integers. Maximum number of elements is 256 for ADSL and ADSL2, 512 for ADSL2+. Interpretation of the value is as defined in ITU-T Rec. G.997.1.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.	object	W	Each instance contains objects associated with a given WAN link. In this case of DSL, each instance corresponds to a single ATM VC. On creation of a WANConnectionDevice instance, there are initially no connection objects contained within.	-	1.0
WANIPConnectionNumberOfEntries	unsignedInt	-	Number of instances of WANIPConnection in this WANConnectionDevice.	-	1.0
WANPPPConnectionNumberOfEntries	unsignedInt	-	Number of instances of WANPPPConnection in this WANConnection Device.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.WANDSLLinkConfig.	object	-	This object models the ATM layer properties specific to a single physical connection of a DSL modem used for Internet access on a CPE. This object is intended for a CPE with a DSL modem WAN interface, and is exclusive of any other WAN*LinkConfig object within a given WAN-ConnectionDevice instance.	-	1.0
Enable	boolean	W	Enables or disables the link. On creation of a WANConnectionDevice, this object is disabled by default.	False	1.0
LinkStatus	string	-	Status of the link. Enumeration of: "Up" "Down" "Initializing" "Unavailable"	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
LinkType	string	W	Indicates the type of DSL connection and refers to the complete stack of protocol used for this connection. Enumeration of: "EoA" (RFC2684 bridged Ethernet over ATM) "IPoA" (RFC2684 routed IP over ATM) "PPPoA" (RFC2364 PPP over ATM) "PPPoE" (RFC2516 PPP over Ethernet on RFC2684 bridged Ethernet over ATM, DEPRECATED) "CIP" (RFC1577 Classical IP over ATM) "Unconfigured" The value "PPPoE" has always been DEPRECATED and "EoA" should be used instead (see Annex B). The ACS MUST NOT set this parameter to "PPPoE" and the CPE MUST reject attempts to do so.	"Unconfig-ured"	1.0
AutoConfig	boolean	-	Indicates if the CPE is currently using some auto configuration mechanisms for this connection. If this variable is TRUE, all writable variables in this connection instance become read-only. Any attempt to change one of these variables SHOULD fail and an error SHOULD be returned.	-	1.0
ModulationType	string	-	Indicates the type of DSL modulation used on the interface associated with this connection (duplication from WANDSLInterfaceConfig). Enumeration of: "ADSL_G.dmt" "ADSL_G.lite" "ADSL_G.dmt.bis" "ADSL_re-adsl" "ADSL_2plus" "ADLS_four" "ADSL_ANSI_T1 .413" "G.shdsl" "IDSL" "HDSL" "SDSL" "VDSL"	-	1.0
DestinationAddress	string(256)	W	Destination address of this link. One of: PVC: VPI/VCI SVC: ATM connection name SVC: ATM address The "PVC:" or "SVC:" prefix is part of the parameter value and MUST be followed by 0 or 1 space characters. For example, possible values for this parameter are "PVC:8/23" or "PVC: 0/35".	-	1.0
ATMEncapsulation	string	W	Identifies the connection encapsulation that will be used. Enumeration of "LLC" "VCMUX"	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
FCSPreserved	boolean	W	This flag tells if a checksum SHOULD be added in the ATM payload. It does not refer to the checksum of one of the ATM cells or AALX packets. In case of LLC or VCMUX encapsulation, this ATM checksum is the FCS field described in RFC 1483. It is only applicable in the upstream direction.	-	1.0
VCSearchList	string	W	Comma separated ordered list of VPI/VCI pairs to search if a link using the DestinationAddress cannot be established. In the form: VPI1/VCI1, VPI2/VCI2, ... Example: "0/35, 8/35, 1/35"	-	1.0
ATMAAL	string	-	Describes the ATM Adaptation Layer (AAL) currently in use on the PVC. Enumeration of: "AAL1" "AAL2" "AAL3" "AAL4" "AAL5"	-	1.0
ATMTransmittedBlocks	unsignedInt	-	The current count of successfully transmitted cells.	-	1.0
ATMReceivedBlocks	unsignedInt	-	The current count of successfully received cells.	-	1.0
ATMQoS	string	W	Describes the ATM Quality Of Service (QoS) being used on the VC. Enumeration of: "UBR" "CBR" "GFR" "VBR-nrt" "VBR-rt" "UBR+" "ABR"	-	1.0
ATMPeakCellRate	unsignedInt	W	Specifies the upstream peak cell rate in cells per second.	-	1.0
ATMMaximumBurstSize	unsignedInt	W	Specifies the upstream maximum burst size in cells.	-	1.0
ATMSustainableCellRate	unsignedInt	W	Specifies the upstream sustainable cell rate, in cells per second, used for traffic shaping.	-	1.0
AAL5CRCErrors	unsignedInt	-	Count of the AAL5 layer cyclic redundancy check errors. This parameter is DEPRECATED because it overlaps with the ATMCRC Errors parameter. If present, it MUST have the same value as the ATMCRCErrors parameter if AAL5 is in use, or 0 if AAL5 is not in use.	-	1.0
ATMCRCErrors	unsignedInt	-	Count of the ATM layer cyclic redundancy check (CRC) errors. This refers to CRC errors at the ATM adaptation layer (AAL). The AAL in use is indicated by the ATMAAL parameter. The value of the ATMCRCErrors parameter MUST be 0 for AAL types that have no CRCs.	-	1.0
ATMHECErrors	unsignedInt	-	Count of the number of Header Error Check related errors at the ATM layer.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.WANATMF5Loopback-Diagnostics.	object	-	This object is provides access to an ATM-layer F5 OAM loopback test.	-	1.0
DiagnosticsState	string	W	Indicates availability of diagnostic data. One of: "None" "Requested" "Complete" "Error_Internal" "Error_Other" If the ACS sets the value of this parameter to Requested, the CPE MUST initiate the corresponding diagnostic test. When writing, the only allowed value is Requested. To ensure the use of the proper test parameters (the writable parameters in this object), the test parameters MUST be set either prior to or at the same time as (in the same SetParameterValues) setting the DiagnosticsState to Requested. When requested, the CPE SHOULD wait until after completion of the communication session with the ACS before starting the diagnostic. When the test is completed, the value of this parameter MUST be either Complete (if the test completed successfully), or one of the Error values listed above. If the value of this parameter is anything other than Complete, the values of the results parameters for this test are indeterminate. When the diagnostic initiated by the ACS is completed (successfully or not), the CPE MUST establish a new connection to the ACS to allow the ACS to view the results, indicating the Event code "8 DIAGNOSTICS COMPLETE" in the Inform message. After the diagnostic is complete, the value of all result parameters (all read-only parameters in this object instance) MUST be retained by the CPE until either this diagnostic is run again, or the CPE reboots. After a reboot, if the CPE has not retained the result parameters from the most recent test, it MUST set the value of this parameter to "None". Modifying any of the writable parameters in this object except for this one MUST result in the value of this parameter being set to "None". While the test is in progress, modifying any of the writable parameters in this object except for this one MUST result in the test being terminated and the value of this parameter being set to "None". While the test is in progress, setting this parameter to Requested (and possibly modifying other writable parameters in this object) MUST result in the test being terminated and then restarted using the current values of the test parameters.	"None"	1.0
NumberOfRepetitions	unsignedInt[1:]	W	Number of repetitions of the ping test to perform before reporting the results.	1	1.0
Timeout	unsignedInt[1:]	W	Timeout in milliseconds for the ping test.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
SuccessCount	unsignedInt	-	Result parameter indicating the number of successful pings (those in which a successful response was received prior to the timeout) in the most recent ping test.	0	1.0
FailureCount	unsignedInt	-	Result parameter indicating the number of failed pings in the most recent ping test.	0	1.0
AverageResponseTime	unsignedInt	-	Result parameter indicating the average response time in milliseconds over all repetitions with successful responses of the most recent ping test. If there were no successful responses, this value MUST be zero.	0	1.0
MinimumResponseTime	unsignedInt	-	Result parameter indicating the minimum response time in milliseconds over all repetitions with successful responses of the most recent ping test. If there were no successful responses, this value MUST be zero.	0	1.0
MaximumResponseTime	unsignedInt	-	Result parameter indicating the maximum response time in milliseconds over all repetitions with successful responses of the most recent ping test. If there were no successful responses, this value MUST be zero.	0	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.WANEthernetLinkConfig.	object	-	This object models the Ethernet link layer properties specific to a single physical connection used for Internet access on a CPE. This object is intended for a CPE with an Ethernet WAN interface, and is exclusive of any other WAN*Link-Config object within a given WANConnection-Device instance. Note that this object is *not* related to the Ethernet protocol layer sometimes used in associated with a DSL connection.	-	1.0
EthernetLinkStatus	string	-	Status of the Ethernet link. Enumeration of: "Up" "Down" "Unavailable"	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.WANPOTSLinkConfig.	object	-	This object models the POTS link layer properties specific to a single physical connection used for Internet access on a CPE. This object is intended for a CPE with a POTS WAN interface, and is exclusive of any other WAN*LinkConfig object within a given WANConnectionDevice instance.	-	1.0
Enable	boolean	W	Enables or disables the link. On creation of a WANConnectionDevice, this object is disabled by default.	False	1.0
LinkStatus	string	-	Status of the link. Enumeration of: "Up" "Down" "Dialing" "Connecting" "Unavailable"	-	1.0
ISPPhoneNumber	string(64)	W	Specifies a list of strings separated by semicolon (;), each string representing a phone number to connect to a particular ISP. The digits of the phone number follow the semantics of the ITU-T E.1 64 specification. Delimiters such as brackets or hyphens between the digits of a phone number are to be ignored by the CPE.	<Empty>	1.0
ISPInfo	string(64)	W	Information identifying the Internet Service Provider. The format of the string is vendor specific.	<Empty>	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
LinkType	string	W	This variable indicates the type of POTS link used for the dialup connection. Enumeration of: "PPP_Dialup"	"PPP-_Dialup"	1.0
NumberOfRetries	unsignedInt	W	The number of times the CPE SHOULD attempt an Internet connection setup before returning error.	-	1.0
DelayBetweenRetries	unsignedInt	W	The number of seconds the CPE SHOULD wait between attempts to setup an Internet connection.	-	1.0
Fclass	string	-	Specifies capabilities of the POTS modem – i.e., if it handles data (0), fax (1,2,2.0), voice (8), DSVD (80). Comma separated list of the following enumeration: "0" " " "2.0" "8" "80"	<Empty>	1.0
DataModulationSupported	string	-	The modulation standard currently being used for data. Enumeration of: "V92" "V90" "V34" "V32bis" "V32"	<Empty>	1.0
DataProtocol	string	-	The protocol standard currently being used for data transfers. Enumeration of: "V42_LAPM" "V42_MNP4" "V1 4" "V80"	-	1.0
DataCompression	string	-	The compression technology implemented on the modem. Enumeration of: "V42bis" "MNP5"	-	1.0
PlusVTRCommandSupported	boolean	-	Capability for full duplex operation with data and voice.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.WANIPConnection.{i}.	object	W	This object enables configuration of IP connections on the WAN interface of a CPE.	-	1.0
Enable	boolean	W	Enables or disables the connection instance. On creation of a WAN IPConnection instance, it is initially disabled.	False	1.0
ConnectionStatus	string	-	Current status of the connection. Enumeration of: "Unconfigured" "Connecting" "Connected" "Pending Disconnect" "Disconneting" "Disconnected"	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
PossibleConnectionTypes	string	-	A comma-separated list indicating the types of connections possible for this connection instance. Each element of the list is an enumeration of: "Unconfigured" "IP_Routed" "IP_Bridged"	-	1.0
ConnectionType	string	W	Specifies the connection type of the connection instance. Enumeration of: "Unconfigured" "IP_Routed" "IP_Bridged"	-	1.0
Name	string(256)	W	User-readable name of this connection.	-	1.0
Uptime	unsignedInt	-	The time in seconds that this connection has been up.	-	1.0
LastConnectionError	string	-	The cause of failure for the last connection setup attempt. Enumeration of: "ERROR_NONE" "ERROR_COMMAND_ABORTED" "ERROR_NOT_ENABLED_FOR_I NTERNET" "ERROR_USER_DISCONNECT" "ERROR_ISP_DISCONNECT" "ERROR _I DLE_DISCONNECT" "ERROR_FORCED_DISCONNECT" "ERROR_NO_CARRIER" "ERROR _IP _CONFIGURATION" "ERROR_UNKNOWN"	"ERROR-_NONE"	1.0
AutoDisconnectTime	unsignedInt	W	The time in seconds since the establishment of the connection after which connection termination is automatically initiated by the CPE. This occurs irrespective of whether the connection is being used or not. A value of 0 (zero) indicates that the connection is not to be shut down automatically.	-	1.0
IdleDisconnectTime	unsignedInt	W	The time in seconds that if the connection remains idle, the CPE automatically terminates the connection. A value of 0 (zero) indicates that the connection is not to be shut down automatically.	-	1.0
WarnDisconnectDelay	unsignedInt	W	Time in seconds the Status remains in the pending disconnect state before transitioning to disconnecting state to drop the connection.	-	1.0
RSIPAvailable	boolean	-	Indicates if Realm-specific IP (RSIP) is available as a feature on the CPE.	-	1.0
NATEnabled	boolean	W	Indicates if Network Address Translation (NAT) is enabled for this connection.	-	1.0
AddressingType	string	W	The method used to assign an address to the WAN side interface of the CPE for this connection. Enumeration of: "DHCP" "Static"	-	1.0
ExternalIPAddress	string	W	This is the external IP address used by NAT for this connection. This parameter is configurable only if the AddressingType is Static.	-	1.0
SubnetMask	string	W	Subnet mask of the WAN interface. This parameter is configurable only if the AddressingType is Static.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
DefaultGateway	string	W	The IP address of the default gateway for this connection. This parameter is configurable only if the AddressingType is Static.	-	1.0
DNSEnabled	boolean	W	Whether or not the device SHOULD attempt to query a DNS server across this connection.	True	1.0
DNSOverrideAllowed	boolean	W	Whether or not a manually set, non-empty DNS address can be overridden by a DNS entry received from the WAN.	False	1.0
DNSServers	string(64)	W	Comma separated list of DNS server IP addresses for this connection. Support for more than three DNS Servers is OPTIONAL.	-	1.0
MaxMTUSize	unsignedInt [1:1540]	W	The maximum allowed size of an Ethernet frame from LAN-side devices.	-	1.0
MACAddress	string	W	The physical address of the WANIPConnection if applicable. Configurable only if MACAddressOverride is present and true (1).	-	1.0
MACAddressOverride	boolean	W	Whether the value of MACAddress parameter can be overridden. If false (0), the CPE's default value is used (or restored if it had previously been overridden).	-	1.0
ConnectionTrigger	string	W	Trigger used to establish the IP connection. Enumeration of: "OnDemand" "AlwaysOn" "Manual" The above values are defined as follows: OnDemand: If this IP connection is disconnected for any reason, it is to remain disconnected until the CPE has one or more packets to communicate over this connection, at which time the CPE automatically attempts to reestablish the connection. AlwaysOn: If this IP connection is disconnected for any reason, the CPE automatically attempts to reestablish the connection (and continues to attempt to reestablish the connection as long it remains disconnected). Manual: If this IP connection is disconnected for any reason, it is to remain disconnected until the user of the CPE explicitly instructs the CPE to reestablish the connection. Note that the reason for an IP connection becoming disconnected to begin with might be either external to the CPE, such as non-renewal of a DHCP lease or momentary disconnection of the physical interface, or internal to the CPE, such as use of the IdleDisconnectTime and/or Auto-DisconnectTime parameters in this object. Note also that the means by which a CPE would keep an IP connection disconnected (while waiting for the designated trigger) if it is otherwise physically connected and has an IP address is a local matter specific to the implementation of the CPE.	"On-Demand"	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
RouteProtocolRx	string	W	Defines the Rx protocol to be used. Enumeration of: "Off" "RIPv1" (OPTIONAL) "RIPv2" (OPTIONAL) "OSPF" (OPTIONAL)	"Off"	1.0
ShapingRate	int[-1:]	W	Rate to shape this connection's egress traffic to. For leaky bucket (constant rate shaping), this is the constant rate. For token bucket (variable rate shaping), this is the average rate. If <= 100, in percent of the rate of the highest rate-constrained layer over which the packet will travel on egress.[8] If > 100, in bits per second. A value of -1 indicates no shaping.	-1	1.1
ShapingBurstSize	unsignedInt	W	Burst size in bytes. For both leaky bucket (constant rate shaping) and token bucket (variable rate shaping) this is the bucket size and is therefore the maximum burst size.	-	1.1
PortMappingNumberOfEntries	unsignedInt	-	Total number of port mapping entries.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.WANIPConnection.{i}.-PortMapping.{i}.	object	W	Port mapping table. This table MUST contain all NAT port mappings associated with this connection, including static and dynamic port mappings programmatically created via local control protocol, such as UPnP. This table MUST NOT contain dynamic NAT binding entries associated with the normal operation of NAT. At most one entry in an instance of this table can exist with all of the same values for RemoteHost, ExternalPort, and PortMapping Protocol. If the ACS attempts to set the parameters of an existing entry such that this requirement would be violated, the CPE MUST reject the request. In this case, the SetParameterValues response MUST include a SetParameterValuesFault element for each parameter in the corresponding request whose modification would have resulted in such a violation. On creation of a new table entry, the CPE MUST choose default values for ExternalPort and PortMapping Protocol such that the new entry does not conflict with any existing entry.	-	1.0
PortMappingEnabled	boolean	W	Enables or disables the port mapping instance. On creation, an entry is disabled by default.	False	1.0

