TECHNICAL REPORT

# TR-043

## Protocols at the U Interface for Accessing Data Networks using ATM/DSL

**Issue: 1.0**
**Issue Date: August 2001**

## 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.

# Table of Contents



**Abstract:**
This document describes protocols that are commonly used or are expected to be commonly used by end-users to access data networks across an ATM over DSL connection. All the listed protocols are useful in satisfying many broadband service requirements that are important for DSL deployment. Certain of the protocols may be selected over others depending upon the service being delivered, and the architectures of the various networks involved in delivering the service to the end user.

# 1 Statement of the project.

## 1.1 Scope

The focus of this document is to document common current and expected (in the near-term) user plane protocols that are transported over ATM over DSL, independent of transmission layer line code, at what is commonly known as the "U reference point" for the application of "access to data networks". This series of recommendations will be dependent upon existing standards, soon-to-be standards, and informational RFCs.

This document reflects The Broadband Forum's consensus on best current practices for deployments of ATM/DSL. "Current" refers to the date of this documents publication.

The doc deals specifically with connection attributes at L2/2.5, not service attributes.

This document will augment information contained in TRs that make reference to and are based on TR-12. Documents that were based on or reference the TR-12 architecture are TR-18, TR-25, and TR-32.

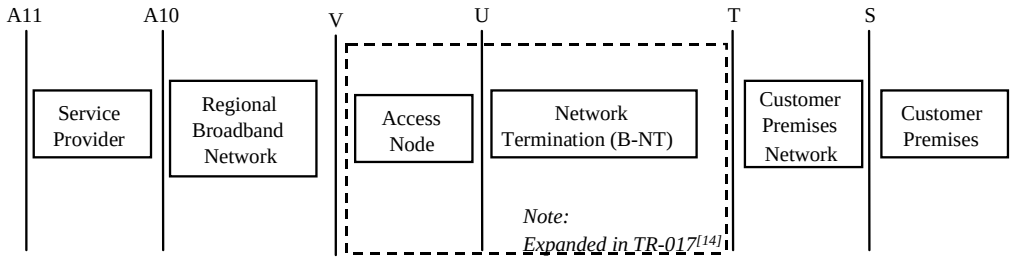
## 1.2 Motivation

TR-012 named PPPoA as The Broadband Forum's standard for use at the "U" interface. This document was written to update the information presented in TR-012, because of changes in the industry over the intervening years. Since publication of TR-012, many service providers have deployed DSL using PPPoE, IP over 2684-encapsulated Ethernet, and IP over AAL5. Part of the reason for this is that there are benefits unique to these solutions that are not provided by PPPoA.

Because these protocols are in wide use, and are used for good reasons, it became necessary for The Broadband Forum to expand its list of "standard" protocols. The new set of protocols needed to be documented, to provide input to Testing and Interoperability, and other Broadband Forum working groups. These groups need input as to what protocols to include in their testing, provisioning, and other scenarios.

# 2 End-to-end Service Interoperability model over DSL systems

## 2.1 Specific Reference model




*NOTE: V, U, S and T correspond to ITU practice*
*A10 and A11 are borrowed from DAVIC as there are no ITU equivalents*

*Figure 1. Architectural reference model*

The end-to-end DSL-based network architecture for convenience can be decomposed into the following subnetworks: the customer premises network, the access network, the regional broadband network and the service provider networks. They are shown in Figure 2.

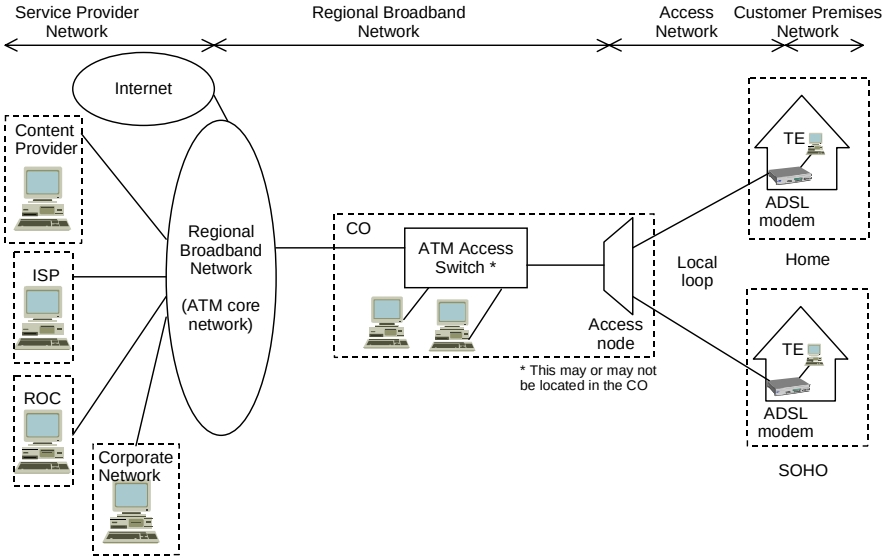



*Figure 2. Example of an end-to-end DSL-based Broadband Network Architecture*

## 2.2 Customer Premises

The customer premises include residences, home offices and small business offices. Each will contain one or more terminal equipment devices (such as PCs, workstations, set-tops, etc.) possibly interconnected by a customer premises network. The DSL modem on the customer premises is called the "B-NT" (Broadband Network Termination).

## 2.3 Access Network

The DSL access network encompasses the DSL modems at customer premises and the access multiplexer system at the CO connected via the local loop. The Broadband TR-017 [2] addresses the layer 2 protocols and specifically describes the implementation of ATM transport over DSL links. TR-017 identifies and defines the functional blocks of ATM-based DSL access network which are formally referred to as Broadband Network Termination (B-NT) for DSL modem and Access Node (AN) for access multiplexer system. The access node is frequently referred to as the "DSLAM" (DSL Access Multiplexer). TR-017 also addresses the control and management planes related to supporting ATM in user plane. It includes the ATM PVC support, signaling for SVC support and operations and maintenance functionality to support ATM over DSL. When the backbone network is ATM, the access node is connected to an ATM access switch. The DSL access node and ATM access switch may or may not be co-located. The function of the access node and access switch is to:

- provide physical port concentration
- provide bandwidth concentration in the form of statistical multiplexing of non-CBR traffic classes
- to possibly provide logical port concentration when a service interworking function is co-located in the access network
- support the ability to offer differentiated services in the network.

