To: T10 Technical Committee
From: Rob Elliott, HP (elliott@hp.com)
Date: 7 May 2007
Subject: 06-373r3 SAS-2 Zone manager password

Revision history
Revision 0 (14 August 2006) First revision
Revision 1 (22 December 2006) Incorporated comments from September 2006 SAS protocol WG.
Revision 2 (5 May 2007) Incorporated comments from April 2007 SAS protocol WG. Changed title from "key"
    to "password" as keys are being added in the cryptographically correct way into SPC-4.
Revision 3 (7 May 2007) Incorporated comments from May 2007 SAS protocol WG.

Related documents
sas2r07 - Serial Attached SCSI - 2 (SAS-2) revision 7

Overview
If zoning is disabled, SAS-2 currently requires a zoning expander device to recognize the administrator's physical presence (the definition of which is vendor-specific) to allow an SMP initiator port to lock the zoning expander device (e.g., to enable zoning). If zoning is enabled, SAS-2 requires either physical presence or that the SMP initiator port have access to zone group 2 to lock (e.g., to disable zoning).

For systems that are remotely managed, an SMP initiator port needs to be able to enable and disable zoning in an expander device without physical presence being asserted. A password-based scheme is proposed. If the SMP ZONE LOCK request contains the correct zone manager password, then the request is processed. If the SMP request contains an incorrect zone manager password (and physical presence is not asserted and the SMP initiator port does not have access to zone group 2), then the request is rejected with a function result of NO MANAGEMENT ACCESS RIGHTS.

The zone manager password is not cryptographically secure; it could be snooped by any expander on the pathway or by a SAS logic analyzer inserted on the pathway. Since it is not designed for one-time use, so a rogue SMP initiator port could replay it later. The intent of the password 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 (e.g., for SAS-3) may define a cryptographically secure mechanism, based on work underway in the Trusted Computing Group, the T10 SSC Working Group for tape data encryption, and the T10 CAP Working Group for general SCSI security.

The zone manager password can be read with an SMP REPORT ZONE MANAGER PASSWORD function by any SMP initiator port if physical presence is asserted, or by the active zone manager in zoning is enabled.

The zone manager password can by changed with an SMP CONFIGURE ZONE MANAGER PASSWORD function by any SMP initiator port if physical presence is asserted or by any SMP initiator port that presents the old password in the request. This lets a system administrator enter the zone manager password while physically present to install the hardware containing the expander. The zone manager 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 zone manager password is proposed as a 32-byte (256-bit) value. The value should be random to withstand random guess attacks. A simple text string is not recommended since it is not random; a SHA-256 hash value of a text string plus a true random number is a better approach (although it is still not secure from replay attacks).

> Editor's Note 1: Access Controls uses 8 bytes (64 bits) for its "management identifier key." 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.

A zoning expander device may or may not remember zoning enabled/disabled, zone configuration details, and the zone manager password through power cycles. The proposed effects of remembering these settings are described in table 1 (SAS-2 does not specify many of these cases today).

Table 1 — Zoning expander device power on behavior

Value after power on			Description (and access to ZONE LOCK other than via physical presence)
Zoning enabled	**Zone configuration saved?**	**Zone manager password**	
0	N/A	0	Expander powers up wide-open (ZPT not used) Any SMP initiator port can lock
		non-zero	Expander powers up wide-open (ZPT not used) Correct zone manager password must be presented to lock
1	no	0	Expander powers up totally closed (ZPT all zeros, all phy ZGs are 0) NEW Any SMP initiator port can lock
	yes	0	Expander powers up with previous zone configuration Any SMP initiator port can lock
		non-zero	Expander powers up with previous zone configuration SMP initiator port must have access to zone group 2 or present the correct zone manager password

Editor's Note 2: Logging of unsuccessful attempts may be added in a followup proposal. Access Controls defines an Invalid Key events counter that records each attempt with a bad password, recording the TransportID of the culprit.

Suggested changes

4.9.1 Zoning overview

...

The zone manager assigns zone groups (see 4.9.3.2) to all phys that are capable of participating in connections through the ZPSDS. Every phy in a SAS domain may be assigned to a zone group. There are 128 zone groups numbered 0 through 127. All phys in a wide port shall be assigned to the same zone group. Zone group numbers are assigned to zoning expander phys as part of the zone phy information (see 4.9.3.1) and assigned to SAS addresses in the zoning expander route table (see 4.9.3.4). The zone groups assigned in one ZPSDS have no relationship to the zone groups assigned in another ZPSDS.

An expander phy inside a ZPSDS shall be assigned to zone group 1. A phy that is attached to the boundary of the ZPSDS (i.e., attached to an expander phy with the INSIDE ZPSDS bit set to zero) belongs to the zone group indicated by the ZONE GROUP field of the expander phy to which it is attached. A phy that is not attached to the boundary of the ZPSDS belongs to a zone group if the ZONE ADDRESS RESOLVED bit is set to one in the boundary expander phy and the zoning expander route table in that expander device contains a zone group value for the phy's SAS address.

Each zoning expander device contains a zone permission table (see 4.9.3.3) that controls whether a connection is allowed between phys based on their zone groups. As defined in 4.9.3.5, a requested connection shall only be established if the zone permission table indicates that access between the zone group of the source port and the zone group of the target port is allowed.

The zoning expander route table (see 4.9.3.4) is an extended version of the expander route table (see 4.6.7.3) that also includes the zone group number of each SAS address.

A zoning expander device may support physical presence detection and/or a zone manager password to allow management access. The zone manager password is 32 bytes long and is specified in Table 2.

Table 2 — Zone manager password

Code	Name	Description
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000h	ZERO	Well-known value that provides access to any zone manager that presents it
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFFh	DISABLED	Well-known value that does not provide access to any zone manager (e.g., zone manager password usage is disabled)
All others	All others	Random value, providing access only to a zone manager that presents the correct value

A zoning expander device ~~may configure the zone permission table, and zone phy information at power on and become part of a ZPSDS without a zone manager configuring the zoning expander device~~ may or may not preserve the following settings during power loss:

 a) zoning enabled;
 b) the zone permission table;
 c) zone phy information; and/or
 d) the zone manager password.