8 For example, for packets destined for a WAN DSL interface, if the ATM layer is rate-constrained, then the rate is calculated relative to this rate. Otherwise, the rate is calculated relative to the physical-layer DSL rate.

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
PortMappingLeaseDuration	unsignedInt	W	Determines the time to live, in seconds, of a port-mapping lease, where "time to live" means the number of seconds before the port mapping expires. A value of 0 means the port mapping is static. Support for dynamic (non-static) port mappings is OPTIONAL. That is, the only value for PortMappingLeaseDuration that MUST be supported is 0. For a dynamic (non-static) port mapping, when this parameter is read, the value represents the time remaining on the port-mapping lease. That is, for a dynamic port mapping, the value counts down toward 0. When a dynamic port-mapping lease expires, the CPE MUST automatically terminate that port mapping, and MUST automatically delete the corresponding PortMapping table entry.	-	1.0
RemoteHost	string	W	This parameter is the IP address of the source of inbound packets. An empty string indicates a 'wildcard' (this will be a wildcard in most cases). CPE are REQUIRED only to support wildcards. When RemoteHost is a wildcard, all traffic sent to the ExternalPort on the WAN interface of the gateway is forwarded to the InternalClient on the InternalPort. When RemoteHost is specified as one external IP address, the NAT will only forward inbound packets from this RemoteHost to the InternalClient, all other packets will be dropped. If a CPE supports non-wildcard values for RemoteHost, it MAY additionally support the ability to have more than one port mapping with the same ExternalPort and PortMappingProtocol, but with differing values of RemoteHost. When wildcard values are used for RemoteHost and/or ExternalPort, the following precedence order applies (with the highest precedence listed first): 1. Explicit RemoteHost, explicit ExternalPort 2. Explicit RemoteHost, wildcard ExternalPort 3. Wildcard RemoteHost, explicit ExternalPort 4. Wildcard RemoteHost, wildcard ExternalPort If an incoming packet matches the criteria associated with more than one entry in this table, the CPE MUST apply the port mapping associated with the highest precedence entry. At most one entry in this table can exist with all of the same values for RemoteHost, ExternalPort, and PortMappingProtocol.	<Empty>	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
ExternalPort	unsignedInt	W	The external port that the NAT gateway would listen on for connection requests to a corresponding InternalPort. Inbound packets to this external port on the WAN interface SHOULD be forwarded to InternalClient on the InternalPort. A value of zero (0) represents a 'wildcard.' If this value is a wildcard, connection request on all external ports (that are not otherwise mapped) will be forwarded to InternalClient. In the wildcard case, the value(s) of InternalPort on InternalClient are ignored. When wildcard values are used for RemoteHost and/or ExternalPort, the following precedence order applies (with the highest precedence listed first): 1. Explicit RemoteHost, explicit ExternalPort 2. Explicit RemoteHost, wildcard ExternalPort 3. Wildcard RemoteHost, explicit ExternalPort 4. Wildcard RemoteHost, wildcard ExternalPort If an incoming packet matches the criteria associated with more than one entry in this table, the CPE MUST apply the port mapping associated with the highest precedence entry. At most one entry in this table can exist with all of the same values for RemoteHost, ExternalPort, and PortMappingProtocol.	-	1.0
InternalPort	unsignedInt	W	The port on InternalClient that the gateway SHOULD forward connection requests to. A value of zero (0) is not allowed.	-	1.0
PortMappingProtocol	string	W	The protocol of the port mapping. Enumeration of: "TCP" "UDP" At most one entry in this table can exist with all of the same values for RemoteHost, ExternalPort, and PortMappingProtocol.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternalClient	string(256)	W	The IP address or DNS host name of an internal client (on the LAN). Support for an IP address is mandatory. If InternalClient is specified as an IP address and the LAN device's IP address subsequently changes, the port mapping MUST remain associated with the original IP address. Support for DNS host names is OPTIONAL. If InternalClient is specified as a DNS host name and the LAN device's IP address subsequently changes, the port mapping MUST remain associated with this LAN device. In this case, it is the responsibility of the CPE to maintain the name-to-address mapping in the event of IP address changes. This can be accomplished, for example, by assigning the DNS host name via use of DHCP option 12 (Host Name) or option 81 (FQDN). Note that the ACS can learn the host name associated with a given LAN device via the Hosts table (InternetGatewayDevice.LANDevice.{i}.Hosts.). Read access to this parameter MUST always return the exact value that was last set by the ACS. For example, if the internal client is set to a DNS host name, it MUST read back as a DNS host name and not as an IP address. An empty string indicates an unconfigured InternalClient. If this parameter is unconfigured, this port mapping MUST NOT be operational. It MUST be possible to set the InternalClient to the broadcast IP address 255.255.255.255 for UDP mappings. This is to enable multiple NAT clients to use the same well-known port simultaneously.	<Empty>	1.0
PortMappingDescription	string(256)	W	User-readable description of this port mapping.	<Empty>	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.WANIPConnection.{i}.-Stats.	object	-	This object contains statistics for all connections within the same WANConnectionDevice that share a common MAC address. The contents of this object SHOULD be identical for each such connection. This object is intended only for WANConnection-Devices that can support an Ethernet-layer on this interface (e.g., PPPoE, IPoE).	-	1.0
EthernetBytesSent	unsignedInt	-	Total number of bytes sent over all connections within the same WANConnectionDevice that share a common MAC address since the CPE was last reset.	-	1.0
EthernetBytesReceived	unsignedInt	-	Total number of bytes received over all connections within the same WANConnection-Device that share a common MAC address since the CPE was last reset.	-	1.0
EthernetPacketsSent	unsignedInt	-	Total number of Ethernet packets sent over all connections within the same WANConnection-Device that share a common MAC address since the CPE was last reset.	-	1.0
EthernetPacketsReceived	unsignedInt	-	Total number of Ethernet packets received over all connections within the same WANConnection-Device that share a common MAC address since the CPE was last reset.	-	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.WANPPPConnection.{i}.	object	W	This object enables configuration of PPP connections on the WAN interface of a CPE.	-	1.0
Enable	boolean	W	Enables or disables the connection instance. On creation of a WANPPPConnection instance, it is initially disabled.	False	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
ConnectionStatus	string	-	Current status of the connection. Enumeration of: "Unconfigured" "Connecting" "Authenticating" "Connected" "Pending Disconnect" "Disconnecting" "Disconnected"	-	1.0
PossibleConnectionTypes	string	-	A comma-separated list indicating the types of connections possible for this connection instance. Each element of the list is an enumeration of: "Unconfigured" "IP_Routed" "DHCP_Spoofed" "PPPoE_Bridged" "PPPoE_Relay" "PPTP_Relay" "L2TP_Relay"	-	1.0
ConnectionType	string	W	Specifies the connection type of the connection instance. Enumeration of: "Unconfigured" "IP_Routed" "DHCP_Spoofed" "PPPoE_Bridged" "PPPoE_Relay" "PPTP_Relay" "L2TP_Relay"	-	1.0
Name	string(256)	W	User-readable name of this connection.	-	1.0
Uptime	unsignedInt	-	The time in seconds that this connection has been up.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
LastConnectionError	string	-	The cause of failure for the last connection setup attempt. Enumeration of: "ERROR_NONE" "ERROR_ISP_TIME_OUT" "ERROR_COMMAND_ABORTED" "ERROR_NOT_ENABLED_FOR_I NTERNET" "ERROR_BAD_PHONE_NUMBER" "ERROR_USER_DISCONNECT" "ERROR_ISP_DISCONNECT" "ERROR_IDLE_DISCONNECT" "ERROR_FORCED_DISCONNECT" "ERROR_SERVER_OUT_OF_RESOURCES" "ERROR_RESTRICTED_LOGON_HOU RS" "ERROR_ACCOUNT_DISABLED" "ERROR_ACCOUNT_EXPIRED" "ERROR_PASSWORD_EXPIRED" "ERROR_AUTHENTICATION_FAILURE" "ERROR_NO_DIALTONE" "ERROR_NO_CARRIER" "ERROR_NO_ANSWER" "ERROR_LINE_BUSY" "ERROR_UNSUPPORTED_BITSPERSECOND" "ERROR_TOO_MANY_LINE_ERRORS" "ERROR _I P_CONFIGURATION" "ERROR_UNKNOWN"	"ERROR-_NONE"	1.0
AutoDisconnectTime	unsignedInt	W	The time in seconds since the establishment of the connection after which connection termination is automatically initiated by the CPE. This occurs irrespective of whether the connection is being used or not. A value of 0 (zero) indicates that the connection is not to be shut down automatically.	-	1.0
IdleDisconnectTime	unsignedInt	W	The time in seconds that if the connection remains idle, the CPE automatically terminates the connection. A value of 0 (zero) indicates that the connection is not to be shut down automatically.	-	1.0
WarnDisconnectDelay	unsignedInt	W	Time in seconds the Status remains in the pending disconnect state before transitioning to disconnecting state to drop the connection.	-	1.0
RSIPAvailable	boolean	-	Indicates if Realm-specific IP (RSIP) is available as a feature on the CPE.	-	1.0
NATEnabled	boolean	W	Indicates if Network Address Translation (NAT) is enabled for this connection.	-	1.0
Username	string(64)	W	Username to be used for authentication.	<Empty>	1.0
Password	string(64)	W	Password to be usef for authentication. When read, this parameter returns an empty string, regardless of the actual value.	<Empty>	1.0
PPPEncryptionProtocol	string	-	Describes the PPP encryption protocol used between the WAN device and the ISP POP. Enumeration of: "None" "MPPE"	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
PPPCompressionProtocol	string	-	Describes the PPP compression protocol used between the WAN device and the ISP POP. Enumeration of: "None" "Van Jacobsen" "STAC LZS"	-	1.0
PPPAuthenticationProtocol	string	-	Describes the PPP authentication protocol used between the WAN device and the ISP POP. Enumeration of: "PAP" "CHAP" "MS-CHAP"	-	1.0
ExternalIPAddress	string	-	This is the external IP address used by NAT for this connection.	-	1.0
RemoteIPAddress	string	-	The remote IP address for this connection.	-	1.0
MaxMRUSize	unsignedInt [1:1540]	W	The maximum allowed size of frames sent from the remote peer.	-	1.0
CurrentMRUSize	unsignedInt [1:1540]	-	The current MRU in use over this connection.	-	1.0
DNSEnabled	boolean	W	Whether or not the device SHOULD attempt to query a DNS server across this connection.	True	1.0
DNSOverrideAllowed	boolean	W	Whether or not a manually set, non-empty DNS address can be overridden by a DNS entry received from the WAN.	False	1.0
DNSServers	string(64)	W	Comma separated list of DNS server IP addresses for this connection. Support for more than three DNS Servers is OPTIONAL.	-	1.0
MACAddress	string	W	The physical address of the WANPPPConnection if applicable. Configurable only if MACAddressOverride is present and true (1). If TransportType is "PPPoA", the value of this parameter is irrelevant and MUST be an empty string.	-	1.0
