TECHNICAL REPORT

TR-124

Functional Requirements for Broadband Residential Gateway Devices

Issue: 2
Issue Date: May 2010

Notice

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

This Broadband Forum Technical Report is provided AS IS, WITH ALL FAULTS. ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, 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 TECHNICAL REPORT ARE SUITABLE FOR ANY PURPOSE, EVEN IF THAT PURPOSE IS KNOWN TO THE COPYRIGHT HOLDER;
(C) THAT THE IMPLEMENTATION OF THE CONTENTS OF THE TECHNICAL REPORT WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

By using this Broadband Forum Technical Report, users acknowledge that implementation may require licenses to patents. The Broadband Forum encourages but does not require its members to identify such patents. For a list of declarations made by Broadband Forum member companies, please see http://www.broadband-forum.org. No assurance is given that licenses to patents necessary to implement this Technical Report will be available for license at all or on reasonable and non-discriminatory terms.

ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, 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 TECHNICAL REPORT; AND (B) ANY OBLIGATION TO UPDATE OR CORRECT THIS TECHNICAL REPORT.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

Issue History

Issue Number	Issue Date	Issue Editor	Changes
1	December 2006	Jaime Fink, 2Wire Jack Manbeck, Texas Instruments	Original
2	May 2010	Barbara Stark, AT&T Ole Trøan, Cisco	Added IPv6 functionality.

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editors	Barbara Stark	AT&T
	Ole Trøan	Cisco
BroadbandHome™ WG Chairs	Greg Bathrick Heather Kirksey	PMC-Sierra Alcatel-Lucent
Vice Chair	Jason Walls	UNH Interoperability Lab
Chief Editor	Michael Hanrahan	Huawei Technologies

TABLE OF CONTENTS

List of Figures

Executive Summary

This Technical Report specifies a superset of requirements for broadband Residential Gateway (RG) devices that are capable of supporting a full suite of voice, data, broadcast video, video on demand and two-way video applications in broadband networks.

The requirements are grouped into modules. This means that a RG can be specified by listing the modules that the device is expected to support. No single device is expected to support all modules.

TR-124 Issue 2 has updated TR-124 Issue 1 to include requirements for IPv6.

1 Purpose and Scope

1.1 Purpose

This Technical Report presents a superset of requirements for broadband Residential Gateway devices that are capable of supporting a full suite of voice, data, broadcast video, video on demand and two-way video applications in broadband networks.

1.2 Scope

A Residential Gateway implementing the general requirements of TR-124 will incorporate at least one embedded WAN interface, routing, bridging, a basic or enhanced firewall, one or multiple LAN interfaces and home networking functionality that can be deployed as a consumer self-installable device.

This document specifies a baseline of Residential Gateway device and application functions needed to support service delivery in routed and bridged broadband network architectures. Devices can be specified that will operate on any of the different types of Broadband Forum defined network architectures. This allows service providers to configure a Residential Gateway device supporting specified TR-124 modular requirements locally via TR-064 and Web Graphical User Interface or remotely via TR-069.

TR-124 provides optional requirements modules for various physical broadband interfaces (e.g., xDSL, Ethernet, GPON) and home networking (LAN) interfaces which may be implemented on Residential Gateways to meet local service provider needs. Furthermore, to accommodate common region-specific service provider requirements that do not apply globally, additional Regional Annexes are included in the TR-124 requirements that may be included in region-specific product profiles (e.g., North American Power and Environmental requirements).

It is intended that these general requirements modules and WAN/LAN interface modules can be used as references to define a specific product implementation that may be needed in future Broadband Forum Technical Recommendations. This checklist style product profile approach (shown in the Product Profile Template section in APPENDIX VI is intended to provide an easy mechanism to define a specific product that is needed by region or by service providers. An example of such a product profile is TR-150 Base Requirements for an ADSL Modem with Routing which refers to TR-124 feature modules and regional annexes.

These requirements are both backward and forward-looking. They attempt to address the needs of current DSL services and architectures as well as starting to address future needs. Some requirements have been included in support of TR-059, TR-064, TR-069, TR-101 and TR-122. Any CPE that claims to be compliant with these technical requirements must meet the requirements that reference those documents. It is understood that CPE that does not claim to be compliant with these referenced requirements may or may not meet any or all of

these requirements. On a periodic basis new general requirements and physical interface modules may be added in future revisions of TR-124.

TR-124 Issue 2 adds IPv6 functionality to the document.

2 References and Terminology

2.1 Conventions

In this Technical Report, 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 [51]**.**

MUST	This word, or the term "REQUIRED", means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means 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 need to 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 need to 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.
By Default	These words indicate that this is a default setting or operation of the unit which MUST be configurable if provided. This term is not included in RFC 2119 [51]**.**

Other Residential Gateway type features not identified in this document may also be implemented in the device. An implementation that includes features not identified in this document MUST be prepared to inter-operate with implementations that do not include these features.

References to CPE or LAN devices indicate other equipment such as hosts including PC and workstations.

In certain cases TR-124 generically refers to new LAN or WAN interface performance monitoring data parameters which have not been specifically defined in the requirements at the time of the publishing of this document. As these requirements are not yet defined, it is expected that vendors may support parameter extensions and basic interface traffic performance statistics until such a time that the Broadband Forum defines further Technical

Recommendations to support new interface parameter data models for possible use with TR-064, TR-069 and the web GUI.

2.2 References

The following references constitute provisions of this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report 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.

NOTE – A number of IETF drafts are referenced in this document. Due to the fact that home networking standards and technology are still being rapidly developed, this was considered necessary. If subsequent drafts or RFCs are published, they will obsolete the draft referenced in this document.

[1] ANSI/TIA-968-A-2002	*Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment to the Telephone Network.*	ANSI / TIA	October 1, 2002
[2] TR-059	*DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services.*	Broadband Forum	September 2003
[3] TR-062	*Auto-Config for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM (TR-037 update).*	Broadband Forum	November 2003
[4] TR-064	*LAN-Side CPE Configuration Specification.*	Broadband Forum	May 2004
[5] TR-067	*ADSL Interop Test Plan (Formerly TR-048).*	Broadband Forum	May 2004
[6] TR-068v2	*Base requirement for an ADSL Modem with Routing.*	Broadband Forum	September 2005
[7] TR-069	*CPE WAN Management*	Broadband	May 2004

	Protocol.	Forum	
[8] TR-098	*Internet Gateway Device Version 1.1 Data Model for TR-069*.	Broadband Forum	September 2005
[9] TR-101	*Migration to Ethernet Based DSL Aggregation.*	Broadband Forum	April 2006
[10] TR-111	*Applying TR-069 to Remote Management of Home Networking Devices*.	Broadband Forum	December 2005
[11] TR-114	*VDSL2 Performance Test Plan*	Broadband Forum	November 2009
[12] TR-115	*VDSL2 Functionality Test Plan*	Broadband Forum	November 2009
[13] TR-122	*Base Requirements for Consumer-Oriented Analog Terminal Adapter Functionality*	Broadband Forum	May 2006
[14] TR-133	*DSLHome TR-064 Extensions for Service Differentiation.*	Broadband Forum	September 2005
[15]	FCC Rules and Regulations Part 15	FCC	
[16]	FCC Rules and Regulations Part 68	FCC	
[17] EN61000-4-4:2004	*Electromagnetic compatibility (EMC). Testing and measurement techniques.*	IEC	February 2005
[18] EN61000-4-5:1995	*Electromagnetic compatibility (EMC). Testing and measurement techniques. Surge immunity test.*	IEC	September 1995
[19] IEEE Std 802.1DTM-2004	*IEEE standard for local and metropolitan area networks--Media access control (MAC) Bridges*.	IEEE	June 2004
[20] IEEE Std 802.1QTM	*IEEE Standards for Local and metropolitan area networks—Virtual Bridged Local Area Networks*.	IEEE	May 7 2003

[21] IEEE Std 802.3u	*Local and Metropolitan Area Networks-Supplement - Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units and Repeater for 100Mb/s Operation, Type 100BASE-T (Clauses 21-30).*	IEEE	June 2005
[22] IEEE Std 802.11a	*Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band.*	IEEE	September 1999
[23] IEEE Std 802.11b	*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band.*	IEEE	September 1999
[24] IEEE Std 802.11e	*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment: Medium Access Method (MAC) Quality of Service Enhancements.*	IEEE	September 2005
[25] IEEE Std 802.11g	*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band.*	IEEE	June 2003
[26] IEEE Std 802.11h	*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe.*	IEEE	September 2003
[27] IEEE Std 802.11i	*Wireless LAN Medium Access Control (MAC) and*	IEEE	June 2004

	Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements		
[28] RFC 768	*User Datagram Protocol*	IETF	August 1980
[29] RFC 791	*Internet Protocol*	IETF	September 1981
[30] RFC 792	*Internet Control Message Protocol*	IETF	September 1981
[31] RFC 793	*Transmission Control Protocol*	IETF	September 1981
[32] RFC 826	*An Ethernet Address Resolution Protocol*	IETF	November 1982
[33] RFC 894	*A Standard for the Transmission of IP Datagrams over Ethernet Networks*	IETF	April 1984
[34] RFC 959	*File Transfer Protocol (FTP)*	IETF	October 1985
[35] RFC 1034	*Domain Names - Concepts and Facilities*	IETF	November 1987
[36] RFC 1035	*Domain Names - Implementation and Specification*	IETF	November 1987
[37] RFC 1042	*A Standard for the Transmission of IP Datagrams over IEEE 802 Networks*	IETF	February 1988
[38] RFC 1191	*Path MTU Discovery*	IETF	November 1990
[39] RFC 1305	*Network Time Protocol (Version 3) Specification, Implementation and Analysis*	IETF	March 1992
[40] RFC 1332	*The PPP Internet Protocol Control Protocol (IPCP)*	IETF	May 1992
[41] RFC 1334	*PPP Authentication Protocols (PAP)*	IETF	October 1992

[42] RFC 1570	*PPP LCP Extensions*	IETF	January 1994
[43] RFC 1661	*The Point-to-Point Protocol (PPP)*	IETF	July 1994
[44] RFC 1867	*Form-based File Upload in HTML*	IETF	November 1995
[45] RFC 1877	*PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*	IETF	December 1995
[46] RFC 1928	*SOCKS Protocol Version 5*	IETF	March 1996
[47] RFC 1990	*The PPP Multilink Protocol (MP)*	IETF	August 1996
[48] RFC 1994	*PPP Challenge Handshake Authentication Protocol (CHAP)*	IETF	August 1996
[49] RFC 1948	*Defending Against Sequence Number Attacks*	IETF	May 1996
[50] RFC 2091	*Triggered Extensions to RIP to Support Demand Circuits*	IETF	January 1997
[51] RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	March 1997
[52] RFC 2131	*Dynamic Host Configuration Protocol*	IETF	March 1997
[53] RFC 2132	*DHCP Options and BOOTP Vendor Extensions*	IETF	March 1997
[54] RFC 2153	*PPP Vendor Extensions*	IETF	May 1997
[55] RFC 2181	*Clarifications to the DNS Specification*	IETF	July 1997
[56] RFC 2246	*The TLS Protocol Version 1.0*	IETF	January 1999
[57] RFC 2364	*PPP over AAL5*	IETF	July 1998
[58] RFC 2388	*Returning Values from Forms: multipart/form-data*	IETF	August 1998
[59] RFC 2453	*RIP Version 2*	IETF	November 1998
[60] RFC 2460	*Internet Protocol, Version 6*	IETF	December

	(IPv6) Specification		1998
[61] RFC 2464	*Transmission of IPv6 Packets over Ethernet Networks*	IETF	December 1998
[62] RFC 2473	*Generic Packet Tunneling in IPv6 Specification*	IETF	December 1998
[63] RFC 2474	*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*	IETF	December 1998
[64] RFC 2475	*An Architecture for Differentiated Services*	IETF	December 1998
[65] RFC 2492	*IPv6 over ATM Networks*	IETF	January 1999
[66] RFC 2516	*A Method for Transmitting PPP Over Ethernet (PPPoE)*	IETF	February 1999
[67] RFC 2597	*Assured Forwarding PHB Group*	IETF	June 1999
[68] RFC 2616	*Hypertext Transfer Protocol -- HTTP/1.1*	IETF	June 1999
[69] RFC 2663	*IP Network Address Translator (NAT) Terminology and Considerations*	IETF	August 1999
[70] RFC 2684	*Multiprotocol Encapsulation over ATM Adaptation Layer 5*	IETF	September 1999
[71] RFC 2818	*HTTP Over TLS*	IETF	May 2000
[72] RFC 2939	*Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types*	IETF	September 2000
[73] RFC 3022	*Traditional IP Network Address Translator (Traditional NAT)*	IETF	January 2001
[74] RFC 3027	*Protocol Complications with the IP Network Address Translator*	IETF	January 2001
[75] RFC 3246	*An Expedited Forwarding*	IETF	March

	PHB (Per-Hop Behavior)		2002
[76] RFC 3260	*New Terminology and Clarifications for Diffserv*	IETF	April 2002
[77] RFC 3261	*SIP: Session Initiation Protocol*	IETF	June 2002
[78] RFC 3280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*	IETF	April 2002
[79] RFC 3315	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*	IETF	July 2003
[80] RFC 3376	*Internet Group Management Protocol, Version 3*	IETF	October 2002
[81] RFC 3484	*Default Address Selection for Internet Protocol version 6 (IPv6)*	IETF	February 2003
[82] RFC 3544	*IP Header Compression over PPP*	IETF	July 2003
[83] RFC 3596	*DNS Extensions to Support IP Version 6*	IETF	October 2003
[84] RFC 3633	*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*	IETF	December 2003
[85] RFC 3646	*DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*	IETF	December 2003
[86] RFC 3810	*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*	IETF	June 2004
[87] RFC 3901	*DNS IPv6 Transport Operational Guidelines*	IETF	September 2004
[88] RFC 3947	*Negotiation of NAT Traversal in the IKE*	IETF	January 2005
[89] RFC 3948	*UDP Encapsulation of IPsec ESP packets*	IETF	January 2005
[90] RFC 4075	*Simple Network Time Protocol (SNTP)*	IETF	May 2005

		Configuration Option for DHCPv6		
[91]	RFC 4191	*Default Router Preferences and More-Specific Routes*	IETF	November 2005
[92]	RFC 4193	*Unique Local IPv6 Unicast Addresses*	IETF	October 2005
[93]	RFC 4213	*Basic Transition Mechanisms for IPv6 Hosts and Routers*	IETF	October 2005
[94]	RFC 4294	*IPv6 Node Requirements*	IETF	April 2006
[95]	RFC 4330	*Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*	IETF	January 2006
[96]	RFC 4361	*Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)*	IETF	February 2006
[97]	RFC 4443	*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*	IETF	March 2006
[98]	RFC 4541	*Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*	IETF	May 2006
[99]	RFC 4605	*Internet Group Management Protocol (IGMP) /Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")*	IETF	August 2006
[100]	RFC 4638	*Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)*	IETF	August 2006
[101]	RFC 4861	*Neighbor Discovery for IPv6*	IETF	September 2007

[102]	RFC 4862	*IPv6 Stateless Address Autoconfiguration*	IETF	September 2007
[103]	RFC 5072	*IP version 6 over PPP*	IETF	September 2007
[104]	RFC 5172	*Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol*	IETF	March 2008
[105]	RFC 5625	*DNS Proxy Implementation Guidelines*	IETF	August 2009
[106]	draft-ietf-tcpm-tcpsecure-12	*Improving TCP's Robustness to Blind In-Window Attacks*	IETF	September 2009
[107]	draft-ietf-softwire-ipv6-6rd-08	*IPv6 via IPv4 Service Provider Networks*	IETF	March 2010
[108]	draft-ietf-softwire-dual-stack-lite-04	*Dual-stack lite broadband deployments post IPv4 exhaustion*	IETF	March 2010
[109]	draft-ietf-softwire-ds-lite-tunnel-option-02	*Dynamic Host Configuration Protocol Option for Dual-Stack Lite*	IETF	March 2010
[110]	draft-ietf-v6ops-cpe-simple-security-10	*Recommended Simple Security Capabilities in Customer Premises Equipment for Providing Residential IPv6 Internet Service*	IETF	March 2010
[111]	ICES-003	*Digital Apparatus*	Industry Canada	February 7, 2004
[112]	ISO 8601:2004	*Data elements and interchange formats — Information interchange — Representation of dates and times*	ISO/IEC	December 2, 2004
[113]	ITU G.984.1	*Gigabit-capable Passive Optical Networks (GPON)*	ITU-T	March 2003
[114]	ITU G.984.2	*Gigabit-capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) layer specification*	ITU-T	March 2003

[115]	ITU G.984.2 Amd1	*Gigabit-capable Passive Optical Networks (G-PON): Physical Media Dependent (PMD) layer specification Amendment 1: New Appendix III - Industry best practice for 2.488 Gbit/s downstream, 1.244 Gbit/s upstream G-PON*	ITU-T	February 2006
[116]	ITU G.984.3	*Gigabit-capable Passive Optical Networks (GPON): Transmission convergence layer specification*	ITU-T	February 2004
[117]	ITU G.984.4	*Gigabit-capable Passive Optical Networks (GPON): ONT Management and Control Interface specification (OMCI)*	ITU-T	June 2004
[118]	ITU G.992.3	*Asymmetric digital subscriber line transceivers 2 (ADSL2)*	ITU-T	January 2005
[119]	ITU G.993.2	*Very high speed digital subscriber line transceivers 2 (VDSL2)*	ITU-T	February 2006
[120]	ITU G.997.1	*Physical layer management for digital subscriber line (DSL) transceivers*	ITU-T	June 2006
[121]	ITU G.998.1	*ATM-based multi-pair bonding*	ITU-T	January 2005
[122]	ITU G.998.2	*Ethernet-based multi-pair bonding*	ITU-T	January 2005
[123]	ITU G.9954	*Phoneline networking transceivers - Enhanced physical, media access, and link layer specifications*	ITU-T	February 2005
[124]	T1.421-2001	*In-Line Filter for Use with Voiceband Terminal Equipment Operating on the Same Wire Pair with High Frequency (up to 12 MHz) Devices*	ANSI	2001
[125]	T1.427.01-	*ATM-based Multi-pair*	ANSI	2004

	2004	*Bonding*		
[126]	T1.427.02-2005	*Ethernet-based Multi-Pair Bonding*	ANSI	2005
[127]	UL 60950 Edition 3	*Safety of Information Technology Equipment*		May 15, 2002

The following information is given for the convenience of users of this Technical Report and does not constitute an endorsement by the Broadband Forum of these products.

- FireWire® and Safari® are registered trademarks of Apple Computer, Inc.
- GSM® is a registered trademark of France Telecom
- HomePlug® is a registered trademark of HomePlug Powerline Alliance, Inc.
- HomePNA® is a registered trademark of HomePNA, Inc.
- IEEE® is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. (IEEE). This publication is not endorsed by the IEEE.
- Internet Explorer® and Microsoft® are registered trademarks of Microsoft Corporation.
- Java® and JavaScript® are registered trademarks of Sun Microsystems, Inc.
- Mozilla® is a registered trademark of the Mozilla Foundation.
- Netscape® is a registered trademark of Netscape Communications Corporation.
- PANTONE® is a registered trademark of Pantone, Inc.
- Wi-Fi® is a registered trademark of the Wi-Fi Alliance
- WPA, WPA2, Protected Setup, WMM and WMM-SA are trademarks of the Wi-Fi Alliance

2.3 Definitions

The following terminology is used throughout this Technical Report.

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 Technical Report defines the following abbreviations:

AAL	ATM Adaptation Layer
ac	alternating current
ADSL	Asynchronous Digital Subscriber Line
ALG	Application Layer Gateway

ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
ATA	Analog Terminal Adapter
ATM	Asynchronous Transfer Mode
CAT3	Category 3
CAT5	Category 5
CHAP	Challenge Handshake Authentication Protocol
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check
CSA	Canadian Standards Association
DBRu	Dynamic Bandwidth Report upstream
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Server
DoS	Denial of Service
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DUID	DHCP Unique Identifier
DUID-EN	DUID based Enterprise Number
EARP	Ethernet Address Resolution Protocol
EIA	Electronic Industries Alliance
FCC	Federal Communications Commission
FQDN	Fully Qualified Domain Name
GEM	G-PON Encapsulation Method
GMT	Greenwich Mean Time
GSM	Global System for Mobile Communications
GTC	G-PON Transmission Convergence
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
Hz	Hertz
IAID	Identification Association Identifier
IEEE®	The Institute of Electrical and Electronics Engineers
IETF	The Internet Engineering Task Force
IP	Internet Protocol

IPCP	Internet Protocol Control Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
Kbps	kilobits per second
LAN	Local Area Network
MAC	Medium Access Control
MRU	Maximum Receive Unit
ms	milli-second
MTBF	Mean Time Between Failure
MTU	Maximum Transit Unit
NAT	Network Address Translation
ND	Neighbor Discovery
NRZ	Non Return to Zero
NS	Neighbor Solicitation
NTP	Network Time Protocol
ONT	Optical Network Terminal
PAP	PPP Authentication Protocol
PC	Personal Computer
PD	Prefix Delegation
POTS	Plain Old Telephone Service
PPP	Point to Point Protocol
PVC	Permanent Virtual Circuit
RA	Router Advertisement
RG	Residential Gateway
RS	Router Solicitation
SIP	Session Initiation Protocol
SN	Serial Number
SNTP	Simple Network Time Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TR	Technical Report
UDP	User Datagram Protocol
UL	Underwriters Laboratories
ULC	Underwriters Laboratories Canada

USB	Universal Serial Bus
Vac	Volts ac
VCI	Virtual Circuit Identifier
Vdc	Volts dc
VDSL	Very high-speed Digital Subscriber Line
VID	VLAN Identifier
VLAN	Virtual LAN
VPI	Virtual Path Identifier
VoIP	Voice over IP
WAN	Wide Area Network
WEP	Wireless Encryption Protocol
Wi-Fi®	Wi-Fi Alliance wireless standards organization
WPA	Wi-Fi Protected Access

3 Technical Report Impact

3.1 Energy Efficiency

This Technical Report contains regional power requirements for Residential Gateway (RG) devices. In general, there is an expectation that these devices will meet all local regulatory requirements for powering and energy consumption.

3.2 IPv6

Issue 2 of this Technical Report has been published specifically to provide requirements needed for deployment of IPv6 capable RGs.

3.3 Security

The requirements in this Technical Report 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

Section	Item	Requirements
GEN		**General Device Requirements**
DESIGN		**Design**
GEN.DESIGN.	1	The device MUST be compact and have a physical profile suitable for desktop.
GEN.DESIGN.	2	The device SHOULD be able to be wall mounted and stand on its side.
GEN.DESIGN.	3	The device MAY have the ability to be mounted horizontally or vertically.
GEN.DESIGN.	4	If wall mounted, the device SHOULD be oriented so that the cabling is routed toward the ground in order to reduce strain on the cabling.
GEN.DESIGN.	5	A detachable wall-mounting bracket MAY be added to the device.
GEN.DESIGN.	6	The power connector at the device MUST be securely connected to avoid accidental disconnect. This means that the connector MUST be either secured via a clip to the box or be held in place with significant force so that it does not readily pull out by minor pulling on the power cord.
GEN.DESIGN.	7	If the power supply is external to the device, it SHOULD be labeled with the device vendor's name and the model number of the device.
GEN.DESIGN.	8	If the power supply is external to the device it SHOULD be either small enough, or appropriately positioned on the power cord, so as not to block other power outlets.
GEN.DESIGN.	9	If the power cable includes an analog to digital conversion brick, that brick MAY have a light on it.
GEN.DESIGN.	10	The device MUST NOT be USB powered.
GEN.DESIGN.	11	The device MUST NOT use the local phone loop for power.
GEN.DESIGN.	12	The model and serial number MUST be visible via external markings on the device.
GEN.DESIGN.	13	The model and serial number MUST be visible via external markings on the product packaging.
GEN.DESIGN.	14	If a console port used for local technician configuration is provided on the device it SHOULD NOT be physically accessible to end users (e.g. it should not be placed on the outside of the device).
GEN.DESIGN.	15	The device MUST have a single function reset button in order to reset the device to the default factory settings.
OPS		**Device Operation**
GEN.OPS.	1	All device firmware and associated system files MUST be pre-installed.
GEN.OPS.	2	The device MUST operate 24 hours a day, 7 days a week without the need to reboot.
GEN.OPS.	3	The MTBF (Mean Time Between Failure) of the device and operating system SHOULD be equal to or exceed 1 year (e.g., it should not need a reboot more than one time per year).
GEN.OPS.	4	The life expectancy of the device SHOULD be at least seven years.

