PROPOSED DRAFT

DRAFT

PD-192

Residential Gateway (RG) IPv6 Requirements (updates to TR-124)

Revision: 02
Revision Date: July 2009

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Proposed Draft is a draft, and has not been approved by members of the Forum. Even if approved, this Broadband Forum Proposed Draft is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Proposed Draft is subject to change. This Broadband Forum Proposed Draft is copyrighted by the Broadband Forum, and portions of this Broadband Forum Working Text may be copyrighted by Broadband Forum members. This Proposed Draft is for use by Broadband Forum members only. Advance written permission by the Broadband Forum is required for distribution of this Broadband Forum Proposed Draft in its entirety or in portions outside the Broadband Forum.

This Broadband Forum Proposed Draft is provided AS IS, WITH ALL FAULTS. ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM PROPOSED DRAFT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY:

(A) OF ACCURACY, COMPLETENESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE;
(B) THAT THE CONTENTS OF THIS BROADBAND FORUM PROPOSED DRAFT ARE SUITABLE FOR ANY PURPOSE, EVEN IF THAT PURPOSE IS KNOWN TO THE COPYRIGHT HOLDER;
(C) THAT THE IMPLEMENTATION OF THE CONTENTS OF THE PROPOSED DRAFT WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

By using this Broadband Forum Proposed Draft, users acknowledge that there is no obligation upon Broadband Forum members to license patents that are necessary to implement a Proposed Draft, and such licensing obligations as may exist with respect to Broadband Forum Technical Reports do not attach until a proposed Technical Report is finalized by the Broadband Forum.

ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM PROPOSED DRAFT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW (A) ANY LIABILITY (INCLUDING DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES UNDER ANY LEGAL THEORY) ARISING FROM OR RELATED TO THE USE OF OR RELIANCE UPON THIS PROPOSED DRAFT; AND (B) ANY OBLIGATION TO UPDATE OR CORRECT THIS PROPOSED DRAFT.

The text of this notice must be included in all copies of this Broadband Forum Proposed Draft.

Revision History

Revision Number	Revision Date	Revision Editor	Changes
00	April 2009	Barbara Stark	Original
01	June 2009	B Stark, O Troan	Updated PPPoE requirements; MLD; additional new content from editors; multiple corrections
02	July 2009	B Stark, O Troan	Updates per review held July 1, 2009. Includes making all instances of "IP" and DHCP specific to v4 or v6.

Technical comments or questions about this Broadband Forum Proposed Draft should be directed to:

Editors:	Barbara Stark	AT&T	barbara.stark@att.com
	Ole Troan	Cisco	ot@cisco.com
BroadbandHome™ WG Chairs	Greg Bathrick	PMC-Sierra	
	Heather Kirksey	Alcatel-Lucent	
	Jason Walls	UNH Interoperability Lab	

TABLE OF CONTENTS

List of Figures

No table of figures entries found.

List of Tables

No table of figures entries found.

Summary

This Proposed Draft describes IPv6 requirements for a residential gateway. It is expected to provide requirements in a format so that they can be added to TR-124, as a revision to that document.

All service providers are currently considering their strategy for migrating to IPv6. These requirements will be a critical part of describing the RGs needed to support that migration.

1 Purpose and Scope

1.1 Purpose

This Proposed Draft provides functional IPv6 requirements for a broadband residential gateway. It is intended to provide an update to TR-124, for IPv6.

1.2 Scope

This Proposed Draft includes requirements in a modular format (consistent with TR-124) such that it includes a comprehensive identification of the functionality needed to provide IPv6 functionality in a broadband residential gateway. Because IPv6 is still not well understood and continues to evolve, this document includes a number of appendices and annexes intended to better explain and clarify the implications and intent of the requirements. These appendices and annexes may or may not be included in a revision of TR-124. That would be determined at a later date. However, these will continue to be included at least until such time as the document enters straw ballot.

2 References and Terminology

2.1 Conventions

In this Proposed Draft, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 **Error! Reference source not found.**.

MUST	This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the adjective "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references constitute provisions of this Proposed Draft. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Proposed Draft are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.
A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

[1] TR-124	*Functional Requirements for Broadband Residential Gateway Devices, Release 2.0*	Broadband Forum	December 2006
[2] RFC 2460	*Internet Protocol, Version 6 (IPv6) Specification*	IETF	December 1998

[3] RFC 2463	*ICMP for the Internet Protocol Version 6 (IPv6)*	IETF	December 1998
[4] RFC 2464	*Transmission of IPv6 Packets over Ethernet Networks*	IETF	December 1998
[5] RFC 2472	*IP version 6 over PPP*	IETF	December 1998
[6] RFC 2492	*IPv6 over ATM Networks*	IETF	January 1999
[7] RFC 2710	*Multicast Listener Discovery (MLD) for IPv6*	IETF	October 1999
[8] RFC 2893	*Transition Mechanisms for IPv6 Hosts and Routers*	IETF	August 2000
[9] RFC 3484	*Default Address Selection for Internet Protocol version 6 (IPv6)*	IETF	February 2003
[10] RFC 3315	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*	IETF	July 2003
[11] RFC 3544	*IP Header Compression over PPP*	IETF	July 2003
[12] RFC 3596	*DNS Extensions to Support IP Version 6*	IETF	October 2003
[13] RFC 3633	*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*	IETF	December 2003
[14] RFC 3646	*DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*	IETF	December 2003
[15] RFC 3901	*DNS IPv6 Transport Operational Guidelines*	IETF	September 2004
[16] RFC 4191	*Default Router Preferences and More-Specific Routes*	IETF	November 2005
[17] RFC 4193	*Unique Local IPv6 Unicast Addresses*	IETF	October 2005
[18] RFC 4294	*IPv6 Node Requirements*	IETF	April 2006
[19] RFC 4861	*Neighbor Discovery for IPv6*	IETF	September 2007
[20] RFC 4862	*IPv6 Stateless Address*	IETF	September

Autoconfiguration 2007

2.3 Definitions

The following terminology is used throughout this Proposed Draft.

RG A Residential Gateway is a device that interfaces between the WAN and LAN IP environment for a consumer broadband customer. It may route or bridge traffic, depending on its configuration and specifications.

2.4 Abbreviations

This Proposed Draft defines the following abbreviations:

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
IP	Internet Protocol
ND	Neighbor Discovery
NS	Neighbor Solicitation
PD	Prefix Delegation
RA	Router Advertisement
RG	Residential Gateway
RS	Router Solicitation

3 Proposed Draft Impact

3.1 Energy Efficiency

This Proposed Draft has no known impact on Energy Efficiency.

3.2 IPv6

This Proposed Draft is intended to address requirements needed for deployment of IPv6 capable RGs.

3.3 Security

The requirements in this Proposed Draft are intended to provide a reasonably secure environment for general consumers, while ensuring that the functionality is usable by consumers, such that they do not feel that the degree of security is preventing them from accomplishing what they want to do.

The requirements are also intended to ensure that the RG does not have a negative impact on the security of the access network and other users of the access network.

4 Residential Gateway Requirements

WAN		**Wide Area Networking (WAN)**		**Editors' working notes**
ATM		**ATM**		No requirement for RFC 2492 support.
CONNECT		**Connection Establishment** Note that this module applies to IPv6 connections as well as IPv4, but only if the device has an IPv6 stack.		
WAN.CONNECT.	1	The device MUST support an "always on" mode for connections. In this mode the device MUST NOT time out connection sessions (ATM, IP and PPP) and MUST automatically re-establish any sessions after disconnection, lease expiration or loss and restoration of power.	MUST	
WAN.CONNECT.	2	The device MUST support a "connect on demand" option for PPPoE connections. In this mode the connection to the broadband network is initiated when outbound traffic is encountered from the local LAN and terminated after a timeout period in which no traffic occurs.	MUST	
WAN.CONNECT.	3	The device MUST support a "manual connect" option for connections. In this mode the connection to the broadband network is initiated manually through the GUI or via TR-064/TR-069 request and, by default, terminates only when done so explicitly by the user, due to a power loss or when the connection is lost.	MUST	
WAN.CONNECT.	4	The interval after which a connection timeout occurs MUST be able to be configured.	MUST	
WAN.CONNECT.	5	A manual way of disconnecting without waiting for a connection timeout MUST be provided.	MUST	
WAN.CONNECT.	6	A default timeout of 20 minutes SHOULD be used for connection timeouts or use an operator-specific configuration.	SHOULD	
WAN.CONNECT.	7	The device MUST follow all standards required to perform an orderly tear down of the associated connections involved at the associated network levels (e.g., issue a DHCPRELEASE message when using DHCPv4, issue LCP Terminate-Request/Terminate-Ack and PADT packet when using PPPoE, etc.) and then restart the connections.	MUST	
WAN.CONNECT.	8	The device MUST detect the loss of communications with a network identified DNS server as indicated by a failed query, and upon	MUST	

		failed query, log the event.	
BRIDGE		**Bridging**	
WAN.BRIDGE.	1	The device MUST be able to bridge IPv4 over Ethernet.	MUST
WAN.BRIDGE.	2	The device MUST be a learning bridge as defined in IEEE 802.1D for all logical and physical Ethernet interfaces, supporting a minimum of 272 MAC addresses.	MUST
WAN.BRIDGE.	3	If bridge mode is enabled for IPv4 on the device by default for LAN connected devices, the device MUST be able to support additional connections for TR-069 remote management addressability (using direct DHCP or Static IPv4, PPP, etc.), and connections for any locally terminated service which require IP (v4 or v6) addressability (e.g. gateway integrated Voice ATA ports, etc.). Note that this special bridge mode that includes a device remote management session connection requires an additional WAN connection from the network. This requirement is considered conditional as a result due to the network side dependency, but the device must support this type of configuration.	MUST
DHCPC		**DHCP Client (DHCPv4)**	
WAN.DHCPC.	1	The device MUST be able to obtain IPv4 network information dynamically on its WAN interface. This information includes IPv4 address, primary and secondary DNS addresses and default gateway address. Dynamically obtaining IPv4 network information is accomplished using DHCP (v4) and / or IPv4CP.	MUST
WAN.DHCPC.	2	If the device is not configured to use a static IPv4 address and the modem fails to detect a PPPoE or DHCPv4 server, then the WAN IPv4 address assignment value SHOULD be set to an undefined value, in order to prevent it from retaining its prior IPv4 address.	SHOULD
WAN.DHCPC.	3	If a device is functioning as a DHCPv4 client, it MUST identify itself in option 61 (client-identifier) in every DHCPv4 message in accordance with IETF RFC 4361 (February 2006), Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4).	MUST

