Understanding and Using the New IPMI v1.5 Specification

Tom Slaight
Server Management Architect
Enterprise Platforms Group
Intel Corporation

February 27, 2001
Agenda

- Platform Management Initiative Update
- IPMI 1.5 Architecture and Feature Overview
- IPMI 1.5 Technology Framework
- LAN and Serial/Modem Specific Features
- Related Technologies: SMBus 2.0, PCI Management Bus, and ASF
- Futures
- Summary and Call to Action
Server Management Challenge
Always Available
Platform Manageability

IN-BAND
OEM
MODEM
LAN
ICMB
Mgmt Card

FRU, Asset, SDR
Sensors & Status
Diags & Utilities
Alerting
Mgmt. Software
System Event Log
Recovery Control
Console Redir.

Copyright © 2001 Intel Corporation.
Platform Management Challenge

Always Available

Cross-Platform Manageability

Enterprise Server
Application Server
Mobile
Desktop
Server Appliance
Front End Server
Always Available Cross-Platform Manageability - why?

- Scalable continuity of features
  - Features scale across system types

- Cross platform software
  - Lowers software development costs
  - Enables differentiation ‘up the stack’

- Higher Quality
  - Common interfaces enable ‘knowledge preservation’

- 3rd Party Component availability
  - Lowers platform developments costs
    - Server sensors at ‘Desktop’ prices
Controller and Component News

- Companies creating Baseboard & Peripheral Management Controllers for IPMI
  - Qlogic Corp., Winbond Electronics Corp., Vitesse Semiconductor, and Agilent* are shipping management controllers for IPMI
  - IPMI firmware and SDKs included in offerings

- New Sensor Components target System Management Applications
  - Many options: Offerings from Philips, Analog Devices, TI, National Semiconductor and others*

More in the Server Management Controllers, Sensors & Tools Presentation - 1pm Thursday
New specifications and technologies enable Always Available cross-platform Manageability
IPMI (Intelligent Platform Management Interface)

- Defines common, abstracted, message-based interfaces to intelligent platform management hardware
- Defines common records for describing platform management devices and their characteristics
- Supports OEM differentiation and value added features
- Promoters: Intel, HP, NEC & Dell
IPMI Promoter, Contributor, and Adopter News

- Acer Inc.
- Agilent Technologies GmbH
- Alberta Microelectronics
- American Megatrends Inc.
- Arima Computer Corp.
- ASUSTek Computer, Inc.
- Blue Wave Systems
- Bull S.A.
- Celestica
- CyberGuard Corporation
- Data General Corporation
- Dell Computer Corporation
- Egenera, Inc.
- ElanVital Corporation
- Ericsson UAB
- Evans & Sutherland
- Eversys Corporation
- Exabyte Corporation
- FORCE Computers GmbH
- Fujitsu, Ltd.
- GoAhead Software, Inc.
- HADCO Corporation
- Hewlett-Packard Company
- Hewlett-Packard GmbH
- Hitachi Ltd.
- Hybricon Corporation
- InnoMediaLogic, Inc.
- Intel Corporation
- Interphase Corporation
- InterWorks Computer Products
- Inventec Corporation
- Ipex ITG
- JMC Products
- L-3 Communications Corp.
- Lynux Works, Inc.
- Macrolink, Inc
- Magnetek, Inc.
- Micro-Star International
- Mitsubishi Electric Corp.
- Information Systems Engineering Center
- National Semiconductor Corp.
- NEC Corporation
- Nematron Corporation
- Network Engines, Inc.
- NOCpulse, Inc.
- Olivetti Computers Worldwide
- Open Source Asia
- PEP Modular Computers
- Phoenix Technologies Ltd.
- Praim, Inc.
- Qlogic Corporation
- Radisys Corporation
- Reliance Computer Corporation
- Sanera Systems, Inc.
- SBS Technologies (Industrial Computers GmbH)
- Scenix
- Semiconductor, Inc.
- Siemens AG
- Silicon Graphics, Inc.
- Stratus Computer Systems Ireland Ltd.
- Sun Microsystems
- Super Micro Computer, Inc.
- Symphony Group Intl. Co., Ltd.
- Synergy Microsystems
- Teknor Applicom, Inc.
- T-Netix, Inc.
- Tatung Co.
- Tektronix
- Texas Micro Corporation
- Toshiba Corporation
- Trimm Technologies
- Tyan Computer Corporation
- Universal Scientific Industrial Corp.
- USAR Systems, Inc.
- Vitesse Semiconductor Corp.
- Vividon, Inc.
- Vooha, Inc.
- Winbond Electronics Corp.
- Ziatech Corporation
Server Management Challenge

