ND1009:2002/05

PNO-ISC/SPEC/009

Layer 2 Tunnelling Protocol

Network Interoperability Consultative Committee
Oftel
50 Ludgate Hill
London
EC4M 7JJ
UK

http://www.oftel.gov.uk/ind_groups/nicc/

Liability

Whilst every care has been taken in the preparation and publication of this document, NICC, nor any committee acting on behalf of NICC, nor any member of any of those committees, nor the companies they represent, nor any person contributing to the contents of this document (together the “Generators”) accepts liability for any loss, which may arise from reliance on the information contained in this document or any errors or omissions, typographical or otherwise in the contents.

Nothing in this document constitutes advice. Nor does the transmission, downloading or sending of this document create any contractual relationship. In particular no licence is granted under any intellectual property right (including trade and service mark rights) save for the above licence to copy, store and distribute this document and to produce derived copyright works.

The liability and responsibility for implementations based on this document rests with the implementer, and not with any of the Generators. If you implement any of the contents of this document, you agree to indemnify and hold harmless the Generators in any jurisdiction against any claims and legal proceedings alleging that the use of the contents by you or on your behalf infringes any legal right of any of the Generators or any third party.

None of the Generators accepts any liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance on the contents of this document for any purpose.

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary,
Network Interoperability Consultative Committee,
Oftel,
50 Ludgate Hill,
London,
EC4M 7JJ.

PNO-ISC SPECIFICATION NUMBER 009
Layer 2 Tunnelling Protocol

NETWORK INTEROPERABILITY CONSULTATIVE COMMITTEE
Office of Telecommunications
50 Ludgate Hill
London EC4M 7JJ

SEE PAGE 2 FOR THE NORMATIVE INFORMATION

0.2 Normative Information

All enquiries about distribution reproduction, changes and clarifications should be addressed in the first instance to the Chairman of the NICC/PNO-IG/ISC at the address on the title page.

DISCLAIMER The contents of this specification have been agreed by the NICC. The information contained herein is the property of the NICC and is supplied without liability for errors or omissions.

0.3 Contents

0.4 History

Revision	Date of Issue	Updated By	Description
Issue 1	September 2001	PNO-ISC	Not published, for internal use within PNO-ISC
Issue 2	May 2002	PNO-ISC	First published Issue

0.5 Issue Control

SECTION	ISSUE	DATE
All	Issue 2	May 2002

0.6 References

[1] IETF RFC 2661 Layer Two Tunnelling Protocol “L2TP”, Townsley, et al August 1999.

[2] IETF RFC 1661 The Point-to-Point Protocol “PPP”, Simpson July 1994.

[3] Code of Practice for Network Operators In Relation to Customer Line Identification Display Services and Other Related Services, 2nd Edition June 1998.

[4] UK Telecommunications (Data Protection and Privacy) Regulations 1999.

[5] IETF RFC2809, “Implementation of L2TP Compulsory Tunnelling via RADIUS”

0.6.1 Reference Sources

[1], [2], [5], available at http://www.ietf.org/rfc.html

[3], *available at* http://www.oftel.gov.uk/ind_groups/cli_group/index.htm

[4], *available at* http://www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/ec_telecomms_data_protection.shtml

0.7 Glossary of terms

0.7.1 Abbreviations

AVP	Attribute Value Pair
BAS	Broadband Access Server
CLI	Caller Line Identification Calling Line Identity
ICRQ	Incoming Call Request
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
L2TP	Layer 2 Tunnelling Protocol
LAC	L2TP Access Concentrator
LCP	Link Control Protocol
LNS	L2TP Network Server
MRU	Maximum Receive Unit
MTU	Maximum Transmission Unit
NAS	Network Access Server
PPP	Point-to-point protocol
RFC	Request For Comment
SOHO	Small Office, Home Office
IP	Internet Protocol [IETF]
RADIUS	Remote Authentication Dial In User Service [IETF]
UDP	User Datagram Protocol [IETF]

0.7.2 Definitions

LAC (L2TP Access Concentrator): A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP Network Server (LNS). PPP connections from remote hosts, connected via either narrow-band or broadband, are concentrated by the LAC, and then tunnelled using L2TP over a network to an LNS. Alternatively a host, which runs L2TP natively, i.e. a local LAC client, may interwork directly with an LNS.