Table 3 describes the reasons that a zoning expander device accepts for honoring an SMP ZONE LOCK function after power on.

Table 3 — Zoning expander device zoning configuration after power on

| Value after power on			Reason(s) that the SMP ZONE LOCK function is accepted		
Zoning enabled	Zone permission table saved	Zone manager password (see table 2 in 4.9.1)	Physical presence asserted	SMP initiator port has access to zone group 2	ZONE MANAGER PASSWORD field in the ZONE LOCK request set to the zone manager password
no	N/A	ZERO		no	yes
		DISABLED			no
		All others			yes
yes	no	ZERO	yes	no	yes
		DISABLED			no
		All others			yes
	yes	ZERO		yes	yes
		DISABLED			no
		All others			yes

4.9.2 Zoning expander device requirements

In addition to the requirements for expander devices described in 4.6, a zoning expander device shall:

  a) contain a zoning expander route table (see 4.9.3.4);
  b) contain active and shadow zone permission tables that supports 128 zone groups (see 4.9.3.3);
  c) contain active and shadow zone phy information for each phy;
  d) if zoning is enabled, allow or deny connection requests based on the active zone permission table (see 4.9.3.5);
  e) set the ZONING SUPPORTED bit to one in its SMP REPORT GENERAL response (see 10.4.3.3);
  f) support the ZONING ENABLED bit in the SMP REPORT GENERAL response;
  g) support the zone lock inactivity timer;
  h) be self-configuring;
  i) contain an SMP initiator port (see 4.6.1); and
  j) support zoning-related SMP functions.

A zoning expander device may include physical presence detection to allow locking (see 4.9.6.2) and enabling or disabling zoning (see 10.4.3.16). The definition of physical presence detection is vendor-specific.
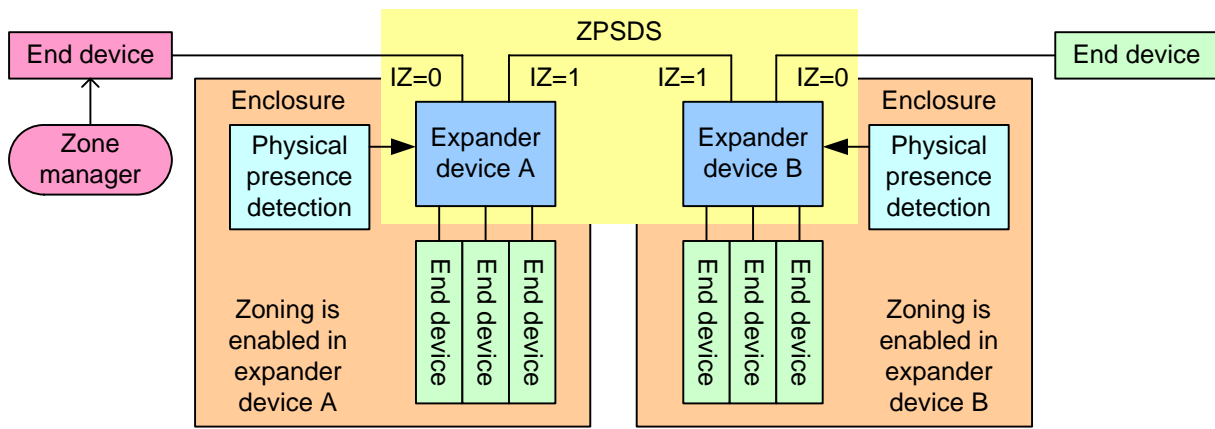
Figure 53 shows an example of two enclosures with physical presence detection where zoning is enabled in the expander device in the left enclosure, but is not enabled in the expander devices in the right enclosure. The zone manager is able to configure zoning in zoning expander device A because the zone group of its

SMP initiator port has access to zone group 2. However, it is not able to enable or configure zoning in expander device B unless physical presence is asserted or it presents the current zone manager password.
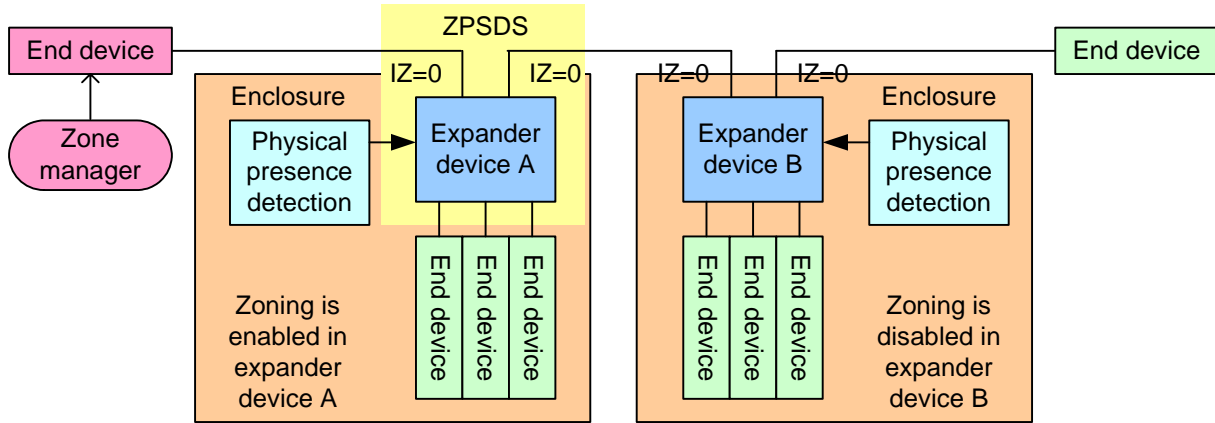
The ZPSDS is extended as shown below after the zone manager on the left:
1) configures zone phy information in each expander device, including setting the INSIDE ZPSDS bit to one in each expander phy that is going to be inside the ZPSDS; and
2) sends a CONFIGURE ZONING request with the ZONING ENABLED bit set to one to expander device B while physical presence is asserted.

IZ = INSIDE ZPSDS bit in the zone phy information

Figure 53 — Physical presence detection extending a ZPSDS example [no change]

Figure 54 shows an example of two enclosures with physical presence detection where zoning is enabled in both the expander devices. The zone manager is able to configure zoning in zoning expander device A because the zone group of its SMP initiator port has access to zone group 2. However, it is not able to

configure zoning in expander device B unless physical presence is asserted <u>or it presents the current zone manager password</u>.

