DSL Forum
Technical Report
TR-044

Auto-Configuration for Basic Internet (IP-based) Services

December 2001

Abstract:

This document describes the procedures recommended to automatically configure connections between B-NT Customer Premises Equipment and Internet Services, focusing on the requirements across the DSL local loop. It specifies the usage of PPP and its related control protocols for services that require authentication, accounting and addressing and DHCP for bridged configurations and extensions beyond the configuration capabilities of a PPP connection.

Table of Contents

Table of Figures

1 Introduction

Consumer Internet Access has evolved from narrowband dial-up modem access to broadband connections provided over a variety of last mile technologies. Service Providers have developed a sophisticated infrastructure to handle authentication, accounting and addressing for mass-market deployment using the Point-to-Point Protocol. These Service Providers want to extend this infrastructure to their high-speed customers with few or no changes. This document describes current best practices for providing access to most Internet (IP-based) services using these standard network technologies.

This document is one of a series of documents that describe an auto-configuration framework across the DSL local loop (the U interface).

- WT-60 [4] provides an overview of the technologies and provides a specific architectural and functional context for the protocols and procedures described herein.
- TR-037 [3] describes use of ATM Forum specifications for configuring the ATM layer of a DSL connection up to the point of exchange of Protocol Data Units across the regional broadband network.
- There are an evolving set of documents within the DSL Forum that describe the overall set of information that maybe required to be configured on a B-NT.

This document provides recommendations for completing the configuration that is started by the mechanisms of TR-037 and required for access to IP-based services.

2 Scope

This document recommends procedures to configure access to IP-based services from an endpoint at the customer premises. This document also prescribes the information to be configured by the recommended procedures. It does not provide solutions for non-IP services such as ATM-hosted voices or video capabilities. It also limits the configuration system to only those mechanisms required to provide IP access. Configuration of services above the IP layer is not the subject of this document.

3 Definitions

All terms and definitions are as established in the document “DSL Auto-Configuration Framework” WT-60 [4]

4 Auto-configuration Procedures

The procedures outlined in this section establish a connectionless IP path between the B-NT and Internet Services. In particular, this section focuses on the configuration following link level connectivity. It presupposes initial path establishment and configuration up to Layer 2 have been achieved via ILMI (or similar procedures for non-ATM DSL links). It focuses on the data link layer (layer 2) and above. It includes the configuration of the network devices required to establish the IP-based service. It does not include the configuration of the services themselves.

There are two overall scenarios under consideration. The first assumes session-oriented access using some variation of PPP. The second assumes an always-on LAN extension paradigm. Direct IP over ATM is for further study.

The procedures used to apply this automatic configuration differ depending on the current state of the IP Service path within its life cycle. The simplified life cycle of an IP services path includes the following stages in order:

1. Establishment
2. Maintenance
3. Termination

The following sections address each phase of this life cycle in order.

4.1 Establishment

After the link level configuration has been established, the DSL network elements, the B-NT and the DSLAM, may then proceed through further automatic configuration steps. Each of these steps is optional and the steps are intended only for use for those IP services and devices that need them. These steps are aimed at establishing configuration and policy at each step until the IP Services path, at layer 3, has been initialized.

The auto-configuration progression includes, in order:

Layer 2-3: including one or more of PPP, PPPoE, IP Network Control Protocol (NCP), L2TP, IP over Ethernet

Layer 3+: DHCP

Beyond this basic set of configuration, the complex configuration of the actual services is outside the scope of this document. The appropriate document covering complex services auto-configuration is identified in the framework document WT-60 [4]

4.1.1 Ethernet

PPPoE and IP over Ethernet both ride over Ethernet. The methods for encapsulating Ethernet (bridged and routed) over AAL5 are described in RFC 2684, Multiprotocol Encapsulation over AAL5 [18]. The RFC specifies a mechanism for extending a packet switched network over the ATM network. There are two modes defined by RFC 2684: -

- VC Multiplexing – supports a single protocol per VC
- Logical Link Control (LLC) Encapsulation – supports a single protocol per PDU

Which mechanism to be used must be pre-designated by the NSP and is communicated to the B-NT via procedures outlined in TR-037 [3].

From the perspective of auto-configuration at establishment, the two variants described in RFC 2684 behave identically.

4.1.2 PPP

The generalized procedure for initiation of a PPP session is:

1) transport variation exchange
2) LCP exchange
3) authentication exchange
4) opening NCPs.

