Point-to-Point Protocol Extension Group
INTERNET DRAFT
Expires May, 1999

Mikael Latvala
Oy L M Ericsson Ab
November, 1998

Semi Connected Mode for PPP links
<draft-ietf-pppext-scm-01.txt>

Status of this Memo

Abstract

The Point-to-Point Protocol (PPP) [1] provides a standard method for transporting multi-protocol datagrams over point-to-point links.

This document introduces a new PPP feature called Semi Connected Mode. When both sides of a point-to-point link agree to use Semi Connected Mode, either side can transparently disconnect and re-establish a circuit-switched connection without having to reconfigure the point-to-point link each time.

Table of Contents

1. Introduction

General Switched Telephone Networks (GSTN) are not well suited for bursty data traffic because the end user is charged for the duration of a circuit-switched connection even though he utilizes the connection only for a fraction of the total connection length.

The current practice among the GSTN customers using circuit-switched data services is to disconnect the link manually when there is no data to send or to receive. This is feasible as long as the user does not need to disconnect and reconnect the link too often and knows when he wants to receive or send data, e.g. when one is reading or sending email. But when the traffic pattern is more unpredictable this becomes quite a tedious or even impossible task, e.g. when one surfs the web or unexpectedly receives a VoIP call request. In addition, some GSTNs, i.e. cellular networks, suffer from long end-to-end delays so that disconnection/reconnection of a physical link is no longer transparent to the user. Therefore it would be convenient if there were a mechanism which would automatically drop a circuit-switched connection if it had been idle for a pre-defined amount of time and re-establish it without having to go through the PPP configuration process when there is data to send or receive.

The concept of dropping the connection without informing the data link layer was introduced in RFC1662 [3]. RFC1662 says that the implementation may "choose to disconnect the physical layer during periods of inactivity". This approach, however, has three problems:

1. Currently there is no mechanism to identify a PPP session. It is crucial that in cases where CLID information is not available, implementations can associate a re-established circuit-switched connection with the existing PPP session. PPP Session-Identifier is described in [10].

2. The PPP implementation cannot advise the peer what the peer should do in case it receives a packet(s) destined for the host in which the implementation is running. Many remote host users insist that they have a final say in whether or not the peer (usually Network Access Server, NAS) can re-establish the physical link.

3. The implementation cannot know whether or not the peer supports the functionality of disconnecting a circuit-switched connection without terminating the PPP session. The only way to deduce this is to probe the peer by sending it a network-layer packet. If the peer does not support this functionality it discards the packet and initiates the PPP link configuration. The discarded packet and the unexpected

delay caused by the link configuration have a negative impact on TCP performance, e.g. on short HTTP transactions. This is especially harmful when the implementation attempts to use the circuit-switched connection in a packet-switched manner.

To fix these problems and to give this concept a more formal standing among other PPP features this document introduces a new PPP feature called Semi Connected Mode (SCM). When properly configured, SCM allows PPP to re-establish a physical link without having to go through the PPP configuration process thus reducing the data connection setup time. This document introduces a PPP option which allows the implementation to find out whether or not NAS supports the SCM feature and to inform the peer of its ability to accept mobile terminated calls.

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST	This word, or the adjective "required", means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.
MAY	This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.

1.2. Terminology

datagram	The unit of transmission in the network layer (such as IP). A datagram may be encapsulated in one or more packets passed to the data link layer.
frame	The unit of transmission at the data link layer. A frame may include a header and/or a trailer, along with some number of units of data.
packet	The basic unit of encapsulation, which is passed across the interface between the network layer and the data link layer. A packet is usually mapped to a frame; the exceptions are when data link layer fragmentation is being performed, or when multiple packets are incorporated into a single frame.
peer	The other end of the point-to-point link.
NAS	A device which is used to terminate dial-up access to a network.
CLID	Calling Line ID, an indication to the receiver of a call as to the phone number of the caller.