### 2.4 Regional Broadband Network

A regional broadband network, interconnects the central offices in a geographical area. The function of the regional broadband network is a combination of transport and possibly switching.

### 2.5 Service Provider Networks

The service provider networks include the ISP POPs, content provider networks, corporate networks and regional operation center (ROC). An ISP POP is for connecting to the Internet and provides ISP services such as e-mail and Web hosting. A content provider network consists of a server farm for distributing content. The corporate networks may be connected to the regional broadband network to allow remote access from a home (telecommuting) or from branch offices. The ROC is operated by the access network operator to manage the entire access network, and possibly to provide value-added services.

## 3 End-to-end Interoperable DSL Network Architecture

### 3.1 Core Network/Regional Broadband Network

Requirements for various configurations of the Core Network can be found in TR-025 [4]. One thing that all the supported network configurations have in common is that they make use of ATM over DSL at the U reference point, identified in [2], going into the access node. The protocols listed below do not change any of the base assumptions or core technologies listed in that document. However, enhancements can be made to that document to better describe the handling of the additional protocol stacks listed below.

### 3.2 Protocol Stacks at the U Reference Point

This section details various protocol stacks that may be used at the U reference point, to support access to data networks and meet the requirements outlined above. All rely on AAL5 over ATM over DSL.

A number of the stacks make use of PPP (Point-to-Point Protocol). Once ATM layer connectivity is established between the customer premises and the service provider network, the session setup and release phases at the link level and network level can be established using PPP.

Several also encapsulate Ethernet over AAL5, allowing the Ethernet used within the end-customer premises to be bridged on to the access network.

See Appendix B for a table directly comparing the protocols listed in this section.

Figure 3 shows the protocol stacks that are documented in this section.

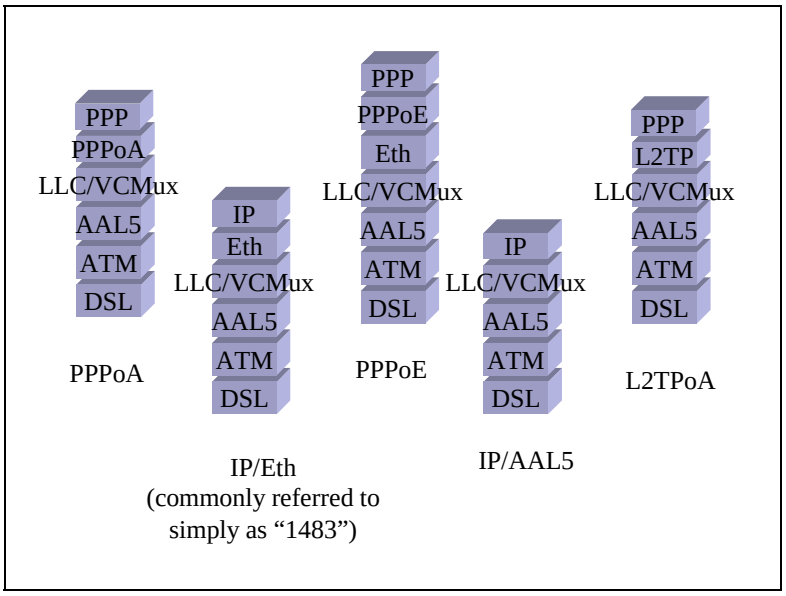



*Figure 3: Protocol Stacks at the "U" Interface*

### *3.2.1 Common Features*

The following protocols are used in more than one of the recommended stacks. They are split out here, so that pros and cons and other attributes of the stacks that are due to the use of these common protocols can be identified once, and not restated each time the common protocol is used. This also makes it more obvious as to what aspect of the stack is the actual cause of that attribute.

#### 3.2.1.1 DSL

The fact that this document is being produced by The Broadband Forum implies that DSL technology will be used at the physical layer, for transporting traffic across twisted copper. No further justification or breakdown of pros and cons will be provided in this document.

#### 3.2.1.2 ATM

ATM is used above the DSL layer in all the stacks discussed in the main body of this document.

**QoS Capabilities**

ATM VCCs can be set up with specific QoS parameters, such as Peak-to-peak CDV (Cell Delay Variation), Maximum CTD (Cell Transfer Delay), and CLR (Cell Loss Ratio). There are also traffic parameters, such as PCR (Peak Cell Rate), SCR (Sustainable Cell Rate), MBS (Maximum Burst Size), MCR (Minimum Cell Rate), and CDVT (Cell Delay Variation Tolerance). These QoS and traffic parameters define specific ATM service categories that may be applied to an ATM VCC. The set of service categories currently defined is CBR (Constant Bit Rate), rt-VBR (real-time Variable Bit Rate), nrt-VBR (non-real-time Variable Bit Rate), UBR (Unspecified Bit Rate), ABR (Available Bit Rate), GFR (Guaranteed Frame Rate), or UBR+ (UBR with MDCR (Minimum Desired Cell Rate).

The most commonly deployed service category for data networking services is UBR, which specifies no QoS or traffic management parameters. When data networking is used for non-real-time applications, it does not have great need for these parameters. Due to the potential impacts of congestion, however, some customers would like to be able to have a minimum guaranteed bandwidth available for their use (as a premium service). This is addressed by the GFR or UBR+ service categories. The original UBR

specifications did not incorporate adaptation layer specific enhancements for congestion management such as PPD/EPD, which has been incorporated into many vendors products and is incorporated into the UBR+ standard.

It is expected that IP will be above the ATM layer at some point in the protocol stack. IP QoS/CoS mechanisms are defined in two forms:

- the INTSERV architecture for which there are specific mappings between INTSERV QoS Mechansisms (best effort, guaranteed service and controlled load) and ATM, as defined in RFCs 2380 through 2382.

  2380: "RSVP over ATM Implementation Requirements"

  2381: "Interoperation of Controlled-Load Service and Guaranteed Service with ATM".