Always Available
Platform Manageability

IN-BAND

Mgmt Card

ICMB

MODEM

LAN

OEM

FRU, Asset, SDR

Sensors & Status

Recovery Control

Diags & Utilities

Alerting

System Event Log

Mgmt. Software

Copyright © 2001 Intel Corporation.
IPMI 1.5

Goals

● Enable Always Available Manageability
  – Incorporate LAN and Serial/Modem access technology into IPMI
  – Unify LAN and Serial out-of-band access capabilities and protocols

● Synch-up with and support emergent and existing standards
  – PPP
  – DMTF Pre-OS Working Group
  – PCI Management Bus / SMBus 2.0
  – Compact PCI
IPMI v1.5 Announced at Intel Developer Forum February 2001

See IPMI v1.5 Technology Demo and IPMI Components in the Intel Pavilion
Agenda

- Platform Management Initiative Update
- IPMI 1.5 Architecture and Feature Overview
- IPMI 1.5 Technology Framework
- LAN and Serial/Modem Specific Features
- Related Technologies: SMBus 2.0, PCI Management Bus, and ASF
- Futures
- Summary and Call to Action
Example Architecture

- **Baseboard**
  - Mgmt NIC
  - SMBus / PCI Mgmt. Bus
  - I²C / SMBus
  - SENSORs & control circuitry
  - IPMI Messages

- **System Bus**

- **LAN**
  - New
  - MODEM / Serial
  - New

- **Remote Mgmt. Card**
  - Aux. IPMB
  - IPMB

- **ICMB Bridge Controller**
  - ICMB

- **System Interface**
  - System Bus

- **Chassis**
  - Enclosure Mgmt. Controller
    - Monitoring & control circuitry
    - FRU SEEPROM
  - SDR, SEL, FRU
  - NV Store

- **Mgmt. NIC**
  - PCI

- **IPMI Messages**
  - RS-232

- **Monitoring & control circuitry**

**Note:** The diagram illustrates the integration of various components such as NICs, Mgmt. NICs, SMAbus/PCI Mgmt. Bus, SMBus, and SMBus/PCI Mgmt. Bus, all connected through IPMI Messages and monitoring & control circuitry.
IPMI 1.5 builds on proven technology

What stays the same

- No changes to system interface operation
  - KCS, BT, SMIC stay the same
- No change to IPMB or ICMB
- Backward compatible with existing IPMI v1.0
  Commands
  - Sensor commands, FRU commands, SEL/SDR access commands to stay the same
- v1.0 SDRs forward compatible with v1.5
  - New v1.5 field, using reserved bits, to identify which channel a sensor or FRU device is on.
IPMI 1.5

What’s New

- IPMI over LAN
  - Ability to send and receive IPMI messages directly to BMC via LAN

- LAN Alerting
  - Via PET (Platform Event Trap)
  - with optional alert-acknowledge support
What’s New

- IPMI over Serial/Modem
  - with Basic, PPP, and Terminal Mode protocols
- Serial/Modem Alerting
  - with TAP (alphanumeric) or Dial Page (numeric) options
- Callback
  - For Basic or PPP mode
  - PPP Call-back with CBCP option
- Serial Port Sharing
IPMI 1.5

What’s New

- Diagnostics Flags
  - Per DMTF Pre-OS Working Group, plus flags equivalent to our present definition
- Multi-level security with multiple user ‘logins’
- LAN & Serial Call-down Alerting
- Supporting Technologies
  - Extended Messaging Model
  - Platform Event Filtering (PEF)
IPMI Manageability

Shared Features & Functions

• Autonomous Manageability
  – Monitoring and Logging occur independent of host processor(s)
    – Accessible when failures make host-processor unavailable
    – Transparent access during run-time
      – without taking processing time
      – without relying on software agents

• Symmetric Manageability
  – Same capabilities available on supported media
    – IPMB, ICMB, Serial/Modem, LAN
IPMI Manageability

Shared Features & Functions

● All Phase Manageability
  – Supports controllable transitions and clean hand-offs between power-down, pre-boot and run-time management

● Extensible Manageability
  – Supports OEM Extensions & Differentiation
  – Specification framework supports extension to cover new media
IPMI v1.5 puts it all together for “Always Available” Manageability

