

in070246

A PROPOSAL FOR INCITS FAST-TRACK PROCESSING
Distributed Management Task Force (DMTF)
Server Management Command Line Protocol (SM CLP) Specification

1. Source of the Proposed Project

1.1 Title: Server Management Command Line Protocol (SM CLP) Specification

1.2 Date Submitted: 1/12/2007

1.3 Proposer

Distributed Management Task Force (DMTF).

Founded in 1992, the Distributed Management Task Force, Inc. (DMTF) is the industry organization leading the development of management standards and integration technology for enterprise and Internet environments.

DMTF's focus is to develop and unify management standards for enterprise and Internet environments. DMTF enables a more integrated and cost effective approach to management through interoperable management solutions by working with key technology vendors and affiliated standards groups.

DMTF standards provide common management infrastructure components for instrumentation, control and communication in a platform-independent and technology-neutral way. DMTF technologies include the Common Information Model (CIM), communication/control protocols like Web-Based Enterprise Management (WBEM), the Systems Management Architecture for Server Hardware (SMASH) initiative and core management services/utilities. Other DMTF standards include System Management BIOS (SMBIOS) and Alert Standard Format (ASF).

With more than 4,400 active participants from over 150 organizations, the DMTF brings the technology industry's customers and top vendors together in a collaborative, work group approach that involves DMTF members in all aspects of specification development and refinement. Board member companies include Broadcom; Cisco Systems; Dell Computer Corp.; EMC; Fujitsu; HP; Hitachi, Ltd; IBM; Intel; Microsoft; Novell; Sun Microsystems; Symantec; and WBEM Solutions.

The DMTF is led by its board of directors, which establishes direction and strategies for the organization and the standards it delivers; a Technical Committee, which oversees the Work Groups to develop and document the DMTF's standards; a Marketing

Committee, which directs the DMTF's overall industry marketing and communications efforts; and an Interoperability Committee, which supplements the resources of the DMTF so that multi-vendor implementations of DMTF technology can be compatible in the industry. The committees collaborate closely with all DMTF members, particularly active members of the Work Groups.

The DMTF works closely with many Alliance Partners in the development of DMTF standards as a common approach to address the challenge of providing interoperable distributed management. Partners include:

- Blade Systems Alliance (BladeS)
- CompTIA
- Consortium for Service Innovation
- Open Grid Forum (OGF)
- Network Applications Consortium (NAC)
- Object Management Group (OMG)
- Printer Working Group
- The Open Group
- Organization for the Advancement Of Structured Information Standards (OASIS)
- Web Services Distributed Management (WSDM) Technical Committee,
- Service Availability Forum (SA Forum)
- Storage Networking Industry Association (SNIA)
- TeleManagement Forum (TMF)
- Trusted Computing Group (TCG)

2. Process Description for the Proposed Project

2.1 Project Type: (D - Development)

This is a new standard. It is developed by DMTF and submitted as a complete specification.

2.2 Type of Document

Standard

2.3 Definitions of Concepts and Special Terms

CIM – Common Information Model. The Common Information Model (CIM) is a conceptual information model for describing computing and business entities in Internet, enterprise and service provider environments. It provides a consistent definition and structure of management information using object-oriented techniques. CIM includes expressions for common elements that must be clearly presented to management applications like classes, properties, methods and associations, to name a few.

CIM-OM - Common Information Model Object Manager (CIM Object Manager). A component that handles request routing to object manager adapters, services and providers based on CIM.

PCI SIG – Peripheral Component Interface Special Interest Group (PCI SIG). This organization develops specifications (such as PCI, PCI-X and PCIe) describing component interconnects & mechanisms used in a computer system.

SMASH – The Systems Management Architecture for Server Hardware (SMASH) is a DMTF Management Initiative describing the architecture, protocols & profiles needed to address the server management domain.

SM CLP – Server Management Command Line Protocol Specification. This technology is a command line oriented access protocol based on the DMTF's CIM/WBEM specifications

SMI-S – The SNIA's Storage Management Interface Specification, which has been designated ANSI INCITS 388. This technology leverages the DMTF's CIM/WBEM specifications.

2.4 Expected Relationship with Approved Reference Models, Frameworks, Architectures, etc.

SM CLP is a key component of the DMTF's Systems Management Architecture for Server Hardware (SMASH) Management Initiative.

SM CLP references the Telnet Protocol Specification, RFC 0854 and Telnet Option Specifications RFC 0855 as maintained by the Internet Engineering Task Force (IETF).

SM CLP is expected to be referenced by the ANSI INCITS 388 Storage Management Standard (e.g. SNIA SMI-S) in the future. SM CLP is normatively referenced by the PCI Firmware 3.0 Specification. This is a specification published by the PCI SIG (<http://www.pcisig.com>) which defines PCI BIOS interfaces.

2.5 Recommended INCITS Development Technical Committee (Existing or New)

No new committee is requested. The DMTF is submitting a completed, existing specification. At the end of this process, the DMTF will license the DMTF SM CLP to INCITS for publication. The DMTF may offer future revisions to the specification as needed, using the same Fast Track process.

