

INTERNET-DRAFT

C. DeSanti  
F. Maino  
K. McCloghrie  
Cisco Systems  
11 July 2008

MIB for Fibre-Channel Security Protocols (FC-SP)  
draft-ietf-imss-fc-fcsp-mib-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects for information related to FC-SP, the Security Protocols defined for Fibre Channel.

## Table of Contents

<a href="#">1</a>	<a href="#">Introduction .....</a>	<a href="#">3</a>
<a href="#">2</a>	<a href="#">The Internet-Standard Management Framework .....</a>	<a href="#">3</a>
<a href="#">3</a>	<a href="#">Overview of Fibre Channel .....</a>	<a href="#">4</a>
<a href="#">3.1</a>	<a href="#">Introduction .....</a>	<a href="#">10</a>
<a href="#">3.2</a>	<a href="#">Zoning .....</a>	<a href="#">11</a>
<a href="#">3.3</a>	<a href="#">Virtual Fabrics .....</a>	<a href="#">11</a>
<a href="#">3.4</a>	<a href="#">Security .....</a>	<a href="#">12</a>
<a href="#">3.4.1</a>	<a href="#">Authentication .....</a>	<a href="#">12</a>
<a href="#">3.4.2</a>	<a href="#">Security Associations .....</a>	<a href="#">13</a>
<a href="#">3.4.3</a>	<a href="#">Fabric Security Policies .....</a>	<a href="#">14</a>
<a href="#">3.4.4</a>	<a href="#">Policy Model .....</a>	<a href="#">15</a>
<a href="#">3.4.5</a>	<a href="#">Policy Objects .....</a>	<a href="#">15</a>
<a href="#">3.4.6</a>	<a href="#">Three Kinds of Switches .....</a>	<a href="#">17</a>
<a href="#">3.4.7</a>	<a href="#">Security Policy Management .....</a>	<a href="#">17</a>
<a href="#">3.4.8</a>	<a href="#">FC-SP Zoning .....</a>	<a href="#">18</a>
<a href="#">4</a>	<a href="#">Document Overview .....</a>	<a href="#">19</a>
<a href="#">4.1</a>	<a href="#">Fibre Channel management instance .....</a>	<a href="#">19</a>
<a href="#">4.2</a>	<a href="#">Entity Name .....</a>	<a href="#">19</a>
<a href="#">4.3</a>	<a href="#">Fabric Index .....</a>	<a href="#">20</a>
<a href="#">4.4</a>	<a href="#">Interface Index .....</a>	<a href="#">20</a>
<a href="#">4.5</a>	<a href="#">Syntax for Policy Object Names .....</a>	<a href="#">20</a>
<a href="#">4.6</a>	<a href="#">Certificates, CAs and CRLs .....</a>	<a href="#">21</a>
<a href="#">4.7</a>	<a href="#">Traffic Selectors .....</a>	<a href="#">22</a>
<a href="#">4.8</a>	<a href="#">The MIB Modules .....</a>	<a href="#">22</a>
<a href="#">4.9</a>	<a href="#">Rate Control for Notifications .....</a>	<a href="#">25</a>
<a href="#">5</a>	<a href="#">Relationship to Other MIB Modules .....</a>	<a href="#">26</a>
<a href="#">6</a>	<a href="#">MIB Module Definitions .....</a>	<a href="#">27</a>
<a href="#">6.1</a>	<a href="#">The T11-FC-SP-TC-MIB Module .....</a>	<a href="#">27</a>
<a href="#">6.2</a>	<a href="#">The T11-FC-SP-AUTHENTICATION-MIB Module .....</a>	<a href="#">43</a>
<a href="#">6.3</a>	<a href="#">The T11-FC-SP-ZONING-MIB Module .....</a>	<a href="#">64</a>
<a href="#">6.4</a>	<a href="#">The T11-FC-SP-POLICY-MIB Module .....</a>	<a href="#">77</a>
<a href="#">6.5</a>	<a href="#">The T11-FC-SP-SA-MIB Module .....</a>	<a href="#">176</a>
<a href="#">7</a>	<a href="#">Acknowledgements .....</a>	<a href="#">232</a>
<a href="#">8</a>	<a href="#">Normative References .....</a>	<a href="#">233</a>
<a href="#">9</a>	<a href="#">Informative References .....</a>	<a href="#">235</a>
<a href="#">10</a>	<a href="#">IANA Considerations .....</a>	<a href="#">236</a>
<a href="#">11</a>	<a href="#">Security Considerations .....</a>	<a href="#">237</a>
<a href="#">12</a>	<a href="#">Authors' Addresses .....</a>	<a href="#">245</a>

## 1. Introduction

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects for information concerning the Fibre Channel Security Protocols (FC-SP), as specified in [[FC-SP](#)]. The FC-SP standard includes the definition of protocols to authenticate Fibre Channel entities, protocols to set up session keys, protocols to negotiate the parameters required to ensure frame-by-frame integrity and confidentiality, and protocols to establish and distribute policies across a Fibre Channel Fabric.

This memo was initially developed by the INCITS T11 committee (<http://www.t11.org>), which subsequently approved it for forwarding to the IETF.

This memo uses one of the following terms:

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 [BCP 14](#), [RFC 2119](#) [[RFC2119](#)].

## 2. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to [section 7 of RFC 3410](#) [[RFC3410](#)].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIV2, which is described in STD 58, [RFC 2578](#) [[RFC2578](#)], STD 58, [RFC 2579](#) [[RFC2579](#)] and STD 58, [RFC 2580](#)

### [3.](#) Overview of Fibre Channel

#### [3.1.](#) Introduction

Fibre Channel (FC) is logically a bidirectional point-to-point serial data channel, structured for high performance. Fibre Channel provides a general transport vehicle for higher level protocols such as Small Computer System Interface (SCSI) command sets, the High-Performance Parallel Interface (HIPPI) data framing, IP (Internet Protocol), IEEE 802.2, and others.

Physically, Fibre Channel is an interconnection of multiple communication points, called N\_Ports, interconnected either by a switching network, called a Fabric, or by a point-to-point link. A Fibre Channel "Node" consists of one or more N\_Ports. A Fabric may consist of multiple Interconnect Elements, some of which are Switches. An N\_Port connects to the Fabric via a port on a Switch called an F\_Port. When multiple FC Nodes are connected to a single port on a Switch via an "Arbitrated Loop" topology, the Switch port is called an FL\_Port, and the Nodes' ports are called NL\_Ports. The term Nx\_Port is used to refer to either an N\_Port or an NL\_Port. The term Fx\_Port is used to refer to either an F\_Port or an FL\_Port. A Switch port, which is interconnected to another Switch port via an Inter-Switch Link (ISL), is called an E\_Port. A B\_Port connects a bridge device with an E\_Port on a Switch; a B\_Port provides a subset of E\_Port functionality.

Many Fibre Channel components, including the Fabric, each Node, and most ports, have globally-unique names. These globally-unique names are typically formatted as World Wide Names (WWNs). More information on WWNs can be found in [\[FC-FS-2\]](#). WWNs are expected to be

persistent across agent and unit resets.

Fibre Channel frames contain 24-bit address identifiers which identify the frame's source and destination ports. Each FC port has both an address identifier and a WWN. When a Fabric is in use, the FC address identifiers are dynamic and are assigned by a Switch. Each octet of a 24-bit address represents a level in an address hierarchy, with a Domain\_ID being the highest level of the hierarchy.

### [3.2.](#) Zoning

Zones within a Fabric provide a mechanism to control frame delivery between Nx\_Ports ("Hard Zoning") or to expose selected views of Name Server information ("Soft Zoning").

Expires 11 January 2009

[Page 4]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

Communication is only possible when the communicating endpoints are members of a common zone. This technique is similar to virtual private networks in that the Fabric has the ability to group devices into Zones.

Hard zoning and soft zoning are two different means of realizing this. Hard zoning is enforced in the Fabric (i.e., Switches) whereas soft zoning is enforced at the endpoints (e.g., Host Bus Adapters) by relying on the endpoints to not send traffic to an N\_Port\_ID not obtained from the Name Server with a few exceptions for well known Addresses (e.g., the Name Server).

Administrators create Zones to increase network security, and prevent data loss or corruption, by controlling access between devices or user groups.

### [3.3.](#) Virtual Fabrics

The standard for an interconnecting Fabric containing multiple Fabric Switch elements is [\[FC-SW-4\]](#). [\[FC-SW-4\]](#) carries forward the earlier specification for the operation of a single Fabric in a physical infrastructure, and augments it with the definition of Virtual Fabrics and with the specification of how multiple Virtual Fabrics can operate within one (or more) physical infrastructures. The use of Virtual Fabrics provides for each frame to be tagged in its header

to indicate which one of several Virtual Fabrics that frame is being transmitted on. All frames entering a particular "Core Switch" [FC-SW-4] (i.e., a physical Switch) on the same Virtual Fabric are processed by the same "Virtual Switch" within that Core Switch.

### 3.4. Security

The Fibre Channel Security Protocols (FC-SP) standard [[FC-SP](#)] describes the protocols used to implement security in a Fibre Channel Fabric, including the definition of:

- protocols to authenticate Fibre Channel entities,
- protocols to set up session keys,
- protocols to negotiate the parameters required to ensure frame-by-frame integrity and confidentiality, and
- protocols to establish and distribute (security) policies across a Fibre Channel Fabric.

#### 3.4.1. Authentication

Two entities may negotiate whether authentication is required and which Authentication Protocol is to be used. Authentication can be used in Switch to Switch, Node to Switch, and Node to Node communication. The defined Authentication Protocols are able to perform mutual authentication with optional shared key establishment. The shared key computed at the end of an Authentication Transaction may be used to establish Security Associations.

The Fabric security architecture is defined for several authentication infrastructures. Secret-based, certificate-based, and password-based authentication infrastructures are accommodated. Specific authentication protocols that directly leverage these three authentication infrastructures are defined.

With a secret-based infrastructure, entities within the Fabric environment that establish a security relationship share a common secret or centralize the secret administration in an external (e.g.,

RADIUS [[RFC2865](#)], Diameter [[RFC3588](#)] or TACACS [[RFC1492](#)]) server. Entities may mutually authenticate with other entities by using the Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) [[FC-SP](#)]. Security Associations may be set up using the session key computed at the end of the DH-CHAP transaction.

With a certificate-based infrastructure, entities within the Fabric environment are certified by a trusted Certificate Authority (CA). The resulting certificates bind each entity to a public-private key pair that may be used to mutually authenticate with other certified entities via the Fibre Channel Certificate Authentication Protocol (FCAP) [[FC-SP](#)]. Security Associations may be set up by using these entity certificates and associated keys or by using the session key computed at the end of the FCAP transaction.

With a password-based infrastructure, entities within the Fabric environment that establish a security relationship have knowledge of the password-based credential material of other entities. Entities may use this credential material to mutually authenticate with other entities using the Fibre Channel Password Authentication Protocol (FCPAP) [[FC-SP](#)]. Security Associations may be set up using the session key computed at the end of the FCPAP transaction.

In addition to DH-CHAP, FCAP and FCPAP, one other Authentication Protocol is defined: IKEv2-AUTH, which refers to the use of an SA Management Transaction of the Security Association Management

Protocol (see below) to perform two functions: not only SA management but also authentication. The credentials used in an IKEv2-AUTH transaction are either strong shared secrets or certificates.

#### 3.4.2. Security Associations

A subset of the IKEv2 protocol [[RFC4306](#)] suitable for Fibre Channel is defined as the (Fibre Channel) Security Association Management protocol [[RFC4595](#)]. This protocol -- which is *not* IPsec -- provides the means to establish Security Associations (SAs) between Fibre Channel entities. Traffic Selectors are defined to specify which type of traffic has to be protected by which SA, and what the characteristics of the protection are. Two mechanisms are available

to protect specific classes of traffic:

- ESP\_Header is used to protect FC-2 frames (see [[FC-FS-2](#)] and the conceptually similar mechanisms in [[RFC4303](#)]), and
- CT\_Authentication is used to protect CT\_IUs (Common Transport Information Units) [[FC-GS-5](#)].

An entity protecting specific classes of traffic maintains an internal Security Association Database (SADB) that contains the currently active Security Associations and Traffic Selectors.

Each active SA has a Security Association entry in the SADB. Each SA entry includes the SA's SPI (the Security Parameters Index which is included in frames transmitted on the SA), a Sequence Number counter, and the parameters for the selected transforms (e.g., encryption algorithm, integrity algorithm, mode of operation of the algorithms, keys).

Each active Traffic Selector has an entry in the SADB which indicates whether it is used for ingress traffic or for egress traffic. These Traffic Selector entries are ordered such that they are searched (when checking for a match) in the given order. Two types of Traffic Selector entries may be present:

- Traffic Selectors entries identifying FC-2 frames or CT\_IUs to be bypassed or discarded; and
- Traffic Selectors entries identifying FC-2 frames or CT\_IUs to be protected or verified. These entries point to the corresponding SA entry defining the parameters and the security processing to be performed.

SAs are unidirectional but they always exist as an SA pair of the same type, one in each direction.

#### [3.4.3.](#) Fabric Security Policies

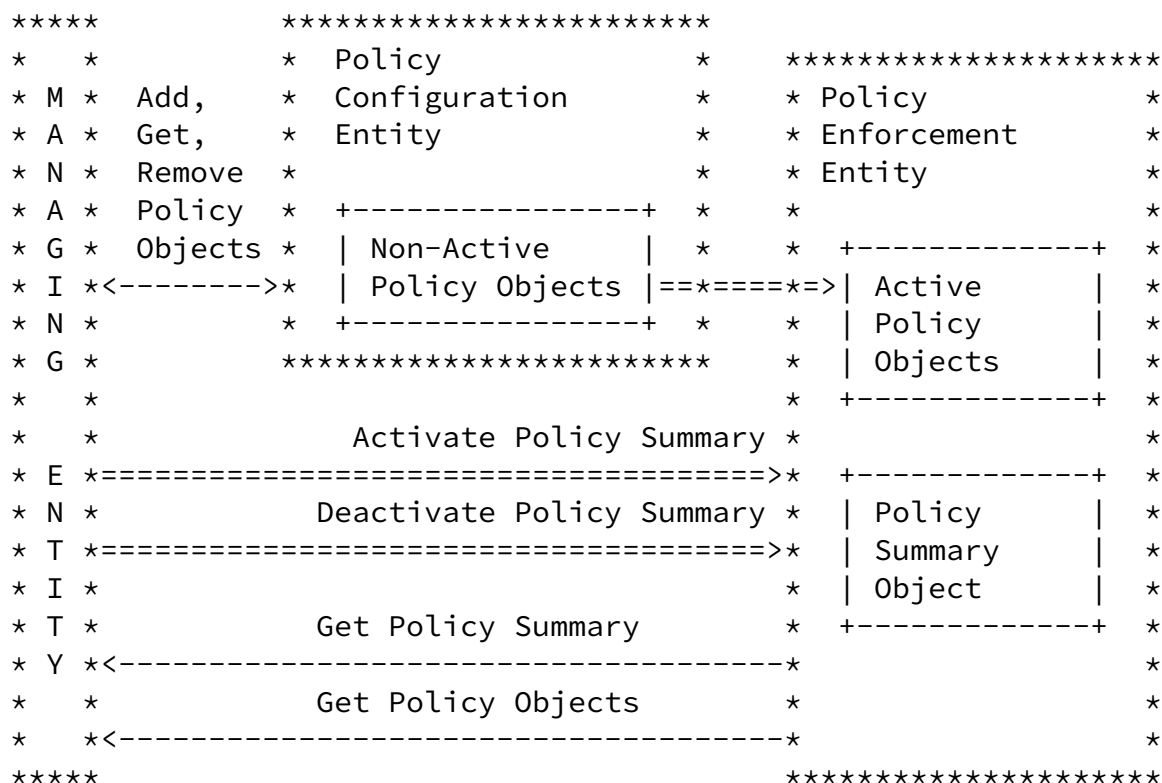
Two separate approaches to defining Policies are adopted in FC-SP, but both approaches follow the same general concept for their Policy



model. One is the definition of a Policy Model for Fabric Policies which focus on Security. These Security Policies specify the membership and connectivity allowed within a Fabric, and also which IP hosts are allowed to manage a Fabric.

The other approach is to define a variant of the Enhanced Zoning model defined in [[FC-SW-4](#)] and [[FC-GS-5](#)], such that the variant specifies extensions for use in a secure environment. This variant of Zoning, denoted as "FC-SP Zoning", follows the same general concepts of the Policy model for Security Policies, but keeps Zoning management and enforcement completely independent from the management and enforcement of other policies.

Figure 25 of [FC-SP] depicts FC-SP's policy management model like this:



Note that the arrows in the picture above are used to indicate the movement of "data", rather than the direction of "messages", e.g., for a "Get" (with no data) in one direction which invokes a "Response" (typically with data) in the reverse direction, the diagram has arrows only for the "with data" direction.

#### 3.4.5. Policy Objects

The Policies to be enforced by a Fabric are specified in a set of Policy Objects. The various types of Policy Objects are:

- The Policy Summary Object is a list of pointers to other Policy Objects, one pointer per each other active Policy Object. Each pointer in a Policy Summary Object is paired with a cryptographic hash of the referenced Policy Object.
- The Switch Membership List Object is a Fabric-wide Policy Object that defines which Switches are allowed to be part of a Fabric.

- The Node Membership List Object is a Fabric-wide Policy Object that defines which Nodes are allowed to be connected to a Fabric.
- The IP Management List Object is a Fabric-wide Policy Object that describes which IP hosts are allowed to manage a Fabric.
- A Switch Connectivity Object is a per-Switch Policy Object that describes the topology restrictions for a specific Switch; it specifies the other Switches or Nodes to which the particular Switch may be connected at the Node level and/or at the Port level.
- Attribute Objects are Fabric-wide Policy Objects that define optional attributes to be associated with Switches or Nodes. They allow the extension of this policy model by defining new attributes as required.

Note that the administratively-specified name for a Fabric is contained in the Switch Membership List Object (not in the Policy Summary Object).

When FC-SP is in use, each Fabric has a set of active Policy Objects:

- one Policy Summary Object,
- one Switch Membership List Object,
- one Node Membership List Object,
- one IP Management List Object,
- zero or more Switch Connectivity Objects, and
- zero or more Attribute Objects.

The active Policy Objects specify the Policies currently being enforced. In addition, policies not currently being enforced are contained in non-active Policy Objects. To change the active Policy Objects, the non-active Policy Objects are edited as necessary and a new Policy Summary Object which includes/references the changed Policy Objects is activated.

#### 3.4.5.1. Policy Object Names

Every Policy Object has a name. In a Fabric's database of Policy Objects, a Policy Object Name is specified as a type/length/value (see section 7.2 of [[FC-SP](#)]). The possible types are:

- Node\_Name
- Restricted Node\_Name
- Port\_Name

- Restricted Port\_Name
- Wildcard
- Negated Wildcard
- Alphanumeric Name
- IPv6 Address Range
- IPv4 Address Range

#### [3.4.6.](#) Three Kinds of Switches

For a Fabric composed of  $n$  Switches and  $m$  Nodes, the potential complexity of Switch Connectivity Objects is  $O(n^2)$  to describe Switch to Switch connections, and  $O(n \cdot m)$  for Switch to Node connections. To provide better scaling, the Switch Connectivity Objects are not Fabric-wide information, but are distributed only to where they are needed. To support this, the policy model supports three kinds of Switches in a Fabric:

- Server Switches, that maintain the Fabric-wide Policy Objects, all the Switch Connectivity Objects, and a full copy of the FC-SP Zoning Database;
- Autonomous Switches, that maintain the Fabric-wide Policy Objects, their own Switch Connectivity Object, and a full copy of the FC-SP Zoning Database; and
- Client Switches, that maintain the Fabric-wide Policy Objects, their own Switch Connectivity Object, and a subset of the FC-SP Active Zone Set (which is the configurations of zones currently being enforced by a Fabric, see section 10.4.3.3 of [[FC-SW-4](#)]).

#### [3.4.7.](#) Security Policy Management

Security Policy can be changed in a server session [[FC-GS-5](#)] with a Security Policy Server. All write access to a Security Policy Server occurs within a server session. While read access to a Security Policy Server may occur at any time, the consistency of the returned data is guaranteed only inside a server session.

The Enhanced Commit Service [[FC-SW-4](#)] is used to perform Fabric operations as and when necessary (see table 144 of [[FC-SP](#)]). Many of these operations are named as if they were acronyms,

e.g., SSB for Server Session Begin; SSE for Server Session End; SW\_ILS for Switch Fabric Internal Link Services; EACA for Enhanced Acquire Change Authorization; ERCA for Enhanced Release Change Authorization; SFC for Stage Fabric Configuration.

Each server session begins and ends, with a SSB request and a SSE request respectively, sent to a Security Policy Server. In the Fabric, the SSB requests a lock of the Fabric via an EACA SW\_ILS, while the SSE requests a release of the lock via the ERCA SW\_ILS [[FC-SW-4](#)]. Active and non-active Policy Objects are persistent in that they survive after the end of a server session.

#### [3.4.8.](#) FC-SP Zoning

To preserve backward compatibility with existing Zoning definitions and implementations, FC-SP Zoning is defined as a variant of the Enhanced Zoning model defined in [[FC-SW-4](#)] and [[FC-GS-5](#)] that follows the general concepts of the Policy model for Security Policy Management, but keeps Zoning management and enforcement completely independent.

FC-SP Zoning allows for some Switches to retain less than a complete replicated copy of the Zoning Database, as follows:

- Server Switches maintain the policies data structures for all Switches in the Fabric plus a replica of the Zoning data structures;
- Autonomous Switches maintain only the subset of policies data structures relevant for their operations plus a replica of the Zoning Database; and
- Client Switches maintain only the subset of policies data structures and the subset of the Active Zone Set relevant for their operations.

When Client Switches are deployed in a Fabric, at least one Server Switch must also be deployed in the same Fabric. A client-server protocol allows Client Switches to dynamically retrieve the Zoning information they may require from the Server Switches.

A management application manages the Fabric Zoning configuration through the Fabric Zone Server, while other policies are managed through the Security Policy Server. A new Zoning Check Protocol replaces the Zone Merge Protocol [[FC-SW-4](#)], and new command codes are defined for the SFC SW\_ILS to distribute the FC-SP Zoning configuration on a Fabric. The Zoning definitions are ordered to allow for the computation of a hash of the Active Zone Set and a hash of the Zone Set Database, plus other optional security data (e.g., for integrity protection of Zoning information).

Expires 11 January 2009

[Page 12]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

## [4.](#) Document Overview

This document defines five MIB modules which together provide the means for monitoring the operation of, and configuring some parameters of, one or more instances of the FC-SP protocols.

### [4.1.](#) Fibre Channel management instance

A Fibre Channel management instance is defined in [[RFC4044](#)] as a separable managed instance of Fibre Channel functionality. Fibre Channel functionality may be grouped into Fibre Channel management instances in whatever way is most convenient for the implementation(s). For example, one such grouping accommodates a single SNMP agent having multiple AgentX [[RFC2741](#)] sub-agents, with each sub-agent implementing a different Fibre Channel management instance.

The object, fcmInstanceIndex, is IMPORTed from the FC-MGMT-MIB [[RFC4044](#)] as the index value to uniquely identify each Fibre Channel management instance, for example within the same SNMP context ([\[RFC3411\] section 3.3.1](#)).

### [4.2.](#) Entity Name

A central capability of FC-SP is the use of an Authentication Protocol. The purpose of each of the possible Authentication Protocols is to allow a Fibre Channel entity to be assured of the identity of each entity with which it is communicating. Examples of such entities are Fibre Channel Switches and Fibre Channel Nx\_Ports.

Each entity is identified by a name. The FC-MGMT-MIB [[RFC4044](#)] defines MIB objects for such names:

- for entities which are Fibre Channel Switches, the definition of a Fibre Channel management instance allows multiple Switches to be managed by the same Fibre Channel management instance. In this case, each entity is a Switch and has the name given by the MIB object, fcmSwitchWWN.
- for entities other than Fibre Channel Switches, a Fibre Channel management instance can manage only one entity, and the name of the entity is given by the MIB object, fcmInstanceWwn.

#### [4.3.](#) Fabric Index

With multiple Fabrics, each Fabric has its own instances of the

Fabric-related management instrumentation. Thus, these MIB modules define all Fabric-related information in tables which are INDEX-ed by an arbitrary integer, named a "Fabric Index". The syntax of a Fabric Index is T11FabricIndex, imported from T11-TC-MIB [[RFC4439](#)]. When a device is connected to a single physical Fabric, without use of any virtual Fabrics, the value of this Fabric Index will always be 1. In an environment of multiple virtual and/or physical Fabrics, this index provides a means to distinguish one Fabric from another.

#### [4.4.](#) Interface Index

Several of the MIB modules defined in this document use the InterfaceIndexOrZero syntax in order to allow information to be specified/instantiated on a per-port/interface basis, e.g., for: statistics, Traffic Selectors, Security Associations, etc. This allows the same object to be used either when there is a separate row for each of multiple ports/interfaces, or when multiple interfaces are represented by a single row. The use of a zero value supports the simpler cases of: a) when there is only one port/interface, b) where the implementation chooses to aggregate the information for multiple ports/interfaces. The minimum (for compliance) requirement is to implement any one of the above cases.

When a Fabric Index and an object with the InterfaceIndexOrZero syntax are used together in a single INDEX clause, the InterfaceIndexOrZero object is listed before the Fabric Index in order to simplify management queries which retrieve information concerning multiple Fabrics connected to the same port/interface.

#### [4.5.](#) Syntax for Policy Object Names

T11FcSpPolicyNameType and T11FcSpPolicyName are two Textual Conventions defined in this document (in the T11-FC-SP-TC-MIB module) to represent the types and values of Policy Object Names (see [section 3.9.1](#) above). However, two of the nine possible types are IPv4 Address Range and IPv6 Address Range. It is standard practice in MIB modules to represent all IP addresses using the standard Textual Conventions defined in [\[RFC4001\]](#) for IP addresses, specifically: InetAddressType and InetAddress. This document adheres to such standard practice to the following extent:

- for MIB objects representing a Policy Object Name which can \*only\* be an IPv4 address range or an IPv6 address range, then those MIB objects are defined as a 3-tuple: (InetAddressType, InetAddress, InetAddress), in which the first address is the low end of the

range, the second address is the high end of the range, and both addresses are of the type given by InetAddressType.

- for MIB objects representing a Policy Object Name which is (possibly) of a different type, i.e., it is not (necessarily) an IPv4 or IPv6 address range, then those MIB objects are defined as a 2-tuple: (T11FcSpPolicyNameType, T11FcSpPolicyName), in which the first object represents the type of Policy Object Name and the second object represents the value of the Policy Object Name. For MIB objects defined in this manner, if and when they represent a range of IP addresses: a) the value of T11FcSpPolicyNameType differentiates between an IPv4 Address Range and an IPv6 Address Range; and b) the value of T11FcSpPolicyName is one string containing the concatenation of the two addresses which are the low and high addresses of the range. This is the same format as used within FC-SP Policy Objects [\[FC-SP\]](#).



#### [4.6.](#) Certificates, CAs and CRLs

In order to authenticate with the FCAP protocol, each entity, identified by a unique Name, is provided with: a digital certificate associated with that Name, the private/public key pair that corresponds to the certificate, and with the Root Certificate (the certificate of the signing Certification Authority). To authenticate another entity, an entity is required to be provided with the certificate of the associated Certification Authority.

FCAP requires entities to support at least four Root Certificates against which received corresponding certificates can be validated. Support for certificate chains and verification of certificate chains containing more than one certificate is optional. Entities need to be able to access a Certificate Revocation List (CRL) for each configured Root Certificate, if one is available from the CA. Certificates on the CRL are considered invalid.

The management of certificates, Certification Authorities and Certificate Revocation Lists is the same in Fibre Channel networks as it is in other networks. Therefore, this document does not define any MIB objects for such management.

#### [4.7.](#) Traffic Selectors

When Traffic Selectors are compared against an ingress or egress frame in order to determine the security processing to be applied to

that frame, there are circumstances in which multiple Traffic Selectors, specifying different actions, can match with the frame. Specifically, when matching against an egress frame to decide which active Security Association to transmit on, or, against an ingress frame unprotected by FC-SP, i.e., without an SPI value in it, to decide which action ('drop' or 'bypass') to apply. For these cases, the MIB includes a unique precedence value for each Traffic Selector such that the one with the numerically lowest precedence value is determined to be the one that matches. In contrast, ingress frames on active Security Associations (i.e., protected by FC-SP) are compared against the set of traffic selectors negotiated when the

Security Association was setup and identified by the SPI value contained in the frame; the action taken depends on whether any Traffic Selector matches, but not on which one.

This difference between ingress and egress Traffic Selectors on active Security Associations is reflected in having separate MIB tables defined for them: the table for Traffic Selectors on egress SAs, `t11FcSpSaTselNegOutTable`, has a precedence value in its INDEX clause, whereas the table for Traffic Selectors on ingress SAs, `t11FcSpSaTselNegInTable`, has an arbitrary integer value in its INDEX clause. For 'drop' and 'bypass' Traffic Selectors, one table, `t11FcSpSaTselDrByTable`, having a precedence value in its INDEX clause, is sufficient for both ingress and egress traffic.

## [4.8.](#) The MIB Modules

### [4.8.1.](#) The T11-FC-SP-TC-MIB Module

This MIB module defines Textual Conventions which are being, or have the potential to be, used in more than one MIB module. The module also defines Object Identifiers to identify the Cryptographic Algorithms listed in [\[FC-SP\]](#) so that they can be used as the value of various MIB objects which specify the algorithms being/to be used by an FC-SP implementation.

### [4.8.2.](#) The T11-FC-SP-AUTHENTICATION-MIB Module

This MIB module specifies the management information required to manage FC-SP Authentication Protocols. It defines three tables:

- `t11FcSpAuEntityTable` -- a table of Fibre Channel entities which can be authenticated using FC-SP's Authentication Protocols, including the names, capabilities and basic configuration parameters of the entities.

- `t11FcSpAuIfStatTable` -- this table has two purposes: to be a list of the mappings of a FC-SP Authentication entity onto an interface, and to contain Authentication Protocol per-interface statistics.
- `t11FcSpAuRejectTable` -- a table of FC-SP Authentication Protocol

transactions which were recently rejected.

It also defines two notifications: one for sending a reject in response to an AUTH message, and another for receiving a reject in response to an AUTH message.

#### [4.8.3.](#) The T11-FC-SP-ZONING-MIB Module

This MIB module specifies the extensions to the T11-FC-ZONE-SERVER-MIB module [[RFC4936](#)] for the management of FC-SP Zoning Servers. Specifically, it augments three tables defined in T11-FC-ZONE-SERVER-MIB:

- t11FcSpZsServerTable -- to this table, it adds FC-SP Zoning information defined for Zone Servers.
- t11ZsStatsTable -- to this table, it adds FC-SP Zoning statistics for Zone Servers.
- t11ZsNotifyControlTable -- to this table, it adds control information for FC-SP Zoning notifications.

It also defines two FC-SP Zoning notifications: one for success and one for failure in the joining of two Fabrics.

#### [4.8.4.](#) The T11-FC-SP-POLICY-MIB Module

This MIB module specifies management information which is used to manage FC-SP policies. The MIB module has five parts:

- Active Policy Objects - read-only MIB objects representing the set of active Policy Objects for each Fabric;
- Activate/Deactivate Operations - read-write MIB objects for invoking operations, either 1) to activate policies which are specified as a set of non-active Policy Objects, or 2) to deactivate the currently-active policies; also included are objects giving the status of invoked operations;
- Non-active Policy Objects - read-create MIB objects to create and

modify non-active Policy Objects;

- Statistics for FC-SP Security Policy Servers;
- The definition and control of notifications for the success or failure of the activation or deactivation of FC-SP policies.

#### 4.8.5. The T11-FC-SP-SA-MIB Module

This MIB module specifies the management information required to manage Security Associations established via FC-SP. All of the tables in this MIB module are INDEX-ed by t11FcSpSaIfIndex, with syntax InterfaceIndexOrZero, which is either non-zero for a specific interface or zero for all (of the management instance's) interfaces to the particular Fabric.

The MIB module consists of six parts:

- a per-Fabric table, t11FcSpSaIfTable, of capabilities, parameters, status information and counters; the counters include non-transient aggregates of per-SA transient counters;
- three tables, t11FcSpSaPropTable, t11FcSpSaTSelPropTable and t11FcSpSaTransTable, specifying the proposals for an FC-SP entity acting as an SA\_Initiator to present to the SA\_Responder during the negotiation of Security Associations. The same information is also used by an FC-SP entity acting as an SA\_Responder to decide what to accept during the negotiation of Security Associations. One of these tables, t11FcSpSaTransTable, is used not only for information about security transforms to propose and to accept, but also as agreed upon during the negotiation of Security Associations;
- a table, t11FcSpSaTSelDrByTable, of Traffic Selectors having the security action of 'drop' or 'bypass' to be applied either to ingress traffic which is unprotected by FC-SP, or to all egress traffic;
- four tables, t11FcSpSaPairTable, t11FcSpSaTSelNegInTable, t11FcSpSaTSelNegOutTable and t11FcSpSaTSelSpiTable, containing information about active bidirectional pairs of Security Associations; in particular, t11FcSpSaPairTable has one row per active bidirectional SA pair, t11FcSpSaTSelNegInTable and t11FcSpSaTSelNegOutTable contain information on the Traffic Selectors negotiated on the SAs, and the t11FcSpSaTSelSpiTable is an alternate lookup table such that the Traffic Selector(s) in use

on a particular Security Association can be quickly determined based on its (ingress) SPI value;

- a table, `t11FcSpSaControlTable`, of control and other information concerning the generation of notifications for events related to FC-SP Security Associations;
- one notification, `t11FcSpSaNotifyAuthFailure`, generated on the occurrence of an Authentication failure for a received FC-2 or CT\_IU frame.

#### [4.9.](#) Rate Control for Notifications

All but one of the notifications defined in the five MIB modules in this document are notifications which are generated based on events occurring in the "control plane", e.g., notifications which are generated at the frequency of operator-initiated activities. The one exception is `t11FcSpSaNotifyAuthFailure`, which is generated based on an event occurring in the "data plane", and could (in a worst case scenario) occur for every received ingress frame. Therefore, a method of rate controlling the generation of notifications is needed for `t11FcSpSaNotifyAuthFailure`, but not for any of the other notifications.

For `t11FcSpSaNotifyAuthFailure`, rate control is achieved by specifying that a) after the first occurrence of an Authentication failure on any particular Security Association, the SNMP notifications for second and subsequent failures are suppressed for the duration of a time window, and b) that even the notification for the first occurrence is suppressed after it is sent in the same time window for a configured (in `t11FcSpSaControlMaxNotifs`) number of Security Associations within a Fabric. Note that while these suppressions prevent the network being flooded with notifications, the Authentication Failures themselves must still be detected and counted.

The length of the time window is given by `t11FcSpSaControlWindow`, a read-write object in the `t11FcSpSaControlTable`. If and when the time since the last generation of the notification is less than the value of `sysUpTime` (e.g., if one or more notifications have occurred since the last re-initialization of the management system), then `t11FcSpSaControlElapsed` and `t11FcSpSaControlSuppressed` contain the

elapsed time since the last notification and the number of notifications suppressed in the window after sending the last one,

respectively. Otherwise, `t11FcSpSaControlElapsed` contains the value of `sysUpTime` and `t11FcSpSaControlSuppressed` has the value zero.

## 5. Relationship to Other MIB Modules

The first standardized MIB module for Fibre Channel [[RFC2837](#)] was focussed on Fibre Channel Switches. It was obsoleted by the more generic Fibre Channel Management MIB [[RFC4044](#)] which defines basic information for Fibre Channel Nodes and Switches, including extensions to the standard IF-MIB [[RFC2863](#)] for Fibre Channel interfaces. Several other MIB modules have since been defined to extend [[RFC4044](#)] for various specific Fibre Channel functionality, (e.g., [[RFC4438](#)], [[RFC4439](#)], [[RFC4625](#)], [[RFC4626](#)], [[RFC4747](#)], [[RFC4936](#)], [[RFC4935](#)], [[RFC4983](#)]).

The MIB modules defined in this memo further extend [[RFC4044](#)] to cover the operation of Fibre Channel Security Protocols, as specified in [[FC-SP](#)].

One part of the FC-SP specification is "FC-SP Zoning" which is an extension/variant of the Fibre Channel Zoning defined in [[FC-GS-5](#)]. Management information for the latter is defined in the T11-FC-ZONE-SERVER-MIB module [[RFC4936](#)]. Consequently, the T11-FC-SP-ZONING-MIB module defined in this document defines the extensions to the T11-FC-ZONE-SERVER-MIB module which are needed to manage FC-SP Zoning.

The MIB modules in this memo import some common Textual Conventions from T11-TC-MIB defined in [[RFC4439](#)] and from INET-ADDRESS-MIB defined in [[RFC4001](#)].

If the RADIUS protocol is used for access to an external server, information about RADIUS Servers is likely to be available from the RADIUS-AUTH-CLIENT-MIB [[RFC4668](#)].

## [6.](#) MIB Module Definitions

### [6.1.](#) The T11-FC-SP-TC-MIB Module

T11-FC-SP-TC-MIB DEFINITIONS ::= BEGIN

IMPORTS

MODULE-IDENTITY, OBJECT-IDENTITY, mib-2,  
Unsigned32                      FROM SNMPv2-SMI                      -- [\[RFC2578\]](#)  
TEXTUAL-CONVENTION FROM SNMPv2-TC;                      -- [\[RFC2579\]](#)

t11FcTcMIB MODULE-IDENTITY

LAST-UPDATED "200801030000Z"

ORGANIZATION "This MIB module was developed through the  
coordinated effort of two organizations:  
T11 began the development and the IETF (in  
the IMSS Working Group) finished it."

CONTACT-INFO

" Claudio DeSanti  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134 USA  
EMail: cds@cisco.com

Keith McCloghrie  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134 USA  
Email: kzm@cisco.com"

DESCRIPTION

"This MIB module defines Textual Conventions for use in the multiple MIB modules which together define the instrumentation for an implementation of the Fibre Channel Security Protocols (FC-SP) specification.

This MIB module also defines Object Identities (for use as possible values of MIB objects with syntax AutonomousType), including OIDs for the Cryptographic Algorithms defined in FC-SP.

Copyright (C) The IETF Trust (2008). This version of this MIB module is part of RFC yyyy; see the RFC itself for full legal notices."

-- RFC Editor: replace yyyy with actual RFC number & remove this note

Expires 11 January 2009

[Page 21]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

REVISION "200801030000Z"

DESCRIPTION

"Initial version of this MIB module, published as RFCyyyy."

-- RFC-Editor, replace yyyy with actual RFC number & remove this note

::= { mib-2 nnn } -- to be assigned by IANA

-- RFC Editor: replace nnn with IANA-assigned number & remove this note

t11FcSpIdentities OBJECT IDENTIFIER ::= { t11FcTcMIB 1 }

t11FcSpAlgorithms OBJECT IDENTIFIER ::= { t11FcSpIdentities 1 }

--

-- Textual Conventions

--

T11FcSpPolicyHashFormat ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"Identifies a cryptographic hash function used to create a hash value which summarizes an FC-SP Policy Object.

Each definition of an object with this TC as its syntax must be accompanied by a corresponding definition of an object with T11FcSpPolicyHashValue as its syntax, and containing the hash value.



The first two cryptographic hash functions are:

Hash Type	Hash Tag	Hash Length (Bytes)
SHA-1	'00000001'h	20
SHA-256	'00000002'h	32

"

#### REFERENCE

- "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.3.1](#) and table 106.
- FIPS PUB 180-2."

SYNTAX OCTET STRING (SIZE (4))

Expires 11 January 2009

[Page 22]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

T11FcSpPolicyHashValue ::= TEXTUAL-CONVENTION

STATUS current

#### DESCRIPTION

"Represents the value of the cryptographic hash function of an FC-SP Policy Object.

Each definition of an object with this TC as its syntax must be accompanied by a corresponding definition of an object with T11FcSpPolicyHashFormat as its syntax. The corresponding object identifies the cryptographic hash function used to create the hash value."

#### REFERENCE

- "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.3.1](#) and table 106."

SYNTAX OCTET STRING (SIZE (0..64))

T11FcSpHashCalculationStatus ::= TEXTUAL-CONVENTION

STATUS           current

DESCRIPTION

"When some kind of 'database' is defined in a set of read-write MIB objects, it is common that multiple changes in the data need to be made at the same time. So, if hash values are maintained for that data, those hash values are only correct if and when they are re-calculated after every change. In such circumstances, the use of an object with this syntax allows the re-calculation of the hash values to be deferred until all changes have been made and therefore the calculation need only be done once after all changes, rather than repeatedly/after each individual change.

The definition of an object defined using this TC is required to specify which one or more instances of which MIB objects contain the hash values operated upon (or whose status is given) by the value of this TC.

When read, the value of an object with this syntax is either:

correct -- the identified MIB object instance(s)  
          contain the correct hash values; or  
stale    -- the identified MIB object instance(s)  
          contain stale (possibly incorrect) values.

Expires 11 January 2009

[Page 23]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

Writing a value of 'calculate' is a request to re-calculate and update the values of the corresponding instances of the identified MIB objects. Writing a value of 'correct' or 'stale' to this object is an error (e.g., 'wrongValue')."

SYNTAX           INTEGER {  
                    calculate(1),  
                    correct(2),  
                    stale(3)  
                  }

T11FcSpAuthRejectReasonCode ::= TEXTUAL-CONVENTION

STATUS           current

DESCRIPTION

"A reason code contained in an AUTH\_Reject message, or in an SW\_RJT (rejecting an AUTH\_ILS), or in an LS\_RJT (rejecting an AUTH-ELS)."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, Table 17, 48, 52."

SYNTAX

```
INTEGER {  
    authFailure(1),  
    logicalError(2),  
    logicalBusy(3),  
    authILSNotSupported(4),  
    authELSNotSupported(5),  
    notLoggedIn(6)  
}
```

T11FcSpAuthRejReasonCodeExp ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"A reason code explanation contained in an AUTH\_Reject message, or in an SW\_RJT (rejecting an AUTH\_ILS), or in an LS\_RJT (rejecting an AUTH-ELS)."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, Tables 18, 48, 52."

SYNTAX

```
INTEGER {  
    authMechanismNotUsable(1),  
    dhGroupNotUsable(2),  
    hashFunctionNotUsable(3),  
    authTransactionAlreadyStarted(4),
```

```
authenticationFailed(5),  
incorrectPayload(6),  
incorrectAuthProtocolMessage(7),  
restartAuthProtocol(8),  
authConcatNotSupported(9),  
unsupportedProtocolVersion(10),  
logicalBusy(11),
```

```

        authILSNotSupported(12),
        authELSNotSupported(13),
        notLoggedIn(14)
    }

```

T11FcSpHashFunctions ::= TEXTUAL-CONVENTION

```

    STATUS          current
    DESCRIPTION
        "A set of zero, one or more hash functions defined for
        use in FC-SP."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
        Fibre Channel - Security Protocols (FC-SP),
        February 2007, Table 14."
    SYNTAX          BITS {
                        md5(0),
                        sha1(1)
                    }

```

T11FcSpSignFunctions ::= TEXTUAL-CONVENTION

```

    STATUS          current
    DESCRIPTION
        "A set of zero, one or more signature functions defined
        for signing certificates for use with FCAP in FC-SP."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
        Fibre Channel - Security Protocols (FC-SP),
        February 2007, tables 38 & 39."
    SYNTAX          BITS {
                        rsaSha1(0)
                    }

```

T11FcSpDhGroups ::= TEXTUAL-CONVENTION

STATUS           current

DESCRIPTION

    "A set of zero, one or more DH Groups defined for use in FC-SP."

