TECHNICAL REPORT

TR-068
Base Requirements for an ADSL Modem with Routing

Issue: 2.0

Issue Date: March 2005

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 DOCUMENTATION 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.

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

Editors	Barbara Stark	BellSouth
DSLHome-Technical ™ Working Group Chairs	Greg Bathrick	Texas Instruments
	George Pitsoulakis	Westell

Abstract:

This Working Text will specify requirements for an ADSL modem with embedded router functionality that can be deployed through retail stores and then configured for customer use by service providers. These requirements will lead to retail devices that can provide customers with consistent features, connectivity and operation.
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. However, these requirements do not fully complement the capabilities specified in TR-059.

Table of Contents

1 SCOPE AND PURPOSE

1.1 Scope

The document presents base requirements for an ADSL modem with embedded router functionality that can be deployed through retail stores and then configured for customer use by service providers. These requirements will lead to retail devices that can provide customers with consistent features, connectivity and operation.

These requirements specify a minimum set of features. It is expected that devices will include these in a superset of features (e.g., wireless, power line, 1394b, firewall, etc…).

These requirements are both backward and forward-looking. They attempt to address the needs of current DSL service and architectures as well as starting to address future needs. Some requirements have been included in support of TR-059, and are marked as [TR-059]. Any CPE that claims to be compliant with TR-059 must meet these requirements. It is understood that CPE that does not claim to be TR-059 compliant may not meet these requirements.

1.2 Requirements

In this document, several words are used to signify the relative importance of the specified requirements.

MUST This word, or the adjective "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 must be understood and carefully weighted before choosing a different course.

MAY This word, or the adjective "OPTIONAL", means that this item is one which vendors may readily implement. Other modem features not identified in this document may also be implemented in the modem and are equivalent to the MAY value.

Throughout this document, the ADSL modem is referred to as "the device". References to CPE indicate other equipment such as hosts including PC and workstations.

Requirements which are in support of TR-059 start with [TR-059].

Requirements which are specific to North America start with [North America].

2 MODEM REQUIREMENTS

2.1 Physical and Power

I - 1 The device **MUST** be compact and have a physical profile suitable for desktop.

I - 2 The device **SHOULD** be able to be wall mounted and stand on its side.

I - 3 The device **MAY** have the ability to be mounted horizontally or vertically.

I - 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.

I - 5 A detachable wall-mounting bracket **MAY** be added to the device.

I - 6 If the device can be wall mounted, specifications for screws and a template **SHOULD** be included with the device.

I - 7 [North America] The device **MUST** be UL 60950 listed. This is the most recent replacement for UL 1950.

I - 8 [North America] 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.

I - 9 [North America] The device **MUST** have the following electrical characteristics:

Voltage: 105 - 125 VAC @ 60 Hz

I - 10 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.

I - 11 [North America] If the power supply is external to the modem, it **MUST** be UL 1310 or UL 60950 listed and certified.

I - 12 If the power supply is external to the device, it **SHOULD** be labeled with the DSL device vendor's name and the model number of the ADSL device.

I - 13 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.

I - 14 If the power cable includes an analog to digital conversion brick, that brick **MAY** have a light on it.

I - 15 The device **MUST** have an on/off switch. This switch **MUST** be positioned on the device in such a manner as to prevent accidental switching.

I - 16 The Device **SHOULD** be tolerant of power fluctuations and brown-outs, continuing to operate normally and maintaining its configuration after these events.

I - 17 If the on/off switch is labeled, it **SHOULD** be labeled "ON/OFF".

I - 18 The device **MAY** be provided with a standby switch on the front, to stop or allow traffic to flow between WAN and LAN connections, without switching the device off and on.

I - 19 The device **SHOULD** be able to detect faults and reset appropriately upon detection.

I - 20 The device **MUST NOT** be USB powered.

I - 21 The device **MUST NOT** use the local phone loop for power.

I - 22 The device **MUST** have the following indicator lights:

`Power  Ethernet  DSL  Internet`

I - 23 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).

I - 24 [North America] The indicator lights **MUST** be labeled and in the order as indicated in I - 22 in a left to right or top to bottom orientation.

I - 25 [North America] Port indicator lights not identified in I - 22 **MUST** be placed between the "Ethernet" and "DSL" lights and labeled (order and text) as identified in I - 23.

I - 26 All port indicator lights **MUST** be located on the front of the device unless summary indicator lights are used.

I - 27 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.

I - 28 The indicator lights **MUST** be readily visible (99% human observer detection in less than 250 milliseconds) at 12 feet with an ambient illumination level of 550 foot-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.

I - 29 When flashing, the indicator lights **MUST** flash at 4 Hz with a duty cycle of 50% (except as specified otherwise in this document).

I - 30 The device **MUST** have a “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 DSLAM 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.

I - 31 The device **MUST** have an indicator light that indicates ADSL layer connectivity. This indicator **MUST** function as follows:

Solid Green	=	DSL good sync
Off	=	Modem power off
Flashing Green	=	DSL attempting sync 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 the modem is trying to train

I - 32 The device **MUST** have an Internet indicator light that indicates whether or not it has at least one DSL device-controlled session up.

This indicator **MUST** function as follows:

Solid Green	=	IP connected (the device has a WAN IP address from IPCP or DHCP and DSL is up or a static IP address is configured, PPP negotiation has successfully complete – if used – and DSL 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	=	Modem power off, modem in bridged mode or ADSL 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 DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)

For bridged mode, the indicator light **MUST** be off.

I - 33 The physical port indicator lamps **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.

I - 34 The device **MUST** have a single function, recessed button with a red circle around it, in order to reset the device to the default factory settings.

I - 35 The reset button on the device **MAY** be labeled as "reset" so a help desk can more easily identify it to a user.

I - 36 Each port on the back of the device **MAY** have an icon displayed near it identifying the type of port.

I - 37 The ports on the device **MUST** be identified by color with the appropriate connection/interface color reflected above, below or around each port.

The ports **MUST** be colored as follows:

- Ethernet Yellow
- Power Black
- Phone Grey
- USB Blue

The preferred Pantone colors for blue and yellow are:

- Blue 285C
- Yellow 114C
- Gray Cool Gray 3U (matte)

I - 38 Each port on the back of the device **MUST** be labeled using icons and/or words, and any words must be spelled out completely (e.g., “Ethernet”, “Power”, …).

I - 39 The device **MUST** operate 24 hours a day, 7 days a week without the need to reboot.

I - 40 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).

I - 41 The life expectancy of the device **SHOULD** be at least seven years.

I - 42 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.

I - 43 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").

I - 44 The device **MUST** complete training within 60 seconds when autosensing is not activated (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"). The default inner pair shall be used for this measurement.

I - 45 The device **MUST** complete training within 60 seconds when autosensing is activated and ADSL is present on the default pair. The device **MUST** complete training within 120 seconds when autosensing is activated and ADSL is not present on the default pair.

I - 46 [North America] The device **MUST** comply with FCC Part 15 rules for Class B devices.

I - 47 [North America] The device **MUST** comply with Industry Canada ICES-003 Class B requirements.

I - 48 [North America] The device **MUST** comply with Industry Canada's "Telecommunication Apparatus Compliance Specification" (IC document CS-03) and be registered with Industry Canada following the procedures highlighted in Industry Canada's "Procedure for Declaration of Conformity and Registration of Terminal Equipment" document (IC document DC-01).

I - 49 [North America] The device **MUST** be certified to meet FCC Part 68, or obtain the appropriate waiver.

I - 50 [North America] The device **MUST** comply with either:

- TIA-968-A, Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment to the Telephone Network, October 2002,

or both:

- TIA/EIA/IS-968, Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment to the Telephone Network, July 2001, and
- TIA/EIA/IS-883, Telecommunications - Telephone Terminal Equipment - Supplemental Technical Requirements for Connection of Stutter Dial Tone Detection Devices and ADSL modems to the Telephone Network, June 2001

I - 51 [North America] The device **MUST** comply with the requirements of Telcordia™ GR-1089-CORE, Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment.

I - 52 [North America] The device **MUST** support the following environmental conditions:

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

I - 53 This device **MUST** preserve local configuration information during power-off and power interruption.

2.2 WAN: ADSL and ATM

I - 54 The device **MUST** include an internal ADSL modem.

I - 55 The device **MUST** comply with requirements as specified in ANSI T1.413-1998, ANSI T1.413a-2001 and ITU 992.1.

I - 56 The device **MUST** support FDM-mode per ANSI T1.413 and ITU-T G.992.1.

I - 57 The device **SHOULD** comply with ITU G.992.3 (ADSL2) and ITU G.992.5 (ADSL2+) by 6/1/2004.

I - 58 The device **SHOULD** comply with ITU G992.3 Annex L (RE-ADSL2) within three months after its approval.

I - 59 The device **SHOULD** comply with ITU G992.5 Annex L (ADSL2) within three months after its approval.

I - 60 The device **MUST** support Trellis coding.

I - 61 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.

I - 62 The device **MUST** only synchronize within the minimum and maximum line rate parameters for a line as identified by the DSLAM or RT.

I - 63 The device **MUST** support dynamic rate adaptation.

I - 64 The device **MUST** support independent upstream and downstream data rate provisioning.

I - 65 The device **MUST** support bit swapping.

I - 66 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).

I - 67 The device **MUST** have a high-pass filter at its ADSL line input to eliminate impulse noise from premises wiring.

I - 68 The device **SHOULD NOT** incorporate an internal splitter (i.e., **SHOULD NOT** have a POTS pass back port).

I - 69 A failure in the device **MUST NOT** impact the private intra-premises network except for those functions provided by the device (i.e. DHCP, DNS, etc.).

I - 70 The device **MUST NOT** cause any failure in or interference with the ADSL network.

I - 71 The default pair used to detect the ADSL signal **MUST** be the inner pair (pins 3 & 4).

I - 72 The device **SHOULD** 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 autosensing, 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 autosensing will be activated with the new default pair.

I - 73 If I - 72 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.

I - 74 Removing AC power from the device **MUST NOT** prohibit POTS from operating.

I - 75 The CRC **MUST** conform to ANSI T1.413-1998 section 7.4.1.3.

