                  Pseudowire Emulation Edge-to-Edge (PWE3)
                       Frame Check Sequence Retention

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Abstract

   This document defines a mechanism for preserving Frame Check Sequence
   (FCS) through Ethernet, Frame Relay, High-Level Data Link Control
   (HDLC), and PPP pseudowires.

Table of Contents

1. Overview

   The specifications for Ethernet, Frame Relay, HDLC, and PPP
   pseudowire encapsulation [1] [2] [3] [9] [10] [11] include a mode of
   use whereby frames are transparently delivered across the pseudowire
   without any header or other alterations by the pseudowire ingress or
   egress Provider Edge (PE). (Note that this mode is inherent for HDLC
   and PPP Pseudowires.)

   However, these specifications all specify that the original Frame
   Check Sequence (FCS) be removed at ingress and regenerated at egress,
   which means that the frames may be subject to unintentional
   alteration during their traversal of the pseudowire from the ingress
   to the egress PE. Thus, the pseudowire cannot absolutely be
   guaranteed to be "transparent" in nature.

   To be more precise, pseudowires, as currently defined, leave the
   payload vulnerable to unintended modification occurring while
   transiting the encapsulating network. Not only can a PW-aware device
   internally corrupt an encapsulated payload, but ANY LSR or router in
   the path can corrupt the encapsulated payload. In the event of such
   corruption, there is no way to detect the corruption through the path
   of the pseudowire. Further, because the FCS is calculated upon
   network egress, any corruption will pass transparently through ALL
   Layer 2 switches (Ethernet and Frame Relay) through which the packets
   travel. Only at the endpoint, assuming that the corrupted packet
   even reaches the correct endpoint, can the packet be discarded, and
   depending on the contents of the packet, the corruption may not ever
   be detected.

   Not only does the encapsulation technique leave the payload
   unprotected, it also subverts the error checking mechanisms already
   in place in SP and customer networks by calculating FCS on
   questionable data.

   In a perfect network comprising perfect equipment, this is not an
   issue. However, as there is no such thing, it is an issue. SPs
   should have the option of saving overhead by yielding the ability to
   detect faults. Equally, SPs should have the option to sacrifice the
   overhead of carrying the original FCS end-to-end to ensure the
   ability to detect faults in the encapsulating network.

   This document defines such a mechanism to allow the ingress PE to
   retain the original frame FCS on ingress to the network, and it
   relieves the egress PE of the task of regenerating the FCS.

This is an OPTIONAL mechanism for pseudowire implementations. For
interoperability with systems that do not implement this document,
the default behavior is that the FCS is removed at the ingress PE and
regenerated at the egress PE, as specified in [1], [2], and [3].

This capability may be used only with Ethernet pseudowires that use
"raw mode" [1], Frame Relay pseudowires that use "port mode" [2] [3],
and HDLC and PPP pseudowires [3].

Note that this mechanism is not intended to carry errored frames
through the pseudowire; as usual, the FCS MUST be examined at the
ingress PE, and errored frames MUST be discarded. The FCS MAY also
be examined by the egress PE; if this is done, errored frames MUST be
discarded. The egress PE MAY also wish to generate an alarm or count
the number of errored frames.

2. Specification of Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in RFC 2119 [6].

3. Signaling FCS Retention with MPLS-Based Pseudowires

When using the signaling procedures in [4], there is a Pseudowire
Interface Parameter Sub-TLV type used to signal the desire to retain
the FCS when advertising a VC label [5]:

       Parameter   Length   Description
          0x0A   4   FCS Retention Indicator

The presence of this parameter indicates that the egress PE requests
that the ingress PE retain the FCS for the VC label being advertised.
It does not obligate the ingress PE to retain the FCS; it is simply
an indication that the ingress PE MAY retain the FCS. The sender
MUST NOT retain the FCS if this parameter is not present in the VC
FEC element.

