Network Working Group
Internet Draft
Document: draft-tsenevir-smpls-02.txt
Category: Informational

Tissa Senevirathne

July 2002

Secure MPLS - Encryption and Authentication of MPLS payloads

Status of this Memo

Abstract

This document specifies a mechanism for securing the MPLS data plane, ie securing any data carried over MPLS. This work is split into two aspects: use of IKE to establish the required security association for secure MPLS and definition of the encapsulation formats required for the encryption and authentication of MPLS payloads. Extensions, under the form of a new Domain of Interpretation, are defined for the use of IKE to set up Security Associations for secure MPLS. Also, two methods are presented to transport IKE messages between edge LSRs: IKE over RSVP and IKE over a separate IP channel. A new RSVP object is defined to exchange security association messages as part of the LSP setup messages. It is thought that the use of a separate IP channel facilitates scaling, especially in the environment where multiple LSPÆs terminate between the same two edge LSRs.

Conventions used in this document

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 [1].

Table of Contents

Conventions used in this document....2
1.0 Introduction:....2
2.0 Use of IKE for Secure MPLS....4
2.1 Security Protocol Identifier....5
2.2 Identification Types....5
2.2.1 Identification Payload....6
3.0 Use of RSVP-TE to transport IKE messages....7
3.0.1 RSVP Transport Message....7
3.1 Secure_MPLS_Message Object....8
4.0 Placement of Secure MPLS, IKE and RSVP-TE....10
4.1 IKE messages and Secure MPLS DOI....11
4.2 Handling of Security Associations....11
5.0 Secure MPLS payload encapsulation....11
5.1 Possible SMPLS encapsulation formats....12
5.2 SMPLS Encapsulation header types....13
5.2.1 SMPLS Authentication Header SMPLS-AH....13
5.2.2 SMPLS Encapsulating Security Payload (SMPLS-ESP)....14
5.3 Outbound Packet Processing....16
5.3.1 Security Association Lookup....16
5.3.2 Integrity Check Value Calculation in SMPLS-AH....16
5.3.3 Integrity Check Value Calculation in SMPLS-ESP....16
5.3.4 MPLS Payload Encryption in SMPLS-ESP....16
5.4 Inbound Packet Processing....17
6.0 Other Issues....18
6.1 Path MTU discovery....18
6.2 LSP Setup Requirements....18
6.3 Intermediate LSR....18
6.4 Label merging....18
6.5 Penultimate Hop popping....19
7.0 Security Considerations....19
8.0 Acknowledgment....19
9.0 References....19
10.0 Author's Addresses....20
Full Copyright Statement....20

1.0 Introduction:

MPLS is gaining popularity as a protocol that provides traffic engineering and other service capabilities beyond the strength of traditional routing. There are several deployments that use MPLS for wide area application or VPN services. However, at present, there

are no established methods to provide MPLS payload encryption and

authentication. In addition, MPLS is gaining popularity in transport of non-IP traffic (Layer 2) over long haul Wide Area Network. Hence, the definition of a protocol agnostic (as opposed to IPSec) security architecture for MPLS is becoming more and more important. This paper presents possible methods to establish security association for MPLS payload encryption and authentication (together with anti-replay).

Encryption and authentication of IP packets are performed using a suite of well-established protocols. This protocol suite is collectively known as IPSec. Internet Key Exchange (IKE) [2] defines the messaging protocol that is used to establish required security associations for key distribution. IKE is a very generic messaging protocol that can be used and tailored to set up Security Associations for a variety of security protocols, so-called Domains of Interpretation (DOI). In particular, the IPsec DOI [3] defines specific extensions and details of adaptation to IKEfor managing Security Associations for IPsec. In IPSec, IKE uses a separate IP Control channel between the end points to negotiate and establish security associations.

Constrained routed Label Switched Paths are used in MPLS to setup traffic engineered tunnels. RSVP-TE [4] or CR-LDP[5] are used for setting up such constrained LSPs. The fact that there is a security association with the LSP can be considered as a constrain on the LSP. IKE is a generic protocol that could be exchanged using any transport protocol other than UDP. Hence, the ability to perform IKE over RSVP-TE or CR-LDP avoids the need of a separate IP control channel. In this paper we present the methods to exchange IKE messages using RSVP-TE extensions. CR-LDP could also be extended for this purpose. Use of CR-LDP for this purpose will be presented in a separate paper.

Security Associations (SA) constructed using IKE are uni-directional in nature. MPLS LSPs are uni-directional in nature. Hence, IKE and Secure MPLS complement with each other without any changes to existing concepts.

In practice, there are multiple LSPs between two edge LSRs. Suppose these LSPs require secure MPLS services. If the management of Secure MPLS services is implemented using IKE over RSVP-TE extensions, there may need to be a separate Phase 1 Security Association for each LSP if the RSVP sessions are not able to share the phase 1 and SMPLS Security Associations. On the other hand if there is a separate control channel to negotiate and establish security associations, that channel may be used for key distribution and management of multiple secure LSPs. This can be achieved with few additions to the existing IKE definitions and will be able to reuse the same ISAKMP code base used for IPSec. In this document we present extensions to IKE under the form of a new DOI (based on the IPSec DOI) to establish secure MPLS services.

Secure MPLS needs to address all the well-known security considerations such as replay attacks, connection hijacking etc.

IPSec encapsulation is designed to address these issues. However, some of the IPSec encapsulation methods become trivial in MPLS. As an example, tunnel mode in IPSec is essentially MPLS LSP. In this document we present a Secure MPLS encapsulation format. Secure MPLS encapsulation format is similar to IPSec, but only addresses the specific needs of MPLS.