PPP session A PPP session is a time interval during which the options negotiated by the Link Control Protocol remain unchanged. The session starts when the LCP reaches the Open state and is concluded by the LCP Terminate-Request packet sent by either end of the point-to-point link.

2. Operation

Semi Connected Mode is a new feature in PPP which allows PPP implementations to terminate and re-establish a physical link without having to reconfigure the point-to-point link. This chapter explains how SCM is negotiated and used. Appendix A describes a modified LCP state transition table for reference.

Nota Bene:

PPP is inherently a symmetrical protocol, i.e. it does not differentiate between the hosts on either end of the point-to-point link. This allows both uplink and downlink to be configured independently of each other. This chapter presents the operation of SCM bearing in mind the symmetrical nature of PPP.

However, the way SCM is implemented makes a clear distinction between PPP implementations running on a remote host (client) and on a NAS (server) because customers using dial-up services want to fully control if and when the circuit-switched connection is dropped, and whether or not the server is allowed to re-establish the circuit-switched connection. Furthermore, only NASs should assign PPP Session-Identifier for point-to-point links because remote hosts lack the necessary information to guarantee the uniqueness of a PPP Session-Identifier within the access network.

Chapter 5 explains how the SCM implementation differs between remote hosts and NASs.

2.1 SCM negotiation

The use of SCM is negotiated during the link establishment phase. The implementation includes the SCM option in a Configure-Request packet thus indicating to the peer its willingness to use SCM.

When the peer receives a Configure-Request packet which has the SCM option it can respond to it in three different ways:

1. If the peer has implemented the SCM feature, is ready to use it, and has accepted the Remote-Term field value it MUST include the SCM option in a Configure-Ack.

2. If the peer supports the SCM feature, but the implementation indicated to the peer that it is ready to accept remote host terminating calls (Remote-Term field) when the peer is actually not able or willing to initiate a call setup procedure, the peer MUST send a Configure-Nak and include the unmodified SCM option in the packet.

3. If the peer does not support the SCM feature it MUST send a Configure-Reject and include the unmodified SCM option in the packet.

Both sides of a point-to-point link must also agree on a PPP Session-Identifier so that the side which accepts a newly re-established physical link (i.e. callee) can associate the physical link with one of the existing PPP sessions.

The side of a point-to-point link which can guarantee that the chosen value of a Session-Identifier is always unique within the access network MUST include the Session-Identifier option in a Configure-Request packet (see chapter 5).

2.2 Terminating and re-establishing a physical link

After having agreed to use SCM and the PPP link has been properly configured (including PPP Session-Identifier) both sides can start sending and receiving network layer packets. If the link has remained idle more than the allowed number of seconds (Idle timer) the implementation MUST terminate the physical link without signaling the Down event.

When the peer notices that the implementation has terminated the physical link it MUST mark the time of the event. Later on it uses this value to determine if that link has been idle more than the allowed time. The peer MUST remove all the PPP sessions from the database which uses SCM and whose physical link has been down more than the time specified by the Expiration timer.

When the physical link is down and the implementation receives a packet from the network layer it MUST:

1. re-establish the circuit-switched connection. If the implementation cannot re-establish the physical link immediately (e.g. received a busy signal) it SHOULD try to re-establish the link "a few times" before signaling the Down event and discarding the network packet.

2. send a LCP Identification packet [9] which carries the value of the Session-Identifier negotiated during the link establishment phase to the peer so that the peer can associate the physical link with the right PPP session.

3. and finally, start sending network layer packets to the peer. If the implementation receives a Configure-Request from the peer after re-establishing the physical link (e.g. database holding the current PPP session information was

destroyed or the PPP session entry expired) it MUST re-configure the PPP link according to [1].