Initiation of access to a Network Service Provider's IP network is as follows:

4.1.2.1 Procedures specific to PPP transport variations:

Some PPP transports have specific startup procedures that must be performed prior to PPP exchange. In the DSL environment, several different means of encapsulating PPP frames are defined. PPP can be carried directly over AAL5 using the mechanisms documented in RFC 2364 [11] , carried in Ethernet frames RFC 2516 [13] which are then encapsulated using the Multiprotocol over ATM standards TR-017 [1], or may be carried using Layer 2 Tunneling Protocol mechanisms as defined in RFC 2661 [17].

L2TP Specific Procedures

Layer Two Tunneling Protocol defined by RFC 2661, with ATM Access Network Extensions as defined in **RFC xxxx** [25], permits multiple PPP sessions to be multiplexed together on a single ATM VCC. This requires that the B-NT implement LAC functionality and perform tunnel establishment procedures with the LNS (which may or may not be located at the VCC network side termination). The recommended procedure is as per RFC 2661. No assumptions should be made about the transport layer by the B-NT in negotiating the tunnel, as the tunnel may span multiple transport layer technologies.

PPPoE specific procedures:

RFC 2516 describes a method for building PPP sessions and encapsulating PPP packets over Ethernet. However, Ethernet is not a point-to-point technology, but a broadcast-based multiple access system. Therefore a device wishing to use the PPP over Ethernet encapsulation must first identify its peer. RFC 2516 defines both a discovery phase and a session phase. The discovery phase involves the use of Ethernet broadcasts to identify one or more Access Concentrators that typically serve as one endpoint of a PPP over Ethernet session. The host selects one of answering Access Concentrators to build a point-to-point session. Details may be found in RFC 2516.

4.1.2.2 Common procedures:

PPP LCP

The PPP, RFC 1661 [7], provides a standardized negotiation algorithm for exchanging configuration information between the peers. The PPP negotiation always starts with the Link Control Protocol (LCP) that is used for establishing, configuring and testing the data-link connection. The LCP negotiation may be followed by an authentication phase and then negotiation of network control protocols (NCPs) that perform basic network layer configuration of higher-layer protocols like IPv4 or IPv6.

The Internet Engineering Task Force has created several standards that describe how PPP should be encapsulated across various data-link layers. There are also several informational documents that describe other implementation of PPP that are in common use, such as PPP over Ethernet RFC 2516.

AAA

In order to ensure that the peers are properly identified and configured, the PPP includes a capability to exchange authentication information, using several alternate mechanisms. The authentication system can also be used to trigger accounting and access control systems. The authentication mechanism is negotiated during LCP exchange.

IP NCP

For Internet services and other services based on the Internet Protocol (IP), a network control protocol, the Internet Protocol Control Protocol (IPCP) has been defined for IP version 4, RFC 1332 [6], and for IP version 6, RFC 2472 [12]. These control protocols provide mechanism for the configuration of IP addresses of the peers. Other extensions provide for specification of Domain Name server addresses, RFC 1877 [8] and for configuration of a subnet of addresses to be used by a peer.

Compliant B-NT devices MUST implement RFC 1877 negotiation of primary and secondary DNS server addresses.

4.1.3 IP over Ethernet

DHCP MUST be used as specified in RFC 2131 [9]. When bridging Ethernet frames across a DSL infrastructure (using RFC 2684 implementations), the same mechanism can be applied.

4.1.4 DHCP INFORM

Additional information may be obtained for an addressed host via the use of the DHCP INFORM operation as described in RFC 2131. This is applicable to PPP scenarios, and is applicable to the LAN extension model once hosts have obtained an address lease. The DHCP INFORM operation skips the addressing aspects of DHCP and allows the client to request other DHCP options based upon their addressed identity.

When combined with user requested options, the DHCP INFORM operation permits additional configuration information to be obtained over multiple transactions. DHCP includes a mechanism for the client to identify what information it is seeking. This Parameter Request List (DHCP option 55) is defined in RFC 2132 [10].

PPP specifics:

For PPP scenarios, when more information is required (beyond address and DNS server) a B-NT MAY use DHCP INFORM. When the specific information is available as a standardized DHCP option, DHCP INFORM MUST be used. For other information, DHCP vendor extensions MAY be used.

Reliability:

Not all B-RASs or NSPs may choose to support responses to the DHCP INFORM message.
Further, since DHCP is not carried over a reliable transport, timing out after a single attempt to solicit configuration information from a DHCP server is not an authoritative indication of a lack of support. Conforming B-NT that require information not available via IPCP MUST make multiple attempts to obtain DHCP information. See RFC 2131 (*sect 4.1*) for recommendations on the retry algorithm.