This document is broadly classified into two parts. Part one presents the use of IKE for Security Association establishment for secure MPLS. Use of RSVP-TE or dedicated IP control channel for IKE message transport are discussed. The newly proposed SMPLS DOI required for negotiating SMPLS Security Associations with IKE is discussed in an accompanying document [6].

The part two of this document presents the Secure MPLS payload formats. Also it defines various Secure MPLS operational modes.

In future, it may be required to further divide this document into multiple documents to cover the full scope of the Secure MPLS. Such work may at least include the following documents

- Secure MPLS Architecture
- Secure MPLS Domain of Interpretation (DOI)
  see [6]
- Secure MPLS message transport
  (Use of RSVP-TE or separate control channel)
- Secure MPLS payload format

2.0 Use of IKE for Secure MPLS

IKE [2] is designed to negotiate security parameters for multiple applications over a single Phase I security association. In practice, between two LSRs there may be multiple LSPs. As suggested earlier, when using RSVP-TE to transport IKE messages, there is no common session between all LSPs. Each RSVP session is unique for that LSP and bound to the life of the LSP. Depending on the actual realization, this may inhibit the ability to use a single Phase I session for multiple LSPs. As a result, edge LSRs would be required to maintain a large amount of individual Security Associations that could have been avoided if a separate control channel was used for the purpose or if all RSVP sessions would be able to share the phase 1 and SMPLS SA information. More importantly, the use of RSVP-TE to carry IKE messages requires extensions to RSVP in terms of a new RSVP message (see section 3.0). This is because IKE requires several exchanges between both parties, which existing RSVP messages cannot cope with.

Hence the use of IKE over UDP/IP as a proxy to establish Security Associations for MPLS appears to be a logical approach. This approach also allows reusing most part of the existing ISAKMP/IKE code base and allows to implement Secure MPLS with few modifications

to IPSec DOI (thereby specified as the new SMPLS DOI). However, a separate IP control channel is required between edge LSRs to carry IKE messages.

The exact definitions for the SMPLS DOI, largely derived from the IPsec DOI, are given in [12]. Some of the related SMPLS DOI definitions are presented in section 2.1 and 2.2.

2.1 Security Protocol Identifier

Section 4.4.1 of IPSec DOI [3] defines various IPSec related Protocol Identifier. We suggest including three more definitions. The suggested definition are presented below:

Protocol ID	Value
PROTO_SMPLS_AH	5
PROTO_SMPLS_ESP	6
PROTO_SMPLS_COMP	7

PROTO_SMPLS_AH

The PROTO_SMPLS_AH type specifies the MPLS payload authentication. The default SMPLS-AH transform provides data origin authentication, integrity, protection and replay detection. For export consideration, SMPLS-AH transform must not provide any payload confidentiality.

PROTO_SMPLS_ESP

The PROTO_SMPLS_ESP type specifies the MPLS payload confidentiality (encryption). Authentication if required must be provided as part of the ESP. The default SMPLS-ESP transform provides data origin authentication, integrity, protection and replay detection.

PROTO_SMPLS_COMP

The PROTO_SMPLS_COMP type specifies MPLS payload compression. The exact algorithms for MPLS payload encryption are under study. Use of payload compression may have at least two direct benefits. Firstly, it eliminates redundancies in the payload data and reduces repetitive patterns in the payload. Secondly it conserve bandwidth on the network by reducing the payload size. The time spent in compressing the payload and time gained in encrypting the reduced payload may increase the total throughput.

2.2 Identification Types

Identification payload in the ISAKMP message helps responder to identify the appropriate LSP and apply correct security policies. In IPSec this is defined as end station address and a port number. In MPLS there may be large number of LSP between two edge LSR. The LSP may not necessarily carry IP payloads. In order to distinguish between different LSP between two given LSR, a unique Tunnel ID is

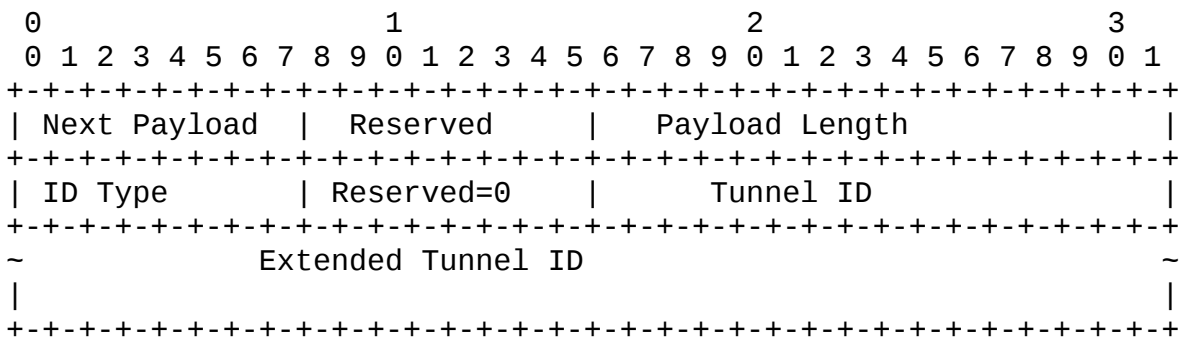
assigned to the LSP [4]. Also [4] suggest to use the extended Tunnel ID to further narrow the scope of the LSP. It is suggested in [4] that the extended Tunnel ID is set to the ingress node IP address. Here we propose to use {Ingress Node Address::Tunnel ID} as the node identifier. This may also be considered as {Extended Tunnel ID::Tunnel ID}. If Extended Tunnel ID is used as part of the ISAKMP identification, it is important that RSVP-TE [4] implementation always use unique values for Extended Tunnel ID.

ID Type	value
ID_SMPLS_IPV4	12
ID_SMPLS_IPV6	13

The values presented above are only suggestions. Exact values need approval from IANA. Section 4.6.2.1 of IPsec DOI [3] explains the definition of other ID Types.