MACAddressOverride	boolean	W	Whether the value of MACAddress parameter can be overridden. If false (0), the CPE's default value is used (or restored if it had previously been overridden). If TransportType is "PPPoA", the value of this parameter is irrelevant and MUST be false.	-	1.0
TransportType	string	-	PPP transport type of the connection. Enumeration of: "PPPoA" "PPPoE" "L2TP" (for future use) "PPTP" (for future use)	-	1.0
PPPoEACName	string(256)	W	PPPoE Access Concentrator.	<Empty>	1.0
PPPoEServiceName	string(256)	W	PPPoE Service Name.	<Empty>	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
ConnectionTrigger	string	W	Trigger used to establish the PPP connection. Enumeration of: "OnDemand" "AlwaysOn" "Manual" The above values are defined as follows: OnDemand: If this PPP connection is disconnected for any reason, it is to remain disconnected until the CPE has one or more packets to communicate over this connection, at which time the CPE automatically attempts to reestablish the connection. AlwaysOn: If this PPP connection is disconnected for any reason, the CPE automatically attempts to reestablish the connection (and continues to attempt to reestablish the connection as long it remains disconnected). Manual: If this PPP connection is disconnected for any reason, it is to remain disconnected until the user of the CPE explicitly instructs the CPE to reestablish the connection. Note that the reason for a PPP connection becoming disconnected to begin with might be either external to the CPE, such as termination by the BRAS or momentary disconnection of the physical interface, or internal to the CPE, such as use of the IdleDisconnectTime and/or Auto-DisconnectTime parameters in this object.	"On-Demand"	1.0
RouteProtocolRx	string	W	Defines the Rx protocol to be used. Enumeration of: "Off" "RIPv1" (OPTIONAL) "RIPv2" (OPTIONAL) "OSPF" (OPTIONAL)	"Off"	1.0
PPPLCPEcho	unsignedInt	-	PPP LCP Echo period in seconds.	-	1.0
PPPLCPEchoRetry	unsignedInt	-	Number of PPP LCP Echo retries within an echo period.	-	1.0
ShapingRate	int[-1:]	W	Rate to shape this connection's egress traffic to. For leaky bucket (constant rate shaping), this is the constant rate. For token bucket (variable rate shaping), this is the average rate. If <= 100, in percent of the rate of the highest rate-constrained layer over which the packet will travel on egress.[8] If > 100, in bits per second. A value of -1 indicates no shaping.	-1	1.1
ShapingBurstSize	unsignedInt	W	Burst size in bytes. For both leaky bucket (constant rate shaping) and token bucket (variable rate shaping) this is the bucket size and is therefore the maximum burst size.	-	1.1
PortMappingNumberOfEntries	unsignedInt	-	Total number of port mapping entries.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.WANPPPConnection.{i}.-PortMapping.{i}.	object	W	Port mapping table. This table MUST contain all NAT port mappings associated with this connection, including static and dynamic port mappings programmatically created via local control protocol, such as UPnP. This table MUST NOT contain dynamic NAT binding entries associated with the normal operation of NAT. At most one entry in an instance of this table can exist with all of the same values for RemoteHost, ExternalPort, and PortMapping Protocol. If the ACS attempts to set the parameters of an existing entry such that this requirement would be violated, the CPE MUST reject the request. In this case, the SetParameterValues response MUST include a SetParameterValuesFault element for each parameter in the corresponding request whose modification would have resulted in such a violation. On creation of a new table entry, the CPE MUST choose default values for ExternalPort and PortMapping Protocol such that the new entry does not conflict with any existing entry.	-	1.0
PortMappingEnabled	boolean	W	Enables or disables the port mapping instance. On creation, an entry is disabled by default.	False	1.0
PortMappingLeaseDuration	unsignedInt	W	Determines the time to live, in seconds, of a port-mapping lease, where “time to live” means the number of seconds before the port mapping expires. A value of 0 means the port mapping is static. Support for dynamic (non-static) port mappings is OPTIONAL. That is, the only value for PortMappingLeaseDuration that MUST be supported is 0. For a dynamic (non-static) port mapping, when this parameter is read, the value represents the time remaining on the port-mapping lease. That is, for a dynamic port mapping, the value counts down toward 0. When a dynamic port-mapping lease expires, the CPE MUST automatically terminate that port mapping, and MUST automatically delete the corresponding PortMapping table entry.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
RemoteHost	string	W	This parameter is the IP address of the source of inbound packets. An empty string indicates a 'wildcard' (this will be a wildcard in most cases). CPE are REQUIRED only to support wildcards. When RemoteHost is a wildcard, all traffic sent to the ExternalPort on the WAN interface of the gateway is forwarded to the InternalClient on the InternalPort. When RemoteHost is specified as one external IP address, the NAT will only forward inbound packets from this RemoteHost to the InternalClient, all other packets will be dropped. If a CPE supports non-wildcard values for RemoteHost, it MAY additionally support the ability to have more than one port mapping with the same ExternalPort and PortMappingProtocol, but with differing values of RemoteHost. When wildcard values are used for RemoteHost and/or ExternalPort, the following precedence order applies (with the highest precedence listed first): 1. Explicit RemoteHost, explicit ExternalPort 2. Explicit RemoteHost, wildcard ExternalPort 3. Wildcard RemoteHost, explicit ExternalPort 4. Wildcard RemoteHost, wildcard ExternalPort If an incoming packet matches the criteria associated with more than one entry in this table, the CPE MUST apply the port mapping associated with the highest precedence entry. At most one entry in this table can exist with all of the same values for RemoteHost, ExternalPort, and PortMappingProtocol.	<Empty>	1.0
ExternalPort	unsignedInt	W	The external port that the NAT gateway would listen on for connection requests to a corresponding InternalPort. Inbound packets to this external port on the WAN interface SHOULD be forwarded to InternalClient on the InternalPort. A value of zero (0) represents a 'wildcard.' If this value is a wildcard, connection request on all external ports (that are not otherwise mapped) will be forwarded to InternalClient. In the wildcard case, the value(s) of InternalPort on InternalClient are ignored. When wildcard values are used for RemoteHost and/or ExternalPort, the following precedence order applies (with the highest precedence listed first): 1. Explicit RemoteHost, explicit ExternalPort 2. Explicit RemoteHost, wildcard ExternalPort 3. Wildcard RemoteHost, explicit ExternalPort 4. Wildcard RemoteHost, wildcard ExternalPort If an incoming packet matches the criteria associated with more than one entry in this table, the CPE MUST apply the port mapping associated with the highest precedence entry. At most one entry in this table can exist with all of the same values for RemoteHost, ExternalPort, and PortMappingProtocol.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
InternalPort	unsignedInt	W	The port on InternalClient that the gateway SHOULD forward connection requests to. A value of zero (0) is not allowed.	-	1.0
PortMappingProtocol	string	W	The protocol of the port mapping. Enumeration of: "TCP" "UDP" At most one entry in this table can exist with all of the same values for RemoteHost, ExternalPort, and PortMappingProtocol.	-	1.0
InternalClient	string(256)	W	The IP address or DNS host name of an internal client (on the LAN). Support for an IP address is mandatory. If InternalClient is specified as an IP address and the LAN device's IP address subsequently changes, the port mapping MUST remain associated with the original IP address. Support for DNS host names is OPTIONAL. If InternalClient is specified as a DNS host name and the LAN device's IP address subsequently changes, the port mapping MUST remain associated with this LAN device. In this case, it is the responsibility of the CPE to maintain the name-to-address mapping in the event of IP address changes. This can be accomplished, for example, by assigning the DNS host name via use of DHCP option 12 (Host Name) or option 81 (FQDN). Note that the ACS can learn the host name associated with a given LAN device via the Hosts table (InternetGatewayDevice.LANDevice.{i}.Hosts.). Read access to this parameter MUST always return the exact value that was last set by the ACS. For example, if the internal client is set to a DNS host name, it MUST read back as a DNS host name and not as an IP address. An empty string indicates an unconfigured InternalClient. If this parameter is unconfigured, this port mapping MUST NOT be operational. It MUST be possible to set the InternalClient to the broadcast IP address 255.255.255.255 for UDP mappings. This is to enable multiple NAT clients to use the same well-known port simultaneously.	<Empty>	1.0
PortMappingDescription	string(256)	W	User-readable description of this port mapping.	<Empty>	1.0
InternetGatewayDevice.WANDevice.{i}.WAN-ConnectionDevice.{i}.WANPPPConnection.{i}.-Stats.	object	-	This object contains statistics for all connections within the same WANConnectionDevice that share a common MAC address. The contents of this object SHOULD be identical for each such connection. This object is intended only for WANConnection-Devices that can support an Ethernet-layer on this interface (e.g., PPPoE, IPoE).	-	1.0
EthernetBytesSent	unsignedInt	-	Total number of bytes sent over all connections within the same WANConnectionDevice that share a common MAC address since the CPE was last reset.	-	1.0
EthernetBytesReceived	unsignedInt	-	Total number of bytes received over all connections within the same WANConnection-Device that share a common MAC address since the CPE was last reset.	-	1.0

Name[1]	Type	Write[2]	Description	Default[3]	Version[4]
EthernetPacketsSent	unsignedInt	-	Total number of Ethernet packets sent over all connections within the same WANConnection-Device that share a common MAC address since the CPE was last reset.	-	1.0
EthernetPacketsReceived	unsignedInt	-	Total number of Ethernet packets received over all connections within the same WANConnection-Device that share a common MAC address since the CPE was last reset.	-	1.0

2.4.1 Inform and Notification Requirements

For an Internet Gateway Device, all of the parameters listed in Table 3 that are present in the data model implementation are REQUIRED on every Inform.

Table 3 – Forced Inform parameters for an Internet Gateway Device

Parameter
InternetGatewayDevice.DeviceSummary
InternetGatewayDevice.DeviceInfo.SpecVersion
InternetGatewayDevice.DeviceI nfo.HardwareVersion
InternetGatewayDevice.DeviceI nfo.SoftwareVersion
InternetGatewayDevice.DeviceInfo.ProvisioningCode
InternetGatewayDevice. ManagementServer.ConnectionRequestURL
InternetGatewayDevice.ManagementServer.ParameterKey
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{j}.WAN{***}Connection.{k}.ExternalIPAddress[9]

Active Notification MUST be enabled for all of the parameters listed in Table 4 that are present in the data model implementation, regardless of the value of the Notification Attribute for these parameters. As a result, any change in the value of these parameters due to an entity other than the ACS MUST result in the CPE initiating a connection to the ACS to issue the Inform method call.