REFERENCE

    "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, Table 15."

SYNTAX           BITS {

                  null(0),

                  group1024(1),

                  group1280(2),

                  group1536(3),

                  group2048(4),

                  group3072(5),

                  group4096(6),

                  group6144(7),

                  group8192(8)

                  }

T11FcSpPolicyObjectType ::= TEXTUAL-CONVENTION

STATUS           current

DESCRIPTION

    "A value which identifies the type of an FC-SP Policy Object."

REFERENCE

    "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, Table 102."

SYNTAX           INTEGER {

                  summary(1),

                  switchMemberList(2),

                  nodeMemberList(3),

                  switchConnectivity(4),

                  ipMgmtList(5),

                  attribute(6)

                  }

T11FcSpPolicyNameType ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"The format and usage of a companion object having T11FcSpPolicyName as its syntax.

Six of the values indicate the same format, i.e., they differ only in semantics. That common format is a Fibre Channel 'Name\_Identifier', i.e., the same syntax as 'FcNameIdOrZero (SIZE(8))'.

These six are three pairs of one restricted and one unrestricted. Each usage of this syntax must specify what the meaning of "restricted" is for that usage, and how the characteristics and behavior of restricted names differ from unrestricted names.

The six are:

- 'nodeName' - a Node\_Name, which is the Name\_Identifier associated with a Fibre Channel Node.
- 'restrictednodeName' - a Restricted Node\_Name.
- 'portName' - the Name\_Identifier associated with a Fibre Channel Port.
- 'restrictedPortName' - a Restricted Port\_Name.
- 'wildcard' - a Wildcard value which is used to identify 'all others' (typically, all other members of a Policy Object, not all other Policy Objects).
- 'restrictedWildcard' - a Restricted Wildcard value.

Other possible values are:

- 'alphaNumericName' - the value begins with an ASCII letter (upper or lower case) followed by (0 ... 63) characters from the set: lower case letters, upper case letters, digits, and the four symbols: dollar-sign (\$), dash (-), caret (^), and underscore (\_).

'ipv6AddressRange' - two IPv6 addresses in network byte order, the numerically smallest first and the numerically largest second; total length is 32 bytes.

'ipv4AddressRange' - two IPv4 addresses in network byte order, the numerically smallest first and the numerically largest second; total length is 8 bytes."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, Table 103."

SYNTAX    INTEGER {  
            nodeName(1),  
            restrictedNodeName(2),  
            portName(3),  
            restrictedPortName(4),  
            wildcard(5),  
            restrictedWildcard(6),  
            alphaNumericName(7),  
            ipv6AddressRange(8),  
            ipv4AddressRange(9)  
          }

T11FcSpPolicyName ::= TEXTUAL-CONVENTION

STATUS            current

## DESCRIPTION

"A syntax used, when defining Policy Objects, for the name of something.

An object which uses this syntax always identifies a companion object with syntax T11FcSpPolicyNameType such that the companion object specifies the format and usage of the object with this syntax.

When the companion object has the value 'wildcard' or 'restrictedWildcard', the value of the T11FcSpPolicyName object is: '0000000000000000'h."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),

February 2007, Table 103."  
SYNTAX OCTET STRING (SIZE (1..64))

Expires 11 January 2009

[Page 28]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

T11FcSpAlphaNumName ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"A syntax used when defining Policy Objects for the name of something, where the name is always in the format specified by:

T11FcSpPolicyNameType = 'alphaNumericName'  
"

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, Table 103."

SYNTAX OCTET STRING (SIZE (1..64))

T11FcSpAlphaNumNameOrAbsent ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"An extension of the T11FcSpAlphaNumName TC which one additional possible value: the zero-length string to indicate the absence of a name."

SYNTAX OCTET STRING (SIZE (0..64))

T11FcSaDirection ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"The direction of frame transmission on a Security Association. Note that Security Associations are unidirectional but they always exist as part of an SA pair of the same type in opposite directions."

SYNTAX INTEGER { ingress(1), egress(2) }



---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

T11FcSpiIndex ::= TEXTUAL-CONVENTION

STATUS            current

DESCRIPTION

"An SPI (Security Parameter Index) value is carried in the SPI field of a frame protected by the ESP\_Header. An SPI is also carried in the SAID field of a Common Transport Information Unit (CT\_IU) protected by CT\_Authentication. An SPI value identifies the Security Association on which the frame is being transmitted."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 4.7.2](#) and 4.7.3."

SYNTAX    Unsigned32 (0..4294967295) -- the default range!!

T11FcSpPrecedence ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

STATUS            current

DESCRIPTION

"The precedence of a Traffic Selector. If a frame matches with two or more Traffic Selectors, then the match which takes precedence is the one with the Traffic Selector having the numerically smallest precedence value. Note that precedence values are not necessarily contiguous."

SYNTAX    Unsigned32 (0..4294967295) -- the default range!!

T11FcRoutingControl ::= TEXTUAL-CONVENTION

DISPLAY-HINT "1x"

STATUS current

DESCRIPTION

"A value stored in the R\_CTL (Routing Control) 8-bit field of an FC-2 frame containing routing and information bits to categorize the frame function.

For FC-2 frames, an R\_CTL value typically distinguishes between control versus data frames, and/or solicited versus unsolicited frames, and in combination with the TYPE field (see T11FcSpType) identifies a particular link layer service/protocol using FC-2.

For CT\_Authentication, the information field in the R\_CTL field contains '02'h for Request CT\_IUs, and '03'h for Response CT\_IUs.

Expires 11 January 2009

[Page 30]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

The comparison of two values having this syntax is done by treating each string as an 8-bit numeric value."

REFERENCE

- " - Fibre Channel - Framing and Signaling-2 (FC-FS-2), ANSI INCITS 424-2007, Project T11/1619-D, February 2007, [section 9.3](#).
- Fibre Channel - Generic Services-5 (FC-GS-5), ANSI INCITS 427-2006, sections [4.5.2.4.2](#), [4.5.2.4.3](#) and table 12."

SYNTAX OCTET STRING (SIZE(1))

T11FcSpType ::= TEXTUAL-CONVENTION

DISPLAY-HINT "2x"

STATUS current

DESCRIPTION

"A value, or combination of values, contained in a frame header used in identifying the link layer service/protocol of a frame. The value is always two octets:

- for FC-2 frames, the first octet is zero and the second octet contains the Data structure type (TYPE) value defined by FC-FS-2. The TYPE value is used in

combination with T11FcRoutingControl to identify a link layer service/protocol.

- for Common Transport Information Units (CT\_IUs), the first octet contains a GS\_Type value and the second octet contains a GS\_Subtype value, defined by FC-GS-5.

The comparison of two values having this syntax is done by treating each string as the numeric value obtained by numerically combining the individual octet's value as follows:

$(256 * \text{1st-octet}) + \text{2nd-octet}$

"

REFERENCE

- " - Fibre Channel - Framing and Signaling-2 (FC-FS-2), ANSI INCITS 424-2007, Project T11/1619-D, February 2007, [section 9.6](#).
- Fibre Channel - Generic Services-5 (FC-GS-5), ANSI INCITS 427-2006, sections [4.3.2.4](#) and [4.3.2.5](#)."

SYNTAX OCTET STRING (SIZE(2))

Expires 11 January 2009

[Page 31]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

T11FcSpTransforms ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"A list of the standardized transforms which are defined by FC-SP for use with ESP\_Header, CT\_Authentication and/or IKEv2 Support."

REFERENCE

- "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [Appendix A.3.1](#), tables A.23, A.24, A.25, A.26."

SYNTAX BITS {  
    encrNull(0),  
    encrAesCbc(1),  
    encrAesCtr(2),  
    encrAesGcm(3),  
    encr3Des(4),  
    prfHmacMd5(5),

```

        prfHmacSha1(6),
        prfAesCbc(7),
        authHmacMd5L96(8),
        authHmacSha1L96(9),
        authHmacMd5L128(10),
        authHmacSha1L160(11),
        encrNullAuthAesGmac(12),
        dhGroups1024bit(13),
        dhGroups2048bit(14)
    }

```

T11FcSpSecurityProtocolId ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"A Security Protocol identifier to identify the protocol by which traffic is to be protected, e.g., ESP\_Header or CT\_Authentication."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 6.3.2.2](#) and table 67."

SYNTAX INTEGER { espHeader(1), ctAuth(2) }

Expires 11 January 2009

[Page 32]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

T11FcSpLifetimeLeft ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"This TC is used for one object of an associated pair of objects. The object with this syntax specifies a remaining lifetime of something, e.g., of an SA, where the lifetime is given in the units specified by the other object of the pair which has T11FcSpLifetimeLeftUnits as its syntax."

SYNTAX Unsigned32

T11FcSpLifetimeLeftUnits ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"An object, defined using T11FcSpLifetimeLeft TC as its syntax, is required to be one of an associated pair of objects such that the other object of the pair is defined with this T11FcSpLifetimeLeftUnits TC as its syntax and with its value specifying the units of the remaining lifetime given by the value of the T11FcSpLifetimeLeft object."

SYNTAX

```
INTEGER {
    seconds(1),          -- seconds
    kiloBytes(2),        -- 10^^3 bytes
    megaBytes(3),        -- 10^^6 bytes
    gigaBytes(4),        -- 10^^9 bytes
    teraBytes(5),        -- 10^^12 bytes
    petaBytes(6),        -- 10^^15 bytes
    exaBytes(7),         -- 10^^18 bytes
    zettaBytes(8),       -- 10^^21 bytes
    yottaBytes(9)        -- 10^^24 bytes
}
```

--

-- Object Identities to identify the Cryptographic Algorithms  
-- listed in FC-SP.

--

```

t11FcSpEncryptAlgorithms
    OBJECT IDENTIFIER ::= { t11FcSpAlgorithms 1 }

t11FcSpEncrNull OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "The ENCR_NULL algorithm."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
           Fibre Channel - Security Protocols (FC-SP),
           February 2007, Table 70."
    ::= { t11FcSpEncryptAlgorithms 1 }

t11FcSpEncrAesCbc OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "The ENCR_AES_CBC algorithm."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
           Fibre Channel - Security Protocols (FC-SP),
           February 2007, Table 70."
    ::= { t11FcSpEncryptAlgorithms 2 }

t11FcSpEncrAesCtr OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "The ENCR_AES_CTR algorithm."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
           Fibre Channel - Security Protocols (FC-SP),
           February 2007, Table 70."
    ::= { t11FcSpEncryptAlgorithms 3 }

t11FcSpEncrAesGcm OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "The ENCR_AES_GCM algorithm."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
           Fibre Channel - Security Protocols (FC-SP),
           February 2007, Table 70."
    ::= { t11FcSpEncryptAlgorithms 4 }

t11FcSpEncr3Des OBJECT-IDENTITY

```

STATUS       current  
DESCRIPTION "The ENCR\_3DES algorithm."  
REFERENCE  
    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
       Fibre Channel - Security Protocols (FC-SP),  
       February 2007, Table 70."  
::= { t11FcSpEncryptAlgorithms 5 }

t11FcSpAuthAlgorithms  
    OBJECT IDENTIFIER ::= { t11FcSpAlgorithms 2 }

t11FcSpAuthNull OBJECT-IDENTITY  
STATUS       current  
DESCRIPTION "The AUTH\_NONE algorithm."  
REFERENCE  
    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
       Fibre Channel - Security Protocols (FC-SP),  
       February 2007, Table 72."  
::= { t11FcSpAuthAlgorithms 1 }

t11FcSpAuthHmacMd5L96 OBJECT-IDENTITY  
STATUS       current  
DESCRIPTION "The AUTH\_HMAC\_MD5\_96 algorithm."  
REFERENCE  
    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
       Fibre Channel - Security Protocols (FC-SP),  
       February 2007, Table 72."  
::= { t11FcSpAuthAlgorithms 2 }

t11FcSpAuthHmacSha1L96 OBJECT-IDENTITY  
STATUS       current  
DESCRIPTION "The AUTH\_HMAC\_SHA1\_96 algorithm."  
REFERENCE  
    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
       Fibre Channel - Security Protocols (FC-SP),  
       February 2007, Table 72."  
::= { t11FcSpAuthAlgorithms 3 }

t11FcSpAuthHmacMd5L128 OBJECT-IDENTITY  
STATUS       current  
DESCRIPTION "The AUTH\_HMAC\_MD5\_128 algorithm."  
REFERENCE  
    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
       Fibre Channel - Security Protocols (FC-SP),

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```

        February 2007, Table 72."
 ::= { t11FcSpAuthAlgorithms 4 }

t11FcSpAuthHmacSha1L160 OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "The AUTH_HMAC_SHA1_160 algorithm."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
           Fibre Channel - Security Protocols (FC-SP),
           February 2007, Table 72."
 ::= { t11FcSpAuthAlgorithms 5 }

t11FcSpEncrNullAuthAesGmac OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "The ENCR_NULL_AUTH_AES_GMAC algorithm."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
           Fibre Channel - Security Protocols (FC-SP),
           February 2007, Table 70."
 ::= { t11FcSpEncryptAlgorithms 6 }

END
```



## [6.2.](#) The T11-FC-SP-AUTHENTICATION-MIB Module

```
--*****
-- FC-SP Authentication Protocols
--
```

```
T11-FC-SP-AUTHENTICATION-MIB  DEFINITIONS ::= BEGIN
```

### IMPORTS

```
    MODULE-IDENTITY, OBJECT-TYPE, OBJECT-IDENTITY,
    NOTIFICATION-TYPE,
    mib-2, Counter32, Unsigned32
                                FROM SNMPv2-SMI  -- [RFC2578]

    MODULE-COMPLIANCE, OBJECT-GROUP,
    NOTIFICATION-GROUP
                                FROM SNMPv2-CONF -- [RFC2580]

    StorageType, AutonomousType,
    TruthValue, TimeStamp
                                FROM SNMPv2-TC   -- [RFC2579]
    InterfaceIndex
                                FROM IF-MIB       -- [RFC2863]
    fcmInstanceIndex,
    FcNameIdOrZero
                                FROM FC-MGMT-MIB  -- [RFC4044]
    t11FamLocalSwitchWwn
                                FROM T11-FC-FABRIC-ADDR-MGR-MIB -- [RFC4439]
    T11FabricIndex
                                FROM T11-TC-MIB   -- [RFC4439]
    T11FcSpDhGroups,
    T11FcSpHashFunctions,
    T11FcSpSignFunctions,
    T11FcSpLifetimeLeft,
    T11FcSpLifetimeLeftUnits,
    T11FcSpAuthRejectReasonCode,
    T11FcSpAuthRejReasonCodeExp
                                FROM T11-FC-SP-TC-MIB;
```

```
t11FcSpAuthenticationMIB  MODULE-IDENTITY
```

```
    LAST-UPDATED  "200801030000Z"
```

```
    ORGANIZATION  "This MIB module was developed through the
                    coordinated effort of two organizations:
```

T11 began the development and the IETF (in the IMSS Working Group) finished it."

CONTACT-INFO

" Claudio DeSanti  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134 USA  
EMail: cds@cisco.com

Expires 11 January 2009

[Page 37]

Internet Draft

Fibre-Channel Security Protocols MIB

July 2008

Keith McCloghrie  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134 USA  
Email: kzm@cisco.com"

DESCRIPTION

"This MIB module specifies the management information required to manage the Authentication Protocols defined by Fibre Channel's FC-SP specification.

This MIB module defines three tables:

- t11FcSpAuEntityTable is a table of Fibre Channel entities which can be authenticated using FC-SP's Authentication Protocols.
- t11FcSpAuIfStatTable is a table with one row for each mapping of an Authentication entity onto an interface, containing statistics information.
- t11FcSpAuRejectTable is a table of volatile information about FC-SP Authentication Protocol transactions which were most recently rejected.

Copyright (C) The IETF Trust (2008). This version of this MIB module is part of RFC yyyy; see the RFC itself for full legal notices."

-- RFC Editor: replace yyyy with actual RFC number & remove this note  
REVISION "200801030000Z"

DESCRIPTION

"Initial version of this MIB module, published as RFCyyyy."

-- RFC-Editor, replace yyyy with actual RFC number & remove this note  
::= { mib-2 nnn } -- to be assigned by IANA  
-- RFC Editor: replace nnn with IANA-assigned number & remove this note

t11FcSpAuMIBNotifications

OBJECT IDENTIFIER ::= { t11FcSpAuthenticationMIB 0 }

t11FcSpAuMIBObjects

OBJECT IDENTIFIER ::= { t11FcSpAuthenticationMIB 1 }

t11FcSpAuMIBConformance

OBJECT IDENTIFIER ::= { t11FcSpAuthenticationMIB 2 }

t11FcSpAuMIBIdentities

OBJECT IDENTIFIER ::= { t11FcSpAuthenticationMIB 3 }

Expires 11 January 2009

[Page 38]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--  
--  
--

-- OIDs defined for use as values of t11FcSpAuServerProtocol

t11FcSpAuServerProtocolRadius OBJECT-IDENTITY

STATUS            current

DESCRIPTION

"This OID identifies RADIUS as the protocol used  
to communicate with an External Server as part of  
the process by which identities are verified.  
In this case, information about the RADIUS Servers  
is likely to be provided in radiusAuthServerExtTable  
defined in the RADIUS-AUTH-CLIENT-MIB."

REFERENCE

"radiusAuthServerExtTable in 'RADIUS Authentication  
Client MIB', [RFC 4668](#), August 2006."

::= { t11FcSpAuMIBIdentities 1 }

t11FcSpAuServerProtocolDiameter OBJECT-IDENTITY

STATUS            current

DESCRIPTION

"This OID identifies Diameter as the protocol used  
to communicate with an External Server as part of  
the process by which identities are verified."

REFERENCE

"[RFC 3588](#), September 2003."  
 ::= { t11FcSpAuMIBIdentities 2 }

t11FcSpAuServerProtocolTacacs OBJECT-IDENTITY

STATUS current

DESCRIPTION

"This OID identifies TACACS as the protocol used to communicate with an External Server as part of the process by which identities are verified."

REFERENCE

"[RFC 1492](#), July 1993."

::= { t11FcSpAuMIBIdentities 3 }

Expires 11 January 2009

[Page 39]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--

-- Configuration for the Authentication Protocols

--

t11FcSpAuEntityTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpAuEntityEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of Fibre Channel entities which can be authenticated using FC-SP's Authentication Protocols.

The purpose of an FC-SP Authentication Protocol is to verify that a claimed name is associated with the claiming entity.

The Authentication Protocols can be used to authenticate

Nx\_Ports, B\_Ports, or Switches."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),

February 2007, [section 3.2.25.](#)"  
 ::= { t11FcSpAuMIBObjects 1 }

t11FcSpAuEntityEntry OBJECT-TYPE

SYNTAX T11FcSpAuEntityEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Information about the configuration and capabilities of an FC-SP entity (which is managed within the Fibre Channel management instance identified by fcmInstanceIndex) on a particular Fabric with respect to FC-SP's Authentication Protocols."

INDEX { fcmInstanceIndex, t11FcSpAuEntityName,  
 t11FcSpAuFabricIndex }

::= { t11FcSpAuEntityTable 1 }

T11FcSpAuEntityEntry ::= SEQUENCE {

t11FcSpAuEntityName FcNameIdOrZero,

t11FcSpAuFabricIndex T11FabricIndex,

t11FcSpAuServerProtocol AutonomousType,

-- Config parameters

t11FcSpAuStorageType StorageType,

t11FcSpAuSendRejNotifyEnable TruthValue,

t11FcSpAuRcvRejNotifyEnable TruthValue,

t11FcSpAuDefaultLifetime Unsigned32,

Expires 11 January 2009

[Page 40]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

t11FcSpAuDefaultLifetimeUnits INTEGER,

t11FcSpAuRejectMaxRows Unsigned32,

-- Capabilities

t11FcSpAuDhChapHashFunctions T11FcSpHashFunctions,

t11FcSpAuDhChapDhGroups T11FcSpDhGroups,

t11FcSpAuFcapHashFunctions T11FcSpHashFunctions,

t11FcSpAuFcapCertsSignFunctions T11FcSpSignFunctions,

t11FcSpAuFcapDhGroups T11FcSpDhGroups,

t11FcSpAuFcapHashFunctions T11FcSpHashFunctions,

t11FcSpAuFcapDhGroups T11FcSpDhGroups

}

t11FcSpAuEntityName OBJECT-TYPE

SYNTAX        FcNameIdOrZero (SIZE (8))

MAX-ACCESS not-accessible

STATUS        current

DESCRIPTION

"The name used to identify the FC-SP entity.

For entities which are Fibre Channel Switches, this value corresponds to the Switch's value of fcmSwitchWWN. For entities other than Fibre Channel Switches, this value corresponds to the value of fcmInstanceWwn for the corresponding Fibre Channel management instance."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 5.3.3](#).

- fcmInstanceWwn & fcmSwitchWWN,  
'Fibre Channel Management MIB', [RFC 4044](#), May 2005."

::= { t11FcSpAuEntityEntry 1 }

t11FcSpAuFabricIndex OBJECT-TYPE

SYNTAX        T11FabricIndex

MAX-ACCESS not-accessible

STATUS        current

DESCRIPTION

"An index value which uniquely identifies a  
particular Fabric to which the entity is attached."

::= { t11FcSpAuEntityEntry 2 }

t11FcSpAuServerProtocol OBJECT-TYPE

SYNTAX        AutonomousType

MAX-ACCESS read-only

STATUS        current

Expires 11 January 2009

[Page 41]

---

Internet Draft        Fibre-Channel Security Protocols MIB

July 2008

DESCRIPTION

"The protocol, if any, used by the entity to communicate with a third party (i.e., an External Server) as part of the process by which it verifies DH-CHAP responses. For example, if the entity is using an external RADIUS server to verify DH-CHAP responses, then this object will have the value t11FcSpAuServerProtocolRadius.

The value, zeroDotZero, is used to indicate that no protocol is being used to communicate with a third party to verify DH-CHAP responses.

When no protocol is being used, or if the third party is unreachable via the specified protocol, then locally configured information (if any) may be used instead."

::= { t11FcSpAuEntityEntry 3 }

t11FcSpAuStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This object specifies the memory realization of configuration information related to an FC-SP Entity on a particular Fabric; specifically, for MIB objects in the row containing this object.

Even if an instance of this object has the value 'permanent(4)', none of the information in the corresponding row of this table needs to be writable."

::= { t11FcSpAuEntityEntry 4 }

t11FcSpAuSendRejNotifyEnable OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"An indication of whether or not the entity should issue t11FcSpAuRejectSentNotify notifications when sending AUTH\_Reject/SW\_RJT/LS\_RJT to reject an AUTH message.

If the value of the object is 'true', then this type of notification is generated. If the value is 'false', this type of notification is not generated."

DEFVAL { false }

::= { t11FcSpAuEntityEntry 5 }

t11FcSpAuRcvRejNotifyEnable OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"An indication of whether or not the entity should issue t11FcSpAuRejectReceivedNotify notifications on the receipt of AUTH\_Reject/SW\_RJT/LS\_RJT messages.

If the value of the object is 'true', then this type of notification is generated. If the value is 'false', this type of notification is not generated."

DEFVAL { false }

::= { t11FcSpAuEntityEntry 6 }

t11FcSpAuDefaultLifetime OBJECT-TYPE

SYNTAX T11FcSpLifetimeLeft

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"When the value of this object is non-zero, it specifies the default value of a lifetime, specified in units given by the corresponding instance of t11FcSpAuDefaultLifetimeUnits. This default lifetime is to be used for any Security Association which has no explicitly-specified value for its lifetime.

An SA's lifetime is either the time interval or the number of passed bytes, after which the SA has to be terminated and (if necessary) replaced with a new SA.

If this object is zero, then there is no default value for lifetime."

DEFVAL { 28800 } -- 8 hours (in units of seconds)

::= { t11FcSpAuEntityEntry 7 }

t11FcSpAuDefaultLifetimeUnits OBJECT-TYPE

SYNTAX T11FcSpLifetimeLeftUnits

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"The units in which the value of the corresponding instance of t11FcSpAuDefaultLifetime specifies a



default lifetime for a Security Association which has no explicitly-specified value for its lifetime."

DEFVAL { seconds }

::= { t11FcSpAuEntityEntry 8 }

#### t11FcSpAuRejectMaxRows OBJECT-TYPE

SYNTAX Unsigned32 (0..1000)

MAX-ACCESS read-write

STATUS current

##### DESCRIPTION

"The maximum number of rows in the t11FcSpAuRejectTable for this entity on this Fabric. If and when an AUTH message is rejected and the t11FcSpAuRejectTable already contains this maximum number of rows for the specific entity and Fabric, the row containing the oldest information is discarded and replaced by a row containing information about the new rejection.

There will be less than this maximum number of rows in the t11FcSpAuRejectTable in exceptional circumstances, e.g., after an agent restart.

In an implementation which does not support the t11FcSpAuRejectTable, this object will always be zero."

::= { t11FcSpAuEntityEntry 9 }

#### t11FcSpAuDhChapHashFunctions OBJECT-TYPE

SYNTAX T11FcSpHashFunctions

MAX-ACCESS read-only

STATUS current

##### DESCRIPTION

"The hash functions which the entity supports when using the DH-CHAP algorithm."

::= { t11FcSpAuEntityEntry 10 }

#### t11FcSpAuDhChapDhGroups OBJECT-TYPE

SYNTAX T11FcSpDhGroups

MAX-ACCESS read-only

STATUS current

##### DESCRIPTION

"The DH Groups which the entity supports when using the DH-CHAP algorithm in FC-SP."

::= { t11FcSpAuEntityEntry 11 }

#### t11FcSpAuFcapHashFunctions OBJECT-TYPE

SYNTAX          T11FcSpHashFunctions  
MAX-ACCESS read-only  
STATUS          current  
DESCRIPTION  
    "The hash functions which the entity supports when  
    specified as Protocol Parameters in the AUTH\_Negotiate  
    message for FCAP in FC-SP."

REFERENCE  
    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
    Fibre Channel - Security Protocols (FC-SP),  
    February 2007, [section 5.5.2.1](#) and table 28."  
::= { t11FcSpAuEntityEntry 12 }

t11FcSpAuFcapCertsSignFunctions OBJECT-TYPE

SYNTAX          T11FcSpSignFunctions  
MAX-ACCESS read-only  
STATUS          current  
DESCRIPTION  
    "The signature functions used within certificates which  
    the entity supports when using FCAP in FC-SP."

REFERENCE  
    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
    Fibre Channel - Security Protocols (FC-SP),  
    February 2007, [section 5.5.4.2](#) and tables 38 & 39."  
::= { t11FcSpAuEntityEntry 13 }

t11FcSpAuFcapDhGroups OBJECT-TYPE

SYNTAX          T11FcSpDhGroups  
MAX-ACCESS read-only  
STATUS          current  
DESCRIPTION  
    "The DH Groups which the entity supports when using the  
    FCAP algorithm in FC-SP."  
::= { t11FcSpAuEntityEntry 14 }

t11FcSpAuFcapHashFunctions OBJECT-TYPE

SYNTAX          T11FcSpHashFunctions  
MAX-ACCESS read-only  
STATUS          current  
DESCRIPTION  
    "The hash functions which the entity supports when using

```
        the FCPAP algorithm in FC-SP."
 ::= { t11FcSpAuEntityEntry 15 }
```

t11FcSpAuFcpapDhGroups OBJECT-TYPE

Expires 11 January 2009

[Page 45]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```
SYNTAX      T11FcSpDhGroups
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The DH Groups which the entity supports when using the
    FCPAP algorithm in FC-SP."
 ::= { t11FcSpAuEntityEntry 16 }
```

```
--
-- The Mapping of Authentication Entities onto Interfaces
-- and Statistics
--
```

t11FcSpAuIfStatTable OBJECT-TYPE

```
SYNTAX      SEQUENCE OF T11FcSpAuIfStatEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "Each FC-SP Authentication entity can operate on one or more
    interfaces, but at most one of them can operate on each
    interface. A row in this table exists for each interface
    to each Fabric on which each Authentication entity operates.

    The objects within this table contain statistics information
    related to FC-SP's Authentication Protocols."
 ::= { t11FcSpAuMIBObjects 2 }
```

t11FcSpAuIfStatEntry OBJECT-TYPE

```
SYNTAX      T11FcSpAuIfStatEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "A set of Authentication Protocols statistics for an FC-SP
    Authentication entity (identified by t11FcSpAuEntityName) on
```

one of its interfaces to a particular Fabric, which is managed within the Fibre Channel management instance identified by fcmInstanceIndex."

```
INDEX    { fcmInstanceIndex, t11FcSpAuEntityName,
           t11FcSpAuIfStatInterfaceIndex,
           t11FcSpAuIfStatFabricIndex }
 ::= { t11FcSpAuIfStatTable 1 }
```

```
T11FcSpAuIfStatEntry ::= SEQUENCE {
    t11FcSpAuIfStatInterfaceIndex    InterfaceIndex,
```

Expires 11 January 2009

[Page 46]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```
    t11FcSpAuIfStatFabricIndex          T11FabricIndex,
    t11FcSpAuIfStatTimeouts             Counter32,
    t11FcSpAuIfStatInAcceptedMsgs       Counter32,
    t11FcSpAuIfStatInLsSwRejectedMsgs   Counter32,
    t11FcSpAuIfStatInAuthRejectedMsgs   Counter32,
    t11FcSpAuIfStatOutAcceptedMsgs      Counter32,
    t11FcSpAuIfStatOutLsSwRejectedMsgs  Counter32,
    t11FcSpAuIfStatOutAuthRejectedMsgs  Counter32
}
```

t11FcSpAuIfStatInterfaceIndex OBJECT-TYPE

```
SYNTAX      InterfaceIndex
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
```

"The interface on which the FC-SP Authentication entity operates and for which the statistics are collected."

```
::= { t11FcSpAuIfStatEntry 1 }
```

t11FcSpAuIfStatFabricIndex OBJECT-TYPE

```
SYNTAX      T11FabricIndex
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
```

"A index value identifying the particular Fabric for which the statistics are collected."

```
::= { t11FcSpAuIfStatEntry 2 }
```

t11FcSpAuIfStatTimeouts OBJECT-TYPE

SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION

"The number of FC-SP Authentication Protocol messages sent by the particular entity on the particular Fabric on the particular interface, for which no response was received within a timeout period.

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

REFERENCE

"Fibre Channel - Security Protocols (FC-SP),  
T11/Project 1570-D/Rev 1.8, June 2006, [section 5.11](#)."

::= { t11FcSpAuIfStatEntry 3 }

Expires 11 January 2009

[Page 47]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

t11FcSpAuIfStatInAcceptedMsgs OBJECT-TYPE

SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION

"The number of FC-SP Authentication Protocol messages received and accepted by the particular entity on the particular Fabric on the particular interface.

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

REFERENCE

"Fibre Channel - Security Protocols (FC-SP),  
T11/Project 1570-D/Rev 1.8, June 2006, [section 5.1](#)."

::= { t11FcSpAuIfStatEntry 4 }

t11FcSpAuIfStatInLsSwRejectedMsgs OBJECT-TYPE

SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION

"The number of FC-SP Authentication Protocol messages received by the particular entity on the particular Fabric

on particular interface, and rejected by a lower-level (SW\_RJT or LS\_RJT) reject.

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

REFERENCE

"Fibre Channel - Security Protocols (FC-SP),  
T11/Project 1570-D/Rev 1.8, June 2006, [section 5.1](#)."

::= { t11FcSpAuIfStatEntry 5 }

t11FcSpAuIfStatInAuthRejectedMsgs OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of FC-SP Authentication Protocol messages received by the particular entity on the particular Fabric on particular interface, and rejected by an AUTH\_Reject message.

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

Expires 11 January 2009

[Page 48]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

REFERENCE

"Fibre Channel - Security Protocols (FC-SP),  
T11/Project 1570-D/Rev 1.8, June 2006, [section 5.1](#)."

::= { t11FcSpAuIfStatEntry 6 }

t11FcSpAuIfStatOutAcceptedMsgs OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of FC-SP Authentication Protocol messages sent by the particular entity on the particular Fabric on the particular interface, which were accepted by the neighbouring entity, i.e., not rejected by an AUTH\_Reject message, nor by a lower-level (SW\_RJT or LS\_RJT) reject.

This counter has no discontinuities other than those

which all Counter32's have when sysUpTime=0."  
REFERENCE  
"Fibre Channel - Security Protocols (FC-SP),  
T11/Project 1570-D/Rev 1.8, June 2006, [section 5.1](#)."  
::= { t11FcSpAuIfStatEntry 7 }

t11FcSpAuIfStatOutLsSwRejectedMsgs OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of FC-SP Authentication Protocol messages sent by the particular entity on the particular Fabric on the particular interface, which were rejected by a lower-level (SW\_RJT or LS\_RJT) reject.

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

REFERENCE  
"Fibre Channel - Security Protocols (FC-SP),  
T11/Project 1570-D/Rev 1.8, June 2006, [section 5.1](#)."  
::= { t11FcSpAuIfStatEntry 8 }

t11FcSpAuIfStatOutAuthRejectedMsgs OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

Expires 11 January 2009

[Page 49]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

"The number of FC-SP Authentication Protocol messages sent by the particular entity on the particular Fabric on the particular interface, which were rejected by an AUTH\_Reject message.

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

REFERENCE  
"Fibre Channel - Security Protocols (FC-SP),  
T11/Project 1570-D/Rev 1.8, June 2006, [section 5.1](#)."  
::= { t11FcSpAuIfStatEntry 9 }

--  
-- Information about Authentication Protocol Transactions  
-- which were recently rejected  
--

t11FcSpAuRejectTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpAuRejectEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of volatile information about FC-SP Authentication Protocol transactions which were recently rejected with an AUTH\_Reject message, or with an SW\_RJT/LS\_RJT.

The maximum number of rows in this table for a specific entity on a specific Fabric is given by the value of the corresponding instance of t11FcSpAuRejectMaxRows.

The syntax of t11FcSpAuRejTimestamp is TimeStamp, and thus its value rolls-over to zero after approximately 497 days. To avoid any confusion due to such a roll-over, rows should be deleted from this table before they are 497 days old.

This table will be empty if no AUTH\_Reject messages, nor any SW\_RJT/LS\_RJT's rejecting an AUTH message, have been sent or received since the last re-initialization of the agent."

::= { t11FcSpAuMIBObjects 3 }

t11FcSpAuRejectEntry OBJECT-TYPE

SYNTAX T11FcSpAuRejectEntry

MAX-ACCESS not-accessible

Expires 11 January 2009

[Page 50]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

STATUS            current

DESCRIPTION

"Information about one AUTH message (either an AUTH\_ELS or an AUTH\_ILS) which was rejected with an AUTH\_Reject, SW\_RJT or LS\_RJT message, sent/received by



the entity identified by values of fcmInstanceIndex and t11FcSpAuEntityName, on an interface to a particular Fabric."

```
INDEX    { fcmInstanceIndex, t11FcSpAuEntityName,
           t11FcSpAuRejInterfaceIndex, t11FcSpAuRejFabricIndex,
           t11FcSpAuRejTimestamp }
 ::= { t11FcSpAuRejectTable 1 }
```

```
T11FcSpAuRejectEntry ::= SEQUENCE {
    t11FcSpAuRejInterfaceIndex    InterfaceIndex,
    t11FcSpAuRejFabricIndex       T11FabricIndex,
    t11FcSpAuRejTimestamp         TimeStamp,
    t11FcSpAuRejDirection         INTEGER,
    t11FcSpAuRejType              INTEGER,
    t11FcSpAuRejAuthMsgString     OCTET STRING,
    t11FcSpAuRejReasonCode        T11FcSpAuthRejectReasonCode,
    t11FcSpAuRejReasonCodeExp     T11FcSpAuthRejReasonCodeExp
}
```

```
t11FcSpAuRejInterfaceIndex OBJECT-TYPE
    SYNTAX      InterfaceIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The interface on which the rejected AUTH message was
        sent or received."
    ::= { t11FcSpAuRejectEntry 1 }
```

```
t11FcSpAuRejFabricIndex OBJECT-TYPE
    SYNTAX      T11FabricIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A index value identifying the particular Fabric on
        which the rejected AUTH message was sent or received."
    ::= { t11FcSpAuRejectEntry 2 }
```

```
t11FcSpAuRejTimestamp OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  not-accessible
```

STATUS           current  
DESCRIPTION  
    "The time at which the AUTH message was rejected. If two rows have the same value of this object for the same entity on the same interface and Fabric, the value of this object for the later one is incremented by one."  
::= { t11FcSpAuRejectEntry 3 }

t11FcSpAuRejDirection OBJECT-TYPE  
SYNTAX           INTEGER { sent(1), received(2) }  
MAX-ACCESS       read-only  
STATUS           current  
DESCRIPTION  
    "An indication of whether the rejection was sent or received by the identified entity.  
  
    The value 'sent(1)' corresponds to a notification of type t11FcSpAuRejectSentNotify; the value 'received(2)' corresponds to t11FcSpAuRejectReceivedNotify."  
::= { t11FcSpAuRejectEntry 4 }

t11FcSpAuRejType OBJECT-TYPE  
SYNTAX           INTEGER {  
                    authReject(1),  
                    swRjt(2),  
                    lsRjt(3)  
                  }  
MAX-ACCESS       read-only  
STATUS           current  
DESCRIPTION  
    "An indication of whether the rejection was an AUTH\_Reject, an SW\_RJT or an LS\_RJT."  
::= { t11FcSpAuRejectEntry 5 }

t11FcSpAuRejAuthMsgString OBJECT-TYPE  
SYNTAX           OCTET STRING (SIZE(0..255))  
MAX-ACCESS       read-only  
STATUS           current  
DESCRIPTION  
    "The binary content of the AUTH message which was rejected, formatted as an octet string (in network byte order) containing the content of the message.  
  
    If the binary content is unavailable, then the length is zero. Otherwise, the first octet of the

message identifies the type of message:

'90'h - an AUTH\_ELS, see Table 6 in FC-SP,  
'40'h - an AUTH\_ILS, see Table 3 in FC-SP, or  
'41'h - an B\_AUTH\_ILS, see Table 5 in FC-SP.

and the remainder of the message may be truncated."

#### REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, Tables 3, 5 and 6."

::= { t11FcSpAuRejectEntry 6 }

#### t11FcSpAuRejReasonCode OBJECT-TYPE

SYNTAX            T11FcSpAuthRejectReasonCode

MAX-ACCESS      read-only

STATUS           current

#### DESCRIPTION

"The reason code with which this AUTH message was  
rejected."

#### REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, Table 17, 48, 52."

::= { t11FcSpAuRejectEntry 7 }

#### t11FcSpAuRejReasonCodeExp OBJECT-TYPE

SYNTAX            T11FcSpAuthRejReasonCodeExp

MAX-ACCESS      read-only

STATUS           current

#### DESCRIPTION

"The reason code explanation with which this AUTH  
message was rejected."

#### REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, Table 17, 48, 52."

::= { t11FcSpAuRejectEntry 8 }

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--  
-- Notifications  
--

**t11FcSpAuRejectSentNotify NOTIFICATION-TYPE**

OBJECTS    { t11FamLocalSwitchWwn,  
              t11FcSpAuRejAuthMsgString,  
              t11FcSpAuRejType,  
              t11FcSpAuRejReasonCode,  
              t11FcSpAuRejReasonCodeExp }

STATUS        current

**DESCRIPTION**

"This notification indicates that a Switch (identified by the value of t11FamLocalSwitchWwn) has sent a reject message of the type indicated by t11FcSpAuRejType in response to an AUTH message.

The content of the rejected AUTH message is given by the value of t11FcSpAuRejAuthMsgString. The values of the Reason Code and Reason Code Explanation in the AUTH\_Reject/SW\_RJT/LS\_RJT are indicated by the values of t11FcSpAuRejReasonCode and t11FcSpAuRejReasonCodeExp."

::= { t11FcSpAuMIBNotifications 1 }

**t11FcSpAuRejectReceivedNotify NOTIFICATION-TYPE**

OBJECTS    { t11FamLocalSwitchWwn,  
              t11FcSpAuRejAuthMsgString,  
              t11FcSpAuRejType,  
              t11FcSpAuRejReasonCode,  
              t11FcSpAuRejReasonCodeExp }

STATUS        current

**DESCRIPTION**

"This notification indicates that a Switch (identified by the value of t11FamLocalSwitchWwn) has received a reject message of the type indicated by t11FcSpAuRejType in response to an AUTH message.

The content of the rejected AUTH message is given by the value of t11FcSpAuRejAuthMsgString. The values of the Reason Code and Reason Code Explanation in the AUTH\_Reject/SW\_RJT/LS\_RJT are indicated by the values of t11FcSpAuRejReasonCode and t11FcSpAuRejReasonCodeExp."