GEN.OPS.	5	The Device SHOULD be tolerant of power fluctuations and brown-outs, continuing to operate normally and maintaining its configuration after these events.
GEN.OPS.	6	The device SHOULD be able to detect faults and reset appropriately upon detection.
GEN.OPS.	7	The device SHOULD include sufficient non-volatile memory to accommodate future control and data plane protocol upgrades over a minimum of four years. The potential upgrades may include: initiating and terminating signaling protocols at IP and ATM layers; logic for packet classification, policing, forwarding, traffic shaping and QoS support at both IP and ATM layers.
GEN.OPS.	8	This device MUST preserve local configuration information during power-off and power interruption.
GEN.OPS.	9	The device MUST complete power up in 60 seconds or less (timing starts when the power is connected and stops when the On/Off power indicator light is "Solid Green").
GEN.OPS.	10	The device SHOULD be self-installable by an end user in under 20 minutes assuming the default configuration and mode of operation for the device. This is the time from when the box is opened to when the user is using the service including any driver installation (assuming no network complications and excluding micro-filter installation and customer ordering/registration).
GEN.OPS.	11	Other than networking drivers (e.g., USB, wireless, etc…), other software or drivers MUST NOT be required on computers and other devices for proper and full use of the device.
GEN.OPS.	12	The device, drivers and any packaged software SHOULD support Macintosh OS 8.6 and above.
GEN.OPS.	13	The device, drivers and any packaged software SHOULD support all Microsoft PC based operating systems which have not yet reached "End of Support" status (see http://support.microsoft.com/lifecycle for more details).
GEN.OPS.	14	The device, drivers and any packaged software MAY support Linux. It is especially desirable to do so with an open interface.
GEN.OPS.	15	The device MUST preserve its configuration across firmware updates.
GEN.OPS.	16	All software revisions SHOULD be backward compatible with all previous versions. There SHOULD be no loss of existing functionality.
GEN.OPS.	17	Software revisions MUST NOT require service provider network changes to maintain proper operation of previous features.
GEN.OPS.	18	The device firmware MUST be identified by a revision number. This revision number MUST be formatted using an X.Y.Z incremental numbering format where X indicates the major release number, Y indicates the minor release number, and Z represents the revision number (e.g. 2.4.1).
GEN.OPS.	19	The vendor SHOULD have a web site where firmware updates and documentation is available.
GEN.OPS.	20	The firmware at the vendor's web site SHOULD include all error correcting updates for the device.
GEN.OPS.	21	The device MUST NOT allow "back door" entry to the unit (e.g., there must be no hidden telnet or web access using secret passwords).

GEN.OPS.	22	All firmware updates MUST be verified using security mechanisms. A checksum mechanism is a minimum requirement for achieving this.
GEN.OPS.	23	All firmware updates SHOULD be verified using a cryptographic "fingerprint" of at least 256 bits.
GEN.OPS.	24	In the event of a failure occurring during an update, the device MUST be able to back off to the prior version of the firmware installed on the device. That is, the prior version of the device's firmware MUST continue to be useable in the event that a firmware update fails to complete. This is not a requirement for a dual image, although that is one manner in which this requirement might be achieved.
NET		**Networking Protocols**
GEN.NET.	1	The device MUST support Ethernet (IEEE 802.3).
GEN.NET.	2	The device MUST support IP Version 4.
GEN.NET.	3	If the device does not support IPV6, it SHOULD be software configurable or upgradeable to support IP Version 6 in the future. This means that the processing power, memory and networking components must be designed appropriately and be sufficiently robust to provide this support.
GEN.NET.	4	The device MUST support the TCP, IP, UDP, routing and associated protocols identified here: - IETF RFC 0768 User Datagram Protocol - IETF RFC 0791 Internet Protocol - IETF RFC 0792 Internet Control Message Protocol - IETF RFC 0793 Transmission Control Protocol - IETF RFC 0826 Ethernet Address Resolution Protocol (ARP) - IETF RFC 0894 Standards for the Transmission of IP Datagrams over Ethernet Networks - IETF RFC 0922 Broadcasting Internet Datagrams in the Presence of Subnets - IETF RFC 0950 Internet Standard Subnetting Procedure - IETF RFC 1009 Requirements for Internet Gateways (Link Layer issues only) - IETF RFC 1042 Standard for the Transmission of IP Datagrams over IEEE 802 Networks - IETF RFC 1112 Host Extensions for IP Multicasting - IETF RFC 1122 Requirements for Internet Hosts - Communication Layers - IETF RFC 1123 Requirements for Internet Hosts - Application and Support - IETF RFC 1256 ICMP Router Discovery Messages (Router Specification only) - IETF RFC 1519 Classless Inter- Domain Routing (CIDR) - IETF RFC 1812 Requirements for IP Version 4 Routers - IETF RFC 1918 Address Allocation for Private Internets - IETF RFC 3600 Internet Official Protocol Standards - IANA Directory of General Assigned Numbers (http://www.iana.org/numbers.html)
GEN.NET.	5	The device MUST support IP over Ethernet.
GEN.NET.	6	The device MUST support, at a minimum, a 256 MAC address table for LAN devices.

NETv6		**IPv6 Networking Protocols**
GEN.NETv6.	1	The device MUST support IP Version 6, which is defined in IETF RFC 2460.
GEN.NETv6.	2	The device MUST support enabling and disabling of IPv6.
WAN		**Wide Area Networking (WAN)**
ATM		**ATM**
WAN.ATM.	1	The device MUST support standard ATM (AAL5) payload format. Note this satisfies TR-101 R-338.
WAN.ATM.	2	The device MUST perform AAL Segmentation and Reassembly (SAR), Convergence Sublayer (CS) functions and CRC check.
WAN.ATM.	3	The device MUST support encapsulation of bridged Ethernet over AAL5 (without FCS) as described in IETF RFC 2684 (formerly IETF RFC 1483).
WAN.ATM.	4	The device MUST be able to use both LLC-SNAP and VC-MUX (null) encapsulation over AAL5 with all supported protocols. The default MUST be LLC-SNAP.
WAN.ATM.	5	The device MAY support encapsulation of IP over AAL5, per IETF RFC 2684.
WAN.ATM.	6	If the device supports IP over AAL5, it MAY support Classical IP according to IETF RFC 2225.
WAN.ATM.	7	The device MUST support ATM CoS. UBR, CBR and VBR-rt MUST be supported (as defined in The ATM Forum Traffic Management Specification Version 4.1).
WAN.ATM.	8	VBR-nrt and UBR with per VC queuing SHOULD be supported.
WAN.ATM.	9	The default ATM CoS for the primary VC MUST be UBR.
WAN.ATM.	10	The device SHOULD support auto configuration as defined in Broadband Forum TR-062 and ILMI 4.0 and its extensions.
WAN.ATM.	11	The device MUST always respond to ATM testing, pings and loopbacks according to ITU-T I.610 (F4, F5).
WAN.ATM.	12	The device SHOULD support initiating an ATM Loopback, and receiving the reply. This satisfies TR-101 R-337.
WAN.ATM.	13	The device MUST provide a default CPID of all 1s (FFFF). This satisfies TR-101 R-339.
WAN.ATM.	14	The device MUST support 0/35 as the default VPI/VCI for the first PVC or use an operator-specific configuration.
WAN.ATM.	15	The device MUST be able to perform an auto search for the VPI/VCI settings for the first PVC based on a defineable search list VPI/VCI sequence order. If the modem reaches a state of session establishment (e.g., IP when the modem is responsible for session termination) after performing the auto search, the default VPI/VCI settings MUST be set to the newly discovered values. The new default pair MUST be stored on the modem across power off situations. If an ATM connection cannot be established after power is restored, the search process starts over again.

WAN.ATM.	16	The device MUST support the following default VPI/VCI auto-search list programmed as a factory default setting in the following sequence, or use an operator-specific sequence configuration: 0/35, 0/38, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51. This default list MUST be overwriteable via the methods discussed in WAN.ATM.19
WAN.ATM.	17	The device MUST be configurable so that the auto-search mechanism can be disabled.
WAN.ATM.	18	The device MUST allow the auto-search list to be redefined using Broadband Forum TR-064 and TR-069.
WAN.ATM.	19	The default VPI/VCI values for all PVCs MUST be configurable. The default value MUST be utilized prior to performing an auto-search but should exclude the default value in the auto-search.
WAN.ATM.	20	The device MUST support VPI values from 0 to 255
WAN.ATM.	21	The device MUST support VCI values from 32 to 65535
ATM.MULTI		**ATM Multi-PVC**
WAN.ATM.MULTI.	1	The device MUST support eight PVCs. This is in addition to support for any implemented ATM UNI control path PVCs (e.g. ILMI auto-configuration PVC, etc.).
WAN.ATM.MULTI.	2	The device MUST allow the protocol stack (e.g., IP over Ethernet, PPPoE, PPPoA, etc…) for each provisioned PVC to be defined separately. If necessary, each PVC can use a different stack and set of protocols.
WAN.ATM.MULTI.	3	There is no default defined VPI/VCI for additional PVCs past the primary PVC defined in WAN.ATM above. The device MUST support auto-search function (see WAN.ATM.17 through 20) on all PVCs and will use the same auto-search sequence identified (skipping over any already in use).
WAN.ATM.MULTI.	4	All supported PVCs MUST NOT require the same VPI value.
WAN.ATM.MULTI.	5	All supported PVCs MUST be able to be active and sending/receiving traffic simultaneously. See requirements LAN.FWD.8, 10, 11 and 15 for more details on interface selection for routing.
WAN.ATM.MULTI.	6	The device MUST support the minimum ATM granularity applicable to the associated DSL protocol in use on a per VC and VP basis. For example, ATM granularity of 32 kbps MUST be supported for ADSL on a per VC and VP basis.
WAN.ATM.MULTI.	7	The device MUST use the same Ethernet MAC address for all interfaces over the same AAL5/ATM/DSL connection.
WAN.ATM.MULTI.	8	The device MUST support multiple levels of CoS simultaneously across separate VCCs (e.g., UBR for PVC 0/35 and CBR for PVC 0/43 where both PVCs are active simultaneously).

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.
WAN.CONNECT.	2	Moved to WAN.CONNECT.ON-DEMAND.1 and 4
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.
WAN.CONNECT.	4	Moved to WAN.CONNECT.ON-DEMAND.6
WAN.CONNECT.	5	A manual way of disconnecting without waiting for a connection timeout MUST be provided.
WAN.CONNECT.	6	Moved to WAN.CONNECT.ON-DEMAND.7
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.
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 failed query, log the event.
CONNECT.ON-DEMAND		**On-Demand Connection Establishment** The On-demand Connection function applies only to IPv4 connections. However, when IPv6 is present, its behavior must take the presence of IPv6 into consideration as described in this module.
WAN.CONNECT.ON-DEMAND.	1	The device MUST support a “connect on demand” option for IPv4 connections that run over PPP. 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.
WAN.CONNECT.ON-DEMAND.	2	If the PPP session only contains IPv4, then the device MUST terminate the PPP session, and any associated PPPoE session (if applicable).
WAN.CONNECT.ON-DEMAND.	3	If the PPP session contains IPv4 and IPv6, then the device MUST terminate only the IPv4 session. This will be done using IPCP commands.
WAN.CONNECT.ON-DEMAND.	4	The device MUST support a "connect on demand" option for IPv4 connections that run over Ethernet.
WAN.CONNECT.ON-DEMAND.	5	To determine whether a connection has IPv4 activity during a timeout interval, the device MUST only consider traffic with an IPv4 ethertype.
WAN.CONNECT.ON-DEMAND.	6	The interval after which a connection timeout occurs MUST be able to be configured.
WAN.CONNECT.ON-DEMAND.	7	A default timeout of 20 minutes SHOULD be used for connection timeouts or use an operator-specific configuration.

WAN.CONNECT.ON-DEMAND.	8	If the device has an active IPv6 connection, and does not have addresses for DNS recursive name servers to be accessed over IPv6, then the "connect on demand" option MUST be disabled.
ETHOAM		**Ethernet OAM**
WAN.ETHOAM.	1	The device MUST support a Maintenance Association End Point (MEP) on a per VLAN basis. Note: The multi-PVC case is for further study. This satisfies TR-101 R-251.
WAN.ETHOAM.	2	The device MUST support a default ME level value of 5 for the Customer Level. This satisfies TR-101 R-252.
WAN.ETHOAM.	3	The device SHOULD support a Loopback Message (LBM) function that can generate a Multicast LBM towards its peer MEP(s). This satisfies TR-101 R-253.
WAN.ETHOAM.	4	The device MUST support a Loopback Reply (LBR) function towards its peer MEP(s) in response to both unicast and multicast LBMs. This satisfies TR-101 R-254.
WAN.ETHOAM.	5	The device MUST support a Linktrace Reply (LTR) function towards its peer MEP(s). This satisfies TR-101 R-255.
WAN.ETHOAM.	6	For business customers and/or premium customers requiring proactive monitoring, the device SHOULD support generating Continuity Check Messages (CCMs). This satisfies TR-101 R-256.
WAN.ETHOAM.	7	The device MUST support turning off sending of CCMs, while keeping the associated MEP active. This satisfies TR-101 R-257.
WAN.ETHOAM.	8	The device MUST support receiving AIS messages. This satisfies TR-101 R-258.
WAN.ETHOAM.	9	The device SHOULD trigger the appropriate alarms for Loss of Continuity. This satisfies TR-101 R-259.
WAN.ETHOAM.	10	The device MUST support a default ME level value of 1 for the Access Link level. This satisfies TR-101 R-261.
WAN.ETHOAM.	11	The device SHOULD support a Loopback Message (LBM) function that can generate a Multicast LBM towards its peer MEP(s). This requirement allows the device to dynamically learn the MAC address of the AN MEP, and test the connectivity to that MEP. Notice that the ability for the device to generate a multicast LBM at the Customer level and at the Access Link level are sufficient to test connectivity to the near edge of the carrier's network and to the BNG, which are the only two points that are visible to the device. A Linktrace initiation capability would provide no added value. Upon receiving a LBM, the device must respond to it by initiating a LBR. In other words, it must support the LBM sink function and the LBR source function. This satisfies TR-101 R-262.
WAN.ETHOAM.	12	The device MUST support a Loopback Reply (LBR) function towards its peer MEP(s), in response to both unicast and multicast LBMs. This satisfies TR-101 R-263.
BRIDGE		**Bridging** Note that the IPv6 parts of this module apply only if the device supports IPv6.
WAN.BRIDGE.	1	The device MUST be able to bridge IPv4 over Ethernet.

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.
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 DHCPv4 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.
WAN.BRIDGE.	4	The device MUST be able to bridge IPv6 over Ethernet (EtherType 0x86DD). This includes bridging of multicast frames.
WAN.BRIDGE.	5	The device MUST be able to manage IPv6 bridging for a WAN interface, separate from IPv4 treatment.
WAN.BRIDGE.	6	The device MUST be able to manage IPv6 bridging separately for each WAN interface (if there are multiple WAN interfaces).
WAN.BRIDGE.	7	When IPv6 bridging is enabled on a WAN interface, the device MUST be configurable to act as a host on that WAN interface (doing SLAAC, etc.). It will not request IA_PD, since that is not a host function.
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 IPCP (IPv4).
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.
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).

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 Broadband 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.
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.
WAN.DHCPC.	6	The DUID-EN field value MAY be printed on the product label on the bottom of the device.
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.
IPv6		**IPv6 WAN Connection**
WAN.IPv6.	1	The device MUST support automated establishment of an IPv6 connection according to the flow in Annex A.2.
WAN.IPv6.	2	The device MUST support dual stack of IPv4 and IPv6 running simultaneously, as described in Section 2 of RFC 4213, "Transition Mechanisms for IPv6 Hosts and Routers".
WAN.IPv6.	3	The device MUST allow the IPv6 stack to be enabled / disabled.
WAN.IPv6.	4	The device MUST support DHCPv6 client messages and behavior per IETF RFC 3315. See WAN.DHCPC.5 for further specifics on IAID value.
WAN.IPv6.	5	The device MUST support RFC 3633, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6."
WAN.IPv6.	6	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
WAN.IPv6.	7	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).
WAN.IPv6.	8	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.
WAN.IPv6.	9	The device MUST support stateless address auto-configuration (SLAAC), as a host, per IETF RFC 4862.
WAN.IPv6.	10	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).
WAN.IPv6.	11	If route information is provided (RFC 4191) and the device has multiple WAN connections, it MUST place the route information in its routing table.
WAN.IPv6.	12	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.
WAN.IPv6.	13	The device MUST support enabling / disabling of this IPv6 WAN connection interface.

WAN.IPv6.	14	The device MUST be able to request the following DHCPv6 options: IA_NA (RFC 3315), Reconfigure Accept (RFC 3315), IA_PD (RFC 3633), and DNS_SERVERS (RFC 3646).
WAN.IPv6.	15	The device SHOULD be able to request the following DHCPv6 options: SNTP_SERVERS (RFC 4075), Domain Search List (RFC 3646), and Client FQDN (RFC4704).
WAN.IPv6.	16	The device MUST be configurable as to which DHCPv6 options it requests via DHCPv6.
WAN.IPv6.	17	The connectivity parameters (obtained via RA and DHCPv6) MUST be persistent across loss of WAN connection (or lack of response from WAN connection).
WAN.IPv6.	18	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.
WAN.IPv6.	19	The device MUST NOT advertise any address prefixes on the WAN using the IPv6 Neighbor Discovery protocol, or advertise itself as a default router
WAN.IPv6.	20	The device MUST provide up to 4 instances of option-data within a single OPTION_VENDOR_OPTS (17) (RFC 3315) with IANA "ADSL Forum" Enterprise Number as the enterprise-number. Each instance will have one of the 4 sub-options from WAN.DHCPC.7 as the vendor-specific opt-code, with the corresponding value in the vendor-specific option-data. If the value of a parameter is empty for the device, then the sub-option MUST be omitted. If there are no values to provide, the entire option MUST be omitted.
TRANS		**Transitional IPv6 WAN Connection**
TRANS.6rd		**6rd Transition Mechanism**
WAN.TRANS.6rd.	1	The device MUST support the 6rd transition mechanism as described in draft-ietf-softwire-ipv6-6rd. This includes being able to configure the necessary parameters via TR-069 and DHCPv4, creation of the prefix, using the created prefix as a “delegated prefix” for purpose of including one of its /64s in RA messages, and modifying the IP header for traffic that goes between the WAN and LAN devices.
WAN.TRANS.6rd.	2	The device MUST support enabling and disabling of this feature on the “default” routed IPv4 connection. 6rd is not applicable to bridged WAN interfaces.
TRANS.DS-LITE		**Dual Stack Lite Transition Mechanism**
WAN.TRANS.DS-LITE.	1	The device MUST support DS-Lite (draft-ietf-softwire-dual-stack-lite) with IPv4 in IPv6 encapsulation (RFC 2473).
WAN.TRANS.DS-LITE.	2	The device MUST support DS-Lite DHCPv6 options to retrieve the address or FQDN of the tunnel concentrator (draft-ietf-softwire-ds-lite-tunnel-option).
WAN.TRANS.DS-LITE.	3	The device MUST configure a static IPv4 default route towards the DS-Lite tunnel.
WAN.TRANS.DS-LITE.	4	The device MUST deactivate the NAPT function on the DS-Lite interface.
WAN.TRANS.DS-LITE.	5	The device MUST support enabling and disabling of DS-Lite.

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.
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.
WAN.PPP.	3	The device MUST support PPPoE over the encapsulated Ethernet as defined in IETF RFC 2516.
WAN.PPP.	4	The device MUST support IETF RFC 4638 in order to accommodate MTU/MRU values greater than 1492 bytes in PPPoE.
WAN.PPP.	5	If the device supports ATM, the device SHOULD support PPP over AAL5 (PPPoA) as defined in IETF RFC 2364.
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).
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.
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).
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.
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.
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.

WAN.PPP.	12	If PPP is used, the device MAY obtain an IPv4 subnet mask on its WAN interface using IPCP (IPv4) extensions. If this is done, then IPv4 subnet masks will be communicated with IPCP (IPv4) using the PPP IPCP (IPv4) 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.
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.
WAN.PPP.	14	The device MUST support RFC 3544, "IP Header Compression over PPP".
PPP.IPv6		**PPP Client for establishment of IPv6 connection**
WAN.PPP.IPv6.	1	The device MUST support IPv6 over PPP per IETF RFC 5072 and RFC 5172.
WAN.PPP.IPv6.	2	The device MUST support establishment of an IPv6 over PPPoE connection according to the flow in Annex A.1.
WAN.PPP.IPv6.	3	The device MUST allow any particular PPP connection to be configurable for IPv4-only, IPv6-only, or both.
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.
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
dot1x		**802.1x Client**
WAN.dot1x.	1	The device MUST support IEEE 802.1X™ acting as a supplicant.
WAN.dot1x.	2	The device MUST be able to respond to an appropriate IEEE 802.1X request and provide certificate information using Extensible Authentication Protocol-Transport Layer Security (EAP/TLS).
WAN.dot1x.	3	The device SHOULD support EAP-MD5 username and password type authentication.
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).
WAN.dot1x.	5	The device MUST perform mutual authentication by authenticating certificate information of the requesting authenticator.

WAN.dot1x.	6	The device MUST be able to store certificate information used to authenticate the authenticator.
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.
WAN.dot1x.	8	The device SHOULD be able to update the information used to validate the authenticator by updated certificates without a firmware upgrade.
WAN.dot1x.	9	The device MUST be able to store information allowing it to authenticate a minimum of eight authenticators.
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.
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.
WAN.dot1x.	12	The device certificate MUST have a validity period greater than the operational lifetime of the device.
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.
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.
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 or IP (v4 or v6) Addresses matching those assigned to the LAN Segment).
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).
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).
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.

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.
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.
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.
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.

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.
WAN.QoS.	6	The device SHOULD support sending the following frame types: untagged frames, priority-tagged frames, and VLAN-tagged 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.
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.
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.
WAN.QoS.	10	The device MUST duplicate the set of queues for each access session. This can be done logically or physically.
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.
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.
WAN.QoS.	15	The packet size threshold before fragmenting AF and BE packets MUST be configurable.
QoS.TUNNEL		**Quality of Service for Tunneled Traffic** This module only applies when the device is an endpoint for a tunnel to the WAN. Note that this module applies to IPv6 if it is used as either the tunneled or the tunneling protocol.
WAN.QoS.TUNNEL.	1	The device MUST be able to mark or remark the Diffserv codepoint of traffic that will be placed over a tunnel, based on classification of that traffic (prior to placing it on the tunnel) using any of the classifiers supported by the device. This only applies when the traffic is going from LAN to WAN.
WAN.QoS.TUNNEL.	2	The device MUST be able to mark the Diffserv codepoint of the underlying tunnel or IEEE 802.1D Ethernet priority of Ethernet that is transporting the tunnel, based on classification of the tunneled traffic using any of the classifiers supported by the device. This only applies when the traffic is going from LAN to WAN.
WAN.QoS.TUNNEL.	3	When the device receives tunneled traffic from the WAN, it MUST be able to mark or remark the Diffserv codepoint of that traffic, based on classification of the tunneled traffic using any of the IP-layer or higher layer classifiers supported by the device.
WAN.QoS.TUNNEL.	4	When the device receives tunneled traffic from the WAN, it MUST be able to mark the IEEE 802.1D Ethernet priority of the LAN Ethernet frame, based on classification of the tunneled traffic using any of the IP-layer or higher layer classifiers supported by the device.
WAN.QoS.TUNNEL.	5	When the device receives tunneled traffic from the WAN, it MUST be able to mark or remark the Diffserv codepoint or mark the IEEE 802.1D Ethernet priority of the LAN Ethernet frame, based on classification of the WAN Ethernet, using any of the Ethernet-layer classifiers supported by the device.

WAN.QoS.TUNNEL.	6	When the device receives tunneled traffic from the WAN, it SHOULD be able to mark or remark the Diffserv codepoint or mark the IEEE 802.1D Ethernet priority of the LAN Ethernet frame, based on classification of the underlying tunnel, using any of the IP-layer classifiers supported by the device.
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.
LAN.GEN.	2	Both NetBios and Zero Config naming mechanisms MAY be used to populate the DNS tables.
LAN.GEN.	3	The device MAY act as a NETBIOS master browser for that name service.
LAN.GEN.	4	The device MUST support multiple subnets being used on the local LAN.
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.
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.
LAN.ADDRESS.	3	The device MUST NOT use auto IP for address assignment of its LAN-side IPv4 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.
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.

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).
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.
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 4862. It MUST always use the same LL address, even after reboot or power failure.
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.
LAN.ADDRESSv6.	3	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).
LAN.ADDRESSv6.	4	The device MAY allow its ULA prefix to be changed through configuration.
LAN.ADDRESSv6.	5	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.
LAN.ADDRESSv6.	6	The devices MUST support RFC 4861 Router Specification requirements (section 6.2).
LAN.ADDRESSv6.	7	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).
LAN.ADDRESSv6.	8	The device SHOULD support configuration of the following elements of a Router Advertisement: MTU (RFC 4861).
LAN.ADDRESSv6.	9	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.
LAN.ADDRESSv6.	10	The device SHOULD advertise DNS server using the RDNSS option in Router Advertisements (RFC 5006).