Table 4 – Forced Active Notification parameters for an Internet Gateway Device

Parameter
InternetGatewayDevice.DeviceI nfo.SoftwareVersion
InternetGatewayDevice.DeviceInfo.ProvisioningCode
InternetGatewayDevice. ManagementServer.ConnectionRequestURL
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{j}.WAN{***}Connection.{k}.ExternalIPAddress[9, 10]

CPE MUST support Active Notification (see [2]) for all parameters defined in the InternetGatewayDevice data model with the exception of those parameters listed in Table 5. For only those parameters listed Table 5, the CPE MAY reject a request by an ACS to enable Active Notification via the SetParameterAttributes RPC by responding with fault code 9009 as defined in [2] (Notification request rejected).
CPE MUST support Passive Notification (see [2]) for all parameters defined in the InternetGatewayDevice data model, with no exceptions.

Table 5 – Parameters for which Active Notification MAY be denied by the CPE

Parameter[11]
InternetGatewayDevice.{i}.DeviceInfo.
UpTime
DeviceLog

[9] Where {i}, {j}, and {k} refer to the default WAN connection, and {***} is either "IP" or "PPP" depending on the type of connection.
[10] The CPE must initiate an Inform whenever either the value of this parameter changes or the default WAN connection changes to a different connection.
[11] The name of a Parameter referenced in this table is the concatenation of the object name shown in the yellow header, and the individual Parameter name.

Parameter[11]
InternetGatewayDevice.ManagementServer.
ParameterKey
InternetGatewayDevice.ManagementServer. ManageableDevice.{i}.
ManufacturerOUI
SerialNumber
ProductClass
InternetGatewayDevice.Time.
CurrentLocalTime
InternetGatewayDevice.Layer2Bridging.
MaxBridgeEntries
MaxFilterEntries
MaxMarkingEntries
InternetGatewayDevice.Layer2Bridging.AvailableInterface.{i}.
AvailableInterfaceKey
InterfaceType
InterfaceReference
InternetGatewayDevice.QueueManagement.
MaxQueues
MaxClassificationEntries
MaxAppEntries
MaxFlowEntries
MaxPolicerEntries
MaxQueueEntries
InternetGatewayDevice.QueueManagement.Policer.{i}.
PossibleMeterTypes
CountedPackets
CountedBytes
InternetGatewayDevice.IPPingDiagnostics.
DiagnosticsState
SuccessCount
FailureCount
AverageResponseTime
MinimumResponseTime
MaximumResponseTime
InternetGatewayDevice.LANDevice.{i}.LANEthernetInterfaceConfig.{i}.Stats.
BytesSent
BytesReceived
PacketsSent
PacketsReceived
InternetGatewayDevice.LANDevice.{i}.LANUSBInterfaceConfig.{i}.Stats.
BytesSent
BytesReceived
CellsSent
CellsReceived
InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.
TotalPSKFailures

Parameter[11]
TotalIntegrityFailures
ChannelsInUse
TotalBytesSent
TotalBytesReceived
TotalPacketsSent
TotalPacketsReceived
TotalAssociations
InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.AssociatedDevice.{i}.
AssociatedDeviceMACAddress
AssociatedDeviceIPAddress
AssociatedDeviceAuthenticationState
LastRequestedUnicastCipher
LastRequestedMulticastCipher
LastPMKId
InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}.
LeaseTimeRemaining
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.
TotalBytesSent
TotalBytesReceived
TotalPacketsSent
TotalPacketsReceived
MaximumActiveConnections
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.
UpstreamCurrRate
DownstreamCurrRate
UpstreamMaxRate
DownstreamMaxRate
UpstreamNoiseMargin
DownstreamNoiseMargin
UpstreamAttenuation
DownstreamAttenuation
UpstreamPower
DownstreamPower
TotalStart
ShowtimeStart
LastShowtimeStart
CurrentDayStart
QuarterHourStart
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.Total.
ReceiveBlocks
TransmitBlocks
CellDelin
LinkRetrain
InitErrors
InitTimeouts
LossOfFraming

Parameter[11]
ErroredSecs
SeverelyErroredSecs
FECErrors
ATUCFECErrors
HECErrors
ATUCHECErrors
CRCErrors
ATUCCRCErrors
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.Showtime.
ReceiveBlocks
TransmitBlocks
CellDelin
LinkRetrain
InitErrors
InitTimeouts
LossOfFraming
ErroredSecs
SeverelyErroredSecs
FECErrors
ATUCFECErrors
HECErrors
ATUCHECErrors
CRCErrors
ATUCCRCErrors
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.LastShowtime.
ReceiveBlocks
TransmitBlocks
CellDelin
LinkRetrain
InitErrors
InitTimeouts
LossOfFraming
ErroredSecs
SeverelyErroredSecs
FECErrors
ATUCFECErrors
HECErrors
ATUCHECErrors
CRCErrors
ATUCCRCErrors
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.CurrentDay.
ReceiveBlocks
TransmitBlocks
CellDelin
LinkRetrain
InitErrors

Parameter[11]
InitTimeouts
LossOfFraming
ErroredSecs
SeverelyErroredSecs
FECErrors
ATUCFECErrors
HECErrors
ATUCHECErrors
CRCErrors
ATUCCRCErrors
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.QuarterHour.
ReceiveBlocks
TransmitBlocks
CellDelin
LinkRetrain
InitErrors
InitTimeouts
LossOfFraming
ErroredSecs
SeverelyErroredSecs
FECErrors
ATUCFECErrors
HECErrors
ATUCHECErrors
CRCErrors
ATUCCRCErrors
InternetGatewayDevice.WANDevice.{i}.WANEthernetInterfaceConfig.Stats.
BytesSent
BytesReceived
PacketsSent
PacketsReceived
InternetGatewayDevice.WANDevice.{i}.WANDSLDiagnostics.
LoopDiagnosticsState
ACTPSDds
ACTPSDus
ACTATPds
ACTATPus
HLINSCds
HLINpsds
QLNpsds
SNRpsds
BITSpsds
GAINSpsds
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANDSLLinkConfig.
ATMTransmittedBlocks
ATMReceivedBlocks

Parameter[11]
AAL5CRCErrors
ATMCRCErrors
ATMHECErrors
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANATMF5LoopbackDiagnostics.
DiagnosticsState
SuccessCount
FailureCount
AverageResponseTime
MinimumResponseTime
MaximumResponseTime
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.
Uptime
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.PortMapping.{i}.
PortMappingLeaseDuration
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.Stats.
EthernetBytesSent
EthernetBytesReceived
EthernetPacketsSent
EthernetPacketsReceived
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.
Uptime
CurrentMRUSize
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.PortMapping.{i}.
PortMappingLeaseDuration
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.Stats.
EthernetBytesSent
EthernetBytesReceived
EthernetPacketsSent
EthernetPacketsReceived

2.4.2 Version 1.0 Data Model Requirements

For version 1.0 of the Internet Gateway Device data model no profiles are defined because the profile mechanism was not supported by that version. However, the requirements for version 1.0 of the data model can easily be mapped to the profiles defined in section 3. Specifically:

- An implementation of version 1.0 of the InternetGatewayDevice data model MUST implement all of the objects and parameters in the Baseline: 1 profile with the exception of the DeviceSummary parameter, which was not part of the version 1.0 data model.
- Each of the following profiles indicate objects and parameters that are conditionally required in the version 1.0 data model:

o EthernetLAN:1 (REQUIRED if CPE has a LAN-side Ethernet interface)

o USBLAN: 1 (REQUIRED if CPE has a LAN-side USB interface)

o WiFiLAN:1 (REQUIRED if CPE has a LAN-side 802.11 interface)

o ADSLWAN: 1 (REQUIRED if CPE has a WAN-side ADSL interface)

o EthernetWAN: 1 (REQUIRED if CPE has a WAN-side Ethernet interface)

- POTSWAN:1 (REQUIRED if CPE has a WAN-side POTS interface)

- Each of the following profiles indicate objects and parameters for which there are no specific requirements in the version 1.0 data model:
  - Time:1
  - IPPing: 1
  - ATMLoopback: 1
  - DSLDiagnostics: 1
- All other objects and parameters associated with version 1.0 of the data model are considered optional.

3 Profile Definitions

This section specifies the profiles defined for the Internet Gateway Device data model. The use of profiles for this data model follows the definition and usage conventions described in [3].

3.1 Notation

The following abbreviations are used to specify profile requirements:

Abbreviation	Description
R	Read support is REQUIRED.
W	Both Read and Write support is REQUIRED. This MUST NOT be specified for a parameter that is defined as read-only.
P	The object is REQUIRED to be present.
C	Creation and deletion of instances of the object via AddObject and DeleteObject is REQUIRED.
A	Creation of instances of the object via AddObject is REQUIRED, but deletion is not required.
D	Deletion of instances of the object via DeleteObject is REQUIRED, but creation is not required.

3.2 Baseline Profile

Table 6 defines the Baseline:1 profile for the InternetGatewayDevice:1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 6 – Baseline:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.	P
DeviceSummary	R
LANDeviceNumberOfEntries	R
WANDeviceNumberOfEntries	R
InternetGatewayDevice.DeviceI nfo.	P
Manufacturer	R
ManufacturerOUI	R
ModelName	R
Description	R
SerialNumber	R
HardwareVersion	R
SoftwareVersion	R
SpecVersion	R
ProvisioningCode	W
UpTime	R
DeviceLog	R
InternetGatewayDevice.ManagementServer.	P
URL	W
Username	W
Password	W
PeriodicInformEnable	W
PeriodicInformInterval	W
PeriodicInformTime	W
ParameterKey	R
ConnectionRequestURL	R

Name	Requirement
ConnectionRequestUsername	W
ConnectionRequestPassword	W
UpgradesManaged	W
InternetGatewayDevice.Layer3Forwarding.	P
DefaultConnectionService	W
ForwardNumberOfEntries	R
InternetGatewayDevice.Layer3Forwarding.Forwarding.{i}.	PC
Enable	W
Status	R
Type	W
DestIPAddress	W
DestSubnetMask	W
SourceIPAddress	W
SourceSubnetMask	W
GatewayIPAddress	W
Interface	W
ForwardingMetric	W
InternetGatewayDevice.LANConfigSecurity.	P
ConfigPassword	W
InternetGatewayDevice.LANDevice.{i}.	P
LAN EthernetInterfaceNumberOfEntries	R
LANUSBInterfaceNumberOfEntries	R
LAN WLANConfigurationNumberOfEntries	R
InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.	P
DHCPServerConfigurable	W
DHCPServerEnable	W
DHCPRelay	R
MinAddress	W
MaxAddress	W
ReservedAddresses	W
SubnetMask	W
DNSServers	W
DomainName	W
IPRouters	W
IPInterfaceNumberOfEntries	R
InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement. IPInterface.{i}.	P
Enable	W
IPInterfaceIPAddress	W
IPInterfaceSubnetMask	W
IPInterfaceAddressingType	W
InternetGatewayDevice.LANDevice.{i}.Hosts.	P
HostNumberOfEntries	R
InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}.	P
IPAddress	R
AddressSource	R
LeaseTimeRemaining	R

Name	Requirement
MACAddress	R
HostName	R
InterfaceType	R
Active	R
InternetGatewayDevice.WANDevice.{i}.	P
WANConnectionNumberOfEntries	R
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.	P
EnabledForInternet	R
WANAccessType	R
Layer1 UpstreamMaxBitRate	R
Layer1 Downstream MaxBitRate	R
PhysicalLinkStatus	R
TotalBytesSent	R
TotalBytesReceived	R
TotalPacketsSent	R
TotalPacketsReceived	R
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.	P
WANIPConnectionNumberOfEntries	R
WANPPPConnectionNumberOfEntries	R
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.	PC
Enable	W
ConnectionStatus	R
PossibleConnectionTypes	R
ConnectionType	W[12]
Name	W
Uptime	R
LastConnectionError	R
RSIPAvailable	R
NATEnabled	W[13]
AddressingType	R
ExternalIPAddress	R
SubnetMask	R
DefaultGateway	R
DNSEnabled	R
DNSOverrideAllowed	R
DNSServers	R
MACAddress	R
ConnectionTrigger	W
RouteProtocolRx	W
PortMappingNumberOfEntries	R

[12] For writing, CPE are required only to support the values that are listed in the corresponding PossibleConnectionTypes parameter.

[13] Write support for this parameter is REQUIRED only if NAT is supported by the CPE.

Name	Requirement
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.Port-Mapping.{i}.	PC
PortMappingEnabled	W
PortMappingLeaseDuration	R
RemoteHost	W
ExternalPort	W
InternalPort	W
PortMappingProtocol	W
InternalClient	W
PortMappingDescription	W
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.Stats.	P[14]
EthernetBytesSent	R[14]
EthernetBytesReceived	R[14]
EthernetPacketsSent	R[14]
EthernetPacketsReceived	R[14]
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.	PC
Enable	W
ConnectionStatus	R
PossibleConnectionTypes	R
ConnectionType	W[12]
Name	W
Uptime	R
LastConnectionError	R
RSIPAvailable	R
NATEnabled	W[13]
Username	W
Password	W
ExternalIPAddress	R
DNSEnabled	R
DNSOverrideAllowed	R
DNSServers	R
MACAddress	R
TransportType	R
PPPoEACName	W
PPPoEServiceName	W
ConnectionTrigger	W
RouteProtocolRx	W
PortMappingNumberOfEntries	R
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.Port-Mapping.{i}.	PC
PortMappingEnabled	W
PortMappingLeaseDuration	R
RemoteHost	W
ExternalPort	W

[14] Required only for WANConnectionDevice instances that are configured to support an Ethernet layer.