```
::= { t11FcSpAuMIBNotifications 2 }
```

Expires 11 January 2009

[Page 54]

---

Internet Draft      Fibre-Channel Security Protocols MIB      July 2008

--  
-- Conformance  
--

```
t11FcSpAuMIBCompliances
    OBJECT IDENTIFIER ::= { t11FcSpAuMIBConformance 1 }
t11FcSpAuMIBGroups
    OBJECT IDENTIFIER ::= { t11FcSpAuMIBConformance 2 }
```

```
t11FcSpAuMIBCompliance MODULE-COMPLIANCE
    STATUS          current
    DESCRIPTION
        "The compliance statement for entities which
        implement one or more of the Authentication Protocols
        defined in FC-SP."
```

```
MODULE -- this module
    MANDATORY-GROUPS { t11FcSpAuGeneralGroup,
                        t11FcSpAuRejectedGroup,
                        t11FcSpAuNotificationGroup }
```

```
GROUP          t11FcSpAuIfStatsGroup
DESCRIPTION
    "These counters, of particular FC-SP messages and
    events, are mandatory only for those systems that
    count such messages/events."
```

-- Write access is not required for any objects in this MIB module:

```
OBJECT          t11FcSpAuStorageType
MIN-ACCESS      read-only
```

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpAuSendRejNotifyEnable

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpAuRcvRejNotifyEnable

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpAuDefaultLifetime

Expires 11 January 2009

[Page 55]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpAuDefaultLifetimeUnits

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpAuRejectMaxRows

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

::= { t11FcSpAuMIBCompliances 1 }

-- Units of Conformance

t11FcSpAuGeneralGroup OBJECT-GROUP

OBJECTS { t11FcSpAuServerProtocol,  
t11FcSpAuStorageType,  
t11FcSpAuSendRejNotifyEnable,  
t11FcSpAuRcvRejNotifyEnable,  
t11FcSpAuDefaultLifetime,

```

        t11FcSpAuDefaultLifetimeUnits,
        t11FcSpAuRejectMaxRows,
        t11FcSpAuDhChapHashFunctions,
        t11FcSpAuDhChapDhGroups,
        t11FcSpAuFcapHashFunctions,
        t11FcSpAuFcapCertsSignFunctions,
        t11FcSpAuFcapDhGroups,
        t11FcSpAuFcapHashFunctions,
        t11FcSpAuFcapDhGroups,
        t11FcSpAuIfStatTimeouts }
STATUS    current
DESCRIPTION
    "A collection of objects for the capabilities and
    configuration parameters of FC-SP's Authentication
    Protocols. The inclusion of t11FcSpAuIfStatTimeouts
    in this group provides information on mappings of
    Authentication entities onto interfaces."
::= { t11FcSpAuMIBGroups 1 }

```

t11FcSpAuIfStatsGroup OBJECT-GROUP

Expires 11 January 2009

[Page 56]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```

OBJECTS { t11FcSpAuIfStatInAcceptedMsgs,
          t11FcSpAuIfStatInLsSwRejectedMsgs,
          t11FcSpAuIfStatInAuthRejectedMsgs,
          t11FcSpAuIfStatOutAcceptedMsgs,
          t11FcSpAuIfStatOutLsSwRejectedMsgs,
          t11FcSpAuIfStatOutAuthRejectedMsgs }
STATUS    current
DESCRIPTION
    "A collection of objects for monitoring the
    operations of FC-SP's Authentication Protocols."
::= { t11FcSpAuMIBGroups 2 }

```

t11FcSpAuRejectedGroup OBJECT-GROUP

```

OBJECTS { t11FcSpAuRejDirection,
          t11FcSpAuRejType,
          t11FcSpAuRejAuthMsgString,
          t11FcSpAuRejReasonCode,
          t11FcSpAuRejReasonCodeExp }
STATUS    current

```

```

DESCRIPTION
    "A collection of objects holding information concerning
    FC-SP Authentication Protocol transactions which were
    recently rejected with an AUTH_Reject, with an SW_RJT,
    or with an LS_RJT."
 ::= { t11FcSpAuMIBGroups 3 }

t11FcSpAuNotificationGroup NOTIFICATION-GROUP
    NOTIFICATIONS { t11FcSpAuRejectSentNotify,
                    t11FcSpAuRejectReceivedNotify }
    STATUS      current
    DESCRIPTION
        "A collection of notifications for use in the management
        of FC-SP's Authentication Protocols."
 ::= { t11FcSpAuMIBGroups 4 }

END

```

Expires 11 January 2009

[Page 57]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

### [6.3.](#) The T11-FC-SP-ZONING-MIB Module

```

--*****
-- FC-SP Zoning
--

T11-FC-SP-ZONING-MIB  DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE,
    NOTIFICATION-TYPE, mib-2,
    Counter32

```



```

                                FROM SNMPv2-SMI                -- [RFC2578]
TruthValue                     FROM SNMPv2-TC                -- [RFC2579]
MODULE-COMPLIANCE, OBJECT-GROUP,
NOTIFICATION-GROUP
                                FROM SNMPv2-CONF              -- [RFC2580]
ifIndex                        FROM IF-MIB                   -- [RFC2863]
t11ZsServerEntry,
t11ZsStatsEntry,
t11ZsNotifyControlEntry,
t11ZsFabricIndex      FROM T11-FC-ZONE-SERVER-MIB    -- [RFC4936]
T11FcSpPolicyHashValue,
T11FcSpPolicyHashFormat,
T11FcSpHashCalculationStatus
                                FROM T11-FC-SP-TC-MIB;

t11FcSpZoningMIB  MODULE-IDENTITY
LAST-UPDATED      "200801030000Z"
ORGANIZATION      "This MIB module was developed through the
coordinated effort of two organizations:
T11 began the development and the IETF (in
the IMSS Working Group) finished it."

CONTACT-INFO
    "
        Claudio DeSanti
        Cisco Systems, Inc.
        170 West Tasman Drive
        San Jose, CA 95134 USA
        EMail: cds@cisco.com

        Keith McCloghrie
        Cisco Systems, Inc.
        170 West Tasman Drive
        San Jose, CA 95134 USA

```

Expires 11 January 2009

[Page 58]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

Email: kzm@cisco.com"

#### DESCRIPTION

"This MIB module specifies the extensions to the T11-FC-ZONE-SERVER-MIB module which are necessary for the management of Fibre Channel's FC-SP Zoning Servers, as defined in the FC-SP specification.

The persistence of values written to these MIB objects is the same as the persistence of the objects they extend, i.e., it is given by the value of the relevant instance of t11ZsServerDatabaseStorageType (defined in the T11-FC-ZONE-SERVER-MIB module).

Copyright (C) The IETF Trust (2008). This version of this MIB module is part of RFC yyyy; see the RFC itself for full legal notices."

-- RFC Editor: replace yyyy with actual RFC number & remove this note  
REVISION "200801030000Z"  
DESCRIPTION  
    "Initial version of this MIB module, published as RFCyyyy."  
-- RFC-Editor, replace yyyy with actual RFC number & remove this note  
    ::= { mib-2 nnn } -- to be assigned by IANA  
-- RFC Editor: replace nnn with IANA-assigned number & remove this note

t11FcSpZsMIBNotifications OBJECT IDENTIFIER ::= { t11FcSpZoningMIB 0 }  
t11FcSpZsMIBObjects OBJECT IDENTIFIER ::= { t11FcSpZoningMIB 1 }  
t11FcSpZsMIBConformance OBJECT IDENTIFIER ::= { t11FcSpZoningMIB 2 }  
t11FcSpZsConfiguration OBJECT IDENTIFIER ::= { t11FcSpZsMIBObjects 1 }  
t11FcSpZsStatistics OBJECT IDENTIFIER ::= { t11FcSpZsMIBObjects 2 }

--  
-- Augmenting the table of Zone Servers  
--

t11FcSpZsServerTable OBJECT-TYPE  
    SYNTAX SEQUENCE OF T11FcSpZsServerEntry  
    MAX-ACCESS not-accessible  
    STATUS current  
    DESCRIPTION  
        "A table which provides FC-SP-specific information about  
        the Zone Servers on each Fabric in one or more Switches."  
    ::= { t11FcSpZsConfiguration 1 }

t11FcSpZsServerEntry OBJECT-TYPE

```

MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION
    "Each entry contains information relevant to FC-SP
    for a particular Zone Server for a particular Fabric
    on a particular Switch. The Fabric and Switch are
    identified in the same manner as in t11ZsServerEntry."
AUGMENTS      { t11ZsServerEntry }
::= { t11FcSpZsServerTable 1 }

```

```

T11FcSpZsServerEntry ::= SEQUENCE {
    t11FcSpZsServerCapabilityObject    BITS,
    t11FcSpZsServerEnabled              TruthValue,
    t11FcSpZoneSetHashStatus            T11FcSpHashCalculationStatus,
    t11FcSpActiveZoneSetHashType        T11FcSpPolicyHashFormat,
    t11FcSpActiveZoneSetHash            T11FcSpPolicyHashValue,
    t11FcSpZoneSetDatabaseHashType      T11FcSpPolicyHashFormat,
    t11FcSpZoneSetDatabaseHash          T11FcSpPolicyHashValue
}

```

t11FcSpZsServerCapabilityObject OBJECT-TYPE

```

SYNTAX        BITS {
                fcSpZoning(0)
            }

```

```

MAX-ACCESS    read-only
STATUS        current

```

DESCRIPTION

"Capabilities of the Zone Server for the particular Fabric on the particular Switch, with respect to FC-SP Zoning:

fcSpZoning -- set to 1 to indicate the Switch is capable of supporting FC-SP Zoning.

"

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, Table 184."

```

::= { t11FcSpZsServerEntry 1 }

```

t11FcSpZsServerEnabled OBJECT-TYPE

```

SYNTAX        TruthValue

```

```

MAX-ACCESS    read-write

```

```

STATUS        current

```

DESCRIPTION

"This object indicates whether the Zone Server for the particular Fabric on the particular Switch, is operating in FC-SP Zoning mode."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, Table 185."

::= { t11FcSpZsServerEntry 2 }

## t11FcSpZoneSetHashStatus OBJECT-TYPE

SYNTAX T11FcSpHashCalculationStatus

MAX-ACCESS read-write

STATUS current

## DESCRIPTION

"When read, the value of this object is either:

correct -- the corresponding instances of both  
t11FcSpActiveZoneSetHash and  
t11FcSpZoneSetDatabaseHash contain  
the correct hash values; or  
stale -- the corresponding instances of  
t11FcSpActiveZoneSetHash and  
t11FcSpZoneSetDatabaseHash contain  
stale (possibly incorrect) values;

Writing a value of 'calculate' is a request to re-calculate and update the values of the corresponding instances of both t11FcSpActiveZoneSetHash and t11FcSpZoneSetDatabaseHash. Writing a value of 'correct' or 'stale' to this object is an error (e.g., 'wrongValue').

When the Active Zone Set and/or the Zone Set Database are updated, it is common that multiple changes need to be made at the same time. In such circumstances, the use of this object allows the hash values to be updated only once after all changes, rather than repeatedly/after each individual change.

If and when the corresponding instance of t11ZsServerDatabaseStorageType has the value 'permanent(4)', then if write access is supported to any instance of a read-write object in any row of any table governed by the 'permanent' value of t11ZsServerDatabaseStorageType, then write access to the corresponding instance of this object must also be supported."

## REFERENCE

"t11ZsServerDatabaseStorageType in  
'Fibre Channel Zone Server MIB', [RFC 4936](#), August 2007."

DEFVAL            { stale }

::= { t11FcSpZsServerEntry 3 }

## t11FcSpActiveZoneSetHashType OBJECT-TYPE

SYNTAX            T11FcSpPolicyHashFormat

MAX-ACCESS       read-only

STATUS            current

## DESCRIPTION

"The format used for the hash value contained in the  
corresponding instance of t11FcSpActiveZoneSetHash."

::= { t11FcSpZsServerEntry 4 }

## t11FcSpActiveZoneSetHash OBJECT-TYPE

SYNTAX            T11FcSpPolicyHashValue

MAX-ACCESS       read-only

STATUS            current

## DESCRIPTION

"The value of the hash for the current Active Zone Set.  
The format of this value is given by the corresponding  
instance of t11FcSpActiveZoneSetHashType."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, Table 187."

::= { t11FcSpZsServerEntry 5 }

## t11FcSpZoneSetDatabaseHashType OBJECT-TYPE

SYNTAX            T11FcSpPolicyHashFormat

MAX-ACCESS       read-only

STATUS            current

## DESCRIPTION

"The format used for the hash value contained in the  
corresponding instance of t11FcSpZoneSetDatabaseHash."

::= { t11FcSpZsServerEntry 6 }

## t11FcSpZoneSetDatabaseHash OBJECT-TYPE

SYNTAX            T11FcSpPolicyHashValue

MAX-ACCESS       read-only

STATUS current

DESCRIPTION

"The value of the hash for the current Zone Set Database.  
The format of this value is given by the corresponding

Expires 11 January 2009

[Page 62]

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

instance of t11FcSpZoneSetDatabaseHashType."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, Table 187."

::= { t11FcSpZsServerEntry 7 }

--

-- Additional Statistics for FC-SP Zoning

--

t11FcSpZsStatsTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpZsStatsEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of statistics specific to FC-SP which are  
maintained by Zone Servers."

::= { t11FcSpZsStatistics 1 }

t11FcSpZsStatsEntry OBJECT-TYPE

SYNTAX T11FcSpZsStatsEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A set of statistics specific to FC-SP for a particular  
Zone Server for a particular Fabric on a particular Switch.  
The Fabric and Switch are identified in the same manner as  
in t11ZsStatsEntry."

AUGMENTS { t11ZsStatsEntry }

::= { t11FcSpZsStatsTable 1 }

T11FcSpZsStatsEntry ::= SEQUENCE {

t11FcSpZsSPCMITrequestsSent Counter32,

t11FcSpZsSPCMITrequestsAccepted Counter32,

```

t11FcSpZsSPCMITrequestsRejected Counter32,
t11FcSpZsZcpRequestsSent Counter32,
t11FcSpZsZcpRequestsAccepted Counter32,
t11FcSpZsZcpRequestsRejected Counter32,
t11FcSpZsZirRequestsAccepted Counter32,
t11FcSpZsZirRequestsRejected Counter32
}

```

```

t11FcSpZsSPCMITrequestsSent OBJECT-TYPE
    SYNTAX Counter32

```

Expires 11 January 2009

[Page 63]

---

Internet Draft      Fibre-Channel Security Protocols MIB      July 2008

```

MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of SP Commit Zone Changes (SPCMIT) operation
    requests sent by the Zone Server.

    This counter has no discontinuities other than those
    which all Counter32's have when sysUpTime=0."
 ::= { t11FcSpZsStatsEntry 1 }

```

```

t11FcSpZsSPCMITrequestsAccepted OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of SP Commit Zone Changes (SPCMIT) operation
        requests received and accepted by the Zone Server.

        This counter has no discontinuities other than those
        which all Counter32's have when sysUpTime=0."
 ::= { t11FcSpZsStatsEntry 2 }

```

```

t11FcSpZsSPCMITrequestsRejected OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of SP Commit Zone Changes (SPCMIT) operation
        requests received but rejected by the Zone Server.

```

This counter has no discontinuities other than those  
which all Counter32's have when sysUpTime=0."  
 ::= { t11FcSpZsStatsEntry 3 }

t11FcSpZsZcpRequestsSent OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of Zoning Check Protocol (ZCP) requests sent  
by the Zone Server.

This counter has no discontinuities other than those  
which all Counter32's have when sysUpTime=0."  
 ::= { t11FcSpZsStatsEntry 4 }

Expires 11 January 2009

[Page 64]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpZsZcpRequestsAccepted OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of Zoning Check Protocol (ZCP) requests received  
and accepted by the Zone Server.

This counter has no discontinuities other than those  
which all Counter32's have when sysUpTime=0."  
 ::= { t11FcSpZsStatsEntry 5 }

t11FcSpZsZcpRequestsRejected OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of Zoning Check Protocol (ZCP) requests received  
but rejected by the Zone Server.

This counter has no discontinuities other than those  
which all Counter32's have when sysUpTime=0."  
 ::= { t11FcSpZsStatsEntry 6 }



t11FcSpZsZirRequestsAccepted OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of Zoning Information Request (ZIR) requests received and accepted by the Zone Server.

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

::= { t11FcSpZsStatsEntry 7 }

t11FcSpZsZirRequestsRejected OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of Zoning Information Request (ZIR) requests received but rejected by the Zone Server.

This counter has no discontinuities other than those

Expires 11 January 2009

[Page 65]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

which all Counter32's have when sysUpTime=0."  
::= { t11FcSpZsStatsEntry 8 }

--

-- Enable/Disable for Notifications

--

t11FcSpZsNotifyControlTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpZsNotifyControlEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of control information for notifications generated due to Zone Server events related to FC-SP Zoning."

::= { t11FcSpZsConfiguration 2 }

```

t11FcSpZsNotifyControlEntry OBJECT-TYPE
    SYNTAX          T11FcSpZsNotifyControlEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "Each entry is an augmentation of the notification control
        information for a Zone Server for a particular Fabric on a
        particular Switch. The Fabric and Switch are identified in
        the same manner as in t11ZsNotifyControlEntry."
    AUGMENTS        { t11ZsNotifyControlEntry }
    ::= { t11FcSpZsNotifyControlTable 1 }

```

```

T11FcSpZsNotifyControlEntry ::= SEQUENCE {
    t11FcSpZsNotifyJoinSuccessEnable    TruthValue,
    t11FcSpZsNotifyJoinFailureEnable    TruthValue
}

```

```

t11FcSpZsNotifyJoinSuccessEnable OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object specifies whether
        t11FcSpZsFabricJoinFailureNotify notifications should be
        generated by the Zone Server for this Fabric."
    ::= { t11FcSpZsNotifyControlEntry 1 }

```

```

t11FcSpZsNotifyJoinFailureEnable OBJECT-TYPE

```

```

    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object specifies whether
        t11FcSpZsFabricJoinSuccessNotify notifications should be
        generated by the Zone Server for this Fabric."
    ::= { t11FcSpZsNotifyControlEntry 2 }

```

--

-- Notifications

--

t11FcSpZsFabricJoinSuccessNotify NOTIFICATION-TYPE

OBJECTS { ifIndex, t11ZsFabricIndex }

STATUS current

DESCRIPTION

"This notification indicates that a Switch which is part of one Fabric (indicated by the value of t11ZsFabricIndex) has successfully joined (on the interface indicated by the value of ifIndex) with a Switch which is part of another Fabric.

If multiple Virtual Fabrics are configured on an interface, and all are successfully joined at the same time, and if the agent so chooses, then it can generate just one notification in which t11ZsFabricIndex has the value 4096."

::= { t11FcSpZsMIBNotifications 1 }

t11FcSpZsFabricJoinFailureNotify NOTIFICATION-TYPE

OBJECTS { ifIndex, t11ZsFabricIndex }

STATUS current

DESCRIPTION

"This notification indicates that an E\_Port on the local Switch has entered the Isolated state because a join between two Fabrics failed. The failure occurred on the local Fabric indicated by the value of t11ZsFabricIndex, on the interface indicated by the value of ifIndex.

If multiple Virtual Fabrics are configured on an interface, and all have a failure to join at the same time, and if the agent so chooses, then it can generate just one notification in which t11ZsFabricIndex has the value 4096."

::= { t11FcSpZsMIBNotifications 2 }

--

-- Conformance

--

```

                                OBJECT IDENTIFIER ::= { t11FcSpZsMIBConformance 1 }
t11FcSpZsMIBGroups  OBJECT IDENTIFIER ::= { t11FcSpZsMIBConformance 2 }

t11FcSpZsMIBCompliance MODULE-COMPLIANCE
    STATUS          current
    DESCRIPTION
        "The compliance statement for entities which
        implement the extensions specified in FC-SP for
        Fibre Channel's Zone Server."

    MODULE -- this module
        MANDATORY-GROUPS { t11FcSpZsObjectsGroup,
                            t11FcSpZsNotificationControlGroup,
                            t11FcSpZsNotificationGroup }

    GROUP          t11FcSpZsStatisticsGroup
    DESCRIPTION
        "These counters, containing Zone Server statistics,
        are mandatory only for those systems which count
        such events."

-- Write access is not required for any objects in this MIB module:

    OBJECT          t11FcSpZsServerEnabled
    MIN-ACCESS      read-only
    DESCRIPTION
        "Write access is not required."

    OBJECT          t11FcSpZoneSetHashStatus
    MIN-ACCESS      read-only
    DESCRIPTION
        "Write access is not required."

    OBJECT          t11FcSpZsNotifyJoinSuccessEnable
    MIN-ACCESS      read-only
    DESCRIPTION
        "Write access is not required."

    OBJECT          t11FcSpZsNotifyJoinFailureEnable
    MIN-ACCESS      read-only

```

DESCRIPTION

"Write access is not required."

::= { t11FcSpZsMIBCompliances 1 }

-- Units of Conformance

t11FcSpZsObjectsGroup OBJECT-GROUP

OBJECTS { t11FcSpZsServerCapabilityObject,  
t11FcSpZsServerEnabled,  
t11FcSpZoneSetHashStatus,  
t11FcSpActiveZoneSetHashType,  
t11FcSpActiveZoneSetHash,  
t11FcSpZoneSetDatabaseHashType,  
t11FcSpZoneSetDatabaseHash  
}

STATUS current

DESCRIPTION

"A collection of objects for Zone configuration  
information of a Zone Server capable of  
operating in FC-SP Zoning mode."

::= { t11FcSpZsMIBGroups 1 }

t11FcSpZsNotificationControlGroup OBJECT-GROUP

OBJECTS { t11FcSpZsNotifyJoinSuccessEnable,  
t11FcSpZsNotifyJoinFailureEnable  
}

STATUS current

DESCRIPTION

"A collection of notification control objects for  
monitoring Zone Server failures specific to FC-SP."

::= { t11FcSpZsMIBGroups 2 }

t11FcSpZsStatisticsGroup OBJECT-GROUP

OBJECTS { t11FcSpZsSPCMITrequestsSent,  
t11FcSpZsSPCMITrequestsAccepted,  
t11FcSpZsSPCMITrequestsRejected,  
t11FcSpZsZcpRequestsSent,  
t11FcSpZsZcpRequestsAccepted,  
t11FcSpZsZcpRequestsRejected,  
t11FcSpZsZirRequestsAccepted,  
t11FcSpZsZirRequestsRejected  
}

STATUS current

DESCRIPTION

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```
        "A collection of objects for collecting Zone Server
          statistics which are specific to FC-SP."
 ::= { t11FcSpZsMIBGroups 3 }
```

```
t11FcSpZsNotificationGroup NOTIFICATION-GROUP
  NOTIFICATIONS { t11FcSpZsFabricJoinSuccessNotify,
                  t11FcSpZsFabricJoinFailureNotify
                  }
  STATUS          current
  DESCRIPTION
    "A collection of notification(s) for monitoring
     Zone Server events which are specific to FC-SP."
 ::= { t11FcSpZsMIBGroups 4 }
```

END

#### [6.4.](#) The T11-FC-SP-POLICY-MIB Module

```
--*****  
-- FC-SP Policy  
--
```

```
T11-FC-SP-POLICY-MIB  DEFINITIONS ::= BEGIN
```

##### IMPORTS

```
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, mib-2,  
    Counter32, Unsigned32  
        FROM SNMPv2-SMI                      -- [RFC2578]  
    RowStatus, StorageType, TimeStamp,  
    TruthValue          FROM SNMPv2-TC        -- [RFC2579]  
    MODULE-COMPLIANCE, OBJECT-GROUP,  
    NOTIFICATION-GROUP  
        FROM SNMPv2-CONF                      -- [RFC2580]  
    SnmpAdminString      FROM SNMP-FRAMEWORK-MIB -- [RFC3411]  
    InetAddress, InetPortNumber,  
    InetAddressType      FROM INET-ADDRESS-MIB -- [RFC4001]  
    fcmInstanceIndex,  
    FcNameIdOrZero,  
    FcDomainIdOrZero     FROM FC-MGMT-MIB      -- [RFC4044]  
    T11NsGs4RejectReasonCode  
        FROM T11-FC-NAME-SERVER-MIB          -- [RFC4438]  
    T11FabricIndex       FROM T11-TC-MIB       -- [RFC4439]  
    T11FcSpAlphaNumName,  
    T11FcSpAlphaNumNameOrAbsent,  
    T11FcSpPolicyName,  
    T11FcSpPolicyNameType,  
    T11FcSpPolicyObjectType,  
    T11FcSpPolicyHashFormat,  
    T11FcSpPolicyHashValue,  
    T11FcSpHashCalculationStatus FROM T11-FC-SP-TC-MIB;
```

```
t11FcSpPolicyMIB  MODULE-IDENTITY
```

LAST-UPDATED "200801030000Z"  
ORGANIZATION "This MIB module was developed through the  
coordinated effort of two organizations:  
T11 began the development and the IETF (in  
the IMSS Working Group) finished it."  
CONTACT-INFO  
" Claudio DeSanti  
Cisco Systems, Inc.

Expires 11 January 2009

[Page 71]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

170 West Tasman Drive  
San Jose, CA 95134 USA  
EMail: cds@cisco.com

Keith McCloghrie  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134 USA  
Email: kzm@cisco.com"

#### DESCRIPTION

"This MIB module specifies the management information required to manage Fabric Policies as defined by Fibre Channel's FC-SP specification.

FC-SP uses the term 'Policy Objects', sometimes abbreviated to just 'Objects', to refer to containers used to hold the data by which Fabric Policies are specified/stored. This obviously has the potential to cause confusion between 'Policy Objects' and 'MIB objects'. The DESCRIPTIONs in this MIB module attempt to avoid such confusion by the use of different adjectives and capitalization, even though such mechanisms are less effective when used in descriptors.

Some types of Policy Objects contain multiple items of information, each of which are held in the same format within the Policy Object. In such cases, FC-SP uses the term 'Entry' to describe each instance of the common format. For example, FC-SP defines an Attribute Policy Object as containing one or more 'Attribute Entries'. Again, this MIB module attempts to avoid confusion by the use of adjectives and capitalization to distinguish an Entry within a Policy



Object from an entry within a MIB table.

A Fabric's database of Policy Objects consists of a set of active Objects which are to be enforced by that Fabric, as well as non-active Objects which are not enforced.

Operations defined (in FC-SP) for Policy Management are:

- Add/Get/Remove operations on individual non-active Policy Objects,
- Activate/Deactivate operations on a Policy Summary Object, and
- Get operations on the active Policy Summary Object and/or on individual active Policy Objects.

Expires 11 January 2009

[Page 72]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

This MIB module has five parts:

- 1) Active Policy Objects - read-only MIB objects representing the set of active Policy Objects for each Fabric,
- 2) Activate/Deactivate Operations
  - a read-write MIB object to invoke an Activate operation of the policies specified via a non-active Policy Summary Object, and
  - a read-write MIB object to invoke a Deactivate operation.
- 3) Non-active Policy Objects
  - read-create MIB objects to allow the creation of non-active Policy Summary Objects (which reference non-active Policy Objects), and
  - read-create MIB objects representing non-active Policy Objects.
- 4) Statistics
- 5) Control information and Notifications

Copyright (C) The IETF Trust (2008). This version

```

        of this MIB module is part of RFC yyyy; see the RFC
        itself for full legal notices."
-- RFC Editor: replace yyyy with actual RFC number & remove this note
REVISION "200801030000Z"
DESCRIPTION
    "Initial version of this MIB module, published as RFCyyyyy."
-- RFC-Editor, replace yyyy with actual RFC number & remove this note
    ::= { mib-2 nnn } -- to be assigned by IANA
-- RFC Editor: replace nnn with IANA-assigned number & remove this note

t11FcSpPoMIBNotifications OBJECT IDENTIFIER ::= { t11FcSpPolicyMIB 0 }
t11FcSpPoMIBObjects       OBJECT IDENTIFIER ::= { t11FcSpPolicyMIB 1 }
t11FcSpPoMIBConformance  OBJECT IDENTIFIER ::= { t11FcSpPolicyMIB 2 }
t11FcSpPoActive          OBJECT IDENTIFIER ::= { t11FcSpPoMIBObjects 1 }
t11FcSpPoOperations       OBJECT IDENTIFIER ::= { t11FcSpPoMIBObjects 2 }
t11FcSpPoNonActive        OBJECT IDENTIFIER ::= { t11FcSpPoMIBObjects 3 }
t11FcSpPoStatistics       OBJECT IDENTIFIER ::= { t11FcSpPoMIBObjects 4 }
t11FcSpPoControl          OBJECT IDENTIFIER ::= { t11FcSpPoMIBObjects 5 }

```

Expires 11 January 2009

[Page 73]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```

--
-- Part 1 - Active Policy Objects
--

```

```

t11FcSpPoTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF T11FcSpPoEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table containing top-level information about active
        FC-SP policies on various Fabrics."
    ::= { t11FcSpPoActive 1 }

t11FcSpPoEntry OBJECT-TYPE
    SYNTAX          T11FcSpPoEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "Each entry contains information about active FC-SP policies

```

for a particular Fabric, managed as part of the Fibre  
Channel management instance identified by fcmInstanceIndex."  
INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex }  
::= { t11FcSpPoTable 1 }

T11FcSpPoEntry ::= SEQUENCE {  
    t11FcSpPoFabricIndex           T11FabricIndex,  
    t11FcSpPoPolicySummaryObjName T11FcSpAlphaNumName,  
    t11FcSpPoAdminFabricName       FcNameIdOrZero,  
    t11FcSpPoActivatedTimeStamp    TimeStamp  
}

t11FcSpPoFabricIndex OBJECT-TYPE  
    SYNTAX           T11FabricIndex  
    MAX-ACCESS       not-accessible  
    STATUS           current  
    DESCRIPTION  
        "An index value which uniquely identifies a particular  
        Fabric."  
    ::= { t11FcSpPoEntry 1 }

t11FcSpPoPolicySummaryObjName OBJECT-TYPE  
    SYNTAX           T11FcSpAlphaNumName  
    MAX-ACCESS       read-only  
    STATUS           current  
    DESCRIPTION

Expires 11 January 2009

[Page 74]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

    "The name of this Fabric's (active) Policy Summary Object."  
REFERENCE  
    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
    Fibre Channel - Security Protocols (FC-SP),  
    February 2007, [section 7.1.3](#) and table 104."  
    ::= { t11FcSpPoEntry 2 }

t11FcSpPoAdminFabricName OBJECT-TYPE  
    SYNTAX           FcNameIdOrZero (SIZE (8))  
    MAX-ACCESS       read-only  
    STATUS           current  
    DESCRIPTION  
        "The administratively-specified name for this Fabric, as

specified in the active Switch Membership List Object. This value is meaningful only when Static Domain\_IDs are in use in a Fabric (see FC-SW-4). Static Domain\_IDs are administratively enabled by a setting of the Switch Flags in each Switch Entry in the Switch Membership List Object. If Static Domain\_IDs are not in use, this value might be '0000000000000000'h.

The t11FamEnable, t11FamFabricName and t11FamConfigDomainIdType objects defined in the T11-FC-FABRIC-ADDR-MGR-MIB module are also concerned with the use of an administratively-specified name for a Fabric and Static Domain\_IDs. When FC-SP Policy is in use in a Fabric, the values of t11FamEnable, t11FamFabricName and t11FamConfigDomainIdType must be read-only and reflect the active Policy Objects. For example, the value of t11FamFabricName must reflect the value of t11FcSpPoAdminFabricName."

#### REFERENCE

- "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and table 108.
- Fibre Channel - Switch Fabric-4 (FC-SW-4), ANSI INCITS 418-2006, April 2006, [section 7.1](#).
- Fibre Channel Fabric Address Manager MIB', [RFC 4439](#), March 2006."

::= { t11FcSpPoEntry 3 }

t11FcSpPoActivatedTimeStamp OBJECT-TYPE

SYNTAX	TimeStamp
MAX-ACCESS	read-only
STATUS	current

Expires 11 January 2009

[Page 75]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

#### DESCRIPTION

"The value of sysUpTime at which this Fabric's Policy Summary Object was last activated, or zero if the same Policy Summary Object has been active since the last restart of the management system."

::= { t11FcSpPoEntry 4 }

--  
-- The table of Policy Summary Objects  
--

t11FcSpPoSummaryTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpPoSummaryEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of information about active Policy Objects listed within FC-SP Policy Summary Objects."

::= { t11FcSpPoActive 2 }

t11FcSpPoSummaryEntry OBJECT-TYPE

SYNTAX T11FcSpPoSummaryEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each entry contains information about one of the active Policy Objects listed within the Policy Summary Object for the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIdIndex.

How many Policy Objects of a given type can be active at any one time for a given Fabric depends on the type, as specified in FC-SP. For some types, it is one per Fabric; for other types, more than one can be active per Fabric. In both of these cases, the absence of any entries in this table for a particular type is equivalent to there being one Policy Object of that type which is empty, e.g., a Switch Membership List Object which identifies zero Switches."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.3](#) and table 104."

INDEX { fcmInstanceIdIndex, t11FcSpPoFabricIndex,  
t11FcSpPoSummaryPolicyNameType,

```

 ::= { t11FcSpPoSummaryTable 1 }

T11FcSpPoSummaryEntry ::= SEQUENCE {
    t11FcSpPoSummaryPolicyNameType T11FcSpPolicyNameType,
    t11FcSpPoSummaryPolicyName      T11FcSpPolicyName,
    t11FcSpPoSummaryPolicyType      T11FcSpPolicyObjectType,
    t11FcSpPoSummaryHashFormat      T11FcSpPolicyHashFormat,
    t11FcSpPoSummaryHashValue       T11FcSpPolicyHashValue
}

t11FcSpPoSummaryPolicyNameType OBJECT-TYPE
    SYNTAX      T11FcSpPolicyNameType {
                    nodeName(1),
                    alphaNumericName(7)
                }
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "The combination of t11FcSpPoSummaryPolicyNameType and
        t11FcSpPoSummaryPolicyName specify the name of the Policy
        Object contained in the Policy Summary Object.

        The type of name is 'nodeName' if the value of the
        corresponding instance of t11FcSpPoSummaryPolicyType is
        'switchConnectivity', or 'alphaNumericName' otherwise."
    ::= { t11FcSpPoSummaryEntry 1 }

t11FcSpPoSummaryPolicyName OBJECT-TYPE
    SYNTAX      T11FcSpPolicyName
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "The combination of t11FcSpPoSummaryPolicyNameType and
        t11FcSpPoSummaryPolicyName specify the name of the Policy
        Object contained in the Policy Summary Object."
    ::= { t11FcSpPoSummaryEntry 2 }

t11FcSpPoSummaryPolicyType OBJECT-TYPE
    SYNTAX      T11FcSpPolicyObjectType
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The 'Identifier' which specifies the type of this
        Policy Object."

```

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.3.1](#) and table 104."

::= { t11FcSpPoSummaryEntry 3 }

## t11FcSpPoSummaryHashFormat OBJECT-TYPE

SYNTAX T11FcSpPolicyHashFormat

MAX-ACCESS read-only

STATUS current

## DESCRIPTION

"The format of this Policy Object's hash value as  
contained in the corresponding instance of the  
t11FcSpPoSummaryHashValue object."

::= { t11FcSpPoSummaryEntry 4 }

## t11FcSpPoSummaryHashValue OBJECT-TYPE

SYNTAX T11FcSpPolicyHashValue

MAX-ACCESS read-only

STATUS current

## DESCRIPTION

"The hash value of this Policy Object, in the format  
identified by the corresponding instance of the  
t11FcSpPoSummaryHashFormat object."

::= { t11FcSpPoSummaryEntry 5 }

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--

-- Switch Entries in Active Switch Membership List Objects

--

t11FcSpPoSwMembTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpPoSwMembEntry

MAX-ACCESS      not-accessible

STATUS           current

DESCRIPTION

"A table of Switch Entries in active Switch Membership List Objects.

One Switch Membership List Object is represented by all of the rows of this table which have the same values of fcmInstanceIndex and t11FcSpPoFabricIndex."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 110."

::= { t11FcSpPoActive 3 }

t11FcSpPoSwMembEntry OBJECT-TYPE

SYNTAX            T11FcSpPoSwMembEntry

MAX-ACCESS      not-accessible

STATUS           current

DESCRIPTION

"Each entry contains information about one Switch Entry within the active Switch Membership List Object for the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,  
         t11FcSpPoSwMembSwitchNameType, t11FcSpPoSwMembSwitchName }

::= { t11FcSpPoSwMembTable 1 }

T11FcSpPoSwMembEntry ::= SEQUENCE {

t11FcSpPoSwMembSwitchNameType    T11FcSpPolicyNameType,

t11FcSpPoSwMembSwitchName        FcNameIdOrZero,

t11FcSpPoSwMembSwitchFlags       BITS,

t11FcSpPoSwMembDomainID          FcDomainIdOrZero,

t11FcSpPoSwMembPolicyDataRole    INTEGER,



```

t11FcSpPoSwMembAuthBehaviour    BITS,
t11FcSpPoSwMembAttribute        T11FcSpAlphaNumNameOrAbsent
}

```

Expires 11 January 2009

[Page 79]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpPoSwMembSwitchNameType OBJECT-TYPE

```

SYNTAX      T11FcSpPolicyNameType {
                nodeName(1),
                restrictedNodeName(2),
                wildcard(5),
                restrictedWildcard(6)
            }

```

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"If the value of this object is 'nodeName' or 'restrictedNodeName', then the combination of this object and t11FcSpPoSwMembSwitchName specify the Switch Name of this Switch Entry.

The membership is restricted or unrestricted based on the name type. Restricted membership means that the Switch is not allowed to be part of the Fabric unless allowed by a specific Switch Connectivity Object. Unrestricted membership means that the Switch is allowed to be part of the Fabric unless disallowed by a specific Switch Connectivity Object.

The values of 'wildcard' and 'restrictedWildcard' provide the means to specify whether to allow/deny membership for Switches not explicitly named in the Switch Membership List Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 110."

::= { t11FcSpPoSwMembEntry 1 }

t11FcSpPoSwMembSwitchName OBJECT-TYPE

```

SYNTAX      FcNameIdOrZero (SIZE (8))

```

MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION

"When the value of t11FcSpPoSwMembSwitchNameType is 'wildcard' or 'restrictedWildcard', this object has the value '0000000000000000'h.

Otherwise, the combination of t11FcSpPoSwMembSwitchNameType and this object specify the Switch Name of this Switch Entry."

Expires 11 January 2009

[Page 80]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 110."  
::= { t11FcSpPoSwMembEntry 2 }

t11FcSpPoSwMembSwitchFlags OBJECT-TYPE

SYNTAX            BITS {  
                  staticDomainID(0),  
                  insistentDomainID(1),  
                  serialPortsAccess(2),  
                  physicalPortsAccess(3),  
                  managerRole(4)  
                  }

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Configurable options in respect to the administration of Policy Objects at this Switch:

    'staticDomainID'        - if this bit is set, the Switch uses the 'Static Domain\_IDs behavior' (as defined in FC-SW-4). This bit needs to have the same setting for all Switches in a Fabric's Switch Membership List Object, or else the Fabric will partition. If this bit is set, the Domain\_ID for the Switch is given by the corresponding instance of t11FcSpPoSwMembDomainID.

    'insistentDomainID'    - if this bit is set, the

Switch uses the 'Insistent Domain\_ID behavior' (see t11FamConfigDomainId of T11-FC-FABRIC-ADDR-MGR-MIB), the Domain\_ID for the Switch is given by the corresponding instance of t11FcSpPoSwMembDomainID.

'serialPortsAccess' - the Switch allows management through serial ports when and only when this bit is set.

'physicalPortsAccess' - the Switch allows management through the physical panel when and only when this bit is set.

'managerRole' - the Switch is allowed to change the Fabric Policy configuration (on receipt of any of the EACA, ESFC, EUFC, ACA, SFC, or UFC SW\_ILSs) if and only if this bit is set.

Expires 11 January 2009

[Page 81]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

Whenever a Fabric has Active Policy Objects, the value of the t11FamConfigDomainIdType object defined in the T11-FC-FABRIC-ADDR-MGR-MIB module must be read-only and reflect the values of the 'staticDomainID' and 'insistentDomainID' bits of this object."

REFERENCE

- "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and table 112.
- Fibre Channel - Switch Fabric-4 (FC-SW-4), ANSI INCITS 418-2006, April 2006, [section 7.1](#).
- t11FamConfigDomainIdType, T11-FC-FABRIC-ADDR-MGR-MIB, Fibre Channel Fabric Address Manager MIB, [RFC 4439](#)."

::= { t11FcSpPoSwMembEntry 3 }

t11FcSpPoSwMembDomainID OBJECT-TYPE

SYNTAX            FcDomainIdOrZero

MAX-ACCESS       read-only

STATUS            current

DESCRIPTION

"The specified Domain\_ID value when either of the 'staticDomainID' or 'insistentDomainID' bits are set in the corresponding instance of t11FcSpPoSwMembSwitchFlags.

Whenever a Fabric has Active Policy Objects, the value of the t11FamConfigDomainId object defined in the T11-FC-FABRIC-ADDR-MGR-MIB module must be read-only and reflect the value of this object."

REFERENCE

- "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and tables 111 and 112.
- t11FamConfigDomainId, T11-FC-FABRIC-ADDR-MGR-MIB, Fibre Channel Fabric Address Manager MIB, [RFC 4439](#)."

::= { t11FcSpPoSwMembEntry 4 }

t11FcSpPoSwMembPolicyDataRole OBJECT-TYPE

SYNTAX	INTEGER {
	client(1),
	autonomous(2),
	server(3)
	}
MAX-ACCESS	read-only
STATUS	current
DESCRIPTION	

"The role of the Switch in terms of which Policy data it retains/maintains:

'client' - the Switch operates as a Client Switch. A Client Switch maintains its own Switch Connectivity Object and all Fabric-wide List Objects. If FC-SP Zoning is used, a Client Switch maintains only the subset of the Active Zone Set that it requires to enforce the current Fabric Zoning configuration.

'autonomous' - the Switch operates as an Autonomous Switch. An Autonomous Switch maintains its own Switch Connectivity Object and all Fabric-wide List Objects. This is the same as 'client' except that if FC-SP Zoning is used, an Autonomous Switch maintains a complete copy of the Fabric Zoning Database.

'server' - the Switch operates as a Server Switch.  
A Server Switch maintains all Fabric-wide List Objects and the Switch Connectivity Objects of each Switch in the Fabric. If FC-SP Zoning is used, a Server Switch maintains a complete copy of the Fabric Zoning Database."

#### REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 113."

::= { t11FcSpPoSwMembEntry 5 }

t11FcSpPoSwMembAuthBehaviour OBJECT-TYPE

SYNTAX BITS {  
mustAuthenticate(0),  
rejectIsFailure(1)  
}

MAX-ACCESS read-only

STATUS current

#### DESCRIPTION

"The authentication behaviour of the Switch:

'mustAuthenticate' - if this bit is set, all connections between this Switch and neighbour Switches must be authenticated.

'rejectIsFailure' - if this bit is set, the rejection of an AUTH\_Negotiate message must be considered as an authentication failure by this Switch."

#### REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 114."

::= { t11FcSpPoSwMembEntry 6 }

t11FcSpPoSwMembAttribute OBJECT-TYPE

SYNTAX T11FcSpAlphaNumNameOrAbsent

MAX-ACCESS read-only

STATUS current

#### DESCRIPTION

"The name of an active Attribute Policy Object which is defined for this Switch, or the zero-length string. The zero-length string indicates that no Attribute Policy Object is defined for this Switch."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 110."

::= { t11FcSpPoSwMembEntry 7 }

--

-- Node Entries in Active Node Membership List Objects

--

t11FcSpPoNoMembTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpPoNoMembEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of Node Entries in active Node Membership List Objects.

One Node Membership List Object is represented by all of the rows of this table which have the same values of fcmInstanceIndex and t11FcSpPoFabricIndex."

::= { t11FcSpPoActive 4 }

t11FcSpPoNoMembEntry OBJECT-TYPE

SYNTAX T11FcSpPoNoMembEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each entry contains information about one Node Entry

within the active Node Membership List Object for the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,

```
        t11FcSpPoNoMembNodeNameType, t11FcSpPoNoMembNodeName }  
 ::= { t11FcSpPoNoMembTable 1 }
```

```
T11FcSpPoNoMembEntry ::= SEQUENCE {  
    t11FcSpPoNoMembNodeNameType    T11FcSpPolicyNameType,  
    t11FcSpPoNoMembNodeName        FcNameIdOrZero,  
    t11FcSpPoNoMembFlags            BITS,  
    t11FcSpPoNoMembCtAccessIndex    Unsigned32,  
    t11FcSpPoNoMembAttribute        T11FcSpAlphaNumNameOrAbsent  
}
```

```
t11FcSpPoNoMembNodeNameType OBJECT-TYPE  
    SYNTAX      T11FcSpPolicyNameType {  
        nodeName(1),  
        restrictedNodeName(2),  
        portName(3),  
        restrictedPortName(4),  
        wildcard(5),  
        restrictedWildcard(6)  
    }
```

```
    MAX-ACCESS not-accessible  
    STATUS      current
```

DESCRIPTION

"If the value of this object is 'wildcard' or 'restrictedWildcard', this Node Entry applies to Nodes not explicitly named in the Node Membership List Object.

Otherwise, the combination of this object and t11FcSpPoNoMembNodeName specify the name of this Node Entry in the active Node Membership List Object. A Node is identified by its Node Name or by one or more of its Port Names.

Restricted membership means that a Node is not allowed to be connected to the Fabric unless allowed by a specific Switch Connectivity Object. Unrestricted membership means that a Node is allowed to be connected to the Fabric unless disallowed by a specific Switch Connectivity Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,

Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 116."  
 ::= { t11FcSpPoNoMembEntry 1 }

t11FcSpPoNoMembNodeName OBJECT-TYPE

SYNTAX FcNameIdOrZero (SIZE (8))

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"If the value of t11FcSpPoNoMembNodeNameType is  
'wildcard' or 'restrictedWildcard', this object has the  
value '0000000000000000'h.

Otherwise, the combination of t11FcSpPoNoMembNodeNameType  
and this object specify the name of this Node Entry is the  
active Node Membership List Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 116."