2.2.1 Identification Payload

Here we present the format of the identification data payload that will be carried in ISAKMP identification messages for IPSec DOI.



Next Payload

Type of the next payload after this. Value of zero (0) indicates that this is the last payload.

Reserved

All reserved fields are set to zero on transmission and ignored on receipt.

Payload Length

Length of the payload in octets, including the generic header.

ID Type

Value describing the Identification data. For Secure MPLS, this is either ID_SMPLS_IPV4 or ID_SMPLS_IPV6.

Tunnel ID

A unique number assigned for this LSP by the ingress node.

Extended Tunnel ID

The extended Tunnel ID or the Ingress node ID. The length of this field depend on the ID type is ID_SMPLS_IPV4 or ID_SMPLS_IPv6.

NOTE:

Here ID_SMPLS_IPV4 or ID_SMPLS_IPV6 only represent the end point addressing.

Other DOI definitions

All other definitions are the same as IPSec DOI [3] definitions.

3.0 Use of RSVP-TE to transport IKE messages

Constrained driven LSPs are setup using either CR-LDP or RSVP-TE. Most often there is a separate CR-LDP or RSVP-TE session per LSP. These LSP signaling sessions can be used to transport other messages. In this section we present use of RSVP-TE to exchange required IKE messages between edge LSRs. The reuse of the RSVP-TE channel to exchange IKE messages avoids the need of a separate IP control channel for this purpose, thus creating a cleaner design with a single control channel. However, RSVP-TE sessions are closely tied to the LSP. The Phase 1 security associations established for one LSP may not be reused for another LSP. As a result, end LSRs may require maintaining multiple Phase 1 security associations. More importantly, as already mentionned in section 2.0 above, IKE requires several peer-to-peer exchanges between both LSRÆs, which RSVP-TE does not provide for. Hence, the use of RSVP-TE to carry IKE messages requires extensions to RSVP in terms of a new RSVP message (see below).

We propose to define a new RSVP-TE object to carry IKE messages. The new object is called Secure_MPLS_message Object. IKE messages are exchanged end-to-end. RSVP messages are exchanged hop by hop. Hence all transit nodes MUST pass the Secure_MPLS_message Object unmodified to the downstream node.

Object Name	Applicable RSVP messages
Secure_MPLS_Message	Transport (see below)

3.0.1 RSVP Transport Message

IKE messages are sent from end-to-end. Intermediate nodes MUST forward the message downstream without modifications. In this regard, RSVP is functioning as a transport protocol for IKE. More established RSVP messages such as Path Message require hop-by-hop processing and are sent with the route alert option in the IP

header. This in turn triggers hop by hop processing. As mentioned earlier, when transporting RSVP messages, only the end nodes are required to process the message. On the other hand RSVP transport messages should not be subject to the RSVP state machine. Hence, we propose to define a new RSVP message type to provide end-to-end message transport ability for RSVP. The payload of the RSVP Transport message can be any of the RSVP objects such as Secure_MPLS_Message Object. Processing of Transport message payloads is considered a local policy. Hence, applications that require transport service from the RSVP MUST register the application with the RSVP module.

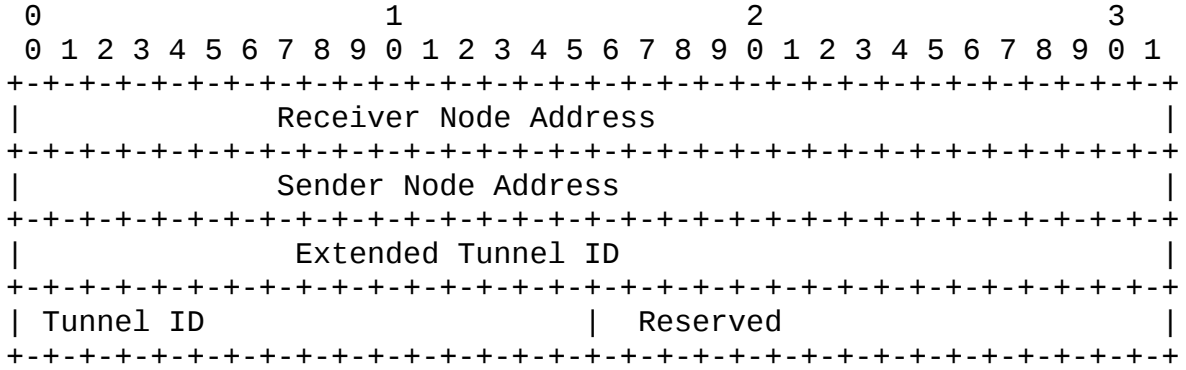
RSVP Message Type	Value
Transport	8

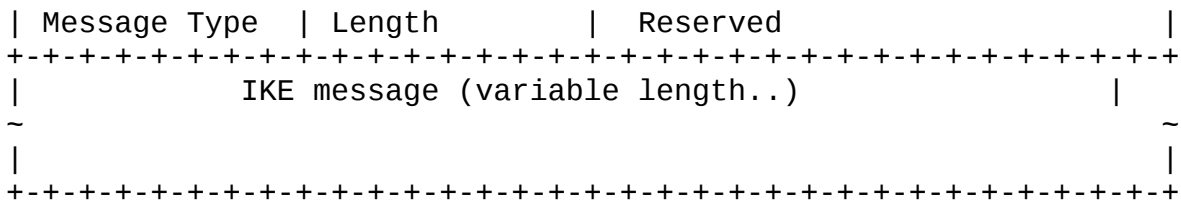
Message types 1 to 7 are defined in [7]. RSVP Transport message MUST NOT be encoded with route alert option.