The left ZPSDS is extended as shown below after the zone manager on the left:
1) sends an ENABLE DISABLE ZONING request with the ZONING ENABLED bit set to zero to expander device B while physical presence is asserted;
2) configures zone phy information in each expander device, including setting the INSIDE ZPSDS bit to one in each expander phy that is going to be inside the ZPSDS; and
3) sends an ENABLE DISABLE ZONING request with the ZONING ENABLED bit set to one to expander device B while physical presence is asserted.
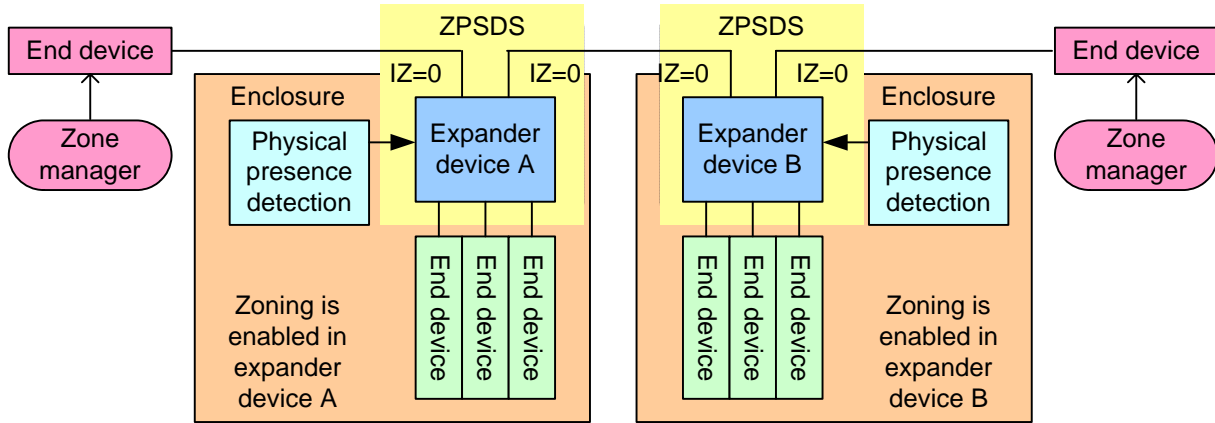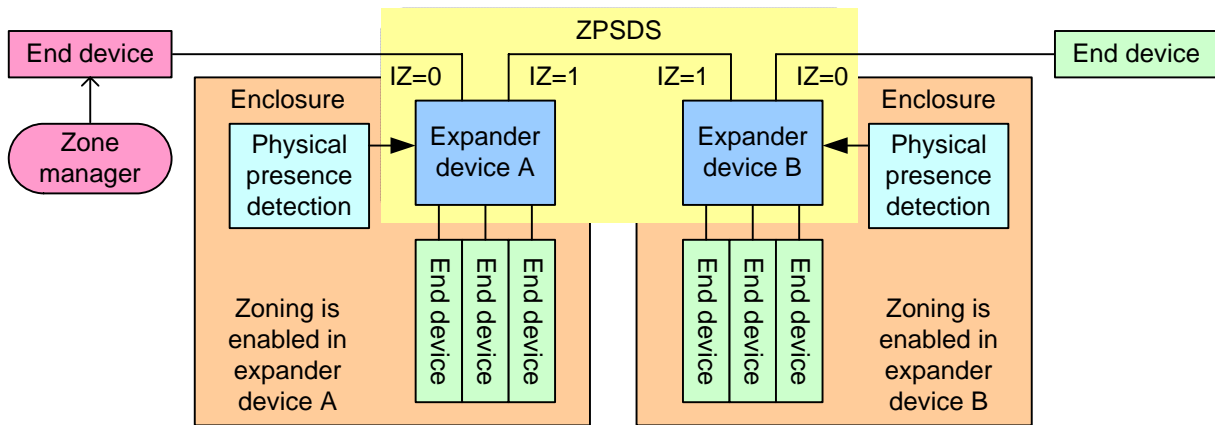
IZ = INSIDE ZPSDS bit in the zone phy information

Figure 54 — Physical presence detection overtaking a ZPSDS example [no change]

4.9.3 Zone operation

4.9.3.1 Zone phy information

Each phy of a zoning expander device shall support the following zone phy information fields:

  a) INSIDE ZPSDS bit;
  b) REQUESTED INSIDE ZPSDS bit;
  c) INSIDE ZPSDS PERSISTENT bit;
  d) ZONE GROUP PERSISTENT bit; and
  e) ZONE GROUP field.

[next paragraph moved here from the last paragraph of the section]

All phys in an expander port shall have the same zone phy information (see 4.9.3.1). ~~The default (e.g., power-on) values for the zone phy information fields are vendor-specific. The zone phy information fields should be~~

6

~~non-volatile and shall be preserved while zoning is disabled.~~ The expander device shall preserve the zone phy information while zoning is disabled and may or may not preserve the zone phy information through power loss (see 4.9.1). If the zoning expander device preserves that zoning is enabled and does not preserve the zone phy information, it shall set the zone phy information as follows:

a) INSIDE ZPSDS bit set to zero;
b) REQUESTED INSIDE ZPSDS bit set to zero;
c) INSIDE ZPSDS PERSISTENT bit set to zero;
d) ZONE GROUP PERSISTENT bit set to zero; and
e) ZONE GROUP field set to 00h.

The INSIDE ZPSDS bit indicates if the phy is inside or on the boundary of a ZPSDS. An INSIDE ZPSDS bit set to zero indicates that the phy is attached to an end device, an expander device that does not support zoning, or a zoning expander device with zoning disabled, or a zoning expander device with zoning enabled that is outside the ZPSDS (i.e., is in another ZPSDS). An INSIDE ZPSDS bit set to one indicates that the phy is attached to a zoning expander device with zoning enabled and is thus inside a ZPSDS. The INSIDE ZPSDS bit only changes following a link reset sequence (see 4.9.4), based on:

a) the REQUESTED INSIDE ZPSDS bit;
b) the REQUESTED INSIDE ZPSDS bit received in the incoming IDENTIFY address frame (see 7.8.2);
c) the INSIDE ZPSDS PERSISTENT bit; and
d) the INSIDE ZPSDS PERSISTENT bit received in the incoming IDENTIFY address frame.

