LSI LOGIC®

Date: 06 January 2000
To: T10 Technical Committee
From: Ralph Weber, LSI Logic Alternate Member of T10
Subj: Access Controls an alternate approach

After careful deliberations, LSI Logic Storage Systems has decided to present a proposal for access controls based on concepts that until now have been deemed proprietary. This proposal offers several advantages over the access controls proposal found in 99-245:

- Clear differentiation from reservations model and features.
- Provision for different internal logical unit to LUN mapping for each initiator.
  - Each host can see a different internal logical unit as LUN 0.
  - This is very important for heterogeneous host support.
  - SAM-2 changes required to support this idea are included in this proposal (already thought desirable by some T10 members).

To the greatest degree possible, this proposal draws on and incorporates ideas found in 99-245r4.

LSI engineers have tested the concepts proposed here on Windows NT, Solaris, HP-UX, and other operating systems to verify that the desired degree of logical unit access restrictions are enforced. A major difference from 99-245 in this regard is that logical units to which an initiator does not have access do not appear in the parameter data returned by the REPORT LUNS command.

Changes in SAM-2

The specific SAM-2 changes are yet to be written. Generally, the changes need to allow different logical units to be presented to different initiators and the same logical unit to be addressed by different initiators using a different LUN value.

The description of these changes will be written in a way that permits them to apply equally to SMU devices, with the result that SMU devices can present different configurations of logical units on each port.

Changes in SPC-2

Change 1) Add the following entries in the Glossary

Access Controls: An optional feature that restricts initiator access to specific logical units and the information about logical units sent to initiators in the parameter data of INQUIRY and REPORT LUNS commands. (See 5.x.)

Access Control List: The data used by a target to provide access controls for initiators.

Internal Logical Unit Number: Used in conjunction with the Access Controls feature (see 3.1.xx) to identify logical units before they are mapped to logical unit numbers. (See 5.x.y.)

Change 2) Add the following entries in the Acronyms

ACL	Access Control List (see 3.1.xx)
iLUN	Internal Logical Unit Number (see 3.1.yy)

Change 3) Add the following clauses to the Model for All Device Types clause

5.x Access Controls

Access controls are an optional target feature that initiators may use to allow only specified initiators or groups of initiators to access specified logical units. Access controls also allow initiators to instruct a target to map a logical unit to different logical unit numbers depending on which initiator accesses the device. Access to a logical unit affects whether the logical unit appears in the parameter data returned by a REPORT LUNS command and how the logical unit responds to INQUIRY commands.

The access controls model provides three states for target operation. The states and key features of each state are as follows:

a) Access Controls Disabled
   a) All devices ship from the factory in this state.
   b) Behavior is identical to that found in devices that do not implement the Access Controls feature.
   c) After exiting this state, return to this state is possible only via an ACCESS CONTROL OUT command with the DISABLE ACCESS CONTROLS service action that means the criteria described in 5.x.1.3.

b) Access Controls Enabled - Access Control List Unconfirmed
   a) Device access is extremely limited.
   b) If the device has retained the access control information across the power failure of vendor specific event that caused the transition to this state, return to the Access Controls Enabled - Access Control List Confirmed state may occur without specific initiator intervention.
   c) This state is entered only after a power failure or other vendor specified event.

c) Access Controls Enabled - Access Control List Confirmed
   a) This is the normal operating state when Access Controls are enabled.
   b) Initiator access and logical unit numbering maps affect REPORT LUNS data sent to each initiator.

5.x.1 describes each state in detail and the mechanisms that produce transitions between the states.

5.x.1 Access Control States

5.x.1.1 Summary of Access Control States

Each access control state requires specific responses from the target when INQUIRY, REPORT LUNS, and other commands are received. The responses are designed to inform the initiator of the target's access control state while not revealing inappropriate information about the logical units within the target.

