To: T10 Technical Committee
From: Rob Elliott, HP (elliott@hp.com)
Date: 16 July 2008
Subject: 08-261r1 SPC-4 Parsing variable-length parameter lists and data

Revision history
Revision 0 (23 June 2008) First revision
Revision 1 (16 July 2008) Incorporated comments from July CAP WG

Related documents
spc4r15 - SCSI Primary Commands - 4 (SPC-4) revision 15

Overview
SCSI software has a poor history of being confused by page length changes. For example, the Caching mode page length changed from 0Ah (10) in SCSI-2 (1993) to 12h (18) in SCSI-3 SBC-1 (before 1996), yet software in 2007-2008 still gets confused. This requires device servers to implement myriads of “compatibility modes” for old software, implementing both old and new format definitions.

This problem affects all structured data in SCSI command sets - diagnostic pages, mode pages, log pages, VPD pages, PERSISTENT RESERVE OUT parameter lists, etc.

SCSI page structures are designed to avoid such confusion, however, and almost always including PAGE LENGTH fields, DESCRIPTOR LENGTH fields, etc. to allow old software to parse new data. However, poorly written software often results in lots of Reserved bytes being included in the page definitions, or new pages being defined rather than expanding old pages.

Some general rules should be included in SPC-4 stating that:

a) a device server shall report an error if it receives unexpected data. Reason: the application client is asking for some functionality that the device server is not going to support. If it ignores the unexpected data, there is no way for the application client to tell. If it rejects it, the application can reformat the data and send it again.
b) an application client should ignore unexpected data. Reason: application client reporting of errors is generally outside the scope of SCSI standards.

This applies to both:

a) the overall length of the parameter list/parameter data (e.g., the VPD page length); and
b) the length of individual parts of that data like descriptors in a descriptor list.

This only applies to structured data defined in command standards; transport protocols might have different rules for their structures (e.g., frame formats).

Suggested changes

5.5 Parsing variable-length parameter lists and parameter data [all new section]

Parameter lists and parameter data (e.g., diagnostic pages, mode pages, log pages, and VPD pages) often include length fields indicating the size of the parameter list or parameter data (e.g., the MODE DATA LENGTH field in the mode parameter header (see 7.4.3)). Parameter lists and parameter data often include descriptor lists and descriptor length fields containing the length of the descriptors in the descriptor lists (e.g., the DESIGNATOR LENGTH field in the designation descriptor used in the Device Identification VPD page (see 7.7.3.1)).

An application client or device server shall not assume that any length field contains the value defined in a SCSI standard.

If a device server receives a parameter list containing a length field (e.g., a PAGE LENGTH field) and containing more bytes than are defined in the standard to which it was designed (e.g., the device server complies with a version of a SCSI standard defining that a parameter list has 24 bytes, but receives a parameter list containing 36 bytes), then it shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

For parameter lists containing a descriptor length field and a descriptor list, if a device server receives more bytes in a descriptor than are defined in the standard to which it was designed (e.g., the device server complies with a version of a SCSI standard defining that a descriptor is 12 bytes, but receives a parameter list containing a 16 byte descriptor), then it shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

An application client should ignore any bytes of parameter data beyond those defined in the standard to which it was designed (e.g., if the application client complies with a version of a SCSI standard defining 24 bytes of parameter data, but receives 36 bytes of parameter data, then it should ignore the last 12 bytes or the parameter data).

For additional response bytes containing a descriptor length field and a descriptor list, an application client should ignore any bytes in each descriptor beyond those defined in the standard to which it was designed (e.g., if the application client complies with a version of a SCSI standard defining that a descriptor has 24 bytes, but receives parameter data containing a descriptor list with a 36 byte descriptor, then it should ignore the last 12 bytes of the descriptor).