To: T10 Technical Committee
From: Rob Elliott, HP (elliott@hp.com)
Date: 14 August 2006
Subject: 06-373r0 SAS-2 Enable and disable zoning by management identifier key

Revision history
Revision 0 (14 August 2006) First revision

Related documents
sas2r05a - Serial Attached SCSI - 2 (SAS-2) revision 5a

Overview
SAS-2 revision 5a allows an administrator's physical presence (the definition of which is vendor-specific) to be used to allow an SMP initiator port that does not have access to zone group 2 to enable or disable zoning in a zoning expander device.

For systems that are remotely managed, an SMP initiator port needs to be able to manage zoning in an expander device without physical presence being asserted. A password-based scheme is proposed. The password is called a "management identifier key" to match the terminology used in the Access Controls commands in SPC-4. If the SMP request contains the correct management identifier key, then the request is processed. If the SMP request contains an incorrect management identifier key, then the request is rejected with a function result of NO MANAGEMENT ACCESS RIGHTS.

The management identifier key is not cryptographically secure; it could be snooped by any expander on the pathway or by a SAS logic analyzer inserted on the pathway. It is not designed for one-time use, so a rogue SMP initiator port could replay it later. The intent of the management identifer key to keep zoning secure from software attacks, not hardware attacks. The ZPSDS is considered trusted, but phys attached to the boundary of the ZPSDS are not trusted. Future proposals may define a cryptographically secure mechanism, based on work underway in the Trusted Computing Group and in the T10 SSC Working Group for tape data encryption.

The management identifier key can be read with an SMP REPORT MANAGEMENT IDENTIFIER KEY function by any SMP initiator port if physical presence is asserted.

The management identifier key can by changed with an SMP CONFIGURE MANAGEMENT IDENTIFIER KEY function by any SMP initiator port if physical presence is asserted or by any SMP initiator port that presents the old key in the request.

The administrator would typically enter the management identifier key while physically present to install the hardware containing the expander. As seen with Wireless Ethernet, default passwords created by the manufacturer providing a misleading level of security; a default of no password is more honest. The password could also be configured through a sideband mechanism (e.g., serial port, Ethernet port, USB key) with security mechanisms outside the scope of the SAS standard.

The manaegment identifier key is defined as a 16-byte (128-bit) value, twice the length of the Access Controls management identifier key. The value should be as random as possible. A simple text string is not recommended since it is too short; a hash value of a text string is a better approach. This makes what is transferred on the wire differ from what the user types on a keyboard.

Editor's Note 1: Access Controls uses 8 bytes (64 bits). 20 bytes (160 bits) would support an untruncated SHA-1 hash; 32 bytes (256 bits) would support SHA-256; 64 bytes (512 bits) would support SHA-512. Are secure hashes overkill since the delivery mechanism is not secure?

Editor's Note 2: Logging of unsuccessful attempts is probably necessary. Access Controls defines an Invalid Key events counter that records each attempt with a bad password, recording the TransportID of the culprit.

Suggested changes

10.4.3.1 SMP function request frame format

...

The FUNCTION field specifies which SMP function is being requested and is defined in table 1. If the value in the FUNCTION field is not supported by the management device server, it shall return a function result of UNKNOWN SMP FUNCTION as described in table 2.

Table 1 — SMP functions (FUNCTION field) (part 1 of 2)

Code	SMP function	Description	Reference
00h	REPORT GENERAL	Return general information about the device	10.4.3.3
01h	REPORT MANUFACTURER INFORMATION	Return vendor and product identification	10.4.3.4
02h	READ GPIO REGISTER	See SFF-8485	
03h	REPORT SELF-CONFIGURATION STATUS	Return status of the discover process in a self-configuring expander device	10.4.3.6
04h	REPORT MANAGEMENT IDENTIFIER KEY	Report the management identifier key	10.4.3.xx
~~04h~~05h - 0Fh	Reserved for general SMP input functions		
10h	DISCOVER	Return information about the specified phy	10.4.3.5
11h	REPORT PHY ERROR LOG	Return error logging information about the specified phy	10.4.3.7
12h	REPORT PHY SATA	Return information about a phy currently attached to a SATA phy	10.4.3.8
13h	REPORT ROUTE INFORMATION	Return phy-based expander route table information	10.4.3.9
14h	REPORT PHY EVENT INFORMATION	Return phy event information for the specified phy	10.4.3.10
15h	REPORT PHY BROADCAST COUNTS	Return Broadcast counts	10.4.3.11
16h	DISCOVER LIST	Return information about the specified phys	10.4.3.12
17h	REPORT EXPANDER ROUTE TABLE	Return contents of the expander-based expander route table	10.4.3.13
18h - 1Fh	Reserved for phy-based SMP input functions		
20h - 3Fh	Reserved for SMP input functions		
40h - 7Fh	Vendor specific		
80h	CONFIGURE GENERAL	Configure the device	10.4.3.14
81h	ENABLE DISABLE ZONING	Enable or disable zoning	10.4.3.15
82h	WRITE GPIO REGISTER	See SFF-8485	
83h	CONFIGURE MANAGEMENT IDENTIFIER KEY	Configure the management identifier key	10.4.3.xx
~~83h -~~ 84h	Reserved for general SMP output functions		