The REQUESTED INSIDE ZPSDS bit is used to establish the boundary of the ZPSDS. The REQUESTED INSIDE ZPSDS bit is transmitted in the IDENTIFY address frame (see 7.8.2) to the attached phy and is used to determine the values of other zone phy information fields after a link reset sequence (see 4.9.4).

> NOTE 1 - The value of the REQUESTED INSIDE ZPSDS bit may be changed by the zoning expander device following a link reset sequence (see 4.9.4).

The INSIDE ZPSDS PERSISTENT bit indicates the method used to determine the value of the INSIDE ZPSDS bit after a link reset sequence (see 4.9.4). The INSIDE ZPSDS PERSISTENT bit is transmitted in the IDENTIFY address frame (see 7.8.2).

The ZONE GROUP field contains a value in the range of 0 to 127 that specifies the zone group to which the phy belongs. The zone group of the SMP initiator port and SMP target port in a zoning expander device shall be 1. 4.9.3.2 defines more about zone groups.

The ZONE GROUP PERSISTENT bit specifies the method of determining the zone group value of the phy after a link reset sequence when the INSIDE ZPSDS bit is set to zero (see 4.9.4).

4.9.3.2 Zone groups

Zone groups function in different ways based on zone group number as shown in table 25.

Table 25 — Zone groups

Zone group	Configurable in zone permission table [a]	Description
0	No	Phys in zone group 0 have access to phys in zone group 1 and do not have access to phys in other zone groups.
1	No	Phys in zone group 1 have access to phys in all zone groups.
2	Yes	Phys in zone group 2 have access to phys in the zone groups indicated by the zone permission table. A management device server in a zoning expander device with zoning enabled only allows management application clients using phys in zone groups with access to zone group 2 to perform the following SMP functions: a) CONFIGURE GENERAL (see 10.4.3.15); b) ~~ENABLE DISABLE ZONING (see 10.4.3.16);~~ and c) ZONE LOCK (see 10.4.3.18) and SMP zone configuration functions (see 4.9.6.3) performed while the zoning expander device is locked. A management device server in a zoning expander device with zoning enabled only allows management application clients to perform certain SMP phy-based control and configuration functions (e.g., 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 phys in the zone groups indicated by the zone permission table. A management device server in a zoning expander device with zoning enabled only allows management application clients using a phy in a zone group with access to zone group 3 to perform certain SMP zoning-related functions (i.e., ZONED BROADCAST (see 10.4.3.17)).
4 to 7	Reserved	
8 to 127	Yes	Phys in zone groups 8 through 127 have access to phys in the zone groups indicated by the zone permission table.
[a] A zone group defined as configurable is able to be changed with the SMP CONFIGURE ZONE PERMISSION TABLE function (see 10.4.3.22).		

4.9.3.3 Zone permission table

The zone permission table specifies access permission between zone groups. If a bit in the zone permission table is set to one then connection requests shall be permitted between phys in the zone groups. If a bit in the zone permission table is set to zero then connection requests between phys in the zone groups shall be rejected with OPEN_REJECT (ZONE VIOLATION) or OPEN_REJECT (RETRY) as described in 4.9.3.5.

The zone permission table structure is shown in table 26.

Table 26 — Zone permission table

Destination zone group (i.e., d)	Source zone group (i.e., s)				
	0	**1**	**2 to 3**	**4 to 7**	**8 to 127**
0	0	1	0	0	0
1	1	1	1	1	1
2 to 3	0	1	ZP[s = 2 to 3, d = 2 to 3] [a]	Reserved [b]	ZP[s = 8 to 127, d = 2 to 3] [a]
4 to 7	0	1	Reserved [b]	Reserved [b]	Reserved [b]
8 to 127	0	1	ZP[s = 2 to 3, d = 8 to 127] [a]	Reserved [b]	ZP[s = 8 to 127, d = 8 to 127] [a]

[a] Shading identifies configurable zone groups.
[b] All reserved ZP bits shall be set to zero (e.g., bits ZP[4 to 7, 4 to 127] are set to zero).

A ZP[s, d] bit set to one specifies that the source zone group (i.e., s) has permission to access the destination zone group (i.e., d). A ZP[s, d] bit set to zero specifies that the source zone group (i.e., s) does not have permission to access the destination zone group (i.e., d).

If ZP[s, d] is set to a value, ZP[d,s] shall be set to the same value.

The zoning expander device shall preserve the zone permission table while zoning is disabled and may or may not preserve the zone permission table through power loss (see 4.9.1). If the zoning expander device preserves that zoning is enabled and does not preserve the zone permission table, it shall set the zone permission table to grant minimal permissions on power on as specified in table 27.

Table 27 — Zone permission table granting minimal permissions

Destination zone group (i.e., d)	Source zone group (i.e., s)				
	0	**1**	**2 to 3**	**4 to 7**	**8 to 127**
0	0	1	0	0	0
1	1	1	1	1	1
2 to 3	0	1	0	Reserved [b]	0
4 to 7	0	1	Reserved [b]	Reserved [b]	Reserved [b]
8 to 127	0	1	0	Reserved [b]	0

[a] Shading identifies configurable zone groups.
[b] All reserved ZP bits shall be set to zero (e.g., bits ZP[4 to 7, 4 to 127] are set to zero).

4.9.6 Zone configuration

4.9.6.1 Zone configuration overview

Zoning expander devices implement a lock to coordinate zoning configuration by zone manager(s).

There are four steps in the zone configuration process:

   1) lock (see 4.9.6.2);
   2) load (see 4.9.6.3);

    3) activate (see 4.9.6.4); and
    4) unlock (see 4.9.6.5).

The management device server in a zoning expander device only accepts SMP zone configuration function requests, SMP ZONE ACTIVATE requests, and SMP ZONE UNLOCK requests when it is locked, and only accepts SMP zone configuration function requests from the zone manager that locked the zoning expander device (i.e., the active zone manager). SMP zone configuration functions change zoning expander shadow values. When changes are complete, the zone manager activates the changes and the zoning expander device sets the zoning expander active values equal to the zoning expander shadow values. The zone manager then unlocks the zoning expander devices.