2.6 Anticipated Frequency and Duration of Meetings

N/A

2.7 Target Date for Initial Public Review (Milestone 4)

The DMTF will submit a completed specification upon acceptance of this proposal.

2.8 Estimated Useful Life of Standard or Technical Report

Indefinite. SM CLP is a technology with significant market potential. Since this was developed by a large consortium, it is expected to have a relatively long life, with revisions planned to extend the standard to additional technologies, features and capabilities.

3. Business Case for Developing the Proposed Standard or Technical Report

3.1 Description

The Server Management Command Line Specification (SM CLP) specification defines a protocol of management commands transmitted over standard character oriented streams. This protocol accesses a Common Information Model Object Manager (CIM-OM) using a human-oriented command set.

SM CLP commands perform a variety of different functions including:

- Configuring systems & their components (devices, services & collections)
- Downloading or uploading firmware to/from systems and components
- Starting, stopping or resetting systems and/or system components
- Controlling property settings for system components.
- Examining the states of systems & system components

Server management applications will use the SM CLP to help them manage heterogeneous servers in a homogeneous fashion.

As an “open systems” specification, the SM-CLP is intended for use across a wide variety of operating systems such as Windows, Linux, Solaris, HP-UX, and AIX, as well as a variety of embedded environments.

3.2. Existing Practice and the Need for a Standard

The need for the standard arises from the need for common access method tools used to manage data center environments regardless of access method, machine state, or vendor.

Currently, only vendor-specific human-oriented access methods are available to perform systems management. These access methods vary both from vendor to vendor and within a vendor’s product line. They also vary dependent on the state of the machine. Finally, the access method can vary between operating systems and between embedded environments. While the access methods may vary, there is still an intersection of features supported by one or more of those access methods that are common to all access methods.

The SM CLP is the culmination of the effort to unify these access methods. The same commands are applicable to both operating system and embedded environments and the commands themselves are not environment dependent. The SM CLP is a human-oriented access method capable of automation using a variety of tools, including scripting environments.

3.3. Implementation Impacts of the Proposed Standard

3.3.1 Development Costs

It is widely believed that development costs will be reduced due to a common interface and standard -- along with cooperation of vendors to develop the standards -- for the following reasons:

- Standards interface specifications are clear and produce more uniform functionality (less work to get to the goal).
- Commonly accepted functionality requires less definition of requirements. Work can start on product functionality sooner.
- Testing and certification is easier due to the possibility of standardized test suites and test and scenarios.
- Quality is higher because there are more opportunities for testing and results are more visible.

3.3.2 Impact on Existing or Potential Markets

- SM CLP will reduce the cost of training IT administrators and make tools easier to use, leading to more customer acceptance of management tools and hence increase the market.
- SM CLP will also allow shorter development times, allowing server management application vendors to ship management applications earlier than they otherwise would.
- Greater interoperability of management tools should encourage IT administrators to more quickly adopt SM CLP-based solutions in their organizations.

3.3.3 Costs and Methods for Conformity Assessment

The DMTF is currently in the process of developing a compliance and interoperability test suite and expected to launch the compliance suite by mid 2007. Conformance assessment can be validated by vendors under this program using the test suite.

3.3.4 Return on Investment

As noted in section 3.3.2, vendor use and customer use of tools that comply with the standard will significantly reduce development and training costs, leading to significantly reduced costs and increased ROI.

3.4 Legal Considerations

3.4.1 Patent Assertions

The proposer is not aware of any patents asserted against this specification.

DMTF members are required to disclose any patent whose essential claims would be infringed upon by implementing the SM CLP document. In addition, any feedback from the public received by the DMTF must also disclose any patent whose essential claims would be infringed upon by implementing the SM CLP document if that feedback was implemented.

3.4.2 Dissemination of the Standard or Technical Report

The proposer is not aware of any IPR assertions that hinder the distribution of this standard.

4. Related Standards Activities

4.1 Existing Standards

The SNIA's SMI-S future support for SM CLP is expected to normatively reference this specification. That would be reflected in the ANSI version of that specification when it has passed INCITS's Fast Track qualification.

There are many de facto and de jure standards that are related to the SM CLP. The DMTF has a number of specifications that directly relate to SM CLP, such as Server Management Managed Element Addressing (SM ME Addressing), SM CLP Mapping Specifications, DMTF Profiles, CIM Infrastructure and Representation of CIM in XML. We are investigating bringing these standards through the fast track process.

In addition, the SM CLP is normatively referenced by the PCI Firmware 3.0 Specification. This is a specification published by the PCI SIG (<http://www.pcisig.com>) which defines PCI BIOS interfaces.

4.2 Related Standards Activity

Related Standards Activity includes the development of the SMI-S specification by the SNIA, which is based on the DMTF's CIM and includes CIM/XML protocol access to the SMI-S profiles. The SM CLP can be used as another access protocol to these profiles.

4.3 Recommendations for Close Liaison.

The DMTF recommends a formal liaison with INCITS Technical Committee T11.

5. Units of Measurement used in the Standard

Not measurement sensitive.