WAN.DHCPC.	4	For the DUID portion of option 61 in DHCPv4 as described in IETF RFC 4361, the device MUST follow the DUID-EN format specified in section 9.3 of RFC 3315. The device MUST use DSL Forum enterprise-number value 3561 in DUID-EN enterprise-number field. For the identifier field of the DUID-EN, the CPE MUST use an ASCII string containing the same content and formatted according to the same rules as defined for HTTP username in Section 3.4.4 of TR-069 Amendment 1.	MUST
WAN.DHCPC.	5	The device IAID value in DHCPv4 and DHCPv6 MUST be a 32 bit number encoded in network byte order. In cases where the device is functioning with a single DHCP client identity, it MUST use value 1 for IAID for all DHCP interactions. IAID is defined in IETF RFC 3315. In cases where the device is functioning with multiple DHCP client identities, the values of IAID have to start at 1 for the first identity and be incremented for each subsequent identity. The device's mapping of IAID to its physical aspects or logical configuration SHOULD be as non-volatile as possible. For example, the device MAY use IAID value 1 for the first physical interface and value 2 for the second. Alternatively, the device MAY use IAID value 1 for the virtual circuit corresponding to the first connection object in the data model and value 2 for the second connection object in the data model.	MUST
WAN.DHCPC.	6	The DUID-EN field value MAY be printed on the product label on the bottom of the device.	MAY

WAN.DHCPC.	7	A device functioning as a DHCPv4 client MUST identify its manufacturer OUI, product class, model name and serial number using vendor-specific options as defined in IETF RFC 3925. Specifically, it MUST use option 125. Note that with exception of ModelName this data contained in this option will be redundant with what is included in the Device ID in option 61. However, this is desirable because these two options serve different purposes. The data in option 125 allows DHCPv4 server to be pre-configured with policy for handling classes of devices in a certain way without requiring DHCPv4 server to be able to parse the unique format used in client-identifier option (which can also vary in TR-069 depending on presence of ProductClass value). On the other hand, the client-identifier serves as an opaque, but predictable identifier. It is predictable because it is the same identifier as used by device for interactions with other services. The same identifier is used for HTTP authentication and in SSL client certificates. Each sub-option value to be provided in option 125 MUST be treated as string encoded into binary using UTF-8. The data MUST be encapsulated in option 125 under enterprise code 3561 in decimal (0x0DE9 in hexadecimal), corresponding to the IANA "ADSL Forum" entry in the Private Enterprise Numbers registry. A specific sub-option is defined for each value and the value must match a corresponding TR-069 / TR-106 parameter as defined in the following table: Sub-option Value Description Corresponding TR-069 / TR-106 parameter 1 Manufacturer OUI .DeviceInfo.ManufacturerOUI 2 Product Class .DeviceInfo.ProductClass 3 Model Name .DeviceInfo.ModelName 4 Serial Number .DeviceInfo.SerialNumber If the value of a parameter is empty for the device, then the sub-option MUST be omitted.	MUST	Need requirement in WAN.IPv6 section for how OPTION_VENDOR_CLASS (16) or OPTION_VENDOR_OPTS (17) is used to provide this info in DHCPv6?
IPv6	TOC	**IPv6 WAN Connection**		
WAN.IPv6.	1	The device MUST support automated establishment of an IPv6 connection according to the flow in Annex A.2.	MUST	
WAN.IPv6.	2	The device MUST support RFC 2460, "Internet Protocol, Version 6 (IPv6) Specification".	MUST	
WAN.IPv6.	3	The device MUST support dual stack of IPv4 and IPv6 running simultaneously, as described in Section 2 of RFC 4213, "Transition	MUST	

		Mechanisms for IPv6 Hosts and Routers".	
WAN.IPv6.	4	The device MUST allow the IPv6 stack to be enabled / disabled.	MUST
WAN.IPv6.	5	The device MUST support DHCPv6 client messages and behavior per IETF RFC 3315. See WAN.DHCPC.5 for further specifics on IAID value.	MUST
WAN.IPv6.	6	The device MUST support RFC 3633, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6."	MUST
WAN.IPv6.	7	The device MUST support specifying in its DHCPv6 prefix delegation request an indication of the length of prefix it requires. If the RG supports multiple LANs, or has PD requests from its LAN, it MUST indicate a preferred prefix length at least equal to the longest length that would enable the RG to assign a /64 prefix to each LAN it supports. Note that the delegated prefix may vary from the requested length	MUST
WAN.IPv6.	8	When sending DHCPv6 messages, the device MUST identify itself in OPTION_CLIENTID (1) (client-identifier) using the same client identifier as for IPv4 (see WAN.DHCPC.3 and .4).	MUST
WAN.IPv6.	9	The device MUST support IPv6 Node Requirements as a host node, per IETF RFC 4294. Note that RFC 2461 reference by RFC 4294 has been obsoleted by RFC 4861.	MUST
WAN.IPv6.	10	The device MUST support stateless address auto-configuration per IETF RFC 4862.	MUST
WAN.IPv6.	11	The device MUST support receipt of route information per RFC 4191. If the device only has one WAN connection, it does not need to place this information in its routing table, but it does need to save it (for possible sending on the LAN interface).	MUST
WAN.IPv6.	12	If route information is provided (RFC 4191) and the device has multiple WAN connections, it MUST place the route information in its routing table.	MUST
WAN.IPv6.	13	If the device does not have a globally-scoped address on its WAN interface after being delegated a prefix, it MUST create addresses for itself from the delegated prefix. It MUST have at least one address and MAY have more. There is currently no algorithm defined for address creation and it should be assumed that different service providers will want different rules for how to create the address, how many addresses to create, and, in the case of multiple addresses, how the different addresses are used.	MUST
WAN.IPv6.	14	The device MUST support enabling / disabling of this IPv6 WAN connection interface.	MUST

WAN.IPv6.	15	The device MUST be able to request the following DHCPv6 options:	MUST	Need to define this list. Needs to include Prefix, Address, DNS; see bbf2008.814 A.3 and A.4 for good DHCPv4 list
WAN.IPv6.	16	The device SHOULD be able to request the following DHCPv6 options:	SHOULD	Need to define this list.
WAN.IPv6.	17	The device MUST be configurable as to which DHCPv6 options it requests via DHCPv6.	MUST	
WAN.IPv6.	18	The connectivity parameters (obtained via RA and DHCPv6) MUST be persistent across reboot, power loss, and loss of WAN connection (or lack of response from WAN connection).	MUST	
WAN.IPv6.	19	The device MUST continue to use the connectivity parameters (obtained via RA or DHCP) and consider them valid until either they expire or the device is explicitly told to use different values.	MUST	
WAN.IPv6.	20	The device MUST NOT advertise any address prefixes on the WAN using the IPv6 Neighbor Discovery protocol, or advertise itself as a default router	MUST NOT	
TRANS		**Transitional IPv6 WAN Connection**		
WAN.TRANS.	1	TBD: candidates include 6rd, softwires, others, but will only be included if enough service providers express interest in any one solution.		This is a placeholder. Any service provider who wants a particular solution supported needs to provide requirements.
PPP		**PPP Client**		
WAN.PPP.	1	The device MUST support PPP and the associated protocols as defined in IETF RFCs 1332, 1334, 1661, 1877, 1994.	MUST	
WAN.PPP.	2	The device MUST support IETF RFCs 1570 and 2153 traffic and operate without fault. This is not stating that specific extensions MUST be supported directly. It is identifying that upon receipt of non-standard or unrecognized PPP extensions from the broadband network (e.g., vendor or proprietary), the device MUST operate without fault.	MUST	
WAN.PPP.	3	The device MUST support PPPoE over the encapsulated Ethernet as defined in IETF RFC 2516.	MUST	
WAN.PPP.	4	The device MUST support IETF RFC 4638 in order to accommodate MTU/MRU values greater than 1492 bytes in PPPoE.	MUST	

WAN.PPP.	5	If the device supports ATM, the device SHOULD support PPP over AAL5 (PPPoA) as defined in IETF RFC 2364.	SHOULD
WAN.PPP.	6	The device MUST be able to save all logins and passwords for PPP sessions originated by the device. Passwords MUST NOT be available outside of the internal operation of the device (e.g., can not be queried nor displayed).	MUST
WAN.PPP.	7	The device MUST not immediately terminate PPPoE sessions and upper layer protocol connections when the physical connection is lost. It should defer the tear down process for two minutes. If the physical connection is restored during that time, the device MUST first attempt to use its previous PPPoE session settings. If these are rejected, then the original PPPoE session can be terminated and a new PPPoE session attempted.	MUST
WAN.PPP.	8	The device SHOULD incorporate a random timing delay prior to starting each IP (v4 or v6) and PPP session. This random timing delay helps to reduce connection failures when a group of users attempt to establish connections to a service provider at the same time (e.g., after power is restored to a neighborhood that had a blackout).	SHOULD
WAN.PPP.	9	The device SHOULD not attempt immediate additional PPP session connections upon receipt of an authentication failure. A back off mechanism SHOULD be implemented to limit repeated attempts to reconnect in this situation. 3 connection attempts SHOULD be made followed by a delay and then repeated by the next sequence of connection attempts. The delay SHOULD be 5 minutes at first, and then repeated every 30 minutes as required. This requirement only applies to automated connection attempts.	SHOULD
WAN.PPP.	10	If the device is using PPPoE client function actively, the device MUST be able to forward PPPoE sessions initiated from LAN devices as additional PPPoE sessions to the WAN interface (this is sometimes known as PPPoE pass-through). Specifically these LAN initiated PPPoE sessions MUST NOT be tunneled inside the device's primary PPPoE client session.	MUST
WAN.PPP.	11	If the network implements the TR-059 type architecture, and when fragmentation is required, the device MUST fragment all PPP sessions that it originates on an access VC using MLPPP interleaving as defined in IETF RFC 1990.	MUST

WAN.PPP.	12	If PPP is used, the device MAY obtain an IPv4 subnet mask on its WAN interface using IPv4CP extensions. If this is done, then IPv4 subnet masks will be communicated with IPv4CP using the PPP IPv4CP option with option code 144, the length of the option being 6 and the mask being expressed as a 32-bit mask (e.g. 0xFFFFFF80), not as a number indicating the consecutive number of 1s in the mask (from 0 to 32). The learned network information MAY, but need not, be used to populate the LAN side embedded DHCP server for the modem. The learned network information is treated as a subnet and not as a collection of individual addresses. That is, the first and last address in the subnet should not be used. The IPv4 address negotiated SHOULD, but need not, be the one assigned to the modem.	MAY
WAN.PPP.	13	The device MUST make the access concentrator name used with PPPoE connections available via the Web GUI, TR-064 or TR-069 request for diagnostic purposes.	MUST
WAN.PPP.	14	The device MUST support RFC 3544, "IP Header Compression over PPP".	
PPP.IPv6	TOC	**PPP Client for establishment of IPv6 connection**	
WAN.PPP.IPv6.	1	The device MUST support IPv6 over PPP per IETF RFC 5072.	MUST
WAN.PPP.IPv6.	2	The device MUST support establishment of an IPv6 over PPPoE connection according to the flow in Annex A.1.	MUST
WAN.PPP.IPv6.	3	The device MUST allow any particular PPP connection to be configurable for IPv4-only, IPv6-only, or both.	MUST
WAN.PPP.IPv6.	4	If the device is configured for multiple PPPoE connections, it MUST be possible to configure it to use the same login and password for all, so that only the domain is unique per connection.	MUST
WAN.PPP.IPv6.	5	The RG MUST NOT tear down a shared (IPv4 and IPv6) PPP session if error conditions prevent only one IP stack (either IPv4 or IPv6) from working. The session MUST be torn down if error conditions apply to both stacks	MUST
dot1x		**802.1x Client**	
WAN.dot1x.	1	The device MUST support IEEE 802.1X™ acting as a supplicant.	MUST
WAN.dot1x.	2	The device MUST be able to respond to an appropriate IEEE 802.1X request and provide certificate information using Extensible	MUST