Name	Requirement
InternalPort	W
PortMappingProtocol	W
InternalClient	W
PortMappingDescription	W
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.Stats.	P[14]
EthernetBytesSent	R[14]
EthernetBytesReceived	R[14]
EthernetPacketsSent	R[14]
EthernetPacketsReceived	R[14]

3.3 EthernetLAN Profile

Table 7 defines the EthernetLAN: 1 profile for the InternetGatewayDevice: 1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 7 – EthernetLAN:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.LANDevice.{i}.LANEthernetInterfaceConfig.{i}.	P
Enable	W
Status	R
MACAddress	R
MACAddressControlEnabled	W[15]
MaxBitRate	W
DuplexMode	W
InternetGatewayDevice.LANDevice.{i}.LANEthernetInterfaceConfig.{i}.Stats.	P
BytesSent	R
BytesReceived	R
PacketsSent	R
PacketsReceived	R

3.4 USBLAN Profile

Table 8 defines the USBLAN: 1 profile for the InternetGatewayDevice: 1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 8 – USBLAN:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.LANDevice.{i}.LANUSBInterfaceConfig.{i}.	P
Enable	W
Status	R
MACAddress	R
MACAddressControlEnabled	W[15]
Standard	R

[15] Support for this parameter is required only if the parameter InternetGatewayDevice.LANDevice. {i}.-LANHostConfigManagement.AllowedMACAddresses is present.

Name	Requirement
Type	R
Rate	R
Power	R
InternetGatewayDevice.LANDevice.{i}.LANUSBInterfaceConfig.{i}.Stats.	P
BytesSent	R
BytesReceived	R
CellsSent	R
CellsReceived	R

3.5 WiFiLAN Profile

Table 9 defines the WiFiLAN: 1 profile for the InternetGatewayDevice: 1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 9 – WiFiLAN:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.	P
Enable	W
Status	R
BSSID	R
MaxBitRate	W
Channel	W
SSID	W
BeaconType	W
MACAddressControlEnabled	W 15
Standard	R
WEPKeyIndex	W
KeyPassphrase	W
WEPEncryptionLevel	R
BasicEncryptionModes	W
BasicAuthenticationMode	W
WPAEncryptionModes	W
WPAAuthenticationMode	W
PossibleChannels	R
BasicDataTransmitRates	W
OperationalDataTransmitRates	W
PossibleDataTransmitRates	R
RadioEnabled	W
AutoRateFallBackEnabled	W
TotalBytesSent	R
TotalBytesReceived	R
TotalPacketsSent	R
TotalPacketsReceived	R
TotalAssociations	R
InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.AssociatedDevice.{i}.	P
AssociatedDeviceMACAddress	R

Name	Requirement
AssociatedDeviceIPAddress	R
AssociatedDeviceAuthenticationState	R
InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.WEPKey.{i}.	P
WEPKey	W
InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.PreSharedKey.{i}.	P
PreSharedKey	W
KeyPassphrase	W

3.6 ADSLWAN Profile

Table 10 defines the ADSLWAN:1 profile for the InternetGatewayDevice:1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 10 – ADSLWAN:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.	P
Enable	W
Status	R
UpstreamCurrRate	R
DownstreamCurrRate	R
UpstreamMaxRate	R
DownstreamMaxRate	R
UpstreamNoiseMargin	R
DownstreamNoiseMargin	R
UpstreamAttenuation	R
DownstreamAttenuation	R
UpstreamPower	R
DownstreamPower	R
ATURVendor	R
ATURCountry	R
ATUCVendor	R
ATUCCountry	R
TotalStart	R
ShowtimeStart	R
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.	P
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.Total.	P
ReceiveBlocks	R
TransmitBlocks	R
CellDelin	R
LinkRetrain	R
InitErrors	R
InitTimeouts	R
LossOfFraming	R
ErroredSecs	R
SeverelyErroredSecs	R
FECErrors	R

Name	Requirement
ATUCFECErrors	R
HECErrors	R
ATUCHECErrors	R
CRCErrors	R
ATUCCRCErrors	R
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.Showtime.	P
ReceiveBlocks	R
TransmitBlocks	R
CellDelin	R
LinkRetrain	R
InitErrors	R
InitTimeouts	R
LossOfFraming	R
ErroredSecs	R
SeverelyErroredSecs	R
FECErrors	R
ATUCFECErrors	R
HECErrors	R
ATUCHECErrors	R
CRCErrors	R
ATUCCRCErrors	R
InternetGatewayDevice.WANDevice.{i}.WANDSLConnectionManagement.	P
ConnectionServiceNumberOfEntries	R
InternetGatewayDevice.WANDevice.{i}.WANDSLConnectionManagement.ConnectionService.{i}.	P
WANConnectionDevice	R
WANConnectionService	R
DestinationAddress	R
LinkType	R
ConnectionType	R
Name	R
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.	PC
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANDSLLinkConfig.	P
Enable	W
LinkStatus	R
LinkType	W [16]
AutoConfig	R
DestinationAddress	W
ATMTransmittedBlocks	R
ATMReceivedBlocks	R
AAL5CRCErrors	R
ATMCRCErrors	R

[16] For writing, CPE need not to support values for this parameter that correspond to modes of operation that are not supported by the CPE.

3.7 EthernetWAN Profile

Table 11 defines the EthernetWAN:1 profile for the InternetGatewayDevice:1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 11 – EthernetWAN:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.WANDevice.{i}.WANEthernetInterfaceConfig.	P
Enable	W
Status	R
MACAddress	R
MaxBitRate	W
DuplexMode	W
InternetGatewayDevice.WANDevice.{i}.WANEthernetInterfaceConfig.Stats.	P
BytesSent	R
BytesReceived	R
PacketsSent	R
PacketsReceived	R
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANEthernetLinkConfig.	P
EthernetLinkStatus	R

3.8 POTSWAN Profile

Table 12 defines the POTSWAN:1 profile for the InternetGatewayDevice:1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 12 – POTSWAN:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPOTSLinkConfig.	P
Enable	W
LinkStatus	R
ISPPhoneNumber	R
ISPInfo	R
LinkType	R
NumberOfRetries	R
DelayBetweenRetries	R

3.9 QoS Profile

Table 13 defines the QoS: 1 profile for the InternetGatewayDevice: 1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 13 – QoS:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.QueueManagement.	P
Enable	W
MaxQueues	R
MaxClassificationEntries	R
ClassificationNumberOfEntries	R

Name	Requirement
MaxAppEntries	R
AppNumberOfEntries	R
MaxFlowEntries	R
FlowNumberOfEntries	R
MaxPolicerEntries	R
PolicerNumberOfEntries	R
MaxQueueEntries	R
QueueNumberOfEntries	R
DefaultForwardingPolicy	W
DefaultPolicer	W
DefaultQueue	W
DefaultDSCPMark	W
DefaultEthernetPriorityMark	W
AvailableAppList	R
InternetGatewayDevice.QueueManagement.Classification.{i}.	PC
ClassificationKey	R
ClassificationEnable	W
ClassificationStatus	R
ClassificationOrder	W
ClassInterface	W
DestIP	W
DestMask	W
DestIPExclude	W
SourceIP	W
SourceMask	W
SourceIPExclude	W
Protocol	W
ProtocolExclude	W
DestPort	W
DestPortRangeMax	W
DestPortExclude	W
SourcePort	W
SourcePortRangeMax	W
SourcePortExclude	W
SourceMACAddress	W
SourceMACExclude	W
DestMACAddress	W
DestMACExclude	W
DSCPCheck	W
DSCPExclude	W
DSCPMark	W
EthernetPriorityCheck	W
EthernetPriorityExclude	W
EthernetPriorityMark	W
VLANIDCheck	W
VLANIDExclude	W

Name	Requirement
ForwardingPolicy	W
ClassPolicer	W
ClassQueue	W
InternetGatewayDevice.QueueManagement.Policer.{i}.	PC
PolicerKey	R
PolicerEnable	W
PolicerStatus	R
CommittedRate	W
CommittedBurstSize	W
MeterType	W
PossibleMeterTypes	R
ConformingAction	W
NonConformingAction	W
CountedPackets	R
CountedBytes	R
InternetGatewayDevice.QueueManagement.Queue.{i}.	PC
QueueKey	R
QueueEnable	W
QueueStatus	R
QueueInterface	W
QueueBufferLength	R
QueueWeight	W
QueuePrecedence	W
REDThreshold	W
REDPercentage	W
DropAlgorithm	W
SchedulerAlgorithm	W
ShapingRate	W
ShapingBurstSize	W
InternetGatewayDevice.Layer3Forwarding.Forwarding.{i}.	-
ForwardingPolicy	W
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.	-
ShapingRate	W
ShapingBurstSize	W
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.	-
ShapingRate	W
ShapingBurstSize	W

3.10 QoSDynamicFlow Profile

Table 14 defines the QoSDynamicFlow: 1 profile for the InternetGatewayDevice: 1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 14 – QoSDynamicFlow:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.QueueManagement.App.{i}.	PC
AppKey	R
AppEnable	W
AppStatus	R
ProtocolIdentifier	W
AppName	W
AppDefaultForwardingPolicy	W
AppDefaultPolicer	W
AppDefaultQueue	W
AppDefaultDSCPMark	W
AppDefaultEthernetPriorityMark	W
InternetGatewayDevice.QueueManagement.Flow.{i}.	PC
FlowKey	R
FlowEnable	W
FlowStatus	R
FlowType	W
FlowTypeParameters	W
FlowName	W
AppIdentifier	W
FlowForwardingPolicy	W
FlowPolicer	W
FlowQueue	W
FlowDSCPMark	W
FlowEthernetPriorityMark	W
InternetGatewayDevice.QueueManagement.Classification .{i}.	-
ClassApp	W

3.11 Bridging Profile

Table 15 defines the Bridging: 1 profile for the InternetGatewayDevice: 1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 15 – Bridging:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.Layer2Bridging.	P
MaxBridgeEntries	R
MaxFilterEntries	R
MaxMarkingEntries	R
BridgeNumberOfEntries	R
FilterNumberOfEntries	R
MarkingNumberOfEntries	R

Name	Requirement
AvailableInterfaceNumberOfEntries	R
InternetGatewayDevice.Layer2Bridging.Bridge.{i}.	PC
BridgeKey	R
BridgeEnable	W
BridgeStatus	R
BridgeName	W
VLANID	W
InternetGatewayDevice.Layer2Bridging.Filter.{i}.	PC
FilterKey	R
FilterEnable	W
FilterStatus	R
FilterBridgeReference	W
ExclusivityOrder	W
FilterInterface	W
VLANIDFilter	W
AdmitOnlyVLANTagged	W
EthertypeFilterList	W
EthertypeFilterExclude	W
SourceMACAddressFilterList	W
SourceMACAddressFilterExclude	W
DestMACAddressFilterList	W
DestMACAddressFilterExclude	W
InternetGatewayDevice.Layer2Bridging.Marking.{i}.	PC
MarkingKey	R
MarkingEnable	W
MarkingStatus	R
MarkingBridgeReference	W
MarkingInterface	W
VLANIDUntag	W
VLANIDMark	W
EthernetPriorityMark	W
EthernetPriorityOverride	W
InternetGatewayDevice.Layer2Bridging.AvailableInterface.{i}.	P
AvailableInterfaceKey	R
InterfaceType	R
InterfaceReference	R

3.12 Time Profile

Table 16 defines the Time:1 profile for the InternetGatewayDevice:1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 16 – Time:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.Time.	P
NTPServer1	W

Name	Requirement
NTPServer2	W
CurrentLocalTime	R
LocalTimeZone	W
LocalTimeZoneName	W
DaylightSavingsUsed	W
DaylightSavingsStart	W
DaylightSavingsEnd	W

3.13 IPPing Profile

Table 17 defines the IPPing: 1 profile for the InternetGatewayDevice: 1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 17 – IPPing:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.IPPingDiagnostics.	P
DiagnosticsState	W
Interface	W
Host	W
NumberOfRepetitions	W
Timeout	W
DataBlockSize	W
DSCP	W
SuccessCount	R
FailureCount	R
AverageResponseTime	R
MinimumResponseTime	R
MaximumResponseTime	R

3.14 ATMLoopback Profile

Table 18 defines the ATMLoopback: 1 profile for the InternetGatewayDevice: 1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 18 – ATM Loopback:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANATMF5Loopback-Diagnostics.	P
DiagnosticsState	W
NumberOfRepetitions	W
Timeout	W
SuccessCount	R
FailureCount	R
AverageResponseTime	R
MinimumResponseTime	R
MaximumResponseTime	R

3.15 DSLDiagnostics Profile

Table 19 defines the DSLDiagnostics: 1 profile for the InternetGatewayDevice: 1 object. The minimum required version for this profile is InternetGatewayDevice: 1.1.