For a ZPSDS to function correctly, all zoning expander devices are required to have identical values in their zone permission tables. To change zone permission tables, a zone manager device locks all zoning expander devices in a ZPSDS.

To change zone phy information, a zone manager locks only the zoning expander devices containing the phys to be changed.

When a zoning expander device with zoning disabled is being added to a ZPSDS (see figure 53 in 4.9.1) or two or more ZPSDSes are being merged (see figure 54 in 4.9.1), the zone manager locks all of the zoning expander devices that are to be included in the final ZPSDS. The zone manager configures the zone phy information in each zoning expander device (e.g., sets the REQUESTED INSIDE ZPSDS bit to one for phys inside the final ZPSDS) and configures all of the zone permission tables to be identical.

If the zone lock inactivity timer expires then the zoning expander device performs the unlock step. The zoning expander device is unlocked and the zoning expander shadow values are not activated.

4.9.6.2 Lock step

The lock step ensures that the same zone manager locks each zoning expander device. A zone manager sends the SMP ZONE LOCK request (see 10.4.3.18) to lock a zoning expander device. A zoning expander device is locked when the ZONE LOCKED bit is set to one in the SMP REPORT GENERAL response and after the SAS address of the zone management server device has been stored. The management device server in a locked zoning expander device processes SMP zone configuration function requests, SMP ZONE ACTIVATE requests, and SMP ZONE UNLOCK requests.

If more than one zone manager attempts to lock a group of zoning expander devices, the following rules ensure that any concurrent requests are resolved:

    1) If the first SMP ZONE LOCK response received by a zone manager has the FUNCTION RESULT field set to ZONE LOCK VIOLATION (see 10.4.3.2), then the group of zoning expander devices is locked by another zone manager and the zone manager should originate no further requests until it receives a Broadcast (Change);
    2) If at least one SMP ZONE LOCK request is successful and at least one other response has:
       A) the FUNCTION RESULT field set to ZONE LOCK VIOLATION (see 10.4.3.2); and
       B) the CONFIGURING bit set to one (see 4.9.6.3),

    then a zoning expander device is locked and being configured by another zone manager. The zone manager that failed to lock the zoning expander devices should unlock all zoning expander devices that it has locked. When a Broadcast (Change) event is received, then the zone manager should retry the lock step; and

    3) If at least one SMP ZONE LOCK request is successful and at least one other response has:
       A) the FUNCTION RESULT field set to ZONE LOCK VIOLATION (see 10.4.3.2); and
       B) the CONFIGURING bit set to zero,

    then another zone manager has locked at least one zoning expander device in the group of zoning expander devices and the zone manager shall evaluate the ACTIVE ZONE MANAGER SAS ADDRESS field in the SMP ZONE LOCK response:

       A) if the returned SAS address has a lower numeric value than the SMP port SAS address of the zone manager, then the zone manager with the higher numeric value SAS address shall repeat

the SMP ZONE LOCK request to all zoning expander devices that it has not already locked until all required zoning expander devices are locked, or until a Broadcast (Change) is received; or

B) if the returned ACTIVE ZONE MANAGER SAS ADDRESS field has a higher numeric value than the SMP port SAS address of the zone manager, then the zone manager with the lower numeric value SAS address shall originate an SMP ZONE UNLOCK request to unlock all zoning expander devices that it locked.

The lock step is complete after a zone manager receives a successful SMP ZONE LOCK response from all required zoning expander devices.

4.9.6.3 Load step

The load step stores SMP zone configuration information as zoning expander shadow values. A zoning expander device only processes SMP zone configuration function requests originated by the active zone manager when it is locked.

The SMP zone configuration functions are:

a) SMP CONFIGURE ZONE PHY INFORMATION (see 10.4.3.21);
b) SMP CONFIGURE ZONE PERMISSION TABLE (see 10.4.3.22); and
c) SMP ENABLE DISABLE ZONING (see 10.4.3.16).

After a locked zoning expander device processes any SMP zone configuration function request, it sets the CONFIGURING bit to one in the SMP REPORT GENERAL response (see 10.4.3.3).

SMP zone configuration functions change the zoning expander shadow values and do not affect the zoning expander active values. The zoning expander shadow values become zoning expander active values during the activate step (see 4.9.6.4).

If the active zone manager receives a response to an SMP zone configuration function with the FUNCTION RESULT field set to ZONE LOCK VIOLATION (see 10.4.3.2), then it should unlock all locked zoning expander devices.

The load step may be skipped when a locked zoning expander device is unlocked:

a) by a zone manager with a higher SAS address during the lock step (see 4.9.6.2); or
b) because the zone lock inactivity timer expires.

4.9.6.4 Activate step

The activate step copies the zoning expander shadow register values to the zoning expander active values. The active zone manager issues one of the following:

a) a Broadcast (Zone Activate) (see 4.1.13); or
b) an SMP ZONE ACTIVATE request (see 10.4.3.19) to all locked zoning expander devices.

After a locked zoning expander device receives a Broadcast (Zone Activate) or processes an SMP ZONE ACTIVATE request, then the zoning expander device sets the zoning expander active values equal to the zoning expander shadow values.

If the active zone manager receives an SMP ZONE ACTIVATE response with the FUNCTION RESULT field set to ZONE LOCK VIOLATION (see 10.4.3.2), then it should unlock all locked zoning expander devices.

The activate step may be skipped when a locked zoning expander device is unlocked:

a) by a zone manager with a higher SAS address during the lock step (see 4.9.6.2); or
b) because the zone lock inactivity timer expires.

4.9.6.5 Unlock step

The unlock step ensures that the active zone manager unlocks the locked zoning expander devices, or if the zone manager fails then the zone lock inactivity timer expires and the zoning expander devices unlock.