		Authentication Protocol-Transport Layer Security (EAP/TLS).	
WAN.dot1x.	3	The device SHOULD support EAP-MD5 username and password type authentication.	SHOULD
WAN.dot1x.	4	The device MUST support receiving IEEE 802.1X EAPOL frames with an individual MAC address (i.e., unicast) as well as frames with a group MAC address (i.e., multicast).	MUST
WAN.dot1x.	5	The device MUST perform mutual authentication by authenticating certificate information of the requesting authenticator.	MUST
WAN.dot1x.	6	The device MUST be able to store certificate information used to authenticate the authenticator.	MUST
WAN.dot1x.	7	The device MUST be able to update the information used to validate the authenticator by either a firmware upgrade or via updated certificates.	MUST
WAN.dot1x.	8	The device SHOULD be able to update the information used to validate the authenticator by updated certificates without a firmware upgrade.	SHOULD
WAN.dot1x.	9	The device MUST be able to store information allowing it to authenticate a minimum of eight authenticators.	MUST
WAN.dot1x.	10	When used with IPv4 over Ethernet and DHCPv4, if the device already has a connection when receiving an IEEE 802.1X request, the device SHOULD subsequently perform a DHCPv4 lease renewal upon successful 802.1X authentication.	SHOULD
WAN.dot1x.	11	Each device MUST have a unique factory-installed private/public key pairs and embedded ITU-T X.509 Version 3 / IETF RFC 3280 certificate that has been signed by the supplier's device certificate authority.	MUST
WAN.dot1x.	12	The device certificate MUST have a validity period greater than the operational lifetime of the device.	MUST
WAN.dot1x.	13	When used with IPv6 over Ethernet and DHCPv6, if the device already has a connection when receiving an IEEE 802.1X request, the device SHOULD subsequently perform a DHCPv6 CONFIRM upon successful 802.1X authentication.	SHOULD
DoS		**Denial of Service Prevention** Note that the IPv6 parts of this module apply only if the device has an IPv6 stack.	

WAN.DoS.	1	The device MUST provide Denial of Service (DOS) protection for itself and all LAN CPE including protection from Ping of Death, SYN Flood LAND and variant attacks. The extent of this protection will be limited when the device is configured as a bridge in which only PPPoE traffic is bridged. This protection MUST be available when the device terminates IP (v4 or v6) or bridges IPv4.	MUST	
WAN.DoS.	2	The device MUST reject packets from the WAN with MAC addresses of devices on the local LAN or invalid IP (v4 or v6) addresses (e.g., broadcast addresses~~, private IP addresses~~ or IP (v4 or v6) Addresses matching those assigned to the LAN Segment).	MUST	Removed restriction on private IP addresses.
WAN.DoS.	3	The device MUST reject any unidentified Ethernet packets (i.e. any packet that is not associated with IP (v4 or v6) or PPPoE protocols).	MUST	
WAN.DoS.	4	The device MUST perform anti-spoofing filtering for IPv6. All IPv6 traffic sent to the WAN from the LAN MUST have an IPv6 source address with a prefix assigned to the LAN by the device, that was delegated from the WAN (through DHCPv6 or configuration).	MUST	
WAN.DoS.	5	Since the device must perform anti-spoofing filtering for IPv6, until it has an IPv6 LAN prefix delegation it MUST filter all upstream IPv6 traffic from the home.	MUST	
QoS		**Quality of Service** Note that the IPv6 parts of this module apply only if the device has an IPv6 stack.		
WAN.QoS.	1	The device MUST support classification of WAN directed LAN traffic and placement into appropriate queues based on any one or more of the following pieces of information: (1) destination IP (v4 or v6) address(es) with subnet mask, (2) originating IP (v4 or v6) address(es) with subnet mask, (3) source MAC address, (4) destination MAC address, (5) protocol (TCP, UDP, ICMP, …) (6) source port, (7) destination port, (8) IEEE 802.1D Ethernet priority, (9) FQDN (Fully Qualified Domain Name) of WAN session, (10) Diffserv codepoint (IETF RFC 3260), (11) Ethertype (IEEE 802.3, 1998 Length/Type Field), and (12) traffic handled by an ALG, and (13) IEEE 802.1Q VLAN identification.	MUST	

WAN.QoS.	2	The device MUST support classification of WAN directed LAN traffic and placement into appropriate queues based on any one or more of the following pieces of information: (1) packet length.	SHOULD
WAN.QoS.	3	The device MUST support the differentiated services field (DS Field) in IP (v4 or v6) headers as defined in IETF RFC 2474.	MUST
WAN.QoS.	4	The device MUST by default recognize and provide appropriate treatment to packets marked with recommended Diffserv Codepoints, whose values and behavior are defined in IETF RFC 2474, 2475, 2597, 3246, and 3260. Specifically, the values shown in the DSCP column of the table below MUST be supported, except the Cs0-7, which are optional.	MUST

Class	Description	DSCP marking (name)	DSCP marking (decimal value)
EF	Realtime	ef	46
AF4 – in-contract	Premium class4 (in)	af41	34
AF4 – out-of-contract	Premium class4 (out)	af42, af43	36, 38
AF3 – in-contract	Premium class3 (in)	af31	26
AF3 – out-of-contract	Premium class3 (out)	af32, af33	28, 30
AF2 – in-contract	Premium class2 (in)	af21	18
AF2 – out-of-contract	Premium class2 (out)	af22, af23	20, 22
AF1 – in-contract	Premium class1 (in)	af11	10
AF1 – out-of-contract	Premium class1 (out)	af12, af13	12, 14
DE/BE	Default / Best Effort	be	0
Cs0 (optional)	Class Selector 0	cs0	0
Cs1 (optional)	Class Selector 1	cs1	8
Cs2 (optional)	Class Selector 2	cs2	16
Cs3 (optional)	Class Selector 3	cs3	24
Cs4 (optional)	Class Selector 4	cs4	32
Cs5 (optional)	Class Selector 5	cs5	40
Cs6 (optional)	Class Selector 6	cs6	48
Cs7 (optional)	Class Selector 7	cs7	56

WAN.QoS.	5	The device MUST be able to mark or remark the Diffserv codepoint or IEEE 802.1D Ethernet priority of traffic identified based on any of the classifiers supported by the device.	MUST
WAN.QoS.	6	The device SHOULD support sending the following frame types: untagged frames, priority-tagged frames, and VLAN-tagged	SHOULD

		frames in the upstream direction. This satisfies TR-101 R-01.	
WAN.QoS.	7	The device SHOULD support setting the priority tag and VLAN ID values. This satisfies TR-101 R-02.	SHOULD
WAN.QoS.	8	The device SHOULD support receiving untagged and VLAN-tagged Ethernet frames in the downstream direction, and SHOULD be able to strip the VLAN tagging from the ones received tagged. This satisfies TR-101 R-03.	SHOULD
WAN.QoS.	9	The device MUST support one Best Effort (BE) queue, one Expedited Forwarding (EF) queue and a minimum of four Assured Forwarding (AF) queues.	MUST
WAN.QoS.	10	The device MUST duplicate the set of queues for each access session. This can be done logically or physically.	MUST
WAN.QoS.	11	The device SHOULD support the appropriate mechanism to effectively implement Diffserv per hop scheduling behaviors. A strict priority scheduler is preferred for EF.	SHOULD
WAN.QoS.	12	The device SHOULD support aggregate shaping of upstream traffic.	
WAN.QoS.	13	The device SHOULD support per-class shaping of upstream traffic.	
WAN.QoS.	14	The device MUST support the capability to fragment traffic on sessions that it originates, in order to constrain the impact of large packets on traffic delay.	MUST
WAN.QoS.	15	The packet size threshold before fragmenting AF and BE packets MUST be configurable.	MUST
LAN		**Local Area Networking (LAN)**	
GEN		**General LAN Protocols**	
LAN.GEN.	1	The device MAY support SOCKS as defined in IETF RFC 1928 for non-ALG access to the public address.	MAY
LAN.GEN.	2	Both NetBios and Zero Config naming mechanisms MAY be used to populate the DNS tables.	MAY
LAN.GEN.	3	The device MAY act as a NETBIOS master browser for that name service.	MAY
LAN.GEN.	4	The device MUST support multiple subnets being used on the local LAN.	MUST
ADDRESS		**Private IPv4 Addressing**	
LAN.ADDRESS.	1	The device MUST be able to be configured to specify alternate public and private subnets (without restriction) for local device addressing.	MUST
LAN.ADDRESS.	2	The device MUST be able to be configured to specify the start and stop addresses within a subnet used for local addressing.	MUST
LAN.ADDRESS.	3	The device MUST NOT use auto IP for address assignment of its LAN-side IPv4	MUST

		address.	
LAN.ADDRESS.	4	The device MUST allow its assigned address and netmask to be specified through the Web GUI and via TR-064/TR-069 interfaces.	MUST
LAN.ADDRESS.	5	If the device is in bridged configuration and LAN side configuration is enabled, the device MUST ARP on the LAN side for the following addresses, in order, and assign itself the first one that is not taken: 192.168.1.254, 192.168.1.63, and then starting from 192.168.1.253 and descending.	
LAN.ADDRESS.	6	The device MUST be able to assign its own WAN IPv4 address (e.g., public address) to a particular LAN device, concurrent with private IPv4 addressing being used for other LAN CPE. In this situation, one device on the LAN is given the same public IPv4 address (through DHCP or manual configuration of the LAN CPE IPv4 stack). Other LAN devices utilize private IPv4 addresses. The device can then be configured as identified in LAN.PFWD.2 so that the LAN device "sharing" the WAN IPv4 address receives all unidentified or unsolicited port traffic to any specific LAN device. If the device is not configured in this manner, then only inbound traffic resulting from outbound traffic from the LAN CPE would be directed to that LAN CPE. The gateway identified to the LAN device must be on the same subnet as that associated with the WAN IPv4 address. Note that the use of the WAN gateway address does not guarantee this since it need not meet this requirement.	MUST
LAN.ADDRESS.	7	When operating in multiple WAN public IPv4 address mode, the device MUST support the up to 16 public IPv4 addresses being used by LAN devices (statically or dynamically issued) and whose traffic must be routed to and from the public IPv4 address associated with the LAN device. Additionally, a Transparent Basic NAT mapping feature MAY be supported, allowing the 16 public address to be mapped to a device's private address. A user configurable option in the Web GUI MUST be provided to enable or disable the firewall on a per public IPv4 basis. This feature must operate concurrently with other LAN usage (e.g., NAPT on the gateway's primary IPv4 address).	MUST

