

INTERNET-DRAFT

Updates: [7178](#)

Intended status: Proposed Standard

Donald Eastlake

Huawei

Mohammed Umair

IPinfusion

Yizhou Li

Huawei

Expires: December 11, 2016

June 12, 2016

TRILL: RBridge Channel Header Extension
<[draft-ietf-trill-channel-tunnel-09.txt](#)>

Abstract

The IETF TRILL (Transparent Interconnection of Lots of Links) protocol includes an optional mechanism (specified in [RFC 7178](#)) called RBridge Channel for the transmission of typed messages between TRILL switches in the same campus and the transmission of such messages between TRILL switches and end stations on the same link. This document specifies extensions to the RBridge Channel protocol header to support two features as follows: (1) a standard method to tunnel payloads whose type can be indicated by Ethertype through encapsulation in RBridge Channel messages; 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/lid-abstracts.html>. The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

INTERNET-DRAFT

TRILL: RBridge Channel Extension

Table of Contents

| | |
|---|--------------------|
| 1. Introduction..... | 3 |
| 1.1 Terminology and Acronyms..... | 3 |
| 2. RBridge Channel Header Extension Format..... | 5 |
| 3. Extended RBridge Channel Payload Types..... | 8 |
| 3.1 Null Payload..... | 8 |
| 3.2 Ethertyped Payload..... | 8 |
| 3.2.1 RBridge Channel Message as the Payload..... | 9 |
| 3.2.2 TRILL Data Packet as the Payload..... | 9 |
| 3.2.3 TRILL IS-IS Packet as the Payload..... | 10 |
| 3.3 Ethernet Frame..... | 11 |
| 4. Extended RBridge Channel Security..... | 14 |
| 4.1 Derived Keying Material..... | 14 |
| 4.2 SType None..... | 15 |
| 4.3 RFC 5310 Based Authentication..... | 15 |
| 4.4 DTLS Pairwise Security..... | 17 |
| 4.5 Composite Security..... | 18 |
| 5. Extended RBridge Channel Errors..... | 19 |
| 5.1 SubERRs under ERR 6..... | 19 |
| 5.2 Secure Nested RBridge Channel Errors..... | 19 |
| 6. IANA Considerations..... | 20 |
| 6.1 Extended RBridge Channel Protocol Number..... | 20 |
| 6.2 RBridge Channel Error Codes Subregistry..... | 20 |
| 7. Security Considerations..... | 21 |
| Normative References..... | 22 |
| Informative References..... | 23 |
| Appendix Z: Change History..... | 24 |
| Acknowledgements..... | 26 |
| Authors' Addresses..... | 27 |

INTERNET-DRAFT

TRILL: RBridge Channel Extension

1. Introduction

The IETF TRILL base protocol [[RFC6325](#)] [[RFC7780](#)] has been extended with the RBridge Channel [[RFC7178](#)] facility to support transmission of typed messages (for example BFD (Bidirectional Forwarding Detection) [[RFC7175](#)]) between two TRILL switches (RBridges) in the same campus and the transmission of such messages 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 message [[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 the RBridge Channel header that provide two additional facilities as follows:

- (1) A standard method to tunnel payloads whose type may be indicated by Ethertype through encapsulation in RBridge Channel messages.
- (2) A method to provide security facilities for RBridge Channel messages.

Use of each of these facilities is optional, except that, as specified below, if this header extension is implemented there are two payload types that MUST be implemented. Both of the above

facilities can be used in the same packet. 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", "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 new terms and acronyms.

application_data - A DTLS [[RFC6347](#)] message type.

Data Label - VLAN or FGL.

DTLS - Datagram Transport Level Security [[RFC6347](#)].

FCS - Frame Check Sequence.

FGL - Fine Grained Label [[RFC7172](#)].

HKDF - Hash based Key Derivation Function [[RFC5869](#)].

IS-IS - Intermediate System to Intermediate Systems [[IS-IS](#)].

PDU - Protocol Data Unit.

MTU - Maximum Transmission Unit

RBridge - An alternative term for a TRILL switch.

SHA - Secure Hash Algorithm [[RFC6234](#)].

Sz - Campus wide minimum link MTU [[RFC6325](#)] [[RFC7780](#)].

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

TRILL switch - A device that implements the TRILL protocol
[[RFC6325](#)] [[RFC7780](#)], sometimes referred to as an RBridge.