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
LAN.DHCPS.	2	The device MUST be a DHCPv4 server to local LAN devices, supporting all LAN devices.
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.
LAN.DHCPS.	4	The device MUST support a minimum of 253 LAN devices.
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.
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.
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.
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.
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.

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.
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.
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.
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.
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.
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.
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.
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.

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.
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 DHCPv4. Once a WAN connection is established, the public IPv4 address provided by the broadband network is passed to the LAN device during the next DHCPv4 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).

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.
DHCPv6S		**DHCPv6 Server**
LAN.DHCPv6S.	1	The device MUST support DHCPv6 server messages and behavior per IETF RFC 3315.
LAN.DHCPv6S.	2	The device MUST support and be configurable to enable/disable address assignment using DHCPv6.
LAN.DHCPv6S.	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.
LAN.DHCPv6S.	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.
LAN.DHCPv6S.	5	The device MUST be configurable to enable/disable prefix delegation via DHCPv6.
LAN.DHCPv6S.	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.
LAN.DHCPv6S.	7	The WAN / ULA prefixes that a device is allowed to further delegate SHOULD be configurable.
LAN.DHCPv6S.	8	The device MUST support DHCPv6 Information_request messages.
LAN.DHCPv6S.	9	The device MUST support the following DHCPv6 options: IA_NA (RFC 3315), IA_PD (RFC 3633), and DNS_SERVERS (RFC 3646).
LAN.DHCPv6S.	10	The device SHOULD support Reconfigure Accept (RFC 3315) and pass the additional set of DHCP options received from the DHCP client on its WAN interface to IPv6 hosts.
LAN.DHCPv6S.	11	The options that the device will provide via DHCPv6 MUST be configurable.
DNS		**Naming Services (IPv4 and general requirements)**
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.
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).

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.
LAN.DNS.	4	The device MUST add the DNS entry "dsldevice" for its own address.
LAN.DNS.	5	The device MAY support additional DNS entries, as there could be additional types of CPE.
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.
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.
LAN.DNS.	8	If DNS Proxy is implemented, it MUST be done according to the recommendations in RFC 5625.
DNSv6		**Naming Services (IPv6)**
LAN.DNSv6.	1	The device MUST act as a DNS server for IPv6-capable LAN devices by supporting IPv6 (AAAA) records in its DNS server (per RFC 3596) and allowing these records to be queried using either IPv4 or IPv6 transport (RFC 3901).
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.
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.
LAN.DNSv6.	4	The device MUST be able to query for A and AAAA records using either IPv4 or IPv6 transport to DNS recursive name servers in the WAN.
LAN.DNSv6.	5	The device SHOULD use a DNS recursive name server obtained through DHCPv6 option (23 - OPTION_DNS_SERVERS) to query for AAAA records to the WAN, as its first choice.
LAN.DNSv6.	6	When the device is proxying DNS queries for LAN devices, it SHOULD use the IPv6 transport regardless of the transport mode used by the LAN device, when querying to the WAN. This is only possible if the device has IPv6 addresses for DNS recursive name servers on the WAN.
LAN.DNSv6.	7	The device MUST support receiving at least 2 DNS recursive name server IPv6 addresses from the network through DHCPv6 option OPTION_DNS_SERVERS (23) (RFC 3646) .

LAN.DNSv6.	8	The device SHOULD allow the user to specify that the network-learned or user-specified DNS recursive name server addresses be passed back to the LAN devices in DHCPv6 responses instead of the device's address itself as the DNS recursive name server(s).
NAT		**NAT/NATP**
LAN.NAT.	1	The device MUST support Network Address Port Translation (NAPT; also known as Port Address Translation) as defined in IETF RFCs 2663, 3022 and 3027.
LAN.NAT.	2	The device MUST support disabling NAPT.
PFWD		**Port Forwarding (IPv4)**
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.
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 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 I.
LAN.PFWD.	4	The "Common Applications Names List" mechanism MUST be integrated with the port forwarding mechanism.
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.
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 I.
PFWDv6		**Port Forwarding (IPv6)**
LAN.PFWDv6.	1	The device MUST support security mechanisms described in draft-ietf-v6ops-cpe-simple-security.
LAN.PFWDv6	2	Individual port forwarding rules MUST be associated with a LAN device, not the IPv6 address of the LAN device, and follow the LAN device should its IPv6 address change.

LAN.PFWDv6	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 I.
ALG		**ALG Functions (IPv4)**
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).
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.
LAN.ALG.	3	The device MUST allow at least one IPv4 IPsec connection from the LAN.
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.
LAN.ALG.	5	The device MUST support LAN device UDP Encapsulation of IPv4 IPsec packets as defined in IETF RFC 3948.
LAN.ALG.	6	The device MUST support LAN device negotiation of NAT-Traversal with IKE as identified in IETF RFC 3947.
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.
LAN.ALG.	8	The device MUST seamlessly handle RTSP traffic to LAN devices with no user intervention required.
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.
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).
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.
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.).
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.

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. This applies to MTU negotiated in IPv4 or IPv6.
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.
LAN.FWD.	8	The device MUST support accepting IP (v4 and v6) forwarding/routing information via the TR-069 interface.
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).
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.
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.
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.
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.
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.
LAN.FWD.	15	The device MUST support all LAN devices concurrently accessing one or more WAN connections.

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.
LAN.FWD.	17	If RIP-2 is supported, it SHOULD be software configurable.
LAN.FWD.	18	If RIP-2 is supported, by default, the device MUST NOT transmit RIP-2 information to WAN connections.
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.
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.
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.
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.
IGMP.ROUTED		**IGMP 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.
LAN.IGMP.ROUTED.	2	The device MUST support IGMPv3 as defined in IETF RFC 3376. This satisfies TR-101 R-192.
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.
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.
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.

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.
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.
LAN.IGMP.ROUTED.	8	It MUST be possible to configure a device WAN-facing IPv4 interface with an IPoE encapsulation and no IPv4 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.
LAN.IGMP.ROUTED.	9	All device LAN ports and interfaces MUST be capable of processing IGMP messages.
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.
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 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).
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.

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.
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.
LAN.IGMP.ROUTED.	16	The device MUST support a minimum of 32 multicast groups.
LAN.IGMP.ROUTED.	17	The device SHOULD support a minimum of 64 multicast groups.
LAN.IGMP.ROUTED.	18	The device MUST be configurable to log (on demand) all IGMP messages on both the LAN and WAN interfaces.
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).
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.
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.
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.
LAN.IGMP.ROUTED.	23	The device MUST be configurable as to how many simultaneous multicast streams are allowed from WAN to LAN.
MLD.ROUTED		**MLD and Multicast in Routed Configurations (IPv6)**
LAN.MLD.ROUTED.	1	The device MUST support MLDv2 as defined in IETF RFC 3810.
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
LAN.MLD.ROUTED.	3	The device SHOULD support functionality as described for IGMP in requirements LAN.IGMP.ROUTED. 6, 10, 17
LAN.MLD.ROUTED.	4	The device MUST be configurable to prevent sending MLD messages to the WAN interfaces for specified multicast addresses or scopes.
LAN.MLD.ROUTED.	5	The device MUST default to not sending MLD messages for scope of 0 through 8.

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 IPv4 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).
LAN.FW.	2	The device MUST support a separate firewall log to maintain records of all transactions that violate firewall rules.
LAN.FW.	3	The firewall log file MUST be able to hold at least the last 100 entries or 10 Kbytes of text.
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.
LAN.FW.	5	If a firewall log is implemented, the device MUST timestamp each firewall log entry.
LAN.FW.	6	The RG MUST support the definition of IPv6 firewall rules separate from IPv4
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.
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.
LAN.FW.SPI.	3	Each type of attack for which protection is provided SHOULD be configurable on the device and on by default.
LAN.FW.SPI.	4	The device MUST support passing and blocking of traffic by use of user and configurable defined rules.

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.
LAN.FW.SPI.	6	The device MUST support the user temporarily disabling specific user defined rules or all user defined rules.
LAN.FW.SPI.	7	The device MUST support the user specifying the order in which firewall rules are processed.
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
LAN.FW.SPI.	9	The device MAY support filtering based on other fields unique to specific protocols.
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
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.
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.

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 application.
LAN.FW.SPI.	14	The device MUST allow for configuration of global firewall values.
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.
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.
FILTER.TIME		**Time of Day Filtering**
LAN.FILTER.TIME.	1	The device MAY support filtering based on time of day on a per LAN device basis.
FILTER.CONTENT		**Content Filtering**
LAN.FILTER.CONTENT.	1	The device MAY support filtering based on Web content or URL string screening techniques on a per LAN device basis.
DIAGNOSTICS		**Automated User Diagnostics**
LAN.DIAGNOSTICS.	1	If the device is on the same subnet as any LAN device, when network connectivity problems occur, the device MUST provide a mechanism which intercepts web browser pages (i.e., port 80 web page requests) and responds to these by directing the web browser to appropriate internal web pages to identify and resolve network connectivity problems including but not limited to: - DSL cannot train - DSL signal not detected - Broadband Ethernet not connected (if applicable) - ATM PVC not detected (if applicable) - IEEE 802.1x failure (if applicable) - PPP server not detected (if applicable) - PPP authentication failed (if applicable) - DHCP not available
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.

LAN.CAPTIVE.	2	The redirection function and associated fields MUST NOT be modifiable by the subscriber.
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.
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.
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.
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.
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
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.
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.
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.
LAN.CAPTIVE.	11	Incremental packet delay through the device due to white list lookup MUST NOT exceed 5 ms.
MGMT		**Management & Diagnostics**
GEN		**General**
MGMT.GEN.	1	Configuration and installation of the device SHOULD minimize the number of restarts of the device when enabling changes.
MGMT.GEN.	2	If software is loaded on LAN CPE for installation or configuration of the device, this software MUST NOT require the associated LAN CPE to restart, except in the case of the installation of networking drivers (e.g., USB, wireless, etc…) or a change in the IP address assignment (e.g., static to DHCP, public to private, private to public or assignment of a specific IP address using DHCP).
MGMT.GEN.	3	The device MUST maintain an internal log of WAN side connection flows (e.g., WAN link layer, DHCP, IP and PPP sessions). At a minimum, the log MUST record the last 250 events. This will include WAN physical interface events initiated by locally or by the access network. The purpose of the log is to provide a trouble shooting aid in resolving line and connection problems.

MGMT.GEN.	4	The device MUST timestamp each log entry.
MGMT.GEN.	5	The factory default timestamp value for log entries SHOULD indicate the elapsed time since the unit was first powered on. The log entry timestamp SHOULD be formatted, consistent with ISO 8601:2000, as follows: PYYYY-MM-DDThh:mm:ss where: P = the letter "P" used to indicate what follows is a time interval (period) data element YYYY = number of years (digits) MM = number of months (digits, 01 – 12; 1 month is the equivalent of 30 days for time interval purposes) DD = number of days (digits, 01 – 30) hh = number of hours (digits, 00 – 24) mm = number of minutes (digits, 00 – 60) ss = number of seconds (digits, 00 – 60) Once the device has established connectivity to an Internet based time server, all log entry timestamps SHOULD be formatted for GMT or user specified time zone (24 hour military format), consistent with ISO 8601:2000, as follows: YYYY-MM-DDThh:mm:ss±hh:mm or YYYY-MM-DDThh:mm:ssZ , where: YYYY = year (digits) MM = month (digits, 01 – 12) DD = day of month (digits, 01 – 31) T = the letter “T”, used to indicate the start of the time of day Z = the letter “Z”, used to indicate that the time is UTC (Coordinated Universal Time) hh = hours (digits, 00 – 24) mm = minutes (digits, 00 – 60) ss = seconds (digits, 00 – 60) ±hh:mm = the difference between local time and UTC in hours and minutes (e.g., -05:00 would indicate Eastern Standard Time, 5 hours behind UTC)
MGMT.GEN.	6	The device MUST have diagnostic information available that allow the user to identify the precise nature of any connection or performance problem. It MUST be able to indicate if the problem is at the Physical Layer, ATM, Ethernet, PPP, or IP layer. This information MUST be accessible from the Web GUI and TR-064/TR-069 interfaces.
MGMT.GEN.	7	The device MUST have an embedded ICMP PING client capable of being initiated via the Web GUI and TR-069 interfaces to PING to WAN and LAN side IP addressable devices.
MGMT.GEN.	8	The device modem log SHOULD reside on the device and be persistent across power loss.
MGMT.GEN.	9	The device modem log SHOULD NOT interfere with the normal performance of the modem. That is, the prioritization of writing log entries to non-volatile storage SHOULD NOT be done at a priority or in a manner that would degrade the user experience nor the connection throughput.

MGMT.GEN.	10	The device MUST be able to start training, establish a network connection and respond to network tests by default upon power up prior to any additional configuration or software installation on the associated PC. The absence of a PC MUST have no impact on these operations.
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.
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)
UPnP.IGD		**UPnP IGD**
MGMT.UPnP.IGD.	1	The device MUST support UPnP InternetGatewayDevice:1 Device Template Version 1.01 Standardized DCP. This specification is made available for download at http://www.upnp.org.
MGMT.UPnP.IGD.	2	If UPnP IGD is supported, it MUST allow the user to enable logging of all UPnP IGD actions and events.
MGMT.UPnP.IGD.	3	If UPnP IGD is supported, the user SHOULD be warned upon enabling it that this may allow applications to configure the box and allow unexpected accessing of local devices.
LOCAL		**Local Management**
MGMT.LOCAL.	1	If the device is in a bridged configuration the device MUST be able to disable all LAN side configuration mechanisms (e.g. Web GUI, TR-064, etc.)
MGMT.LOCAL.	2	A configuration mechanism from the PC to the device based on XML MUST be supported as defined in Broadband Forum TR-064.
MGMT.LOCAL.	3	The TR-064 based LAN side configuration mechanism MUST operate independently of the status or configuration of UPnP IGD in the device.
MGMT.LOCAL.	4	The device MUST be configurable via embedded, easy-to-use Web GUI pages.
MGMT.LOCAL.	5	TR-064 and Web GUI authorization MUST time out after 30 minutes.
MGMT.LOCAL.	6	The Web GUI pages MUST be available when the device is in bridged mode.
MGMT.LOCAL.	7	The device MUST NOT require browser support of Java, ActiveX nor VBSCRIPT in its web pages.
MGMT.LOCAL.	8	The Web GUI pages SHOULD minimize internal page complexity (e.g., excessive use of frames, pop-ups, style sheets, JavaScript, etc…) that places demands on browser resources or causes interoperability problems with different browsers. In general, all pages SHOULD load within five seconds.

MGMT.LOCAL.	9	The web interface MUST be OS independent and browser independent (e.g., must work with Opera, Mozilla, Safari, Netscape and Internet Explorer). The web interface MUST work with Netscape 4.7, Microsoft Internet Explorer 4.0 and later versions of these browsers.
MGMT.LOCAL.	10	The device MUST have a software mechanism by which the user can reset it to default factory settings.
MGMT.LOCAL.	11	The device MUST support a modem access code (i.e., password) that protects it from being updated (firmware, configuration, operational state, etc…) from the local LAN. Additional password discussion is identified in Broadband Forum TR-064 and TR-069.
MGMT.LOCAL.	12	If a default modem access code has been set, the default modem access code MUST be on the bottom of the device.
MGMT.LOCAL.	13	If a default modem access code has been set, the device MUST force the user to accept the default modem access code or install a new modem access code prior to allowing any initial configuration (e.g., during initial installation or after a modem reset to factory defaults).
MGMT.LOCAL.	14	The user MUST be able to disable the use of the modem access code. The user MUST be warned in the Web GUI of the implications of under-taking this action.
MGMT.LOCAL.	15	The device MUST support updating of its firmware via the Web GUI and TR-064 interfaces.
MGMT.LOCAL.	16	The device MUST use standard protocols when using FTP, HTTP and HTTPS as defined in IETF RFCs 959, 2616, 2246, and 2818.
MGMT.LOCAL.	17	The device MUST support restarting the broadband connection (all layers) via the Web GUI and TR-064.
MGMT.LOCAL.	18	The device SHOULD be able to copy log files to a PC on the local LAN or network server in ASCII text format, using the Web GUI and TR-064 interfaces.
MGMT.LOCAL.	19	The device MUST have a quick start page in the Web GUI allowing for rapid configuration in a minimum number of steps (e.g., on a single page). Default values for PPPoE and PVC can be used to facilitate this.
MGMT.LOCAL.	20	The model and firmware/software versions MUST be easily identifiable via the Web GUI interface.
MGMT.LOCAL.	21	The Web GUI interface MUST allow the user to browse and select an update file from a local PC and use HTTP to update the device using this file (see IETF RFCs 1867, 2388 and HTML 4.1 specifications for more details).
MGMT.LOCAL.	22	If the device has been configured to do so, the Web GUI MUST allow the user to specify that firmware be updated from a pre-defined web location. The device MUST allow the web location to be specified by the TR-064/TR-069 interfaces.
MGMT.LOCAL.	23	The web location MAY be pre-defined by the modem manufacturer. This value is overridden by the mechanisms and information identified in requirement MGMT.LOCAL.21.

MGMT.LOCAL.	24	If the device has been configured to allow updating from a pre-defined web location, the device MUST display an update button in the Web GUI. The user can then select the update button to initiate an update using a file retrieved via ftp or http as identified in the associated URL (2 URLs may be hard coded; the second URL will be used if file retrieval is not possible from the first URL).
MGMT.LOCAL.	25	If the device has been configured to allow updating from a pre-defined web location, the mechanism used to identify the availability of an update, the description of the update and the actual update SHOULD operate solely based on the presence (or absence) of named files returned in a directory list using the web location URL. For example, a device might retrieve the directory list, find the update associated with the modem by the presence of the following file: Vendor-model-v100210-n100215.pkg This would identify that for device "model" from "vendor" currently running version 10.02.10 there exists an update whose version is 10.02.15. The text describing the update, if available, might be located in a file of the name: Vendor-model-v100210-n100215.txt
MGMT.LOCAL.	26	If the device has been configured to do so, the Web GUI MUST display a web link to which the user may go to browse for update files and other update information. The device MUST allow this URL to be specified and overridden by TR-064/TR-069 interfaces.
MGMT.LOCAL.	27	The web link MAY be set to a default value by the modem manufacturer.
REMOTE.TR-069		**Remote Management (TR-069)**
MGMT.REMOTE.TR-069.	1	The device MUST support the remote management protocol as defined in Broadband Forum TR-069 CPE WAN Management protocol.
MGMT.REMOTE.TR-069.	2	The device MUST support Broadband Forum TR-098 Gateway Device Version 1.1 Data Model for TR-069 with support for the TR-098 Baseline:1 profile
MGMT.REMOTE.TR-069.	3	If the device supports built-in file sharing clients (e.g. Windows Networking, CIFS, Samba) or includes integrated storage server functions, the device MUST NOT allow the use of the TR-069 file transfer mechanisms (i.e. Upload and Download RPCs) to place or retrieve files that are not explicitly authorized by the user on network shared storage locations which the device may have access to.
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.

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.
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.
MGMT.REMOTE.WEB.	4	Temporary WAN side remote access MUST NOT allow for changing the device password.
MGMT.REMOTE.WEB.	5	Temporary WAN side remote access MUST be disabled by default.
MGMT.REMOTE.WEB.	6	Temporary WAN side remote access SHOULD be through HTTP over TLS (i.e., https using TLS).
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.
MGMT.REMOTE.WEB.	8	If a default port is used for temporary WAN side remote access, it MUST be 51003.
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.
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.
MGMT.REMOTE.WEB.	11	The user MUST be able to change the User ID for all temporary WAN side remote access sessions.
MGMT.REMOTE.WEB.	12	The device MUST allow only one temporary WAN side remote access session to be active at a time.
MGMT.REMOTE.WEB.	13	All other direct access to the device from the WAN side MUST be disabled and blocked by default.
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.
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.
MGMT.NTP.	3	The device MUST support the use of time server identification by both domain name and IP (v4 or v6) address.
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.
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.
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.
MGMT.NTP.	7	The time client SHOULD support DNS responses with CNAMEs or multiple A or AAAA records.

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.
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.
MGMT.NTP.	10	The frequency with which the device updates its time from a time server SHOULD be able to be configured.
IF.WAN		**WAN Interface Modules**
ADSL		**ADSL and ADSL2+**
IF.WAN.ADSL.	1	The device MUST include an internal ADSL modem.
IF.WAN.ADSL.	2	The device MUST complete training within the following timeframes (timing starts when the On/Off power indicator light is "Solid Green", when the DSLAM port is enabled and stops when the ADSL layer connectivity indicator is "Solid Green"): - 60 seconds, for single mode operation on the default inner pair assuming line auto-sensing is not activated, or if auto-sensing is activated and ADSL is present on the default pair - 120 seconds, for auto-mode operation or for single mode operation if line auto-sensing is activated and ADSL is not present on the default pair - 150 seconds, for DELT-based auto-mode operation on the default inner pair assuming line auto-sensing is not activated.
IF.WAN.ADSL.	3	The device MUST pass the tests identified in Broadband Forum TR-048, "*ADSL Interoperability Test Plan*", and any subsequent updates or replacements to that document that exist at the time that the modem is tested, prior to its initial deployment. Within 6 months, modems produced after changed or new test requirements have been approved MUST conform to those new requirements.
IF.WAN.ADSL.	4	The device MUST train and pass data against all ITU 992.1 based ATU-C deployed in North America using TR-067 criteria.
IF.WAN.ADSL.	5	The device MUST comply with requirements as specified in ANSI T1.413-1998, ANSI T1.413a-2001 and ITU 992.1 for Annex A or Annex B depending upon regional requirements
IF.WAN.ADSL.	6	The device MUST support FDM-mode per ANSI T1.413 and ITU-T G.992.1.
IF.WAN.ADSL.	7	The device MUST comply with ITU G.992.3 (ADSL2) and ITU G.992.5 (ADSL2+).
IF.WAN.ADSL.	8	The device SHOULD comply with ITU G992.3 Annex L (RE-ADSL2).
IF.WAN.ADSL.	9	The device MUST support Trellis coding.
IF.WAN.ADSL.	10	The device MUST be rate-adaptive and able to support all speeds between the minimum and maximum applicable to the associated DSL protocol in use (e.g., ADSL, ADSL2, ADSL2+, RE-ADSL, ...) and in the minimum increment applicable to the associated DSL protocol in use. For example, for ADSL, the device MUST be able to support speeds in 32 kbps increments from 32 kbps to 8 Mbps downstream and 32 kbps to 800 kbps upstream.

IF.WAN.ADSL.	11	The device MUST support dynamic rate adaptation.
IF.WAN.ADSL.	12	The device MUST support independent upstream and downstream data rate provisioning.
IF.WAN.ADSL.	13	The device MUST support bit swapping.
IF.WAN.ADSL.	14	The device MUST support both fast and interleaved paths. This is not a requirement for dual latency support (e.g., running Fast and Interleaved at the same time to two different locations).
IF.WAN.ADSL.	15	The device MUST have a high-pass filter at its ADSL line input to eliminate impulse noise from premises wiring.
IF.WAN.ADSL.	16	The device SHOULD NOT incorporate an internal splitter (i.e., SHOULD NOT have a POTS pass back port).
IF.WAN.ADSL.	17	The default pair used to detect the ADSL signal MUST be the inner pair (pins 3 & 4).
IF.WAN.ADSL.	18	The device SHOULD provide line auto-sensing capabilities to automatically detect and select the ADSL signal on either the inner pair (pins 3 & 4) or outer pair (pins 2 & 5) of an RJ-11 jack. If the modem reaches showtime after performing the DSL auto-sensing, the default pair will be set to the newly discovered pair. This can be the inner pair or the outer pair. The new default pair is store on the modem across power off situations. DSL auto-sensing will be activated with the new default pair.
IF.WAN.ADSL.	19	If DSL line auto-sensing is implemented, the device MUST allow disabling of the automatic detection of the ADSL signal on the inner and outer pairs and allow specification of which pair to search for the DSL signal.
IF.WAN.ADSL.	20	The device MUST conform to ANSI T1.413-1998 section 7.4.1.3 CRC requirements.
IF.WAN.ADSL.	21	The device MUST support remote testing, remote diagnostics, performance monitoring, surveillance information access and other information access as identified in ANSI T1.413-1998 and ITU G.997.1. At a minimum non-optional requirements from these standards MUST be supported. Additional parameters are identified in TR-064 and TR-098 profiles.
IF.WAN.ADSL.	22	The device MUST provide detailed information for current connections and associated parameters including ADSL sync rate, power for both upstream and downstream directions, FEC error count, CRC error count, line attenuation, signal-to-noise margins, relative capacity of line, trained bit rate, graph of bits per tone, and loss of signal, loss of frame and loss of power counts. Additional parameters are identified in TR-064 and TR-098 profiles.
VDSL2		**VDSL2**
IF.WAN.VDSL2.	1	The device MUST include an internal VDSL2 modem.
IF.WAN.VDSL2.	2	The device MUST be able to terminate the VDSL2 signal through the inner pair of a 6-position (pins 3 and 4) or 8-position (pins 4 and 5) mini-modular jack (e.g., RJ-11, RJ-14, RJ-45).
IF.WAN.VDSL2.	3	The device MAY be able to terminate VDSL2 over other connections, such as coax.
IF.WAN.VDSL2.	4	The device MUST be compliant with ITU-T G.993.2.

