INTERNET-DRAFT
Updates: 7178
Intended status: Proposed Standard

Expires: September 7, 2015

Donald Eastlake
Huawei
Mohammed Umair
IPinfusion
Yizhou Li
Huawei

March 8, 2015

TRILL: RBridge Channel Tunnel Protocol
<draft-ietf-trill-channel-tunnel-04.txt>

Abstract

The IETF TRILL (Transparent Interconnection of Lots of Links) protocol includes an optional mechanism, called RBridge Channel and specified in RFC 7178, for the transmission of typed messages between TRILL switches in the same campus and between TRILL switches and end stations on the same link. This document specifies two optional extensions to the RBridge Channel protocol: (1) A standard method to tunnel a variety of payload types by encapsulating them in an RBridge Channel message; and (2) A method to support security facilities for RBridge Channel messages. This document updates RFC 7178.

Status of This Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Distribution of this document is unlimited. Comments should be sent to the authors or the TRILL working group mailing list: trill@ietf.org

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html. The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Table of Contents

1. Introduction

The IETF TRILL base protocol [RFC6325] has been extended with an optional RBridge Channel [RFC7178] facility to support transmission of typed messages (for example BFD [RFC7175]) between two TRILL switches (RBridges) in the same campus and between RBridges and end stations on the same link. When sent between RBridges in the same campus, a TRILL Data packet with a TRILL header is used and the destination RBridge is indicated by nickname. When sent between a RBridge and an end station on the same link in either direction a native RBridge Channel messages [RFC7178] is used with no TRILL header and the destination port or ports are indicated by a MAC address. (There is no mechanism to stop end stations on the same link, from sending native RBridge Channel messages to each other; however, such use is outside the scope of this document.)

This document updates [RFC7178] and specifies extensions to RBridge Channel that provides two additional facilities as listed below. Implementation and use of each of these facilities is optional, except that there are two payload types that MUST be implemented. Both of these facilities can be used in the same packet.

(1) A standard method to tunnel a variety of payload types by encapsulating them in an RBridge Channel message.

(2) A method to provide security facilities for RBridge Channel messages.

In case of conflict between this document and [RFC7178], this document takes precedence.

1.1 Terminology and Acronyms

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].

This document uses terminology and acronyms defined in [RFC6325] and [RFC7178]. Some of these are repeated below for convenience along with additional terms and acronyms.

AES - Advanced Encryption Standard.

CCM - Counter with CBC-MAC

Data Label - VLAN or FGL.

DTLS - Datagram TLS [RFC6347].

FGL - Fine Grained Label [RFC7172].

HKDF - Hash based Key Derivation Function [RFC5869].

RBridge - An alternative term for a TRILL switch.

SHA - Secure Hash Algorithm [RFC6234].

TRILL - Transparent Interconnection of Lots of Links or Tunneled Routing in the Link Layer.

TRILL switch - A device that implements the TRILL protocol [RFC6325], sometimes referred to as an RBridge.

2. Channel Tunnel Packet Format

The general structure of an RBridge Channel message between two TRILL switches (RBridges) in the same campus is shown in Figure 1 below. The structure of a native RBridge Channel message sent between an RBridge and an end station on the same link, in either direction, is shown in Figure 2 and, compared with the first case, omits the TRILL Header, inner Ethernet addresses, and Data Label. A Protocol field in the RBridge Channel Header gives the type of RBridge Channel message and indicates how to interpret the Channel Protocol Specific Payload [RFC7178].

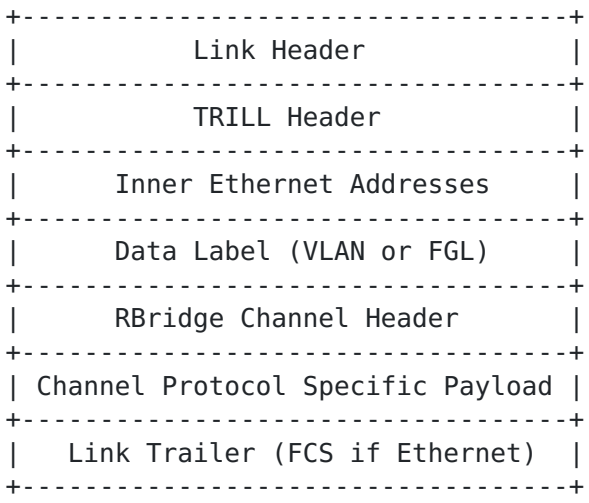

Figure 1. RBridge Channel Packet Structure

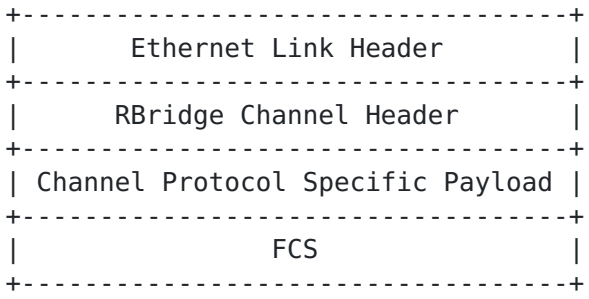

Figure 2. Native RBridge Channel Frame

The RBridge Channel Header looks like this:

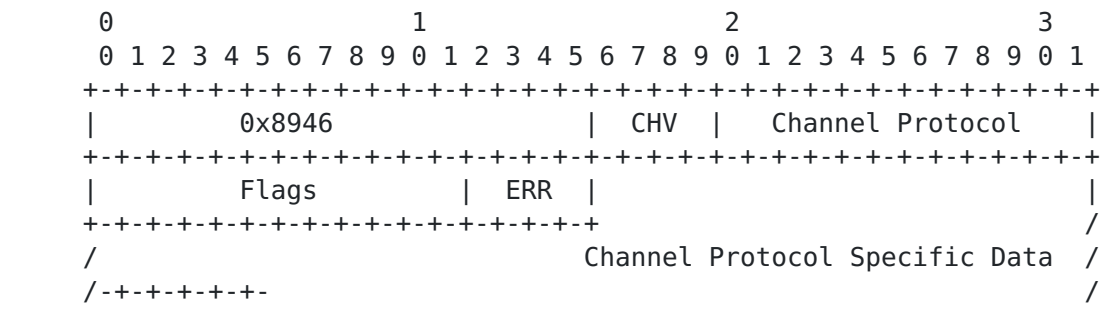

Figure 3. RBridge Channel Header

where 0x8946 is the RBridge Channel Ethertype and CHV is the Channel Header Version, currently zero.

The extensions specified herein are in the form of an RBridge Channel protocol, the Channel Tunnel Protocol. Figure 4 below expands the RBridge Channel Header and Protocol Specific Payload above for the case of the Channel Tunnel Protocol.

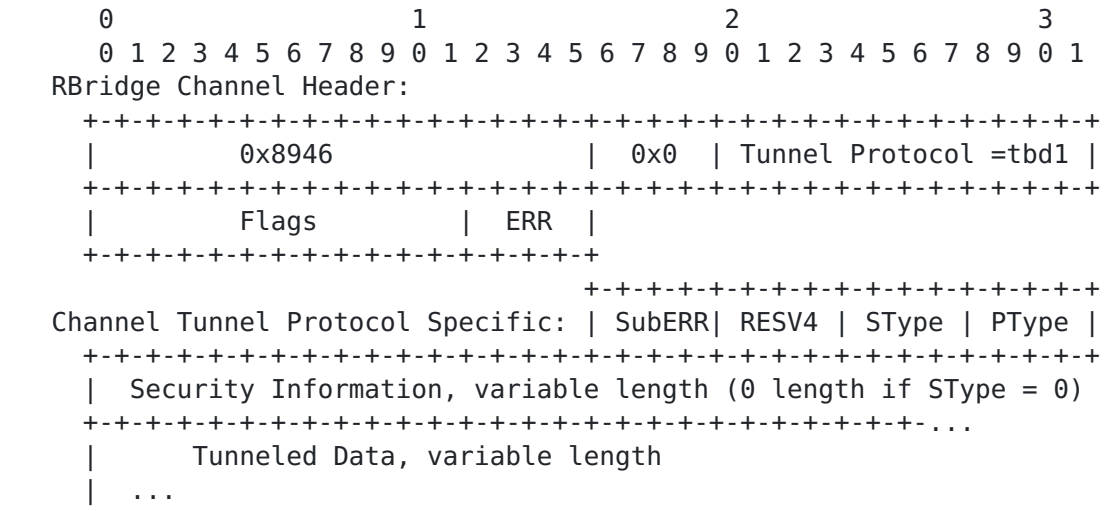

Figure 4. Channel Tunnel Header Structure

The RBridge Channel Header field specific to the RBridge Channel Tunnel Protocol is the Protocol field. Its contents MUST be the value allocated for this purpose (see Section 6).

The RBridge Tunnel Channel Protocol Specific Data fields are as follows:

SubERR: This field provides further details when a Tunnel Channel error is indicated in the RBridge Channel ERR field. If ERR is zero, then SubERR MUST be sent as zero and ignored on receipt. See Section 5.

RESV4: This field MUST be sent as zero. If non-zero when received, this is an error condition (see Section 4).

SType: This field describes the type of security information and features, including keying material, being provided. See Section 4.

PType: Payload type. This describes the tunneled data. See Section 3 below.

Security Information: Variable length information. Length is zero if SType is zero. See Section 4.

The Channel Tunnel protocol is integrated with the RBridge Channel facility. Channel Tunnel errors are reported as if they were RBridge Channel errors, using newly allocated code points in the ERR field of the RBridge Channel Header supplemented by the SubERR field.

3. Tunnel Payload Types

The RBridge Channel Tunnel Protocol can carry a variety of payloads as indicated by the PType field. Values are shown in the table below with further explanation after the table.