Table 1 — SMP functions (FUNCTION **field)** (part 2 of 2)

Code	SMP function	Description	Reference
85h	ZONED BROADCAST	Transmit the specified Broadcast on the expander ports in the specified zone group(s)	10.4.3.16
86h - 8Fh	Reserved for general SMP output functions		
90h	CONFIGURE ROUTE INFORMATION	Change phy-based expander route table information	10.4.3.17
91h	PHY CONTROL	Request actions by the specified phy	10.4.3.18
92h	PHY TEST FUNCTION	Request a test function by the specified phy	10.4.3.19
93h	CONFIGURE PHY EVENT INFORMATION	Configure phy event information for the specified phy	10.4.3.20
94h - 9Fh	Reserved for phy-based SMP output functions		
A0h - BFh	Reserved for SMP output functions		
C0h - FFh	Vendor specific		

10.4.3.2 SMP function response frame format

...

The FUNCTION RESULT field is defined in table 2.

Table 2 — FUNCTION RESULT **field** (part 1 of 2)

Code	Name	SMP function(s)	Description
00h	SMP FUNCTION ACCEPTED	All	The management device server supports the SMP function. The ADDITIONAL RESPONSE BYTES field contains the requested information.
01h	UNKNOWN SMP FUNCTION	Unknown	The management device server does not support the requested SMP function. The ADDITIONAL RESPONSE BYTES field may be present but shall be ignored.
02h	SMP FUNCTION FAILED	All	The management device server supports the SMP function, but the requested SMP function failed. The ADDITIONAL RESPONSE BYTES may be present but shall be ignored.
03h	INVALID REQUEST FRAME LENGTH	All	The management device server supports the SMP function, but the SMP request frame length was invalid (i.e., did not match the frame size defined for the function). The ADDITIONAL RESPONSE BYTES may be present but shall be ignored.
...	...	...	...

Table 2 — FUNCTION RESULT **field** (part 2 of 2)

Code	Name	SMP function(s)	Description
20h	SMP ZONE VIOLATION	CONFIGURE GENERAL, ENABLE DISABLE ZONING, ZONED BROADCAST, PHY CONTROL, PHY TEST FUNCTION, CONFIGURE PHY EVENT INFORMATION	The management device server supports the function, but zoning is enabled and the SMP initiator port does not have access to a necessary zone group according to the zone permission table (see 4.9.3.2). The ADDITIONAL RESPONSE BYTES may be present but shall be ignored.
21h	~~PHYSICAL PRESENCE NOT ASSERTED~~NO MANAGEMENT ACCESS RIGHTS	ENABLE DISABLE ZONING	Physical presence or a management identifier key was required but was not detected by the expander device when the SMP function was requested.
22h	UNKNOWN ENABLE DISABLE ZONING VALUE	ENABLE DISABLE ZONING	The ENABLE DISABLE ZONING field is set to 11b (i.e., Reserved).
All others	Reserved		

10.4.3.3 REPORT MANAGEMENT IDENTIFIER KEY function [all new, changes not highlighted]

The REPORT MANAGEMENT IDENTIFIER KEY function returns the management identifier key. This SMP function shall be implemented by all management device servers in zoning expander devices. This function shall only be processed from SMP initiator ports that have access to zone group 2 (see 4.9.3.2).

Table 3 defines the request format.