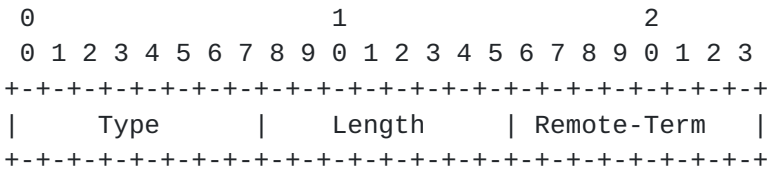
3. LCP Configuration Option for SCM

Description

The LCP configuration option for SCM allows the remote host and the NAS implementations to negotiate whether SCM is used. By default SCM is disabled.

Only the remote host implementation can include the SCM option in Configure-Request packets. The remote host implementation indicates in the Remote-Term field if it accepts remote host terminating calls.

A summary of the SCM Configuration Option format is shown below. The fields are transmitted from left to right.



Type

TBD

Length

3

Remote-Term

The Remote-Term field is one octet and indicates whether the implementation accepts call setup requests (terminating call). If the implementation does not accept remote host terminating calls the peer SHOULD drop all the packets destined to the remote host when the physical link between the remote host and NAS is down. Acceptable values of the Remote-Term field are:

0 The remote host does not accept call setup requests.

1 The remote host accepts call setup requests.

4. Implementation Requirements

4.1 Remote hosts

The remote host implementation SHOULD include the SCM option in a Configure-Request packet. In case the remote host implementation receives a SCM option in a Configure-Request packet from the peer it SHOULD Configure-Nak it.

The remote host implementation MUST have an Idle timer which determines how long the physical link can be idle before it is terminated. The implementation SHOULD offer the end user the option of configuring the Idle timer value so that the end user can find a value which satisfies his needs.

The remote host implementation MUST ack the Session-Identifier option it receives from NAS. After having re-established the physical link the remote host implementation MUST first sent a LCP Identification packet [9] which has the value of the Session-Identifier in the Message field before it can send network layer packets to the peer.

The remote host implementation MUST include a mechanism so that the end user can decide whether or not he wants to accept the call request. This can be done beforehand by listing CLIDs where calls can be originated or by prompting the end user to accept a call each time the physical layer receives a call request. An implementation whose physical layer cannot provide CLID information, or does not trust a carrier-provided CLID SHOULD request the peer to authenticate itself (see chapter 6. Security Considerations).

SCM is valid only for the duration of a PPP session. When restarted after an unexpected crash or shutdown, the implementation MUST always start a new PPP session. The implementation MUST also start a new PPP session after failing to terminate the old session.

To avoid NAS from having stale PPP session entries in its database the remote host implementation SHOULD terminate the PPP session properly before the end user logs off or brings the host down.

4.2 Network Access Server

The NAS implementation SHOULD NOT include the SCM option in a Configure-Request. The NAS implementation MUST respond to the SCM option it receives from the remote host as explained in chapter

2. Furthermore, it MUST NOT disconnect the physical link. Rather, it observes the status of the physical link and acts accordingly when the remote host disconnects the link.

The NAS implementation MUST include a Session-Identifier option in a Configure-Request packet. The remote-host must accept the Session-Identifier before SCM can be used. If NAS receives a Configure-Request packet which contains a Session-Identifier option it SHOULD ack the Session-Identifier option but not use the value specified by the option to identify the point-to-point link. NAS MUST guarantee that the value of a Session-Identifier option it sends to the remote host is unique within the access network.

The NAS implementation MUST re-establish the physical link when it receives a packet destined to the remote host and if the remote host told NAS that it can accept remote host terminated calls. If NAS fails to re-establish the physical link after a number of unsuccessful attempts it MUST remove the PPP session entry from the database. When a physical link belonging to a PPP session is re-established NAS must initialize the field in the PPP session entry which marks the time when the physical link was last terminated.