I - 76 The device performance and throughput **MUST** keep up with the DSL line rate.

I - 77 Failure or removal of LAN CPE connected to the DSL device **MUST NOT** prohibit POTS from operating.

I - 78 The device **MUST** support standard ATM (AAL5) payload format.

I - 79 The device **MUST** perform AAL Segmentation and Reassembly (SAR), Convergence Sublayer (CS) functions and CRC check.

I - 80 PCR shaping **MUST** be provided in the upstream direction when the interface between the PC and the device has more bandwidth than the ADSL connection provides.

I - 81 The device **MUST** support ATM QoS. UBR, CBR and VBR-rt **MUST** be supported (as defined in The ATM Forum Traffic Management Specification Version 4.1).

I - 82 VBR-nrt and UBR with per VC queuing **SHOULD** be supported.

I - 83 The default ATM QoS for all VC's **MUST** be UBR.

I - 84 The device **MUST** support multiple levels of QoS listed above simultaneously across separate VCCs (e.g., UBR for PVC 0/35 and CBR for PVC 0/43 where both PVCs are active simultaneously).

I - 85 The device **SHOULD** support auto configuration as defined in The Broadband Forum TR-037 and ILMI 4.0 and its extensions.

I - 86 The device **MUST** always respond to ATM testing, pings and loopbacks according to ITU-T I.610 (F4, F5).

I - 87 The device **MUST** support 0/35 as the default VPI/VCI for the first PVC.

I - 88 The device **MUST** be able to perform an auto search for the VPI/VCI settings for the first PVC. This search **MUST** be the following VPI/VCI's in sequence looking for a first-success: 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, 8/59.

The default VPI/VCI identified in I - 87 is searched prior to this auto search list.

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 will be set to the newly discovered values. The new default pair is stored on the modem across power off situations. If an ATM connection cannot be established after a power restoral, the search process starts over again.

I - 89 The device **MUST** be configurable so that the auto-search mechanism can be disabled.

I - 90 The device **MUST** allow the auto-search list to be redefined using the XML based interface.

I - 91 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.

I - 92 The device **MUST** support VPI values from 0 to 255

I - 93 The device **MUST** support VCI values from 32 to 65535

I - 94 The device **MUST** pass the tests identified in The 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.

I - 95 The device **MUST** train and pass data against all ITU 992.1 based ATU-C deployed in North America using TR-048 (and future updates).

2.3 Multiple PVCs

I - 96 The device **MUST** support eight PVCs.

I - 97 There is no default defined VPI/VCI past the first PVC which is identified in I - 87 above. Auto-search is supported on all PVCs and will use the same auto-search sequence identified (skipping over any already in use). This auto-search is defined in I - 88 through I - 90.

I - 98 All supported PVCs **MUST NOT** require the same VPI value.

I - 99 All supported PVCs **MUST** be able to be active and sending/receiving traffic simultaneously. See I - 119, I - 120, I - 210 and I - 211 for more details on interface selection for routing.

I - 100 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.

2.4 WAN: Access Protocols

I - 101 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.

I - 102 The device **MUST** support Ethernet (IEEE 802.3).

I - 103 The device **MUST** support encapsulation of bridged Ethernet over AAL5 (without FCS) as described in IETF RFC 2684 (formerly IETF RFC 1483).

I - 104 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.

I - 105 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)

I - 106 The device **MUST** support IP over the encapsulated Ethernet.

I - 107 The device **MUST** be able to bridge IP over Ethernet.

I - 108 The device **MUST** be able to route IP over Ethernet to LAN CPE.

I - 109 The device **MAY** support encapsulation of IP over AAL5, per IETF RFC 2684.

I - 110 If the device supports IP over AAL5, it **MAY** support Classical IP according to IETF RFC 2225.

I - 111 The device **MUST** include built-in PPPoE client functionality.

I - 112 [TR-059] The device **MUST** be capable of initiating at least two PPPoE sessions per PVC and route the IP traffic above that to the LAN CPE.

I - 113 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.

I - 114 The device **MUST** support PPPoE over the encapsulated Ethernet as defined in IETF RFC 2516.

I - 115 The device **MUST** support mini-jumbo frames when bridging Ethernet over AAL5 such that it will be possible to allow establishment of PPPoE protocols from the device with ultimate 1500 byte Ethernet or IP payloads.

For example, in the PPPoE case the WAN side encapsulations would be:

WAN (ATM CPCS-PDU payload)

	Ethernet Header (bytes)	PPPoE header (bytes)	PPP protocol id (bytes)	IP Data (bytes)	Total Bytes
1500 Byte Ethernet (with LLC/SNAP)	26	6	2	38 - 1492	72 - 1526
1500 Byte IP (over Ethernet with LLC/SNAP)	26	6	2	38 – 1500	72 – 1534

I - 116 The device **MUST** support manually setting, through the GUI and XML interfaces, an MTU to be used in negotiating MTU, overriding the default MTU.

I - 117 The device **MUST** support PPP and the associated protocols identified below:

- IETF RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- IETF RFC 1334 PPP Authentication Protocols (PAP)

- IETF RFC 1661 The Point-to-Point Protocol (PPP)
- IETF RFC 1877 PPP IPCP Extensions for Name Server Addresses (limited to DNS addresses unless the device supports NetBIOS)

- IETF RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)

I - 118 The device **MUST** support the following:

- IETF RFC 1570 PPP LCP Extensions

- IETF RFC 2153 PPP Vendor Extensions

This is not stating that specific extensions **MUST** be supported. It is identifying that upon receipt of non-standard or unrecognized PPP extensions from the DSL network (e.g., vendor or proprietary), the device **MUST** operate without fault.

I - 119 [TR-059] 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) destination IP address(es) with subnet mask,

(2) originating IP 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.

I - 120 [TR-059] The device **SHOULD** 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.

I - 121 [TR-059] The device **MUST** be able to bridge or route IP over an Ethernet session concurrently with at least one device-originated PPPoE session on each PVC that is running bridged Ethernet over the AAL.

I - 122 The device **MUST NOT** bridge or route between WAN connections (i.e., WAN to WAN) except when explicitly configured to do so.

I - 123 The device **SHOULD** support PPPoA as defined in IETF RFC 2364.

I - 124 The device **MUST** be configured by default to PPPoE.

I - 125 PPPoE bridging 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).

I - 126 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).

I - 127 The device **MUST** support an "always on" mode for connections. In this mode the device **MUST NOT** time out DSL sessions (ATM, IP and PPP) and **MUST** automatically re-establish any sessions after disconnection, lease expiration or loss and restoration of power.

I - 128 The device **MUST** support a “connect on demand” option for connections. In this mode the connection to the DSL network is initiated when outbound traffic is encountered from the local LAN and terminated after a timeout period in which no traffic occurs.

I - 129 The device **MUST** support a “manual connect” option for connections. In this mode the connection to the DSL network is initiated manually through the GUI or an XML request and, by default, terminates only when done so explicitly by the user, due to a power loss or when the connection is lost.

I - 130 The default mode for connections **MUST** be “connect on demand”.

I - 131 The interval after which a connection timeout occurs **MUST** be able to be configured.

I - 132 A manual way of disconnecting without waiting for a connection timeout **MUST** be provided.

I - 133 A default timeout of 20 minutes **SHOULD** be used for connection timeouts.

I - 134 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.

I - 135 The device **SHOULD** incorporate a random timing delay prior to starting each IP 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 restoral of power to a neighborhood that had a blackout).

I - 136 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.

I - 137 The device **MUST** be able to bridge PPPoE sessions initiated from LAN devices (sometimes known as PPPoE pass-through).

Only PPPoE traffic **MUST** be bridged unless bridging of other traffic is specifically enabled.

I - 138 The device **MUST** support a minimum of eight LAN device initiated PPPoE sessions from each LAN device.

I - 139 The device **MUST** be able to bridge eight sessions per PVC.

I - 140 The device **MUST** be able to bridge 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.

I - 141 The device **MUST** allow for pass-through of IP 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 IP).

I - 142 The device **MUST** allow LAN CPE to originate IPsec sessions to an external network. This function **MUST** work properly through the NAPT function of the DSL device.

I - 143 The device **MUST** allow at least one IPsec connection from the LAN.

I - 144 The device **SHOULD** allow multiple users on the LAN to launch independent and simultaneous IPsec sessions.

I - 145 The device **MUST** support LAN device UDP Encapsulation of IPsec packets as defined in draft-ietf-ipsec-udp-encaps-08.txt and its successors.

I - 146 The device **MUST** support LAN device negotiation of NAT-Traversal with IKE as identified in draft-ietf-ipsec-nat-t-ike-08.txt and its successors.

I - 147 A minimum of 4 concurrent LAN IPsec sessions **SHOULD** be supported per LAN device. These sessions can be to the same or unique destinations.

I - 148 The device **MUST** support Path MTU discovery (described in IETF RFC 1191) so that a LAN device can be told what to set its MTU to.

2.5 LAN: Physical Interfaces

I - 149 The device **MUST** support use of a straight-through (patch) cable between the Ethernet Interface and a PC.

I - 150 The device **SHOULD** automatically sense the transmit and receive pair on the Ethernet physical connection.

I - 151 The device **MUST** have at least one 10BASET Ethernet port (RJ-45 jack) for connecting it to the home data network.

I - 152 If the device supports 100BASET it **MUST** be able to support both 10BASET and 100BASET with auto negotiate for speed and duplex on a port-by-port basis according to IEEE 802.3u.

I - 153 The device **MUST** support, at a minimum, a 256 MAC address table for LAN devices.

I - 154 The Ethernet LAN interface **SHOULD** allow for adjusting the inter-frame and collision back off timers so that P traffic (as defined in IEEE 802.1P) can get statistically better treatment on broadcast LAN Segments.

I - 155 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 doesn’t get power across the USB interface) slave device for a host computer.

I - 156 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 (i.e., **MUST NOT** require DSL modem drivers on LAN CPE).

I - 157 If the device has a client USB port, the USB port **MUST** be based on the USB 1.1 (or later) technical specification.

I - 158 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.

I - 159 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.

