To: T10 Technical Committee
From: Rob Elliott, HP (elliott@hp.com)
Date: 24 June 2006
Subject: 06-208r2 SAS-2 Restrict access to SMP write functions

Revision history
Revision 0 (24 April 2006) First revision
Revision 1 (5 June 2006) Incorporated comments from 2 June 2006 SAS-2 zoning teleconference.
Revision 2 (24 June 2006) Incorporated comments from 20 June 2006 SAS-2 zoning WG.

Related documents
sas2r03a - Serial Attached SCSI - 2 (SAS-2) revision 3a

Overview
In a zoning expander device, SMP output (write) functions should not be allowed from arbitrary SMP initiator ports. For example, an SMP initiator port in one zone group should not be able to disable or reset a phy in another zone group using the PHY CONTROL function.

Table 1 — SMP output (write) function handling

Function	Proposal
CONFIGURE GENERAL	Only allow access by SMP initiator ports whose zone groups have access to zone group 2 (i.e., the zoning manager)
ZONED BROADCAST	(already in sas2r03a) Only allow access by SMP initiator ports whose zone groups have access to zone group 3
CONFIGURE ROUTE INFORMATION	Only supported by externally configurable expanders, so irrelevant
PHY CONTROL, PHY TEST FUNCTION, CONFIGURE PHY EVENT INFORMATION	Only allow access by SMP initiator ports whose zone groups have access to: a) zone group 2 (so the zoning manager can make changes, without having to be granted access to each zone group itself); or b) the zone group of the expander phy (so normal SMP initiator ports can make changes if they can see and use that expander phy)

Suggested changes

4.8.3.2 Zone groups ~~types~~

Zone groups function in different ways based on zone group number as shown in table 22.

Table 22 — Zone groups ~~types~~ (part 1 of 2)

Zone group	Configurable zone permission table entries	Description
0	No	Phys in zone group 0 ~~have access to no other phys~~ only have access to other phys in zone group 1.
1	No	Phys in zone group 1 have access to other phys in all zone groups.

Table 22 — Zone groups types (part 2 of 2)

Zone group	Configurable zone permission table entries	Description
2	Yes	Phys in zone group 2 have access to other phys based on the zone permission table. ~~Phys in zone groups with access to zone group 2 are allowed to perform SMP zoning configuration functions.~~ A management device server in a zoning expander device only allows management application clients using phys in zone groups with access to zone group 2 to perform the following SMP functions: a) SMP zoning configuration functions (e.g., CONFIGURE ZONE PERMISSION); and b) SMP expander configuration functions (i.e., CONFIGURE GENERAL). ~~Phys in zone groups without access to zone group 2 are:~~ ~~a) prohibited from performing SMP zoning configuration functions.~~ A management device server in a zoning expander device only allows management application clients to perform certain SMP phy-based control and configuration functions (i.e., PHY CONTROL, PHY TEST FUNCTION, and CONFIGURE PHY EVENT INFORMATION) if the zone group of the management application client's phy has access to zone group 2 or the zone group of the specified phy.
3	Yes	Phys in zone group 3 have access to other phys based on the zone permission table. A management device server in a zoning expander device only allows management application clients using a phy in a ~~Phys in~~ zone groups with access to zone group 3 ~~are allowed~~ to perform certain SMP zoning-related functions (i.e., ZONED BROADCAST). ~~Phys in zone groups without access to zone group 3 are prohibited from performing certain SMP zoning-related functions (i.e., ZONED BROADCAST).~~
4 to 7	Reserved	
8 to 127	Yes	Phys in zone groups 8 through 127 have access to other phys based on the zone permission table.