[2.](#) RBridge Channel Header Extension Format

The general structure of an RBridge Channel message between two TRILL switches (RBridges) in the same campus is shown in Figure 2.1 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 2.2 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](#)].

```
+-----+
|           Link Header           |
+-----+
```

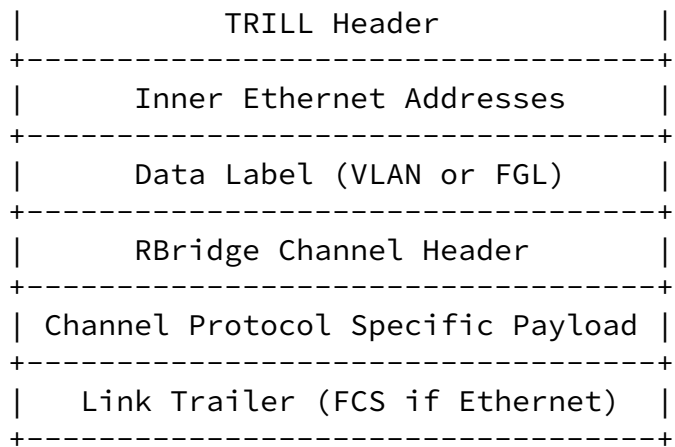


Figure 2.1 RBridge Channel Packet Structure

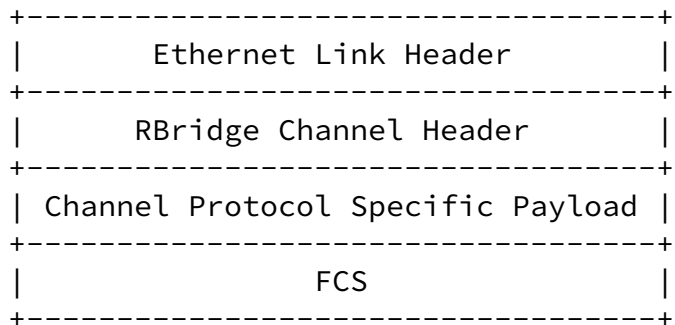
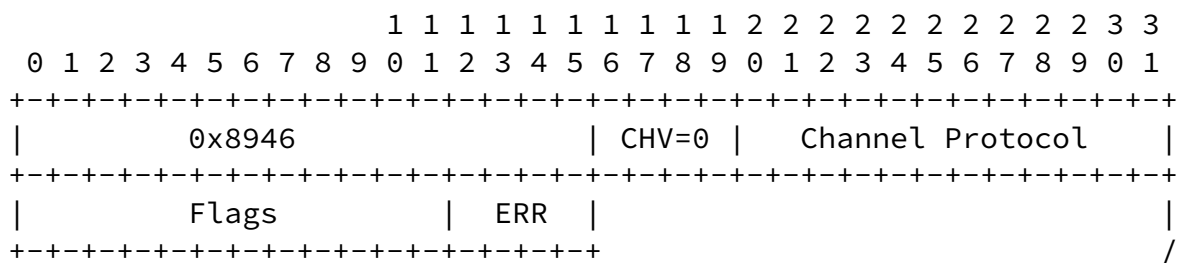


Figure 2.2 Native RBridge Channel Frame

The RBridge Channel Header looks like this:



```

/                                     Channel Protocol Specific Data      /
/---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
/

```

Figure 2.3 RBridge Channel Header

where 0x8946 is the RBridge Channel Ethertype and CHV is the Channel Header Version. This document is based on RBridge Channel version zero.

The header extensions specified herein are in the form of an RBridge Channel protocol, the RBridge Channel Extension Protocol. Figure 2.4 below expands the RBridge Channel Header and Protocol Specific Payload above for the case where the header extension is present.

```

1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
RBridge Channel Header:
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           0x8946           | CHV=0 | Channel Protocol=[TBD] |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Flags           | ERR   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
                                     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
Header Extension Specific:         | SubERR| RESV4 | SType | PType |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Security Information, variable length (0 length if SType = 0) /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+...
|   Tunneled Data, variable length
|   ...

```

Figure 2.4 RBridge Channel Header Extension Structure

The RBridge Channel Header Protocol field is used to indicate that the header extension is present. Its contents MUST be the value allocated for this purpose (see [Section 6](#)). The use of an RBridge Channel protocol to indicate extension makes it easy to determine if a remote RBridge in the campus supports extension since RBridges advertise in their LSP which such protocols they support.

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

SubERR: This field provides further details when an 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 5](#)).

SType: This field describes the type of security information and features, including keying material, being used or provided by the extended RBridge Channel message. 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 RBridge Channel Header Extension is integrated with the RBridge Channel facility. Extension 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.

INTERNET-DRAFT

TRILL: RBridge Channel Extension

3. Extended RBridge Channel Payload Types

The Extended RBridge Channel 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 | Ethertyped Payload |
| 3 | 3.3 | Ethernet Frame |
| 4-14 | | Unassigned |
| 15 | | Reserved |

Table 3.1 Payload Type Values

While implementation of the RBridge Channel Header Extension is optional, if it is implemented PType 1 (Null) MUST be implemented and PType 2 (Ethertyped Payload) with the RBridge Channel Ethertype MUST be implemented. PType 2 for any Ethertypes other than the RBridge Channel Ethertype MAY be implemented. PType 3 MAY be implemented.

The processing of any particular extended header RBridge Channel 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 for messages such as key negotiation or the like where only security information is present. It indicates that there is no payload. Any data after the Security Information field is ignored. If the RBridge Channel Header Extension is implemented, the Null Payload MUST be supported in the sense that an "Unsupported PType" error is not returned (see [Section 5](#)). Any particular use of the Null Payload should specify what VLAN or FGL and what priority should be used in the inner Data Label of the RBridge Channel message (or in an outer VLAN tag for the native RBridge Channel message case) when those values are relevant.