I - 160 The USB port **MUST** be covered with a sticker than warns the customer not to install the USB cable until instructed to do so in the documentation or installation software.

I - 161 If the device has only one Ethernet port and only one client USB port, the device **SHOULD** be configurable through XML 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.

2.6 WAN and LAN: IP Addressing and DHCP Server

I - 162 [TR-059] 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 address(es) with subnet mask,

(2) originating IP 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.

I - 163 [TR-059] The device **SHOULD** 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) IEEE 802.1Q VLAN identification, and

(2) packet length.

I - 164 [TR-059] The device **MUST** support the differentiated services field (DS Field) in IP headers as defined in IETF RFC 2474.

164 .1 [TR-059] 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 Table 1 must be supported, except the Cs0-7, which are optional.

Table 1: Supported Default DSCP Markings

Class	Description	DSCP marking (name)	DSCP marking (decimal value)
EF	Realtime	ef	46
AF4 – in-contract AF4 – out-of-contract	Premium class4 – in-contract Premium class4 – out-of-contract	af41 af42, af43	34 36, 38
AF3 – in-contract AF3 – out-of-contract	Premium class3 – in-contract Premium class3 – out-of-contract	af31 af32, af33	26 28, 30
AF2 – in-contract AF2 – out-of-contract	Premium class2 – in-contract Premium class2 – out-of-contract	af21 af22, af23	18 20, 22
AF1 – in-contract AF1 – out-of-contract	Premium class1 – in-contract Premium class1 – out-of-contract	af11 af12, af13	10 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

I - 165 [TR-059] The device **MUST** be able to mark or remark the Diffserv codepoint or IEEE 802.1D user priority of traffic based on the classification information identified in I - 162 and I - 163 above.

I - 166 [TR-059] The device **MUST** support one Best Effort (BE) queue, one Expedited Forwarding (EF) queue and a minimum of four Assured Forwarding (AF) queues.

I - 167 [TR-059] The device **MUST** duplicate the set of queues for each access session. This can be done logically or physically.

I - 168 [TR-059] The device **SHOULD** support the appropriate mechanism to effectively implement Diffserv per hop scheduling behaviors. A strict priority scheduler is preferred for EF.

I - 169 [TR-059] 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.

169 .1 [TR-059] When fragmentation is required, the device **MUST** fragment all PPP sessions that it originates on an access VC using MLPPP interleaving (RFC 1990).

I - 170 [TR-059] The packet size threshold before fragmenting AF and BE packets **MUST** be configurable.

I - 171 The device **MUST** be able to obtain IP network information dynamically on its WAN interface. This information includes IP address, primary and secondary DNS addresses and default gateway address.

Dynamically obtaining IP network information is accomplished using DHCP and / or IPCP.

I - 172 If PPP is used, the device **MAY** obtain an IP subnet mask on its WAN interface using IPCP extensions. If this is done, then IP subnet masks will be communicated with IPCP using the PPP IPCP 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 IP address negotiated should, but need not, be the one assigned to the modem.

I - 173 If the device is not configured to use a static IP address and the modem fails to detect a PPPoE or DHCP server, then the WAN IP address assignment value **SHOULD** be set to an undefined value, in order to prevent it from retaining its prior IP address.

I - 174 The device **MUST** provide application layer support for host name mapping, booting, and management including DHCP 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

I - 175 The device **MUST** be a DHCP server to local LAN devices, supporting all LAN devices.

I - 176 The embedded DHCP server function of the device **MUST** be able to operate while in bridged mode. The default state should be on in bridged and router mode.

I - 177 The device **MUST** support a minimum of 253 LAN devices.

I - 178 The device **MUST** support turning off the embedded DHCP server via a configuration change.

I - 179 The device **MAY** incorporate auto-detection of other DHCP servers on the local LAN and, if configured to do so, disable the internal DHCP server functionality of the DSL device in this situation.

In this situation, the DSL device would try to obtain a configuration for its LAN port through DHCP. If a DHCP response was received, the device would then use the information in the DHCP response (e.g., IP Address, subnet and DNS information) and disable its internal DHCP server. If implemented and a DHCP response is received, this requirement takes precedence over I - 190.

I - 180 The embedded DHCP 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.

I - 181 The device **MUST** support all LAN devices concurrently accessing one or more WAN connections.

I - 182 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 DHCP leases for local device addressing.

I - 183 The device **MUST** use a default netmask of 255.255.255.0 for assignment to DHCP leases for local device addressing.

I - 184 The device **MUST** be able to be configured to specify alternate public and private subnets (without restriction) for local device addressing.

I - 185 The device **MUST** be able to be configured to specify the start and stop addresses within a subnet used for local addressing.

I - 186 The default lease time for DHCP information provided to LAN CPE which do not share the WAN side IP address **MUST** be configurable. The default value **MUST** be 24 hours.

I - 187 The default lease time for DHCP information provided to LAN CPE which share the WAN side IP address **MUST** be configurable. The default value **MUST** be 10 minutes.

I - 188 When the domain name that the embedded DHCP server passes to LAN CPE has not been set, the value "domain_not_set.invalid" **SHOULD** be used.

I - 189 When the device's embedded DHCP server is enabled, the device itself **MUST** default to the address 192.168.1.254 (with a netmask of 255.255.255.0).

I - 190 When the device's embedded DHCP 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.

I - 191 The device **MUST NOT** use auto IP for address assignment of its LAN-side address.

I - 192 The device **MUST** allow its assigned address and netmask to be specified through the XML and GUI interfaces.

I - 193 The device **MAY** support SOCKS (IETF RFC 1928) for non-ALG access to the public address.

I - 194 Both NetBios and Zero Config naming mechanisms **MAY** be used to populate the DNS tables.

I - 195 The device **MAY** act as a NETBIOS master browser for that name service.

I - 196 The device **MUST** support multiple subnets being used on the local LAN.

I - 197 The device **MUST** be able to assign its WAN IP address (e.g., public address) to a particular LAN device, concurrent with private IP addressing being used for other LAN CPE.

In this situation, one device on the LAN is given the same public IP address (through DHCP or manual configuration of the LAN CPE IP stack). Other LAN devices utilize private IP addresses. The device can then be configured as identified in I - 219 so that the LAN device "sharing" the WAN IP 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 IP address. Note that the use of the WAN gateway address does not guarantee this since it need not meet this requirement.

I - 198 When using a WAN IP address assigned to a LAN device, the user **MUST** be able to configure if this LAN device can directly communicate with other CPE on the local LAN.

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.

I - 199 The device **MAY** allow the embedded DHCP server to be configured so that specific MAC addresses can be identified as being served or not served.

I - 200 The device **MAY** allow the embedded DHCP server to be configured with a default setting (provide IP addresses or do not provide IP addresses) for devices with unspecified MAC addresses.

I - 201 The embedded DHCP server functionality of the device **SHOULD** provide a mechanism by which an IP 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 IP address or device name) and the MAC address may be transparent to the user. These addresses may include the ability to assign an address outside of the default subnet, as identified in I - 184 and I - 197.

For example, the device might have a default WAN side IP address which is used for NAPT to a subset of devices and an additional set of WAN side IP addresses which are

bridged. The embedded DHCP server might be used to assign this second set of IP addresses to specific LAN CPE.

I - 202 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 GUI) **MUST** be passed between the DSL network and the designated LAN device as if the DSL device was not present.

One possible implementation is for the embedded DHCP server to issue one and only one private address in this situation, with the start and stop address for the embedded DHCP server being the same.

The LAN device can be assigned either a private IP address (i.e., using 1:1 NAT) or the public IP address (i.e., using IP Passthrough) of the modem (as identified in I - 197). The type of IP address to be used (private or public) is configured through the GUI and XML interfaces. The default is a public IP address.

If a WAN connection is not available when the device is configured to use a public IP address, the LAN device is provided with a private IP address from the device via DHCP. Once a WAN connection is established, the public IP address provided by the DSL network is passed to the LAN device during the next DHCP lease renewal.

The DSL device acts as the default gateway to the LAN devices when private IP addressing is in use. When public IP addressing is in use, the gateway identified to the LAN device should be that identified in I - 197 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).

I - 203 The device **MUST** operate by default in the multiple PC mode of operation (i.e., full NAPT router).

I - 204 The device **MUST** support IP Version 4.

I - 205 The device **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.

2.7 Routing and NAPT

I - 206 The device **MUST** support Network Address Port Translation (NAPT; also known as Port Address Translation) as identified in the documents below:
a) IETF RFC 2663 IP Network Address Translator Terminology and Considerations
b) IETF RFC 3022 Traditional IP Network Address Translator
c) IETF RFC 3027 Protocol Complications with the IP Network Address Translator

I - 207 The device **MUST** support disabling NAPT.

I - 208 The device **MUST** maintain route table entries for all connections it maintains on the WAN (e.g., per PVC, IP and PPP sessions) and for all LAN networks (including subnets).

I - 209 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.

I - 210 [TR-059] The device **MUST** support the ability to accept IP 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, IETF RFC 2453) messages to fulfill this task.

210 .1 [TR-059] The device **MUST** be configurable to accept Triggered RIP messages, as defined in IETF RFC 2091.

I - 211 [TR-059] The device **MAY** support additional mechanisms to accept IP routing information.

I - 212 [TR-059] RIP-2 functionality **SHOULD** be software configurable.

I - 213 By default, the device **MUST NOT** transmit RIP-2 information to WAN connections.

I - 214 The device **MUST** include port forwarding configurations and Application Level Gateways (ALGs) 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.

I - 215 The device **SHOULD** include port forwarding configurations and ALGs for other major applications and protocols that do not function properly with NAT or NAPT. Some potential candidates are identified in Appendix A.

I - 216 The ALG mechanism **MUST** be integrated with the port forwarding mechanism.

I - 217 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 IP 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 IP address of the LAN device, and follow the LAN device should its IP address change.

I - 218 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 instead of a port number and protocol type. A partial list of applications for potential inclusion are identified in Appendix A.

I - 219 The port forwarding mechanism **MUST** be able to be configured to direct all unidentified or unsolicited port traffic to any specific LAN device.

