Network Working Group I. Learmonth
Internet-Draft HamBSD
Obsoletes: 1226 (if approved) May 19, 2020
Intended status: Experimental
Expires: November 20, 2020

Internet Protocol Encapsulation of AX.25 Frames
draft-learmonth-rfc1226-bis-02

Abstract

This document describes a method for the encapsulation of AX.25 Link Access Protocol for Amateur Packet Radio frames within IP version 4 and version 6 packets. Obsoletes RFC1226.

Note

Comments are solicited and should be addressed to the author(s).

The sources for this draft are at:

https://github.com/irl/draft-rfc1226-bis

1. Introduction

This document describes a method for the encapsulation of AX.25 Link Access Protocol for Amateur Packet Radio [AX.25]) frames within IPv4 and IPv6 packets. It obsoletes [RFC1226].

AX.25 is a data link layer protocol originally derived from layer 2 of the X.25 protocol suite and designed for use by amateur radio operators. It is used extensively by amateur packet radio networks worldwide.

In addition to specifying how packets should be encapsulated, it gives recommendations for DiffServ codepoint marking of the encapsulating headers based on the AX.25 frame content and provides security considerations for the use of this encapsulation method.

2. Terminology

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 [RFC2119].

3. Internet Protocol Encapsulation

Each AX.25 frame is encapsulated in one IP version 4 or version 6 datagram using protocol number 93 as assigned in the Assigned Internet Protocol Numbers registry [protocol-numbers]. For AX.25 version 2.0, the maximum frame size expected is 330 bytes and implementations MUST be prepared to handle frames of this size. Higher frame sizes can be negotiated by AX.25 version 2.2 and so this is a minimum requirement and not a limit.

HDLC framing elements (flags and zero-stuffing) are omitted, as the IP datagram adequately delimits the beginning and end of each AX.25 frame. The CRC-16-CCITT frame check sequence (normally generated by the HDLC transmission hardware) is included trailing the information field. In all other respects, AX.25 frames are encapsulated unaltered.

3.1. Priority Frames

In normal operation, the DiffServ codepoint field [RFC2474] in the encapsulating IP header SHOULD be set to best effort (BE). The exception to this is "priority frames" as specified for AX.25 version 2.2, including acknowledgement and digipeat frames, which SHOULD have the DiffServ codepoint set to AF21 [RFC2597]. A slot is reserved on the radio channel for the transmission of these frames and the use of this codepoint will permit the frames to arrive promptly at the station for transmission.

For the avoidance of doubt: on decapsulation the AX.25 frame MUST NOT be modified regardless of the DiffServ codepoint on the received encapsulating IP header. The receiver MUST NOT use the DiffServ codepoint to infer anything about the nature of the encapsulated packet. It has been shown that while the AF21 codepoint may be remarked while crossing administrative boundaries, it is unlikely that priority inversion will occur due to remarking where such remarking occurs [Cust18].

3.2. Automatic Packet Reporting System

Automatic Packet Reporting System [APRS] is an amateur radio-based system for real time digital communications for local situational awareness. APRS uses AX.25 frames for addressing, and additionally assigns special meaning to some of the reserved bits of an AX.25 frame header.

As a special case, when used with the Automatic Packet Reporting System [APRS], priority frames will not occur. If a tunnel is configured as carrying APRS data, the DiffServ codepoint SHOULD by default be set to AF11 [RFC2597]. Where the "Precedence Bit" [RR-bits] is set (i.e. it is zero) in an APRS packet, the DiffServ codepoint should be set to BE. Where the "Operator Present Bit" [RR-bits] is set (i.e. it is zero), the DiffServ codepoint MAY be set to AF21 [RFC2597].

Again, for the avoidance of doubt: on decapsulation the AX.25 frame MUST NOT be modified regardless of the DiffServ codepoint on the received encapsulating IP header. The receiver MUST NOT use the DiffServ codepoint to infer anything about the nature of the encapsulated packet. It has been shown that while AF codepoints may be remarked while crossing administrative boundaries, it is unlikely that priority inversion will occur, either with the BE traffic or between AF PHBs due to remarking where such remarking occurs [Cust18].

