Network Working Group
Request for Comments: 4595
Category: Informational

F. Maino
Cisco Systems
D. Black
EMC Corporation

July 2006

# Use of IKEv2 in the Fibre Channel Security Association Management Protocol

## Status of This Memo



## Copyright Notice



## Abstract

This document describes the use of IKEv2 to negotiate security protocols and transforms for Fibre Channel as part of the Fibre Channel Security Association Management Protocol. This usage requires that IKEv2 be extended with Fibre-Channel-specific security protocols, transforms, and name types. This document specifies these IKEv2 extensions and allocates identifiers for them. Using new IKEv2 identifiers for Fibre Channel security protocols avoids any possible confusion between IKEv2 negotiation for IP networks and IKEv2 negotiation for Fibre Channel.

Table of Contents

## 1. Introduction

Fibre Channel (FC) is a gigabit-speed network technology primarily used for Storage Networking. Fibre Channel is standardized in the T11 [T11] Technical Committee of the InterNational Committee for Information Technology Standards (INCITS), an American National Standard Institute (ANSI) accredited standards committee.

FC-SP (Fibre Channel Security Protocols) is a T11 Technical Committee working group that has developed the "Fibre Channel Security Protocols" standard [FC-SP], a security architecture for Fibre Channel networks.

The FC-SP standard defines a set of protocols for Fibre Channel networks that provides:

1. device-to-device (hosts, disks, switches) authentication;

2. management and establishment of secrets and security associations;

3. data origin authentication, integrity, anti-replay protection, confidentiality; and

4. security policies distribution.

Within this framework, a Fibre Channel device can verify the identity of another Fibre Channel device and establish a shared secret that will be used to negotiate security associations for security protocols applied to Fibre Channel frames and information units. The same framework allows for distributions within a Fibre Channel fabric of policies that will be enforced by the fabric.

FC-SP has adapted the IKEv2 protocol [RFC4306] to provide authentication of Fibre Channel entities and setup of security associations.

### 1.1. Requirements Notation

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].

## 2. Overview

Fibre Channel defines two security protocols that provide security services for different portions of Fibre Channel traffic: the ESP_Header defined in [FC-FS] and CT_Authentication defined in [FC-GS-4].

The ESP_Header protocol is a transform applied to FC-2 Fibre Channel frames. It is based on the IP Encapsulation Security Payload [RFC4303] to provide origin authentication, integrity, anti-replay protection, and optional confidentiality to generic fibre channel frames. The CT_Authentication protocol is a transform that provides the same set of security services for Common Transport Information Units, which are used to convey control information. As a result of the separation of Fibre Channel data traffic from control traffic, only one protocol (either ESP_Header or CT_Authentication) is applicable to any FC Security Association (SA).

Security associations for the ESP_Header and CT_Authentication protocols between two Fibre Channel entities (hosts, disks, or switches) are negotiated by the Fibre Channel Security Association Management Protocol, a generic protocol based on IKEv2 [RFC4306].

Since IP is transported over Fibre Channel [RFC4338] and Fibre Channel/SCSI are transported over IP [RFC3643], [RFC3821] there is the potential for confusion when IKEv2 is used for both IP and FC traffic. This document specifies identifiers for IKEv2 over FC in a fashion that ensures that any mistaken usage of IKEv2/FC over IP will result in a negotiation failure due to the absence of an acceptable proposal (and likewise for IKEv2/IP over FC). This document gives an overview of the security architecture defined by the FC-SP standard, including the security protocols used to protect frames and to negotiate SAs, and it specifies the entities for which new identifiers have been assigned.

## 3. Fibre Channel Security Protocols

The Fibre Channel protocol is described in [FC-FS] as a network architecture organized in 5 levels. The FC-2 level defines the FC frame format (shown in Figure 1), the transport services, and control functions required for information transfer.

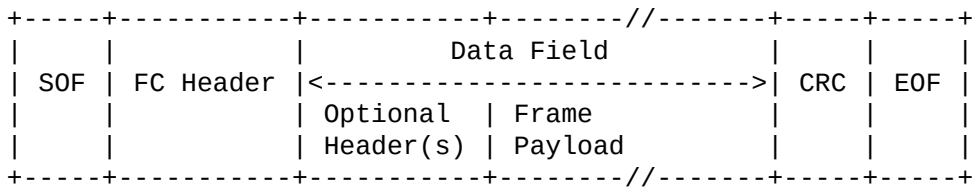


Figure 1: Fibre Channel Frame Format

Fibre Channel Generic Services share a Common Transport (CT) at the FC-4 level defined in [FC-GS-4]. The CT provides access to a Service (e.g., Directory Service) with a set of service parameters that facilitates the usage of Fibre Channel constructs.