The LAN device may be using either a private IP address or the public WAN IP address (as identified in I - 197).

2.8 Firewall

I - 220 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 or bridges IP.

I - 221 The device **MUST** reject packets from the WAN with MAC addresses of devices on the local LAN or invalid IP addresses (e.g., broadcast addresses, private IP addresses or IP Addresses matching those assigned to the LAN Segment).

I - 222 The device **MUST** drop or deny access requests from WAN side connections to LAN side devices and the DSL device itself except in direct response to outgoing traffic or as explicitly permitted through configuration of the DSL device (e.g., for port forwarding or management).

I - 223 The device **MAY** support a more robust firewall, such as one which provides a full OSI 7 layer stack stateful packet inspection and packet filtering function.

I - 224 The device **MAY** support a separate firewall log to maintain records of all transactions that violate firewall rules.

I - 225 The firewall log file **SHOULD** be able to hold at least the last 100 entries or 10 Kbytes of text.

I - 226 If a firewall log is implemented, the file entries **SHOULD** not be cleared, except when the device is reset to its factory default settings.

I - 227 If a firewall log is implemented, the device **MUST** timestamp each firewall log entry.

2.9 Naming Services

I - 228 The device **MUST** act as a DNS name server to LAN devices, passing its address back to these devices in DHCP requests as the DNS name server.

I - 229 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 DHCP responses instead of the DSL modem address itself as the DNS name server(s).

I - 230 When the device learns DNS name server addresses from multiple WAN connections, the DSL 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.

I - 231 The device **MUST** add the DNS entry "dsldevice" for its own address.

I - 232 The device **MAY** support additional DNS entries, as there could be additional types of CPE.

I - 233 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 DHCP 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.

I - 234 The device **SHOULD** provide a manual mechanism for overriding the learned names of all LAN CPE except that for the DSL device itself.

2.10 User Interface and Management

I - 235 A console port that allows end user access (e.g., placed on the outside of the device) **SHOULD NOT** be provided on the device.

I - 236 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 the user is surfing including any driver installation (assuming no network complications and excluding micro-filter installation and customer ordering/registration).

I - 237 Configuration and installation of the device **SHOULD** minimize the number of restarts of the device when enabling changes.

I - 238 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).

I - 239 Other than networking drivers (e.g., USB, wireless, etc…), other software or drivers **MUST NOT** be required for proper and full use of the device.

I - 240 If UPnP IGD is supported, it **MUST** be disabled as a default.

I - 241 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 traffic to access local devices.

I - 242 If UPnP IGD is supported, it **MUST** allow the user to log all UPnP IGD actions and events.

I - 243 An XML based WAN side auto configuration mechanism **MUST** be supported as defined in The Broadband Forum TR-069.

I - 244 A configuration mechanism from the PC to the device based on XML **MUST** be supported as defined in The Broadband Forum Working Text TR-064.

I - 245 The XML based LAN side configuration mechanism **MUST** operate independently of the status or configuration of UPnP IGD in the device.

I - 246 The device **MUST** be configurable via embedded, easy-to-use web pages.

I - 247 XML and GUI authorization **MUST** time out after 30 minutes.

I - 248 The web pages **MUST** be available when the device is in bridged mode.

I - 249 The device, drivers and any packaged software **SHOULD** support Macintosh OS 8.6 and above.

I - 250 The device, drivers and any packaged software **SHOULD** support all Microsoft PC based operating systems which have not yet reached "End of Life" status (see http://www.microsoft.com/windows/lifecycleconsumer.mspx for more details).

I - 251 The device, drivers and any packaged software **MAY** support Linux. It is especially desirable to do so with an open interface.

I - 252 The device **MUST NOT** require browser support of Java, ActiveX nor VBSCRIPT in its web pages.

I - 253 The web 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.

I - 254 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.

I - 255 The device **MUST** have a software mechanism by which the user can reset it to default factory settings.

I - 256 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 The Broadband Forum TR-064 and TR-069.

I - 257 The device modem access code **MUST** be set to a default modem access code of a length of 10 decimal digits (0 through 9).

I - 258 The default modem access code **SHOULD** be unique for each DSL device, when in factory default mode or pre-installation mode (e.g., as shipped or after a modem reset to factory defaults).

I - 259 The device modem access code **MUST NOT** be displayed nor broadcast in any way by the device (e.g., through HTML or as a MAC address).

I - 260 The default modem access code **MUST** be on the bottom of the DSL device.

I - 261 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).

I - 262 The user **MUST** be able to disable the use of the modem access code. The user **MUST** be warned in the GUI of the implications of under-taking this action.

I - 263 The device **MUST** be able to provide web pages to allow temporary manual remote access to its GUI from the WAN. Primary requirements relating to this mode of operation are identified in I - 264 through I - 275 below.

I - 264 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.

I - 265 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.

I - 266 Temporary WAN side remote access **MUST NOT** allow for changing the device password.

I - 267 Temporary WAN side remote access **MUST** be disabled by default.

I - 268 Temporary WAN side remote access **SHOULD** be through HTTP over TLS (i.e., https using TLS).

I - 269 The device **SHOULD** use a randomly selected port for temporary WAN side remote access to prevent hacking of a well known port.

I - 270 If a default port is used for temporary WAN side remote access, it **MUST** be 51003.

I - 271 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.

I - 272 The User ID for all temporary WAN side remote access sessions, if required based on the method of implementation, **MUST** be "tech" by default.

I - 273 The user **MUST** be able to change the User ID for all temporary WAN side remote access sessions**.**

I - 274 The device **MUST** allow only one temporary WAN side remote access session to be active at a time.

I - 275 All other direct access to the device from the WAN side **MUST** be disabled and blocked by default.

I - 276 The device **MUST** support updating of its firmware via the GUI and XML interfaces.

I - 277 The device **MUST** use standard protocols when using FTP and HTTP (e.g., FTP - IETF RFC 959, HTTP - IETF RFC 2616, HTTPS - IETF RFCs 2246, 2818).

I - 278 The vendor **SHOULD** have a web site where firmware updates and documentation is available.

I - 279 The documentation **SHOULD** include manuals containing detailed installation procedures, corrective actions for troubleshooting, and subsequent release notes for all software versions, network driver versions, modem firmware versions, fixes and changes.

I - 280 The firmware at the vendor's web site **SHOULD** include all error correcting updates for the device.

I - 281 All software revisions **SHOULD** be backward compatible with all previous versions. There **SHOULD** be no loss of existing functionality.

I - 282 Software revisions **MUST NOT** require service provider network changes to maintain proper operation of previous features.

I - 283 The vendor of the device **MUST** adhere to a vendor self-defined standard numbering and revisioning scheme for all firmware releases and all documentation.

I - 284 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).

I - 285 All firmware updates **MUST** be verified using security mechanisms. A checksum mechanism is a minimum requirement for achieving this.

I - 286 All firmware updates **SHOULD** be verified using an acryptographic "fingerprint" of at least 256 bits.

I - 287 In the event of a failure occurring during an update, the device **SHOULD** be able to back off to the prior version of the firmware installed on the DSL device.

That is, the prior version of the device's firmware **SHOULD** continue to be useable in the event that a firmware update fails to complete.

This is not a requirement for a dual image, but that is one manner in which this requirement might be achieved.

I - 288 The device **MUST** have diagnostics tools 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 ADSL, ATM, Ethernet, PPP, or IP layer. These tools **MUST** be accessible from the GUI and XML interfaces.

I - 289 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-069.

I - 290 The device **MUST** support restarting the broadband connection (all layers) via the GUI and XML interfaces.

I - 291 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 DHCP, issue LCP Terminate-Request/Terminate-Ack and PADT packet when using PPPoE, etc.) and then restart the connections.

I - 292 The model and serial number **MUST** be visible via external markings on the device.

I - 293 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, TR-069, I - 288 and I - 289.

I - 294 The device **MUST** maintain an internal log of ATM status and WAN side connection flows (e.g., DHCP, IP and PPP sessions). At a minimum, the log **MUST** record the last 250 modem events. This will include modem training events initiated by the modem or by the DSLAM. The purpose of the log is to provide a trouble shooting aid in resolving line and connection problems.

I - 295 The device **MUST** timestamp each log entry.

I - 296 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)

I - 297 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 GUI and XML interface.

I - 298 The device modem log **SHOULD** reside on the device and be persistent across power loss.

I - 299 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.

I - 300 The device **MUST** support an internal clock with a date and time mechanism.

I - 301 The device clock **MUST** be able to be set via an internal time client using NTP (IETF RFC 1305) or SNTP (IETF RFC 2030) from an Internet source.

I - 302 The device **MUST** support the use of time server identification by both domain name and IP address.

I - 303 If the device includes default time server values, they **SHOULD** be specified by domain name and not by IP address.

I - 304 The device **SHOULD** allow configuration of the primary and alternate time server values in addition to or in place of any default values.

I - 305 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 example, draft-mills-sntp-v4-00.txt identifies that the time server names used should be those of servers the manufacturer or seller operates as a customer convenience or those for which specific permission has been obtained from the operator of the time server.

I - 306 The time client **SHOULD** re-resolve any time server IP address obtained from a domain name on a periodic interval, but not less than the time-to-live field in the DNS response.

I - 307 The time client **SHOULD** support DNS responses with CNAMEs or multiple A records.

I - 308 The default frequency with which the device updates its time from a time server **MUST NOT** be less than 60 minutes.

I - 309 The default frequency with which the device updates its time from a time server **MUST NOT** be greater than 24 hours.

I - 310 The frequency with which the device updates its time from a time server **SHOULD** be able to be configured.

I - 311 The time server discovery and selection stage used by the time client **SHOULD** check each candidate time server in a round robin fashion, with a response timeout between each request to each time server.

If no time server has responded during a round of checking, the response timeout **SHOULD** be exponentially incremented (e.g., doubled) and the time servers checked again.

The round robin checking and exponential incrementing of the response timeout **SHOULD** continue until a time server is discovered or a search limit is reached.

I - 312 The device **SHOULD** support the [S]NTP access-refusal mechanism, so that a server returning a Stratum value of zero (0; sometimes termed a kiss-o'-death reply) in response to a client request causes the client to cease sending requests to that server.