::= { t11FcSpPoNoMembEntry 2 }

t11FcSpPoNoMembFlags OBJECT-TYPE

SYNTAX BITS {  
    scsiEnclosureAccess(0),  
    authenticationRequired(1)  
}

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Configurable options in respect to the administration  
of Policy Objects at this Node:

    'scsiEnclosureAccess' - the Node is allowed to  
control any Switch through SCSI Enclosure Services if this  
bit is set. If a Switch does not support SCSI Enclosure  
Services, this bit is ignored.

    'authenticationRequired' - the Node is required to  
authenticate itself to any Switch to which it is connected  
if and only if this bit is set."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 118."



Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```
::= { t11FcSpPoNoMembEntry 3 }
```

t11FcSpPoNoMembCtAccessIndex    OBJECT-TYPE

SYNTAX            Unsigned32 (0..4294967295)

MAX-ACCESS       read-only

STATUS            current

DESCRIPTION

"If the value of this object is zero, then access by this Node to Generic Services is not limited by a Common Transport Access Specifier.

Otherwise, the limits are specified by the set of Common Transport Access Descriptors contained in those rows of the t11FcSpPoCtDescrTable for the same Fabric and for which the value of t11FcSpPoCtDescrSpecifierIndex is the same as the value of this object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP), February 2007,  
[section 7.1.4.1](#) and tables 118/119/120/121."

```
::= { t11FcSpPoNoMembEntry 4 }
```

t11FcSpPoNoMembAttribute    OBJECT-TYPE

SYNTAX            T11FcSpAlphaNumNameOrAbsent

MAX-ACCESS       read-only

STATUS            current

DESCRIPTION

"The name of an active Attribute Policy Object which is defined for this Node, or the zero-length string. The zero-length string indicates that no Attribute Policy Object is defined for this Node."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 116."

```
::= { t11FcSpPoNoMembEntry 5 }
```

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--  
--  
-- Common Transport Access Descriptors  
--

**t11FcSpPoCtDescrTable OBJECT-TYPE**

SYNTAX            SEQUENCE OF T11FcSpPoCtDescrEntry

MAX-ACCESS       not-accessible

STATUS            current

**DESCRIPTION**

"A table of Common Transport Access Descriptors being used within active Policy Objects.

A Common Transport Access Specifier is a list of Common Transport Access Descriptors which specify whether a Node is allowed to access a Generic Service or Sub-Server.

An active Common Transport Access Specifier is represented by all rows of this table which have the same values of fcmInstanceIndex, t11FcSpPoFabricIndex, and t11FcSpPoCtDescrSpecifierIndex."

::= { t11FcSpPoActive 5 }

**t11FcSpPoCtDescrEntry OBJECT-TYPE**

SYNTAX            T11FcSpPoCtDescrEntry

MAX-ACCESS       not-accessible

STATUS            current

**DESCRIPTION**

"Each entry contains information about one Common Transport Access Descriptor of an active Common Transport Access Specifier used within the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,  
         t11FcSpPoCtDescrSpecifierIndex, t11FcSpPoCtDescrIndex }

::= { t11FcSpPoCtDescrTable 1 }

```

T11FcSpPoCtDescrEntry ::= SEQUENCE {
    t11FcSpPoCtDescrSpecifierIndex    Unsigned32,
    t11FcSpPoCtDescrIndex              Unsigned32,
    t11FcSpPoCtDescrFlags               BITS,
    t11FcSpPoCtDescrGsType              OCTET STRING,
    t11FcSpPoCtDescrGsSubType           OCTET STRING
}

```

Expires 11 January 2009

[Page 88]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```

t11FcSpPoCtDescrSpecifierIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION
        "An index value which uniquely identifies a particular
        Common Transport Access Specifier within a Fabric."
    ::= { t11FcSpPoCtDescrEntry 1 }

```

```

t11FcSpPoCtDescrIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION
        "An index value which uniquely identifies a particular
        Common Transport Access Descriptor within a Common Transport
        Access Specifier."
    ::= { t11FcSpPoCtDescrEntry 2 }

```

```

t11FcSpPoCtDescrFlags OBJECT-TYPE
    SYNTAX      BITS {
                    allow(0),
                    gsTypeWildcard(1),
                    gsSubTypeWildcard(2),
                    readOnly(3)
                }
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The flag bits which specify how access is to be limited by
        this Common Transport Access Descriptor:

```

- allow -- access to the specified Generic Service and Server is allowed if this bit is set, and to be denied if this bit is not set.
- gsTypeWildcard -- if this bit is set, the Generic Service to be allowed/denied is specified by the value of t11FcSpPoCtDescrGsType. If this bit is set, then the gsSubTypeWildcard bit must not be set.
- gsSubTypeWildcard -- if this bit is set, the Generic Service to be allowed/denied is specified by the value of t11FcSpPoCtDescrGsSubType. If this bit is set, then the gsTypeWildcard bit must not be set.

Expires 11 January 2009

[Page 89]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

    - readOnly -- if this bit is set then access is to be granted only for reading."  
 ::= { t11FcSpPoCtDescrEntry 3 }

t11FcSpPoCtDescrGsType OBJECT-TYPE

SYNTAX           OCTET STRING (SIZE (1))

MAX-ACCESS      read-only

STATUS           current

DESCRIPTION

"The GS\_Type of the Generic Service (e.g., the FC-GS-5 Management Service) which is subject to access control. This value is ignored if the gsTypeWildcard bit is not set in the corresponding value of t11FcSpPoCtDescrFlags."

REFERENCE

"Fibre Channel - Generic Services-5 (FC-GS-5),  
 ANSI INCITS 427-2006, [section 4.3.2.4](#)."

::= { t11FcSpPoCtDescrEntry 4 }

t11FcSpPoCtDescrGsSubType OBJECT-TYPE

SYNTAX           OCTET STRING (SIZE (1))

MAX-ACCESS      read-only

STATUS           current

DESCRIPTION

"The GS\_Subtype of the Generic Server (e.g., the Fabric Zone Server) which is subject to access control. This value is

ignored if the gsSubTypeWildcard bit is not set in the corresponding value of t11FcSpPoCtDescrFlags."

REFERENCE

"Fibre Channel - Generic Services-5 (FC-GS-5),  
ANSI INCITS 427-2006, [section 4.3.2.5](#)."

::= { t11FcSpPoCtDescrEntry 5 }

Expires 11 January 2009

[Page 90]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--

--

-- Switches/Nodes in Active Switch Connectivity Objects

--

t11FcSpPoSwConnTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpPoSwConnEntry

MAX-ACCESS      not-accessible

STATUS           current

DESCRIPTION

"A table of active Switch Connectivity Objects.

A Switch Connectivity Object defines to which other  
Switches or Nodes a particular Switch may/may not be  
connected at the Node level and/or at the Port level."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.6.1](#), tables 123/124."

```
::= { t11FcSpPoActive 6 }
```

t11FcSpPoSwConnEntry OBJECT-TYPE

SYNTAX T11FcSpPoSwConnEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each entry contains the name of either a Switch or a Node with which any port of a particular Switch, or a particular port of that Switch, is allowed or not allowed to be connected.

The particular Switch is on the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,  
t11FcSpPoSwConnSwitchName, t11FcSpPoSwConnAllowedType,  
t11FcSpPoSwConnPortNameOrAll,  
t11FcSpPoSwConnAllowedIndex }

```
::= { t11FcSpPoSwConnTable 1 }
```

T11FcSpPoSwConnEntry ::= SEQUENCE {

t11FcSpPoSwConnSwitchName FcNameIdOrZero,

t11FcSpPoSwConnAllowedType INTEGER,

t11FcSpPoSwConnPortNameOrAll FcNameIdOrZero,

t11FcSpPoSwConnAllowedIndex Unsigned32,

Expires 11 January 2009

[Page 91]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

```
t11FcSpPoSwConnAllowedNameType T11FcSpPolicyNameType,  
t11FcSpPoSwConnAllowedName T11FcSpPolicyName  
}
```

t11FcSpPoSwConnSwitchName OBJECT-TYPE

SYNTAX FcNameIdOrZero (SIZE (8))

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The name of the particular Switch for which this Switch Connectivity Object specifies topology restrictions."

```
::= { t11FcSpPoSwConnEntry 1 }
```

t11FcSpPoSwConnAllowedType OBJECT-TYPE

SYNTAX INTEGER { switch(1), node(2) }

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This object specifies whether this row refers to Switch-to-Switch or Switch-to-Node connectivity, i.e., whether the corresponding instance of t11FcSpPoSwConnAllowedName specifies the name of a Switch or the name of a Node."

::= { t11FcSpPoSwConnEntry 2 }

t11FcSpPoSwConnPortNameOrAll OBJECT-TYPE

SYNTAX FcNameIdOrZero (SIZE(0 | 8))

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This object specifies either the particular port to which this topology restriction applies, or if the value is the zero-length string, that the topology restriction applies to all ports on the particular Switch.

In the FC-SP Policy Database, restrictions for a particular port are formatted within a Port Connectivity Entry of a Switch Connectivity Object, whereas restrictions for all ports on the Switch are specified in the main part of a Switch Connectivity Object, i.e., not in a Port Connectivity Entry."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.6.1](#), tables 123/124."

Expires 11 January 2009

[Page 92]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

::= { t11FcSpPoSwConnEntry 3 }

t11FcSpPoSwConnAllowedIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"When multiple rows in this table apply to the same port(s) in the same Switch's Switch Connectivity Object, this object provides a unique index value to distinguish between such rows."

::= { t11FcSpPoSwConnEntry 4 }

t11FcSpPoSwConnAllowedNameType OBJECT-TYPE

SYNTAX T11FcSpPolicyNameType {  
     nodeName(1),  
     restrictedNodeName(2),  
     portName(3),  
     restrictedPortName(4),  
     wildcard(5),  
     restrictedWildcard(6)  
 }

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"If the value of this object is 'wildcard' or 'restrictedWildcard', this row specifies whether connectivity is allowed/not allowed with entities not explicitly named by other rows.

Otherwise, the combination of t11FcSpPoSwConnAllowedNameType and t11FcSpPoSwConnAllowedName specify the name of:

- a Switch (if t11FcSpPoSwConnAllowedType = 'switch'), or
- a Node (if t11FcSpPoSwConnAllowedType = 'node')

to which connectivity is:

- allowed by 'nodeName' and 'portName',
- not allowed by 'restrictedNodeName' and 'restrictedPortName'."

::= { t11FcSpPoSwConnEntry 5 }

t11FcSpPoSwConnAllowedName OBJECT-TYPE

SYNTAX T11FcSpPolicyName (SIZE (8))



STATUS current

DESCRIPTION

"If the value of t11FcSpPoSwConnAllowedNameType is 'wildcard' or 'restrictedWildcard', this object has the value '0000000000000000'h.

Otherwise, the combination of t11FcSpPoSwConnAllowedNameType and t11FcSpPoSwConnAllowedName specify the name of:

- a Switch (if t11FcSpPoSwConnAllowedType = 'switch'), or
- a Node (if t11FcSpPoSwConnAllowedType = 'node')

to which connectivity is allowed/restricted."

::= { t11FcSpPoSwConnEntry 6 }

--

-- IP Management Entries in Active IP Management List Objects

--

t11FcSpPoIpMgmtTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpPoIpMgmtEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of IP Management Entries in active IP Management List Objects. A IP Management List Object is a Fabric-wide Policy Object that describes which IP hosts are allowed to manage a Fabric.

One IP Management List Object is represented by all of the rows of this table which have the same values of fcmInstanceIndex and t11FcSpPoFabricIndex."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.7](#)"

::= { t11FcSpPoActive 7 }

t11FcSpPoIpMgmtEntry OBJECT-TYPE

SYNTAX T11FcSpPoIpMgmtEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each entry contains information about one IP Management Entry within the active IP Management List Object for the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex.

The Policy Object Name of an IP Management Entry Policy Object is either an IPv6 Address Range or an IPv4 Address Range, where in each case, the range is specified as two addresses: the low and high ends of the range. In particular, since the Policy Object Name in this situation can only be an IPv6 Address Range or an IPv4 Address Range, it is represented here by three MIB objects defined as a (InetAddressType, InetAddress, InetAddress) tuple, in which the first address is the low end of the range, the second address is the high end of the range, and both addresses are of the type designated by InetAddressType.

In theory, the use of t11FcSpPoIpMgmtEntryNameLow and t11FcSpPoIpMgmtEntryNameHigh (which both have the syntax of InetAddress) in the INDEX could cause the need for excessively-long OIDs. In practice, this can't happen because FC-SP doesn't allow these objects to be specified as DNS names."

```
INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,
        t11FcSpPoIpMgmtEntryNameType,
        t11FcSpPoIpMgmtEntryNameLow,
        t11FcSpPoIpMgmtEntryNameHigh }
 ::= { t11FcSpPoIpMgmtTable 1 }
```

```
T11FcSpPoIpMgmtEntry ::= SEQUENCE {
    t11FcSpPoIpMgmtEntryNameType    InetAddressType,
    t11FcSpPoIpMgmtEntryNameLow     InetAddress,
    t11FcSpPoIpMgmtEntryNameHigh    InetAddress,
    t11FcSpPoIpMgmtWkpIndex         Unsigned32,
    t11FcSpPoIpMgmtAttribute        T11FcSpAlphaNumNameOrAbsent
}
```

t11FcSpPoIpMgmtEntryNameType OBJECT-TYPE

```
SYNTAX      InetAddressType
            -- INTEGER { ipv4(1), ipv6(2) }
MAX-ACCESS  not-accessible
STATUS      current
```

DESCRIPTION

"The combination of t11FcSpPoIpMgmtNameType,

t11FcSpPoIpMgmtNameLow and t11FcSpPoIpMgmtNameHigh specify the IP Address range of this IP Management Entry in the IP Management List Object.

The FC-SP specification does not allow the use of a DNS domain name to specify the address at the lower end or at the higher end of the IP Address range, nor does it allow the specification of a zone index. Therefore, the type of address must be one of: 'ipv4', or 'ipv6'."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, sections [7.1.7.1](#) & 7.1.2, tables 103/126."

::= { t11FcSpPoIpMgmtEntry 1 }

t11FcSpPoIpMgmtEntryNameLow OBJECT-TYPE

SYNTAX            InetAddress (SIZE(4 | 16))

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"The lower end of an Internet address range. The type of this address is given by the corresponding instance of t11FcSpPoIpMgmtEntryNameType.

The combination of t11FcSpPoIpMgmtNameType, t11FcSpPoIpMgmtNameLow and t11FcSpPoIpMgmtNameHigh specify the IP Address range of this IP Management Entry in the IP Management List Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, sections [7.1.7.1](#) & 7.1.2, tables 103/126."

::= { t11FcSpPoIpMgmtEntry 2 }

t11FcSpPoIpMgmtEntryNameHigh OBJECT-TYPE

SYNTAX            InetAddress (SIZE(4 | 16))

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"The higher end of an Internet address range. The type of this address is given by the corresponding instance

of t11FcSpPoIpMgmtEntryNameType.

The combination of t11FcSpPoIpMgmtNameType,  
t11FcSpPoIpMgmtNameLow and t11FcSpPoIpMgmtNameHigh

Expires 11 January 2009

[Page 96]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

specify the IP Address range of this IP Management  
Entry in the IP Management List Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, sections [7.1.7.1](#) & 7.1.2, tables 103/126."

::= { t11FcSpPoIpMgmtEntry 3 }

t11FcSpPoIpMgmtWkpIndex OBJECT-TYPE

SYNTAX            Unsigned32 (0..4294967295)

MAX-ACCESS       read-only

STATUS            current

DESCRIPTION

"This object identifies the restrictions for IP management  
access by IP hosts in this range of IP addresses, specified  
as the set of Well Known Protocols Access Descriptors  
contained in those rows of the t11FcSpPoWkpDescrTable for  
which the value of t11FcSpPoWkpDescrSpecifierIndex is the  
same as the value of this object. A value of zero indicates  
that this IP Management Entry does not identify a Well Known  
Protocols Access Specifier."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.7.1](#) and tables 127/129."

::= { t11FcSpPoIpMgmtEntry 4 }

t11FcSpPoIpMgmtAttribute OBJECT-TYPE

SYNTAX            T11FcSpAlphaNumNameOrAbsent

MAX-ACCESS       read-only

STATUS            current

DESCRIPTION

"The name of an active Attribute Policy Object which is  
defined for this IP Management entry, or the zero-length  
string. The zero-length string indicates that no Attribute

Policy Object is defined for this IP Management entry."  
REFERENCE  
"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.7.1](#) and table 128."  
::= { t11FcSpPoIpMgmtEntry 5 }

Expires 11 January 2009

[Page 97]

---

Internet Draft      Fibre-Channel Security Protocols MIB      July 2008

--  
-- Well-Known Protocol Access Descriptors  
--

t11FcSpPoWkpDescrTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpPoWkpDescrEntry  
MAX-ACCESS       not-accessible  
STATUS            current

DESCRIPTION

"A table of the Well-Known Protocol Access Descriptors  
being used within active Policy Objects.

A Well-Known Protocol Access Specifier is a list of  
Well-Known Protocol Access Descriptors each of which  
specifies a protocol number, a port number and/or various  
flags specifying how IP management access is restricted.

A Well-Known Protocol Transport Access Specifier is  
represented by all rows of this table which have the  
same values of fcmInstanceIndex, t11FcSpPoFabricIndex,  
and t11FcSpPoWkpDescrSpecifierIndex."

::= { t11FcSpPoActive 8 }

t11FcSpPoWkpDescrEntry OBJECT-TYPE

SYNTAX            T11FcSpPoWkpDescrEntry  
MAX-ACCESS       not-accessible  
STATUS            current

DESCRIPTION

"Each entry contains information about one Well-Known

Protocol Access Descriptor of a Well-Known Protocol  
Access Specifier used within the Fabric identified by  
t11FcSpPoFabricIndex and managed within the Fibre Channel  
management instance identified by fcmInstanceIndex."

```
INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,
        t11FcSpPoWkpDescrSpecifierIndex, t11FcSpPoWkpDescrIndex }
 ::= { t11FcSpPoWkpDescrTable 1 }
```

```
T11FcSpPoWkpDescrEntry ::= SEQUENCE {
    t11FcSpPoWkpDescrSpecifierIndex Unsigned32,
    t11FcSpPoWkpDescrIndex          Unsigned32,
    t11FcSpPoWkpDescrFlags          BITS,
    t11FcSpPoWkpDescrWkpNumber      Unsigned32,
    t11FcSpPoWkpDescrDestPort       InetPortNumber
}
```

Expires 11 January 2009

[Page 98]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpPoWkpDescrSpecifierIndex OBJECT-TYPE

SYNTAX            Unsigned32 (1..4294967295)

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"An index value which uniquely identifies a particular  
Well-Known Protocol Access Specifier within a Fabric."

```
::= { t11FcSpPoWkpDescrEntry 1 }
```

t11FcSpPoWkpDescrIndex OBJECT-TYPE

SYNTAX            Unsigned32 (1..4294967295)

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"An index value which uniquely identifies a particular  
Well-Known Protocol Access Descriptor within a Well-Known  
Protocol Access Specifier."

```
::= { t11FcSpPoWkpDescrEntry 2 }
```

t11FcSpPoWkpDescrFlags OBJECT-TYPE

```
SYNTAX            BITS {
                    allow(0),
                    wkpWildcard(1),
```

```

        destPortWildcard(2),
        readOnly(3)
    }
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
    "The flag bits which specify how access is to be limited by
    this Well-Known Protocol Access Descriptor:

    - allow -- IP management access using this protocol/port
      is allowed if this bit is set, and to be denied if this
      bit is not set.

    - wkpWildcard -- if this bit is set, the IP Protocol number
      of the Well-Known Protocol to be allowed/denied is
      specified by the value of t11FcSpPoWkpDescrWkpNumber.

    - destPortWildcard -- if this bit is set, the Destination
      (TCP/UDP) Port number of the Well-Known Protocol to be
      allowed/denied is specified by the value of
      t11FcSpPoWkpDescrDestPort.
```

Expires 11 January 2009

[Page 99]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```

    - readOnly -- if this bit is set then access is to be
      granted only for reading."
```

#### REFERENCE

```

    "- ANSI INCITS 426-2007, T11/Project 1570-D,
      Fibre Channel - Security Protocols (FC-SP),
      February 2007, section 7.1.7.1 and table 131."
```

```

 ::= { t11FcSpPoWkpDescrEntry 3 }
```

t11FcSpPoWkpDescrWkpNumber OBJECT-TYPE

```

SYNTAX          Unsigned32 (0..255)
```

```

MAX-ACCESS      read-only
```

```

STATUS          current
```

#### DESCRIPTION

```

    "When the 'wkpWildcard' bit is set in the corresponding
    instance of t11FcSpPoWkpDescrFlags, this object specifies
    the IP protocol number of the Well-Known Protocol."
```

#### REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.7.1](#) and table 131.  
- <http://www.iana.org/assignments/protocol-numbers>."  
 ::= { t11FcSpPoWkpDescrEntry 4 }

t11FcSpPoWkpDescrDestPort OBJECT-TYPE

SYNTAX InetPortNumber

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"When the 'destPortWildcard' bit is set in the corresponding instance of t11FcSpPoWkpDescrFlags, this object specifies the Destination (TCP/UDP) Port number of the Well-Known Protocol. When the 'destPortWildcard' bit is reset, this object is ignored (and can have the value zero)."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.7.1](#) and table 131.  
- <http://www.iana.org/assignments/port-numbers>."

::= { t11FcSpPoWkpDescrEntry 5 }

--

-- Attribute Entries in Active Attribute Policy Objects

--

t11FcSpPoAttribTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpPoAttribEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of the Attribute Policy Objects being used within active Policy Objects. In the FC-SP Policy Database, each



Attribute Policy Object consists of an Attribute Object Name and a set of Attribute Entries.

An active Attribute Policy Object is represented by all the Attribute Entries in this table which have the same value of t11FcSpPoAttribName."

::= { t11FcSpPoActive 9 }

t11FcSpPoAttribEntry OBJECT-TYPE

SYNTAX T11FcSpPoAttribEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each row contains information specific to an Attribute Entry contained within an Attribute Policy Object which is active within the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex.

For some types of Attribute Policy Objects, it is valuable to break-out some semantically-significant parts of the Policy Object's value into their own individual MIB objects; for example, to extract the one or more individual Authentication Protocol Identifiers and associated Authentication Protocol Parameters out of an Attribute Object containing a 'AUTH\_Negotiate Message Payload'. For such types, another MIB table is defined to hold the extracted values in MIB objects specific to the Attribute Policy Object's type. In such cases, the t11FcSpPoAttribExtension object in this table points to the other MIB table.

If the value of one Attribute Entry is too large (more than 256 bytes) to be contained within the value of one instance

of t11FcSpPoAttribValue, then one row in this table contains the first 256 bytes, and one (or more) other row(s) in this table contain the rest of the value."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,  
t11FcSpPoAttribName, t11FcSpPoAttribEntryIndex,

```
        t11FcSpPoAttribPartIndex }  
 ::= { t11FcSpPoAttribTable 1 }
```

```
T11FcSpPoAttribEntry ::= SEQUENCE {  
    t11FcSpPoAttribName          T11FcSpAlphaNumName,  
    t11FcSpPoAttribEntryIndex    Unsigned32,  
    t11FcSpPoAttribPartIndex     Unsigned32,  
    t11FcSpPoAttribType          Unsigned32,  
    t11FcSpPoAttribValue         OCTET STRING,  
    t11FcSpPoAttribExtension     OBJECT IDENTIFIER  
}
```

```
t11FcSpPoAttribName OBJECT-TYPE  
    SYNTAX          T11FcSpAlphaNumName  
    MAX-ACCESS      not-accessible  
    STATUS          current  
    DESCRIPTION  
        "The name of the Attribute Policy Object containing one  
        or more Attribute Entries."  
    REFERENCE  
        "- ANSI INCITS 426-2007, T11/Project 1570-D,  
        Fibre Channel - Security Protocols (FC-SP),  
        February 2007, section 7.1.8.1 and table 133."  
 ::= { t11FcSpPoAttribEntry 1 }
```

```
t11FcSpPoAttribEntryIndex OBJECT-TYPE  
    SYNTAX          Unsigned32 (1..4294967295)  
    MAX-ACCESS      not-accessible  
    STATUS          current  
    DESCRIPTION  
        "A unique value to distinguish this Attribute Entry  
        from other Attribute Entries contained in the same  
        Attribute Policy Object."  
    REFERENCE  
        "- ANSI INCITS 426-2007, T11/Project 1570-D,  
        Fibre Channel - Security Protocols (FC-SP),  
        February 2007, section 7.1.8.1, tables 133/134."  
 ::= { t11FcSpPoAttribEntry 2 }
```

```
t11FcSpPoAttribPartIndex OBJECT-TYPE
```

SYNTAX            Unsigned32 (1..4294967295)

MAX-ACCESS      not-accessible

STATUS           current

DESCRIPTION

"When the value of an Attribute Entry is shorter than 257 bytes, the whole value is contained in one instance of t11FcSpPoAttribValue, and the value of this object is 1.

If the value of an Attribute Entry is longer than 256 bytes, then that value is divided up on 256 byte boundaries such that all parts are 256 bytes long except the last part which is shorter if necessary, with each such part contained in a separate row of this table, and the value of this object is set to the part number. That is, this object has the value of 1 for bytes 0-255, the value of 2 for bytes 256-511, ... etc."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.8.1](#), tables 134/135."

::= { t11FcSpPoAttribEntry 3 }

t11FcSpPoAttribType OBJECT-TYPE

SYNTAX            Unsigned32 (1..4294967295)

MAX-ACCESS      read-only

STATUS           current

DESCRIPTION

"The type of attribute. The first type to be defined is:

t11FcSpPoAttribType	t11FcSpPoAttribValue
=====	=====
'00000001'h	The AUTH_Negotiate Message Payload
"	

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP), February 2007,  
[section 7.1.8.1](#), tables 134/135 and table 10."

::= { t11FcSpPoAttribEntry 4 }

t11FcSpPoAttribValue OBJECT-TYPE

SYNTAX            OCTET STRING (SIZE (0..256))

MAX-ACCESS      read-only

STATUS           current

DESCRIPTION

"The value of an Attribute Entry is divided up on 256 byte

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

boundaries such that all parts are 256 bytes long except the last part which is shorter if necessary, and each such part is contained in a separate instance of this object.

The value of this object is independent of whether some parts of its value are broken-out into separate MIB objects pointed to by the corresponding instance of t11FcSpPoAttribExtension."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP), February 2007,  
[section 7.1.8.1](#), tables 134/135 and table 10."

::= { t11FcSpPoAttribEntry 5 }

## t11FcSpPoAttribExtension OBJECT-TYPE

SYNTAX            OBJECT IDENTIFIER

MAX-ACCESS      read-only

STATUS           current

## DESCRIPTION

"For some types of Attribute Policy Object, the value of this MIB object points to type-specific MIB objects which contain individual/broken-out parts of the Attribute Policy Object's value. If this object doesn't point to such type-specific MIB objects, then it contains the value: zeroDotZero.

In particular, when the value of t11FcSpPoAttribType indicates 'AUTH\_Negotiate Message Payload', one or more Authentication Protocol Identifiers and their associated Authentication Protocol Parameters are embedded within the value of the corresponding instance of t11FcSpPoAttribValue; MIB objects to contain these individual values are defined in the t11FcSpPoAuthProtTable. Thus, for an 'AUTH\_Negotiate Message Payload' Attribute, the value of this object contains an OID within the t11FcSpPoAuthProtTable, e.g., of the whole table, of an individual row, or of an individual instance within the table."

::= { t11FcSpPoAttribEntry 6 }

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--  
--  
--

-- Auth. Protocol Parameters in Active Attribute Policy Objects

t11FcSpPoAuthProtTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpPoAuthProtEntry

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"A table of Authentication Protocol Identifier and Authentication Protocol Parameters which are embedded in Attribute Policy Objects being used within active Policy Objects.

This table is used for Attribute Entries of Attribute Policy Objects for which the value of t11FcSpPoAttribType indicates 'AUTH\_Negotiate Message Payload' and the value of t11FcSpPoAttribExtension contains the OID of this table."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP), February 2007,  
sections [5.3.2](#) & 7.1.8.1, tables 134/135 and tables 10/11."

::= { t11FcSpPoActive 10 }

t11FcSpPoAuthProtEntry OBJECT-TYPE

SYNTAX            T11FcSpPoAuthProtEntry

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"Each entry contains information about an Authentication Protocol which is extracted out of the Attribute Entry (identified by t11FcSpPoAttribEntryIndex) of the Policy Attribute Object (identified by t11FcSpPoAttribName) which is active within the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex.

If the value of one Attribute Protocol Parameters string is too large (more than 256 bytes) to be contained within the value of one instance of t11FcSpPoAuthProtParams, then one row in this table contains the first 256 bytes, and one (or more) other row(s) in this table contain the rest of the value."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,  
t11FcSpPoAttribName, t11FcSpPoAttribEntryIndex,

Expires 11 January 2009

[Page 105]

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

t11FcSpPoAuthProtIdentifier,  
t11FcSpPoAuthProtPartIndex }  
::= { t11FcSpPoAuthProtTable 1 }

T11FcSpPoAuthProtEntry ::= SEQUENCE {  
t11FcSpPoAuthProtIdentifier Unsigned32,  
t11FcSpPoAuthProtPartIndex Unsigned32,  
t11FcSpPoAuthProtParams OCTET STRING  
}

t11FcSpPoAuthProtIdentifier OBJECT-TYPE  
SYNTAX Unsigned32 (0..4294967295)  
MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION

"The Authentication Protocol Identifier:

1	=	DH-CHAP
2	=	FCAP
3	=	FCPAP
4	=	IKEv2
5	=	IKEv2-AUTH
240 thru 255	=	Vendor Specific Protocols

all other values are 'Reserved' (by T11)."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 5.3.2](#), table 11."

::= { t11FcSpPoAuthProtEntry 1 }

t11FcSpPoAuthProtPartIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"When the value of an Attribute Protocol Parameters string is shorter than 257 bytes, the whole value is contained in one instance of t11FcSpPoAuthProtParams, and the value of this object is 1. (This includes the case when the Attribute Protocol Parameters string is zero bytes in length.)

If the value of an Authentication Protocol Parameters string is longer than 256 bytes, then that value is divided up on 256 byte boundaries such that all parts are 256 bytes long

Expires 11 January 2009

[Page 106]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

except the last part which is shorter if necessary, with each such part contained in a separate row of this table, and the value of this object is set to the part number. That is, this object has the value of 1 for bytes 0-255, the value of 2 for bytes 256-511, ... etc."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 5.3.2](#), table 10."

::= { t11FcSpPoAuthProtEntry 2 }

t11FcSpPoAuthProtParams OBJECT-TYPE

SYNTAX OCTET STRING (SIZE (0..256))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of an Authentication Protocol Parameters string is divided up on 256 byte boundaries such that all parts are 256 bytes long except the last part which is shorter if necessary, and each such part is contained in a separate instance of this object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 5.3.2](#), table 10."

::= { t11FcSpPoAuthProtEntry 3 }

Expires 11 January 2009

[Page 107]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--

-- Part 2 - Activate/De-Activate Operations

--

--

-- Objects to Invoke Activate/De-Activate Operations

--

t11FcSpPoOperTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpPoOperEntry

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

    "A table which allows Activate and Deactivate operations  
    to be invoked for FC-SP Policies on various Fabrics.

    Activating a new policy configuration is a two-step  
    process:



- 1) create a single Policy Summary Object as a set of rows in the t11FcSpPoNaSummaryTable specifying a set of Policy Objects which describe the new configuration; and
- 2) activate that Policy Summary Object using the t11FcSpPoOperActivate object defined in this table.

Deactivating the current policy configuration is a one step process: the current Policy Summary Object is deactivated using the t11FcSpPoOperDeActivate object."

```
::= { t11FcSpPoOperations 1 }
```

t11FcSpPoOperEntry OBJECT-TYPE

SYNTAX T11FcSpPoOperEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each entry allows an Activate and/or Deactivate operation to be invoked on a particular Fabric, which is managed as part of the Fibre Channel management instance identified by fcmInstanceIndex."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex }

```
::= { t11FcSpPoOperTable 1 }
```

T11FcSpPoOperEntry ::= SEQUENCE {

t11FcSpPoOperActivate T11FcSpAlphaNumName,

t11FcSpPoOperDeActivate T11FcSpAlphaNumName,

Expires 11 January 2009

[Page 108]

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

```

t11FcSpPoOperResult      INTEGER,
t11FcSpPoOperFailCause   SnmpAdminString
}

```

t11FcSpPoOperActivate OBJECT-TYPE

SYNTAX T11FcSpAlphaNumName

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"Writing the name of a Policy Summary Object into this object is a request to activate the policy configuration described by the combination of all rows in t11FcSpPoNaSummaryTable which have that name as their

value of t11FcSpPoNaSummaryName and are for the same Fabric.

Before issuing such a request, the relevant rows in the t11FcSpPoNaSummaryTable must exist and represent a complete and consistent Policy Summary Object. If they do not, the request will fail with t11FcSpPoOperResult having the 'badSummaryObject' value.

When read, the value of this object is always the zero-length string.

Writing to this object does not delete (or in any way affect) any rows in the MIB tables for non-active Policy Objects."

#### REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.3.6.2](#)"

::= { t11FcSpPoOperEntry 1 }

#### t11FcSpPoOperDeActivate OBJECT-TYPE

SYNTAX T11FcSpAlphaNumName

MAX-ACCESS read-write

STATUS current

#### DESCRIPTION

"Writing the current value of t11FcSpPoPolicySummaryObjName into this object (for a particular Fabric) is a request to deactivate that Fabric's current policy configuration. Writing any other value into this object is an error (e.g., 'wrongValue')."

Expires 11 January 2009

[Page 109]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

When read, the value of this object is always the zero-length string."

#### REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.3.6.3](#)"

::= { t11FcSpPoOperEntry 2 }

t11FcSpPoOperResult OBJECT-TYPE

SYNTAX            INTEGER {  
                    activateSuccess(1),  
                    badSummaryObject(2),  
                    activateFailure(3),  
                    deactivateSuccess(4),  
                    deactivateFailure(5),  
                    inProgress(6),  
                    none(7)  
                    }

MAX-ACCESS       read-only

STATUS            current

DESCRIPTION

"This object indicates the status/result of the last activation/deactivation which was invoked via the corresponding instance of t11FcSpPoOperActivate or t11FcSpPoOperDeActivate.

When the value of this object is 'inProgress', the values of the corresponding instances of t11FcSpPoOperActivate and t11FcSpPoOperDeActivate cannot be modified.

The value 'badSummaryObject' indicates an activation request which did not name a complete and consistent Policy Summary Object.

The value 'none' indicates activation/de-activation has not been attempted since the last restart of the management system."

::= { t11FcSpPoOperEntry 3 }

t11FcSpPoOperFailCause OBJECT-TYPE

SYNTAX            SnmpAdminString (SIZE (0..64))

MAX-ACCESS       read-only

STATUS            current

DESCRIPTION

"A textual message indicating the reason for the

most recent activation/de-activation failure, or the zero-length string if no information is available (e.g., because the corresponding instance of `t11FcSpPo0perResult` has the value 'none').

When the corresponding instance of `t11FcSpPo0perResult` is either 'activateFailure' or 'deactivateFailure', the value of this object indicates the reason for that failure."

::= { t11FcSpPo0perEntry 4 }

--

-- Part 3 - Non-Active Policy Objects

--

--

-- Non-Active Policy Summary Objects Available for Activation

--

t11FcSpPoNaSummaryTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpPoNaSummaryEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of non-active Policy Summary Objects available to be activated.

The functionality of this table deviates slightly from FC-SP in that FC-SP specifies that the only Policy Summary Object is the Active one, i.e., FC-SP does not store non-active Policy Summary Objects in the Policy Database. Instead, FC-SP requires a new Policy Summary Object to be created for, and embedded within, every Activate (APS) request. Thus, the newly-created Policy Summary Object outlasts the APS request only as the new active Policy Summary Object and only if the APS succeeds. In contrast, the Activate operation provided by this MIB module consists of two steps:

- 1) create a non-active Policy Summary Object as a set of entries in this table describing a new configuration;
- 2) activate a Policy Summary Object (stored as a set of entries in this table) using t11FcSpPoOperActivate.

These two steps are only loosely connected, i.e., the result of the first operation is a non-active Policy Summary Object which is retained (in this table) even if it isn't immediately activated. Even after an attempt to activate it succeeds or fails, a non-active Policy Summary Object is not deleted, but is retained and still available for subsequent modification/re-use."

::= { t11FcSpPoNonActive 1 }

t11FcSpPoNaSummaryEntry OBJECT-TYPE

SYNTAX T11FcSpPoNaSummaryEntry

MAX-ACCESS not-accessible

STATUS current

## DESCRIPTION

"Each entry contains information about one non-active Policy Object within a non-active Policy Summary Object defined for potential use on the Fabric identified by t11FcSpPoFabricIndex, and managed within the Fibre Channel management instance identified by fcmInstanceId.

A non-active Policy Summary Object is described by a set of entries in this table which have the same value of t11FcSpPoNaSummaryName.

As and when a Policy Summary Object is activated using the t11FcSpPoOperActivate object, if the activation is successful, existing rows (if any) in MIB tables for active Policy Objects are deleted and replaced by the appropriate new set of rows. Existing rows in this table and/or in other tables for non-active Policy Objects are not affected by the activate operation.

The StorageType of a row in this table is specified by the instance of t11FcSpPoStorageType which is INDEX-ed by the same values of fcmInstanceId and t11FcSpPoFabricIndex."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.3](#) and table 104."

INDEX { fcmInstanceId, t11FcSpPoFabricIndex,  
t11FcSpPoNaSummaryName, t11FcSpPoNaSummaryPolicyType,  
t11FcSpPoNaSummaryPolicyIndex }  
::= { t11FcSpPoNaSummaryTable 1 }

T11FcSpPoNaSummaryEntry ::= SEQUENCE {  
t11FcSpPoNaSummaryName            T11FcSpAlphaNumName,  
t11FcSpPoNaSummaryPolicyType      T11FcSpPolicyObjectType,  
t11FcSpPoNaSummaryPolicyIndex    Unsigned32,  
t11FcSpPoNaSummaryPolicyNameType T11FcSpPolicyNameType,  
t11FcSpPoNaSummaryPolicyName      T11FcSpPolicyName,  
t11FcSpPoNaSummaryHashStatus      T11FcSpHashCalculationStatus,  
t11FcSpPoNaSummaryHashFormat      T11FcSpPolicyHashFormat,  
t11FcSpPoNaSummaryHashValue       T11FcSpPolicyHashValue,  
t11FcSpPoNaSummaryRowStatus       RowStatus

}

t11FcSpPoNaSummaryName OBJECT-TYPE  
SYNTAX T11FcSpAlphaNumName

Expires 11 January 2009

[Page 113]

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The name of the non-active Policy Summary Object which  
contains this Policy Object."

::= { t11FcSpPoNaSummaryEntry 1 }

t11FcSpPoNaSummaryPolicyType OBJECT-TYPE

SYNTAX T11FcSpPolicyObjectType

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The 'Identifier' (i.e., the type) of this Policy Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.3.1](#) and table 104."

::= { t11FcSpPoNaSummaryEntry 2 }

t11FcSpPoNaSummaryPolicyIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A unique integer value to distinguish this Policy Object  
from any others which have the same type and which are  
contained in the same Policy Summary Object."

::= { t11FcSpPoNaSummaryEntry 3 }

t11FcSpPoNaSummaryPolicyNameType OBJECT-TYPE

SYNTAX T11FcSpPolicyNameType {  
    nodeName(1),  
    alphaNumericName(7)  
}

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The combination of t11FcSpPoNaSummaryPolicyNameType and t11FcSpPoNaSummaryPolicyName specify the name of the non-active Policy Object identified by this row.

The type of name must be 'nodeName' if the value of the corresponding instance of t11FcSpPoNaSummaryPolicyType is 'switchConnectivity', or 'alphaNumericName' otherwise."

::= { t11FcSpPoNaSummaryEntry 4 }

Expires 11 January 2009

[Page 114]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

t11FcSpPoNaSummaryPolicyName OBJECT-TYPE

SYNTAX T11FcSpPolicyName

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The combination of t11FcSpPoNaSummaryPolicyNameType and t11FcSpPoNaSummaryPolicyName specify the name of the non-active Policy Object identified by this row."

::= { t11FcSpPoNaSummaryEntry 5 }

t11FcSpPoNaSummaryHashStatus OBJECT-TYPE

SYNTAX T11FcSpHashCalculationStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"When read, the value of this object is either:

correct -- the corresponding instance of  
t11FcSpPoNaSummaryHashValue contains  
the correct value; or

stale -- the corresponding instance of  
t11FcSpPoNaSummaryHashValue contains  
a stale (possibly incorrect) value;

Writing a value of 'calculate' is a request to re-calculate and update the value of the corresponding instance of t11FcSpPoNaSummaryHashValue. Writing a value of 'correct' or 'stale' to this object is an error (e.g., 'wrongValue')."

DEFVAL { stale }



::= { t11FcSpPoNaSummaryEntry 6 }

t11FcSpPoNaSummaryHashFormat OBJECT-TYPE

SYNTAX T11FcSpPolicyHashFormat

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The format of this Policy Object's hash value as contained in the corresponding instance of the t11FcSpPoNaSummaryHashValue object."

DEFVAL { '00000001'h }

::= { t11FcSpPoNaSummaryEntry 7 }

t11FcSpPoNaSummaryHashValue OBJECT-TYPE

SYNTAX T11FcSpPolicyHashValue

MAX-ACCESS read-only

Expires 11 January 2009

[Page 115]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

STATUS current

DESCRIPTION

"The hash value of this Policy Object, in the format identified by the corresponding instance of the t11FcSpPoNaSummaryHashFormat object."

DEFVAL { "" }

::= { t11FcSpPoNaSummaryEntry 8 }

t11FcSpPoNaSummaryRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The status of this row.

Before a row in this table can have 'active' status, a non-Active Policy Object must already be represented in the table corresponding to the value of t11FcSpPoNaSummaryPolicyType with the name given by the combination of t11FcSpPoNaSummaryPolicyNameType and t11FcSpPoNaSummaryPolicyName. If such Policy Object gets deleted from the relevant table, the row in this table must also get deleted.

When a row has 'active' status, the only write-able MIB objects in this table are t11FcSpPoNaSummaryHashStatus and t11FcSpPoNaSummaryRowStatus."  
 ::= { t11FcSpPoNaSummaryEntry 9 }

Expires 11 January 2009

[Page 116]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--

-- Non-Active Switch Membership List Objects

--

t11FcSpPoNaSwListTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpPoNaSwListEntry

MAX-ACCESS      not-accessible

STATUS           current

DESCRIPTION

    "A table of non-active Switch Membership List Objects."

REFERENCE

    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
       Fibre Channel - Security Protocols (FC-SP),  
       February 2007, [section 7.1.4.1](#) and table 108."

::= { t11FcSpPoNonActive 2 }

t11FcSpPoNaSwListEntry OBJECT-TYPE

SYNTAX            T11FcSpPoNaSwListEntry  
MAX-ACCESS       not-accessible  
STATUS            current  
DESCRIPTION

"Each entry contains information about one non-active Switch Membership List Object for the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex.

The StorageType of a row in this table is specified by the instance of t11FcSpPoStorageType which is INDEX-ed by the same values of fcmInstanceIndex and t11FcSpPoFabricIndex."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,  
         t11FcSpPoNaSwListName }  
::= { t11FcSpPoNaSwListTable 1 }

T11FcSpPoNaSwListEntry ::= SEQUENCE {  
    t11FcSpPoNaSwListName            T11FcSpAlphaNumName,  
    t11FcSpPoNaSwListFabricName      FcNameIdOrZero,  
    t11FcSpPoNaSwListRowStatus       RowStatus  
}

t11FcSpPoNaSwListName OBJECT-TYPE  
SYNTAX            T11FcSpAlphaNumName  
MAX-ACCESS       not-accessible  
STATUS            current  
DESCRIPTION

Expires 11 January 2009

[Page 117]

---

Internet Draft       Fibre-Channel Security Protocols MIB

July 2008

"The name of the Switch Membership List Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 108."

::= { t11FcSpPoNaSwListEntry 1 }

t11FcSpPoNaSwListFabricName OBJECT-TYPE  
SYNTAX            FcNameIdOrZero  
MAX-ACCESS       read-create  
STATUS            current

#### DESCRIPTION

"The administratively-specified Fabric\_Name. This value is meaningful only when static Domain\_IDs are used in a Fabric. If Static Domain\_IDs are not used, the Fabric\_Name is dynamically determined, in which case the value of this object can be '0000000000000000'h or the zero-length string."

#### REFERENCE

- "- t11FamConfigDomainId, T11-FC-FABRIC-ADDR-MGR-MIB, Fibre Channel Fabric Address Manager MIB, [RFC 4439](#);
- "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, table 108."

::= { t11FcSpPoNaSwListEntry 2 }

#### t11FcSpPoNaSwListRowStatus OBJECT-TYPE

SYNTAX            RowStatus  
MAX-ACCESS       read-create  
STATUS            current

#### DESCRIPTION

"The status of this row. Values of object instances within the row can be modified at any time.

If a row in this table is deleted, any row in the t11FcSpPoNaSwMembTable for the same Switch Membership List Object will also get deleted."

::= { t11FcSpPoNaSwListEntry 3 }

--

-- Switch Entries in Non-Active Switch Membership List Objects

--

#### t11FcSpPoNaSwMembTable OBJECT-TYPE

SYNTAX           SEQUENCE OF T11FcSpPoNaSwMembEntry  
 MAX-ACCESS      not-accessible  
 STATUS           current  
 DESCRIPTION  
     "A table of Switch Entries in non-active Switch Membership  
     List Objects."  
 REFERENCE  
     "- ANSI INCITS 426-2007, T11/Project 1570-D,  
     Fibre Channel - Security Protocols (FC-SP),  
     February 2007, [section 7.1.4.1](#) and table 110."  
 ::= { t11FcSpPoNonActive 3 }

#### t11FcSpPoNaSwMembEntry OBJECT-TYPE

SYNTAX           T11FcSpPoNaSwMembEntry  
 MAX-ACCESS      not-accessible  
 STATUS           current  
 DESCRIPTION  
     "Each entry contains information about one Switch which  
     is listed in a Switch Entry of a non-active Switch Membership  
     List Object for the Fabric identified by t11FcSpPoFabricIndex  
     and managed within the Fibre Channel management instance  
     identified by fcmInstanceIdIndex.

A row cannot exist unless there is a row in  
 t11FcSpPoNaSwListTable for the given Switch Membership List  
 Object, i.e., the row in t11FcSpPoNaSwListTable for a  
 Switch Membership List Object must be created before (or  
 simultaneously) with a row in this table for a Switch  
 Entry in that Switch Membership List Object, and when a  
 row in t11FcSpPoNaSwListTable is deleted all rows in this  
 table for Switch Entries in that Switch Membership List  
 Object also get deleted.

The StorageType of a row in this table is specified by the  
 instance of t11FcSpPoStorageType which is INDEX-ed by the  
 same values of fcmInstanceIdIndex and t11FcSpPoFabricIndex."

INDEX { fcmInstanceIdIndex, t11FcSpPoFabricIndex,  
         t11FcSpPoNaSwListName,  
         t11FcSpPoNaSwMembSwitchNameType,  
         t11FcSpPoNaSwMembSwitchName }

```
::= { t11FcSpPoNaSwMembTable 1 }
```

```
T11FcSpPoNaSwMembEntry ::= SEQUENCE {  
    t11FcSpPoNaSwMembSwitchNameType  T11FcSpPolicyNameType,  
    t11FcSpPoNaSwMembSwitchName       FcNameIdOrZero,  
    t11FcSpPoNaSwMembFlags             BITS,  
    t11FcSpPoNaSwMembDomainID          FcDomainIdOrZero,  
    t11FcSpPoNaSwMembPolicyDataRole    INTEGER,  
    t11FcSpPoNaSwMembAuthBehaviour     BITS,  
    t11FcSpPoNaSwMembAttribute         T11FcSpAlphaNumNameOrAbsent,  
    t11FcSpPoNaSwMembRowStatus         RowStatus  
}
```

t11FcSpPoNaSwMembSwitchNameType OBJECT-TYPE

```
SYNTAX      T11FcSpPolicyNameType {  
                nodeName(1),  
                restrictedNodeName(2),  
                wildcard(5),  
                restrictedWildcard(6)  
            }
```

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"If the value of this object is 'nodeName' or 'restrictedNodeName', then the combination of this object and t11FcSpPoNaSwMembSwitchName specify the Switch Name of this Switch Entry.

The membership is restricted or unrestricted based on the name type. Restricted membership means that the Switch is not allowed to be part of the Fabric unless allowed by a specific Switch Connectivity Object. Unrestricted membership means that the Switch is allowed to be part of the Fabric unless disallowed by a specific Switch Connectivity Object.

The values of 'wildcard' and 'restrictedWildcard' provide the means to specify whether to allow/deny membership for Switches not explicitly named in the Switch Membership List Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 110."