LNS (L2TP Network Server): A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP Access Concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunnelled from the remote system (originator) by the LAC.

0.8 Scope

This document specifies the UK requirements for the Layer 2 Tunnelling Protocol (L2TP).].

The transport of the L2TP is not within the scope of this specification.

0.9 Future Considerations

0.9.1 Future Consideration 1

At the time this specification was written the Public Network Operators Interconnect Standards Committee (PNO-ISC) was aware that the L2TP RFC 2661 [1] was in the process of being extended by the IETF. When the IETF have completed these extensions the PNO-ISC will review and revise this specification to take into consideration the changes made to L2TP which are relevant for the UK.

Further information on the IETF extensions to L2TP can be found at:

http://www.ietf.org/html.charters/l2tpext-charter.html.

0.9.2 Future Consideration 2

There is a UK requirement for CLI data to be handled according to its privacy markings when within a telecoms operators environment. Oftel have suggested that CLI information must be supplied with all CLI data (including "CLI Available, CLI Unavailable and CLI Withheld"), (See section 9.3).

The support of this capability is dependant upon there being suitable agreed methods implemented, this is outside of the L2TP-TG domain as it will impact other IP based delivery methods services and be dependant upon the end service solutions offered.

1 Introduction

The Public Network Operators Interconnect Standards Committee (PNO-ISC) has produced this UK delta of IETF RFC 2661 [1]. This document specifies the profile to be used for a national Layer 2 Tunnelling Protocol (L2TP) interface.

1.1 Background

PPP provides a standard method for transporting user datagrams over point-to-point links. L2TP [1] extends the use of PPP as an encapsulation and negotiation protocol to allow the transport of PPP between different networks and nodes via the establishment of a tunnel between a L2TP Access Concentrator (LAC) and L2TP Network Server (LNS). The tunnel consists of a control connection and zero or more L2TP sessions.

1.2 Network Architecture Reference Model

The network architecture reference model used is described in figure 1 below:

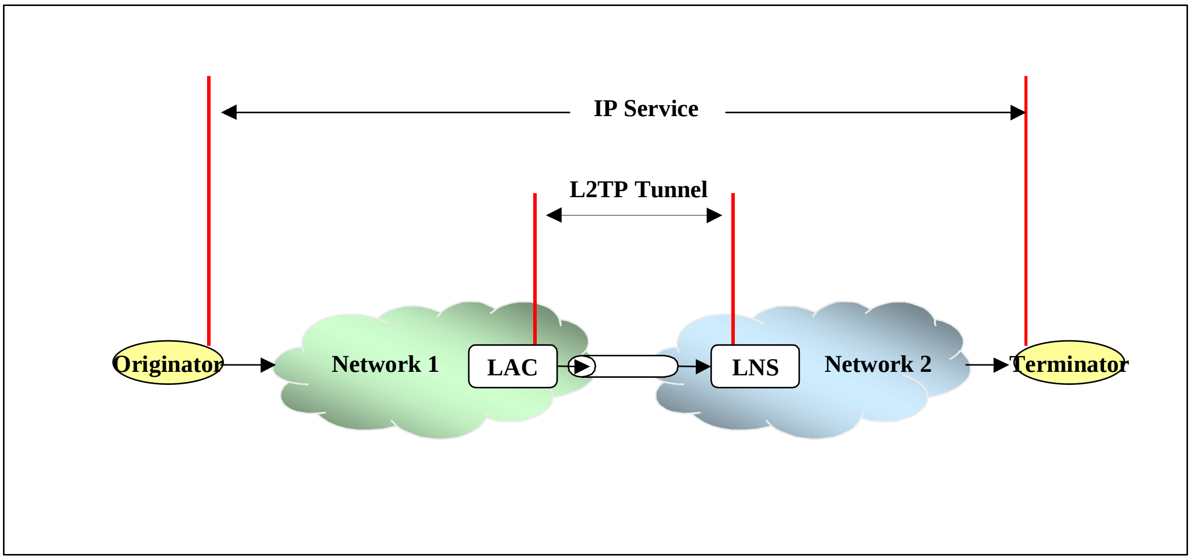

Figure 1 Network Architecture Reference Model

2 Sequence Numbers on the data channel

2.1 IETF RFC 2661 Paragraph references

This is covered in RFC2661 [1] paragraph 5.4.