3.2 Ethertyped Payload

A PType of 2 indicates that the payload of the extended RBridge Channel message begins with an Ethertype. A TRILL switch supporting the RBridge Channel Header Extension MUST support a PType of 2 with a

payload beginning with the RBridge Channel Ethertype as described in [Section 3.2.1](#). Other Ethertypes, including the TRILL and L2-IS-IS Ethertypes as described in [Section 3.2.2](#) and 3.2.3, MAY be supported.

3.2.1 RBridge Channel Message as the Payload

A PType of 2 whose payload has an initial RBridge Channel Ethertype indicates an encapsulated RBridge Channel message. A typical reason for sending an RBridge Channel message inside an extended RBridge Channel message is to provide security services, such as authentication or encryption, for the encapsulated message.

This RBridge Channel message type looks like the following:

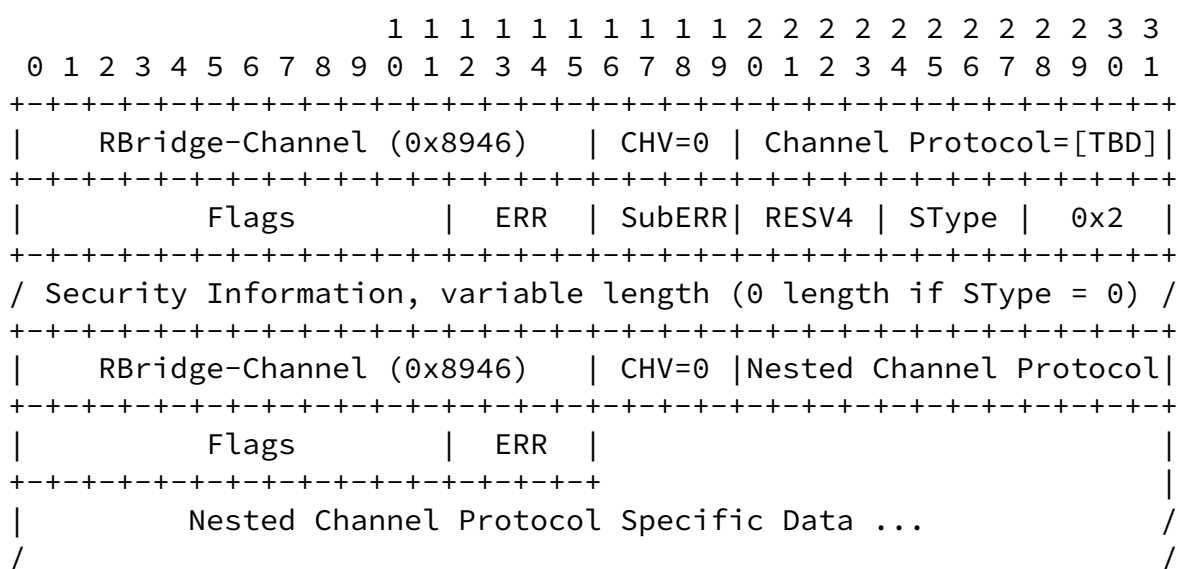


Figure 3.1 Message Structure with RBridge Channel Payload

3.2.2 TRILL Data Packet as the Payload

A PType of 2 whose payload has an initial TRILL Ethertype indicates an encapsulated TRILL Data packet as shown in the figure below. If this Ethertype is supported for PType = 2 and the message meets local policy for acceptance, the TRILL Data packet is handled as if it had been received by the destination TRILL switch on the port where the Extended RBridge Channel message was received.

```

      1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   RBridge-Channel (0x8946)   | CHV=0 | Channel Protocol=[TBD] |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Flags             | ERR  | SubERR| RESV4 | SType | 0x2  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
/ Security Information, variable length (0 length if SType = 0) /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   TRILL (0x22F3)            | V |A|C|M| RESV  |F| Hop Count |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Egress Nickname           |   Ingress Nickname           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
/                               Optional Flags Word                               /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               Inner.MacDA                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Inner.MacDA continued     |   Inner.MacSA                 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               Inner.MacSA (cont.)              |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               Inner Data Label (2 or 4 bytes)
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+...
|   TRILL Data Packet payload
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+...
```

Figure 3.2 Message Structure with TRILL Data Packet Payload

The optional flags word is only present if the F bit in the TRILL Header is one [RFC7780].

3.2.3 TRILL IS-IS Packet as the Payload

A PType of 2 and an initial L2-IS-IS Ethertype indicates that the payload of the Extended RBridge Channel protocol message is an encapsulated TRILL IS-IS PDU as shown in Figure 3.3. If this Ethertype is supported for PType = 2, 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 (LSP) by some TRILL switch or switches with an immediate requirement for the link state information. A link local IS-IS PDU (Hello, CSNP, or PSNP [IS-IS]; MTU-probe or MTU-ack [RFC7176]; or circuit scoped FS-LSP, FS-CSNP or FS-PSNP [RFC7356]) would not normally be sent via this Extended RBridge Channel method except possibly to encrypt it since such PDUs can just be transmitted on the link and do not normally need RBridge Channel handling.