PType	Section	Description
0		Reserved
1	3.1	Null
2	3.2	RBridge Channel message
3	3.3	TRILL Data packet
4	3.4	TRILL IS-IS packet
5	3.5	Ethernet Frame
6-14		(Available for assignment by IETF Review)
15		Reserved

Table 1. Payload Type Values

While implementation of the Channel Tunnel protocol is optional, if it is implemented PTypes 1 (Null) and 2 (RBridge Channel message) MUST be implemented. PTypes 3, 4, and 5 MAY be implemented. The processing of any particular Channel Protocol message and its payload depends on meeting local security and other policy at the destination TRILL switch or end station.

3.1 Null Payload

The Null payload type (PType=1) is intended to be used for testing or messages such as key negotiation or the like. It indicates that there is no payload. Any data after the Security Information fields is ignored. Any particular use of the Null Payload should specify what VLAN or priority should be used when relevant.

3.2 RBridge Channel Message Payload

A PType of 2 indicates that the payload of the Channel Tunnel message is an encapsulated RBridge Channel message without the initial RBridge Channel Ethertype. Typical reasons for sending an RBridge Channel message inside a Channel Tunnel message are to provide security services, such as authentication or encryption.

This payload type looks like the following:

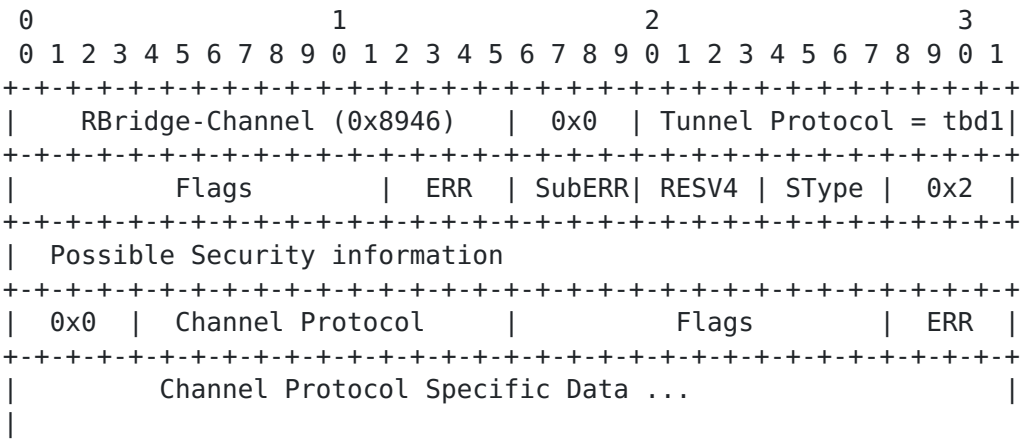

Figure 5. Tunneled Channel Message Channel Tunnel Structure

3.3 TRILL Data Packet

A PType of 3 indicates that the payload of the Tunnel protocol message is an encapsulated TRILL Data packet as shown in the figure below. (There is no TRILL Ethertype before the inner TRILL Data packet because that is just part of the Ethernet link header for a TRILL Data packet, not part of the TRILL header itself. The Optional Flags Word is only present if the F bit in the TRILL Header is 1.) If this PType is implemented and the message meets local policy for acceptance, the tunneled TRILL Data packet is handled as if it had been received by the destination TRILL switch on the port where the Channel Tunnel message was received.