5.x.1.2 Access Controls Disabled state

A target in the Access Controls Disabled state functions exactly like a target that has not implemented the Access Controls feature. All SCSI devices ship from their manufacturer in the Access Controls Disabled state. Successful processing of an ACCESS CONTROL OUT command with the MANAGE ACL service action causes the target to transition from the Access Controls Disabled state to the Access Controls Enabled - Access Control List Confirmed state.

To reduce the possibility of rogue actions disabling access controls, transition from the Access Controls Enabled - Access Control List Confirmed state to the Access Controls Disabled state requires two steps occurring in a specific order:

1) The target must transition from the Access Controls Enabled - Access Control List Confirmed state to the Access Controls Enabled - Access Control List Unconfirmed state as the result of a power failure or vendor specific action; and
2) If the first command received by the device server after entering the Access Controls Enabled - Access Control List Unconfirmed state is an ACCESS CONTROL OUT command with the DISABLE ACCESS CONTROLS service action that meets the criteria described in 5.x.1.3, the transition to the Access Controls disabled state occurs. Otherwise, the device remains in the Access Controls Enabled - Access Control List Unconfirmed state or transitions to the Access Controls Enabled - Access Control List Confirmed state as described in 5.x.1.3.

5.x.1.3 Access Controls Enabled - Access Control List Unconfirmed state

A target in the Access Controls Enabled - Access Control List Unconfirmed state formerly was operating in the Access Controls Enabled - Access Control List Confirmed state but has experienced a power failure or vendor specific event. If the target has preserved the access control information during the event that caused the transition to the Access Controls Enabled - Access Control List Unconfirmed state, return to the Access Controls Enabled - Access Control List Confirmed state occurs when the device server receives a command from any initiator unless the command received is an ACCESS CONTROL OUT command with DISABLE ACCESS CONTROLS service action.

If the target has not preserved the access control information during the event that caused the transition to the Access Controls Enabled - Access Control List Unconfirmed state, it remains in this state until an ACCESS CONTROL OUT command with RESTORE ACCESS CONTROLS service action is received. The ACCESS CONTROL IN command with REPORT ACL service action should be used to determine the validity of the target's access control information. When recovery from the event that caused the transition to the Access Controls Enabled - Access Control List Unconfirmed state requires changes in the target's access control information, the ACCESS CONTROL OUT command with the MANAGE ACL service action should be used to accomplish these changes followed by the ACCESS CONTROL OUT command with RESTORE ACCESS CONTROLS service action to return to the Access Controls Enabled - Access Control List Unconfirmed state.

While in the Access Controls Enabled - Access Control List Unconfirmed state the target rejects all commands except:

INQUIRY with the CmdDt and EVPD bits set to zero
REPORT LUNS
ACCESS CONTROL IN
ACCESS CONTROL OUT with RESTORE ACCESS CONTROLS service action
ACCESS CONTROL OUT with MANAGE ACL service action

All other command shall be terminated with a CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID COMMAND OPERATION CODE.

The parameter data returned in response to an INQUIRY command shall be as described in 7.5.1 with the following exceptions:

a) The peripheral qualifier shall be 011b and the peripheral device type shall be 1Fh for any addressed logical unit; and
b) Any vendor specific fields defined to contain the unit serial number shall be filled with zeros.

Note: The ACLstate field contains 11b, indicating that the device is in the Access Controls Enabled - Access Control List Unconfirmed state.

A successful ACCESS CONTROL OUT command with DISABLE ACCESS CONTROLS service action causes a transition from the Access Controls Enabled - Access Control List Unconfirmed state to the Access Controls Disabled state. To be successful, the ACCESS CONTROL OUT command with DISABLE ACCESS CONTROLS service action shall meet the following requirements:

a) It shall be the first command the device server receives from any initiator after entering the Access Controls Enabled - Access Control List Unconfirmed state. If this requirement is not met, the access control state shall not be changed and the command shall be terminated with a CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN CDB.
b) The parameter data shall contain the unit serial number normally reported in the unit serial number vital product data page (see 8.4.5). If this requirement is not met, the access control state shall not be changed and the command shall be terminated with a CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN PARAMETER LIST.