```
::= { t11FcSpPoNaSwMembEntry 1 }
```

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

**t11FcSpPoNaSwMembSwitchName OBJECT-TYPE**

SYNTAX            FcNameIdOrZero (SIZE (8))

MAX-ACCESS       not-accessible

STATUS            current

**DESCRIPTION**

"If the value of t11FcSpPoSwMembSwitchNameType is 'wildcard' or 'restrictedWildcard', this object has the value '0000000000000000'h.

Otherwise, the combination of t11FcSpPoNaSwMembSwitchNameType and this object specify the Switch Name of this Switch Entry."

**REFERENCE**

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and table 110."

::= { t11FcSpPoNaSwMembEntry 2 }

**t11FcSpPoNaSwMembFlags OBJECT-TYPE**

SYNTAX            BITS {  
                  staticDomainID(0),  
                  insistentDomainID(1),  
                  serialPortsAccess(2),  
                  physicalPortsAccess(3),  
                  managerRole(4)  
                  }

MAX-ACCESS       read-create

STATUS            current

**DESCRIPTION**

"Configurable options in respect to the administration of Policy Objects at this Switch:

'staticDomainID'        - the Switch uses the 'Static Domain\_IDs behavior' (as defined in FC-SW-4) when this bit is set. This bit should have the same setting for all Switches in a Fabric's Switch Membership List Object, or else the Fabric will partition. If this bit is set, the 'insistentDomainID' bit must not be set.

'insistentDomainID'    - if this bit is set, the Switch uses the 'Insistent Domain\_IDs behavior' (as defined in FC-SW-4), and the 'staticDomainID' bit must not be set.

'serialPortsAccess' - the Switch allows management through serial ports when and only when this bit is set.

Expires 11 January 2009

[Page 121]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

'physicalPortsAccess' - the Switch allows management through the physical panel when and only when this bit is set.

'managerRole' - the Switch is allowed to change the Fabric Policy configuration (on receipt of any of the EACA, ESFC, EUFC, ACA, SFC, or UFC SW\_ILSs) if this bit is set."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and table 112."

::= { t11FcSpPoNaSwMembEntry 3 }

t11FcSpPoNaSwMembDomainID OBJECT-TYPE

SYNTAX            FcDomainIdOrZero

MAX-ACCESS       read-create

STATUS            current

DESCRIPTION

"The Domain\_ID to be used when either the 'staticDomainID' bit or the 'insistentDomainID' bit is set in the corresponding value of t11FcSpPoNaSwMembFlags."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and tables 111 and 112."

::= { t11FcSpPoNaSwMembEntry 4 }

t11FcSpPoNaSwMembPolicyDataRole OBJECT-TYPE

SYNTAX            INTEGER {  
                    client(1),  
                    autonomous(2),  
                    server(3)  
                    }

MAX-ACCESS       read-create

STATUS            current



## DESCRIPTION

"The role of the Switch in terms of which Policy data it retains/maintains:

'client' - the Switch operates as a Client Switch. A Client Switch maintains its own Switch Connectivity Object and all Fabric-wide List Objects. If FC-SP Zoning is used, a Client Switch maintains only the

Expires 11 January 2009

[Page 122]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

subset of the Active Zone Set that it requires to enforce the current Fabric Zoning configuration.

'autonomous' - the Switch operates as an Autonomous Switch. An Autonomous Switch maintains its own Switch Connectivity Object and all Fabric-wide List Objects. This is the same as 'client' except that if FC-SP Zoning is used, an Autonomous Switch maintains a complete copy of the Fabric Zoning Database.

'server' - the Switch operates as a Server Switch. A Server Switch maintains all Fabric-wide List Objects and the Switch Connectivity Objects of each Switch in the Fabric. If FC-SP Zoning is used, a Server Switch maintains a complete copy of the Fabric Zoning Database."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and table 113."

::= { t11FcSpPoNaSwMembEntry 5 }

t11FcSpPoNaSwMembAuthBehaviour OBJECT-TYPE

SYNTAX            BITS {  
                  mustAuthenticate(0),  
                  rejectIsFailure(1)  
                  }

MAX-ACCESS       read-create

STATUS            current

## DESCRIPTION

"The authentication behaviour of the Switch:

'mustAuthenticate' - if this bit is set, all connections between this Switch and neighbour Switches must be authenticated.

'rejectIsFailure' - if this bit is set, the rejection of an AUTH\_Negotiate message must be considered as an authentication failure by this Switch."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and table 114."

::= { t11FcSpPoNaSwMembEntry 6 }

t11FcSpPoNaSwMembAttribute OBJECT-TYPE

Expires 11 January 2009

[Page 123]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

SYNTAX            T11FcSpAlphaNumNameOrAbsent

MAX-ACCESS       read-create

STATUS            current

DESCRIPTION

"The name of a non-active Attribute Policy Object which is defined for this Switch. The zero-length string indicates that no non-active Attribute Policy Object is defined for this Switch.

The effect of having no rows in the t11FcSpPoNaAttribTable for which the value of t11FcSpPoNaAttribName is the same as the value of this object, is the same as this object's value being the zero-length string."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and table 110."

::= { t11FcSpPoNaSwMembEntry 7 }

t11FcSpPoNaSwMembRowStatus OBJECT-TYPE

SYNTAX            RowStatus

MAX-ACCESS       read-create

STATUS            current

DESCRIPTION

"The status of this row. Values of object instances

within the row can be modified at any time.

A row cannot exist unless there is a row in the t11FcSpPoNaSwListTable for the Switch Membership List Object containing the Switch Entry for this Switch, i.e., the row in t11FcSpPoNaSwListTable for a Switch Membership List Object must be created before (or simultaneously) with a row in this table for a Switch Entry in that Switch Membership List Object; and when a row in t11FcSpPoNaSwListTable is deleted, any row in this table for a Switch Entry in that Switch Membership List Object also gets deleted."

::= { t11FcSpPoNaSwMembEntry 8 }

Expires 11 January 2009

[Page 124]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--

-- Node Entries in Non-Active Node Membership List Objects

--

t11FcSpPoNaNoMembTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpPoNaNoMembEntry

MAX-ACCESS      not-accessible

STATUS           current

DESCRIPTION

"A table of Node Entries in non-active Node Membership List Objects.

One Node Membership List Object is represented by all the rows in this table which have the same value of t11FcSpPoNaNoMembListName."

::= { t11FcSpPoNonActive 4 }

t11FcSpPoNaNoMembEntry OBJECT-TYPE

SYNTAX           T11FcSpPoNaNoMembEntry

MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION

"Each entry contains information about one Node Entry of a non-active Node Membership List Object for the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex.

The StorageType of a row in this table is specified by the instance of t11FcSpPoStorageType which is INDEX-ed by the same values of fcmInstanceIndex and t11FcSpPoFabricIndex."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,  
t11FcSpPoNaNoMembListName,  
t11FcSpPoNaNoMembNodeNameType,  
t11FcSpPoNaNoMembNodeName }  
::= { t11FcSpPoNaNoMembTable 1 }

T11FcSpPoNaNoMembEntry ::= SEQUENCE {  
t11FcSpPoNaNoMembListName T11FcSpAlphaNumName,  
t11FcSpPoNaNoMembNodeNameType T11FcSpPolicyNameType,  
t11FcSpPoNaNoMembNodeName FcNameIdOrZero,  
t11FcSpPoNaNoMembFlags BITS,  
t11FcSpPoNaNoMembCtAccessIndex Unsigned32,  
t11FcSpPoNaNoMembAttribute T11FcSpAlphaNumNameOrAbsent,  
t11FcSpPoNaNoMembRowStatus RowStatus

Expires 11 January 2009

[Page 125]

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

}

t11FcSpPoNaNoMembListName OBJECT-TYPE

SYNTAX T11FcSpAlphaNumName

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The name of the non-active Node Membership List Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 116."

::= { t11FcSpPoNaNoMembEntry 1 }

t11FcSpPoNaNoMembNodeNameType OBJECT-TYPE

```
SYNTAX      T11FcSpPolicyNameType {
              nodeName(1),
              restrictedNodeName(2),
              portName(3),
              restrictedPortName(4),
              wildcard(5),
              restrictedWildcard(6)
            }
```

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"If the value of this object is 'wildcard' or 'restrictedWildcard', this Node Entry applies to Nodes not explicitly named in the Node Membership List Object.

Otherwise, the combination of this object and t11FcSpPoNaNoMembNodeName specify the name of this Node Entry in the active Node Membership List Object. A Node is identified by its Node Name or by one or more of its Port Names.

Restricted membership means that a Node is not allowed to be connected to the Fabric unless allowed by a specific Switch Connectivity Object. Unrestricted membership means that a Node is allowed to be connected to the Fabric unless disallowed by a specific Switch Connectivity Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and table 116."

Expires 11 January 2009

[Page 126]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

::= { t11FcSpPoNaNoMembEntry 2 }

t11FcSpPoNaNoMembNodeName OBJECT-TYPE

```
SYNTAX      FcNameIdOrZero (SIZE (8))
```

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"If the value of t11FcSpPoNaNoMembNodeNameType is 'wildcard' or 'restrictedWildcard', this object has the value '0000000000000000'h.

Otherwise, the combination of t11FcSpPoNaNoMembNodeNameType and this object specify the name of this Node Entry is the active Node Membership List Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 116."

::= { t11FcSpPoNaNoMembEntry 3 }

t11FcSpPoNaNoMembFlags OBJECT-TYPE

SYNTAX BITS {  
scsiEnclosureAccess(0),  
authenticationRequired(1)  
}

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Configurable options in respect to the administration of Policy Objects at this Node:

'scsiEnclosureAccess' - the Node is allowed to control any Switch through SCSI Enclosure Services if this bit is set. If a Switch does not support SCSI Enclosure Services, this bit is ignored.

'authenticationRequired' - the Node is required to authenticate itself to any Switch to which it is connected if and only if this bit is set."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.4.1](#) and table 118."

::= { t11FcSpPoNaNoMembEntry 4 }

SYNTAX            Unsigned32 (0..4294967295)

MAX-ACCESS      read-create

STATUS           current

DESCRIPTION

"If the value of this object is zero, then access by this Node to Generic Services is not limited by a Common Transport Access Specifier.

Otherwise, the limits are specified by the set of Common Transport Access Descriptors contained in those rows of the t11FcSpPoNaCtDescrTable for which the value of t11FcSpPoNaCtDescrSpecifierIndex is the same as the value of this object. No such rows in t11FcSpPoNaCtDescrTable has the same effect as this object's value being zero."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and tables 118/119/120/121."

::= { t11FcSpPoNaNoMembEntry 5 }

t11FcSpPoNaNoMembAttribute OBJECT-TYPE

SYNTAX           T11FcSpAlphaNumNameOrAbsent

MAX-ACCESS      read-create

STATUS           current

DESCRIPTION

"The name of a non-active Attribute Policy Object which is defined for this Node. The zero-length string indicates that no non-active Attribute Policy Object is defined for this Node.

The effect of having no rows in the t11FcSpPoNaAttribTable for which the value of t11FcSpPoNaAttribName is the same as the value of this object, is the same as this object's value being the zero-length string."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.4.1](#) and table 116."

::= { t11FcSpPoNaNoMembEntry 6 }

t11FcSpPoNaNoMembRowStatus OBJECT-TYPE

SYNTAX           RowStatus

MAX-ACCESS      read-create

STATUS           current

## DESCRIPTION

"The status of this row. Values of object instances within the row can be modified at any time."

::= { t11FcSpPoNaNoMembEntry 7 }

--

--

-- Non-Active Common Transport Access Descriptors

--

## t11FcSpPoNaCtDescrTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpPoNaCtDescrEntry

MAX-ACCESS not-accessible

STATUS current

## DESCRIPTION

"A table of Common Transport Access Descriptors referenced by non-active Policy Objects.

A Common Transport Access Specifier is a list of Common Transport Access Descriptors which specify whether a Node is allowed to access a Generic Service or Sub-Server.

A non-active Common Transport Access Specifier is represented by all rows of this table which have the same values of fcmInstanceIndex, t11FcSpPoFabricIndex, and t11FcSpPoNaCtDescrSpecifierIndex."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.5](#)"

::= { t11FcSpPoNonActive 5 }

## t11FcSpPoNaCtDescrEntry OBJECT-TYPE

SYNTAX T11FcSpPoNaCtDescrEntry

MAX-ACCESS not-accessible

STATUS current

## DESCRIPTION

"Each entry contains information about one Common Transport Access Descriptor of an non-active Common Transport Access Specifier used within the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex.

The StorageType of a row in this table is specified by the instance of t11FcSpPoStorageType which is INDEX-ed by the



Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

same values of fcmInstanceIndex and t11FcSpPoFabricIndex."  
 INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,  
           t11FcSpPoNaCtDescrSpecifierIndex, t11FcSpPoNaCtDescrIndex }  
 ::= { t11FcSpPoNaCtDescrTable 1 }

T11FcSpPoNaCtDescrEntry ::= SEQUENCE {  
     t11FcSpPoNaCtDescrSpecifierIndex Unsigned32,  
     t11FcSpPoNaCtDescrIndex Unsigned32,  
     t11FcSpPoNaCtDescrFlags BITS,  
     t11FcSpPoNaCtDescrGsType OCTET STRING,  
     t11FcSpPoNaCtDescrGsSubType OCTET STRING,  
     t11FcSpPoNaCtDescrRowStatus RowStatus  
 }

t11FcSpPoNaCtDescrSpecifierIndex OBJECT-TYPE  
     SYNTAX Unsigned32 (1..4294967295)  
     MAX-ACCESS not-accessible  
     STATUS current  
     DESCRIPTION  
         "An index value which uniquely identifies a particular  
         Common Transport Access Specifier within a Fabric."  
     ::= { t11FcSpPoNaCtDescrEntry 1 }

t11FcSpPoNaCtDescrIndex OBJECT-TYPE  
     SYNTAX Unsigned32 (1..4294967295)  
     MAX-ACCESS not-accessible  
     STATUS current  
     DESCRIPTION  
         "An index value which uniquely identifies a particular  
         Common Transport Access Descriptor within a Common Transport  
         Access Specifier."  
     ::= { t11FcSpPoNaCtDescrEntry 2 }

t11FcSpPoNaCtDescrFlags OBJECT-TYPE  
     SYNTAX BITS {  
         allow(0),  
         gsTypeWildcard(1),  
         gsSubTypeWildcard(2),  
         readOnly(3)  
     }  
     MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The flag bits which specify how access is to be limited by this Common Transport Access Descriptor:

Expires 11 January 2009

[Page 130]

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

- allow -- access to the specified Generic Service and Server is allowed if this bit is set, and to be denied if this bit is not set.
- gsTypeWildcard -- if this bit is set, the Generic Service to be allowed/denied is specified by the value of t11FcSpPoNaCtDescrGsType, and the gsSubTypeWildcard bit must not also be set.
- gsSubTypeWildcard -- if this bit is set, the Generic Service to be allowed/denied is specified by the value of t11FcSpPoNaCtDescrGsSubType, and the gsTypeWildcard bit must not also be set.
- readOnly -- if this bit is set then access is to be granted only for reading."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.5.1](#), and tables 117, 118, and 120."

::= { t11FcSpPoNaCtDescrEntry 3 }

t11FcSpPoNaCtDescrGsType OBJECT-TYPE

SYNTAX OCTET STRING (SIZE (1))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The GS\_Type of the Generic Service (e.g., the FC-GS-5 Management Service) which is subject to access control. This value is ignored if the gsTypeWildcard bit is not set in the corresponding value of t11FcSpPoNaCtDescrFlags."

REFERENCE

"- ANSI INCITS 427-2006, Fibre Channel - Generic Services-5 (FC-GS-5), [section 4.3.2.4](#).

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.5.1](#) and table 120."  
 ::= { t11FcSpPoNaCtDescrEntry 4 }

t11FcSpPoNaCtDescrGsSubType OBJECT-TYPE  
SYNTAX OCTET STRING (SIZE (1))  
MAX-ACCESS read-create  
STATUS current  
DESCRIPTION

Expires 11 January 2009

[Page 131]

---

Internet Draft      Fibre-Channel Security Protocols MIB      July 2008

"The GS\_Subtype of the Generic Server (e.g., the Fabric Zone Server) which is subject to access control. This value is ignored if the gsSubTypeWildcard bit is not set in the corresponding value of t11FcSpPoNaCtDescrFlags."

REFERENCE

"- ANSI INCITS 427-2006,  
Fibre Channel - Generic Services-5 (FC-GS-5),  
[section 4.3.2.5](#).  
"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.5.1](#) and table 120."  
 ::= { t11FcSpPoNaCtDescrEntry 5 }

t11FcSpPoNaCtDescrRowStatus OBJECT-TYPE  
SYNTAX RowStatus  
MAX-ACCESS read-create  
STATUS current  
DESCRIPTION  
    "The status of this row. Values of object instances  
    within the row can be modified at any time."  
 ::= { t11FcSpPoNaCtDescrEntry 6 }

--  
-- Switches/Nodes in Non-Active Switch Connectivity Objects  
--

t11FcSpPoNaSwConnTable OBJECT-TYPE  
SYNTAX SEQUENCE OF T11FcSpPoNaSwConnEntry

MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION

"A table of non-active Switch Connectivity Objects.

A Switch Connectivity Object defines to which other Switches or Nodes a particular Switch may/may not be connected at the Node level and/or at the Port level."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.6](#)."

::= { t11FcSpPoNonActive 6 }

t11FcSpPoNaSwConnEntry OBJECT-TYPE

SYNTAX T11FcSpPoNaSwConnEntry

Expires 11 January 2009

[Page 132]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION

"Each entry contains the name of a Switch/Node with which any port of a particular Switch on a particular Fabric, or a particular port on that Switch, is allowed or not allowed to be connected.

The particular Fabric is identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex.

The StorageType of a row in this table is specified by the instance of t11FcSpPoStorageType which is INDEX-ed by the same values of fcmInstanceIndex and t11FcSpPoFabricIndex."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,  
t11FcSpPoNaSwConnSwitchName,  
t11FcSpPoNaSwConnAllowedType,  
t11FcSpPoNaSwConnPortNameOrAll,  
t11FcSpPoNaSwConnAllowedIndex }

::= { t11FcSpPoNaSwConnTable 1 }

T11FcSpPoNaSwConnEntry ::= SEQUENCE {

```

t11FcSpPoNaSwConnSwitchName      FcNameIdOrZero,
t11FcSpPoNaSwConnAllowedType      INTEGER,
t11FcSpPoNaSwConnPortNameOrAll    FcNameIdOrZero,
t11FcSpPoNaSwConnAllowedIndex     Unsigned32,
t11FcSpPoNaSwConnAllowedNameType  T11FcSpPolicyNameType,
t11FcSpPoNaSwConnAllowedName      FcNameIdOrZero,
t11FcSpPoNaSwConnRowStatus        RowStatus
}

t11FcSpPoNaSwConnSwitchName OBJECT-TYPE
    SYNTAX      FcNameIdOrZero (SIZE (8))
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION
        "The name of the Switch for which this Switch Connectivity
        Object specifies topology restrictions."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
        Fibre Channel - Security Protocols (FC-SP),
        February 2007, section 7.1.6.1 and table 123."
    ::= { t11FcSpPoNaSwConnEntry 1 }

```

Expires 11 January 2009

[Page 133]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```

t11FcSpPoNaSwConnAllowedType OBJECT-TYPE
    SYNTAX      INTEGER { switch(1), node(2) }
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION
        "This object specifies whether this row refers to an
        'Allowed Switch' which concerns Switch-to-Switch
        connectivity, or an 'Allowed Node' which concerns
        Switch-to-Node connectivity. Consequently, this object's
        value indicates whether the corresponding instance of
        t11FcSpPoNaSwConnAllowedName specifies the name of a Switch
        or the name of a Node."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
        Fibre Channel - Security Protocols (FC-SP),
        February 2007, section 7.1.6.1 and table 123."
    ::= { t11FcSpPoNaSwConnEntry 2 }

```

t11FcSpPoNaSwConnPortNameOrAll OBJECT-TYPE

SYNTAX FcNameIdOrZero (SIZE(0 | 8))

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This object specifies either the particular port on which this topology restriction applies, or if the value is the zero-length string, that the topology restriction applies to all ports of the Switch.

In other words, if this object's value contains the name of a port, then this row represents a 'Port Connectivity Entry' (as described in FC-SP) within a Switch Connectivity Object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.6.1](#) and tables 123/124."

::= { t11FcSpPoNaSwConnEntry 3 }

t11FcSpPoNaSwConnAllowedIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"When multiple rows in this table refer to different 'Allowed Switches' or to different 'Allowed Nodes' for the same port(s) in the same Switch Connectivity Object, this

object provides a unique index value to distinguish between such rows."

::= { t11FcSpPoNaSwConnEntry 4 }

t11FcSpPoNaSwConnAllowedNameType OBJECT-TYPE

SYNTAX T11FcSpPolicyNameType {  
    nodeName(1),  
    restrictedNodeName(2),  
    portName(3),  
    restrictedPortName(4),  
    wildcard(5),

```

        restrictedWildcard(6)
    }
MAX-ACCESS      read-create
STATUS          current
DESCRIPTION
    "If the value of this object is 'wildcard' or
    'restrictedWildcard', this row specifies whether
    connectivity is allowed/not allowed with entities not
    explicitly named by other rows.

    Otherwise, the combination of
    t11FcSpPoNaSwConnAllowedNameType and
    t11FcSpPoNaSwConnAllowedName specify the name of:

    - a Switch (if t11FcSpPoNaSwConnAllowedType = 'switch'), or
    - a Node (if t11FcSpPoNaSwConnAllowedType = 'node')

    to which connectivity is allowed/not allowed."
REFERENCE
    "- ANSI INCITS 426-2007, T11/Project 1570-D,
    Fibre Channel - Security Protocols (FC-SP),
    February 2007, section 7.1.6.1 and tables 123/124."
 ::= { t11FcSpPoNaSwConnEntry 5 }

```

```

t11FcSpPoNaSwConnAllowedName OBJECT-TYPE
SYNTAX          FcNameIdOrZero (SIZE (8))
MAX-ACCESS      read-create
STATUS          current
DESCRIPTION
    "If t11FcSpPoNaSwConnAllowedNameType has the value
    'wildcard' or 'restrictedWildcard', this object has the
    value '0000000000000000'h.

    Otherwise, the combination of

```

```

t11FcSpPoNaSwConnAllowedNameType and
t11FcSpPoNaSwConnAllowedName specify the name of:

- a Switch (if t11FcSpPoNaSwConnAllowedType = 'switch'), or
- a Node (if t11FcSpPoNaSwConnAllowedType = 'node')

```

to which connectivity is allowed/not allowed."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.6.1](#) and tables 123/124."

::= { t11FcSpPoNaSwConnEntry 6 }

t11FcSpPoNaSwConnRowStatus OBJECT-TYPE

SYNTAX RowStatus  
MAX-ACCESS read-create  
STATUS current  
DESCRIPTION

"The status of this row. Values of object instances  
within the row can be modified at any time."

::= { t11FcSpPoNaSwConnEntry 7 }

--

-- IP Management Entries in Non-Active IP Management List Objects

--

t11FcSpPoNaIpMgmtTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpPoNaIpMgmtEntry  
MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION

"A table of IP Management Entries in non-active IP  
Management List Objects. The IP Management List Object is a  
Fabric-wide Policy Object that describes which IP hosts are  
allowed to manage a Fabric.

One non-active IP Management List Object is represented by  
all rows of this table which have the same values of  
fcmInstanceIndex and t11FcSpPoFabricIndex."

::= { t11FcSpPoNonActive 7 }

t11FcSpPoNaIpMgmtEntry OBJECT-TYPE

SYNTAX T11FcSpPoNaIpMgmtEntry  
MAX-ACCESS not-accessible



STATUS           current  
DESCRIPTION

"Each entry contains information about one IP Management entry within a non-active IP Management List Object for the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIndex.

The Policy Object Name of an IP Management Entry Policy Object is either an IPv6 Address Range or an IPv4 Address Range. In a Fabric's database of Policy Objects, every Policy Object Name, including these IP address ranges, is represented as a (T11FcSpPolicyNameType, T11FcSpPolicyName) tuple. In contrast, this MIB module uses the conventional MIB syntax for IP addresses, and therefore represents the Policy Object Name of an IP Management Entry Policy Object as a (InetAddressType, InetAddress, InetAddress) tuple.

In theory, the use of t11FcSpPoNaIpMgmtEntryNameLow and t11FcSpPoNaIpMgmtEntryNameHigh, which have the syntax of InetAddress, in the INDEX could cause the need for excessively-long OIDs. In practice, this can't happen because FC-SP doesn't allow these objects to be specified as DNS names.

The StorageType of a row in this table is specified by the instance of t11FcSpPoStorageType which is INDEX-ed by the same values of fcmInstanceIndex and t11FcSpPoFabricIndex."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,  
          t11FcSpPoNaIpMgmtListName,  
          t11FcSpPoNaIpMgmtEntryNameType,  
          t11FcSpPoNaIpMgmtEntryNameLow,  
          t11FcSpPoNaIpMgmtEntryNameHigh }  
::= { t11FcSpPoNaIpMgmtTable 1 }

T11FcSpPoNaIpMgmtEntry ::= SEQUENCE {  
    t11FcSpPoNaIpMgmtListName       T11FcSpAlphaNumName,  
    t11FcSpPoNaIpMgmtEntryNameType   InetAddressType,  
    t11FcSpPoNaIpMgmtEntryNameLow    InetAddress,  
    t11FcSpPoNaIpMgmtEntryNameHigh   InetAddress,  
    t11FcSpPoNaIpMgmtWkpIndex        Unsigned32,  
    t11FcSpPoNaIpMgmtAttribute       T11FcSpAlphaNumNameOrAbsent,  
    t11FcSpPoNaIpMgmtRowStatus       RowStatus  
}

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

**t11FcSpPoNaIpMgmtListName OBJECT-TYPE**

SYNTAX            T11FcSpAlphaNumName

MAX-ACCESS       not-accessible

STATUS            current

**DESCRIPTION**

"The name of a non-active Node Membership List Object."

**REFERENCE**

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.7.1](#) and table 125."

::= { t11FcSpPoNaIpMgmtEntry 1 }

**t11FcSpPoNaIpMgmtEntryNameType OBJECT-TYPE**

SYNTAX            InetAddressType { ipv4(1), ipv6(2) }

MAX-ACCESS       not-accessible

STATUS            current

**DESCRIPTION**

"The combination of t11FcSpPoNaIpMgmtEntryNameType,  
t11FcSpPoNaIpMgmtNameLow and t11FcSpPoNaIpMgmtNameHigh  
specify the IP Address range of this IP Management  
Entry in the IP Management List Object.

The FC-SP specification does not allow this address to  
be specified using a DNS domain name, nor does it allow  
the specification of zone indexes. Therefore, the  
type of address must be one of: 'ipv4', or 'ipv6'."

**REFERENCE**

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, sections [7.1.7.1](#) and table 126."

::= { t11FcSpPoNaIpMgmtEntry 2 }

**t11FcSpPoNaIpMgmtEntryNameLow OBJECT-TYPE**

SYNTAX            InetAddress (SIZE(4 | 16))

MAX-ACCESS       not-accessible

STATUS            current

**DESCRIPTION**

"The lower end of an Internet address range. The type  
of this address is given by the corresponding instance  
of t11FcSpPoNaIpMgmtEntryNameType.

The combination of t11FcSpPoNaIpMgmtEntryNameType,  
t11FcSpPoNaIpMgmtNameLow and t11FcSpPoNaIpMgmtNameHigh

specify the IP Address range of this IP Management Entry in the IP Management List Object."

Expires 11 January 2009

[Page 138]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

#### REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, sections [7.1.7.1](#) and table 126."

::= { t11FcSpPoNaIpMgmtEntry 3 }

#### t11FcSpPoNaIpMgmtEntryNameHigh OBJECT-TYPE

SYNTAX            InetAddress (SIZE(4 | 16))

MAX-ACCESS       not-accessible

STATUS            current

#### DESCRIPTION

"The higher end of an Internet address range. The type of this address is given by the corresponding instance of t11FcSpPoNaIpMgmtEntryNameType.

The combination of t11FcSpPoNaIpMgmtEntryNameType, t11FcSpPoNaIpMgmtNameLow and t11FcSpPoNaIpMgmtNameHigh specify the IP Address range of this IP Management Entry in the IP Management List Object."

#### REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, sections [7.1.7.1](#) and table 126."

::= { t11FcSpPoNaIpMgmtEntry 4 }

#### t11FcSpPoNaIpMgmtWkpIndex OBJECT-TYPE

SYNTAX            Unsigned32 (0..4294967295)

MAX-ACCESS       read-create

STATUS            current

#### DESCRIPTION

"This object identifies the restrictions for IP management access by IP hosts in this range of IP addresses.

The restrictions are specified as the set of Well Known Protocols Access Descriptors contained in those rows of the t11FcSpPoNaWkpDescrTable for which the value of t11FcSpPoNaWkpDescrSpecifierIndx is the same as the value

of this object. If there are no such rows or if the value of this object is zero, then this IP Management Entry does not identify any Well Known Protocols Access restrictions."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.7.1](#) and tables 127/129."

::= { t11FcSpPoNaIpMgmtEntry 5 }

Expires 11 January 2009

[Page 139]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpPoNaIpMgmtAttribute OBJECT-TYPE

SYNTAX            T11FcSpAlphaNumNameOrAbsent

MAX-ACCESS       read-create

STATUS            current

DESCRIPTION

"The name of a non-active Attribute Policy Object which is defined for this IP Management entry. The zero-length string indicates that no non-active Attribute Policy Object is defined for it.

The effect of having no rows in the t11FcSpPoNaAttribTable for which the value of t11FcSpPoNaAttribName is the same as the value of this object, is the same as this object's value being the zero-length string."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.7.1](#) and table 128."

::= { t11FcSpPoNaIpMgmtEntry 6 }

t11FcSpPoNaIpMgmtRowStatus OBJECT-TYPE

SYNTAX            RowStatus

MAX-ACCESS       read-create

STATUS            current

DESCRIPTION

"The status of this row. Values of object instances within the row can be modified at any time."

::= { t11FcSpPoNaIpMgmtEntry 7 }

--  
--  
--

-- Non-Active Well-Known Protocol Access Descriptors

t11FcSpPoNaWkpDescrTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpPoNaWkpDescrEntry

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"A table of the Well-Known Protocol Access Descriptors  
referenced from non-active Policy Objects.

A Well-Known Protocol Access Specifier is a list of  
Well-Known Protocol Access Descriptors each of which  
specifies a protocol number, a port number and/or various  
flags specifying how IP management access is restricted.

A non-active Well-Known Protocol Transport Access Specifier  
is represented by all rows of this table which have the same  
values of fcmInstanceIndex, t11FcSpPoFabricIndex, and  
t11FcSpPoNaWkpDescrSpecifierIndx."

::= { t11FcSpPoNonActive 8 }

t11FcSpPoNaWkpDescrEntry OBJECT-TYPE

SYNTAX            T11FcSpPoNaWkpDescrEntry

MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION

"Each entry contains information about one Well-Known Protocol Access Descriptor of a non-active Well-Known Protocol Access Specifier used within the Fabric identified by t11FcSpPoFabricIndex and managed within the Fibre Channel management instance identified by fcmInstanceIdIndex.

The StorageType of a row in this table is specified by the instance of t11FcSpPoStorageType which is INDEX-ed by the same values of fcmInstanceIdIndex and t11FcSpPoFabricIndex."

INDEX { fcmInstanceIdIndex, t11FcSpPoFabricIndex,  
t11FcSpPoNaWkpDescrSpecifierIndx,  
t11FcSpPoNaWkpDescrIndex }  
::= { t11FcSpPoNaWkpDescrTable 1 }

T11FcSpPoNaWkpDescrEntry ::= SEQUENCE {  
t11FcSpPoNaWkpDescrSpecifierIndx Unsigned32,  
t11FcSpPoNaWkpDescrIndex Unsigned32,

Expires 11 January 2009

[Page 141]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

t11FcSpPoNaWkpDescrFlags BITS,  
t11FcSpPoNaWkpDescrWkpNumber Unsigned32,  
t11FcSpPoNaWkpDescrDestPort InetPortNumber,  
t11FcSpPoNaWkpDescrRowStatus RowStatus  
}

t11FcSpPoNaWkpDescrSpecifierIndx OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)  
MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION

"An index value which uniquely identifies a particular non-active Well-Known Protocol Access Specifier within a Fabric."

::= { t11FcSpPoNaWkpDescrEntry 1 }

t11FcSpPoNaWkpDescrIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)  
MAX-ACCESS not-accessible

STATUS           current  
DESCRIPTION  
    "An index value which uniquely identifies a particular  
    Well-Known Protocol Access Descriptor within a  
    non-active Well-Known Protocol Access Specifier."  
 ::= { t11FcSpPoNaWkpDescrEntry 2 }

t11FcSpPoNaWkpDescrFlags OBJECT-TYPE

SYNTAX           BITS {  
                    allow(0),  
                    wkpWildcard(1),  
                    destPortWildcard(2),  
                    readOnly(3)  
                  }

MAX-ACCESS       read-create

STATUS           current

DESCRIPTION  
    "The flag bits which specify how access is to be limited by  
    this Well-Known Protocol Access Descriptor:

- allow -- IP management access using this protocol/port  
is allowed if this bit is set, and to be denied if this  
bit is not set.
- wkpWildcard -- if this bit is set, the IP Protocol number  
of the Well-Known Protocol to be allowed/denied is

Expires 11 January 2009

[Page 142]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

specified by the value of t11FcSpPoNaWkpDescrWkpNumber.

- destPortWildcard -- if this bit is set, the Destination  
(TCP/UDP) Port number of the Well-Known Protocol to be  
allowed/denied is specified by the value of  
t11FcSpPoNaWkpDescrDestPort.
- readOnly -- if this bit is set then access is to be  
granted only for reading."

REFERENCE

- "- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.7.1](#) and table 131."

::= { t11FcSpPoNaWkpDescrEntry 3 }

t11FcSpPoNaWkpDescrWkpNumber OBJECT-TYPE

SYNTAX Unsigned32 (0..255)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"When the 'wkpWildcard' bit is set in the corresponding instance of t11FcSpPoNaWkpDescrFlags, this object specifies the IP protocol number of the Well-Known Protocol."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.7.1](#) and table 131.  
- <http://www.iana.org/assignments/protocol-numbers>."

::= { t11FcSpPoNaWkpDescrEntry 4 }

t11FcSpPoNaWkpDescrDestPort OBJECT-TYPE

SYNTAX InetPortNumber

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"When the 'destPortWildcard' bit is set in the corresponding instance of t11FcSpPoNaWkpDescrFlags, this object specifies the Destination (TCP/UDP) Port number of the Well-Known Protocol. When the 'destPortWildcard' bit is reset, this object is ignored (and can have the value zero)."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.1.7.1](#) and table 131.  
- <http://www.iana.org/assignments/port-numbers>."

Expires 11 January 2009

[Page 143]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

::= { t11FcSpPoNaWkpDescrEntry 5 }

t11FcSpPoNaWkpDescrRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION



```

        "The status of this row.  Values of object instances
        within the row can be modified at any time."
 ::= { t11FcSpPoNaWkpDescrEntry 6 }

--
-- Attribute Entries in Non-Active Attribute Policy Objects
--

t11FcSpPoNaAttribTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF T11FcSpPoNaAttribEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A table of the Attribute Policy Objects being used within
        non-active Policy Objects.

        A non-active Attribute Policy Object is represented by all
        the Attribute Entries in this table which have the same
        value of t11FcSpPoNaAttribName."
 ::= { t11FcSpPoNonActive 9 }

t11FcSpPoNaAttribEntry OBJECT-TYPE
    SYNTAX      T11FcSpPoNaAttribEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Each entry contains information about one Attribute
        Entry contained within an Attribute Policy Object
        which is non-active within the Fabric identified by
        t11FcSpPoFabricIndex and managed within the Fibre Channel
        management instance identified by fcmInstanceIndex.

        For some types of Attribute Policy Objects, it is valuable
        to break-out some semantically-significant parts of the
        Policy Object's value into their own individual MIB
        objects; for example, to extract the one or more individual
        Authentication Protocol Identifiers and associated

```

containing a 'AUTH\_Negotiate Message Payload'. For such types, another MIB table is defined to hold the extracted values in MIB objects specific to the Attribute Policy Object's type. In such cases, the t11FcSpPoNaAttribExtension object in this table points to the other MIB table.

If the value of one Attribute Entry is too large (more than 256 bytes) to be contained within the value of one instance of t11FcSpPoNaAttribValue, then one row in this table contains the first 256 bytes, and one (or more) other row(s) in this table contain the rest of the value.

The StorageType of a row in this table is specified by the instance of t11FcSpPoStorageType which is INDEX-ed by the same values of fcmInstanceIndex and t11FcSpPoFabricIndex."

```
INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex,
        t11FcSpPoNaAttribName, t11FcSpPoNaAttribEntryIndex,
        t11FcSpPoNaAttribPartIndex }
 ::= { t11FcSpPoNaAttribTable 1 }
```

```
T11FcSpPoNaAttribEntry ::= SEQUENCE {
    t11FcSpPoNaAttribName      T11FcSpAlphaNumName,
    t11FcSpPoNaAttribEntryIndex Unsigned32,
    t11FcSpPoNaAttribPartIndex Unsigned32,
    t11FcSpPoNaAttribType      Unsigned32,
    t11FcSpPoNaAttribValue      OCTET STRING,
    t11FcSpPoNaAttribExtension  OBJECT IDENTIFIER,
    t11FcSpPoNaAttribRowStatus  RowStatus
}
```

```
t11FcSpPoNaAttribName OBJECT-TYPE
    SYNTAX      T11FcSpAlphaNumName
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "The name of the Attribute Policy Object containing one
        or more Attribute Entries."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
        Fibre Channel - Security Protocols (FC-SP),
        February 2007, section 7.1.8.1 and table 133."
    ::= { t11FcSpPoNaAttribEntry 1 }
```

**t11FcSpPoNaAttribEntryIndex OBJECT-TYPE**

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS not-accessible

STATUS current

**DESCRIPTION**

"A unique value to distinguish this Attribute Entry from other Attribute Entries contained in the same Attribute Policy Object."