If this occurs during the discovery and selection stage for a time server, then the discovery mechanism should continue on to the next time server in its list of those to check or increase the response timeout as identified above.

If this occurs when the device is periodically updating its clock, then the discovery and selection stage for a time server should be re-initiated.

I - 313 The device **SHOULD** validate response packets for malformed time protocol packets (invalid flags – such as client query flag, bad packet size, …) and ignore invalid packets.

I - 314 The device **SHOULD** ignore time protocol response packets with a source IP address other than that of the time server that the modem queried.

I - 315 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.

I - 316 The device **MUST** make the access concentrator name used with PPPoE connections available via XML and GUI for diagnostic purposes.

I - 317 The device **MUST** have a PING client built into the unit.

I - 318 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.

2.11 Graphical User Interface

2.11.1 General

I - 319 The device **MUST** have a quick start page 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.

I - 320 The model and firmware/software versions **MUST** be easily identifiable via the GUI interface.

2.11.2 Software Updates

I - 321 The web 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).

I - 322 If the device has been configured to do so, the web interface **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 either WAN side or LAN side mechanisms as identified in I - 243 and I - 244.

I - 323 The web location **MAY** be pre-defined by the modem manufacturer. This value is overridden by the mechanisms and information identified in I - 322.

I - 324 If the device has been configured to allow updating from a pre-defined web location, the device **MUST** display an update button in the 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).

I - 325 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

I - 326 If the device has been configured to do so, the web interface **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 by either WAN side or LAN side mechanisms as identified in I - 243 and I - 244.

I - 327 The web link **MAY** be pre-defined by the modem manufacturer. This value is overridden by the mechanisms and information identified in I - 326.

I - 328 The device **MUST** preserve its configuration across firmware updates.

2.12 Packaging

I - 329 Cables **MUST** be colored as identified in I - 37.

I - 330 The device **MUST** be packaged with a quick start or installation guide.

I - 331 The Quick Start Guide **SHOULD** be made available in alternate formats including large print.

I - 332 All necessary end user documentation **MUST** be included with the device.

I - 333 Additional detailed product documentation **SHOULD** be included with the device.

I - 334 The model and serial number **MUST** be visible via external markings on the product packaging.

I - 335 All device firmware and associated system files **MUST** be pre-installed.

I - 336 A phone cable with two pairs and RJ-11 endpoints **MUST** be packaged with the product to connect the device to the ADSL wall jack on the WAN interface. The cable **MUST** be a minimum length of 6 feet. The endpoints **MUST** meet the specifications for a miniature 6-position plug in TIA-968-A.

I - 337 The phone cable **SHOULD** be CAT3 or CAT5 and be a length of 14 feet.

I - 338 A CAT5 (or better) straight through (patch) Ethernet cable with RJ-45 endpoints **MUST** be packaged with the product to connect the device to the first computer. The cable **MUST** be a minimum length of 6 feet. The endpoints **MUST** meet the specifications for a miniature 8-position unkeyed plug in TIA-968-A.

I - 339 If the device has a USB port, the packaging **MUST** clearly state for which operating systems this is supported.

I - 340 If the device has a client USB port, a USB Implementers Forum certified USB 2.0 high-speed cable **MUST** be packaged with the device. The cable **MUST** be a minimum length of 6 feet.

APPENDIX A 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 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, 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, 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 B Example Queuing for a DSL Router

Figure 1 shows 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 ∑ 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

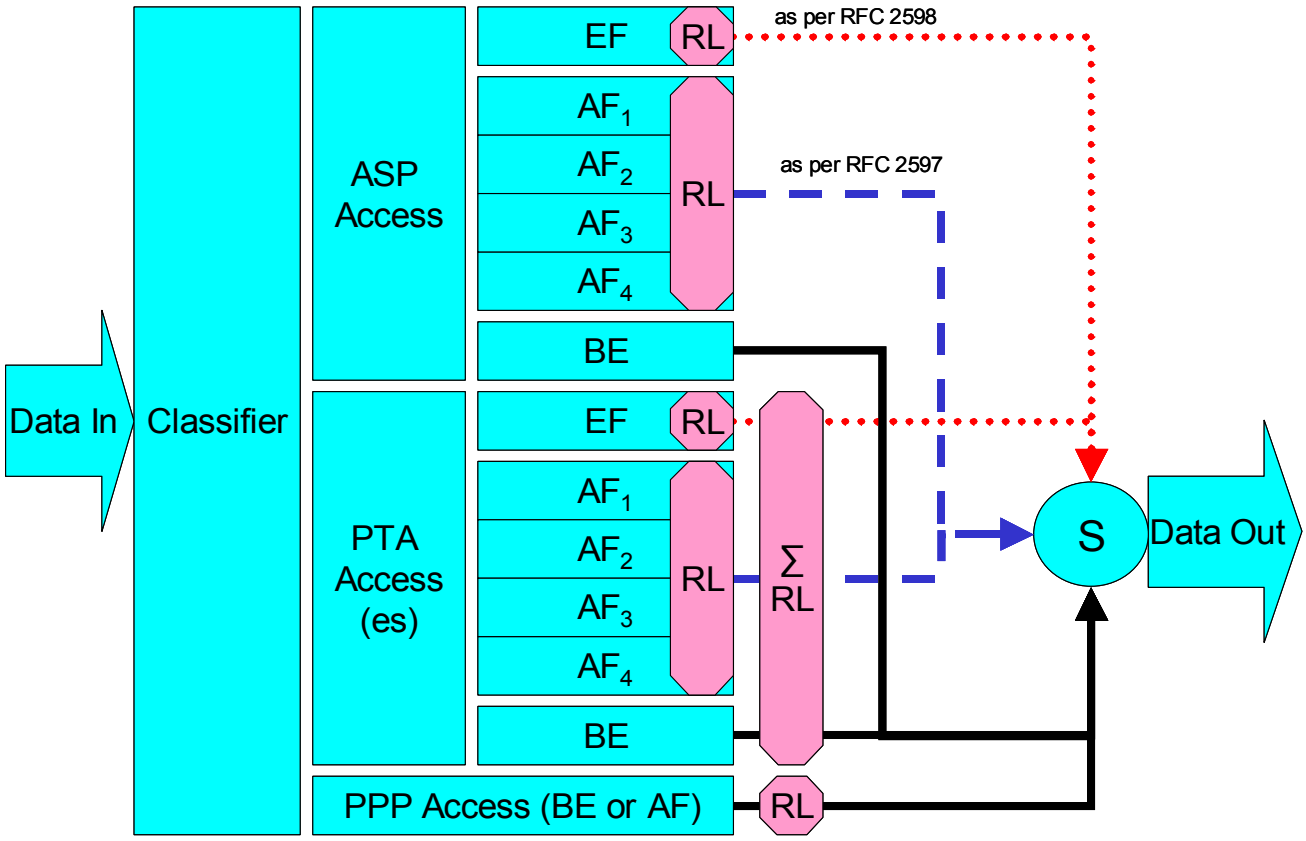


Figure 1 - Queuing and Scheduling Example for DSL Router

In Figure 1 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 C Examples of Potential Configurations

C.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.

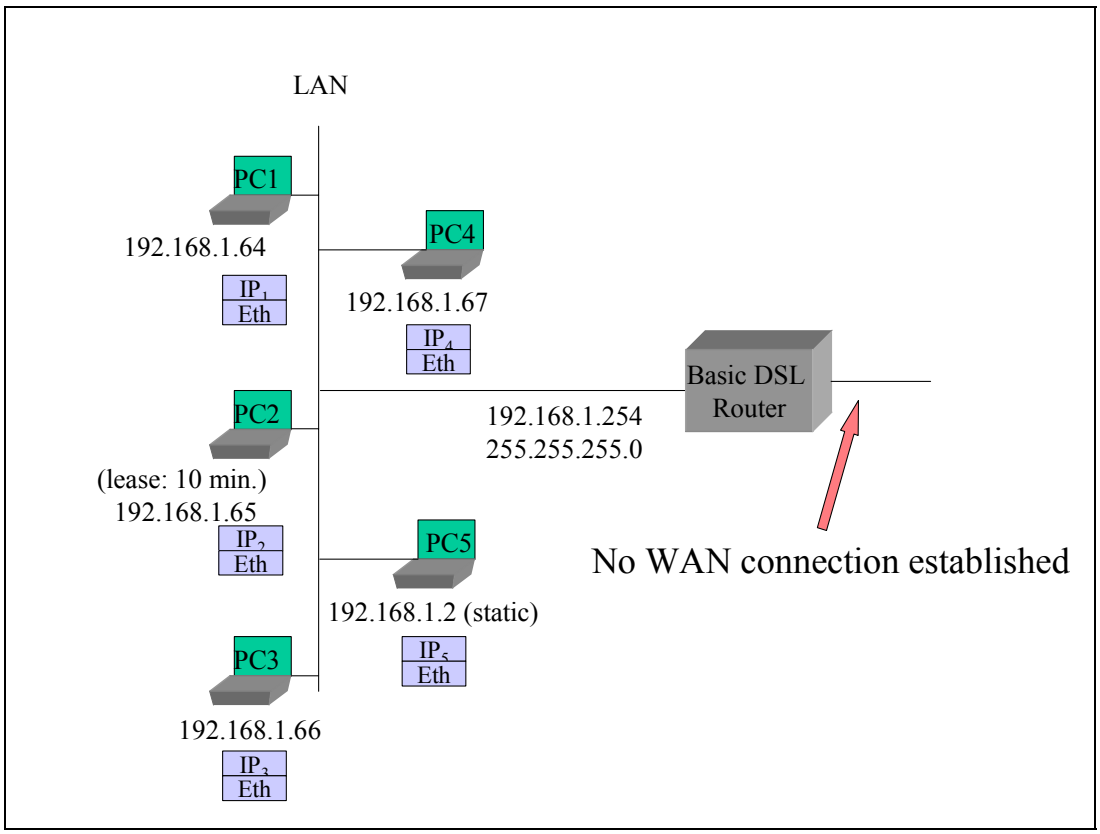
Since the single PC case is a simple subset of the multi-PC case (except when explicitly using the single PC mode of operation [I - 202], see the scenario in Section C.5), it will not be directly addressed. The network that will be used in this sequence of examples has 5 PCs. They are described as being 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.