LAN.ADDRESS.	8	When using a WAN IPv4 address assigned to a LAN device, the user MUST be able to configure if this LAN device can directly communicate with other devices on the local LAN without the need to traverse the broadband connection. This will only be done to the extent which the device can control the isolation (e.g., routing and internal switch fabric). It does not extend to isolation external to the device (e.g., external switch or router) which are outside of the control of the device.	MUST	
ADDRESSv6		**LAN IPv6 Addressing**		
LAN.ADDRESSv6.	1	The device MUST create a Link Local (LL) address for its LAN interface, and perform Duplicate Address Discovery (DAD), per RFC 4861. It MUST always use the same LL address, even after reboot or power failure.	MUST	
LAN.ADDRESSv6.	2	The device SHOULD try alternate LL addresses, if DAD fails. The vendor can define the algorithm to be used in this case.	SHOULD	
LAN.ADDRESSv6.	3	The device MUST send a Router Solicitation to the LAN, to determine if there are other routers present.	MUST	Ole: Violates RFC4861 on router behaviour.
LAN.ADDRESSv6.	4	If the device determines other routers are present in the LAN, and that another router is advertising a ULA prefix, the device MUST be configurable to automatically use this information to decide not to advertise its own ULA prefix.	MUST	Ole: Need more consideration
LAN.ADDRESSv6.	5	If another router is advertising a valid/preferred ULA for SLAAC (RFC 4862), the device SHOULD generate an address from that ULA, for use on the LAN. This applies to all advertised ULAs.	SHOULD	Should the device generate addresses from all advertised prefixes, or just ULA?
LAN.ADDRESSv6.	6	The device MUST have a ULA prefix [RFC 4193]. It MUST always maintain the same prefix, even after reboot or power failure, unless this prefix is changed through configuration (in which case it maintains the changed value).	MUST	
LAN.ADDRESSv6.	7	The device MAY allow its ULA prefix to be changed through configuration.	MAY	
LAN.ADDRESSv6.	8	The device MUST support advertising a /64 from its ULA prefix through Router Advertisement to be enabled / disabled. When enabled, this /64 will be included in RA messages, with L=1, A=1, and reasonable timer values.	MUST	Do we want to provide guidance as to which /64 to select? E.g., the /64 that takes the prefix plus enough zeroes to make it a /64?

LAN.ADDRESSv6.	9	The device MUST support Stateless Address Auto Configuration (SLAAC) from IETF RFC 4862.	MUST	
LAN.ADDRESSv6.	10	The device MUST support configuration of the following elements of a Router Advertisement: "M and O" flags (RFC 4861), Route Information (RFC 4191), and Default Router Preference (Prf) (RFC 4191).	MUST	
LAN.ADDRESSv6.	11	The device SHOULD support configuration of the following elements of a Router Advertisement: MTU (RFC 4861).	SHOULD	
LAN.ADDRESSv6.	12	The device MUST advertise (in RA) a /64 prefix from all prefixes delegated via the WAN interface. This will have L=1, A=1, and lifetimes per the received (from the WAN) delegation.	MUST	Do we want to provide guidance as to which /64 to select? E.g., the /64 that takes the prefix plus enough zeroes to make it a /64?
DHCPS		**DHCPv4 Server**		
LAN.DHCPS.	1	The device MUST provide application layer support for host name mapping, booting, and management including DHCPv4 and the Domain Name System (DNS) protocol. This includes support for the standards below: - IETF RFC 1034 Domain Names - Concepts and Facilities - IETF RFC 1035 Domain Names - Implementation and Specification - IETF RFC 2131 Dynamic Host Configuration Protocol - IETF RFC 2132 DHCP Options and BOOTP Vendor Extensions - IETF RFC 2181 Clarifications to the DNS Specification - IETF RFC 2939 Procedure for Defining New DHCP Options and Message Types	MUST	
LAN.DHCPS.	2	The device MUST be a DHCPv4 server to local LAN devices, supporting all LAN devices.	MUST	
LAN.DHCPS.	3	The embedded DHCPv4 server function of the device MUST be able to operate while in bridged mode. The default state should be on in bridged and routed mode.	MUST	
LAN.DHCPS.	4	The device MUST support a minimum of 253 LAN devices.	MUST	
LAN.DHCPS.	5	The device MUST support turning off the embedded DHCPv4 server via a configuration change locally via the Web GUI and remotely via TR-064/TR-069 interfaces.	MUST	

LAN.DHCPS.	6	The device MAY incorporate auto-detection of other DHCPv4 servers on the local LAN and, if configured to do so, disable the internal DHCPv4 server functionality of the device in this situation. In this situation, the device would try to obtain a configuration for its LAN port through DHCPv4. If a DHCPv4 response was received, the device would then use the information in the DHCPv4 response (e.g., IPv4 Address, subnet and DNS information) and disable its internal DHCPv4 server. If implemented and a DHCPv4 response is received, this requirement takes precedence over requirement LAN.DHCPS.15.	MAY
LAN.DHCPS.	7	The embedded DHCPv4 server functionality of the device MUST verify that an address is not in use prior to making it available in a lease (e.g., via Ping or ARP table validation) even when lease information shows that it is not in use.	MUST
LAN.DHCPS.	8	If the device is in a routed configuration (i.e. full NAPT router), the device MUST use the default start address of 192.168.1.64 and the default stop address of 192.168.1.253 for assignment to DHCPv4 leases for local device addressing, or use an operator-specific configuration.	MUST
LAN.DHCPS.	9	If the device is in a routed configuration (i.e. full NAPT router), the device MUST use a default netmask of 255.255.255.0 for assignment to DHCPv4 leases for local device addressing, or use an operator-specific configuration.	MUST
LAN.DHCPS.	10	If the device is in a bridged configuration for LAN device traffic (i.e. NAT/NAPT is not enabled), the device MUST support the enabling and configuration of the local device DHCPv4 server (address range and subnet mask) remotely via TR-069 interface. This address range may be either public or private addresses (assuming that the service provider is providing the NAT/NAPT function in the network). Note that this assumes that a separate management IP (v4 or v6) interface has been established to the device expressly for the purpose of TR-069 remote management.	MUST
LAN.DHCPS.	11	The default lease time for DHCPv4 information provided to LAN CPE which do not share the WAN side IPv4 address MUST be configurable. The default value MUST be 24 hours, or use an operator-specific configuration.	MUST

LAN.DHCPS.	12	The default lease time for DHCPv4 information provided to LAN CPE which share the WAN side IPv4 address MUST be configurable. The default value MUST be 10 minutes, or use an operator-specific configuration.	MUST
LAN.DHCPS.	13	When the domain name that the embedded DHCPv4 server passes to LAN CPE has not been set, the value "domain_not_set.invalid" SHOULD be used.	SHOULD
LAN.DHCPS.	14	If the device is in a routed configuration (i.e. full NAPT router) and the device's embedded DHCPv4 server is enabled, the device itself MUST default to the address 192.168.1.254 (with a netmask of 255.255.255.0), or use an operator-specific configuration.	MUST
LAN.DHCPS.	15	When the device's embedded DHCPv4 server is disabled, the device MUST ARP for the following addresses, in order, and assign itself the first one that is not taken: 192.168.1.254, 192.168.1.63, and then starting from 192.168.1.253 and descending.	MUST
LAN.DHCPS.	16	The device MAY allow the embedded DHCPv4 server to be configured so that specific MAC addresses can be identified as being served or not served.	MAY
LAN.DHCPS.	17	The device MAY allow the embedded DHCPv4 server to be configured with a default setting (provide IPv4 addresses or do not provide IPv4 addresses) for devices with unspecified MAC addresses.	MAY
LAN.DHCPS.	18	The embedded DHCPv4 server functionality of the device SHOULD provide a mechanism by which an IPv4 address can be assigned to a particular LAN device by MAC address. The user interface to establish this association may use an alternate mechanism to identify this assignment (e.g., by selecting the device using its current IPv4 address or device name) and the MAC address may be transparent to the user. These addresses may include the ability to assign an address within the default subnet or an address from additional public/private subnets that may be provisioned. For example, the device might have a default WAN side IPv4 address which is used for NAPT to a subset of devices and an additional set of WAN side IPv4 addresses which are bridged. The embedded DHCPv4 server might be used to assign this second set of IPv4 addresses to specific LAN CPE.	SHOULD

LAN.DHCPS.	19	The device MUST support a single PC mode of operation. In this mode of operation only a single LAN device is supported. Note that this is not the default mode of operation. In this configured mode, all network traffic, except for configured management traffic destined for the modem itself (e.g., temporary remote access to the Web GUI) MUST be passed between the access network and the designated LAN device as if the device was not present. One possible implementation is for the embedded DHCPv4 server to issue one and only one private address in this situation, with the start and stop address for the embedded DHCPv4 server being the same. The LAN devices can be assigned either a private IPv4 address (i.e., using 1:1 NAT) or the public IPv4 address of the modem (i.e., using IP Pass-through as identified in requirement LAN.ADDRESS.6). The type of IPv4 address to be used (private or public) is configured through the Web GUI and TR-064/TR-069 interfaces. The default is a public IPv4 address. If a WAN connection is not available when the device is configured to use a public IPv4 address, the LAN device is provided with a private IPv4 address from the device via DHCP. Once a WAN connection is established, the public IPv4 address provided by the broadband network is passed to the LAN device during the next DHCP lease renewal. The Broadband Residential Gateway acts as the default gateway to the LAN devices when private IPv4 addressing is in use. When public IPv4 addressing is in use, the gateway identified to the LAN device should be that identified in requirement LAN.ADDRESS.6 above. No other restrictions (e.g., restricted routing for other devices) need to be implemented to meet this requirement (e.g., no routing restrictions on traffic from secondary devices on the LAN).	MUST
LAN.DHCPS.	20	If the device is configured in a routed configuration (i.e. full NAPT router), the device MUST operate by default in the multiple PC mode of operation, or use an operator-specific configuration.	MUST

