To: T10 Technical Committee
From: Robert Griswold, Crossroads Systems, Inc. (rgriswold@crossroads.com)
Date: March 6, 2002
Subject: MSC Management commands proposal

Revision History

Revision 0 (January 16, 2002) first revision

Revision 1 (February 25, 2002) second revision: The proposal remains focused on transporting management structures and data in-band over SCSI CDBs, but attempts to follow more established in-band methods, taking into account the nature of management data flow. The initial command structure has been removed from this proposal.

Following discussions regarding security, it is believed that this proposal does not expose security risks, as these commands are CDB in nature, and are executed on layers that are transparent to security. All security contexts will be established before these commands are executed.

Review of the FC and IB SNMP transport models are needed for further development of this command structure.

Overview

The initial thinking of those who have provided input into the MSC project centers around building the commands that could be used to transport management data to and from devices that include management server entities. It is expected that these commands will support SNMP structures and data, but would not be limited to that method of management data presentation.

Following the January 2002 CAP meeting, it became clear that the work that needs to happen to make this initial proposal into the MSC document actually be acceptable to all members of the T10, would require actual working group meetings. This is due to the fact that any one members understanding of management and SCSI encapsulation of that data, being too limited to give a broad enough coverage would not carry at CAP meetings without WG input.

The following are areas that need attention from the MSC WG, either as challenges to current assumptions, or development of concepts:

- SPC-3 will need changes to define the MSC command model.
- SNMP and XML (CIM) Encapsulation should be available with the MSC Management data commands, allowing both to self-describe in the encapsulation.
- Security for SNMP (Version 1 or 2) and XML (CIM) data must be guaranteed above the CDB transport layer, as this encapsulation cannot exist in an insecure environment.
    - SNMP (Version 3) has some concepts of built-in security; these and other security concepts for CIM-based managment will be handled in ULPs that exist above the SCSI CDB layer.
- Any encapsulation effort should focus on the most popular methods of management protocols, versus standardizing on versions of SNMP, XML (CIM) or others that are too far out in their development, or are under-accepted. Though

the development of these commands should not naturally omit the inclusion of newer developing management standards.

- CDB Definitions for MSC Management Data commands should employ the concept of Service Actions, limiting any needs for opcode assignment, while allowing multiple service actions to be defined.
- If it is assumed that most device servers understand some sort of management definition for their class of devices, the encapsulation should be easy enough to encourage the use of this method, as in-band reporting of such data.
- Both management data structures and the data itself should be able to be encapsulated, allowing non-aware applications clients to gain knowledge of a device servers structures.
    - Device Servers will not be allowed to send management structures, without being requested by the application client. Application clients that can read, parse, and compile SNMP MIB structures (MIB definition text files) should be allowed to retrieve that structure, assuming it resides in the device server.
    - Device Servers will alert the application client about whether or not it holds a current structure file, and if so, what versions (if multiples exist), and how to get the correct version.
- Both bi-directional and request – response versions of the commands need to be built. For SCSI transports and protocols where bidi is well understood and easily implemented, this is a feature that must be enabled.
    - This may require use of a SCSI tag (or some other marker) to be sure that responses are attributed to the correct request.
    - In-order delivery of management commands could be guaranteed by use of an only-one-transfer allowed at a time method.
- Build MSC Management command traps (SNMP / XML (CIM)) to be AER capable. Since IB SRP and iSCSI all understand AER, and FCP AER can be adopted, it makes sense to allow traps to be implemented in this fashion.
- Build the MSC Management commands to focus on functional reliability, versus speed. Since it may be more important to know the request and response executed correctly, versus that the command got to the receiver quickly, the building of commands to handle failure conditions, even if they take exceptionally long, is paramount.