Table 19 – DSLDiagnostics:1 profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.WANDevice.{i}.WANDSLDiagnostics.	P
LoopDiagnosticsState	W
ACTPSDds	R
ACTPSDus	R
ACTATPds	R
ACTATPus	R
HLINSCds	R
HLINpsds	R
QLNpsds	R
SNRpsds	R
BITSpsds	R
GAINSpsds	R

3.16 DeviceAssociation Profile

The DeviceAssociation:1 profile implies support for all of the Gateway requirements defined in Annex F of [2], including the support for the data model parameters as shown in Table 20. The minimum required version for this profile is InternetGatewayDevice: 1.2.

Table 20 – DeviceAssociation:1 Profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.ManagementServer.	-
ManageableDeviceNumberOfEntries	R
InternetGatewayDevice.ManagementServer. ManageableDevice.{i}.	P
ManufacturerOUI	R
SerialNumber	R
ProductClass	R

3.17 UDPConnReq Profile

The UDPConnReq: 1 profile for an Internet Gateway Device implies support for all of the CPE requirements defined in Annex G of [2], including support for the data model parameters as shown in Table 21. The minimum required version for this profile is InternetGatewayDevice: 1.2.

Table 21 – UDPConnReq :1 Profile definition for InternetGatewayDevice:1

Name	Requirement
InternetGatewayDevice.ManagementServer.	-
UDPConnectionRequestAddress	R
UDPConnection Req uestAddressNotification Limit	W
STUNEnable	W
STUNServerAddress	W
STUNServerPort	W

Name	Requirement
STUNUsername	W
STUNPassword	W
STUNMaximumKeepAlivePeriod	W
STUNMinimumKeepAlivePeriod	W
NATDetected	R

Normative References

The following documents are referenced by this specification.

[1] RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels,* http://www.ietf.org/rfc/rfc2119.txt

[2] TR-069 Amendment 1, *CPE WAN Management Protocol,* DSL Forum Technical Report

[3] TR-106, Data Model Template for TR-069-Enabled Devices, DSL Forum Technical Report

[4] Simple Object Access Protocol (SOAP) 1.1, http://www.w3.org/TR/2000/NOTE-SOAP-20000508

[5] Organizationally Unique Identifiers (OUIs), http://standards.ieee.org/faqs/OUI.html

[6] RFC 2616, *Hypertext Transfer Protocol -- HTTP/1.1*, http://www.ietf.org/rfc/rfc2616.txt

[7] HTML 4.01 Specification, http://www.w3.org/TR/html4

[8] RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax,* http://www.ietf.org/rfc/rfc3986.txt

[9] RFC 3489, *STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs),* http://www.ietf.org/rfc/rfc3489.txt

[10] References on RED (Random Early Detection) Queue Management, http://www.icir.org/floyd/red.html

[11] *Blue: A New Class of Active Queue Management Algorithms,* http://www.thefengs.com/wuchang/work/blue

Annex A. Queuing and Bridging

A.1 Queuing and Bridging Model

Figure 2 shows the queuing and bridging model for an Internet Gateway Device. This model relates to the QueueManagement object as well as the Layer2Bridging and Layer3Forwarding objects. The elements of this model are described in the following sections.

Note – the queuing model described in this Annex is meant strictly as a model to clarify the intended behavior of the related data objects. There is no implication intended that an implementation must be structured to conform to this model.

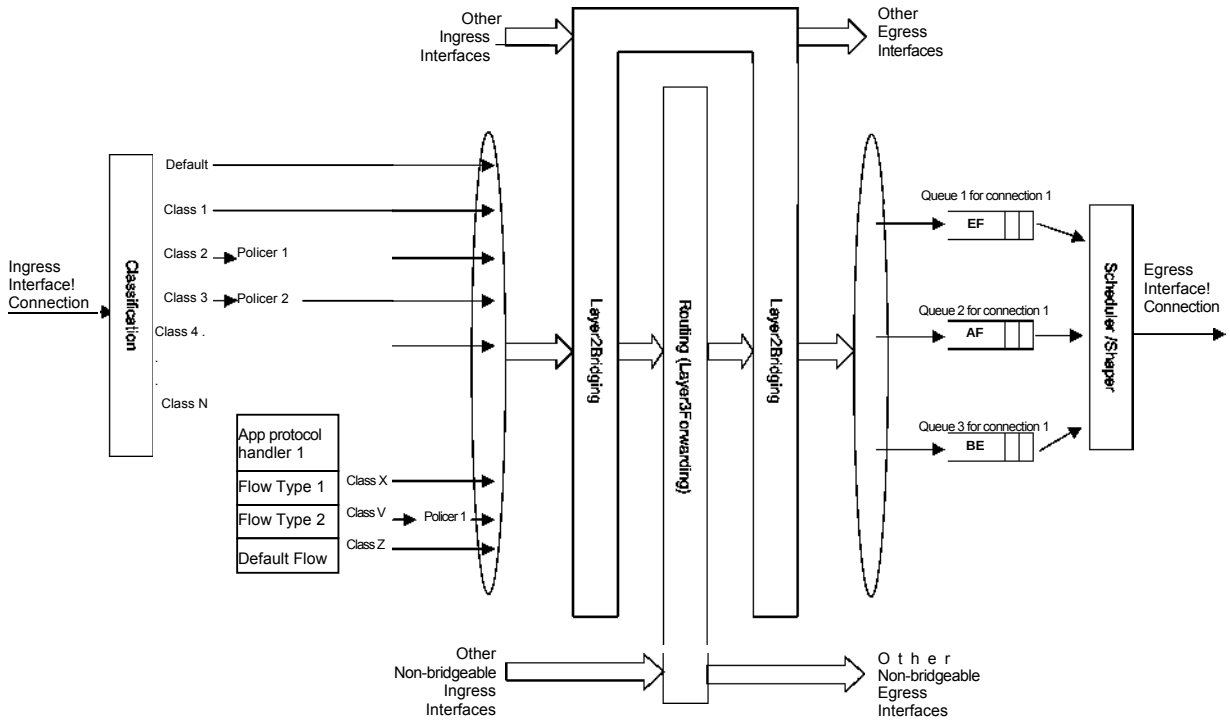


Figure 2 – Queuing model of an Internet Gateway Device

A.1 .1 Packet Classification

The Classification table within the QueueManagement object specifies the assignment of each packet arriving at an ingress interface to a specific internal class. This classification may be based on a number of matching criteria, such as destination and source IP address, destination and source port, and protocol.

Each entry in the Classification table includes a series of elements, each indicated to be a Classification Criterion. Each classification criterion can be set to a specified value, or can be set to a value that indicates that criterion is not to be used. A packet is defined to match the classification criteria for that table entry

only the packet matches all of the specified criteria. That is, a logical AND operation is applied across all classification criteria within a given Classification table entry.

Note – to apply a logical OR to sets of classification criteria, multiple entries in the Classification table can be created that specify the same resulting queuing behavior.

For each classification criterion, the Classification table also includes a corresponding "exclude" flag. This flag may be used to invert the sense of the associated classification criterion. That is, if this flag is false for a given criterion, the classifier is to include only packets that meet the specified criterion (as well as all others). If this flag is true for a given criterion, the classifier is to include all packets except those that meet the associated criterion (in addition to meeting all other criteria).

For a given entry in the Classification table, the classification is to apply only to those interfaces specified by the ClassInterface element. This element may specify a particular ingress interface, all LAN-side interfaces, all WAN-side interfaces, a local IP-layer source within the Internet Gateway Device, or all sources. Depending on the particular interface, not all classification criteria may be applicable. For example, Ethernet layer classification criteria would not apply to packets arriving on a non-bridged ATM VC.

Packet classification is modeled to include all ingress packets regardless of whether they ultimately will be bridged or routed through the Internet Gateway Device. The packet classifier is not modeled to apply to packets that are embedded in a tunnelled connection (such as, PPPoE, L2TP, or tunnelled IPsec). In such cases, classification would apply only to the outer tunnel packets, but not the embedded packets contained within. An exception is for tunnels that terminate in the Internet Gateway Device itself. That is, for connections that terminate in the Internet Gateway Device, such as a PPP connection, the classification is applied to the IP packets contained within.

A.1.1.1 Classification Order

The class assigned to a given packet corresponds to the first entry in the Classification table (given the specified order of the entries in the table) whose matching criteria match the packet. If there is no entry that matches the packet, the packet is assigned to a default class.

Classification rules are sensitive to the order in which they are applied because certain traffic may meet the criteria of more than one Classification table entry. The ClassificationOrder parameter is responsible for identifying the order in which the Classification entries are to be applied.

The following rules apply to the use and setting of the ClassificationOrder parameter:

- ClassificationOrder goes in order from 1 to n, where n is equal to the number of entries in the Classification table. 1 is the highest precedence, and n the lowest. For example, if entries with ClassificationOrder of 4 and 7 both have rules that match some particular traffic, the traffic will be classified according to the entry with the 4.
- The CPE is responsible for ensuring that all ClassificationOrder values are unique and sequential.
    - If an entry is added (number of entries becomes n+ 1), and the value specified for ClassificationOrder is greater than n+1, then the CPE will set ClassificationOrder to n+1.
    - If an entry is added (number of entries becomes n+ 1), and the value specified for ClassificationOrder is less than n+1, then the CPE will create the entry with that specified value, and increment the ClassificationOrder value of all existing entries with ClassificationOrder equal to or greater than the specified value.
    - If an entry is deleted, the CPE will decrement the ClassificationOrder value of all remaining entries with ClassificationOrder greater than the value of the deleted entry.
    - If the ClassificationOrder value of an entry is changed, then the value will also be changed for other entries greater than or equal to the lower of the old and new values, and less than the larger of the old and new values. If the new value is less than the old, then these other entries will all have ClassificationOrder incremented. If the new value is greater than the old, then the other entries will have ClassificationOrder decremented and the changed entry will be given a

value of <new value>-1. For example, an entry is changed from 8 to 5. The existing 5 goes to 6, 6 to 7, and 7 to 8. If the entry goes from 5 to 8, then 6 goes to 5, 7 to 6, and the changed entry is 7. This is consistent with the behavior that would occur if the change were considered to be an Add of a new entry with the new value, followed by a Delete of the entry with the old value.

A.1 .1.2 Dynamic Application Specific Classification

In some situations, traffic to be classified cannot be identified by a static set of classification criteria. Instead, identification of traffic flows may require explicit application awareness. The model accommodates such situations via the App and Flow tables in the QueueManagement object.

Each entry in the App table is associated with an application-specific protocol handler, identified by the ProtocolIdentifier, which contains a URN. For a particular CPE, the AvailableAppList parameter indicates which protocol handlers that CPE is capable of supporting, if any. A list of standard protocol handlers and their associated URNs is specified in section A.3, though a CPE may also support vendor-specific protocol handlers as well. Multiple App table entries may refer to the same ProtocolIdentifier.

The role of the protocol handler is to identify and classify flows based on application awareness. For example, a SIP protocol handler might identify a call-control flow, an audio flow, and a video flow. The App and Flow tables are used to specify the classification outcome associated with each such flow.

For each App table entry there may be one or more associated Flow table entries. Each flow table identifies a type of flow associated with the protocol handler. The FlowType element is used to identify the specific type of flow associated with each entry. For example, a Flow table entry for a SIP protocol handler might refer only to the audio flows associated with that protocol handler. A list of standard FlowType values is given in section A.3, though a CPE may also support vendor-specific flow types.

A protocol handler may be defined as being fed from the output of a Classification table entry. That is, a Classification entry may be used to single out control traffic to be passed to the protocol handler, which then subsequently identifies associated flows. Doing so allows more than one instance of a protocol handler associated with distinct traffic. For example, one could define two App table entries associated with SIP protocol handlers. If the classifier distinguished control traffic to feed into each handler based on the destination IP address of the SIP server, this could be used to separately classify traffic for different SIP service providers. In this case, each instance of the protocol handler would identify only those flows associated with a given service. Note that the Classification table entry that feeds each protocol handler wouldn't encompass all of the flows; only the traffic needed by the protocol handler to determine the flows—typically only the control traffic.

A.1 .1.3 Classification Outcome

Each Classification entry specifies a tuple composed of either:

- A Queue and optional Policer, or
- An App table entry

Each entry also specifies:

- Outgoing DiffServ and Ethernet priority marking behavior
- A ForwardingPolicy tag that may be referenced in the Layer3Forwarding table to affect packet routing (note that the ForwardingPolicy tag affects only routed traffic)

Note that the information associated with the classification outcome is modeled as being carried along with each packet as it flows through the system.

If a packet does not match any Classification table entry, the DefaultQueue, DefaultPolicer, default markings, and default ForwardingPolicy are used.

If a Queue/Policer tuple is specified, classification is complete. If, however, an App is specified, the packet is passed to the protocol handler specified by the ProtocolIdentifier in the specified App table entry

for additional classification (see section A. 1.1.2). If any of the identified flows match the FlowType specified in any Flow table entry corresponding to the given App table entry (this correspondence is indicated by the App identifier), the specified tuple and markings for that Flow table entry is used for packets in that flow. Other flows associated with the application, but not explicitly identified, use the default tuple and markings specified for that App table entry.