Table 3 — REPORT MANAGEMENT IDENTIFIER KEY request

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (40h)							
1	FUNCTION (04h)							
2	Reserved							
3	REQUEST LENGTH (00h)							
4	(MSB)			CRC				
7								(LSB)

The SMP FRAME TYPE field shall be set to 40h.

The FUNCTION field shall be set to 04h.

The REQUEST LENGTH field shall be set to 00h.

The CRC field is defined in 10.4.3.1.

Table 4 defines the response format.

Table 4 — REPORT MANAGEMENT IDENTIFIER KEY response

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (41h)							
1	FUNCTION (04h)							
2	FUNCTION RESULT							
3	RESPONSE LENGTH (03h)							
4	(MSB)				EXPANDER CHANGE COUNT			
5								(LSB)
6					Reserved			
7								
8	(MSB)				MANAGEMENT IDENTIFIER KEY			
15								(LSB)
16	(MSB)				CRC			
19								(LSB)

The SMP FRAME TYPE field shall be set to 41h.

The FUNCTION field shall be set to 04h.

The FUNCTION RESULT field is defined in 10.4.3.2.

The RESPONSE LENGTH field shall be set to 03h.

The EXPANDER CHANGE COUNT field is defined in the SMP REPORT GENERAL response (see 10.4.3.3).

The CRC field is defined in 10.4.3.2.

[end of all-new section, change highlights resume]

10.4.3.14 CONFIGURE GENERAL function

The CONFIGURE GENERAL function requests actions by the device containing the management device server. This SMP function may be implemented by any management device server. In zoning expander devices, if zoning is enabled then this function shall only be processed from SMP initiator ports that have access to zone group 2 (see 4.9.3.2).

Table 5 defines the request format.

Table 5 — CONFIGURE GENERAL request

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (40h)							
1	FUNCTION (80h)							
2	Reserved							
3	REQUEST LENGTH (~~03h~~07h)							
4	(MSB)							
5	EXPECTED EXPANDER CHANGE COUNT							(LSB)
6								
7	Reserved							
8	Reserved				UPDATE MANAGEMENT IDENTIFIER KEY	UPDATE STP SMP I_T NEXUS LOSS TIME	UPDATE STP MAXIMUM CONNECT TIME LIMIT	UPDATE STP BUS INACTIVITY TIME LIMIT
9	Reserved							
10	(MSB)							
11	STP BUS INACTIVITY TIME LIMIT							(LSB)
12	(MSB)							
13	STP MAXIMUM CONNECT TIME LIMIT							(LSB)
14	(MSB)							
15	STP SMP I_T NEXUS LOSS TIME							(LSB)
16	(MSB)							
31	MANAGEMENT IDENTIFIER KEY							(LSB)
~~16~~32	(MSB)							
~~19~~35	CRC							(LSB)

The SMP FRAME TYPE field shall be set to 40h.

The FUNCTION field shall be set to 80h.

The REQUEST LENGTH field shall be set to ~~03h~~07h.

If the management device server is not in an expander device or the EXPECTED EXPANDER CHANGE COUNT field is set to 0000h, the EXPECTED EXPANDER CHANGE COUNT field shall be ignored. If the management device server is in an expander device and the EXPECTED EXPANDER CHANGE COUNT field is not set to 0000h, then:

a) if the EXPECTED EXPANDER CHANGE COUNT field contains the current expander change count (i.e., the value of the EXPANDER CHANGE COUNT field that would be returned by an SMP REPORT GENERAL response at this time), the management device server shall process the function; and
b) If the EXPECTED EXPANDER CHANGE COUNT field does not contain the current expander change count, the management device server shall return a function result of INVALID EXPANDER CHANGE COUNT in the response frame.

An UPDATE MANAGEMENT IDENTIFIER KEY bit set to one specifies that the MANAGEMENT IDENTIFIER KEY field shall be honored. An UPDATE MANAGEMENT IDENTIFIER KEY bit set to zero specifies that the MANAGEMENT IDENTIFIER KEY field shall be ignored.

An UPDATE STP BUS INACTIVITY TIME LIMIT bit set to one specifies that the STP BUS INACTIVITY TIME LIMIT field shall be honored. An UPDATE STP BUS INACTIVITY TIME LIMIT bit set to zero specifies that the STP BUS INACTIVITY TIME LIMIT field shall be ignored.