Note: While a target is in the Access Controls Enabled - Access Control List Unconfirmed state, an initiator wishing to disable access controls must learn the unit serial number by a mechanism other than examining the results of a SCSI command. The unit serial number VPD page cannot be retrieved because setting the EVPD bit to one in the INQUIRY CDB is prohibited in this state. Returning the unit serial number in a vendor specific field in the Standard INQUIRY data also is prohibited.

5.x.1.4 Access Controls Enabled - Access Control List Confirmed state

The Access Controls Enabled - Access Control List Confirmed state is the normal operating state for the access controls feature. While in this state, the target limits access to logical units and assigns logical unit numbers in the manner described in 5.x.3. There should not be a SCSI command capable of causing a device to leave this state and enter the Access Controls Enabled - Access Control List Unconfirmed state. It shall not be possible for a device to leave this state and enter the Access Controls Disabled state.

5.x.1.5 Transitions between access control states

A device leaves its manufacturing site in the Access Controls Disabled state and remains in that state until an ACCESS CONTROL OUT command with MANAGE ACL service action is successfully processed, when it enters the Access Controls Enabled - Access Control List Confirmed state. The device remains in the Access Controls Enabled - Access Control List Confirmed state until a power failure or vendor specific event changes the state to Access Controls Enabled - Access Control List Unconfirmed.

If a device in the Access Controls Enabled - Access Control List Unconfirmed state has retained the access control information, receipt of any command other than an ACCESS CONTROL OUT with DISABLE ACCESS CONTROLS service action causes a transition to the Access Controls Enabled - Access Control List Confirmed state. If a device in the Access Controls Enabled - Access Control List Unconfirmed state has not retained the access control information, an ACCESS CONTROL OUT command with RESTORE ACCESS CONTROLS is required to change the state to Access Controls Enabled - Access Control List Confirmed.

The only time a transition from the Access Controls Enabled - Access Control List Unconfirmed state to the Access Controls Disabled state occurs is when the first command received by the device server after entering the Access Controls Enabled - Access Control List Unconfirmed state is an ACCESS CONTROL OUT command with DISABLE ACCESS CONTROLS service action.

5.x.2 Access Controls Security Features

Preventing abuse of any feature is a constant battle between the protective mechanisms and inventive ways to circumvent them. For this reason, a standard cannot provide the only deterrent to abuse of the features defined in that standard. The standards process is not fast enough to respond to changing methods of circumvention.

This standard lays the ground work for protecting the Access Controls feature from abuse, as described in the clauses below. However, the primary burden for protecting the Access Controls feature lies with the initiators and targets that implement the Access Controls. For example, initiators should restrict usage of the ACCESS CONTROL IN and ACCESS CONTROL OUT commands to applications and application clients exhibiting the privileges of a system administrator. Targets should limit the mechanisms by which the Access Controls Enabled - Access Control List Unconfirmed state can be entered, since this is a required first step in a path that leads to disabling access controls entirely.

5.x.2.1 Maintaining Active Access Controls

Once access controls are established, it shall be impossible to disable access controls without first entering the Access Controls Enabled - Access Control List Unconfirmed state. The mechanisms for entering the Access Controls Enabled - Access Control List Unconfirmed state are severely limited, restricted to power failures and an extremely small list of vendor specific events.

The transition from the Access Controls Enabled - Access Control List Unconfirmed state to the Access Controls Disabled state is accomplished using the ACCESS CONTROL OUT command with the DISABLE ACCESS CONTROLS service action. Rogue use of this command is deterred as follows:

a) The ACCESS CONTROL OUT command with the DISABLE ACCESS CONTROLS service action is required to be the first command a device server receives after entering the Access Controls Enabled - Access Control List Unconfirmed state;
b) The ACCESS CONTROL OUT command with the DISABLE ACCESS CONTROLS service action requires the unit serial number as a parameter; and

c) While in the Access Controls Enabled Access Control List Unconfirmed state, the INQUIRY command does not return the unit serial number because the CmdDt and EVPD bits are restricted to having a value of zero.