If the active zone manager originated Broadcast (Zone Activate), then it sends an SMP ZONE UNLOCK request (see 10.4.3.20) with the ACTIVATE REQUIRED bit set to one to each of the locked zoning expander

devices. This ensures that each zoning expander device has performed the activate step before it performs the unlock step. If it receives an SMP ZONE UNLOCK response with the FUNCTION RESULT field set to NOT ACTIVATED (see 10.4.3.2), then the zone manager retries the SMP ZONE UNLOCK request a vendor-specific number of times, then originates an SMP ZONE ACTIVATE request to each locked zoning expander device.

If the active zone manager originated SMP ZONE ACTIVATE request(s), then after all the SMP ZONE ACTIVATE functions have successfully completed it sends an SMP ZONE UNLOCK request with the ACTIVATE REQUIRED bit set to zero to each of the locked zoning expander devices. If it receives an SMP ZONE UNLOCK response with the FUNCTION RESULT field set to BUSY (see 10.4.3.2), then the zone manager retries the SMP ZONE UNLOCK request.

When the SMP ZONE UNLOCK request is successful or the zone lock inactivity timer expires, then the zoning expander device is unlocked and shall:

a) set the ZONE LOCKED bit to zero in the SMP REPORT GENERAL response (see 10.4.3.3);
b) set the CONFIGURING bit to zero in the SMP REPORT GENERAL response;
c) if the zone lock timer expired, originate a Broadcast (Change) from zone group 1; and
d) if the zone lock timer processed an SMP ZONE UNLOCK request, originate a Broadcast (Change) from each zone group whose zone permission table entries or zone phy information has changed or from zone group 1.

When all SMP ZONE UNLOCK requests are successful the configuration process is complete.

4.9.6.6 Zone lock inactivity timer

The zone lock inactivity timer is supported by all zoning expander devices. The use of a timer ensures that if the zone manager disappears without performing the unlock step that all locked zoning expander devices are unlocked.

When a zoning expander device processes an SMP ZONE LOCK request (see 10.4.3.18) then the zone lock inactivity timer default value is set to the value of the ZONE LOCK INACTIVITY TIME LIMIT field.

The zone lock inactivity timer is initialized and started if the default value is non-zero and:

a) the zoning expander device completes processing of any SMP zone configuration function request or SMP ZONE ACTIVATE request while the ZONE LOCKED bit is set to one in the SMP REPORT GENERAL response (see 10.4.3.3); or
b) the zoning expander device completes processing of a successful SMP ZONE LOCK request.

The zone lock inactivity timer is stopped if:

a) the ZONE LOCK INACTIVITY TIME LIMIT field is set to zero in an SMP ZONE LOCK request; or
b) the ZONE LOCKED bit is set to zero in the SMP REPORT GENERAL response (e.g., an SMP ZONE UNLOCK request (see 10.4.3.20) is processed, or the zone lock inactivity timer expires).

If the zone lock inactivity timer expires then the zoning expander device:

a) sets the ZONE LOCKED bit to zero in the SMP REPORT GENERAL response;
b) sets the CONFIGURING bit to zero in the SMP REPORT GENERAL response; and
c) sends Broadcast (Change) on all ports.

If the zone lock inactivity timer expires while the zoning expander device is processing an SMP configuration function then the zoning expander device may complete the request successfully or returns a function result of ZONE LOCK VIOLATION.

4.9.6.7 Enable a zoning expander device

If a zoning expander device has the ZONING SUPPORTED bit set to one and the ZONING ENABLED bit set to zero in the REPORT GENERAL response (see 10.4.3.3), then a zone manager configures the zoning expander device using the zone configuration process. This ensures that the zone permission table is the same in all zoning expander devices inside the ZPSDS.

Changes made by the SMP ENABLE DISABLE ZONING function sent by the active zone manager become active during the activate step (see 4.9.6.4).

10.4.3.1 SMP function request frame format

...

The FUNCTION field specifies which SMP function is being requested and is defined in table 212. 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 214.

Table 212 — SMP functions (FUNCTION **field)**

Code	SMP function	Description	Reference
...	...		
05h	REPORT ZONE MANAGER PASSWORD	Report the zone manager password	10.4.3.xx
05h06h - 0Fh	Reserved for general SMP input functions		
...	...		
83h	CONFIGURE ZONE MANAGER PASSWORD	Configure the zone manager password	10.4.3.xy
83h - 84h	Reserved for general SMP output functions		

10.4.3.2 SMP function response frame format

...

Editor's Note 3: must be locked to run ENABLE DISABLE ZONING per 4.9.6.3. so item a) in 21h is inconsistent

The FUNCTION RESULT field is defined in table 214.

Table 214 — FUNCTION RESULT **field** (part 1 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	NO MANAGEMENT ACCESS RIGHTS	~~ENABLE DISABLE ZONING,~~ ZONE LOCK	~~Either~~Any of the following are true: ~~a) the ZONE ENABLE bit is set to zero and a zoning expander device processes an ENABLE DISABLE ZONING request when the PHYSICAL PRESENCE bit is zero; or~~ b) ~~the ZONE ENABLE bit is set to one~~zoning is enabled, ~~and a zoning expander device processes a ZONE LOCK request when~~ the ZONE LOCK bit is set to zero, the PHYSICAL PRESENCE bit is set to zero, the ZONE MANAGER PASSWORD field is not set to the current zone manager password, and the zone manager does not have access to zone group 2~~;~~ c) zoning is enabled, the ZONE LOCK bit is set to one, and the request did not originate from the active zone manager; or d) zoning is disabled, the PHYSICAL PRESENCE bit is set to zero, the ZONE MANAGER PASSWORD field is not set to the current zone manager password. The ADDITIONAL RESPONSE BYTES field may be present but shall be ignored.
22h	UNKNOWN ENABLE DISABLE ZONING VALUE	ENABLE DISABLE ZONING	The ENABLE DISABLE ZONING field is set to 11b (i.e., Reserved). The ADDITIONAL RESPONSE BYTES field may be present but shall be ignored.
23h	ZONE LOCK VIOLATION	ENABLE DISABLE ZONING, ZONE LOCK, ZONE ACTIVATE, ZONE UNLOCK, CONFIGURE ZONE PHY INFORMATION, CONFIGURE ZONE PERMISSION TABLE	~~The ZONE ENABLE bit is set to one~~Zoning is enabled and: a) an unlocked zoning expander device receives an SMP zone configuration function request, a ZONE ACTIVATE request, or a ZONE UNLOCK request from an SMP initiator port that is not the active zone manager; or b) a locked zoning expander device receives an SMP ZONE LOCK request, an SMP zone configuration function request, a ZONE ACTIVATE request, or a ZONE UNLOCK request from an SMP initiator port that is not the active zone manager.