NAS implementations MUST have a database in which they store the current PPP sessions. Session-Identifier [10] SHOULD be used as the key for the database. After having detected that the remote host has terminated the physical link, NAS implementations MUST start the Expiration timer. NAS implementations use this timer to periodically check for PPP sessions whose physical links have been down longer than the allowed time. Implementations MUST remove all the entries which do not satisfy this requirement. In order to differentiate physical links which are up from links that have been terminated, NAS SHOULD allocate a unique value for the timer which indicates that a link is up. NAS implementation SHOULD assign this value to the Expiration timer when NAS creates a new PPP session entry.

NAS implementations must be able to cope with the modem hunt-group problem. It is possible that NAS has more than one entity between which the control of PPP sessions and the associated physical links is distributed. NAS MUST guarantee that the entity, which has a PPP session entry in its database when the remote host terminates the physical link of the PPP session, either:

1. regains the control of the physical link belonging to that PPP session when the link is re-established, or

1. alternatively, transfers the PPP session entry to another entity which now controls the physical link between the remote host and the NAS entity, or deletes the PPP session entry thus forcing the reconfiguration of the PPP link.

It is beyond the scope this document to discuss these solutions in greater detail.

NAS implementations MAY inform ISP of the time durations when the physical link was up so that the remote user is not charged for the times when the link was down. If ISP honors this information NAS SHOULD pass it to the RADIUS server at the end of the RADIUS accounting service [5] delivery.

When the NAS implementation receives a Terminate-Request from the remote host it MUST remove the PPP session entry from the database.

Implementation Note:

L2TP tunnel between NAS (=LAC) and Authenticator Server (AS, see picture in chapter 4.3) might cause problems when SCM option is negotiated. Because LAC may have negotiated LCP with the remote host without LNS being involved in the negotiation, LCP must send LCP CONFREQs to LNS for its approval. If LNS refuses to accept LCP CONFREQs and wants to renegotiate LCP, it is possible that during the second round of negotiation LNS does not accept SCM option because SCM has not been implemented in it.

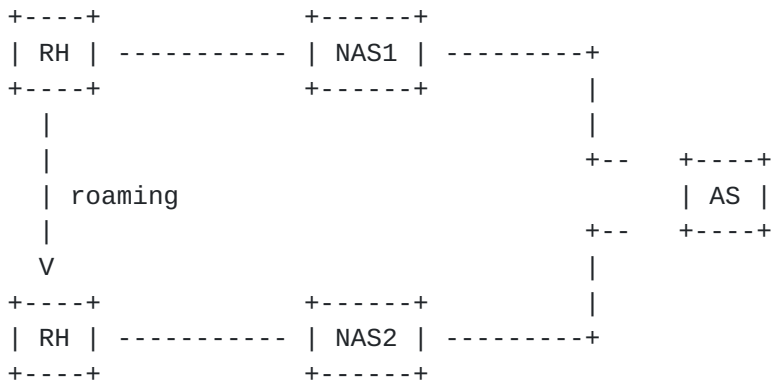
To be able to use SCM even though LNS does not support this feature, LAC implementers/administrators should make sure that LCP CONFREQs LAC sends to LNS are accepted by LNS. This means that LAC MUST remove at least the SCM option from CONFREQs it sends to LNS. If LNS accepts LAC's LCP CONFREQs SCM can be used because both LAC and the remote host agreed to use it.

4.3 Roaming hosts

Some remote hosts may be so-called mobile hosts which can roam to a new area served by another NAS (NAS2). Roaming can be a problem if the SCM is in use (the physical link has been temporarily terminated) and the remote host has roamed to a new area without terminating the PPP session with old NAS (NAS1).

In many cases the Authenticator Server (AS) does allow end users to have more than one active PPP session at any given time. If

the new location is serviced by a new NAS (NAS2) it is possible that NAS2 cannot grant access to the remote host because AS refused to authenticate the remote host due to the existing PPP session. E.g. some RADIUS servers [4] do not allow end users to have more than one open PPP session at any given time. This scenario can also take place in access networks where there is a L2TP tunnel between NAS and AS (NAS = LAC, AS = LNS).