**REFERENCE**

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.8.1](#), tables 133/134."

::= { t11FcSpPoNaAttribEntry 2 }

**t11FcSpPoNaAttribPartIndex OBJECT-TYPE**

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS not-accessible

STATUS current

**DESCRIPTION**

"When the value of an Attribute Entry is shorter than 257 bytes, the whole value is contained in one instance of t11FcSpPoNaAttribValue, and the value of this object is 1.

If the value of an Attribute Entry is longer than 256 bytes, then that value is divided up on 256 byte boundaries such that all parts are 256 bytes long except the last part which is shorter if necessary, with each such part contained in a separate row of this table, and the value of this object is set to the part number. That is, this object has the value of 1 for bytes 0-255, the value of 2 for bytes 256-511, ... etc."

**REFERENCE**

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 7.1.8.1](#), tables 134/135."

::= { t11FcSpPoNaAttribEntry 3 }

**t11FcSpPoNaAttribType OBJECT-TYPE**

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS read-create

STATUS current

**DESCRIPTION**

"The type of attribute. The first type to be defined is:

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpPoNaAttribType	t11FcSpPoNaAttribValue
=====	=====
'00000001'h	The AUTH_Negotiate Message Payload
"	

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP), February 2007,  
[section 7.1.8.1](#), tables 134/135 and table 10."

::= { t11FcSpPoNaAttribEntry 4 }

## t11FcSpPoNaAttribValue OBJECT-TYPE

SYNTAX            OCTET STRING (SIZE (0..256))

MAX-ACCESS      read-create

STATUS           current

## DESCRIPTION

"The value of an Attribute Entry is divided up on 256 byte boundaries such that all parts are 256 bytes long except the last part which is shorter if necessary, and each such part is contained in a separate instance of this object.

When the value of the corresponding instance of t11FcSpPoNaAttribExtension is not zeroDotZero, then the same underlying management data has its value contained both in this object and in the individual/broken-out parts pointed to by t11FcSpPoNaAttribExtension. Thus, after any modification of the underlying management data, e.g., after a Set operation to the value of either MIB representation, then that modification is reflected in the values of both MIB representations."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP), February 2007,  
[section 7.1.8.1](#), tables 134/135 and table 10."

::= { t11FcSpPoNaAttribEntry 5 }

## t11FcSpPoNaAttribExtension OBJECT-TYPE

SYNTAX            OBJECT IDENTIFIER

MAX-ACCESS      read-only

STATUS           current

## DESCRIPTION

"For some types of Attribute Policy Object, the value of

this MIB object points to type-specific MIB objects which contain individual/broken-out parts of the Attribute Policy Object's value. If this object doesn't point to such type-specific MIB objects, then it contains the value:

Expires 11 January 2009

[Page 147]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

zeroDotZero.

In particular, when the value of `t11FcSpPoNaAttribType` indicates 'AUTH\_Negotiate Message Payload', one or more Authentication Protocol Identifiers and their associated Authentication Protocol Parameters are embedded within the value of the corresponding instance of `t11FcSpPoNaAttribValue`; MIB objects to contain these individual values are defined in the `t11FcSpPoNaAuthProtTable`. Thus, for an 'AUTH\_Negotiate Message Payload' Attribute, the value of this object would contain the OID of `t11FcSpPoNaAuthProtTable`.

When the value of this object is not `zeroDotZero`, then the same underlying management data has its value contained in both the individual/broken-out parts pointed to by this object and in the corresponding instance of `t11FcSpPoNaAttribValue`. Thus, after any modification of the underlying management data, e.g., after a Set operation to the value of either MIB representation, then that modification is reflected in the values of both MIB representations."

::= { t11FcSpPoNaAttribEntry 6 }

`t11FcSpPoNaAttribRowStatus` OBJECT-TYPE

SYNTAX            RowStatus  
MAX-ACCESS       read-create  
STATUS            current  
DESCRIPTION

"The status of this row. Values of object instances within the row can be modified at any time."

::= { t11FcSpPoNaAttribEntry 7 }

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--  
-- Auth. Protocol Parameters in Non-Active Attribute Policy Objects  
--

**t11FcSpPoNaAuthProtTable OBJECT-TYPE**

SYNTAX            SEQUENCE OF T11FcSpPoNaAuthProtEntry

MAX-ACCESS       not-accessible

STATUS            current

**DESCRIPTION**

"A table of Authentication Protocol Identifier and Authentication Protocol Parameters which are embedded in Attribute Policy Objects being used within non-active Policy Objects.

This table is used for Attribute Entries of Attribute Policy Objects for which the value of t11FcSpPoNaAttribType indicates 'AUTH\_Negotiate Message Payload' and the value of t11FcSpPoNaAttribExtension contains the OID of this table."

**REFERENCE**

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, sections [5.3.2](#) & 7.1.8.1, tables 134/135 and tables 10/11."

::= { t11FcSpPoNonActive 10 }

**t11FcSpPoNaAuthProtEntry OBJECT-TYPE**

SYNTAX            T11FcSpPoNaAuthProtEntry

MAX-ACCESS       not-accessible

STATUS            current

## DESCRIPTION

"Each row contains information about an Authentication Protocol which is extracted out of the Attribute Entry (identified by `t11FcSpPoNaAttribEntryIndex`) of the non-active Policy Attribute Object (identified by `t11FcSpPoNaAttribName`) for the Fabric identified by `t11FcSpPoFabricIndex` and managed within the Fibre Channel management instance identified by `fcmInstanceIndex`.

If the value of one Attribute Protocol Parameters string is too large (more than 256 bytes) to be contained within the value of one instance of `t11FcSpPoNaAuthProtParams`, then one row in this table contains the first 256 bytes, and one (or more) other row(s) in this table contain the rest of the value.

Expires 11 January 2009

[Page 149]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

The same underlying management data which is represented in rows of this table is also represented by the corresponding instances of `t11FcSpPoNaAttribValue`. Thus, after any modification of the underlying management data, e.g., after a Set operation to the value of either MIB representation, then that modification is reflected in the values of both MIB representations."

INDEX { `fcmInstanceIndex`, `t11FcSpPoFabricIndex`,  
          `t11FcSpPoNaAttribName`, `t11FcSpPoNaAttribEntryIndex`,  
          `t11FcSpPoNaAuthProtIdentifier`,  
          `t11FcSpPoNaAuthProtPartIndex` }  
 ::= { `t11FcSpPoNaAuthProtTable 1` }

`T11FcSpPoNaAuthProtEntry` ::= SEQUENCE {  
    `t11FcSpPoNaAuthProtIdentifier`    Unsigned32,  
    `t11FcSpPoNaAuthProtPartIndex`    Unsigned32,  
    `t11FcSpPoNaAuthProtParams`       OCTET STRING,  
    `t11FcSpPoNaAuthProtRowStatus`    RowStatus  
}

`t11FcSpPoNaAuthProtIdentifier` OBJECT-TYPE  
SYNTAX            Unsigned32 (0..4294967295)  
MAX-ACCESS       not-accessible

STATUS current

DESCRIPTION

"The Authentication Protocol Identifier:

1 = DH-CHAP

3 = FCPAP

4 = IKEv2

5 = IKEv2-AUTH

240 thru 255 = Vendor Specific Protocols

all other values are 'Reserved' (by T11)."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 5.3.2](#), table 11."

::= { t11FcSpPoNaAuthProtEntry 1 }

t11FcSpPoNaAuthProtPartIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

Expires 11 January 2009

[Page 150]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

"When the value of an Attribute Protocol Parameters string is shorter than 257 bytes, the whole value is contained in one instance of t11FcSpPoNaAuthProtParams, and the value of this object is 1. (This includes the case when the Attribute Protocol Parameters string is zero bytes in length.)

If the value of an Authentication Protocol Parameters string is longer than 256 bytes, then that value is divided up on 256 byte boundaries such that all parts are 256 bytes long except the last part which is shorter if necessary, with each such part contained in a separate row of this table, and the value of this object is set to the part number. That is, this object has the value of 1 for bytes 0-255, the value of 2 for bytes 256-511, ... etc."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),



February 2007, [section 5.3.2](#), table 10."  
 ::= { t11FcSpPoNaAuthProtEntry 2 }

t11FcSpPoNaAuthProtParams OBJECT-TYPE

SYNTAX OCTET STRING (SIZE (0..256))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The value of an Authentication Protocol Parameters string is divided up on 256 byte boundaries such that all parts are 256 bytes long except the last part which is shorter if necessary, and each such part is contained in a separate instance of this object."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 5.3.2](#), table 10."

::= { t11FcSpPoNaAuthProtEntry 3 }

t11FcSpPoNaAuthProtRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The status of this row. Values of object instances within the row can be modified at any time."

::= { t11FcSpPoNaAuthProtEntry 4 }

Expires 11 January 2009

[Page 151]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--

-- Part 4 - Statistics

--

t11FcSpPoStatsTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpPoStatsEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of statistics maintained by FC-SP Security Policy Servers."

```
::= { t11FcSpPoStatistics 1 }
```

t11FcSpPoStatsEntry OBJECT-TYPE

SYNTAX T11FcSpPoStatsEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A set of statistics for the FC-SP Security Policy Server on the Fabric identified by the value of t11FcSpPoFabricIndex, and managed within the Fibre Channel management instance identified by fcmInstanceIndex."

INDEX { fcmInstanceIndex, t11FcSpPoFabricIndex }

```
::= { t11FcSpPoStatsTable 1 }
```

T11FcSpPoStatsEntry ::= SEQUENCE {

t11FcSpPoInRequests Counter32,

t11FcSpPoInAccepts Counter32,

t11FcSpPoInRejects Counter32

}

t11FcSpPoInRequests OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of FC-SP Policy Management Requests (e.g., GPS, APS, etc.) received by this FC-SP Security Policy Server on this Fabric.

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),

```
::= { t11FcSpPoStatsEntry 1 }
```

t11FcSpPoInAccepts OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only  
STATUS current  
DESCRIPTION

"The number of times that this FC-SP Security Policy Server sent an Accept CT\_IU on this Fabric in response to a received FC-SP Policy Management Request (e.g., GPS, APS, etc.).

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.3](#)."

::= { t11FcSpPoStatsEntry 2 }

t11FcSpPoInRejects OBJECT-TYPE

SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION

"The number of times that this FC-SP Security Policy Server sent a Reject CT\_IU on this Fabric in response to a received FC-SP Policy Management Request (e.g., GPS, APS, etc.).

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.3](#)."

::= { t11FcSpPoStatsEntry 3 }

--  
-- Part 5 - Control Information & Notifications  
--

--  
-- Control Information  
--

t11FcSpPoServerAddress OBJECT-TYPE

SYNTAX FcNameIdOrZero  
MAX-ACCESS accessible-for-notify  
STATUS current

DESCRIPTION

"The WWN of the FC-SP Security Policy Server which  
received a request which is referenced in a  
notification."

::= { t11FcSpPoControl 1 }

t11FcSpPoControlTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpPoControlEntry  
MAX-ACCESS not-accessible  
STATUS current

DESCRIPTION

"A table of control information, including the memory  
realization of FC-SP Policy Databases, and concerning  
the generation of notifications due to FC-SP  
Policy-related events."

::= { t11FcSpPoControl 2 }

t11FcSpPoControlEntry OBJECT-TYPE

SYNTAX T11FcSpPoControlEntry  
MAX-ACCESS not-accessible  
STATUS current

DESCRIPTION

"Each entry contains control information specific to FC-SP  
Policy and Policy-related events for the Fabric identified  
by the value of t11FcSpPoFabricIndex, and managed within  
the Fibre Channel management instance identified by  
fcmInstanceIdIndex."

INDEX { fcmInstanceIdIndex, t11FcSpPoFabricIndex }

::= { t11FcSpPoControlTable 1 }

T11FcSpPoControlEntry ::= SEQUENCE {

t11FcSpPoStorageType StorageType,

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpPoNotificationEnable	TruthValue,
t11FcSpPoLastNotifyType	INTEGER,
t11FcSpPoRequestSource	FcNameIdOrZero,
t11FcSpPoReasonCode	T11NsGs4RejectReasonCode,
t11FcSpPoCtCommandString	OCTET STRING,
t11FcSpPoReasonCodeExp	Unsigned32,
t11FcSpPoReasonVendorCode	OCTET STRING

}

t11FcSpPoStorageType OBJECT-TYPE

SYNTAX            StorageType

MAX-ACCESS      read-write

STATUS           current

DESCRIPTION

"This object specifies the memory realization of FC-SP Policy Objects and related information for a particular Fabric; specifically, for:

- rows created and/or modified for the particular Fabric in these tables:

```

t11FcSpPoNaSummaryTable
t11FcSpPoNaSwListTable
t11FcSpPoNaSwMembTable
t11FcSpPoNaNoMembTable
t11FcSpPoNaCtDescrTable
t11FcSpPoNaSwConnTable
t11FcSpPoNaIpMgmtTable
t11FcSpPoNaWkpDescrTable
t11FcSpPoNaAttribTable

```

- the activate and deactivate actions invoked through the t11FcSpPoOperActivate and t11FcSpPoOperDeActivate objects for the particular Fabric; and
- modified information contained in the same row as an instance of this object.

Even if an instance of this object has the value 'permanent(4)', none of the information defined in this MIB module for the given Fabric needs to be writable."

```
::= { t11FcSpPoControlEntry 1 }
```

**t11FcSpPoNotificationEnable OBJECT-TYPE**

SYNTAX            TruthValue

MAX-ACCESS       read-write

STATUS            current

**DESCRIPTION**

"This object specifies whether the following types of notifications:

t11FcSpPoNotifyActivation,  
t11FcSpPoNotifyActivateFail,  
t11FcSpPoNotifyDeactivation and  
t11FcSpPoNotifyDeactivateFail

should be generated for this Fabric."

::= { t11FcSpPoControlEntry 2 }

**t11FcSpPoLastNotifyType OBJECT-TYPE**

SYNTAX            INTEGER {  
                  none(1),  
                  activation(2),  
                  activateFail(3),  
                  deactivation(4),  
                  deactivateFail(5)  
                  }

MAX-ACCESS       read-only

STATUS            current

**DESCRIPTION**

"An indication of which of the following types of notification is currently being/was most recently generated for the Fabric:

'activation'        -- t11FcSpPoNotifyActivation  
'activateFail'     -- t11FcSpPoNotifyActivateFail  
'deactivation'      -- t11FcSpPoNotifyDeactivation  
'deactivateFail'   -- t11FcSpPoNotifyDeactivateFail

The value 'none' indicates that none of these types of

notifications have been generated since the last restart of the network management system, and therefore that the corresponding instances of: t11FcSpPoRequestSource, t11FcSpPoReasonCode, t11FcSpPoCtCommandString, t11FcSpPoReasonCodeExp and t11FcSpPoReasonVendorCode are irrelevant."

::= { t11FcSpPoControlEntry 3 }

Expires 11 January 2009

[Page 156]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpPoRequestSource OBJECT-TYPE

SYNTAX            FcNameIdOrZero

MAX-ACCESS       read-only

STATUS            current

DESCRIPTION

"The WWN of the source of the (Activate Policy Summary or Deactivate Policy Summary) request for which the current/most recent notification of the type indicated by the corresponding instance of t11FcSpPoLastNotifyType is being/was generated.

If no source is available, the value of this object is the zero-length string."

DEFVAL { "" }

::= { t11FcSpPoControlEntry 4 }

t11FcSpPoReasonCode OBJECT-TYPE

SYNTAX            T11NsGs4RejectReasonCode

MAX-ACCESS       read-only

STATUS            current

DESCRIPTION

"The reason code associated with the failure which is indicated when the value of the corresponding instance of t11FcSpPoLastNotifyType is 'activateFail' or 'deactivateFail'.

For other values of t11FcSpPoLastNotifyType, the value of this object is 'none(1)'."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),

February 2007, [section 7.3.6.2](#) & 7.3.6.3"  
 ::= { t11FcSpPoControlEntry 5 }

t11FcSpPoCtCommandString OBJECT-TYPE

SYNTAX OCTET STRING (SIZE (0..255))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The binary content of the failed request which is indicated when the value of the corresponding instance of t11FcSpPoLastNotifyType is 'activateFail' or 'deactivateFail'. The content of the request is formatted as an octet string (in network byte order) containing the CT\_IU, as described in Table 2 of [[FC-GS-5](#)] (including the

Expires 11 January 2009

[Page 157]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

preamble).

For other values of t11FcSpPoLastNotifyType, or if the CT\_IU's content is unavailable, the value of this object is the zero-length string.

When the length of this object is 255 octets, it contains the first 255 octets of the CT\_IU (in network-byte order)."

::= { t11FcSpPoControlEntry 6 }

t11FcSpPoReasonCodeExp OBJECT-TYPE

SYNTAX Unsigned32 (0..255)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The reason code explanation associated with the failure which is indicated when the value of the corresponding instance of t11FcSpPoLastNotifyType is 'activateFail' or 'deactivateFail'.

For other values of t11FcSpPoLastNotifyType, the value of this object is zero."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,



Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.3.6.2](#) & 7.3.6.3"  
 ::= { t11FcSpPoControlEntry 7 }

t11FcSpPoReasonVendorCode OBJECT-TYPE

SYNTAX OCTET STRING (SIZE (0 | 1))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The vendor-specific reason code associated with the failure which is indicated when the value of the corresponding instance of t11FcSpPoLastNotifyType is 'activateFail' or 'deactivateFail'.

For other values of t11FcSpPoLastNotifyType, or if no vendor-specific reason code is available, the value of this object is the zero-length string."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),

Expires 11 January 2009

[Page 158]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

February 2007, [section 7.3.6.2](#) & 7.3.6.3"  
 ::= { t11FcSpPoControlEntry 8 }

--

-- Notification definitions

--

t11FcSpPoNotifyActivation NOTIFICATION-TYPE

OBJECTS { t11FcSpPoServerAddress,  
          t11FcSpPoPolicySummaryObjName,  
          t11FcSpPoRequestSource }

STATUS current

DESCRIPTION

"This notification is generated whenever a Security Policy Server (indicated by the value of t11FcSpPoServerAddress) successfully completes the execution of an Activate Policy Summary request. The value of t11FcSpPoRequestSource indicates

the source of the APS request. The value of t11FcSpPoPolicySummaryObjName indicates the name of the activated Policy Summary Object."  
 ::= { t11FcSpPoMIBNotifications 1 }

t11FcSpPoNotifyActivateFail NOTIFICATION-TYPE

OBJECTS { t11FcSpPoServerAddress,  
t11FcSpPoRequestSource,  
t11FcSpPoCtCommandString,  
t11FcSpPoReasonCode,  
t11FcSpPoReasonCodeExp,  
t11FcSpPoReasonVendorCode }

STATUS current

DESCRIPTION

"This notification is generated whenever a Security Policy Server (indicated by the value of t11FcSpPoServerAddress) fails to complete the execution of an Activate Policy Summary request.

The value of t11FcSpPoCtCommandString indicates the rejected request, and the values of t11FcSpPoReasonCode, t11FcSpPoReasonCodeExp and t11FcSpPoReasonVendorCode indicate the reason for the rejection. The value of t11FcSpPoRequestSource indicates the source of the request."

REFERENCE

Expires 11 January 2009

[Page 159]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.3.6.2](#)."  
 ::= { t11FcSpPoMIBNotifications 2 }

t11FcSpPoNotifyDeactivation NOTIFICATION-TYPE

OBJECTS { t11FcSpPoServerAddress,  
t11FcSpPoRequestSource }

STATUS current

DESCRIPTION

"This notification is generated whenever a Security Policy Server (indicated by the value of t11FcSpPoServerAddress) successfully completes the

execution of a Deactivate Policy Summary request.  
The value of t11FcSpPoRequestSource indicates  
the source of the DPS request."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 7.3.6.3](#)."

::= { t11FcSpPoMIBNotifications 3 }

t11FcSpPoNotifyDeactivateFail NOTIFICATION-TYPE

OBJECTS { t11FcSpPoServerAddress,  
t11FcSpPoRequestSource,  
t11FcSpPoCtCommandString,  
t11FcSpPoReasonCode,  
t11FcSpPoReasonCodeExp,  
t11FcSpPoReasonVendorCode }

STATUS current

DESCRIPTION

"This notification is generated whenever a Security Policy  
Server (indicated by the value of t11FcSpPoServerAddress)  
fails to complete the execution of a Deactivate Policy  
Summary request.

The value of t11FcSpPoCtCommandString indicates the  
rejected request, and the values of t11FcSpPoReasonCode,  
t11FcSpPoReasonCodeExp and t11FcSpPoReasonVendorCode  
indicate the reason for the rejection. The value of  
t11FcSpPoRequestSource indicates the source of the  
request."

::= { t11FcSpPoMIBNotifications 4 }

Expires 11 January 2009

[Page 160]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--

-- Conformance

--

t11FcSpPoMIBCompliances

OBJECT IDENTIFIER ::= { t11FcSpPoMIBConformance 1 }

t11FcSpPoMIBGroups      OBJECT IDENTIFIER ::= { t11FcSpPoMIBConformance 2 }

```

t11FcSpPoMIBCompliance MODULE-COMPLIANCE
    STATUS          current
    DESCRIPTION
        "The compliance statement for entities which
        support the Fabric Policies defined in FC-SP,"

MODULE -- this module
    MANDATORY-GROUPS { t11FcSpPoActiveObjectsGroup }

    GROUP          t11FcSpPoNonActiveObjectsGroup
    DESCRIPTION
        "These objects are mandatory for FC-SP Security Policy
        Servers."

    GROUP          t11FcSpPoNotifyObjectsGroup
    DESCRIPTION
        "These objects are mandatory for FC-SP Security Policy
        Servers."

    GROUP          t11FcSpPoNotificationGroup
    DESCRIPTION
        "These notifications are mandatory for FC-SP Security
        Policy Servers."

    GROUP          t11FcSpPoOperationsObjectsGroup
    DESCRIPTION
        "These objects are mandatory only for FC-SP Security
        Policy Servers which support the activation/deactivation
        of policies via SNMP."

    GROUP          t11FcSpPoStatsObjectsGroup
    DESCRIPTION
        "These objects are optional."

-- Write access is not required for any objects in this MIB module:

    OBJECT          t11FcSpPoOperActivate

```

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoOperDeActivate

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoStorageType

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNotificationEnable

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaSummaryPolicyNameType

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaSummaryPolicyName

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaSummaryHashStatus

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaSummaryRowStatus

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaSwListFabricName

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaSwListRowStatus

MIN-ACCESS    read-only

DESCRIPTION

"Write access is not required."

OBJECT        t11FcSpPoNaSwMembFlags

MIN-ACCESS    read-only

DESCRIPTION

"Write access is not required."

OBJECT        t11FcSpPoNaSwMembDomainID

MIN-ACCESS    read-only

DESCRIPTION

"Write access is not required."

OBJECT        t11FcSpPoNaSwMembPolicyDataRole

MIN-ACCESS    read-only

DESCRIPTION

"Write access is not required."

OBJECT        t11FcSpPoNaSwMembAuthBehaviour

MIN-ACCESS    read-only

DESCRIPTION

"Write access is not required."

OBJECT        t11FcSpPoNaSwMembAttribute

MIN-ACCESS    read-only

DESCRIPTION

"Write access is not required."

OBJECT        t11FcSpPoNaSwMembRowStatus

MIN-ACCESS    read-only

DESCRIPTION

"Write access is not required."

OBJECT        t11FcSpPoNaNoMembFlags

MIN-ACCESS    read-only

DESCRIPTION

"Write access is not required."

OBJECT        t11FcSpPoNaNoMembCtAccessIndex

MIN-ACCESS    read-only

DESCRIPTION

"Write access is not required."

OBJECT        t11FcSpPoNaNoMembAttribute

MIN-ACCESS      read-only

DESCRIPTION

    "Write access is not required."

OBJECT            t11FcSpPoNaNoMembRowStatus

MIN-ACCESS      read-only

DESCRIPTION

    "Write access is not required."

OBJECT            t11FcSpPoNaCtDescrFlags

MIN-ACCESS      read-only

DESCRIPTION

    "Write access is not required."

OBJECT            t11FcSpPoNaCtDescrGsType

MIN-ACCESS      read-only

DESCRIPTION

    "Write access is not required."

OBJECT            t11FcSpPoNaCtDescrGsSubType

MIN-ACCESS      read-only

DESCRIPTION

    "Write access is not required."

OBJECT            t11FcSpPoNaCtDescrRowStatus

MIN-ACCESS      read-only

DESCRIPTION

    "Write access is not required."

OBJECT            t11FcSpPoNaSwConnAllowedNameType

MIN-ACCESS      read-only

DESCRIPTION

    "Write access is not required."

OBJECT            t11FcSpPoNaSwConnAllowedName

MIN-ACCESS      read-only

DESCRIPTION

    "Write access is not required."

OBJECT            t11FcSpPoNaSwConnRowStatus

MIN-ACCESS      read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaIpMgmtWkpIndex

Expires 11 January 2009

[Page 164]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaIpMgmtAttribute

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaIpMgmtRowStatus

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaWkpDescrFlags

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaWkpDescrWkpNumber

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaWkpDescrDestPort

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaWkpDescrRowStatus

MIN-ACCESS read-only

DESCRIPTION

"Write access is not required."

OBJECT t11FcSpPoNaAttribType



```

MIN-ACCESS    read-only
DESCRIPTION
    "Write access is not required."

OBJECT        t11FcSpPoNaAttribValue
MIN-ACCESS    read-only
DESCRIPTION
    "Write access is not required."

OBJECT        t11FcSpPoNaAttribRowStatus

```

Expires 11 January 2009

[Page 165]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```

MIN-ACCESS    read-only
DESCRIPTION
    "Write access is not required."

OBJECT        t11FcSpPoNaAuthProtParams
MIN-ACCESS    read-only
DESCRIPTION
    "Write access is not required."

OBJECT        t11FcSpPoNaAuthProtRowStatus
MIN-ACCESS    read-only
DESCRIPTION
    "Write access is not required."

```

```
 ::= { t11FcSpPoMIBCompliances 1 }
```

-- Units of Conformance

```

t11FcSpPoActiveObjectsGroup OBJECT-GROUP
    OBJECTS {      t11FcSpPoPolicySummaryObjName,
                    t11FcSpPoAdminFabricName,
                    t11FcSpPoActivatedTimeStamp,
                    t11FcSpPoSummaryPolicyType,
                    t11FcSpPoSummaryHashFormat,
                    t11FcSpPoSummaryHashValue,
                    t11FcSpPoSwMembSwitchFlags,
                    t11FcSpPoSwMembDomainID,
                    t11FcSpPoSwMembPolicyDataRole,
                    t11FcSpPoSwMembAuthBehaviour,

```

```

t11FcSpPoSwMembAttribute,
t11FcSpPoNoMembFlags,
t11FcSpPoNoMembCtAccessIndex,
t11FcSpPoNoMembAttribute,
t11FcSpPoCtDescrFlags,
t11FcSpPoCtDescrGsType,
t11FcSpPoCtDescrGsSubType,
t11FcSpPoSwConnAllowedNameType,
t11FcSpPoSwConnAllowedName,
t11FcSpPoIpMgmtWkpIndex,
t11FcSpPoIpMgmtAttribute,
t11FcSpPoWkpDescrFlags,
t11FcSpPoWkpDescrWkpNumber,
t11FcSpPoWkpDescrDestPort,
t11FcSpPoAttribType,
t11FcSpPoAttribValue,

```

Expires 11 January 2009

[Page 166]

Internet Draft

Fibre-Channel Security Protocols MIB

July 2008

```

        t11FcSpPoAttribExtension,
        t11FcSpPoAuthProtParams
    }
STATUS    current
DESCRIPTION
    "A collection of MIB objects which contain information
    about active Policy Objects which express Fibre Channel
    Security (FC-SP) policy."
 ::= { t11FcSpPoMIBGroups 1 }

t11FcSpPoOperationsObjectsGroup OBJECT-GROUP
OBJECTS {
    t11FcSpPoOperActivate,
    t11FcSpPoOperDeActivate,
    t11FcSpPoOperResult,
    t11FcSpPoOperFailCause
}
STATUS    current
DESCRIPTION
    "A collection of MIB objects which allow a new set of
    Fibre Channel Security (FC-SP) policies to be activated
    or an existing set to be deactivated."
 ::= { t11FcSpPoMIBGroups 2 }

```

t11FcSpPoNonActiveObjectsGroup OBJECT-GROUP  
OBJECTS { t11FcSpPoStorageType,  
t11FcSpPoNaSummaryPolicyNameType,  
t11FcSpPoNaSummaryPolicyName,  
t11FcSpPoNaSummaryHashStatus,  
t11FcSpPoNaSummaryHashFormat,  
t11FcSpPoNaSummaryHashValue,  
t11FcSpPoNaSummaryRowStatus,  
t11FcSpPoNaSwListFabricName,  
t11FcSpPoNaSwListRowStatus,  
t11FcSpPoNaSwMembFlags,  
t11FcSpPoNaSwMembDomainID,  
t11FcSpPoNaSwMembPolicyDataRole,  
t11FcSpPoNaSwMembAuthBehaviour,  
t11FcSpPoNaSwMembAttribute,  
t11FcSpPoNaSwMembRowStatus,  
t11FcSpPoNaNoMembFlags,  
t11FcSpPoNaNoMembCtAccessIndex,  
t11FcSpPoNaNoMembAttribute,  
t11FcSpPoNaNoMembRowStatus,  
t11FcSpPoNaCtDescrFlags,  
t11FcSpPoNaCtDescrGsType,

Expires 11 January 2009

[Page 167]

---

Internet Draft

Fibre-Channel Security Protocols MIB

July 2008

t11FcSpPoNaCtDescrGsSubType,  
t11FcSpPoNaCtDescrRowStatus,  
t11FcSpPoNaSwConnAllowedNameType,  
t11FcSpPoNaSwConnAllowedName,  
t11FcSpPoNaSwConnRowStatus,  
t11FcSpPoNaIpMgmtWkpIndex,  
t11FcSpPoNaIpMgmtAttribute,  
t11FcSpPoNaIpMgmtRowStatus,  
t11FcSpPoNaWkpDescrFlags,  
t11FcSpPoNaWkpDescrWkpNumber,  
t11FcSpPoNaWkpDescrDestPort,  
t11FcSpPoNaWkpDescrRowStatus,  
t11FcSpPoNaAttribType,  
t11FcSpPoNaAttribValue,  
t11FcSpPoNaAttribExtension,  
t11FcSpPoNaAttribRowStatus,  
t11FcSpPoNaAuthProtParams,

```

        t11FcSpPoNaAuthProtRowStatus
    }
    STATUS    current
    DESCRIPTION
        "A collection of MIB objects which contain information
        about non-active Policy Objects available for activation
        in order to change Fibre Channel Security (FC-SP) policy."
    ::= { t11FcSpPoMIBGroups 3 }

t11FcSpPoStatsObjectsGroup OBJECT-GROUP
    OBJECTS {
        t11FcSpPoInRequests,
        t11FcSpPoInAccepts,
        t11FcSpPoInRejects
    }
    STATUS    current
    DESCRIPTION
        "A collection of MIB objects which contain statistics
        which can be maintained by FC-SP Security Policy Servers."
    ::= { t11FcSpPoMIBGroups 4 }

t11FcSpPoNotifyObjectsGroup OBJECT-GROUP
    OBJECTS {
        t11FcSpPoNotificationEnable,
        t11FcSpPoServerAddress,
        t11FcSpPoLastNotifyType,
        t11FcSpPoRequestSource,
        t11FcSpPoReasonCode,
        t11FcSpPoCtCommandString,
        t11FcSpPoReasonCodeExp,

```

Expires 11 January 2009

[Page 168]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```

        t11FcSpPoReasonVendorCode
    }
    STATUS    current
    DESCRIPTION
        "A collection of MIB objects to control the generation of
        notifications concerning Fibre Channel Security (FC-SP)
        policy, and to hold information contained in such
        notifications."
    ::= { t11FcSpPoMIBGroups 5 }

t11FcSpPoNotificationGroup NOTIFICATION-GROUP

```

```

NOTIFICATIONS {    t11FcSpPoNotifyActivation,
                   t11FcSpPoNotifyActivateFail,
                   t11FcSpPoNotifyDeactivation,
                   t11FcSpPoNotifyDeactivateFail
                   }
STATUS    current
DESCRIPTION
    "A collection of notifications of events concerning
    Fibre Channel Security (FC-SP) policy."
 ::= { t11FcSpPoMIBGroups 6 }

```

END

Expires 11 January 2009

[Page 169]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

## [6.5.](#) The T11-FC-SP-SA-MIB Module

```

--*****
-- FC-SP Security Associations

```

--

T11-FC-SP-SA-MIB DEFINITIONS ::= BEGIN

IMPORTS

```
MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE,
Unsigned32, Counter32, Counter64, TimeTicks, Gauge32,
mib-2                FROM SNMPv2-SMI                -- [RFC2578]
RowStatus, StorageType, AutonomousType, TimeStamp,
TruthValue           FROM SNMPv2-TC                 -- [RFC2579]
MODULE-COMPLIANCE, OBJECT-GROUP,
NOTIFICATION-GROUP
                                FROM SNMPv2-CONF       -- [RFC2580]

InterfaceIndex,
InterfaceIndexOrZero  FROM IF-MIB                   -- [RFC2863]
fcmInstanceIndex,
FcAddressIdOrZero     FROM FC-MGMT-MIB               -- [RFC4044]
T11FabricIndex        FROM T11-TC-MIB                -- [RFC4439]
T11FcSpType,
T11FcSpiIndex,
T11FcSpLifetimeLeft,
T11FcSpLifetimeLeftUnits,
T11FcSpSecurityProtocolId,
T11FcRoutingControl,
T11FcSaDirection,
T11FcSpPrecedence,
T11FcSpTransforms     FROM T11-FC-SP-TC-MIB;
```

t11FcSpSaMIB MODULE-IDENTITY

```
LAST-UPDATED "200801030000Z"
ORGANIZATION "This MIB module was developed through the
              coordinated effort of two organizations:
              T11 began the development and the IETF (in
              the IMSS Working Group) finished it."

CONTACT-INFO
    " Claudio DeSanti
      Cisco Systems, Inc.
      170 West Tasman Drive
      San Jose, CA 95134 USA
      EMail: cds@cisco.com
```

Expires 11 January 2009

[Page 170]

Keith McCloghrie  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134 USA  
Email: kzm@cisco.com"

#### DESCRIPTION

"This MIB module specifies the management information required to manage Security Associations established via Fibre Channel's FC-SP specification.

The MIB module consists of six parts:

- a per-Fabric table, t11FcSpSaIfTable, of capabilities, parameters, status information and counters; the counters include non-transient aggregates of per-SA transient counters;
- three tables, t11FcSpSaPropTable, t11FcSpSaTSelPropTable and t11FcSpSaTransTable, specifying the proposals for an FC-SP entity acting as an SA\_Initiator to present to the SA\_Responder during the negotiation of Security Associations. The same information is also used by an FC-SP entity acting as an SA\_Responder to decide what to accept during the negotiation of Security Associations. One of these tables, t11FcSpSaTransTable, is used not only for information about security transforms to propose and to accept, but also as agreed upon during the negotiation of Security Associations;
- a table, t11FcSpSaTSelDrByTable, of Traffic Selectors having the security action of 'drop' or 'bypass' to be applied either to ingress traffic which is unprotected by FC-SP, or to all egress traffic;
- four tables, t11FcSpSaPairTable, t11FcSpSaTSelNegInTable, t11FcSpSaTSelNegOutTable and t11FcSpSaTSelSpiTable, containing information about active bidirectional pairs of Security Associations; in particular, t11FcSpSaPairTable has one row per active bidirectional SA pair, t11FcSpSaTSelNegInTable and t11FcSpSaTSelNegOutTable contain information on the Traffic Selectors negotiated on the SAs, and the t11FcSpSaTSelSpiTable is an alternate lookup table such that the Traffic Selector(s) in use on a particular Security Association can be quickly determined based on the (ingress) SPI value;

- a table, t11FcSpSaControlTable, of control and other information concerning the generation of notifications for events related to FC-SP Security Associations;
- one notification, t11FcSpSaNotifyAuthFailure, generated on the occurrence of an Authentication failure for a received FC-2 or CT\_IU frame.

Copyright (C) The IETF Trust (2008). This version of this MIB module is part of RFC yyyy; see the RFC itself for full legal notices."

-- RFC Editor: replace yyyy with actual RFC number & remove this note  
REVISION "200801030000Z"

DESCRIPTION

"Initial version of this MIB module, published as RFCyyyy."

-- RFC-Editor, replace yyyy with actual RFC number & remove this note  
::= { mib-2 nnn } -- to be assigned by IANA

-- RFC Editor: replace nnn with IANA-assigned number & remove this note

t11FcSpSaMIBNotifications OBJECT IDENTIFIER ::= { t11FcSpSaMIB 0 }  
t11FcSpSaMIBObjects OBJECT IDENTIFIER ::= { t11FcSpSaMIB 1 }  
t11FcSpSaMIBConformance OBJECT IDENTIFIER ::= { t11FcSpSaMIB 2 }  
t11FcSpSaBase OBJECT IDENTIFIER ::= { t11FcSpSaMIBObjects 1 }  
t11FcSpSaConfig OBJECT IDENTIFIER ::= { t11FcSpSaMIBObjects 2 }  
t11FcSpSaActive OBJECT IDENTIFIER ::= { t11FcSpSaMIBObjects 3 }  
t11FcSpSaControl OBJECT IDENTIFIER ::= { t11FcSpSaMIBObjects 4 }



Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```
--
--
--
```

```
t11FcSpSaIfTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF T11FcSpSaIfEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A table containing per-Fabric information related to
        FC-SP Security Associations."
    ::= { t11FcSpSaBase 1 }
```

```
t11FcSpSaIfEntry OBJECT-TYPE
    SYNTAX      T11FcSpSaIfEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Each entry contains information related to Security
        Associations on a particular Fabric, and managed as part
        of the Fibre Channel management instance identified by
        fcmInstanceIndex."
    INDEX { fcmInstanceIndex, t11FcSpSaIfIndex,
            t11FcSpSaIfFabricIndex }
    ::= { t11FcSpSaIfTable 1 }
```

```
T11FcSpSaIfEntry ::= SEQUENCE {
    t11FcSpSaIfIndex      InterfaceIndexOrZero,
    t11FcSpSaIfFabricIndex T11FabricIndex,
    -- capabilities
    t11FcSpSaIfEspHeaderCapab T11FcSpTransforms,
    t11FcSpSaIfCTAuthCapab    T11FcSpTransforms,
    t11FcSpSaIfIKEv2Capab     T11FcSpTransforms,
    t11FcSpSaIfIkev2AuthCapab TruthValue,
    -- parameters and status
    t11FcSpSaIfStorageType    StorageType,
    t11FcSpSaIfReplayPrevention TruthValue,
```

```

t11FcSpSaIfReplayWindowSize    Unsigned32,
t11FcSpSaIfDeadPeerDetections Counter32,
t11FcSpSaIfTerminateAllSas     INTEGER,
    -- summary frame counters
t11FcSpSaIfOutDrops            Counter64,
t11FcSpSaIfOutBypasses        Counter64,
t11FcSpSaIfOutProcesses        Counter64,
t11FcSpSaIfOutUnMatcheds       Counter64,

```

Expires 11 January 2009

[Page 173]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```

    t11FcSpSaIfInUnprotUnmtchDrops Counter64,
        -- aggregates of per-SA transient counters
    t11FcSpSaIfInDetReplays          Counter64,
    t11FcSpSaIfInUnprotMtchDrops     Counter64,
    t11FcSpSaIfInBadXforms           Counter64,
    t11FcSpSaIfInGoodXforms          Counter64,
    t11FcSpSaIfInProtUnmtchs         Counter64
}

```

t11FcSpSaIfIndex OBJECT-TYPE

SYNTAX            InterfaceIndexOrZero

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"This object has a non-zero value to identify a particular interface, or the value zero to indicate that the information in this row applies to all (of the management instance's) interfaces to the particular Fabric.

If any row has a non-zero value of t11FcSpSaIfIndex, then all rows for the same Fibre Channel management instance must also have a non-zero value of t11FcSpSaIfIndex and thereby be specific to a particular interface.

As and when zero values of t11FcSpSaIfIndex are used in this table, then they must also be used in each other table which has t11FcSpSaIfIndex in its INDEX clause."

::= { t11FcSpSaIfEntry 1 }

t11FcSpSaIfFabricIndex OBJECT-TYPE

SYNTAX            T11FabricIndex

MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION  
    "An index value which uniquely identifies a particular  
    Fabric."  
 ::= { t11FcSpSaIfEntry 2 }

t11FcSpSaIfEspHeaderCapab OBJECT-TYPE  
SYNTAX T11FcSpTransforms  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION  
    "A list of the standardized transforms supported by this  
    entity on this interface for ESP\_Header protection."

Expires 11 January 2009

[Page 174]

---

Internet Draft      Fibre-Channel Security Protocols MIB      July 2008

REFERENCE  
    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
    Fibre Channel - Security Protocols (FC-SP),  
    February 2007, [Appendix A.3.1](#), tables A.23, A.25."  
 ::= { t11FcSpSaIfEntry 3 }

t11FcSpSaIfCTAuthCapab OBJECT-TYPE  
SYNTAX T11FcSpTransforms  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION  
    "A list of the standardized transforms supported by this  
    entity on this interface for CT\_Authentication protection."

REFERENCE  
    "- ANSI INCITS 426-2007, T11/Project 1570-D,  
    Fibre Channel - Security Protocols (FC-SP),  
    February 2007, [Appendix A.3.1](#), tables A.23, A.25."  
 ::= { t11FcSpSaIfEntry 4 }

t11FcSpSaIfIKEv2Capab OBJECT-TYPE  
SYNTAX T11FcSpTransforms  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION  
    "A list of the standardized transforms supported by this

entity on this interface with IKEv2 protection."  
REFERENCE  
"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [Appendix A.3.1](#), tables A.23, A.24,  
A.25, A.26."  
 ::= { t11FcSpSaIfEntry 5 }

t11FcSpSaIfIkev2AuthCapab OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"An indication of whether the entity is capable of supporting the IKEv2-AUTH protocol on this interface, i.e., concatenation of Authentication and SA Management Transactions, such that an SA Management Transaction is used to perform both the authentication function and SA management."

REFERENCE

Expires 11 January 2009

[Page 175]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 6.7.2](#), and table A.27."  
 ::= { t11FcSpSaIfEntry 6 }

t11FcSpSaIfStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This object specifies the memory realization of information related to FC-SP Security Associations for interface(s) to a particular Fabric; specifically, for rows created and/or modified in these tables:

t11FcSpSaPropTable  
t11FcSpSaTSelDrByTable  
t11FcSpSaControlTable

and, for modified information contained in the same row as an instance of this object.

Even if an instance of this object has the value 'permanent(4)', none of the information defined in this MIB module for interface(s) to the given Fabric need to be writable."

::= { t11FcSpSaIfEntry 7 }

t11FcSpSaIfReplayPrevention OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This object indicates whether anti-replay protection is enabled for frame reception on this interface.

Note that the replay-protection mechanism in FC-SP is conceptually similar to the corresponding mechanism in IPsec ESP."

REFERENCE

"IP Encapsulating Security Payload (ESP),  
[RFC 4303](#), December 2005, [section 3.3.3](#)."