4.2 Maintenance

The mechanisms in this section are specific to the situation where the IP services path was already established (as outlined in section 4.1). Maintenance refers to configuration changes to an existing connection. Such auto-configuration can be initiated under several circumstances including:

- B-NT restarts.
- B-RAS or NSP service reset or reconfiguration.
- Service originated B-NT reset.
- Service reset.

Regardless of the cause of the update, the mechanisms used in reconfiguration are directly dependent on the mechanisms used in establishing the connection. The means of applying the updates are protocol specific.

4.2.1 PPP

It is possible for a PPP session to be established without actually having an active connection (active IP service) running upon it. If a new connection is needed, a Configure Request message and its reply are exchanged between the two halves of the PPP session. In some states this request is valid and an updated connection is established with the configured values. However, it may also be necessary to tear down the PPP session and establish a new one to meet the client demands. The complete state transition table for PPP is defined in The Point to Point Protocol, RFC 1661.

4.2.2 L2TP

The L2TP behavior during maintenance is similar to PPP but less volatile. An L2TP tunnel may support multiple PPP sessions (one PPP stream per session) between a LAC and LNS pair. As such, PPP sessions may be torn down and new ones established during operational reconfigurations without tearing down the L2TP tunnel. The new PPP sessions will need to be established and configured, as necessary to meet the new session requirements. These new sessions are accomplished within the L2TP tunnel via the Control Connection for the tunnel. In this manner the L2TP tunnel is more stable.

However, as with PPP, if the new configuration requires capabilities outside the existing tunnel's ability to deliver, (for example higher bandwidth than the current VC is configured for) then a new tunnel must be established. It is valid to have multiple tunnels between the same LAC and LNS pair. Therefore, unlike PPP, when a new tunnel must be established to meet the updated requirements, the original tunnel need not be torn down. The establishment of the new tunnel is achieved through the Control Connection for the tunnel as outlined in the preceding establishment section.

Most attributes of the tunnel transport (such as the use of packet sequencing) can be transparently modified by procedures outlined in RFC 2661.

4.2.3 PPPoA

The trigger events discussed above would not normally result in a change from the expected role of the B-NT from bridge to router. Therefore, for most maintenance there is no change in behavior. This is because the multi-protocol encapsulation is VC based not session based.

However, if during an active session, a change occurs between VC Multiplexing and LLC Encapsulation, i.e. the type of session, router or bridge changes, then it is detected and the session is discontinued and the PPP connection torn down.

In this instance there is no operational updating occurring, the connection is removed and must be re-established. See RFC 2364 for more details.

4.2.4 DHCP

DHCP is designed to support configuration changes and provides the mechanism for transmitting them. The mechanism used to establish the new auto-configuration differs depending on which end of the path originated the update, the client or service side:

Client Initiated Updates:

If the client (B-NT) side of the path initiates the changes, the behavior is effectively identical to the establishment sequence previously described. The reconfiguration results in a new DHCP INFORM request being sent to the DHCP server. The behavior thereafter is the same as an establishment sequence.

In addition to the asynchronous updates that may arise for the reasons outlined above, DHCP has a built-in mechanism to keep the client current. When a DHCP server offers configuration data it also tags this data with a time limit. When this DHCP lease on the information expires, it is the client's duty to renew the lease with the granting DHCP server. In this manner, the protocol ensures the client synchronizes with the server on a regular basis. This gives the server the opportunity to update any stale or altered configuration data. The method for lease (and data) renewal is to issue a DHCP REQUEST operation where the IP address is already set just as in a DHCP INFORM operation. The behavior thereafter is the same as an establishment sequence.

Service side updates:

Service-side update can be achieved by variations of client polling or, where PPP is in use, by tearing down the LCP layer. DHCP FORCERENEW command is the preferred method for service-side updates. (RFC 3203 [24])

- For DHCP addressed hosts, the DHCP server can influence the polling rate via the use of specific lease times.
- DHCP addressed hosts may issue DHCP INFORM requests at a rate higher than that triggered by the use of address lease times.
- For addressed hosts that only use the inform option, they may periodically re-issue DHCP INFORM requests to maintain configuration freshness.

If the service side of the IP path wishes to cause a reconfiguration, then additional steps are required. The DHCP server is used to notify the client that it needs to pick up new configuration data. It achieves this by sending a DHCP message to the client of type DHCP FORCERENEW. On receipt of the DHCP FORCERENEW message,

the client issues a DHCP INFORM request to the server. Thereafter, the behavior follows that of client initiated updates, as defined above.