DHCPSv6		**DHCPv6 Server**		
LAN.DHCPSv6.	1	The device MUST support DHCPv6 server messages and behavior per IETF RFC 3315.	MUST	
LAN.DHCPSv6.	2	The device MUST support and be configurable to enable/disable address assignment using DHCPv6.	MUST	
LAN.DHCPSv6.	3	The device MUST either have an algorithm or allow configuration (or both) as to which /64 prefix to use, from any received WAN prefixes or its own ULA prefix.	MUST	
LAN.DHCPSv6.	4	The device SHOULD be configurable to support rules as to which host devices will be assigned addresses through DHCPv6. That is, it should be possible for a service provider to place their own host devices in the premises and have the RG only support DHCPv6 address assignment to those devices. Note that this does not require use of the RA "M" flag, as the service provider host devices can be configured to always use DHCPv6 for address assignment. The DUID may help to identify host devices.	SHOULD	
LAN.DHCPSv6.	5	The device MUST be configurable to enable/disable prefix delegation via DHCPv6.	MUST	
LAN.DHCPSv6.	6	The device MUST support delegation of any received WAN prefix and its own ULA prefix, that is shorter than /64, using mechanisms of RFC 3633.	MUST	
LAN.DHCPSv6.	7	The WAN / ULA prefixes that a device is allowed to further delegate SHOULD be configurable.	SHOULD	
LAN.DHCPSv6.	8	The device MUST support DHCPv6 Information_request messages.	MUST	
LAN.DHCPSv6.	9	The device MUST support the following DHCPv6 options:	MUST	Need to determine what this list of options is.
LAN.DHCPSv6.	10	The device SHOULD support the following DHCPv6 options:	SHOULD	list TBD
LAN.DHCPSv6.	11	The values of the following options SHOULD be configurable:	SHOULD	TBD
LAN.DHCPSv6.	12	The options that the device will provide via DHCPv6 MUST be configurable.	MUST	
DNS		**Naming Services (IPv4)**		
LAN.DNS.	1	The device MUST act as a DNS name server to LAN devices, passing its address back to these devices in DHCPv4 requests as the DNS name server.	MUST	
LAN.DNS.	2	The device SHOULD allow the user to specify that the network learned or user specified DNS addresses be passed back to the LAN devices in DHCPv4 responses instead of the device's address itself as the DNS name server(s).	SHOULD	

LAN.DNS.	3	When the device learns DNS name server addresses from multiple WAN connections, the device MUST query a server on each connection simultaneously and provide the requesting LAN client with the first returned positive result from these DNS servers. A negative response will not be transmitted to a LAN device until all WAN DNS servers have either timed out or returned a negative response to a common query. Service providers may choose not to provide DNS name server addresses on certain connections in a multiple connection configuration.	MUST	
LAN.DNS.	4	The device MUST add the DNS entry "dsldevice" for its own address.	MUST	
LAN.DNS.	5	The device MAY support additional DNS entries, as there could be additional types of CPE.	MAY	
LAN.DNS.	6	The device MUST maintain local DNS entries for a minimum of 253 local LAN devices. This information can be obtained through auto discovery (e.g., from DHCPv4 requests, such as Client Identifier, and other protocol information). When unknown, the entry MUST be of the form "unknownxxxxxxxxxxxx" where "x" represents the MAC address of the associated LAN device.	MUST	
LAN.DNS.	7	The device SHOULD provide a manual mechanism for overriding the learned names of all LAN CPE except that for the Broadband Residential Gateway itself.	SHOULD	
DNSv6		**Naming Services (IPv6)**		
LAN.DNSv6.	1	The device MUST support IPv6 (AAAA) records in its DNS server (per RFC 3596) and allow these records to be queried using either IPv4 or IPv6 transport (RFC 3901).	MUST	
LAN.DNSv6.	2	The device MUST attach all known (for the host device) globally scoped IPv6 addresses to the DNS record for a particular host device (see LAN.DNS.6), as AAAA records for that device.	MUST	
LAN.DNSv6.	3	The device SHOULD support dynamic DNS (DDNS) for devices to provide their own DNS information. This would override any DNS entries the RG may have created for the IP addresses included in the DDNS request.	SHOULD	Reference? Some have suggested MUST?
LAN.DNSv6.	4	The device MUST be able to query for A and AAAA records using either IPv4 or IPv6 transport to DNS servers in the WAN.	MUST	

LAN.DNSv6.	5	The device SHOULD use a DNS server obtained through DHCPv6 option (23 - OPTION_DNS_SERVERS) to query for AAAA records to the WAN, as its first choice. Similarly, it SHOULD use a DNS server obtained through DHCPv4 option (6 - Domain Server) to query for A records.	SHOULD	
LAN.DNSv6.	6	When the device is proxying DNS queries for LAN devices, it SHOULD use the same transport as the LAN device, when querying to the WAN.	SHOULD	
LAN.DNSv6.	7	The device MUST support receiving at least 2 DNS server IPv6 addresses from the network through DHCPv6 option OPTION_DNS_SERVERS (23) (RFC 3646) .	MUST	
LAN.DNSv6.	8	The device SHOULD allow the user to specify that the network learned or user specified DNS addresses be passed back to the LAN devices in DHCPv6 responses instead of the device's address itself as the DNS name server(s).	SHOULD	
PFWD		**Port Forwarding (IPv4 only)**		for v4 only; need new section for v6 describing the ability to have the RG block unsolicited inbound traffic to LAN device GUAs. Consider RFC 4864 section 4.2 and simple-security draft
LAN.PFWD.	1	The device MUST support port forwarding. That is, the device MUST be able to be configured to direct traffic based on any combination of source IPv4 address, source protocol (TCP and UDP) and port (or port range) to a particular LAN device and port (or port range on that device). Individual port forwarding rules MUST be associated with a LAN device, not the IPv4 address of the LAN device, and follow the LAN device should its IPv4 address change.	MUST	For IPv6, do we want to just keep it simple and close / open ports, for all app protocols? Do we want to simplify further and make it all or nothing (all inbound ports statically kept open to an IPv6 GUA, or none)?
LAN.PFWD.	2	The port forwarding mechanism MUST be able to be configured to direct all inbound unidentified or unsolicited port traffic originating from a user-selected public IPv4 address to any user selected LAN device. The LAN device may be using either a private IPv4 address or the public WAN IPv4 address as identified in requirement LAN.ADDRESS.6	MUST	

		and LAN.ADDRESS.7.		
LAN.PFWD.	3	The port forwarding mechanism of the device SHOULD be easy to configure for common applications and user protocols (e.g., ftp, http, etc.) by specifying a protocol name or application name in a "Common Applications Names List" instead of a port number and protocol type. A partial list of applications for potential inclusion are identified in Appendix A.	SHOULD	Can this apply to v6? ok as SHOULD. A bit of a disconnect with subsequent MUSTs.
LAN.PFWD.	4	The "Common Applications Names List" mechanism MUST be integrated with the port forwarding mechanism.	MUST	
LAN.PFWD.	5	The device MUST include port forwarding configurations and "Common Applications Name Listings" for the following applications and protocols that do not function properly with NAT or NAPT: FTP client, H.323, SIP, IPsec, PPTP, MSN Messenger, AOL Instant Messenger, Yahoo Messenger and ICQ.	MUST	This may still be true for v6, since we need to keep it easy to do these things when unsolicited inbound traffic is being blocked; do we want to make sure some of these ports are open by default, like for ftp and sip? Simple-security defines some of these.
LAN.PFWD.	6	The device SHOULD include port forwarding configurations and "Common Applications Name Listings" for other major applications and protocols that do not function properly with NAT or NAPT. Some potential candidates are identified in Appendix A.	SHOULD	
ALG		**ALG Functions (IPv4 only)**		v4 only; no v6 analog, although some have been proposed for certain scenarios.
LAN.ALG.	1	The device MUST allow for pass-through of IPv4 traffic in which the payload is compressed or encrypted (e.g., VPN traffic). This means other LAN CPE MUST be able to originate PPTP and L2TP sessions to an external network (over IPv4).	MUST	
LAN.ALG.	2	The device MUST allow LAN CPE to originate IPv4 IPsec sessions to an external network. This function MUST work properly through the NAPT function of the device.	MUST	
LAN.ALG.	3	The device MUST allow at least one IPv4 IPsec connection from the LAN.	MUST	

LAN.ALG.	4	The device MUST allow multiple users on the LAN to launch independent and simultaneous IPv4 IPsec sessions. These sessions can be to the same or unique destinations.	MUST	
LAN.ALG.	5	The device MUST support LAN device UDP Encapsulation of IPv4 IPsec packets as defined in IETF RFC 3948.	MUST	
LAN.ALG.	6	The device MUST support LAN device negotiation of NAT-Traversal with IKE as identified in IETF RFC 3947.	MUST	
LAN.ALG.	7	A minimum of 4 concurrent LAN IPv4 IPsec sessions SHOULD be supported per LAN device. These sessions can be to the same or unique destinations.	SHOULD	
LAN.ALG.	8	The device MUST seamlessly handle RTSP traffic to LAN devices with no user intervention required.	MUST	
FWD		**Connection Forwarding** Note that the IPv6 parts of this module apply only if the device has an IPv6 stack.		
LAN.FWD.	1	The device MUST be able to route IP (v4 or v6) over Ethernet to LAN CPE.	MUST	
LAN.FWD.	2	PPPoE forwarding and associated operation in the device MUST NOT fail nor operate improperly in the presence of vendor-specific PPPoE extensions which may be in use by LAN devices (i.e., the device MUST interoperate with well known PPPoE client software).	MUST	
LAN.FWD.	3	The device MUST support a minimum of eight LAN device initiated PPPoE sessions from each LAN device being forwarded to a logical WAN connection.	MUST	
LAN.FWD.	4	The device MUST be able to forward up to eight PPPoE sessions per logical WAN interface (i.e. PVC, IETF RFC 2684 connection, VLAN, etc.).	MUST	
LAN.FWD.	5	The device MUST be able to forward PPPoE sessions at all times when encapsulating Ethernet over AAL5. This applies when the device has set up zero or more PPPoE sessions and/or when the device is also running IP over Ethernet. The default setting MUST be for this pass-through to be on.	MUST	
LAN.FWD.	6	The device MUST support manually setting (via the Web GUI and TR-064/TR-069 interfaces) an MTU to be used in negotiating MTU, overriding the default MTU ~~via the Web GUI and TR-064/TR-069 interfaces.~~ This applies to MTU negotiated in IPv4 or IPv6.	MUST	
LAN.FWD.	7	The device MUST support Path MTU discovery as defined in IETF RFC 1191 so that a LAN device can be told what to set its MTU to for IPv4 traffic.	MUST	Applies to IPv4 only because MTU is included in RA for IPv6?