A Common Transport Information Unit (CT_IU) is the common Fibre Channel Sequence used to transfer all information between a Client and a Server. The first part of the CT_IU, shown in Figure 2, contains a preamble with information common to all CT_IUs. An optional Extended CT_IU Preamble carries the CT_Authentication protocol that provides authentication and, optionally, confidentiality to CT_IUs. The CT_IU is completed by an optional Vendor-Specific Preamble and by additional information as defined by the preamble.

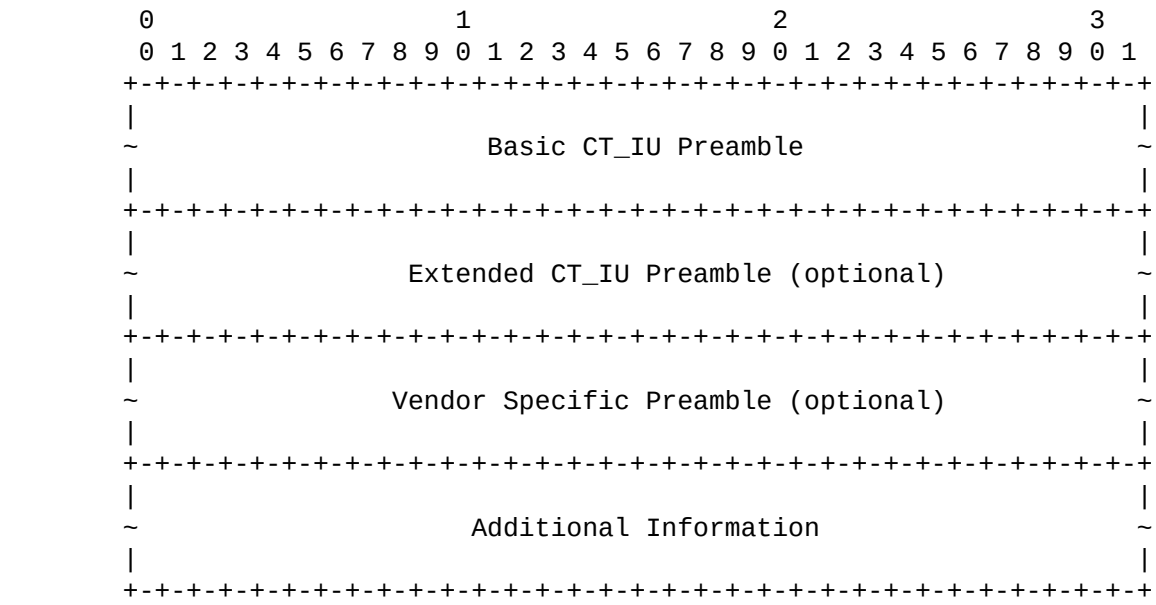


Figure 2: CT_IU

Two security protocols are defined for Fibre Channel: the ESP_Header protocol that protects the FC-2 level, and the CT_Authentication protocol that protects the Common Transport at the FC-4 level.

Security Associations for the ESP_Header and CT_Authentication protocols are negotiated by the Fibre Channel Security Association Management Protocol.

## 3.1. ESP_Header Protocol

ESP_Header is a security protocol for FC-2 Fibre Channel frames that provides origin authentication, integrity, anti-replay protection, and confidentiality. ESP_Header is carried as the first optional header in the FC-2 frame, and its presence is signaled by a flag in the DF_CTL field of the FC-2 header.

Figure 3 shows the format of an FC-2 frame encapsulated with an ESP_Header. The encapsulation format is equivalent to the IP Encapsulating Security Payload [RFC4303], but the scope of the authentication covers the entire FC-2 header. The Destination and Source Fibre Channel addresses (D_ID and S_ID) and the CS_CTL/ Priority field are normalized before computation of the Integrity Check value to allow for address translation.