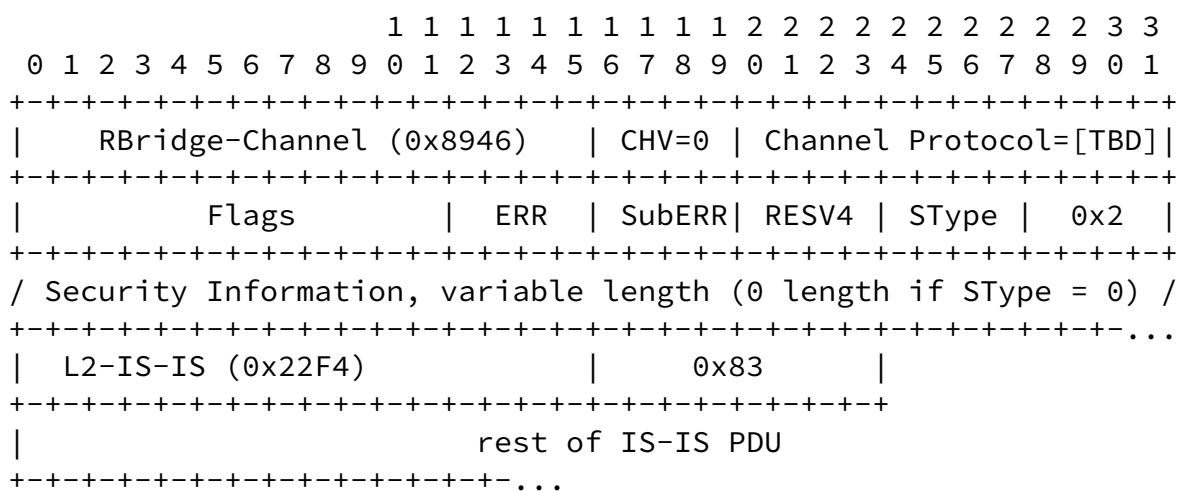


Figure 3.3 Message Structure with TRILL IS-IS Packet Payload

3.3 Ethernet Frame

If PType is 3, the extended RBridge Channel payload is an Ethernet frame as might be received from or sent to an end station except that the encapsulated Ethernet frame's FCS is omitted, as shown in Figure 3.4. (There is still an overall final 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 encapsulated frame is handled as if it had been received on the port on which the Extended RBridge Channel 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 priority 7 SHOULD only be used for messages critical to establishing or maintaining adjacency and priority 6 SHOULD only be used for other important control messages.

[illegible]

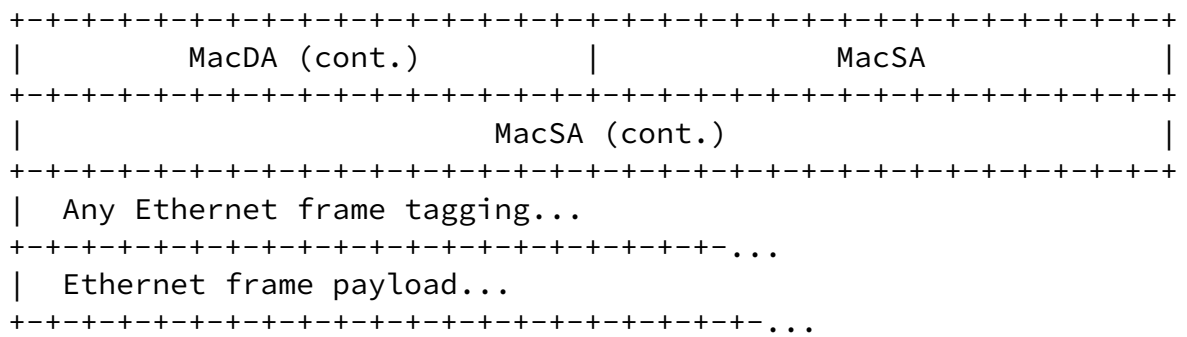


Figure 3.4 Message Structure with Ethernet Frame Payload

In the case of a non-Ethernet link, such as a PPP (Point-to-Point Protocol) link [[RFC6361](#)], the ports on the link are considered to have link local synthetic 48-bit MAC addresses constructed as described below. These constructed addresses MAY be used as a MacSA. If the RBridge Channel message is individually addressed to a link local port, 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. By the use of such a MacSA and either such a unicast MacDA or a group addressed MacDA, an Ethernet frame can be sent between two TRILL switch ports connected by a non-Ethernet link.

These synthetic TRILL switch port MAC addresses for non-Ethernet ports 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 3.5. (Both the Port ID of the port on which a TRILL Hello is sent and the nickname of the sending TRILL switch appear in the Special VLANs and Flags sub-TLV [[RFC7176](#)] in TRILL IS-IS Hellos.) The resulting MAC address has the Local bit on and the Group bit off [[RFC7042](#)]. However, since there will be no Ethernet end stations on a non-Ethernet link in a TRILL campus, such synthetic MAC addresses cannot conflict on the link with a real Ethernet port address regardless of their value.