IPMI Manageability

- Autonomous Manageability
- All-Phase Manageability
- Extensible Manageability
- Always Available Manageability
- Symmetric Manageability
Agenda

- Platform Management Initiative Update
- IPMI 1.5 Architecture and Feature Overview
- IPMI 1.5 Technology Framework
- LAN and Serial/Modem Specific Features
- Related Technologies: SMBus 2.0, PCI Management Bus, and ASF
- Futures
- Summary and Call to Action
IPMI v1.5 Technology

New Core Elements

Extended Messaging

Users, Authentication, & Privileges

Autonomous Actions & Alerting
Extended Messaging

**v1.5 Channel Model**

- Channel numbers identify different BMC ‘Ports’
  - Used to route messages between different interfaces
- Allows for multiple IPMB, LAN, Serial, etc., connections to BMC
  - Up to seven channels supported, plus IPMB and System Interface
  - Increases scalability for Enterprise-class servers
  - Supports Compact PCI applications of IPMI
Extended Messaging

v1.5 Channel Model

● Provides common commands for messaging between channels
  – Unify bridging between IPMB, LAN, Modem/Serial, and local system management software

● Provides common commands for security configuration and control
  – User Names, Passwords, and Privileges
  – Current Privilege Level
  – Privilege Level Limits

Reduces Media-specific Software
Extended Messaging

Sessions

• A session is used for two purposes:
  – As a framework for Authentication
  – To support multiple IPMI Messaging streams on a single channel

• Some channels are session-based, and multi-session – E.g. LAN

• Some may be single-session – E.g. Serial/modem

• Others are session-less
  – e.g. IPMB and System Interface
  – Session-less channels do not have Users or authentication
Extended Messaging

**Sessions**

- A session must be **activated** before it can be used
  - via an *Activate Session* Command

- A session can be terminated (closed)
  - by a *Close Session* command
  - by an inactivity timeout
  - by illegal activity, such as out-of-range sequence numbers
Extended Messaging

Sessions

- Multi-session channels have authenticated packets and a **Session Header**
  - Header separate from encapsulated IPMI Message Data
  - Holds **Session ID** that is used to identify the session once it’s been activated
  - Holds Authentication Type (e.g. MD5)
  - Holds Signature
    - 16-byte Message Authentication Code, Password, or numeric key
  - Holds Session Sequence Number...
Extended Messaging

Session Sequence Numbers

- Multi-session packets have **session sequence numbers**
  - protect against replay attacks
  - distinguish duplicate packets at datalink layer

- Two sets of session sequence numbers:
  - Tracked separately to support different number of outgoing versus incoming packets
  - **Outbound**: From BMC to Remote Console
  - **Inbound**: From Remote Console to BMC
IPMI v1.5 Technology

Key New Elements

- Extended Messaging
- Users, Authentication, & Privileges
- Autonomous Actions & Alerting
Users

- A **User** is a set of information that is used to select the password and privileges for an IPMI Session
  - Users are identified externally by User Name
  - Internally identified via a ‘User ID’
  - Users can be configured on *per channel* basis
    - Can have different sets of users for different channels
- IPMI Passwords are separate from BIOS and Operating System passwords
Users, Privileges, & Authentication

**Users**

Implementation Options

- Implementation picks number of possible Users per channel
- User names can be fixed or configurable
- User privilege limits can be fixed or configurable
- Minimum requirement is one User with fixed name and privileges
  - Options reduce resources required for peripheral controller applications

Options allow implementations to fit the needs of the system
Users, Privileges, & Authentication

Privilege Levels

Four privilege levels determine which commands can be executed:

- **Callback** Level (most restrictive)
  - User can only execute commands to trigger a Callback

- **User** Level
  - Access restricted to status retrieval commands, e.g. SDR read, SEL read, FRU read, sensor readings, sensor status
  - No access to low-level write or bridging functions

- **Operator** Level
  - Full access to IPMI commands and bridging functions, except for configuration commands that could disable communication

- **Administrator** Level
  - Operator capabilities, plus ability to remotely change communication and user configuration options
Privilege Limits determine the maximum privilege level that a User can operate at

- Users have a configurable Privilege Limit
  - Sets maximum privilege level that a User can operate at

- Channels also have a configurable Privilege Limit
  - Overrides User Privilege Limit
  - Allows setting a ‘global maximum’ without having to change individual user’s
Users, Privileges, & Authentication