LAN.FWD.	8	The device MUST support accepting IP (v4 and v6) forwarding/routing information via the TR-069 interface.	MUST
LAN.FWD.	9	The device MUST maintain route table entries for all connections it maintains on the WAN (e.g., per PVC, IP (v4 and v6) and PPP sessions) and for all LAN networks (including subnets).	MUST
LAN.FWD.	10	The device MUST allow for the selection of which traffic to forward over which connection (in the case of multiple PVCs, multiple PPPoE sessions, GPON Port ID, etc…) according to any one or more of the following pieces of information: (1) destination IP (v4 or v6) address(es) with subnet mask, (2) originating IP (v4 or v6) address(es) with subnet mask, (3) source MAC address, (4) destination MAC address, (5) protocol (TCP, UDP, ICMP, …) (6) source port, (7) destination port, (8) IEEE 802.1D user priority, (9) FQDN (Fully Qualified Domain Name) of WAN session, (10) DiffServ codepoint (IETF RFC 3260), (11) Ethertype (IEEE 802.3, 1998 Length/Type Field), and (12) traffic handled by an ALG.	MUST
LAN.FWD.	11	The device MUST allow for the selection of which traffic to forward over which connection (in the case of multiple PVCs, multiple PPPoE sessions, etc…) according to any one or more of the following pieces of information: (1) IEEE 802.1Q VLAN identification, and (2) packet length.	MUST
LAN.FWD.	12	The device MUST NOT bridge or route between WAN connections (i.e., WAN to WAN) except when explicitly configured to do so.	MUST
LAN.FWD.	13	The device MUST NOT forward UPnP traffic (including UPnP multicast messages) to the WAN interface. This applies to both bridged and routed style configurations. This satisfies TR-101 R-201.	MUST
LAN.FWD.	14	The device SHOULD be able to restrict the routing information for each WAN connection to specific LAN devices. For example, a user might have four PCs in their home, have a WAN connection to the Internet and have a WAN connection to an employer's network. The device could be configured to allow all PCs access to the Internet, but only one specific PC might be allowed to send traffic over the WAN interface to the employer's network.	SHOULD
LAN.FWD.	15	The device MUST support all LAN devices concurrently accessing one or more WAN connections.	MUST

LAN.FWD.	16	If the network implements a TR-059 architecture, the device MUST support the ability to accept IPv4 routes dynamically pushed from the WAN. This allows it to set up routing tables to support routing traffic over multiple connections (PVCs, PPPoE sessions, etc…). In particular, the device MUST be configurable to accept RIP Version 2 (RIP-2) messages as defined in IETF RFC 2453 to fulfill this task.	MUST	for v4 only; v6 routing via RFC 4191 covered in IPv6 WAN Connection.
LAN.FWD.	17	If RIP-2 is supported, it SHOULD be software configurable.	SHOULD	
LAN.FWD.	18	If RIP-2 is supported, by default, the device MUST NOT transmit RIP-2 information to WAN connections.	MUST	
LAN.FWD.	19	If the network implements a TR-059 architecture, the device MUST be configurable to accept Triggered RIP messages, as defined in IETF RFC 2091.	MUST	
LAN.FWD.	20	If the network implements a TR-059 architecture, the device MUST be able to bridge IPv4 or route IPv4 or IPv6 over an Ethernet session concurrently with at least one device-originated PPPoE session on each PVC that is running bridged Ethernet over the AAL.	MUST	
LAN.FWD.	21	If the network implements a TR-059 architecture, the device MUST be capable of initiating at least two PPPoE sessions per PVC and forward the IP (v4 or v6) traffic above that to the LAN CPE.	MUST	
IGMP.BRIDGED		**IGMP and Multicast in Bridged Configurations (IPv4)**		
LAN.IGMP.BRIDGED.	1	If in a bridge type architecture and an IGMP Querier is supported in the access network, the device MUST support IGMP snooping per IP bridge to an individual LAN addressable port or interface level (each Ethernet port, USB (PC), Wi-Fi, etc.). On a per interface basis only the multicast streams specifically requested by clients on the LAN interface in question may be placed on the interface. A recommended reference implementation can be found in IETF RFC 4541.	MUST	
IGMP.ROUTED		**IGMP/MLD and Multicast in Routed Configurations (IPv4)**		
LAN.IGMP.ROUTED.	1	The device MUST support an IGMP Proxy-Routing function as defined in IETF RFC 4605. This satisfies TR-101 R-191.	MUST	
LAN.IGMP.ROUTED.	2	The device MUST support IGMPv3 as defined in IETF RFC 3376. This satisfies TR-101 R-192.	MUST	

LAN.IGMP.ROUTED.	3	The device MUST support IGMP proxy-routing with local NAT and firewall features including establishing any pin-holes in the firewall for the multicast streams received (after join). This satisfies TR-101 R-193.	MUST
LAN.IGMP.ROUTED.	4	When the device is configured with multiple WAN-facing IPv4 interfaces (e.g. PPP or IPoE), the IGMP Proxy-Routing function MUST be able to configure a filter for multicasting upstream IGMP messages to one or more interfaces. This satisfies TR101 requirements R-194 and R-195.	MUST
LAN.IGMP.ROUTED.	5	When the device receives an IGMP membership query on a given WAN-facing IPv4 interface, the IGMP Proxy-Routing function MUST only send a corresponding membership report on this specific interface. This satisfies TR-101 R-196.	MUST
LAN.IGMP.ROUTED.	6	The device SHOULD be able to classify IGMP requests according to source IPv4/MAC address or incoming LAN physical port on the device to distinguish between multicast services (e.g. IPTV and some other Best Effort Internet multicast application). This satisfies TR-101 R-197.	SHOULD
LAN.IGMP.ROUTED.	7	The device MUST have a way of suppressing the flooding of multicast to all LAN devices by only sending the traffic to selected ports/interfaces, either through configuration of dedicated ports connecting to multicast hosts or IGMP Proxy-Routing (where the traffic is only sent to host devices that have joined the multicast group). This satisfies TR-101 R-198.	MUST
LAN.IGMP.ROUTED.	8	It MUST be possible to configure a device WAN-facing IPv4 interface with an IPoE encapsulation and no IP address visible by the access network. It MUST be possible to receive multicast traffic on such an interface, independent of whether upstream IGMP is sent on this interface or not. The device's IGMP Proxy-Routing function MUST be able to send upstream IGMP traffic on such an interface, using an unspecified (0.0.0.0/::) IPv4 source address. This satisfies TR-101 requirements R-235, R-236 and R-237.	MUST
LAN.IGMP.ROUTED.	9	All device LAN ports and interfaces MUST be capable of processing IGMP messages.	MUST
LAN.IGMP.ROUTED.	10	The device SHOULD be able to allow (default) or discard IGMP join requests based on the source interface, port and host. This satisfies the requirement stated in TR-101 R-199.	SHOULD
LAN.IGMP.ROUTED.	11	The device MUST support IGMP snooping per IPv4 bridge to an individual LAN addressable port or interface level (each Ethernet port, USB (PC), Wi-Fi, etc.). A recommended reference implementation can be found in IETF RFC	MUST

		4541.	
LAN.IGMP.ROUTED.	12	The device MUST be configurable to prevent sending IGMP messages to the WAN interfaces for specified multicast groups or ranges (such as 239.0.0.0 through 239.255.255.255 for IPv4, which are limited scope or administratively scoped addresses).	MUST
LAN.IGMP.ROUTED.	13	The device MUST default to not sending IGMP messages for 239.0.0.0 through 239.255.255.255 to the WAN interfaces. This satisfies TR-101 R-201.	MUST
LAN.IGMP.ROUTED.	14	The device MUST have a join and leave latency less than 20 ms. This means that when the device receives a leave, it must stop sending the stream to that device (although it is expected to continue sending to other devices that have not left) in less than 20 ms. The device must not wait for the results of a membership query before it stops sending the stream. Rather, it must rely on its membership database to know whether there are other devices receiving that stream. When the device receives a join, its portion of the overall time for starting the sending of that stream must not be greater than 20 ms.This latency definition handles southbound join/leave; however a definition for the northbound join/leave latency will also be useful. Also, the northbound as well as southbound latency definition involves a tradeoff between multicast system dynamics (lower latency -> higher dynamics) and bandwidth efficiency (low latency -> better bandwidth efficiency). A statistical analysis will be helpful, based on empirical TV channel switching dynamics, when available.	MUST
LAN.IGMP.ROUTED.	15	The device MUST support IGMP immediate leave (also known as fast leave) with explicit host tracking. This satisfies TR-101 R-200.	MUST
LAN.IGMP.ROUTED.	16	The device MUST support a minimum of 32 multicast groups.	MUST
LAN.IGMP.ROUTED.	17	The device SHOULD support a minimum of 64 multicast groups.	SHOULD
LAN.IGMP.ROUTED.	18	The device MUST be configurable to log (on demand) all IGMP messages on both the LAN and WAN interfaces.	MUST
LAN.IGMP.ROUTED.	19	The device MUST be able to provide a summary of the current state of IGMP group memberships as managed by the device (e.g., multicast groups and LAN devices currently associated with each multicast group).	MUST
LAN.IGMP.ROUTED.	20	The device MUST be able to provide a summary of IGMP activity over specific time periods (e.g., previous hour, previous day, since reboot, etc.), per multicast stream and per host device.	MUST

LAN.IGMP.ROUTED.	21	The device MUST be able to report the IGMP statistics and logs through the Web GUI and TR-064/TR-069 interfaces.	MUST
LAN.IGMP.ROUTED.	22	The device MUST be capable of supporting LAN to LAN multicast between devices on a shared medium, and between devices on separate switched LAN interfaces.	MUST
LAN.IGMP.ROUTED.	23	The device MUST be configurable as to how many simultaneous multicast streams are allowed from WAN to LAN.	MUST
MLD.ROUTED		**MLD and Multicast in Routed Configurations (IPv6)**	
LAN.MLD.ROUTED.	1	The device MUST support MLDv2 as defined in IETF RFC 3810.	MUST
LAN.MLD.ROUTED.	2	The device MUST support functionality as described for IGMP in requirements LAN.IGMP.ROUTED. 1, 3-5, 7, 9, 11, 14-16, 18-23	MUST
LAN.MLD.ROUTED.	3	The device SHOULD support functionality as described for IGMP in requirements LAN.IGMP.ROUTED. 6, 10, 17	SHOULD
LAN.MLD.ROUTED.	4	The device MUST be configurable to prevent sending IGMP messages to the WAN interfaces for specified multicast addresses or scopes.	MUST
LAN.MLD.ROUTED.	5	The device MUST default to not sending IGMP messages for scope of 0 through 5..	MUST
FW		**Firewall (Basic)** Note that this module applies to IPv6 as well as IPv4, but only if the device has an IPv6 stack.	
LAN.FW.	1	The device MUST drop or deny access requests from WAN side connections to LAN side devices and the device itself except in direct response to outgoing traffic or as explicitly permitted through configuration of the device (e.g., for port forwarding or management).	MUST
LAN.FW.	2	The device MUST support a separate firewall log to maintain records of all transactions that violate firewall rules.	MUST
LAN.FW.	3	The firewall log file MUST be able to hold at least the last 100 entries or 10 Kbytes of text.	MUST
LAN.FW.	4	If a firewall log is implemented, the file entries SHOULD not be cleared, except when the device is reset to its factory default settings.	SHOULD
LAN.FW.	5	If a firewall log is implemented, the device MUST timestamp each firewall log entry.	MUST
LAN.FW.	6	The RG MUST support the definition of IPv6 firewall rules separate from IPv4	MUST
FW.SPI		**Firewall (Advanced)** Note that this module applies to IPv6 as well as IPv4, but only if the device has an IPv6 stack.	