3.1 Secure_MPLS_Message Object

The Secure MPLS Message object is assigned with Class value of 25 (TBD). Presently, there are two C_Types. C_Type 1 indicates that this is an IKE message with Extended tunnel ID in IP V4 format. C_Type 2 indicates that this is an IKE message with extended tunnel ID in IP V6 format. All other C_Type values are unused.

Class=25, C_Type=1





Receiver Node Address

Receiver IP V4 Address

Sender Node Address

Sender IP V4 Address

Extended Tunnel ID

Extended Tunnel ID in IP V4 format

Tunnel ID

Unique number assigned to this LSP. See [4] for details.

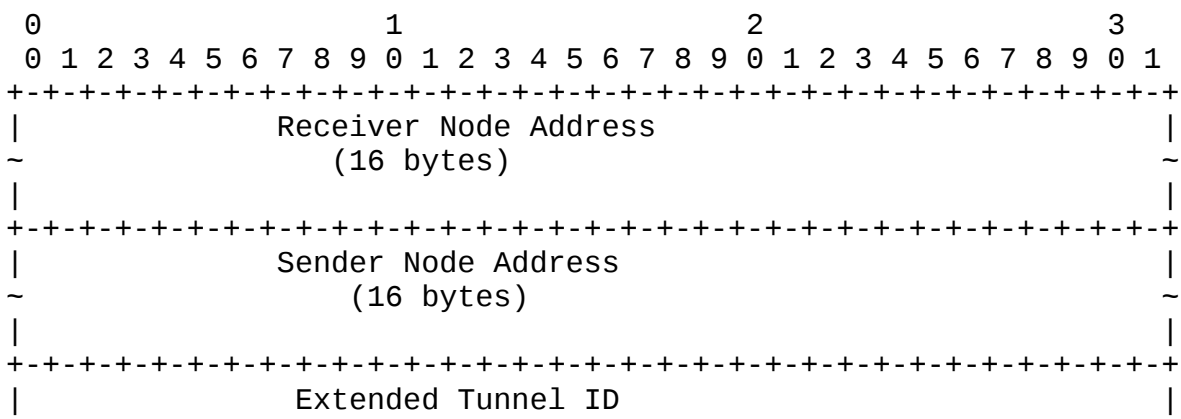
Message Type

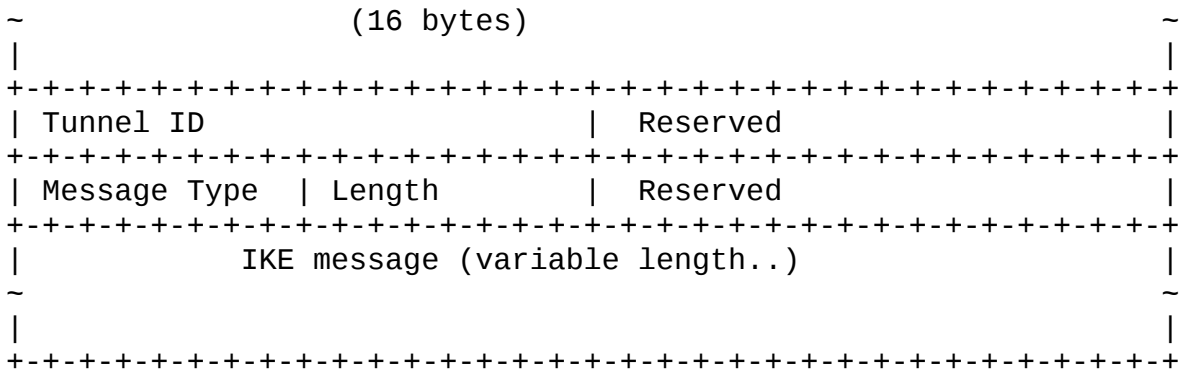
Indicates the type of the payload. Message type 1 is assigned to indicate that payload is ISAKMP. All other values are presently reserved.

Length

Length of the IKE message in octets. Value zero (0) indicates that there is no message in the payload.

Class=25, C_Type=2





Receiver Node Address

Receiver IP V6 Address

Sender Node Address

Sender IP V6 Address

Extended Tunnel ID

Extended Tunnel ID in IP V6 format

Tunnel ID

Unique number assigned to this LSP. See [4] for details.

Message Type

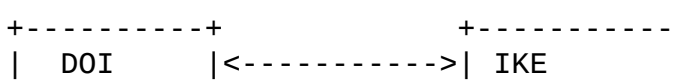
Indicates the type of the payload. Message type 1 is assigned to indicate that payload is IKE. All other values are presently reserved.