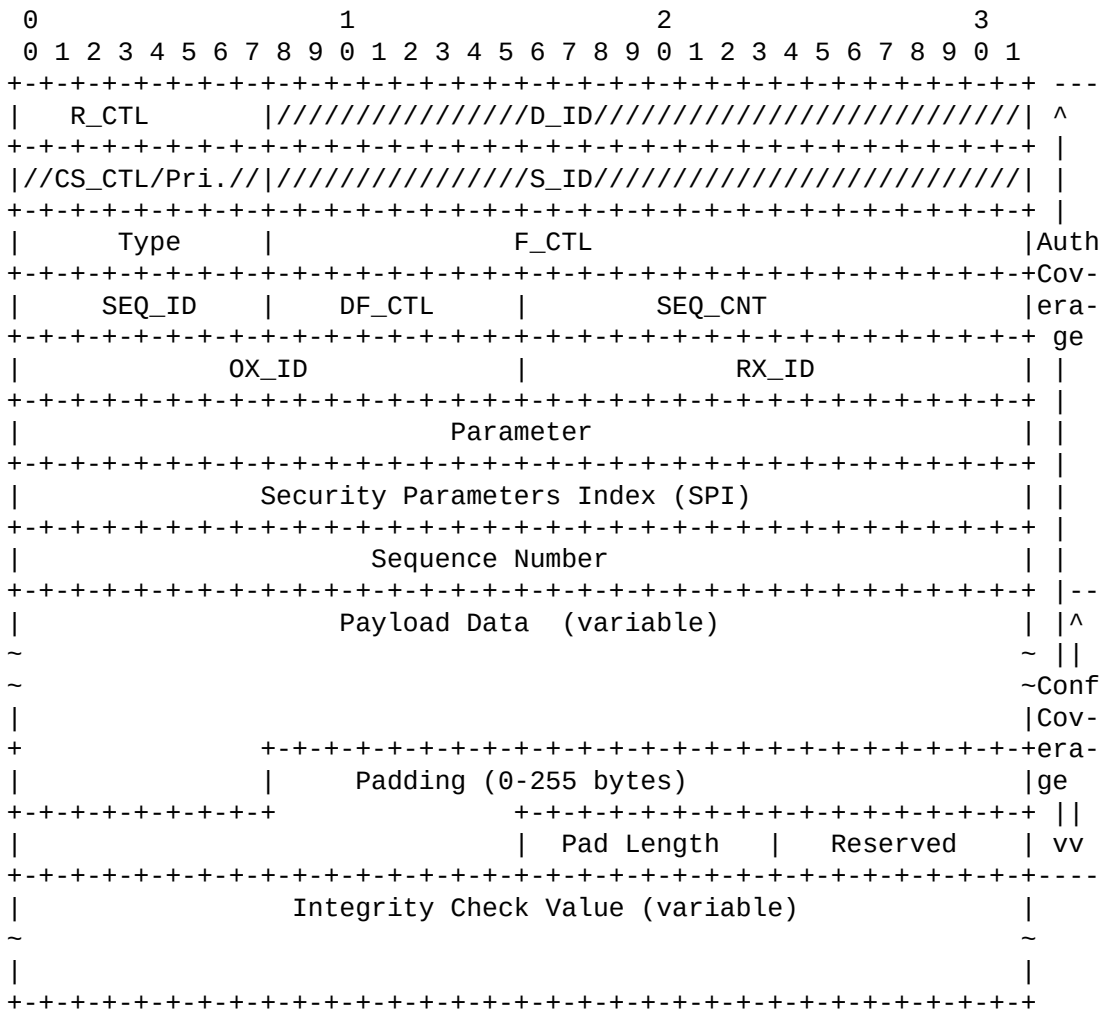


Figure 3: ESP_Header Encapsulation

All the security transforms that are defined for the IP Encapsulating Security Payload, such as AES-CBC [RFC3602], can be applied to the ESP_Header protocol.

## 3.2. CT_Authentication Protocol

CT_Authentication is a security protocol for Common Transport FC-4 Information Units that provides origin authentication, integrity, and anti-replay protection. The CT_Authentication protocol is carried in the optional extended CT_IU preamble

The extended CT_IU preamble, shown in Figure 4, includes an Authentication Security Association Identifier (SAID), a transaction ID, the N_port name of the requesting node, a Time Stamp used to prevent replay attacks, and an Authentication Hash Block.

The scope of the Authentication Hash Block Covers all data words of the CT_IU, with the exception of the frame_header, the IN_ID field in the basic CT_IU preamble, the Authentication Hash Block itself, and the frame CRC field.