IF.WAN.VDSL2.	5	The device MUST include support for the following application reference models from ITU-T G.993.2: - G.993.2 section 5.4.2, Data with POTS service - G.993.2 section 5.4.1, Data service (no POTS or ISDN)
IF.WAN.VDSL2.	6	The device SHOULD support simultaneous transmission of US0 and US1 in profiles for which the capability of US0 has been indicated.
IF.WAN.VDSL2.	7	The device MUST pass the functionality test plan of TR-115,
IF.WAN.VDSL2.	8	The device MUST pass the VDSL2 performance and interoperability test plans of TR-114.
IF.WAN.VDSL2.	9	[North America] The device MUST be compliant with ITU-T G.993.2 Annex A.
IF.WAN.VDSL2.	10	[Europe] The device MUST be compliant with ITU-T G.993.2 Annex B.
IF.WAN.VDSL2.	11	[Europe] The device MUST include support for the following application reference model from ITU-T G.993.2: - G.993.2 section 5.4.3, Data with ISDN service
xDSL		**xDSL General Requirements**
IF.WAN.xDSL.	1	Removing AC power from the device MUST NOT prevent POTS from operating.
IF.WAN.xDSL.	2	A failure in the device MUST NOT impact the private intra-premises network except for those functions provided by the device (e.g., DHCP, DNS).
IF.WAN.xDSL.	3	The device MUST NOT cause any failure in or interference with the xDSL network.
IF.WAN.xDSL.	4	Failure or removal of LAN CPE connected to the DSL device MUST NOT prohibit POTS from operating.
IF.WAN.xDSL.	5	The device MUST only synchronize within the minimum and maximum line rate parameters for a line as identified by the DSLAM or RT.
IF.WAN.xDSL.	6	The device performance and throughput MUST keep up with the DSL line rate.
xDSL.INP		**xDSL INP Values**
IF.WAN.xDSL.INP.	1	The device MUST support ADSL INP values of 0, ½, 1, and 2. Note that for certain DSL types such as ADSL 1 ITU-T G.992.1 do not support setting INP values in the ATU-R.
IF.WAN.xDSL.INP.	2	The device MAY support additional INP settings as specified in the appropriate ITU-T recommendations specific to each type of DSL.
xDSL.BOND		**xDSL Bonding**
IF.WAN.xDSL.BOND.	1	If the device supports ATM-based bonding, it MUST comply with ATIS T1.427.01 and ITU-T G.998.1 standards.
IF.WAN.xDSL.BOND.	2	If the device supports Ethernet-based bonding, it MUST comply with ATIS T1.427.02 and ITU-T G.998.2 standards.

IF.WAN.xDSL.BOND.	3	If the device supports DSL bonding, the device MAY support the following parameters in the web user interface and in vendor specific extensions to TR-064 and TR-069: - Group parameters (per group instance): o Group ID (group number assigned from ATM based xTU-C) o Status (valid values include: Operational, Unavailable) o Number of Links (number of DSL links in the group) o RX Cell Loss (total number of cells lost in the receive direction for all ATM links) - Link parameters (per link instance) o Group ID (to which the link is a member for all ATM links) o Link Status (valid values include: Not in use, Standby, Available) o Data Rate (Should return the TC-Layer data rate in bits/sec (in case of ATM, the ATM cell rate at the ATM layer after removal of idle/incorrect cells)
IF.WAN.xDSL.BOND.	4	The device MUST support the bonding mechanism (as described in requirements IF.WAN.xDSL.BOND.1 and 2) associated with the underlying TPS-TC of the device's xDSL link.
IF.WAN.xDSL.BOND.	5	When the device has been configured to perform xDSL bonding of 2 pairs and uses a single mini-modular jack to connect to the xDSL lines, it MUST search for the signals on the inner pair (pins 3 & 4 for 6-pin, pins 4 & 5 for 8-pin) and outer pair (pins 2 & 5 for 6-pin, pins 3 & 6 for 8-pin) of the jack.
IF.WAN.xDSL.BOND.	6	When the device has been configured to perform xDSL bonding of 2 pairs and uses two separate mini-modular jacks to connect to the xDSL lines, the pair used to detect the xDSL signal on both jacks MUST be the inner pair (pins 3 & 4 for 6-pin, pins 4 & 5 for 8-pin).
IF.WAN.xDSL.BOND.	7	If one of the xDSL connections drops, the remaining xDSL connection(s) MUST NOT be dropped, provided that the minimum provisioned data rate is met.
IF.WAN.xDSL.BOND.	8	If xDSL bonding is supported by the device, the device MUST be clearly labeled indicating this feature.
IF.WAN.xDSL.BOND.	9	If the device supports xDSL bonding, it MUST allow manual configuration of the following options for the source of the broadband connection - DSL Line 1 only (single xDSL link on inner pair only if a single jack, or jack 1 if presented on separate jacks) - DSL Line 2 only (single xDSL link on outer pair only if a single jack, or jack 2 if presented on separate jacks) - xDSL bonding (both xDSL links) using pairs for bonding described in IF.WAN.xDSL.BOND.5 and 6).
IF.WAN.xDSL.BOND.	10	If the device supports xDSL bonding, the Web GUI on the device MUST indicate when bonding is in use in terms of the connection type.
IF.WAN.xDSL.BOND.	11	When bonding has been enabled on the device, the Web GUI and TR-064/TR-069 interfaces MUST indicate the state of the bonded lines even if one is not up.

xDSL.REPORT		xDSL Reporting of Physical Layer Issues
IF.WAN.xDSL.REPORT.	1	The device MUST be capable of reporting a DSL Re-Initialization Cause Code parameter via DSL Forum TR-069 to the ACS. When the product re-initializes its DSL connection, it MUST store, in non-volatile memory, a code indicating the cause of the re-initialization. After re-initialization and after a data connection is available to the TR-069 server, the product MUST report to the server the cause code. At a minimum, the following cause codes MUST be supported: 1) Autonomous re-initialization of the DSL connection 2) Loss of local power 3) External re-initialization, e.g., via a local 'reset' 4) Cause not determined
IF.WAN.xDSL.REPORT.	2	The device MUST support all requirements in ITU-T Rec. G.997.1 (PLOAM).
IF.WAN.xDSL.REPORT.	3	The device MUST be capable of generating threshold-crossing alerts reported via DSL Forum TR-069 to the ACS for all mandatory performance-monitoring parameters (defined in ITU-T G.997.1) during a data collection interval for which threshold values have been assigned.
IF.WAN.xDSL.REPORT.	4	The device MUST allow the setting of data collection intervals (per ITU-T G.997.1), and reporting schedules via DSL Forum TR-069 to the ACS for performance monitoring at all monitoring points of the device. Modifications to these parameters shall not be allowed until the associated data collection is deactivated.
xDSL.SEALING		**DC Sealing Current**
IF.WAN.xDSL.SEALING.	1	The device MUST provide for the termination of sealing current on either, or both, DSL line pairs. A sample circuit implementation reference diagram is provided in Appendix V.
IF.WAN.xDSL.SEALING.	2	The DC termination for sealing current MUST be capable of conducting at least 20mA of current.
IF.WAN.xDSL.SEALING.	3	The DC termination MUST meet the requirements as specified in ANNEX I of ITU-T Recommendation G.992.3.

IF.WAN.xDSL.SEALING.	4	A Low Pass filter MUST be in place between the DC termination and the DSL line. The filter MUST meet the following requirements, which are based on xDSL in-line filter requirements in ANSI T1.421-2001: - It MUST introduce less than 25 Ohms DC resistance Tip-Ring, when DC termination side is shorted. - It MUST have an impedance, from either conductor to ground, greater than 5 MΩ. - The capacitance, from either conductor to ground, MUST be less than 1nF on the loop side - The attenuation MUST be at least 65dB between 25 kHz – 12.0 MHz. - The input impedance, looking from network side into the LPF when terminated in the ON state on the termination side, MUST result in an bridging loss on the DSL line of not more than 0.25 dB, when measured at any frequency between 25 kHz and 12.0 30.0 MHz. - The DC resistance between Tip and Ring, when the DC termination side is open, MUST be at least 3.5 MΩ. - The input impedance, looking from network side into the LPF when terminated in the ON state on the termination side, MUST result in an bridging loss in the voice band of not more than 0.5 dB, when measured at any frequency between 200 Hz and 4.0 kHz.
IF.WAN.xDSL.SEALING.	5	The device MUST support enabling and disabling of the DC termination capability through its Local Web GUI, and TR-064/TR-069 interfaces.
IF.WAN.xDSL.SEALING.	6	The device SHOULD be able to detect the presence of POTS service on a line.
IF.WAN.xDSL.SEALING.	7	If POTS is detected by the device, the termination MUST NOT be applied.
xDSL.SURGE		**AC Power Surge Protection**
IF.WAN.xDSL.SURGE.	1	The device MUST tolerate an AC surge, as specified in EN 61000-4-5, Test Level 3; - Criteria 1: The product MUST not — as a result of the surge — transmit or receive bit errors for more than 2 seconds. - Criteria 2: The product MUST not — as a result of the surge — re-initialize. - Criteria 3: The product MUST not — as a result of the surge — transmit a ‘dying gasp’ message.
IF.WAN.xDSL.SURGE.	2	The device MUST tolerate Electrical Fast Transients on the AC mains, as specified in EN 61000-4-4, Test Level 3: - Criteria 1: The product MUST not — as a result of the Electrical Fast Transients — transmit or receive bit errors at a rate greater than 10E-7 (care should be taken to ensure that fast transients are not coupled to the DSL pair). - Criteria 2: The product MUST not — as a result of the Electrical Fast Transients — re-initialize. - Criteria 3: The product MUST not — as a result of the Electrical Fast Transients — transmit a ‘dying gasp’ message.

ETH		Ethernet (WAN)
IF.WAN.ETH.	1	If the device supports an optional WAN Ethernet port, it MUST support 10BASE-T/100BASE-T presented on an RJ-45 jack.
IF.WAN.ETH.	2	If the device supports both a WAN Ethernet port in addition to another physical WAN link type (e.g., ADSL, VDSL2, ONT function, etc.), simultaneous use of both WAN ports MUST NOT be supported.
IF.WAN.ETH.	3	An automatic WAN port selection function MAY be supported as follows: Upon first boot-up or power cycle of the device, the device MUST wait until fully operational prior to attempting to selecting the source WAN port to use. The device MUST first search for a DSL signal prior to selecting the Ethernet port as the WAN link. This is intended to avoid race conditions that happen because DSL typically requires a longer duration of time to detect physical layer than Ethernet. If both Ethernet and DSL signals are detected simultaneously, the device MUST by default select the DSL link as the WAN source port. Once the source of the physical signal has been detected on a valid source connector, it MUST be used persistently until power is removed from the device or the selection is overridden via Web GUI or TR-069. In other words, even if a connection is lost, the device MUST NOT automatically switch to an alternate link source (e.g. DSL to Ethernet, or Ethernet to DSL). Note that automatic pair detection schemes are excluded from this requirement - meaning that DSL Line 1/2 auto selection, and Ethernet Auto-MDIX/MDX MUST still operate properly to accommodate end user faulty wiring that may occur. For example if DSL Line 1 is detected first, the customer disconnects DSL and reconnects to Line 2 instead the device should allow this type of switching and connect to DSL on Line 2 and not by accident switch to a potentially present Ethernet signal instead.
IF.WAN.ETH.	4	The device MUST support configuring the current default WAN port being used via Web GUI or TR-069 extension. This should result in immediate switching to the selected port by the user or operator.
IF.WAN.ETH.	5	Any Ethernet port used as a WAN link SHOULD be non-blocking for LAN to LAN and LAN to WAN traffic flows. This may occur in some implementations that utilize one port of a multi-port Ethernet switch for WAN use, sometimes as a result requiring LAN to LAN traffic to be forwarded and processed through the device CPU.
GPON		**GPON**
IF.WAN.GPON.	1	The device MUST include an integrated GPON ONT interface.
IF.WAN.GPON.	2	The device MUST comply with all mandatory requirements for the ONT as specified in ITU G.984.1 (General Characteristics), G.984.2 Amd 1 (Physical Media Dependent Layer), G.984.3 (Transmission Convergence Layer) and G.984.4 (ONT Management and Control Interface).

IF.WAN.GPON.	3	The device MUST support requirements contained in Table 3.2 of ITU-T G.984.2 Amd1 (optical budget, source type, transmitter range, mean launched power min/max, extinction ratio, etc.).
IF.WAN.GPON.	4	The device MUST support the maximum logical reach of 60 km.
IF.WAN.GPON.	5	The device MUST use NRZ coding and scrambling in both directions.
IF.WAN.GPON.	6	The device MUST realize the mapping of GEM frames into GTC payload (and inversely extract GEM frames from GTC payload).
IF.WAN.GPON.	7	The device MUST be able to use the activation Configured SN method in conformance with ITU-T G.984.3.
IF.WAN.GPON.	8	The device SHOULD be able to use the activation Discovered SN method in conformance with ITU-T G.984.4.
IF.WAN.GPON.	9	The device MUST support a downstream rate of 2488.32 Mbps and an upstream rate of 1244.16 Mbps.
IF.WAN.GPON.	10	The device MUST support downstream and upstream traffic on the same fiber.
IF.WAN.GPON.	11	The device MUST support encapsulation of Ethernet frames using the GEM (GPON Encapsulation Method) encapsulation.
IF.WAN.GPON.	12	The device MUST NOT support encapsulation of ATM.
IF.WAN.GPON.	13	The device MUST support a minimum of 4 active Alloc-Ids.
IF.WAN.GPON.	14	The device SHOULD support a minimum of 8 active Alloc-Ids.
IF.WAN.GPON.	15	The device MUST support the full range (4096) of Alloc-ID values.
IF.WAN.GPON.	16	The device MUST support the full range (4096) of Port-ID values.
IF.WAN.GPON.	17	The device SHOULD support a minimum of 32 Port-Ids
IF.WAN.GPON.	18	The device MUST support a minimum of 8 Port-IDs mapped to GEM frames for user data.
IF.WAN.GPON.	19	The device SHOULD support a minimum of 2 GEM ports mapped to GEM frames for management traffic.
IF.WAN.GPON.	20	The device MUST support a minimum of 1 Port-ID for multicast traffic.
IF.WAN.GPON.	21	The device MUST support Forward Error Correction RS(255,239) as per ITU G.984.3 on the downstream link.
IF.WAN.GPON.	22	The device MUST support Forward Error Correction RS(255,239) as per ITU G.984.3 on the upstream link.
IF.WAN.GPON.	23	The device MUST support non-dynamic mode of operation.
IF.WAN.GPON.	24	The device MUST support dynamic bandwidth allocation (DBA) with the SR (status reporting) mode (mode 0) of operation.
IF.WAN.GPON.	25	The device MUST support an embedded OAM channel, a PLOAM channle and an OMCI channel in conformance with ITU-T G.984.4.
IF.WAN.GPON.	26	The device MUST support basic GPON interface statistics collection, and display any applicable diagnostics results in the Web GUI and via TR-069.
MoCA		**MoCA (WAN)**
IF.WAN.MoCA.	1	The device MUST support a MoCA WAN interface compliant with the MoCA Alliance specification. Information regarding the specification is available only to members of the MoCA Alliance, further details can be obtained from the consortium at http://www.mocalliance.org.

IF.WAN.MoCA.	2	The device MUST present the MoCA WAN link on an F-connector type coaxial connector.
IF.WAN.MoCA.	3	The device MUST provide a facility to enable or disable the MoCA WAN port in the Web GUI, TR-064 and via TR-069.
IF.WAN.MoCA.	4	If the device supports a MoCA WAN interface and additional WAN physical interfaces (e.g. xDSL, Ethernet, etc.), the device SHOULD be able to automatically detect and connect through the active interface if only one such interface is connected.
IF.WAN.MoCA.	5	If multiple WAN interface types are supported, the device MUST allow configuration via the Web GUI, TR-064 and via TR-069 of the default WAN interface that must be used as the active interface. This is intended to prevent inadvertent auto-switching between interfaces due to user wiring issues or temporary service outages.
IF.WAN.MoCA.	6	If the device supports a MoCA WAN port and additional WAN physical interfaces (e.g. xDSL, Ethernet, etc.), simultaneous use of more than one WAN port MUST NOT be supported.
IF.WAN.MoCA.	7	If the device supports both WAN and LAN MoCA connection, it MUST NOT use the same channel for both connections.
IF.WAN.MoCA.	8	The device port MAY have limited support for only two MoCA devices on the MoCA WAN link.
IF.WAN.MoCA.	9	The MoCA LAN port MUST support PER (Packet Error Rate) less than 1E-6 on the MoCA link. Note that PER is the measurement of link layer error. Any additional PER caused by the dropping of packets as a result of the device over saturating the MoCA link is not included in the link layer PER specified in this requirement.
IF.WAN.MoCA.	10	The MoCA LAN port MUST support the following configurable parameters: - Channel - Privacy - Security Key Password (used to generate security keys for the MoCA link). - Manual or auto-selection of Network Coordinator through interfaces such a Web GUI.
IF.WAN.MoCA.	11	The device default Security Key Password MUST be compliant with the MoCA specification.
IF.WAN.MoCA.	12	The device MAY support configuring a custom Security Key Password to meet Service Provider requirements.
IF.WAN.MoCA.	13	If the MoCA LAN port can operate on more than one channel the device MUST support manual channel selection in the Web GUI, TR-064 or via TR-069. The frequency range for MoCA LAN port spans from 850MHz to 1.5GHz and each MoCA LAN channel covers 50MHz band.

IF.WAN.MoCA.	14	The power control function of a MoCA LAN port MUST be compliant with the following requirements: - The adjustable range of output power MUST be at least in 25db attenuation range - The target PHY rate is the maximum rate that a MoCA link should support. - If the measured PHY rate is less than the Target PHY rate, it MUST be within 30Mbps of the target PHY rate unless the output power is already at maximum. - The measured PHY rate MAY be greater than the target PHY rate
IF.WAN.MoCA.	15	The MoCA LAN network MUST support the following sustain aggregate MAC throughput with PER < 1E-6 with 50db attenuation (measured aggregate MAC throughput is based on 1500 bytes packet and independent of the traffic pattern): - 125Mbps with 2 MoCA devices in the network - 117.5Mbps with 3 MoCA devices in the network - 110.5Mbps with 4 MoCA devices in the network - 103.8Mbps with 5 MoCA devices in the network - 98Mbps with 6 and above MoCA devices in the network.
IF.WAN.MoCA.	16	The device to device ping reply time (round trip) across two MoCA devices on the same RF channel MUST be within 7ms on average and 10ms maximum.
IF.WAN.MoCA.	17	The device MUST reach optimal MoCA link layer capacity in 5 minutes after power cycle.
IF.WAN.MoCA.	18	The device SHOULD reach optimal MoCA link layer capacity in 3 minutes after power cycle.
IF.WAN.MoCA.	19	The device MUST support sending/receiving packet to/from at least 64 MAC addresses on the MoCA interface.
IF.WAN.MoCA.	20	The device MUST support basic MoCA interface statistics collection, parameter provisioning, and display diagnostics results in the Web GUI, TR-064 and via TR-069.
IF.LAN		**LAN Interface Modules**
ETH		**Ethernet (LAN)**
IF.LAN.ETH.	1	The device MUST support use of a straight-through (patch) cable between the Ethernet Interface and a PC.
IF.LAN.ETH.	2	The device SHOULD automatically sense the transmit and receive pair on the Ethernet physical connection.
IF.LAN.ETH.	3	The device MUST have at least one 10/100BASE-T Ethernet port (RJ-45 jack) for connecting it to the home data network.
IF.LAN.ETH.	4	The device MUST be able to support both 10BASE-T and 100BASE-T with auto negotiate for speed and duplex on a port-by-port basis according to IEEE 802.3u.
IF.LAN.ETH.	5	The Ethernet LAN interface SHOULD allow for adjusting the inter-frame and collision back off timers so that traffic marked with Ethernet priority (as defined in IEEE 802.1D) can get statistically better treatment on broadcast LAN Segments.

ETH.SWITCH		Ethernet Switch
IF.LAN.ETH.SWITCH.	1	If the device supports additional Ethernet ports for connecting multiple Ethernet devices to the home network, the device MUST provide 10BASE-T/100BASE-T switched Ethernet functionality (e.g. not a hub only). Requirements for individual Ethernet port functionality MUST comply with all "MUST" requirements in the IF.LAN.ETH section.
USB.PC		**USB (PC)**
IF.LAN.USB.PC.	1	The device SHOULD have a client USB port (series "B" receptacle), allowing it to be a non-powered (i.e., it has its own power source and does not get power across the USB interface) remote device for a host computer.
IF.LAN.USB.PC.	2	If the device has a client USB port, the USB interface MUST appear to the PC or other host device to be an Ethernet port (i.e., the PC drivers are Ethernet drivers), and not appear as a DSL modem (e.g., MUST NOT require device modem drivers on LAN CPE).
IF.LAN.USB.PC.	3	If the device has a client USB port, the USB port MUST be based on the USB 1.1 (or later) technical specification.
IF.LAN.USB.PC.	4	If the device has a client USB port and USB 2.0 is supported, the USB interface MUST still work with the USB 1.1 based USB host controller based on the USB 2.0 standard.
IF.LAN.USB.PC.	5	Over the USB interface, the device SHOULD support USB drivers for Windows 98, Windows 98 Second Edition, Windows Millennium Edition, Windows XP (Home and Professional), Windows 2000, Macintosh OS 8.6, Macintosh OS 9.x and Macintosh OS 10.x. Any drivers that are PC-based or run on the PC SHOULD be Microsoft WHQL certified. Drivers SHOULD be available for new Microsoft and Macintosh operating systems within 30 days of General Availability.
IF.LAN.USB.PC.	6	If the device has only one Ethernet port and only one client USB port, the device SHOULD be configurable through the TR-064/TR-069 interface so that only the Ethernet or client USB port is to be active at any one time. In this configuration, whenever one of the ports is in use, the other is disabled. If neither is in use, both are enabled. The default configuration of the device SHOULD be that both ports are active at the same time.
VOICE.ATA		**Voice ATA Ports**
IF.LAN.VOICE.ATA.	1	If the device supports VoIP ports integrated directly into the product, it MUST comply with TR-122 requirements specific to RG Integrated ATA Ports.
IF.LAN.VOICE.ATA.	2	If the device supports VoIP ports integrated directly into the product, it MUST provide one LED on the front panel of the product per unique line instance supported to indicate status and be located between the last LAN LED indicator and the Broadband LED indicator. For behavior specifications and labeling requirements of the VoIP port LEDs, refer to TR-122.