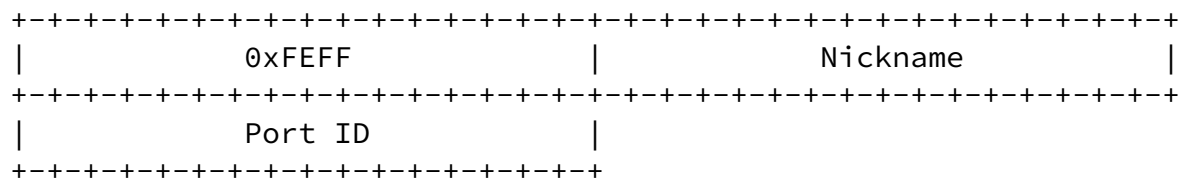


Figure 3.5 Synthetic MAC Address

4. Extended RBridge Channel Security

Table 4.1 below gives the assigned values of the SType field and their meaning. Use of DTLS Pairwise Security (SType = 2) or Composite Security (SType = 3) is RECOMMENDED.

While [[RFC5310](#)] based authentication is also specified and can be use for both pairwise and multi-destination traffic, it provides only authentication and is not considered to meet current security standards. For example, it does not provide for key negotiation; thus, its use is NOT RECOMMENDED.

The Extended RBridge Channel DTLS based security specified in [Section 4.4](#) and the Composite Security specified in [Section 4.5](#) below are intended for pairwise (known unicast) use. That is, the case where the M bit in the TRILL Header is zero and any Outer.MacDA is individually addressed.

Multi-destination Extended RBridge Channel packets would be those with the M bit in the TRILL Header set to one or, in the native RBridge Channel case, the Outer.MacDA would be group addressed. The DTLS Pairwise Security and Composite Security STypes can also be used in the multi-destination case by serially unicasting the messages to all data accessible R Bridges (or stations in the native RBridge Channel case) in the recipient group. For TRILL Data packets, that group is specified by the Data Label; for native frames, the group is specified by the groupcast destination MAC address. It is intended to specify a true group keyed SType to secure multi-destination packets in a separate document [[GroupKey](#)].

| SType | Section | Meaning |
|-------|---------|--|
| ----- | ----- | ----- |
| 0 | 4.2 | None |
| 1 | 4.3 | [RFC5310] Based Authentication |
| 2 | 4.4 | DTLS Pairwise Security |
| 3 | 4.5 | Composite Security |
| 4-14 | | Available for assignment by IETF Review |
| 15 | | Reserved |

Table 4.1 SType Values

4.1 Derived Keying Material

In some cases, it is possible to use material derived from [[RFC5310](#)]

IS-IS keying material as an element of Extended RBridge Channel security. It is assumed that the IS-IS keying material is of high quality. The material actually used is derived from the IS-IS keying material as follows:

Derived Material =

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

where "|" indicates concatenation, HKDF is as in [RFC5869], SHA256 is as in [RFC6234], IS-IS-key is the input IS-IS keying material, "Extended Channel" is the 16-character ASCII [RFC20] string indicated without any leading length byte or trailing zero byte, 0x0S is a single byte where S is the SType for which this key derivation is being used and the upper nibble is zero, and L is the length of output-derived material needed.

Whenever IS-IS keying material is being used as above, the underlying [RFC5310] keying material might expire or be invalidated. At the time of or before such expiration or invalidation, the use of the Derived Material from the IS-IS keying material MUST cease. Continued security MAY use new derived material from currently valid [RFC5310] keying material.

4.2 SType None

No security services are being invoked. The length of the Security Information field (see Figure 2.4) is zero.

4.3 RFC 5310 Based Authentication

This SType provides security for Extended RBridge Channel messages similar to that provided for [IS-IS] PDUs by the [IS-IS] Authentication TLV. The Security Information (see Figure 2.4) is as shown in Figure 4.1.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|------|---|---|---|---|---|--|
| | | | | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | | |
| +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+ | | | | | | | | | | | | | | | | | |
| RESV | | | | | | | | | | | Size | | | | | | |

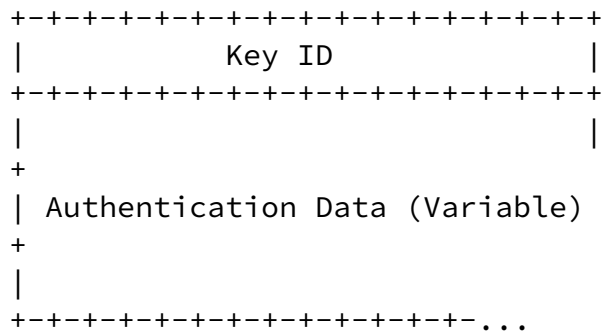
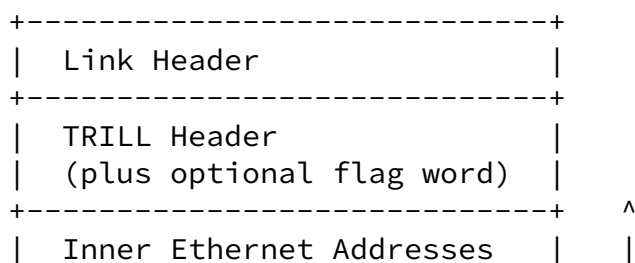