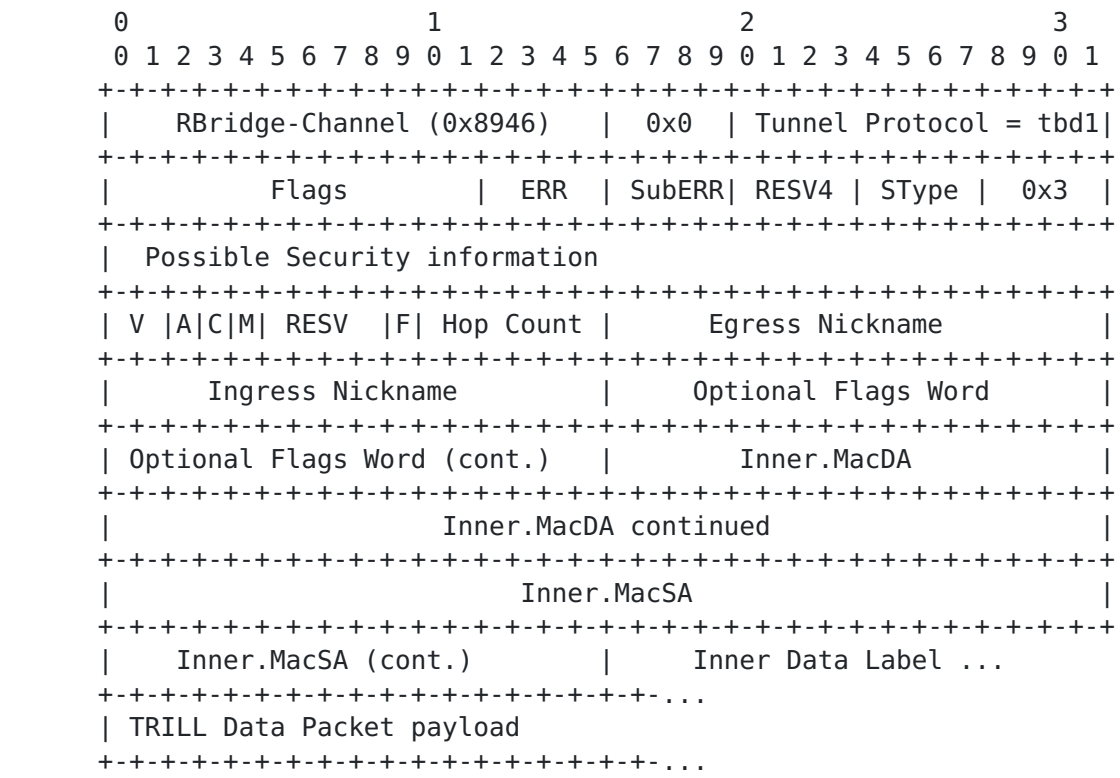

Figure 6. Nested TRILL Data Packet Channel Tunnel Structure

3.4 TRILL IS-IS Packet

A PType of 4 indicates that the payload of the Tunnel protocol message is an encapsulated TRILL IS-IS PDU packet without the initial L2-IS-IS Ethertype as shown in the figure below. If this PType is implemented, the tunneled TRILL IS-IS packet is processed by the destination RBridge if it meets local policy. One possible use is to expedite the receipt of a link state PDU by some TRILL switch or switches with an immediate requirement for the enclosed link state PDU. Any link local IS-IS PDU (Hello, CSNP, or PSNP [IS-IS]; MTU-probe, MTU-ack [RFC7176]; or circuit scoped FS-LSP, FS-CSNP or FS-PSNP [RFC7356]) received via this channel tunnel payload type MUST be discarded.

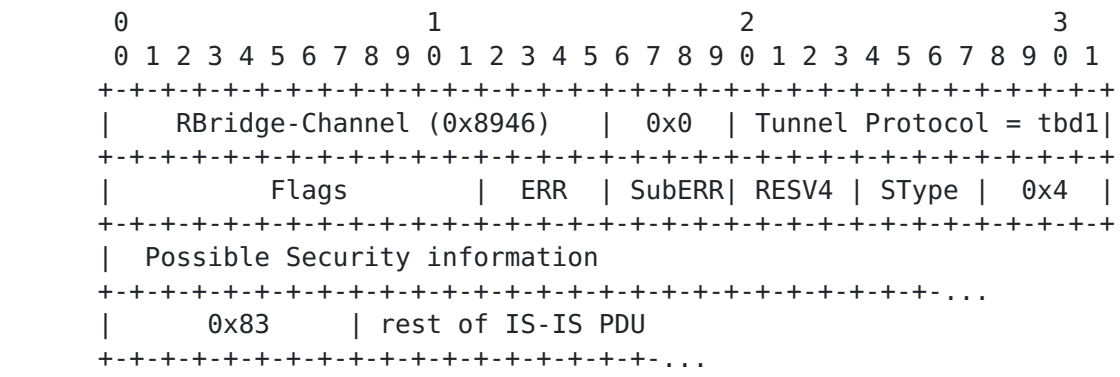

Figure 7. Tunneled TRILL IS-IS Packet Structure

3.5 Ethernet Frame

If PType is 5, the Tunnel Protocol payload is an Ethernet frame as might be received from or sent to an end station except that the tunneled Ethernet frame's FCS is omitted, as shown in Figure 8. (There is still an overall FCS if the RBridge Channel message is being sent on an Ethernet link.) If this PType is implemented and the message meets local policy, the tunneled frame is handled as if it had been received on the port on which the Tunnel Protocol message was received.

The priority of the RBridge Channel message can be copied from the Ethernet frame VLAN tag, if one is present, except that priorities 6 or 7 SHOULD only be used for important control messages.