5.x.2.2 Preventing Rogue Changes in Access Controls

Three mechanisms are provided to reduce or prevent rogue changes in access control information:

a) Management Identifiers
b) Unit Attention notification for access control changes
c) Limits on the frequency and extent of access control changes

5.x.2.2.1 Management Identifiers

The ACCESS CONTROL OUT and ACCESS CONTROL IN commands include a MANAGEMENT IDENTIFIER field, required to contain a non-zero value. The principal function of the Management Identifier is provision of an audit trail for uses of the ACCESS CONTROL IN and ACCESS CONTROL OUT commands. The ACCESS CONTROL IN command with REPORT MANAGEMENT IDENTIFIERS service action returns recently used Management Identifiers.

When an initiator sends a one in the MMID (Match Management ID) bit of an ACCESS CONTROL OUT or ACCESS CONTROL IN command, the device server shall compare the MANAGEMENT IDENTIFIER field contents from the current command with the MANAGEMENT IDENTIFIER field contents in the next ACCESS CONTROL OUT or ACCESS CONTROL IN command received from any initiator. If the MANAGEMENT IDENTIFIER field contents in the next command do not match those in the current command, the next command shall be rejected. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to ACCESS CONTROL CHANGES BLOCKED (xxh/xxh).

By setting the MMID bit to one, an initiator can turn the management identifier into a password that limits use of the ACCESS CONTROL OUT and ACCESS CONTROL IN commands. However, initiators should be cautious about sending MMID equal to one because if the initiator forgets the password management identifier the only way to restore management capabilities for the access controls in a device is to cause a transition to the Access Controls Disabled state and reprogram the entire access control data. Therefore, it is recommended that the MMID value of one be used only as a temporary response when rogue use of the ACCESS CONTROL OUT command is suspected.

5.x.2.2.2 Unit Attention notification for access control changes

Successful completion of an ACCESS CONTROL OUT command with the MANAGE ACL service action shall generate a unit attention condition with an additional sense code of ACCESS CONTROL INFORMATION CHANGED (2Ah/xxh) for all initiators. Initiators concerned with the security of access control information should monitor this unit attention condition. To increase the probability of detecting rogue use of the ACCESS CONTROL OUT command with the MANAGE ACL service action, initiators may poll for this unit attention condition using the TEST UNIT READY command.

5.x.2.2.3 Limits on the frequency and extent of access control changes

Devices may place limits on the frequency and extent of access control changes. The intent of such limits is increasing the probability that rogue attempts to change the access controls will be detected because more ACCESS CONTROL OUT commands will be required to accomplish sweeping changes. All restrictions on the frequency and extent of access control changes are vendor specific. The information in this standard represents suggestions or examples of how such restrictions may be constructed beneficially.

When vendor specific limits on the frequency or extent of access control changes prevent processing of an ACCESS CONTROL OUT command, the command shall be terminated with a CHECK CONDITION status. The sense shall be set to ILLEGAL REQUEST and the additional sense code shall be set to ACCESS CONTROL CHANGES BLOCKED.

Vendors may chose to be less restrictive on the frequency or extent of access control changes when the parameter data for all ACCESS CONTROL OUT commands contain the same non-zero Management Identifier value. When several initiators and management sources coordinate their management of the access controls in a device, they should also coordinate the Management Identifier. The target may take consistent, repeated use of the same Management Identifier as an indication that access control management is properly authorized. Conversely, the target may take receipt of a previously unused Management Identifier as an indication of a rogue attempt to change the access controls.

The vendors of less complex devices (e.g., devices with only one logical unit) may place more restrictions on the frequency of access control changes. Simpler devices contain fewer objects needing access controls. Thus, it would be reasonable for a vendor to assume a normally lower frequency of access control commands and block repeated use of such commands sooner than would be the case in a more complex device.