Figure 4.1 SType 1 Security Information

- o RESV: Four bits that MUST be sent as zero and ignored or receipt.
- o Size: Set to 2 + the size of Authentication Data in bytes.
- o Key ID: specifies the keying value and authentication algorithm that the Key ID specifies for TRILL IS-IS LSP [\[RFC5310\]](#) Authentication TLVs. The keying material actually used is derived as shown in [Section 4.1](#).
- o Authentication Data: The authentication data produced by the derived key and algorithm associated with the Key ID acting on the part of the TRILL Data packet shown. Length of the authentication data depends on the algorithm. The authentication value is included in the security information field and is treated as zero when authentication is calculated.

As show in Figure 4.2, the area covered by this authentication starts with the byte immediately after the TRILL Header optional Flag Word if it is present. If the Flag Word is not present, it starts after the TRILL Header Ingress Nickname. In either case, it extends to just before the TRILL Data packet link trailer. For example, for an Ethernet packet it would extend to just before the FCS.



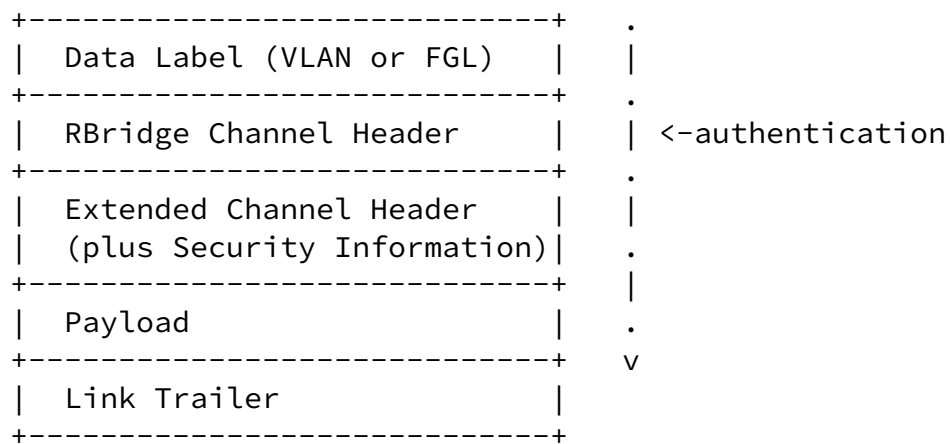


Figure 4.2. SType 1 Authentication Coverage

In the native RBridge Channel case this authentication coverage is as specified in the above paragraph except that it starts with the RBridge Channel Ethertype, since there is no TRILL Header, inner Ethernet addresses, or inner Data Label (see Figure 4.3).

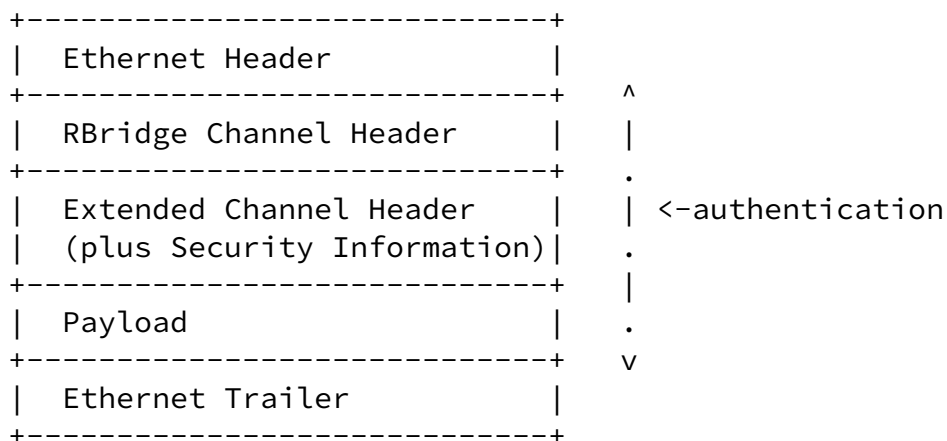


Figure 4.3. Native SType 1 Authentication Coverage

While RBridges, which are IS-IS routers, can reasonably be expected to hold [RFC5310] keying, so that this SType can be used for RBridge Channel messages, how end stations might come to hold [RFC5310] keying is beyond the scope of this document. Thus this SType might not be applicable to native RBridge Channel messages.

[4.4](#) DTLS Pairwise Security

DTLS [[RFC6347](#)] supports key negotiation and provides both encryption and authentication. The RBridge Channel Extended Header DTLS Pairwise SType uses a negotiated DTLS version that MUST NOT be less than 1.2.