WIRELESS.AP		Wireless: General Access Point Functions
IF.LAN.WIRELESS.AP.	1	The device SHOULD have the ability to mitigate interference generated by wireless and other devices operating in the same or neighboring frequencies by using interference cancellation, management or antenna techniques.
IF.LAN.WIRELESS.AP.	2	The device MUST have the ability to scan the frequency spectrum and select the best channel upon RESET and power on.
IF.LAN.WIRELESS.AP.	3	The device MAY have the ability to perform interference detection dynamically and automatically switch to the best available channel. Interference detection techniques if implemented MUST NOT impact normal operation, performance or availability of the wireless function.
IF.LAN.WIRELESS.AP.	4	The device's Wi-Fi access point MUST be able to have the channel configured to a fixed value selectable through the GUI.
IF.LAN.WIRELESS.AP.	5	The device MUST allow the user to select which LAN devices are allowed to access it through the wireless interface (i.e., MAC address filtering). By default, this restriction will be disabled.
IF.LAN.WIRELESS.AP.	6	The device Web GUI MUST provide indicators regarding the operational status of the wireless LAN and devices accessing the device using the wireless interface. This includes but is not limited to the data elements below. For the AP device itself, the following are the minimum required data elements (some may be per SSID if multiple SSIDs are supported): - SSID(s) - SSID broadcast status - radio/SSID MAC address (if different from residential gateway) - IEEE 802.11b only, 802.11g only 802.b/g mixed mode selection - maximum power level - configured data rate(s) - supported data rate(s) - authentication information - encryption information - key management information - current signal strength - radio status (disabled, enabled) - current radio channel - radio channel selection (fixed, automatic, etc…) - ERP-PBCC status (if supported; enabled, disabled) - DSSS-OFDM status (if supported; enabled, disabled) - packets transmitted - error packets transmitted - packets received - error packets transmitted - devices connected - VLAN identification - DSCP identification For each wireless client connected to the device AP, the following are the minimum required data elements: - SSID used

		- authentication used - encryption used - connection state - connected device rate - protocol used (IEEE 802.11b, 802.11g)
IF.LAN.WIRELESS.AP.	7	The device MUST be Wi-Fi CERTIFIED™ for all applicable IEEE 802.11 standards supported by the device.
IF.LAN.WIRELESS.AP.	8	The device MUST be Wi-Fi CERTIFIED™ for WPA2-Personal.
IF.LAN.WIRELESS.AP.	9	The device SHOULD be Wi-Fi CERTIFIED™ for WPA2-Enterprise.
IF.LAN.WIRELESS.AP.	10	The device MUST be Wi-Fi CERTIFIED™ for Protected Setup as an AP type device with registrar support.
IF.LAN.WIRELESS.AP.	11	The device MUST support the Wi-Fi Protected Setup push button method and MUST include a physical push button and corresponding indicator light.
IF.LAN.WIRELESS.AP.	12	The device MUST implement a Wi-Fi Protected Setup registrar user interface in the Web GUI to allow users to enter Wi-Fi device Protected Setup PIN codes.
IF.LAN.WIRELESS.AP.	13	The device MUST be Wi-Fi CERTIFIED™ for WMM (Wi-Fi Multimedia subset function of 802.11e).
IF.LAN.WIRELESS.AP.	14	The device MAY be Wi-Fi CERTIFIED™ for WMM Scheduled Access
IF.LAN.WIRELESS.AP.	15	The device MUST be Wi-Fi CERTIFIED™ for Power Save (U-APSD function of 802.11e) within 90 days of certification being offered by Wi-Fi alliance approved testing facilities.
IF.LAN.WIRELESS.AP.	16	A minimum of 32 devices (without traffic) MUST be able to simultaneously connect to the AP of The device.
IF.LAN.WIRELESS.AP.	17	The device MUST support WEP using a 40 bit key (WEP-40). This is sometimes referred to as 64 bit WEP.
IF.LAN.WIRELESS.AP.	18	The device MUST support WEP using a 104 bit key (WEP-104) as identified in IEEE 802.11i. This is sometimes referred to as 128 bit WEP.
IF.LAN.WIRELESS.AP.	19	The device MUST support both entry of hexadecimal encryption keys for use with WEP and ASCII based pass phrases for use with WPA.
IF.LAN.WIRELESS.AP.	20	Wireless MUST be enabled by default on the device using a unique authentication/encryption key and relatively unique SSID name (e.g. "SSIDNAME1234" where the digits represent the last 4 digits of the device serial number), or use an operator-specific configuration.
IF.LAN.WIRELESS.AP.	21	If wireless is enabled by default, the SSID and key MUST be printed on a label on the bottom of the device, or use an operator-specific packaging requirement.
IF.LAN.WIRELESS.AP.	22	The device MUST allow disabling the broadcasting of the primary user SSID via the Web GUI. By default broadcasting MUST be enabled.
IF.LAN.WIRELESS.AP.	23	By default, the device MUST block association requests that do not specify a valid SSID. That is, The device MUST block association requests that probe for “any” SSID.

IF.LAN.WIRELESS.AP.	24	The device SHOULD support a minimum of four SSIDs. In this case each should have its own unique characteristics including protocol configuration, data rate supported, authentication, encryption and broadcasting status. These SHOULD be used in combination with forwarding and firewall mechanisms in the device to direct traffic to specific connections and destinations.
IF.LAN.WIRELESS.AP.	25	The device MUST support a mechanism based on source SSID of incoming wireless traffic of setting the Differentiated Services Code Point (DSCP) in the IP header as defined in IETF RFC 2474.
IF.LAN.WIRELESS.AP.	26	The device MUST support setting the Ethernet VLAN identifier, defined in IEEE 802.1Q, of incoming wireless traffic to a configurable value based on SSID.
WIRELESS.11g		**Wireless: 802.11g Access Point**
IF.LAN.WIRELESS.11g.	1	The device SHOULD have internal antennas.
IF.LAN.WIRELESS.11g.	2	The device's antenna system MUST NOT have a uni-directional antenna that limits coverage to a single direction.
IF.LAN.WIRELESS.11g.	3	The device MUST include an effective Multi-Antenna (at least 2) design for diversity reception.
IF.LAN.WIRELESS.11g.	4	The device SHOULD include an effective Multi-Antenna (at least 2) design for diversity transmit.
IF.LAN.WIRELESS.11g.	5	The device SHOULD support use of an external antenna(s) for improved performance beyond the requirements identified here.
IF.LAN.WIRELESS.11g.	6	The device SHOULD have separate antennas for transmit and receive.
IF.LAN.WIRELESS.11g.	7	If an external antenna can be used with the device, the device SHOULD have a robust connector (e.g., must be durable and must not accidentally come off) for this connection.
IF.LAN.WIRELESS.11g.	8	The device's Wi-Fi access point MUST have a Maximum Transmit Power (EIRP) equal to or greater than 200 mW (23.01 dBm) when operating in the 802.11b mode.
IF.LAN.WIRELESS.11g.	9	The device's Wi-Fi access point MUST have a Maximum Transmit Power (EIRP) equal to or greater than 100 mW (20 dBm) when operating in the 802.11g mode.
IF.LAN.WIRELESS.11g.	10	The device's Wi-Fi access point output power MUST be configurable between a minimum of 30 mW and the maximum capable from The device.

IF.LAN.WIRELESS.11g.	11	The device Wi-Fi access point MUST meet the following minimum Receiver Sensitivity, Maximum Allowable Path Loss (computed as EIRP-Receiver Sensitivity) and Delay Spread Tolerance specifications:

Data Rate	RX Sensitivity	Max. Allowable Path Loss Delay Spread	Tolerance at <1% FER
802.11b			
11 Mbps	-82 dBm	104 dB	65 ns
5.5 Mbps	-87 dBm	107 dB	225 ns
2 Mbps	-90 dBm	110 dB	400 ns
1 Mbps	-93 dBm	113 dB	500 ns
802.11g			
54 Mbps	-71 dBm	87 dB	120 ns
48 Mbps	-73 dBm	89 dB	120 ns
36 Mbps	-77 dBm	93 dB	240 ns
24 Mbps	-80 dBm	96 dB	240 ns
18 Mbps	-82 dBm	98 dB	300 ns
12 Mbps	-86 dBm	102 dB	300 ns
9 Mbps	-87 dBm	103 dB	300 ns
6 Mbps	-89 dBm	105 dB	300 ns

IF.LAN.WIRELESS.11g.	12	The device Wi-Fi access point MUST have an effective automatic data rate selection algorithm to allow the system to work close to its specified receiver sensitivity so as to maximize the AP coverage and throughput.
IF.LAN.WIRELESS.11g.	13	The device MUST be Wi-Fi CERTIFIED™ for IEEE 802.11g
WIRELESS.11a		**Wireless: 802.11a Access Point**
IF.LAN.WIRELESS.11a.	1	The device MUST support and be Wi-Fi CERTIFIED™ for IEEE 802.11a. Note that no radio requirements have been specified in detail for 802.11a when operating in dual-mode with 2.4GHz 802.11b/g
WIRELESS.11h		**Wireless: 802.11h Access Point**
IF.LAN.WIRELESS.11h.	1	The device MUST support an 802.11h wireless access point. Note that no radio requirements have been specified in detail for 802.11h when operating in dual-mode with 2.4GHz 802.11b/g
HomePNA		**HomePNA (Phoneline/Coax)**
IF.LAN.HomePNA.	1	The device MUST be compliant with all requirements in ITU-T Revision of G.9954 - Home networking transceivers – Enhanced physical, media access, and link layer specifications
IF.LAN.HomePNA.	2	The device MUST support any of the following connector options for HomePNA: a) F-connector coaxial interface b) Modular RJ-11 style phone interface (optionally RJ-14 or RJ-45 connectors) c) Both option A & B interfaces
IF.LAN.HomePNA.	3	The HomePNA interface type MUST be configurable and persistent across device restarts and reboots. This parameter MUST be independent of the configuration settings which may be in use by other HomePNA devices on the local LAN.
IF.LAN.HomePNA.	4	The device MUST support enable/disable HomePNA interface. The default MUST be enabled, or use an operator-specific configuration. This parameter MUST be independent of the configuration settings which may be in use by other HomePNA

		devices on the local LAN.
IF.LAN.HomePNA.	5	The device MUST periodically collect Ethernet layer and channel performance data from HomePNA devices in the HomePNA network and report the data via Web GUI, TR-064 and TR-069.
IF.LAN.HomePNA.	6	The device MUST collect HomePNA network utilization information based on device utilization and network idle time and report the data via Web GUI, TR-064 and TR-069.
IF.LAN.HomePNA.	7	The device MUST be able to collect performance monitoring data from at least 10 HomePNA network devices in every HomePNA interface and report the data via Web GUI, TR-064 and TR-069.
IF.LAN.HomePNA.	8	The device MUST enable provisioning of the specific HomePNA devices from which performance monitoring data will be collected via Web GUI, TR-064 and TR-069.
IF.LAN.HomePNA.	9	Ethernet layer performance data MUST be associated with the individual device's information: - HomePNA MAC Address - HomePNA Station/Node ID - Master/End point device indication
IF.LAN.HomePNA.	10	Channel performance monitoring data MUST include the following: - Channel host source and destination MAC addresses - Channel HomePNA source and destination MAC addresses - Channel HomePNA PHY rate - Channel estimated SNR - Number of packets sent in channel. This parameter MUST be synchronized at both transmitter and receiver ends. - Number of pre-LARQ packets received in channel. This parameter MUST be synchronized at both transmitter and receiver ends for network packet loss calculation purpose.
IF.LAN.HomePNA.	11	Channel performance monitoring data SHOULD include the following: - Number of post-LARQ packets received in channel. This parameter MUST be synchronized at both transmitter and receiver ends for network packet loss calculation purpose.
IF.LAN.HomePNA.	12	The device MUST be able to configure and execute full or partial network diagnostics using HomePNA CERT protocol (defined in ITU Revision of G.9954) and MUST collect diagnostics results from all HomePNA devices under test. The device MUST collect the following diagnostics results between any two nodes in network and report the following results via Web GUI, TR-064 and TR-069: - Baud and PHY rate - SNR - Number of received test packets - Line attenuation

IF.LAN.HomePNA.	13	The device MUST be able to read the following configuration parameters from HomePNA devices in the HomePNA network. The device MAY optionally enable provisioning of all parameters or a subset of the configuration parameters to be read from local HPNA devices: - Noise margin - Desired PER - MAC address - Device Master/End point mode - LARQ enabling
IF.LAN.HomePNA.	14	The device MUST support at least one of the following spectral modes: - Spectral mode A: 4-20MHz – twisted pair/coax - Spectral mode B: 12-28MHz – twisted pair/coax - Spectral mode C: 36-52MHz – coax only - Spectral mode D: 4-36MHz – coax only
IF.LAN.HomePNA.	15	The device MAY support more than one HomePNA network operating in different spectral modes on the same or different physical coax wires.
IF.LAN.HomePNA.	16	If xDSL and HomePNA coexist on the device, the xDSL and HomePNA signals MUST NOT interfere with each other or impact performance in any valid spectrum band plan combinations described in the table below:

	Band "A"		Band "B"		Band "C"	Band "D"
	Phone	Coax	Phone	Coax	Coax	Coax
ADSL 1/2/2+	Yes	Yes	Yes	Yes	Yes	Yes
VDSL2 8x	No	No	Yes	Yes	Yes	No
VDSL2	No	No	No	No	Yes	No

IF.LAN.HomePNA.	17	The device MUST NOT support both HomePNA and xDSL simultaneously on the same physical wire if the xDSL and HomePNA spectrum bands used are not indicated as valid in the HomePNA spectrum compatibility table above.
IF.LAN.HomePNA.	18	The device MUST implement sufficient filtering and isolation to that HomePNA and xDSL interfaces which will not interfere each other spectrum of the device.
IF.LAN.HomePNA.	19	The device MUST support layer 2 relative QoS on the HomePNA interface.
IF.LAN.HomePNA.	20	The device MUST be able to prioritize network traffic based on at least Diffserv code points and IEEE 802.1D user priorities for relative QoS.
IF.LAN.HomePNA.	21	The device SHOULD support layer 2 guaranteed QoS on the HomePNA interface.
IF.LAN.HomePNA.	22	The device SHOULD be able to reserve bandwidth (media access time) on the network for services requesting QoS guarantees so as to meet QoS requirements for throughput (rate), latency and jitter.
IF.LAN.HomePNA.	23	The device SHOULD enable provisioning of QoS classification filters and traffic specifications in the HomePNA device.

IF.LAN.HomePNA.	24	The device MUST support classification of LAN directed traffic and placement into appropriate queues on the device side of the HomePNA interface based on any one or more of the following pieces of information: - Destination MAC address - Destination IP address(es) with subnet mask - Source IP address(es) with subnet masks - Ethernet Type - IP ToS - Protocol Type - Source Port - Destination Port - 802.1D user priority - VLAN ID
MoCA		**MoCA (LAN)**
IF.LAN.MoCA.	1	The device MUST support a MoCA LAN interface compliant with the MoCA Alliance specification. Information regarding the specification is available only to members of the MoCA Alliance, further details can be obtained from the consortium at http://www.mocalliance.org.
IF.LAN.MoCA.	2	The device MUST present the MoCA LAN link on an F-connector type coaxial connector.
IF.LAN.MoCA.	3	The device MUST provide a facility to enable or disable the MoCA LAN port via the Web GUI, TR-064 and TR-069.
IF.LAN.MoCA.	4	The MoCA LAN port MUST support PER (Packet Error Rate) less than 1E-6 on the MoCA link. Note that PER is the measurement of link layer error. Any additional PER caused by the dropping of packets as a result of the device over saturating the MoCA link is not included in the link layer PER specified in this requirement.
IF.LAN.MoCA.	5	The MoCA LAN port MUST support the following configurable parameters: - Channel - Privacy - Security Key Password (used to generate security keys for the MoCA link). - Manual or auto-selection of Network Coordinator through interfaces such a Web GUI.
IF.LAN.MoCA.	6	The device default Security Key Password MUST be compliant with the MoCA specification.
IF.LAN.MoCA.	7	The device MAY support configuring a custom Security Key Password to meet Service Provider requirements.
IF.LAN.MoCA.	8	If the MoCA LAN port can operate on more than one channel the device MUST support manual channel selection in the Web GUI or via TR-069. The frequency range for MoCA LAN port spans from 850MHz to 1.5GHz and each MoCA LAN channel covers 50MHz band.

IF.LAN.MoCA.	9	The power control function of a MoCA LAN port MUST be compliant with the following requirements: - The adjustable range of output power MUST be at least in 25db attenuation range - The target PHY rate is the maximum rate that a MoCA link should support. - If the measured PHY rate is less than the Target PHY rate, it MUST be within 30Mbps of the target PHY rate unless the output power is already at maximum. - The measured PHY rate MAY be greater than the target PHY rate
IF.LAN.MoCA.	10	The MoCA LAN network MUST support the following sustain aggregate MAC throughput with PER < 1E-6 with 50db attenuation (measured aggregate MAC throughput is based on 1500 bytes packet and independent of the traffic pattern): - 125Mbps with 2 MoCA devices in the network - 117.5Mbps with 3 MoCA devices in the network - 110.5Mbps with 4 MoCA devices in the network - 103.8Mbps with 5 MoCA devices in the network - 98Mbps with 6 and above MoCA devices in the network.
IF.LAN.MoCA.	11	The device to device ping reply time (round trip) across two MoCA devices on the same RF channel MUST be within 7ms on average and 10ms maximum.
IF.LAN.MoCA.	12	The device MUST reach optimal MoCA link layer capacity in 5 minutes after power cycle.
IF.LAN.MoCA.	13	The device SHOULD reach optimal MoCA link layer capacity in 3 minutes after power cycle.
IF.LAN.MoCA.	14	The device MUST support sending/receiving packet to/from at least 64 MAC addresses on the MoCA interface.
IF.LAN.MoCA.	15	The device MUST support MoCA interface statistics collection, parameter provisioning, and display diagnostics results via the Web GUI, TR-064 and TR-069.
IF.LAN.MoCA.	16	The device SHOULD be able to reserve bandwidth (media access time) on the network for services requesting QoS guarantees so as to meet QoS requirements for throughput (rate), latency and jitter.
HomePlugAV		**HomePlug AV (LAN)**
IF.LAN.HomePlugAV.	1	The device MUST be compliant with the HomePlug AV Specification. Information regarding the specification is available only to members of the HomePlug Powerline Alliance, further details can be obtained from the alliance at http://www.homeplug.org.
IF.LAN.HomePlugAV.	2	The device MUST support one of the following connector options for HomePlug: a) Powerline b) F-connector type coaxial connector (note this is not formally an option with HomePlug alliance but is supported by vendor implementations) c) Both A & B hybrid configuration using coaxial OR simultaneous mode by switch or relay

IF.LAN.HomePlugAV.	3	If option c) is supported in IF.LAN.HomePlugAV.2, the HomePlug interface connector type MUST be configurable and persistent across device restarts and reboots. This parameter MUST be independent of the configuration settings which may be in use by other HomePlug devices on the local LAN.
IF.LAN.HomePlugAV.	4	The device MUST periodically collect Ethernet layer and channel performance data from HomePlug devices in the HomePlug network and report the data via Web GUI, TR-064 or TR-069.
IF.LAN.HomePlugAV.	5	Ethernet layer performance data MUST be associated with the individual device's information: - HomePlug device MAC Address
IF.LAN.HomePlugAV.	6	The device MUST collect HomePlug network utilization information based on device utilization and network idle time and report the data via Web GUI, TR-064 or TR-069.
IF.LAN.HomePlugAV.	7	The device MUST support configuring a custom Security Key Password.
IF.LAN.HomePlugAV.	8	The device MUST be able to collect performance monitoring data from other devices on the powerline network and report the data via Web GUI, TR-064 or TR-069.
IF.LAN.HomePlugAV.	9	The device MUST enable provisioning of the specific HomePlug device from which performance monitoring data will be collected via Web GUI, TR-064 or TR-069.
IF.LAN.HomePlugAV.	10	The device MUST implement sufficient filtering and isolation to the HomePlug and Ethernet interfaces which will not create interference.
IF.LAN.HomePlugAV.	11	The device MUST support layer 2 relative QoS on the HomePlug interface.
IF.LAN.HomePlugAV.	12	The device MUST be able to prioritize network traffic based on at least Diffserv code points and IEEE 802.1p user priorities for relative QoS.
IF.LAN.HomePlugAV.	13	The device SHOULD support layer 2 guaranteed QoS on the HomePlug interface.
IF.LAN.HomePlugAV.	14	The device SHOULD be able to reserve bandwidth (media access time) on the network for services requesting QoS guarantees so as to meet QoS requirements for throughput (rate), latency and jitter.
IF.LAN.HomePlugAV.	15	The device SHOULD enable provisioning of QoS classification filters and traffic specifications in the HomePlug device.
REGIONAL		**Regional Annexes**
NA.POWER		**North American Power and Environmental**
REGIONAL.NA.POWER.	1	The device MUST be UL 60950 listed. This is the most recent replacement for UL 1950.
REGIONAL.NA.POWER.	2	The device MUST display proof of CSA (Canadian Standards Association) or ULC (Underwriters Laboratories Canada) certification for CAN/CSA C22.2 No. 60950. This is the Canadian equivalent to, and is identical to, UL 60950.
REGIONAL.NA.POWER.	3	The device MUST meet all requirements when operating with the following line voltages: Brownout: 96 to 127 Vac @ 60 +/- 0.1 Hz Reserve: 105 to 129 Vac @ 60 +/- 3.0 Hz

REGIONAL.NA.POWER.	4	If the power supply is external to the device, it MUST be UL 1310 or UL 60950 listed and certified.
REGIONAL.NA.POWER.	5	The device MUST comply with FCC Part 15 rules for Class B devices.
REGIONAL.NA.POWER.	6	The device MUST comply with Industry Canada ICES-003 Class B requirements.
REGIONAL.NA.POWER.	7	The device MUST comply with the requirements of Telecordia® GR-1089-CORE, Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment. Class A3 source voltages are not permitted.
REGIONAL.NA.POWER.	8	The device MUST support the following environmental conditions:

Environment	Temperature	Altitude	Relative Humidity	MWB
Operating System Ambient	0o C to 40o C	-60 to 2134 m (-197 to 7000 ft)	8% to 95% non-condensing	23 o C
Shipping	-25o C to 65o C		low humidity for low temperatures, 90% at 45o C, 30% at 65o C	29 o C

NA.LED North American LED Indicators

REGIONAL.NA.LED.	1	The device MUST have at a minimum the following indicator lights (labeling of all ports is subject to localized requirements): Power Ethernet Broadband Internet
REGIONAL.NA.LED.	2	All physical ports and bridged connection types on the device (e.g., Ethernet, USB, Wireless, HomePlug, HomePNA, 1394, etc…) MUST have a link integrity indicator lamp on the device (1 per port if a separate physical port is present or per connection type if a separate port is not present).
REGIONAL.NA.LED.	3	The indicator lights MUST be in the order as indicated in requirement REGIONAL.NA.LED.1 in a left to right or top to bottom orientation.
REGIONAL.NA.LED.	4	Port indicator lights for all additional LAN Interfaces (beyond the standard Ethernet indicator) MUST be placed between the "Ethernet" and "Broadband" lights defined in requirement REGIONAL.NA.LED.1 (note that labeling of all ports is subject to localized requirements).
REGIONAL.NA.LED.	5	All port indicator lights MUST be located on the front of the device unless summary indicator lights are used.
REGIONAL.NA.LED.	6	Physical port indicator lights MAY be located next to the port and other than on the front of the device, so long as there is a summary indicator light for the associated interface type with the other port indicator lights on the front of the unit. For example, there may be Ethernet port indicator lights located on the back of the unit by each Ethernet connection as long as there is a summary indicator for the Ethernet connections on the front of the device in the standard location.

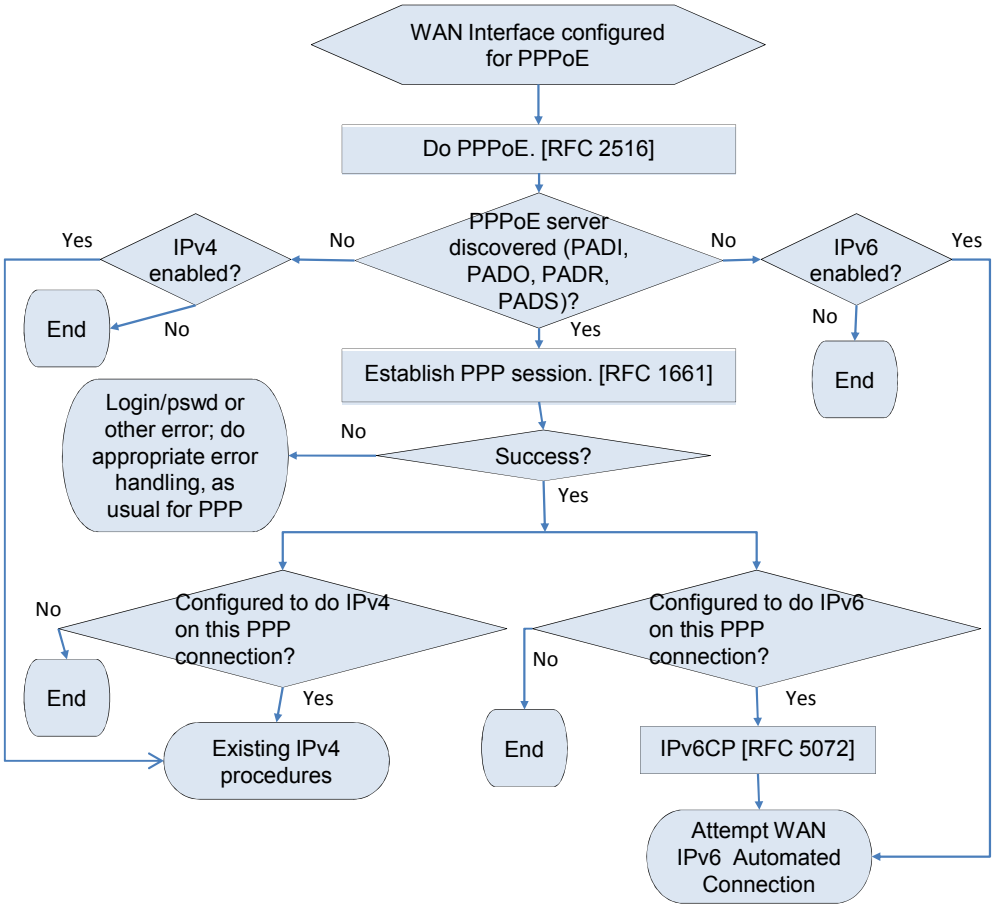
REGIONAL.NA.LED.	7	The indicator lights MUST be readily visible (99% human observer detection in less than 250 milliseconds) at 4 meters with an ambient illumination level of 5920 meter-candles. Visibility MUST be maintained over a horizontal viewing angle of +/- 80 degrees and a vertical viewing angle of -20 to +45 degrees off the central axis.
REGIONAL.NA.LED.	8	When flashing, the indicator lights MUST flash at 4 Hz with a duty cycle of 50% (except as specified otherwise in this document).
REGIONAL.NA.LED.	9	The device MUST have an On/Off power indicator light. The power indicator MUST function as follows: Solid Green = Power on Off = Power off Red = POST (Power On Self Test) failure (not bootable) or Device malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the access network or passing customer data. This may be identified at various times such after power on or during operation through the use of self testing or in operations which result in a unit state that is not expected or should not occur.
REGIONAL.NA.LED.	10	The device MUST have an indicator light that indicates Broadband interface layer connectivity. This indicator MUST function as follows: Solid Green = Broadband physical connection is established (e.g. DSL sync) Off = Broadband interface powered off, no signal detected Flashing Green = Signal detected, in process of synchronizing Flashing at 2 Hz with a 50% duty cycle when trying to detect carrier signal Flashing at 4 Hz with a 50% duty cycle when the carrier has been detected and trying to train
REGIONAL.NA.LED.	11	If additional Broadband interfaces (2 or more) are supported that operate simultaneously with the primary Broadband link (e.g. xDSL bonding, Ethernet simultaneous with xDSL, etc.), the device MUST support a Broadband light to indicate the status of each link. The behavior for this indicator MUST follow the requirements described in REGIONAL.NA.LED.10.