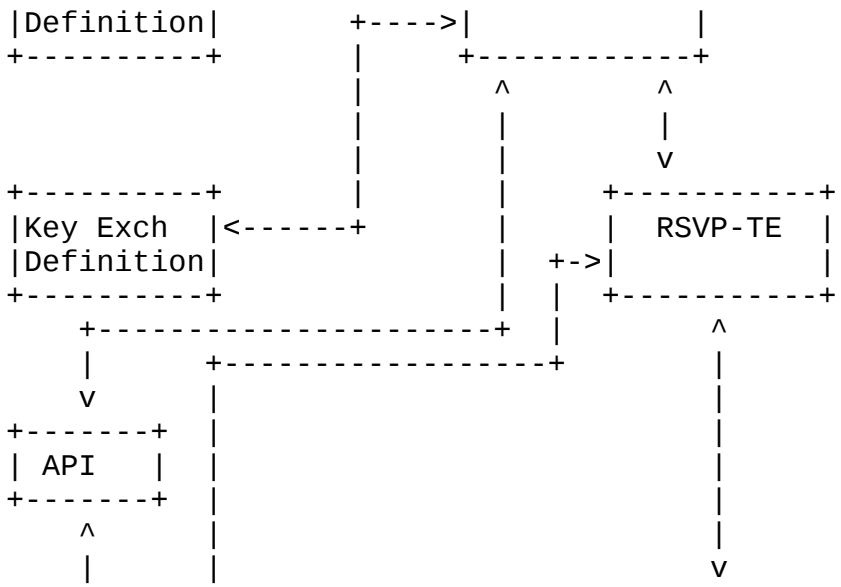
Length

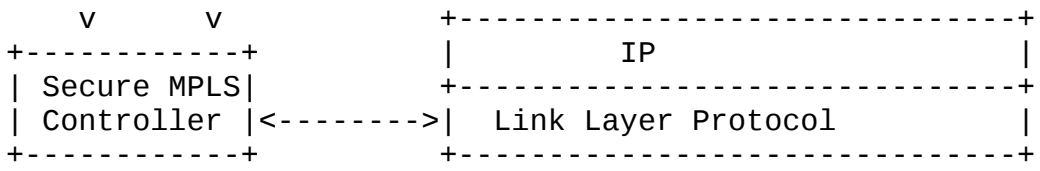
Length of the IKE message in octets. Value zero (0) indicates that there is no message in the payload.

4.0 Placement of Secure MPLS, IKE and RSVP-TE

IKE by design is not tied to a specific transport protocol. IKE security associations are unidirectional in nature. MPLS LSPs are unidirectional in nature as well. Hence, Secure MPLS concepts and IKE complement, without any changes to the original concepts.







4.1 IKE messages and Secure MPLS DOI

IKE messages carried in RSVP-TE payloads are defined for Secure MPLS DOI. In order for IKE to properly handle Secure MPLS messages, it is important that Secure MPLS defines its own DOI. It is suggested that a specific value for Domain Identifier for Secure MPLS DOI be requested from IANA.

Within the Secure MPLS DOI, the required parameters are defined. At present most of the definitions are in line with the IPSec DOI [3] with few exceptions. A separate document for the Secure MPLS DOI has been produced [6].

4.2 Handling of Security Associations

Although Phase 2 SA's (ie. SMPLS SA's) created with IKE are unidirectional, a Phase 2 negotiation actually sets up two separate such SA's: one for each direction. As an example, consider LSR A requiring to setup a secure LSP to LSR B. Once LSR A has set up a SMPLS SA with LSR B (to be used for protecting A->B traffic), also a complementary SMPLS SA exists that can be used to protect the B->A traffic. If LSR B needs to set up a secure LSP towards LSR A, it can possibly directly use the conforming SMPLS SA mentioned above to secure MPLS data traffic from B->A.

If both LSR's initiate a phase 2 negotiation in parallel, they will end up with a total of 4 SMPLS SA's (two in each direction). Several principles can be applied to determine which SA to actually use in each direction, such as for example keeping the SA which was

initiated by LSR A for A->B traffic and the SA which was initiated by LSR B for B->A traffic.

5.0 Secure MPLS payload encapsulation

Secure MPLS payload encapsulation, in addition to providing authentication and confidentiality, provides a variety of security services such as replay protection, protection against connection hijacking etc. The IPSec community has performed extensive work in this area. In this paper we adapt the concepts used in IPSec to provide authentication and encryption services to MPLS payloads.

Borrowing from the model and the names used in the IPSec community, we define two headers as SMPLS-AH and SMPLS-ESP.

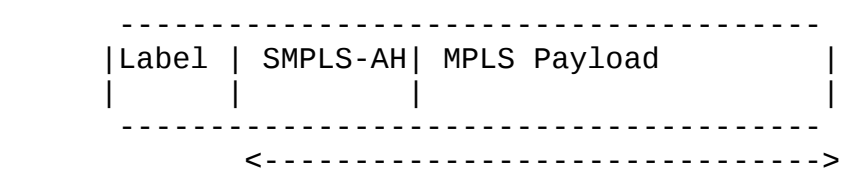
We propose to use SHIM encapsulation method for SMPLS-AH and SMPLS-ESP.

SMPLS-AH, if present, MUST be immediately after the Label Stack sequence.

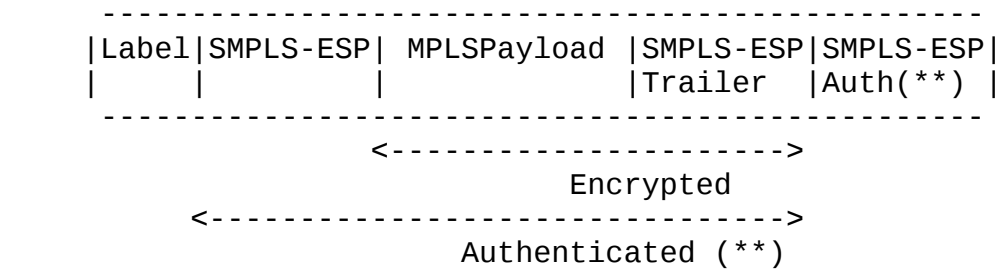
SMPLS-ESP, if present, MUST be immediately after the Label Stack sequence if SMPLS-AH is not present. If SMPLS-AH is present, SMPLS-ESP MUST be immediately after the SMPLS-AH.

5.1 Possible SMPLS encapsulation formats

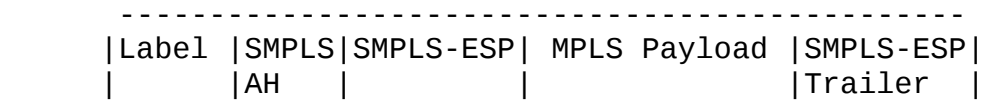
1. SMPLS-AH

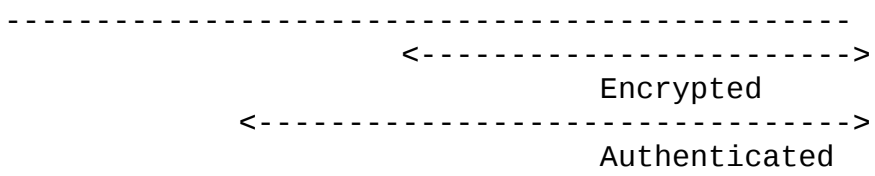


2. SMPLS-ESP



3. SMPLS-AH-ESP





(**) Indicates optional fields

Label - one or more MPLS label

Note: Above diagrams are not to scale.