  2382: "A Framework for Integrated Services and RSVP over ATM"

- the DIFFSERV architecture which does not have specific ATM mappings; but work in modifying ATM traffic management to incorporate DIFFSERV concepts is nearing completion at the ATM Forum TM Working group.

ATM QoS guarantees apply to the aggregate of all traffic within the VCC. No ATM layer mechanisms exist to ensure QoS for a subset of the traffic transported by a VCC.

Current deployments of ATM also use PVCs, which require that the service category and required characteristics be defined at time of setup, and not change over time. In theory, SVCs can be set up on an "as needed" basis with the necessary CoS; but they are not widely deployed.

**Auto-Configuration**
ILMI 4.0 is the ATM management protocol selected to implement auto-configuration. See "Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATMDSL CPE Auto-Configuration" TR-037 [12] for a description of auto-configuration of ATM connections, service identification, adaptation layer specifics and encapsulations sitting above the ATM layer.

**Session Multiplexing**
ATM supports multiple ATM PVCs and/or SVCs being transported across the same physical layer, at the same time. For each VCC that is established, one or more sessions (of higher layer protocols) can be placed across that VCC. See "Multi-Protocol Support" in section on AAL5, 3.2.1.3, for further details on multiplexing more than one protocol across a single VCC.

**Payload Efficiency**
For short payloads that do not conform precisely to the size of ATM cells, ATM can be inefficient. This is particularly evident in real-time applications, which tend to have shorter packets. Shorter packets pay a higher price. In data networking, however, most payloads tend to be much longer, and the overhead is less. The minimum overhead is 5 octets of header in every 53 octet ATM cell, causing an immediate overhead of over 10%, before any other protocols are stacked on top. Appendix C shows the payload efficiencies of various protocol stacks, given various payload sizes.

**Current Deployment Status**
Most deployments of DSL today use ATM as the layer 2 protocol. Of these, the vast majority use UBR PVCs for data access.

**Standards**
The ATM Forum and the ITU-T define ATM standards.

#### 3.2.1.3 AAL5

AAL5 is the standard ATM Adaptation Layer used for transport of datagrams over ATM. It was specifically proposed for data applications, although it can be used for all ATM service categories. Its chief advantages are its ubiquity (implemented in all ATM-based devices), efficiency, and simplicity. It is not necessarily the best solution for real-time applications, but can be used.

**Error Detection**
AAL5 provides for error detection but not error correction. This is deferred to higher protocol layers. AAL5 provides a per PDU 32-bit CRC (Cyclic Redundancy Check) protection (the same as for Ethernet), which can be used to detect transmission errors. Use of the CRC may be disabled for applications that are tolerant of bit errors.

Loss of an AAL5 trailer cell will lead to concatenation of partial PDUs. For this reason congestion discard mechanisms will specifically target non-trailer cells (via the use of cell loss priority tagging, CLP 0/1).

**Payload Efficiency**
AAL5 adds 8 octets of overhead to each PDU, in the form of a trailer containing length and CRC. If a protocol multiplexing header such as LLC encapsulation of the protocol above AAL5 is used, then this adds additional overhead. The length of the header is a function of what is being encapsulated. VC multiplexing adds less overhead, but does not permit multiple protocols/sessions to be transported across a single VCC. The adaptation function requires that PDUs begin on cell boundaries. Appendix C shows the payload efficiencies of various protocol stacks, given various payload sizes.

**Session Multiplexing**
AAL5 provides no session multiplexing within a VCC.

**Multi-Protocol Support**
Protocols are encapsulated over AAL5 according to RFC 2684. That document describes two mechanisms for multiplexing data over AAL5: Logical Link Control encapsulation and Virtual Circuit multiplexing.

The LLC Encapsulation method allows multiplexing of multiple protocols over a single ATM virtual connection (VC). The protocol type of each PDU is identified by a prefixed IEEE 802.2 Logical Link Control (LLC) header. This may permit devices to interwork because it is a self-identifying protocol.

In the VC Multiplexing method, each ATM VC carries PDUs of exactly one protocol type. When multiple protocols need to be transported, there is a separate VC for each.VC multiplexing adds no overhead (implying better payload efficiency), while LLC multiplexing requires a link control header.

**Current Deployment Status**
Deployments of ATM/DSL for data networking use AAL5 as the ATM Adaptation Layer. The form of protocol multiplexing used with AAL5 depends on the protocol being encapsulated.

**Standards**
AAL Standards are defined in ITU-T I.363.1, .3, and .5 and by the ATM Forum. IETF RFC 2684 [6] is the proposed standard for encapsulating protocols over AAL5.

For new equipment the backward compatibility between RFC 1483 and RFC 2684 must be taken into account. According to RFC 2684 - the update for 1483 - the receiving bridge (i.e. ATU-R ) should pad frames under a certain length. Older equipment designed according 1483 may not be strictly compliant to RFC 2684.

#### 3.2.1.4 Ethernet

Several of the protocol stacks encapsulate Ethernet over the ATM layer.

**Error Detection**
Ethernet provides 32-bit CRC protection per Ethernet frame. If encapsulated over AAL5, then this is in addition to the error checking performed using the AAL5 trailer.

However, the Ethernet CRC is optional when encapsulated over AAL5. If LLC encapsulation is used, the PID field of the SNAP header indicates the presence of the CRC field.

**Payload Efficiency**
The Ethernet II/DIX header (RFC 894) adds 14 octets of header per Ethernet frame to the payload (1500 bytes). Using LLC/SNAP (IEEE 802.3, RFC 1042) encapsulation within the Ethernet frame limits the frame size to 1492 octets (since it needs 8 octets for LLC/SNAP encapsulation). This should not be confused with RFC 2684 LLC encapsulation that can be used within AAL5. When using LLC encapsulation to encapsulate bridged Ethernet over AAL5 (see [6]), an additional 8 octets (at least) is needed. Appendix C shows the payload efficiencies of various protocol stacks, given various payload sizes.