When DTLS pairwise security is used, the entire payload of the Extended RBridge Channel packet, starting just after the null Security Information and ending just before the link trailer, is one or more DTLS records [[RFC6347](#)]. As specified in [[RFC6347](#)], DTLS records MUST be limited by the path MTU, in this case so each record fits entirely within a single Extended RBridge Channel message. A minimum path MTU can be determined from the TRILL campus minimum MTU Sz, which will not be less than 1470 bytes, by allowing for the TRILL Data packet, extended RBridge Channel, and DTLS framing overhead. With this SType, the security information between the extended RBridge Channel header and the payload is null because all the security information is in the payload area.

The DTLS Pairwise keying is set up between a pair of RBridges independent of Data Label using messages of a priority configurable at the RBridge level which defaults to priority 6. DTLS message types other than application_data can be the payload of an extended RBridge Channel message with a TRILL Header using any Data Label. Actual application_data sent within such a message using this SType SHOULD use the Data Label and priority as specified for that application_data. In this case, the PType value in the RBridge

Channel Header Extension applies to the decrypted application_data.

TRILL switches that implement the extended RBridge Channel DTLS Pairwise SType SHOULD support the use of certificates for DTLS but certificate size may be limited by the DTLS requirement that each record fit within a single message.

TRILL switches that support the extended RBridge Channel DTLS Pairwise SType MUST support the use of pre-shared keys. If the psk_identity (see [[RFC4279](#)]) is two bytes, it is interpreted as a [[RFC5310](#)] Key ID and the value derived as shown in [Section 4.1](#) from that key is used as a pre-shared key for DTLS negotiation. A psk_identity with a length other than two bytes MAY be used to indicate other implementation dependent pre-shared keys. Pre-shared

keys used for DTLS negotiation SHOULD be shared only by the pair of end points; otherwise, security could be attacked by diverting messages to another end point holding that pre-shared key.

[4.5](#) Composite Security

Composite Security (SType = 3) is the combination of DTLS Pairwise Security and [\[RFC5310\]](#) Based Authentication. On transmission, the DTLS record or records to be sent are secured as specified in [Section 4.4](#) then used as the payload for the application of Authentication as specified in [Section 4.3](#). On reception, the [\[RFC5310\]](#) based authentication is verified first and an error returned if it fails. Then the DTLS record(s) are processed.

An advantage of Composite Security is that the payload is authenticated and encrypted with a modern security protocol and, in addition, the RBridge Channel Header and (except in the native case) preceding MAC addresses and Data Label are provided with some authentication.

[5](#). Extended RBridge Channel Errors

RBridge Channel Header Extension errors are reported like RBridge Channel 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 |

Table 5.1 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 shown in the table below.

| SubERR | Meaning (for ERR = 6) |
|--------|--|
| ----- | ----- |
| 0 | Reserved |
| 1 | Non-zero RESV4 nibble |
| 2 | Unsupported SType |
| 3 | Unsupported PType |
| 4 | Unknown Key ID |
| 5 | Unsupported Ethertype with PType = 2 |
| 6 | Unsupported authentication algorithm for SType = 1 |

Table 5.2 SubERR values under ERR 6

[5.2](#) Secure Nested RBridge Channel Errors

If
 an extended RBridge Channel message is sent with security and with
 a payload type (PType) indicating an Ethertyped payload and the
 Ethertype indicates 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 extended
 RBridge Channel message using the same type of security. In this
 case, the ERR field in the Extended RBridge Channel envelope is set
 to 8 indicating that there is a nested error in the message being
 tunneled back.

[6. IANA Considerations](#)

This section lists IANA Considerations.

[6.1 Extended RBridge Channel Protocol Number](#)

IANA is requested to assign TBD [4 recommended] from the range assigned by Standards Action as the RBridge Channel protocol number to indicate RBridge Channel Header Extension.

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

| Protocol | Description | Reference |
|----------|---------------------------|-----------------|
| TBD[4] | RBridge Channel Extension | [this document] |

[6.2 RBridge Channel Error Codes Subregistry](#)

IANA is requested to create a "RBridge Channel Error Codes" subregistry under the "RBridge Channel Protocols" registry. The header information is as follows:

Registration Procedures: IETF Review
References: [[RFC7178](#)] [this document]

The subregistry is to have columns and entries as follows:

| Code | Meaning | Reference |
|------|---------|-----------|
| ---- | ----- | ----- |

[populate rows for codes 0 through 5 from [Section 3.2 of RFC7178](#) with reference [[RFC7178](#)]]

[populate rows for codes 6 through 8 from Table 5.1 of this document with reference [this document]]

| | |
|------|------------|
| 9-15 | Unassigned |
| 16 | Reserved |

INTERNET-DRAFT

TRILL: RBridge Channel Extension

7. Security Considerations

The RBridge Channel Header Extension 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 given, when specifying an RBridge Channel protocol, to recommending or requiring use of the security features of the RBridge Channel Header Extension.

On the negative side, the optional ability to tunnel more payload types and to tunnel them between TRILL switches and to and from end stations can increase risk unless precautions are taken. The processing of decapsulating extended RBridge Channel payloads is not a good place to be liberal in what you accept. This is because 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 accept payload types required and then only with adequate security for the particular circumstances.

See the first paragraph of [Section 4](#) for recommendations on SType usage.