C.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.

C.2.1 No WAN Connection

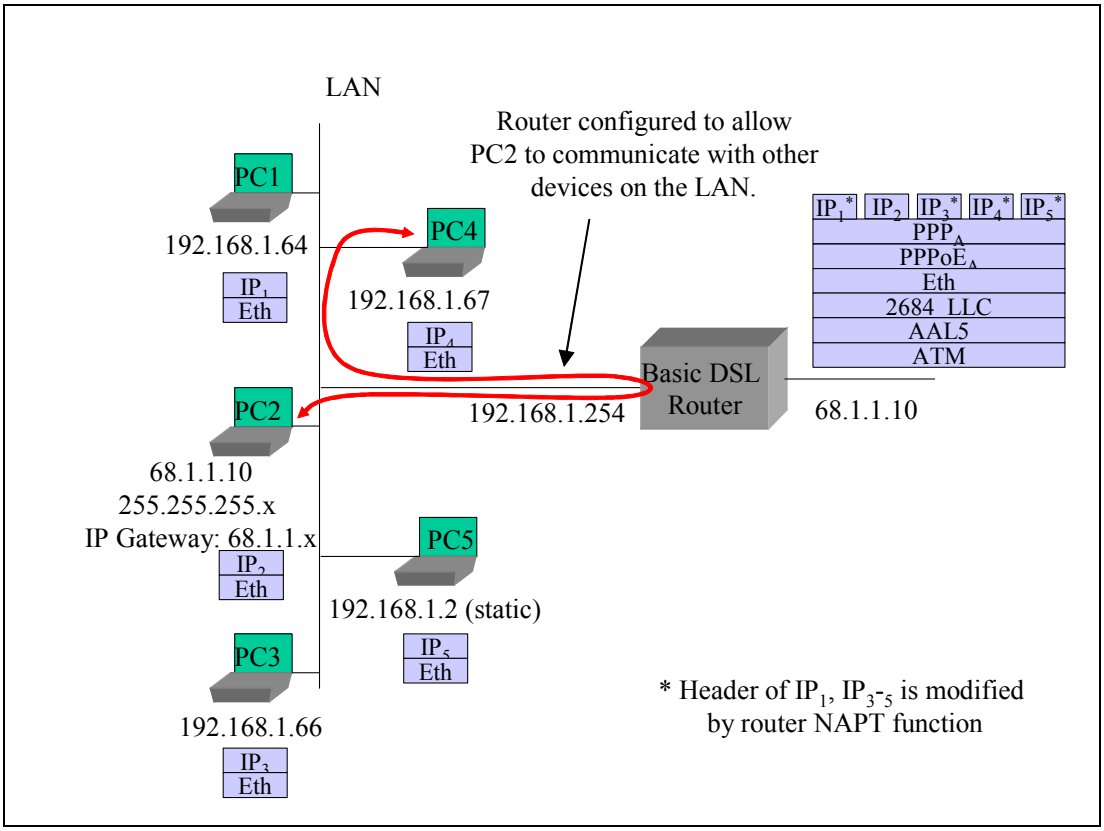
- The router has no WAN connection up.
- The router has been configured to give PC2 its WAN address via its embedded DHCP server. Since the router has no WAN connection, it will give PC2 a private address with a 10 minute lease time [I - 187].
- PC5 has been configured with a static IP address.
- PCs 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 [I - 182], an IP gateway address (and LAN-side address of the device) of 192.168.1.254 [I - 189], a DNS server address of 192.168.1.254 [I - 228] and an IP address lease time for all PCs but PC2 of 24 hours [I - 186].



C.2.2 Router Sets Up PPPoE to an ISP

This scenario is the same as presented above with the following exceptions:

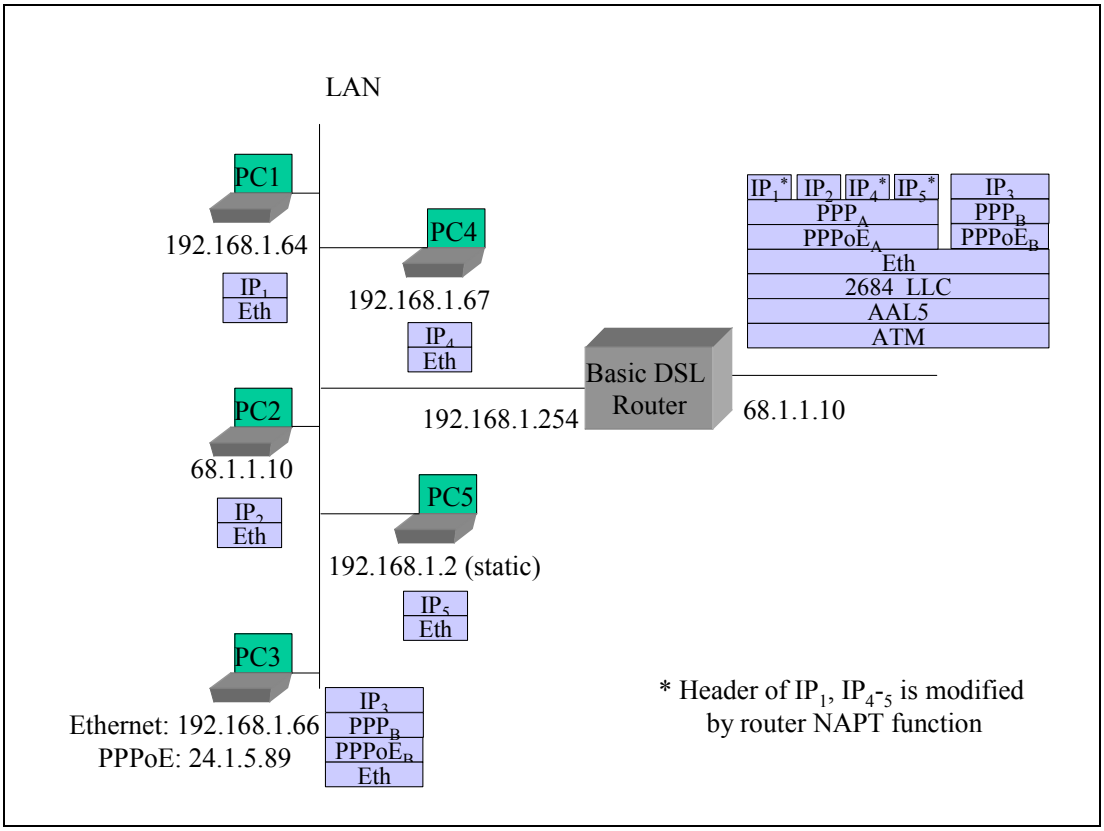
- The router sets up a PPPoE session to ISP – it obtains an IP address and DNS server addresses via IPCP [I - 103, I - 104, I - 111, I - 117, I - 171].
- The router gives its public IP address to PC2 [I - 197].
- The router is configured to allow PC2 to communicate with other devices on the LAN [I - 198].



C.2.3 PC3 Sets Up Its Own PPPoE Session

This scenario is the same as presented above with the following exceptions:

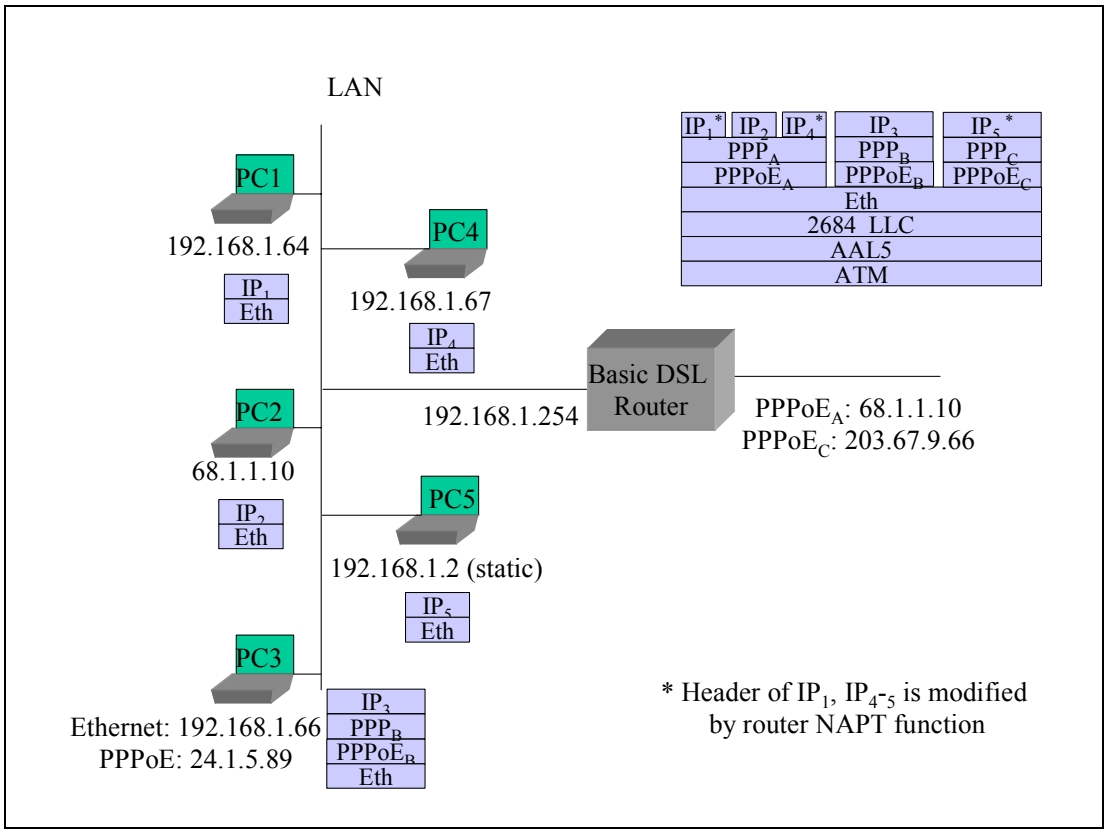
- PC3 uses a PPPoE client to establish its own PPPoE session. While the private IP address from the router is still associated with PC3's Ethernet interface, PC3 also has a public IP address associated with its own PPPoE interface. Common behavior is for all IP traffic of PC3 to now use this PPPoE interface [I - 137, I - 140].