Table 214 — FUNCTION RESULT **field** (part 2 of 2)

Code	Name	SMP function(s)	Description
24h	NOT ACTIVATED	ZONE UNLOCK	The ACTIVATE REQUIRED bit in the request is set to one but the locked zoning expander device has not processed the activate step.
25h	UNKNOWN ZONE PHY INFORMATION VALUE	CONFIGURE ZONE PHY INFORMATION	A specified zone phy information value is not supported. The ADDITIONAL RESPONSE BYTES field may be present but shall be ignored.
26h	NO PHYSICAL PRESENCE	CONFIGURE ZONE MANAGER PASSWORD	The NEW ZONE MANAGER PASSWORD field is set to DISABLED (see table 2 in 4.9.1), but physical presence is not asserted.
...	...		

Editor's Note 4: Need to decide on wording: "zoning is enabled" vs. "the ZONING ENABLED bit is set to one in the REPORT GENERAL response" throughout. Same for locked, physical presence, etc.

...

Table 215 defines the priority of the SMP function results defined in table 214.

Table 215 — Function result priority (part 1 of 2)

SMP function	SMP function result priority
...	...
ENABLE DISABLE ZONING (see 10.4.3.15)	1) INVALID REQUEST FRAME LENGTH; 2) ZONE LOCK VIOLATION; 3) UNKNOWN ENABLE DISABLE ZONING VALUE; 4) NO MANAGEMENT ACCESS RIGHTS; 5) INVALID EXPANDER CHANGE COUNT; 6) SMP FUNCTION FAILED; and 7) SMP FUNCTION ACCEPTED
ZONED BROADCAST (see 10.4.3.17)	1) INVALID REQUEST FRAME LENGTH; 2) SMP ZONE VIOLATION; 3) SMP FUNCTION FAILED; and 4) SMP FUNCTION ACCEPTED
ZONE LOCK (see 10.4.3.18)	1) INVALID REQUEST FRAME LENGTH; 2) ZONE LOCK VIOLATION; 3) NO MANAGEMENT ACCESS RIGHTS; 4) INVALID EXPANDER CHANGE COUNT; 5) SMP FUNCTION FAILED; and 6) SMP FUNCTION ACCEPTED
ZONE ACTIVATE (see 10.4.3.19)	1) INVALID REQUEST FRAME LENGTH; 2) ZONE LOCK VIOLATION; 3) INVALID EXPANDER CHANGE COUNT; 4) SMP FUNCTION FAILED; and 5) SMP FUNCTION ACCEPTED

Table 215 — Function result priority (part 2 of 2)

SMP function	SMP function result priority
ZONE UNLOCK (see 10.4.3.20)	1) INVALID REQUEST FRAME LENGTH; 2) ZONE LOCK VIOLATION; 3) NOT ACTIVATED; 4) BUSY; 5) SMP FUNCTION FAILED; and 6) SMP FUNCTION ACCEPTED
CONFIGURE ZONE PHY INFORMATION (see 10.4.3.21)	1) INVALID REQUEST FRAME LENGTH; 2) PHY DOES NOT EXIST; 3) ZONE LOCK VIOLATION; 4) UNKNOWN ZONE PHY INFORMATION VALUE; 5) INVALID EXPANDER CHANGE COUNT; 6) SMP FUNCTION FAILED; and 7) SMP FUNCTION ACCEPTED
CONFIGURE ZONE PERMISSION (see 10.4.3.22)	1) INVALID REQUEST FRAME LENGTH; 2) ZONE LOCK VIOLATION; 3) INVALID EXPANDER CHANGE COUNT; 4) SMP FUNCTION FAILED; and 5) SMP FUNCTION ACCEPTED
...	...

...

10.4.3.15 ENABLE DISABLE ZONING function

The ENABLE DISABLE ZONING function enables or disables zoning. 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 the zoning expander device is locked.~~ and:

> a) ~~the request is received from an SMP initiator port that has access to zone group 2 (see 4.9.3.2); or~~
> b) ~~the request is received from any SMP initiator port while physical presence is asserted.~~

This function is an SMP zone configuration function (see 4.9.6.3).

> Editor's Note 5: All the checking is done in ZONE LOCK. Once locked, the active zone manager can do whatever it wants.

Table 260 defines the request format.

Table 260 — 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)							
4	(MSB)			EXPECTED EXPANDER CHANGE COUNT				
5								(LSB)
6				Reserved				
7								
8	Reserved						ENABLE DISABLE ZONING	
9				Reserved				
11								
12	(MSB)			CRC				
15								(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.

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 261.

Table 261 — ENABLE DISABLE ZONING field

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

The CRC field is defined in 10.4.3.1.

Table 262 defines the response format.

Table 262 — 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)							
7				CRC				(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.

10.4.3.18 ZONE LOCK function

The ZONE LOCK function locks a zoning expander device to provide exclusive access to SMP zone configuration functions (see 4.9.6.3) for one zone manager. All zoning expander devices shall support this function.

If:

a) the ZONING ENABLED bit is set to one~~and~~, the ZONE LOCKED bit is set to zero in the REPORT GENERAL response (see 10.4.3.3), and the SMP initiator port has access to zone group 2;
b) the ZONING ENABLED bit is set to one, the ZONE LOCKED bit is set to zero in the REPORT GENERAL response (see 10.4.3.3), and the PHYSICAL PRESENCE ASSERTED bit is set to one in the REPORT GENERAL response; or
c) the ZONING ENABLED bit is set to one, the ZONE LOCKED bit is set to zero in the REPORT GENERAL response (see 10.4.3.3), and the request contains the correct zone manager password; or
d) the ZONING ENABLED bit is set to one ~~and~~, the ZONE LOCKED bit is set to one in the REPORT GENERAL response, and the request originated from the active zone manager;
e) the ZONING ENABLED bit is set to zero and the PHYSICAL PRESENCE ASSERTED bit is set to one in the REPORT GENERAL response; or
f) the ZONING ENABLED bit is set to zero and the request contains the correct zone manager password,

then the management device server shall:

a) set the ACTIVE ZONE MANAGER SAS ADDRESS field to the SAS address of the SMP initiator port in the ZONE LOCK response and the REPORT GENERAL response; and
b) set the ZONE LOCKED bit to one in the REPORT GENERAL response.