**Current Deployment Status**
Ethernet over AAL5 is very widely deployed, both as IP/Ethernet/AAL5, and as PPPoE/Ethernet/AAL5. LLC encapsulation of bridged Ethernet frames over AAL5 is the most widely deployed variant of Ethernet over AAL5 (allowing for multiplexing of Ethernet connections across a single ATM PVC).

**Multi Protocol Support**
Ethernet comes in several forms. The two most prevalent are Ethernet II and IEEE 802.3, both of which can support multiple protocols through the use of a protocol discriminator field in the frame header.

#### 3.2.1.5 PPP

PPP at some level above ATM increases the utility of ATM as an access technology. Essential operational functions can be delivered over ATM using features well-established in PPP:

**Auto-Configuration**
PPP embodies a suite of protocols that permit significant negotiation of link layer configuration parameters. The link control protocol (LCP) permits link specifics such as compression, encryption, MTU size, use of multi-link and multi-class support etc. to be negotiated at the start of a PPP session. Upon completion of the authentication phase, network control protocols (NCPs) can be opened, which permit either address discovery or address assignment to be performed. DNS and WINs can be also discovered with proprietary IPCP (the Internet Protocol NCP) extensions.

Where additional IP configuration is required, PPP supports use of DHCP above it to provide configuration of the domain name, DNS server, and default gateway. PPP's well-defined negotiation system has been extended to allow configuration of parameters for many different aspects of a connection, including multiple simultaneous network protocols (IPv4, IPX, IPv6) as well as connection capabilities including encryption and compression. Not all negotiated options of PPP are applicable. See RFC 2364 for further reference.

**Service Selection**
Some architectures support provide service selection at the PPP layer (e.g. LAC/BAS). Through the specification of the domain that the user is attempting to reach, the user can specify the service they are attempting to connect to. See RFC 2486 (how to do qualified domain name signaling).

**QoS Capabilities**
PPP has no QoS capabilities itself, it is transparent to the service model of the serving transport layer. PPP can be augmented with mechanisms to multiplex traffic of differing latency requirements although this requires additional packet fragmentation above the PPP layer (effectively frames in fragments in frames in cells).

**Session Demarcation**
PPP allows the beginning and ending of a network layer session to be clearly demarcated.

**Security**
PPP sessions can be easily established and torn down. This means that the session does not have to be always-on, which provides some added security to the end user in the form of reduced exposure to hacking, and allows the NSP to better utilize its equipment resources.

**Authentication, Authorization, and Accounting (AAA)**
The use of PPP allows NSPs to use existing AAA mechanisms, which they have already deployed. This includes, among others, the use of PAP, CHAP, and token-based systems for authentication, and the use of RADIUS back office systems to do billing, usage metering, and other AAA functions.

**Payload Efficiency**
PPP adds 2 octets of overhead in the form of a protocol multiplexing header. Appendix C shows the payload efficiencies of various protocol stacks, given various payload sizes.

**Multi Protocol Support**
PPP is capable of transporting multiple protocols simultaneously. Each PPP packet includes a protocol identifier field. A protocol-specific Network Configuration Protocol (NCP) must be negotiated for each protocol to be transported.

**Current Deployment Status**
PPP is the most widely deployed mechanism for establishing sessions with NSPs and for doing AAA functions.

### *3.2.2 PPP over ATM (PPP/AAL5/ATM/DSL)*

PPPoA inherits all the traits of DSL, ATM, and AAL5 that have been described above.

**QoS Capabilities**
See “QoS Capabilities” in section on PPP, 3.2.1.5 and on ATM, (3.2.1.2). Since PPPoA dedicates an ATM VCC per PPP session, that PPP session inherits the QoS of that underlying VCC. This allows for separate QoS per PPP session.

**Auto-Configuration**
See “Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATMDSL CPE Auto-Configuration” TR-037 [12] for a description of auto-configuration of PPPoA as the Layer 2.5 protocol sitting above the ATM layer.

See “Auto Configuration” in section on PPP, 3.2.1.5, for a description of auto-configuration capabilities above PPP.

**Service Selection**
See “Service Selection” in section on PPP, 3.2.1.5.

**Security**
See “Security” in section on PPP, 3.2.1.5.

**Authentication, Authorization, and Accounting (AAA)**
See “Authentication, Authorization, and Accounting (AAA)” in section on PPP, 3.2.1.5.

**Session Demarcation**
See “Session Demarcation” in section on PPP, 3.2.1.5.

**Session Multiplexing**
PPPoA supports only a single session per VCC; therefore PPPoA is dependent on ATM session multiplexing. (See "Session Multiplexing" in sections on ATM, 3.2.1.2.) In many deployments a single data PVC is being provisioned, limiting these end customers to a single PPPoA session.

Many CPE and PC software vendors provide Network Address/Port Translation (NAPT) capability to permit multiple hosts on a home network to share a single IP address. This overcomes some of the limitations of the PPPoA service model; but this has limitations, as the full IP service model for both TCP and UDP is not supported.

**Payload Efficiency**
PPPoA does not add any extra octets to the payload, beyond that which has already been described for ATM, AAL5, and PPP. The PPP and AAL overhead in this case is only added once per datagram. Appendix C shows the payload efficiencies of various protocol stacks, given various payload sizes.

**Current Deployment Status**
As the original protocol stack defined by The Broadband Forum in TR-12, this protocol is widely available, and is also widely used. It is particularly common to see PPPoA used in NIC card and USB DSL modem implementations.

**Standards**
PPP over ATM (PPPoA) is specified in the IETF proposed standard for PPP over ATM [3]. In TR-12, The Broadband requires null encapsulation (VC multiplexing) to be the default for PPPoA deployment.

### *3.2.3 IP over Ethernet (IP/Ethernet/AAL5/ATM/DSL)*

**QoS Capabilities**
A number of techniques for accomplishing QoS using IP have been documented and are being standardized by the IETF. If used, these mechanisms may operate independently of ATM QoS (where IP QoS queuing discipline is implemented above ATM) or may use VCC multiplexing and map specific IP flows onto ATM service categories.

QoS that might be defined across the U interface cannot be guaranteed end to end unless 802.1P/Q is employed or layer violations are implemented. There are mapping and overhead issues associated with this. It is not considered in this document and a topic for further study.