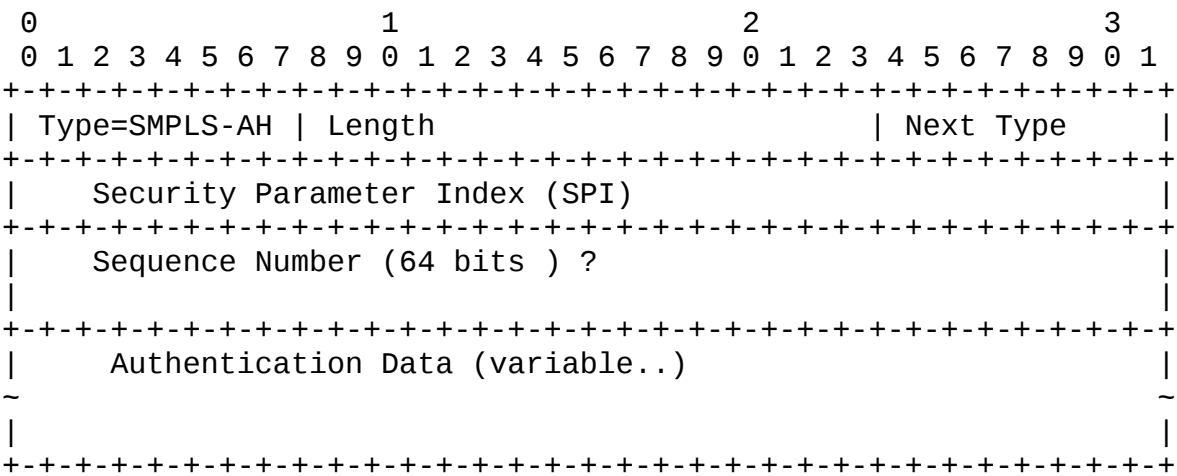
Above encapsulation formats are presented to cover all possible combinations. However, one may implement authentication using ESP with NULL encryption as presented in RFC 2410 [8]. When requiring authentication and encryption one may choose to use format in above 2 with SMPLS-ESP authentication. Hence, it may be possible to cover all cases with a single SMPLS-ESP encapsulation format. However, use of null encryption with ESP for authentication, instead of SMPLS-AH is open for discussion and suggestions.

5.2 SMPLS Encapsulation header types

There are two SMPLS encapsulations defined.

Type	Value
Last Header	0
SMPLS-AH	1
SMPLS-ESP	2
unused	3-255

5.2.1 SMPLS Authentication Header SMPLS-AH



Type

Type of this header. It is set to one (1) to indicate that it is SMPLS-AH.

Length

Length including Type/Length field in octets.

Next Type

Type of the next header. This is either 2 to indicate that the next header is SMPLS-ESP or 0 to indicate that MPLS payload follows immediately.

Security Parameter Index (SPI)

The SPI is an arbitrary 32-bit integer. SPI combined with {Extended Tunnel ID::Tunnel ID} uniquely identify the security association for this datagram. All other interpretation of the SPI including the range of values is as defined in [9].

Sequence Number

This unsigned 64-bit field contains a monotonically increasing counter value (sequence number). It is mandatory and is always present even if the receiver does not elect to enable the anti-replay service for a specific SA. Processing of the Sequence Number field is at the discretion of the receiver, i.e., the sender MUST always transmit this field, but the receiver need not act upon it (see the discussion of Sequence Number Verification in the "Inbound Packet Processing" section below).

The sender's counter and the receiver's counter are initialized to 0 when a SA is established. (The first packet sent using a given SA will have a Sequence Number of 1; see Section 3.3.2 of [9] for more details on how the Sequence Number is generated.) If anti-replay is enabled (the default), the transmitted Sequence Number must never be allowed to cycle. Thus, the sender's counter and the receiver's counter MUST be reset (by establishing a new SA and thus a new key) prior to the transmission of the 2^64th packet on a SA.