See [[RFC7457](#)] for Security Considerations of DTLS for security.

If IS-IS authentication is not being used, then [[RFC5310](#)] keying information would not normally be available but that presumably represents a judgment by the TRILL campus operator that no security is needed.

See [[RFC7178](#)] for general RBridge Channel Security Considerations and [[RFC6325](#)] for general TRILL Security Considerations.

INTERNET-DRAFT

TRILL: RBridge Channel Extension

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 routing 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](http://www.rfc-editor.org/info/rfc20), DOI 10.17487/RFC0020, October 1969, <<http://www.rfc-editor.org/info/rfc20>>.
- [RFC2119] - Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](http://www.rfc-editor.org/info/rfc2119), [RFC 2119](http://www.rfc-editor.org/info/rfc2119), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC4279] - Eronen, P., Ed., and H. Tschofenig, Ed., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", [RFC 4279](http://www.rfc-editor.org/info/rfc4279), DOI 10.17487/RFC4279, December 2005, <<http://www.rfc-editor.org/info/rfc4279>>.
- [RFC5310] - Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", [RFC 5310](http://www.rfc-editor.org/info/rfc5310), DOI 10.17487/RFC5310, February 2009, <<http://www.rfc-editor.org/info/rfc5310>>.
- [RFC5869] - Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", [RFC 5869](http://www.rfc-editor.org/info/rfc5869), May 2010, <<http://www.rfc-editor.org/info/rfc5869>>.
- [RFC6325] - Perlman, R., Eastlake 3rd, D., Dutt, D., Gai, S., and A. Ghanwani, "Routing Bridges (RBridges): Base Protocol

Specification", [RFC 6325](#), DOI 10.17487/RFC6325, July 2011, <<http://www.rfc-editor.org/info/rfc6325>>.

[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](#), DOI 10.17487/RFC7172, May 2014, <<http://www.rfc-editor.org/info/rfc7172>>.

[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>>.

D. Eastlake, M. Umair, & Y. Li

[Page 22]

INTERNET-DRAFT

TRILL: RBridge Channel Extension

[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](#), DOI 10.17487/RFC7178, May 2014, <<http://www.rfc-editor.org/info/rfc7178>>.

[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>>.

[RFC7780] - Eastlake 3rd, D., Zhang, M., Perlman, R., Banerjee, A., Ghanwani, A., and S. Gupta, "Transparent Interconnection of Lots of Links (TRILL): Clarifications, Corrections, and Updates", [RFC 7780](#), DOI 10.17487/RFC7780, February 2016, <<http://www.rfc-editor.org/info/rfc7780>>.

Informative References

[RFC6234] - Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", [RFC 6234](#), DOI 10.17487/RFC6234, May 2011, <<http://www.rfc-editor.org/info/rfc6234>>.

[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.

[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>>.

[GroupKey] - D. Eastlake et al, "Group Keying Protocol", [draft-ietf-trill-group-keying](#), work in progress.

Appendix Z: Change History

RFC Editor: Please delete this Appendix before publication.

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 [[RFC7780](#)].
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.

From -04 to -05

1. Primary change is collapsing the previous PTypes 2, 3, and 4 for RBridge Channel message, TRILL Data, and TRILL IS-IS into one by

D. Eastlake, M. Umair, & Y. Li

[Page 24]

INTERNET-DRAFT

TRILL: RBridge Channel Extension

- including the Ethertype. Previous PType 5 is renumbered as 3.
2. Add Channel Tunnel Crypto Suites to IANA Considerations
 3. Add some material to Security Considerations,
 4. Assorted Editorial changes.

From -05 to -06

Fix editorials found during WG Last Call.

From -06 to -07

Minor editorial changes resulting for Shepherd review.

From -07 to -08

Move group keyed security out of the draft. Simplify and improve remaining security provisions.

From -08 to -09

1. Updates based on Routing Directorate review.
2. Improvements to specification of pairwise DTLS and significant other security improvements.

The contributions of the following are hereby gratefully acknowledged:

Jonathan Hardwick, Susan Hares, Gayle Noble, and Yaron Sheffer

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

INTERNET-DRAFT

TRILL: RBridge Channel Extension

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

INTERNET-DRAFT

TRILL: RBridge Channel Extension

Copyright, Disclaimer, and Additional IPR Provisions

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License. The definitive version of an IETF Document is that published by, or under the auspices of, the IETF. Versions of IETF Documents that are published by third parties, including those that are translated into other languages, should not be considered to be definitive versions of IETF Documents. The definitive version of these Legal Provisions is that published by, or under the auspices of, the IETF. Versions of these Legal Provisions that are published by third parties, including those that are translated into other languages, should not be considered to be definitive versions of these Legal Provisions. For the avoidance of doubt, each Contributor to the IETF Standards Process licenses each Contribution that he or she makes as part of the IETF Standards Process to the IETF Trust pursuant to the provisions of [RFC 5378](#). No language to the contrary, or terms, conditions or rights that differ from or are inconsistent with the rights and licenses granted under [RFC 5378](#), shall have any effect and shall be null and void, whether published or posted by such Contributor, or included with or in such Contribution.