~~Use of the SMP CONFIGURE PHY ZONE function and SMP CONFIGURE ZONE PERMISSION function shall be restricted based on the zone group 2 permission bits and the source zone group of the SMP initiator port requesting the function (see 4.8.3.5). If the SMP request is CONFIGURE PHY ZONE or CONFIGURE ZONE PERMISSION and:~~

~~a) if the ZP[s, 2] bit is set to one, the management device server shall process the function request; and~~
~~b) if the ZP[s, 2] bit is set to zero, the management device server shall not process the function request and shall return a function result of SMP ZONE VIOLATION in the response frame (see 10.4.3.2).~~

~~Use of the SMP ZONED BROADCAST function shall be restricted based on the zone group 3 permission bits and the source zone group of the SMP initiator port requesting the function (see 4.8.3.5). If the SMP request is ZONED BROADCAST and:~~

~~a) if the ZP[s, 3] bit is set one, the management device server shall process the function request.; and~~
~~b) if the ZP[s, 3] bit is set to zero, the management device server shall not process the function request and shall return a function result of SMP ZONE VIOLATION in the response frame (see 10.4.3.2).~~

Editor's Note 1: The table and the descriptions in 10.4.3.xx already cover those requirements.

10.4.3.2 SMP function response frame format

...

The FUNCTION RESULT field is defined in table 197.

Table 197 — FUNCTION RESULT **field**

Code	Name	SMP function(s)	Description
...	...	...	...
20h	SMP ZONE VIOLATION	CONFIGURE GENERAL, ZONED BROADCAST, PHY CONTROL, PHY TEST FUNCTION, CONFIGURE PHY EVENT INFORMATION	The SMP target port supports the function, but zoning is enabled and the application zone permission table bit is set to zero (e.g., the ZP[s, 3] bit is set to zero and the request was ZONED BROADCAST)(see 4.8.3.2). the SMP initiator port does not have access to a necessary zone group according to the zone permission table (see 4.8.3.2)

10.4.3.10 CONFIGURE GENERAL function

The CONFIGURE GENERAL function requests actions by the device containing the SMP target port. This SMP function may be implemented by any SMP target port. In zoning expander devices, this function shall only be processed from SMP initiator ports that have access to zone group 2 (see 4.8.3.2).

...

10.4.3.11 ZONED BROADCAST function

The ZONED BROADCAST function requests that the specified BROADCAST be transmitted on all the ports that are in one or more specified zone groups, with the exception of the port on which the ZONED BROADCAST function was received (see 4.8.5). This SMP function shall be supported by SMP target ports in zoning expander devices (see 4.8). Other SMP target ports shall not support this SMP function. This SMP function shall only be processed from SMP initiator ports that have access to zone group 3 (see 4.8.3.2).

...

10.4.3.12 CONFIGURE ROUTE INFORMATION

The CONFIGURE ROUTE INFORMATION function sets an expander route entry within the expander route table of a configurable expander device. This SMP function shall be supported by SMP target ports in expander devices if the CONFIGURABLE ROUTE TABLE field is set to one in the REPORT GENERAL response data. Other SMP target ports shall not support this SMP function.

...

10.4.3.13 PHY CONTROL function

The PHY CONTROL function requests actions by the specified phy. This SMP function may be implemented by any SMP target port. In zoning expander devices, this function shall only be processed from SMP initiator ports that have access to zone group 2 or the zone group of the specified phy (see 4.8.3.2).

...

10.4.3.14 PHY TEST FUNCTION function

The PHY TEST FUNCTION function requests actions by the specified phy. This SMP function may be implemented by any SMP target port. In zoning expander devices, this function shall only be processed from SMP initiator ports that have access to zone group 2 or the zone group of the specified phy (see 4.8.3.2).

...

10.4.3.15 CONFIGURE PHY EVENT INFORMATION function

The CONFIGURE PHY EVENT INFORMATION function configures phy event information (see 4.10) about the specified phy. This SMP function may implemented by any SMP target port. In zoning expander devices, this function shall only be processed from SMP initiator ports that have access to zone group 2 or the zone group of the specified phy (see 4.8.3.2).

...