Vendor restrictions on the extent of access control changes also are related to the complexity of the device. A device with only one logical unit has only one object on which access controls may be placed. Any change in access controls affects the whole extent of access controls within that device. A device with many logical units may reject as covering too large an extent changes that affect more than half of the logical units. But, such restrictions are not practical in less complex devices.

ACCESS CONTROL OUT commands received while in the Access Controls Enabled - Access Control List Unconfirmed state shall not be subjected to frequency or extent of access control changes tests.

5.x.3 Access Controls operational model

When a device is in the Access Controls Enabled - Access Control List Confirmed state, the access controls feature provides control over whether an initiator or group of initiators can access a logical unit and how that logical unit is addressed (what LUN is used to address the logical unit). For the purposes of this access controls, initiators are identified in one of two ways:

a) TransportID - a protocol-specific value that uniquely identifies one initiator; or
b) AccessID - a value that is independent of the transport protocol and identifies one initiator or a group of initiators.

Details of these two methods for identifying initiators are discussed in 5.x.3.4. Regardless of how an initiator is identified for access control purposes, the initiator either has access to a logical unit or it does not. The behavior of access controls on a logical unit are discussed in 5.x.3.1 and 5.x.3.2. Additionally, the access controls feature allows initiators to define different relationships between logical units and LUN values for different initiators or groups of initiators. The definition and management of LUN values is discussed in 5.x.3.3.

The ACCESS CONTROL OUT command with MANAGE ACL service action is used to establish and manage all logical unit access controls and any initiator defined relationships between logical units and LUN values.

5.x.3.1 Logical unit access control

If an initiator has access to a logical unit, all operations proceed as if access controls are not in effect. If an initiator does not have access to a logical unit, the device server shall behave as follows for that logical unit:

a) In the Standard INQUIRY data (see 7.5.1), the peripheral qualifier shall be 011b and the peripheral device type shall be 1Fh;
b) The LUN for the logical unit shall not appear parameter list returned by the REPORT LUNS command; and
c) In all other respects, the logical unit shall behave as if the device server is not capable of supporting a device at this LUN.

If LUN values are initiator managed, any LUN that has not been assigned to a logical unit shall be treated as if it addresses an inaccessible logical unit.

Logical unit access controls are established by associating one initiator identifier (either TransportID or AccessID) with a list of logical units in the parameter data of an ACCESS CONTROL OUT command with MANAGE ACL service action. The structure of the parameter data allows several associations of initiator identifier to one or more logical units to be processed by one ACCESS CONTROL OUT command with MANAGE ACL service action. The initiator identifiers processed by one ACCESS CONTROL OUT command with MANAGE ACL service action can be a mix of TransportID and AccessID type identifiers.

5.x.3.2 All logical units inaccessible

If an initiator does not have access to any logical units in a target, the device server shall reject all commands except:

INQUIRY with the CMDDT and EVPD bits set to zero
REPORT LUNS with the INTERNAL bit set to zero
ACCESS CONTROL OUT with ACCESS ID ENROLL service action

All other commands shall be terminated with a CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID COMMAND OPERATION CODE.

The parameter data returned for a REPORT LUNS command shall include only LUN 0 and the MORE bit shall be set to one. The application client should recognize that the MORE bit being equal to one indicates that successful processing of an ACCESS CONTROL OUT command with ACCESS ID ENROLL service action will result in a change data returned by the REPORT LUNS command.