REGIONAL.NA.LED.	12	The device MUST have an Internet indicator light that indicates whether or not it has at least one broadband WAN interface active. This indicator MUST function as follows: Solid Green = IP connected (the device has a WAN IP address from IPCP/DHCP/Static and Broadband link is is up) and no traffic detected. If the IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present. If the session is dropped for any other reason, the light is turned off. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails. Off = Broadband physical connection power off, device in bridged mode with no IP address assigned to the device, or Broadband physical interface connection not present Flickering Green = IP connected and IP Traffic is passing thru the device (either direction) Red = Device attempted to become IP connected and failed (no 802.1x, DHCP, PPPoE, PPPoA response or authentication failure, etc.)
REGIONAL.NA.LED.	13	A LAN interface physical port indicator light MUST function as follows: Solid Green = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection) Flashing Green = LAN activity present (traffic in either direction) Off = No activity, modem power off, no cable or no powered device connected to the associated port.
REGIONAL.NA.LED.	14	If the device supports the Wi-Fi Protected Setup pushbutton method (IF.LAN.WIRELESS.AP.11), the device SHOULD have the following indicators with timing and flashing frequency as defined in the Wi-Fi Alliance Protected Setup Specification available from the Wi-Fi Alliance (www.wi-fi.org): Green = "In Progress" and "Success" status Red = "Error" and "Session Overlap" status If necessary in order to improve usability over the current Wi-FI Alliance recommendations, devices MAY use a modified timing and flashing frequency in order to improve usability. Note: This is a deviation from the three color indicator option and behaviors described by the Wi-Fi Alliance.
REGIONAL.NA.LED.	15	The indicator for Wi-Fi Protected Setup pushbutton method, if present, MUST be located within close proximity to the pushbutton or next to the Wireless status indicator.

Annex A IPv6 Flow Diagrams

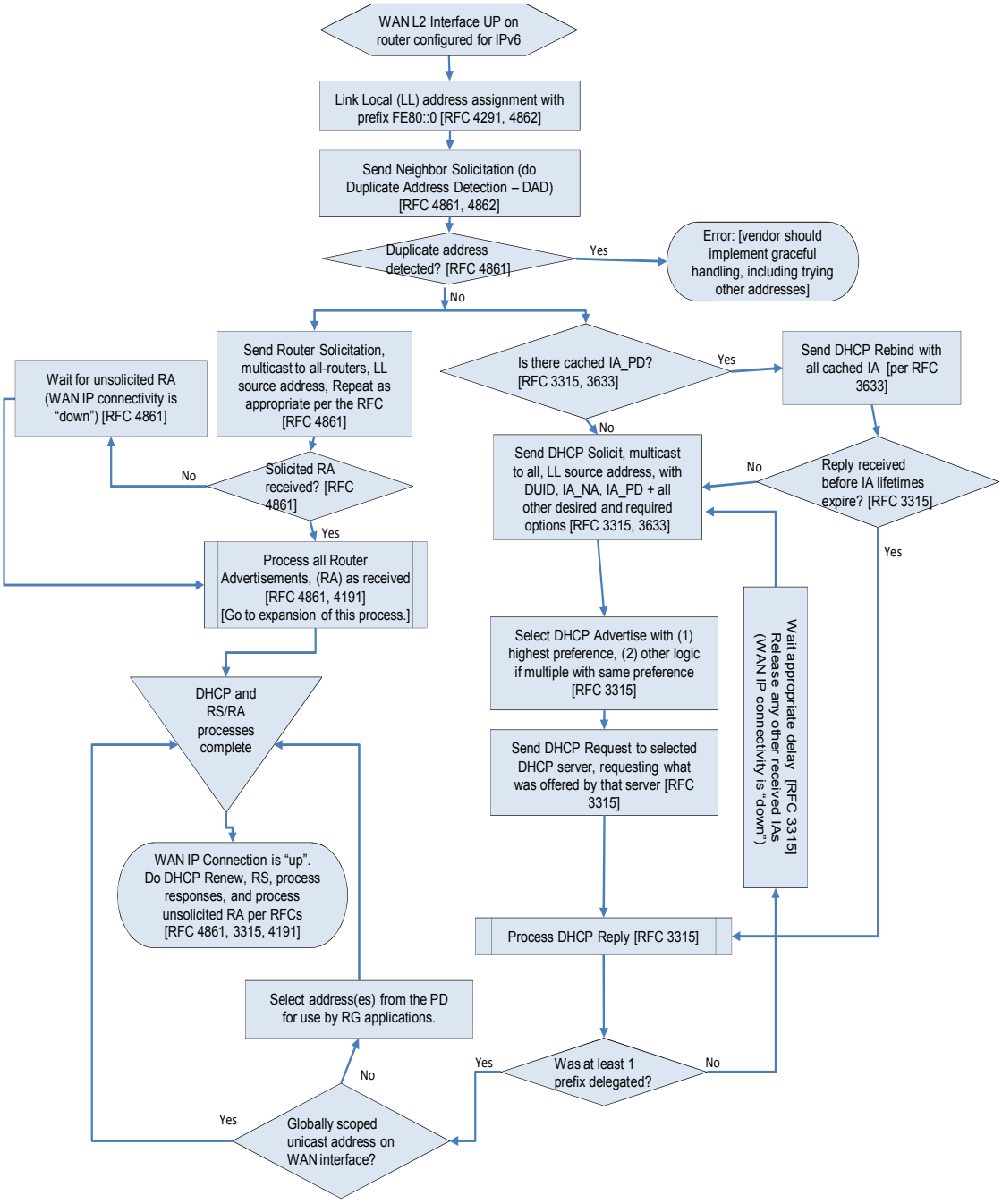
The flows in this annex are referenced by requirements in the body, and are therefore normative.

A.1 WAN PPPoE Automated Connection Flow

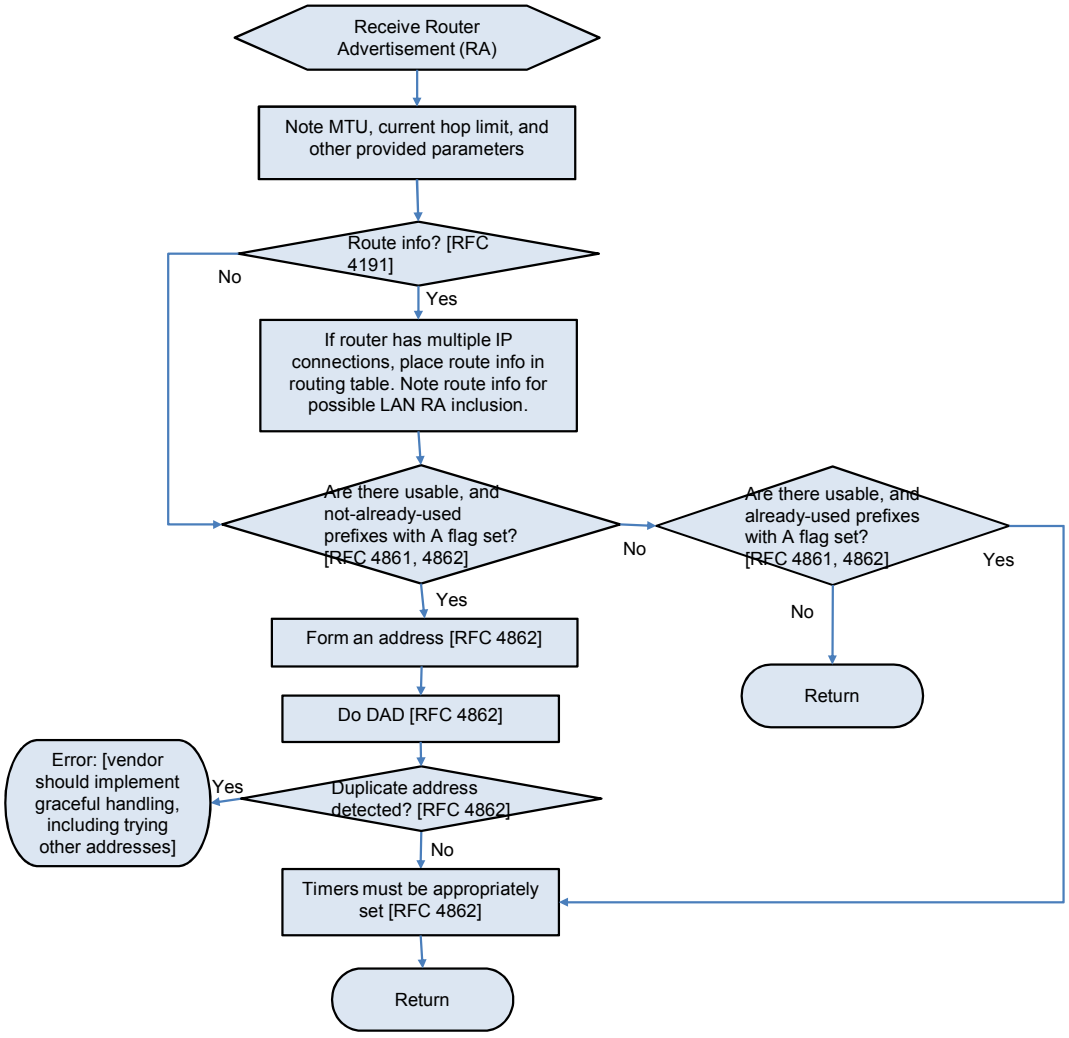


A.2 WAN IPv6 Automated Connection Flow

This flow assumes no manually configured prefix or address.



A.3 Receive Router Advertisement Subroutine Flow



APPENDIX I Application Level Gateway (ALG) and Port Forwarding List

This appendix is a partial list of applications and protocols which should work through the usage of pre-defined port forwarding configurations and ALGs. It is not a comprehensive list of all applications. It is expected that support for more applications will be needed with time.

A

Active Worlds, Age of Empires, Age of Kings, Age of Wonders, Aliens vs. Predator, America Online, Anarchy Online, AOL Instant Messenger, Asheron's Call, Audiogalaxy Satellite

B

Baldur's Gate, BattleCom, Battlefield communicator, Black and White, Buddy Phone

C

Calista IP Phone, Camerades, CarbonCopy32 host, Citrix Metaframe / ICA Client, Counter Strike, CU-SeeMe

D

Dark Reign, Dark Reign 2, Decent 3, Decent Freespace, Deerfield MDaemon EMail Server, Delta Force, Delta Force 2, Delta Force: Land Warrior, Delta Three PC to Phone, Descent 3, Descent Freespace, Diablo (1.07+), Diablo I, Diablo II (Blizzard Battle.net), Dialpad, Direct Connect, DirectX Games, DNS Server, Doom, Doom Server, Drakan, Dwyco Video Conferencing

E

Elite Force, Everquest

F

F-16, Mig 29, F-22, Lightning 3, F-22 Raptor, F-22 Raptor (Novalogic), Falcon 4.0, Fighter Ace II, Figher Ace II for DX play, FlightSim98, FreeTel, FTP Client, FTP Server, FW1VPN

G

GameSpy Online, Ghost Recon, GNUtella, Go2Call

H

H.323, Half Life, Half Life Server, Heretic II Server, Hexen II, HomeWorld, Hotline Client, Hotline Server, HTTP Server, HTTPS Server

I

I'76, ICMP Echo, ICQ Old, ICQ 2001b, ICUII Client, ICUII Client Version 4.xx, iGames, IMAP Client, IMAP Client v.3, IMAP server, Internet Phone, Internet Phone Addressing Server, iPhone, IPSec Encryption, IPSec ESP, IPSec IKE, IRC, IStreamVideo2HP, Ivisit

K

Kali, Doom & Doom II, KaZaA, Kojan Immortal Souvereigns

L

L2TP, LapLink Gold, LapLink HOst, Limewire, LIVvE, LocationFree®, Lotus Notes Server

M

MechWarrior 3, Medal of Honor: Allied Assault, Microsoft DirectPlay, Midtown Madness, mIRC DCC, IRC DCC, mIRC Chat, mIRC IDENT, Monopoly Host, Motocross Madness, Motorhead Server, MPlayer Games Network, MSN Game Zone, MSN Game Zone (DX 7 & 8 play), MSN Messenger, Myth (Bungie.net, Myth II)

N
Napster, Need for Speed 3, Hot Pursuit, Need for Speed 5, Porsche, Net2Phone, NetMech, NetMeeting, Default PC, NNTP Server, Nox, ntald Traditional Unix Talk Daemon, NTP
O
OKWeb, OKWin, Operation FlashPoint, Outlaws
P
Pal Talk, pcAnywhere v7.5, pcAnywhere host, pcAnywhere remote, PCTelecommute, Phone Free, POP Client, POP3 Server, Polycom ViaVideo H.323, PPTP
Q
Quake 2, Quake 3, Quake 3 Server, QuickTime Server, QuickTime/Real Audio Client, QuakeWord,
R
Rainbow Six, RAdmin, RDP, RealAudio, Red Alert, Remote Anything, Remote Desktop 32, Remotely AnyWhere, Remotely Possible Server, Return to Castle Wolfenstein, Rise of Rome, Rlogin/Rcp, Roger Wilco, Rogue Spear, RTSP
S
Scour Media, SDP, Shiva VPN, Shout Cast Server, SIP, Slingbox™, SMTP Server, Soldier of Fortune, Speak Freely, SQL*NET Tools, SSH Secure Shell, SSH Server, StarCraft, Starfleet Command, Starsiege: Tribes, SWAT3
T
Telnet Server, The 4th Coming, Tiberian Sun: Command & Conquor III (& Dune 2000) , Timbuktu Pro, Total Annihilation
U
Ultima Online, Unreal Server, Unreal Tournament, USENET News Service
V
VNC, Virtual Network Computing, VDO Video, VoxChat, VoxPhone 3.0
W
Warbirds 2, Webcam (TrueTech), Webcam32, Webforce Compcore MPEG-1 Player2.0, Web Server, WebPhone 3.0, Westwood Online, C&C, Windows 2000 Terminal Server
X
X Windows, XP Remote Desktop
Y
Yahoo Messenger Chat, Yahoo Pager, Yahoo Messenger Phone
Z
ZNES

APPENDIX II Example Queuing for a DSL Router

This section presents the queuing and scheduling discipline envisioned for upstream traffic through the DSL router in support of future services offerings delivered over the architecture described in TR-059.

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 (Best Effort) treatment is given to the non-IP-aware access sessions (PPPoE started behind the DSL Router 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 $\sum$ 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 of the TR-059 architecture, 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.[1] Such an arrangement would be 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.

[1] 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.

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 IETF RFC 2597)
3. BE – black solid line

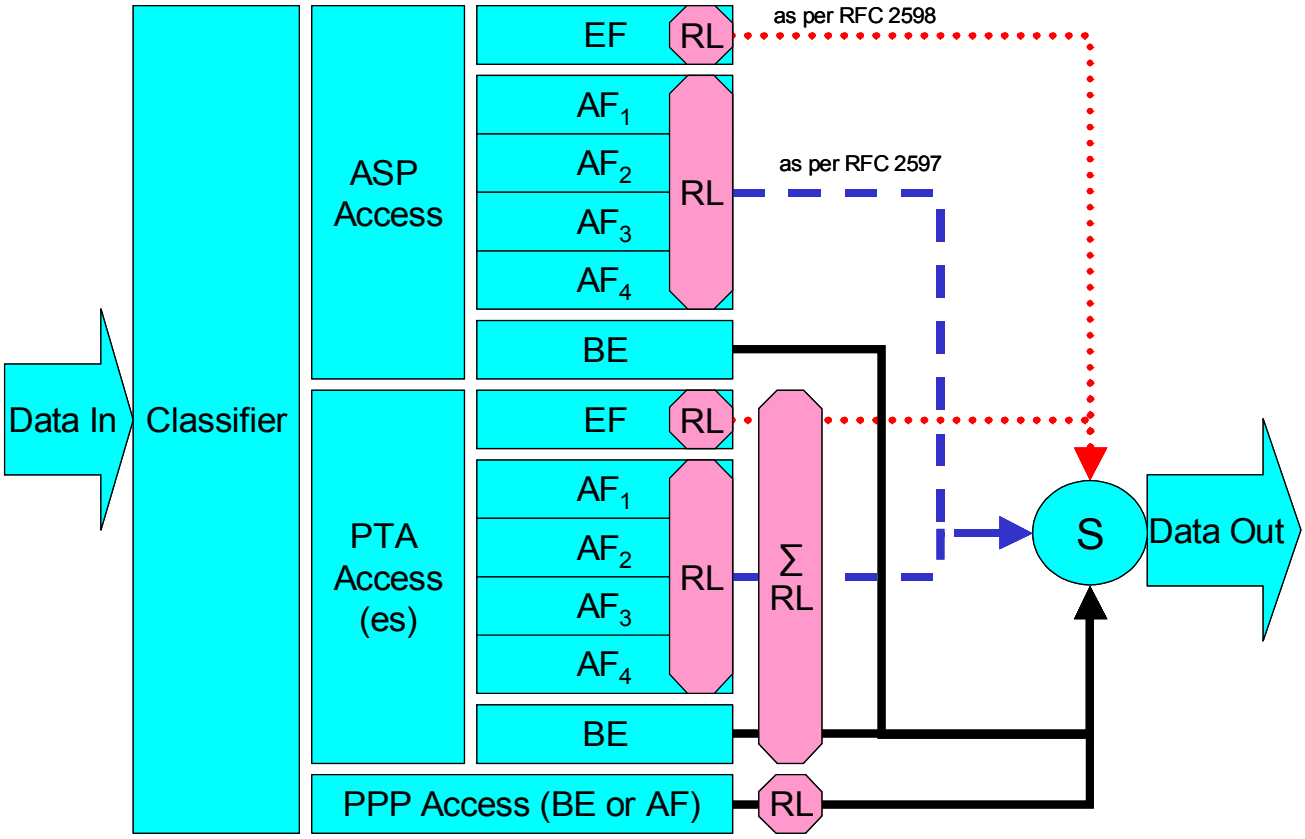


Figure 1 - Queuing and Scheduling Example for DSL Router

In Figure 1 - Queuing and Scheduling Example for DSL Router
the following abbreviations apply:

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

APPENDIX III Routed Architecture – Examples of Potential Configurations

III.1 Introduction

The pictures and descriptions in the following scenarios are intended to provide examples of the interworking of many of the requirements in this document.
Since the single PC case is a simple subset of the multi-PC case (except when explicitly using the single PC mode of operation [LAN.DHCPS.19]), it will not be directly addressed. The network that will be used in this sequence of examples has 5 PCs. They are described as being connected over Ethernet. Naturally, there could easily be wireless, powerline, or phoneline networking used. The actual physical medium is not relevant. The PCs could also be devices other than PCs. That is also not relevant to these scenarios.

III.2 Basic DSL Modem as Router Initiating One or More PPPoE Sessions

The four scenarios that follow build upon one another to describe a number of the capabilities required in this document. They show PPPoE being used in all cases for WAN connectivity, with the embedded DHCP server in the DSL router enabled.

III.2.1 No WAN Connection

- The router has no WAN connection up.
- The router has been configured to give PC2 its WAN address via its embedded DHCP server. Since the router has no WAN connection, it will give PC2 a private address with a 10 minute lease time (as defined in LAN.DHCPS.12).
- PC5 has been configured with a static IP address.
- PCs 1-4 are configured to make DHCP requests. The router responds to all DHCP requests with IP addresses in the range of 192.168.1.64 to 192.168.1.253 [LAN.DHCPS.8], an IP gateway address (and LAN-side address of the device) of 192.168.1.254 [LAN.DHCPS.14], a DNS server address of 192.168.1.254 [LAN.DNS.1] and an IP address lease time for all PCs but PC2 of 24 hours [LAN.DHCPS.11].

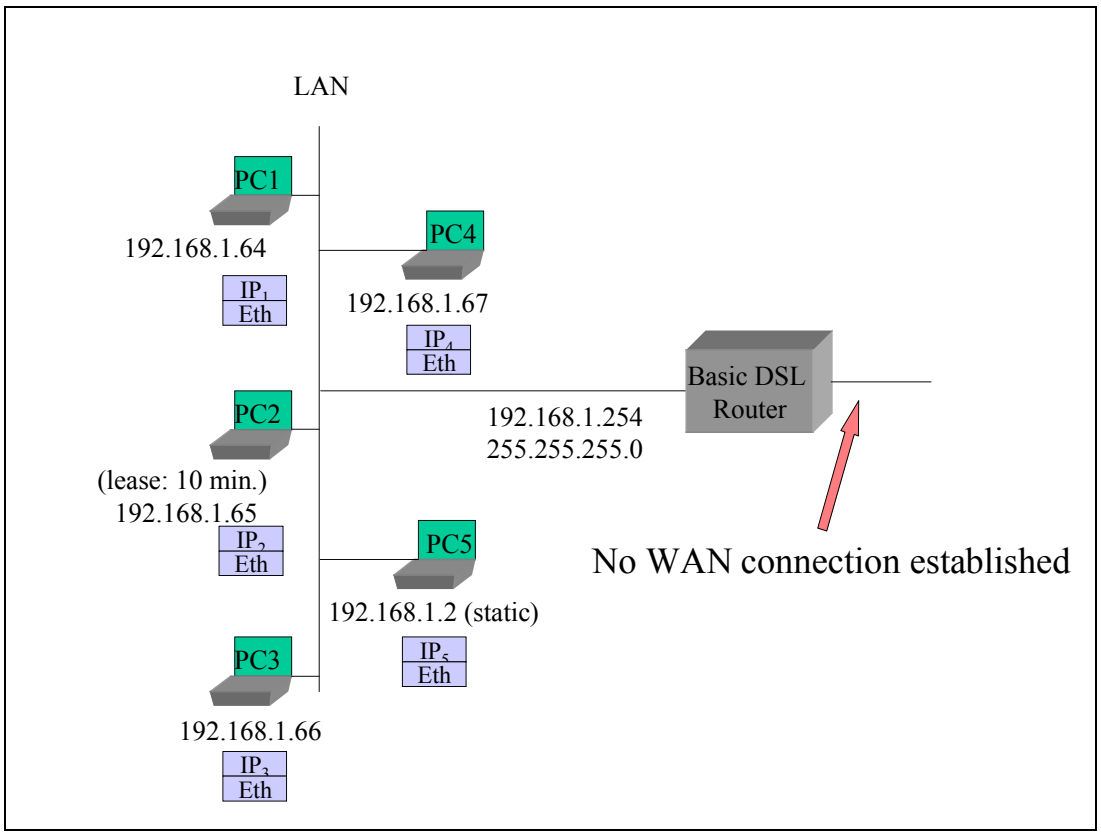


Figure 2 - Example of no WAN Connection Configuration

III.2.2 Router Sets Up PPPoE to an ISP

This scenario is the same as presented in the "No WAN Connection" example above with the following exceptions:

- The router sets up a PPPoE session to ISP – it obtains an IP address and DNS server addresses via IPCP [WAN.PPP.1)
- The router gives its public IP address to PC2 [LAN.DHCPS.18]
- The router is configured to allow PC2 to communicate with other devices on the LAN [LAN.ADDRESS.8].