Authentication

- IPMI Challenge/Response
  - User-specific challenge must be correctly responded to in order to activate a session
  - Following Authentication Algorithm types in the spec:
    - Straight Password, MD2, MD5, OEM, NONE
- ‘Dummy’ Challenge/Response transaction is performed if authentication type is set to ‘Straight Password’ or ‘none’
  - Allows software to use same ‘login’ command sequence regardless of authentication type
Users, Privileges, & Authentication

Authentication options

- **‘Per Message’ Authentication**
  - Each message in session is signed and authenticated
  - Can be turned off to reduce overhead on physically secure / non-shared connections such as serial/modem
  - Can be turned off just for User level commands

- **Link Authentication**
  - Connection authenticated before IPMI messages sent
  - For PPP only. Common PPP link authentication protocols supported - e.g. CHAP, PAP, MS-CHAP
  - Two level security possible
  - One set of User ‘password’ info for link and a different set for User access
Users, Privileges, & Authentication

Access Mode options

Additional channel restrictions based on system phase.

● Disabled
  – Channel unavailable for IPMI Messaging

● Pre-boot only (for serial/modem channel)
  – Channel only available during POST, and when system is powered-down or hard reset. BIOS disables port prior to initiating boot.

● Always Available
  – Mgmt. Connection available during all phases of system operation.
  – For serial/modem, port is disabled or hidden from OS use

● Shared
  – Management connection available during all phases of system operation, and also available for system use
  – For serial/modem, BMC will ‘answer the phone’ if OS does not.
Activating a session

Uses an IPMI Challenge/Response

1. Remote Console issues a `Get Authentication Capabilities` command to the BMC

2. BMC returns Authentication Types (authentication algorithms e.g. MD5) it supports

3. Remote Console issues a `Get Session Challenge` command with User Name, requested Authentication Type, starting outbound sequence number

4. BMC returns challenge string and temporary Session ID

5. Remote Console uses session info, user password, and challenge to generate signed `Activate Session` command to BMC

6. If code verifies, BMC returns Session ID along with the starting inbound sequence number
Example: LAN Session Activation

Discovery
- RMCP PING
  - IPMI Supported
  - RMCP PONG
- Get Channel Authentication Capabilities, Rq
  - Clear, Channel=current
  - Get Channel Authentication Capabilities, Rs
  - Clear, Auth=MD5

Activation
- Get Session Challenge, Rq
  - Clear, Auth=MD5
  - Get Session Challenge, Rs
  - Clear, Challenge Str, temp session ID
  - Authenticated, temp session ID, Outbound Seq, Challenge, MD5( ),
  - Authenticated, Session ID, MD5( )
- Activate Session, Rq
  - Authenticated
  - Activate Session, Rs
  - Set Privilege Level, Rq
  - Authenticated
  - Set Privilege Level, Rs
  - Close Session, Rq
  - Authenticated
  - Close Session, Rs
  - Discovery
  - Activation
  - Active
IPMI v1.5 Technology

Key New Elements

Extended Messaging

Users, Authentication, & Privileges

Autonomous Actions & Alerting
Autonomous Actions & Alerting

Platform Event Filtering

- Generic BMC method for generating a selectable action on a given event
  - Supporting technology for Alerting
- Event Messages matched against entries in ‘Event Filter Table’
- Wildcarding allows multiple events to match one filter
  - E.g. One filter matching all temperature sensor events
  - Another matching only “Chassis Intrusion on Door 1” events
Autonomous Actions & Alerting

Platform Event Filtering

- Each ‘Event Filter’ entry configurable to generate selectable actions:
  - Reset
  - Power Off
  - Power Cycle
  - Diagnostic Interrupt / NMI
  - OEM
  - Alert

- ‘Immediate’ actions take priority over Alerts
Alert Policies

- **Alert Policy Table** holds **Alert Policy Entries**

- A policy entry selects an **Alert Destination**
  - and whether destination will always be used, or used only if previous destination failed

- An **Alert Policy** is a collection of policy entries
  - Each policy identified by a ‘policy number’

- PEF filter entry that triggers Alert action specifies Alert Policy number

- Alert Policy Table can hold more than one policy
Alert Strings

- Some alerts, such as alphanumeric pages, require an Alert String
  - Kept in a configurable ‘Alert String Table’ that is part of the PEF configuration parameters

- Alert String look-up:
  - On Event Filter basis (Event-filter specific)
  - On combination of Event Filter and Destination
Agenda