An UPDATE STP MAXIMUM CONNECT TIME LIMIT bit set to one specifies that the STP MAXIMUM CONNECT TIME LIMIT field shall be honored. An UPDATE STP MAXIMUM CONNECT TIME LIMIT bit set to zero specifies that the STP MAXIMUM CONNECT TIME LIMIT field shall be ignored.

An UPDATE STP SMP I_T NEXUS LOSS TIME bit set to one specifies that the STP SMP I_T NEXUS LOSS TIME field shall be honored. An UPDATE STP SMP I_T NEXUS LOSS TIME bit set to zero specifies that the STP SMP I_T NEXUS LOSS TIME field shall be ignored.

The STP BUS INACTIVITY TIME LIMIT field contains the maximum period that an STP target port is permitted to maintain a connection (see 4.1.11) without transferring a frame to the STP initiator port. This value shall be the number of 100 μs increments between frames that the STP target port transmits during a connection. When this number is exceeded, the STP target port shall close the connection. A value of zero in this field specifies that there is no bus inactivity time limit. This value is reported in the STP BUS INACTIVITY TIME LIMIT field in the SMP REPORT GENERAL response (see 10.4.3.3). The bus inactivity time limit is enforced by the port layer (see 8.2.3).

The STP MAXIMUM CONNECT TIME LIMIT field contains the maximum duration of a connection (see 4.1.11). This value shall be the number of 100 μs increments that an STP target port transmits during a connection after which the STP target port shall connection at the next opportunity (e.g., a value of one in this field means that the time is less than or equal to 100 μs and a value of two in this field means that the time is less than or equal to 200 μs). If an STP target port is transferring a frame when the maximum connection time limit is exceeded, the STP target port shall complete transfer of the frame before closing the connection. A value of zero in this field specifies that there is no maximum connection time limit. This value is reported in the STP MAXIMUM CONNECT TIME LIMIT in the SMP REPORT GENERAL response (see 10.4.3.3). The maximum connection time limit is enforced by the port layer (see 8.2.3).

The STP SMP I_T NEXUS LOSS TIME field contains the time that an STP target port or SMP initiator port shall retry connection requests that are rejected with responses indicating the destination port may no longer be present (see 8.2.2) before recognizing an I_T nexus loss (see 4.5). Table 6 defines the values of the STP SMP I_T NEXUS LOSS TIME field. This value is enforced by the port layer (see 8.2.2).

Table 6 — STP SMP I_T NEXUS LOSS TIME field

Code	Description
0000h	Vendor-specific amount of time.
0001h to FFFEh	Time in milliseconds.
FFFFh	The port shall never recognize an I_T nexus loss (i.e., it shall retry the connection requests forever).

NOTE 1 - The default value of the STP SMP I_T NEXUS LOSS TIME field should be non-zero. It is recommended that this value be 2 000 ms.

NOTE 2 - An STP initiator port should retry connection requests for the time indicated by the STP SMP I_T NEXUS LOSS field in the SMP REPORT GENERAL response for the STP target port to which it is trying to establish a connection.

The MANAGEMENT IDENTIFIER KEY field contains a key used to allow permission to enable and disable zoning without physical presence.

The CRC field is defined in 10.4.3.1.

Table 5 defines the response format.

Table 7 — CONFIGURE GENERAL response

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (41h)							
1	FUNCTION (80h)							
2	FUNCTION RESULT							
3	RESPONSE LENGTH (00h)							
4	(MSB)			CRC				
7								(LSB)

The SMP FRAME TYPE field shall be set to 41h.

The FUNCTION field shall be set to 80h.

The FUNCTION RESULT field is defined in 10.4.3.2.

The RESPONSE LENGTH field shall be set to 00h.

The CRC field is defined in 10.4.3.2.

10.4.3.15 ENABLE DISABLE ZONING function

The ENABLE DISABLE ZONING function requests actions by the expander device containing the SMP target port. This SMP function shall be supported by SMP target ports in zoning expander devices (see 4.9). Other SMP target ports shall not support this SMP function. This SMP function shall only be processed if:

a) the request is received from an SMP initiator port that has access to zone group 2 (see 4.9.3.2);
b) the request contains the current management identifier key; or
c) the request is received from any SMP initiator port while physical presence is asserted.

Table 8 defines the request format.