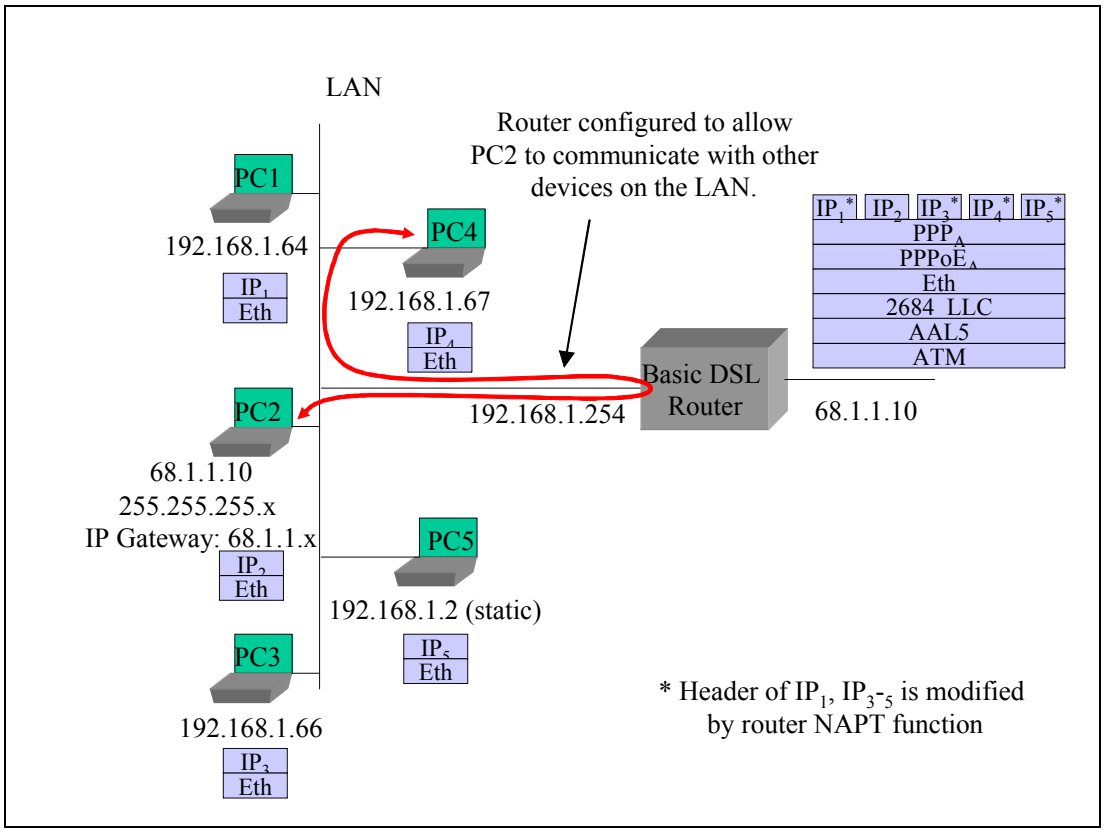


Figure 3 - Example of Router Sets Up PPPoE to an ISP

III.2.3 PC3 Sets Up Its Own PPPoE Session

This scenario is the same as presented in III.2.1 with the following exceptions:

- PC3 uses a PPPoE client to establish its own PPPoE session. While the private IP address from the router is still associated with PC3's Ethernet interface, PC3 also has a public IP address associated with its own PPPoE interface. Common behavior is for all IP traffic of PC3 to now use this PPPoE interface [WAN.PPP.10, LAN.FWD.5].

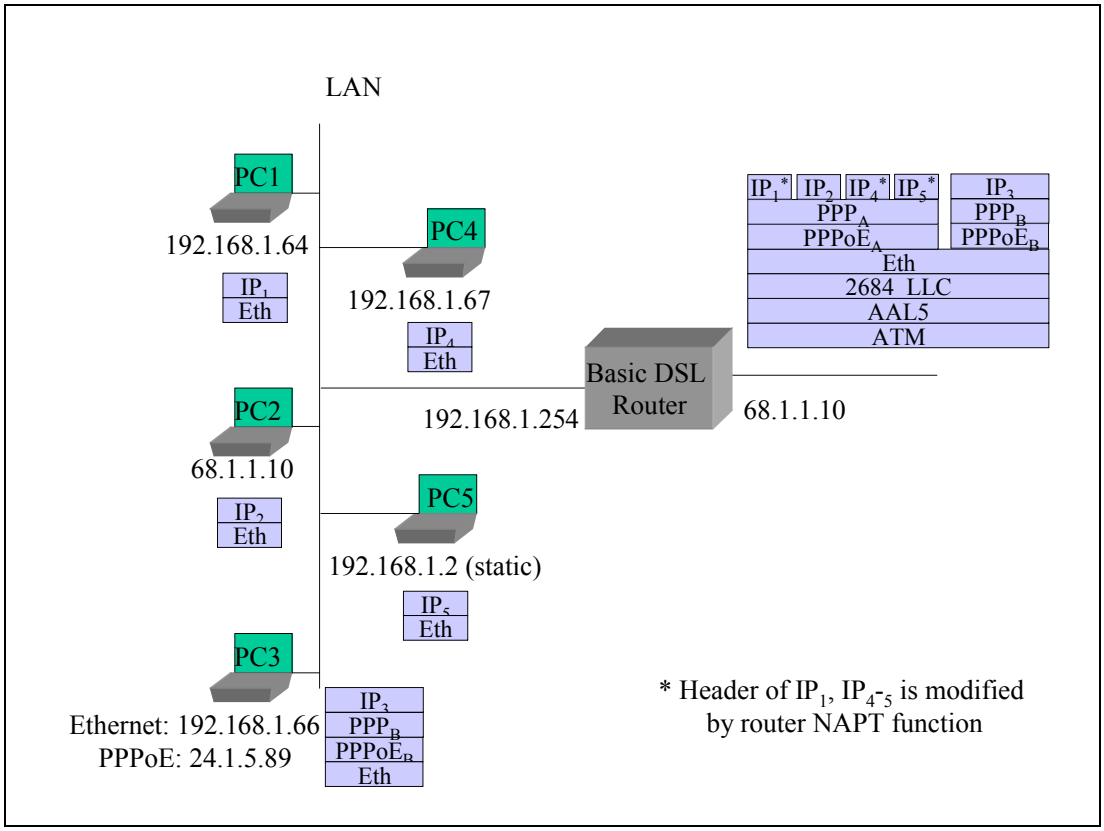


Figure 4 – Example of PC3 Sets Up Its Own PPPoE Session

III.2.4 Router Sets Up a Second PPPoE Session

This scenario is the same as presented in III.2.1 with the following exceptions:

- The router sets up second PPPoE session ($PPPoE_C$). It gets an IP address and DNS addresses through IPCP. It gets routing information from RIP-2 [LAN.FWD.15], manual entry, or other mechanisms [LAN.FWD.8]. $PPPoE_A$ remains the default route [LAN.FWD.20].
- PC5 requests a DNS lookup for a URL. The router sends simultaneous URL lookup requests to DNS servers on both PPPoE connections. The DNS server on the $PPPoE_A$ connection fails to resolve the URL and the $PPPoE_C$ connection returns an IP address. The router returns the IP address to PC5 [LAN.DNS.3].
- PC5 sends IP packets to the returned IP address. The router determines from its routing table that this goes to the $PPPoE_C$ connection.

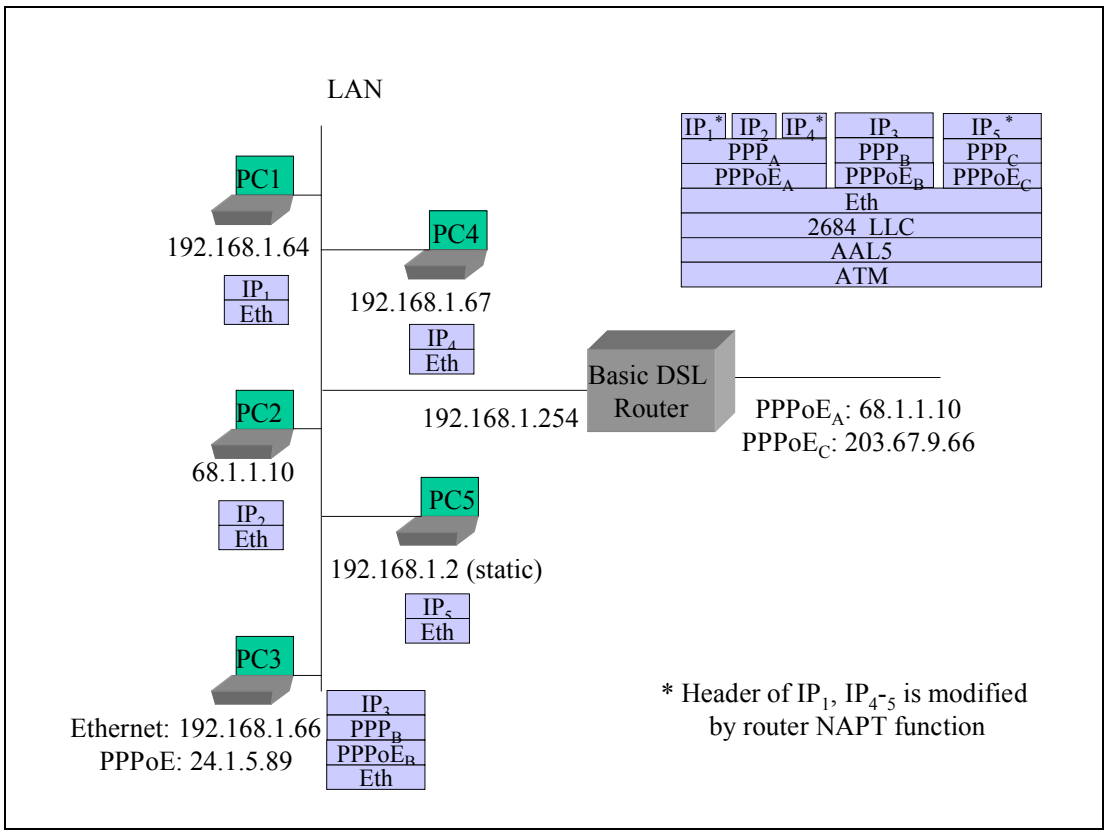


Figure 5 - Example of Router Sets Up a Second PPPoE Session

III.3 "RFC 2684 Bridged" Mode

The next three scenarios deal IETF RFC 2684 Bridged mode configuration cases where the network is not expecting any PPP login or the router is not doing any PPP. The first case has the router using its DHCP client to the WAN, acting as a DHCP server to the LAN, and doing routing and NAPT to PCs on the LAN. The second case has the router not establishing a WAN connection, and individual PCs setting up their own PPPoE sessions. In the third case, the router's embedded DHCP server is also disabled, and the PCs are getting IP addresses from the WAN.

III.3.1 Router in IP-routed "RFC 2684 Bridged" Mode, Embedded DHCP Server On

- The router provides an IP address to each device that it receives a DHCP request from.
- PC5 uses a static IP address and does not send a DHCP request to the router.
- The router has been configured to give PC2 its WAN address. When the router has no WAN connection, it gives PC2 a private address with a short lease time.
- The router issues a DHCP request and establishes an IP session to the WAN [WAN.ATM.3, WAN.ATM.4, LAN.FWD.1.
- The router gives its public IP address to PC2.

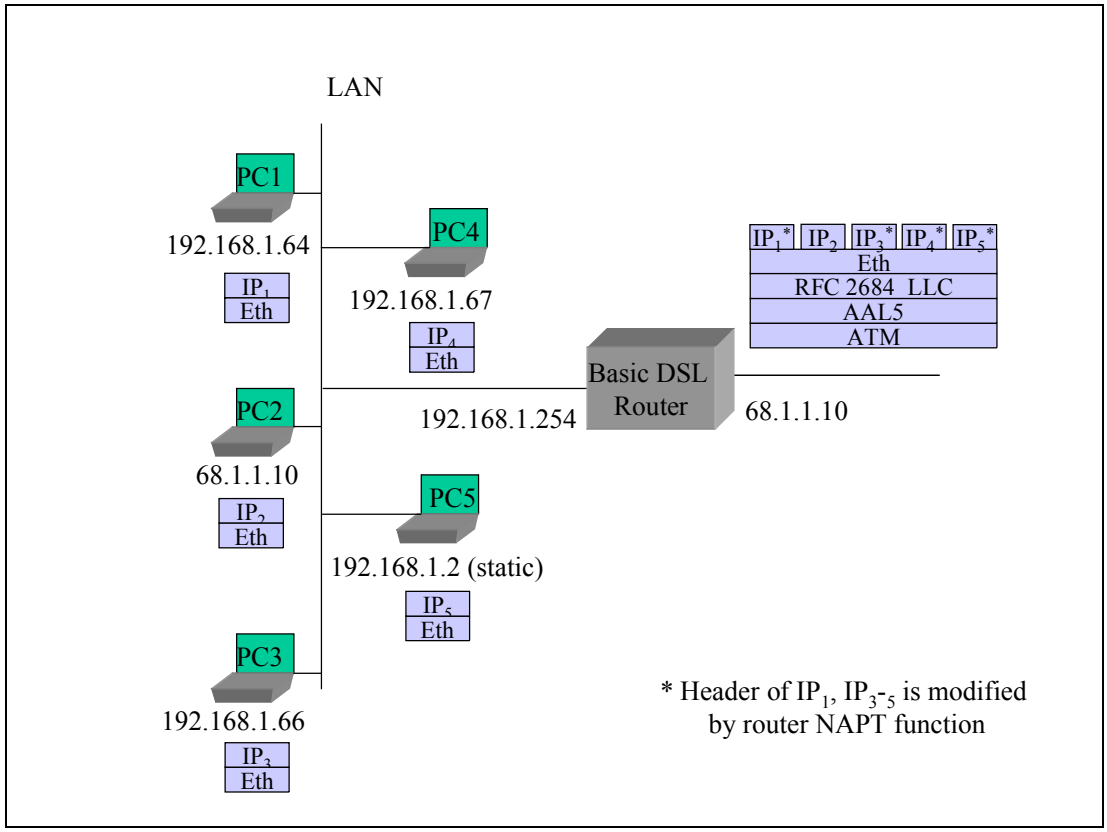


Figure 6 - Example of Router in 2684 Bridged Mode with DHCP Server On

III.3.2 Router in Bridged Mode, Embedded DHCP Server On

- The router provides a private IP address to each device that it receives a DHCP request from [LAN.DHCPS.3].
- The router does not establish any IP or PPP sessions to the WAN.
- No device can get a DHCP response from the WAN, since the router will intercept all DHCP requests that come to it.
- PC1 and PC3 each use a PPPoE client to establish their own PPPoE sessions [WAN.PPP.10, LAN.FWD.5]. While the private IP address from the router is still associated with their PC Ethernet interfaces, PC1 and PC3 also have a public IP address associated with their respective PPPoE interfaces. Common behavior is for all IP traffic of PC1 and PC3 to now use their own PPPoE interfaces.
- PCs that do not establish their own PPPoE connection cannot connect to the WAN, but they can communicate with other PCs on the LAN.

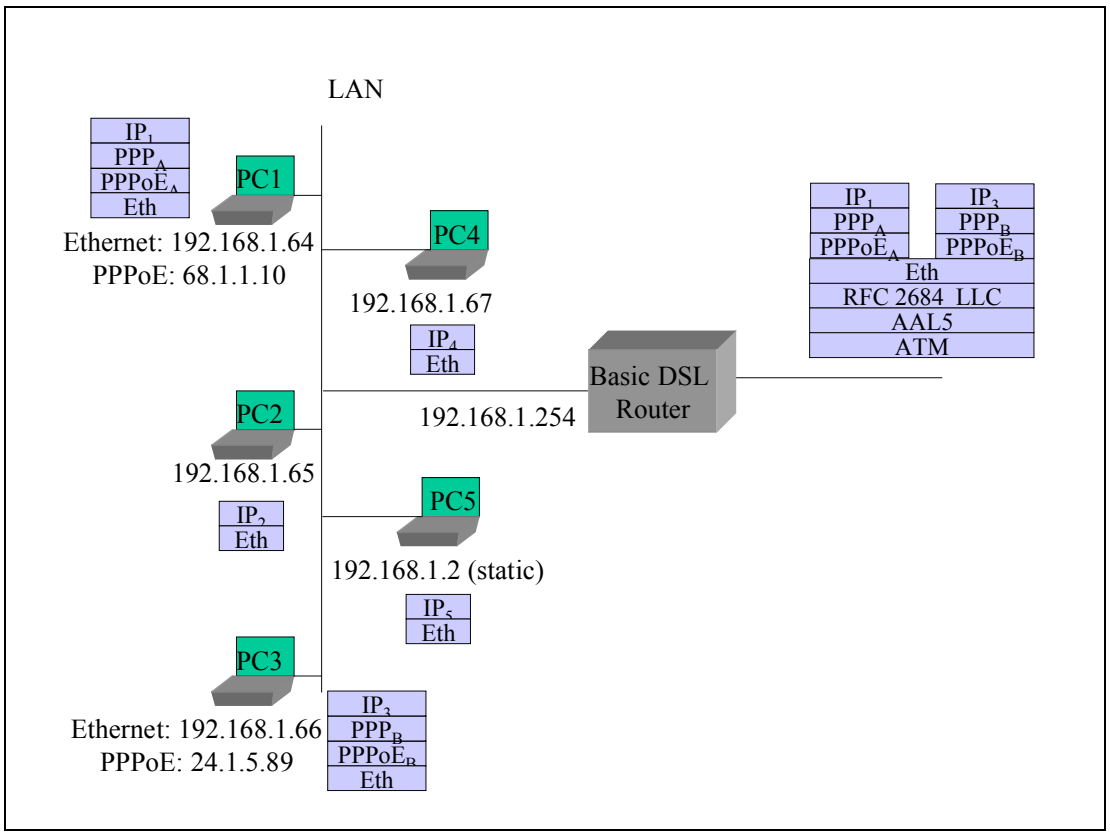


Figure 7 - Example of Router in Bridged Mode with DHCP Server On

III.3.3 Router in Bridged Mode, Embedded DHCP Server Off

- The router does not establish any IP or PPP sessions to the WAN.
- All DHCP requests are bridged on to the WAN [WAN.BRIDGE.1].

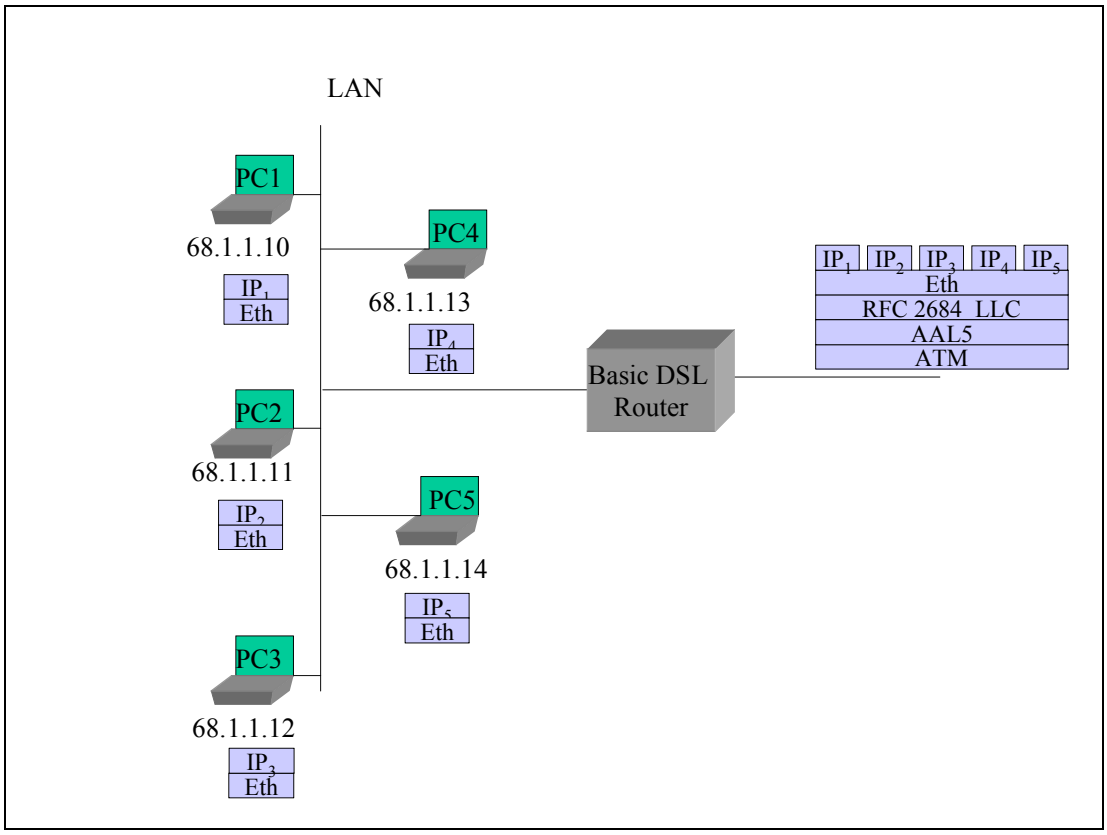


Figure 8 - Example of Router in Bridged Mode with DHCP Server off

III.4 Simultaneous IP and PPPoE WAN Sessions

TR-059 requirements have PPPoE and IP sessions running simultaneously over the same PVC. Here are some examples of how this might look, assuming the network is capable of terminating PPPoE and IP at the same time on the same PVC.
Note: Simultaneous IP and PPPoE is not well supported in the network today. Most equipment terminating the ATM PVC does not support both IP and PPPoE connections at the same time.

III.4.1 Router in IP-routed "2684 Bridged" Mode, Embedded DHCP Server On

- The router provides an IP address to each device that it receives a DHCP request from.
- PC5 uses a static IP address and does not send a DHCP request to the router.
- The router has been configured to give PC2 its WAN address. When the router has no WAN connection, it gives PC2 a private address with a 10 minute lease time.
- The router issues a DHCP request and establishes an IP session to the WAN.
- The router gives its public IP address to PC2.
- PC3 uses a PPPoE client to establish its own PPPoE session [WAN.PPP.10, LAN.FWD.5]. While the private IP address from the router is still associated with PC3's Ethernet interface, PC3 also has a public IP address associated with its own PPPoE interface. Common behavior is for all IP traffic of PC3 to now use this PPPoE interface.

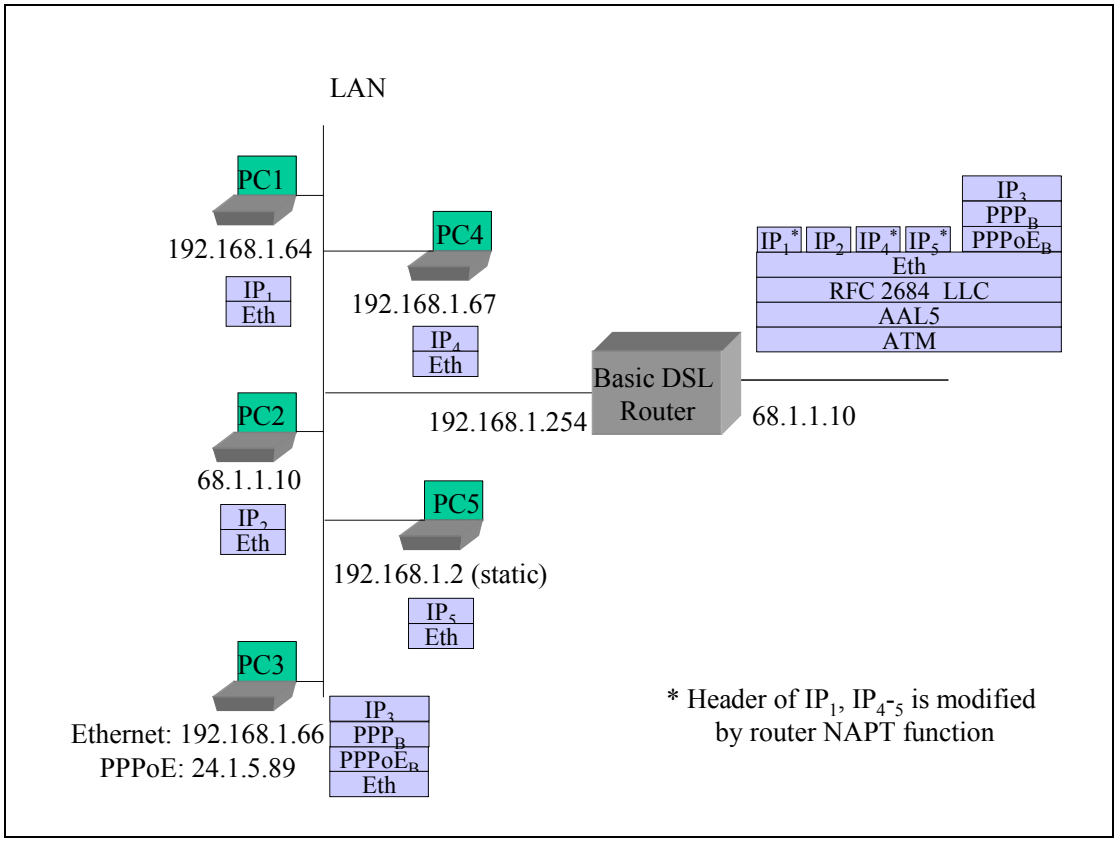


Figure 9 - Example of Router in Routed 2684 Mode

III.4.2 Router Sets Up IP as a Second Session

Assuming the scenario in section III.2.3 as a base, add:

- The router sets up connection IP_C [LAN.FWD.19]. It gets an IP address and DNS addresses through a DHCP client request. It gets routing information from RIP-2 [LAN.FWD.15]. $PPPoE_A$ remains the default route.
- PC5 requests a DNS lookup for a URL. The router sends simultaneous URL lookup requests to DNS servers on both connections. The DNS server on the $PPPoE_A$ connection fails to resolve the URL and the IPC connection returns an IP address. The router returns the IP address to PC5 [LAN.DNS.3].
- PC5 sends IP packets to the returned IP address. The router determines from its routing table that this goes to connection IPC.