C.2.4 Router Sets Up a Second PPPoE Session

This scenario is the same as presented above 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 [I - 210], manual entry, or other mechanisms [I - 211]. $PPPoE_A$ remains the default route [I - 112].
- 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 [I - 230].
- PC5 sends IP packets to the returned IP address. The router determines from its routing table that this goes to the $PPPoE_C$ connection.

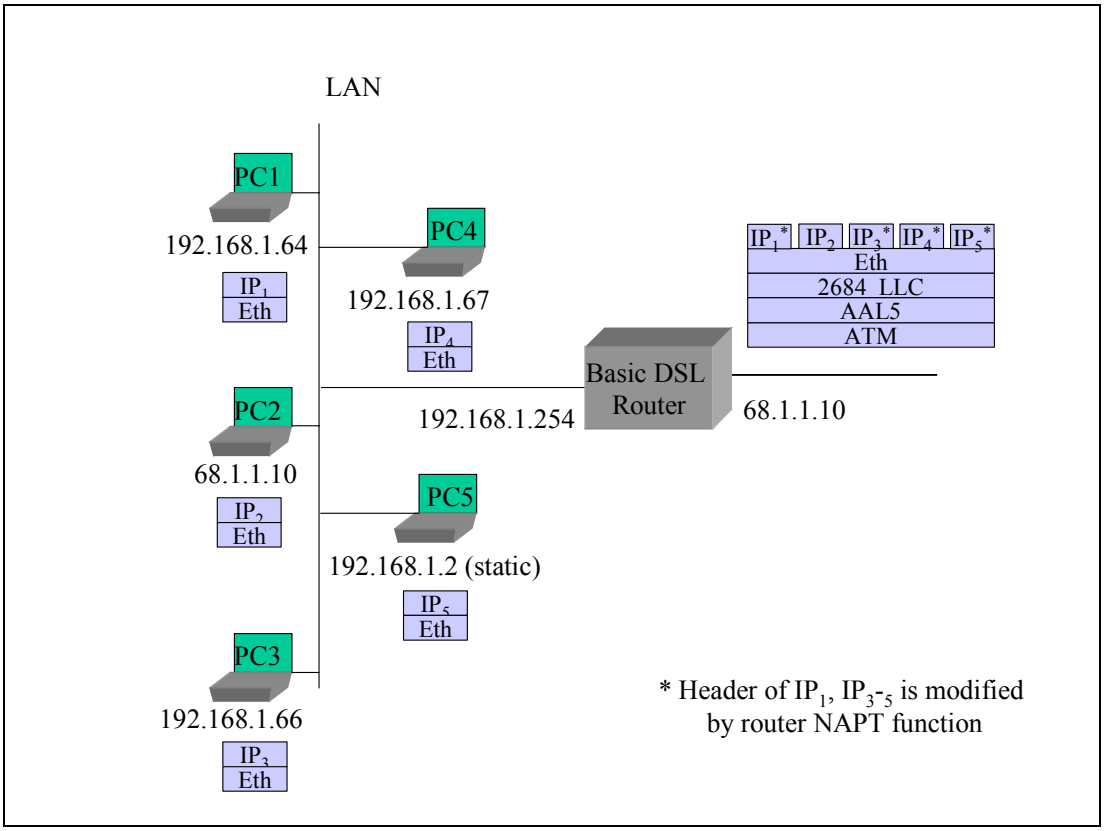


C.3 "2684 Bridged" Mode

The next three scenarios deal with cases where either 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.

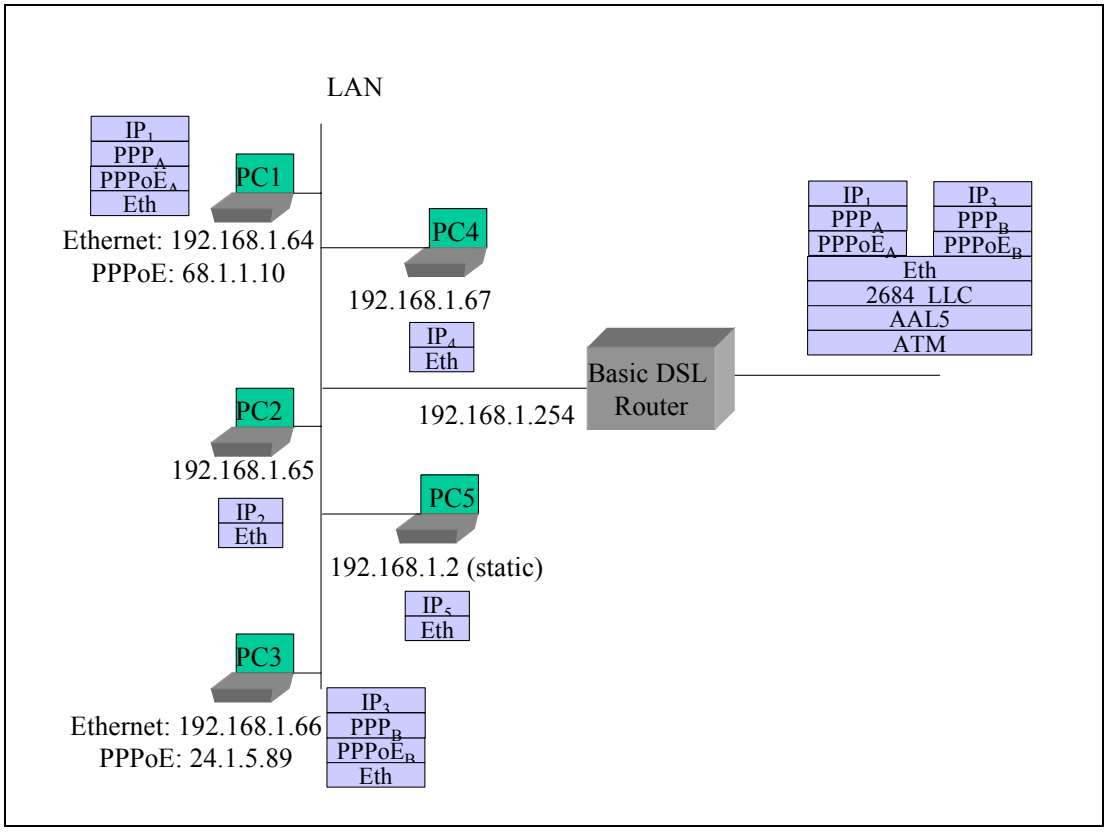
C.3.1 Router in IP-routed "2684 Bridged" Mode, Embedded DHCP Server On

- 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 short lease time.
- The router issues a DHCP request and establishes an IP session to the WAN [I - 103, I - 104, I - 108].
- The router gives its public IP address to PC2.



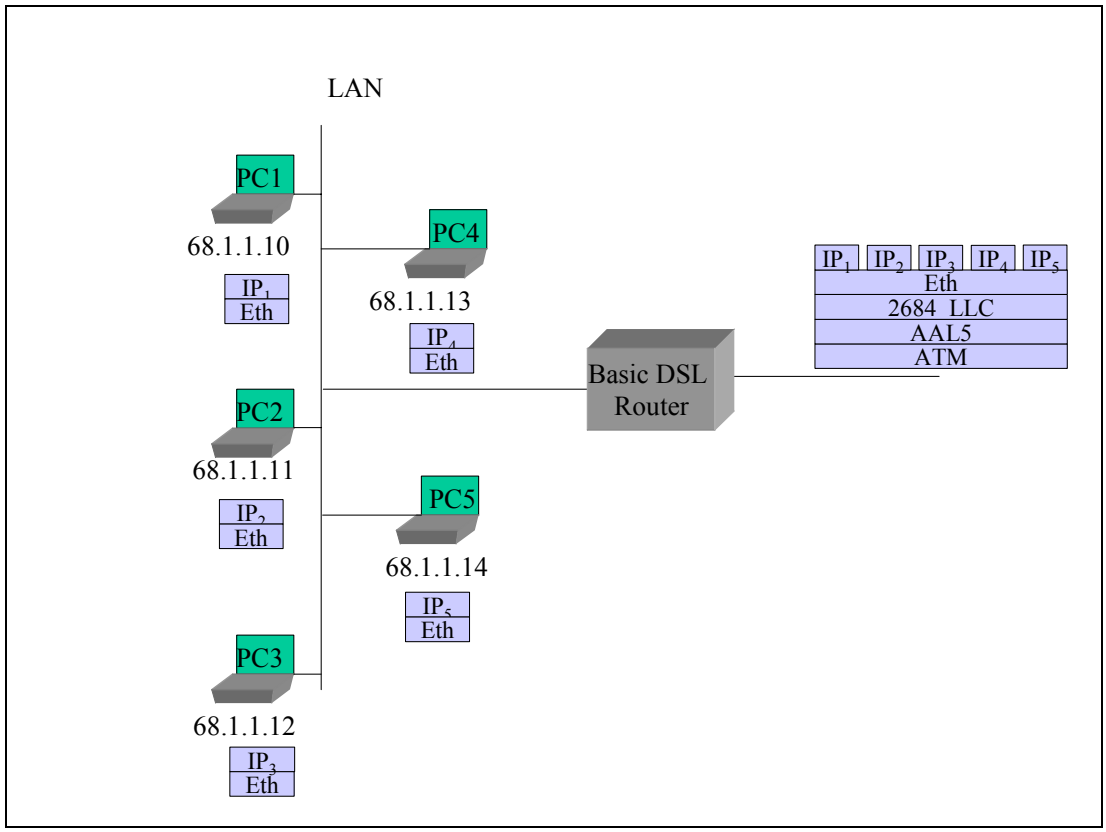
C.3.2 Router in Bridged Mode, Embedded DHCP Server On

- The router provides a private IP address to each device that it receives a DHCP request from [I - 176].
- 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 [I - 137, I - 140]. 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.