The parameter includes a 16-bit FCS length field, which indicates the
length of the original FCS being retained. For Ethernet pseudowires,
this length will always be set to 4. For HDLC, PPP, and Frame Relay
pseudowires, this length will be set to either 2 or 4. Since the FCS
length on these interfaces is a local setting, retaining the FCS only
makes sense if the FCS length is identical on both ends of the
pseudowire. Including the FCS length in this parameter allows the
PEs to ensure that the FCS is only retained when it makes sense.

Since unknown parameters are silently ignored [4], backward
compatibility with systems that do not implement this document is
provided by requiring that the FCS be retained ONLY if the FCS
Retention Indicator with an identical setting for the FCS length has
been included in the advertisements for both directions on a
pseudowire.

If the ingress PE recognizes the FCS Retention Indicator parameter
but does not wish to retain the FCS with the indicated length, it
need only issue its own label mapping message for the opposite
direction without including the FCS Retention Indicator. This will
prevent FCS retention in either direction.

If PWE3 signaling [4] is not in use for a pseudowire, then whether
the FCS is to be retained MUST be identically provisioned in both PEs
at the pseudowire endpoints. If there is no provisioning support for
this option, the default behavior is to remove the FCS.

4. Signaling FCS Retention with L2TPv3-Based Pseudowires

   This section uses the following terms as defined in [7]:

      Incoming-Call-Request (ICRQ)
      Incoming-Call-Reply (ICRP)
      Incoming-Call-Connected (ICCN)
      Attribute Value Pair (AVP)
      L2TP Control Connection Endpoint (LCCE)

   When using the signaling procedures in [7], the FCS Retention AVP,
   Attribute Type 92, is used.