> Editor's Note 6: In other words: if enabled and unlocked, allow based on ZG 2, physical presence, and password. If enabled and locked, only allow from the active zone manager. If not enabled, allow based on physical presence and password.

When the management device server changes the ZONE LOCKED bit from zero to one, the locked zoning expander device sets the zoning expander shadow values equal to the zoning expander active values.

Table 263 defines the request format.

Table 263 — ZONE LOCK request

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (40h)							
1	FUNCTION (86h)							
2	Reserved							
3	REQUEST LENGTH (~~01h~~0Ah)							
4	(MSB)			EXPECTED EXPANDER CHANGE COUNT				
5								(LSB)
6	(MSB)			ZONE LOCK INACTIVITY TIME LIMIT				
7								(LSB)
8	(MSB)			ZONE MANAGER PASSWORD				
39								(LSB)
~~8~~40	(MSB)			CRC				
~~11~~43								(LSB)

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

The FUNCTION field shall be set to 86h.

The REQUEST LENGTH field shall be set to ~~01h~~0Ah.

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

An ACTIVATE REQUIRED bit set to one specifies that the zoning expander device shall be unlocked only if the activate step has been completed. An ACTIVATE REQUIRED bit set to zero specifies that the zoning expander device shall be unlocked.

The ZONE LOCK INACTIVITY TIME LIMIT field specifies the minimum time that the locked expander device shall allow between any SMP zone configuration function requests or SMP ZONE LOCK requests from the active zone manager (i.e., the maximum time that a zone manager may allow to pass without accessing the locked expander device) and is reported in the SMP REPORT GENERAL response(see 10.4.3.18). This field specifies the number of 100 ms increments that a locked zoning expander device shall remain locked without processing any SMP zone configuration function or SMP ZONE LOCK function (e.g., a value of one in this field means that the time is less than or equal to 100 ms and a value of two in this field means that the time is less than or equal to 200 ms). A value of zero in this field specifies that there is no zone lock inactivity time limit (i.e., the zone lock inactivity timer is disabled).

The ZONE MANAGER PASSWORD field contains a password used to allow permission to lock without physical presence being asserted.

The CRC field is defined in 10.4.3.1.

Table 264 defines the response format.

Table 264 — ZONE LOCK response

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (41h)							
1	FUNCTION (86h)							
2	FUNCTION RESULT							
3	RESPONSE LENGTH (03h)							
4	Reserved							
7								
8	ACTIVE ZONE MANAGER SAS ADDRESS							
15								
16	(MSB)							
19	CRC							(LSB)

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

The FUNCTION field shall be set to 86h.

The FUNCTION RESULT field is defined in 10.4.3.2.

The RESPONSE LENGTH field shall be set to 03h.

The ACTIVE ZONE MANAGER SAS ADDRESS field is defined in the REPORT GENERAL response (see 10.4.3.3).

The CRC field is defined in 10.4.3.2.

10.4.3.3 REPORT ZONE MANAGER PASSWORD function [all new, changes not highlighted]

The REPORT ZONE MANAGER PASSWORD function returns the zone manager password. This SMP function shall be implemented by all management device servers in zoning expander devices. This 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); or
   b) the request is received from any SMP initiator port while physical presence is asserted.

Editor's Note 7: This function does not care about the locked state.

Table 216 defines the request format.

Table 265 — REPORT ZONE MANAGER PASSWORD request

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (40h)							
1	FUNCTION (05h)							
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 05h.

The REQUEST LENGTH field shall be set to 00h.

The CRC field is defined in 10.4.3.1.

Table 217 defines the response format.

Table 266 — REPORT ZONE MANAGER PASSWORD 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 (0Ah)							
4	(MSB)				EXPANDER CHANGE COUNT			
5								(LSB)
6					Reserved			
7								
8	(MSB)				ZONE MANAGER PASSWORD			
39								(LSB)
40	(MSB)				CRC			
43								(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 0Ah.

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.

10.4.3.15 CONFIGURE ZONE MANAGER PASSWORD function [all new, changes not highlighted]

The CONFIGURE ZONE MANAGER PASSWORD 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 any SMP initiator port and specifies the correct zone manager password; or
b) the request is received from any SMP initiator port while physical presence is asserted.

Table 267 defines the request format.

Table 267 — CONFIGURE ZONE MANAGER PASSWORD request

Byte\Bit	7	6	5	4	3	2	1	0
0	SMP FRAME TYPE (40h)							
1	FUNCTION (83h)							
2	Reserved							
3	REQUEST LENGTH (28h)							
4	(MSB)							
5	\multicolumn{8}{c}{EXPECTED EXPANDER CHANGE COUNT}						(LSB)
6								
7	Reserved							
8	(MSB)							
39	\multicolumn{8}{c}{ZONE MANAGER PASSWORD}						(LSB)
40	(MSB)							
71	\multicolumn{8}{c}{NEW ZONE MANAGER PASSWORD}						(LSB)
72	(MSB)							
75	CRC							(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 28h.

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 ZONE MANAGER PASSWORD field does not match the current zone manager password 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 ZONE MANAGER PASSWORD field contains the new value for the zone manager password maintained by the management device server. A NEW ZONE MANAGER PASSWORD field set to zero specifies that the zone manager password is disabled and all zone managers have access. A NEW ZONE MANAGER PASSWORD field set to DISABLED (see table 2 in 4.9.1) specifies that the zone manager password is disabled and shall only be allowed if physical presence is asserted.

Editor's Note 8: This prevents a zone manager with access only by the password method from disable its own access forever by setting the password to DISABLED. Disabling the password method is only allowed if physical presence is proven. This function does not care about the locked state.

The CRC field is defined in 10.4.3.1.

Table 268 defines the response format.

Table 268 — CONFIGURE ZONE MANAGER PASSWORD 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)							
7			CRC					(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]