LAN.FW.SPI.	1	The device MUST support a more robust firewall, such as one which provides a full OSI 7 layer stack stateful packet inspection and packet filtering function.	MUST
LAN.FW.SPI.	2	The device SHOULD provide protection for the following: - Port scans - Packets with same source and destination addresses - Broadband packets with a broadcast source address - Broadband packets with a LAN source address - Invalid fragmented IP (v4 or v6) packets - Fragmented TCP packets - Packets with invalid TCP flag settings (NULL, FIN, Xmas, etc…) - Fragmented packet headers (TCP, UDP and ICMP) - Inconsistent packet header lengths - Packet flooding - Excessive number of sessions - Invalid ICMP requests - Irregular sequence differences between TCP packets The extent of this protection will be limited when the device is configured as a bridge in which only PPPoE traffic is bridged. This protection MUST be available when the device terminates IP (v4 or v6) or bridges IPv4.	SHOULD
LAN.FW.SPI.	3	Each type of attack for which protection is provided SHOULD be configurable on the device and on by default.	SHOULD
LAN.FW.SPI.	4	The device MUST support passing and blocking of traffic by use of user and configurable defined rules.	MUST
LAN.FW.SPI.	5	The device MUST support setting firewall rules by the TR-069 ACS which can not be altered by the user. If firewall rules are set via security policies in TR-098 profiles, or via other mechanism such as TR-069 file download, the rules MUST NOT be able to be overridden by user firewall rules.	MUST
LAN.FW.SPI.	6	The device MUST support the user temporarily disabling specific user defined rules or all user defined rules.	MUST
LAN.FW.SPI.	7	The device MUST support the user specifying the order in which firewall rules are processed.	MUST

LAN.FW.SPI.	8	The device SHOULD support specification of any of the following in a firewall rule: - destination IP (v4 or v6) address(es) with subnet mask - originating IP (v4 or v6) address(es) with subnet mask - source MAC address - destination MAC address - protocol (0-255, or by alias: TCP, UDP, ICMP, IP, IGMP, eigrp, gre, ipinip, pim, nos, ospf, …) - source port - destination port - IEEE 802.1D user priority - FQDN (Fully Qualified Domain Name) of WAN session - DiffServ codepoint (IETF RFC 3260) - Ethertype (IEEE 802.3, 1998 Length/Type Field) - Traffic fitting an ALG filter - IEEE 802.1Q VLAN identification - packet length - TCP flags (urg, ack, psh, rst, syn, fin) - IP option values (potentially name aliases) - logical interface of source - logical interface of destination	SHOULD
LAN.FW.SPI.	9	The device MAY support filtering based on other fields unique to specific protocols.	MAY
LAN.FW.SPI.	10	The device SHOULD support firewall rules which support generic pattern matching against the header or data payload of traffic. Logically this can be envisioned as: match(header[offset[,length|max]],condition) match(payload[offset[,length|max]], condition) where condition is (relationship, data) such as (=, ne, all, one, and, or) for a hex field (=, ne, gt, ge, lt, le) for a decimal/hex field (=, ne, contains) for a string field	SHOULD
LAN.FW.SPI.	11	The device SHOULD support a set of pre-defined rules to which the user can set or reset their firewall settings to.	SHOULD
LAN.FW.SPI.	12	If a set of pre-defined rules has been set on the device, the device rule set SHOULD be able to be used as the basis for a user maintained set of firewall rules.	SHOULD
LAN.FW.SPI.	13	In addition to blocking or passing traffic identified by a firewall filter, the device MUST support other actions as well, including but not limited to: - logging on success or failure, - notification on success or failure (to email or pager if supported), - sending notification to a PC monitor application (either originator and or centralized source), and - requesting verification from a PC monitor	MUST

		application.	
LAN.FW.SPI.	14	The device MUST allow for configuration of global firewall values.	MUST
LAN.FW.SPI.	15	The device firewall SHOULD be either ICSA certified or be able to display all the attributes necessary for ICSA certification for the current version of either the Residential Category or the Small/Medium Business (SMB) Category.	SHOULD
LAN.FW.SPI.	16	Unless configured otherwise, DOS, port blocking and stateful packet inspection MUST be provided to all LAN devices receiving traffic from the WAN interface.	MUST
CAPTIVE		**Captive Portal with Web Redirection** Note that this module applies to IPv6 as well as IPv4, but only if the device has an IPv6 stack.	
LAN.CAPTIVE.	1	The device and the ACS MUST support a redirect function, which, when enabled, intercepts WAN destination IP (v4 or v6) HTTP requests and responds to these by substituting a specified URL in place of the web page request. The URL, as well as a list of locations for which this redirect would be bypassed (i.e., white list), MUST be set through the TR-069 interface. The actual captive portal to be redirected to may be established at the time the white list is defined or the white list defined first and the captive portal specified at a later time.	MUST
LAN.CAPTIVE.	2	The redirection function and associated fields MUST NOT be modifiable by the subscriber.	MUST
LAN.CAPTIVE.	3	The device MUST support turning on and off the redirect function when the captive portal URL field is populated and cleared respectively by the TR-069 ACS.	MUST
LAN.CAPTIVE.	4	All port 80 traffic, excluding that associated with the white list, MUST be redirected when the redirect function is turned on in the device.	MUST
LAN.CAPTIVE.	5	The captive portal that traffic is redirected to MUST be defined as an IP (v4 or v6) address or a URL with a maximum length of 2,000 characters.	MUST
LAN.CAPTIVE.	6	The redirect white list MUST support 512 separate list entries which can be individual IP (v4 or v6) addresses, a range of IPv4 addresses, an IPv6 prefix, or any combination thereof. For a range of IPv4 addresses a subnet mask is required.	MUST

LAN.CAPTIVE.	7	Variable length subnet masking (VLSM) MUST be supported in the redirect white list. For example:- Individual IPv4 Address: ipaddress or ipaddress/32 or ipaddress 255.255.255.255 - Range of 64 IPv4 addresses ipaddress/26 or ipaddress 255.255.192.0	MUST	
LAN.CAPTIVE.	8	The device MUST support only one set or captive portal and redirect settings as a time. If new settings are needed, the ACS will submit these to overwrite the existing values within the device.	MUST	
LAN.CAPTIVE.	9	A valid set of redirect settings MUST be enabled in a device within five seconds of the redirect URL being sent from the ACS.	MUST	
LAN.CAPTIVE.	10	The redirect function MUST be disabled on the device within five seconds of the captive portal string being cleared in a device by an empty redirect URL being sent from the ACS.	MUST	
LAN.CAPTIVE.	11	Incremental packet delay through the device due to white list lookup MUST NOT exceed 5 ms.	MUST	
MGMT		**Management & Diagnostics**		
UPnP		**UPnP**		
MGMT.UPnP.	1	The device MUST support UPnP Device Architecture 1.0. This specification is made available for download at http://www.upnp.org.	MUST	Once new v6 UDA is done, we should reference it.
MGMT.UPnP.	2	The device MUST support UPnP device identification of the UPnP Device Architecture. The device MUST display itself as a network device with the following information: - Manufacturer Name - Modem Name - Model Number - Description (e.g. VendorName Wireless Gateway) - Device Address (e.g. http://192.168.1.254)	MUST	
REMOTE.WEB		**Remote Management (Web Browser)** Note that this module applies to IPv6 as well as IPv4, but only if the device has an IPv6 stack.		
MGMT.REMOTE.WEB.	1	The device MUST be able to allow temporary manual remote access to its Web GUI remotely from the WAN interface.	MUST	
MGMT.REMOTE.WEB.	2	When temporary WAN side remote access is enabled to the device, the remote access session MUST be started within 20 minutes and the activated session MUST time out after 20 minutes of inactivity.	MUST	
MGMT.REMOTE.WEB.	3	The user MUST be able to specify that the temporary WAN side remote access is a read only connection or one which allows for updates. The default MUST be read only.	MUST	

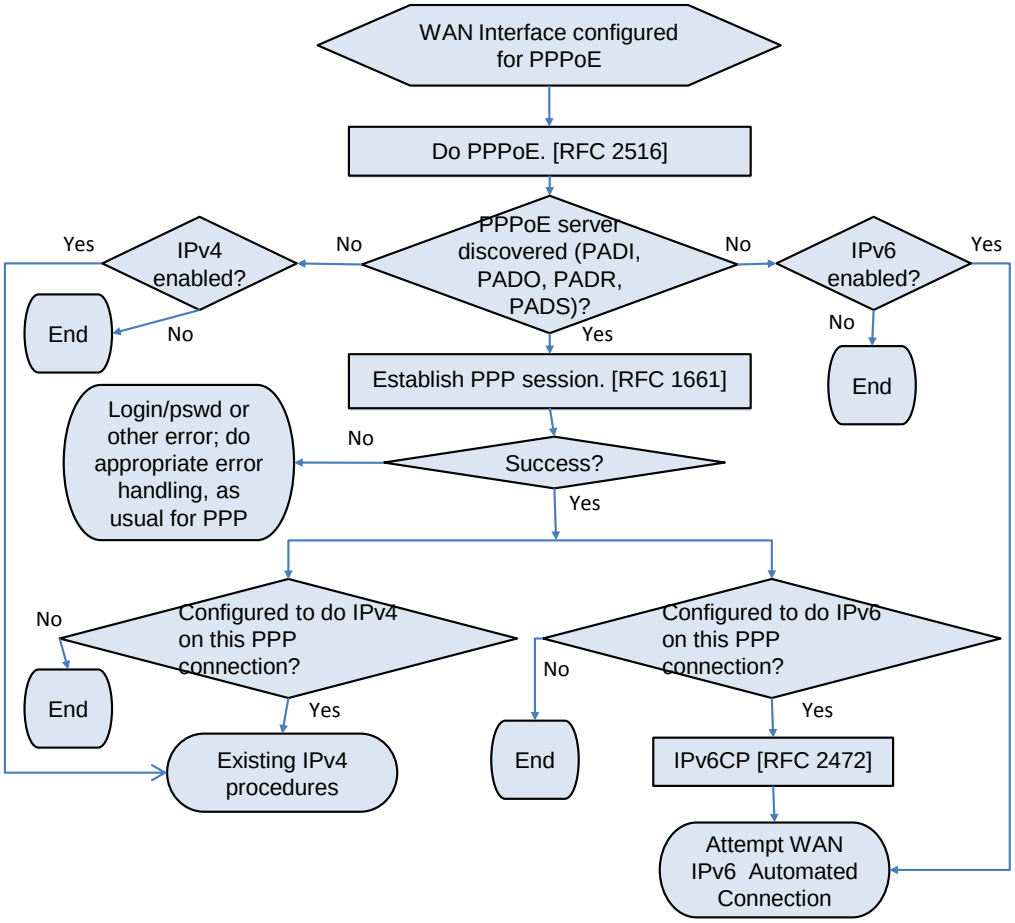
MGMT.REMOTE.WEB.	4	Temporary WAN side remote access MUST NOT allow for changing the device password.	MUST
MGMT.REMOTE.WEB.	5	Temporary WAN side remote access MUST be disabled by default.	MUST
MGMT.REMOTE.WEB.	6	Temporary WAN side remote access SHOULD be through HTTP over TLS (i.e., https using TLS).	SHOULD
MGMT.REMOTE.WEB.	7	The device SHOULD use a randomly selected port for temporary WAN side remote access to prevent hacking of a well known port.	SHOULD
MGMT.REMOTE.WEB.	8	If a default port is used for temporary WAN side remote access, it MUST be 51003.	MUST
MGMT.REMOTE.WEB.	9	The user MUST specify a non-blank password to be used for each temporary WAN side remote access session. This information MUST not be saved across sessions.	MUST
MGMT.REMOTE.WEB.	10	The User ID for all temporary WAN side remote access sessions, if required based on the method of implementation, MUST be "tech" by default.	MUST
MGMT.REMOTE.WEB.	11	The user MUST be able to change the User ID for all temporary WAN side remote access sessions.	MUST
MGMT.REMOTE.WEB.	12	The device MUST allow only one temporary WAN side remote access session to be active at a time.	MUST
MGMT.REMOTE.WEB.	13	All other direct access to the device from the WAN side MUST be disabled and blocked by default.	MUST
NTP		**Network Time Client** Note that this module applies to IPv6 as well as IPv4, but only if the device has an IPv6 stack.	
MGMT.NTP.	1	The device MUST support an internal clock with a date and time mechanism.	MUST
MGMT.NTP.	2	The device clock MUST be able to be set via an internal time client from an Internet source using IETF RFC 1305.	MUST
MGMT.NTP.	3	The device MUST support the use of time server identification by both domain name and IP (v4 or v6) address.	MUST
MGMT.NTP.	4	If the device includes default time server values, they SHOULD be specified by domain name and not by IP (v4 or v6) address.	SHOULD
MGMT.NTP.	5	The device SHOULD allow configuration of the primary and alternate time server values in addition to or in place of any default values.	SHOULD
MGMT.NTP.	6	If the device includes default time server values or time server values are identified in documentation, these values SHOULD be selected using industry best practices for NTP and SNTP clients, as published in section 10 of IETF RFC 4330.	SHOULD
MGMT.NTP.	7	The time client SHOULD support DNS responses with CNAMEs or multiple A records.	SHOULD