A service side reset, as may be triggered by a DHCP FORCERENEW, will cause the client to trustingly seek new configuration information. Compliant implementations MUST use the DHCP Authentication mechanism as described in RFC 3118 [23] to minimize the likelihood of abuse of the DHCP FORCERENEW mechanism by unauthorized agents. This mechanism will ensure only authorized DHCP servers force the clients into reconfiguration activity. This is achieved via the use of a shared token that would not be of common knowledge. Similarly to the DHCP Relay Agent option, it is proposed that the DHCP authentication mechanism use the PPP_ID as the shared token passed as the configuration token.

4.3 Termination

The procedures in this section discuss the tearing down of an IP services pathway. They assume the connection was already established (as outlined in section 4.1). As with maintenance, such auto-configuration can be initiated under several circumstances including:

- B-NT restarts.
- NSP service disabling.
- Service originated termination.
- Service reset.

The means of tearing down an established and auto-configured IP services connection differ by the underlying protocol.

4.3.1 PPP

Termination of a pathway established by PPP involves the tearing down of the PPP session. A PPP tear down may be initiated from either participating end in the session. The mechanism for this is described in RFC 1661.

4.3.2 L2TP

When an IP path associated with a specific client is torn down, this translates to the teardown of the corresponding PPP session within the L2TP tunnel between the LAC and LNS in question. The mechanism for achieving this is the Control Connection for the tunnel. The process for tearing down these sessions within the tunnel is documented in RFC 2661 and RFC xxxx [25].

The tear down of the session does not translate directly to the tear down of the tunnel. The NSP must decide the policy in this respect. They may choose to tear down the tunnel if this was the last active session within it. They may choose to wait an allotted segment of time before collapsing the still empty tunnel. Or they may choose to keep the tunnel intact, performing idle tunnel removal as a separate network management and engineering activity. The policy decision is up to the NSP.

Similarly, it must be recognized that if the NSP chooses to tear down a non-empty tunnel, there are impacts. All of the PPP sessions within the tunnel will be lost if the tunnel is destroyed. It is recommended the service provider apply a service transition activity to move new sessions from the targeted tunnel to a new one until the targeted tunnel is empty. At that time it is safe to tear down the tunnel.

4.3.3 AAL5 (RFC 2684)

This layer in the auto-configuration protocol stack really supplies a transport mechanism for extending IP paths across multiple layer 2 boundaries. As such, the establishment and tearing down of these connections are tied more to the higher order protocols using them. Essentially, the mechanism is an "always-on" transport protocol.

When a PPP session is torn down, the protocol encapsulation is not destroyed. It just goes idle until it is needed again. In the case of VC Multiplexing this means the entire stream is no longer active. In the case of LLC encapsulation, it means a given stream of PDUs no longer flow. This allows more space for other carried PDUs in the same VC.

What would result in the tearing down of the encapsulation transports would be the removal of the underlying protocol. In this case that would be the removal of the VC over which the encapsulations are applied. No control mechanisms at the encapsulation level are required to allow this to happen.

4.3.4 DHCP

For PPP addressed hosts that only use DHCP INFORM, tearing down the PPP session performs service termination.

For DHCP addressed hosts, service termination corresponds to the DHCP client hitting a state machine reset, and being denied an address in subsequent transactions. In such cases the DHCP server refuses to grant service, replying with a DHCP NAK instead of a DHCP ACK when the request comes in. State machine reset occurs due to lease time expiry or can be triggered by the DHCP FORCERENEW message.

5 Configuration Details

As discussed above, there are three key auto-configuration protocols. These are

- PPP
- L2TP
- DHCP

The details of how they can be used to automatically configure connections are outlined below, including the controlling protocols and configuration options involved.

5.1 PPP

5.1.1 LCP

The Link Control Protocol specification defines a small number of configuration options. Of particular interest for DSL-based PPP sessions are:

- Maximum-Receive-Unit (MRU) and
- Authentication-Protocol.

The MRU configuration is important in PPP over Ethernet implementations because the PPPoE specification adds a demultiplexing header that takes up additional header space. If the MRU is not managed correctly, PPPoE session will not successfully transport IP payloads.

The Authentication-Protocol option is used to identify the authentication mechanism to be used for the session. The primary mechanisms include a simple clear-text password exchanges (PAP) and a more secure challenge handshake mechanism (CHAP), both defined in RFC 1332. RFC 2364 includes an informative section on PPP options that should not be enabled or are irrelevant for broadband implementations (e.g. address and control field compression).

Implementation of this recommendation SHOULD use both the Maximum-Receive-Unit and Authentication-Protocol options.

5.1.2 IPCP

The only configuration option that is required for successful transport of IP over PPP is the IP-Address configuration option. There are compression options, typically more useful over slower links, which are also part of the IPCP specification.

Implementations using PPP and IPCP for Internet services MUST use the IP-Address configuration option to negotiate configuration of the local IP address.