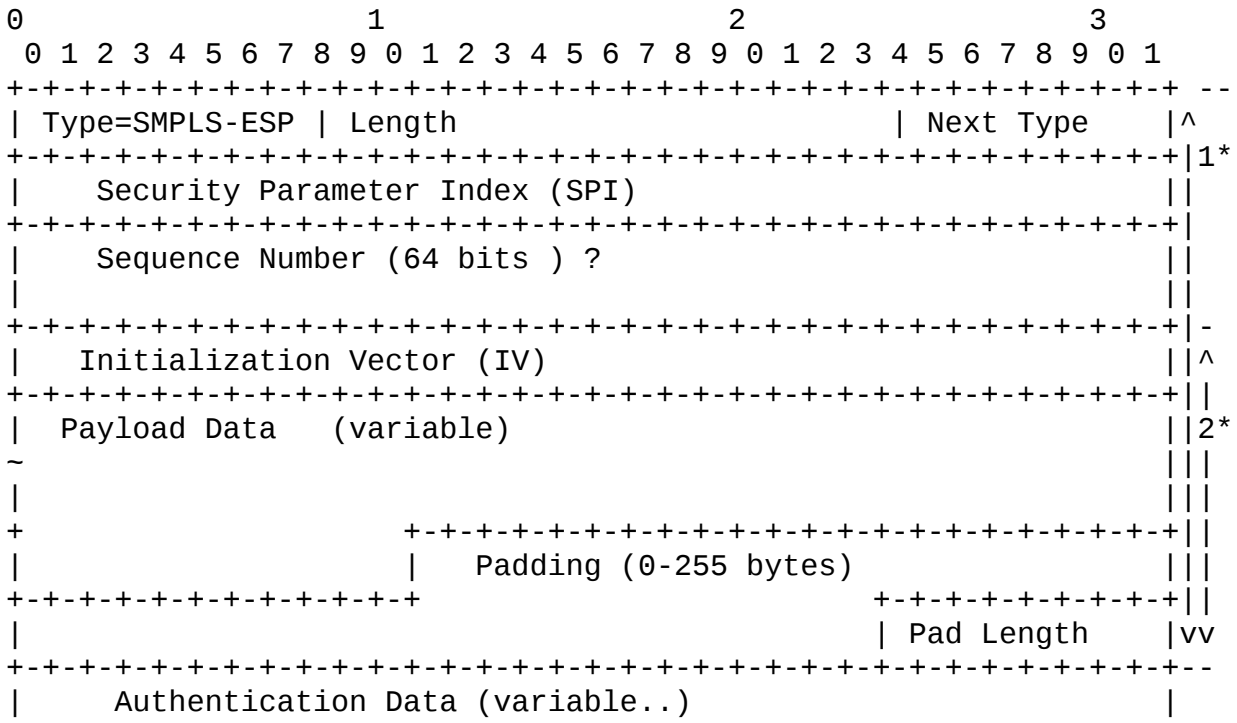
In this paper we have chosen a 64-bit sequence number as opposed to 32-bit number in [9]. It is anticipated that more and more 10Gig pipes using MPLS. In such situation traffic may be aggregated to a single MPLS LSP and 32-bit counter may not be adequate.

Authentication Data

This is a variable length field and contains the Integrity Check Value (ICV) for this packet. The Authentication Data field is a multiple of 32 bits and determined by the ICV computation method.

See [9] for details of the authentication field.

5.2.2 SMPLS Encapsulating Security Payload (SMPLS-ESP)



1* - represents Authentication coverage
2* - represents Confidentiality coverage. NOTE: IV is not encrypted, though considered as part of crypto text.

Type

Type of this header. It is set to two (2) to indicate that it is SMPLS-ESP

Length

Length including Type/Length field in octets.

Next Type

Type of the next header. This is always set to zero (0) for SMPLS-ESP header.

Security Parameter Index (SPI)

The SPI is an arbitrary 32-bit integer. SPI, combined with Extended Tunnel ID::Tunnel ID, uniquely identify the security association for this datagram. All other interpretation of the SPI including the

range of values is as defined in [10].

Sequence Number

See section 5.2.1 on sequence number field above for further explanations on this field.

Payload Data and Initialization Vector

See section 2.3 of [10] for a detailed discussion of these fields.

Padding

See section 2.4 of [10] for a detailed discussion of this field.

Pad Length

See section 2.5 of [10] for a detailed discussion of this field.

Authentication Data

This is a variable length field and contains the Integrity Check Value (ICV) for this packet. The Authentication Data field is a multiple of 32 bits and determined by the ICV computation method. See [10] for details of the authentication field.

Note:

In ESP [10] the Next Header field contains the protocol ID of the IP payload. This was necessary in [10] as the original IP header was replaced with AH/ESP header. However, in MPLS, unmodified IP header is contained in the payload or the payload is non-IP. Hence, in Secure MPLS such explicit denotation of the payload protocol ID is not required.

5.3 Outbound Packet Processing

In Secure MPLS, the sender encapsulates the MPLS payload in the suggested formats above (SMPLS-AH or SMPLS-ESP). The sender is also required to construct the SMPLS-ESP or SMPLS-AH header as specified in this document and dictated by the Security Association associated to the MPLS packet.

5.3.1 Security Association Lookup

SMPLS-ESP or SMPLS_AH is applied to an outbound packet only after the MPLS implementation determines that the packet is associated with a SA that calls SMPLS-ESP or SMPLS-AH processing respectively. The SMPLS requirement may be derived by FEC (Forward Equivalence Class) lookup. The exact procedure is beyond the scope of this document. However, if enough interest is generated, a separate document may be created for the purpose.

5.3.2 Integrity Check Value Calculation in SMPLS-AH

The calculation of ICV for MPLS payload is quite similar to the calculation of ICV of IP packets in section 3.3.3 of [9], except that the SMPLS-AH authentication procedure only covers the SMPLS-AH and the data payloads. The MPLS header labels stack is inherently mutable and is therefore not covered. This simplifies some of the overheads in IPSec encapsulations.

See section 3.3.3 of [9] for detail procedure in ICV calculation and sequence number generation.

5.3.3 Integrity Check Value Calculation in SMPLS-ESP

The Integrity Check Value (ICV) for SMPLS-ESP is optional. The security association lookup specifies a given SMPLS-ESP Security Association contain an ICV. If required ICV for SMPLS-ESP is calculated using methods specified in [10].

5.3.4 MPLS Payload Encryption in SMPLS-ESP

In case SMPLS-ESP must be applied to the MPLS payload, the encryption of MPLS payload is quite similar to the encryption procedure of IP packets in [10], except that SMPLS-ESP makes no attempt to identify the payload protocol type.

See section 3.3.2 of [10] for a detailed procedure in encryption and sequence number generation.

5.4 Inbound Packet Processing

Inbound packet processing follows through the following steps

- Perform Label Lookup
- Security Association Lookup
- Sequence Number Verification
- Integrity Check Value Verification
- Payload decryption (Only required for SMPLS-ESP)

Label Lookup

Egress LSR performs a label lookup on the incoming packet. If that indicates this router is the Egress LSR and the associated LSP is carrying Secure MPLS data, Secure MPLS module is invoked.