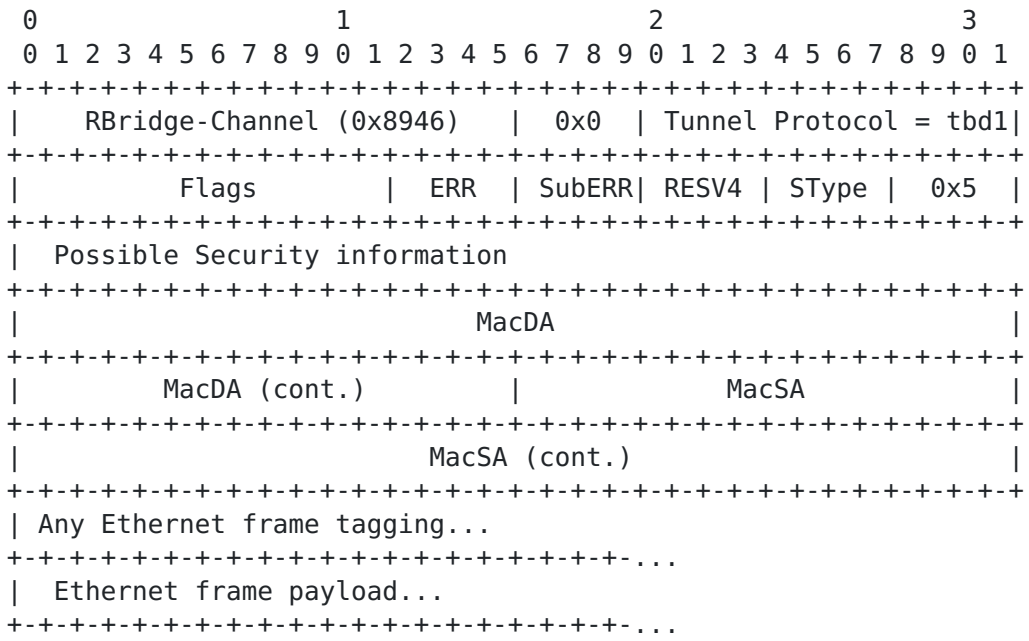

Figure 8. Ethernet Frame Channel Tunnel Structure

In the case of a non-Ethernet link, such as a PPP link [RFC6361], the ports on the link are considered to have link local synthetic 48-bit MAC addresses constructed by concatenating three 16-bit quantities. This constructed address MAY be used as the MacSA and, if the RBridge Channel message is link local, the source TRILL switch will have the information to construct such a MAC address for the destination TRILL switch port and that MAC address MAY be used as the MacDA.

These MAC addresses are constructed as follows: 0xFEFF, the nickname of the TRILL switch used in TRILL Hellos sent on that port, and the Port ID that the TRILL switch has assigned to that port, as shown in Figure 9. (Both the nickname and Port ID of the port on which a TRILL Hello is sent appear in the Special VLANs and Flags sub-TLV [RFC7176] in that Hello.) The resulting MAC address has the Local bit on and the Group bit off [RFC7042]. Since end stations are connected to TRILL switches over Ethernet, there will be no end stations on a non-Ethernet link in a TRILL campus. Thus such synthetic MAC addresses cannot conflict on the link with a real Ethernet port address.

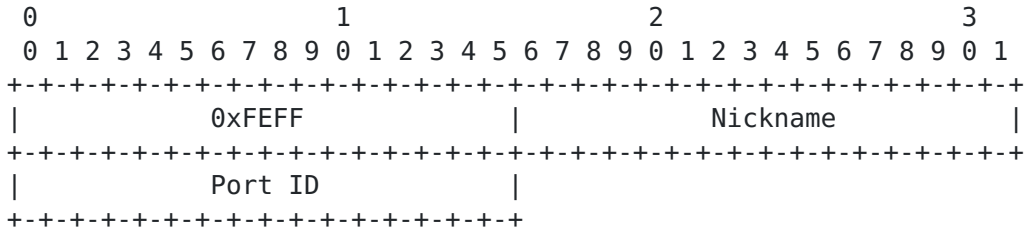

Figure 9. Synthetic MAC Address

4. Security, Keying, and Algorithms

The following table gives the assigned values of the SType field and their meaning.

SType	Section	Meaning
0	4.4	None
1	4.5	[RFC5310] Based Authentication
2	4.6	DTLS Based Security
3	4.7	[RFC5310] Based Encryption and Authentication
4-14		Available for assignment on IETF Review
15		Reserved

Table 3. SType Values

4.1 Basic Security Format

For all SType values except zero, the Security Information starts with a byte of flag bits and a byte of remaining length as follows:

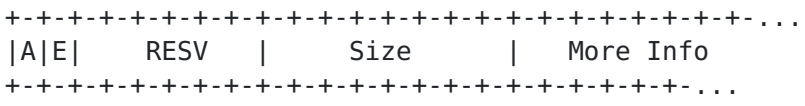

Figure 12. Security Information Format

The fields are as follows:

A: Zero if authentication is not being provided. One if it is.

E: Zero if encryption is not being provided. One if it is.

RESV: Six reserved bits that MUST be sent as zero and ignored on receipt. In the future, meanings may be assigned to these bits and those meanings may differ for different STypes.

Size: The number of bytes, as an unsigned integer, of More Info in the Security Information after the Size byte itself.

More Info: Additional Security Information of length Size. Contents depends on the SType.

The A and E bits are intended as hints and to assist is debugging. They are not guaranteed to be correct. They can be interpreted as follows:

A	E	Comments
0	0	Neither authentication nor encryption is being provided.
1	0	Authentication only. The payload should be parsable by a security ignorant receiver. The Size field permits skipping the More Info field.
0	1	Encryption only. Some form of opportunistic security [RFC7435].
1	1	Authentication and Encryption.