A.1.2 Policing

The Policer table defines the policing parameters for ingress packets identified by either a Classification table entry (or the default classification) or a dynamic flow identified by a protocol handler identified in the App table.

Each Policer table entry specifies the packet handling characteristics, including the rate requirements and behavior when these requirements are exceeded.

A.1.3 Queuing and Scheduling

The Queue table specifies the number and types of queues, queue parameters, shaping behavior, and scheduling algorithm to use. Each Queue table entry specifies a set of egress interfaces for which a queue with the corresponding characteristics must exist.

> *Note – If the CPE can determine that among the interfaces specified for a queue to exist, packets classified into that queue cannot egress to a subset of those interfaces (from knowledge of the current routing and bridging configuration), the CPE may choose not to instantiate the queue on those interfaces.*
>
> *Note – Packets classified into a queue that exit through an interface for which the queue is not specified to exist, must instead use the default queuing behavior. The default queue itself must exist on all egress interfaces.*

The model defined here is not intended to restrict where the queuing is implemented in an actual implementation. In particular, it is up to the particular implementation to determine at what protocol layer it is most appropriate to implement the queuing behavior (IP layer, Ethernet MAC layer, ATM layer, etc.). In some cases, however, the QueueManagement configuration would restrict the choice of layer where queueing can be implemented. For example, if a queue is specified to carry traffic that is bridged, then it could not be implemented as an IP-layer queue.

> *Note – care should be taken to avoid having multiple priority queues multiplexed onto a single connection that is rate shaped. In such cases, it the possibility exists that high priority traffic can be held back due to rate limits of the overall connection exceeded by lower priority traffic. Where possible, each priority queue should be shaped independently using the shaping parameters in the Queue table.*

The scheduling parameters defined in the Queue table apply to the first level of what may be a more general scheduling hierarchy. This specification does not specify the rules that an implementation must apply to determine the most appropriate scheduling hierarchy given the scheduling parameters defined in the Queue table.

As an example, take a situation where the output of four distinct queues is to be multiplexed into a single connection, and two entries share one set of scheduling parameters while the other two entries share a different set of scheduling parameters. In this case, it may be appropriate to implement this as a scheduling hierarchy with the first two queues multiplexed with a scheduler defined by the first pair, and the second two queues being multiplexed with a scheduler defined by the second pair. The lower layers of this scheduling hiearchy cannot be directly determined from the content of the Queue table.

A.1.4 Bridging

For each interface, the output of the classifier is modeled to feed a set of layer-2 bridges as specified by the Layer2Bridging object. Each bridge specifies layer-2 connectivity between one or more layer-2 LAN and/or WAN interfaces, and optionally one or more layer-3 connections to the local router.

Each bridge corresponds to a single entry in the Bridge table of the Layer2Bridging. Each entry contains (by reference) one or more Filter table entries. Each Filter table entry specifies an interface or set of interfaces to include in the bridge, and may also specify layer-2 filter criteria to selectively bridge traffic among the specified interfaces.

Each Filter table entry selects one or more interfaces among those listed in the AvailableInterface table. This table would normally include all layer-2 interfaces that include an Ethernet MAC layer. This would exclude, for example, a non-bridged ATM VC carrying IPoA or PPPoA. A given entry may refer to a specific layer-2 interface, all available LAN interfaces, all available WAN interfaces, or all available LAN and WAN interfaces. A Filter table entry may also include LAN-side or WAN-side layer-3 connections to the local router, such as PPP or IP connections. When including a layer-3 connection in a bridge, this overrides the default association of that connection with a layer-2 object as indicated by the connection object hierarchy.

> *Note – from the point of view of a bridge, packets arriving into the bridge from the local router (either LAN-side or WAN-side) are treated as ingress packets, even though the same packets, which just left the router, are treated as egress from the point of the router. For example, a Filter table entry might admit packets on ingress to the bridge from a particular WANIPConnection, which means that it admits packets on their way out of the router over this layer-3 connection.*

A.1.4.1 Filtering

Traffic from a given interface (or set of interfaces) may be selectively admitted to a given Bridge, rather than bridging all traffic from that interface. Each entry in the Filter table includes a series filter criteria. Each filter criterion can be set to a specified value, or can be set to a value that indicates that criterion is not to be used. A packet is admitted to the Bridge only if the packet matches all of the specified criteria. That is, a logical AND operation is applied across all filter criteria within a given Filter table entry.

> *Note – to apply a logical OR to sets of filter criteria, multiple entries in the Filter table can be created that refer to the same interfaces and the same Bridge table entry.*

For each filter criterion, the Filter table also includes a corresponding "exclude" flag. This flag may be used to invert the sense of the associated filter criterion. That is, if this flag is false for a given criterion, the Bridge will admit only packets that meet the specified criterion (as well as all others). If this flag is true for a given criterion, the Bridge will admit all packets except those that meet the associated criterion (in addition to meeting all other criteria).

Note that because the filter criteria are based on layer-2 packet information, if the selected interface for a given Filter table entry is a layer-3 connection from the local router, the layer-2 filter criteria do not apply.

A.1 .4.2 Exclusivity Order

Each Filter table entry is defined as either exclusive or non-exclusive. Any packet that matches the filter criteria of one or more exclusive filters is admitted to the Bridge associated with the first exclusive entry in the Filter table (relative to the specified ExclusivityOrder).

If there is no exclusive filter that matches a packet, then the packet is admitted to all Bridges associated with non-exclusive filters that match the packet.

The following rules apply to the use and setting of the ExclusivityOrder parameter:

- If the ExclusivityOrder is zero, the filter is defined to be non-exclusive.
- If the ExclusivityOrder is one or greater, the filter is defined to be exclusive.

- Among exclusive filters, the ExclusivityOrder goes in order from 1 to n, where n is equal to the number of exclusive filters. 1 is the highest precedence, and n the lowest.
- The CPE is responsible for ensuring that all ExclusivityOrder values among exclusive filters are unique and sequential.
    - If an exclusive filter is added (number of exclusive filters becomes n+1) or a non-exclusive filter is changed to be exclusive, and the value specified for ExclusivityOrder is greater than n+1, then the CPE will set ExclusivityOrder to n+1.
    - If an exclusive filter is added (number of entries becomes n+1) or a non-exclusive filter is changed to be exclusive, and the value specified for ExclusivityOrder is less than n+1, then the CPE will create the entry with that specified value, and increment the ExclusivityOrder value of all existing exclusive filters with ExclusivityOrder equal to or greater than the specified value.
    - If an exclusive filter is deleted or an exclusive filter is changed to non-exclusive, the CPE will decrement the ExclusivityOrder value of all remaining exclusive filter with ExclusivityOrder greater than the value of the deleted entry.
    - If the ExclusivityOrder value of an exclusive filter is changed, then the value will also be changed for other exclusive filters greater than or equal to the lower of the old and new values, and less than the larger of the old and new values. If the new value is less than the old, then these other entries will all have ExclusivityOrder incremented. If the new value is greater than the old, then the other entries will have ExclusivityOrder decremented and the changed entry will be given a value of <new value>-1. For example, an entry is changed from 8 to 5. The existing 5 goes to 6, 6 to 7, and 7 to 8. If the entry goes from 5 to 8, then 6 goes to 5, 7 to 6, and the changed entry is 7. This is consistent with the behavior that would occur if the change were considered to be an Add of a new exclusive filter with the new value, followed by a Delete of the exclusive filter with the old value.

A.1 .4.3 Egress from a Bridge

Packets admitted to a bridge from any interface are bridged across all of the interfaces considered part of that bridge. An interface is considered part of a bridge if it is specified by any of the Filter table or Marking table entries that are associated with the bridge. That is, the union of all interfaces specified either for potential admission into the bridge or for special marking treatment on egress are considered part of the bridge. This may include both layer-2 interfaces as well as layer-3 connections to the local router.

For a given bridge, packets on egress may optionally be marked distinctly for specific interfaces. The Marking table allows the CPE to be configured to selective either remove all VLANID/priority marking from a packet on egress, or modify the VLANID and/or Ethernet priority marking on egress. This may be done selectively per interface, across a class of interfaces, or for all interfaces.

A.2 Default Layer 2/3 QoS Mapping

Table 22 presents a "default" mapping between layer 2 and layer 3 QoS. In practice, it is a guideline for automatic marking of DSCP (layer 3) based upon Ethernet Priority (layer 2) and the other way around. Please refer to the QueueManagement object DSCPMark and EthernetPriorityMark parameters (and related parameters) for configuration of a default automatic DSCP / Ethernet Priority mapping.

Automatic marking of DSCP or Ethernet Priority is likely only in the following cases:

- WAN - LAN: to map DSCP (layer 3) to Ethernet Priority (layer 2)
- LAN - WAN: to map Ethernet Priority (layer 2) to DSCP (layer 3)

Automatic marking in the LAN - LAN case is unlikely, since LAN QoS is likely to be supported only at layer 2, and LAN DSCP values, if used, will probably be a direct representation of Ethernet Priority, e.g. Ethernet Priority shifted left by three bits.

In the table, grayed and bolded items are added to allow two-way mapping between layer 2 and layer 3 QoS (where the mapping is ambiguous, the grayed values should be ignored and the bolded values should be used). If, when mapping from layer 3 to layer 2 QoS, the DSCP value is not present in the table, the mapping should be based only on the first three bits of the DSCP value, i.e. on DSCP & 111000.

Table 22 – Default Layer 2/3 QoS Mapping

Layer 2		Layer 3	
Ethernet Priority	Designation	DSCP	Per Hop Behavior
001 (1)	BK	000000 (0x00)	Default
010 (2)	spare	000000 (0x00)	
000 (0)	BE	000000 (0x00) **000000 (0x00)**	Default CS0
011 (3)	EE	001110 (0x0e) 001100 (0x0c) 001010 (0x0a) **001000 (0x08)**	AF13 AF12 AF11 CS1
100 (4)	CL	010110 (0x16) 010100 (0x14) 010010 (0x12) **010000 (0x1 0)**	AF23 AF22 AF21 CS2
101 (5)	VI	011110 (0x1e) 011100 (0x1c) 011010 (0x1a) **011000 (0x18)**	AF33 AF32 AF31 CS3
110 (6)	VO	100110 (0x26) 100100 (0x24) 100010 (0x22) **100000 (0x20)**	AF43 AF42 AF41 CS4
110 (6)	VO	101110 (0x2e) **101000 (0x28)**	EF CS5
111 (7)	NC	110000 (0x30) **111000 (0x38)**	CS6 CS7

A.3 URN Definitions for App and Flow Tables

A.3.1 ProtocolIdentifier

Table 23 lists the URNs defined for the ProtocolIdentifier parameter in the App table of the QueueManagement service. Additional standard or vendor-specific URNs may be defined following the standard synax for forming URNs.

Table 23 – ProtocolIdentifer URNs

URN	Description
urn:dslforum-org:sip	Session Initiaion Protocol (SIP) as defined by RFC 3261.
urn:dslforum-org:h.323	ITU-T Recommendation H.323
urn:dslforum-org:h.248	ITU-T Recommendation H.248 (MEGACO)
urn:dslforum-org:mgcp	Media Gateway Control Protocol (MGCP) as defined by RFC 3435
urn:dslforum-org:pppoe	Bridged sessions of PPPoE

A.3.2 FlowType

A syntax for forming URNs for the FlowType parameter in the Flow table of the QueueManagement service are defined for the Session Description Protocol (SDP) as defined by RFC 2327. Additional standard or vendor-specific URNs may be defined following the standard synax for forming URNs.

A URN to specify an SDP flow is formed as follows:

```
urn:dslforum-org: sdp- [MediaType] - [Transport]
```

[MediaType] corresponds to the "media" sub-field of the "m" field of an SDP session description.

[Transport] corresponds to the "transport" sub-field of the "m" field of an SDP session description.

Non-alphanumeric characters in either field are removed (e.g., "rtp/avp" becomes "rtpavp").

For example, the following would be valid URNs referring to SDP flows:

```
urn: dslforum-org: sdp-audio-rtpavp
urn: dslforum-org: sdp-video-rtpavp
urn: dslforum-org: sdp-data-udp
```

For FlowType URNs following this convention, there is no defined use for FlowTypeParameters, which should be left empty.

For the ProtocolIdentifier urn:dslforum-org:pppoe, a single flow type is defined referring to the entire PPPoE session. The URL for this FlowType is:

```
urn: dslforum-org :pppoe
```

A.3.3 FlowTypeParameters

For the FlowType urn:dslforum-org:pppoe, Table 24 specifies the defined FlowTypeParameter values.

Table 24 – FlowTypeParameter values for FlowType urn:dslforum-org:pppoe

Name	Description of Value
ServiceName	The PPPoE service name. If specified, only bridged PPPoE sessions designated for the named service would be considered part of this flow. If this parameter is not specified, or is empty, bridged PPPoE associated with any service considered part of this flow.
ACName	The PPPoE access concentrator name. If specified, only bridged PPPoE sessions designated for the named access concentrator would be considered part of this flow. If this parameter is not specified, or is empty, bridged PPPoE associated with any access concentrator considered part of this flow.
PPPDomain	The domain part of the PPP username. If specified, only bridged PPPoE sessions in which the domain portion of the PPP username matches this value are considered part of this flow. If this parameter is not specified, or is empty, all bridged PPPoE sessions are considered part of this flow.