4. IANA Considerations

Protocol number 93 is assigned in [protocol-numbers] and should be updated to point to this document.

5. Security Considerations

With the exception of control signals exchanged between earth command stations and space stations in the amateur-satellite service, amateur radio transmissions cannot be encoded for the purpose of obscuring their meaning. In essence, this means that cryptography that requires the use of secrets to decipher a message cannot be used where the possibility exists that a packet will be transmitted by an amateur radio station.

The CRC-16-CCITT provides for an integrity check but does not guarantee the authenticity of the packet. In many jurisdictions it is a requirement for amateur radio stations that are Internet connected that they verify that packets for transmission have originated from licensed radio amateurs. In order to provide this guarantee, IPSec [RFC4301] MUST be employed to provide authentication of packets. A transport mode SA SHOULD be negotiated between the IP endpoints to use IP Authentication Headers (AH) [RFC4302] with the traffic selector matching packets with IP protocol number 93. In cases where NAT traversal is required, a tunnel mode SA MAY be used instead of transport. In cases where traffic is guaranteed to not pass via an amateur radio link, ESP [RFC4303] MAY be used instead of AH. ESP MUST NOT be used where there is the possibility that the encapsulating packet will be transmitted via an amateur radio link.

When transmitted by an amateur radio station, many propagation modes will permit wide reception of a packet. As such, receivers MUST implement anti-replay protection by verifying received sequence numbers [RFC4302][RFC4303]. The size of the anti-replay window may need to be scaled to account not only for the speed of the link, but also for packet loss that may occur on amateur radio links. Following extended packet loss a sender may have advanced the sequence number beyond the window size allowed. Dead peer detection [RFC5996] can be used to renegotiate SAs in this case and so SHOULD be enabled for any SA expected to traverse an amateur radio link that is expected to have varying propagation charachteristics.

Given the need for anti-replay protection, it is not possible to manually key the SAs. An automatic keying protocol such as IKEv1 [RFC2409] or IKEv2 [RFC5996] MUST be used to establish SAs. The exact details of the automatic keying protocol to use and its paramaters are not specified in this document.

6. Acknowledgements

The author would like to acknowledge the work of Brian Kantor who authored the original specification [RFC1226] that this document updates.

7. References

7.1. Normative References

[AX.25] Tucson Amateur Packet Radio Corporation, "AX.25 Link Access Protocol for Amateur Packet Radio Version 2.2", July 1998, <https://www.tapr.org/pdf/AX25.2.2.pdf>.

[protocol-numbers] IANA, "Assigned Internet Protocol Numbers", <http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <https://www.rfc-editor.org/info/rfc2474>.

[RFC2597] Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, DOI 10.17487/RFC2597, June 1999, <https://www.rfc-editor.org/info/rfc2597>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RR-bits] Bruninga, B., "APRS Future Use of AX.25 SSID RR Bits", December 2012, <http://aprs.org/aprs12/RR-bits.txt>.

7.2. Informative References

[APRS] Wade, I., Ed., "APRS Protocol Reference", August 2000, <http://www.aprs.org/doc/APRS101.PDF>.

[Cust18] Custura, A., Secchi, R., and G. Fairhurst, "Exploring DSCP modification pathologies in the Internet", Computer Communications Vol. 127, pp. 86-94, DOI 10.1016/j.comcom.2018.05.016, September 2018.

[RFC1226] Kantor, B., "Internet protocol encapsulation of AX.25 frames", RFC 1226, DOI 10.17487/RFC1226, May 1991, <https://www.rfc-editor.org/info/rfc1226>.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, DOI 10.17487/RFC2409, November 1998, <https://www.rfc-editor.org/info/rfc2409>.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, DOI 10.17487/RFC5996, September 2010, <https://www.rfc-editor.org/info/rfc5996>.

Author's Address

Iain R. Learmonth
HamBSD

Email: irl@hambsd.org