2.2 Descriptive text/clarification

Sequence Numbers are mandatory for the control messages (see section 3.1 of RFC 2661 [1], 4th paragraph below figure 3.1) and information is provided on how to use the sequence numbers in section 5.8 of the RFC. Sequence numbers are optional for Data Messages and if they are present no information is given on how they are to be used.

Some LNS devices currently discard out of order data, if sequencing is enabled. The use of sequencing is unlikely to improve results, primarily because of the use of IP when using PPP over L2TP; and IP works healthily when packets arrive out of order.

If sequence numbers are received when not expected this would not cause a problem. The wording in the standard is not ambiguous.

The use in the UK of sequence numbers on the data messages is not a requirement.

2.3 UK Requirement

No extra UK requirement, RFC 2661 [1] paragraph 5.4 applies

3 Hello Message

3.1 IETF RFC 2661 Paragraph references

This is covered in RFC2661 [1] paragraph 5.5.

3.2 Descriptive text/clarification

The use of Hello messages is optional and if used timer values would have to be defined.

The standard does not prescribe how often Hello messages should be sent, but a good implementation would probably use it. Even if a peer does not expect Hello messages, it should still ZLB-Ack it, should it receive one - this completes loop checking connectivity to the peer.

Implementations shall be "Hello" tolerant.

The UK shall permit the reception of Hello messages but their use is not mandated.

3.3 UK Requirement

No extra UK requirement, RFC 2661 [1] paragraph 5.5 applies.

4 Back-off algorithms

4.1 IETF RFC 2661 Paragraph references

This is covered in RFC2661 [1] paragraph 5.8.

4.2 Descriptive text/clarification

The RFC2661 [1] defines the use of a back-off algorithm.

The UK needs to define the use of back off times in the algorithm for the UK.

The RFC2661 [1] states that implementations MUST employ an algorithm and may use the recommended default timer of 1 second.

4.3 UK Requirement

Retransmission timer, initial value of 1 second followed by an exponential back off.

If no peer response is detected after 5 retransmissions, the tunnel and all sessions within shall be cleared.

5 Congestion Control

5.1 IETF RFC 2661 Paragraph references

This is covered in RFC2661 [1] paragraph 5.8.

5.2 Descriptive text/clarification

The default recommended in RFC 2661 [1]; is basic but good enough in most situations.

There are enhancements to congestion control in RFC2661bis, which is not yet available. This issue would need to be addressed again in the future once RFC2661 [1] has been replaced.

5.3 UK Requirement

No extra UK requirement, RFC 2661 [1] paragraph 5.8 applies

6 Session Establishment

6.1 IETF RFC 2661 Paragraph references

This is covered in RFC2661 [1] paragraphs 4.4.5 and 6.6.

6.2 Descriptive text/clarification

There are two methods of establishment, the choice of which is dependent on the way the vendor's LAC interacts with the client during session establishment and hence how it then interacts with the LNS. RFC 2661 [1] permits either method without one being preferred over the other.

There appears to be a need for flexibility here since each are equally valid and should be available.

In the UK the LNS would have to be able to react appropriately depending on which information is populated in the optional attributes present in the ICRQ and associated messages.

During the L2TP call set-up, the LAC and LNS should enable either of the end to end PPP Link Control and Authentication behaviours as discussed in RFC2661 [1] 6.6 and 4.4.5, and detailed in RFC2809 [5].

IETF RFC2809 [5], “Implementation of L2TP Compulsory Tunnelling via RADIUS” [5], discusses the operation of PPP, the Access Server and Tunnel Server, and the options for authentication at the BAS/NAS and LNS, and covers these session establishment options in detail.

6.3 UK Requirement

The UK shall allow use of either method of PPP Link Control and authentication as described in RFC2661 [1].

The UK shall permit the sending and reception of Proxy LCP and authentication AVPs as described in RFC2661 [1].