C.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 [I - 107].



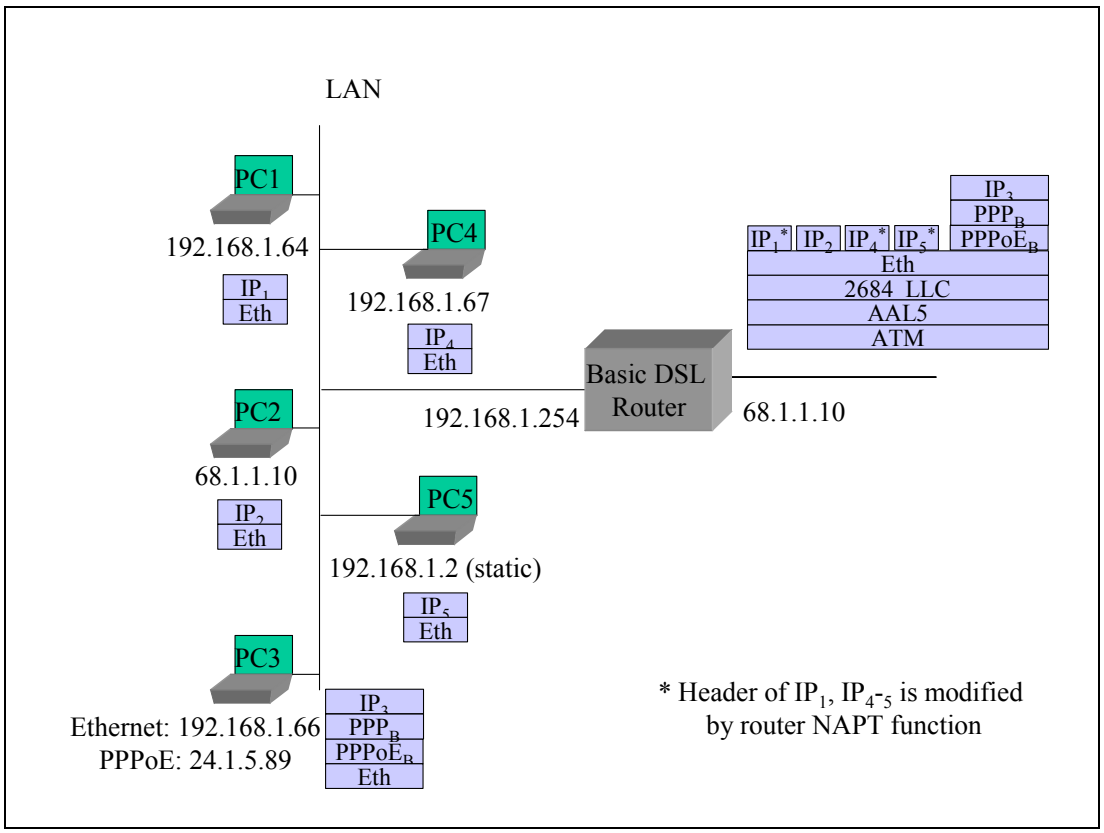
C.4 Simultaneous IP and PPPoE WAN Sessions

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.

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

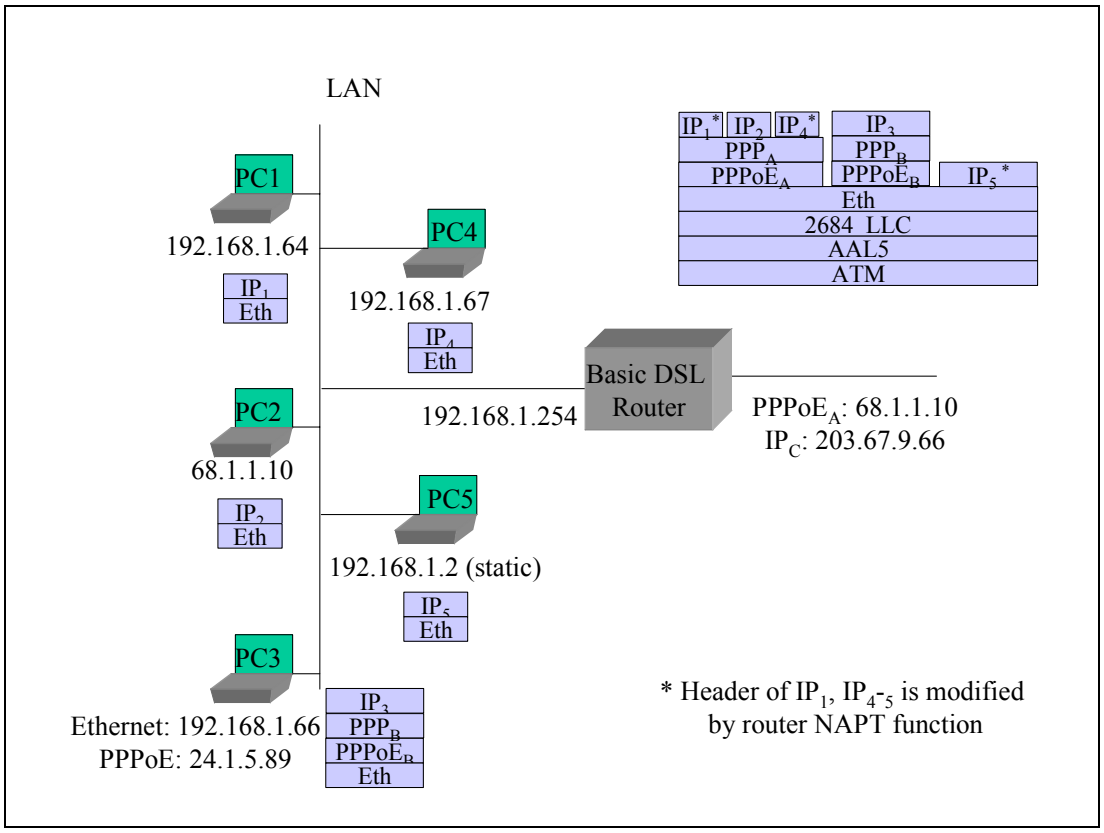
- The router provides an IP address to each device that it receives a DHCP request from.
- PC5 uses a static IP address and does not send a DHCP request to the router.
- The router has been configured to give PC2 its WAN address. When the router has no WAN connection, it gives PC2 a private address with 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 [I - 137, I - 140]. 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.



C.4.2 Router Sets Up IP as a Second Session

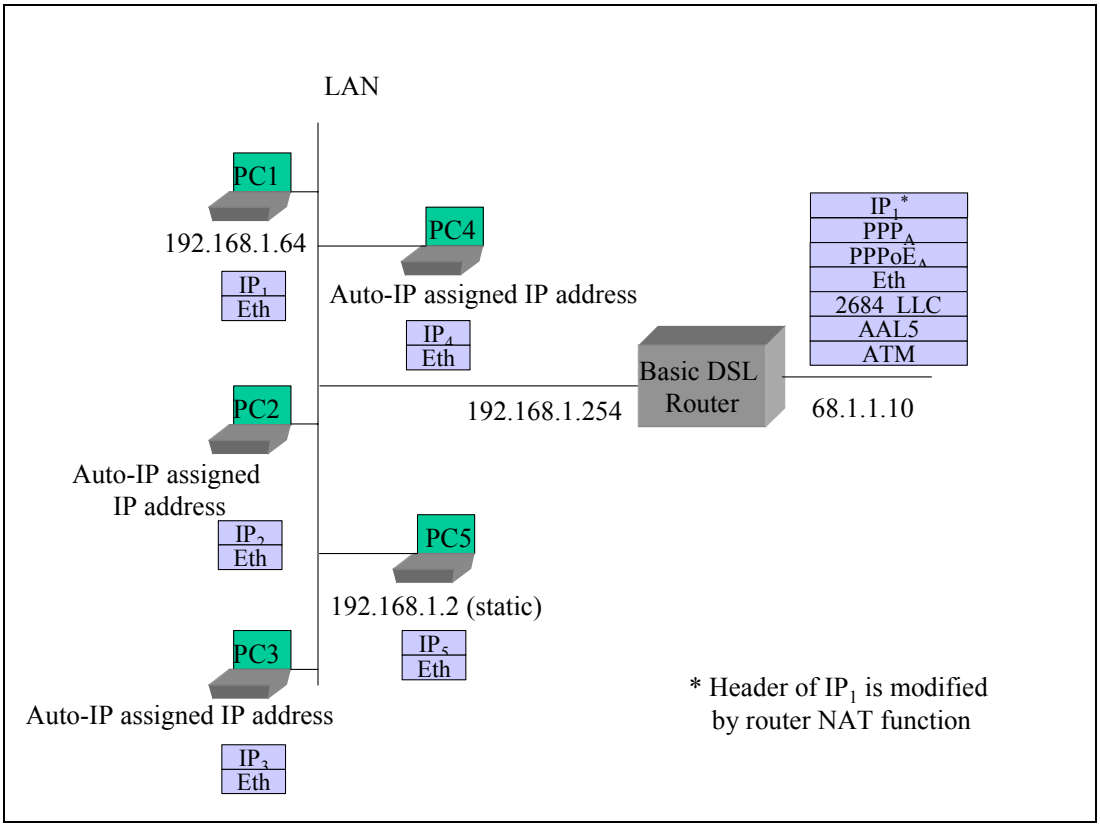
Assuming the scenario in section C.2.3 as a base, add:

- The router sets up connection IP_C [I - 121]. It gets an IP address and DNS addresses through a DHCP client request. It gets routing information from RIP-2 [I - 210]. $PPPoE_A$ 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 IP_C connection returns an IP address. The router returns the IP address to PC5 [I - 230].
- PC5 sends IP packets to the returned IP address. The router determines from its routing table that this goes to connection IP_C.



C.5 Single PC Mode of Operation

- The router is configured to use the single PC mode of operation [I - 202].
- 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 C.2.



C.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 [I - 171, I - 172].
- The router gives public IP addresses to certain PCs when they issue DHCP requests again [I - 201].
- PC5 is set for static IP and does not issue a DHCP request.