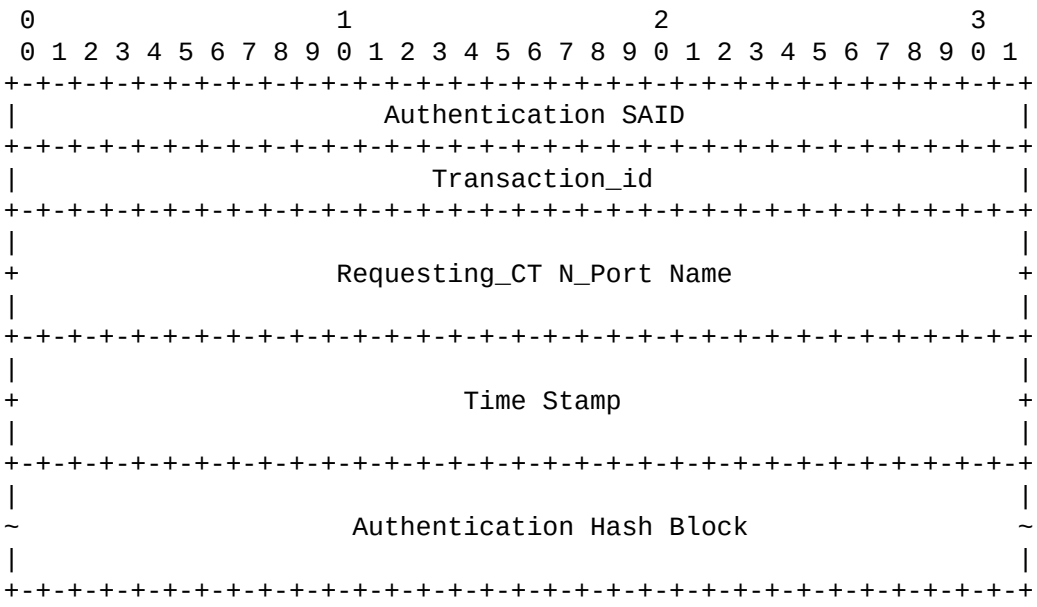


Figure 4: Extended CT_IU Preamble

The Authentication Hash Block is computed as an HMAC keyed hash of the CT_IU, as defined in [RFC2104]. The entire output of the HMAC computation is included in the Authentication Hash Block, without any truncation. Two transforms are defined: HMAC-SHA1-160 that is based on the cryptographic hash function SHA1 [NIST.180-1.1995], and HMAC-MD5-128 that is based on the cryptographic hash function MD5 [RFC1321].

## 4. The FC SA Management Protocol

Fibre Channel entities negotiate security associations for the protocols described above by using the Fibre Channel Security Association Management protocol, as defined in [FC-SP]. The protocol is a modified subset of the IKEv2 protocol [RFC4306] that performs the same core operations, and it uses the Fibre Channel AUTH protocol to transport IKEv2 messages.

The protocol supports only the basic features of IKEv2: initial exchange to create an IKE SA and the first child SA, the CREATE_CHILD_SA exchange to negotiate additional SAs, and the INFORMATIONAL exchange, including notification, delete, and vendor ID payloads. IKEv2 features that are not supported for Fibre Channels include: negotiation of multiple protocols within the same proposal, capability to handle multiple outstanding requests, cookies, configuration payload, and the Extended Authentication Protocol (EAP) payload.

The following subsections describe the additional IANA assigned values required by the Fibre Channel Security Association Management protocol, as defined in [FC-SP]. All the values have been allocated from the new registries created for the IKEv2 protocol [RFC4306].

### 4.1. Fibre Channel Name Identifier

Fibre Channels entities that negotiate security associations are identified by an 8-byte Name. Support for this name format has been added to the IKEv2 Identification Payload, introducing a new ID type beyond the ones already defined in Section 3.5 of [RFC4306]. This ID Type MUST be supported by any implementation of the Fibre Channel Security Association Management Protocol.

The FC_Name_Identifier is then defined as a single 8-octet Fibre Channel Name:

| ID Type | Value |
|---|---|
| ID_FC_NAME | 12 |

### 4.2. ESP_Header and CT_Authentication Protocol ID

Security protocols negotiated by IKEv2 are identified by the Protocol ID field contained in the proposal substructure of a Security Association Payload, as defined in Section 3.3.1 of [RFC4306].