Many devices designed for connection to the Internet also implement a mechanism for discovering the addresses of primary and secondary Domain Name servers, RFC

1877. Implementation of this recommendation MUST use the mechanisms defined in RFC 1877 to discover Domain Name services.

5.2 L2TP

L2TP control channel setup can be performed by either the LAC or the LNS. As the LAC is a transitory entity in the network, it would naturally make sense that the LAC default behavior was to initiate a control channel at startup.

L2TP control channel establishment between a LAC and an LNS includes an optional CHAP-like authentication step. If implemented, this would require the configuration of security information in the B-NT, specifically a shared secret of some form.

Control channel establishment involves the exchange of information much of which is inherent to the implementation.

5.3 DHCP

DHCP supports a wide variety of configuration options. Some of these options are directly applicable to a PPP connectivity model. Some of these options are directly applicable to an extended LAN model (such as with RFC 2684). Some of these options are applicable in both connectivity paradigms. Most of the options involve data that is assigned by the DHCP server to be used in configuration of the client. However, there are a few options, e.g. User Class, which are configurable at the client to help refine the client identification to the server.

The general guidelines for DHCP clients are:

- Must behave as per RFC 2131
- Must allow any valid field and option specified in RFCs 951, 2131, 2132, 2563, 2937, 3004 and 3011 without faulting

6 Operational Considerations

6.1 Use of DHCP Relay Agent

A DHCP server does not have to be embedded in a B-RAS. The B-RAS can pass DHCP messages unmodified. However, this has the effect of decoupling the DHCP server from having direct authoritative knowledge of the connectivity to the subscriber AND adding broadcast traffic to the NSP network. Both are undesirable effects. The solution is to deploy a relay agent in the B-RAS.

As a relay agent, the network device must have a means of identifying a specific client being addressed and configured. This is both for the purposes of identifying the subscriber and service, and to permit correct steering of the downstream server response (and avoiding the need to broadcast specific responses to all clients).

When PPP is the mechanism for initial establishment of the session and the IP address, the relay agent should use the PPP login identifier (PPP_ID) to identify each

separate client to the DHCP server. The relay agent device determines PPP_ID of the client during initialization. Thereafter, the device puts the PPP_ID in the remote-id sub-option field of the DHCP Relay Agent option on outbound DHCP traffic. By tagging the outbound traffic, the relay agent enables the DHCP server to differentiate between individual clients all behind the same port and to target replies back to the same clients.

There may also be value in having a specific circuit in the service side be addressable. Such as in the case where there are multiple network application server (NAS) communities reachable by the same DSLAM. By tagging the DHCP requests for the appropriate NAS community, the DHCP server knows the service community for which the client is to be configured. This may be accomplished through the DHCP Relay Agent option, circuit_id sub-option field.

The capability to act as and support the behavior of a DHCP Relay Agent is optional. If a network element does not support this functionality, it should ignore the Relay Agent option and its sub-options with no impacts. For more details see RFC 3046, DHCP Relay Agent Information Option [22].

7 Flow through and OSS considerations

Use of PPP_ID brings forth the benefits of single sign-on allowing for one ID and authentication/password mechanism for all higher levels of connectivity and configuration. These benefits also apply when complex configuration (as discussed in the framework document) is taken into account.

Two of the single sign-on benefits of using the client's PPP_ID as a common key are achieved in DHCP. As discussed above, the DHCP Relay Agent can use the PPP_ID of the client to relay the DHCP requests and responses correctly and efficiently. Similarly, the DHCP Authentication mechanism can take advantage of the PPP_ID that is known to both parties. It can be used as the configuration token that provides the basis for verifying that the client and server talking to each other are who they say they are.

In both DHCP cases, the client PPP_ID can be known to the NSP in advance and can be bulk or pre-provisioned in the DHCP servers before the client attempts to gain service.

8 Security considerations

Implementations of the PPP include the capability to identify and authenticate peers of a PPP connection. While the mechanisms are not foolproof, they do provide security equivalent to that being used by other Internet access methods. B-NT L2TP implementations may be able to establish tunnels without authentication (depending on whether the CHAP challenge is employed). However this is considered to be a minimal risk:

- For L2TP over AAL5 the tunnel originator can be authoritatively known.

- For PPP over L2TP over AAL5, PPP authentication mechanisms will still be employed by the LNS.

As mentioned above, DHCP also has a mechanism to ensure some minor level of security. The details of DHCP authentication are documented in RFC 3118 [23]. This mechanism ensures only valid servers and clients are communicating and configuring. They may use the PPP_ID as a shared key for the configuration token.