::= { t11FcSpSaIfEntry 8 }

t11FcSpSaIfReplayWindowSize OBJECT-TYPE

Expires 11 January 2009

[Page 176]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

SYNTAX Unsigned32

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"The size of the replay window to be used when anti-replay protection is enabled for frame reception on this interface.

Note that the replay-protection mechanism in FC-SP is conceptually similar to the corresponding mechanism in IPsec ESP."

REFERENCE

"IP Encapsulating Security Payload (ESP),

[RFC 4303](#), December 2005, [section 3.4.3](#)."  
 ::= { t11FcSpSaIfEntry 9 }

t11FcSpSaIfDeadPeerDetections OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of times that a dead peer condition has been detected on this interface.

This counter has no discontinuities other than those which all Counter32's have when sysUpTime=0."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 8.5.3.3](#)."

::= { t11FcSpSaIfEntry 10 }

t11FcSpSaIfTerminateAllSas OBJECT-TYPE

SYNTAX INTEGER { noop(1), terminate(2) }

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"Setting this object to 'terminate' is a request to terminate all outstanding Security Associations on this interface.

When read, the value of this object is always 'noop'.

Setting this object to 'noop' has no effect."

::= { t11FcSpSaIfEntry 11 }

Expires 11 January 2009

[Page 177]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpSaIfOutDrops OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of output frames which were dropped, instead of being transmitted on this interface, because they matched

an active (at that time) Traffic Selector with an action of 'Drop'.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaIfEntry 12 }

t11FcSpSaIfOutBypasses OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of output frames which were transmitted unchanged by FC-SP on this interface because they matched an active (at that time) Traffic Selector with an action of 'Bypass'.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaIfEntry 13 }

t11FcSpSaIfOutProcesses OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of output frames which were protected by FC-SP before being transmitted on this interface because they matched an active (at that time) Traffic Selector with an action of 'Process'.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaIfEntry 14 }

t11FcSpSaIfOutUnMatcheds OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

#### DESCRIPTION

"The number of frames which were transmitted unchanged by FC-SP on this interface because they did not match any Traffic Selector active at that time.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaIfEntry 15 }

#### t11FcSpSaIfInUnprotUnmtchDrops OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

#### DESCRIPTION

"The number of frames received on this interface which were dropped because they were unprotected and did not match any Traffic Selector active at that time.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaIfEntry 16 }

#### t11FcSpSaIfInDetReplays OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

#### DESCRIPTION

"The number of times that a replay has been detected on a Security Association which is currently active or was previously active on this interface. Note that a frame which is discarded because it is 'behind' the window, i.e., too old, is counted as a replay.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaIfEntry 17 }

#### t11FcSpSaIfInUnprotMtchDrops OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

#### DESCRIPTION

"The number of times that a frame received on this interface was dropped because it matched with a Traffic



Selector for a Security Association which was active at the time of receipt but the frame was not protected as negotiated for that Security Association.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaIfEntry 18 }

#### t11FcSpSaIfInBadXforms OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

##### DESCRIPTION

"The number of times that a frame received on this interface was dropped because of a failure of one of the transforms negotiated for the Security Association on which it was received.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaIfEntry 19 }

#### t11FcSpSaIfInGoodXforms OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

##### DESCRIPTION

"The number of frames received on this interface on a Security Association for which the transforms negotiated for that Security Association were successfully applied, and which matched a Traffic Selector for that Security Association.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaIfEntry 20 }

#### t11FcSpSaIfInProtUnmtchs OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

##### DESCRIPTION

"The number of frames received on this interface which were dropped because they did not match any of the Traffic Selectors negotiated for the Security Association on which

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

they were received, even though the Security Association's transforms were successfully applied.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaIfEntry 21 }

--

-- Proposals to present in Security Association negotiation

--

t11FcSpSaPropTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpSaPropEntry

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"A table of proposals for an FC-SP entity acting as an SA\_Initiator to present to the SA\_Responder during the negotiation of Security Associations. This information is also used by an FC-SP entity acting as an SA\_Responder to decide what to accept during the negotiation of Security Associations."

::= { t11FcSpSaConfig 1 }

t11FcSpSaPropEntry OBJECT-TYPE

SYNTAX            T11FcSpSaPropEntry

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"Each entry contains information about one proposal for the FC-SP entity to present, or what to accept, during the negotiation of Security Associations on one or more interfaces (identified by t11FcSpSaIfIndex) to a particular Fabric (identified by t11FcSpSaIfFabricIndex), and managed as part of the Fibre Channel management instance identified by fcmInstanceIndex.

The StorageType of a row in this table is specified by the instance of t11FcSpSaIfStorageType which is INDEX-ed by the same values of fcmInstanceIndex, t11FcSpSaIfIndex

```
        and t11FcSpSaIfFabricIndex."
INDEX   { fcmInstanceIndex, t11FcSpSaIfIndex,
          t11FcSpSaIfFabricIndex,
          t11FcSpSaPropIndex }
```

Expires 11 January 2009

[Page 181]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```
::= { t11FcSpSaPropTable 1 }
```

```
T11FcSpSaPropEntry ::= SEQUENCE {
    t11FcSpSaPropIndex          Unsigned32,
    t11FcSpSaPropSecurityProt   T11FcSpSecurityProtocolId,
    t11FcSpSaPropTSelListIndex  Unsigned32,
    t11FcSpSaPropTransListIndex Unsigned32,
    t11FcSpSaPropAcceptAlgorithm INTEGER,
    t11FcSpSaPropOutMatchSucceeds Counter64,
    t11FcSpSaPropRowStatus      RowStatus
}
```

```
t11FcSpSaPropIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "An index value which uniquely identifies a particular
        proposal for use on one or more interfaces to a Fabric."
    ::= { t11FcSpSaPropEntry 1 }
```

```
t11FcSpSaPropSecurityProt OBJECT-TYPE
    SYNTAX      T11FcSpSecurityProtocolId
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "The Security Protocol identifier for this proposal, i.e.,
        whether the proposal is for traffic to be protected using
        ESP_Header or CT_Authentication."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
        Fibre Channel - Security Protocols (FC-SP),
        February 2007, section 6.3.2.2 and table 67."
    ::= { t11FcSpSaPropEntry 2 }
```

t11FcSpSaPropTselListIndex OBJECT-TYPE

SYNTAX           Unsigned32  
MAX-ACCESS       read-create  
STATUS           current  
DESCRIPTION

"When the value of this object is non-zero, it points to the proposal's list of Traffic Selectors. The value must be non-zero in an active row of this table.

The identified list is represented by all rows in the

Expires 11 January 2009

[Page 182]

---

Internet Draft       Fibre-Channel Security Protocols MIB

July 2008

t11FcSpSaTselPropTable for which t11FcSpSaTselPropListIndex has the same value as this object (and with corresponding values of t11FcSpSaIfIndex and fcmInstanceId)."

::= { t11FcSpSaPropEntry 3 }

t11FcSpSaPropTransListIndex OBJECT-TYPE

SYNTAX           Unsigned32  
MAX-ACCESS       read-create  
STATUS           current  
DESCRIPTION

"When the value of this object is non-zero, it points to the proposal's list of Transforms. The value must be non-zero in an active row of this table.

The identified list is represented by all rows in the t11FcSpSaTransTable for which t11FcSpSaTransListIndex has the same value as this object (and with corresponding values of t11FcSpSaIfIndex and fcmInstanceId)."

::= { t11FcSpSaPropEntry 4 }

t11FcSpSaPropAcceptAlgorithm OBJECT-TYPE

SYNTAX           INTEGER {  
                    intersection(1),  
                    union(2),  
                    other(3)  
                  }  
MAX-ACCESS       read-create  
STATUS           current  
DESCRIPTION

"The algorithm by which an SA\_Responder in an SA negotiation decides on which Traffic Selectors to specify in a response to an IKE\_Create\_Child\_SA request. This algorithm is used when the Traffic Selectors specified by an SA\_Initiator in an IKE\_Create\_Child\_SA request overlap with this proposal's list of Traffic Selectors:

intersection(1) - the SA\_Responder specifies the largest subset of what the SA\_Initiator proposed which is also a subset of this proposal's Traffic Selectors.

union(2) - the SA\_Responder specifies the smallest superset of what the SA\_Initiator proposed which is also a superset of this proposal's Traffic Selectors.

Expires 11 January 2009

[Page 183]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

other(3) - the SA\_Responder uses some other algorithm.  
"

::= { t11FcSpSaPropEntry 5 }

t11FcSpSaPropOutMatchSucceeds OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of egress frames that have matched a Traffic Selector which was negotiated to select traffic for an SA based on this proposal being accepted.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaPropEntry 6 }

t11FcSpSaPropRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The status of a row. Values of object instances

within an active row can be modified at any time.

The status cannot be set to 'active' unless and until the instances of t11FcSpSaPropTSelListIndex and t11FcSpSaPropTransListIndex in the row have been set to point to active rows in the t11FcSpSaTSelPropTable and t11FcSpSaTransTable tables, respectively. A row in this table is deleted if the active rows it points to are deleted."

::= { t11FcSpSaPropEntry 7 }

--  
-- Traffic Selector Proposals  
--

t11FcSpSaTSelPropTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpSaTSelPropEntry

MAX-ACCESS       not-accessible

STATUS            current

DESCRIPTION

"A table containing information about Traffic Selectors to propose and/or to accept during the negotiation of Security Associations."

REFERENCE

- "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 6.4.5](#).
- Use of IKEv2 in FC-SP, [RFC 4595](#),

July 2006, [section 4.4.](#)"  
 ::= { t11FcSpSaConfig 2 }

t11FcSpSaTSelPropEntry OBJECT-TYPE

SYNTAX T11FcSpSaTSelPropEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each entry contains information about one Traffic Selector within a list of Traffic Selectors to propose, or for use in determining what to accept during Security Association negotiation.

One such list is configured for use on a Fabric by configuring the list's value of t11FcSpSaTSelPropListIndex as the value of an instance of t11FcSpSaPropTSelListIndex, for corresponding values of t11FcSpSaIfIndex and fcmInstanceIndex. Further, the proposing and accepting of Traffic Selectors is only done as a part of a proposal specified by a row of the t11FcSpSaPropTable, i.e., in combination with the proposing and accepting of security transforms as specified by the combination of t11FcSpSaPropTSelListIndex and t11FcSpSaPropTransListIndex in one row of the t11FcSpSaPropTable.

The StorageType of a row in this table is specified by the instance of t11FcSpSaTSelPropStorageType in that row."

INDEX { fcmInstanceIndex, t11FcSpSaIfIndex,

Expires 11 January 2009

[Page 185]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpSaTSelPropListIndex, t11FcSpSaTSelPropPrecedence }  
 ::= { t11FcSpSaTSelPropTable 1 }

T11FcSpSaTSelPropEntry ::= SEQUENCE {

t11FcSpSaTSelPropListIndex      Unsigned32,  
t11FcSpSaTSelPropPrecedence      T11FcSpPrecedence,  
t11FcSpSaTSelPropDirection      T11FcSaDirection,  
t11FcSpSaTSelPropStartSrcAddr    FcAddressIdOrZero,  
t11FcSpSaTSelPropEndSrcAddr      FcAddressIdOrZero,  
t11FcSpSaTSelPropStartDstAddr    FcAddressIdOrZero,  
t11FcSpSaTSelPropEndDstAddr      FcAddressIdOrZero,

```

t11FcSpSaTSelPropStartRCtl    T11FcRoutingControl,
t11FcSpSaTSelPropEndRCtl      T11FcRoutingControl,
t11FcSpSaTSelPropStartType    T11FcSpType,
t11FcSpSaTSelPropEndType      T11FcSpType,
t11FcSpSaTSelPropStorageType  StorageType,
t11FcSpSaTSelPropRowStatus    RowStatus
}

t11FcSpSaTSelPropListIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "An index value which identifies a particular list of
        Traffic Selectors."
    ::= { t11FcSpSaTSelPropEntry 1 }

t11FcSpSaTSelPropPrecedence OBJECT-TYPE
    SYNTAX      T11FcSpPrecedence
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "The precedence of this Traffic Selector.  Each
        Traffic Selector within a particular list of
        Traffic Selectors must have a different precedence.

        If an egress frame matches multiple Traffic Selectors,
        it should be transmitted on the SA associated with the
        Traffic Selector having the numerically smallest
        precedence value."
    ::= { t11FcSpSaTSelPropEntry 2 }

t11FcSpSaTSelPropDirection OBJECT-TYPE
    SYNTAX      T11FcSaDirection

```

```

MAX-ACCESS   read-create
STATUS       current
DESCRIPTION

```

```

    "An indication of whether this Traffic Selector is
    to be proposed for ingress or egress traffic."

```



```

DEFVAL    { egress }
::= { t11FcSpSaTSelPropEntry 3 }

t11FcSpSaTSelPropStartSrcAddr OBJECT-TYPE
    SYNTAX      FcAddressIdOrZero (SIZE (3))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "The numerically smallest 24-bit value of a source address
        (S_ID) of a frame which will match with this Traffic
        Selector."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
        Fibre Channel - Security Protocols (FC-SP),
        February 2007, section 6.4.5."
    DEFVAL      { '000000'h }
    ::= { t11FcSpSaTSelPropEntry 4 }

t11FcSpSaTSelPropEndSrcAddr OBJECT-TYPE
    SYNTAX      FcAddressIdOrZero (SIZE (3))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "The numerically largest 24-bit value of a source address
        (S_ID) of a frame which will match with this Traffic
        Selector."
    REFERENCE
        "- ANSI INCITS 426-2007, T11/Project 1570-D,
        Fibre Channel - Security Protocols (FC-SP),
        February 2007, section 6.4.5."
    DEFVAL      { 'FFFFFF'h }
    ::= { t11FcSpSaTSelPropEntry 5 }

t11FcSpSaTSelPropStartDstAddr OBJECT-TYPE
    SYNTAX      FcAddressIdOrZero (SIZE (3))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "The numerically smallest 24-bit value of a destination
        address (D_ID) of a frame which will match with this

```

Traffic Selector."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 6.4.5](#)."

DEFVAL { '000000'h }

::= { t11FcSpSaTSelPropEntry 6 }

t11FcSpSaTSelPropEndDstAddr OBJECT-TYPE

SYNTAX FcAddressIdOrZero (SIZE (3))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The numerically largest 24-bit value of a destination  
address (D\_ID) of a frame which will match with this  
Traffic Selector."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 6.4.5](#)."

DEFVAL { 'FFFFFF'h }

::= { t11FcSpSaTSelPropEntry 7 }

t11FcSpSaTSelPropStartRctl OBJECT-TYPE

SYNTAX T11FcRoutingControl

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The numerically smallest 8-bit value contained within a  
Routing Control (R\_CTL) field of a frame which will match  
with this Traffic Selector."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 6.4.5](#)."

DEFVAL { '00'h }

::= { t11FcSpSaTSelPropEntry 8 }

t11FcSpSaTSelPropEndRctl OBJECT-TYPE

SYNTAX T11FcRoutingControl

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The numerically largest 8-bit value contained within a  
Routing Control (R\_CTL) field of a frame which will match

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

with this Traffic Selector."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 6.4.5](#)."

DEFVAL { 'FF'h }

::= { t11FcSpSaTSelPropEntry 9 }

## t11FcSpSaTSelPropStartType OBJECT-TYPE

SYNTAX T11FcSpType

MAX-ACCESS read-create

STATUS current

## DESCRIPTION

"The numerically smallest of a range of possible 'type'  
values of frames which will match with this Traffic  
Selector."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 6.4.5](#)."

DEFVAL { '0000'h }

::= { t11FcSpSaTSelPropEntry 10 }

## t11FcSpSaTSelPropEndType OBJECT-TYPE

SYNTAX T11FcSpType

MAX-ACCESS read-create

STATUS current

## DESCRIPTION

"The numerically largest of a range of possible 'type'  
values of frames which will match with this Traffic  
Selector."

## REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 6.4.5](#)."

DEFVAL { 'FFFF'h }

::= { t11FcSpSaTSelPropEntry 11 }

## t11FcSpSaTSelPropStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

## DESCRIPTION

"This object specifies the memory realization of the information in this row.

Expires 11 January 2009

[Page 189]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

Even if an instance of this object has the value 'permanent(4)', none of the information in its row needs to be writable."

::= { t11FcSpSaTSelPropEntry 12 }

t11FcSpSaTSelPropRowStatus OBJECT-TYPE

SYNTAX            RowStatus  
MAX-ACCESS       read-create  
STATUS            current  
DESCRIPTION

"The status of this row. Values of object instances within the row can be modified at any time."

::= { t11FcSpSaTSelPropEntry 13 }

--

-- Transform Proposals

--

t11FcSpSaTransTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpSaTransEntry  
MAX-ACCESS       not-accessible  
STATUS            current  
DESCRIPTION

"A table containing information about security transforms to propose, to accept and/or agreed upon during the negotiation of Security Associations."

::= { t11FcSpSaConfig 3 }

t11FcSpSaTransEntry OBJECT-TYPE

SYNTAX            T11FcSpSaTransEntry  
MAX-ACCESS       not-accessible  
STATUS            current  
DESCRIPTION

"Each entry contains information about one proposal within a list of security transforms to be proposed, to be accepted, or already agreed upon, for use on a pair of Security

Associations on one or more interfaces (identified by t11FcSpSaIfIndex), managed as part of the Fibre Channel management instance identified by fcmInstanceId.

One such list is configured to be proposed or accepted for use on a Fabric, by having the list's value of t11FcSpSaTransListIndex be the value of an instance of t11FcSpSaPropTransListIndex for that Fabric. Further,

Expires 11 January 2009

[Page 190]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

the proposing and accepting of security transforms is only done as a part of a proposal specified by a row of the t11FcSpSaPropTable, i.e., in combination with the proposing and accepting of Traffic Selectors as specified by the combination of t11FcSpSaPropTSelListIndex and t11FcSpSaPropTransListIndex in one row of the t11FcSpSaPropTable.

The security (encryption and integrity) transform in use on an SA pair is indicated by having the pair's values of t11FcSpSaPairTransListIndex and t11FcSpSaPairTransIndex contain the values of t11FcSpSaTransListIndex and t11FcSpSaTransIndex for the transform's row in this table.

The StorageType of a row in this table is specified by the instance of t11FcSpSaTransStorageType in that row."

INDEX { fcmInstanceId, t11FcSpSaIfIndex,  
          t11FcSpSaTransListIndex, t11FcSpSaTransIndex }  
::= { t11FcSpSaTransTable 1 }

T11FcSpSaTransEntry ::= SEQUENCE {  
    t11FcSpSaTransListIndex      Unsigned32,  
    t11FcSpSaTransIndex          Unsigned32,  
    t11FcSpSaTransSecurityProt    T11FcSpSecurityProtocolId,  
    t11FcSpSaTransEncryptAlg      AutonomousType,  
    t11FcSpSaTransEncryptKeyLen   Unsigned32,  
    t11FcSpSaTransIntegrityAlg    AutonomousType,  
    t11FcSpSaTransStorageType     StorageType,  
    t11FcSpSaTransRowStatus       RowStatus  
}

t11FcSpSaTransListIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An index value which uniquely identifies a particular list of security transforms to be proposed, to be accepted, or already agreed upon."

::= { t11FcSpSaTransEntry 1 }

t11FcSpSaTransIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS not-accessible

STATUS current

Expires 11 January 2009

[Page 191]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

DESCRIPTION

"An index value which uniquely identifies one security transform within a list identified by t11FcSpSaTransListIndex."

::= { t11FcSpSaTransEntry 2 }

t11FcSpSaTransSecurityProt OBJECT-TYPE

SYNTAX T11FcSpSecurityProtocolId

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The Security Protocol identifier which indicates whether this transform is for traffic to be protected using ESP\_Header or using CT\_Authentication."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, [section 6.3.2.2](#) and table 67."

::= { t11FcSpSaTransEntry 3 }

t11FcSpSaTransEncryptAlg OBJECT-TYPE

SYNTAX AutonomousType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The Encryption Algorithm for this transform."  
REFERENCE  
"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 6.3.2.3](#) and tables 69 & 70."  
::= { t11FcSpSaTransEntry 4 }

t11FcSpSaTransEncryptKeyLen OBJECT-TYPE

SYNTAX Unsigned32  
MAX-ACCESS read-create  
STATUS current

DESCRIPTION

"The key length in bits to be used with an encryption algorithm which has a variable length key. This object is ignored when the corresponding instance of t11FcSpSaTransEncryptAlg specifies an algorithm with a fixed length key."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),

Expires 11 January 2009

[Page 192]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

February 2007, [section 6.3.2.5](#) and table 77."  
::= { t11FcSpSaTransEntry 5 }

t11FcSpSaTransIntegrityAlg OBJECT-TYPE

SYNTAX AutonomousType  
MAX-ACCESS read-create  
STATUS current

DESCRIPTION

"The Integrity Algorithm for this transform."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, [section 6.3.2.3](#) and tables 69 & 72."

::= { t11FcSpSaTransEntry 6 }

t11FcSpSaTransStorageType OBJECT-TYPE

SYNTAX StorageType  
MAX-ACCESS read-create  
STATUS current

#### DESCRIPTION

"This object specifies the memory realization of the information in this row.

Even if an instance of this object has the value 'permanent(4)', none of the information in its row needs to be writable."

::= { t11FcSpSaTransEntry 7 }

#### t11FcSpSaTransRowStatus OBJECT-TYPE

SYNTAX            RowStatus  
MAX-ACCESS       read-create  
STATUS            current

#### DESCRIPTION

"The status of this row.

When an instance of t11FcSpSaPairTransListIndex points to a row in this table, values of object instances in the row cannot be modified nor can the row be deleted. Otherwise, a row can be modified or deleted at any time."

::= { t11FcSpSaTransEntry 8 }

Expires 11 January 2009

[Page 193]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

--  
-- Traffic Selectors for Drop & Bypass  
--

#### t11FcSpSaTSelDrByTable OBJECT-TYPE

SYNTAX            SEQUENCE OF T11FcSpSaTSelDrByEntry  
MAX-ACCESS       not-accessible  
STATUS            current

#### DESCRIPTION

"A table containing Traffic Selectors to select which traffic is to be dropped or is to bypass further security processing."

#### REFERENCE



- "- ANSI INCITS 426-2007, T11/Project 1570-D,  
Fibre Channel - Security Protocols (FC-SP),  
February 2007, sections [4.6](#), [4.7](#), and [6.4.5](#).
- Use of IKEv2 in FC-SP, [RFC 4595](#),  
July 2006, [section 4.4](#)."

::= { t11FcSpSaTSELDrByConfig 4 }

t11FcSpSaTSELDrByEntry OBJECT-TYPE

SYNTAX T11FcSpSaTSELDrByEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each entry represents one Traffic Selector having the security action of 'drop' or 'bypass' which is applied based on a precedence value, either to ingress traffic which is unprotected by FC-SP, or to all egress traffic on one or more interfaces (identified by t11FcSpSaIfIndex) to a particular Fabric (identified by t11FcSpSaIfFabricIndex), and managed as part of the Fibre Channel management instance identified by fcmInstanceIndex.

The StorageType of a row in this table is specified by the instance of t11FcSpSaIfStorageType which is INDEX-ed by the same values of fcmInstanceIndex, t11FcSpSaIfIndex and t11FcSpSaIfFabricIndex."

INDEX { fcmInstanceIndex, t11FcSpSaIfIndex, t11FcSpSaIfFabricIndex,  
t11FcSpSaTSELDrByDirection, t11FcSpSaTSELDrByPrecedence }

::= { t11FcSpSaTSELDrByTable 1 }

T11FcSpSaTSELDrByEntry ::= SEQUENCE {

t11FcSpSaTSELDrByDirection T11FcSaDirection,

t11FcSpSaTSELDrByPrecedence T11FcSpPrecedence,

Expires 11 January 2009

[Page 194]

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

t11FcSpSaTSELDrByAction	INTEGER,
t11FcSpSaTSELDrByStartSrcAddr	FcAddressIdOrZero,
t11FcSpSaTSELDrByEndSrcAddr	FcAddressIdOrZero,
t11FcSpSaTSELDrByStartDstAddr	FcAddressIdOrZero,
t11FcSpSaTSELDrByEndDstAddr	FcAddressIdOrZero,
t11FcSpSaTSELDrByStartRCTL	T11FcRoutingControl,
t11FcSpSaTSELDrByEndRCTL	T11FcRoutingControl,

```

    t11FcSpSaTSelDrByStartType      T11FcSpType,
    t11FcSpSaTSelDrByEndType        T11FcSpType,
    t11FcSpSaTSelDrByMatches        Counter64,
    t11FcSpSaTSelDrByRowStatus      RowStatus
}

```

t11FcSpSaTSelDrByDirection OBJECT-TYPE

SYNTAX T11FcSaDirection

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An indication of whether this Traffic Selector is  
for ingress or egress traffic."

::= { t11FcSpSaTSelDrByEntry 1 }

t11FcSpSaTSelDrByPrecedence OBJECT-TYPE

SYNTAX T11FcSpPrecedence

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The precedence of this Traffic Selector. If and when a  
frame is compared against multiple Traffic Selectors, and  
multiple of them have a match with the frame, the security  
action to be taken for the frame is that specified for the  
matching Traffic Selector having the numerically smallest  
precedence value."

::= { t11FcSpSaTSelDrByEntry 2 }

t11FcSpSaTSelDrByAction OBJECT-TYPE

SYNTAX INTEGER { drop(1), bypass(2) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The security action to be taken for a frame which  
matches this Traffic Selector."

DEFVAL { drop }

::= { t11FcSpSaTSelDrByEntry 3 }

t11FcSpSaTSelDrByStartSrcAddr OBJECT-TYPE

SYNTAX           FcAddressIdOrZero (SIZE (3))  
 MAX-ACCESS      read-create  
 STATUS           current  
 DESCRIPTION  
     "The numerically smallest 24-bit value of a source address  
     (S\_ID) of a frame which will match with this Traffic  
     Selector."  
 DEFVAL      { '000000'h }  
 ::= { t11FcSpSaTSelDrByEntry 4 }

t11FcSpSaTSelDrByEndSrcAddr OBJECT-TYPE  
 SYNTAX           FcAddressIdOrZero (SIZE (3))  
 MAX-ACCESS      read-create  
 STATUS           current  
 DESCRIPTION  
     "The numerically largest 24-bit value of a source address  
     (S\_ID) of a frame which will match with this Traffic  
     Selector."  
 DEFVAL      { 'FFFFFF'h }  
 ::= { t11FcSpSaTSelDrByEntry 5 }

t11FcSpSaTSelDrByStartDstAddr OBJECT-TYPE  
 SYNTAX           FcAddressIdOrZero (SIZE (3))  
 MAX-ACCESS      read-create  
 STATUS           current  
 DESCRIPTION  
     "The numerically smallest 24-bit value of a destination  
     address (D\_ID) of a frame which will match with this  
     Traffic Selector."  
 DEFVAL      { '000000'h }  
 ::= { t11FcSpSaTSelDrByEntry 6 }

t11FcSpSaTSelDrByEndDstAddr OBJECT-TYPE  
 SYNTAX           FcAddressIdOrZero (SIZE (3))  
 MAX-ACCESS      read-create  
 STATUS           current  
 DESCRIPTION  
     "The numerically largest 24-bit value of a destination  
     address (D\_ID) of a frame which will match with this  
     Traffic Selector."  
 DEFVAL      { 'FFFFFF'h }  
 ::= { t11FcSpSaTSelDrByEntry 7 }

t11FcSpSaTSelDrByStartRctl OBJECT-TYPE

SYNTAX            T11FcRoutingControl  
MAX-ACCESS       read-create  
STATUS            current  
DESCRIPTION  
    "The numerically smallest 8-bit value contained within a  
    Routing Control (R\_CTL) field of a frame which will match  
    with this Traffic Selector."  
DEFVAL     { '00'h }  
::= { t11FcSpSaTSelDrByEntry 8 }

t11FcSpSaTSelDrByEndRctl OBJECT-TYPE

SYNTAX            T11FcRoutingControl  
MAX-ACCESS       read-create  
STATUS            current  
DESCRIPTION  
    "The numerically largest 8-bit value contained within a  
    Routing Control (R\_CTL) field of a frame which will match  
    with this Traffic Selector."  
DEFVAL     { 'FF'h }  
::= { t11FcSpSaTSelDrByEntry 9 }

t11FcSpSaTSelDrByStartType OBJECT-TYPE

SYNTAX            T11FcSpType  
MAX-ACCESS       read-create  
STATUS            current  
DESCRIPTION  
    "The numerically smallest of a range of possible 'type'  
    values of frames which will match with this Traffic  
    Selector."  
DEFVAL     { '0000'h }  
::= { t11FcSpSaTSelDrByEntry 10 }

t11FcSpSaTSelDrByEndType OBJECT-TYPE

SYNTAX            T11FcSpType  
MAX-ACCESS       read-create  
STATUS            current  
DESCRIPTION  
    "The numerically largest of a range of possible 'type'  
    values of frames which will match with this Traffic  
    Selector."  
DEFVAL     { 'FFFF'h }  
::= { t11FcSpSaTSelDrByEntry 11 }

t11FcSpSaTSelDrByMatches OBJECT-TYPE

SYNTAX            Counter64

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

MAX-ACCESS      read-only

STATUS          current

DESCRIPTION

"The number of frames for which the action specified by the corresponding instance of t11FcSpSaTSELDrByAction was taken because of a match with this Traffic Selector.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaTSELDrByEntry 12 }

t11FcSpSaTSELDrByRowStatus OBJECT-TYPE

SYNTAX          RowStatus

MAX-ACCESS      read-create

STATUS          current

DESCRIPTION

"The status of this row. Values of object instances within the row can be modified at any time."

::= { t11FcSpSaTSELDrByEntry 13 }

--

-- Active Security Associations

--

t11FcSpSaPairTable OBJECT-TYPE

SYNTAX          SEQUENCE OF T11FcSpSaPairEntry

MAX-ACCESS      not-accessible

STATUS          current

DESCRIPTION

"A table containing information about active bidirectional pairs of Security Associations."

::= { t11FcSpSaActive 1 }

t11FcSpSaPairEntry OBJECT-TYPE

SYNTAX          T11FcSpSaPairEntry

MAX-ACCESS      not-accessible

STATUS          current

DESCRIPTION

"Each entry contains information about one active bidirectional pair of Security Associations on an interface to a particular Fabric (identified by

t11FcSpSaIfFabricIndex), managed as part of the Fibre Channel management instance identified by fcmInstanceIndex."  
INDEX { fcmInstanceIndex, t11FcSpSaPairIfIndex,

Expires 11 January 2009

[Page 198]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpSaIfFabricIndex, t11FcSpSaPairInboundSpi }  
::= { t11FcSpSaPairTable 1 }

T11FcSpSaPairEntry ::= SEQUENCE {  
    t11FcSpSaPairIfIndex           InterfaceIndex,  
    t11FcSpSaPairInboundSpi        T11FcSpiIndex,  
    t11FcSpSaPairSecurityProt       T11FcSpSecurityProtocolId,  
    t11FcSpSaPairTransListIndex    Unsigned32,  
    t11FcSpSaPairTransIndex        Unsigned32,  
    t11FcSpSaPairLifetimeLeft      Unsigned32,  
    t11FcSpSaPairLifetimeLeftUnits INTEGER,  
    t11FcSpSaPairTerminate         INTEGER,  
    t11FcSpSaPairInProtUnMatches   Counter64,  
    t11FcSpSaPairInDetReplays      Counter64,  
    t11FcSpSaPairInBadXforms       Counter64,  
    t11FcSpSaPairInGoodXforms      Counter64  
}

t11FcSpSaPairIfIndex OBJECT-TYPE

SYNTAX           InterfaceIndex

MAX-ACCESS       not-accessible

STATUS           current

DESCRIPTION

"This object identifies the interface to the particular  
Fabric on which this SA pair is active."

::= { t11FcSpSaPairEntry 1 }

t11FcSpSaPairInboundSpi OBJECT-TYPE

SYNTAX           T11FcSpiIndex

MAX-ACCESS       not-accessible

STATUS           current

DESCRIPTION

"The SPI value which is used to indicate that an incoming  
frame was received on the ingress SA of this SA pair."

::= { t11FcSpSaPairEntry 2 }

t11FcSpSaPairSecurityProt OBJECT-TYPE

SYNTAX T11FcSpSecurityProtocolId

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The object indicates whether this SA uses ESP\_Header to protect FC-2 frames, or CT\_Authentication to protect Common Transport Information Units (CT\_IUs)."

::= { t11FcSpSaPairEntry 3 }

Expires 11 January 2009

[Page 199]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

t11FcSpSaPairTransListIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The combination of this value and the value of the corresponding instance of t11FcSpSaPairTransIndex identify the row in the t11FcSpSaTransTable which contains the transforms which are in use on this SA pair."

::= { t11FcSpSaPairEntry 4 }

t11FcSpSaPairTransIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The combination of this value and the value of the corresponding instance of t11FcSpSaPairTransListIndex identify the row in the t11FcSpSaTransTable which contains the transforms which are in use on this SA pair."

::= { t11FcSpSaPairEntry 5 }

t11FcSpSaPairLifetimeLeft OBJECT-TYPE

SYNTAX T11FcSpLifetimeLeft

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The remaining lifetime of this SA pair, given in the units specified by the value of the corresponding

```
        instance of t11FcSpSaPairLifetimeLeft."
 ::= { t11FcSpSaPairEntry 6 }
```

t11FcSpSaPairLifetimeLeftUnits OBJECT-TYPE

```
SYNTAX      T11FcSpLifetimeLeftUnits
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The units in which the value of the corresponding
    instance of t11FcSpSaPairLifetimeLeft specifies the
    remaining lifetime of this SA pair."
 ::= { t11FcSpSaPairEntry 7 }
```

t11FcSpSaPairTerminate OBJECT-TYPE

```
SYNTAX      INTEGER { noop(1), terminate(2) }
MAX-ACCESS  read-write
```

Expires 11 January 2009

[Page 200]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

```
STATUS      current
DESCRIPTION
```

```
    "Setting this object to 'terminate' is a request
    to terminate this pair of Security Associations.
```

```
    When read, the value of this object is always 'noop'.
    Setting this object to 'noop' has no effect."
```

```
 ::= { t11FcSpSaPairEntry 8 }
```

t11FcSpSaPairInProtUnMatches OBJECT-TYPE

```
SYNTAX      Counter64
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
```

```
    "The number of frames received on this SA for which the
    SA's transforms were successfully applied to the frame,
    but the frame was still dropped because it did not match
    any of the SA's ingress Traffic Selectors.
```

```
    This counter has no discontinuities other than those
    which all Counter64's have when sysUpTime=0."
```

```
 ::= { t11FcSpSaPairEntry 9 }
```



t11FcSpSaPairInDetReplays OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of times that a replay has been detected on this Security Association. Note that a frame which is discarded because it is 'behind' the window, i.e., too old, is counted as a replay.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaPairEntry 10 }

t11FcSpSaPairInBadXforms OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of times that a received frame was dropped because one of the transforms negotiated for this Security Association failed.

Expires 11 January 2009

[Page 201]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaPairEntry 11 }

t11FcSpSaPairInGoodXforms OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of received frames for which the transforms negotiated for this Security Association, were successfully applied.

This counter has no discontinuities other than those which all Counter64's have when sysUpTime=0."

::= { t11FcSpSaPairEntry 12 }

--  
-- Negotiated Ingress Traffic Selectors  
--

t11FcSpSaTSelNegInTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpSaTSelNegInEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table containing information about ingress Traffic Selectors which are in use on active Security Associations."

REFERENCE

- "- ANSI INCITS 426-2007, T11/Project 1570-D, Fibre Channel - Security Protocols (FC-SP), February 2007, sections [4.6](#), [4.7](#), and [6.4.5](#).
- Use of IKEv2 in FC-SP, [RFC 4595](#), July 2006, [section 4.4](#)."

::= { t11FcSpSaActive 2 }

t11FcSpSaTSelNegInEntry OBJECT-TYPE

SYNTAX T11FcSpSaTSelNegInEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each entry contains information about one ingress Traffic Selector which is in use on an active Security Association"

Expires 11 January 2009

[Page 202]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

on an interface (identified by t11FcSpSaPairIfIndex) to a particular Fabric (identified by t11FcSpSaIfFabricIndex), managed as part of the Fibre Channel management instance identified by fcmInstanceIndex."

INDEX { fcmInstanceIndex, t11FcSpSaPairIfIndex,  
          t11FcSpSaIfFabricIndex, t11FcSpSaTSelNegInIndex }

::= { t11FcSpSaTSelNegInTable 1 }

T11FcSpSaTSelNegInEntry ::= SEQUENCE {

  t11FcSpSaTSelNegInIndex            Unsigned32,

  t11FcSpSaTSelNegInInboundSpi      T11FcSpiIndex,

```

t11FcSpSaTSELNegInStartSrcAddr  FcAddressIdOrZero,
t11FcSpSaTSELNegInEndSrcAddr    FcAddressIdOrZero,
t11FcSpSaTSELNegInStartDstAddr  FcAddressIdOrZero,
t11FcSpSaTSELNegInEndDstAddr    FcAddressIdOrZero,
t11FcSpSaTSELNegInStartRctl     T11FcRoutingControl,
t11FcSpSaTSELNegInEndRctl       T11FcRoutingControl,
t11FcSpSaTSELNegInStartType     T11FcSpType,
t11FcSpSaTSELNegInEndType       T11FcSpType,
t11FcSpSaTSELNegInUnpMtchDrops  Counter64
}

t11FcSpSaTSELNegInIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION
        "An index value to distinguish an ingress Traffic Selector
        from all others currently in use by Security Associations
        on the same interface to a particular Fabric."
    ::= { t11FcSpSaTSELNegInEntry 1 }

t11FcSpSaTSELNegInInboundSpi OBJECT-TYPE
    SYNTAX      T11FcSpiIndex
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The SPI of the ingress SA on which this Traffic Selector
        is in use.