A.4 Example Queuing Architecture for RG (from TR-059)

The queuing and scheduling discipline envisioned upstream for the RG is shown in Figure 3.

There are multiple access sessions supported in this model, however, all traffic is classified and scheduled in a monolithic system. So, while it might appear at first that the Diffserv queuing and scheduling might apply only to IP-aware access – in fact all access, IP, Ethernet, or PPP is managed by the same system that adheres to the Diffserv model.

For example, at the bottom of the figure, BE treatment is given to the non-IP-aware access sessions (PPPoE started behind the RG or delivered to an L2TP tunnel delivery model). This queue might be repeated several times in order to support fairness among multiple PPPoE accesses – or it may be a monolithic queue with separate rate limiters applied to the various access sessions.

The PTA access is a single block of queues. This is done because NSP access typically works with a single default route to the NSP, and managing more than one simultaneously at the RG would be perilous. The ∑ rate limiter would limit the overall access traffic for a service provider.

Rate limiters are also shown within the EF and AF service classes because the definition of those Diffserv types is based on treating the traffic differently when it falls into various rates.

Finally, at the top of the diagram is the ASP access block of queues. In phase 1A, these queues are provisioned and provide aggregate treatment of traffic mapped to them. In phase 1B, it will become possible to assign AF queues to applications to give them specific treatment instead of aggregate treatment. The EF service class may also require a high degree of coordination among the applications that make use of it so that its maximum value is not exceeded.

Notable in this architecture is that all the outputs of the EF, AF, and BE queues are sent to a scheduler (**S**) that pulls traffic from them in a strict priority fashion. In this configuration EF traffic is, obviously, given highest precedence and BE is given the lowest. The AF service classes fall in-between.

Note that there is significant interest in being able to provide a service arrangement that would allow general Internet access to have priority over other (bulk rate) services.[17] Such an arrangement would be

[17] This “bulk rate” service class would typically be used for background downloads and potentially for peer-to-peer applications as an alternative to blocking them entirely.

accomplished by assigning the bulk rate service class to BE and by assigning the default service class (Internet access) as AF with little or no committed information rate.

Given this arrangement, the precedence of traffic shown in the figure is arranged as:

1. EF – red dotted line
2. AF – blue dashed line (with various precedence among AF classes as described in RFC2597)
3. BE – black solid line

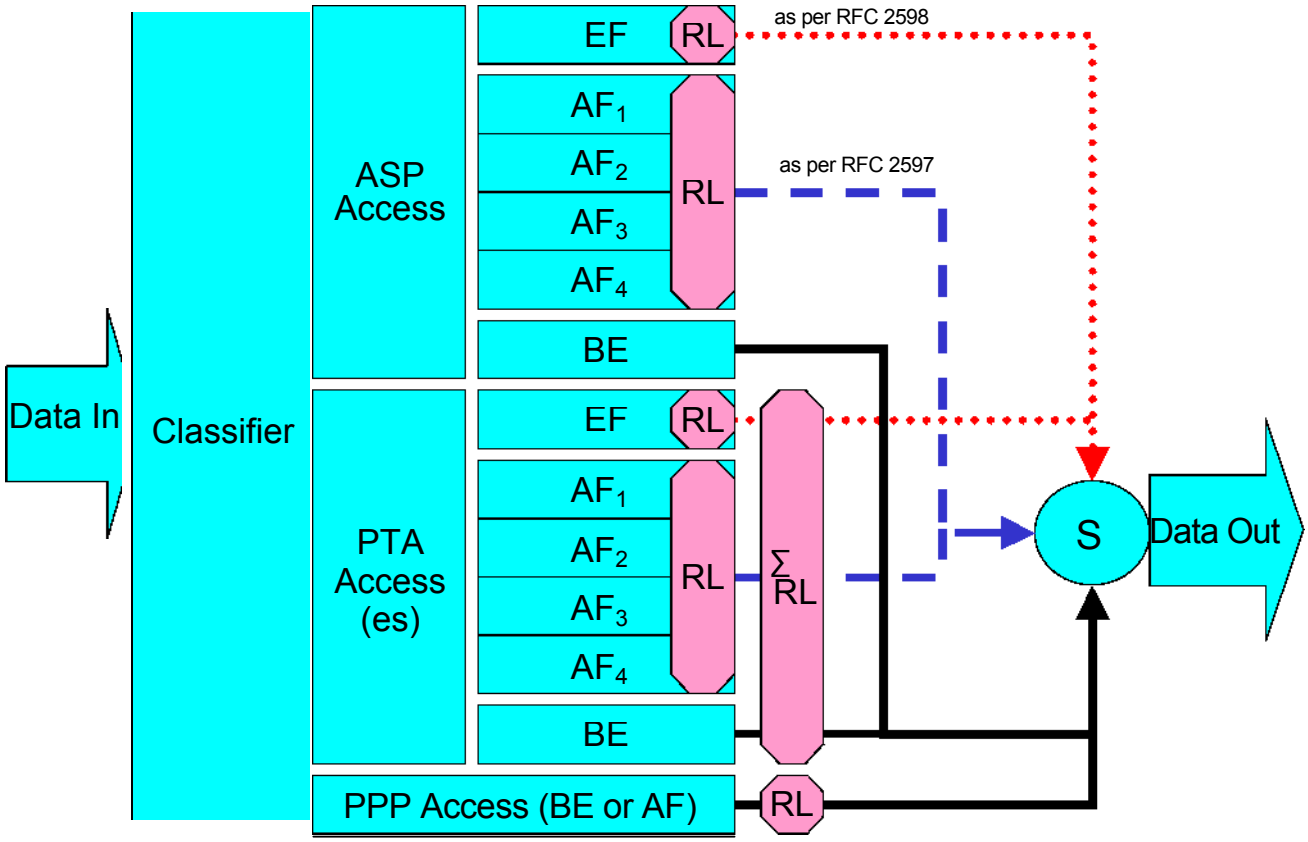


Figure 3 – Queuing and Scheduling Example for RG

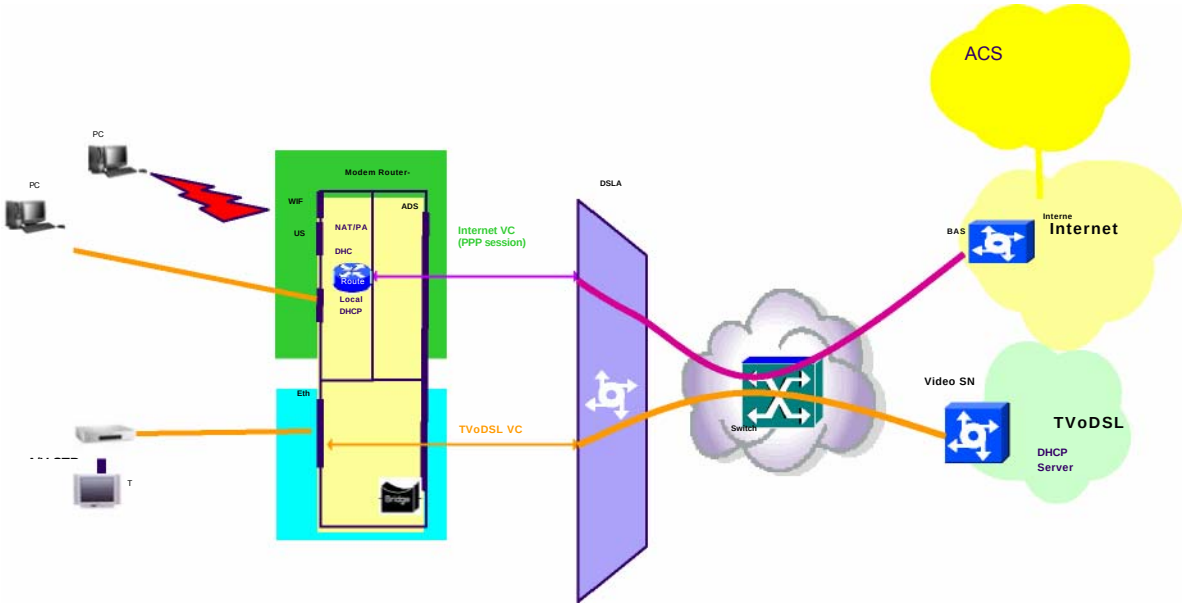
In Figure 3 the following abbreviations apply:

ASP – Application Service Provider
PTA – PPP Terminated Aggregation
PPP – Point-to-Point Protocol
EF – Expedited Forwarding – as defined in RFC 3246
AF – Assured Forwarding – as defined in RFC 2597
BE – Best Effort forwarding
RL – Rate Limiter
∑RL – Summing Rate Limiter (limits multiple flows)
S – Scheduler

A.5 Layer2Bridging Use Case: Interface Based Bridging

In an ITU-H.610 architecture using multi-VC and multi-edges to offer multi-services (high speed Internet, TVoDSL, etc.), one VC or a group of VCs are associated with each service. Regarding the CPE, some services may be layer-2 based if the service provider needs to have a layer-2 view of the home devices (for example, set-top boxes). If the services are offered by different service providers, and shared Internet access is also provided via the Internet Gateway, conflict between the local DHCP server and remote DHCP servers can occur. If there is no QoS on the home network there may also be issues regarding the priority of different streams. One solution is to associate one or more physical ports of the Internet Gateway with a specific service associated with one or more VCs.

As an example, Ethernet port 1 may be dedicated to a TVoDSL service and this port would be included in the same bridge with the VCs supporting the TVoDSL service. In this case, the other home network ports would be associated with the shared Internet access service. To achieve this, an interface-based bridge would be created using the Layer2Bridging object. A Bridge table entry would be created along with associated Filter table entries for Ethernet port 1, and each VC associated with the TVoDSL service. In this



case no filter criteria would be used in each Filter table entry. If the subscriber's services are modified, the Layer2Bridging configuration may need to be modified accordingly.

Figure 4 – Example of interface-based bridging

Annex B. LinkType and ConnectionType Interdependencies

For DSL CPE, the parameters LinkType in the WANDSLLinkConfig object and ConnectionType in the WANPPPConnection and WANIPConnection objects are interdependent. The LinkType parameter describes the ATM-layer encapsulation to be used for the corresponding ATM VC (in conjunction with the ATMEncapsulation parameter). The value of LinkType determines the possible types of connections that can be carried over the corresponding VC. Specifically, the LinkType determines:

- Whether the associated WANConnectionDevice object can contain WANPPPConnection objects, WANIPConnection objects, or both.
- The allowed values for the ConnectionType parameter within a WANPPPConnection object or WANIPConnection contained within the corresponding WANConnectionDevice.

Table 25 summarizes these interdependencies for a WANPPPConnection. For each value of LinkType listed across the top of the table, the table indicates allowed values of the ConnectionType for a WANPPPConnection. Entries with a check mark are allowed values, while entries marked "Forbidden" are not allowed.

For the columns that are marked "WANPPPConnection Forbidden," it is invalid to create a WANPPPConnection object in a WANConnectionDevice for which the LinkType is so configured.

Table 25 – LinkType and ConnectionType Interdependencies for a WANPPPConnection

LinkType / ConnectionType	PPPoA	EoA	IPoA	ClP	PPPoE	Unconfigured
IP_Routed	1	1	WANPPP-Connection Forbidden	WANPPP-Connection Forbidden	WANPPP-Connection Forbidden	WANPPP-Connection Forbidden
DHCP_Spoofed	1	1				
PPPoE_Bridged	Forbidden	1				
PPTP_Relay	1	1				
L2TP_Relay	1	1				
PPPoE_Relay	1	Forbidden				
Unconfigured	1	1				

Table 26 summarizes these interdependencies for a WANIPConnection. For each value of LinkType listed across the top of the table, the table indicates allowed values of the ConnectionType for a WANIPConnection. Entries with a check mark are allowed values, while entries marked "Forbidden" are not allowed.

For the columns that are marked "WANIPConnection Forbidden," it is invalid to create a WANIPConnection object in a WANConnectionDevice for which the LinkType is so configured.

Table 26 – LinkType and ConnectionType Interdependencies for a WANIPConnection

LinkType / ConnectionType	PPPoA	EoA	IPoA	CIP	PPPoE	Unconfigured
IP_Routed	WANIP-Connection Forbidden	1	1	1	WANIP-Connection Forbidden	WANIP-Connection Forbidden
IP_Bridged		1	Forbidden	Forbidden		
Unconfigured		1	1	1		

Note that the LinkType value of "PPPoE" is DEPRECATED since creation of either type of WAN connection object is forbidden when this value is set. This is due to the service-provider requirement to allow both PPPoE and IP simultaneously on the same ATM VC. To support PPPoE, the LinkType "EoA" MUST be used, since this LinkType also allows IP connections.

Note also that while the value "Unconfigured" is an allowed value for the LinkType and ConnectionType, a WAN connection can only be operational if both the corresponding LinkType and ConnectionType are set to values other than "Unconfigured".