Even with the authentication option, DHCP must be used with care. A security improvement can be gained with judicious use of the circuit_id sub-option of the DHCP Relay Agent option combined with the DHCP Client Identifier option. In the instance where multiple B-NT's share the same VC to a RAS, which is acting as a relay agent, an exposure exists. If a broadcast DHCP request is sent from one of the B-NT's on the shared VC via the relay agent, then, with no additional refining information, when the reply is received at the relay agent it would be necessary to multicast the reply to each of the B-NT's on the shared VC. By using the two options named above, the VC can be uniquely identified (by the Client Identifier) and the specific B-NT on the shared VC can be identified through the Circuit_ID. The result is a unicast reply is sent only to the originator of the request, as per the original intent of the DHCP design.

This recommendation does not address the security of the underlying data-link layer, nor does it address the security of the information carried over the IP layer.

9 References

[1]	TR-017	ATM over ADSL Recommendation	DSL Forum	March 1999
[2]	TR-032	CPE Architecture Recommendations for Access to Legacy Data Networks	DSL Forum	May 2000.
[3]	TR-037	Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM	DSL Forum	March 2001
[4]	WT-60	DSL Auto-Configuration Framework – Initial Baseline	DSL Forum	March 2001
[5]	RFC 951	Bootstrap Protocol (BOOTP)	Bill Croft, John Gilmore	September 1985
[6]	RFC 1332	Internet Protocol Control Protocol	McGregor G.	May 1992
[7]	RFC 1661	Point-to-Point Protocol	Simpson W.	June 1994
[8]	RFC 1877	PPP Internet Protocol Control Protocol Extensions for Name Server Addresses	S. Cobb.	December 1995
[9]	RFC 2131	Dynamic Host Configuration Protocol	Droms R..	March 1997
[10]	RFC 2132	DHCP Options and BOOTP Vendor Extensions	Alexander, R. Droms	March 1997
[11]	RFC 2364	PPP Over AAL5	Gross, G.	July 1998
[12]	RFC 2472	IP Version 6 over PPP	Haskin, E. Allen.	December 1998
[13]	RFC 2516	Method for Transmitting PPP Over Ethernet (PPPoE)	Mamakos, L.	February 1999

[14]	RFC 2563	DHCP Option to Disable Stateless Auto Configuration in IPv4 Clients		May 1999
[15]	RFC 2608	Service Location Protocol, Version 2	Guttman et.al	June 1999
[16]	RFC 2610	DHCP Options for Service Location Protocol	C. Perkins, E. Guttman	June 1999
[17]	RFC 2661	Layer Two Tunneling Protocol "L2TP"	W. Townsley, A. Valencia A. Rubens, G. Pall, G. Zorn, B. Palter	August 1999
[18]	RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5	Grossman, D., Heinanen, J.	September 1999
[19]	RFC 2937	The Name Service Search Option for DHCP	C. Smith	September 2000
[20]	RFC 3004	The User Class Option for DHCP	G. Stump, R. Droms, Y. Gu, R. Vyaghrapuri, A. Demirtjis, B. Beser, J. Privat	November 2000
[21]	RFC 3011	The IPv4 Subnet Selection Option for DHCP	G. Waters	November 2000
[22]	RFC 3046	DHCP Relay Agent Information Option	M. Patrick	January 2001
[23]	RFC 3118	Authentication for DHCP Messages	R. Droms, W. Arbaugh,	June 2001
[24]	RFC 3203	DHCP Reconfigure Extension	P. De Schrijver, Y. T'Joens, C. Hublet	December 2001
[25]	RFC xxxx	Layer Two Tunnelling Protocol: ATM Access Network Extensions	Y. T'Joens, P. Crivellari, B. Sales	January 2001

Appendix A: Use Cases (Informative)

There are several use cases that will help to illustrate that procedures outlined in this document. They include:

Direct DSL Connected PC, PPP only

1. Establish a PPP connection between a B-NT and an IP Service provider where the B-NT is the PC itself with an embedded DSL modem:
    a. The VC connection is established between the DSLAM and the B-NT.
    b. In order to connect to the network a PPP session must be established.
    c. As part of the initial network engineering the type of multi-protocol encapsulation to be used over the ATM portion of the link must be predetermined. The choices are VC-Multiplexed or Logical Link Control (LLC). If VC-Multiplexing is used then a single PPP session will be mapped to a single VC. However, if LLC is used, each PDU must be prefixed with an in-band LLC header.
    d. The PPP session is initiated by running the PPP client on the PC.
    e. Link Control Protocol (LCP) negotiation is used to establish the basic link operation and negotiates authentication.
    f. When connectivity is reached with the service end PPP termination, the client must be authenticated. A user ID and password must be supplied. This will be verified and authenticated by the ISP.
    g. IPCP is used to assign an IP address to the client from the ISP's subnet. The address is assigned only for the duration of the PPP session.
    h. IPCP is also used to provide primary and secondary DNS server addresses (RFC 1877).
    i. The PC is configured and operational.