The following protocol IDs have been defined to identify the Fibre Channel ESP_Header and the CT_Authentication security protocols:

| Protocol ID | Value |
|---|---|
| FC_ESP_HEADER | 4 |
| FC_CT_AUTHENTICATION | 5 |

The existing IKEv2 value for ESP (3) is deliberately not reused in order to avoid any possibility of confusion between IKEv2 proposals for IP security associations and IKEv2 proposals for FC security associations.

The number and type of transforms that accompany an SA payload are dependent on the protocol in the SA itself. An SA payload proposing the establishment of a Fibre Channel SA has the following mandatory and optional transform types.

| Protocol | Mandatory Types | Optional Types |
|---|---|---|
| FC_ESP_HEADER | Integrity | Encryption, DH Groups |
| FC_CT_AUTHENTICATION | Integrity | Encryption, DH Groups |

## 4.3. CT_Authentication Protocol Transform Identifiers

The CT_Authentication Transform IDs defined for Transform Type 3 (Integrity Algorithm) are:

| Name | Number | Defined in |
|---|---|---|
| AUTH_HMAC_MD5_128 | 6 | FC-SP |
| AUTH_HMAC_SHA1_160 | 7 | FC-SP |

These transforms differ from the corresponding _96 transforms used in IPsec solely in the omission of the truncation of the HMAC output to 96 bits; instead, the entire output (128 bits for MD5, 160 bits for SHA-1) is transmitted. MD5 support is required due to existing usage of MD5 in CT_Authentication; SHA-1 is RECOMMENDED in all new implementations.

## 4.4. Fibre Channel Traffic Selectors

Fibre Channel Traffic Selectors allow peers to identify packet flows for processing by Fibre Channel security services. A new Traffic Selector Type has been added to the IKEv2 Traffic Selector Types Registry defined in Section 3.13.1 of [RFC4306]. This Traffic Selector Type MUST be supported by any implementation of the Fibre Channel Security Association Management Protocol.

Fibre Channel traffic selectors are defined in [FC-SP] as a list of FC address and protocol ranges, as shown in Figure 5.

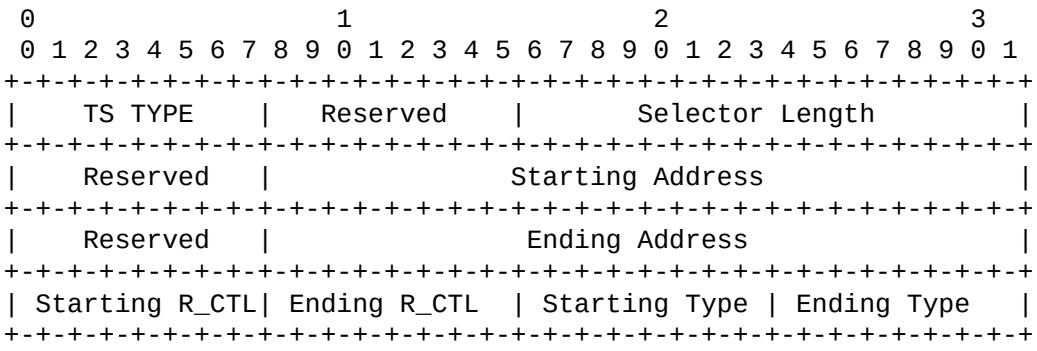


Figure 5: Fibre Channel Traffic Selector

The following table lists the assigned value for the Fibre Channel Traffic Selector Type field:

| TS Type | Value |
|---|---|
| TS_FC_ADDR_RANGE | 9 |

The Starting and Ending Address fields are 24-bit addresses assigned to Fibre Channel names as part of initializing Fibre Channel communications (e.g., for a switched Fibre Channel Fabric, end nodes acquire these identifiers from Fabric Login, FLOGI).

The Starting and Ending R_CTL fields are the 8-bit Routing Control identifiers that define the category and, in some cases, the function of the FC frame; see [FC-FS] for details.

As a result of the separation of Fibre Channel data traffic from control traffic, only one protocol (either ESP_Header or CT_Authentication) is applicable to any FC Security Association. When the Fibre Channel Traffic Selector is defined for the ESP_Header protocol, the Starting Type and Ending Type fields identify the range of FC-2 protocols to be selected. When the Fibre Channel Traffic Selector is defined for the CT_Authentication protocol, the FC-2 Type is implicitly set to the value '20h', which identifies CT_Authentication information units, and the Starting Type and Ending Type fields identify the range of Generic Service subtypes (GS_Subtype) to be selected. See [FC-FS] and [FC-GS-4] for details.