5.x.3.3 Managed LUN values

By using the TBD ACL entry page code in the parameter data sent for an ACCESS CONTROL OUT with MANAGE ACL service action, an initiator requests that logical units be given specific LUN values for a specified initiator identifier (either TransportID or AccessID). The TBD ACL entry page contains one initiator identifier followed by a series of paired values assigning one logical unit to a LUN value. Multiple TBD ACL entry pages may be sent by one ACCESS CONTROL OUT with MANAGE ACL service action establishing different logical unit to LUN value mappings for different initiator identifiers. The initiator identifiers processed by one ACCESS CONTROL OUT command with MANAGE ACL service action can be a mix of TransportID and AccessID type identifiers. Also, one ACCESS CONTROL OUT command with MANAGE ACL service action can process a mix of logical unit access and LUN value assignment ACL entries.

When establishing LUN values, the ACCESS CONTROL OUT command with MANAGE ACL service action requires an iLUN (internal logical unit number) to identify the logical unit for each LUN value assignment. This information along with a unique identifier value for each logical unit is obtained using the REPORT LUNS command with the INTERNAL bit set to one in the CDB. The data returned by the REPORT LUNS command with the INTERNAL bit set to one is a list of paired values. Each value pair contains one iLUN and one unique identifier value. When determining LUN value assignments, the application client should use the unique identifier values to recognize which iLUN is properly associated with which LUN.

The target's iLUN to unique identifier assignments may change over time. So, the REPORT LUNS parameter data includes a generation number value, indicating which time bounded iLUN assignments the are found in the other parameter data. The TBD ACL entry page includes this generation number so that the device server can verify that the iLUN values in the page match those currently in use by the target and reject the command if they do not. Targets should minimize changes in the relationship between iLUN values and unique identifiers so that a REPORT LUNS command followed quickly by an ACCESS CONTROL OUT command with MANAGE ACL service action will be processed successfully.

Support for the LUN value management feature of access controls is optional even if all other access controls features are supported. Targets indicate their inability to support the LUN value management feature by rejecting the REPORT LUNS command when the INTERNAL bit set to one or by returning REPORT LUNS parameter data that does not have the INTERNAL bit set to one when the INTERNAL bit is set to one in the CDB.

5.x.3.4 Identifying initiators for access controls

Two methods are provided for identifying initiators when using access controls: TransportID and AccessID.

A TransportID format is specific to the transport protocol used by the service delivery subsystem. Using TransportID format identifiers requires the application client and possibly system management personnel to be familiar with details of the transport protocol. Also, replacement of failed system components and other system events can produce changes in TransportID values, which in turn requires changes in the access control information. However, a TransportID grants access to logical units based on properties known to the transport without requiring an enrollment from the initiator. This makes TransportID access useful in instances where initiator software cannot be modified to enroll for access rights, e.g., operating systems that have not been modified to enroll or boot device drivers that don't have the code space to add the enrollment function.

The AccessID format is common to all transport protocols, thus eliminating all the protocol related difficulties associated with the TransportID format. However, to gain logical unit access, an initiator must send an ACCESS CONTROL OUT command with ACCESS ID ENROLL service action and the AccessID it wishes to enroll, which represents an additional programming requirement on the initiator's application client. Beyond the advantages of lifting the restrictions associated with TransportID values, using AccessID values allow several initiators (an SMU host, or several SMU hosts in a cluster) to be given identical access to a group of logical units or assigned LUN values using a single ACL entry page sent in one ACCESS CONTROL OUT command with MANAGE ACL service action.

Change n) All command definitions are still to be written.

> The command definitions in 99-245 will be the basis for the command definitions proposed here. The 99-245 definitions will be modified as little as possible. The only exceptions considered so far are as follows.

I have a preference to fix the size of the INITIATOR IDENTIFIER field. A fixed length field will be easier for both application clients and device severs to work with and it should be possible to fix the length at the largest currently defined length.

The MANAGE ACL parameter list defines a PAGE CODE field and then defines only one page code value. To me, it makes more sense to have the page code indicate function, e.g. one page code for creating an access control entry and a different page code for removing an access control entry.

The parameter list header does not contain a length for the ACL entry pages. This oversight will prevent future additions of different parameter data following the ACL entry pages. So, a length field will be added to the parameter list header.