- Platform Management Initiatives Update
- Platform Management Architecture and IPMI Feature Overview
- IPMI 1.5 Technology Framework
- LAN & Serial/Modem Specific Features
- Related Technologies: SMBus 2.0, PCI Management Bus, and ASF
- Futures
- Summary and Call to Action
LAN Format

- Standards based:
  - 802.3 transport
  - UDP
  - DMTF Pre-OS WG RMCP Packet

- Supports multiple sessions on channel

- Supports per message authentication

Works with common network stacks and tools
LAN Alerts

- Delivered as SNMP Traps
  - Format follows the Platform Event Trap (PET) Format Specification
  - IPMI supports optional *PET Acknowledge* message and retries
Serial/Modem PPP Mode

- Standards based:
  - PPP transport
  - UDP
  - DMTF Pre-OS WG RMCP Packet

- Supports multiple sessions on channel

- High commonality and re-use with LAN Software

Can leverage OS support for PPP/UDP - at cost of overhead
Serial/modem Basic Mode

- Minimal Framing
  - Simple escaping and START/STOP characters
- Uses IPMI challenge/response for authentication
- No per-message authentication
- No support for multiple sessions

Low overhead, but requires more IPMI-specific communication
Serial/modem Terminal Mode

- Supports small number of text commands
  - Reset, Power On/Off, Diagnostic Interrupt
  - Set Boot Flags
  - Get Overall Health Status

- Simple line editing support

- IPMI messages encoded as “Hex-ASCII”

- Works with Microsoft* ‘Whistler’
  Headless specification

- Intended for ‘glass house’ environment
  - Limited authentication (simple password)
  - No per-message authentication
  - Single session

Transition vehicle for legacy management environments
Serial/Modem Alerts

- **Dial Page**
  - BMC uses modem to dial ‘touch tones’ for numeric paging

- **TAP Page**
  - BMC dials a TAP (Telocator Access Protocol) v1.8 paging service and delivers an alphanumeric page

- **PPP Alert**
  - BMC calls a PPP Account and delivers a PET format SNMP trap to designated IP Address
Serial/Modem Callback

- Three types of Callback Supported
  - Basic Mode Callback
  - PPP Mode Callback
    - uses IPMI commands to initiate callback
  - PPP CBCP Callback
    - uses Microsoft* CBCP (Callback Control Protocol)

- Callback Privilege level
  - User can only initiate a callback
IPMI Remote Access

Serial Port Sharing

- Enables sharing serial connection between BMC and software/BIOS
  - BMC controls switch via command or ‘snooping’ for data patterns
  - Supports Microsoft* ‘Whistler’ escape sequences
Agenda

- Platform Management Initiative Update
- IPMI 1.5 Architecture and Feature Overview
- IPMI 1.5 Technology Framework
- LAN and Serial/Modem Specific Features
- Related Technologies: SMBus 2.0, PCI Management Bus, and ASF
- Futures
- Summary and Call to Action
Inter-related Specifications

What are they?

How do they relate to IPMI?
Alert Standard Forum

- Specification from DMTF Pre-OS Working Group
- Applies to OS-absent management space
  - Does not replace existing OS-present management HW / SW specifications.
- Defines interfaces to enable interoperable alerting solutions from NIC and System vendors
- Specifies supporting requirements for alerting-capable systems, NICs and sensor devices
- Defines extensible architecture to support future alerting solutions and OEM differentiation
ASF Specification Elements

- **LAN Alerts Format**
  - Provides common SNMP trap for platform events

- **RMCP Network Protocols**
  - Remote Management and Control Protocol
  - UDP datagram based

- **Alert Transmitting NIC behavior**
  - Alerting Device Polling responsibilities
  - Required RMCP support
ASF Specification Elements

- Supporting SMBIOS structures and ACPI Control Method interfaces
  - Enable system software to discover ASF interfaces
  - Reports addresses of ‘legacy’ SMBus devices

- Management SMBus interfaces
  - To alerting NICs
  - To ‘legacy’ poll-able SMBus devices
  - To ASF Sensor Devices...
ASF Sensor Devices

- Specification of common SMBus interface for Sensor Devices
  - Provides commands for retrieving event status in a standardized, abstracted format
  - Provides commands for providing asynchronous notification w/o requiring SMBAlert line
    - Includes ability to send asynchronous notification of events to SMBus host controller
  - Data can be easily mapped to a Platform Event Trap or IPMI Event

- Designed to work with PCI Management Bus...
PCI Management Bus

- Provides SMBus connection across the PCI slots
  - 3.3 V Bus with timing and electricals per SMBus 2.0 ‘high power’ specification
  - Remains operative on standby power