### 4.5. Negotiating Security Associations for FC and IP

The ESP_header and CT_Authentication protocols are Fibre-Channel-specific security protocols that apply to Fibre Channel frames only. The values identifying security protocols, transforms, selectors, and name types defined in this document MUST NOT be used during IKEv2 negotiation for IPsec protocols.

## 5. Security Considerations

The security considerations in IKEv2 [RFC4306] apply, with the exception of those related to NAT traversal, EAP, and IP fragmentation. NAT traversal and EAP, in fact, are not supported by the Fibre Channel Security Association Management Protocol (which is based on IKEv2), and IP fragmentation cannot occur because IP is not used to carry the Fibre Channel Security Association Management Protocol messages.

Fibre Channel Security Association Management Protocol messages are mapped over Fibre Channel Sequences. A Sequence is able to carry up to 4 GB of data; there are no theoretical limitations to the size of IKEv2 messages. However, some Fibre Channel endpoint implementations have limited sequencing capabilities for the particular frames used to map IKEv2 messages over Fibre Channel. To address these limitations, the Fibre Channel Security Association Management Protocol supports fragmentation of IKEv2 messages (see Section 5.9 of [FC-SP]). If the IKEv2 messages are long enough to trigger fragmentation, it is possible that attackers could prevent the IKEv2 exchange from completing by exhausting the reassembly buffers. The chances of this can be minimized by using the Hash and URL encodings instead of sending certificates (see Section 3.6 of [RFC4306]).

## 6. IANA Considerations

The standards action of this document establishes the following values allocated by IANA in the registries created for IKEv2 [RFC4306].

Allocated the following value for the IKEv2 Identification Payload ID Types Registry (Section 3.5 of [RFC4306]):

| ID Type | Value |
|---|---|
| ID_FC_NAME | 12 |

Allocated the following values for the IKEv2 Security Protocol Identifiers Registry (Section 3.3.1 of [RFC4306]):

| Protocol ID | Value |
|---|---|
| FC_ESP_HEADER | 4 |
| FC_CT_AUTHENTICATION | 5 |

Allocated the following values for Transform Type 3 (Integrity Algorithm) for the IKEv2 Integrity Algorithm Transform IDs Registry (Section 3.3.2 of [RFC4306]):

| Name | Number |
|---|---|
| AUTH_HMAC_MD5_128 | 6 |
| AUTH_HMAC_SHA1_160 | 7 |

Allocated the following value for the IKEv2 Traffic Selector Types Registry (Section 3.13.1 of [RFC4306]):

| TS Type | Value |
|---|---|
| TS_FC_ADDR_RANGE | 9 |

# 7. References

## 7.1. Normative References

[NIST.180-1.1995]
National Institute of Standards and Technology, "Secure Hash Standard", NIST 180-1, April 1995.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

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

[RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.

[RFC3643] Weber, R., Rajagopal, M., Travostino, F., O'Donnell, M., Monia, C., and M. Merhar, "Fibre Channel (FC) Frame Encapsulation", RFC 3643, December 2003.

[RFC3821] Rajagopal, M., E. Rodriguez, E., and R. Weber, "Fibre Channel Over TCP/IP (FCIP)", RFC 3602, July 2004.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4338] DeSanti, C., Carlson, C., and R. Nixon, "Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel", RFC 4338, January 2006.

## 7.2. Informative References

[FC-FS] INCITS Technical Committee T11, ANSI INCITS 373-2003, "Fibre Channel - Framing and Signaling (FC-FS)".

[FC-GS-4] INCITS Technical Committee T11, ANSI INCITS 387-2004, "Fibre Channel - Generic Services 4 (FC-GS-4)".

[FC-SP] INCITS Technical Committee T11, ANSI INCITS xxx-200x, "Fibre Channel - Security Protocols (FC-SP)".

[T11] INCITS Technical Commitee T11, "Home Page of the INCITS Technical Committee T11", <http://www.t11.org>.

## Authors' Addresses

Fabio Maino
Cisco Systems
375 East Tasman Drive
San Jose, CA 95134
US

Phone: +1 408 853 7530
EMail: fmaino@cisco.com
URI: http://www.cisco.com/

David L. Black
EMC Corporation
176 South Street
Hopkinton, MA 01748
US

Phone: +1 508 293-7953
EMail: black_david@emc.com
URI: http://www.emc.com/

## Full Copyright Statement



## Intellectual Property



## Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).