RH = remote host
AS = Authenticator server (RADIUS server, L2TP Network Server)
NAS = Network access server

To prevent this scenario from happening, NAS implementations should be able to inquire what PPP sessions other NASs have and, if needed, ask another NAS to release the PPP session information, or to terminate the PPP session when the remote host roams to a new location. It is beyond the scope of this document to discuss these solutions in greater detail.

5. Timers

Idle timer

The Idle timer tells the remote host implementation how many seconds a physical link can be idle before it is terminated. The end user SHOULD be able to adjust the timer according to his preference.

Remote host implementations SHOULD impose a lower boundary for the Idle timer. Considering that the most of the traffic flows use TCP the lower boundary SHOULD not be less than RTO preventing the physical link from being terminated while the remote host is waiting for an acknowledgement. However, because the value of RTO varies in time based on the state of a link(s) the only recommendation that can be given is that the value of the Idle timer SHOULD be no less than 3 sec which [6] is specified as an initial RTO value.

Remote host implementations can either expect the end user to play with the Idle timer value, or implement a mechanism which mirrors the current values of RTOs and assigns the lowest of them to the Idle timer.

Expiration timer

The Expiration timer determines how long the physical link can be down without NAS removing the PPP session entry from its database. The value of this timer should be high enough to make circuit-switched data service resemble packet-switched data service.

6. Security Considerations

One way to provide security in SCM is to rely on CLID, which can be used to authenticate the peer, or on a PPP Session-Identifier.

It is, however, possible that GSTN and/or hardware cannot provide CLID, or that the implementation desires a stronger authentication mechanism, e.g. CHAP [7] or some mechanism used by EAP [8]. In these cases the authenticator MUST be able to request the peer to authenticate itself immediately after the physical link has been re-established.

Implementation Note:

It is left up to the implementation to decide what to do with network packets which the implementation receives before the peer has authenticated itself. To make the disconnection/reconnection of the physical link as transparent as possible to the end user the implementation SHOULD accept the network layer packets within a certain time frame even though the peer has not yet authenticated itself. In case of NAS the implementation can either buffer the packets or forward them (preferred) while waiting for the authentication response from the peer. If the peer fails to authenticate itself the implementation MUST immediately close the connection, discard all the buffered packets and clear the peer's PPP session entry.

REFERENCES

[1] Simpson, W., Editor, "The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links," RFC 1661, July 1994.

[2] Valencia, A. et al., "Layer Two Tunneling Protocol "L2TP"", draft-ietf-pppext-l2tp-09.txt, January 1998.

[3] Simpson, W., Editor. "PPP in HDLC-like Framing", RFC 1662, July 1994.

[4] C. Rigney, et. al., "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[5] C. Rigney, "RADIUS accounting", RFC 2139, April 1997.

[6] R. Braden, Editor, "Requirements for Internet Hosts --

Communication Layers", RFC 1122, October 1989.

[7] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[8] L. Blunk and J. Volbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[8] Simpson, W., Editor, "PPP LCP Extensions", RFC 1570, January 1994.

[10] Latvala, M., "PPP Session-Identifier Option", "work in progress" draft-ietf-pppext-sessid-00.txt, November 1998.

CONTACTS

Questions about this paper can be directed to:

Mikael Latvala
Oy LM Ericsson Ab
SF-02420 Jorvas, Finland

E-Mail: mikael.latvala@ericsson.com
Voice: +358 9 299 2850
GSM: +358 40 507 2555
Fax: +358 9 299 3247

Appendix A: LCP Translation Table

The Semi-Connected phase SHOULD be implemented by adding one new state, Semi-Connected, six new events, and seven new actions to the LCP's state translation table. The new events can cause a legal transition only in the Request-Sent, Request-Ack, Opened or Semi-Connected state which is the reason why only those four states are shown in the table below. The new functionalities can be implemented without sacrificing the integrity of the "traditional" PPP implementation.