**Auto-Configuration**
See "Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATMDSL CPE Auto-Configuration" TR-037 [12] for a description of the mechanism used to communicate configuration of IP over Ethernet transported by the ATM layer.

Auto configuration of IP address, DNS server, etc., can be accomplished through DHCP (RFC 2131), which is host initiated via a Layer 3 broadcast. Within this message the host can identify itself, specific attributes of itself (e.g. manufacturer and model) and specify what configuration parameters it is seeking. Multiple or redundant servers may respond with configuration offers which would include address and address lease time information and other configuration attributes.

**Service Selection**
There are no service selection capabilities in this protocol stack.

**Security**
This stack provides for an always-on connection, which may be considered less secure than a session-driven connection due to the increased exposure to hacking. Powering down the DSL modem or the computer will turn the connection off in this case.

**Authentication, Authorization, and Accounting (AAA)**
There are no AAA mechanisms available. If the NSP receives the Ethernet MAC address, it may choose to use that for authentication. This can become complicated if the user changes their DSL modem, causing the MAC address to change.

**Session Demarcation**
There is no session demarcation.

**Session Multiplexing**
With IP there are no sessions. It is possible, however to do voluntary tunneling above the IP (see Appendix A), to establish sessions with networks that are off the IP network the user is connected to (generally the Internet).

Multiple ATM PVCs can be used to establish connections to multiple IP networks. See 3.2.1.2.

**Multi-Protocol Support**
It is possible to transport PPPoE sessions concurrently with IP/Ethernet. It is possible to multiplex other protocols (IPX etc.) concurrently over Ethernet.

**Payload Efficiency**
This stack has the payload efficiency characteristics described for ATM (3.2.1.2), AAL5 (3.2.1.3), and Ethernet (3.2.1.4). Appendix C shows the payload efficiencies of various protocol stacks, given various payload sizes.

**Current Deployment Status**
This is protocol stack is very widely deployed, currently. Many of the access providers who have deployed it, however, are converting their embedded base to PPPoE. This is chiefly due to the desire to be able to use sessions (more efficient use of network resources) and the desire to do authentication and use existing AAA mechanisms.

**Scalability**
A simple bridged service requires the NSP termination to dynamically learn the MAC addresses of devices in the premises network. The assumption is that the home subnet is bounded to some reasonably small number of devices as to not impact the scalability of the network termination.

**Standards**
See AAL5 “Standards” (3.2.1.3) for encapsulating the Ethernet over AAL5.

IP used directly over Ethernet without a PPP layer is specified in IETF RFCs 846 and 1042 (Ethernet II or IEEE SNAP encapsulation).

To do auto configuration of IP parameters, DHCP (RFC 2131) or BOOTP can be used.

### *3.2.4 PPP over Ethernet (PPP/PPPoE/Ethernet/AAL5/ATM/DSL)*

**QoS Capabilities**
See “QoS Capabilities” in section on PPP, 3.2.1.5.

**Auto-Configuration**
See “Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATMDSL CPE Auto-Configuration” TR-037 [12] for a description of auto-configuration of PPPoE as the Layer 2.5 protocol sitting above the ATM layer.

See “Auto Configuration” in section on PPP, 3.2.1.5, for a description of auto-configuration capabilities above PPP.

**Service Selection**
See "Service Selection" in section on PPP, 3.2.1.5. In addition to this, PPPoE supports a discovery mechanism for determining the correct Ethernet destination for establishing the desired connection. Currently, PPPoE is always destined for the network equipment at the other end of the ATM PVC, so that this is not really needed.

**Security**
See "Security" in section on PPP, 3.2.1.5.

**Authentication, Authorization, and Accounting (AAA)**
See "Authentication, Authorization, and Accounting (AAA)" in section on PPP, 3.2.1.5.

**Session Demarcation**
See "Session Demarcation" in section on PPP, 3.2.1.5.

**Session Multiplexing**
See "Session Multiplexing" in sections on ATM and AAL5, 3.2.1.2 and 3.2.1.3, for a description of the mechanisms that can be used to accomplish ATM layer session multiplexing. PPPoE supports a hierarchy of session multiplexing. An individual Ethernet MAC end point may use the multiplexing identifier in the PPPOE shim header to originate more than one PPP session. Multiple Ethernet MAC endpoints may originate PPPoE sessions onto a single ATM VCC. At the same time, it should also be noted that PPPoE can be used side-by-side with other layer 3 protocols directly over Ethernet.

**Payload Efficiency**
In addition to the payload overhead added by ATM (3.2.1.2), AAL5 (3.2.1.3), Ethernet (3.2.1.4), and PPP (3.2.1.5) (per Ethernet frame), PPPoE adds another 6 octets per Ethernet frame. Note that PPPoE does not support fragmentation of the payload; therefore the implementation of PPP within PPPoE must negotiate an MRU value that limits the size of PPP packets to that which can be transported across Ethernet. Appendix C shows the payload efficiencies of various protocol stacks, given various payload sizes.

**Current Deployment Status**
PPPoE is strongly deployed in both North America and Europe. Many providers are moving towards it as the protocol of choice. It provides the interaction with their existing AAA mechanisms, allows for sessions to be used (instead of always-on connections), and it allows multiple sessions to be established across a single PVC.

**Standards**
See AAL5 "Standards" (3.2.1.3) for encapsulating the Ethernet over AAL5.

PPP over Ethernet (PPPoE) is specified in IETF RFC 2516 [5].

PPPoE currently is documented only as an Informational RFC, and is not on an IETF standards track[1]. It has been noted this RFC does not define a fragmentation mechanism.

### *3.2.5 IP/AAL5/ATM/DSL*

IP can be encapsulated directly over AAL5 (according to RFC 2684 [6]), without an intervening Ethernet or PPP layer. This can be done with or without ATMARP address registration as defined in RFC 2225 [13].

[1]The "Informational" designation is usually used to document "de-facto" protocols or best practices. It indicates that the RFC was considered technically sound by a review by the IESG but is not a product of the IETF working group process.