- Uses SMBus 2.0 Address Resolution Protocol (ARP) to assign addresses to Add-in cards
  - Fixed address devices can still be used on baseboard
PCI Management Bus

‘ASF’ desktop application

LAN Controller A

LAN Controller B

PCI SMBus

SMBus Host Controller

System Bus

NIC(s) Poll Sensor Devices & send alert when event detected

ASF Sensor Device

ASF Sensor Device

System Management Software can poll Sensor Devices during run-time
PCI Management Bus

Server/IPMI application

BMC Polls Sensor Devices

Events Logged

BMC ‘pushes’ events out to NIC(s)

ASF Sensor Device

SEL

LAN Controller B

LAN Controller A

PCI SMBus

System Bus

System Management Software accesses abstracted sensors and logged events during run-time
IPMI, SMBus 2.0, & PCI Management Bus Synergy

- IPMI support is discoverable via SMBus 2.0 UDID (Unique Device ID)
- IPMI v1.5 supports SMBus and PCI Management Bus as channel types
- BMC can serve as SMBus Host controller
  - Non-overlapping protocols enable one controller to simultaneously receive and discriminate ‘SMBus’ and ‘IPMI’ messages

IPMI, SMBus, & PCI Management Bus specifications are complementary
IPMI/ASF Synergy

- Shared management packet format
  - IPMI uses ASF ‘RMCP’ packet format for IPMI over LAN and PPP and for LAN discovery

- Common LAN Alert Format
  - Both use IPMI PET (Platform Event Trap) Specification for SNMP Traps

- Common sensor and event type enumerations
  - ASF uses IPMI enumerations for Alerts and Sensor Device Status

- Common boot control flags
  - IPMI uses superset of ASF boot flags

- Common BIOS error & progress codes
  - IPMI uses ASF BIOS Error and Progress codes

IPMI and ASF are Complementary
Agenda

- Platform Management Initiative Update
- IPMI 1.5 Architecture and Feature Overview
- IPMI 1.5 Technology Framework
- LAN and Serial/Modem Specific Features
- Related Technologies: SMBus 2.0, PCI Management Bus, and ASF
- Futures
- Summary and Call to Action
Platform Management Futures

- More links with ASF with proposed ASF ‘2.0’ specification
  - Targeting support for ‘pass-through’ messaging on PCI Management Bus
- Enhanced PCI Management Bus support
- H/W-independent System Interfaces
  - EFI & ACPI-based I/F’s under consideration
- InfiniBand* H/W Management with IPMI

*All trademarks and brands are the property of their respective owners
IPMI over InfiniBand*

Provides Always Accessible Manageability via InfiniBand media

- For host system & peripheral chassis as well as InfiniBand module management
- IPMI messaging supported as a message class in InfiniBand Hardware Management specification

More to come....

*All trademarks and brands are the property of their respective owners
Agenda

- Platform Management Initiative Update
- IPMI 1.5 Architecture and Feature Overview
- IPMI 1.5 Technology Framework
- LAN and Serial/Modem Specific Features
- Related Technologies: SMBus 2.0, PCI Management Bus, and ASF
- Futures
- Summary and Call to Action
Summary

● New initiatives and specifications enable competitive server management features

● IPMI v1.5 technology provides the foundation for Always Available Manageability

● IPMI will continue to evolve to support new interfaces, capabilities, and standards
Where to Get More Info

IPMI Web Site

- Latest IPMI Specifications & Errata
  - Updated document revisions
- FAQ and Integration Guides
- Mailing List
- Presentations
- Tools
- IPMI Conformance Test Suite

developer.intel.com/design/servers/ipmi
Where to Get More Info
ASF, SMBus 2.0, and PCI Management Bus

- DMTF Pre-OS Working Group (ASF specifications)
  - Specification available to DMTF (Distributed Management Task Force) members
  - Membership info: www.dmtf.org

- SMBus 2.0
  - Published by the SMBus Working Group of the Smart Battery Systems Implementers Forum (SBS-IF)
  - Specification available from www.smbus.org

- PCI Management Bus (PCI Specifications)
  - PCI SIG (Peripheral Component Interconnect Special Interest Group): www.pcisig.com
Call to Action

Get the specs and deploy IPMI 1.5 in your new designs
Understanding and Using the New IPMI v1.5 Specification
Tom Slaight
Intel Corporation

Questions?

Please remember to turn in your session survey form.