Because of the asymmetrical nature of SCM small 'c' indicates events which are seen by the remote host (client) and small 's' events seen by NAS (server).

Events

CSC = Close event, SCM configured, no peer
DSC = Down event, SCM configured
IDT = Idle timer expired
ETE = Expiration timer expired
DUP+ = Packet from the upper layer
DUP- = Packet from the upper layer, no peer

Actions

rel = re-establish link
tel = terminate link
ssi = send session id
dse = delete session entry
sit = start idle timer
set = start expr timer
iet = initialize expr timer

	State			
Events	7 Ack-Rcvd	8 Ack-Sent	9 Opened	10 Semi-Connected
Up-c	-	-	-	sit/9
Up-s	-	-	-	iet/9
Down	1	1	tld/1	-
Open	7	8	9r	-
Close-c	irc,str/4	irc,str/4	tld,irc,str/4	rel,tld,irc,str/4
Close-s	irc,str/4	irc,str/4	tld,irc,str/4	rel,tld,irc,dse,str/4
TO+	scr/6	scr/8	-	-
TO-	tlf/3p	tlf/3p	-	-
RCR+	sit,sca,tlu/9	sca/8	tld,scr,sca/8	-
RCR-	scn/7	scn/6	tld,scr,scn/6	-
RCA	scr/6x	sit,irc,tlu/9	tld,scr/6x	-
RCN	scr/6x	irc,scr/8	tld,scr/6x	-
RTR	sta/6	sta/6	tld,zrc,sta/5	-
RTA	6	8	tld,scr/6	-

RUC	scj/7 scj/8 scj/9 -

RXJ+	6	8	9	-
RXJ-	tlf/3	tlf/3	tld,irc,str/5	-
RXR	7	8	ser/9	-
CSCc	-	-	-	tld/1
CSCs	-	-	-	tld,dse/1
DSCc	-	-	10	-
DSCs	-	-	set/10	-
IDT	-	-	tel/10	-
ETE	-	-	-	tld,dse/1
DUP+c	-	-	-	rel,ssi,sit/9
DUP+s	-	-	-	rel,iet/9
DUP-c	-	-	-	tld/1
DUP-s	-	-	-	tld,dse/1

Events

Close event when SCM configured (CSC)

This event occurs when the automaton is in the Semi-Connected state, the network administrator (human or program) indicates that the link is not allowed to be Opened, and the implementation is not able to re-establish the physical link to properly terminate the point-to-point link.

Down event when SCM configured (DSC)

This event occurs when the PPP link is configured to use SCM, the automaton is in the Opened state, and a lower layer indicates that it is no longer ready to carry packets. Usually the event takes place when the remote host terminates the physical link because the point-to-point link has remained idle too long.

Idle timer expired (IDT)

This event occurs when the PPP link is configured to use SCM, the automaton is in the Opened state, and the Idle timer expires. Event noticed only by the remote host.

Expiration timer expired (EXE)

This event occurs when the PPP link is configured to use SCM, the automaton is in the Semi-Connected state, and the Expiration timer expires. Event noticed only by NAS.

Datagram from the upper layer (DUP)

This event occurs when the PPP link is configured to use SCM, the automaton is in the Semi-Connected state, and a upper layer has given a packet to PPP to transfer to the peer.

The DUP+ event indicates that the peer is still available so that the physical link can be re-established and packets can be sent to the peer.

The DUP- event indicates that the peer is not available and that the physical link cannot be re-established.

Actions

Re-establish link (rel)

The physical link is re-established.

Terminate link (tel)

The physical link is terminated.

Start expiration timer (set)

This action prompts NAS to start the Expiration timer.

Start idle timer (sit)

This action prompts the remote host to start the Idle timer.

Send session id (ssi)

This action causes the implementation to send a LCP Identification packet to the peer.

Initialize expiration timer (iet)

This action causes NAS to initialize the Expiration timer to a value which indicates that the physical link is up.