MGMT.NTP.	8	The default frequency with which the device updates its time from a time server MUST NOT be less than 60 minutes, or use an operator-specific configuration.	MUST
MGMT.NTP.	9	The default frequency with which the device updates its time from a time server MUST NOT be greater than 24 hours, or use an operator-specific configuration.	MUST
MGMT.NTP.	10	The frequency with which the device updates its time from a time server SHOULD be able to be configured.	SHOULD

Annex A: Flow Diagrams

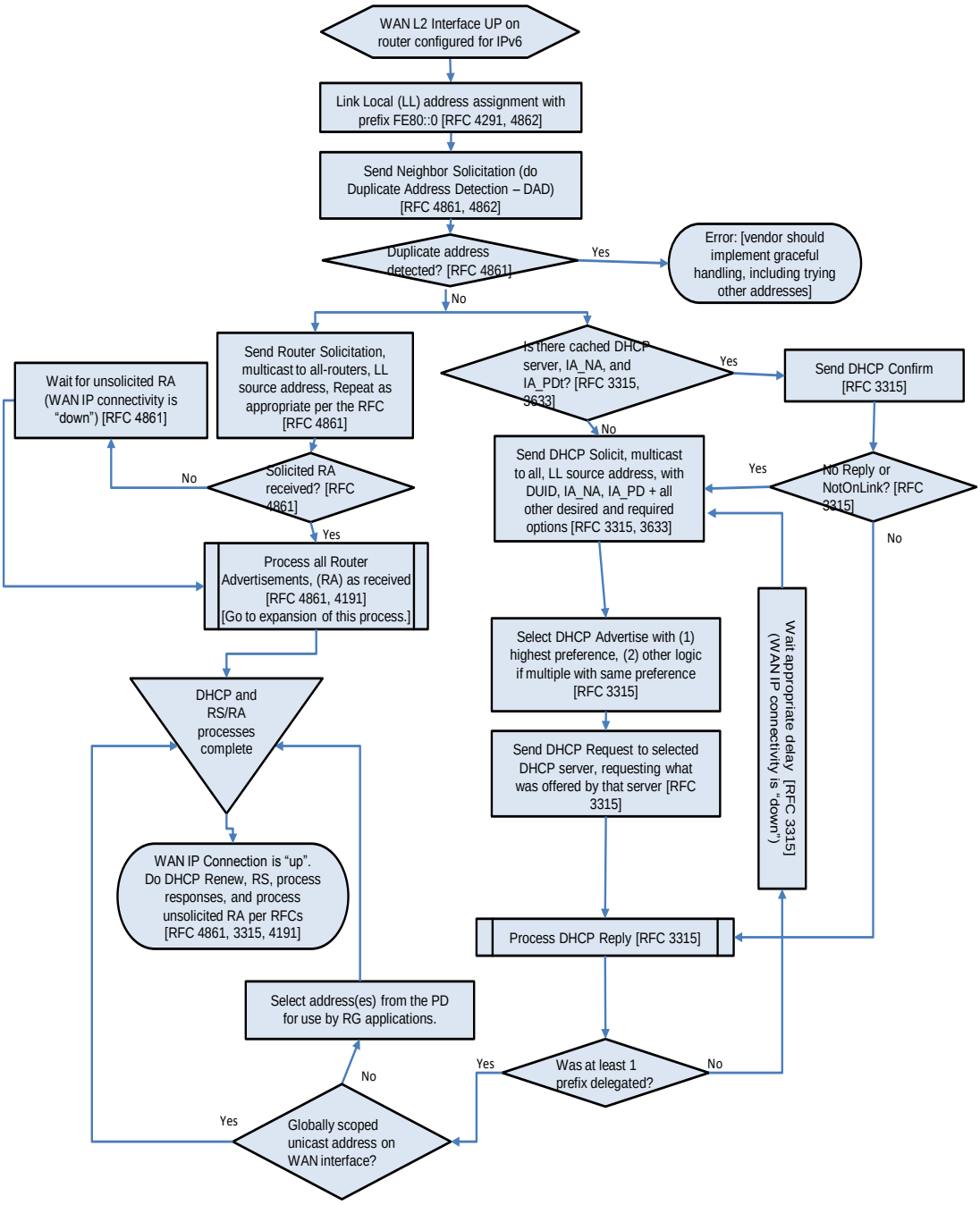
The flows in this annex are referenced by requirements in the body, and are therefore normative.

A.1 WAN PPPoE Automated Connection Flow

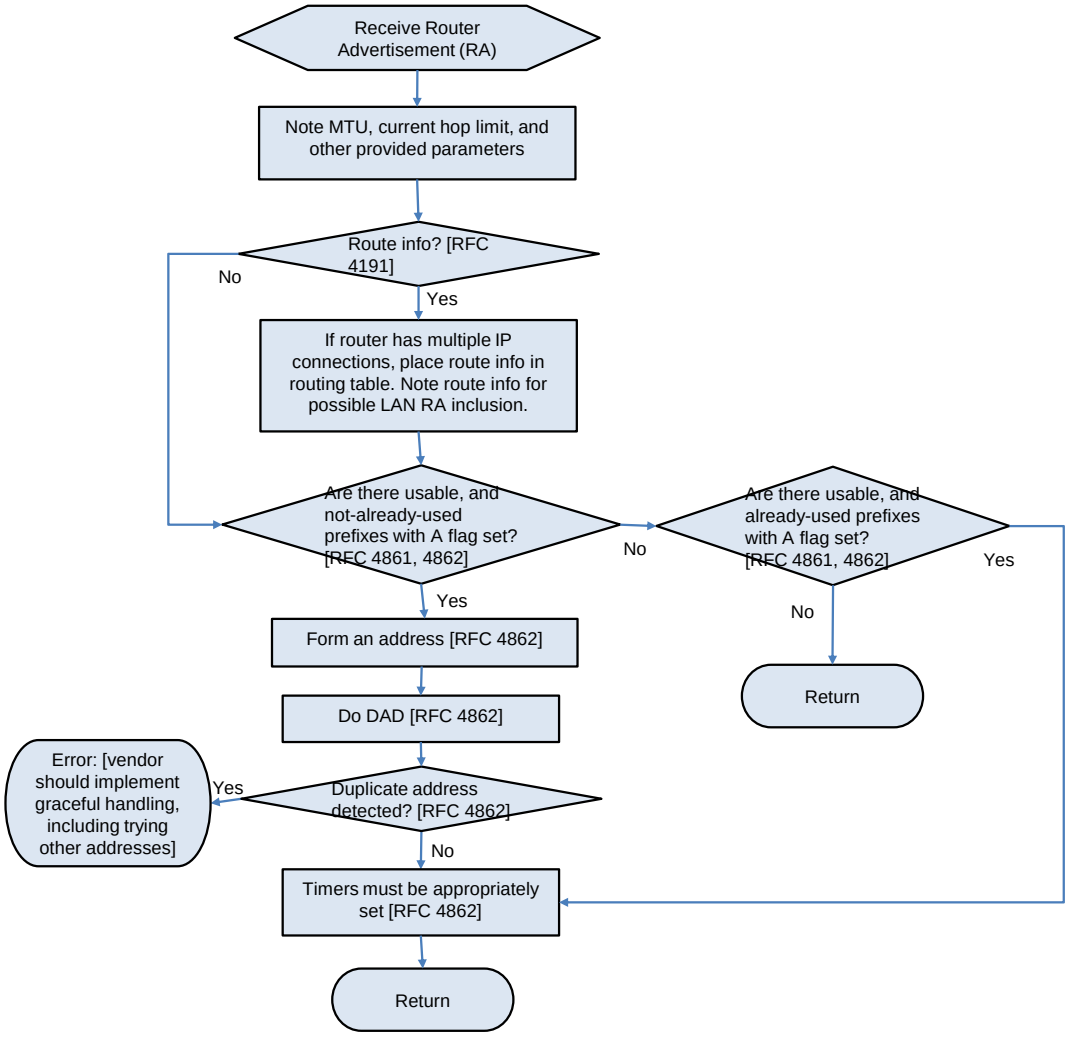


A.2 WAN IPv6 Automated Connection Flow

This flow assumes no manually configured prefix or address.



A.3 Receive Router Advertisement Subroutine Flow



End of Broadband Forum Proposed Draft PD-192