4.2 Authentication and Encryption Coverage

Authentication in the RBridge Channel case (see Figure 1) is computed across the inner Ethernet Addresses, Data Label, relevant Channel Tunnel header information, and the payload. To be more precise, the covered area starts with the byte immediately after the TRILL Header ingress nickname or optional flag word, if present, and extends to just before the TRILL Data packet link trailer, for example just before the FCS for Ethernet. If an authentication value is included in the Info field specified in Section 4.1, it is treated as zero when authentication is calculated. If an authentication value is included in a payload after the security information, it is calculated as provided by the SType and algorithms in use.

Authentication in the native RBridge Channel case (see Figure 2), is as specified in the above paragraph except that it starts with the RBridge Channel Ethertype, since there are no TRILL Header, inner Ethernet address, or Data Label.

If encryption is provided, it covers the payload from right after the Channel Tunnel header security information through to just before the TRILL Data packet link trailer.

4.3 Derived Keying Material

In some cases, it is possible to use keying material derived from [RFC5310] IS-IS keying material. In such cases, the More Info field shown in Section 4.1 includes a two byte Key ID to identify the IS-IS keying material. The keying material actually used in Channel Tunnel security is derived from the IS-IS keying material as follows:

HKDF-Expand-SHA256 (IS-IS-key, "Channel Tunnel" | 0x0S, L)

where "|" indicates concatenation, HKDF is as in [RFC5869], SHA256 is as in [RFC6234],IS-IS-key is the input keying material, "Channel Tunnel" is the 14-character [RFC20] string indicated, 0x0S is a single byte where S is the SType for which this key derivation is being used, and L is the length of output keying material needed.

4.4 SType None

No security services are being invoked. The length of the Security Information field (see Figure 6) is zero.

4.5 RFC 5310 Based Authentication

The Security Information (see Figure 6) is the flags and Size bytes specified in Section 4.1 with the value of the [RFC5310] Key ID and Authentication Data as shown in Figure 13.

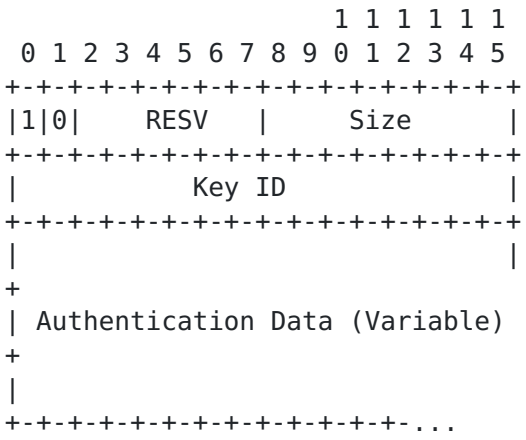

Figure 13. SType 1 Security Information

- RESV: Six bits that MUST be sent as zero and ignored or receipt.
- Size: Set to 2 + the size of Authentication Data in bytes.
- Key ID: specifies the same keying value and authentication algorithm that that Key ID specifies for TRILL IS-IS LSP [RFC5310] Authentication TLVs. The keying material actually used is derived as shown in Section 4.3.
- Authentication Data: The authentication data produced by the key and algorithm associated with the Key ID acting on the packet as specified in Section 4.2. Length of authentication data depends on the algorithm.

4.6 DTLS Based Security

DTLS supports key negotiation and provides both encryption and authentication. This optional SType in Channel Tunnel uses DTLS 1.2 [RFC6347]. It is intended for pairwise use. The presumption is that in the RBridge Channel case (Figure 1) the M bit in the TRILL Header would be zero and in the native RBridge Channel case (Figure 2), the Outer.MacDA would be individually addressed.

TRILL switches that implement the Channel Tunnel DTLS SType SHOULD support the use of certificates for DTLS. In this case the Size field shown in Section 4.1 MUST be zero and the Security Information is as shown in Figure 14.

Also, if they support certificates, they MUST support the following algorithm:

o TLS_RSA_WITH_AES_128_CBC_SHA256 [RFC5246]

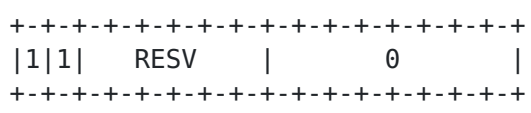

Figure 14. DTLS Cert or Special Pre-shared Key Security Information

TRILL switches that support the Channel Tunnel DTLS SType MUST support the use of pre-shared keys for DTLS. The Size field as shown in Section 4.1 MUST be either zero or 2. If Size is zero as shown in Figure 14, a pre-shared key specifically associated with Channel Tunnel DTLS is used. If Size is 2 as shown in Figure 15, a two byte [RFC5310] Key ID is present and the pre-shared key is derived from the secret key associated with that Key ID as shown in Section 4.3.

The following cryptographic algorithms MUST be supported for use with pre-shared keys:

o TLS_PSK_WITH_AES_128_CBC_SHA256 [RFC5487]

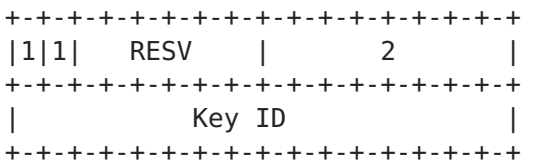

Figure 15. DTLS Derived Pre-shared Key Security Information

When DTLS security is used, the entire payload of the Channel Tunnel packet, starting just after the Security Information and ending just before the link trailer, is a DTLS record [RFC6347].