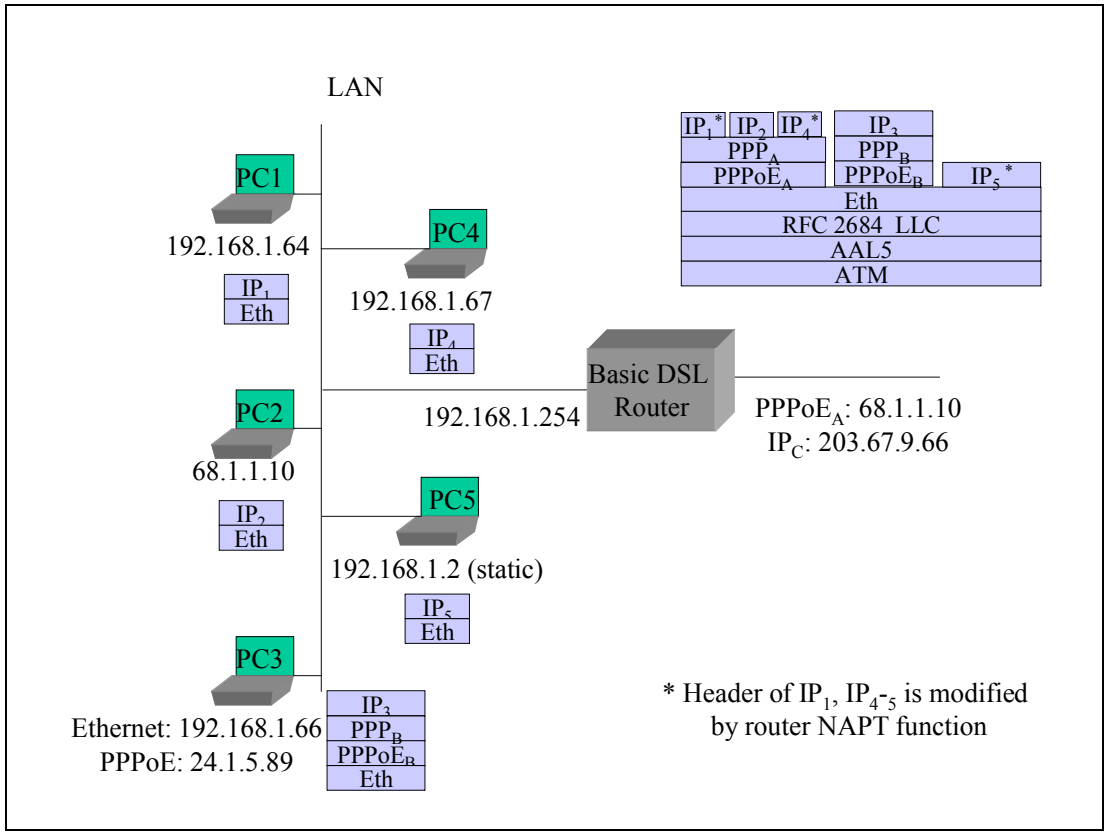


Figure 10 - Example of Router Sets Up Second IP Connection

III.5 Single PC Mode of Operation

- The router is configured to use the single PC mode of operation [LAN.DHCPS.19].
- The router's embedded DHCP server is on. The embedded DHCP server has only one address lease available in this case.
- PC1 is the first device seen, so it is identified as the “single PC”.
- PC1 is provided with a private IP address and 1:1 NAT is performed between the WAN and PC1 by the router. The subnet mask sent to PC1 is 255.255.255.0.
- Alternately PC1 could be given the router’s public address instead, as with PC2 in the scenarios in section III.2.

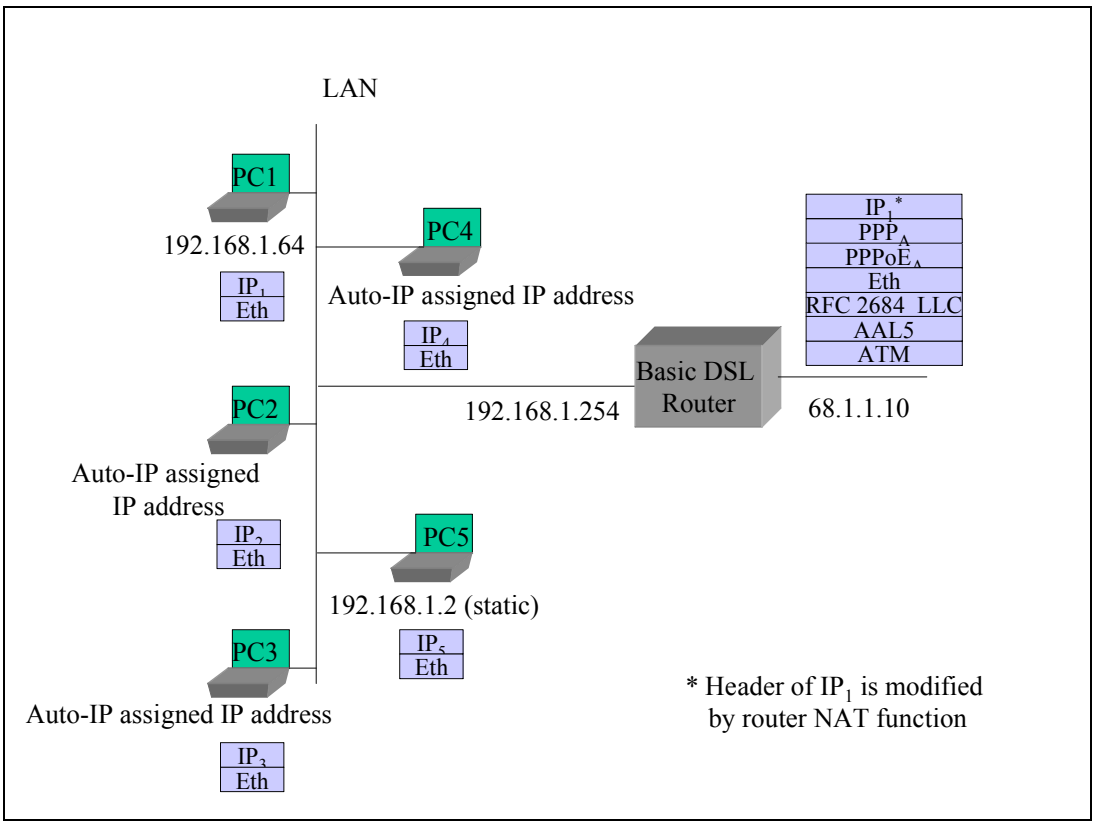


Figure 11 - Example of Single PC Mode of Operation

III.6 Router Embedded DHCP Server Gives Out Public IP Addresses (from use of IPCP extension)

- The router initially gives private IP addresses to PCs, before setting up its PPPoE session.
- The router sets up PPPoE to ISP and gets IP address and DNS server addresses via IPCP. It also gets a subnet mask via an IPCP extension [WAN.DHCPC.1, WAN.PPP.12].
- The router gives public IP addresses to certain PCs when they issue DHCP requests again [LAN.DHCPS.18].
- PC5 is set for static IP and does not issue a DHCP request.

APPENDIX IV Bridged Architecture – Examples of Potential Configurations

IV.1 Introduction

The pictures and descriptions in the following scenarios are intended to provide examples of the bridge interworking of many of the requirements in this document.
The network that will be used in this sequence of examples has 5 PCs. They are described as being connected over Ethernet. Naturally, there could easily be wireless, powerline, or phoneline networking used. The actual physical medium is not relevant. The PCs could also be devices other than PCs. That is also not relevant to these scenarios.

IV.2 Managed Bridge

- The device will have an IP address for management as (described in section WAN.BRIDGE), which is obtained using a DHCP client on the WAN interface. This address can also be used for other gateway originated services such as an attached telephony device.
- The DHCP server of the device is configured with the appropriate IP address range and subnet mask by the ACS.
- The PCs are configured to use DHCP for assignment of an IP address. All DHCP requests from the PCs are processed by the DHCP server (described in section LAN.DHCPS] on the device. Note that the scope of these addresses is specific to the Service Provider network (i.e., they may be public or private depending on the access network design). If private, it is assumed that the Service Provider has the NAT functionality in their network.
- All subsequent data exchanges between the PCs and device are performed using 802.1d bridging techniques (described in section WAN.BRIDGE).
- The device filters specific message types (e.g., UPnP or DHCP) from being sent to the WAN (described in section LAN.FW).

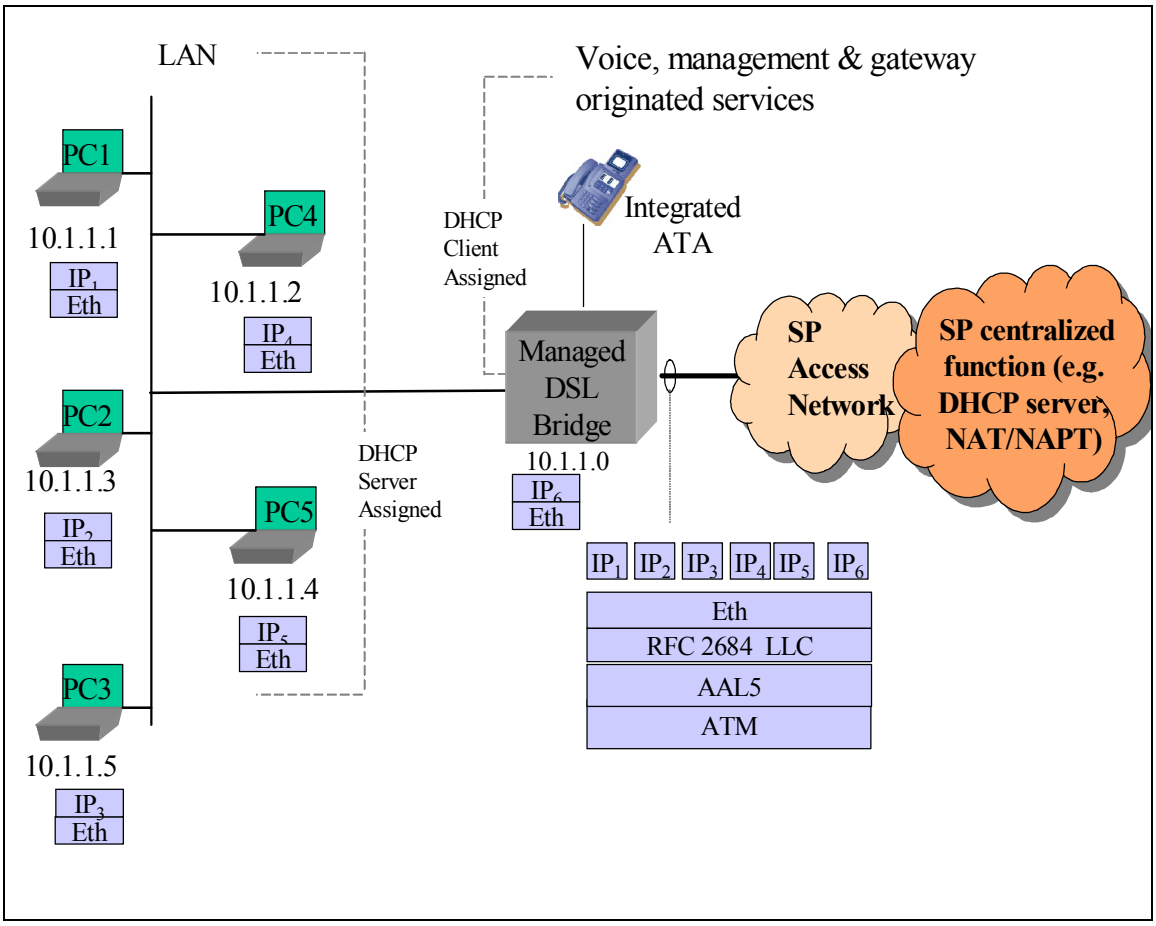


Figure 12 - Example of Managed Bridge Configuration

IV.2.1 Local Management

- The device may allow access to a local management interface via a default address (described in section LAN.ADDRESS).

IV.3 Unmanaged Bridge

- The device does not establish any layer 3 connectivity to the WAN.
- All DHCP requests from the PCs are bridged to the WAN (described in section WAN.BRIDGE).

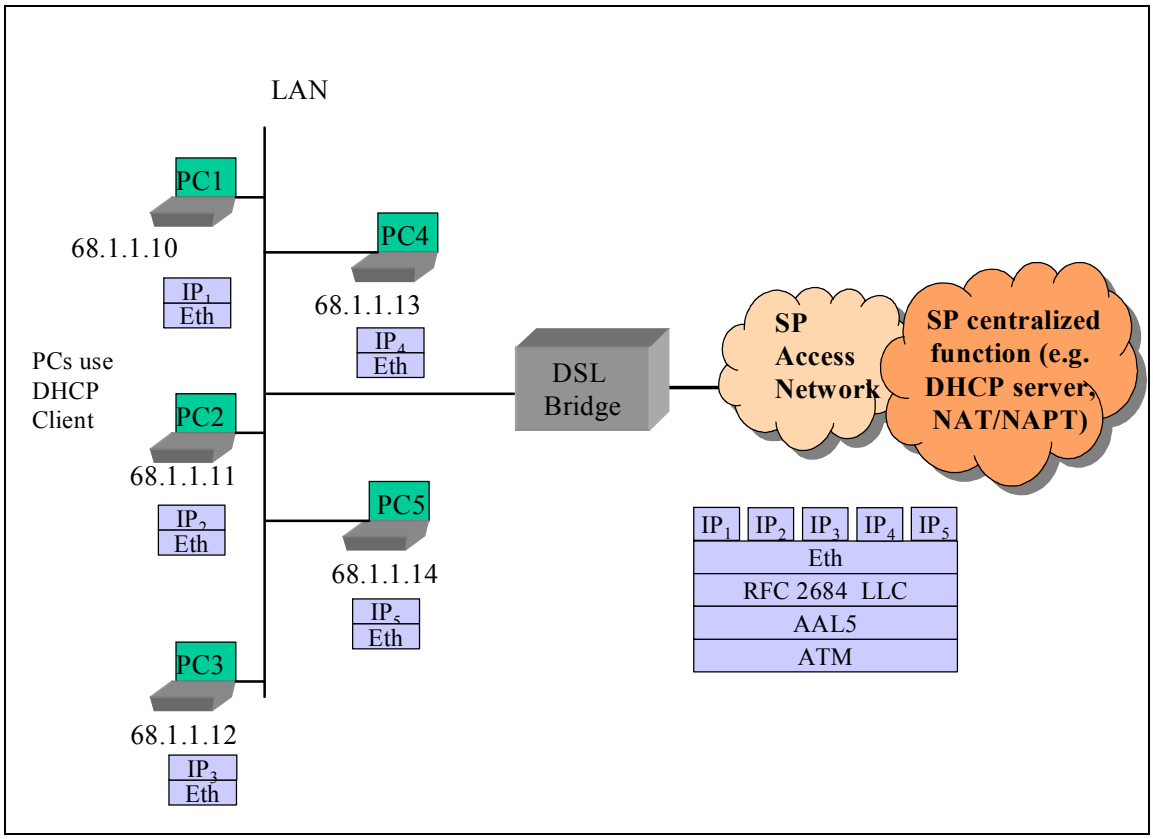


Figure 13 - Example of Unmanaged Bridge Configuration

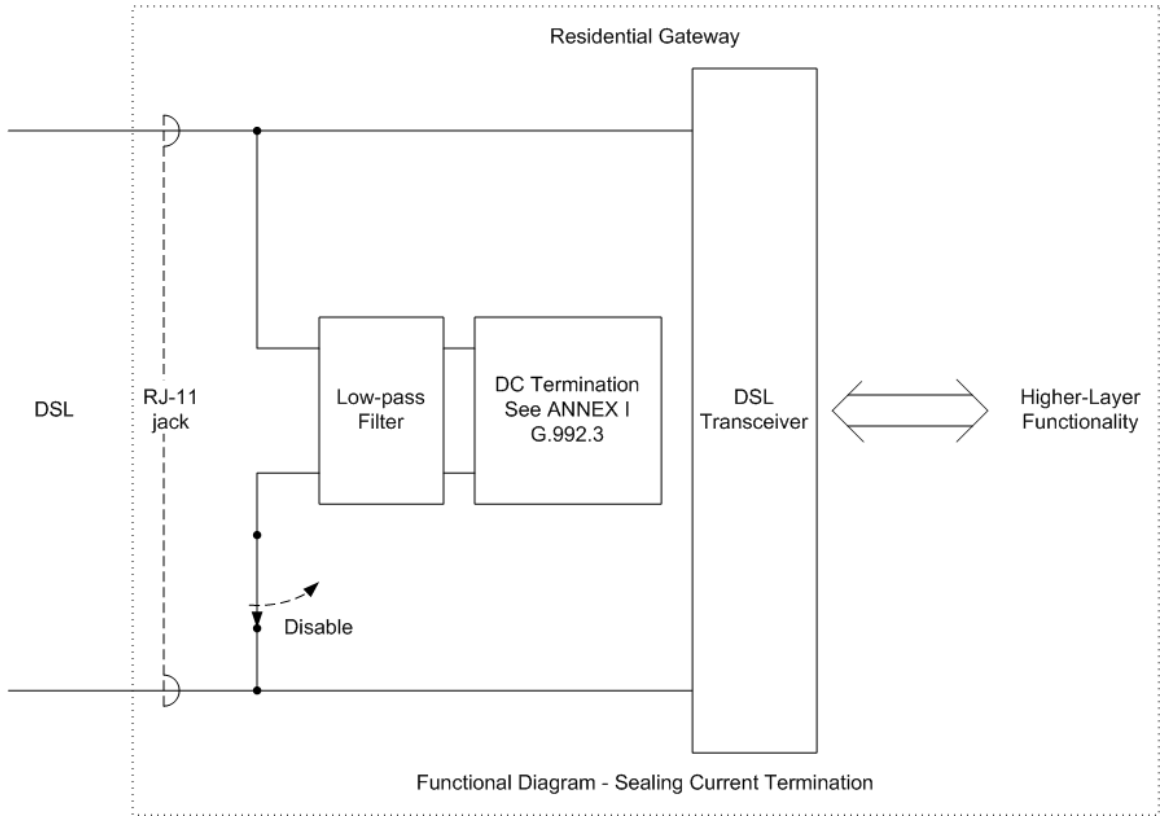
IV.3.1 Local Management

- The device may allow access to a local management interface via a default address (described in section LAN.ADDRESS).

APPENDIX V Sealing Current References

Sealing current is also known in the telecommunications industry as “whetting current” and “wetting current”. Sealing current may be sourced by the ATU-C in certain service providers that deploy “dry loop” DSL circuits, meaning that DSL is being delivered in the absence of typical Central Office or Remote Terminal fed analog POTS service on the copper pair.

The following functional diagram depicts a sealing current circuit design specified in the IF.WAN.SEALING optional module which can be implemented on an xDSL Residential Gateway product.



Functional Diagram - Sealing Current Termination

APPENDIX VI Product Profile Template

VI.1 Introduction

To accommodate the many different Residential Gateway implementations that will be needed due to various localized market needs, LAN/WAN interfaces, and different services that will be delivered in operator's networks, WT-124 endeavors to define a superset of general requirements and optional modules which can be implemented on a Residential Gateway.

In order to create a specific product based on the WT-124 modularized requirements, it is necessary for either the Broadband Forum (in the form of new TR documents) or for individual network operators to specify the following details to define a specific desired product implementation:

1. A filled out product profile matrix template as shown in the example below to indicate required modules
2. Any line item edits to requirements (changes to current WT-124 requirements).
3. Any additional new requirements that are needed in the product.
4. Any configuration defaults needed. These should refer to WT-124 requirements that are establishing a different or new default value required in the implementation.
5. Localized regulatory, certifications, powering and product labeling requirements as necessary.

VI.2 Instructions for Completing a Product Profile Template

The following instructions apply to filling out the product profile template below:

- Any modules marked with a check mark (✓) will be considered required, meaning that all MUST requirements in that section are to be satisfied (with exception of any specific line item edits that have been made as discussed in section VI.1).
- Any modules that are *not* marked with a check MAY be implemented on the product, but are not considered required. Any vendor implementing any module, regardless of being considered required or not, MUST comply with all MUST requirements in the module (i.e., partial implementations of a module MUST NOT be provided).
- If a module is explicitly not to be included in the product, it must be marked with an x mark (✗) to indicate that it MUST NOT be included.
- For the optional LAN/WAN modules, where appropriate it may be necessary to specify the number or ports/lines to be implemented (e.g., "Qty. 4" under the IF.LAN.ETH.SWITCH to indicate 4 ports).

VI.3 Product Profile Template

Section	Title	Required? (✓,×, or blank)
GEN	**General Device Requirements**	
DESIGN	Design	
OPS	Device Operation	
NET	Networking Protocols	
NETv6	IPv6 Networking Protocols	
WAN	**Wide Area Networking (WAN)**	
ATM	ATM	
ATM.MULTI	ATM Multi-PVC	
CONNECT	Connection Establishment	
CONNECT.ON-DEMAND	On-Demand Connection Establishment	
ETHOAM	Ethernet OAM	
BRIDGE	Bridging	
DHCPC	DHCP Client (DHCPv4)	
IPv6	IPv6 WAN Connection	
TRANS	Transitional IPv6 WAN Connection	
TRANS.6rd	6rd Transition Mechanism	
TRANS.DS-LITE	Dual Stack Lite Transition Mechanism	
PPP	PPP Client	
PPP.IPv6	PPP Client for establishment of IPv6 connection	
dot1x	802.1x Client	
DoS	Denial of Service Prevention	
QoS	Quality of Service	
QoS.TUNNEL	Quality of Service for Tunneled Traffic	
LAN	**Local Area Networking (LAN)**	
GEN	General LAN Protocols	
ADDRESS	Private IPv4 Addressing	
ADDRESSv6	LAN IPv6 Addressing	
DHCPS	DHCPv4 Server	
DHCPv6S	DHCPv6 Server	
DNS	Naming Services (IPv4 and general requirements)	
DNSv6	Naming Services (IPv6)	
NAT	NAT/NATP	
PFWD	Port Forwarding (IPv4)	
PFWDv6	Port Forwarding (IPv6)	
ALG	ALG Functions (IPv4)	
FWD	Connection Forwarding	
IGMP.BRIDGED	IGMP and Multicast in Bridged Configurations (IPv4)	
IGMP.ROUTED	IGMP and Multicast in Routed Configurations (IPv4)	
MLD.ROUTED	MLD and Multicast in Routed Configurations (IPv6)	
FW	Firewall (Basic)	

FW.SPI	Firewall (Advanced)	
FILTER.TIME	Time of Day Filtering	
FILTER.CONTENT	Content Filtering	
DIAGNOSTICS	Automated User Diagnostics	
CAPTIVE	Captive Portal with Web Redirection	
MGMT	**Management & Diagnostics**	
GEN	General	
UPnP	UPnP	
UPnP.IGD	UPnP IGD	
LOCAL	Local Management	
REMOTE.TR-069	Remote Management (TR-069)	
REMOTE.WEB	Remote Management (Web Browser)	
NTP	Network Time Client	
IF.WAN	**WAN Interface Modules**	Enter Quantity
ADSL	ADSL and ADSL2+	
VDSL2	VDSL2	
xDSL	xDSL General Requirements	
xDSL.INP	xDSL INP Values	
xDSL.BOND	xDSL Bonding	
xDSL.REPORT	xDSL Reporting of Physical Layer Issues	
xDSL.SEALING	DC Sealing Current	
xDSL.SURGE	AC Power Surge Protection	
ETH	Ethernet (WAN)	
GPON	GPON	
MoCA	MoCA (WAN)	
IF.LAN	**LAN Interface Modules**	Enter Quantity
ETH	Ethernet (LAN)	
ETH.SWITCH	Ethernet Switch	
USB.PC	USB (PC)	
VOICE.ATA	Voice ATA Ports	
WIRELESS.AP	Wireless: General Access Point Functions	
WIRELESS.11g	Wireless: 802.11g Access Point	
WIRELESS.11a	Wireless: 802.11a Access Point	
WIRELESS.11h	Wireless: 802.11h Access Point	
HomePNA	HomePNA (Phoneline/Coax)	
MoCA	MoCA (LAN)	
HomePlugAV	HomePlug AV (LAN)	
REGIONAL	**Regional Annexes**	
NA.POWER	North American Power and Environmental	
NA.LED	North American LED Indicators	

End of Broadband Forum Technical Report TR-124