Security Association Lookup

Security Association Lookup is performed within the Secure MPLS module. The incoming Label provides a mapping to the {Extended Tunnel ID::Tunnel ID} tuple. The combination of this identifier with Security Parameter Index (SPI) and Header Type (SMPLS-ESP or SMPLS-AH) determines a unique Security Association (SA). Note that Header Type (SMPLS-ESP or SMPLS-AH) combined with the same LSP ID and numerically similar SPI is required to generate a different Security Association. Hence, the Header Type field (SMPLS-ESP or SMPLS-AH) is considered in resolving the SA.

If there is no SA present for this flow, the packet MUST be discarded. As specified in [9] and [10] the event may be audited. In addition to the information required in [9] and [10], log event SHOULD contain the SMPLS-ESP as the flow type. Instead of the end station IP address it SHOULD display the Extended Tunnel ID:: Tunnel ID tuple.

Sequence Number verification

Sequence number verification is performed using methods specified in [9] and [10] for SMPLS-AH and SMPLS-ESP respectively.

Integrity Check Value Verification

For SMPLS-ESP, the ICV (if authentication is provided in SMPLS-ESP) is verified using the methods specified in section 3.4.4 of [10].

For SMPLS-AH, the ICV is verified using the methods specified in section 3.4.4 of [9]. The only difference is that the ICV is calculated and verified over the SMPLS-AH and data payloads. The

MPLS label stack header is mutable and is therefore not considered for the ICV calculation/verification.

MPLS Payload Decryption in SMPLS-ESP

Packet decryption procedure is similar to [10]. However, in secure MPLS there are no attempts made to reconstruct the IP header (if IP traffic is being carried). During the setup time it is indicated that the corresponding LSP is either IP or Layer 2 packet. Accordingly, decrypted payload is handed over to the appropriate forwarding module.

6.0 Other Issues

6.1 Path MTU discovery

As MPLS payloads are encrypted, intermediate LSRs are unable to perform fragmentation upon MTU size violations. Hence it is essential that the ingress LSR performs path MTU discovery and performs necessary fragmentation before encapsulation. There are several documents published on this. MTU path discovery in Layer 2

MPLS tunnels are presented in [11]. We suggest taking a similar approach in discovering path MTU size for Secure MPLS LSP.

6.2 LSP Setup Requirements

Secure MPLS paths require different handling. Hence the LSP signaling protocol MUST carry indication to the effect that this LSP is secure MPLS. At present, either CR-LDP or RSVP-TE is used to setup constrained LSP.

In RSVP-TE we propose to define a new flag in Session Attribute object. The new flag is called Secure MPLS. All intermediate nodes MUST pass this flag downstream.

Flag

0x08 Secure MPLS
: This flag indicates that this LSP is carrying encrypted payload and no attempt be made to interpret payload data, except by the end routers. All intermediate nodes must pass this parameter to the downstream routers.

See [4] for details on the format of the Session Attribute object.

6.3 Intermediate LSR

Intermediate LSRs MUST not attempt to interpret data. Upon errors, an intermediate LSR SHOULD silently discard the packets. If RSVP-TE is used to transport IKE messages, they should transparently forward such messages to the downstream node.

6.4 Label merging

Secure MPLS presented in this document is a derivative of IKE. As such it can only establish security association with point-to-point LSP. Label merged LSP may be considered as a multi-point-to-point LSP. In such situations concepts presented in secure multicast documents may be used. Security implementation in Label merge LSP is considered beyond the scope of this document.

6.5 Penultimate Hop popping

As explained above, incoming Label and subsequently {Extended Tunnel ID::Tunnel ID} is used to perform Security Parameter Database lookup. Penultimate hop popping eliminate the ability of such lookup and MUST not be performed in secure MPLS LSP.

7.0 Security Considerations

The methods presented in this document are not known to alter the security level of ISAKMP or IKE. The Secure MPLS architecture presented here improves the level of security offered in MPLS

implementation.

8.0 Acknowledgment

The work presented in this document has been influenced significantly by the work presented in sited references and on going work at the IETF. Olivier Paradence of Alcatel provided valuable comments and suggestions.

9.0 References

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

2 Harkins, D., and et.al., Internet Key Exchange (IKE), RFC 2409, November 1998.

3 Piper, D., The Internet IP Security Domain of Interpretation for ISAKMP, RFC 2407, November 1998.

4 Awduche, D., and et. al., RSVP-TE: Extensions to RSVP for LSP Tunnels, Work in Progress, August 2000.

5 Jamoussi, Bilel., and et. al., Constrained-Based LSP setup using LDP, Work in Progress, July 2000.

6 Senevirathn, T., and Paridaens, O., Secure MPLS Domain of Interpretation for ISAKMP, Work In Progress, January 2001.

7 Braden, R., and et.al., Resource ReSerVation Protocol (RSVP), RFC 2205, September 1997.

8 Glenn, R., and Kent, S., The NULL Encryption Algorithm and Its Use with IPSec, RFC 2410, November 1998.

9 Kent, S., and Atkinson R, IP Authentication Header, RFC 2402, November 2000.

10 Kent, S. and Atkinson, R., IP Encapsulating Security Payload (ESP), RFC 2406, November 1998.

11 Senevirathne, T., and Billinghurst, P., Use of CR-LDP or RSVP-TE to Extend 802.1Q Virtual LANs across MPLS Networks, Work In Progress, October 2000.

10.0 Author's Addresses

Tissa Senevirathne
1567 Bellevile Way,
Sunnyvale CA 94087

Email:tsenevir@hotmail.com
Tel:408-245-5897

Full Copyright Statement