4.7 RFC 5310 Based Encryption and Authentication

This SType is based on pre-existing [RFC5310] keying material but does not use any algorithm that may be associated with a Key ID under [RFC5310]. Instead it uses the derived key as specified in Section 4.3 with the algorithm specified by a Crypto Suite ID. Key negotiation is not provided and this SType is intended for multi-destination message use. The presumption is that in the RBridge Channel case (Figure 1) the M bit in the TRILL Header would be one and in the native RBridge Channel case (Figure 2), the Outer.MacDA would be group addressed.

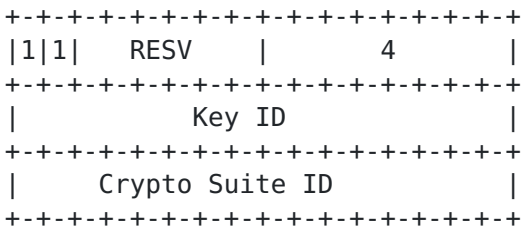

Figure 16. DTLS Derived Pre-shared Key Security Information

4.7.1 Channel-Tunnel-CCM

The initially specified Crypto Suite has ID 0x0001, is called Channel-Tunnel-CCM (Channel Tunnel Counter with CBC-MAC), and is mandatory to implement if this SType is supported.

Channel-Tunnel-CCM is based on [RFC3610] using AES-128 as the encryption function. The minimum authentication field size permitted is 8 octets. There is additional authenticated data which is the authenticated data indicated in Section 4.2 up to but not including any of the Tunneled Data (Figure 4). The message size is limited to 2**16 - 2**8 bytes so the length of the length of message field is always 2 bytes. There are thus 13 bytes available for nonce [RFC3610]. Since it is possible that the same Key ID could be used by different TRILL switches, the nonce MUST include an identifier for the originating TRILL switch. It is RECOMMENDED that this be the first 6 bytes of its IS-IS System ID as these will be unique across the campus. The remaining 7 bytes (56 bits) need to be such that the nonce is always unique for a particular key, for example a counter for which care is taken that it is always incremented after each use and its value is preserved over TRILL switch crashes, re-starts, and

the like. Should there be a danger of exhausting such a counter, the TRILL switch MUST take steps such as causing re-keying of the [RFC5310] key ID it is using and/or changing to use a different Key ID.

5. Channel Tunnel Errors

RBridge Channel Tunnel Protocol errors are reported like RBridge Channel level errors. The ERR field is set to one of the following error codes:

ERR	Meaning
6	Unknown or unsupported field value
7	Authentication failure
8	Error in nested RBridge Channel message
(more TBD?)	

Table 4. Additional ERR Values

5.1 SubERRs under ERR 6

If the ERR field is 6, the SubERR field indicates the problematic field or value as show in the table below.

SubERR	Meaning (for ERR = 6)
0	Non-zero RESV4 nibble
1	Unsupported SType
2	Unsupported PType
4	Unsupported crypto algorithm
5	Unknown Key ID
(more TBD)	

Table 5. SubERR values under ERR 6

5.2 Nested RBridge Channel Errors

If
   a Channel Tunnel message is sent with security and with a payload type (PType) indicating a nested RBridge Channel message
and
   there is an error in the processing of that nested message that results in a return RBridge Channel message with a non-zero ERR field,
then that returned message SHOULD also be nested in an Channel Tunnel message using the same type of security. In this case, the ERR field in the Channel Tunnel envelope is set to 8 indicating that there is a nested error being tunneled back.

6. IANA Considerations

IANA has assigned tbd1 as the RBridge Channel protocol number the "Channel Tunnel" protocol from the range assigned by Standards Action.

The added RBridge Channel protocols registry entry on the TRILL Parameters web page is as follows:

Protocol	Description	Reference
tbd1	Tunnel Channel	[this document]

7. Security Considerations

The RBridge Channel tunnel facility has potentially positive and negative effects on security.

On the positive side, it provides optional security that can be used to authenticate and/or encrypt RBridge Channel messages. Some RBridge Channel message payloads, such as BFD [RFC7175], provide their own security but where this is not true, consideration should be give to requiring use of the security features of the Tunnel Protocol.

On the negative side, the optional ability to tunnel various payload types and to tunnel them not just between TRILL switches but to and from end stations can increase risk unless precautions are taking. The processing of decapsulated Tunnel Protocol payloads is not a good place to be liberal in what you accept as the tunneling facility makes it easier for unexpected messages to pop up in unexpected places in a TRILL campus due to accidents or the actions of an adversary. Local policies should generally be strict and only process payload types required and then only with adequate authentication for the particular circumstances.

In connection with the use of DTLS for security as specified in Section 4.5, see [RFC7457].