        This value can be used to find the SA pair's row in the
        t11FcSpSaPairTable."
    ::= { t11FcSpSaTSELNegInEntry 2 }

t11FcSpSaTSELNegInStartSrcAddr OBJECT-TYPE

```

```

SYNTAX      FcAddressIdOrZero (SIZE (3))
MAX-ACCESS   read-only
STATUS      current
DESCRIPTION
    "The numerically smallest 24-bit value of a source address

```

```

        (S_ID) of a frame which will match with this Traffic
        Selector."
 ::= { t11FcSpSaTSelNegInEntry 3 }

t11FcSpSaTSelNegInEndSrcAddr OBJECT-TYPE
    SYNTAX      FcAddressIdOrZero (SIZE (3))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The numerically largest 24-bit value of a source address
        (S_ID) of a frame which will match with this Traffic
        Selector."
 ::= { t11FcSpSaTSelNegInEntry 4 }

t11FcSpSaTSelNegInStartDstAddr OBJECT-TYPE
    SYNTAX      FcAddressIdOrZero (SIZE (3))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The numerically smallest 24-bit value of a destination
        address (D_ID) of a frame which will match with this
        Traffic Selector."
 ::= { t11FcSpSaTSelNegInEntry 5 }

t11FcSpSaTSelNegInEndDstAddr OBJECT-TYPE
    SYNTAX      FcAddressIdOrZero (SIZE (3))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The numerically largest 24-bit value of a destination
        address (D_ID) of a frame which will match with this
        Traffic Selector."
 ::= { t11FcSpSaTSelNegInEntry 6 }

t11FcSpSaTSelNegInStartRctl OBJECT-TYPE
    SYNTAX      T11FcRoutingControl
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The numerically smallest 8-bit value contained within a

```

Routing Control (R\_CTL) field of a frame which will match with this Traffic Selector."  
 ::= { t11FcSpSaTSelNegInEntry 7 }

t11FcSpSaTSelNegInEndRCtl OBJECT-TYPE

SYNTAX T11FcRoutingControl

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The numerically largest 8-bit value contained within a Routing Control (R\_CTL) field of a frame which will match with this Traffic Selector."

::= { t11FcSpSaTSelNegInEntry 8 }

t11FcSpSaTSelNegInStartType OBJECT-TYPE

SYNTAX T11FcSpType

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The numerically smallest of a range of possible 'type' values of frames which will match with this Traffic Selector."

::= { t11FcSpSaTSelNegInEntry 9 }

t11FcSpSaTSelNegInEndType OBJECT-TYPE

SYNTAX T11FcSpType

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The numerically largest of a range of possible 'type' values of frames which will match with this Traffic Selector."

::= { t11FcSpSaTSelNegInEntry 10 }

t11FcSpSaTSelNegInUnpMtchDrops OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of times that a received frame was dropped because it matched with this Traffic Selector but the frame was not protected as negotiated for the Security Association identified by t11FcSpSaTSelNegInInboundSpi.

This counter has no discontinuities other than those

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

which all Counter64's have when sysUpTime=0."  
 ::= { t11FcSpSaTSELNegInEntry 11 }

--  
 -- Negotiated Egress Traffic Selectors  
 --

t11FcSpSaTSELNegOutTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpSaTSELNegOutEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table containing information about egress Traffic  
 Selectors which are in use on active Security  
 Associations."

REFERENCE

"- ANSI INCITS 426-2007, T11/Project 1570-D,  
 Fibre Channel - Security Protocols (FC-SP),  
 February 2007, sections [4.6](#), [4.7](#), and [6.4.5](#).  
 - Use of IKEv2 in FC-SP, [RFC 4595](#),  
 July 2006, [section 4.4](#)."

::= { t11FcSpSaActive 3 }

t11FcSpSaTSELNegOutEntry OBJECT-TYPE

SYNTAX T11FcSpSaTSELNegOutEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each entry contains information about one egress Traffic  
 Selector which is in use on an active Security Association  
 on an interface (identified by t11FcSpSaPairIfIndex) to  
 a particular Fabric (identified by t11FcSpSaIfFabricIndex),  
 managed as part of the Fibre Channel management instance  
 identified by fcmInstanceIndex."

INDEX { fcmInstanceIndex, t11FcSpSaPairIfIndex,  
 t11FcSpSaIfFabricIndex, t11FcSpSaTSELNegOutPrecedence }

::= { t11FcSpSaTSELNegOutTable 1 }

T11FcSpSaTSELNegOutEntry ::= SEQUENCE {

t11FcSpSaTSELNegOutPrecedence T11FcSpPrecedence,

t11FcSpSaTSELNegOutInboundSpi T11FcSpiIndex,

t11FcSpSaTSELNegOutStartSrcAddr FcAddressIdOrZero,

t11FcSpSaTSelNegOutEndSrcAddr	FcAddressIdOrZero,
t11FcSpSaTSelNegOutStartDstAddr	FcAddressIdOrZero,

Expires 11 January 2009

[Page 206]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpSaTSelNegOutEndDstAddr	FcAddressIdOrZero,
t11FcSpSaTSelNegOutStartRCtl	T11FcRoutingControl,
t11FcSpSaTSelNegOutEndRCtl	T11FcRoutingControl,
t11FcSpSaTSelNegOutStartType	T11FcSpType,
t11FcSpSaTSelNegOutEndType	T11FcSpType

}

t11FcSpSaTSelNegOutPrecedence OBJECT-TYPE

SYNTAX            T11FcSpPrecedence

MAX-ACCESS      not-accessible

STATUS           current

DESCRIPTION

"The precedence of this Traffic Selector. If and when a frame is compared against multiple Traffic Selectors, and multiple of them have a match with the frame, the security action to be taken for the frame is that specified for the matching Traffic Selector having the numerically smallest precedence value."

::= { t11FcSpSaTSelNegOutEntry 1 }

t11FcSpSaTSelNegOutInboundSpi OBJECT-TYPE

SYNTAX            T11FcSpiIndex

MAX-ACCESS      read-only

STATUS           current

DESCRIPTION

"The SPI of the ingress SA of the SA pair for which this Traffic Selector is in use on the egress SA.

This value can be used to find the SA pair's row in the t11FcSpSaPairTable."

::= { t11FcSpSaTSelNegOutEntry 2 }

t11FcSpSaTSelNegOutStartSrcAddr OBJECT-TYPE

SYNTAX            FcAddressIdOrZero (SIZE (3))

MAX-ACCESS      read-only

STATUS           current

DESCRIPTION

"The numerically smallest 24-bit value of a source address (S\_ID) of a frame which will match with this Traffic Selector."

::= { t11FcSpSaTSelNegOutEntry 3 }

t11FcSpSaTSelNegOutEndSrcAddr OBJECT-TYPE  
SYNTAX FcAddressIdOrZero (SIZE (3))  
MAX-ACCESS read-only

Expires 11 January 2009

[Page 207]

---

Internet Draft      Fibre-Channel Security Protocols MIB      July 2008

STATUS current

DESCRIPTION

"The numerically largest 24-bit value of a source address (S\_ID) of a frame which will match with this Traffic Selector."

::= { t11FcSpSaTSelNegOutEntry 4 }

t11FcSpSaTSelNegOutStartDstAddr OBJECT-TYPE  
SYNTAX FcAddressIdOrZero (SIZE (3))  
MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The numerically smallest 24-bit value of a destination address (D\_ID) of a frame which will match with this Traffic Selector."

::= { t11FcSpSaTSelNegOutEntry 5 }

t11FcSpSaTSelNegOutEndDstAddr OBJECT-TYPE  
SYNTAX FcAddressIdOrZero (SIZE (3))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The numerically largest 24-bit value of a destination address (D\_ID) of a frame which will match with this Traffic Selector."

::= { t11FcSpSaTSelNegOutEntry 6 }

t11FcSpSaTSelNegOutStartRctl OBJECT-TYPE

SYNTAX T11FcRoutingControl

MAX-ACCESS read-only

STATUS current



DESCRIPTION

"The numerically smallest 8-bit value contained within a Routing Control (R\_CTL) field of a frame which will match with this Traffic Selector."

::= { t11FcSpSaTSelNegOutEntry 7 }

t11FcSpSaTSelNegOutEndRctl OBJECT-TYPE

SYNTAX T11FcRoutingControl

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The numerically largest 8-bit value contained within a Routing Control (R\_CTL) field of a frame which will match with this Traffic Selector."

Expires 11 January 2009

[Page 208]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

::= { t11FcSpSaTSelNegOutEntry 8 }

t11FcSpSaTSelNegOutStartType OBJECT-TYPE

SYNTAX T11FcSpType

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The numerically smallest of a range of possible 'type' values of frames which will match with this Traffic Selector."

::= { t11FcSpSaTSelNegOutEntry 9 }

t11FcSpSaTSelNegOutEndType OBJECT-TYPE

SYNTAX T11FcSpType

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The numerically largest of a range of possible 'type' values of frames which will match with this Traffic Selector."

::= { t11FcSpSaTSelNegOutEntry 10 }

--

-- Traffic Selectors index-ed by SPI

--

t11FcSpSaTselSpiTable OBJECT-TYPE

SYNTAX SEQUENCE OF T11FcSpSaTselSpiEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table identifying the Traffic Selectors in use on particular Security Associations, index-ed by their (ingress) SPI values."

::= { t11FcSpSaActive 4 }

t11FcSpSaTselSpiEntry OBJECT-TYPE

SYNTAX T11FcSpSaTselSpiEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"Each entry identifies one Traffic Selector in use on an SA pair on the interface (identified by t11FcSpSaPairIfIndex) to a particular Fabric (identified by t11FcSpSaIfFabricIndex), and managed as part of the Fibre

Expires 11 January 2009

[Page 209]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

Channel management instance identified by fcmInstanceIndex."  
INDEX { fcmInstanceIndex, t11FcSpSaPairIfIndex,  
t11FcSpSaIfFabricIndex,  
t11FcSpSaTselSpiInboundSpi, t11FcSpSaTselSpiTrafSelIndex }  
::= { t11FcSpSaTselSpiTable 1 }

T11FcSpSaTselSpiEntry ::= SEQUENCE {  
t11FcSpSaTselSpiInboundSpi T11FcSpiIndex,  
t11FcSpSaTselSpiTrafSelIndex Unsigned32,  
t11FcSpSaTselSpiDirection T11FcSaDirection,  
t11FcSpSaTselSpiTrafSelPtr Unsigned32  
}

t11FcSpSaTselSpiInboundSpi OBJECT-TYPE

SYNTAX T11FcSpiIndex

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An SPI value which identifies the ingress Security

Association of a particular SA pair."  
 ::= { t11FcSpSaTSelSpiEntry 1 }

t11FcSpSaTSelSpiTrafSelIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An index value which distinguishes between the  
(potentially multiple) Traffic Selectors in use on  
this Security Association pair."

::= { t11FcSpSaTSelSpiEntry 2 }

t11FcSpSaTSelSpiDirection OBJECT-TYPE

SYNTAX T11FcSaDirection

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This object indicates whether this Traffic Selector  
is being used for ingress or for egress traffic."

::= { t11FcSpSaTSelSpiEntry 3 }

t11FcSpSaTSelSpiTrafSelPtr OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-only

STATUS current

Expires 11 January 2009

[Page 210]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

DESCRIPTION

"This object contains a pointer into another table which  
can be used to obtain more information about this Traffic  
Selector.

If the corresponding instance of t11FcSpSaTSelSpiDirection  
has the value 'egress', then this object contains the  
value of t11FcSpSaTSelNegOutPrecedence in the row of  
t11FcSpSaTSelNegOutTable which contains more information.

If the corresponding instance of t11FcSpSaTSelSpiDirection  
has the value 'ingress', then this object contains the  
value of t11FcSpSaTSelNegInIndex which identifies the row

```
        in t11FcSpSaTSelNegInTable containing more information."
 ::= { t11FcSpSaTSelSpiEntry 4 }
```

Expires 11 January 2009

[Page 211]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```
--
-- Notification information & control
--
```

```
t11FcSpSaControlTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF T11FcSpSaControlEntry
    MAX-ACCESS   not-accessible
```

STATUS           current  
DESCRIPTION  
      "A table of control and other information concerning  
      the generation of notifications for events related  
      to FC-SP Security Associations."  
::= { t11FcSpSaControl 1 }

t11FcSpSaControlEntry OBJECT-TYPE

SYNTAX           T11FcSpSaControlEntry  
MAX-ACCESS       not-accessible  
STATUS           current  
DESCRIPTION

"Each entry identifies information for the one or more  
interfaces (identified by t11FcSpSaIfIndex) to a  
particular Fabric (identified by t11FcSpSaIfFabricIndex),  
and managed as part of the Fibre Channel management  
instance identified by fcmInstanceIndex.

The StorageType of a row in this table is specified by  
the instance of t11FcSpSaIfStorageType which is INDEX-ed  
by the same values of fcmInstanceIndex, t11FcSpSaIfIndex  
and t11FcSpSaIfFabricIndex."

INDEX { fcmInstanceIndex, t11FcSpSaIfIndex,  
          t11FcSpSaIfFabricIndex }  
::= { t11FcSpSaControlTable 1 }

T11FcSpSaControlEntry ::= SEQUENCE {  
  t11FcSpSaControlAuthFailEnable TruthValue,  
  t11FcSpSaControlInboundSpi     T11FcSpiIndex,  
  t11FcSpSaControlSource          FcAddressIdOrZero,  
  t11FcSpSaControlDestination     FcAddressIdOrZero,  
  t11FcSpSaControlFrame           OCTET STRING,  
  t11FcSpSaControlElapsed          TimeTicks,  
  t11FcSpSaControlSuppressed       Gauge32,  
  t11FcSpSaControlWindow           Unsigned32,  
  t11FcSpSaControlMaxNotifs        Unsigned32,  
  t11FcSpSaControlLifeExcdEnable   TruthValue,  
  t11FcSpSaControlLifeExcdSpi      T11FcSpiIndex,

t11FcSpSaControlLifeExcdDir      T11FcSaDirection,

```

    t11FcSpSaControlLifeExcdTime    TimeStamp
}

t11FcSpSaControlAuthFailEnable OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS           current
    DESCRIPTION
        "This object specifies whether a t11FcSpSaNotifyAuthFailure
        notification should be generated for the first occurrence
        of an Authentication failure within a time window for this
        Fabric."
    ::= { t11FcSpSaControlEntry 1 }

t11FcSpSaControlInboundSpi OBJECT-TYPE
    SYNTAX          T11FcSpiIndex
    MAX-ACCESS      read-only
    STATUS           current
    DESCRIPTION
        "The SPI value of the ingress Security Association on
        which was received the last frame for which a
        t11FcSpSaNotifyAuthFailure was generated.

        If no t11FcSpSaNotifyAuthFailure notifications have
        been generated, the value of this object is zero."
    ::= { t11FcSpSaControlEntry 2 }

t11FcSpSaControlSource OBJECT-TYPE
    SYNTAX          FcAddressIdOrZero
    MAX-ACCESS      read-only
    STATUS           current
    DESCRIPTION
        "The S_ID contained in the last frame for which a
        t11FcSpSaNotifyAuthFailure was generated.

        If no t11FcSpSaNotifyAuthFailure notifications have
        been generated, the value of this object is the
        zero-length string."
    ::= { t11FcSpSaControlEntry 3 }

t11FcSpSaControlDestination OBJECT-TYPE
    SYNTAX          FcAddressIdOrZero
    MAX-ACCESS      read-only
    STATUS           current

```

## DESCRIPTION

"The D\_ID contained in the last frame for which a t11FcSpSaNotifyAuthFailure was generated.

If no t11FcSpSaNotifyAuthFailure notifications have been generated, the value of this object is the zero-length string."

::= { t11FcSpSaControlEntry 4 }

## t11FcSpSaControlFrame OBJECT-TYPE

SYNTAX OCTET STRING (SIZE (0..256))

MAX-ACCESS read-only

STATUS current

## DESCRIPTION

"The binary content of the last frame for which a t11FcSpSaNotifyAuthFailure was generated. If more than 256 bytes of the frame are available, then this object contains the first 256 bytes. If less than 256 bytes of the frame are available, then this object contains the first N bytes, where N is greater or equal to zero.

If no t11FcSpSaNotifyAuthFailure notifications have been generated, the value of this object is the zero-length string."

::= { t11FcSpSaControlEntry 5 }

## t11FcSpSaControlElapsed OBJECT-TYPE

SYNTAX TimeTicks

MAX-ACCESS read-only

STATUS current

## DESCRIPTION

"The elapsed time since the last generation of a t11FcSpSaNotifyAuthFailure notification on the same Fabric, or the value of sysUpTime if no t11FcSpSaNotifyAuthFailure notifications have been generated since the last restart."

::= { t11FcSpSaControlEntry 6 }

## t11FcSpSaControlSuppressed OBJECT-TYPE

SYNTAX Gauge32

MAX-ACCESS read-only

STATUS current

## DESCRIPTION

"The number of occurrences of an Authentication failure on a Fabric which were suppressed because they occurred

on the same Fabric within the same time window as a previous Authentication failure for which a t11FcSpSaNotifyAuthFailure notification was generated.

The value of this object is reset to zero on a restart of the network management subsystem, and whenever a t11FcSpSaNotifyAuthFailure notification is generated. In the event that the value of this object reaches its maximum value, it remains at that value until it is reset on the generation of the next t11FcSpSaNotifyAuthFailure notification."

::= { t11FcSpSaControlEntry 7 }

#### t11FcSpSaControlWindow OBJECT-TYPE

SYNTAX            Unsigned32 (1..4294967295)

UNITS             "seconds"

MAX-ACCESS       read-write

STATUS            current

##### DESCRIPTION

"The length of a time window which begins when a t11FcSpSaNotifyAuthFailure notification is generated for any Security Association on a particular Fabric. For the duration of the time window, further Authentication failures occurring for the same Security Association are counted but no t11FcSpSaNotifyAuthFailure notification is generated.

When this object is modified before the end of a time window, that time window is immediately terminated, i.e., the next Authentication failure on the relevant Fabric after the modification will cause a new time window to begin with the new length."

DEFVAL    { 300 }

::= { t11FcSpSaControlEntry 8 }

#### t11FcSpSaControlMaxNotifs OBJECT-TYPE

SYNTAX            Unsigned32

MAX-ACCESS       read-write

STATUS            current

##### DESCRIPTION

"The maximum number of t11FcSpSaNotifyAuthFailure notifications to be generated per Fabric within a



t11FcSpSaControlWindow time window. Subsequent Authentication failures occurring on the same Fabric in the same time window are counted but no t11FcSpSaNotifyAuthFailure notification is generated.

Expires 11 January 2009

[Page 215]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

When this object is modified before the end of a time window, that time window is immediately terminated, i.e., the next Authentication failure on the relevant Fabric after the modification will cause a new time window to begin with the new length."

DEFVAL    { 16 }  
::= { t11FcSpSaControlEntry 9 }

t11FcSpSaControlLifeExcdEnable OBJECT-TYPE

SYNTAX        TruthValue  
MAX-ACCESS    read-write  
STATUS        current  
DESCRIPTION

"This object specifies whether t11FcSpSaNotifyLifeExceeded notifications should be generated for this Fabric."

DEFVAL    { true }  
::= { t11FcSpSaControlEntry 10 }

t11FcSpSaControlLifeExcdSpi OBJECT-TYPE

SYNTAX        T11FcSpiIndex  
MAX-ACCESS    read-only  
STATUS        current  
DESCRIPTION

"The SPI of the SA which was most recently terminated because its lifetime (in seconds or in passed bytes) was exceeded. Such terminations include those due to a failed attempt to renew an SA after its lifetime was exceeded."

::= { t11FcSpSaControlEntry 11 }

t11FcSpSaControlLifeExcdDir OBJECT-TYPE

SYNTAX        T11FcSaDirection  
MAX-ACCESS    read-only  
STATUS        current  
DESCRIPTION

"The direction of frame transmission on the SA which was most recently terminated because its lifetime (in seconds or in passed bytes) was exceeded."  
 ::= { t11FcSpSaControlEntry 12 }

t11FcSpSaControlLifeExcdTime OBJECT-TYPE

SYNTAX           TimeStamp  
MAX-ACCESS       read-only  
STATUS            current  
DESCRIPTION

Expires 11 January 2009

[Page 216]

---

Internet Draft       Fibre-Channel Security Protocols MIB

July 2008

"The time of the most recent termination of an SA due to its lifetime (in seconds or in passed bytes) being exceeded. Such terminations include those due to a failed attempt to renew an SA after its lifetime was exceeded."  
 ::= { t11FcSpSaControlEntry 13 }

--  
-- Notification definitions  
--

t11FcSpSaNotifyAuthFailure NOTIFICATION-TYPE

OBJECTS           { t11FcSpSaControlInboundSpi,  
                    t11FcSpSaControlSource,  
                    t11FcSpSaControlDestination,  
                    t11FcSpSaControlFrame,  
                    t11FcSpSaControlElapsed,  
                    t11FcSpSaControlSuppressed }

STATUS            current

DESCRIPTION

"When this notification is generated, it indicates the occurrence of an Authentication failure for a received FC-2 or CT\_IU frame. The t11FcSpSaControlInboundSpi, t11FcSpSaControlSource and t11FcSpSaControlDestination objects in the varbindlist are the frame's SPI, source and destination addresses, respectively. t11FcSpSaControlFrame provides the (beginning of the) frame's content if such is available.

This notification is generated only for the first occurrence of an Authentication failure on a Fabric within a time window. Subsequent occurrences of an Authentication Failure on the same Fabric within the same time window are counted but suppressed.

The value of t11FcSpSaControlElapsed contains (a lower bound on) the elapsed time since the last generation of this notification for the same Fabric. The value of t11FcSpSaControlSuppressed contains the number of generations which were suppressed in the time window after that last generation, or zero if unknown."

::= { t11FcSpSaMIBNotifications 1 }

t11FcSpSaNotifyLifeExceeded NOTIFICATION-TYPE  
OBJECTS { t11FcSpSaControlLifeExcdSpi,

Expires 11 January 2009

[Page 217]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

                                t11FcSpSaControlLifeExcdDir }  
STATUS                   current  
DESCRIPTION  
    "This notification is generated when the lifetime (in seconds or in passed bytes) of an SA is exceeded, and the SA is either immediately terminated or is terminated because an attempt to renew the SA fails. The values of t11FcSpSaControlLifeExcdSpi and t11FcSpSaControlLifeExcdDir contain the SPI and direction of the terminated SA."

::= { t11FcSpSaMIBNotifications 2 }

--  
-- Conformance  
--

t11FcSpSaMIBCompliances

                                OBJECT IDENTIFIER ::= { t11FcSpSaMIBConformance 1 }  
t11FcSpSaMIBGroups   OBJECT IDENTIFIER ::= { t11FcSpSaMIBConformance 2 }

t11FcSpSaMIBCompliance MODULE-COMPLIANCE

STATUS                   current  
DESCRIPTION

"The compliance statement for entities which implement  
FC-SP Security Associations."

```
MODULE -- this module
MANDATORY-GROUPS
{ t11FcSpSaCapabilityGroup,
  t11FcSpSaParamStatusGroup,
  t11FcSpSaSummaryCountGroup,
  t11FcSpSaProposalGroup,
  t11FcSpSaDropBypassGroup,
  t11FcSpSaActiveGroup,
  t11FcSpSaNotifInfoGroup,
  t11FcSpSaNotificationGroup
}

-- The following is an auxiliary (listed in an INDEX clause)
-- object for which the SMIV2 does not allow an OBJECT clause
-- to be specified, but for which this MIB has the following
-- compliance requirement:
--     OBJECT          t11FcSpSaIfIndex
--     DESCRIPTION
--         Compliance requires support for either one of:
```

Expires 11 January 2009

[Page 218]

---

Internet Draft      Fibre-Channel Security Protocols MIB      July 2008

```
--          - individual interfaces using ifIndex values, or
--          - the use of the zero value.

-- Write access is not required for any objects in this MIB module:
```

```
OBJECT          t11FcSpSaIfStorageType
MIN-ACCESS      read-only
DESCRIPTION     "Write access is not required."
```

```
OBJECT          t11FcSpSaTSelPropStorageType
MIN-ACCESS      read-only
DESCRIPTION     "Write access is not required."
```

```
OBJECT          t11FcSpSaTransStorageType
MIN-ACCESS      read-only
DESCRIPTION     "Write access is not required."
```

OBJECT	t11FcSpSaIfReplayPrevention
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaIfReplayWindowSize
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaIfTerminateAllSas
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaPropSecurityProt
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaPropTSelListIndex
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaPropTransListIndex
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaPropAcceptAlgorithm
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."

Expires 11 January 2009

[Page 219]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

OBJECT	t11FcSpSaPropRowStatus
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelPropDirection
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelPropStartSrcAddr
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."

OBJECT	t11FcSpSaTSelPropEndSrcAddr
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelPropStartDstAddr
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelPropEndDstAddr
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelPropStartRctl
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelPropEndRctl
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelPropStartType
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelPropEndType
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelPropRowStatus
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTransSecurityProt

MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTransEncryptAlg
MIN-ACCESS	read-only

DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTransEncryptKeyLen
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTransIntegrityAlg
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTransRowStatus
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelDrByAction
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelDrByStartSrcAddr
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelDrByEndSrcAddr
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelDrByStartDstAddr
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelDrByEndDstAddr
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelDrByStartRctl
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelDrByEndRctl
MIN-ACCESS	read-only

DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelDrByStartType
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelDrByEndType
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaTSelDrByRowStatus
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaPairTerminate
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaControlAuthFailEnable
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaControlWindow
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaControlMaxNotifs
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."
OBJECT	t11FcSpSaControlLifeExcdEnable
MIN-ACCESS	read-only
DESCRIPTION	"Write access is not required."

```
::= { t11FcSpSaMIBCompliances 1 }
```

```
-- Units of Conformance
```

```
t11FcSpSaCapabilityGroup OBJECT-GROUP
    OBJECTS { t11FcSpSaIfEspHeaderCapab,
               t11FcSpSaIfCTAuthCapab,
               t11FcSpSaIfIKEv2Capab,
               t11FcSpSaIfIkev2AuthCapab
             }
    STATUS   current
```



Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

## DESCRIPTION

"A collection of objects containing information related to capabilities of FC-SP entities."

::= { t11FcSpSaMIBGroups 1 }

## t11FcSpSaParamStatusGroup OBJECT-GROUP

OBJECTS { t11FcSpSaIfStorageType,  
          t11FcSpSaIfReplayPrevention,  
          t11FcSpSaIfReplayWindowSize,  
          t11FcSpSaIfDeadPeerDetections,  
          t11FcSpSaIfTerminateAllSas  
          }

STATUS current

## DESCRIPTION

"A collection of objects containing parameters and status information related to FC-SP entities."

::= { t11FcSpSaMIBGroups 2 }

## t11FcSpSaSummaryCountGroup OBJECT-GROUP

OBJECTS { t11FcSpSaIfOutDrops,  
          t11FcSpSaIfOutBypasses,  
          t11FcSpSaIfOutProcesses,  
          t11FcSpSaIfOutUnMatcheds,  
          t11FcSpSaIfInUnprotUnmtchDrops,  
          t11FcSpSaIfInDetReplays,  
          t11FcSpSaIfInUnprotMtchDrops,  
          t11FcSpSaIfInBadXforms,  
          t11FcSpSaIfInGoodXforms,  
          t11FcSpSaIfInProtUnmtchs  
          }

STATUS current

## DESCRIPTION

"A collection of objects containing summary counters for FC-SP Security Associations."

::= { t11FcSpSaMIBGroups 3 }

## t11FcSpSaProposalGroup OBJECT-GROUP

OBJECTS { t11FcSpSaPropSecurityProt,  
          t11FcSpSaPropTSelListIndex,  
          t11FcSpSaPropTransListIndex,  
          t11FcSpSaPropAcceptAlgorithm,  
          t11FcSpSaPropOutMatchSucceeds,  
          t11FcSpSaPropRowStatus,

t11FcSpSaTSelPropDirection,  
t11FcSpSaTSelPropStartSrcAddr,

Expires 11 January 2009

[Page 223]

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

t11FcSpSaTSelPropEndSrcAddr,  
t11FcSpSaTSelPropStartDstAddr,  
t11FcSpSaTSelPropEndDstAddr,  
t11FcSpSaTSelPropStartRctl,  
t11FcSpSaTSelPropEndRctl,  
t11FcSpSaTSelPropStartType,  
t11FcSpSaTSelPropEndType,  
t11FcSpSaTSelPropStorageType,  
t11FcSpSaTSelPropRowStatus  
}

STATUS    current

DESCRIPTION

"A collection of objects containing information  
related to making and accepting proposals for  
FC-SP Security Associations."

::= { t11FcSpSaMIBGroups 4 }

t11FcSpSaDropBypassGroup OBJECT-GROUP

OBJECTS { t11FcSpSaTSelDrByAction,  
t11FcSpSaTSelDrByStartSrcAddr,  
t11FcSpSaTSelDrByEndSrcAddr,  
t11FcSpSaTSelDrByStartDstAddr,  
t11FcSpSaTSelDrByEndDstAddr,  
t11FcSpSaTSelDrByStartRctl,  
t11FcSpSaTSelDrByEndRctl,  
t11FcSpSaTSelDrByStartType,  
t11FcSpSaTSelDrByEndType,  
t11FcSpSaTSelDrByMatches,  
t11FcSpSaTSelDrByRowStatus  
}

STATUS    current

DESCRIPTION

"A collection of objects containing information  
about Traffic Selectors of traffic to drop or bypass  
for FC-SP Security."

::= { t11FcSpSaMIBGroups 5 }

t11FcSpSaActiveGroup OBJECT-GROUP

```
OBJECTS { t11FcSpSaPairSecurityProt,
          t11FcSpSaPairTransListIndex,
          t11FcSpSaPairTransIndex,
          t11FcSpSaPairLifetimeLeft,
          t11FcSpSaPairLifetimeLeftUnits,
          t11FcSpSaPairTerminate,
          t11FcSpSaPairInProtUnMatches,
```

Expires 11 January 2009

[Page 224]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

```
          t11FcSpSaPairInDetReplays,
          t11FcSpSaPairInBadXforms,
          t11FcSpSaPairInGoodXforms,
          t11FcSpSaTransSecurityProt,
          t11FcSpSaTransEncryptAlg,
          t11FcSpSaTransEncryptKeyLen,
          t11FcSpSaTransIntegrityAlg,
          t11FcSpSaTransStorageType,
          t11FcSpSaTransRowStatus,
          t11FcSpSaTSELNegInInboundSpi,
          t11FcSpSaTSELNegInStartSrcAddr,
          t11FcSpSaTSELNegInEndSrcAddr,
          t11FcSpSaTSELNegInStartDstAddr,
          t11FcSpSaTSELNegInEndDstAddr,
          t11FcSpSaTSELNegInStartRctl,
          t11FcSpSaTSELNegInEndRctl,
          t11FcSpSaTSELNegInStartType,
          t11FcSpSaTSELNegInEndType,
          t11FcSpSaTSELNegInUnpMtchDrops,
          t11FcSpSaTSELNegOutInboundSpi,
          t11FcSpSaTSELNegOutStartSrcAddr,
          t11FcSpSaTSELNegOutEndSrcAddr,
          t11FcSpSaTSELNegOutStartDstAddr,
          t11FcSpSaTSELNegOutEndDstAddr,
          t11FcSpSaTSELNegOutStartRctl,
          t11FcSpSaTSELNegOutEndRctl,
          t11FcSpSaTSELNegOutStartType,
          t11FcSpSaTSELNegOutEndType,
          t11FcSpSaTSELNegSpiDirection,
          t11FcSpSaTSELNegSpiTrafSelPtr
        }
```

STATUS current

DESCRIPTION

"A collection of objects containing information related to currently active FC-SP Security Associations."

::= { t11FcSpSaMIBGroups 6 }

t11FcSpSaNotifInfoGroup OBJECT-GROUP

OBJECTS { t11FcSpSaControlAuthFailEnable,  
t11FcSpSaControlInboundSpi,  
t11FcSpSaControlSource,  
t11FcSpSaControlDestination,  
t11FcSpSaControlFrame,  
t11FcSpSaControlElapsed,  
t11FcSpSaControlSuppressed,

Expires 11 January 2009

[Page 225]

---

Internet Draft Fibre-Channel Security Protocols MIB

July 2008

t11FcSpSaControlWindow,  
t11FcSpSaControlMaxNotifs,  
t11FcSpSaControlLifeExcdEnable,  
t11FcSpSaControlLifeExcdSpi,  
t11FcSpSaControlLifeExcdDir,  
t11FcSpSaControlLifeExcdTime  
}

STATUS current

DESCRIPTION

"A collection of objects containing information related to notifications of events concerning FC-SP Security Associations."

::= { t11FcSpSaMIBGroups 7 }

t11FcSpSaNotificationGroup NOTIFICATION-GROUP

NOTIFICATIONS { t11FcSpSaNotifyAuthFailure,  
t11FcSpSaNotifyLifeExceeded  
}

STATUS current

DESCRIPTION

"A collection of notifications of events concerning FC-SP Security Associations."

::= { t11FcSpSaMIBGroups 8 }

END

## 7. Acknowledgements

This document was initially developed and approved by the INCITS Task Group T11.5 (<http://www.t11.org>) as the SM-FSM project. We wish to acknowledge the contributions and comments from the INCITS Technical Committee T11, including the following:

T11 Chair: Robert Snively, Brocade  
T11 Vice Chair: Claudio DeSanti, Cisco Systems  
T11.5 Chair: Roger Cummings, Symantec  
T11.5 members:  
    David Black, EMC  
    Don Fraser, HP  
    Larry Hofer, Brocade  
    Scott Kipp, Brocade  
    Ralph Weber, ENDL

The document was subsequently a work item of the IMSS Working Group

Expires 11 January 2009

[Page 226]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

(of the IETF), chaired by David Black (EMC Corporation). Bert Wijnen (Alcatel-Lucent) deserves many thanks for his thorough review of all five MIB modules in this (large!) document. We also wish to acknowledge Dan Romascanu (Avaya), the IETF Area Director, for his comments and assistance.

## 8. Normative References

[RFC2578]

McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)", STD 58, [RFC 2578](#), April 1999.

[RFC2579]

McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, [RFC 2579](#), April 1999.

[RFC2580]

McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Conformance Statements for SMIV2", STD 58, [RFC 2580](#), April 1999.

[RFC2863]

McCloghrie, K., and F. Kastenholz, "The Interface\$ Group MIB", [RFC 2863](#), June 2000.

[RFC3411]

Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 58, [RFC 3411](#), December 2002.

[RFC4001]

Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", [RFC 4001](#), February 2005.

[RFC4044]

K. McCloghrie, "Fibre Channel Management MIB", [RFC 4044](#), May 2005.

[RFC4303]

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

Expires 11 January 2009

[Page 227]

---

Internet Draft

Fibre-Channel Security Protocols MIB

July 2008

[RFC4306]

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

[RFC4438]

"Fibre-Channel Name Server MIB", DeSanti, C., Gaonkar, V., Vivek, H.K., McCloghrie, K., and S. Gai, [RFC 4438](#), April 2006.

[RFC4439]

DeSanti, C., Gaonkar, V., McCloghrie, K., and S. Gai, "Fibre Channel Fabric Address Manager MIB", [RFC 4439](#), March 2006.

[RFC4936]

DeSanti, C., Vivek, H.K., McCloghrie, K., and S. Gai, "Fibre Channel Zone Server MIB", [RFC 4936](#), August 2007.

[FC-FS-2]

"Fibre Channel - Framing and Signaling-2 (FC-FS-2)", ANSI INCITS 424-2007, <http://www.t11.org/t11/stat.nsf/upnum/1619-d>, February 2007.

[FC-GS-5]

"Fibre Channel - Generic Services - 5 (FC-GS-5)", ANSI INCITS 427-2006, <http://www.t11.org/t11/stat.nsf/upnum/1677-d>, December 2006.

[FC-SP]

"Fibre Channel - Security Protocols (FC-SP)", ANSI INCITS 426-2007, <http://www.t11.org/t11/stat.nsf/upnum/1570-d>, T11/Project 1570-D, February 2007.

[FC-SW-4]

"Fibre Channel - Switch Fabric-4 (FC-SW-4)", <http://www.t11.org/t11/stat.nsf/upnum/1674-d>, ANSI INCITS 418-2006, April 2006.

[RFC2119]

S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), [BCP 0014](#), March 1997.

## [9](#). Informative References

[RFC1492]

C. Finseth, "An Access Control Protocol, Sometimes Called TACACS",

Expires 11 January 2009

[Page 228]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

[RFC 1492](#), July 1993.

[RFC2741]

Daniele, M., Wijnen, B., Ellison, M., and D. Francisco, "Agent Extensibility (AgentX) Protocol Version 1", [RFC 2741](#), January 2000.

[RFC2837]

K. Teow, "Definitions of Managed Objects for the Fabric Element in Fibre Channel Standard", [RFC 2837](#), May 2000.

[RFC2865]

Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.

[RFC3410]

Case, J., Mundy, R., Partain, D. and B. Stewart, "Introduction and Applicability Statements for Internet- Standard Management Framework", [RFC 3410](#), December 2002.

[RFC3588]

Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", [RFC 3588](#), September 2003.

[RFC4595]

Maino, F., and D. Black, "Use of IKEv2 in the Fibre Channel Security Association Management Protocol", [RFC 4595](#), July 2006.

[RFC4625]

DeSanti, C., McCloghrie, K., Kode, S., and S. Gai, "Fibre Channel Routing Information MIB", [RFC 4625](#), August 2006.

[RFC4626]

DeSanti, C., Gaonkar, V., McCloghrie, K., and S. Gai, "MIB for Fibre Channel's Fabric Shortest Path First (FSPF) Protocol", [RFC 4626](#), August 2006.

[RFC4668]

D. Nelson, "RADIUS Authentication Client MIB for IPv6", [RFC 4668](#), August 2006.

[RFC4747]

Kipp, S., Ramkumar, G., and K. McCloghrie, "The Virtual Fabrics MIB", [RFC 4747](#), November 2006.

[RFC4935]



Channel Fabric Configuration Server MIB", [RFC 4935](#), August 2007.

[RFC4983]

DeSanti, C., Vivek, H.K., McCloghrie, K., and S. Gai, "Fibre Channel Registered State Change Notification (RSCN) MIB", [RFC 4983](#), August 2007.

#### 10. IANA Considerations

IANA is requested to make one MIB OID assignment, under the appropriate subtree, for each of the five MIB modules defined in this document.

## 11. Security Considerations

In this section, the first sub-section explains why this document does not define MIB objects for particular items of (management) information. This is followed by one sub-section for each of the MIB modules defined in [section 6](#), listing their individual Security Considerations. The section concludes with Security Considerations common to all of these MIB modules.

The key word "RECOMMENDED" contained in this section is to be interpreted as described in [BCP 14](#) [[RFC2119](#)].

### 11.1. Information not defined in this document

This document doesn't define any MIB objects for the secrets which need to be known/determined by FC-SP entities in order to use DH-CHAP to authenticate each other. Such secrets are "highly sensitive" and need to be "strong secrets" (e.g., randomly generated and/or from an external source, see section 5.4.8 of [[FC-SP](#)]) rather than just passwords. Thus, such secrets need to be managed by mechanisms other than the MIB modules defined here.

### 11.2. The T11-FC-SP-TC-MIB Module

This MIB module defines some data types and assigns some Object Identifiers, for use as the syntax and as values of MIB objects respectively, but it itself defines no MIB objects. Thus, there is no direct read or write access via a management protocol, such as SNMP, to these definitions. Nevertheless, it does include the assignment of enumerations and OIDs to represent cryptographic algorithms/transforms, and it is appropriate for such assignments to be augmented with new assignments as and when new algorithms/transforms are available.

### 11.3. The T11-FC-SP-AUTHENTICATION-MIB Module

There are several management objects defined in this MIB module with a MAX-ACCESS clause of read-write. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These objects and their sensitivity/vulnerability are:

    t11FcSpAuStorageType

- could cause changes in the configuration to be retained or

not retained over restarts, against the wishes of management.

t11FcSpAuSendRejNotifyEnable

t11FcSpAuRcvRejNotifyEnable

- could cause the suppression of SNMP notifications (e.g., of authentication failures or protocol failures), or the disruption of network operations due to the generation of unwanted notifications.

t11FcSpAuDefaultLifetime

t11FcSpAuDefaultLifetimeUnits

- could cause the lifetimes of Security Associations to be extended longer than might be secure, or shortened to cause an increase in the overhead of using security.

t11FcSpAuRejectMaxRows

- could cause a smaller audit trail of Authentication rejects, thereby hiding the tracks of an attacker, or a larger audit trail of Authentication rejects causing resources to be wasted.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the tables and objects and their sensitivity/vulnerability:

t11FcSpAuEntityTable

- the capabilities of FC-SP Authentication entities in terms of what cryptographic algorithms they support, and various configuration parameters of FC-SP Authentication entities.

t11FcSpAuIfStatTable

- the mapping of which FC-SP Authentication entities operate on which interfaces.

t11FcSpAuRejectTable

- an audit trail of authentication failures and other Authentication Protocol failures.

There are several management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These objects and their sensitivity/vulnerability are:

t11FcSpZsServerEnabled

- could cause FC-SP Zoning mode to be enabled or not enabled, against the wishes of management.

t11FcSpZoneSetHashStatus

- could cause an FC-SP implementation to recalculate the values of the Active Zone Set Hash and the Zone Set Database Hash more frequently than is required by management.

t11FcSpZsNotifyJoinSuccessEnable

t11FcSpZsNotifyJoinFailureEnable

- could cause the suppression of SNMP notifications that a Switch in one Fabric has successfully joined/failed to join with a Switch in another Fabric, or the disruption of network operations due to the generation of unwanted notifications.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the objects and their sensitivity/vulnerability:

t11FcSpZsServerCapabilityObject

t11FcSpZsServerEnabled

- the FC-SP Zoning capabilities and status of the FC-SP

implementation.

t11FcSpZoneSetHashStatus  
t11FcSpActiveZoneSetHashType  
t11FcSpActiveZoneSetHash  
t11FcSpZoneSetDatabaseHashType  
t11FcSpZoneSetDatabaseHash

- the current values of the Active Zone Set Hash and the Zone Set Database Hash.

Expires 11 January 2009

[Page 233]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

#### [11.5.](#) The T11-FC-SP-POLICY-MIB Module

There are many management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. The objects and tables and their sensitivity/vulnerability are:

t11FcSpPoNaSummaryTable  
t11FcSpPoNaSwListTable  
t11FcSpPoNaSwMembTable  
t11FcSpPoNaNoMembTable  
t11FcSpPoNaCtDescrTable  
t11FcSpPoNaSwConnTable  
t11FcSpPoNaIpMgmtTable

- could change the currently inactive FC-SP Fabric Policies, so as to allow unauthorized connectivity of Switches and/or Nodes to the network, or between Switches in the network, or, to prohibit such connectivity even when authorized.

t11FcSpPoNaIpMgmtTable  
t11FcSpPoNaWkpDescrTable

- could change the currently inactive FC-SP Fabric Policies, so as to allow unauthorized management access to Switches, or prohibit authorized management access to Switches.

t11FcSpPoNaSummaryTable  
t11FcSpPoNaSwMembTable

t11FcSpPoNaNoMembTable  
t11FcSpPoNaAttribTable  
t11FcSpPoNaAuthProtTable

- could change the currently inactive FC-SP Fabric Policies, so as to allow Security Associations with reduced security or require Security Associations which are unnecessarily-secure.

t11FcSpPoOperActivate  
t11FcSpPoOperDeActivate

- could cause the currently active FC-SP Fabric Policies to be de-activated and currently inactive FC-SP Fabric Policies (e.g., those modified as above) to be activated instead.

t11FcSpPoStorageType

- could cause changes in the configuration and/or in FC-SP Fabric Policies to be retained or not retained over restarts,

Expires 11 January 2009

[Page 234]

---

Internet Draft      Fibre-Channel Security Protocols MIB

July 2008

against the wishes of management.

t11FcSpPoNotificationEnable

- could cause the suppression of SNMP notifications on the successful/unsuccessful activation/de-activation of Fabric Policies, and thereby hide successful/failed attempts to make unauthorized changes, or cause the disruption of network operations due to the generation of unwanted notifications.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the tables and their sensitivity/vulnerability:

t11FcSpPoTable  
t11FcSpPoSummaryTable  
t11FcSpPoSwMembTable  
t11FcSpPoNoMembTable  
t11FcSpPoCtDescrTable  
t11FcSpPoSwConnTable

t11FcSpPoIpMgmtTable  
t11FcSpPoWkpDescrTable  
t11FcSpPoAttribTable  
t11FcSpPoAuthProtTable

- the currently active FC-SP Fabric Policies which can be examined by an attacker looking for possible security vulnerabilities in the active policies.

#### [11.6.](#) The T11-FC-SP-SA-MIB Module

There are several management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These objects and their sensitivity/vulnerability are:

t11FcSpSaIfStorageType  
t11FcSpSaTSelPropStorageType  
t11FcSpSaTransStorageType

- could cause changes in configuration information related to FC-SP Security Associations to be retained or not retained over restarts, against the wishes of management.

t11FcSpSaIfReplayPrevention  
t11FcSpSaIfReplayWindowSize

- could cause changes in the operation of anti-replay protection, thereby permitting an attacker to conduct replay attacks, or requiring FC-SP implementations to engage in unnecessary protection against replay.

t11FcSpSaIfTerminateAllSas  
t11FcSpSaPairTerminate

- could cause FC-SP Security Associations to be aborted unnecessarily.

t11FcSpSaControlAuthFailEnable

- could cause the suppression of SNMP notifications on the occurrence of Authentication failures for received FC-2 or CT\_IU frames, thereby hiding attempts to subvert security measures, or cause the disruption of network operations due to the generation of unwanted notifications.

#### t11FcSpSaControlLifeExcdEnable

- could cause the suppression of SNMP notifications on the occurrence of an FC-SP Security Association exceeding its lifetime, thereby possibly causing disruption to network usage due to a delay in determining the problem and/or re-establishing the Security Association.

#### t11FcSpSaControlWindow

- could cause the suppression of second and subsequent SNMP notifications on the occurrence of Authentication failures for received FC-2 or CT\_IU frames, thereby masking repeated attempts to subvert security measures, or cause the disruption of network operations due to the generation of unwanted notifications.

#### t11FcSpSaControlMaxNotifs

- could cause the suppression of all SNMP notifications on the occurrence of Authentication failures for received FC-2 or CT\_IU frames, thereby masking attempts to subvert security measures, or cause the disruption of network operations due to the generation of unwanted notifications.

#### t11FcSpSaPropTable

#### t11FcSpSaTSelPropTable

#### t11FcSpSaTransTable

- could cause an FC-SP entity to propose the setup of Security Associations which apply to a different selection of traffic and/or using different security transforms, such that some traffic has a reduced level of security which might improve an attacker's chance of subverting security, or an increased level of security which would involve unnecessary security processing, or cause the negotiation of Security Associations to fail to find commonly-acceptable parameters such that no



Security Associations can be established.

t11FcSpSaTSELDrByTable

- could cause an FC-SP entity to select different sets of traffic which are: a) to be sent/received without being protected by FC-SP security, thereby providing an attacker with access to read authentic traffic or the ability to introduce unauthentic traffic; or b) to be dropped instead of being sent/after being received, thereby causing disruption to network usage.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the tables and objects and their sensitivity/vulnerability:

t11FcSpSaIfTable

- information concerning the capabilities, parameters and status of an FC-SP entity's support for Security Associations.

t11FcSpSaPropTable

t11FcSpSaTSELPropTable

t11FcSpSaTransTable

- information on the proposals which will be used by an FC-SP entity to negotiate Security Associations.

t11FcSpSaTSELDrByTable

- information on which subsets of traffic an FC-SP entity will send or receive without being protected by FC-SP security, or will drop before sending/after receiving.

t11FcSpSaPairTable

t11FcSpSaTSELNegInTable

t11FcSpSaTSELNegOutTable

t11FcSpSaTSELSpiTable

- information on which Security Associations are currently

active, what subsets of traffic they are carrying, and what security protection is being given to them.

#### 11.7. Recommendations common to all MIB Modules

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is RECOMMENDED that implementors consider the security features as provided by the SNMPv3 framework (see [\[RFC3410\]](#), [section 8](#)), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

Because the two algorithms currently specified for T11FcSpPolicyHashFormat are SHA-1 and SHA-256, the definition of T11FcSpHashCalculationStatus expresses a concern in regard to not incrementally recomputing the hashes after each change when a series of multiple related changes are being made. This method of reducing computation is intended as a responsiveness measure (i.e., cooperating SNMP managers and agents can get things done faster), not as a DoS countermeasure. Nevertheless, implementations should also consider the DoS possibilities in these scenarios; potential countermeasures include: requiring authentication for SETs and the rate-limiting of SET operations if they can cause significant computation.

## 12. Authors' Addresses

Claudio DeSanti  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134 USA  
Phone: +1 408 853-9172  
EMail: cds@cisco.com

Fabio Maino  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134 USA  
Phone: +1 408 853-7530  
EMail: fmaino@cisco.com

Keith McCloghrie  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA USA 95134  
Phone: +1 408-526-5260  
Email: kzm@cisco.com

## Full Copyright Statement

Copyright (C) The IETF Trust (2008). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Disclaimer of validity

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has

made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

#### Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

Expires 11 January 2009

[Page 240]