Table 8 — ENABLE DISABLE ZONING request

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (40h)							
1	FUNCTION (81h)							
2	Reserved							
3	REQUEST LENGTH (~~02h~~06h)							
4	(MSB)			EXPECTED EXPANDER CHANGE COUNT				
5								(LSB)
6				Reserved				
7								
8	Reserved						ENABLE DISABLE ZONING	
9				Reserved				
11								
12	(MSB)			MANAGEMENT IDENTIFIER KEY				
23								(LSB)
~~12~~24	(MSB)			CRC				
~~15~~27								(LSB)

The SMP FRAME TYPE field shall be set to 40h.

The FUNCTION field shall be set to 81h.

The REQUEST LENGTH field shall be set to ~~02h~~06h.

The EXPECTED EXPANDER CHANGE COUNT field is defined in the CONFIGURE GENERAL request (see 10.4.3.14).

The ENABLE DISABLE ZONING field is defined in table 9.

Table 9 — ENABLE DISABLE ZONING field

Code	Description
00b	No change
01b	Enable zoning
10b	Disable zoning
11b	Reserved

If physical presence is not asserted and the MANAGEMENT IDENTIFIER KEY field does not match the current management identifier key maintained by the management device server, then the management device server shall return a function result of NO MANAGEMENT ACCESS in the response frame.

The CRC field is defined in 10.4.3.1.

Table 10 defines the response format.

Table 10 — ENABLE DISABLE ZONING response

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (41h)							
1	FUNCTION (81h)							
2	FUNCTION RESULT							
3	RESPONSE LENGTH (00h)							
4	(MSB)	CRC						
7								(LSB)

The SMP FRAME TYPE field shall be set to 41h.

The FUNCTION field shall be set to 81h.

The FUNCTION RESULT field is defined in 10.4.3.2.

The RESPONSE LENGTH field shall be set to 00h.

The CRC field is defined in 10.4.3.2.

10.4.3.15 CONFIGURE MANAGEMENT IDENTIFIER KEY function [all new, changes not highlighted]

The CONFIGURE MANAGEMENT IDENTIFIER KEY function requests actions by the expander device containing the SMP target port. This SMP function shall be supported by SMP target ports in zoning expander devices (see 4.9). Other SMP target ports shall not support this SMP function. This SMP function shall only be processed if:

a) the request contains the current management identifier key; or
b) the request is received from any SMP initiator port while physical presence is asserted.

Table 11 defines the request format.

Table 11 — CONFIGURE MANAGEMENT IDENTIFIER KEY request

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (40h)							
1	FUNCTION (83h)							
2	Reserved							
3	REQUEST LENGTH (09h)							
4	(MSB)	EXPECTED EXPANDER CHANGE COUNT						
5								(LSB)
6		Reserved						
7								
8	(MSB)	MANAGEMENT IDENTIFIER KEY						
23								(LSB)
24	(MSB)	NEW MANAGEMENT IDENTIFIER KEY						
47								(LSB)
48	(MSB)	CRC						
51								(LSB)

The SMP FRAME TYPE field shall be set to 40h.

The FUNCTION field shall be set to 83h.

The REQUEST LENGTH field shall be set to 09h.

The EXPECTED EXPANDER CHANGE COUNT field is defined in the CONFIGURE GENERAL request (see 10.4.3.14).

If physical presence is not asserted and the MANAGEMENT IDENTIFIER KEY field does not match the current management identifier key maintained by the management device server, then the management device server shall return a function result of NO MANAGEMENT ACCESS in the response frame.

The NEW MANAGEMENT IDENTIFIER KEY field contains the new value for the management identifier key maintained by the management device server. A NEW MANAGEMENT IDENTIFIER KEY field set to zero specifies that the management identifier key is disabled.

The CRC field is defined in 10.4.3.1.

Table 12 defines the response format.

Table 12 — CONFIGURE MANAGEMENT IDENTIFIER KEY response

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (41h)							
1	FUNCTION (83h)							
2	FUNCTION RESULT							
3	RESPONSE LENGTH (00h)							
4	(MSB)			CRC				
7								(LSB)

The SMP FRAME TYPE field shall be set to 41h.

The FUNCTION field shall be set to 83h.

The FUNCTION RESULT field is defined in 10.4.3.2.

The RESPONSE LENGTH field shall be set to 00h.

The CRC field is defined in 10.4.3.2.

[end of all-new section]