**QoS Capabilities**
A number of techniques for accomplishing QoS for IP by mapping onto ATM Trraffic management have been documented and are being standardized by the IETF (Intserv ISATM effort) and by the ATM Forum for IP diffserv (Addendum to TM 4.1 Differentiated UBR, Final Ballot, June 2000)..

**Auto-Configuration**
See "Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATMDSL CPE Auto-Configuration" TR-037 [12] for a description of auto-configuration of IP over AAL5.

Auto configuration of IP address, DNS server, etc., can be accomplished in proprietary ways using DHCP, similar to IP over Ethernet. The proprietary component is that the edge router is required to replicate downstream DHCP broadcasts on all VCCs.

If true switched "Classical IP" is implemented as in RFC 2225 [13], then the Service Provider needs to include an ATMARP or NHRP and MARS server to handle IP-ATM address resolution, and to handle IP multicast and broadcast services. (which works very well using point-to-multipoint ATM connections). Auto configuration of hosts on a switched Classical IP LIS can be augmented to discover the NBMA interworking infrastructure via use of the ILMI service directory as described in [14], [15] and [16].

**Service Selection**
There are no service selection capabilities in this protocol stack if implemented for PVCs. Use of NHRP does provide some of the infrastructure for VCC multiplexing for QoS purposes as well as simple switched meshing of hosts within an NSP ATM LIS.

**Security**
This stack provides for an always-on connection, which may be considered less secure than a session-driven connection. Powering down the DSL modem or the computer will turn the connection off in this case, however.

**Authentication, Authorization, and Accounting (AAA)**
There are no AAA mechanisms available, other than by using IPsec-based mutual authentication mechanisms.

**Session Demarcation**
There is no session demarcation.

**Session Multiplexing**
With IP there are no sessions. It is possible, however to do voluntary tunneling above the IP (see Appendix A), to establish sessions with networks that are off the IP network the user is connected to (generally the Internet).

Multiple ATM VCCs can be used to establish connections to multiple IP networks. See 3.2.1.2.

**Payload Efficiency**
This stack has the payload efficiency characteristics described for ATM (3.2.1.2) and AAL5 (3.2.1.3). Appendix C shows the payload efficiencies of various protocol stacks, given various payload sizes.

**Current Deployment Status**
IPOA has been deployed in several of the early DSL deployments, notably in the Far East (Singapore, Hong Kong), and typically for Video on Demand applications. There are deployments in the United States as well.

**Standards**

If IP-ATM address resolution is needed, then an ATMARP server (ATM Address Resolution Protocol) needs to be implemented as described in RFC 2225 [13]. If the complexity of ARP is not necessary, then simply encapsulating the IP using RFC 2684 suffices.

To do auto configuration of IP parameters, DHCP (RFC 2131) or BOOTP can be used in proprietary deployments.

# 4 References


[1] The Broadband Forum TR-010, "Requirements & Reference Models for ADSL Access Networks: The "SNAG" Document"

[2] The Broadband Forum TR-017, "ATM over ADSL Recommendations"

[3] M. Kaycee, G. Gross, A. Lin, A. Malis, J. Stephens, "PPP over AAL5," IETF RFC2364, July 1998

[4] The Broadband Forum TR-025, "Core Network Architecture for Access to Legacy Data Networks over ADSL"

[5] L. Mamakos, et al, "A Method for Transmitting PPP Over Ethernet", IETF RFC2516, February 1999

[6] D. Grossman, J. Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", IETF RFC2684, September 1999

[7] W. Townsley, et al, "Layer Two Tunnelling Protocol (L2TP)" IETF RFC2661, August 1999

[8] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", IETF RFC 2401, November 1998

[9] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", IETF RFC 2406, November 1998

[10] Kent, S. and R. Atkinson, "IP Authentication Header", IETF RFC 2402, November 1998.

[11] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", IETF RFC 2409, November 1998

[12] The Broadband Forum TR-037, "Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM"

[13] M. Laubach, J. Halpern, "Classical IP and ARP over ATM", IETF RFC 2225, April 1998

[14] M. Davison , "ILMI-Based Server Discovery for ATMARP", IETF RFC 2601. June 1999.

[15] M. Davison, "ILMI-Based Server Discovery for MARS.", IETF RFC 2602. June 1999.

[16] M. Davison, "ILMI-Based Server Discovery for NHRP", IETF RFC 2603. June 1999.


# 5 Glossary

| | |
|---|---|
| AAA | Authentication, Authorization, and Accounting |
| AAL | ATM Adaptation Layer |
| AAL5 | ATM Adaptation Layer 5 |
| ADSL | Asymmetric Digital Subscriber Line |
| ARP | Address Resolution Protocol |
| ATM | Asynchronous Transfer Mode |
| ATU-R | Access Termination Unit - Remote (at customer end) |
| B-NT | Broadband Network Termination |
| BOOTP | Bootstrap Protocol |
| CDV | Cell Delay Variation |
| CHAP | Challenge Handshake Authentication Protocol |
| CO | Central Office |
| CO | Connection Oriented |
| CPCS | Common Part Convergence Sublayer |
| CPE | Customer Premises Equipment |
| CRC | Cyclic Redundancy Check |
| CTD | Cell Transfer Delay |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name Service |
| DSL | Digital Subscriber Line |

| | |
|---|---|
| ESP | Encapsulating Security Payload |
| GFR | Guaranteed Frame Rate |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPOA | IP over ATM |
| IPX | Interworking Packet Exchange |
| IPsec | Secure Internet Protocol |
| ISP | Internet Service Provider |
| ITU-T | International Telecommunications Union - Technical |
| L2TP | Layer 2 Tunneling Protocol |
| LAC | L2TP Access Concentrator |
| LLC | Logical Link Control |
| LNS | L2TP Network Server |
| MAC | Medium Access Control |
| NIC | Network Interface Card |
| NSP | Network Service Provider |
| PAP | Password Authentication Protocol |
| PC | Personal Computer |
| PDU | Packet Data Unit |
| PID | Protocol Identifier Governing Connection Types |
| POP | Point of Presence |
| PPP | Point-to-Point Protocol |
| PPPoA | Point-to-point Protocol over ATM |
| PPPoE | Point-to-Point Protocol over Ethernet |
| PVC | Permanent Virtual Circuit |
| RADIUS | Remote Access Dial-In User Service |
| RFC | Request For Comments |
| ROC | Regional Operations Center |
| SNAG | Service Network Architecture Group (The Broadband Forum) |
| SNAP | Sub Network Access Protocol |
| SVC | Switched Virtual Circuit |
| TR | Technical Report |
| UBR | Unspecified Bit Rate |
| VC | Virtual Circuit |
| VCC | Virtual Circuit Connection |