See [RFC7178] for general RBridge Channel Security Considerations.

See [RFC6325] for general TRILL Security Considerations.

Normative References

[IS-IS] - ISO/IEC 10589:2002, Second Edition, "Information technology -- Telecommunications and information exchange between systems -- Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)", 2002.

[RFC20] - Cerf, V., "ASCII format for network interchange", STD 80, RFC 20, October 1969, <http://www.rfc-editor.org/info/rfc20>.

[RFC2119] - Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3610] - Whiting, D., Housley, R., and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, September 2003, <http://www.rfc-editor.org/info/rfc3610>.

[RFC5246] - Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC5310] - Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, February 2009.

[RFC5487] - Badra, M., "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", RFC 5487, March 2009, <http://www.rfc-editor.org/info/rfc5487>.

[RFC5869] - Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, May 2010, <http://www.rfc-editor.org/info/rfc5869>.

[RFC6325] - Perlman, R., D. Eastlake, D. Dutt, S. Gai, and A. Ghanwani, "RBridges: Base Protocol Specification", RFC 6325, July 2011.

[RFC6347] - Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012, <http://www.rfc-editor.org/info/rfc6347>.

[RFC7172] - Eastlake 3rd, D., Zhang, M., Agarwal, P., Perlman, R., and D. Dutt, "Transparent Interconnection of Lots of Links (TRILL): Fine-Grained Labeling", RFC 7172, May 2014.

[RFC7176] - Eastlake 3rd, D., Senevirathne, T., Ghanwani, A., Dutt, D., and A. Banerjee, "Transparent Interconnection of Lots of Links (TRILL) Use of IS-IS", RFC 7176, May 2014,

<http://www.rfc-editor.org/info/rfc7176>.

[RFC7178] - Eastlake 3rd, D., Manral, V., Li, Y., Aldrin, S., and D. Ward, "Transparent Interconnection of Lots of Links (TRILL): RBridge Channel Support", RFC 7178, May 2014.

[RFC7356] - Ginsberg, L., Previdi, S., and Y. Yang, "IS-IS Flooding Scope Link State PDUs (LSPs)", RFC 7356, September 2014, <http://www.rfc-editor.org/info/rfc7356>.

[rfc7180bis] - Eastlake, D., Zhang, M., Perlman, R. Banerjee, A., Ghanwani, A., and S. Gupta, "TRILL: Clarifications, Corrections, and Updates", Draft-ietf-trill-rfc7180bis, work in progress.

Informative References

[RFC6234] - Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, May 2011.

[RFC6361] - Carlson, J. and D. Eastlake 3rd, "PPP Transparent Interconnection of Lots of Links (TRILL) Protocol Control Protocol", RFC 6361, August 2011

[RFC7042] - Eastlake 3rd, D. and J. Abley, "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", BCP 141, RFC 7042, October 2013.

[RFC7175] - Manral, V., Eastlake 3rd, D., Ward, D., and A. Banerjee, "Transparent Interconnection of Lots of Links (TRILL): Bidirectional Forwarding Detection (BFD) Support", RFC 7175, May 2014.

[RFC7435] - Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, December 2014, <http://www.rfc-editor.org/info/rfc7435>.

[RFC7457] - Sheffer, Y., Holz, R., and P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)", RFC 7457, February 2015, <http://www.rfc-editor.org/info/rfc7457>.

Appendix Z: Change History

From -00 to -01

1. Fix references for RFCs published, etc.

2. Explicitly mention in the Abstract and Introduction that this document updates [RFC7178].

3. Add this Change History Appendix.

From -01 to -02

1. Remove section on the "Scope" feature as mentioned in http://www.ietf.org/mail-archive/web/trill/current/msg06531.html

2. Editorial changes to IANA Considerations to correspond to draft-leiba-cotton-iana-5226bis-11.txt.

3. Improvements to the Ethernet frame payload type.

4. Other Editorial changes.

From -02 to -03

1. Update TRILL Header to correspond to [rfc7180bis].

2. Remove a few remnants of the "Scope" feature that was removed from -01 to -02.

3. Substantial changes to and expansion of Section 4 including adding details of DTLS security.

4. Updates and additions to the References.

5. Other minor editorial changes.

From -03 to -04

1. Add SType for [RFC5310] keying based security that provides encryption as well as authentication.

2. Editorial improvements and fixes.

Acknowledgements

The contributions of the following are hereby acknowledged:

TBD

The document was prepared in raw nroff. All macros used were defined within the source file.

Authors' Addresses

Donald E. Eastlake, 3rd
Huawei Technologies
155 Beaver Street
Milford, MA 01757 USA

Phone: +1-508-333-2270
EMail: d3e3e3@gmail.com

Mohammed Umair
IPinfusion

EMail: mohammed.umair2@gmail.com

Yizhou Li
Huawei Technologies
101 Software Avenue,
Nanjing 210012, China

Phone: +86-25-56622310
EMail: liyizhou@huawei.com

Copyright, Disclaimer, and Additional IPR Provisions