Direct DSL Connected PC

2. Establish a PPP connection between B-NT and IP Service provider[1]. Where the B-NT is the PC itself with an embedded DSL modem. DHCP is used to set the web, domain, name and configuration servers for the connected client:
    a. Initial VC connection is established between the DSLAM and the B-NT
    b. In order to connect to the network a PPP session must be established.
    c. As part of the initial network engineering the type of multi-protocol encapsulation to be used over the ATM portion of the link must be

[1] Note that with only slight modification, this scenario can be applied to PPP extension architectures as described in TR-032 [2]

predetermined. The choices are VC-Multiplexed or Logical Link Control (LLC). If VC-Multiplexing is used then a single PPP session will be mapped to a single VC. However, if LLC is used, each PDU must be prefixed with an in-band LLC header.

d. The PPP session is initiated by running the PPP client on the CPE PC.

e. Link Control Protocol (LCP) negotiation is used to establish the basic link operation and negotiates authentication.

f. When connectivity is reached with the service end PPP termination, the client must be authenticated. A user ID and password must be supplied. This will be verified and authenticated by the ISP.

g. NCP is used to assign an IP address to the client from the ISP's subnet. The address is assigned only for the duration of the PPP session.

h. Once PPP connectivity is established and an IP address is assigned then the terminating PC will issue a DHCP INFORM message. The message will include the PC's Client Identifier (if available) and the assigned IP address in the ciaddr field of the request.

i. The ISP's DHCP server will respond with the appropriate configuration information in a DHCP ACK message. The configuration information will be obtained by the DHCP server looking up the appropriate entry, keyed by IP address and Client ID. The information will be passed as follows:

j. Configuration Server passed in **siaddr** field

k. Domain passed in **Domain Option** (option 15)

l. Web Server passed in **Default Web Server Option** (option 72)

m. The PC is configured and operational.

Residential Gateway to CPE LAN

3. A CPE LAN is insulated from the public IP network by a Residential Gateway (RGW). The RGW acts as a network address translator (NAT), a service location protocol (SLP), RFC 2608 [15], proxy and a session initiation protocol (SIP) proxy.

    a. The RGW establishes connectivity to the RAS. Either PPP or IP over Ethernet may be used. (Where authentication is required, the RGW will be manually configured with the appropriate User ID and Password for the service).

    b. The IP address, when it is assigned, is bound to the network interfacing side of the RGW, not the CPE LAN side.

    c. Once IP connectivity has been established, as described in Use Case Number 2 above, a DHCP INFORM message is sent. If SLP is being used, the **Parameter Request List Option** (option 55) in this message is

configured to request the **Service Location Protocol (SLP) Option** (option 78)

d. When the ISP's DHCP server responds with a DHCP ACK, option 78 is set to the URL of the SLP server.

e. The RGW extracts the SLP server from the message and populates a resident DHCP server for the CPE LAN.

f. When a device from within the CPE LAN performs a DHCP request, the RGW will not forward the request. Instead, the RGW will reply directly to the CPE LAN device granting it an address from the CPE LAN's subnet and identifying itself as the SLP server.

g. Any SLP requests originating from the CPE LAN will be relayed to the network by the B-NT SLP proxy, which can similarly inspect and modify responses should specific services require similar ALG proxy functions (e.g. SIP).

A Change in Service

4. Consider the PPP session from use case 2. Now change the connection to a higher bandwidth.

   a. Initialization will occur as per Use Case #2 above.

   b. The customer then makes a request for higher bandwidth from the service provider.

   c. The service provider sets up for the new service (i.e. a higher bandwidth defined against the service.) The change of layer 2 may introduce a service interruption that will tear down the current PPP session.

   d. The user attempts to re-enter by starting the PPP session all over again.

   e. The remainder of the PPP initialization will follow the process from Use Case #2.

Multiple Service Providers

5. This document recognizes the possibility of auto-provisioning of multiple IP network interfaces for DSL CPE. This "multi-homing" approach to IP network connectivity can open up the possibility of a number of conflicting parameters being defined for IP routing and service-related ISP parameters (news, email, etc.). The issues of multi-homing are beyond the scope of this recommendation. Instead, the relevant documents within the IETF regarding multi-homing should be consulted. For conflicting parameters involving ISP services such as email or news the policy for resolving these conflicts would be left up to individual implementations.