# Appendix A Voluntary Tunnelling Mechanisms

Voluntary tunnelling mechanisms are generally considered a means to permit end-systems to tunnel across an NSP (IP-based) network. This assumes that the user already has access to the NSP, and is attempting to access a second data network by going across the first data network. However, tunnelling can also be used to create a connection across an IP-based core network to the NSP. It could be argued that the core network, in this case, is an NSP, since it must provide the end user with an IP address, in order to set up the tunnel. But since the user may not be able to "surf" widely, given this IP address, it appears to be rather a grey area. It is because of this that voluntary tunnelling mechanisms are documented here as being of interest at the U interface.

None of these mechanisms are currently in use as a means of connecting the end user to the NSP across the core network, from the U interface. But these are considered highly likely near-term future scenarios. The use of L2TP between the LAC of the core network and LNS of the NSP (see [4] for description of this architecture) already exists.

## A.1 L2TP (L2TP/IP/any stack from 3.2)

L2TP provides a mechanism for voluntarily tunneling multiple PPP sessions from the premises. Layer 2 Tunneling Protocol (L2TP) is specified in IETF RFC 2661 [7]. Although it is possible for L2TP to be transported directly across AAL5 (without an intervening IP layer), that implementation is not in use at this time. Current L2TP implementations have it transported across an IP layer.

## A.2 IPsec (IPsec/IP/any stack from 3.2)

It is expected that IPsec will be used heavily in connecting to corporate networks. IPsec provides secure voluntary tunneling over pre-existing layer 3 connectivity using any of the methods outlined in Section 3.2. IPsec is specified in RFCs 2401 [8], 2402 [10], 2406 [9], and 2409 [11]. Other RFCs also apply.

## Appendix B Comparison Table

| Criteria | PPPoA/AAL5 | IP/Ethernet/ AAL5 | PPPoE/Eth/ AAL5 | IP/AAL5 |
|---|---|---|---|---|
| QoS Capabilities | From ATM below and IP above; ATM and IP QoS are separate | From ATM below and IP; ATM and IP QoS are separate | From ATM below and IP above; ATM and IP QoS are separate | From ATM below and IP; ATM and IP QoS are separate |
| Auto-Configuration | TR-037, and discovery protocols | TR-037, and discovery protocols | TR-037, and discovery protocols | TR-037, and discovery protocols |
| Service Selection | PPP domain | None | PPP domain, PPPoE discovery | None |
| Security | Not always-on | Always on | Not always-on | Always on |
| Authentication, Authorization, and Accounting (AAA) | Using PPP | None (MAC address can be authenticated) | Using PPP | None |
| Session Demarcation | PPP sessions | None | PPP sessions | None |
| Session Multiplexing | Distinct PPP sessions, using ATM PVCs | None, but multiple connections using ATM PVCs | Distinct PPP sessions, using PPPoE or ATM PVCs | None, but multiple connections using ATM PVCs |
| Multi-Protocol Support | Can be done through NCPs | Can be encapsulated using AAL5 LLC, Ethernet | Can be encapsulated using AAL5 LLC, Ethernet, and NCPs | None |
| Payload Efficiency | Most overhead is from AAL5/ATM, some from PPP | Most overhead is from AAL5/ ATM, some from Ethernet | Most overhead is from AAL5/ ATM, some from PPPoE, PPP, and Ethernet | Overhead is from AAL5/ ATM |
| Current Deployment Status | Widely deployed | Widely deployed | Widely deployed | Deployed for VoD is Asia |

## Appendix C Protocol Efficiency

These tables identify the payload efficiency of the various protocols included in this document. Also included in these tables, for the sake of comparison, are PPPoE/HDLC and Ethernet. It should be noted that when the protocols are over ATM, there is little difference in efficiency for most payload sizes. The following numbers were used in making some of these calculations. Sample calculations are shown, using Excel spreadsheet formula notation.

- AAL5 adds an 8 octet CPCS trailer to the payload
- LLC encapsulation adds 8 octets per AAL5 payload (without LAN FCS)
- AAL5 payloads use 48 octets per ATM cell
- PPP Protocol ID adds 2 octets; if PPPoA, this is 2 octets per AAL5 payload; if PPPoE, this is 2 octets per Ethernet frame
- PPPoE header adds 6 octets per Ethernet frame
- Ethernet adds 14 octets per Ethernet frame
- An Ethernet frame with LLC/SNAP encapsulation can contain up to 1492 octets (used in PPPoE/Eth/AAL5 and IP/Eth/AAL5)
- An Ethernet frame without LLC/SNAP encapsulation can contain up to 1500 octets (used in PPPoE/HDLC and Ethernet)
- There is a total of 53 octets per ATM cell, with a 5 octet ATM header

To calculate the number of Ethernet frames that will be used to transport a payload: ROUNDUP(IP payload/Ethernet frame size) to the next integer; for PPPoE/Eth/AAL5 transporting a payload of 1024 octets, this is ROUNDUP(1024/1492) = 1.

To calculate the number of ATM cells that will be needed for VCMux IP/AAL5: ROUNDUP((IP payload + 8)/48), where 8 is the AAL5 overhead, and 48 is the number of AAL5 octets in an ATM cell.