7 Releasing a tunnel

7.1 IETF RFC 2661 Paragraph references

This is covered in RFC2661 [1] paragraph 7.6.

7.2 Descriptive text/clarification

This is concerned with when to release a tunnel (not a session) when there are no sessions present. In theory the tunnel can be left in place indefinitely waiting for a new session to be established. At the other end of the scale the tunnel could be removed as soon as the last remaining session is cleared.

The decision on when to release a tunnel may be related to the keep alive (hello) messages.

Either side of the interface (LAC or LNS) can release the tunnel when they wished.

7.3 UK Requirement

No extra UK requirement, RFC 2661 [1] paragraph 7.6 applies

8 Fragmentation

8.1 IETF RFC 2661 Paragraph references

This is covered in RFC2661 [1] paragraph 8.1.

8.2 Descriptive text/clarification

RFC2661 [1] states for L2TP over UDP/IP fragmentation:

"IP fragmentation may occur as the L2TP packet travels over the IP substrate. L2TP makes no special efforts to optimise this. A LAC implementation MAY cause its LCP to negotiate for a specific MRU, which could optimise for LAC environments in which the MTU's of the path over which the L2TP packets are likely to travel have a consistent value."

Fragmentation is dependent on MRU size and the underlying transport.

The use of fragmentation and the need to manage packet size to minimise or avoid its impact is an implementation option dependent on the environment in which L2TP is used and the services carried.

8.3 UK Requirement

No specific UK requirement

9 Attributes

9.1 IETF RFC 2661 Paragraph references

This is covered in RFC2661 [1] paragraph 4.4

9.2 Descriptive text/clarification

This concerns those attribute descriptions that have the phrase ‘Contact between the administrator of LAC and LNS may be necessary’, particularly ‘called number’, ‘calling number’ and ‘sub-address’.

9.3 UK Requirement

In order to be able to comply with the UK Telecommunications (Data Protection and Privacy) Regulations 1999 [4] and relevant European data protection legislation, appropriate rules such as those defined in the *Code of Practice for Network Operators in relation to Customer Line Identification Display Services and Other Related Services [3]* must be followed with respect to all CLI data.

The application of this CLI requirement would be dependent upon the service description of the particular service offering (i.e. whether the CLI would be used for presentation to the called customer). It would also depend upon the status of the recipient of the information i.e. it would not be appropriate to forward CLI Information with a classification of "Unavailable" or "Withheld" to a body not conformant to the relevant *Code of Practice*.

Due to the constrains of the existing L2TP specification, these CLI requirements may be satisfied by assuming a default classification of “Available” and only sending CLIs of that class. In which case, any CLI information that does not have an “Available” classification shall not be included in the Calling Number AVP.

Alternatively, as a non mandatory option, if the terminating operator/ISP requests the delivery of all CLI data and the originating network supports this option then all CLI data may be sent, but must be treated by the recipient network as “Unavailable”. This latter option is only applicable where the recipient is conformant to a relevant *Code of Practice* and so the privacy of the CLI is guaranteed to be respected.

The CLI information provided shall be a number suitable for display purposes and shall include a leading “0” or “00”.

It should be noted that some existing implementations of L2TP which are designed for use in a purely national CLI environment generate CLI information without including the leading “0” or “00”. Whilst CLI information in this format is potentially ambiguous, there is no requirement to include these prefixes where both the tunnel originator and the terminating operator/ISP agree to use this format. It should be noted that CLIs which do not include a leading “0” or “00” are not suitable for display in their unmodified form.

Future development of this specification may allow all CLI classifications, types and associated indicators to be explicitly included (paragraph 0.9.2 refers) which may be acted upon in order to satisfy the requirements of the CLI *Code of Practice*.

9.4 Advisory Information.

a) CLIs which do not include a leading "0" or "00" should not be used directly in a CLI display service.

b) CLIs not including a leading “0” or “00” are potentially ambiguous in a national/international CLI environment. Knowledge of UK and other national numbering plans may help to resolve ambiguity;

c) Terminating operators/ISP’s can distinguish potentially ambiguous CLIs from the unambiguous CLIs (which include a leading “0” or “00”).

END OF PNO-ISC/SPEC/009