   The Attribute Value field for this AVP has the following format:

```
       0                   1
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |            FCS Length          |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   The FCS Length is a 2-octet unsigned integer.

   The presence of this AVP in an ICRQ or ICRP message indicates that an
   LCCE (PE) requests that its peer retain FCS for the L2TP session
   being established. If the receiving LCCE recognizes the AVP and
   complies with the FCS retention request, it MUST include an FCS
   Retention AVP as an acknowledgement in a corresponding ICRP or ICCN
   message. FCS Retention is always bidirectional; thus, FCS is only

   retained if both LCCEs send an FCS Retention AVP during session
   establishment.

   The Attribute Value is a 16-bit FCS length field, which indicates the
   length of the original FCS being retained. For Ethernet pseudowires,
   this length will always be set to 4. For HDLC, PPP, and Frame Relay
   pseudowires, this length will be set to either 2 or 4. Since the FCS
   length on these interfaces is a local setting, retaining the FCS only
   makes sense if the FCS length is identical on both ends of the
   pseudowire. Including the FCS length in this AVP allows the PEs to
   ensure that the FCS is only retained when doing so makes sense.

   The Length of this AVP is 8. The M bit for this AVP MUST be set to 0
   (zero). This AVP MAY be hidden (the H bit MAY be 1 or 0).

5. Security Considerations

   This mechanism enhances the data integrity of transparent Ethernet,
   Frame Relay, and HDLC pseudowires, because the original FCS, as
   generated by the Customer Edge (CE), is included in the
   encapsulation. When the encapsulated payload passes FCS checking at
   the destination CE, it is clear that the payload was not altered
   during its transmission through the network (or at least to the
   accuracy of the original FCS; but that is demonstrably better than no
   FCS at all).

   Of course, nothing comes for free; this requires the additional
   overhead of carrying the original FCS (in general, either two or four
   octets per payload packet).

   This signaling is backward compatible and interoperable with systems
   that do not implement this document.

6. Applicability Statement

   In general, this document is intended to further extend the
   applicability of the services defined by [1], [2], and [3] to make
   them more suitable for use in deployments where data integrity is an
   issue (or at least is as much of an issue as in the original services
   that defined the FCS usage in the first place). There are some
   situations where this extension is not necessary, such as where the
   inner payloads have their own error-checking capabilities (such as
   TCP). But for inner payloads that do rely on the error-detecting
   capabilities of the link layer (such as SNA), this additional
   protection can be invaluable.

   When pseudowires are being used to connect 802.1 bridges, this
   document allows pseudowires to comply with the requirement that all
   media interconnecting 802.1 bridges have (at least) 32-bit FCS
   protection.

   Note that this document is one possible alternative for a service
   provider to enhance the end-to-end data integrity of pseudowires.
   Other mechanisms may include the use of end-to-end IPsec between the
   PEs, or internal mechanisms in the P routers to ensure the integrity
   of packets as they are switched between ingress and egress
   interfaces. Service providers may wish to compare the relative
   strengths of each approach when planning their pseudowire
   deployments; however, an argument can be made that it may be wasteful
   for an SP to use an end-to-end integrity mechanism that is STRONGER
   than the FCS generated by the source CE and checked by the
   destination CE.

7. IANA Considerations

   This document does not specify any new registries for IANA to
   maintain.

   Note that [5] allocates the FCS Retention Indicator interface
   parameter; therefore, no further IANA action is required.

   IANA assigned one value within the L2TP "Control Message Attribute
   Value Pairs" section as per [8]. The new AVP is 92 and is referred
   to in the IANA L2TP parameters registry as "FCS Retention".

8. Acknowledgement

   The authors would like to thank Mark Townsley for the text in Section
   4.

9. Normative References

   [1] Martini, L., Rosen, E., El-Aawar, N., and G. Heron,
        "Encapsulation Methods for Transport of Ethernet over MPLS
        Networks", RFC 4448, April 2006.

   [2] Martini, L., Ed., Kawa, C., Ed., and A. Malis, Ed.,
        "Encapsulation Methods for Transport of Frame Relay over
        Multiprotocol Label Switching (MPLS) Networks", RFC 4619,
        September 2006.

   [3]   Martini, L., Rosen, E., Heron, G., and A. Malis, "Encapsulation
         Methods for Transport of PPP/High-Level Data Link Control (HDLC)
         over MPLS Networks", RFC 4618, September 2006.

   [4]   Martini, L., Rosen, E., El-Aawar, N., Smith, T., and G. Heron,
         "Pseudowire Setup and Maintenance Using the Label Distribution
         Protocol (LDP)", RFC 4447, April 2006.

   [5]   Martini, L., "IANA Allocations for Pseudowire Edge to Edge
         Emulation (PWE3)", BCP 116, RFC 4446, April 2006.

   [6]   Bradner, S., "Key words for use in RFCs to Indicate Requirement
         Levels", BCP 14, RFC 2119, March 1997.

   [7]   Lau, J., Townsley, M., and I. Goyret, "Layer Two Tunneling
         Protocol - Version 3 (L2TPv3)", RFC 3931, March 2005.

   [8]   Townsley, W., "Layer Two Tunneling Protocol (L2TP) Internet
         Assigned Numbers Authority (IANA) Considerations Update", BCP
         68, RFC 3438, December 2002.

   [9]   Aggarwal, R., Townsley, M., and M. Dos Santos, "Transport of
         Ethernet Frames over Layer 2 Tunneling Protocol Version 3
         (L2TPv3)", RFC 4719, November 2006.

   [10] Townsley, M., Wilkie, G., Booth, S., Bryant, S., and J. Lau,
         "Frame Relay over Layer 2 Tunneling Protocol Version 3
         (L2TPv3)", RFC 4591, August 2006.

   [11] Pignataro, C. and M. Townsley, "High-Level Data Link Control
         (HDLC) Frames over Layer 2 Tunneling Protocol, Version 3
         (L2TPv3)", RFC 4349, February 2006.

Authors' Addresses

   Andrew G. Malis
   Tellabs
   90 Rio Robles Dr.
   San Jose, CA 95134

   EMail: Andy.Malis@tellabs.com

   David Allan
   Nortel Networks
   3500 Carling Ave.
   Ottawa, Ontario, CANADA

   EMail: dallan@nortel.com

   Nick Del Regno
   MCI
   400 International Parkway
   Richardson, TX 75081

   EMail: nick.delregno@mci.com