For LLC IP/AAL5, this becomes: ROUNDUP((IP payload + 8 + 8)/48)
For VCMux PPPoA, this becomes: ROUNDUP((IP payload + 8 + 2)/48)
For VCMux IP/Eth/AAL5, this becomes: ROUNDUP(((Ethernet frames*14) + IP payload + 8)/48)
For LLC IP/Eth/AAL5, this becomes: ROUNDUP(((Ethernet frames*14) + IP payload + 8 + 8)/48)
For VCMux PPPoE/Eth/AAL5, this becomes: ROUNDUP(((Ethernet frames*(14 + 6 + 2)) + IP payload + 8)/48)
For LLC PPPoE/Eth/AAL5, this becomes: ROUNDUP(((Ethernet frames*(14 + 6 + 2)) + IP payload + 8 + 8)/48)

To calculate the total number of octets used in a stack using ATM: number of ATM cells*53
To calculate the total number of octets in the Ethernet stack: INT(IP payload/1500)*1516 + IF(MOD(IP payload,1500),MAX(48,MOD(IP payload,1500))+16,0)
To calculate the total number of octets in the PPPoE/HDLC stack: INT(IP payload/1500)*(1516+4) + IF(MOD(IP payload,1500),MAX(48,MOD(IPpayload,1500))+16+4,0)

*To calculate the overhead: Total octets/IP payload – 1*

*Table 1: Payload Efficiency for Protocols with PPP*

| IP Payload | PPPoA/AAL5 VC | | | PPPoE/Eth/AAL5 VC | | | | PPPoE/Eth/AAL5 LLC | | | | PPPoE/HDLC | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Cells | Total Octets | Over-head | Frame | Cells | Total Octets | Over-head | Frame | Cells | Total Octets | Over-head | Frame | Total Octets | Over-head |
| 40 | 2 | 106 | 165% | 1 | 2 | 106 | 165% | 1 | 2 | 106 | 165% | 1 | 68 | 70% |
| 48 | 2 | 106 | 121% | 1 | 2 | 106 | 121% | 1 | 2 | 106 | 121% | 1 | 68 | 42% |
| 64 | 2 | 106 | 66% | 1 | 2 | 106 | 66% | 1 | 3 | 159 | 148% | 1 | 84 | 31% |
| 128 | 3 | 159 | 24% | 1 | 4 | 212 | 66% | 1 | 4 | 212 | 66% | 1 | 148 | 16% |
| 256 | 6 | 318 | 24% | 1 | 6 | 318 | 24% | 1 | 7 | 371 | 45% | 1 | 276 | 8% |
| 512 | 11 | 583 | 14% | 1 | 12 | 636 | 24% | 1 | 12 | 636 | 24% | 1 | 532 | 4% |
| 768 | 17 | 901 | 17% | 1 | 17 | 901 | 17% | 1 | 17 | 901 | 17% | 1 | 788 | 3% |
| 1024 | 22 | 1166 | 14% | 1 | 22 | 1166 | 14% | 1 | 23 | 1219 | 19% | 1 | 1044 | 2% |
| 1280 | 27 | 1431 | 12% | 1 | 28 | 1484 | 16% | 1 | 28 | 1484 | 16% | 1 | 1300 | 2% |
| 1500 | 32 | 1696 | 13% | 2 | 33 | 1749 | 17% | 2 | 33 | 1749 | 17% | 1 | 1520 | 1% |
| 3000 | 63 | 3339 | 11% | 3 | 65 | 3445 | 15% | 3 | 65 | 3445 | 15% | 2 | 3040 | 1% |
| 10240 | 214 | 11342 | 11% | 7 | 217 | 11501 | 12% | 7 | 217 | 11501 | 12% | 7 | 10380 | 1% |

*Table 2: Payload Efficiency for Protocols Without PPP*

| IP Payload | IP/Eth/AAL5 VC | | | | IP/Eth/AAL5 LLC | | | | IP/AAL5 VC | | | IP/AAL5 LLC | | | IP/Ethernet | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Frames | Cells | Total Octets | Over-head | Frames | Cells | Total Octets | Over-head | Cells | Total Octets | Over-head | Cells | Total Octets | Over-head | Frames | Total Octets | Over-head |
| 40 | 1 | 2 | 106 | 165% | 1 | 2 | 106 | 165% | 1 | 53 | 33% | 2 | 106 | 165% | 1 | 64 | 60% |
| 48 | 1 | 2 | 106 | 121% | 1 | 2 | 106 | 121% | 2 | 106 | 121% | 2 | 106 | 121% | 1 | 64 | 33% |
| 64 | 1 | 2 | 106 | 66% | 1 | 2 | 106 | 66% | 2 | 106 | 66% | 2 | 106 | 66% | 1 | 80 | 25% |
| 128 | 1 | 4 | 212 | 66% | 1 | 4 | 212 | 66% | 3 | 159 | 24% | 3 | 159 | 24% | 1 | 144 | 13% |
| 256 | 1 | 6 | 318 | 24% | 1 | 6 | 318 | 24% | 6 | 318 | 24% | 6 | 318 | 24% | 1 | 272 | 6% |
| 512 | 1 | 12 | 636 | 24% | 1 | 12 | 636 | 24% | 11 | 583 | 14% | 11 | 583 | 14% | 1 | 528 | 3% |
| 768 | 1 | 17 | 901 | 17% | 1 | 17 | 901 | 17% | 17 | 901 | 17% | 17 | 901 | 17% | 1 | 784 | 2% |
| 1024 | 1 | 22 | 1166 | 14% | 1 | 22 | 1166 | 14% | 22 | 1166 | 14% | 22 | 1166 | 14% | 1 | 1040 | 2% |
| 1280 | 1 | 28 | 1484 | 16% | 1 | 28 | 1484 | 16% | 27 | 1431 | 12% | 27 | 1431 | 12% | 1 | 1296 | 1% |
| 1500 | 2 | 32 | 1696 | 13% | 2 | 33 | 1749 | 17% | 32 | 1696 | 13% | 32 | 1696 | 13% | 1 | 1516 | 1% |
| 3000 | 3 | 64 | 3392 | 13% | 3 | 64 | 3392 | 13% | 63 | 3339 | 11% | 63 | 3339 | 11% | 2 | 3032 | 1% |
| 10240 | 7 | 216 | 11448 | 12% | 7 | 216 | 11448 | 12% | 214 | 11342 | 11% | 214 | 11342 | 11% | 7 | 10352 | 1% |