Appendix B: State Transition Diagrams

Generic PPP state transition diagram

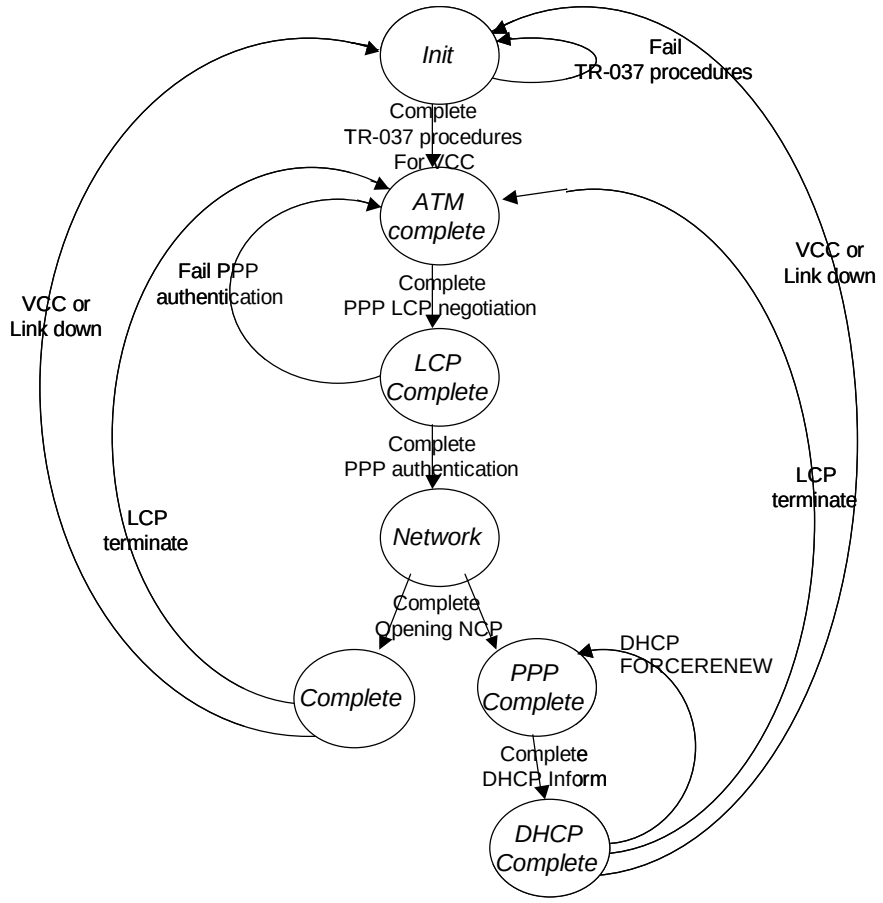

Figure B.1 Generic PPP state transition diagram

Generic Ethernet state transition diagram

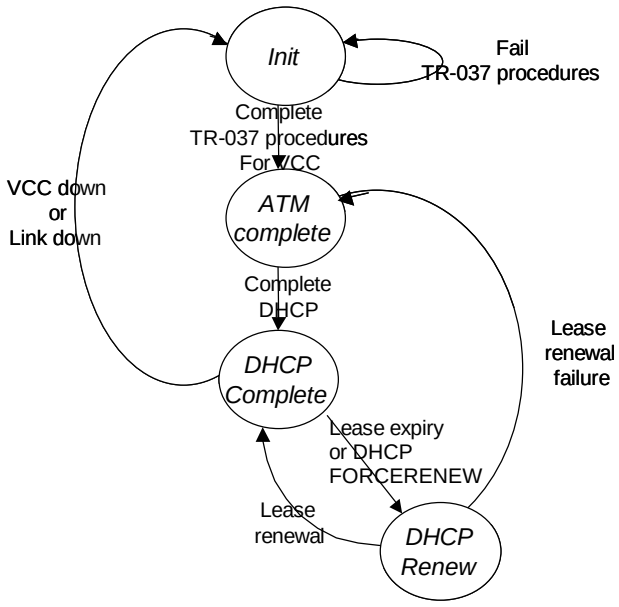

Figure B.2 Generic Ethernet state transition diagram

Appendix C: Caveats

The ILMI mechanism of TR-037 constrains each ATM virtual circuit connection to supporting a single encapsulation method. Therefore, deployments that support multiple services must use multiplexing methods above the link-layer encapsulation. For example, a single ATM virtual circuit connection may be configured to support RFC 2684 encapsulation. Multiple services over the single VCC could be provided using higher layer multiplexing such as PPPoE or L2TP.